Vascular Pattern Recognition

And its Application in Privacy-Preserving Biometric Online-Banking Systems

Daniel Hartung

Thesis submitted to Gjøvik University College
for the degree of Doctor of Philosophy in Information Security

2012

Vascular Pattern Recognition

Faculty of Computer Science and Media Technology
Gjøvik University College

Vascular Pattern Recognition and its Application in Privacy-Preserving Biometric Online-Banking Systems / Daniel Hartung
Doctoral Dissertations at Gjøvik University College 2-2012
ISBN: 978-82-93269-01-4
ISSN: 1893-1227

To those I love, to life and to science.

Declaration of Authorship

I, Daniel Hartung, hereby declare that this thesis and the work presented in it is entirely my own. Where I have consulted the work of others, this is always clearly stated.

Signed:

(Daniel Hartung)

Date:

Summary

Authentication is a key building block in security systems and many applications to prevent access to information, services, assets or locations for non-authorized persons or processes. Common methods based on knowledge or possession are however not scalable and practical in human-to-machine communication. Passwords are difficult to remember if chosen appropriately and distinct for the increasing number of different applications, they can be forgotten, spied-out and passed on to other persons. Tokens, like keys or cards, can be forwarded, stolen, lost or destroyed in a similar way. Biometric systems, as the third factor, use body properties to allow for convenient authentication. The main difference lies in a strong link between electronic identifier and physical identity which leads to desirable properties like non-repudiation, difficulty of replication, theft and loss. On the other hand this may challenge privacy and may lead to identity theft, disclosure of sensitive information and profiling if digital biometric identifiers are exposed.

Vascular biometric systems use information about the blood vessel structures inside the hand area (finger, palm or wrist) and overcome problems of latent prints (as with fingerprints, DNA) or unnoticed acquisition on distance (as with face) and liveness issues. Still, the before mentioned problems of biometric systems exist and privacy enhancing technologies (PETs) were introduced to overcome them. Some PETs enable revocation of biometric references, unlimited references from the same biometric source and unlinkability between the generated templates. In addition the sensitive data is sealed. In order to utilize PETs like the helper data scheme (HDS) some requirements, like a fixed-length structure of the feature representation, have to be met. The goal of this thesis is to meet those requirements and to make use of the HDS. In addition we strive for the application in real-life scenarios.

One of the main applications that we identified for such a system is online banking. Those systems, as of today, are secured with authentication systems based on knowledge or possession and constantly a vulnerable target of criminal activity. Since the recent systems are mostly broken, new alternatives are needed. So we designed a protocol based on the HDS that merges information about online transactions with secure biometric references to enable secure online banking with the desirable properties of biometric systems: hence the name BTAP – biometric transaction authentication protocol.

The work on representing patterns compatible to the HDS has been achieved for fingerprint-based systems using spectral minutiae. Therefore we designed algorithms to extract minutiae to represent the topology of the blood vessel network with its branch and end points. Transforming the location and orientation information of the feature points into spectral vein minutiae leads to a translation invariant, fixed-length representation that allows for alignment-free scale and rotation corrections. Those properties are especially important for hygienic, contact-free sensors without guidance for the hand or finger.

A performance evaluation revealed that the transformed spectral vein minutiae lead to low recognition errors for sub-modalities including palm, palm dorsal (back of hand) and wrist vein patterns. In a multi-reference scenario the performance for quantized spectral minutiae based on palm vein patterns and a simple Hamming distance could even be improved to a perfect separation between genuine and imposter attempts. The quantized, binary feature vectors are utilized in the first stages of the HDS, they are very compact and could also be used for extremely fast comparison systems or for biometric indexing.

In conclusion our work shows that vascular patterns can be transformed into high-

performance representations meeting the requirements of the privacy-enhancing HDS that is the core for the proposed online banking protocol BTAP. After solving issues with the reproducibility of feature vectors, we will be able to combine vein patterns with BTAP to overcome drawbacks of biometric systems to perform secure, convenient, affordable and user accepted biometric online banking transaction authentication.

Bringing the work into a larger perspective, we can state that BTAP is an innovative instance where a biometric system is shifted from a binary authentication decision-making scheme to an integral part of an abstract security protocol. The combination of data from the application with keys released from biometric templates opens new possibilities and represents a recent paradigm shift in biometric systems. General digital biometric signature schemes and biometric message authentication primitives with a strong relation to a natural person are the next step.

Acknowledgments

NISlab, the Norwegian Information Security laboratory at Gjøvik University College, hosted me for the last four years and supported me to conduct my PhD project leading to this dissertation.

I want to express my gratitude towards my supervisor and mentor Christoph Busch. His enthusiasm about biometric research in particular and about life in general was impressive and inspiring. He motivated and guided when help was needed, but also gave the freedom to explore and to grow when it was time to do so. Without him this work would have been impossible in many ways.

Many thanks to my second supervisor Stephen Wolthusen, the evaluation committee members Bernadette Dorizzi, Raymond Veldhuis and Patrick Bours as well as to my friend Kalman Graffi for their valuable feedback on the dissertation and the project.

It was a time of ups and downs from a professional and personal perspective, one perceived lifetime compressed into few months. I learned many things and forgot even more. However, there are those things that will last and that will not be forgotten: the support from my fellow PhD students Anika, Ctirad, Danish, Gabriele, Goitom, Guoqiang, Hai, Lisa, Mark, Martin, Mohammad, Soumik, Steven, Sukalpa and Takashi, from my co-workers Bian, Davrondzhon and Raghavendra and my office mate Knut, from the professors and postdocs at NISlab and the colleagues at the Norwegian Color Research Laboratory. I will remember the nights working in the University, the coffee and ping-pong breaks, the international cooking sessions, outdoor adventures and discussions about work and life. A special thanks also to all participants of the data collection GUC45, who hung on and gave my research a foundation and a human touch. Furthermore I was in the lucky situation to supervise Anika, Jan, Jesper, Martin and Sophie who were excellent students and who taught me a lot.

During the project I was privileged to cooperate with partners from industry and academics. Many thanks to Takashi Shinzaki (Fujitsu Laboratories Ltd.) and Hisao Ogata (Hitachi-Omron Terminal Solutions, Corp.) and their co-workers for the support. The research stay with Fujitsu Laboratories Ltd. in Japan was fascinating, inspiring and refreshing. Many thanks also to the academic partners and co-authors of our publications: to Haiyun Xu for insights into the spectral minutiae approach, to Martin Drahansky (Brno University of Technology) for the start-up support, to Rasmus Larsen (Danmarks Tekniske Universitet), to the colleagues of the Fraunhofer Institute for Visual Computing (IGD) for their support, to Nanyang Technological University for sharing the vein databases and for Raul Sanchez-Reillo, Oscar Miguel Hurtado and Jaime Uriarte-Antonio (University Carlos III de Madrid) for hosting me in Spain and sharing their knowledge and data. There, I did not only find new ideas and motivated researchers but also friends and eventually my destiny.

I want to thank my family and my friends for always being there for me and for supporting me to follow my dreams. Finally, I want to thank Noelia for enduring this time, for standing on my side and for giving meaning to many things.

Contents

List of Figures

List of Tables

Part I

Overview

Chapter 1

Introduction

1.1 Motivation

Authentication is key in our information society. In order to access services, assets, physical locations or information a decision is needed to whether a subject is authorized to do so. It is not feasible to manually recognize and authenticate individuals in large-scale, automated systems. The well-established methods for automatic authentication based on knowledge and possession are being challenged during the last decades by biometric systems. The main difference lies in the bijective relation between electronic identifier and physical identity. This leads to several interesting properties like non-repudiation, difficulty of replication, theft and loss.

Biometrics offer great advantages over traditional authentication methods, however the relation between digital representation and physiological or behavioral body properties challenges privacy. The potential for misuse is immanent. Criminals can use it for identity theft and profiling, governments can use the technology for controlling the population. Therefore special care has to be taken when designing systems using biometric data. In many cases raw data contains medical information: the data itself has to be treated as private and highly sensitive. For those reasons we propagate the incorporation of security features and privacy protection as early as possible during the design phase of the applications and the biometric pipelines.

Nowadays biometric systems are commonly based on fingerprint or 2D-face information mainly due to historical, financial and user-convenience considerations. However, the sensors of these systems can in many cases be easily circumvented with fake artifacts; liveness and fake detection are not trivial. Furthermore the biometric information must be considered public, since face images can be easily acquired on a distance if not available in the seemingly non-disintegrating "memories" of the Internet. Fingerprints on the other hand are left unintentionally on surfaces of objects throughout that we touch in everyday life. It is a trivial task, and widely utilized in crime investigation, to collect those latent prints. Those two modalities were by far researched most and hence are considered mature regarding recognition performance and will continue to be utilized mainly in low-cost and multimodal systems.

Consequently the biometric research community made efforts to find new modalities that overcome these drawbacks. One approach, that is only possible due to recent technological developments, is to penetrate unintrusive into the human body and gather information from there. Hidden to the naked eye and resilient to the latent copy problem, vein patterns were discovered to be useful in biometric authentication.

Commonly, vein patterns from the backside of the inner eye (retina recognition) and vein patterns from the limbs are distinguished. The latter is referred to as vascular pattern recognition or vein recognition, the information originates mostly from the hand area and is the focus of this work. We distinguish four sub-modalities: finger, palm, hand dorsal and wrist vein biometrics. Our goal is to improve the recognition performance of vein patterns from different hand-based modalities and most importantly to enhance the privacy properties utilizing privacy enhancing technologies (PETs) to overcome general problems of biometric systems. How such an enhanced biometric system can be utilized as authen-

tication scheme without the need for storing sensitive data is investigated for one specific use case: the authentication of online banking transactions.

1.2 Goals

The initial goals following the motivation are summarized in the following. They are transformed into more concrete research questions found in Section 1.3. We want to select a biometric modality that overcomes latent copy, and distance-acquisition problems. The selected modality has to be analyzed for weak points regarding privacy and approaches solving potential privacy and data storage problems have to be identified. The design and implementation of a biometric subsystem based on the selected modality that satisfies the requirements of the identified privacy protection approach is our main goal. An evaluation of the biometric performance of the proposed biometric subsystem shall prove the applicability. Furthermore we want to find one or more realistic application scenarios with real-life impact that can make use of such a privacy-enhanced biometric subsystem. We want to design a modality-independent system for improving the application scenario. The formal security features and proper functionality of the system has to be proven.

1.3 Research Questions

The following questions have evolved during the project from the goals defined earlier. They form the red line of this dissertation:

Q1: Are there privacy issues arising with vascular biometric systems and can technical solutions be utilized to protect the privacy of data subjects?

Q2: Are there practical scenarios that benefit from such a system? Can protocols be designed that make use of state-of-the-art template protection schemes?

Q3: Is it possible to design a single algorithm for multiple sub-modalities of vascular pattern recognition resulting in high recognition rates? Can the problem of vascular pattern recognition be reduced to other, well-known (biometric) problems? Can the requirements on the algorithm of state-of-the-art template protection schemes be met?

Q4: Can the biometric performance – besides the fake resistance and liveness detection capabilities – be increased with multi-sensor and/or multimodal approaches?

Figure 1.1 indicates the relation between posed research questions and published articles. All articles highlighted in bold letters are included in the thesis.

1.4 Structure of the Dissertation

This thesis consists of three parts: the introduction in Part I; the research papers in the main Part II and additional work less tightly related with the research questions as well as a brief introduction to biometric systems and our database can be found in Part III.

After a short introduction to the state of the art in Chapter 2 we continue in Chapter 3 to clarify the approach towards our goals and our contributions to the research questions. The main part includes a motivation for privacy protection in vascular biometrics (Chapter 4), preparative papers on contrast in vascular images (Chapter 5) followed by an approach for quality assessment of biometric vein samples (Chapter 6). Feature point extraction from vein skeletons is presented in Chapter 7. A feature extraction and comparison approach based on the vein skeleton structure and spatial distance is given in Chapter 8. The main feature extraction pipeline is introduced in Chapter 9. As contribution to multimodal systems a feature extraction method for finger knuckles is introduced in Chapter 10. The following Chapters 11 and 12 describe the biometric transaction authentication protocol.

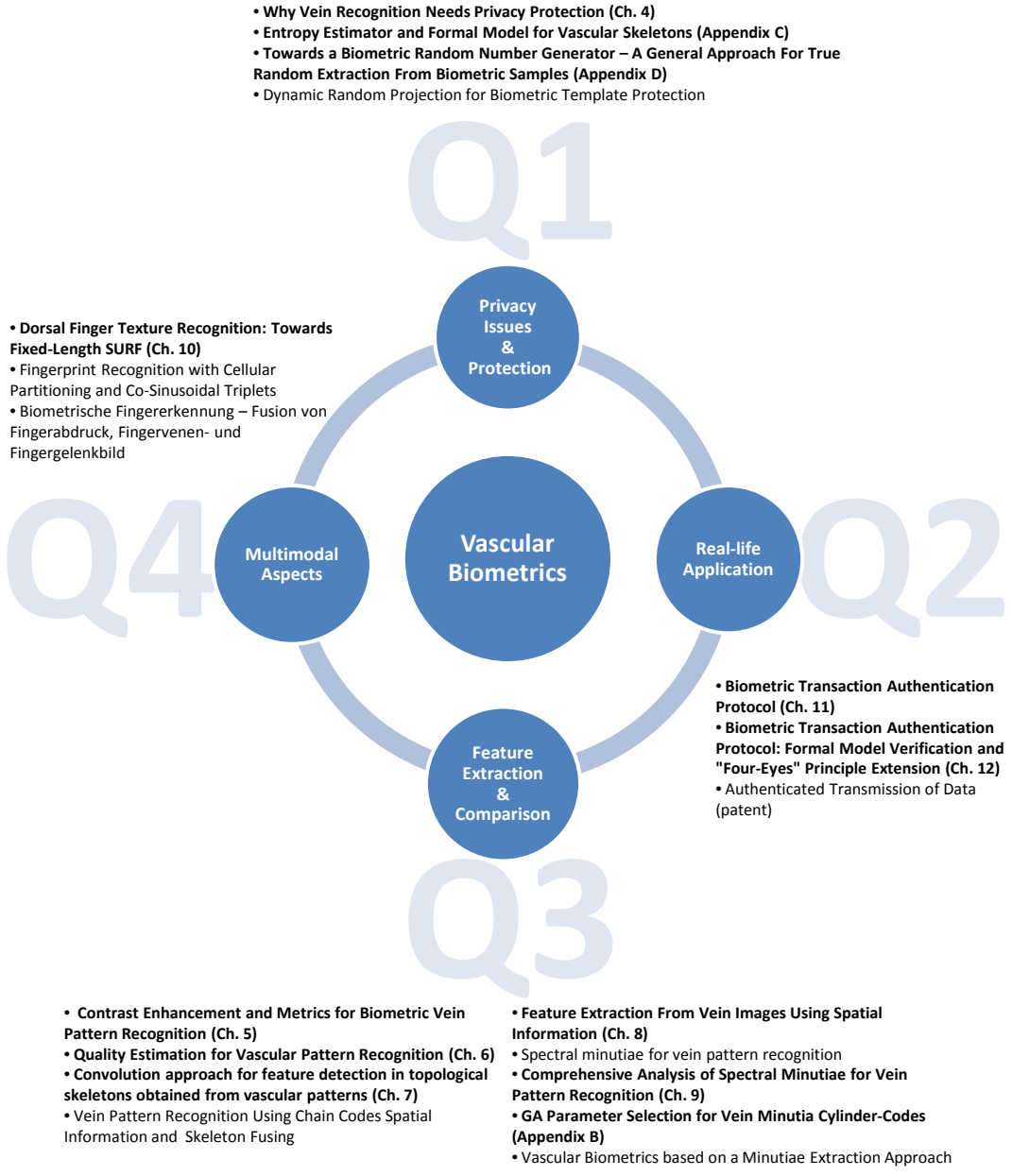


Figure 1.1: Overview of this PhD thesis: research question clusters Qx and related articles (bold = enclosed in Parts II and III).

In Part III a short introduction into biometric systems can be found (Appendix A), an additional feature extraction approach for vein minutiae is described in Appendix B. Interesting for privacy protection schemes, an approach towards the estimation of entropy in vascular skeletons is given in Appendix C. An approach towards random number generation from biometric information e.g. for nonces in security protocols can be found in Appendix D. The multimodal dataset gathered during the project is described in Appendix E. A mapping from the chapters into functional blocks of a biometric pipeline is shown in Figure 1.2.

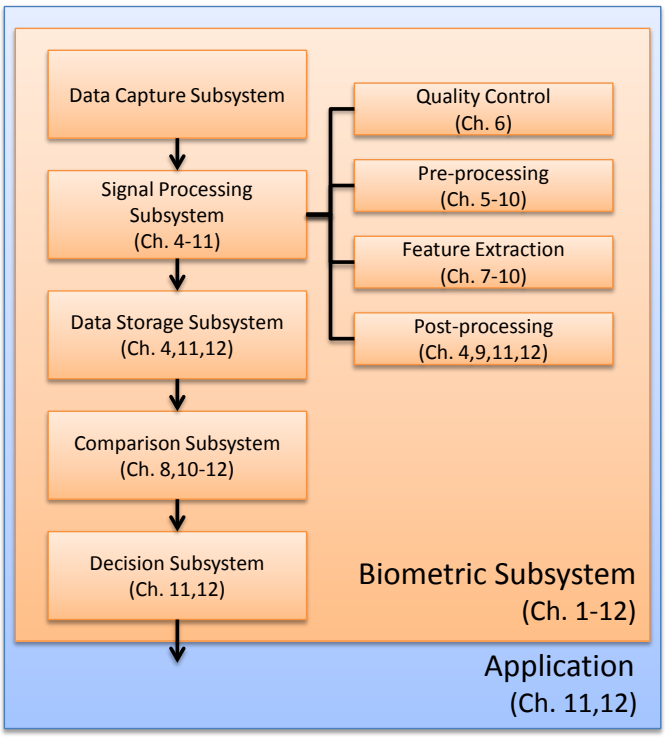


Figure 1.2: Mapping of chapters into biometric pipeline.

1.5 List of Publications

Attached Research Articles

- [70] HARTUNG, D. Entropy estimator and formal model for vascular skeletons. In Biometric Measurements and Systems for Security and Medical Applications(BIOMS), 2011 IEEE Workshop on (September 2011), pp. 1-5.

- [71] HHARTUNG, D., AND BUSCH, C. Why vein recognition needs privacy protection. In Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 09) (September 2009), pp. 1090-1095.

- [72] HARTUNG, D., AND BUSCH, C. Biometric transaction authentication protocol. In Proceedings of the 2010 Fourth International Conference on Emerging Security Information, Systems and Technologies (Washington, DC, USA, 2010), SECURWARE 10, IEEE Computer Society, pp. 207-215.

- [74] HARTUNG, D., AND BUSCH, C. Biometric Transaction Authentication Protocol: Formal Model Verification and "Four-Eyes" Principle Extension. In LNCS 7126, Financial Cryptography and Data Security (2012).
- [75] HARTUNG, D., AND KÜCKELHAHN, J. Dorsal finger texture recognition: Investigating fixed-length surf. In Proceedings of the IEEE International Conference on Systems, Man and Cybernetics, Seoul, Korea, October 14-17, 2012 (2012).
- [76] HARTUNG, D., MARTIN, S., AND BUSCH, C. Quality estimation for vascular pattern recognition. In Hand-Based Biometrics (ICHB), 2011 International Conference on (November 2011), pp. 1-6.
- [78] HARTUNG, D., OLSEN, M. A., XU, H., NGUYEN, H. T., AND BUSCH, C. Comprehensive analysis of spectral minutiae for vein pattern recognition. In IET Biometrics (March 2012), vol. 1, pp. 25-36.
- [80] HARTUNG, D., WOLD, K., GRAFFI, K., AND PETROVIC, S. Towards a biometric random number generator - a general approach for true random extraction from biometric samples. In BIOSIG (2011), pp. 267-274.
- [166] OLSEN, M., HARTUNG, D., BUSCH, C., AND LARSEN, R. Convolution approach for feature detection in topological skeletons obtained from vascular patterns. In IEEE Symposium Series on Computational Intelligence 2011 (April 2011).
- [168] OLSEN, M. A., HARTUNG, D., BUSCH, C., AND LARSEN, R. Contrast enhancement and metrics for biometric vein pattern recognition. In Advanced Intelligent Computing Theories and Applications, vol. 93 of Communications in Computer and Information Science. Springer Berlin Heidelberg, 2010, pp. 425-434.
- [178] PFLUG, A., HARTUNG, D., AND BUSCH, C. Feature extraction from vein images using spatial information and chain codes. Information Security Technical Report, (2012).

Additional Research Articles

- [73] HARTUNG, D., AND BUSCH, C. Biometrische Fingererkennung - Fusion von Fingerabdruck, Fingervenen- und Fingergelenkbild. In 12. Deutscher IT-Sicherheitskongress des BSI: Sicher in die digitale Welt von morgen (10.-12. Mai, 2011), SecuMedia-Verlag.
- [77] HARTUNG, D., OLSEN, M. A., XU, H., AND BUSCH, C. Spectral minutiae for vein pattern recognition. In Biometrics (IJCB), 2011 International Joint Conference on (October 2011), pp. 1-7.
- [79] HARTUNG, D., PFLUG, A., AND BUSCH, C. Vein pattern recognition using chain codes spatial information and skeleton fusing. In Sicherheit (2012), pp. 245-256.
- [85] HIRZEL, J., HARTUNG, D., AND BUSCH, C. Fingerprint recognition with cellular partitioning and co-sinusoidal triplets. In BIOSIG (2010), pp. 109-114.
- [228] URIARTE-ANTONIO, J., HARTUNG, D., PASCUAL, J., AND SANCHEZ-REILLO, R. Vascular biometrics based on a minutiae extraction approach. In Security Technology (ICCST), 2011 IEEE International Carnahan Conference on (October 2011), pp. 1-7.
- [270] YANG, B., HARTUNG, D., SIMOENS, K., AND BUSCH, C. Dynamic random projection for biometric template protection. In Biometrics: Theory Applications and Systems (BTAS), 2010 Fourth IEEE International Conference on (2010), IEEE, pp. 1-7.

International Patents

- [21] BUSCH, C., AND HARTUNG, D. (EN) AUTHENTICATED TRANSMISSION OF DATA, June 2011. (WO/2011/063992).

Chapter 2

State of the Art

This chapter gives background information about vascular hand pattern recognition. In order to qualify as a biometric modality, every system can be assessed against several desirable criteria (derived from [105]), which are:

- Universality: the characteristic should be covered by the whole population
- Uniqueness: the characteristic is unique and not determined solely by the genome
- Performance: reliable differentiation between individuals
- Permanence: the characteristic should be time-invariant
- Collectability: the characteristic can be measured
- Acceptability: system is accepted by users
- Circumvention: system is difficult to spoof

Nadort presented in 2007 [163] possibilities and limitations of hand vein patterns as biometric modality and addressed the mentioned criteria. A management-view introduction to vein recognition can be found in [253] published in 2010. The International Organization for Standardization (ISO) defined a vascular biometrics data interchange format in [104].

We will discuss in the following mostly about the physiological background leading to the observable patterns, the imaging technologies, liveness detection capabilities and privacy issues that arise with the use of vascular pattern-based biometric systems.

2.1 Physiological Background

2.1.1 Cardiovascular System

The circulatory system consists of the cardiovascular system and, depending on the definition, includes also the lymph system. It can be found in humans and many animals, as it is the basis of vascular pattern recognition it is described here based on [211, 252]. Its main function is to maintain homeostasis – a constant set of conditions within cells. It transports oxygen, nutrients, minerals, enzymes, hormones and other substances to every cell in the body for storage or consumption. Metabolism residuals are carried away for excretion or recycling. Furthermore heat is regulated utilizing the cardiovascular system reaching all parts of the body. It also takes an important role in the immune system.

Two circles can be identified within the cardiovascular system, both are connected and powered by the heart, in principle a complex pump structure of valves and muscles. The *pulmonary* circulation loops from the heart to the lungs. In the blood vessels of the lungs oxygen-depleted blood is re-oxygenized and carbon dioxide, a residue of the metabolism, is released into the environment. The *systemic* circulation loops from the heart to all other parts of the body to maintain homeostasis. As a subsystem, the *coronary* system, maintains the heart itself.

Within the systemic loop, oxygen-saturated blood is carried from the heart through a network of blood vessels to all body regions and back towards the heart – to be re-oxygenized in the pulmonary system and fed back into the systemic loop. The structure and properties of the vessels change with the distance to the heart, the blood within the systemic loop passes the heart into arteries with thick vascular walls, fast flowing and with high pressure, later it branches out into arterioles and finally into numerous thin-walled, semi-permeable capillaries where substances and liquids are exchanged between the slow flowing blood and the tissue. Post-capillary venules funnel the low-oxygen blood back into venules that are also utilized to store blood adapting the diameter of these vessels. The venules stream into veins that finally transport the blood back to the heart again – the circle is closed.

Veins are separated in two groups: superficial (cutaneous) and deep veins. The superficial veins are located beneath the skin and transport the blood towards the deep veins that are commonly covered with connective tissue.

2.1.2 Veins and Arteries

Major differences exist between veins and arteries (Figure 2.1). The three layers constituting the blood vessel walls (endothelium, muscle coat, adventitia) are of different size, the smooth muscle cells of the arterial wall is thicker and stronger. In this way arteries are able to handle the high pressure blood stream from the heart (typically around 120mmHg/80mmHg for systole and diastole). Vein walls are thinner and more flexible in order to adapt to the stored blood volume. Valves prevent the back-flow of the low pressure blood stream ($\sim$10-15 mmHg). The diameter is larger than those of comparable paired arteries, thus offering a larger volume. Most of the blood volume is located in the systemic veins ($\sim$61%), only $\sim$7% in the capillares, 11% in the arteries, 9% in the heart and 12% in the pulmonary circle. The estimated length of the capillary network is enourmous (around 40000 km), every capillary has an inner diameter of around $8\mu m$ (comparison: hair diameter $\sim 100\mu m$), just enough to have hemoglobin pass through [252].

Veins are generally located closer to the proximity of the skin than arteries. One possible explanation is that superficial injuries damaging vessels carrying low pressure blood result in less blood loss which is advantageous. Another possible explanation is based on advantages for thermal regulation.

2.1.3 Development of Blood Vessels

Interesting and relevant for the biometric vein recognition is the development of cardiovascular structures, since they form the basis for vascular pattern recognition. During *ontogenesis* (development of an organism), in the early stages of the prenatal development, typically in week 3-4 after fertilization (week 5-6 of pregnancy), the early circulatory system has developed and the heart begins to contract. The early circulatory systems significantly and abruptly changes with birth and the separation in two different circles is started. Since support of oxygen and nutrients through the placenta and the umbilical vein is no longer available, the lungs of the newborn have to work on their own for the first time to saturate the blood with oxygen. To achieve this, the *ductus arteriosus*, a shortcut between the aorta and the pulmonary artery, needs to be closed within the first postnatal days. A shortcut from the right atrium to the left one, the *foramen ovale* is also closed soon thereafter. In addition, the umbilical vein, supporting the fetus with oxygenated blood from the *placenta* is closed. Other than that, the main arteriovenous structures remain unchanged thereafter.

The process of the emerging or the genesis of blood vessels itself is complicated and still not fully understood. Persson et al. published a review article on this issue [176]. They state that three categories of vessel growth/emerging are commonly distinguished:

- *Vasculogenesis*

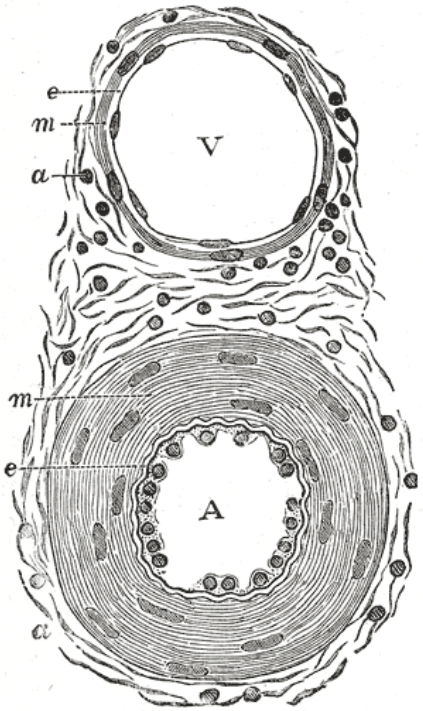


Figure 2.1: Sample transverse section through blood vessels. V: vein, A: artery. e: endothelium, m: muscle coat, a: adventitia, the connective tissue for anchorage in environment (Figure 448 in [63]).

- *Angiogenesis*
- *Arteriogenesis*

Vasculogenesis describes the process of the formation of new blood vessels during *ontogenesis*. The formation of this primary network is mostly genetically determined. The capillarization of the network is referred to as *angiogenesis* and is triggered by metabolic processes to guarantee oxygen-support of new-grown tissue. Arteriogenesis however is defined as the outgrowing of existing blood vessels and is influence by *hemodynamics* – the dynamics of the blood flow. There are many parameters to be considered like e.g. the geometry and elasticity of the vessel, the blood pressure and flow speed, additionally the composition of blood makes *hemodynamics* difficult to predict, seemingly leading to chaotic growth behaviour of the vessels.

Another review article [52] summarizes the current understanding of the emergence of precursor cells as the basis of the primary vascular plexus and the molecular mechanisms that control the development and the differentiation of the different blood and lymphatic vessels.

2.1.4 Blood

The composition of blood is well understood, it is a composition of fluid *plasma* and cellular parts. The largest proportion of cells in the blood are with 99% red blood cells (*erythrocytes*). The proportion of cellular parts of the blood is defined as *hematocrit*, it is changing from birth on, leveling at about 40% for females and 45% for males. Erythrocytes consist of the protein *hemoglobin* surrounded by a plasma membrane. Fetal *erythrocytes* differ from those of adults, they contain a nucleus and different types of hemoglobin (HbF). Adult blood

contains less than 1% of HbF, the majority of hemoglobin is of type A (HbA). Hemoglobin has the property of binding oxygen with its iron atoms (Fe++), in this way most of the oxygen needed for the metabloism is transported in the blood to the tissues. Oxygen-saturated blood in the systemic ateries has a bright-red color due to the oxyhemoglobin (HbO_2), oxygen-depleted blood in the systemic veins has a darker, violet color due to the deoxyhemoglobin (Hb). The other one per cent of cellular parts in the blood are mainly *thrombocytes* for *hemostasis* and white blood cells (*leukocytes*) for immune system support.

The complexity of the blood vessel patterns can further be understood when investigating two additional phenomena: i) redundancy and reconnection is an evolutionary principle that also applies to blood vessels. It prevents failure of necessary blood flow (infarct) to and from body tissue and therefore increases probability for survival in case of damage of parts of the circular system. ii) Arteriovenous *anastomosis* instead describes the principle of connections between arterioles and venules. The reason being that a maximal blood supply of all body parts is not possible at the same time. These shortcuts are being utilized for blood regulation and can be closed to route blood flow through the capillaries or opened for shortcut.

2.1.5 Skin and Blood Vessels

The major veins of the upper extremity are depicted in Figure 2.2, the hand veins in Figure 2.3. The skin of the hand, starting in the wrist area, differs from the skin of the forearm: it is harder and the epidermis is thicker but it also is extremely sensitive and vascular, the skin of the fingers and the thumb become thinner. The opposite sides of palm and palm dorsal (dorsum of the hand) have different skin types: in the palm, the skin is thicker and hairless, optimized for anchorage and grabbing, in contrast the dorsum skin of the hand is thinner, highly flexible and not necessary hairless. Figure 2.4 illustrates the two different skin types with the three layers they are composed of: the superficial (i) epidermis and the deeper layers (ii) dermis and (iii) hypodermis. Fingerprint sensors capture information from the the ridge structure of the fingertips at the outmost layer (i), whereas vein sensors capture information from lower levels. The first blood vessels can be found directly below the epidermis, the main trunks are located deep in the hypodermis (Figure 2.4). The epidermis is nourished by diffusion from the dermis. The thickness of the skin varies from person to person and depending on the location in the body.

2.2 Imaging of Blood Vessels

Visualizing the interior of the human body was mainly used for diagnosis and for medical science. The Egyptians were the first to discover around 1000 B.C. the significance of the cardiovascular system to health issues, blood-letting was utilized as a therapeutic therapy [201]. As of today, the significance of diseases related to the cardiovascular system is clear and proven: the World Health Organization (WHO) classifies it among the main causes of death in the world [256]. Hence the analysis and the imaging of the blood vessels is of high interest.

New technologies made it possible to gather information *in vivo* from the inside of the body without opening tissue. With the discovery of the X-ray by Röntgen in 1895 [189], it was possible to create *in vivo* images of bone structures. Antonio Egas Moniz developed cerebral angiography in 1927/1928 and summarized his findings in [160]. He injected a contrast agent absorbing X-rays into the human brain to visualize the blood vessels and to detect abnormalities like *aneurysms*. Based on this principle *angiography* (*angio* = vessel, *graphy* = imaging) is still performed today. The term refers to medical imaging techniques that visualize the internal organs and in particular the arteries and veins. In the following we will discuss the most prominent technologies. Since the 1940s medical ultrasound was developed, in the 1980s magnetic resonance imaging was introduced. The breakthrough of

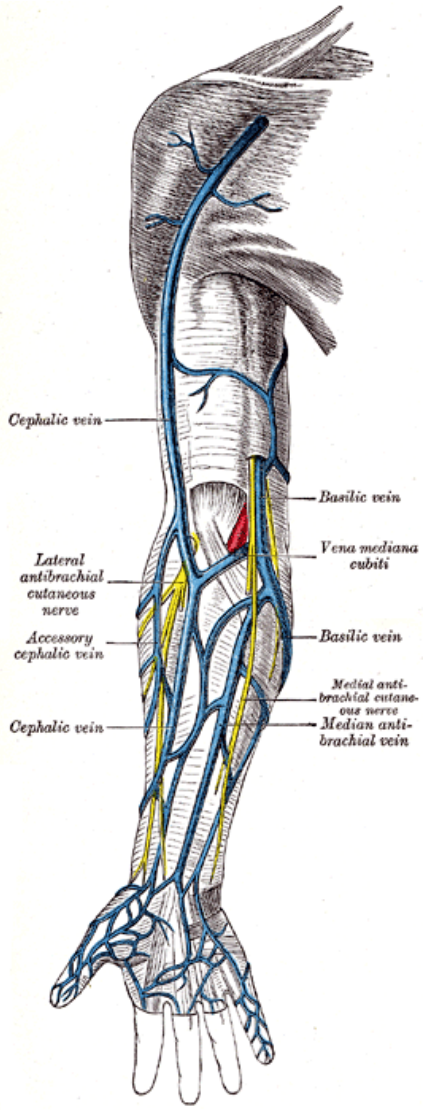


Figure 2.2: Major veins of the upper extremity (Figure 574 in [63]).

using vein patterns for biometric purposes are based on the development of near-infrared optical approaches in 1991 [172]. Different imaging approaches are discussed here, example scans are given and the appropriateness for biometric purposes is discussed.

2.2.1 X-ray

The X-rays in a wavelength between 10 nanometer and 1 picometer (Figure 2.5) get absorbed by high-density materials like bones more than by soft tissue. The Beer-Lambert law describes the absorbance E_λ as a relationship between incident intensity of radiation I_0 and the measured intensity I_1 after passing through the medium, which in fact can be described by the length of the passage d, the specific absorbance coefficient ϵ_λ and the molar concentration c as:

$$E_\lambda = \log(\frac{I_0}{I_1}) = \epsilon_\lambda * c * d. \tag{2.1}$$

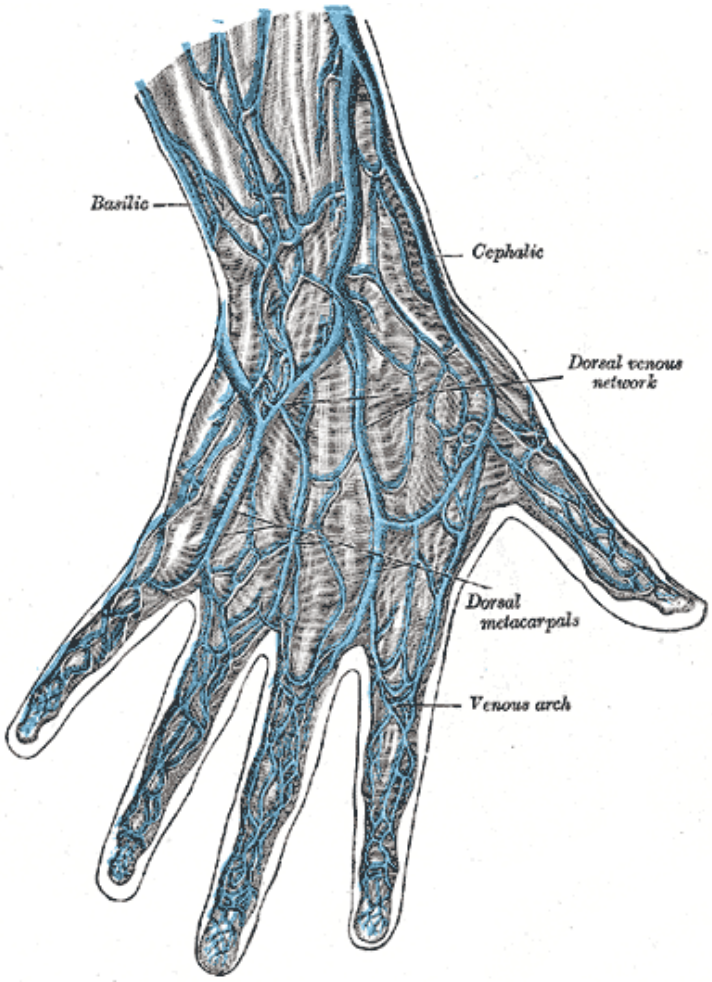


Figure 2.3: Major veins of the hand area (Figure 573 in [63]).

The coefficient ϵ_λ is for X-ray radiation proportional to the power of four with the atomic number (number of protons in the nucleus of one atom) of the substance. Calcium in the bones has an atomic number of $Z = 20$ which is significantly higher than the elements that the tissue is mostly composed of e.g. hydrogen ($Z = 1$), carbon ($Z = 6$), nitrogen ($Z = 7$) and oxygen ($Z = 8$). Lead with $Z = 82$ is commonly used to block the radiation. The molar concentration c is defined as the ratio between density and molar mass. Both are depending on the element, the latter one is defined as the atomic weight (similar to number of protons plus neutrons) multiplied with the molar mass constant.

The radiation can be created in X-ray tubes and the intensity I_1 can be captured on X-ray sensitive film. Bones absorbing high amounts of the rays appear bright, other areas where the film is highly exposed appear dark.

Fluoroscopy is an imaging technique to acquire live and continuous image sequences of the interior of the body. Opposite to the X-ray source a fluorescent screen or nowadays an image intensifier is placed. The image intensifier can transform the radiation into visible light which is captured by a common charge-coupled-device (CCD). If a radio contrast agent is used, blood vessels and the cardiovascular function can be visualized in this way.

X-ray computed tomography (CT) is a medical imaging technique on the basis of computer-processed X-rays used since the 1970s. In CT, 2D-slices of radiographic images are created and automatically rendered into volume data. Instead of film, digital detectors are used.

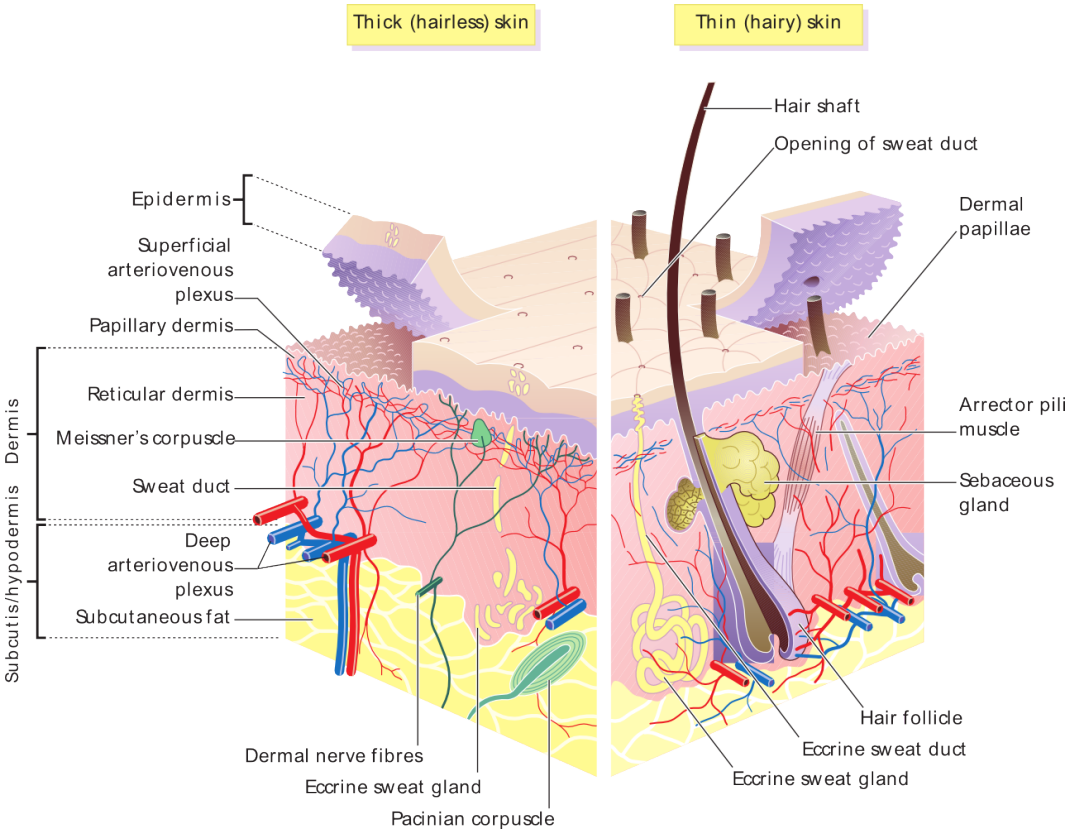


Figure 2.4: Cross section through the skin. Thick, hairless skin as found in palm and thin skin as found in dorsum of the hand (source: Wikipedia, shared under Creative Commons Attribution-Share Alike 3.0 Unported license).

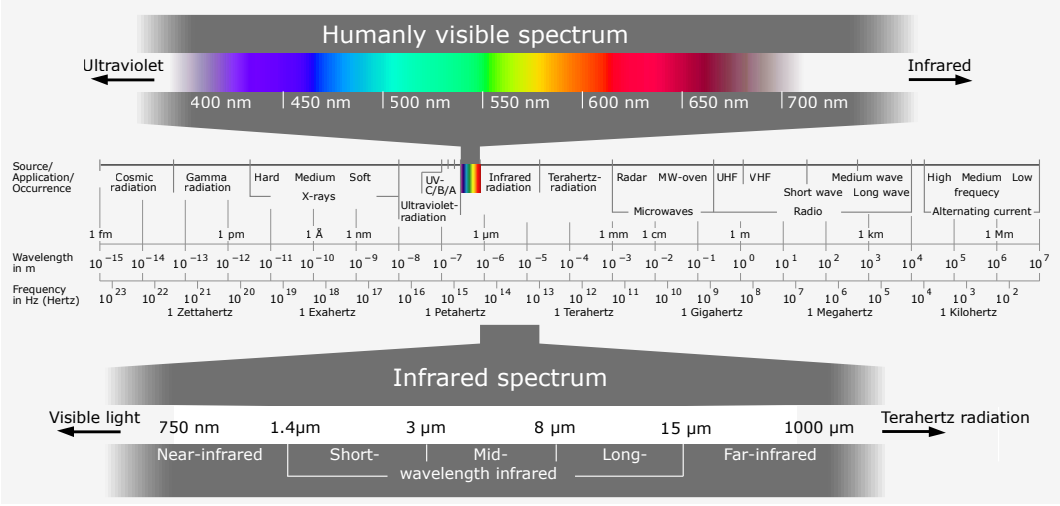


Figure 2.5: Electromagnetic spectrum (modified; source: Wikipedia, shared under Creative Commons Attribution-Share Alike 3.0 Unported license).

Computed tomography angiography (CTA) uses CT technology to visualize blood vessels. High-resolution images of fine structures are possible with CTA, one example volume-CTA scan of hands is given in Figure 2.6.

Figure 2.6: CT-angiography scan of hands (shared by Wikimedia Commons, captured with Siemens Somatom SR16, enhanced with contrast agent).

X-rays are ionizing radiation and are classified as carcinogen by the World Health Organization (WHO). The use of contrast agents to enhance the imaging is controversial since the risk of serious reactions and death is documented (meta-study in [24]). In a CTA context the contrast has to be injected intrusively. Capturing devices are bulky and expensive. All these properties disqualify X-ray-based imaging of blood vessels for biometric purposes.

2.2.2 Magnetic Resonance Imaging (MRI)

Magnetic resonance imaging (MRI) is used for visualizing organs and tissues, it is a spectroscopic approach based not on the electromagnetic waves but on the nuclear magnetic resonance. MRI was developed in the 1980s. Paul Lauterbur and Peter Mansfield were honored with the Nobel Prize in Physiology or Medicine (2003) for their discovery.

A strong magnetic field aligns the spin of charged hydrogen nuclei (protons) inside the body (63% of our body consists of hydrogen [252]). A second pulsed magnetic field is applied in a right angle to the first one, its frequency (around 10 MHz) is identical with the frequency of the spin of the protons around the magnetic field. The proton spin is aligned in direction and synchrony to the pulsed magnetic field, the relaxation time of the protons depends on the tissue type (surrounding atoms) and it can be measured to compute the MRI image. Relaxation of the spin after the pulse is called $T1$ relaxation, relaxation of the synchrony $T2$.

Magnetic resonance angiography (MRA) is focusing on the visualization of blood vessels. The imaging of venous blood is blood oxygen-level dependent and therefore referred to as *BOLD venography* or *susceptibility weighted imaging (SWI)*.

MRI is known for high soft tissue contrast. It does not depend on ionizing radiation as X-ray, however metal pieces inside or in close proximity of the body get heated and displaced and can cause harm; electronic devices can be damaged. Further drawbacks are expensive, noisy and large scanners and scanning times. Current research focuses on real-time MRI. Scanners for the hand or even the finger could substantially be smaller and less expensive.

Frames extracted from a MRA-3D-scan of a left hand can be seen in Figure 2.7. The resolution and the volume character would make it an excellent source for biometric purposes.

2.2.3 Ultrasound

Ultrasound (US) waves are sound waves with a frequency above the average human audible limit of around 20kHz. Medical ultrasonography uses those ultra-high-frequency sound waves (usually from 2-18 MHz) to capture *in vivo* and unintrusive cross-sections of internal soft tissues.

Ultrasonic sensors are transceivers sending sound waves and recording the echo, this is usually done using piezoelectric crystals and the piezoelectric effect: if the crystal is activated with an electric signal it emits sound waves. The reflected echo produces an electric signal at the crystal which can be measured. The reflectance of the sound waves is depending on the *echogenicy* of the tissue. Liquids are *anechoic* since they virtually do not reflect sound.

To visualize blood vessels the Doppler effect is used in *Doppler sonography*. The flowing blood shifts the frequency of the emitted signal. If the blood is flowing towards the probe, the frequency gets higher and vice versa. In Doppler mode the probe can sense the frequency shift and the velocity and direction of the blood can be interpolated, the image can be augmented with this additional information. In Figure 2.8 a Doppler image of an carotid artery is shown with the velocity measure of the blood flow.

As described in [147] US can be used for fingerprint recognition by measuring the difference of the echo from the fingerprint ridges and those from the valleys with the trapped air. Gray-scale US can image the internal anatomical structure of human fingers, or Doppler US can visualize the blood flow inside the finger as shown in [165].

Sensors are less expensive and more compact compared to CT or MRI. However, to mitigate the reflection from air between the probe and the body, water-based gels are applied to the skin which is not practical in biometric systems.

2.2.4 Far-Infrared Approach

As described in Section 2.1, one function of the vascular system is thermal regulation. In cold environments the body has to generate heat and distribute it into the exposed periphery. If the body is too warm, blood is cooled down in the superficial veins. This temperature gradient can be measured, since heated objects will emit electromagnetic radiation in the far-infrared (FIR) spectrum (Figure 2.5). The human body emits radiation in the range of $3-14\mu m$, however the atmospheric transmittance is almost zero for electromagnetic radiation between $5-8\mu m$. The windows of $3-5$ and $8-14\mu m$ are appropriate to capture the human body heat far-infrared radiation. Since the body is actively emitting the radiation, no active illumination is needed for the capturing process.

Thermal imaging has already been used e.g. in 2D-face recognition [84, 277] and in ear recognition [248].

Before we go into details of the published approaches, we want to point out that the term *vascular* or *vein* biometrics may be misleading. The FIR imaging technology is based on the depth of the vessels inside the tissue. As discussed in Section 2.1.2, veins can be found closer to the skin with larger diameters and a larger carried blood volume than arteries, hence it is more likely to visualize veins than arteries. For compliance with the literature we still use the common terminology.

Lin and Fan developed a FIR vein recognition system based on the palm dorsal in 2003 [54, 140]. In their experiments they captured 960 FIR images from 32 data subjects, in 3 sessions with a one week break in between. In each session 10 images were recorded. The sensor recorded in the wavelength of $3.4-5\mu m$ with a native resolution of 256×256 elements. A biometric performance of 2.3% EER could be achieved. Worth mentioning

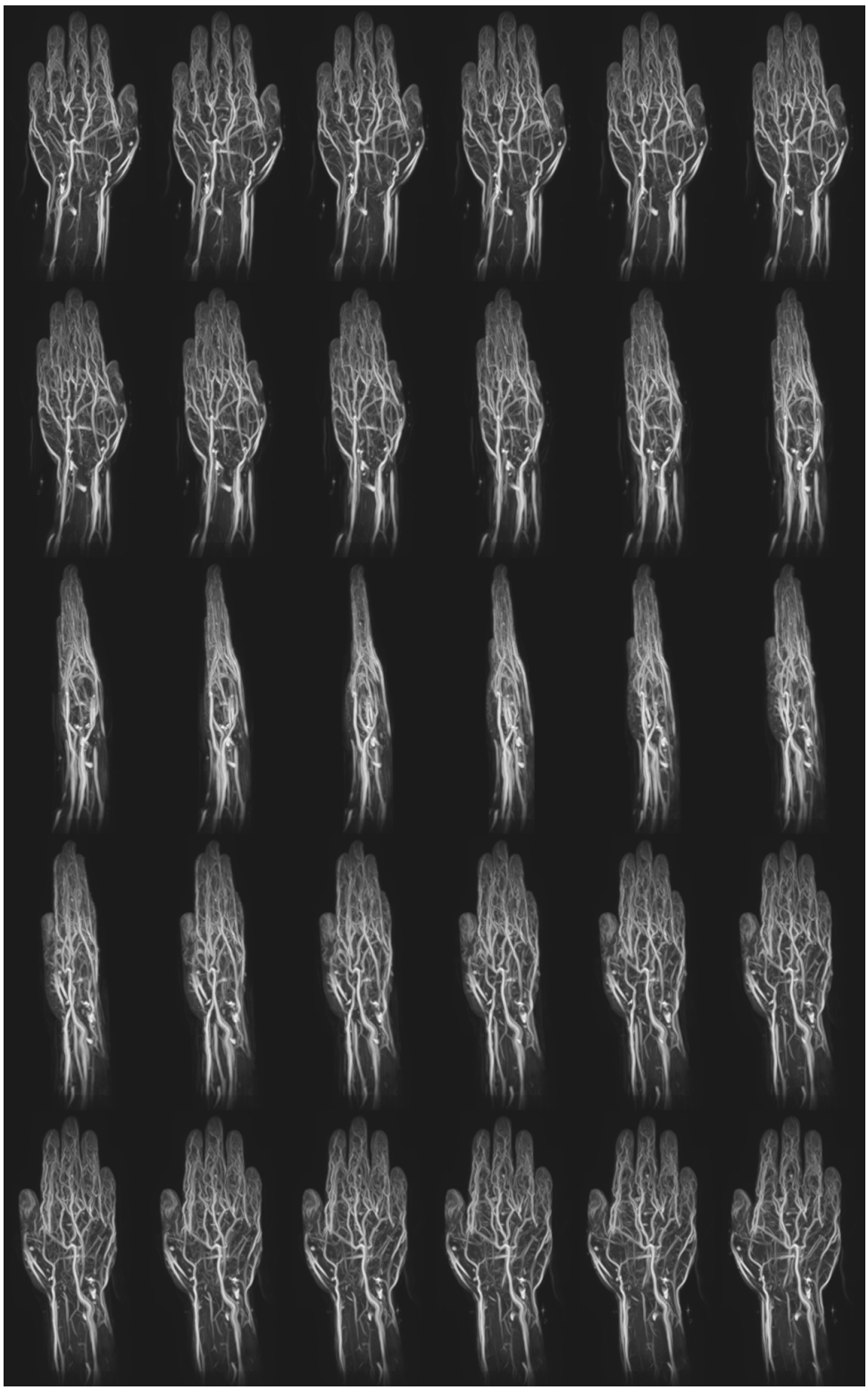


Figure 2.7: Magnetic resonance angiographic (MRA) 3D-scan of left hand (courtesy of Fujitsu Laboratories Ltd.).

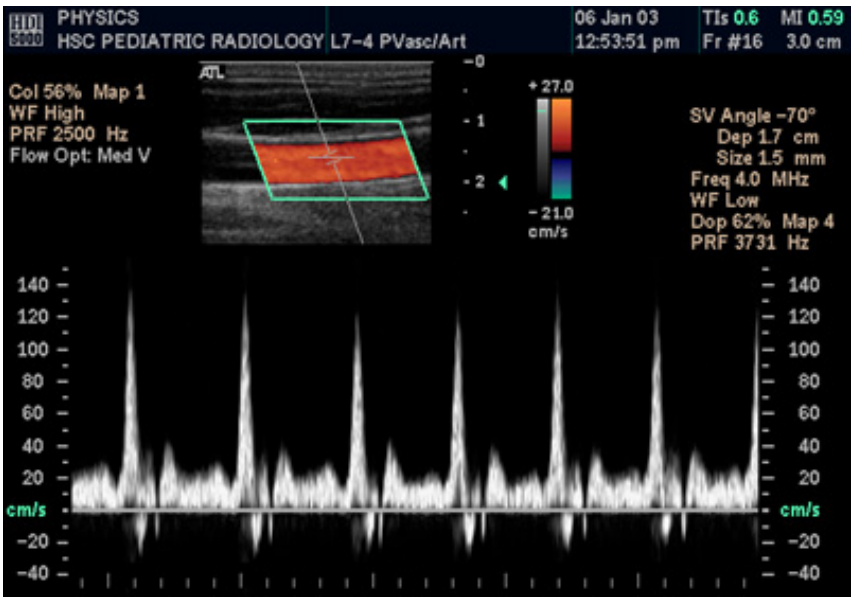
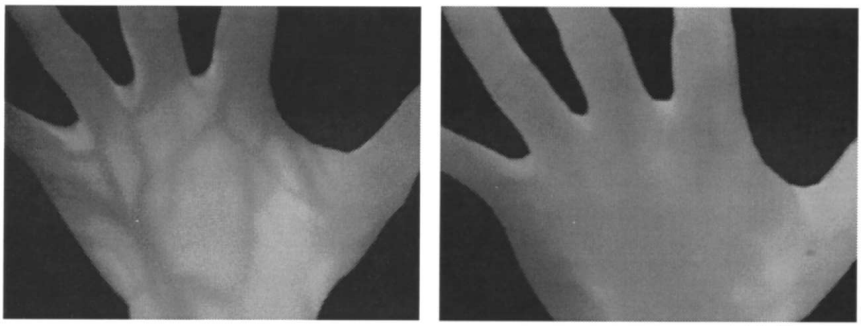


Figure 2.8: Medical spectral Doppler visualizing a common carotid artery and the speed of blood flow (shared by Daniel W. Rickey 2006 on Wikimedia Commons).

is that cases with no visible temperature gradient and cases with inversed temperature distribution (tissue warmer than blood vessels) are reported (Figures 2.9(a) and 2.9(b)).

In 2009 Kumar et al. [126] introduced another approach to FIR vein capturing and generated a large database from 100 subjects. The recognition accuracy is given with 0.1% FAR and 1.5% FRR.



(a) (b)

Figure 2.9: Abnormal thermal images (obtained from [140]): (a) measured temperature of blood vessels smaller than surrounding tissue; (b) no vein pattern visible.

Wang and Leedham investigated in 2005 [237] the influencing of the surroundings on capturing in near- as in far-infrared. The sensor used for data collection is sensitive in the spectral range of $8 - 14\mu m$. One result of the experimental data collection was that thermal imaging is only applicable to the palm-dorsal region and not to wrist or palm [239], their work is extended in [238, 240–242]. Sample images from the study are given in Figure 2.10. Figure 2.11 shows limitations of the FIR approach. Figure 2.11(a) shows the difficulties to visualize vein patterns from the palm and wrist area in FIR spectrum. The changes of the FIR image taken from the same hand are depicted in Figure 2.11(b).

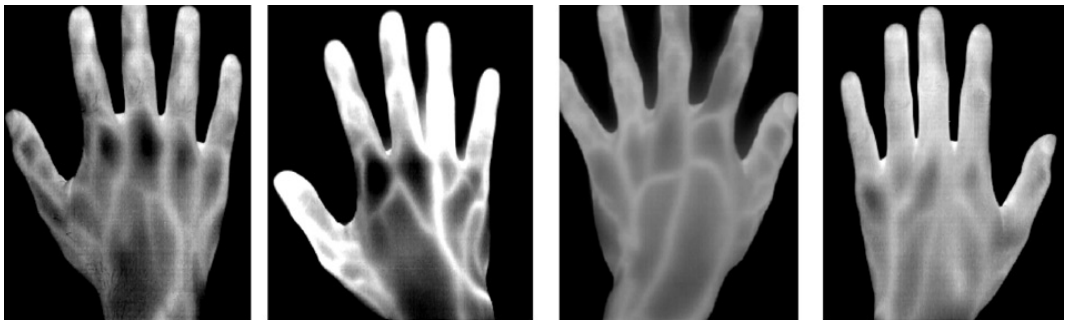
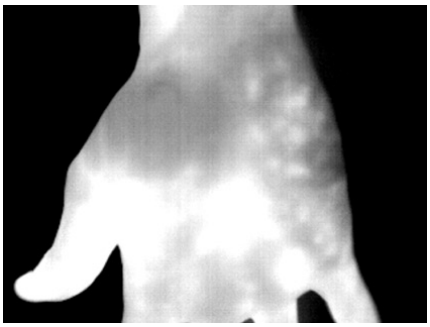
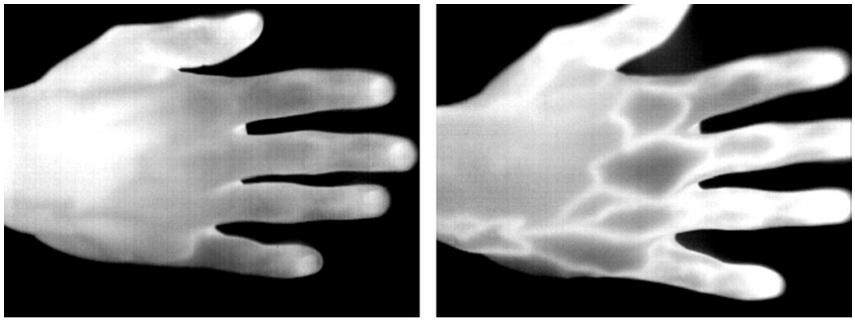


Figure 2.10: Sample FIR palm dorsal images obtained from [241].



(a)



(b)

Figure 2.11: FIR images indicating limitations of the approach (obtained from [241]): (a) no visible vein pattern for wrist and palm area; (b) significant changes in FIR images of the same hand "taken a few weeks apart".

The limited number of studies on far-infrared imaging for vein patterns revealed some shortcomings: the resolution of the images is limited, fine structures cannot be captured due to the heat spread in the tissue. The variability over time is large and dependent on environmental factors, in [241], high ambient temperatures between 30-34° Celsius and humidity over 80% led to poor contrast between veins and tissue. Only the palm dorsal area proved to be useful for FIR hand biometrics. Furthermore the FIR-sensors are expensive compared to visible light CCDs. Nonetheless recognition accuracy was almost perfect for the experiments conducted in the studies [140, 239, 241] under controlled lab conditions.

The dorsal venous network (Figure 2.3) is located above the tendons of the extensor digitorum muscle. When the muscle extends the four digits of the hand the veins can be temporarily slightly displaced. This effect may limit the utilization of the palm-dorsal submodality and therefore the FIR approach.

2.2.5 Near-Infrared Approach

Already in 1961 the relation between near-infrared radiation (NIR) and visualization of vascular structures is documented. Lunnen gave practical advises for medical photographers on how to capture diseased skin in [143]. He mentions the use of "invisible" radiation like ultra-violet and infrared (Figure 2.5) for this purpose, and describes the increasing penetration depth with larger wavelength. The absorption by venous blood in the subcutaneous layers of the skin is mentioned as well and the difference between conventional and infrared photography is shown with sample images of same hand – veins are visible in the latter case. In the paper a reference is given to [82], the title indicates that infrared photography was used even before in dermatology (1933). Unfortunately the paper is not available any longer. The author of [143] gives recommendations for the capturing process in near-infrared: active illumination from a NIR-light source ("tungsten filament bulb, flash bulb or electronic flash discharge"), infrared-sensitive sensor ("infra-red sensitive negative") and a pass filter for NIR light. This very basic idea of an imaging system for vascular structures is still the same as of today.

The principle behind the observed phenomena is that the electromagnetic absorbance of different substances differs depending on the molecular composition. Various literature mostly from the medical field investigated the propagation of electromagnetic radiation in tissue, an introduction to the topic can be found in [231], a review in [32]. In [5] an overview of skin properties of the human body are presented.

As it turns out, the permeability of human tissue is high for radiation in the wavelength 600-1400 nm [231], 600-1300 nm [5] depending on the source. This "therapeutic window" defines the range of wavelength with the maximum depth of penetration in tissue.

The dominant chromophores in the skin (epidermis) are melanins, they are responsible for the pigmentation and absorb light in the ultraviolet and visible range. Different forms of melanin exist in the human skin, most commonly eumelanin and also pheomelanin, their extinction coefficients as a function of the wavelength are given in Figure 2.12(c) in $[cm^{-}1(mol/l)^{-}1]$. As can be seen, the extinction coefficients decrease exponentially with increasing wavelengths. Thus the influence of melanin on the overall absorption gets smaller for larger wavelength enabling the "therapeutic window". The absorption of other parts of tissue, mainly water and fat, are negligible for NIR-wavelength below 1000 nm.

As discussed in Section 2.1.4 the erythrocytes constitute the major part of cells inside blood. Depending on the oxygen level of the hemoglobin (Hb/HbO_2), the spectral absorbance changes (Figure 2.12(a)). The absorption of the two forms is equal around 800 nm, for shorter waves Hb absorbs more radiation and for longer waves HbO_2 exceeds the absorption of Hb.

When NIR-light reaches the skin, it gets scattered while penetrating deeper into the tissue. In a window between 750-950 nm, the light can penetrate deep enough into the skin to reach the superficial blood vessels. An example of effective penetration depth is given in Figure 2.13. Light gets absorbed in these depth by the hemoglobin in the blood. Due to the

positioning and volume of venous vessels and blood, it can be assumed that mostly veins absorb the radiation. This absorption can be captured by CCDs. The scattering inside the tissue causes the images to be slightly blurred.

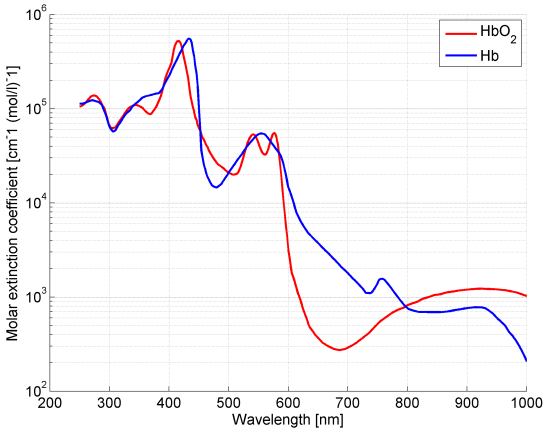
CCDs are in most cases sensitive to NIR radiation, while being interesting to construct vein sensors, this feature is not intended in visible light photography. Therefore a NIR-filter (blocking only NIR) is located in front of the sensor to avoid noise, and guarantee high quality visible light images. In cheap cameras this filter is missing and thus NIR can be sensed. In case of vascular pattern recognition the CCD without a NIR-block-filter can be equipped instead with a NIR-pass filter, blocking the visible light to avoid reflections and unwanted details from the skin. In order to control the amount of NIR light, cheap and cold light emitting diodes (LEDs) are used.

How the wavelength of the illumination effects the reflectance images of fingers is shown in Figure 2.14. The images were captured at the VideometerLab multi-spectral system of DTU (Technical University of Denmark) [229], the LED light sources are calibrated and produce even and diffuse lighting from 385-1050 nm. It can be noticed that for shorter wavelengths superficial skin structures are visible, the vascular structures are discernible from 850 nm on. Another attempt of capturing multi-spectral palm images is shown in Figure 2.15 for selected wavelengths.

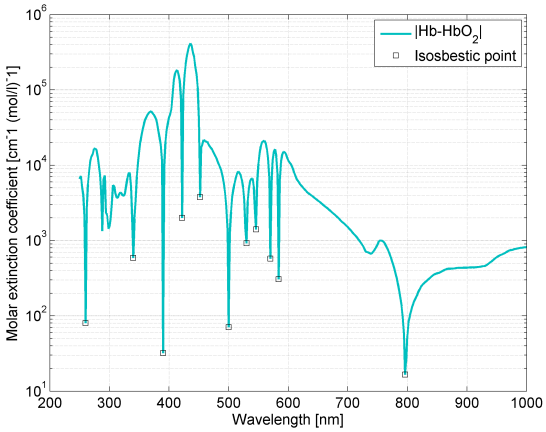
Instead of measuring the reflectance, where the sensor and the illumination system are placed on the same side of the probe, the transmittance of light through tissue can be measured as well. In the latter case the sensor has to capture the scattered light shining through the probe. This is only feasible for thin parts like the finger or it requires strong light sources. An example image taken with an unmodified consumer camera (Canon Powershot G9) without any filters is given in Figure 2.16. The hand was placed against a 11W compact fluorescent lamp.

The first approaches to utilize vascular palm dorsal (backhand) patterns for biometric purposes are reported by MacGregor and Welford [172, 173]. "Veincheck" or "vein pattern I.D." as it is referred to, is introduced with few technical details in [172]. The already known setup is described: tungsten bulb, sensor (here the electronic version: charge coupled device (CCD)) with infrared pass filter. As representation a hexagonal grid is laid over the raw vein patterns and the activated nodes are stored as a connectivity matrix. How this is done is not explained, also the comparison is described on a high abstraction-level: "The exact form of the matching algorithm compares the presence of like connections in the two networks mapped onto the hexagonal grid." [172]. Feasibility of the approach could be shown with simulations and a comparison of twenty different vein patterns with a perfect separation. In [173] the comparison was defined as an inverted Hamming distance-ratio of the hexagonal connectivity matrices. Veincheck was researched by a private and a governmental-backed sector institutions, hence the focus on productizing the new technology: "Vein check is unlikely to come to market in a fully automated form for at least another two years.". Before that would happen, a manual comparison of vein patterns by security guards is recommended.

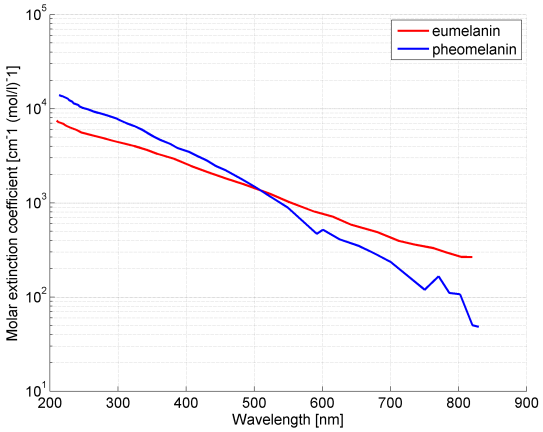
Since then a number of capturing devices for NIR vein imaging have been proposed for the three main sub-modalities of finger, palm, palm dorsal but also for the wrist area. Articles describing capturing devices for finger veins can be found in [31,40,81,112,130,136, 138, 162, 230, 235, 257, 258, 266, 273, 275, 276, 286, 287], Shimooka et al. utilized a commercial sensor in [206] that is not available anymore. [156–159, 269] refer to a commercial database from Hitachi Labs. Wrist vein imaging devices are investigated in [37, 171, 239, 241]. Most research has been focused on palm dorsal vein patterns, capturing devices are proposed in [8, 39, 55, 92, 93, 113, 127, 172, 173, 203, 204, 209, 214, 218, 233, 236, 239, 239, 241, 243, 244]. [83] uses data from [8]. Palm vein-focused research can be found in [30,37,62,67,68,132,155,234, 247,291], Sanchez-Reillo et al. investigated in [194] the influence of illumination conditions, different temperatures and extreme humidity on system and algorithm performance for palm vein data. [37] discusses a multi-spectral band selection.



(a)



(b)



(c)

Figure 2.12: Absorption capacity in molar extinction coefficient in relation with wavelength of: (a) hemoglobin in oxygenized HbO_2 and de-oxygenized Hb configuration; (b) absolute difference of HbO_2 and Hb; (c) eumelanin and pheomelanin. Based on data from [181,182].

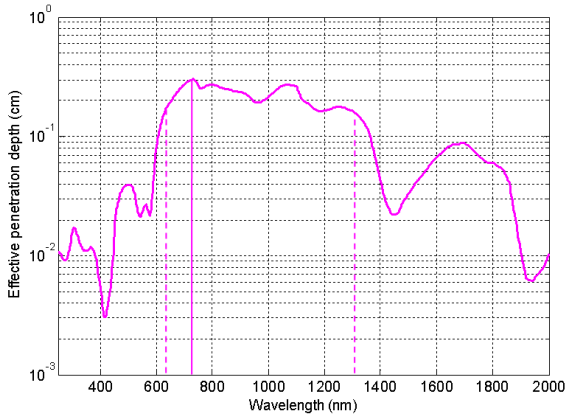


Figure 2.13: Effective penetration depth of light in breast tissue in cm (source: Wikipedia, shared under Creative Commons Attribution-ShareAlike 3.0 Unported license).

Common for the finger vein imaging systems is a transmission setup with top or side illumination, for all other sub-modalities (palm, palm dorsal, wrist) a reflection setup is used.

Some of the approaches include multimodal or multi-spectral capabilities. [138] proposes a sensor system for finger veins and fingerprints, [112] utilizes in addition the shape of the finger. [127] uses palm dorsal vein patterns and the knuckle structure. In [204] the authors combine palm dorsal vein features with hand geometry and fingerprints. Palm prints are combined with palm vein images in [67, 68, 234].

Certain databases consist of multimodal data from the hand area as described in Section 2.5.1. For example the CASIA Multi-Spectral Palmprint Database V1.0 covers palm veins and palm prints in the multi-spectral images, details are described in [67, 68]. Interesting is that the same sensor is used for the different spectral bands. SDUMLA-HMT contains multiple modalities, from the hand area it is limited to finger veins and fingerprints acquired with different sensors [276]. The Hong Kong Polytechnic University Image Database V1.0 contains finger vein and finger texture images acquired with the same capturing device but different sensors. The Bosphorus hand vein dataset and the GPDS100 database both contain palm dorsal vein patterns. Our own database that was composed during the PhD project is in the following referred to as *GUC45*. It contains finger veins, finger knuckles and fingerprints from different sensors (Appendix E).

NIR imaging is established as a de-facto standard for vein imaging. This has several reasons: the approach is able to produce high quality images of various sub-modalities (finger, pal, palm dorsal and wrist) resulting in low classification errors (more in Section 2.6). Imaging quality does not depend on the environmental conditions as in the FIR approach. Furthermore the sensors are cheap and compact since common CCDs are sensitive to the specific wavelength. Industrial sensors are based on the same technology, finger vein systems are developed by Hitachi [87, 88, 122], palm vein systems by Fujitsu [60, 246].

2.2.6 Discussion

As of now the NIR technique proved to be advantageous in comparison with other approaches and is established as a de-facto standard for vein imaging. However other approaches might prove to be useful in the future for three dimensional imaging or improved liveness detection (as discussed in Section 2.3). Recently attempts have been proposed to extract vein patterns from visible light cameras for forensic applications [219]. In their work, authors claim to inverse the process of skin color formation to derive distributions

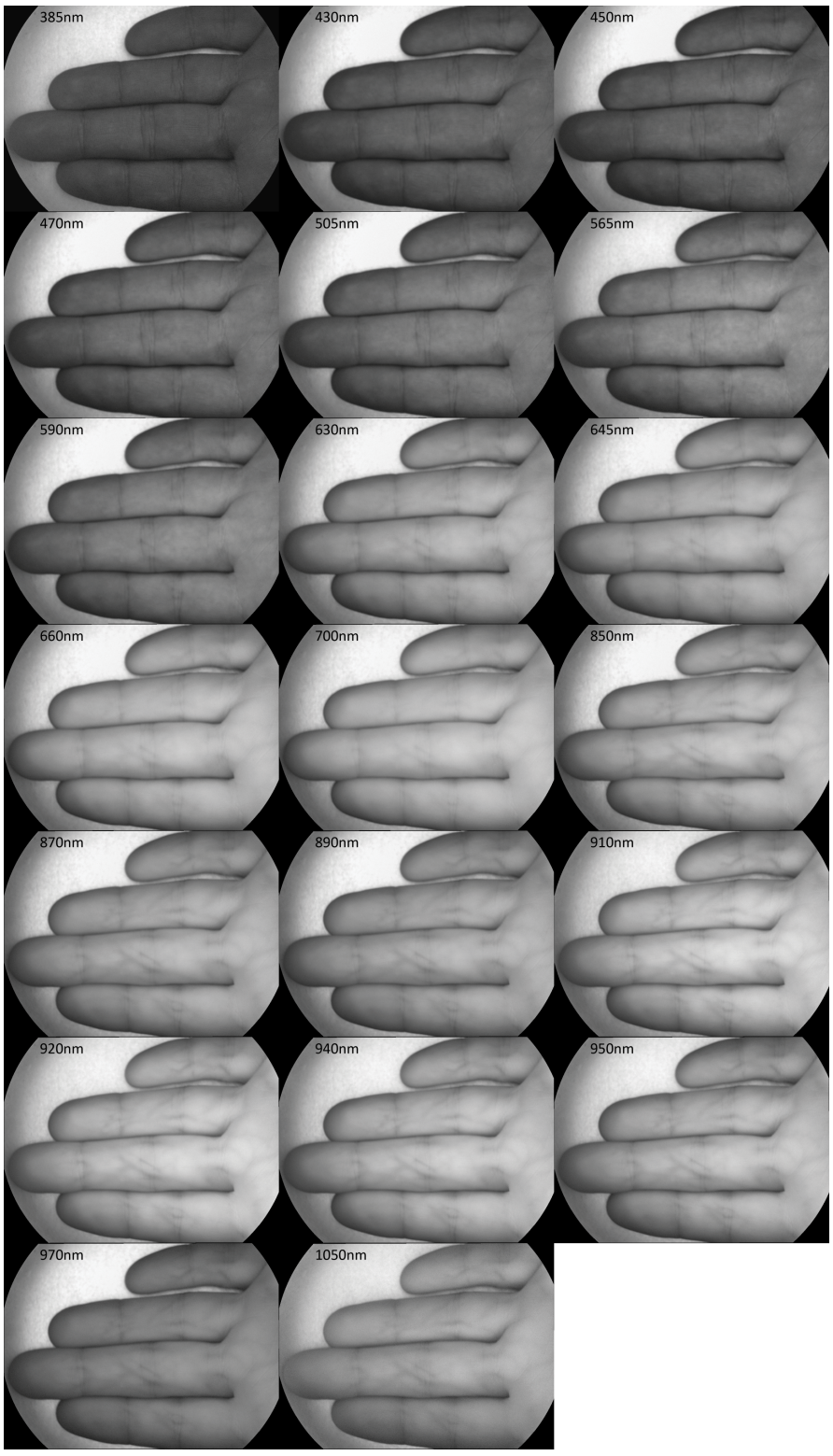


Figure 2.14: Finger reflectance images captured at VideometerLab [229]. Wavelengths varying between 385-1050 nm.

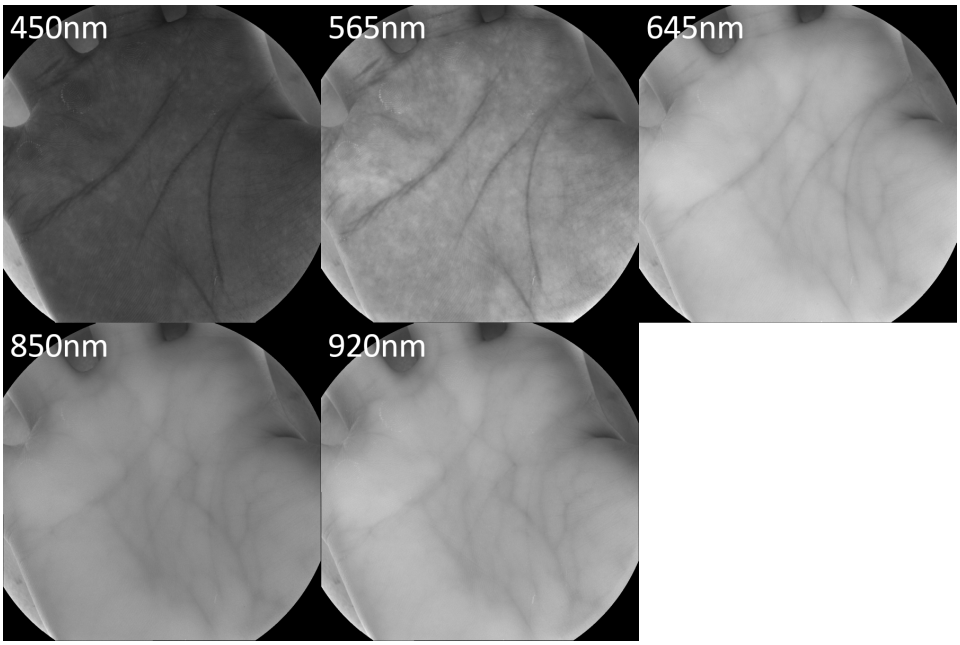


Figure 2.15: Palm reflectance images captured at VideometerLab [229]. Selected wavelengths between 450-920 nm.

Figure 2.16: Finger transmittance image captured with unmodified Canon Powershot G9 (no filters). Background illumination: 11W compact fluorescent lamp.

of various pigments, the depth of the dermis as well as hemoglobin to finally visualize the vein patterns. This technique could be used in the future to further simplify the design of the sensors for vein recognition.

After investigating the basics of the imaging approaches, it can be assumed that veins and arteries both are visualized with the commonly used NIR approach due to the similarity in the NIR absorption. However, as discussed in Section 2.1.2, veins can be found closer to the skin with larger diameters and a larger overall blood volume is carried by the veins, hence it is more likely to visualize veins with the NIR approach than arteries. For simplicity and consistency we continue to use the term *vein* recognition.

The focus of the research community so far had to lay on the development of sensors and on the acquirement of experimental data, before working on algorithmic aspects. This can be explained with the restrictive policies applied to commercial vein imaging products that commonly do not release raw images. The limited focus on open and standardized datasets was further decelerating the progress. Besides the need for constructing such imaging devices, database acquisition is time-intense and new issues of comparability arise since the results on different datasets are hardly comparable – almost every single capture device proposal comes along with its own database and its own comparison algorithm.

A recent and pleasant development initiated by the research community is the development of open databases, more on this in Section 2.5. In the future private industry should re-consider its position on the non-disclosure policy of valuable information like raw images from sensors and large experimental databases. Their argument is that customers see security issues with the disclosure of raw sensor data which follows an antiquated security-by-obscurity paradigm. Instead, research work could be catalyzed and the results could flow back into the products.

At last we want to discuss the trend of minimizing the size of biometric sensors and give examples for vein sensors. Private sector research aims at shrinking the size of the sensors for the integration in portable devices and mobile phones [81]. Remarkable developments are described in the literature, e.g. in [86] a finger vein sensor is integrated in a hand grip with possible applications for door handles. As a next step the development of micro sensors with heights of a few millimeters was tackled [61, 89]. Sample images of the established generations of sensors can be found in Figure 2.17, the minimized sensors are shown in Figures 2.18 and 2.19. With the size, the costs for the systems will likely decrease and new applications and markets might be discovered. The integration in computer mice, tablet computers and mobile phones could also initiate a paradigm shift from static to more continuous and seamless authentication for physiological biometric modalities.

2.3 Circumvention – Liveness Detection Capabilities

In remote and unsupervised authentication scenarios it is crucial to detect spoofing attempts and fake artifacts. It is well known, that fingerprint copies of sufficient quality can be created from latent prints. For example it is reported in [293] and [216] from 2000/2002 and in [49] from 2011, that commercial fingerprint sensors could be circumvented using artifacts. To avoid or at least to complicate that such an artifact successfully circumvents the biometric sensor, liveness detection mechanisms are needed, where physiological signs of life are measured. [222, 255] give an overview of liveness detection methods in biometric systems, [147] gives a comprehensive overview of liveness in fingerprint recognition, [49] summarizes the possibilities of spoofing prevention related to the finger and the hand area. [35] introduces a taxonomy for fingerprint-based liveness detection methods.

[222] distinguishes three liveness detection categories for physiological biometric modalities:

1. Observing intrinsic properties of living body
2. Recording involuntary properties of living body

Figure 2.17: Commercial vein sensors from left to right: reflective palm vein sensor (Fujitsu *PalmSecure*, without hand guide), transmission finger vein sensors (side illumination Hitachi *UBreader*, top illumination *UBReader2*).

(a) (b) (c)

Figure 2.18: Miniaturized palm vein sensors from Fujitsu (obtained from [61]): (a) left: sensor from 2011 model, right: new prototype sensor; (b) new prototype sensor integrated in tablet computer; (c) new prototype sensor integrated in laptop touchpad.

Figure 2.19: Miniaturized finger vein sensor from Hitachi (obtained from [89]).

3. Capturing bodily responses to external stimuli

1. refers to physical, electrical and optical properties that are intrinsic to tissue, DNA or body liquids. 2. summarizes involuntary signals that are dynamic like the pulse, blood pressure and flow, perspiration, brain wave signals (EEG) and electric heart signals (ECG, EKG). The third category refers to all measurements that are based on a prior stimulation and can be considered equivalent to challenge-response approaches from classic cryptography. Reflex (pupil dilation) and intentional signals (e.g. eye blinking on command) can be distinguished.

Two categories about the information utilized to ensure liveness can be summarized: (a) improved quantity by acquiring additional information or (b) improved quality by acquiring more precise information. Furthermore liveness detection mechanisms can be integrated (i) at the software-layer and (ii) at hardware or sensor-level. In order to maintain the contact-less character of most vein sensors, the distinction between contact-less (-) and contact-based (+) mechanisms is useful here.

Practical trade-offs between the security gain and many aspects like the cost of (additional) sensor, time span of acquisition, user convenience, bulkiness of solution etc. have to be considered and restrict the actual implementation. Biometric modalities that feature intrinsic liveness detection at software layer are therefore advantageous.

The literature describes several possibilities to distinguish between alive samples from the hand area and artifacts or severed and cadaver body parts. In the following we will name promising methods and discuss the applicability to vein recognition. Before, we want to briefly explain why vein recognition is described to feature intrinsic liveness detection: the argumentation is twofold, first as an intrinsic property of the body, the spectral absorption of blood and the tissue are indications of liveness. This assumes that the commonly used optical approach is utilized for the imaging, that the spectral properties are difficult to replicate and that the properties will vanish in case of severed body parts. In case of other mechanisms for imaging, intrinsic temperature gradients or the involuntary property of blood flow can be used for argumentation. The second point is that veins are located inside the body under the skin, [147] argues that sub-surface information makes a strong liveness detection against fake attacks due to the non-latent character and the difficulty to capture the information.

Software based approaches are limited to the already existing information, specific information can be found as fingerprint-based approaches show, e.g. in [217] liveness detection based on the valley noise analysis was carried out or in [34] an analysis pointed out that software-based dynamic and static approaches combined show an improved performance to recognize artifacts.

2.3.1 Multimodal Approaches for Liveness Detection

Adding additional biometric modalities increases the difficulty to circumvent the system. If we consider a fake attack, first, additional biometric data needs to be acquired by an adversary and second, the artifact(s) needs to meet quality criteria of two or more independently verifiable sources at the same time. If we consider severed body parts, liveness features from two or more sources can be used to identify the imposter attempt.

The hand area features a remarkable amount of information that can be utilized for biometric purposes. To name prominent physiological candidates: skin structure-based (fingerprint, palm print, finger knuckle), geometry-based (hand and finger), subcutaneous biometrics (palm vein, backhand vein, finger vein, wrist vein, nailbed).

There are good arguments pro and some arguments contra using sources of biometric information from the same physical area of the body. If the sensor can capture more than one trait concurrently, user convenience and possibly user throughput can be improved since only one body part needs to be presented. However, this makes the adversary's job to acquire the information in the same way more easy. The approach can lead to sensor

designs that are less bulky and more cost efficient. One question to answer is if the short physical distance may lead to a correlation of the modalities. Loss or damage of body parts on the other hand may lead to a complete disqualification for the system depending on the implementation. Obviously the choice of modalities is more restricted and it may be suboptimal regarding biometric performance or liveness detection capabilities.

2.3.2 Multi-spectral Analysis for Liveness Detection

In a multi-spectral approach, electromagnetic radiation of different or additional wavelength other than the visible light is used. The motivation is that visible light composes only a tiny fraction of the whole spectrum (Figure 2.5) and radiation with other wavelengths may reveal information that can be used for a more accurate imaging process and for liveness detection.

Regarding liveness detection it is important to mention that absorption, reflection and transmission of electromagnetic radiation varies for different materials depending on the wavelength. Absorption spectroscopy describes the absorption behaviour of materials under radiation of different wavelengths. An example of hemoglobin in the range of 200-1000 nm wavelength is given in Figure 2.12(a).

To ensure that a probe image originates from a live body characteristic, its spectral absorbance properties in specific ranges of the spectrum can be measured and compared with the expected ones. Commonly used sensors based on charge-coupled devices (CCD) technology are sensitive beyond the visible light spectrum into the near-infrared region.

This technology is already in use to identify artifacts in fingerprint recognition (e.g. [190]).

2.3.3 Pulse and Oxygen Level of Blood for Liveness Detection

Pulse oximetry is a non-invasive approach to measure the blood oxygen-level, it is often used in a medical context and dates back to the 1940s [153]. The measurements are based on the oxygen saturation ratio SpO_2 as the ratio of the concentration C of oxygen saturated hemoglobin HbO_2 and the concentration of both types of hemoglobin in systemic arterial blood:

$$SpO_2 = \frac{C_{HbO_2}}{C_{Hb} + C_{HbO2}}. \tag{2.2}$$

To calculate this ratio, optical approaches are used usually in a transmission setup at thin tissue areas like the fingertip or the ear lap. The spectral absorbance, measured in the molar extinction coefficient, differs significantly for Hb and HbO_2 as shown in Figure 2.12(a). Pulse oximetry commonly uses two LEDs in the wavelength of red (660nm) and near-infrared light (around 920nm) with corresponding photo receptors to measure the spectral absorbance.

At the first wavelength the absorption of Hb is high, at the latter one HbO_2 has a high absorption as illustrated in Figures 2.12(a) and 2.12(b). With the pulse, the observed intensity of the light reaching the photo receptors changes. The frequency of the pulsating component is equal to the pulse and can be used itself for liveness detection. The difference indicates the absorbance solely caused by the blood (and not the tissue). By measuring the ratio of light received at 600 and 920nm, a calibrated device can look up the value for SpO_2. If there is no pulse, pulse oximetry does not work.

As shown in [188] it can be the basis of liveness detection in biometric systems. Transmission pulse oximetry (TPO) could be utilized in combination with finger vein sensors, reflective pulse oximetry (RPO), where the emitters and receptors of the light are on the same side of the tissue are an interesting candidate for liveness detection with palm vein sensors. However, the method is not instantaneous and requires information from the

visible and near-infrared spectrum. In theory all NIR vein sensors can capture this information with minimal changes in the hardware. Pulse oximetry does not work as reliable with smokers, where the rate of carboxyhemoglobin ($COHb$) of the blood can reach more than 5%. The $COHb$ cannot be distinguished from HbO_2 [200].

2.3.4 Pulse Glucometry for Liveness Detection

The *blood glucose level (BGL)* must be regularly measured by patients suffering from Diabetes mellitus. Currently glucose meters are based on an invasive process of pricking the skin and dropping a blood sample (up to 1 μl) on a test strip, that is analyzed by the meter.

Another rather new approach is non-invasive, a near-infrared optical approach (900-1700 nm) was developed in 2006 and was subsequently improved in [267, 268]. The approach captures the pulsating signals from the arterial blood 100-1800 times per second to perform a spectrophotometric analysis to calculate the BGL.

The BGL is known to vary over a single day depending on the meal times and the diet. However, the measure could prove effective against fake attacks and certainly can help to prevent attacks based on severed body parts since a pulse is required and the spectrophotometric analysis is optimized to detect the BGL in blood. It is tempting to argue that the instability over the daytime can in fact be utilized to have a stronger time-depended liveness feature. On the other hand, BGL reveals health-related information and patterns of behaviour, thus has to be treated with care.

2.3.5 Perspiration for Liveness Detection

The effect of perspiration is used mainly for thermoregulation, the sweat pores in the palm and fingers can be directly observed with high-resolution optical capture devices or the effect of perspiration can be observed in a time-series of sample images as in [170, 199]. We did experiments utilizing a high-resolution digital microscope (Keyence VHX-1000E) to visualize the sweat pores and make perspiration visible. In Figure 2.20 a fingertip is shown, two frames from a video sequence where the perspiration effect can be observed is shown in Fig 2.21.

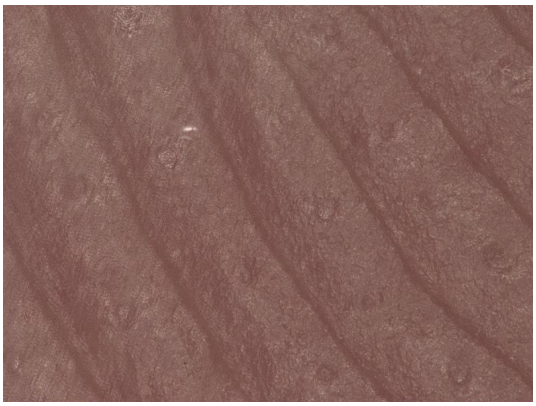


Figure 2.20: Fingertip with sweat pores (taken with Keyence VHX-1000E).

The perspiration effect is visible with high-resolution sensors as shown above, or its effects are indirectly measurable when e.g. the perspired liquids increase contact to sensors with a total internal reflection design. The indirect measurements are until now focusing on contact-based sensors, which is in contrast to commercial vein sensors.

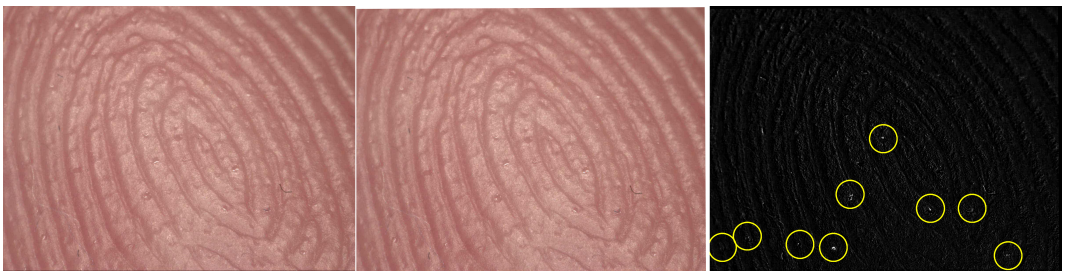


Figure 2.21: Two frames from fingertip video taken with Keyence VHX-1000E with a time lapse of ca. 1 second. Third image indicates their differences and the perspiration effect: white spots refer to changes and correspond to location of the sweat pores (highlighted with circles).

2.3.6 Elasticity for Liveness Detection

Human tissue is a highly elastic material and it deforms when pressure is applied to it. In the same way it transforms on surfaces like contact-based fingerprint readers. Those transformations can be measured over time and could be utilized to distinguish human tissue from other substances. In [6] artifacts made from silicone, gelatin, latex and wood glue were utilized in the experimental section. However, it is uncertain that the approach for skin distortion analysis holds for more advanced artifacts.

Since most vein sensors follow contact-less designs, this principle can not be applied directly. However, oftentimes a guide is available to fix the finger or hand in a certain position. The movements and deformations of the tissue on contact with the guide can be observed. In non-guided designs, the variations over time caused by muscle contractions can be observed.

2.3.7 Discussion

The argumentation that the limited availability and the difficulty to acquire biometric information without consent leads to stronger liveness detection is questionable. In this context it can be discussed if and how Kerckhoff's principle applies not only to cryptosystems but also to biometric systems. He stated that the security of a cryptosystem should solely depend on the key, the details about the system itself should be public knowledge. Should the security of the system be based on the difficulty to acquire biometric information or on the difficulty to replicate it with all its (liveness) features?

Vendors of vein pattern sensors claim that liveness detection mechanisms are embedded in the devices without disclosing additional information.

In this context an independent study from 2006 [56] investigated the liveness detection capabilities of various modalities including palm dorsal. The tested vein-based system, a TechSphere VP-II[1], could only partially be circumvented. The liveness detection could not prevent the testers to enroll and authenticate an artifact based on a latex glove over a water bottle. Only if the liveness detection was turned off during enrolment and verification, fake artifacts (e.g. based on re-drawn vein patterns on paper) could be used to spoof the sensor. The model of the pattern was acquired in two ways: (i) in visible light when superficial veins were visible, or (ii) with a slightly modified Sony DCR-TRV9E Digital Video Camera Recorder with "nightshot" function. In this mode, the infrared-block filter in front of the sensor is removed, the aperture is fully opened and near-infrared LEDs are activated.

The other study from 2005 on liveness detection capabilities and fake attacks in vein recognition has been published (in Japanese language only) [224]. The authors tested the

[1] As of today, TechSphere as the only vendor offering solutions based on the backside of the hand disappeared from the vein sensor market.

liveness detection capabilities of one commercially available finger vein system with remarkable results. Two artifacts made from different epoxy resins and one artifact made from a radish vegetable stick could not be detected as artifacts. In fact, they could be used for enrolment and for verification with an almost 100% verification accuracy, even one week after the radish was enrolled. As it turned out, the NIR sensor produced patterns from the artifacts and could be spoofed.

To the best of our knowledge independent research from the biometric field on the disintegration of observable vein patterns after abscission or necrosis is not available. It can be vaguely argued that a severed body part will lose the blood over time and hence, measurements of the spectral properties, the blood flow or the emitted heat will fail.

Interesting literature can be found in the field of forensic pathologists, who are interested in measuring postmortem changes of the human body and in particular changes of the cardiovascular system to estimate time and cause of death. In [200] the author shows in experiments on *livor mortis* (*livor* = bluish color, *mortis* = of death) that the theory of postmortem re-saturation of hemoglobin with oxygen is valid. This effect is measurable with a spectrographic analysis up into the lower skin layers (lower dermis) in low temperature environments (down to 4° Celsius). The explanation is that the cold temperatures improve the oxygen binding of hemoglobin and thus diffusion of oxygen from the environment takes place [213].

In [223] changes are described that take place during the early postmortem interval. Within 30 minutes to three hours after death *Livor mortis* are visible on the lower parts of the body as purple colored spots on the skin. This is due to gravitational effects on the blood. *Livor mortis* can shift in the first 12 to 18 hours after death if the body position is changed, this is assumed to be due to the high fraction of still intact erythrocytes and the gravitation. After 18 to 24 hours after death, the *livor mortis* become fixed and cannot be changed with pressure on the skin. *Hemolysis*, the disintegration of erythrocytes, sets in. The released hemoglobin diffuses through the vessel walls into the surrounding tissue. In extreme cases in cold environments, *livor mortis* were still shifting after 48 hours.

The color of the *livor mortis* is also an interesting object of investigation for forensic pathologists. In [223] it is described that the color in the early phase is reddish and gets darker with time. This effect can be explained with the prevailing oxygenized hemoglobin at the early phase and a continuous oxygen dissociation from the hemoglobin. Also the cells continue to consume oxygen even after time of death (up to eight hours in skeletal muscle cells). The result of these processes is de-oxygenized hemoglobin Hb with its darker slightly bluish color, as regularly found in the veins. Cold ambient temperatures (below 15° Celsius) inhibit oxygen dissociation and lead to a re-oxygenation and light red colored *livor mortis*.

Livor mortis can be absent if large amounts of blood were lost prior to death (65% of blood volume in adults). In case of drowning death, *livor mortis* can be absent due to the water pressure on the skin surface. They can become visible after recovery from cold water up to 72 hours after death in this case.

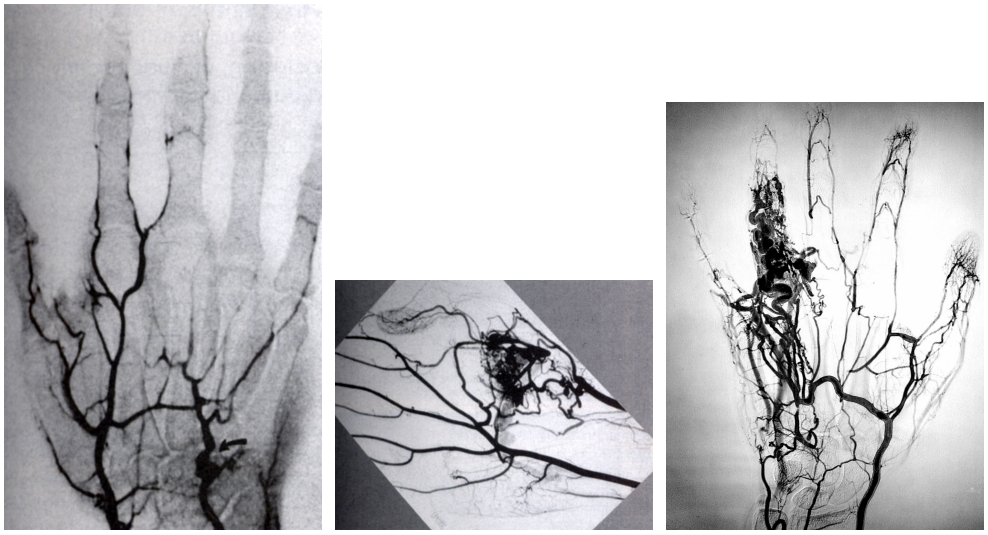
Smaller blood vessels and especially veins can crack when blood is pooled due to gravity in the areas of *livor mortis*. This phenomena is called *vibices* or death spots [223] and is visible as small dark spots. *Autolysis*, "the self-digestion" of cells, starts when the oxygen support stops and *pH*-level decreases. Inner vessel layers begin to change color to reddish and light-brown. Anaerobic bacteria start the degradation of soft tissue (*putrefaction*). Hemoglobin and other proteins in the blood are their major source of energy. Spreading of the bacteria takes place from the gut through the blood vessels. Hemoglobin is formed into sulfhemoglobin from the endogenous bacteria metabolism. The bacteria growth and the autolysis of *erythrocytes* lead to "venous marbling". The superficial epidermal blood vessels become visible as dark structures. The same article also mentions that freezing reduces the post-mortem changes to a very low rate close to zero.

As research from forensic pathology shows, blood vessel patterns can be observed post-

mortem. How the commonly used vein pattern sensors react to the processes is not researched. As a conclusion, the intrinsic liveness detection properties can and should optimally be augmented with one or more additional methods as introduced in this chapter.

2.4 Privacy Issues & Template Protection

The vascular system is for a good reason subject to medical research, the World Health Organization (WHO) classifies it among the main causes of death in the world [256]. In Chapter 4, privacy issues with hand vein patterns are discussed: medical additional information can be found within the structure of the blood vessels – the basis of vein pattern recognition. Several examples of the hand area are given in Figure 2.22. A severe medical condition like tumors can lead to *angiogenesis* to prevent infarct of growing tumor tissue. In Figure 2.22(c) such an example of blood vessel structure changes is shown: *angioma* is a tumor of the vessel walls and leads to unnatural growth of the vessels.



(a) (b) (c)

Figure 2.22: Abnormal hand vein images: (obtained from [140]): (a) *hypothenar hammer syndrome* (obtained from [131]); (b) *arteriovenous malformation* (obtained from [131]); (b) *angioma* – benign tumor made up from vascular or lymphatic vessels (©Dr Michel Royon / Wikimedia Commons).

Templates – the compact representation of a biometric source – stored in biometric systems can be encrypted to avoid data leakage, however, a comparison of two templates in the encrypted domain is not possible due to the noise sensitivity of standard cryptographic functions. Such a security measure is therefore not sufficient for biometric data. An international standard dealing with *Biometric Information Protection* can be found in [101]. Biometric systems have four major privacy risks: (i) identity fraud, (ii) cross-matching, (iii) irrevocability and (iv) leaking of sensitive medical information [116]. Privacy enhancing technologies (PETs) were developed as a consequence to overcome those shortcomings. PETs in biometric authentication systems aim to feature (i) irreversibility, (ii) renewability and (iii) unlinkability. PETs are based on modifying the template before it is stored, hence they are also referred to as template protection mechanisms.

Section 9.1 discusses different approaches to template protection. [18, 106, 187] give a good overview over existing approaches. Well-known existing schemes for template protection are: fuzzy commitment [109], the helper data scheme (HDS) [225], cancelable biometrics [185], biometric encryption [210], fuzzy vault [108], shielding functions [141], fuzzy

extractors [114], extended PIR [19]. They can be classified as feature transformation and key-based systems according to Kelkboom [116] and Zhou [288].

Feature transformation-based systems may overcome privacy issues for the stored biometric references, however, they are solely designed for a classic authentication scenario. Key-based systems, also referred to as biometric cryptosystems (BCSs) are more flexible and can be further distinguished into key-binding (such as the HDS) or key-generation schemes. In a key-binding scheme a chosen cryptographic key is fused with the biometric template and released during verification making use of helper data. In key-generation schemes the key is solely extracted from the biometric information itself.

Biometric subsystems can be extended with a BCS and can then be easily integrated in higher-abstraction security protocols. In Chapters 11 and 12 we motivate our decision for the choice of the PET and we propose a protocol integrating information from the application with HDS secured templates to authenticate data on the example of online banking transactions.

2.5 Databases

The availability of data has a major influence in biometric research. In vascular biometrics no datasets are publicly available that are captured with product sensors, vendors up to date follow restrictive information policies often completely denying the extraction of biometric raw samples from the sensors. These restrictive politics made the development of scientific prototype devices necessary in order to gather data for research purposes. The majority of the early research papers on vascular recognition are therefore also focused on sensorial aspects, see also Sections 2.2.4 and 2.2.5.

When we started the project there were no publicly available datasets to work with, so we followed two approaches to get access to data for our work: i) get in touch with other researchers working on vein recognition that already completed gathering datasets, and ii) create our own test set with extended multi-sensor and modality features (finger vein, print and finger knuckle) and meta-data about data subjects as well of the environment over a longer period of time. The latter database was composed during the PhD project and is in the following referred to as *GUC45*.

Our approach i) was fruitful and we got access to a several non-public datasets. The first two databases were gathered in 2006 in Singapores Nanyang Technological University and contain a subset of samples that were used in several publications [240, 242]. The two parts contain 732 palm dorsal vein samples in the near-infrared and 173 in the far-infrared spectrum from 122, respectively, 34 data subjects. We refer to them as Singapore NIR (*SNIR*) and Singapore FIR (*SFIR*) according to the capturing spectral band. Even though they were taken under laboratory conditions with little variations we utilized them throughout the thesis.

The third database is referred to as *UC3M*. It was collected in 2010 at the University Carlos III of Madrid [171]. The dataset consists of 348 vein images in the near-infrared spectrum from the wrist areas of 29 data subjects. The dataset was taken under different illumination intensities to optimize the capturing device and it does not reflect an operational database.

For more details about SNIR, SFIR, UC3M we refer to Section 9.4. A summary of the most important features are given in Table 2.1, sample images are given for example in Figures 9.3(a), 9.4(a) and 9.5(a). GUC45 is described in an extra chapter (Appendix E). The small sample sets restrict the confidence of a biometric performance evaluation. According to [249], the "rule of 3" can be applied to estimate the a posteriori confidence interval for the calculation of the false non-match rate (FNMR). With a 95% confidence the lowest error regarding the FNMR can be approximated with $3/N$, with N equal to the number genuine comparisons. This is a limiting factor especially for the SFIR dataset where a minimum FNMR error of 1.73% can be established. According to the "rule of 30", at least 30 error

must occure to estimate the true error rate within ± 30% of the observed rate with a 90% confidence. As can be seen in the table the datasets provide too few genuine comparisons to estimate the FNMR with a high confidence according to this criteria.

With the selected databases all sub-modalities but palm veins, including FIR and NIR capturing approaches are covered.

Property	**SNIR** [242]	**SFIR** [242]	**UC3M** [171]	**GUC45** [73]
Frequency Band	NIR	FIR	NIR	NIR — visible
Modality	Back of Hand (2)	Back of Hand (2)	Wrist (2)	Finger vein ($10 \times 3^{\dashv}$) finger knuckle (10) fingerprint ($10 \times 2^{\dashv}$)
Data Subjects	122	34	29	45, 45, 44
Sessions	1	1	1	12, 12, 4
Images per Session	2×3	$2\times \sim 3$	2×6	10×2
Images	732	173	348	10800($\times 3^{\dashv}$), 10800, 3560($\times 2^{\dashv}$)
Genuine Comparisons	732	170	870	
Imposter Comparisons	266814	14708	59508	
Resolution (px)	$644 \times 492^{\perp}$	320×240	$640 \times 480^{\perp}$	$512 \times 240^{\dagger}$
Depth	8 Bit	8 Bit	8 Bit	8 Bit
Limitation on FNMR‡	0.41%	1.73%	0.34%	
Limitation on FNMR*	4.10%	17.64%	3.45%	

Table 2.1: Properties of the biometric vein datasets used throughout the experiments. $^{\perp}$Image size reduced by 50% in each spatial dimension for experiments. †For the experiment the images are cropped to size 468×122 to eliminate most non-finger area. $^{\dashv}$Different sensors or finger orientation used (details in Appendix E). ‡Upper bound of FNMR according to "rule of 3". *Upper bound of FNMR according to "rule of 30".

2.5.1 Public Databases

Only very recently public "reference" datasets of reasonable quality were published online that make benchmarking of research work possible and that help to further intensify work in this area. However, most of them are not yet well-known and utilized by the community. In this section we will give an overview of datasets covering various sub-modalities.

2.5.1.1 The Hong Kong Polytechnic University Finger Image Database (Version 1.0)

The Hong Kong Polytechnic University Image Database contains finger vein and finger texture images. In the paper where the database is first introduced the authors mention their motivation to publish the dataset: "...as currently there is no finger-vein image database publicly available for the researchers elsewhere." [130]. The objective was to "establish large-scale finger vein image database for the research and make it available in the public domain to further more promising research efforts." [221]. Work on the development started in April 2009 and finished in March 2010. The self-built sensor captured finger vein and finger skin texture image simultaneously and contactless. In two sessions, six images from index and middle finger veins and textures (left hand) were captured from 156 subjects. Since not all subjects participated in both sessions the number of samples is 6264.

Sample images from the database are given in Figure 2.23. Information about the database can found on the homepage [221] as well as in the paper [130].

2.5.1.2 PKU Finger Vein Database (V2-V4)

The finger vein databases are gathered by the Artificial Intelligence Lab of Peking University. Three datasets are described (V2-V4):

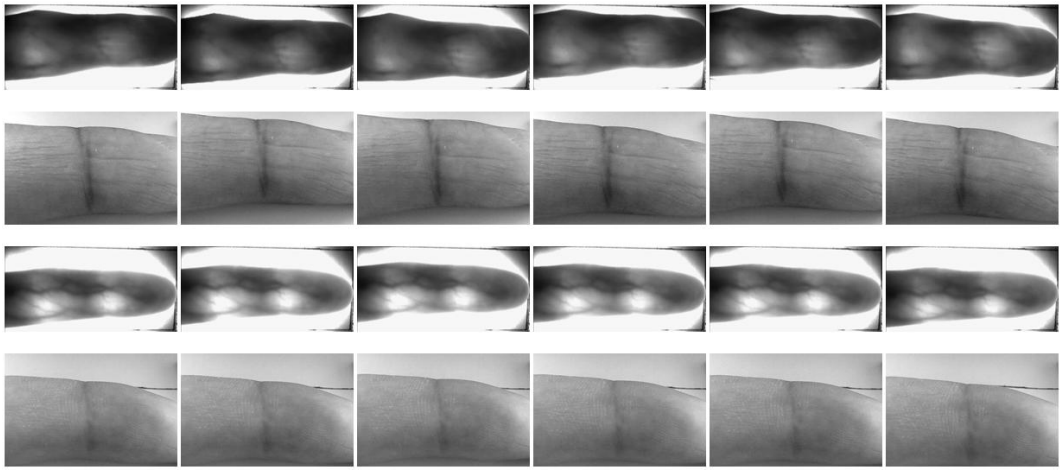


Figure 2.23: Sample images of the Hong Kong Polytechnic University Finger Image Database (Version 1.0) obtained from [221].

- V2 (dated 2008/12/01) contains 4674 gray-scale finger vein samples from 431 fingers collected in 2008.
- V3 (dated 2009/05/22) 5379 gray-scale finger vein images from 398 different fingers.
- V4 (dated 2011/04/21) contains 1597 gray-scale finger vein samples from 200 fingers (approx. eight impressions each). The data is first automatically preselected and later manually to ensure high quality of the images.

On the homepage [4] a list of submitted algorithms and their performance evaluation can be found, a detailed description is missing. [40] is related to the database as it describes how the intensity of the lighting is adapted to produce finger vein images of high contrast in all regions.

2.5.1.3 CASIA Multi-Spectral Palmprint Image Database V1.0

The dataset is published by the Institute of Automation, Chinese Academy of Sciences and it contains palm images captured with a self-designed multi-spectral imaging device (460, 630, 700, 850, 940 nm + "white light"). The larger wavelengths allow to observe the vein patterns. 100 volunteers participated in two session, in each session three image sets of both hands were captured. Some of the resulting 7200 palm images are shown in Figure 2.24.

Additional information can be found on the homepage [33], related papers are [67, 68]. The database was used for the evaluation of feature extractors by external researchers for example in [155, 291].

2.5.1.4 SDUMLA-HMT Database

The SDUMLA-HMT is a multimodal biometric database from the Joint Lab for Intelligent Computing and Intelligent Systems of Wuhan University. It was gathered in 2010 including information from face, finger vein, gait, iris and fingerprint (multiple sensors). All the biometric information comes from the same 106 volunteers. The authors claim in [64] to have released the first open finger vein database. Six samples from index, middle and ring finger of both hands are captured, resulting in 3816 images.

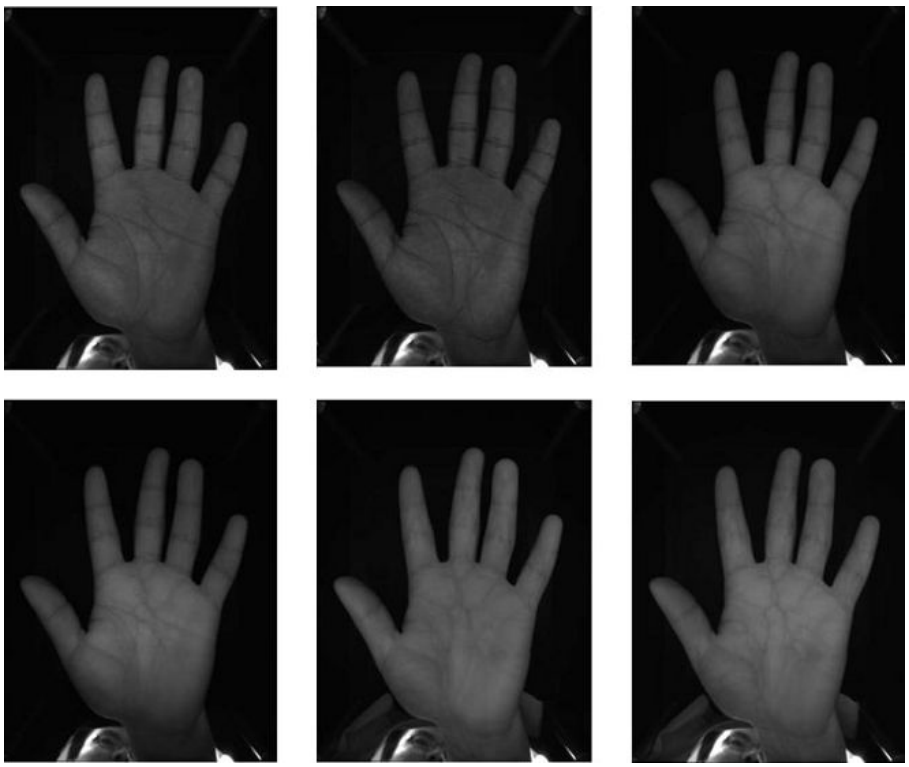


Figure 2.24: Sample images of the CASIA Multi-Spectral Palmprint Image Database V1.0 obtained from [33].

Samples are given in Figure 2.25. The homepage gives detailed explanations about the different modalities and the capturing procedures [64], in [276] the information is available in paper form.

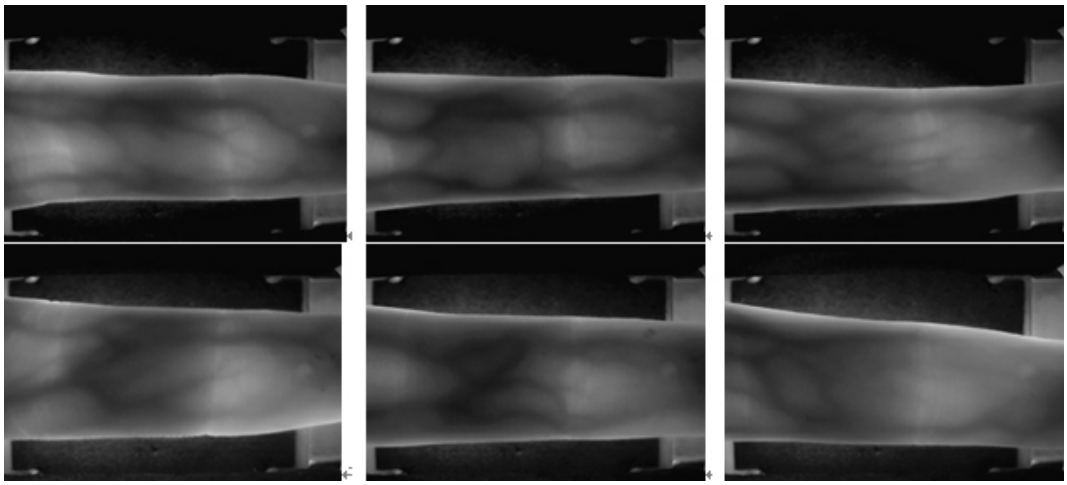


Figure 2.25: Sample images of the vein part of the SDUMLA-HMT database obtained from [64].

2.5.1.5 Bosphorus Hand Vein Database

The dataset is composed by Bogazici University and it is based on palm dorsal vein patterns. The data is acquired in NIR from 100 subjects under different conditions: three left hand palm images under (B) carrying a 3 kg bag for 1 minute, (A) squeezing an elastic ball for 1 minute, (I) cooling the hand with an ice pack. Three images from both hand for (N) normal conditions. And additionally left hand images of 25 subjects after 2-5 months. Overall 1575 images are included. The homepage of the database can be found in [15].

2.5.1.6 GPDS100 Vein Databases

The Universidad de Las Palmas de Gran Canaria made a palm dorsal vein dataset available. It is split into three parts the GPDS100VeinsCCDcylindrical, the GPDS100VeinsCMOScylindrical and GPDS100VeinsCMOSergonomic part. The first is captured with a CCD camera, the latter ones with a CMOS webcam in NIR. The first set contains 10 samples from 102 subjects, the latter ones 10 samples from 103 subjects. Two sessions recording 5 samples from the right hand were conducted. The two CMOS-sets use different handles: "a cylindrical handle with two pegs" and "an ergonomic handle which fix the hand position in a suitable way for the user.", hence the naming [227]. The same source contains information about GDPS100 Vein Databases and databases covering other modalities. Information can also be found in [55].

2.5.2 Discussions

The most important properties of the introduced datasets are summarized in Tables 2.1 and 2.2. Such an overview of public datasets containing vein data was missing until today to the best of our knowledge. As can be seen from the table almost all submodalities of hand vein pattern recognition are available, only a wrist dataset is missing. Unfortunately all vein (parts of the) datasets are captured in near-infrared only.

It has to be mentioned that this is a great achievement of the community, still some issues could be improved. There are some limitations that should be mentioned as well. The table clearly identifies one problem of the available datasets: description is often imprecise, possibly important information is scattered in continuous text or simply not available. The exact procedures that were utilized to capture the data is missing in almost all cases. Dissemination and acceptance of the public datasets is yet very limited, as can be seen by the comments of some groups publishing their data. There exist examples, e.g. the CASIA Multi-Spectral Palmprint Image Database V1.0 that has been used in various publications [155, 291] already, other datasets are only used from researchers of the hosting organization.

In some cases, the availability is limited, from personal experience we can state that the registration and access to the data seems to be restricted in other cases. This could be due to technical problems or a semi-public dissemination strategy. To furthermore enhance the possibilities of comparability, test protocols should be recommended, standardized testing platforms would be advantageous as well. To enable easy adaption of test platforms the structure and the file naming should be unified. As an additional effort to improve vein recognition some of the datasets contain multimodal information, which is a valuable development. Augmentation of the raw data with additional measures of the environment or metadata would enrich the data collection even further.

We are planning to improve the dissemination of the information by offering a centralized place where links to the specific homepages can be found.

Property	**PolyU** [221]	**PKU(V2,V3,V4)** [4]	**CASIA** [33]
Frequency Band	NIR — visible	NIR	Multi-spectral(6)
Modality	Finger vein and texture (2)	Finger vein	Palm (2)
Data Subjects	156	431,398,200 (fingers)	100
Sessions	2	?	2
Images per Session	$\sim 2^{\perp} \times 6 \times 2$	?	$2 \times 3 \times 6$
Images	6264	4674,5379,1597	7200
Resolution (px)	?	?	?
Depth	?	?	8 Bit
Property	**SDUMLA** [64]	**Bosphorus** [15]	**GDPS**† [227]
Frequency Band	NIR	NIR	NIR
Modality	Finger vein (6) and others	Palm dorsal	Palm dorsal (1)
Data Subjects	106	100	102,103,103
Sessions	?	?	2
Images per Session	6×6	$3 \times X^{\dashv}$	5
Images	3816	1575	1020,1030,1030
Resolution (px)	320×240	300×240	?
Depth	?	8 Bit	?

Table 2.2: Public vein databases (names shortened, details in Section 2.5.1). ?: unclear or missing information. $^{\perp}$Not all volunteers showed in both sessions. $^{\dashv}$See text description (Section 2.5.1.5). †Dataset three-split (Section 2.5.1.6).

2.6 Feature Extraction and Comparison

Most of the literature introduced in Section 2.2.5 proposes not only a capturing device but also algorithms for feature extraction and comparison. Here we will review some promising approaches and we will classify them according to criteria like the type of feature representation and comparison. A focus in the context of the thesis is given to approaches that are compatible with state-of-the-art template protection schemes like the helper data scheme (HDS) [225]. In order to use such a feature post-processing the templates need to be of fixed-length and structure, alignment free and possibly invariant to affine transformation like scaling, rotations or translations. The problem of affine transformations is often limited due to the sensor device design, handles or guides keep the region of interest in place. However, a feature representation that can handle those variations is applicable more generally.

2.6.1 Representation

All proposed representations of 2D vein patterns can be classified as (i) image or pixel-based, (ii) skeleton-based or (iii) interest point-based or derived versions thereof.

(i) Pixel-based approaches feature a low level of abstraction, they can be implemented efficiently since in the easiest case the sensor image itself can be utilized as a reference. This representation is usually of fixed-length and structure since the sensor resolution does not change. Transformations can be compensated if alignment is performed.

(ii) A more abstract representation of the blood vessels is the one-pixel wide *skeleton* representing its topology. More processing is needed to extract the skeletons and new errors might be introduced: usually a segmentation and morphological operators lead to this form. On the other hand storage requirements are small, efficient graph-based comparison can be performed. New information such as the angles of the blood vessel representation can be utilized. Skeletons can be stored as binary images of fixed-length and structure, also here transformations can be compensated if alignment is performed.

(iii) Interest points, such as minutiae location and possibly the orientation (bifurcations and branch points), can be utilized to represent the skeleton in a more abstract form. This

abstract representation is often based on (ii), thus requires more processing but less storage. The number of minutiae points will vary depending on noise and other influencing factors, thus it can not be considered to be of fixed-length and structure. Efficient post-processing based on simple rules may remove false minutiae and improve recognition accuracy. For example the following situations can be easily prevented: clusters of minutiae points are likely occurring due to noise; endpoints in close proximity to branch points are likely to be caused by skeletonization errors; close endpoints facing each other are likely caused by segmentation errors and do not represent an actual break in the blood vessels. Perhaps the largest advantage is that minutiae-based systems are well researched for fingerprint systems and the already generated knowledge can be applied in the context of vein pattern recognition. Also template protection schemes like the fuzzy vault [108] were specifically designed for (fingerprint) minutiae systems and could be adapted to vein minutiae. In Chapter 9 we show – based on knowledge from fingerprint systems – how minutiae points are transformed into a fixed-length and structure representation that is alignment-free.

2.6.2 Comparison Strategies

The HDS template protection scheme works on fixed-length vectors: simplified it can be stated that each element $R(i)$ of the reference vector at position i is compared to the corresponding element $P(i)$ of the probe vector. Approaches for feature comparison based on sophisticated strategies can not be applied here. A decent biometric performance based on a comparison of element pairs is therefore required to find approaches that could be utilized in conjunction with the HDS.

Current survey articles about vein recognition can be found in [144, 265] but they are very limited. A new attempt to capture vein recognition related articles is given in Table 2.3, 2.4, 2.5 and 2.6. To first structure the data, we arrange it according to the submodality, then it is sorted according to the author(s). The overview of the state of the art is complemented with information about the invariance to transformations and about the reported performance. However, the performances can be considered to be of limited value, oftentimes EERs around 1% are measured with limited possibilities for comparisons as discussed in Section 2.2.5 due to differences in the databases and the evaluation protocols.

Our own proposals introduced in Part II and articles published with our contribution are highlighted in bold letters to clarify the relation with the state of the art.

As can be seen from the tables, most approaches are pixel-based (i) and thus are of fixed length. Some approaches are skeleton-based (ii) and a number are minutiae-based (iii). The latter case is commonly not of fixed length. Only a few approaches consider transformation invariance to some extend [8, 30, 77–79, 127, 178, 218, 228, 266]. In some of those cases a registration or alignment of the reference and the probe is necessary [8, 30, 79, 178, 218, 218, 228], which is not applicable in the HDS. Others are not of fixed length [127, 228] and are therefore not fulfilling the requirements of the HDS. Another approach not filtered yet suffers from a very low number of features: the feature vectors extracted in [266] have a length of 10 elements which is not sufficient for a strong brute-force resistance of the HDS-secured templates.

Based on the analysis of existing approaches there is clearly a need of feature representation and comparison strategies compatible with the HDS. The spectral minutiae introduced for fingerprint [261, 262] and our proposal for adapting them to vein minutiae [77, 78] is a promising approach on how to combine vein data from touch-free sensors with the HDS.

Ref	Author (Year)	Type[1]	Dataset[2]	Performance	Remarks
[66]	Guan et a. (2010)	i	(?/132/5/660)	∼94% Rec.-rate	LDA-based
[65]	Guan et a. (2011)	i	(?/132/5/660)	∼94% Rec.-rate	PCA-based
[79,178]	**Hartung/Pflug et al. (2012)**	ii (reg RT)	UC3M,GUC45[3]	1.38% EER/ 25% EER	Chain code + location
[136]	Lee et al. (2009)	iii	(80/640/10/6400)	0.76% EER	no thumbs, MHD
[266]	Li et al. (2007)	i (5R,5RTS)	(32/128/2/256)	92.7% Rec-rate	10 Moment invariants + Hausdorff
[156]	Miura et al. (2002)	i	(678/?/?/?)	0.145% EER	Line tracking + xor
[157]	Miura et al. (2004)	i	(678/?/?/?)	0.145% EER	Line tracking + xor
[158,159]	Miura et al. (2005)	i	(678/?/?/?)	0.0009% EER	Maximum curvature + correlation
[162]	Mulyono et al. (2008)	i	(100/200/5/1000)	0% FAR, 0.28% FRR	Comparison [157]
[206]	Shimooka et al. (2004)	i	(?/?/?/?)	∼0	Inspired by immune system
[235]	Wang K. et al. (2010)	i	(?/300/5/1500)		Orientational filtering
[258]	Wu et al. (2009)	i	(25/50/10/500)	99.2% Ident.-rate	Radon transf. + NN
[257]	Wu et al. (2011)	i	(10/10/10/100)	99% Ident.-rate	PCA + NN
[269]	Yanagawa et al. (2007)	i	(506/506/2/1012)	∼0	Comparison [157]
[271]	Yang J. et al. (2010)	i	(100/100/10/1000)	1.3% EER	Energy maps-based
[275]	Yang W. et al. (2009)	i	(60/60/4/240)	100% Ident.-rate	Multi-spectral
[274]	Yang W. et al. (2011)	i	(?/220/2/440)	0.44% EER	Location and direction coding
[287]	Zhang et al. (2005)	i	(400/400/8/3200)	0.13% EER	wavelet trans. + NN
[286]	Zhang et al. (2006)	i	(400/400/8/3200)	0.128% EER	curvelet trans. + NN

Table 2.3: Survey of finger vein-related literature. ?: unclear or missing information. [1]according to 2.6.1, brackets indicate invariance to (R)otation, (T)ranslation and (S)caling, eventually (reg)istration may be necessary. [2](capture subjects/biometric sources/samples per source/files). [3]According to Section 2.5.

Ref	Author (Year)	Type[1]	Dataset[2]	Performance	Remarks
[30]	Chen et al. (2009)	i/ii (reg RT)	(250/500/12/6000)	0.64%	SMM, skeleton + segmented version
[62]	Fuksis et al. (2011)	i	(50/50/5/250)	1% EER, fused 0% EER	palm print + binary biohash extension
[68]	Hao Y. et al. (2008)	i	CASIA v1.0[5]	0.57% EER	Ordinal palmprint Hamming distance
[132]	Ladoux et al. (2009)	iii (RTS)	(24/24/60[5]/1440)[4]	0% EER	SIFT-based [142]
[155]	Mirmohamadsa-deghi et al. (2011)	i	CASIA v1.0[5]	0.4%EER 0.09% EER	Local binary patterns Local derivative patterns
[247]	Watanabe et al (2005)		(70000/140000/?/?)	0.00008% FAR 0.01% FRR	Fujitsu Research
[291]	Zhou et al. (2010)	i	CASIA v1.0	2% EER 1% EER 2% EER 5% EER	Multiscale vessel enh. Localized radon trans. Ordinal representation Laplacianpalm (LPP)

Table 2.4: Survey of palm vein-related literature. ?: unclear or missing information. [1]according to 2.6.1, brackets indicate invariance to (R)otation, (T)ranslation and (S)caling, eventually (reg)istration may be necessary. [2](capture subjects/biometric sources/samples per source/files). [3]Multi-spectral images. [4]Acquired in two sessions. [5]According to Section 2.5.

Ref	Author (Year)	Type[1]	Dataset[2]	Performance	Remarks
[8]	Badawi (2006)	i (reg R)	(500/1000/5/5000)	0.7% EER	Overlap of segmented images
[39]	Cross et al. (1995)	ii	(20/20/5/100)	0% FAR, 5% FRR	Dilated skeletons multi-sample fusion
[54]	Fan et al. (2003)	i	(?/?/30/?)	2.3% EER	FIR, Multi-scale filter + NN
[140]	Fan et al. (2004)	i	(32/32/30/960)[4]	2.3% EER	[54]
[55]	Ferrer et al. (2009)	i	(150/?/?/?)	1.42% EER	Gabor filter Hamming distance
[71]	**Hartung et al. (2009)**	i	SNIR	0.55% EER	Correlation/ Hamming distance
[77]	**Hartung et al. (2011)**	iii (T[RS][6])	UC3M,SNIR,SFIR[5]	5.9%/1.35%/ 3.6% EER	Spectral minutiae (SML)
[78]	**Hartung et al. (2012)**	iii (T[RS][6])	UC3M,SNIR,SFIR[5]	3.11%/0.41%/ 0.15% EER	Spectral minutiae (SML+SMC)
[83]	Khan et al. (2009)	ii	200 files from [8]	0% EER	PCA-based
[119]	Khan et al. (2010)	ii	200 files from [8]	0% EER	PCA-based
[126]	Kumar et al. (2009)	i	(100/?/3/?)	0.1%FAR 1.5% FRR	FIR, Gabor wavelets
[127]	Kumar et al. (2009)	iii (RT)	(100/?/?/?)	1.14% EER	Minutiae triangulation knuckle shape
[203]	Shahin et al. (2007)	i	subset of [8] (50/100/5/500)	0.25% EER	Correlation of segmented images
[209]	Soni et al. (2010)	iii	(341/?/?/1750)	0.64% EER	Minutiae location + orientation
[218]	Tanaka et al. (2004)	i (reg RT)	(25/?/?/?)	FAR 0.73% FRR 4%	FFT, phase only correlation vertical, horizontal shift
[228]	**Uriarte-Antonio et al. (2011)**	iii (reg RT)	UC3M2[7],SNIR[7]	2.27%/ 1.63% EER	Miutiae location + orientation
[233]	Wang H. et al. (2011)	iii	(?/?/?/400)	0.7% EER	SIFT-based [142]
[236]	Wang K. et al. (2006)	i/ii	(100/100/5/500) 0.5% FRR	0% FAR, Fusion	Invariable Moments K-L transform Vein geometry
[237]	Wang L. et al. (2005)	ii	(12/12/9/108)	0% EER	FIR, Local thresholding + LHD
[239]	Wang L. et al. (2006)	ii	(30/60/9/540)	0% EER	NIR/FIR, Local thresholding + LHD
[241]	Wang L. et al. (2007)	ii	(150/300/9/2700)		NIR, Local thresholding + LHD
[241]	Wang L. et al. (2007)	ii	(30/60/9/540)		FIR, Local thresholding + LHD
[242]	Wang L. et al. (2008)	iii	(47/?/?/?)	0% EER	FIR, MHD
[243]	Wang Y. et al. (2010)	i	(102/204/10/2040)	90.88% Rec-rate	partition local binary pattern (CWPLBP)
[244]	Wang Y. et al. (2011)	i	(102/204/10/2040)	98.83% Rec-rate	partition local binary pattern (CWPLBP)+ ECC

Table 2.5: Survey of palm dorsal vein-related literature. ?: unclear or missing information. [1]according to 2.6.1, brackets indicate invariance to (R)otation, (T)ranslation and (S)caling, eventually (reg)istration may be necessary. [2](capture subjects/biometric sources/samples per source/files). [3]Multi-spectral images. [4]Acquired in three sessions. [5]According to Section 2.5. [6]R,S are transformed into alignment-free translations. [7]Captured with the same sensor as UC3M, but fixed settings for lighting, (121/121/5/605).

Ref	Author (Year)	Type[1]	Dataset[2]	Performance	Remarks
[79,178]	**Hartung/Pflug et al. (2012)**	ii (reg RT)	UC3M,GUC45[3]	1.38% EER/ 25% EER	Chain code + location
[77]	**Hartung et al. (2011)**	iii (T[RS][4])	UC3M,SNIR,SFIR[3]	5.9%/1.35%/ 3.6% EER	Spectral minutiae (SML)
[78]	**Hartung et al. (2012)**	iii (T[RS][4])	UC3M,SNIR,SFIR[3]	3.11%/0.41%/ 0.15% EER	Spectral minutiae (SML+SMC)
[228]	**Uriarte-Antonio et al. (2011)**	iii (reg RT)	UC3M2[5], SNIR[5]	2.27%/ 1.63% EER	Miutiae location + orientation

Table 2.6: Survey of wrist vein-related literature. ?: unclear or missing information. [1]according to 2.6.1, brackets indicate invariance to (R)otation, (T)ranslation and (S)caling, eventually (reg)istration may be necessary. [2](capture subjects/biometric sources/samples per source/files). [3]According to Section 2.5. [4]R,S are transformed into alignment-free translations. [5]Captured with the same sensor as UC3M, but fixed settings for lighting, (121/121/5/605).

2.7 Discussions

To come back to the evaluation criteria introduced in the beginning of Chapter 2 and to summarize the state of the art analysis we come the the following conclusions:

- Universality: as introduced in the physiological background (Section 2.1), it is obvious that a healthy human needs to have blood vessels in the areas of consideration. However, as indicated in Section 2.2, the affordable imaging technologies are not capable of perfectly capturing the information. A study from 2006 [94] has shown that the failure to enroll rate is quite low and lower than in iris-based systems.
- Uniqueness: In Section 2.1 the partly random genesis of the blood vessels is described. Section 2.2 gives examples of the high complexity of vein patterns in the hand area.
- Performance: the research work introduced in Section 2.6 shows the high recognition performance that can be achieved utilizing this modality.
- Permanence: it is known that vascular patterns change over time e.g. in case of medical conditions (Section 2.4) or due to physical exercise. However, this is usually a slow process and furthermore since the modality is located within the body, it is less likely to be altered.
- Collectability: simple capturing technologies exist and are available as explained in Section 2.2.
- Acceptability: vein patterns can be recorded without touching the sensor (hygienic), without harming the body, they are hidden inside the body and are not related to criminal investigation. These are good arguments for a possible high user acceptance. The success in the East-Asian region seems to support this claim.
- Circumvention: advanced possibilities for liveness detection exist as discussed in Section 2.3.

For the extend of the thesis we decided to focus on algorithmic aspects of NIR vein images since the imaging technology is the most promising and commercially successful. The research questions formulated in Section 1.3 aim at extending the importance of privacy issues with vein patterns (Q1). To overcome those issues we strive to utilize HDS-based template protection schemes mainly due to the binary verification decision, binary, compact and secure templates and a modular structure utilizing standard cryptography

building blocks. It solves the problem of medical information that might be included in the vein patterns. For this, an alignment-free and fixed-length representation of vein patterns is needed since the state of the art is lacking those approaches with sufficiently large feature vectors. This algorithm must lead to a high recognition accuracy and sufficiently long binary sequences. Preferably the algorithm is adaptable to multiple sub-modalities (Q3). The state of the art is also lacking systems making full use of the template protection schemes (Q2) and finally the questions arose if the current trend of utilizing information from multiple biometric sources can help to increase the liveness detection capabilities and overcome potential limitations with the biometric performance (Q4).

Chapter 3

Contributions and Conclusions

3.1 Contributions

Here we describe the contributions regarding our initial goals and the research questions in a compact form.

Q1: Are there privacy issues arising with vascular biometric systems and can technical solutions be utilized to protect the privacy of data subjects?

(Addressed in Chapter 4 [71])

- Vascular pattern recognition with its non-latent character and the properties discussed in Chapter 2 was identified as the modality of choice.
- The literature survey about vein biometrics revealed that no critical analysis was performed yet. Our investigation attached in Chapter 4 clearly identifies medical information that could be extracted from the vein patterns. In conclusion the use of privacy enhancing technologies with vein biometrics is recommended if not inevitable.
- Classic cryptography can solve problems with the storage of sensitive information, but the comparison of the inherent noisy biometric templates cannot be performed in the encrypted domain. A second survey showed that new approaches of privacy enhancing technologies (PETs) were developed, often designed modality-independent and implemented for multiple modalities to overcome the known issues. However, a vascular pattern-based privacy enhanced system have never been proposed before.
- The key-binding and releasing PETs allow for the combination of biometric secure templates with standard cryptographic systems. One state-of-the-art instance, the helper data scheme (HDS) [225], seemed to be the most promising candidate for solving the privacy and data storage problems. It utilizes a binary verification decision, binary, compact and secure templates and standard cryptography building blocks. The HDS requires feature vectors of fixed length and structure. To guarantee a high performance of the template-protected system, the features should have a sufficient length to avoid brute force attacks, the comparison of the underlying biometric features must be performed element-wise and it should result in a high base performance. In addition no registration a reference and a probe can be performed.

Q2: Are there practical scenarios that benefit from such a system? Can protocols be designed that make use of state-of-the-art template protection schemes?

(Addressed in Chapters 11 [72] and 12 [74])

- The biometric research community searches for application scenarios besides the already exploited border control and national identity schemes. One scenario that we identified for such a biometric system is authentication in online banking. A recent study from 2012 initiated by Deutsch Bank Research [41] confirms this growing need for security in online banking. The work also refers to a study that investigated the

user acceptance regarding technologies for increasing the online banking security. Biometric technologies placed second, right behind TAN-based approaches. However, TAN-based and other established mechanisms based on knowledge and possession for securing online transactions are widely broken. The problem of repudiation of transactions secured with those mechanisms is immanent and can be solved with biometrics.

- As a consequence we sketched a system to secure online banking transactions with template-protected biometric features. The underlying protocol is called BTAP and is introduced in Chapter 11. It is modality independent and based on the HDS as well as on a separate hardware token for the processing of the biometric pipeline and the BTAP. Transaction information is fused with a HDS-released key and send for the verification to a banking server. No biometric information is stored outside the token and the template is in addition protected by the HDS.
- The BTAP is specified, its security properties and the correct functionality are proven in Chapter 12 using a formal model, the applied pi calculus.

Q3: Is it possible to design a single algorithm for multiple sub-modalities of vascular pattern recognition resulting in high recognition rates? Can the problem of vascular pattern recognition be reduced to other, well-known (biometric) problems? Can the requirements on the algorithm of state-of-the-art template protection schemes be met?

(Addressed in Chapters 5-9 [76, 78, 166, 168, 178])

- The requirements of the HDS have been satisfied for minutiae-based fingerprint systems in the past. Therefore our approach was to map the vein patterns into a similar minutiae-based representation. The minutiae of a fingerprint describe the end and branch points of the fingerprint ridges, the equivalent in vein patterns describe the topology of the blood vessels. A transformation of the location and orientation information from the varying number of minutiae points into spectral minutiae [264] results in HDS-compatible feature vectors of fixed length and structure that are also translation invariant. Rotations and scaling changes can be compensated without a registration of two vectors which is useful in combination with hygienic and contact-free vein sensors.
- The next step was the design and implementation of a biometric pipeline based on vascular patterns fulfilling the requirements of the HDS and thus the BTAP: in order to perform evaluations we needed to access vascular databases. The approach to access the data was three-fold: (i) first, we contacted other research groups and successfully gained access to subsets of data published in [242] and [171] which we used throughout the work for internal comparability of the results. To make the results comparable with the state of the art, we implemented algorithms from [50, 242] and [30]. (ii) The second approach was the gathering of our own dataset. We successfully captured data from 45 participants of Gjøvik University College (hence hereafter referred to as GUC45) over a long period of time in 12 sessions. The database contains multimodal (finger vein, finger knuckle, fingerprints) as well as multi-sensorial data. Also metadata about the capture subjects and the environmental conditions during the sessions were acquired (Appendix E). However, the quality of the images proved to be very challenging. (iii) The last approach was to perform an evaluation on an undisclosed, large, high-quality database of palm vein patterns at the end of the project, the latest results on this data are described in Section 3.2.
- We investigated the effect of contrast enhancement pre-processing on vein patterns in Chapter 5 with the conclusion that a trade-off between the level of enhancement, the introduction of noise and required execution time is necessary.

- A new feature point detector for minutiae was developed that works with image skeletons. It is fast and more flexible than existing approaches as it is able to extract the location and additionally orientational information (Chapter 7 and 9).
- We developed a quality control for vein patterns that is useful in the unsupervised scenario of online banking (Chapter 6). We proved the effectiveness in an evaluation for different sub-modalities. With the system, low-quality samples can be directly refused to improve the enrolment process and the biometric performance. Another application is the guidance of the capture subject during operation.
- The pipeline based on spectral vein minutiae is described in Chapter 9. The evaluation shows that an excellent biometric performance is reached while the requirements of the HDS are fulfilled. The solution is a flexible, unifying approach that is applicable to various submodalities like palm dorsal and wrist veins captured with different imaging techniques.
- A second biometric feature extraction and comparison algorithm was designed to investigate if state-of-the-art performance could be reached in a multi-reference scenario using vein skeletal information on a different abstraction level. The approach is described in Chapter 8, the evaluation revealed that indeed a high, competitive performance can be reached. However, the approach is not compatible with HDS or BTAP since the comparison requires the registration of the samples.
- In Section 3.2 we present the latest results regarding quantized features – as they are utilizes within the HDS. The biometric performance of the compact, binary features from the spectral vein minutiae are further improved with a multi-reference training. In fact, a perfect distinction between imposter and genuine comparisons of 1450 palm vein images from 145 different palms can be reached with a superb comparison speed. This promising result is embittered by the fact that the intra-class variance is still too high to result in a high performance of the secured templates. The discussion in Section 3.3.1 points out possible solutions.

Q4: Can the biometric performance – besides the fake resistance and liveness detection capabilities – be increased with multi-sensor and/or multimodal approaches?

(Addressed in Chapter 10 [75] and Appendix E)

- As mentioned earlier, to investigate this question the GUC45 database was acquired as a multimodal testing database.
- We introduce in Chapter 10 a feature extraction approach for finger knuckle images from our database. The idea is to use SURF [11] descriptors and map them into a fixed-length form to enable a possible fusion in the HDS and to solve issues with the high intra-class variance. The biometric performance however is decreasing significantly when transforming the SURF points into a HDS-compatible form.
- The design of the spectral minutiae vein pipeline allows the fusion with fingerprint data on feature and other levels to increase the biometric performance.
- As the evaluation in Section 3.2 revealed, the biometric performance of the proposed solution does not necessary need to be improved, however liveness detection will benefit from additional modalities.

3.2 Latest Results

We strive to merge our work on a system that enables data and person authentic online banking transactions with our high performance biometric system using vascular patterns

of the palm. One of the major unsolved problems of nowadays online banking was addressed by our previous work: how to realize non-repudiation of authentic transactions without introducing privacy issues for the customers. Here, a major step towards the practical realization of such a system utilizing vascular patterns is presented.

The two building blocks – the BTAP and the spectral vein minutiae biometric subsystem – and their incorporation are depicted in Figure 3.1.

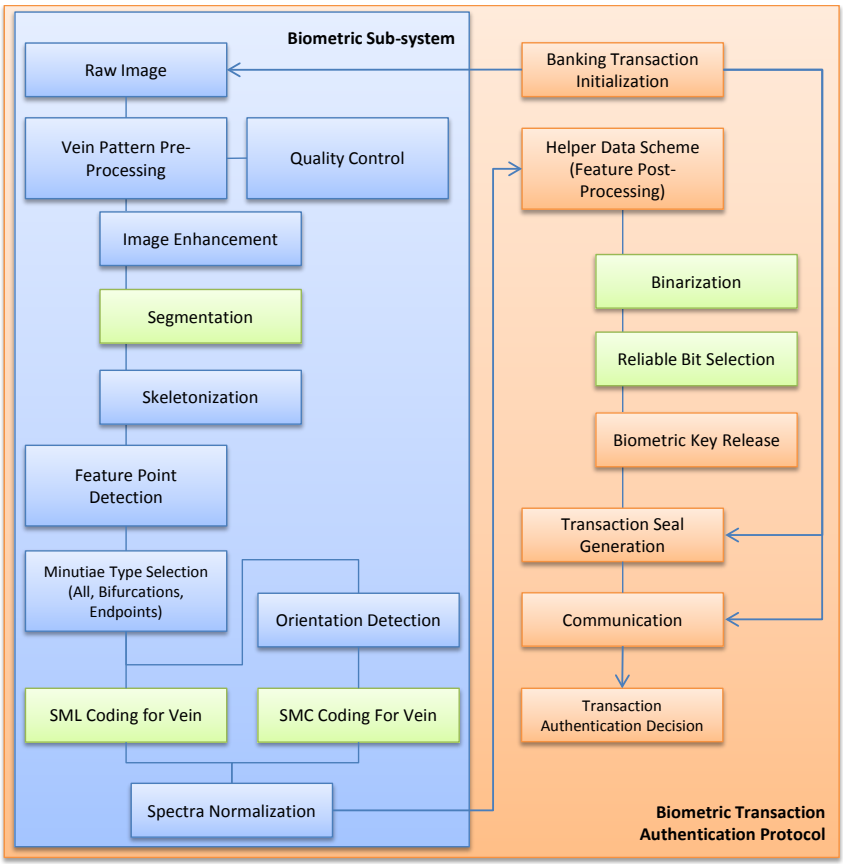


Figure 3.1: Flowchart of the adapted biometric vein system based on [78] inside the BTAP [72, 74]. Green: functional blocks addressed in this section; parameter optimization of pipeline as discussed in Section 3.2.1; new performance results as in Section 3.2.1.

3.2.1 Simulations

In May 2012 the developed pipeline based on [78] could be applied to a large palm vein dataset. Due to non disclosure agreements, the organizations name and any sensitive information as raw images can not be mentioned in the report. Image quality and the large number of biometric samples per source (max. images 12 per session per palm) qualify the dataset for the analysis of reliability of single elements of the feature vectors. This estimation of reliable features is a critical step in the helper data scheme (HDS) to find and extract reproducible and discriminative components.

The pipeline was extended and adapted to the specifics of the data: the optimization process was performed on a small subset of 296 samples from 28 palms. Evaluation was performed on normalized data that was made available. Parameters had to be greedily optimized due to time restrictions and a relatively slow Matlab implementation. This pro-

cedure unlikely leads to globally optimal parameters for the feature extraction and comparison, but is practical and may still lead to high recognition accuracy.

Adaptation of contrast enhancement algorithm: the previous methods introduced large amounts of noise. Therefor, we chose the contrast-limited adaptive histogram equalization (CLAHE) [292] with a low parameter for the clip limit (0.01) to minimize the noise for the cost of a strong contrast enhancement.

Adaptation of segmentation algorithm parameter: the previously utilized Frangi filter had to be adapted to the data, vein structures in the raw images were thinner and more complex than in [78]. The filter scales were chosen as $\sigma = [2, 3, 4]$ after evaluation on the test set. β correction values were adapted after evaluation to $\beta_1 = 2.5$; and $\beta_2 = 20$. Segmentation is based on a single threshold $T_s = 11$ selected by minimizing the EER utilizing a modified Hausdorff performance evaluation on the test set.

Adaptation of spectral minutiae configuration: large-scale simulations of different parameter configurations and different comparison strategies including SML (location based spectral minutiae), SMC (location and orientation based spectral minutiae) and their fast rotation variants were performed. The complex modulus normalization of the spectra was outperforming the second approach introduced in [78].

Best results were achieved with the following configuration according to nomenclature in [78]: $M = 128$, $N = 256$, $\sigma = 0.32$, $\lambda_\mathrm{l} = 0.05$, $\lambda_\mathrm{h} = 0.6$[1]. The change in λ_l indicates low location errors of the minutiae maps. The results were analyzed distinguishing between endpoints, bifurcation points separately and their combination. In general the measured performance of spectra generated from the bifurcation points exceeded those of the endpoints.

Untrained and Unprotected Feature Vectors

The performance evaluation of the spectral minutiae (all minutiae types considered) on the evaluation set revealed that SML outperformed SMC and that the fast rotation methods further improve recognition performance in terms of EER (3.94% vs. 4.83% EER). This result is contradicting those achieved for fingerprints, one explanation can be the higher robustness of minutiae orientations extracted from fingerprints. In vein patterns no orientational field can be extracted. Furthermore, the utilized angle extractor considers only a 3×3 neighborhood around the minutiae. A score level fusion of SML and SMC could furthermore reduce the EER to 2.28%. How the biometric performance changes when feature selection based on reliability estimation is applied, is described next.

Trained Binary Feature Vectors

The HDS requires a binarization of the feature vectors and optionally a selection of most discriminative elements from a feature vector. For the simulations we split the evaluation set further into a training sub-set for the binarization and the reliability estimation of the components and an evaluation sub-set. The dataset featured up to 12 samples per palm, we decided to include exactly 10 samples per palm to include more data subjects. From the 10 samples, 7 were dedicated for the training and 3 for the final evaluation of binary feature vectors. The spectra had to be scaled down by a factor of 2 in each spacial dimension (bicubic interpolation) to $128 \times 64 = 8192$ components due to implementational restrictions.

Statistics about the means of each component for the binarization and about reliability of every component were collected and utilized as described in [225]. A simple and very fast Hamming distance was used for the score computation. The biometric performance of the binarized feature vectors XBV with $2^i - 1$ most reliable elements on the final evaluation set is summarized in Figures 3.2 and 3.3 with a receiver operating characteristic (ROC) for one specific configuration (SML spectra from bifurcation points). Recognition accuracy is peaking around 1023-4095 selected reliable bits with a perfect separation of the full (symmetric) comparison set of 435 genuine and 93960 imposter attempts.

[1] M, N are the dimensions in radial and angular direction of the polar-logarithmic grid, σ refers to the sigma of the Gaussian filtering, λ_l, λ_h refer to the distance range from which the radial values are extracted from.

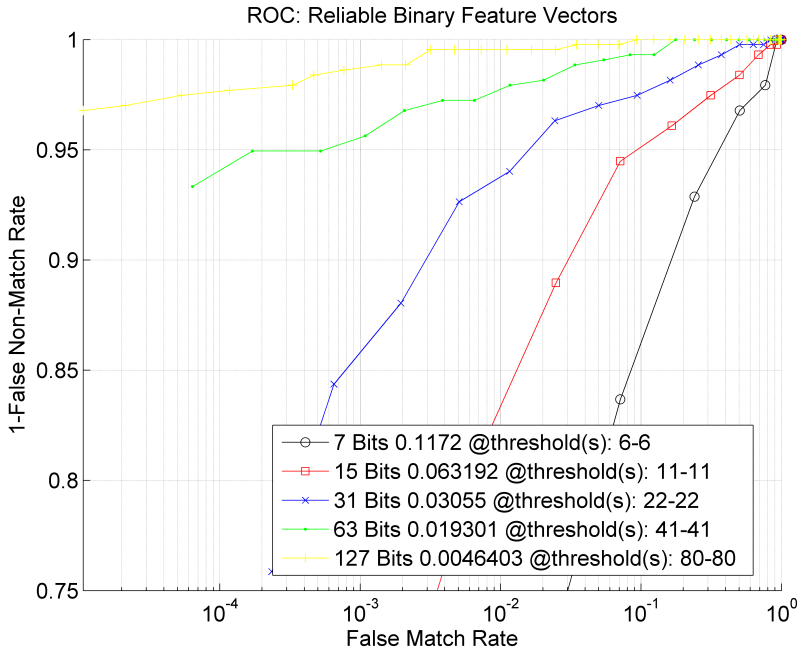


Figure 3.2: Receiver operating characteristic (ROC) of reliable binary feature vectors using Hamming distance, length: 7-127 bits. Logarithmic scale on x-axis. Legend: selected reliable bits, EER, threshold(s).

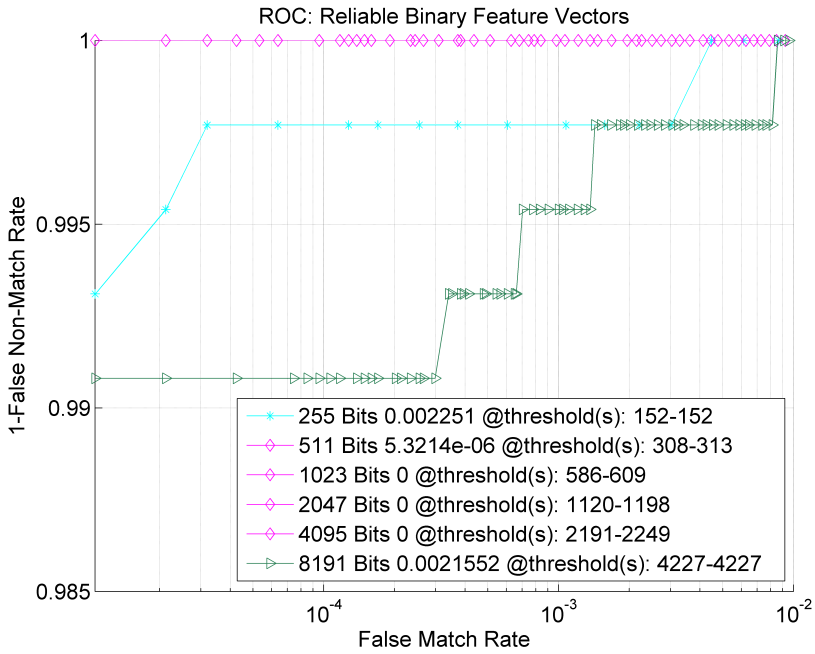


Figure 3.3: Receiver operating characteristic (ROC) of reliable binary feature vectors using Hamming distance, length: 255-8191 bits. Logarithmic scale on x-axis. Legend: selected reliable bits, EER, threshold(s). Note that the graphs for 512-4096 bits are overlapping.

As indicated by the threshold values in the legend of the figures, there is still a large intra-class variation. This is verified when investigating the score distributions: imposter scores are located close to 0.5 using a normalized Hamming distance, indicating almost random variations in the comparison pairs. However, genuine attempt scores are also high, indicating high Hamming distances. A BCH error correction code, as used in HDS, has limited capacities for the correction of the codewords, even if 30% of bit errors could be corrected, a FNMR of more than 35% would be the result (with 0% FMR). More research is needed to solve this issue.

3.3 Future Directions

Many interesting aspects about vascular pattern recognition are already discussed in Chapter 2. Here we want to summarize the future work for the different categories introduced in the sections of Chapter 2.

Imaging Three dimensional imaging of vein patterns is an attractive research direction. The rich information included in the position of the veins is currently mapped on a two dimensional sensor. The depth information of the veins inside the limbs is lost. Most interesting candidate for the additional dimension is certainly the finger vein modality that is commonly captured with a transmission of light. Another line of research is the miniaturization for cheap and embedded sensors while maintaining the good biometric performance. The imaging from standard camera sensors as indicated by current work [219] is certainly promising as well. The general trend of constructing multimodal sensors is especially tempting for the hand area due to the richness of modalities including vascular biometrics. One aspect that will be critical for the commercial success is the open access to raw sensor information from vendors. This will likely increase the trust in the technology, catalyze future research and enable independent evaluations and the interoperability. This leads directly to the next aspect: **Circumvention** The security-by-obscurity paradigm for commercial products should be overcome and independent evaluation should be performed. The already mentioned trend of multimodal approaches for improved liveness detection needs to be explored. As discussed in Section 2.3.7 a clarification on the visibility of vein patterns that are captured post-mortem, after death, is needed for the liveness claims related with vascular pattern recognition. **Privacy issues** In the future the acknowledgment of the necessity of template protection from the vendors and from legislative authorities is needed for large-scale deployments and commercial interest. One interesting line of research motivated by our work is making use of the full potential of template protection schemes for new security protocols and applications. **Databases** Common standard datasets and common protocols for the assessment and comparison of algorithm performance are needed and the research community has started to work on this issue as described in Section 2.5. However, further dissemination is needed. **Feature extraction and comparison** Standardization of vein features and interchange formats exceeding the current standard [104] is needed. It does not acknowledge skeletonized vein patterns or minutiae-based representations as data format. Also the wrist area is not specified as body region for the imaging of vascular patterns. As mentioned earlier, the independent performance analysis of commercial vein sensors of the latest generation is recommended to support the claims of the vendors and to have confidence in large-scale biometric systems based on vein patterns. In general the assessment of algorithms according to the above mentioned standard testsets and procedures will be useful. Future feature extraction and comparison algorithms for vascular patterns should be designed to be utilized for template protection schemes. To further improve the recognition accuracy, algorithm fusion based on the different abstraction levels of vein patterns (pixel, skeleton, minutiae) are an interesting line of research.

One of the practical questions raised during our work is if the trusted sensor and environment, that BTAP requires for securing online banking transactions, can be replaced with

mobile devices? The current work on utilizing the sensors of mobile devices for biometric purposes and the approaches for imaging vein patterns with standard sensors certainly motivates to investigate in this direction.

The optimization of the full parameter space of the spectral minutiae pipeline is future work that might close the performance gap in the investigated databases to the state of the art. Furthermore the pipeline will be evaluated on publicly available datasets. With regards to multimodal approaches it is interesting to investigate if the spectral minutiae pipeline can be utilized for other modalities as well. In particular the finger knuckle pipeline introduced in the thesis needs an increased performance with fixed-length features.

In the following we want to focus on improvements of our own work.

3.3.1 Overcoming High Intra-class Variance

The quantization of the real-valued feature vectors produces features with a high intra-class variance. To overcome this problem, new methods have been developed. In [28, 29] the DROBA principle is introduced that optimizes the detection rate of a biometric system independent from the quantization scheme. Based on dynamic programming and greedy search, L bits from a feature vector are selected. Instead of extracting exactly b bit for each component, none, one or several bits can be extracted depending on the influence on the detection rate. It could be shown that the false accept rate (FAR) is similar to fixed b-bit systems as utilized in our approach, but the false reject rate (FRR) is lower. Since the FRR is the system performance equivalent of the FNMR, this approach could improve our solution. Per contra the DROBA approach has a disadvantage as shown in [117]: since the mapping from component to number of extracted bits is individual for a data subject, the leakage of this additional helper data is leaking information that can be utilized by an adversary to improve the probability of false accepts. It could be empirically estimated, that if DROBA is restricted to two or three bits per component, this problem can be minimized without influencing the biometric performance.

Another approach is presented in [261], where the feature space of the spectral minutiae representation is first reduced by using Principal Component Analysis (Column-PCA) on the columns and the Discrete Fourier Transform (Line-DFT) on the lines. PCA is decorrelating the features, however a direct application to the spectra is not feasible. To overcome the small sample size problem it is applied to the columns of the spectral minutiae, effectively increasing the training sample size. Another problem is solved with this approach too: the rotation invariance of the spectra is based on circular shifts of the columns, when using Column-PCA the spectra do not need to be aligned since only the column sequence is changed which does not effect the training. Features in the horizontal direction can be reduced using Line-DFT in combination or independent of Column-PCA, since each line spectrum is periodic. The number of columns respectively elements of the spectra that are kept define the feature reduction rate. The reduction of the feature size does not affect the recognition performance significantly. However, lower FNMR could not be measured and therefore the approach does not solve the mentioned problem directly. The authors recommend further feature reduction using PCA and Linear Discriminant Analysis (LDA) with a ROBA bit extraction scheme or a 2D Gabor bit extraction for the combination with fuzzy commitment-based template protection schemes like the HDS.

In [262] two binarization schemes are presented based on [261]. *Spectral bits* are extracted from Column-PCA-reduced real-valued spectra. From each component one bit is extracted based on its sign, a masking-out of elements close to zero increases reliability. *Phase bits* are extracted using Line-DFT feature reduction on the spectra. Masking is applied as in the latter case, but here each complex-valued element is mapped to two bits depending on the signs of the real-valued and the imaginary component. An experimental analysis revealed that the performance of the binarization hardly influences the biometric performance. Fusion of the quantized features reduced the FRR slightly. The bit masking can be implemented within the HDS using the reliable bit selection.

In a recent work on spectral minutiae for fingerprint [205], the large intra-class variation with error rates above 40%, could be resolved using a new 3-layer coding scheme. The approach proposes to add additional redundancy: to utilize erasure codes – here fountain codes [145] – on partitions (packets) of the secret as an extra layer of encoding and an insertion of zeros in the quantized biometric information. The codes have the property that after receiving a certain number of packets the original information can be reconstructed. The name follows the idea of filling a bucket from a fountain: it does only matter that the bucket is full. In the proposed algorithm every packet is then encoded with an ECC. The insertion of zeros in between consecutive bits ensures that half of each packet is received correctly. Results on the FVC2000-DB2 fingerprint data show a similar performance of unprotected and protected features around 6% and 6.5% EER eventhough the fractional intra-class distance was very high with 40%-50%. The results of the unprotected features are similar to the case of our proposed vein pattern system, hence it can be expected that the approach is applicable.

Instead of increasing the bit extraction, in the earlier steps of the pipeline an extensive optimization of the parameters for the feature extraction algorithm could further improve the quality and stability of the feature vectors.

A different approach is focused on increasing the quantity of information: if data from multiple modalities is available, longer feature vectors could be created by simply concatenating them. The component selector can then chose the most reliable components from more sources. In this context a combination with other hand-based modalities does make sense. In Chapter 10 we tried to create fixed-length SURF feature vectors from finger (knuckle) skin images with limited success. We want to use of the fact that the proposed biometric pipeline is based on spectral minutiae, the same algorithm proved to be effective with fingerprint data. The feature vectors can be fused on feature level or as a concatenated form in the HDS to decrease the intra-class variance.

3.3.2 Updating Template Protection Schemes

The helper data scheme is investigated extensively in the related literature such as in [288]. Kelkboom in [116] recommended improvements to the HDS based on their latest research work: DROBA-based bit extractors should be limited to avoid reversibility, linear error-correcting codes should not be used to avoid linkability of templates, a bit randomizer should be applied before the storage to overcome decodability attacks and finally subject specific helper data should be utilized with care. Those modifications should be considered for the HDS-core of the BTAP.

Another question still to be answered is the long-term security of PET-protected biometric templates. The answer is out of the scope of this work, but nonetheless interesting and important to discuss. Can we ensure the security, and therefore the privacy, for the next decades with drastic technological changes ahead? Are we and the PETs prepared to face a post-quantum-computer time?

3.4 Conclusions

As we could show, the biometric modality of vein pattern recognition is an interesting candidate for biometric cryptosystems: it is more privacy-preserving than most modalities due to the position in the body and it reaches high recognition accuracy. We could confirm that the approach of utilizing minutiae – similar to fingerprint minutiae – for vein patterns is valid regarding the biometric performance. Minutiae points are the most common feature for utilization with template protection schemes, including the most prominent instances fuzzy commitment and fuzzy vault. Furthermore elaborate representations and comparison algorithms like the spectral minutiae and the minutia cylinder-codes have been proposed for minutiae points. This knowledge is accessible for vein patterns as described in this thesis.

Concluding the latest results it can be stated that the proposed vascular biometric system based on spectral minutiae is delivering high recognition performance in binary feature vector form. The vectors are of fixed length and structure, very compact and could be utilized in scenarios with limited storage capacities for templates, for large-scale systems where comparison speed is essential, and for biometric indexing. Another interesting point of this work is that multimodal systems based on palm vein and fingerprint, as currently developed, could be based on the very same spectral minutiae feature extraction system.

The constitutes a work major step towards utilizing vascular patterns with template protection schemes to further enhance the strong points of the modality. As the features are compatible with the HDS template protection scheme and it is one core building block of the Biometric Transaction Authentication Protocol (BTAP), online banking transactions can be secured using vascular patterns when the before mentioned problems of the high intra-class variance are solved. In Section 3.2 we pointed out solutions to the high this problem.

Then, an alternative to TAN-based systems can be realized that solves the problem of repudiation for service providers, while an improved convenience for customers can be offered. The usage of a privacy protection scheme prevents leakage of sensitive information, cross-matching and profiling. In addition concerns from the data subjects to use biometrics can be reduced and legislative privacy protection requirements can be fulfilled.

Bringing the work into a larger perspective, we can state that BTAP is one of the first instances where a biometric system is shifted from a binary authentication decision-making scheme to an integral part of an abstract security protocol. The possibility to share information with a strong non-repudiation property has initiated a paradigm shift in the biometric research.

Other approaches are focused on general schemes for secret sharing (session key) for secure communication and for mutual authentication between clients and servers [110] or between two clients using a trusted third party [111]. The protocols are based on the fuzzy commitment and extend it with additional permutations for template diversification, and for the usage of multiple biometric features. Instead of a simple authentication decision based on the released secret it is used as renewable session key for a secure communication. The approach of *bipartite biotokens* [197, 198], extends the concept of fuzzy vaults [108] for fingerprint minutiae to allow the generation of public and private biometric template parts. The authors describe in [195, 196] how this concept can be utilized to realize biometric public key infrastructures.

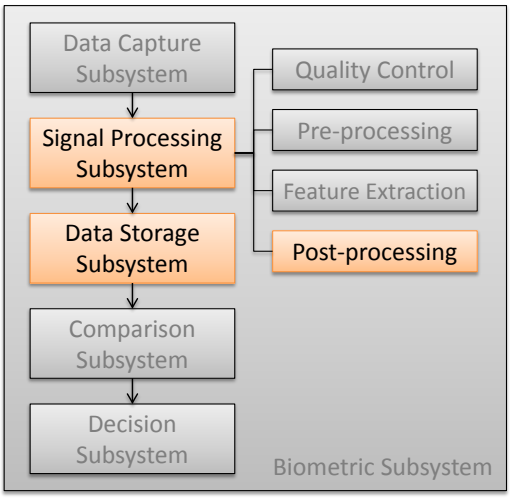
In BTAP, data from the application is directly combined with keys released from biometric templates, only the key needs to be stored at the server side for authentication. It is designed to sign small amounts of data that can be visualized within a secure environment (e.g. for online banking transactions). General digital biometric signature schemes and biometric message authentication primitives with a strong relation to a natural person are the next step. Issues that need to be addressed are the "what-you-see-is-what-you-sign"-problem of current computer systems and the extraction of strong keys from biometric samples.

Part II

Research Papers

Chapter 4

Why Vein Recognition Needs Privacy Protection



This paper motivates the application of privacy enhancing technologies (PET) in biometric systems based on vein patterns. In the biometric pipeline this can be implemented in the post-processing block of the features, hence the highlight in the overview figure above. Sensitive medical information can be extracted from the vein images as shown here and further discussed in Section 2.4. Early experiments show the applicability of such a PET, namely the helper data scheme (HDS). The introduced feature extraction and comparison approach is however dependent on the registration of the images which is not applicable in the HDS.
The paper was published in: [71] HARTUNG, D., AND BUSCH, C. Why vein recognition needs privacy protection. In Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 09) (September 2009), pp. 1090-1095.

Abstract

This paper describes the emerging biometric modality of vein recognition and privacy concerns that arise with its widespread use. Current sensors are able to capture vein patterns inside the human body, this is considered as a "private" biometric characteristic. In fact two medical disease patterns are presented that can be extracted from the vein patterns. In order to be compliant with data privacy protection laws privacy enhancing mechanisms have to be applied in vein recognition systems. Experiments of applying the helper data scheme to a back-hand vein database were conducted with remarkable results. A privacy-enhanced verification system can be realized, which shows good biometric performance under laboratory conditions.

4.1 Vein Recognition

The randomness of vein patterns is epigenetic, even identical twins can be distinguished. During the embryonic period the blood vessels are formed, this process of growth is not determined by the DNA sequence.

The pattern is available at every healthy human, making it an interesting research objective. Commercial applications evolved out of this research, nowadays many ATMs in Japan and Brazil are secured using this biometric modality. With the upcoming changes of the liability situation in the Single Euro Payments Area (SEPA) it is likely that this biometric technology will also be widespread in Europe.

The patterns are commonly extracted from images of the palm, the back of the hand or fingers as seen in Figure 4.1. Recently Yanagawa et al. showed that the diversity of finger vein patterns among different persons is competitive to iris-based systems [269]. The International Biometrics Group (IBG) 6th report 2006 confirms recognition rates fairly at the same level for two different vein and one iris-based authentication system [94]. An interesting aspect of vein recognition is the fact that the information is not visible, it is hidden inside the body. Unlike fingerprints it is not possible to leave a vein pattern representation unintentionally in public places and thus it is not possible for an attacker to acquire the pattern in daily life or to replicate it. Furthermore there is no relation to criminal prosecution. How vein images are captured is described in the next section.

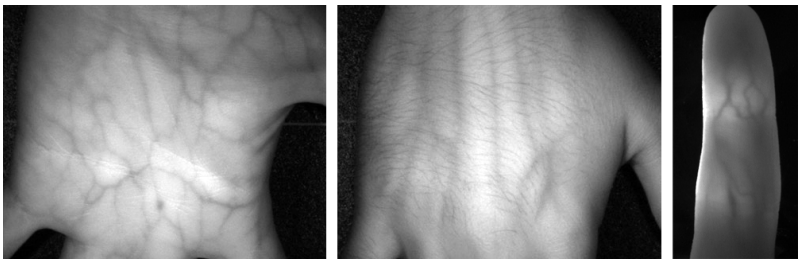


Figure 4.1: Palm, back-hand taken from [241] and finger vein images [81]

4.1.1 Imaging Techniques

The imaging approach makes use of the absorption capacity of particular substances in the blood running through the veins. To capture the image, the region of interest is illuminated with a near-infrared (NIR) light source with wavelengths around 700 to 1,000 nm. A reflection or transmission technique can be used. Deoxygenized hemoglobin highly absorbs rays within this wavelength band while the surrounding tissue does not. NIR-sensitive optical sensors are used to capture the image of the vein pattern. Examples are shown in Figure 4.1.

The diameter of the blood vessels and their depth inside the body are limiting factors for the feature extraction process, which is described in the next section.

4.1.2 Feature Extraction

The feature extraction process is starting from a captured vein image sample. The pattern, the abstract structure of the veins, has to be extracted from the noisy vein image, a sample is shown in Figure 4.2 taken from [159]. Features used for comparison are localized in the extracted vein skeletal pattern. Various algorithms are published based on line tracking [157], local thresholding [241], curvelets and neuronal networks [286], as well as maximum curvature points [159]. The algorithms of those publications all have the same outcome: a vein pattern for authentication purposes, which needs to be stored and processed. Example vein patterns are shown in Figure 4.2 and 4.3. Why this may conflict with privacy protection directives is explained in the following section.

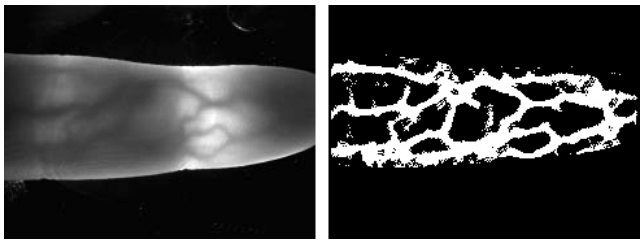


Figure 4.2: Finger vein image and corresponding vein pattern based on maximum curvature points [159]

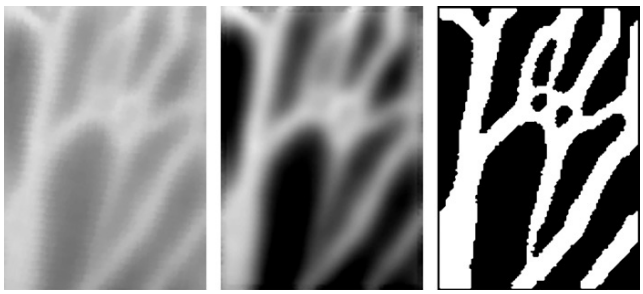


Figure 4.3: Original vein image, after noise reduction and after local thresholding [241]

4.2 Privacy Concerns

Biometric systems are exposed to privacy concerns since there is an intrinsic link between the stored biometric template and the person it originates from. The advantages, offered by biometric authentication, are inverted when the stored data is stolen – the data theft becomes an identity theft. The problem is that you cannot simply change a biometric characteristic like a key or password. Revocation and reissuing of a specific biometric characteristic is not feasible in common biometric systems.

Another privacy related aspect is cross-matching: if the same modality is used in different application contexts (access control, financial services, eCommerce services etc.), a profile can be constructed linking the stored data in different databases.

Furthermore biometric data can contain information about physical traits of humans - the risk of storing medical or health related information is therefore always existent.

4.2.1 Medical Issues with Vein Patterns

Diseases related to the cardiovascular system are among the main causes of death in the world [256]. Vein patterns used in biometric systems could also reveal information about the medical state of a human. The authors found several examples of vascular diseases related to the finger or the hand.

In general the diameter and the position of the veins are of medical interest. An example is thrombosis, where a blood clot (thrombus) blocks the blood flow in the cardiovascular system. Diseases changing the position and the structure of the vein network affect all feature extraction methods resulting in a vein pattern.

After a literature survey on radiological publication two examples of disease patterns are found that change the appearance of the hand vein pattern: arteriovenous malformation (AVM) is a congenital disorder where veins and arteries are connected in an abnormal way. A contrast-enhanced radiographic example is given in Figure 4.5 taken from [131]. Another abnormality is the hypothenar hammer syndrome (HHS) which is also identifiable throughout the vein pattern of the hand (Figure 4.4 taken from [131]). HHS is a thrombosis of the superficial palmar arch of the ulnar artery and is caused by repeated mechanical force, as seen in fighting sports or the work with vibrating tools (e.g. a hammer).

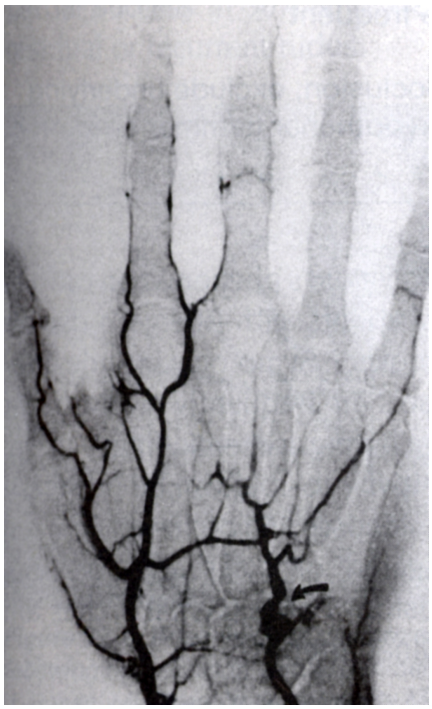


Figure 4.4: Hypothenar hammer syndrome [131]

Those examples illustrate that vascular image data may contain health related information. Since the ISO standard for the vascular interchange format [103] uses those image based vein patterns, the medical information is still available in the stored references. The next section describes the legislative view on this special kind of personal data.

4.2.2 Legislative Regulations

Special acts are implemented to secure the privacy rights of individuals. An introduction to data protection and biometric systems is given by Meints in [149]. In the following the relevant European and the Norwegian regulations are introduced.

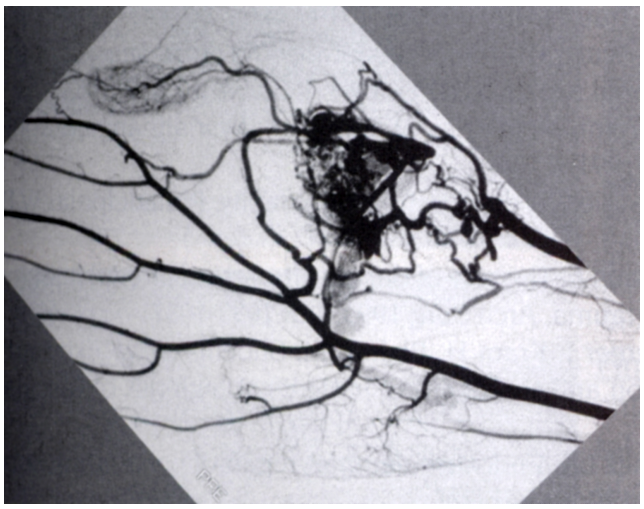


Figure 4.5: Arteriovenous malformation [131]

The European data privacy principles are formulated with the "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data". In article 2 important terms are defined, interesting in our context are the first two definitions (a) and (b) of "personal data" and its processing, which covers the usage in biometric systems. Article 8 specifies the handling of health related personal data. Generally member states should prohibit processing of this "special category of data". Article 6 (c) defines the need for the adequateness and non-extensiveness of the data in relation to its purpose.

The Norwegian "Act of 14 April 2000 No. 31 relating to the processing of personal data (Personal Data Act)" follows the European directive with some differences, nevertheless the definitions for "personal data" and "processing of personal data" also apply to our context. Section 2 defines health related information as "sensitive personal data".

These two regulations both challenge the common praxis in biometric systems based on vein recognition. As shown, vein data may contain medical, health-related information and therefore the principle of adequateness in a biometric authentication system is violated. Since the usage is prohibited by law, the stored data has to be transformed into a non-revealing form.

Current research on template protection [186, 225, 289] show one possible way to construct biometric authentication systems that satisfy the regulations. After the enrolment of a data subject, no information about the original biometric sample is revealed. Even for the comparison of templates the biometric information does not need to be revealed as needed in the classical case of encrypted databases.

4.3 Experiments

The following experiments show a solution to the data privacy challenges associated with vein images. A feature extraction algorithm based on local thresholding [241] is used to extract vein patterns from backhand vein images. These feature vectors are then further processed to be compliant with the helper data scheme for privacy enhancement [225]. Finally the performance based on the raw feature vectors and the processed versions is evaluated.

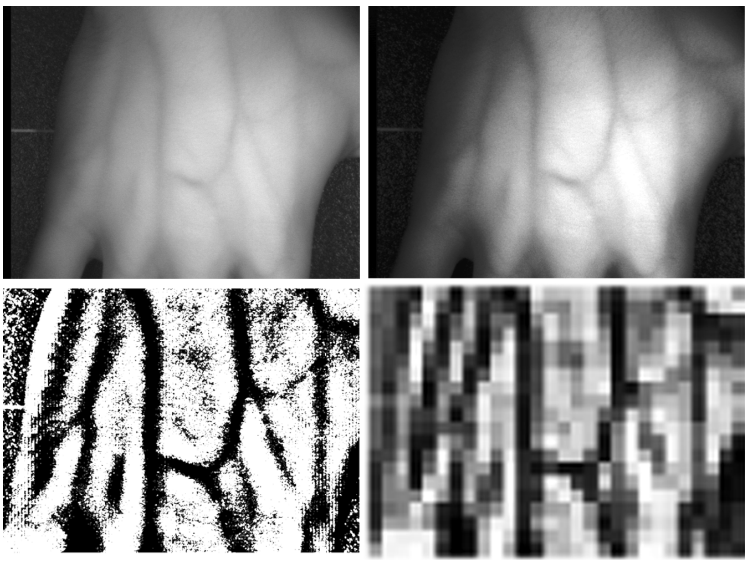


Figure 4.6: Processing steps of the feature extraction algorithm: normal image, histogram optimized, local thresholding applied [gray-scale representation of binary image], resized feature image.

4.3.1 Database

The database was gathered by the Nanyang Technological University in Singapore [164] and consists of a near infrared and a far infrared part. The near infrared part, that is used in the experiments, contains 122 data subjects with 3 samples for each hand taken in one session with a reflection technique. The resolution of the gray-scale images is 644 x 492 pixels.

4.3.2 Feature Extraction

Features are extracted directly from the histogram-optimized images, the local thresholding algorithm [241] was used. The value of each pixel in the feature space f is affected by the surrounding pixels of the original image I: if the pixel intensity exceeds the mean value of a defined area around the actual one it is set to 255, otherwise 0.

$$f(x,y) = \begin{cases} 255, & \text{if } I(x,y) > \mu_{I(x,y)} \\ 0, & \text{otherwise} \end{cases}$$

The parameter μ was set to the mean of 30 x 30 pixel blocks, after this step 50 pixels were cropped from each edge of the feature image due to irregularities at the boarders. The resulting feature image has a resolution of 544 x 392 pixels. To further decrease the variance[1] caused by noise, the images were resized[2] with factor 20 to a size of 28 x 20 pixels. Resulting feature vectors have 560 elements[3]. Figure 4.6 shows the three different steps towards the feature vector.

4.3.3 Privacy Enhancing Mechanism

Among the several privacy enhancing mechanisms is the helper data scheme [225] which is sketched in Figure 4.7. The scheme can process any biometric data, as long as the created

[1] Variance between samples from the same source.
[2] By means of bicubic interpolation.
[3] Composed by concatenating rows of the image.

feature vectors have the same dimension. Basically the biometric data is merged with a random secret into a secure form during the enrolment. Beforehand feature vectors are binarized, reliable bits are extracted. These bits are combined using boolean exclusive or (XOR) with an error encoded random and secret bit vector. The hash of the secret, the indexes of the reliable bits (helper data) and the secured template are stored in the database.

During the verification the data belonging to the biometric claim is loaded. The probe feature vector is binarized again, bits are extracted using the stored reliable indexes. The boolean XOR is applied to the stored secured template and the probe reliable bit vector. The hash of this result is compared with the stored hash. If the error decoder is able to correct the bit flips caused by noise, an identical hash value is produced, the biometric claim is verified.

In the experiment a reliable bit vector is generated from an intermediate (unprotected) feature vector in the following manner:

1. Center the feature vectors around its mean (subtract the mean from each feature vector).

2. Map every value to binary 1 exceeding zero (larger than the mean), the rest to binary 0 (smaller than the mean).

In this way, the bits are equally distributed and statistically independent. The binarized feature vectors consist of 560 bit values each.

The reliable bit extraction block estimates the optimized reliability and discrimination power R of every component k for each subject i. Assuming Gaussian distributed components, the following formula can be used:

$$R_{i,k} = \frac{1}{2}(1 + \mathrm{Erf}(\frac{\mu_{\mathrm{intra}} - \mu_{\mathrm{inter}}}{\sqrt{2v_{i,k}}}))$$

Here the variance (v), the intra-class mean (μ_{intra}) and the inter-class mean (μ_{inter}) has to be computed in advance. Erf stands for the Gaussian error function.

The components having the highest reliability value R are selected as candidates for the reliable bit vector. Since those vectors are used in the helper data scheme, performance estimations can be computed for the whole system taking into account the error correction capability of the ECC-block.

4.4 Results

4.4.1 Unprotected Features

The histograms of genuine and imposter attempts are shown in Figure 4.8(a) for the unsecured 560-dimensional feature vectors. A good performance with an equal error rate at 0.55% is measured (Figure 4.8(d)) using the 1-correlation as distance metric.

4.4.2 Binarized Features

The extracted binary feature vectors perform at about the same level as the unprotected feature vectors. The distribution using the Hamming distance is shown for genuine and imposter attempts in Figure 4.8(b). The DET is shown in Figure 4.8(d), the equal error rate is around 0.55%.

4.4.3 Protected Features

The reliability estimation of the components leads to a mean value of 520 perfectly reliable bits per data subject. When selecting the the 255 most reliable bits from the binarized

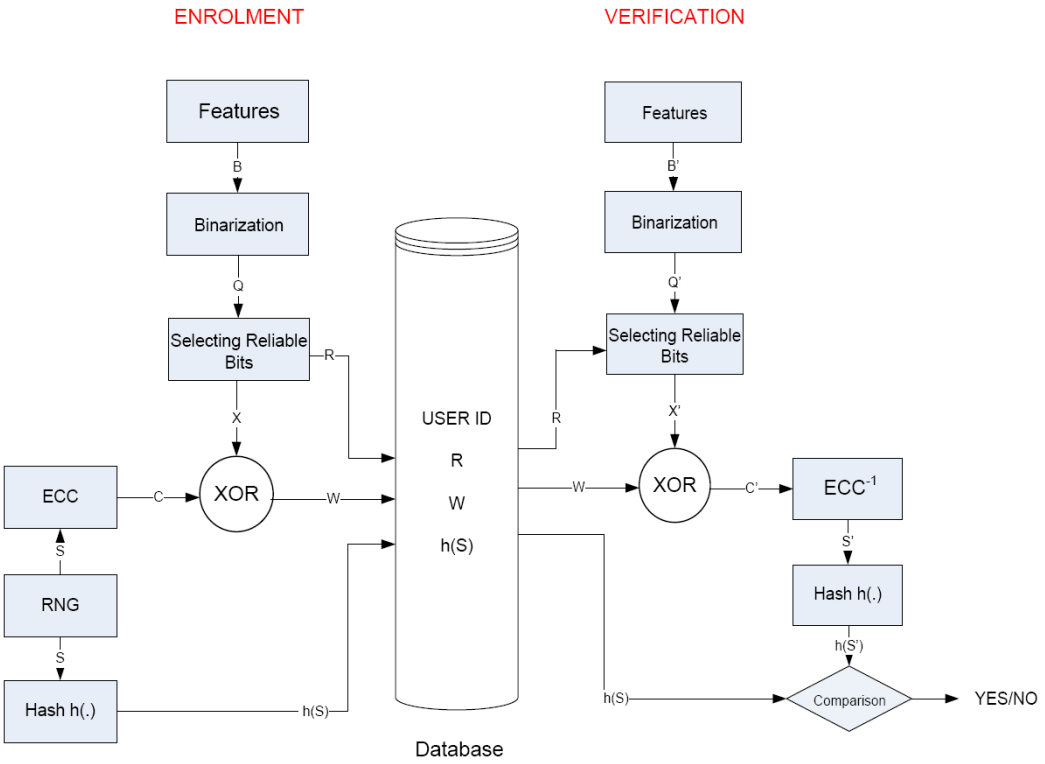


Figure 4.7: Block diagram of the helper data scheme.

feature vectors, performance is increasing. The reliable bit estimation was performed on 2 out of 3 samples per data subject. If training and validation sets are strictly separated, no FNMR can be computed. Considering the 2 samples taken for the reliability estimation as a stored reference for testing, no false non match was measured.

For a threshold in the Hamming distance of 0.18 no false match was measured as well. The distribution of genuine and imposter attempts are shown in Figure 4.8(c). Those reliable bit vectors could be used in the helper data scheme. In the case that the error correction block is able to correct 18% bit errors, imposters and genunies are perfectly separated and the privacy is protected. The DET-curve is also plotted in Figure 4.8(d).

4.5 Conclusions

In this paper the need for privacy enhancing technologies when processing vein data is shown: disease patterns are presented which can be extracted from vein patterns. No other publication is known to the authors that deals with this delicate topic. One possible solution is the application of a privacy enhancing scheme. The helper data scheme satisfies the regulations, because no information about the biometric characteristic can be extracted from the stored secure template and the helper data.

The experimental section describes a feature extraction algorithm based on local thresholding and the binarization and reliable bit extraction block of the helper data scheme. For the first time a privacy enhancing scheme was applied in the context of back-hand vein data. The results are remarkable, a robust authentication system guaranteeing privacy can be constructed for this specific database of 122 data subjects.

It has to be mentioned that the performance can only be reached in laboratory environments – the database was taken in only one session, the variation in the original data

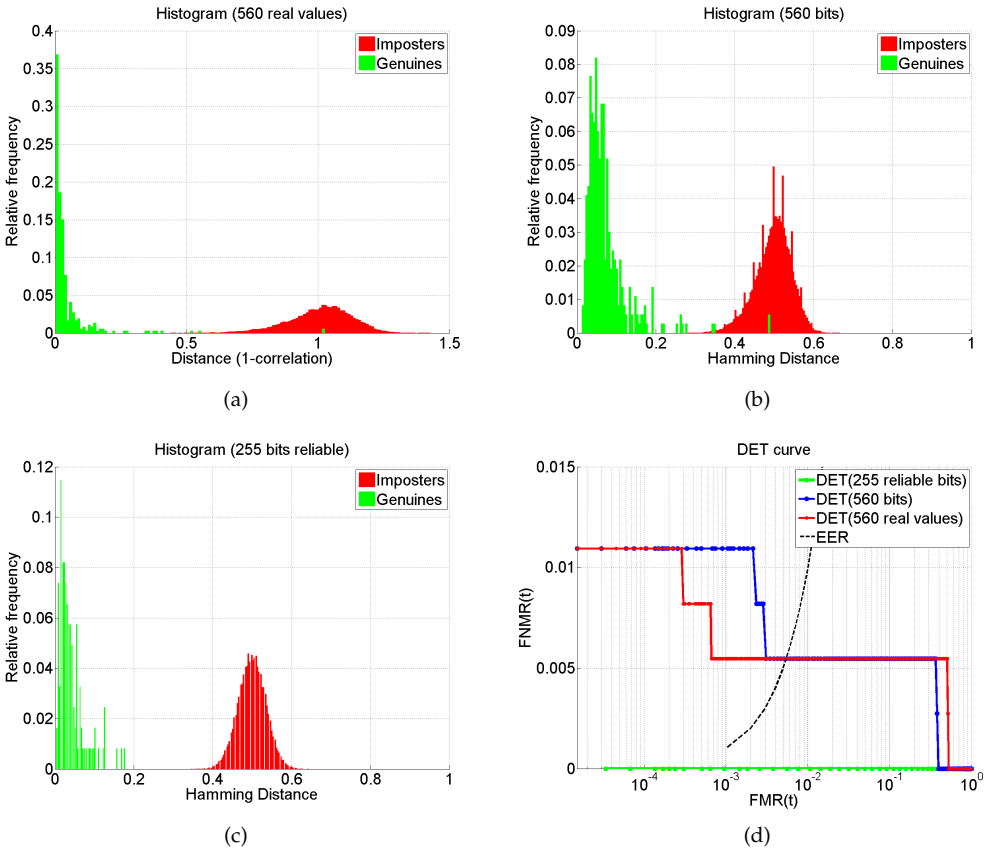
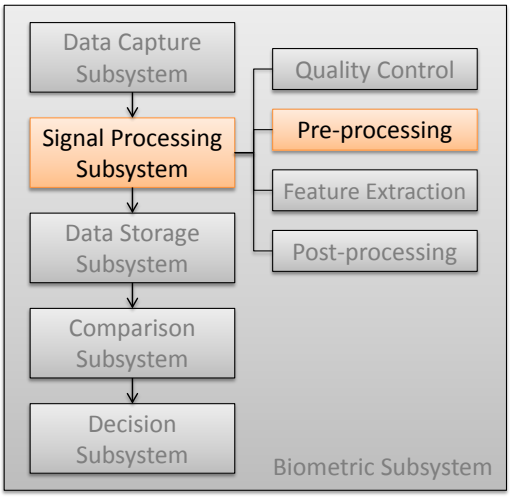


Figure 4.8: Histogram of genuine and imposter attempts: (a) unprotected 560-dimensional features, (b) 560-bit features, (c) reliable binarized features; (d) DET curves of the different feature vectors.

is therefore fairly low. To confirm the results of the experiments a large-scale database is needed and in preparation. Further research is needed in the field of normalization of vein images. To satisfy security constraints in the helper data scheme long reliable bit features are needed, multimodal, multi-spectral solutions could be the way to go.

Chapter 5

Contrast Enhancement and Metrics for Biometric Vein Pattern Recognition



On the way to an effective pipeline for biometric vein recognition, the pre-processing and specifically the contrast enhancement are of interest. The investigation revealed, that a trade-off between the level of contrast enhancement and additional noise introduction has to be made. Differences in processing capabilities of integrated sensors could further restrict the choices of algorithms, hence statistics about the efficiency are included in the work.
The paper was published in: [168] OLSEN, M. A., HARTUNG, D., BUSCH, C., AND LARSEN, R. Contrast enhancement and metrics for biometric vein pattern recognition. In Advanced Intelligent Computing Theories and Applications, vol. 93 of Communications in Computer and Information Science. Springer Berlin Heidelberg, 2010, pp. 425-434.

Abstract

Finger vein pattern recognition is a biometric modality that uses features found in the blood vessel structure of the fingers. Vein pattern images are captured using a specialized infrared sensitive sensor which due to physical properties of the hemoglobin present in the blood stream give rise to a slight intensity difference between veins and tissue. We investigate five different contrast enhancement algorithms, which range from high to low computational complexity, and evaluate the performance by using five different quantitative contrast measuring methods.

5.1 Introduction

Contrast enhancement is an important aspect of vein pattern recognition due to uneven lighting and low contrast across the biometric sample as captured by infrared sensitive devices. The contrast between vein structures and the surrounding tissue is of special interest because the quality of the subsequent feature extraction depends on how well the vein structure can be separated from the rest of the image. Furthermore, the complexity of segmenting the image is lowered if the veins are clearly separated from the surrounding tissue. For the purposes of vein patterns it is desirable that the captured image has a high contrast. Highly sensitive sensors and controlled lighting environments can be used to achieve even illumination and good contrast in the resulting image but the cost for doing so can be prohibitively high. For biometric sensors, cost and size should be minimized in order for widespread adoption to occur. Low cost sensors and lighting setups yield lower quality images and thus it is necessary to perform digital post processing. We investigate the influence that several different contrast enhancement methods have on vein pattern samples from three vein pattern databases. By estimating the contrast gains achieved by the contrast enhancements we seek to establish a relationship between contrast and biometric performance.

5.2 Image Enhancement

In Wang et al. [242] a method for enhancing the contrast in back of hand vein pattern images acquired by a far infrared sensor is presented. The algorithm proposed can be divided into three steps: 1) Removal of speckling noise using a 5×5 median filter; 2) Suppression of high frequency noise using a 7×7 adaptive Wiener filter; 3) Image normalization based on local mean and variance. The image normalization is performed on a pixel-wise basis using (5.1). Here $I(x, y)$ is the source image value, μ and σ^2 are the image global mean and variance respectively, μ_d and σ_d^2 are the desired image mean and variance, and $I'(x, y)'$ is the contrast enhance image value.

$$I'(x,y) = \begin{cases} \mu_d + \sqrt{\frac{\sigma_d^2 \cdot (I(x,y)-\mu)^2}{\sigma^2}} & \text{, if } I(x,y) > \mu \\ \mu_d - \sqrt{\frac{\sigma_d^2 \cdot (I(x,y)-\mu)^2}{\sigma^2}} & \text{otherwise} \end{cases} \tag{5.1}$$

5.2.1 Spatio-Temporal Retinex-like Envelope with Stochastic Sampling.

The Spatio-Temporal Retinex-like Envelope with Stochastic Sampling (STRESS) algorithm [120] is an image contrast enhancing algorithm which is inspired by the properties of the human eye. The algorithm works on a per pixel basis. Local references for maximum and minimum values are found and used as an envelope for each pixel. The pixel value is updated using a linear scaling between the maximum and minimum envelopes for local contrast enhancement. A stochastic sampling (pixel count is N_s) around and including each pixel ($I(x, y)$) within the Euclidean distance d is used in order to determine the maximum and minimum intensity value in the neighborhood of the pixel. The pixel count

determines how well the neighbor minimum and maximum intensities are estimated; if too few pixels are visited then the estimate is likely to deviate from the true minimum and maximum values. It is possible to visit the whole neighborhood to increase precision but this will increase computation time as this has to be done for each pixel. The maximum and minimum values $s_{\max}$ and $s_{\min}$ are then used to determine the neighborhood intensity range r (5.2) and the relative intensity value v of the center pixel (5.3).

$$r = s_{\max} - s_{\min} \tag{5.2}$$

$$v = \begin{cases} 1/2 & \text{, if } r = 0 \\ (I(x,y) - s_{\min})/r & \text{, otherwise} \end{cases} \tag{5.3}$$

To prevent outliers in the intensity range an average over N_i iterations is calculated:

$$\bar{r} = \frac{1}{N_i} \sum_{i=1}^{N_i} r_i \tag{5.4}$$

$$\bar{v} = \frac{1}{N_i} \sum_{i=1}^{N_i} v_i \tag{5.5}$$

The envelopes $E_{\max}$ and $E_{\min}$ are calculated:

$$E_{\max} = I(x,y) - \bar{v}\bar{r} \tag{5.6}$$

$$E_{\min} = I(x,y) + (1-\bar{v})\bar{r} = E_{\min} + \bar{r} \tag{5.7}$$

The envelopes are used as local references for respectively the lowest (black) and highest (white) possible intensities. If $I(x,y)$ is close in intensity to the local highest intensity as defined by $E_{\max}$ then the intensity of $I(x,y)$ should be close to white in the image. A linear scaling between $E_{\max}$ and $E_{\min}$ is performed on $I(x,y)$:

$$I'(x,y) = \frac{I(x,y) - E_{\min}}{E_{\max} - E_{\min}} \tag{5.8}$$

For out experiments we use $r = 20, N_s = 20$ and $N_i = 20$.

5.2.2 Partitioned Iterated Function System Based Contrast Enhancement.

A contrast enhancement algorithm based on the theory of Partitioned Iterated Function System (PIFS) was proposed by Economopoulos et al. [51]. PIFS is based on the self-similarity found within an image and its main application is in image compression. The main components of the contrast enhancement approach is to partition the image $I(x,y)$ into two sets of blocks. The blocks in the first set are known as range blocks while those in the second set are called domain blocks. The range blocks are non-overlapping and of size $w_x \times w_y$ pixels and each contain a vector of pixel values in I which are covered by the range block. The domain blocks are of size $2w_x \times 2w_y$ pixels and each contain a vector of the average value of pixel intensities in each distinct 2×2 sub-block within I that is covered by the domain block. The range blocks and domain blocks are indexed by their position in I and are addressed as respectively r_{ij} and d_{kl}. The set of range blocks have a corresponding set of mean values, $\mu_{R_{ij}}$, of each vector r_{ij}. Similarly for the domain blocks, $\mu_{D_{kl}}$ contains the mean value of the vector d_{kl}. For each range block r_{ij} a domain block which minimizes the squared Euclidean distance is found with the expression:

$$E(k,l;i,j) = ||\gamma(d_{kl} - 1\mu_{D_{kl}} - (r_{ij} - 1\mu_{R_{ij}})) \tag{5.9}$$

In (5.9) γ is a predefined contrast parameter constant. The minimization process results in a mapping where each range block has a corresponding domain block. Next, a global contractive transform is performed on I as

$$W(I)(x,y) = \sum_{ij}[\gamma(I(2(x-x_i)+u_{k(i,j)}, 2(y-y_j)+v_{l(i,j)}) - \mu_{D_{k(i,j)l(i,j)}})] + \mu_{R_{ij}} \quad (5.10)$$

Using Equations 5.9 and 5.10 the image is encoded using $\gamma = 0.8$. The encoded image is decoded by reapplying Equations 5.9 and 5.10 with $\gamma = 0.1$. The result,$I_{\mathrm{LP}}(x,y)$ is a low-pass version of $I(x,y)$. A high-pass version is obtained by $I_{\mathrm{HP}}(x,y) = I(x,y) - I_{\mathrm{LP}}(x,y)$. Finally, the contrast enhanced image $I'(x,y)$ is obtained by:

$$I'(x,y) = I(x,y) + \lambda I_{\mathrm{HP}}(x,y) \quad (5.11)$$

where λ adjusts the contrast gain. In our case we set $\lambda = 1.0$ and $w_x = w_y = 4$).

5.2.3 Linear Unsharp Masking.

The linear unsharp masking approach is constructed as a 3×3 negative Laplacian filter as shown in (5.12). The mask is applied to I resulting in a highpass version I_{HP}. The enhanced image is obtained using (5.11).

$$h(x,y) = \begin{bmatrix} 0 & -1 & 0 \\ -1 & 4 & -1 \\ 0 & -1 & 0 \end{bmatrix} \quad (5.12)$$

5.2.4 Contrast Limited Adaptive Histogram Equalization.

Contrast Limited Adaptive Histogram Equalization (CLAHE) [292] is a histogram equalization method which operates by partitioning the image into regions and perform histogram equalization on each region separately. The equalization is performed by computing the cumulative distribution function for each $w_x \times w_y$ region.

5.3 Contrast Metrics

Measuring contrast is possible with different approaches, a standardized solution does not exist. As contrast measurement and evaluation is not uniquely defined for all images we include several methods for this purpose. To assess the performance of the contrast enhancing algorithms discussed in Section 5.2 we apply five quantitative contrast measurements to the enhanced images. The contrast gain C_{GAIN} is found as

$$C_{\mathrm{GAIN}} = \bar{C_{I'}} - \bar{C_I}, \quad (5.13)$$

where I is the source image and I' is the contrast enhanced image.

5.3.1 PIFS contrast enhancement metric

In [51] a contrast metric is proposed where the contrast at pixel location (x,y) is expressed by

$$c(x,y) = \frac{lv(x,y)}{lm(x,y)}, \quad (5.14)$$

where lv is the variance and lm is the mean. The PIFS contrast enhancement metric is thus found by first determining the ratio of the image intensity variance and the image intensity mean in a sliding $w_x \times w_y$ window, and then taking the average of this ratio across the entire image. The method is robust towards small changes in image intensity.

5.3.2 Weighted-Level Framework Contrast

In [208] the Weighted-Level Framework (WLF) contrast measurement method is introduced. The method is divided into several steps: the image is first sub-sampled at several levels to create a multi-level pyramid. On each level the local contrast is computed to create local contrast maps. The global contrast measure is obtained by performing a weighted recombination of the local contrast maps.

5.3.3 Michelson Contrast

The Michelson contrast [152] is defined as

$$C_{\text{michelson}} = \frac{I_{\max} - I_{\min}}{I_{\max} + I_{\min}}, \tag{5.15}$$

where $I_{\max}$ and $I_{\min}$ are the maximum and minimum luminance levels. Thus, for an image which covers the entire dynamic range the contrast will be regarded as maximal. The Michelson contrast measurement is expected to be a relatively poor estimator of contrast because a small change (e.g. a single pixel) in either maximum or minimum intensity can lead to a large change in the estimated contrast. The Michelson contrast value ranges from 0 to 1.0.

5.3.4 Local Michelson Contrast

The idea of the Michelson Contrast is pushed further on through applying the metric on subsets of the image. Inspired by [10], we use a local version of the Michelson Contrast with the following properties: Three different block sizes are chosen that divide the image into subparts, those parts are then evaluated by the original Michelson Measurement. The block size $w_x \times w_y$ are generated in each of the three iterations $i = 1, ..., 3$ from the image size $s()$ in the following manner:

$$w_{x_i} = \frac{s(x)}{10i} \tag{5.16}$$

$$w_{y_i} = \frac{s(y)}{10i} \tag{5.17}$$

The Local Michelson Contrast (LMC) metric is the average of the resulting values from all iterations on all non overlapping sub pixel blocks of the given sizes $w_x \times w_y$.

5.3.5 RMS Contrast

The RMS contrast [174] is defined as

$$C_{\text{RMS}} = \sqrt{\frac{1}{MN} \sum_{x=0}^{N-1} \sum_{y=0}^{M-1} (I(x,y) - \bar{I})^2}, \tag{5.18}$$

where I is normalized such that $0 \leq I(x,y) \leq 1$ and $\bar{I}$ is the mean image gray level. The RMS contrast is independent of the spatial distribution of contrast and the frequency content. As the metric is more robust towards small changes in the images it is more suitable for estimation of contrast between several images than the Michelson contrast.

Property	GUC45	SingaporeNIR	SingaporeFIR
Frequency Band	NIR	NIR	FIR
Modality	Finger (10)	Back of Hand (2)	Back of Hand (2)
Data Subjects	45	122	34
Sessions	12	1	1
Images per Session	10×2	2×3	2×3
Images	10.800	732	202
Resolution (px)	$512 \times 240^{\dagger}$	644×492	320×240
Depth		8 Bit gray-scale	
Samples in Experiments	540 (2.5%)	100	100

Table 5.1: Properties of the biometric vein datasets used in the experimental section. †For the experiment the images are cropped to size 468×122 to eliminate most non-finger area.

Method	Complexity (avg. ACT)	GUC45	SingaporeNIR	SingaporeFIR
STRESS†	high (8.86)	6.173	15.841	4.565
PIFS	very high (70.338)	44.145	133.448	33.42
CLAHE	low (0.033)	0.028	0.042	0.029
L.Unsharp M.	very low (0.002)	**0.002**	**0.002**	**0.002**
Wang	medium (0.386)	0.357	0.636	0.164

Table 5.2: Average Computation Times (ACT) of the contrast enhancement methods (in seconds per image, lowest marked in bold) for the different data sets and a complexity approximation based on the average ACT. †The STRESS algorithm is called as an executable external to MATLAB.

5.4 Experiments

In order to get a general idea of the contrast enhancement capabilities for different algorithms a broad set of biometric vein databases is being used for the experiments. The contrast enhancing methods Wang2007, STRESS, WLF, PIFS-based enhancement, linear unsharp masking, and CLAHE were applied to gray-scale vein pattern images from three biometric data sets: GUC45, SingaporeNIR, SingaporeFIR. The GUC45 dataset contains finger vein images as captured by a proprietary near infrared (NIR) sensor. The SingaporeNIR dataset contains back of hand vein pattern images obtained from a NIR sensor. The SingaporeFIR dataset contains back of hand vein pattern images obtained from a far infrared sensitive sensor. The properties of the sets are shown in Table 5.1, sample images are provided within the next section.

Table 5.2 gives an overview of the contrast enhancement methods and their computational complexity based on the average enhancement time per image from the evaluation.

Apart from the original image we have 6 images from applying the contrast enhancement methods to the original. The contrast of each image is computed using the 5 different contrast measurements.

5.5 Contrast Enhancement Results

For this reason several contrast measurement methods were chosen, to cover the spectrum of approaches, from perception-oriented to simple and fast mathematical methods.

Database	Method	PIFS C.	WLF	RMS	Michelson	LMC	Mean
GUC45							
	STRESS	**241,1**	**10,0**	**46,1**	3,3	**292,3**	**118,5**
	PIFS	79,8	1,5	10,0	3,3	64,1	31,8
	CLAHE	44,9	-1,0	13,9	1,5	73,2	26,5
	L.Unsharp M.	109,5	2,0	10,2	3,3	170,3	59,1
	Wang	11,4	0,3	43,1	-4,0	-22,2	5,7
SingaporeNIR							
	STRESS	**2896,9**	5,4	30,1	0,5	**584,3**	**703,5**
	PIFS	85,7	0,0	0,6	0,5	106,6	38,7
	CLAHE	200,6	-0,1	11,8	-0,9	177,1	77,7
	L.Unsharp M.	322,9	0,0	3,0	0,5	207,1	106,7
	Wang	-7,8	**16,2**	**67,6**	0,5	87,4	32,8
SingaporeFIR							
	STRESS	**123,6**	-49,0	-8,9	0,0	**130,5**	**39,2**
	PIFS	27,3	**-0,4**	0,0	0,0	8,8	7,2
	CLAHE	-3,3	-45,6	-0,3	-1,8	57,2	1,2
	L.Unsharp M.	63,4	-0,7	**3,1**	0,0	29,3	19,0
	Wang	-49,1	-61,6	-4,4	-33,3	-14,5	-32,6

Table 5.3: Mean contrast gain in percentage for GUC45, SingaporeNIR and SingaporeFIR database with the highest gain for each metric marked in bold.

Method	Complexity (avg. ACT)	GUC45	SingaporeNIR	SingaporeFIR
PIFS Contrast	high (7.644)	4.89	13.992	4.051
WLF	very high (22.859)	14.866	41.669	12.043
RMS Contrast	low (0.011)	0.007	0.02	0.005
Michelson Contrast	very low (0.004)	**0.002**	**0.009**	**0.002**
LMC	medium (3.847)	3.529	3.7	4.313

Table 5.4: Average Computation Times (ACT) of the contrast measuring methods (in seconds per image, fastest marked in bold) for the different data sets and a complexity approximation based on the average ACT.

Contrast measurement methods as reviewed in Section 5.3 were applied to the processed images in order to evaluate the potential gain. The chosen methods cover the spectrum of possible approaches, from perception-oriented to simple and fast mathematical methods. Table 5.3 show the mean contrast gain in percentage for each of the databases GUC45, SingaporeNIR and SingaporeFIR. For the three databases the STRESS algorithm yields the highest mean contrast gain percentage. The results shown in the table represent the mean value of the mean contrast gains over three runs. Table 5.4 show the methods and their properties, the computational complexity is again abstracted from the average execution time per image in the evaluation. For a qualitative assessment of the contrast enhancement methods one image out of every dataset is shown as originally captured as well as the resulting enhanced versions (Figure 5.1). All enhancement methods are able to improve the average contrast of the datasets. The introduction of additional noise is possible by applying the enhancement methods, therefore it is also included in the experiments. Table 5.6

summarizes the estimated noise power levels for each dataset and contrast enhancement method applied. In order to not only consider the contrast gain, but also the computational complexity, a combined table is computed showing the average contrast gain over all data sets per time (Table 5.5). With this information it is possible to find the application specific contrast enhancement method which is fulfilling also the computational requirements.

Method	PIFS C.	WLF	RMS	Michelson	LMC
STRESS	0.9232	-0.0356	0.0268	0	0.4947
PIFS	0.0027	-0.0000	0	0	0.0009
CLAHE	20.4266	-5.5128	2.6504	-0.0816	29.4678
L.Unsharp M.	**919.1596**	**3.8296**	**37.6478**	**9.5111**	**826.6191**
Wang	-0.7062	-1.1435	1.4241	-0.7592	-0.4315

Table 5.5: Contrast gain factor per time (Contrast gain/ACT).

Method	GUC45	SingaporeNIR	SingaporeFIR	Mean
Original	0.0042	0.0004	0.0036	0.0027
STRESS	0.0153	0.0244	0.0107	0.0168
PIFS	0.0078	0.0008	0.0050	0.0045
CLAHE	0.0069	0.0017	0.0047	0.0044
L.Unsharp M.	0.0085	0.0021	0.0074	0.0060
Wang	0.0062	0.0004	0.0033	0.0033

Table 5.6: Noise power estimates.

5.6 Conclusions[1]

The paper is giving an overview of contrast enhancement and contrast measurement methods appropriate for biometric vein pattern enhancement. The computational complexity of each method is approximated through the average computation time per image from the three biometric databases that cover different modalities in vein pattern recognition like finger and back of hand as well as different spectral bands (Table 5.1). Different contrast measures assure a neutral evaluation of the contrast gain from the various enhancement methods. It can be seen that the STRESS algorithm is enhancing the contrast of the sample vein images most averaging the results from the contrast measures but it is also increasing the noise in the resulting images more than the other methods. The Linear Unsharp Mask and also to some extend CLAHE contrast enhancements are recommended for applications where computational complexity is of concern.

[1]In a retro perspective it can be stated that the noise level introduced by STRESS is influencing the biometric performance negatively. Instead, less intrusive methods, in particular the CLAHE method, are recommended. This reflects also the subjectively perceived image quality of the enhanced images. However, the visibility of the veins in the STRESS-enhanced images is perceived larger. The contrast metrics classified CLAHE-enhanced images on 3rd or 4th place according to a ranked interpretation of Table 5.3 which indicates that the perceived image quality can not be captured by the introduced metrics. In Chapter 6 we therefore proposed a different approach to quantify the quality of the images.

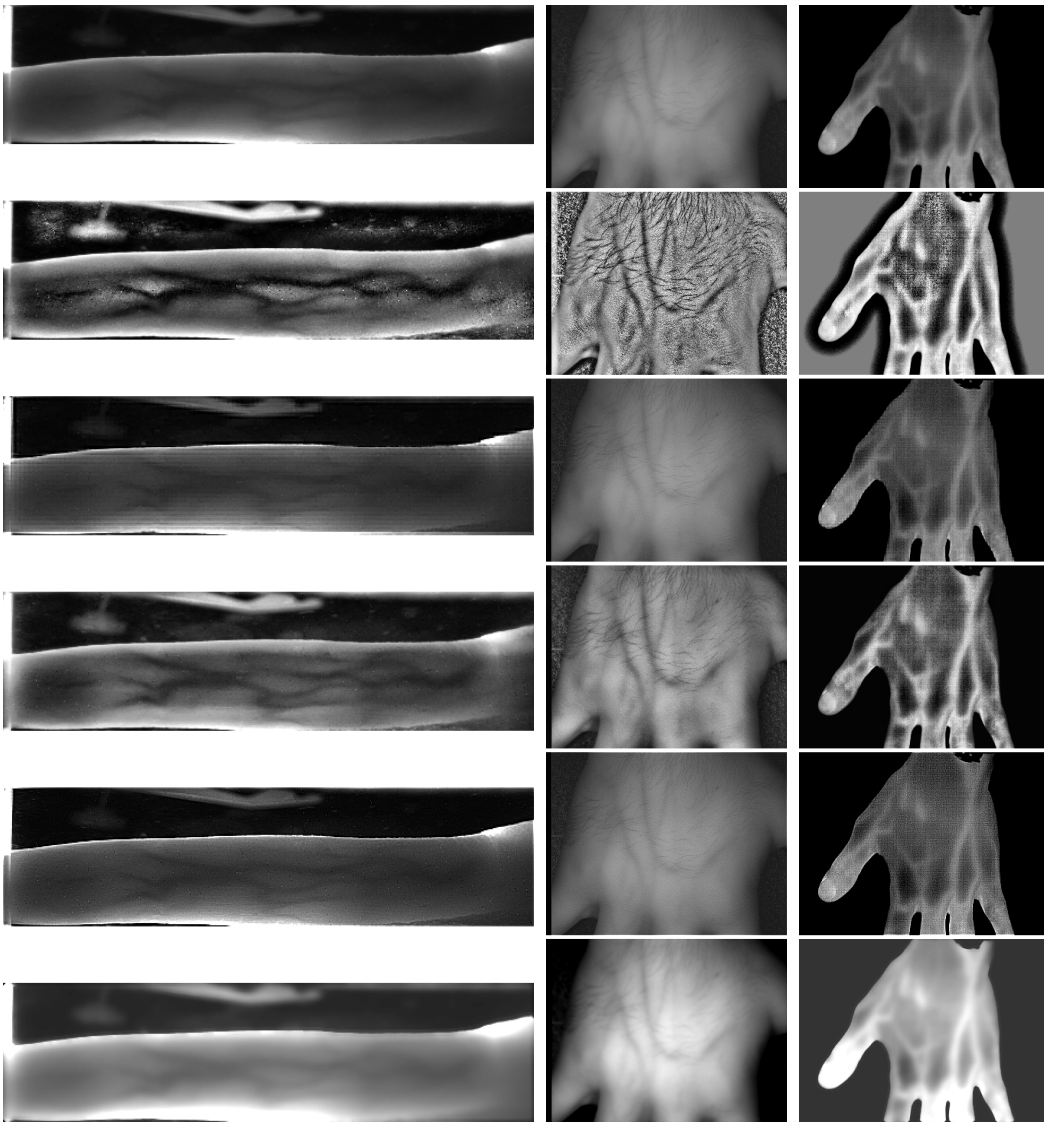


Figure 5.1: Contrast enhancement. From left to right: GUC45 (finger placed horizontally, some background visible), SingaporeNIR, SingaporeFIR database example. From top to down: original, STRESS, PIFS, CLAHE, Linear Unsharp Mask, Wang enhanced image.

5.7 Future Work

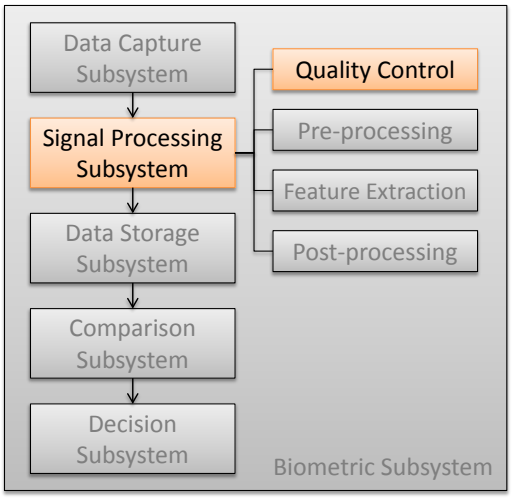
In order to verify the impact of the contrast (gain) on the vein pattern based biometric systems, a biometric performance evaluation of the enhanced images is needed. After this step, a reasonable quality measure for vein pattern images can be constructed using the results of this paper. Another interesting question is whether or not it does make sense to combine two or more of the enhancement methods to gain an advanced contrast gain.

5.8 Acknowledgments

Many thanks to our supervisors, to the participants of the GUC45 database and to the vendor of the infrared sensor, to Nanyang Technological University for giving access to their vein databases, to Colorlab at Gjøvik University College for supplying an implementation of the STRESS algorithm.

Chapter 6

Quality Estimation for Vascular Pattern Recognition



The biometric performance of a system depends on the quality of the enrolled biometric samples. It is therefore fundamental to ensure a minimal level of quality. Furthermore quality estimation is useful for selecting subsequent steps in the pipeline (algorithms / parameters) and in unsupervised scenarios for user guidance. Here we propose and prove the effectiveness of an algorithm for estimating the quality of wrist and palm dorsal (NIR/FIR) veins that works on the images itself with the option to utilize meta-data about the environment and the data subject as well. Unfortunately the contrast measures introduced in the last chapter could not be used for the approach since the only two fast methods (RMS, Michelson) did not prove to be reliable (Tables 5.3 and 5.4).

Note that due to the page limit in the original paper comprehensive arguments for the selection of the Gray Level Co-Occurrence Matrix (GLCM), the metrics and the parameters could not be included. It should be done here: the GLCM was successfully utilized for quality control in [151], however it was applied globally on the whole image since no background was visible on the palm images. In the data that we utilized, background and edges of the limbs might be present that can influence the quality estimation. We decided therefore to utilize the GLCM, but in a local manner based on a simple block structure representing the actual limb. The selection of texture measures is based on expert knowledge of the specific dataset. Further details are given in Section 4.7.3 in [148] and are summarized here (θ refers to the angle of the GLCM metric with $\theta = 0$ considering horizontal transitions): GUC45 - the values generated by the Contrast, Correlation and Energy measures can not accurately rate the visibility of veins because these measures are highly affected by artifacts within the image (e.g. very bright finger edges) and the non-uniformity

of gray-levels among images. The most relevant measurements are generated by the Homogeneity measure. The texture pairs are vertically oriented because most of the veins are horizontally defined ($\theta = 90$). UC3M - Wrist samples, captured under NIR light, show good segmentation and contrast from the background. Although veins are generally well defined, light intensity varies from one sample to another. The consequence is that some parts of the veins are smoothed or even erased. The measures selected to grade the quality of wrist samples are both Correlation and Contrast because the wrist images may have large areas where no veins are visible even though the quality of the sample is optimal. The texture pairs are horizontally defined ($\theta = 0$). SNIR - Back of the hand vein samples of this database have stable properties. They have uniform illumination, noise-free background and the hand is clearly segmented from the background. Thus the quality score is based on the Homogeneity measure and the disposition of the pixel pairs is horizontal direction ($\theta = 0$). Lower homogeneity values indicate higher block quality. SFIR - Back of the hand vein samples of this database show that the tissue regions have large ranges of gray values where veins are represented as white regions. Thus high homogeneity in the sample indicates well defined veins. The Homogeneity measure uses horizontal texture pairs ($\theta = 0$).

The selection of the parameters is based on an empirical evaluation of a subset of image pairs resulting in very high or low genuine comparison scores for each dataset.
The paper was published in: [76] HARTUNG, D., MARTIN, S., AND BUSCH, C. Quality estimation for vascular pattern recognition. In Hand-Based Biometrics (ICHB), 2011 International Conference on (November 2011), pp. 1-6.

Abstract

The quality of captured samples is a critical aspect in biometric systems. In this paper we present a quality estimation algorithm for vascular images, which uses global and local features based on a Gray Level Co-Occurrence Matrix (GLCM) and optionally available metadata. An evaluation of the algorithm using different processing methods and vein sample databases shows convincing results: disregarding low estimated quality sample images helps to increase the performance. Moreover, metadata gives accurate indications on sample quality. The algorithm works on low level raw images, it is fast and therefore qualified to be used in feedback mode during enrolment or verification operation.

6.1 Introduction

Recently, biometric authentication processes have been augmented with vein recognition method that provides undeniable benefits compared to traditional systems, e.g. based on fingerprints. Vein recognition is fake resistant against an intentional presentation of an artifact and provides reliable biometric performance comparable to iris recognition performance. The fake resistance capability of a vein recognition system strengthens its application in non-supervised environments such as subject towards client computer authentication in a home environment or customer / cardholder authentication against an ATM machine that are operated in a semi-public yet non-supervised environment.

In order to achieve a reliable biometric performance for a verification attempt specifically the enrolment of the data subject is critical, since the reference for further comparisons is created. A low quality reference will result in low performance of the overall system.

The quality estimation could also be very useful in the guidance of the data subject as it will indicate potentially incorrect placement of the finger / hand on the capture device and whether or not the image must be re-taken from the biometrics characteristic. Such feedback can be communicated to the applicant without further interaction of an operator. While the automatic assessment of a fingerprint's signal quality is a standard procedure according to ISO standards and technical reports [96], there is little literature focusing on the automatic assessment of vein images.

The approach presented in this paper covers this gap and provides a method that can automatically generate quality scores for sample images of various vein modalities. In this paper, a quality assessment algorithm is proposed that analyses the image characteristics of the sample and that uses knowledge of sample metadata influence on the performance of the system. The efficiency of quality prediction of the algorithm is verified using different sample databases containing finger vein samples stored with subject and environmental metadata from NISlab (GUC45), wrist samples from University Carlos III Madrid (UC3M) and dorsal hand images from Nanyang Technological University Singapore captured in near- and far-infrared (SNIR/SFIR). Details about the databases are shown in Table 6.1.

The paper is structured as follow: Section 6.2 presents previous work of quality assessment in biometrics. The proposed quality assessment algorithm for vein recognition systems is described in Section 6.3 followed by a description of the experimental setup and results. Finally, Section 6.5 concludes this paper and indicates future work.

6.2 Related work

Biometrics community agrees that quality assessment distinguishes the *Character* (inherent to the biometric trait), the *Fidelity* (degree of similarity between the sample and its source) and the *Utility* (prediction of the contribution of the sample to the system performance). The latter is the result of both *Character* and *Fidelity* thus is the most important quality measure.

The International Standard Organization (ISO) has defined a multipart standard that specifies generic guidelines [100], factors influencing the quality of samples [99] and recommendations for the implementation of quality metrics. Currently only guidances for fingerprint, face and iris recognition has been defined [96–98]. Quality assessment has been especially researched for multimodal applications [124, 179, 180] but also for fingerprint, face and iris recognition [43, 59]. Nevertheless, recent research in vein recognition has been conducted.

Michael et al. [151] implemented a quality controller accepting samples for which a Gray Level Co-Occurrence Matrix (GLCM) metric meets predefined thresholds. Pascual et al. [171] built a vein recognition system where quality of the produced samples were measured through objective measurements such as contrast, variance and light distribution between vein and skin area. Several studies have demonstrated the correlation between quality and influencing factors of different nature and with different degrees of influence. In vein recognition, few publicly available research experiments focused on the analysis of influencing factors.

Sanchez-Reillo et al. [194] examined the impact of different light, temperature and humidity environments on the performance of a vein recognition systems. Yuksel et al. [278] tested appearance- and geometry-based feature extraction algorithms on samples where hands were stressed by different activities. Raghavendra et al. [184] and Lee et al. [137] artificially degraded the sample images quality and could prove a decrease in biometric performance. Yang et al. [272] and Wu et al. [259] investigated different hand areas and found differences in the performance.

6.3 Proposed Quality Assessment Algorithm

Standardization bodies still do not have defined guidelines on quality estimation for vein recognition systems. The proposed algorithm could be used as a bases for the definition of such a standard. During the design of the algorithm the other ISO quality standards were taken into account. In [96] the recommended measures for fingerprint images are orientation certainty, ridge-valley structure or orientation flow analysis; all of these measures are based on the ridge-valley structures in the fingerprint image which are not comparable to the vein structures in vascular-based systems. However the draft iris standard [98] gives general measures that are also taken into account in the proposed algorithm: e.g. contrast, gray scale density, size and orientation as well as boundary shape and usable size of the biometric trait.

The proposed quality assessment algorithm is designed in a feedback mode prior to any preprocessing method. Firstly, it assesses the quality using conventional image-based methods. Secondly, a non-image-based method is implemented based on performance estimation of metadata that characterizes the sample. The generated quality scores are normalized between 0 and 100 where 100 indicates excellent quality.

6.3.1 Image-based

The image-based method shall evaluate both global and local features of the sample, for the remainder of this paper we will refer to it as *image-based analysis*.

6.3.1.1 Mask Correlation

The global quality assessment evaluates the quality of the sample mask. The mask defines the region of interest of the sample, distinguishing between background and body limb. The implemented segmentation process may produce undesired image deficiencies such as holes and islands. First, using the non-parametric Kendall rank correlation the similarity between the sample mask M and an average mask M_μ is evaluated, then the proportion of

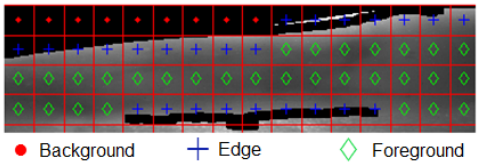


Figure 6.1: Block categorization of a sample from GUC45.

holes M_{hole} and islands M_{isl} is combined into the quality score S_{mask} as follows:

$$S_{\text{mask}} = \text{corr}(M, M_\mu) \cdot (1 - (\alpha_1 \cdot M_{\text{isl}} + (1 - \alpha_1) \cdot M_{\text{hole}})), \tag{6.1}$$

where the parameter $0 \leq \alpha_1 \leq 1$ is weighting the influence of image deficiencies.

6.3.1.2 Local Gray Level Co-Occurrence

The vein sample images are then partitioned into blocks of the same size, depending on the size of both image and veins. The blocks are then categorized as: *background* (the block does not contain any biometric trait), *edges* (the block contains the edge of the biometric trait) or *foreground* (the block contains only the biometric trait). Figure 6.1 shows a sample with the categorization of the blocks. The local quality assessment is based on Gray Level Co-Occurrence Matrix (GLCM) and is inspired by the quality assessment method proposed by Michael et al. [151]. GLCM has been originally proposed by Haralick et al. [69] and evaluates the frequency of specific pixel intensity pairs in a determined spatial combination. Based on the matrix several texture measurements ϕ are defined: e.g. Contrast, Correlation, Energy and Homogeneity.

The GLCM is calculated for each block B_f that has been categorized as *foreground*. The quality score of the local block-based analysis S_{blk} is generated as follows (described in pseudo code):

$S_{\text{blk}} = 0$
FOREACH block B_f in $\{\text{foreground}\}$ DO
  IF $(T_{\min} < \phi(\text{GLCM}(B_f)) < T_{\max})$ DO
    $S_{\text{blk}} = S_{\text{blk}} + (1/|\{\text{foreground}\}|)$
  END
END

with thresholds $T_{\min}$ and $T_{\max}$ specific to both texture measure ϕ and database. These thresholds describe the range for which a meaningful and rich texture of the vein image can be expected. The process above can be executed several times with alternating ϕ and parameters for the GLCM-calculations, then a fusion has to be made, here the minimum value is taken as measure S_{blk}. The thresholds have been selected through empirical investigations on images generating the best and worst genuine comparison scores.

Both mask and block scores are combined to the image-based quality score S_{img}:

$$S_{\text{img}} = \alpha_2 \cdot S_{\text{blk}} + (1 - \alpha_2) \cdot S_{\text{mask}} \tag{6.2}$$

with $0 \leq \alpha_2 \leq 1$ weighting the influence of the two measures.

6.3.2 Metadata

The metadata-based method relies on an analysis of the performance changes measured in equal error rates (EER) of sample sets that share a certain factor. Each sample is supplemented by a set of factors which belongs to a metadata category. For instance, the category *Gender* has both factors *Male* and *Female*. The factors selected for the experiments

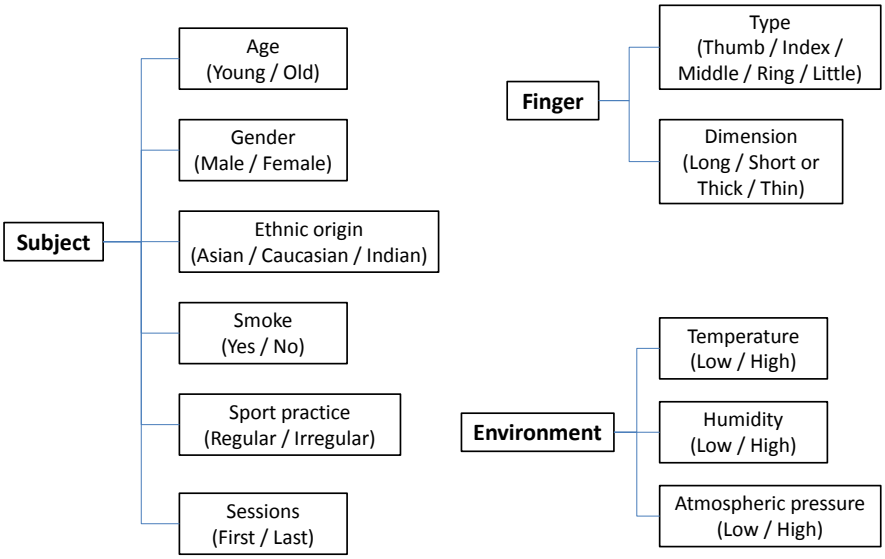


Figure 6.2: Metadata categories and their factors.

are based on finger, subject and environmental properties that were captured within the GUC45 database, they are presented in Figure 6.2. Other metadata could be used like capture system characteristics. In a verification scenario the whole metadata could be used, since the identity claim can point to the subject and finger or limb data. The environmental data can be gathered during capture time and is available also in an identification scenario.

6.3.2.1 Precalculation

For each factor, an EER is generated by selecting samples specified by the factor of interest. This is completed for each factor and pair of preprocessing and comparison methods: first, within each category the impact of the factors on system performance is measured. Let $C_i = \{f_1, f_2, ..., f_m\}$ be the set of m factors for category C_i, with $i = 1, ..., n$:

$$E_{f_j}^{\min} = \min(\mathrm{EER}_{C_i}) - \mathrm{EER}_{f_j} \tag{6.3}$$

$$E_{f_j}^{\max} = \max(\mathrm{EER}_{C_i}) - \mathrm{EER}_{f_j} \tag{6.4}$$

with $j = 1, ..., m$, $\min(\mathrm{EER}_{C_i})$ and $\max(\mathrm{EER}_{C_i})$ are the minimal and maximal EER in the category C_i, respectively. EER_{f_j} is the EER of factor f_j in category C_i. Both maximal and minimal EERs used in Equations 6.3 and 6.4 enable to measure how much the factors within a category impact the performance of the system. Both $E_{f_j}^{\min}$ and $E_{f_j}^{\max}$ are then combined:

$$E_{f_j} = E_{f_j}^{\min} + E_{f_j}^{\max}. \tag{6.5}$$

The weight W_{total} is needed later for normalization and is computed from the one factor $f_{\max}^{C_i} = \max(E_{C_i})$ of each category that influences performance most:

$$W_{\mathrm{total}} = \sum_{i=1}^{n} f_{\max}^{C_i}. \tag{6.6}$$

Results from Equations 6.3-6.6 can be precalculated once.

6.3.2.2 Metadata Influence on Sample

Let $F = \{f_1, f_2, ..., f_n\}$ be the set of n factors characterizing the sample. Then the weight of influence of all factors W characterizing the sample is added up:

$$W = \sum_{z=1}^{l} E_{f_z} \tag{6.7}$$

This weight can either be positive when factors increase the performances or negative otherwise.

6.3.2.3 Normalization

In order to transform the metadata weight into a normalized score, the weight is first shifted and then normalized between 0 and 100. It is relative to the maximal weight possible W_{total}:

$$S_{\text{meta}} = 100 \cdot \frac{(W + W_{\text{total}})}{2 \cdot W_{\text{total}}} \tag{6.8}$$

Although the metadata score can indicate a performance improvement (values above 50) it may decrease the global score, when later the metadata score is combined with the image based score. This will happen, if the metadata score level is less than the image-based score level. So the metadata score must be re-evaluated on the basis of the image-based score. Therefore the weight $W_{\text{img\_meta}}$ is calculated to shift the image-based score S_{img} according to the influence of the metadata of the sample.

$$W_{\text{img\_meta}} = \begin{cases} \frac{2(S_{\text{meta}}-50)}{100} \cdot S_{\text{img}} & if\ S_{\text{meta}} \leq 50 \\ \frac{2(S_{\text{meta}}-50)}{100} \cdot (100 - S_{\text{img}}) & if\ S_{\text{meta}} > 50 \end{cases} \tag{6.9}$$

The weight is combined with the image-based score as follows:

$$S_{\text{img\_meta}} = (S_{\text{img}} + W_{\text{img\_meta}}) \tag{6.10}$$

6.3.3 Final Quality Score

The final score S of the proposed quality assessment algorithm for vein images is calculated as follows:

$$S = \alpha_3 \cdot S_{\text{img}} + (1 - \alpha_3) \cdot S_{\text{img\_meta}}, \tag{6.11}$$

with $0 \leq \alpha_3 \leq 1$ weighting between the image-based score and the metadata based score.

6.4 Experiments

To verify the capabilities of the proposed algorithm to assess biometric sample quality several experiments are performed on different vein databases. The characteristics and the GLCM texture parameters of the different data sets are summarized in Table 6.1.

Samples of GUC45 have heterogeneous finger positions, contrast and brightness. Additionally, subject and environment metadata characterizing the captured sample is recorded. On the other hand samples from UC3M, SNIR and SFIR databases have homogeneous hand position, contrast and brightness, and recorded in one session, thus in general generate better EERs.

Table 6.1: Databases characteristics.

Name	**GUC45 [73]**	**UC3M [171]**	**SNIR [242]**	**SFIR [242]**
Trait	10 Fingers	2 Wrists	2 Dorsal hands	2 Dorsal hands
Subjects	45	29	122	33
Attempts	2	6	3	3
Sessions	12	1	1	1
Total	10 800	348	732	173
Light	NIR	NIR	NIR	FIR
GLCM	Homogeneity	Correlation Contrast	Homogeneity	Homogeneity
Block size	25	40	30	30
Thresholds $\{T_{\min}, T_{\max}\}$	{0.4, 0.7}	{0.85, 0.98}	{0.6, 0.8}	{0.95,∞}
$\{\alpha_1, \alpha_2, \alpha_3\}$	{0.5, 0.5, 0.5}	{0.5, 0.5, -}	{0.5, 0.5, -}	{0.5, 0.5, -}

6.4.1 Setup

Different preprocessing and comparison method combinations have been used throughout the experiments. With GUC45, the preprocessing based on Otsu [169] and the comparison strategy based on Modified Hausdorff Distance (MHD) [242] as well as a combination of Chan-Vese [27] and Similarity-based Mix Matching (SMM) [30] are being used. The algorithm of Wang [242] did not show convincing results. Image-based, metadata-based quality assessment algorithms as well as the combination of both are used in the experiments. Tables 6.2 and 6.3 indicate the number of genuine and imposter scores randomly selected for different quality levels and summarizes the results for the comparison and preprocessing pairs Otsu and MHD and Chan-Vese and SMM, respectively.

With UC3M, SNIR and SFIR, both Otsu and Wang [242] preprocessing methods are used with both Location-Based Spectral Minutiae Representation (SML) [260] and SMM. The preprocessing based on Wang's methods was preferred to Chan-Vese for the reason of computational complexity. These sample databases have no recorded metadata, so only the image-based algorithm could be tested. The different parameter values for the weighting factors α are set to 0.5, using the arithmetic mean.

6.4.2 Examples for Quality Assessment

For all experiments, the classification of low and high quality samples is achieved, example of correct classifications for the datasets are given in Figure 6.3.

6.4.3 Results on GUC45

The very challenging image quality of the GUC45 database is reflected in the high error rates. With the pair Otsu and MHD, system performance is improved by less than 10%. The image-based analysis has the lowest performance improvement with 4.99% because it considers samples with numerous features (low homogeneity) as high quality images. But detected features can be of diverse natures that are not identified by the image-based analysis such as veins or light artifacts. The metadata-based analysis has a performance improvement by 6.48% between high quality and without assessment. Moreover, it achieves the best performance improvement between low and high quality samples with 14.79%. Based on the ratio between *without* and *high quality*, the best performance improvement is produced by the metadata- and image-based analysis with 9.87%. This can be explained by the fact that the combination refines the high quality scores by removing eventual quality assessment errors that falsely accepted poor quality samples.

With the pair Chan-Vese and SMM the quality assessment algorithms using image-based analysis generate the best performance improvement because the comparison method SMM is sensitive to the linearity and continuity of the vein pattern in the processed sample

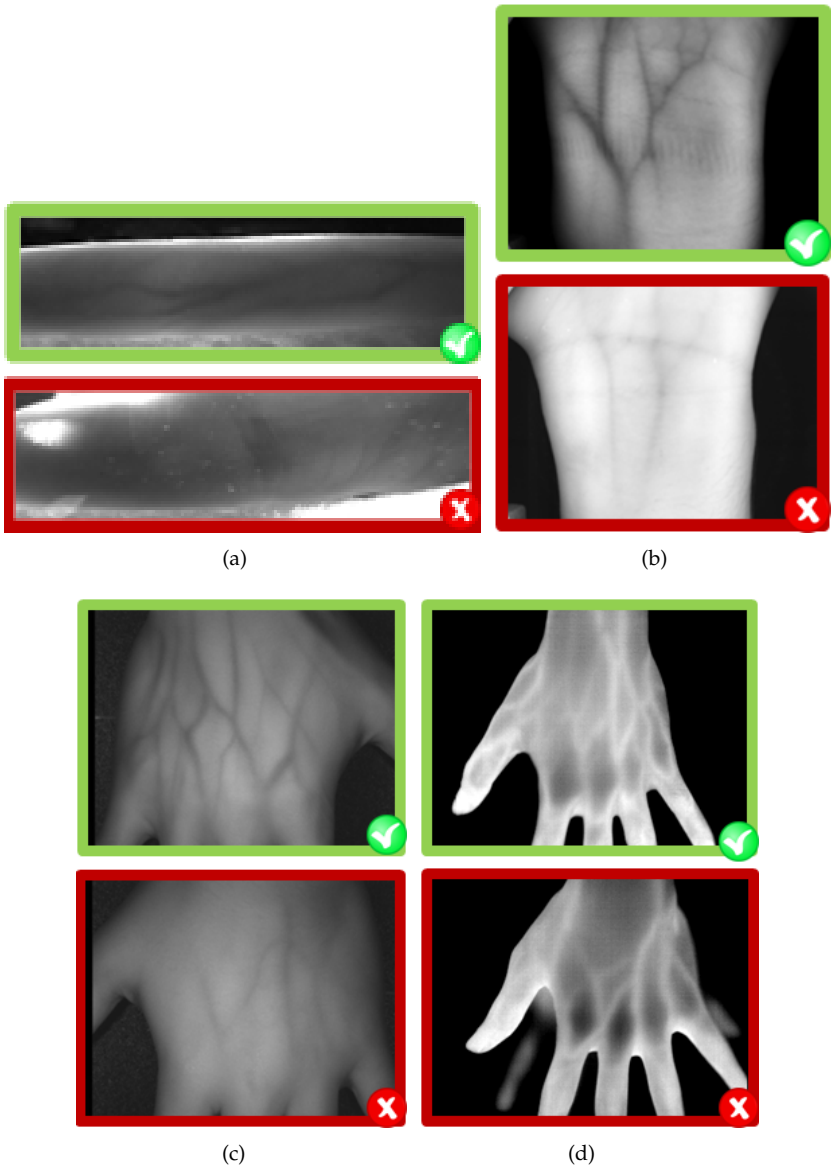


Figure 6.3: Classification examples of the quality assessment algorithm: (a) GUC45; (b) UC3M; (c) SNIR; (d) SFIR; Green check mark: high quality sample, red cross: low quality sample.

Table 6.2: EERs (in %) of GUC45 database generated by the method pair Otsu/MHD with different quality assessment approaches and performance improvement.

Quality analysis	Quality level	Number of scores genuine / imposter	EER
-	Without	29 702 / 13 070 888	33.88%
Image (S_{img})	Low	1 426 / 136 299	36.15%
	High	1 072 / 130 806	32.18%
	Improvement (Without/High)		**4.99%**
	Improvement (Low/High)		**10.97%**
Metadata (S_{meta})	Low	2 985 / 77 070	37.178%
	High	1 092 / 11 894	31.68%
	Improvement (Without/High)		**6.48%**
	Improvement (Low/High)		**14.79%**
Image Metadata ($S, \alpha_3 = 0.5$)	Low	1 171 / 99 180	34.50%
	High	1 089 / 93 552	30.53%
	Improvement (Without/High)		**9.87%**
	Improvement (Low/High)		**11.50%**

Table 6.3: EERs (in %) of GUC45 database generated by the method pair Chan-Vese/SMM with different quality assessment approaches and performance improvement.

Quality analysis	Quality level	Number of scores genuine / imposter	EER
-	Without	12 173 / 390 964	29.18%
Image (S_{img})	Low	1 219 / 17 792	31.50%
	High	1 288 / 22 426	24.11%
	Improvement (Without/High)		**17.38%**
	Improvement (Low/High)		**23.47%**
Metadata (S_{meta})	Low	1 299 / 4 430	32.11%
	High	1 580 / 28 577	27.27%
	Improvement (Without/High)		**6.53%**
	Improvement (Low/High)		**15.06%**
Image Metadata ($S, \alpha_3 = 0.5$)	Low	1 151 / 16 245	31.97%
	High	1 239 / 11 690	24.82%
	Improvement (Without/High)		**14.94%**
	Improvement (Low/High)		**22.38%**

image. The image-based analysis has the best performance improvement with 17.38%. The metadata analysis shows a performance improvement by only 6.53%. The reason might be that not all influencing factors were analysed for this preprocessing and comparison pair (i.e. finger types). So further factors increasing or decreasing the system performance remain unknown. The image and metadata analysis improves the performance by 14.94%, this result can be explained by the fact that samples identified as low and high quality have been excluded by this analysis.

Further experiments have shown that preprocessing and comparison methods have different requirements concerning the properties of image samples. Moreover, regardless of image properties, metadata like finger, subject and environment properties, provides accurate indications on the performance of samples on the recognition system. In particular male performed better than female, non-smokers better than smokers, Asians better than Caucasians or Indians and samples captured during last sessions performed better than those from the first ones.

Table 6.4: EERs of UC3M database at different quality levels and processing methods and performance improvement using S_{img}.

Quality level	Number of scores genuine / imposter	Otsu		Wang2007	
		SML	SMM	SML	SMM
Without	870 / 49 590	7.13%	1.15%	10.29%	5.75%
Low	191 / 6 945	10.00%	3.14%	13.09%	8.38%
High	181 / 7 031	5.53%	0.55%	7.73%	4.42%
Improvement (Without/High)		**22.47%**	**51.93%**	**24.8%**	**23.09%**
Improvement (Low/High)		**49.75%**	**82.41%**	**40.91%**	**47.24%**

Table 6.5: EERs of SNIR database at different quality levels and processing methods and performance improvement using S_{img}.

Quality level	Number of scores genuine / imposter	Otsu		Wang2007	
		SML	SMM	SML	SMM
Without	732 / 177 876	0.55%	0.27%	0.96%	0.27%
Low	227 / 19 686	0.44%	0%	1.32%	0.44%
High	228 / 20 968	0.44%	0%	0.88%	0%
Improvement (Without/High)		**19.74%**	**100%**	**8.27%**	**100%**
Improvement (Low/High)		**0.43%**	**0%**	**33.63%**	**100%**

Table 6.6: EERs of SFIR database at different quality levels and processing methods and performance improvement using S_{img}.

Quality level	Number of scores genuine / imposter	Otsu		Wang2007	
		SML	SMM	SML	SMM
Without	169 / 9 684	5.33%	2.37%	6.51%	4.73%
Low	26 / 659	7.69%	7.69%	11.54%	7.69%
High	28 / 630	3.57%	0%	3.57%	0%
Improvement (Without/High)		**32.94%**	**100%**	**45.13%**	**100%**
Improvement (Low/High)		**53.57%**	**100%**	**69.05%**	**100%**

6.4.4 Results on other Databases

The combination of any preprocessing and comparison method on UC3M samples improves the performances as shown in Table 6.4. The best improvement is achieved with Otsu and SMM by over 51.93%. Other methods improve performance by about 23%.

On SNIR samples, performances are improved by 100% with SMM, with SML 19.74% for Otsu and 8.27% for Wang as presented in Table 6.5. But the identification of low quality samples with Otsu fails because the classification has separated sample combinations that degrade the performances of the system. A manual analysis has identified that the performance decrease is caused by samples with important diagonal and horizontal hand translation and hairy hands.

Using SFIR data, the performance of the system is improved for any configuration and especially with SMM that achieves 100%. The rates are exposed in Table 6.6. Some of the rates of low and high quality are the same among the configuration and shows that the characteristics of the selected samples impact similarly both preprocessing and comparison methods.

6.4.5 Throughput

An important concern in quality estimation after sensor acquisition is the throughput. For each sample database the time required by preprocessing methods and the quality

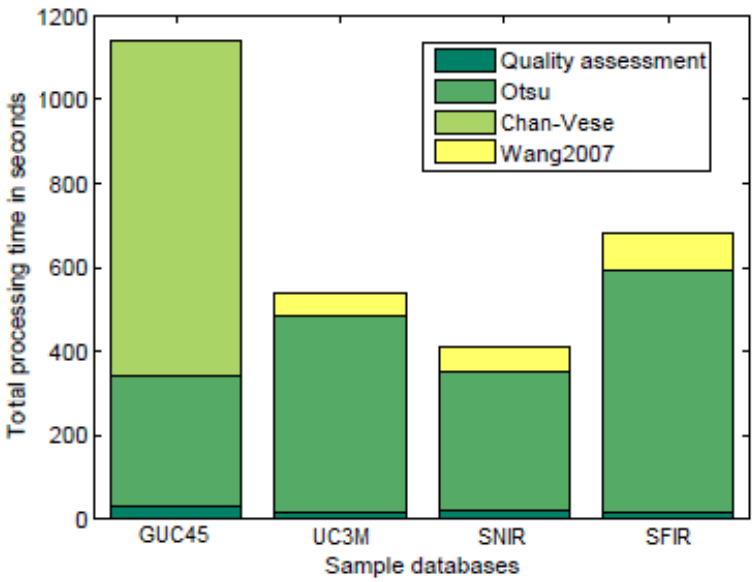


Figure 6.4: Throughput (in seconds) of preprocessing and quality assessment methods.

checker is measured and compared using 50 samples randomly selected. With GUC45 the metadata- and image-based analysis is used, while with the other databases the image-based analysis is applied. The results of the throughput investigation, presented in Figure 6.4, show that for any sample database the proposed quality assessment algorithm is faster than any preprocessing method used in the experiments. The runtime of a naive Matlab implementation was 300-650 ms per sample.

6.5 Conclusions and Future Work

This paper proposes a modular quality assessment algorithm for vein recognition systems based on the analysis of the image and metadata characterizing the image. The experiments conducted with diverse processing methods and on several databases have shown in general a substantial improvement in the biometric performance of the vein recognition systems. The image analysis is especially efficient, when samples of a database have similar characteristics on which static thresholds are defined like the position, similar brightness and contrast. Moreover, the proposed quality analysis requires significantly less computational effort than any preprocessing method used.

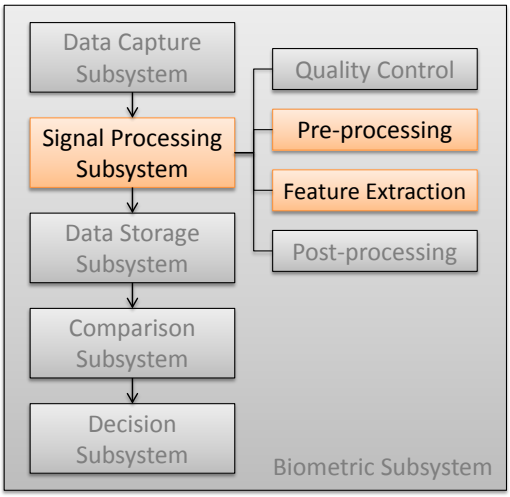
Used in a feedback mode during operation, especially during the enrolment, the proposed quality assessment algorithm can help to create higher quality references, which will influence the overall system performance positively. The quality assessment can help to make decisions to either re-capture a new sample or to adapt the recognition algorithms. In a multimodal system the assessment can be used to weight the different signals accordingly.

It has been shown in the experiments that the assessment is flexible and adaptable to different vein data like finger, wrist and dorsal hand images even though the parameter space was optimized empirically.

Future work will focus on the parameter optimization. Also problems regarding the utilization of metadata have to be solved, as new issues such as privacy concerns or new physical attacks may arise. Attacker could influence environmental factors artificially for their gain. Since throughput is a major issue, the algorithm will be implemented in more efficient programming languages or in hardware.

Chapter 7

Convolution Approach for Feature Point Detection in Topological Skeletons



Minutiae points are a compact representation and easy to compare not only for fingerprints but also for vascular patterns. Here, we propose an efficient algorithm, that extracts bifurcation and end points from eight-connected skeletons. The approach is based on convolution and proves to be more flexible than the known crossing number approach. In Chapter 9 the same approach is extended to extract angles between joining branches of a skeleton.
The paper was published in: [166] OLSEN, M., HARTUNG, D., BUSCH, C., AND LARSEN, R. Convolution approach for feature detection in topological skeletons obtained from vascular patterns. In IEEE Symposium Series on Computational Intelligence 2011 (April 2011).

Abstract

In image processing connected structures can be reduced to an abstract binary skeleton. These skeletons are 1-pixel wide structures which retain the topology of the segmented image. They are used for computer vision, edge detection or high level feature extraction for example in biometric systems. In this paper a fast method on how to extract specific feature points from skeletonized structures is presented. The convolution of the skeleton image with a bi-dimensional mask of size $M \times N$ enables us to identify arbitrary structures of the mask size in the skeleton. Of special interest are branch and endpoints of the vein skeletons to get high level features for biometric comparisons. The problem can here be reduced to the following: in an 8-connected skeleton within a 3x3 mask there are 8 structures that correspond to endpoints and 18 to branch points. After applying the convolution, the search for feature points corresponds to finding the 26 different filter response values in the resulting signal. We describe how the convolution approach is applied to biometric vein recognition systems and compare the method with the crossing number approach.

7.1 Introduction

Abstraction is usually needed in image processing to cope with the vast amount of data. In order to get reasonable information, high level features need to be extracted from images. Often the shape of objects in images are of interest, it is used for example in pattern recognition, machine vision and feature extraction. The topological skeleton can help to describe the properties of such a shape. It is a 1-pixel wide high level abstract representation keeping the core properties like the topology, connectivity, length and direction of the shape. Constructing skeletons usually demands binarized images and can be achieved using iterated morphological operations performed on the image. The proposed method is based on the skeletal representation and will hence not focus on the process of extracting skeletons from images.

The question how to extract feature points from biometric data motivated this work and is used to visualize the proposed method. Of interest in biometric systems are features that can be extracted in a reliable manner from physiological and behavioral biometric traits. In fingerprint recognition for example, the ridges and valleys of the fingertip skin surface are used as features, distinguishing different data subjects. A comparison of raw images from the region of interest will rise sever problems: the fingertip might be misplaced or swiveled, lighting conditions, dirt and distortions of the skin will make a direct comparison unreasonable. To avoid those factors higher level features need to be extracted from an image to extract the core biometric information. One approach that is followed for fingerprint recognition, is the comparison of *minutiae*, the bifurcation and endpoints of the fingerprint ridges. First the skeletal pattern of the ridges is extracted and secondly the skeleton is analyzed for the specific patterns of those points.

In this paper the idea of extracting the before mentioned feature points in an efficient and reliable manner is presented using a convolution approach on the skeleton. The next section will focus on the background of topological skeletons and in specific the skeletonization process. Section 7.3 describes the convolution approach for feature point detection, Section 7.3.1 describes the application for endpoint detection. The application for branch point detection is covered in Section 7.3.2. Section 7.4 shows results from the proposed algorithm performed on skeletonized vein images. The last sections concludes this paper and indicates future works.

7.2 Background and Related Work

In order to formalize the method, a definition for the skeleton is needed. In the literature sometimes the *medial axis* is used as a synonym for the concept of skeletons, also the term

thinning is used as the process of skeletonization. Not only the name convention is still diverse, there are also different definitions and formalizations of skeletons. The definition of when two pixels are topologically connected depends on with which connectivity rule we regard the binarized image [25]. The skeletonization performed here assumes 8-connectivity and will be described by the thinning process.

7.2.1 Thinning

Thinning of the binarized image can be performed by iteratively eroding the image with a 3×3 structuring element while checking that the topology remains the same. In [133] several skeletonization methods are compared and one method for thinning which is also implemented in MATLAB is described here. The algorithm is outlined as follows[1]: The neighborhood around pixel p are enumerated as $x_1, x_2, ..., x_8$. The binary image is divided into two subfields in a checkerboard pattern. Alternating between the two subfields the pixel p is deleted when the following conditions are true:

1. $X_H(p) = 1$, i.e. in the 4-neighborhood of p there is exactly one crossover from 1 to 0.
2. $2 \leq \min\{n_1(p), n_2(p)\} \leq 3$, and
3. For the first sub-iteration: $(x_2 \vee x_3 \vee \neg x_8) \wedge x_1 = 0$ or for the second sub-iteration: $(x_6 \vee x_7 \vee \neg x_4) \wedge x_5 = 0$.

$$X_H(p) = \sum_{i=1}^{4} b_i \tag{7.1}$$

where

$$b_i = \begin{cases} 1 & \text{, if } \neg x_{2i-1} \wedge (x_{2i} \vee x_{2i+1}) \\ 0 & \text{, otherwise} \end{cases} \tag{7.2}$$

$$n_1(p) = \sum_{k=1}^{4} x_{2k-1} \vee x_{2k} \tag{7.3}$$

$$n_2(p) = \sum_{k=1}^{4} x_{2k} \vee x_{2k+1} \tag{7.4}$$

7.2.2 Crossing number

The crossing number [7] is a method for detecting bifurcations and endpoints in a binary skeletonized image. The crossing number cn is calculated by investigating the 8-neighborhood of each pixel p in order to determine the count of crossovers occurrences. $\mathrm{cn}(p)$ is found to be half the sum of the differences between pairs of adjacent pixels in an ordered sequence of the 8-neighborhood of p and $\mathrm{val}(p) \in \{0, 1\}$ [147]:

[1] It is an extension of [285] described in [133]. Note that the choice of the thinning algorithm is for comparison purposes only: the proposed method works on any skeletonization algorithm. However, in some cases additional patterns for bifurcations and endpoints have to be considered (this occurs when the definition of the one pixel width varies). The selection of the skeletonization algorithm for the biometric pipeline is elaborated in Section 8.3.2.

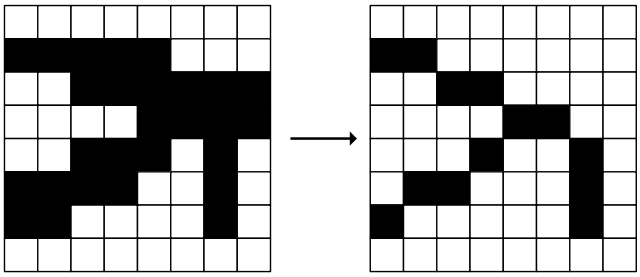


Figure 7.1: Example of skeletonization.

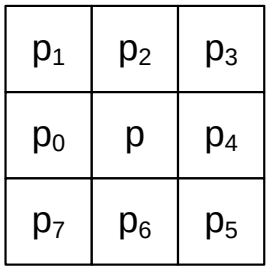


Figure 7.2: Relative locations and ordering of the eight neighborhood of p.

$$\mathrm{cn}(p) = \frac{1}{2}\sum_{i=1}^{8} \left|\mathrm{val}(p_{i \bmod 8}) - \mathrm{val}(p_{i-1})\right|, \tag{7.5}$$

where $p_0, p_1, ..., p_7$ are the pixels in the ordered sequence of the 8-neighborhood of p (shown in Figure 7.2). For a pixel p with $\mathrm{val}(p) = 1$, p is: a 1-pixel island if $\mathrm{cn}(p) = 0$, if $\mathrm{cn}(p) = 2$ then p is an intermediate ridge point; a ridge endpoint if $\mathrm{cn}(p) = 1$; a ridge bifurcation if $\mathrm{cn}(p) = 3$; a complex bifurcation or crossover if $\mathrm{cn}(p) > 3$.

In [207] a run length coding based method for bifurcation and endpoint detection which does not require thinning is presented. The run length coding requires that the input image is binary and it is performed in two dimensions, thus allowing for the detection of starting, ending, merging, and splitting runs. Since the method does not rely on thinning it should have a low computational complexity while maintaining a reliable detecting performance.

In [135] a detection method which uses an extension to Gabor filters is applied to detect discontinuities in a fingerprint image. The discontinuities are interpreted as features. It is not immediately possible to detect if the feature is a bifurcation or an endpoint. Due to this deficiency we will not consider the Gabor filter minutiae detection method.

7.3 Convolution Based Feature Detection

In a vein pattern certain structures such as endpoints and bifurcations can be detected by convolving the skeleton image with a single bi-dimensional filter G and a two look up tables T_e and T_b, where T_e and T_b are the sets of filter response values for respectively endpoints and bifurcations. The 2D discrete convolution of $I(x, y)$ with the filter $G(x, y)$ of size $M \times N$ is defined as

$$I'(x,y) = G(x,y) * I(x,y) \tag{7.6}$$

$$= \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} G(m,n) I(x(m), y(n)) \tag{7.7}$$

where

$$x(m) = x - (m - \frac{M-1}{2})$$

and

$$y(n) = y - (n - \frac{N-1}{2})$$

In the term $I(x(m), y(n)$, the subtractions from x and y correspond to flipping G along both dimensions and then multiply with the values in I which are beneath the filter as it slides across the image.

From Equation 7.7 we obtained a map of filter responses, I'. Further, we have the set of endpoint response values T_e, and bifurcation response values T_b. For each index $I'(x,y)$ we determine if it belongs in either T_e or T_b, and if so we register the index as either endpoint or bifurcation.

More generally we can, in a binary image, detect any structure which fits within an $M \times N$ window by constructing an $M \times N$ mask where the mask values are unique powers of 2. This is possible because any given structure that can be described within the window will activate a unique subset of the values in H resulting in a specific response. By comparing the response with a look up table containing activations for specific patterns thus identifying the spatial positions of endpoints and bifurcations or any other pattern fitting the window. An example of a 3×3 mask with unique power of 2 values and the corresponding flipped version is shown in Figure 7.3. An example of convolving a binary image with the mask is given in Figure 7.4 (values outside the image are treated as zeros). The figure shows the filter response as the image is convoluted with the filter. If we want to detect three-pixel structures like the one shown then we just have to note where the filter response is equal to 392.

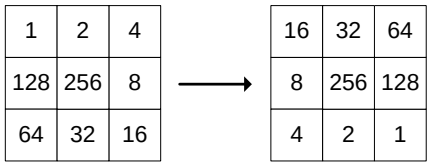


Figure 7.3: Mask used for feature detection.

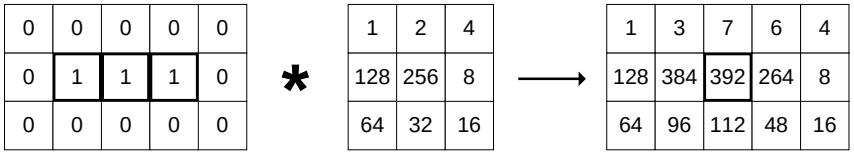


Figure 7.4: Convoluting a binary image with a 3×3 powers of 2 mask.

7.3.1 Endpoint Detection

Using the convolution approach described in Section 7.3 it is possible to find endpoints in a skeleton. Endpoints in biometric data like in vein pattern images are not necessarily true

endpoints in the sense that a vein has an end wall. It might as well be because the vein turns and extends parallel to the normal of the sensor plane. As we cannot distinguish the two forms using just the reflectance data obtained from a single side of the finger, we will consider them both as endpoints.

An endpoint in a skeletonized binary image is any active pixel which has exactly one active neighboring pixel; in an 8-connectivity setting there are eight such possibilities. Using the filter values from the mask in Figure 7.3 we can derive the response values for each of the eight possible configurations - this is shown in Figure 7.5. The endpoint response values are $T_e = \{257, 258, 260, 264, 272, 288, 320, 384\}$.

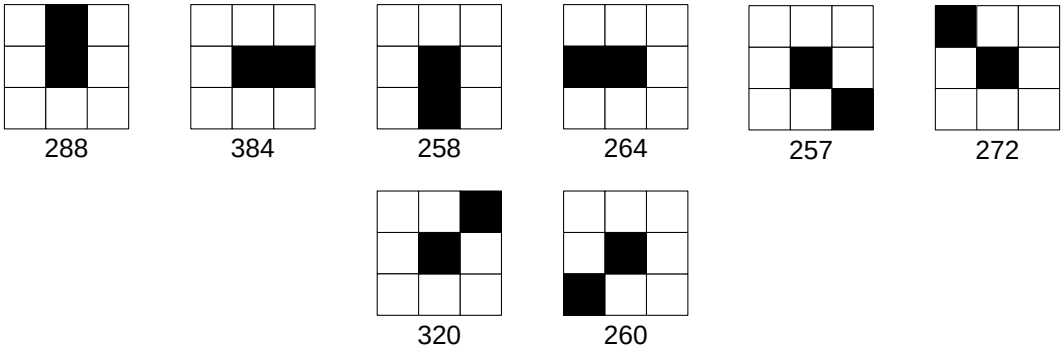


Figure 7.5: Endpoint patterns and their corresponding filter response.

7.3.2 Branch Point Detection

Branch points are points where two or more branches join. In the context of biometric vein pattern recognition such a branch may be observed when a vein splits into two or more veins, or when two or more veins cross each other at different depths in the tissue. As with endpoints, we do not distinguish between the two situations in the extraction of bifurcation points.

Any such branch can be detected by a 3×3 mask like the one shown in Figure 7.3. An exhaustive list of the bifurcation patterns and their corresponding response levels to the filter is shown in Figure 7.6. The bifurcations response values are $T_b = \{277, 293, 297, 298, 325, 329, 330, 337, 338, 340, 341, 394, 402, 404, 418, 420, 424, 426\}$.

7.4 Feature Extraction Examples and Experiments

Figure 7.7 shows an example vein pattern image and its segmented version in Figure 7.7(a). The image is transformed to a skeleton representing the topology of the vein pattern (Figure 7.7(b)) as described earlier. The skeleton is cleaned from small islands and artifacts like spurious branches. The endpoints and branch points are detected using the convolution based feature detection (Equation 7.7) . In Figure 7.7(d) the skeleton and features are overlayed on the cropped input image. The figure show that the skeleton is located on top of the veins and that the convolution approach is able to detect all end and branch points. The computational effort for the convolution and the crossing numbers approach is simulated using a database consisting of 11660 finger vein images having a size of 111×401 pixel and an average skeleton coverage of 3.47% of the image. For each algorithm we iterate across the entire dataset, applying the algorithm on the image and recording the time spent detecting the features.

The results shown in Table 7.1 are obtained from performing the experiment three times and averaging across them. For each method we show the mean, standard deviation, max-

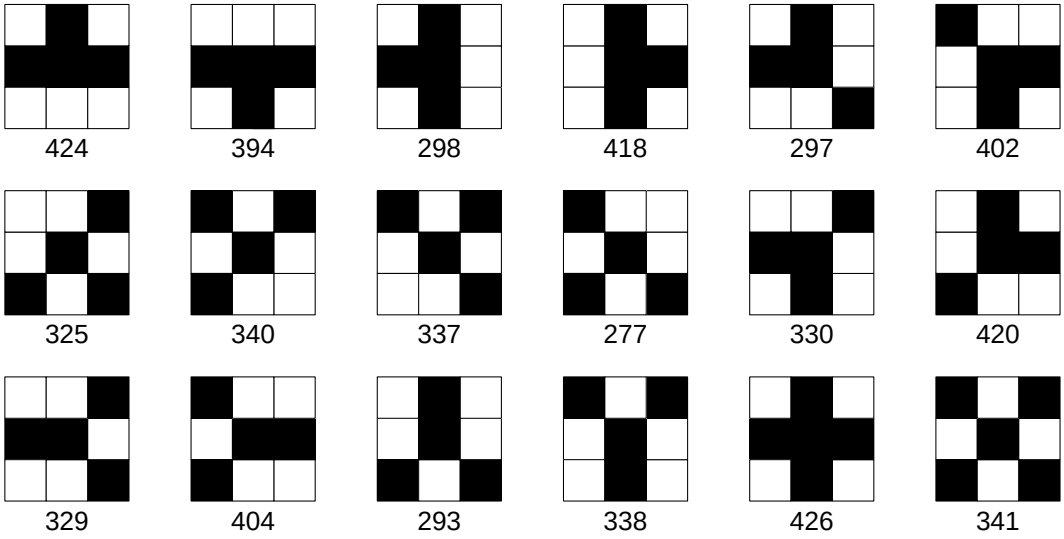


Figure 7.6: Bifurcation patterns and their corresponding filter response.

Method	Std. dev	Mean	Max	Min
Convolution endp.	0.0001	0.0014	0.0051	0.0012
Convolution bif.	0.0001	0.0014	0.0024	0.0012
Window endp.	0.0022	0.1219	0.1488	0.1178
Window bif.	0.0122	0.1067	0.1783	0.0658
Crossing number†	0.0008	0.0079	0.0129	0.0026
Convolution†	0.0001	0.0018	0.0048	0.0017

Table 7.1: Results from experiment. Numbers are in seconds. †Both endpoint and bifurcation detection included.

imum and minimum time (in seconds) for performing the processing. The two first rows show the convolution approach respectively for endpoint and for bifurcation detection. We can see that the time spent on is close to equal which means that most of the processing time is spent convolving the mask and image. Thus the process can be sped up by performing endpoint and bifurcation detection in one pass (method Convolution, last line in the table). The average computation time for the extraction of the end- and bifurcation points for one skeletonized image using the convolution approach is about 0.0018 seconds on a Intel Core i7 (avg. number of endpoints: 38.17, bifurcations: 35.66). Compared to the crossing number approach which uses about 0.0079 seconds per image this translates to a speedup of roughly 4.3 times.

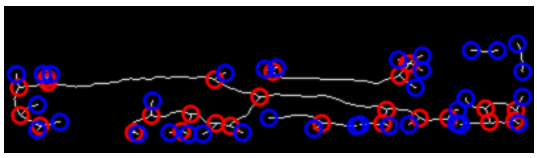
7.5 Conclusions and Future Work

The convolution approach presented herein is able to detect arbitrary patterns within the mask size and is therefore also qualified for the application of feature point detection in biometric systems based on skeleton structure like vein patterns or fingerprint ridges. The convolution approach is very efficient as shown in the experiment. When using the convolution approach a speedup of roughly 4.3 times is achieved compared to using the crossing number approach. The speedup is significant as biometric systems work on increasingly large datasets and need to be operating in near real time so as to maximize throughput.

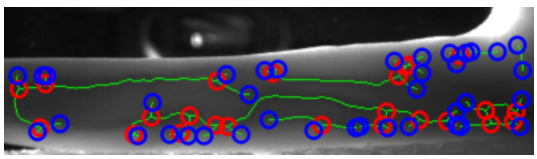
One drawback of the feature point detection using convolution is that the patterns need

(a) Segmentation of a vein pattern image.

(b) Skeletonization of segmented image.



(c) Skeleton with features marked.



(d) Overlayed with input image.

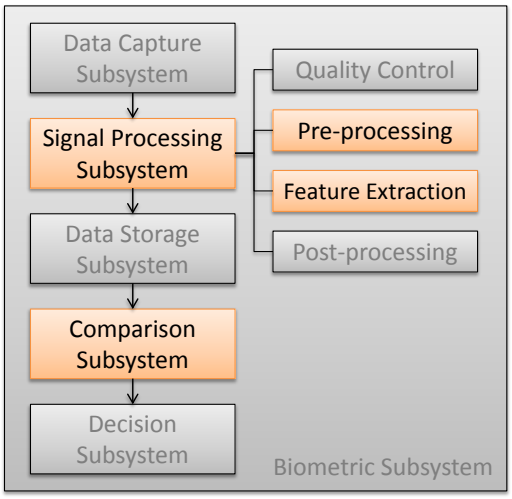
Figure 7.7: Skeleton and features (bifurcations in red, endpoints in blue) from a sample finger vein image (preprocessed with STRESS [120], segmented with LoG).

to be known in advance. The number of possible patterns is growing exponentially with the mask size, but in practice the number of desired patterns is often limited. The extendability of the method is a desirable as arbitrary features can be detected by updating the mask and the set of filter responses to detect. For vein pattern recognition a 3×3 neighborhood gives sufficient information for the distinction between end- and bifurcation points. In the context of other image processing applications other sets of patterns are of interest and still the same underlying concept of convolution and filter response matching can be applied.

In the context of biometrics the skeleton needs to be stable, small islands and false minutiae can disturb the comparison of two biometric samples, research has to focus on the reliable extraction of those skeletons.

Chapter 8

Feature Extraction From Vein Images Using Spatial Information and Chain Codes



A biometric pipeline for comparison of finger and wrist vein images is introduced here. The comparison is based on the distance and orientation of vein skeletons and results in a state-of-the-art recognition accuracy, however, the algorithm has major drawbacks: (i) comparison process is complex and expensive in computation; (ii) features are not compatible to HDS. Parts of the developed pre-processing are re-used for succeeding algorithms as the one introduced in Chapter 9.
The original paper was published in: [79] HARTUNG, D., PFLUG, A., AND BUSCH, C. Vein pattern recognition using chain codes spatial information and skeleton fusing. In Sicherheit (2012), pp. 245256. The attached extended version is published in: [178] PFLUG, A., HARTUNG, D., AND BUSCH, C. Feature extraction from vein images using spatial information and chain codes. Information Security Technical Report, (2012).

Abstract

The pattern formed by subcutaneous blood vessels is unique attribute of each individual and can therefore be used as a biometric characteristic. Exploiting the specific near infrared light absorption properties of blood, the capture procedure for this biometric characteristic is convenient and allows contact-less sensors. However, image skeletons extracted from vein images are often unstable, because the raw vein images suffer from low contrast. We propose a new chain code based feature encoding method, using spatial and orientation properties of vein patterns, which is capable of dealing with noisy and unstable image skeletons. Chain code comparison and a selection of preprocessing methods have been evaluated in a series of different experiments in single and multi-reference scenarios on two different vein image databases. The experiments showed that chain code comparison outperforms minutiae-based approaches and similarity based mix matching.

8.1 Introduction

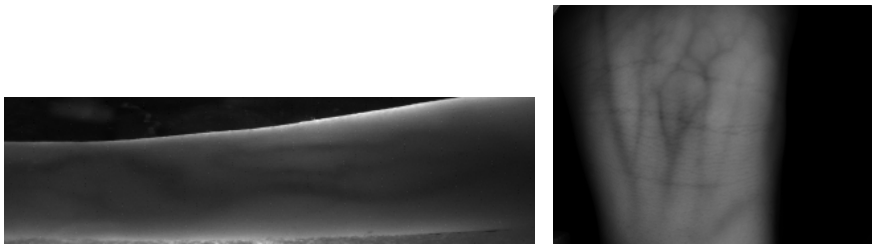
Intended to be a robust approach for liveness detection in fingerprint and hand geometry systems, vein recognition evolved to an independent biometric modality over the last decade. Classically the capturing process can be categorized in near and far infrared approaches. Vein recognition systems based on the near infrared approach are exploiting differences in the light absorption properties of the de-oxygenated blood flowing in subcutaneous blood vessels and the surrounding tissue. Veins become visible, as seen in Figure 8.1, as dark tubular structures. They absorb higher quantities of the infrared light emitted by the LED of the sensor, than the surrounding tissue. Alternatively in the far infrared approach the heat radiation of the body can be measured. Because the temperature of blood is typically higher than the temperature of the surrounding tissue, the temperature gradient between the blood vessels and the tissue can be measured in this spectrum. Additionally, vein scanners can work contact-less, hence they are considered to be more hygienic than systems requiring direct physical contact. This makes them particularly suitable for applications in public areas.

Vein patterns evolve during the embryonic vasculogenesis. Their final structure is mainly influence by the process of cell division and can therefore expected to be random [52]. Even though scientific research about the uniqueness of vein patterns is sparse, many resources state that vein patterns are unique among individuals. Due to the fact, that the network of blood vessels forming the vein patterns is located underneath the skin, a vein pattern is hard to forge without the data subject's knowledge. Known approaches for forging vein patterns not only include the subject's knowledge but also his cooperation, such as shown in [56].

It is also expected, that the position of veins is constant over a whole lifetime [107]. Offering the same user convenience as fingerprints while being highly secure against forging, vein recognition has been applied in various fields of authentication and access control during the last years such as ATMs or airports. As a reaction to increasing misuse of bank cards for instance, a number of large banks in Japan integrated vein recognition systems into their ATMs [247]. The German logistics service DHL decided to use vein recognition for access control to high security areas at their new hub at Leipzig airport [254].

Still vein recognition faces challenges: limitations in capturing in-vivo images from the inside of the body, as well as ambient sunlight, temperature and varying skin properties like the pigmentation, or the thickness influence the image quality. As a result of all these factors the raw images delivered by the sensor have a low contrast, contain noise and a non-uniform brightness. Sophisticated algorithms for the preprocessing like contrast enhancement and segmentation as well as the final feature extraction and comparison are necessary to handle the variations and the noise.

In this paper we contribute a new chain code based feature extraction method and investigate its performance in combination with fusion techniques of image skeletons. The



(a) (b)

Figure 8.1: Finger/wrist vein samples images from: (a) GUC45; (b) UC3M database.

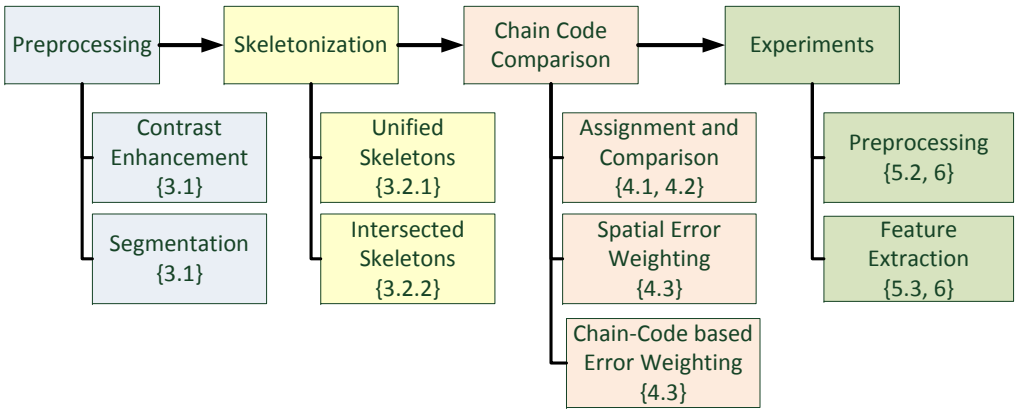


Figure 8.2: Structure of this paper [refers to in-chapter numbering].

fusion aims at enhancing the biometric performance and the robustness against noise. Our approach is compared with minutiae-based feature extraction and a state-of-the-art geometry-based direct comparison approach.Moreover we measure the impact of different segmentation methods, image skeleton extractors and error weighting schemes on the biometric performance of our chain code based feature extractor. The experiments using finger vein images and wrist vein images showed that chain code comparison combined with skeleton fusing performs better than alternative direct comparison methods from the literature. An illustration of the work flow of our benchmark system in connection to the structure of this work is illustrated in Figure 8.2

The rest of this work is structured as follows. Section 2 will give an elaborate overview over relevant work in the field of vein recognition including work on the enhancement of vascular images. In Section 3, image enhancement, segmentation algorithms, the extraction of image skeletons and the skeleton fusing techniques used during the benchmarks in this paper will be described. After having introduced all necessary preprocessing steps, Section 4 will focus on the extraction and comparison of chain codes. The experiments and benchmarks conducted on the vein data will then be presented in Section 5. Finally Section 6 will conclude the paper with some future perspectives concerning vein recognition.

The paper extends the work from [79]. It contains an elaborate survey on the state of the art in the field of vein recognition and also introduces a new weighting scheme as an extension of the already published paper. Moreover we provide more details on the proposed algorithm and also present additional experimental results including the impact of skeleton pruning and the impact of different parameters on chain code comparison.

8.2 State of the Art

Since the first suggestion to use the blood vessel network as a biometric characteristic was made more than one decade ago [121], a large number of different techniques for extracting and comparing vein patterns have been made. This section gives an overview of preprocessing, feature extraction and comparison algorithms.

8.2.1 Preprocessing

As stated above, vein images tend to suffer from low contrast and noise. This raises the necessity for contrast enhancement methods. these methods suppress noise and enhance the local contrast of a vein image. Olsen achieved good results by using the STRESS algorithm [120, 168], which not only enhances the image's contrast but also balances irregular shading. A very fast and simple method for contrast enhancement is Wang and Leedham's normalization method [237]. It stretches the contrast by normalizing the gray values contained in the images but is not able to compensate irregular shading.

Another common problem with vein images is noise, which is hard to remove without loosing information about the vein contours. Due to the imaging technique used by the sensor, the vein's edges are blurry. Deepika and Kandaswamy [45] solve this problem by using the non-linear diffusion method, which smoothens homogeneous image regions and preserves the vein's edges. The GSZ-Shock Filter used by Deepalmar and Madheswaran [44] can also be used for this purpose. If no explicit edge enhancement is needed, noise can be reduced by using a Gaussian filter [30] or dyadic wavelet transform [266].

Since many feature extraction algorithms work on image skeletons, the vein images must be segmented after the noise has been removed. A well-established histogram based segmentation approach was proposed by Otsu [169]. His method calculates a number of thresholds based on the gray level histogram in such a way that large quantities of similar gray values are considered as representing an object. Wang and Leedham [237] propose an algorithm called Adaptive Local Thresholds, which segments normalized images by using the local brightness information of the image. However this method has problems with blurry edges and low local contrast.

With their algorithms Repeated Line Tracking [157] and its successor Maximum Curvature Points [159], Miura and Nagasaka proposed two segmentation methods, which are robust to irregular shading and blurry edges. The maximum curvature points algorithm analyses brightness changes in cross-sectional image profiles and hence is not affected by a vein's width and brightness. Repeated Line Tracking starts at various random points in the vein image and follows light-colored structures in the image. All pixels visited by the algorithm are tracked in a separate locus image, which is representing the location of the veins after the algorithms has terminated. A modified version of repeated line tracking is used by Yang et. al. [275].

A widely used segmentation algorithm in different applications for segmentation algorithms is the active contours method as proposed by Chan and Vese [27]. It has been applied to vein images of palm dorsal by Soni et. al. [209]. Active contours works with the principle of the intensity gradient. At least one initial shape is placed at a random point in the image before active contours moves, splits, merges and warps this shape until it represents the contours of the veins displayed in the image.

A completely different approach to segmentation are filter based methods. Olsen achieved good segmentation results by using the standard technique of Laplacian of Gaussian [168], whereas Vlachos and Dermatas designed a dedicated compound filter, which is specialized in detecting horizontal, tubular structures [230]. A similar approach has been propose din a earlier publication by Frangi et. al. [58], who also designed a special filter for detecting blood vessels in retina images.

8.2.2 Feature Extraction and Comparison

A multitude of different feature extractors and comparison algorithms have been proposed over time. This chapter categorizes different comparison algorithms applied in vein recognition following the features they are using. We differentiate between local comparison methods, which use certain details of the image for feature extraction, whereas holistic methods use whole images or image skeletons for comparison.

8.2.2.1 Holistic Methods

One of the most famous holistic comparison methods is the principal component analysis (PCA), which used in numerous pattern recognition tasks. In [119] Khan et. al. applied PCA on image skeletons derived from hand vein images. Principal component analysis can also be applied directly on enhanced images [236].

Xueyan et. al. derive vein descriptors using invariant moments for distinguishing the segmented vein images from different subjects. In [65] Guan et. al. have proposed to use bi-directional weighted modular PCA and compared the performance of different flavor of their algorithm with each other. In their studies, which were conducted with 132 subjects and a self-made capturing device, bi-directional weighted modular PCA showed the best performance among the other tested approaches. In a later approach Guan et. al. also evaluate the performance of an approach based on linear discriminant analysis on the same database, but could not improve the biometric performance with this approach [66].

All feature extraction and comparison algorithms enumerated so far are working with statistical properties of vein images. Chen et. al. [30] propose two algorithms for direct point-wise comparison, which overcome problems with affine transformations. Iterative Closest Point Matching (ICPM) is a modified version of the Iterative Closest Points algorithm for registering images. The second algorithm proposed by Chen et al., Similarity-based Mix-matching (SMM), compensates small translation and rotation errors by comparing the segmented version of one image with the image skeleton of the other one.

Yang and Li [271] propose a set extract energy maps from the responses of steerable filters. Based on the amount of energy returned by a filter, they assign a gray value to each block of 5x5 pixels in the vein image. The resulting images with each pixel representing the average response of a 5x5 block in the vein image are then compared bit pixel by pixel. They evaluate the performance of their feature extraction technique by using a database, which consists of 100 subjects, and showed that their approach performances other approaches. However they do not provide results using other databases.

In [155], Mirmohamadsadeghi and Drygajlo apply histograms of local binary patterns (LBP) as well as local derivative patterns (LDP) for feature extraction on palm vein images. In elaborate experiments they evaluated the behaviour of these descriptors under different constraints and also measured the performance of different distance measures for the histograms. They were able to achieve promising results with both descriptors, especially with a histogram intersection method.

8.2.2.2 Local Methods

Known as established features from fingerprints, minutiae have also been used for extracting features from skeletonized vein images [228]. Because minutiae are composed of spatial coordinates, they are subject to translation and rotation. This issue is addressed by projecting minutiae points into frequency space [260], where translation gets eliminated and rotation becomes translation. Spectral minutiae have also been applied to vein recognition [228] in different variants. SML performs an element-wise comparison of two minutiae-spectra in frequency space, whereas SML fast Rotate (SMLFR) compares the spectra while trying different translations of them. However the number of minutiae contained in the image can be very small. Instead of comparing their positions directly, it is also possible to use the distances between all minutiae as features [236]. Wang further proposes to use the line

segments, which are separated by endpoints and bifurcations [237]. Fan et. al. propose to use the watershed algorithm for detecting dominant points from a vein image [54]. Three different filters generate a multi resolution representations of these dominant points, which serve as features.

8.3 Preprocessing

8.3.1 Contrast Enhancement and Segmentation

As already mentioned, all vein images have to be enhanced in a preprocessing stage before features can be extracted from the image. The vein images used during our experiments are first enhanced by using adaptive non-local means taken from [212] followed by the noise suppressing and edge enhancing non-linear diffusion algorithm [250].

The image enhancement step is followed by a segmentation step. In order to see, if there is an image segmentation method, which is particularly suitable for segmenting vein images, three different segmentation methods have been compared. The first of these methods is Otsu's histogram-based segmentation [169]. Additionally the active contours algorithm proposed by Chan and Vese [27] and the multi-scale filter method by Frangi et. al. [58] have been tested on the finger vein images.

8.3.2 Skeletonization

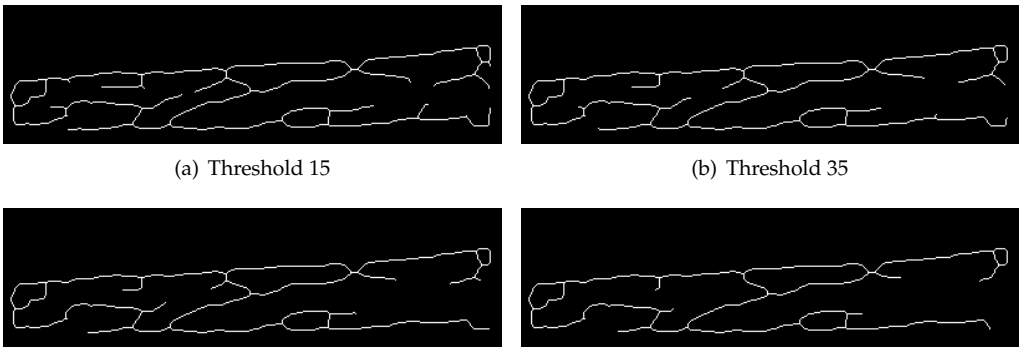
In the approaches we used in our experiments, skeleton images are the basis for feature extraction. Because of noise and poor contrast, these skeletons can look different, even though they come from the same biometric source. In order to improve the reliability of the extracted image skeletons and hence the reliability of the extracted features, we propose to use fast marching skeletonization[1] as proposed in [220] in combination with two different approaches for fusing multiple skeletons to a single one. The goal is to create a more stable version than any of the input skeletons.

In fast marching skeletonization incremental indices are assigned to each pixel on the edge of the figure. Then they are collapsed until only the center line is left. From the difference between two neighboring indices in the collapsed figure, a local weight of a branch can be determined. For those parts of the image skeleton, derived from the center part of the figure, the difference between the indices is high and so is their weight. These fine-grained branches are likely to be artifacts, which were introduced by segmentation errors or noise and can be removed by applying a threshold. All skeleton points where the difference between their indices falls below the threshold are deleted. All other points are kept. Hence, depending on the threshold, more or less of these remote branches are cut off. The larger the threshold value, the more details are removed (see Figure 8.3).

8.3.3 Skeleton Fusing

In order to further enhance the stability of skeletons, we propose two basic fusing techniques. The first one is called skeleton unification and produces a skeleton which possesses all branches and details, of the input skeletons. The second one, called skeleton intersecting, combines a variable number of input skeletons and delivers combined skeletons which possess only the branches which the majority of the input skeletons has in common. The goal is to create a more stable version than any of the input skeletons.

[1]The skeletonization algorithm by Zhang and Suen [285] introduced in Chapter 7 proved to be error prone for noisy shapes like segmented vein patterns. In some cases new edges were introduced from noisy parts of the segmented image. Therefore we decided to utilize the fast marching skeletonization. It is based on the fast marching method by Sethian [202] and can be classified as a *distance transform* (DT) method where the resulting skeleton lies along the singularities. The main advantages are the real-time execution with similar results to other DT approaches, the robustness with respect to noisy boundaries and the possibility for pruning of spurious branches.



(a) Threshold 15 (b) Threshold 35

(c) Threshold 50 (d) Threshold 75

Figure 8.3: Skeletons extracted by fast marching skeletonization methods using different thresholds. The higher the threshold the more details are cut off from the skeleton.

(a) (b) (c)

Figure 8.4: Fusion based on unification (GUC45 samples) using $n = 3$ input skeletons: (a) superimposed structure S_{uni_1}; (b) disk-shape structuring element dilated structure S_{uni_2}; (c) final unified skeleton S_{uni}.

(a) (b) (c)

Figure 8.5: Fusion based on intersection (GUC45 samples) with $n = 5$ input skeletons and threshold $t = 3$: (a) dilated density structure S_{int_2}; (b) S_{int_3} (threshold t applied to segment S_{int_2}); (c) final intersection skeleton S_{int}.

8.3.3.1 Unified Skeletons

For deriving a unified skeleton it takes n input skeletons, where n was set to 3 in our experiments. In a first step, all input skeletons $S_i(x, y)$ are aligned using ICP [192] and then super-imposed to a common structure S_{uni_1} (Figure 8.4(a)).

$$S_{\text{uni}_1}(x, y) = \cup_{i=1}^{n} S_i(x, y) \tag{8.1}$$

The registered input skeletons are fused together by dilating the superimposed figure S_{uni_1} with a disk-shaped structuring element (Figure 8.4(b)) to get S_{uni_2}. Afterwards the fast marching skeletonization algorithm [220] is applied to the dilated figure in order to create the unified skeleton S_{uni} (Figure 8.4(c)).

8.3.3.2 Intersected Skeletons

The second proposed algorithm creates an intersected skeleton, which possesses only those features which occur in at least t of the input skeletons. An example for skeleton intersection with $n = 5$ input skeletons is illustrated in Figure 8.5. The intersected skeleton in

Figure 8.5 consists of the lines which occur in at least three of the five input skeletons ($t \geq 3$).

Similarly to the unification approach, the input skeletons S_i need to be aligned to each other. Then each of the n input skeletons is dilated with a disk-shaped structuring element, creating binary structures S_{int_1}. These dilated skeletons are then added up to form a common unified density structure called S_{int_2}.

$$S_{\text{int}_2}(x,y) = \sum_n S_{\text{int}_{1\text{n}}}(x,y) \tag{8.2}$$

S_{int_2} contains values between 0 and n. All input skeletons having a pixel that is classified as vein at position (x,y) in case of $S_{\text{int}_2} = n$ and 0, meaning that none of the input skeletons has any veins at this coordinate. Now a threshold value t with $1 \leq t \leq n$ is applied to S_{int_2} resulting in S_{int_3}. In this step all pixels which at least occur t times in the input skeletons are kept, all other pixels are set to zero.

$$S_{\text{int}_3}(x,y) = \begin{cases} 1 & \text{for} \quad S_{\text{int}_2} \geq t \\ 0 & \text{else} \end{cases} \tag{8.3}$$

Finally the fast marching skeletonization is applied again, which results in the intersected skeleton S_{int}.

8.4 Chain Code Comparison

Similarities between two image skeletons can be determined by measuring the relative positions of the skeleton lines as well as their relative orientation. Two lines, which are parallel should be considered to be more similar than two non-parallel skeleton lines. Chain code based feature extraction uses the position of each pixel on a skeleton line in combination with its local orientation reflected by the chain code value for feature encoding. This enables the algorithm to find associated points between the probe and the reference skeleton and to measure parallelism.

8.4.1 Preliminaries and Chain Code Assignment

Before chain code values can be assigned to an image skeleton, some preliminaries have to be met. In a first step the probe and the reference skeleton have to be aligned with each other. As for skeleton fusing, we used ICP for skeleton alignment. Moreover all points where veins split up (bifurcations) have to be removed from the image skeleton in order to avoid ambiguities. To make sure all chain codes refer to a common starting point, a reading direction has to be defined. In our work, chain code extraction started from the bottom left corner of the image and ended at the top right corner. If the reading direction is fixed, chain codes extracted from the same shape with different coordinates will be identical. After the skeletons are computed, the feature extraction module iterates over each pixel (x,y) of the skeleton starting from the bottom left corner. Each skeleton pixel is assigned a chain code value according to the relative position of its successor in reading direction (see Figure 8.6). The chain code assignment for each pixel indexed by its coordinates x and y in the skeleton image I_{skel} is defined as

$$C(x,y) = \begin{cases} 1 & \text{if} \quad I_{\text{skel}}(x+1,y) = 1 \\ 3 & \text{if} \quad I_{\text{skel}}(x+1,y+1) = 1 \\ 5 & \text{if} \quad I_{\text{skel}}(x,y+1) = 1 \\ 7 & \text{if} \quad I_{\text{skel}}(x-1,y+1) = 1 \\ 9 & \text{if} \quad I_{\text{skel}}(x-1,y) = 1 \\ 0 & \text{else} \end{cases} \tag{8.4}$$

8.4.2 Comparison

After chain code assignment, the similarity between two aligned chain codes C and C' is calculated. The algorithm tries to find pairs of associated points by searching in orthogonal direction to the local orientation of the chain code value stored at the currently examined point. The search for associated pixels stops if either an associated point could be found or if the maximum search depth d_{max} is exceeded. When a pair of associated skeleton points has been found, their similarity is calculated based on their spatial distance d and the chain code difference c.Where (x, y) and (x', y') are the coordinates of the two associated points and $C(x, y)$ and $C'(x', y')$ are their chain code values.

$$d = \sqrt{|x - x'|^2 + |y - y'|^2} \tag{8.5}$$

$$c = |C(x, y) - C'(x', y')|^2 \tag{8.6}$$

The local error E at the point (x, y) is then calculated as follows.

$$E(x, y) = \frac{d + c}{E_{\max}} \tag{8.7}$$

$$E_{\max} = \frac{d_{\max} + c_{\max}}{2} \tag{8.8}$$

The values for $d_{\max}$ and $c_{\max}$ denote the maximum search depth and the maximum possible difference between two chain code values. Following Equation 8.6 and the scheme sketched in Figure 8.6, $c_{\max} = 8^2 = 64$. The local error is stored at position (x, y) in an error map E, which has the same size as the input images.

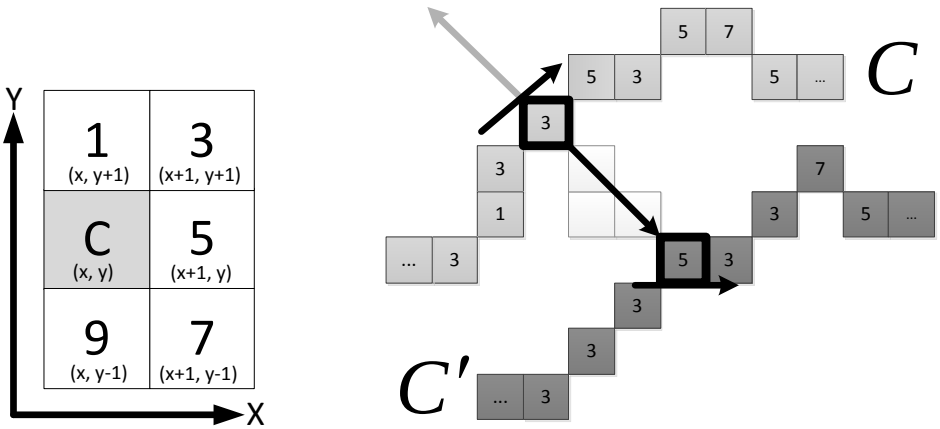
The assignment of associated points is depending on the order of the two skeletons to be compared (probe/reference). If we start with the reference skeleton and search for an associated pixel in the probe skeleton, a different pixel pair can be identified as if we would have started the other way around. This also means that the local error depends on the order of the two skeletons. This is handled by computing two error maps E_1 and E_2. E_1 contains all local errors calculated by using C as reference and C' as probe skeleton and E_2 contains all local errors using C' as probe and C as reference, respectively. The total error map E_{total} is the sum of local errors for each point in the skeleton images and is computed as follows:

$$E_{\text{total}}(x, y) = E_1(x, y) + E_2(x, y) \tag{8.9}$$

Finally the similarity score of the skeletons to compare is defined as:

$$\text{Score} = 1 - \frac{\sum_x \sum_y E_{\text{total}}(x, y)}{\sum_x \sum_y E_{\max}} \tag{8.10}$$

An example of how a point pair can be found by using the local chain code value is shown in Figure 8.6(b). The algorithm starts at the boldly bordered point in C and searches in orthogonal direction for a corresponding point in C'. After two mated points have been identified, their local error, which is a value between 0 (no error) and 2 (maximum error) is calculated. The global distance measure between all points in C and C' is, as stated before, the weighted sum of all local errors.



(a) (b)

Figure 8.6: Chain code extraction scheme for feature extraction from prepared image skeletons and calculation of local error using the spacial distance between two associated pixels and the chain code difference

8.4.3 Error Weights

Caused by the position of the infrared-LEDs in the sensor and the human physiology, the contrast is not the same throughout the image region. Especially the edge regions of the image are typically darker than the center region of the image, which means that local error extracted from the center regions of the image are more likely to be reliable than local error in the edge regions. In order to take this into account a weighting function $\omega_1(x, y)$ is introduced which assigns higher weights to the local errors in the center regions of the image. It calculates a weight for each local error according to its position in the image. $width$ represents the total width of the image. An threshold value t is defined, which specifies the image region where the weight of the local error decreases. We assigned an error weight smaller than one to the leftmost quarter of errors and the rightmost quarter of error respectively. Hence the value 0.25 for t was used here. w denotes the total with of the image.

$$\omega_1(x, y) = \begin{cases} \frac{y-x}{w-t} & \text{if} \quad x < w - t \\ \frac{t-x}{t} & \text{if} \quad x > t \\ 1 & \text{else} \end{cases} \tag{8.11}$$

Another possibility of error weighting is based on the fact that most veins in our finger vein image are horizontal, which is caused by the architecture of the sensor. Hence, the portability of being a noise artifacts is assumed to be higher, the more a chain code value differs from horizontal orientation. As the local chain codes for the veins have already been assigned, this information can additionally be used for applying a weighting factor based on the local orientation of a line, namely the local chain code value. As mentioned above, chain code values already indicate the local orientation of a skeleton line, hence the local error can also be weighted using the chain code values. ω_2 calculates a weighting factor for each error depending on the chain code value C in the comparison image. The constant h represents the chain code value assigned to a line with horizontal orientation. For our chain code extraction scheme, h is set to 5.

Database	GUC45	UC3M*
Frequency Band	NIR (850nm)	
Sensor	non-commercial	
Modality	Finger (10)	Wrist (2)
Data Subjects	45	29
Sessions	12	1
Images per Session	10×2	2×6
Images	10800	348
Resolution (px)	$512 \times 240^{\dagger}$	640×480
Depth	8 Bit gray-scale	

Table 8.1: Properties of the biometric vein datasets used in the experimental section. †For the experiment the images are cropped to size 468×122 to eliminate most non-finger area. *Details published in [171].

$$\omega_2(C) = \begin{cases} 1-(C-h)^2 & \text{if} \quad C \neq h \\ 1 & \text{else} \end{cases} \tag{8.12}$$

8.5 Experimental Setup

All experiments were conducted on the basis of a modular vein verification system implemented in MATLAB. The benchmark system allows for arbitrary combinations of different segmentation, feature extraction and comparison modules. The main quality measure used for benchmarking different pipeline configurations is the equal error rate (EER). We conducted two different experiments, one covering aspects of preprocessing in connection with chain code comparison and the second one dealing with the comparison of selected feature extraction, error weighting and comparison approaches. Information about both experiments and the databases which were used during the evaluation is provided in this section.

8.5.1 Vein Databases

In the experiments two different vein databases were used. Their main properties are summarized in Table 8.1. In both cases the images were captured with a CCD-camera and illuminated with NIR light at a wavelength of 850nm. The GUC45 dataset contains finger vein images from 45 data subjects collected at Gjøvik University College in Norway over a long period of time. Each finger, including the thumbs, was captured two times during each of the 12 sessions, which results in 10800 unique vein images in total. The images from GUC45 suffer from low contrast and high noise, which makes it hard for any algorithm to extract stable skeletons and hence to achieve a low error rate on this data. However this fact makes them particularly interesting for research purposes as it allows for exploring the limitations of algorithms for feature extraction and comparison.

The second database, called UC3M, consists of wrist vein images, which were collected as described in [171]. The focus of this experiment was to evaluate the effect of different illumination intensities on the visibility of veins. For each of the 29 users, 6 images were taken for each hand under three different illumination settings. This results into 348 images in total.

8.5.2 Preprocessing

The preprocessing stage consists of three steps, namely image enhancement, segmentation and skeletonization. During image enhancement, noise should be removed and at the same time image contrast should be enhanced. In order to meet both criteria, different methods are combined. In a first step, the vein images are enhanced with adaptive non-local means as proposed by Struc and Pavesic [212] followed by non-linear diffusion for noise suppressing and edge enhancement [250].

The image enhancement step is followed by a segmentation step. In order to see, if there is an image segmentation method, which is particularly suitable for segmenting vein images, three different segmentation methods have been benchmarked. The first of these methods is Otsu's histogram-based segmentation [169]. Additionally the active contours algorithm proposed by Chan and Vese [27] and the multi-scale filter method by Frangi et. al. [58] have been tested on the vein images.

Preprocessing is concluded by the skeletonization approach proposed by Telea and van Wijk [220]. For determining the influence of skeleton pruning on the EER, we compared the biometric performance of different pipelines using chain code comparison and Otsu's segmentation algorithm with different thresholds during the skeletonization step.

8.5.3 Feature Extraction Evaluation

For comparing the biometric performance of chain code comparison to other feature extraction methods, we evaluated chain code comparison on GUC45 and UC3M. We compared the performance to the evaluation results of spectral minutiae (SML and SMLFR) as proposed in [77], Similarity-based Mix-Matching (SMM) [30] and the performance of chain code comparison on single references and fused skeletons. In all experiments using fused skeletons, the fused skeleton served as the reference image and a skeleton extracted from one vein image was used as the probe image.

We investigate the influence of the maximum search distance on the error rate of chain code comparison and evaluated the discriminating potential of spatial and chain code distance. Furthermore evaluate the influence of the previously introduced error weighting schemes on the EER. For doing this we configured a pipeline using Otsu's segmentation algorithm, fast marching skeletonization with a threshold of 35 and chain code comparison for feature extraction.

8.6 Results

In our experiments, the segmentation algorithms came to slightly different results, but had a minor effect on the overall system's performance. The measured performance difference between the different segmentation algorithms on GUC45 is less than 2% points in terms of the EER. The main difference between the evaluated segmentation approaches was in terms of computation time, however the approach by Frangi and Niessen performed slightly better on the UC3M dataset.

In contrast to the preprocessing step, the impact of the feature extraction and comparison method is significant. Table 8.2 summarizes the performance measures for each of the datasets. The results for GUC45 were obtained using Otsu's segmentation algorithm, whereas the EER measures on UC3M are based on Frangi and Niessen's filter-based approach. For each of the evaluated configurations we measured the EER and the operating point for 0.1% FAR. Furthermore we provide the 90% confidence intervals for each of the measured performance indicators.

The images in GUC45 have a particularly low contrast and therefore cannot be expected to give good biometric performance. However, GUC45 is a challenge for all tested algorithms. In addition, it also contains multiple samples per subject. The results of the different feature extraction and comparison approaches on GUC45 are summarized in Figure

8.7. The best performance could be achieved with chain code comparison using unified skeletons as reference samples and skeletons derived from only one image as probes. This configuration was named Fused Union. With an EER of 24.67% Fused Union outperformed all other configurations including SMM, but also single reference chain code comparison. This shows that already a simple skeleton fusing approach like the proposed one, enhances the quality of image skeletons and improves the system performance. None of the error weighting schemes has an effect on the performance of chain code comparison. On average, ω_2 had a slightly better performance than ω_1, but the confidence value indicate that there is no statistically significant difference between these two configurations.

Further investigations on the performance of Fused Union for each finger on GUC45 showed, that the fingers of the left hand appear to be more suited for vein recognition than the right hand fingers (see Figure 8.7(b)). In our experiments, the highest error rate was measured with images from the thumbs (Fingers indices 5 and 6). The EER of configurations using intersected skeletons increases the more input skeletons are used. A reason for this could be that unstable skeletons have only few intersecting parts, which results in fused skeletons with low details. Less details however mean less discriminative power and results in increasing error rates.

For the UC3M dataset an excellent biometric performance could be measured without the skeleton fusion techniques proposed. SMM and the chain code algorithm perform at the same level (EER around 1% EER). Skeleton fusion could reduce the EER to 0.63%, whereas skeleton intersection with $n = 3$ and $t = 2$ yielded an EER of 0.67%.

Whereas the segmentation did not have any effect on the EER, the level of detail in the skeletons had a measurable effect on the performance of chain code comparison. Figure 8.7(c) shows, that a careful selection of the threshold during fast marching skeletonization can deliver a considerable improvement of the overall performance. The lowest EER could be achieved when using a threshold of 35. The performance obtained from other thresholds is similar and moves around approximately 31% EER. The only outlier is the threshold 5. The reason for this are artifacts, introduces by fast marching skeletoization during the assignment of indices. These artifacts are removed when applying thresholds above 15, but are sill part of the skeleton for low thresholds.

Experiments on the behaviour of chain code comparison using different search depths showed, that the careful choice of this parameter is crucial, as the spatial distance between two skeleton points appeared to have a larger impact on the biometric performance than the difference between two adjacent chain codes. The reason for this is that there the possible variance between two chain code values is small compared to the variance of the spatial distance. The maximum search depth should be chosen according to the resolution of the input vein images and the expected density of the vein patterns. For GUC and UC3M a maximum search depth of 9 pixels delivered the best performance.

8.7 Conclusions and Future Work

The proposed chain code algorithm as well as the state of the art SMM [30] algorithm perform very similar on the chosen datasets, it seems the quality of the images is a limiting factor here. Only a multi-reference approach could further improve the results.

Even though the proposed comparison on Fused Union skeletons showed promising results, the algorithm's time wise performance is not impressive compared to other feature extraction and comparison algorithms. Future work focuses on reducing the required computing time by replacing the pixel-based chain code extraction with a convolution-based approach and by selecting less reference points for skeleton registration and comparison in order to further decrease the size of the feature vector.

Further improvements could also be made by extending the error calculation to complete line segments in order to make chain code comparison less sensitive to single outliers and more sensitive to mismatching line segments. Moreover, additional simulations

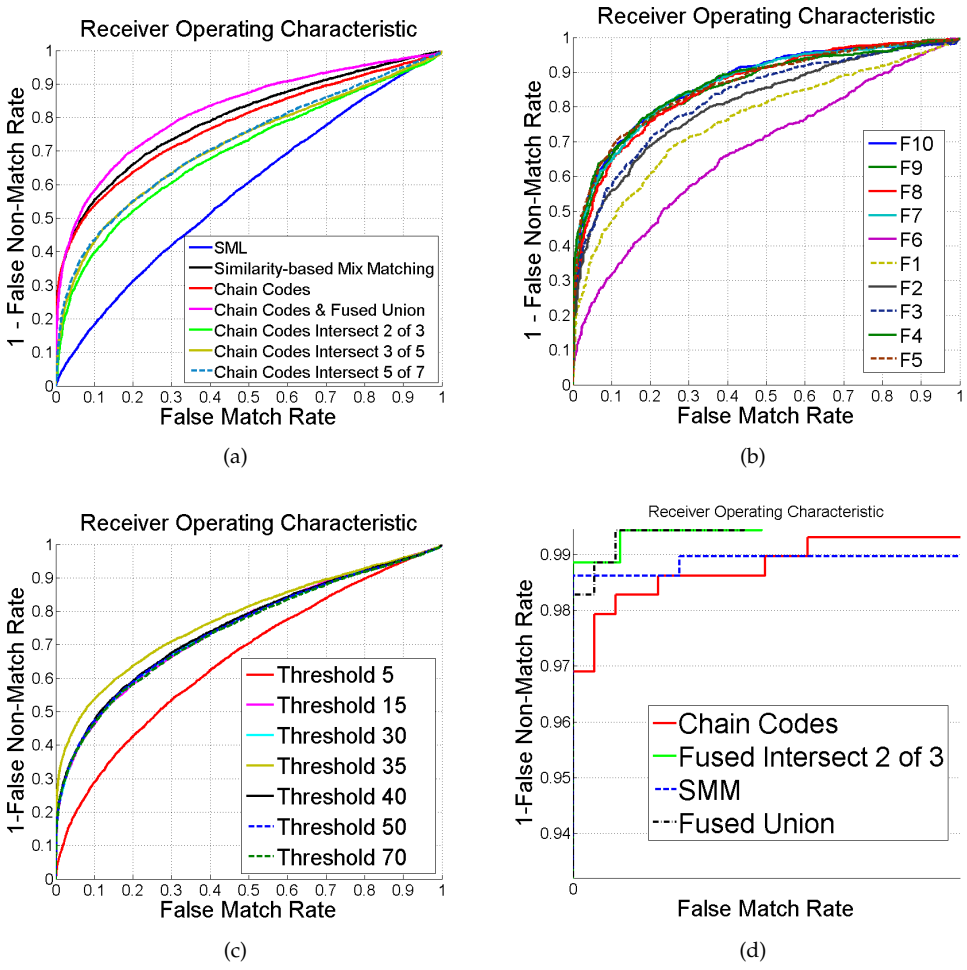


Figure 8.7: ROC curves for (a) selection of feature extraction algorithms and (b) *Fused Union* configuration, different finger samples from GUC45 dataset. Finger indices are assigned according to the ISO-standard [102] with indices 1 until 5 for the right hand fingers in indices 6 until 10 for the left hand fingers, where counting always starts from the thumbs. (c) shows ROC curves for a selection of different thresholds in fast marching skeletonization using chain code comparison. (d) shows ROC curves for chain code pipelines and SMM on the UC3M dataset

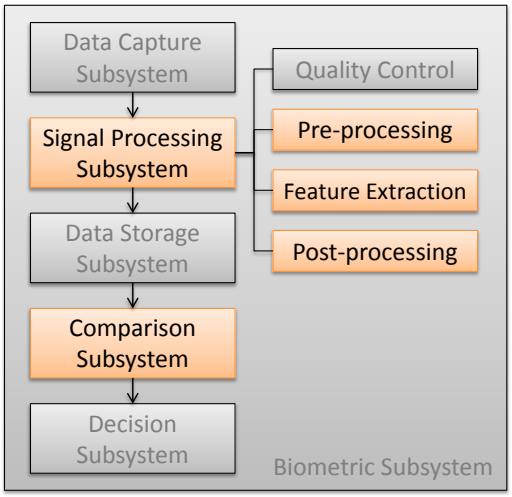
Comparison Algorithm	GUC45		UC3M	
	EER	OP	EER	OP
Chain Codes	29.06 (±0.73)	77.97 (±0.67)	1.38 (±1.27)	3.10 (±1.68)
Chain Codes with ω_1	29.42 (±0.89)	78.65 (±0.66)	1.38 (±1.13)	1.72 (±1.26)
Chain Codes with ω_2	28.44 (±0.72)	77.041 (±0.68)	2.07 (±1.37)	4.48 (±1.99)
Fused Union	25.21 (±0.71)	84.15 (±0.62)	0.63 (±0.87)	1.72 (±1.62)
Fused Intersect t=2, n=3	34.49 (±0.89)	95.60 (±0.34)	0.67 (±1.10)	1.15 (±1.33)
Fused Intersect t=3, n=5	32.87 (±0.92)	93.71 (±0.43)	NA	NA
Fused Intersect t=5, n=7	32.20 (±0.97)	97.27 (±0.31)	NA	NA
SMM	27.84 (±0.71)	78.40 (±1.13)	1.38 (±0.67)	1.38 (±1.13)
SML	39.089	NA	6.13	NA
SMLFR	40.25	NA	5.90	NA

Table 8.2: Benchmark results (EER in % and OP = FNMR at 0.1% FMR) for finger vein (GUC45) and wrist images (U3CM). The numbers in brackets after each result are the 90% confidence interval for the results. NA: not measured in the experiments.

on different vein datasets will also show the feasibility of the approach for different vein modalities.

Chapter 9

Comprehensive Analysis of Spectral Minutiae for Vein Pattern Recognition



The transformation of minutiae points into the spectral minutiae representation has interesting properties: it has been shown that recognition accuracy for fingerprints is high, in addition the representation is of fixed length and the comparison can be done element-wise. The latter two properties of the resulting feature vectors are a requirement for template protection schemes based on fuzzy commitment like the HDS. Furthermore, the approach is robust to translations of the input, rotations and scaling can be compensated. A single pipeline is designed that processes wrist and palm dorsal (NIR/FIR) raw vein images into spectral minutiae resulting in very high recognition accuracy.
The original paper was published in: [77] HARTUNG, D., OLSEN, M. A., XU, H., AND BUSCH, C. Spectral minutiae for vein pattern recognition. In Biometrics (IJCB), 2011 International Joint Conference on (October 2011), pp. 1-7. The attached extended version is published in: [78] HARTUNG, D., OLSEN, M. A., XU, H., NGUYEN, H. T., AND BUSCH, C. Comprehensive analysis of spectral minutiae for vein pattern recognition. In IET Biometrics (March 2012), vol. 1, pp. 25-36.

Abstract

Similar to biometric fingerprint recognition, characteristic minutiae points – here end and branch points – can be extracted from skeletonized vein images to distinguish individuals. An approach to extract those vein minutiae and to transform them into a fixed-length, translation invariant representation where scaling and rotations can be easily compensated is presented in this study[1]. The proposed solution based on spectral minutiae is evaluated against other comparison strategies on three different datasets of wrist and palm dorsal vein samples. The authors' analysis shows a competitive biometric performance while producing features that are compatible with state-of-the-art template protection systems. In addition, a modified and more distinctive, but not transform or rotation invariant, representation is proposed and evaluated.

9.1 Introduction

Intended to be a robust approach for liveness detection in fingerprint and hand geometry systems, vein recognition evolved to an independent biometric modality over the last decade [16]. Classically the capturing process can be categorized as a near- or a far-infrared approach. Vein recognition systems based on the near-infrared approach are exploiting differences in the light absorption properties of the de-oxygenated blood flowing in subcutaneous blood vessels and the surrounding tissue. Veins become visible as dark tubular structures. They absorb higher quantities of the near-infrared light, that is commonly emitted by light-emitting diodes (LEDs) of the sensor, than the tissue. Alternatively in the far-infrared approach the heat radiation of the body can be measured [242]: the temperature gradient between the blood vessels carrying the warm blood and the tissue can be measured in this spectrum.

Vein patterns evolve during the embryonic vasculogenesis. Their final structure is mostly influenced by random factors [52]. Scientific research about the uniqueness of vein patterns is sparse and many sources state that vein patterns are unique among individuals. It is also expected that the position of veins is constant over a whole lifetime [46]. As vein scanners work contact-less, they are considered to be more hygienic than systems requiring direct physical contact. This makes vein recognition particularly suited for applications in public environments.

Owing to the fact that the mesh of blood vessels forming the vein patterns are located underneath the skin, a person's individual vein patterns is hard to forge; no latent prints are left unintentionally. Offering the same user convenience as fingerprints while being highly secure against forging, vein recognition has been applied in various fields of access control during the last few years. Besides this privacy protecting property, there are also privacy concerns reported in vein recognition systems since disease patterns can be read from the biometrics reference images [71]. There are some attempts to prevent the proliferation of sensitive data from biometric references. First, to overcome the linkability between different databases and second to enable revocation capacities, so that multiple identifiers can be constructed from the same biometric trait. It is not sufficient to simply encrypt biometric templates with classic cryptographic functions since they cannot be compared in the encrypted domain. The goal is to introduce pseudonymous identifiers that cannot be tracked back to the data subject. At the same time profiling should be denied, multiple pseudonymous identifiers of the same data subject should be unlinkable.

An overview of existing biometric template protection systems is given in [18]. The proposed harmonized reference architecture is integrated in the international standard ISO/IEC 24745 *Biometric Information Protection* and its nomenclature is used throughout this paper. Jain *et al.* [106] gives a comprehensive introduction to the topic of biometric template security with a focus on template database security. The authors propose a categorization

[1] In the article scale invariance was mentioned by mistake.

of template protection schemes and discuss pros and cons. One interesting category covers key-binding biometric cryptosystems, they enable the integration of biometric systems into cryptographic protocols. As one advantage the authors mention the tolerance towards intra-user variability and the adaptability through error correction. However, the major drawback described in this paper is that sophisticated comparators cannot be utilized because to requirements on the structure of the feature vectors.

The fuzzy commitment scheme [109] is one of the systems for template protection falling in this category. It introduced error-correcting codes and cryptographic functions to secure biometric data. The helper data scheme (HDS) [225, 226] uses the principle of fuzzy commitments to protect the privacy of biometric features and to satisfy the above-mentioned requirements. It is an extension of classic biometric systems where the extracted feature vectors are further processed. In the scheme, the above-mentioned restriction applies: no specifically designed comparator can be used, the feature vectors must be of fixed-length and structure, so that components can be analyzed for reliability and can consistently be reconstructed from biometric data.

Current work in vein recognition is not focused on solving this issue. However, in [127] a hand vein-based authentication system using Delaunay triangulation of minutiae was presented. The approach is based on the extraction of minutiae groups to form triplets as well as a triplet type, determined from the composition of endpoints and bifurcations. The resulting rotation and translation invariant feature vector is variable in length as determined by the number of identified triplets. Other approaches focus on the extraction of local binary patterns or derived versions [137, 155], which are dependent on alignment based on minutiae points or a region of interest selection. The feature vectors are of fixed length, but they are not invariant against translation, scaling or rotation.

The goal of this paper is to investigate an algorithm that transforms feature vectors from vein patterns into a fixed-length and structure representation compatible with the HDS without loosing performance compared to the original representation [77]. The proposed feature extraction method for vein patterns is based on minutiae points, known from fingerprint recognition, where the position of end and branch points from the skeletal representation of vein patterns are being used. Owing to noise from various sources such as the sensor, the biometric trait, or the pre-processing these feature points cannot be reconstructed perfectly; their amount and their position will vary. To overcome these issues an approach called *spectral minutiae* is applied to the original vein minutiae. This approach was applied very successfully to fingerprint minutiae [264].

In this work, we further analyse the spectral minutiae for vein recognition: we propose a fast orientation estimator of the minutiae, which then can be used to encode the complex spectral minutiae (SMC). Further, we propose a second normalization method for the spectra that increases recognition performance at the cost of invariance to affine transformation of the input data. In addition, a mutual information-based comparator is included and investigated. The experimental section covers an extensive set of investigations: performance for the different types of minutiae is analyzed, statistics about the computational requirements are provided and score-level fusion techniques are applied to further increase the biometric performance. The pipeline of the proposed pre-processing and the feature extraction algorithm is sketched in Figure 9.1, the comparison strategies are shown in Figure 9.2. In bold letters the newly introduced parts are highlighted, and the corresponding sections are given in curly brackets.

The structure of the paper is as follows: beginning with the introduction of the vein pattern pre-processing and feature extraction system in Section 9.2, the approach of mapping those features into a fixed-length, translation invariant representation is given in Section 9.3. The following Section 9.4 is showing the feasibility of the approach using simulations over several databases. Details about the databases and the performance evaluation are described there as well. In the last section conclusions and future works are given.

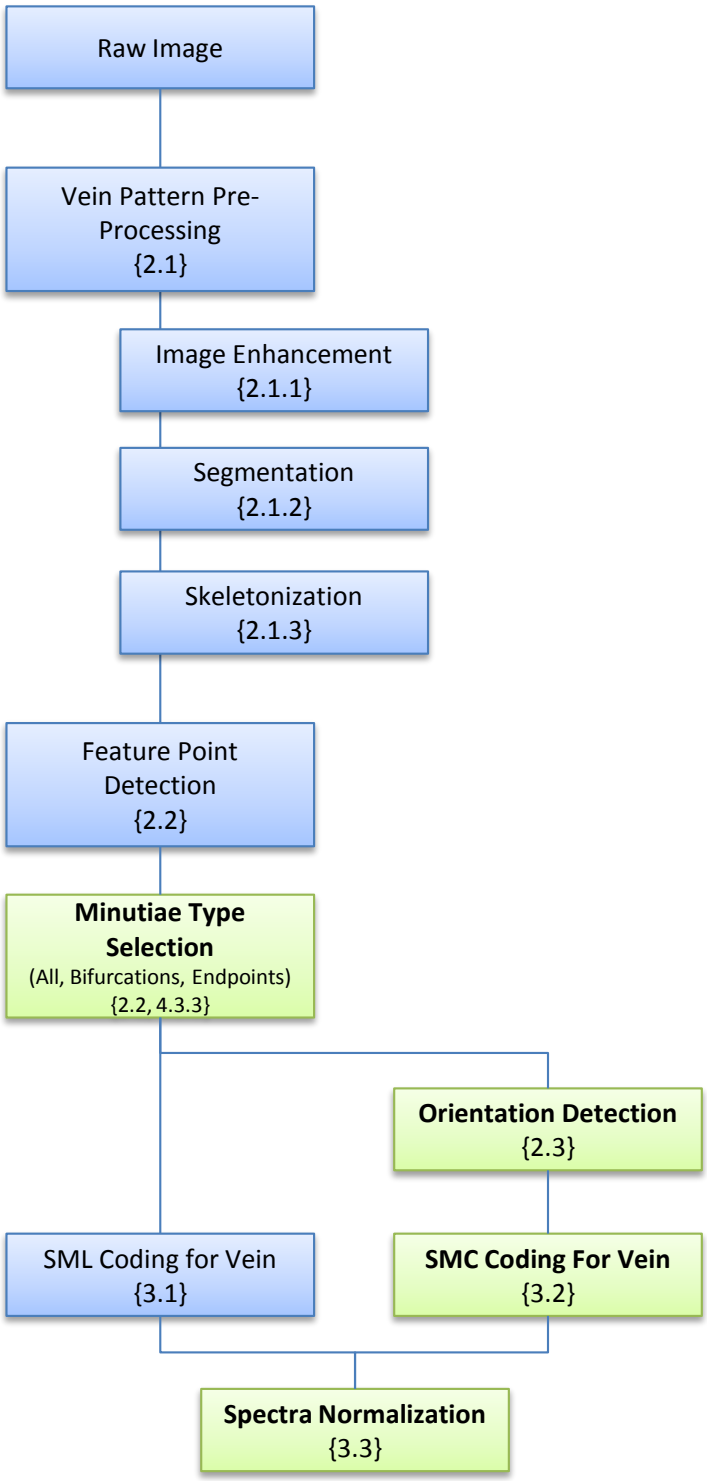


Figure 9.1: Overview biometric pipeline. Bold: newly proposed algorithms with regard to [77]. Corresponding sections given in curly brackets [refers to in-chapter numbering].

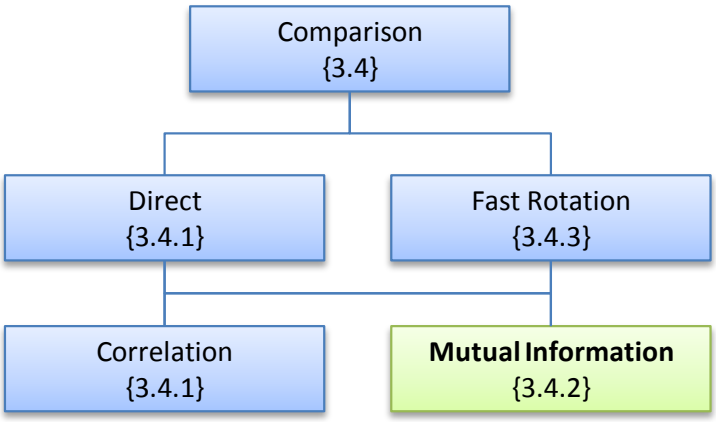


Figure 9.2: Overview spectral comparison strategies. Bold: newly proposed algorithms with regard to [77]. Corresponding sections given in curly brackets [refers to in-chapter numbering].

9.2 Proposed Biometric Vascular Pattern Recognition System

The biometric system based on vein data is introduced in this section. One challenge in vein recognition systems is to cope with noise and low contrast in the captured images. Vein image quality is subject to several factors such as ambient light, air temperature, skin color and varying thicknesses of the skin layers and the limbs. As a result of all these factors sensors usually deliver images suffering from an unfavorable signal-to-noise ratio, low contrast and non-uniform brightness. The vein recognition system has to cope with global and local contrast changes in the image, while suppressing noise. Therefore sophisticated image processing is indispensable in order to improve the images.

Unlike in fingerprint, it is not possible to extract or estimate an orientation field based on the veins. The veins are sparse compared to the fingerprint ridges and their orientations do not seem to be as strongly correlated. The orientational field in fingerprints can be estimated from gray-scale images and can be used to extract minutiae locations and orientations. In vein recognition the enhanced images must be segmented before an image skeleton representing the topological structure of the data subject's veins can be extracted. Minutiae feature points are extracted based on this skeleton and will form the input to the spectral minutiae post-processing which is introduced in Section 9.3.

9.2.1 Vein Pattern Pre-Processing

The proposed solution is not performing a region of interest (ROI) selection to be as generic as possible. Therefore the first step in the pre-processing pipeline is the contrast enhancement.

9.2.1.1 Contrast enhancement

For the proposed system the images are first enhanced by using the adaptive non-local means algorithm which was successfully applied to face recognition in [212], followed by the noise suppressing and edge enhancing non-linear diffusion algorithm [250]. At this point the image is inverted such that veins now appear as high-intensity pixels, whereas the tissue between the veins appear as low intensity. The results of the algorithm applied to raw wrist and dorsal palm vein images can be seen in Figures 9.3(b), 9.4(b) and 9.5(b).

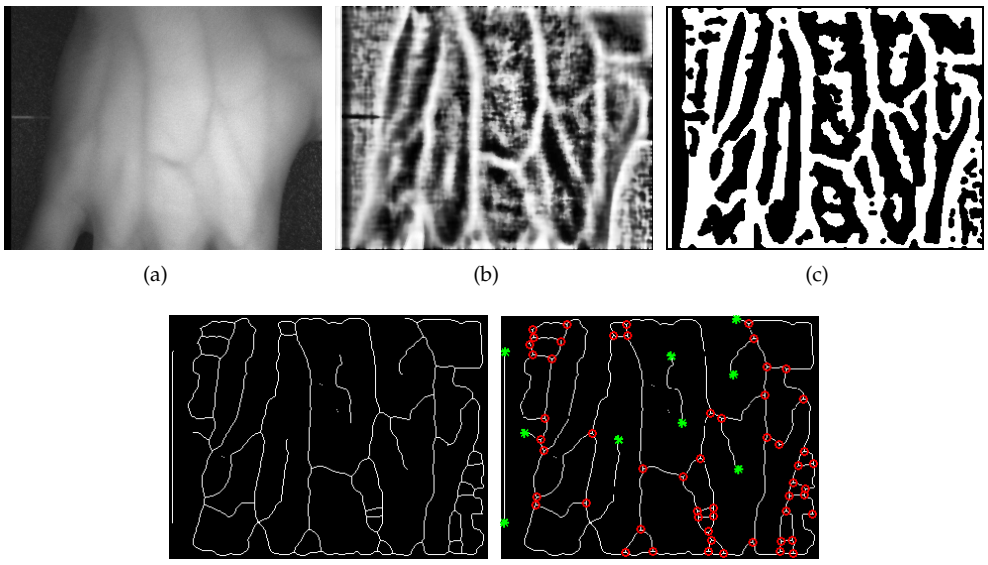


Figure 9.3: Sample dorsal hand vein (SNIR) after different stages of the pre-processing pipeline of the proposed system: (a) raw, cropped vein image; (b) contrast enhanced image; (c) segmentation of an optimized vein pattern image; (d) skeletonization of segmented image; (e) overlay of extracted minutiae points and skeleton. Red circles: endpoints, blue stars: branch points

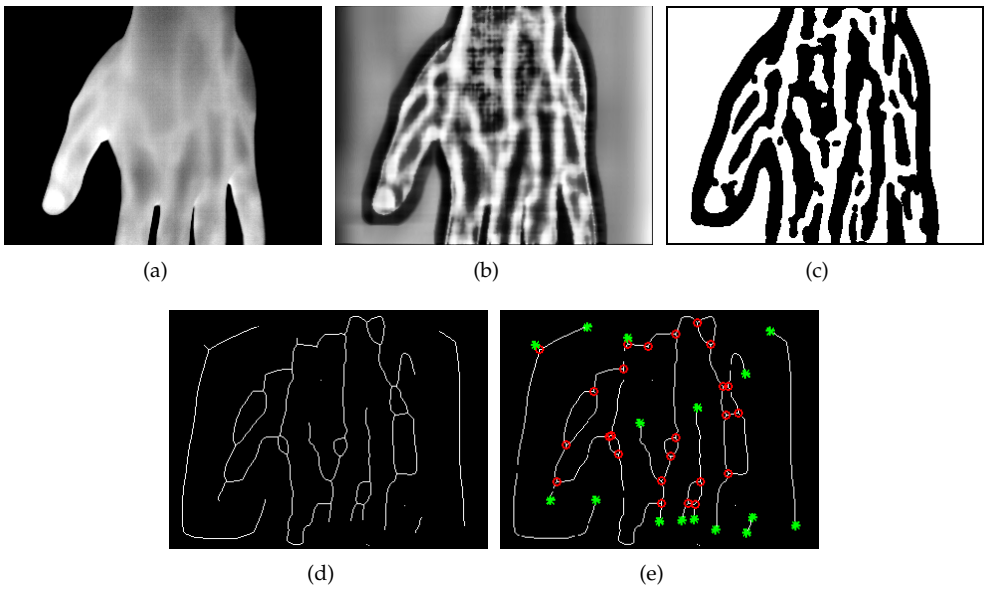


Figure 9.4: Sample far-infrared dorsal hand vein image (SFIR-GT) [171], (a) raw, cropped vein image; (b) contrast enhanced image; (c) segmentation of an optimized vein pattern image; (d) skeletonization of segmented image; (e) overlay of extracted minutiae points and skeleton. Red circles: endpoints, blue stars: branch points

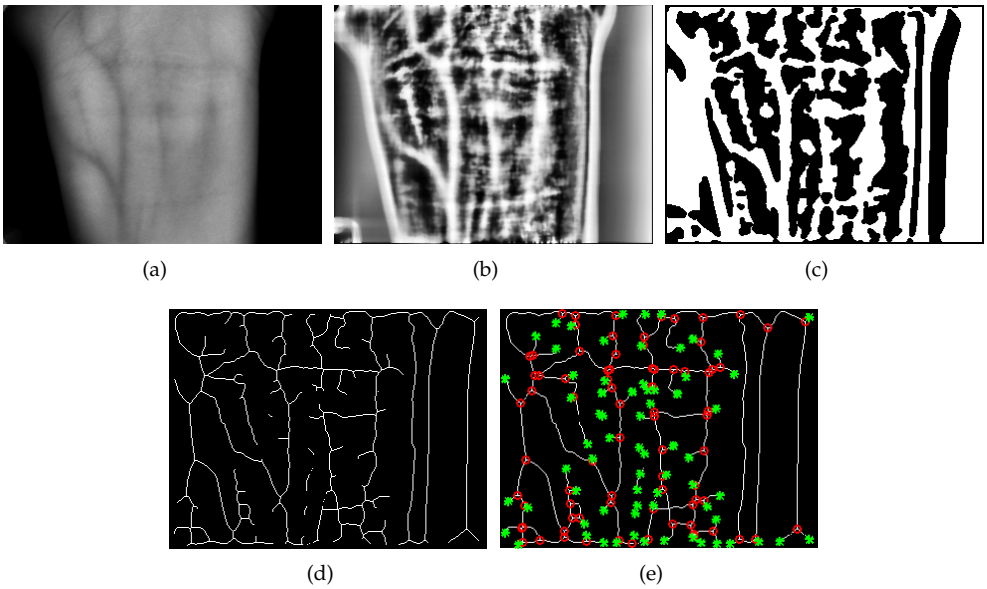


Figure 9.5: Sample wrist vein image (UC3M) [171], (a) raw, cropped vein image; (b) contrast enhanced image; (c) segmentation of an optimized vein pattern image; (d) skeletonization of segmented image; (e) overlay of extracted minutiae points and skeleton. Red circles: endpoints, blue stars: branch points

9.2.1.2 Segmentation

The multi-scale filter method by Frangi *et al.* [58], designed for simultaneous noise and background suppression in medical imaging of vessels, is used as a segmentation method on the vein images. The method searches for tubular structures in the image by analyzing the second-order information (Hessian). The second-order derivative of a Gaussian kernel generates a probe kernel that can measure contrast inside a defined range in the direction of the derivative. An eigenvalue analysis of the Hessian gives the direction of smallest curvature and thus the direction of the vessel, the eigenvalues can be used to classify pixels as vessel or background. Figures 9.3(c), 9.4(c) and 9.5(c) show the effect of the method applied to the contrast enhanced images.

9.2.1.3 Skeletonization

Skeletons are extracted by the fast marching skeletonization algorithm [220]. One advantage of this method is the built-in pruning method, which allows cutting off certain branches from the image skeleton. In fast marching skeletonization, incremental indices are assigned to each pixel on the edge of the figure. Then they are collapsed until only the center line remains. From the difference between two neighboring indices, it can be concluded, how close a skeleton branch is to the center of the figure. The difference between indices at fine-grained branches at the edge of the image skeleton is small, whereas it is large in the center part. These fine-grained branches are most likely artifacts, which were introduced by segmentation errors or noise and can be removed by applying a threshold. The skeleton points where the difference between their indices falls below the threshold are deleted. All other points are kept. Hence, depending on the threshold, more or less of these remote branches are cut off. Examples are shown in Figures 9.3(d), 9.4(d) and 9.5(d).

9.2.2 Feature Point Detection

After extracting the skeletal representation from a vein image, the specific feature points have to be extracted. An efficient and reliable method is proposed in [166]. It is based on convoluting the binary image with a filter consisting of unique power of two values to get unique filter responses for every pattern in the mask size. The end as well as the branch points of the vascular skeleton can be found by searching for their pre-computed filter response values in the filter response of the image. The extracted minutiae points are overlayed with the corresponding skeletons in Figures 9.3(e), 9.4(e) and 9.5(e).

9.2.3 Orientation Detection

The same approach for extraction the minutiae location can be also used to extract the orientations. We propose a fast and reliable method to detect the orientation of minutiae points in an eight-connected binary image within a 3x3 pixel window size based on [166]. Therefore the mask of the convolution approach has to be adapted as shown in Figure 9.6.

The geometrical interpretation of the approach is straightforward for the endpoints: the orientation is defined as the absolute angle (towards an upwards defined zero angle) facing the direction of the skeletonized vein (Figure 9.7). In case of bifurcation or trifurcation points the orientation is defined as the sum of all absolute angles facing the existing veins within modulo 360. It should be noted that neighboring bifurcation patterns (as shown in Figure 9.8), are assigned the maximum distance of 180, which is reasonable since the pairs are geometrically inverse, mirrored on one axis through the center of the mask. The two cases of trifurcation points (the last two patterns) are also distinguished using the mask from Figure 9.6.

After applying the mask to the binarized image, the orientations can be extracted at the positions identified with the algorithm described in Section 9.2.2.

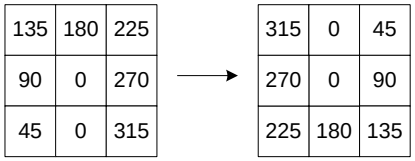


Figure 9.6: Filter mask used for orientation detection. Left side: kernel, right side: as applied on binary image.

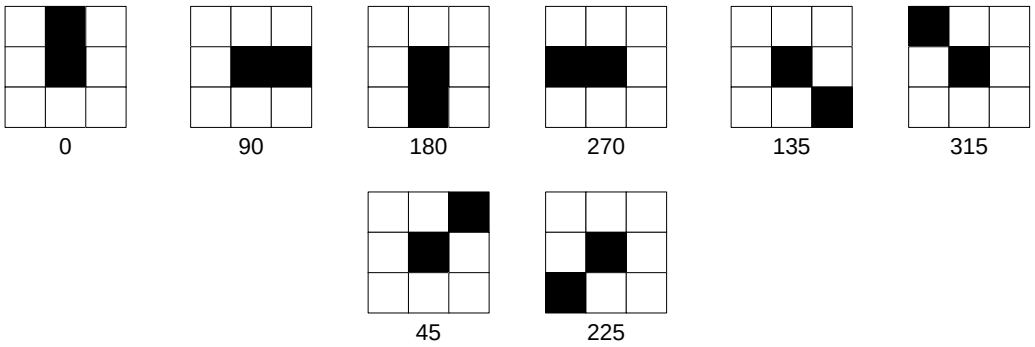


Figure 9.7: Endpoint patterns and their corresponding filter response.

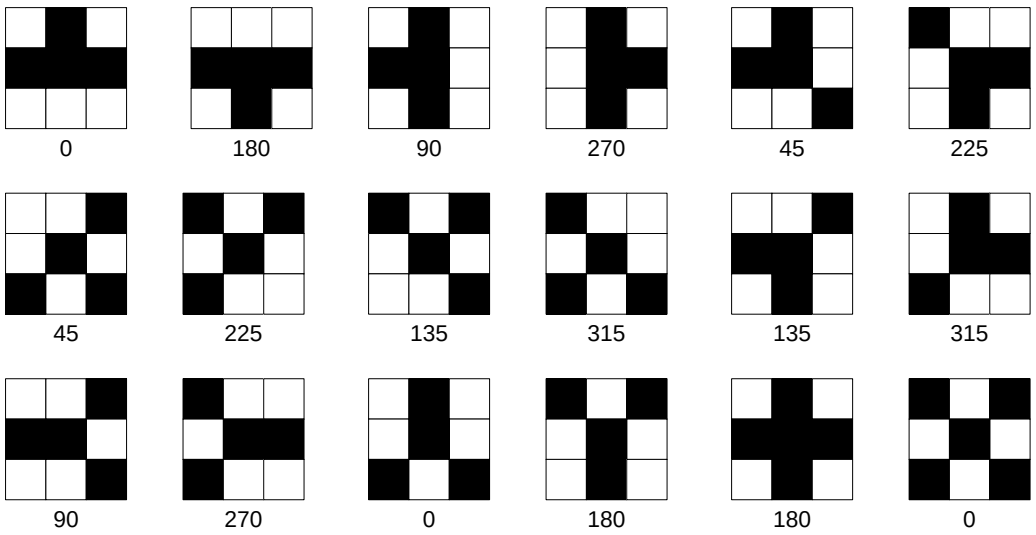


Figure 9.8: Bifurcation patterns and their corresponding filter response.

9.3 Spectral Minutiae

The *spectral minutiae* representation is a method to represent a fingerprint minutiae set as a fixed-length feature vector, which is invariant to translation, rotation and scaling. This approach enables the combination of minutiae-based recognition systems with template protection schemes based on the HDS and allow for fast minutiae-based comparison as well. Considering the similar characteristics of vein and fingerprint minutiae patterns, we applied this method to the extracted vein minutiae.

In the following sections, we introduce two spectral minutiae representations to encode the vein minutiae; the first one is solely based on the location of the points and the second one incorporates in addition their orientation. The location-based spectral minutiae (SML) representation approach was presented in [260, 264], and the complex spectral minutiae (SMC) representation in [263].

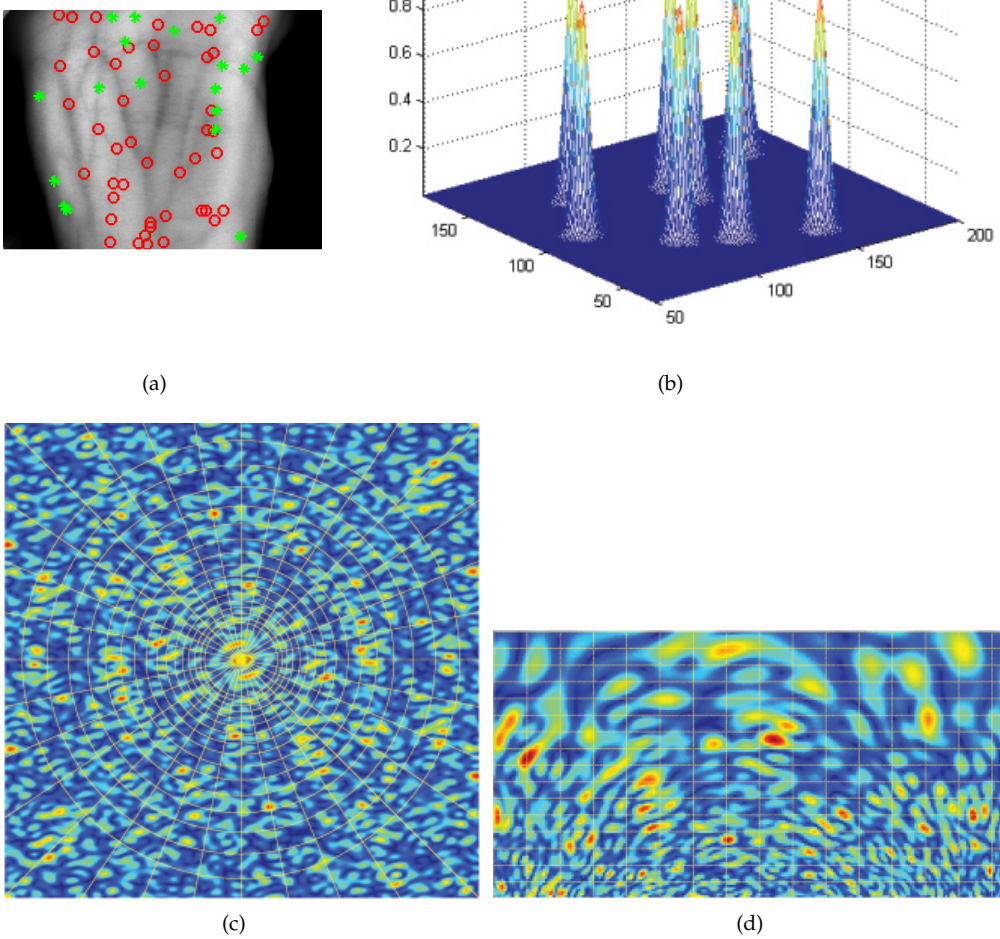
9.3.1 SML Approach

Assume that we have a fingerprint or vein pattern with Z minutiae. In SML, we code the minutiae locations by indicator functions

$$m(x, y; \sigma_{\mathrm{L}}^2) = \sum_{i=1}^{Z} \frac{1}{2\pi\sigma_{\mathrm{L}}^2} \exp(-\frac{(x - x_i)^2 + (y - y_i)^2}{2\sigma_{\mathrm{L}}^2}), \tag{9.1}$$

with (x_i, y_i) the location of the i-th minutiae in the image. Thus, in the spatial domain, each minutiae is represented by an isotropic two-dimensional (2D) Gaussian function with variance σ^2, illustrated in Figure 9.9(b). In this way, the signal is more robust to small variations of the minutiae locations.

Taking the Fourier transform of $m(x, y; \sigma_{\mathrm{L}}^2)$ and keeping only the magnitude of the Fourier spectrum (in order to make the spectrum invariant to translation of the input), we obtain the SML representation



(a) (b)

(c) (d)

Figure 9.9: Illustration of the SML representation procedure. (a) vein pattern and its minutiae points; (b) representing minutiae points as isotropic two-dimensional Gaussian functions. (c) the Fourier spectrum in a Cartesian coordinate and a polar-logarithmic sampling grid. (d) the Fourier spectrum sampled on a polar-logarithmic grid.

$$\mathcal{M}_{\mathrm{L}}(\omega_{\mathrm{x}}, \omega_{\mathrm{y}}; \sigma_{\mathrm{L}}^2) = \left| \exp\left(-\frac{\omega_{\mathrm{x}}^2 + \omega_{\mathrm{y}}^2}{2\sigma_{\mathrm{L}}^{-2}} \right) \sum_{i=1}^{Z} \exp(-\mathrm{j}(\omega_{\mathrm{x}} x_i + \omega_{\mathrm{y}} y_i)) \right|. \tag{9.2}$$

In order to obtain the final spectral representations, the continuous spectra SML (9.2) need to be sampled on a polar-logarithmic grid. A polar mapping transforms rotation to translation in the horizontal direction, whereas a logarithmic mapping transforms scaling to translation in the vertical direction. In the radial direction λ, we use $M = 128$ samples between λ_{l} and λ_{h}. In the angular direction β, we use $N = 256$ samples uniformly distributed between $\beta = 0$ and $\beta = \pi$. A polar-logarithmic sampling process is illustrated in Figure 9.9(c) and Figure 9.9(d).[2]

9.3.2 SMC Approach

As an additional feature specific to minutiae points besides their location, the orientation of the veins in those points can be measured and used. As shown in [263] there are different ways of incorporating the orientation θ into the spectral minutiae. We will focus on the SMC approach that yielded better performance on fingerprint data compared other approaches.

In SMC the minutiae information is encoded as a 2D Gaussian in the spatial domain as in the SML approach. Additionally, each Gaussian is assigned a complex amplitude based on the orientation of the original minutiae shifting the phase in the frequency domain. The complex spectral minutiae representation is defined as the magnitude of the Fourier spectrum

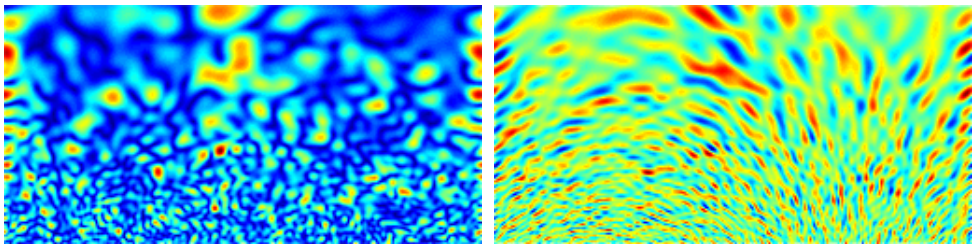
$$\mathcal{M}_{\mathrm{C}}(\omega_{\mathrm{x}}, \omega_{\mathrm{y}}; \sigma_{\mathrm{C}}^2) = \left| \exp\left(-\frac{\omega_{\mathrm{x}}^2 + \omega_{\mathrm{y}}^2}{2\sigma_{\mathrm{C}}^{-2}} \right) \sum_{i=1}^{Z} \exp(-\mathrm{j}(\omega_{\mathrm{x}} x_i + \omega_{\mathrm{y}} y_i) + \mathrm{j}\theta_i) \right|. \tag{9.3}$$

The mapping into the polar-logarithmic sampling grid is done as in the case of SML, the difference being that the parameters for the angular direction are chosen between $\beta = 0$ and $\beta = 2\pi$, since the SMC is not symmetrical.

9.3.3 Normalization of Spectra

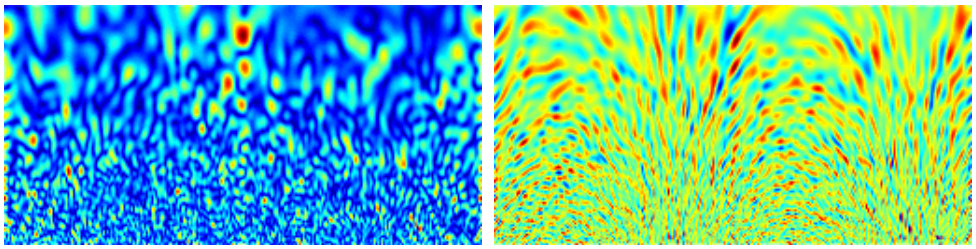
As described in (9.2) and (9.3), we want to keep the magnitude of the spectrum. We used two approaches that return for each imaginary element $z = a + bj$ of the spectrum (a) the complex modulus as $\sqrt{(a^2 + b^2)}$ or (b) the real-valued part a of the spectrum.

[2] The selection of the parameters is based on recommendation for fingerprint [264]: the fingerprint sensors that were utilized for the acquisition of the databases featured a 500 dpi optical resolution which resulted in an image resolution of around 256×400 (MCYT fingerprint) or 296×560 (FVC2002-DB2). From those images in average 20-70 minutiae could be extracted and were utilized for the SM parameter optimization. Since the resolution does not significantly differ from the ones of the vein databases (Table 9.1) and the amount of detected minutiae is in a similar range (Table 9.5) the parameters are deployed in the proposed vascular pattern pipeline. However, the selection is likely to be non-optimal. In case of the UC3M data the generic selection of the parameters seems to have a negative effect on the performance, this could be due to the larger amount of detected minutiae. In line with the experience from SM for fingerprints, a manual optimization did reveal that M, N does not influence the biometric performance significantly. In Section 3.2.1 SM parameters are optimized for a palm vein database indicating the influence of the λ_{l} parameter on the performance. The optimization further revealed that the pre-processing and in particular the segmentation introduced here can be further improved and has a stronger influence on the performance than the SM parameters. This has to be considered as future work at least for the UC3M data as this may reduce the amount of falsely detected minutiae.



(a) (b)

Figure 9.10: Sample SML spectra as described in 9.3.3. (a) complex modulus; (b) real-valued spectrum.



(a) (b)

Figure 9.11: Sample SMC spectra as described in 9.3.3. (a) complex modulus; (b) real-valued spectrum.

Two resulting spectra are shown in Figure 9.10 for SML and SMC in Figure 9.11. The performance evaluation of approach (a) is reflected in Table 9.2 and yields higher error rates compared to approach (b), which is then used further on throughout the paper.

It has to be stated although that approach (a) results in a translation and rotation invariant representation in contrast to method (b). Depending on the dataset and the layout of the system approach (a) could be more appropriate.

9.3.4 Comparison Subsystem

Different comparison strategies are considered, the direct and the fast rotation shift search. Both can be utilized with a correlation or mutual information approach. They are described in this section.

9.3.4.1 Direct Comparison

Let $R(m,n)$ and $T(m,n)$ be the two sampled minutiae spectra in the polar-logarithmic domain, respectively, achieved from the *reference* sample and *test* sample (probe sample) – originating from a fingerprint or a vein source. Both $R(m,n)$ and $T(m,n)$ are normalized to have zero mean and unit energy and are of fixed length $M \times N$. As a similarity score, the normalized cross-correlation with zero lag of two minutiae spectra was chosen, which is a common similarity measure in image processing. Therefore the SML correlation (SML-C), respectively, SMC correlations (SMC-C) similarity score between R and T is defined as

$$S_{\mathrm{DC}}^{(R,T)} = \frac{1}{MN} \sum_{m=1,n=1}^{M,N} R(m,n)T(m,n). \tag{9.4}$$

9.3.4.2 Mutual Information-based Comparison

The similarity between $R(m,n)$ and $T(m,n)$ can also be measured by mutual information. In contrast with the correlation measure that considers linear relationship, the mutual information from information theory [38] is utilized to quantify the non-linear relationship between the two variables. If we consider two sampled spectra $R(m,n)$ and $T(m,n)$ as vectors as follows: $R(m,n) = (r_1, r_2, ..., r_{MN}), T(m,n) = (t_1, t_2, ..., t_{MN})$, then the SML/SMC mutual information (SML-MI/SMC-MI) as similarity score between them is given as:

$$S_{\mathrm{MI}}^{(R,T)} = \sum_{i=1}^{MN} \sum_{j=1}^{MN} p(r_i, t_j) \log \left(\frac{p(r_i, t_j)}{p(r_i)p(t_j)} \right), \tag{9.5}$$

where $p(r_i, t_j)$ is the joint probability distribution function of R and T; and p_{r_i} and p_{r_i} are the marginal probability distribution functions of R and T respectively.

9.3.4.3 Fast Rotation Shift Searching

Rotations might not only be a problem in fingerprint recognition but as well in vein recognition, depending on the capture device used for the acquisition. The fast rotation shift search algorithm introduced in [260] makes a costly normalization of the minutiae points unnecessary by compensating for rotations by testing several rotated spectra. As we applied the polar-logarithmic transform to the Fourier spectra, rotations become circular shifts in the horizontal direction in our minutiae spectra. We chose to test rotations from $-10\,^\circ$ to $+10\,^\circ$ as starting points, which corresponds to circular shifts from -15 units to +15 units in the polar-logarithmic domain.

Let $T_k(m,n)$ be defined as $T(m,n)$ with a circular shift k in the horizontal direction. For each shift attempt, a new similarity score $S^{(R,T_k)}$ is calculated using (9.4) or (9.5). Finally, the highest score is chosen as the similarity score and the corresponding shift k is recorded as the best shift (i.e. the best rotation).

We applied a fast search for the best shift. This algorithm consists of the following steps:
(1) Five circular shifts ($k = -12, -6, 0, 6, 12$) are applied to $T(m,n)$ and the similarity scores $S^{(R,T_k)}$ are calculated. The maximum value of $S^{(R,T_k)}$ is denoted as S_1 and its corresponding shift k is denoted as k_1;
(2) Two circular shifts ($k = k_1 - 2, k_1 + 2$) are applied to $T(m,n)$, and the similarity scores $S^{(R,T_k)}$ are calculated. The maximum value of $S^{(R,T_k)}$ and S_1 is denoted as S_2, and its corresponding shift k is denoted as k_2;
(3) Two circular shifts ($k = k_2 - 1, k_2 + 1$) are applied to $T(m,n)$, and the similarity scores $S^{(R,T_k)}$ are calculated. The maximum value of $S^{(R,T_k)}$ and S_2 is denoted as S_{final}.

Using this fast rotation shift search algorithm, only nine shift trials need to be tested, instead of 31 shift trials for an exhaustive search. After these steps, the value S_{final} is recorded as the final similarity score between R and T.

The scores can be computed for SML as well as for the SMC approaches, when using the correlation or direct comparison approach we referred to it SML-C-FR and SMC-C-FR, for the mutual information measure, we us SML-MI-FR and SMC-MI-FR respectively.

9.4 Experiments

The simulations are designed to examine the performance – measured in equal error rates (EER) – of different comparison strategies used in vein recognition. Three datasets, which main properties are described in Table 9.1, will give a broad basis for conclusions about the proposed approach of using spectral minutiae as features.

9.4.1 Databases

The first two databases were gathered in 2006 in Singapores Nanyang Technological University and contain a subset of samples that were used in several publications [240, 242]. The two parts contain 732 palm dorsal vein samples in the near-infrared and 173 in the far-infrared spectrum from 122, respectively, 34 data subjects. We refer to them as Singapore NIR (SNIR) and Singapore FIR (SFIR) according to the capturing spectral band.

During the experiments, ground truth errors in the SFIR database were discovered, the naming of some files were erroneous, thus imposter comparisons were considered as genuine and vice versa. These errors were resulting in a limited performance of about 2.37% equal error rate (EER) using the proposed algorithms with normalisation method (b) (Section 9.3.3) and the SMM algorithm. The naming errors have been corrected and the corrected version is referred to as *SFIR-GT*. This version also features inverted images to consider the nature of the far-infrared data.

The third database used for the experiment is referred to as *UC3M* [171]. It was collected in 2010 in the University Carlos III of Madrid. The dataset consists of 348 vein images in the near-infrared spectrum from the wrist areas of 29 data subjects. The dataset was taken under different illumination intensities to optimize the capturing device and does not reflect an operational database.

One limitation of the datasets is that they were captured during only one session, which limits the variability in the signals. In addition, the sizes of the databases limit the significance of the results.

Property	**SNIR**	**SFIR**	**UC3M**
Frequency Band	NIR	FIR	NIR
Modality	Back of Hand (2)	Back of Hand (2)	Wrist (2)
Data Subjects	122	34	29
Sessions	1	1	1
Images per Session	2×3	$2\times \sim 3$	2×6
Images	732	173	348
Genuine Comparisons	732	170	870
Imposter Comparisons	266814	14708	59508
Resolution (px)	$(644 \times 492)^{\perp}$	320×240	$(640 \times 480)^{\perp}$
Depth	8 Bit	8 Bit	8 Bit

Table 9.1: Properties of the biometric vein datasets used in the experimental section. $^{\perp}$Image size reduced by 50% in each spatial dimension for experiments.

9.4.2 Comparison Strategies

Our selection of comparison strategies covers a range of different features types that are used. We distinguish here between minutiae-based approaches and geometrical based ones.

Table 9.3 shows the comparison strategies used in the simulations, from the literature we selected the Hausdorff distance, modified Hausdorff (MHD) [50, 242], and Similarity-based Mix-matching (SMM) [30].

The first category is represented by the Hausdorff as well as the MHD algorithms that use the location of the minutiae points directly. The SML algorithm is based on the spectral minutiae representation of the minutiae location, the SMC approach in addition on the orientation. Both are introduced in Section 9.3, for their comparison different approaches are introduced in detail in Section 9.3.4. A correlation (-C) or mutual information (-MI) in combination with the fast rotation (-FR) strategy is used.

Formally the Hausdorff distance between two sets of numbers $A = \{a_1, a_2, ..., a_n\}$ and $B = \{b_1, b_2, ..., b_m\}$ is defined as

$$S_{\mathrm{H}}(A, B) = \max \left\{ \max_{a \in A} \min_{b \in B} ||b - a||, \max_{b \in B} \min_{a \in A} ||a - b|| \right\} \tag{9.6}$$

Where $||b - a||$ is the Euclidean distance between the points a and b.

The MHD is more resilient to outliers and defined as

$$S_{\mathrm{MHD}}(A, B) = \frac{1}{|A|} \sum_{a_i \in A} \min_{b_j \in B} ||a_i - b_j|| \tag{9.7}$$

Were $|A|$ is the number of elements in A.

The Similarity-based Mix-matching (SMM) algorithm proposed by Chen et al*et al.* [30] uses geometrical properties of image skeletons and segmented images to overcome problems with affine transformations. It compensates small translation and rotation errors by comparing the segmented version of the reference sample with the image skeleton of the test sample. The computational effort is higher than the feature point-based approaches.

9.4.3 Performance Evaluation

The evaluation is based on three databases using the EER as main metric. The proposed system of pre-processing and feature point detection and orientation estimation from Section 9.2 is used. During the skeletonization approach using the fast marching algorithm, images from the UC3M database are pruned using a radial threshold of 15, whereas the threshold is set to 75 for the other datasets based on an empirical evaluation of the skeleton variability. All other parameters are generic across the datasets.

Within the simulations the full amount of genuine and imposter comparisons were taken into account for the EER calculations and plots as indicated in Table 9.1.

The biometric performance results are summarized in Table 9.3 giving the EER as well as the error margin with a confidence interval of 90%. Table 9.4 shows the evaluation results of the false non-match rate (FNMR) at a fixed rate of 0.1% false match rate (FMR) and the error margin again at a confidence interval of 90%. The Receiver operating characteristics (ROC) are plotted in Figure 9.12 using a logarithmic scale on the x-axis to increase details in the interesting low false positive region.

All proposed algorithms and the ones from the literature are (re-)implemented in Matlab.

Comparison	SNIR	SFIR	UC3M
Hausdorff	34.65%	25.84%	42.50%
MHD†	1.13%	3.88%	10.61%
SMM$^{\vdash}$	0.27%	2.37%	1.26%
SML-C-a)$^{\diamond}$	1.35%	3.60%	6.13%
SML-C-FR-a)$^{\diamond}$	1.62%	4.33%	5.90%

Table 9.2: Previous results of the evaluation of the proposed SML in comparison to other comparison strategies in equal error rates. †Modified Hausdorff distance as proposed in [50, 242]. $^{\vdash}$Similarity-based Mix-matching [30]. $^{\diamond}$Normalization as described in Section 9.3.3.

Comparison	SNIR	SFIR-GT	UC3M
Hausdorff	34.64% ± 1.08%	21.43% ± 2.88%	42.5% ± 1.09%
MHD†	1.23% ± 0.35%	1.69% ± 0.93%	11.96% ± 1.01%
SMM⊢	0.27% ± 0.17%	0.04% ± 0.02%	1.26% ± 0.35%
SML-C	0.55% ± 0.24%	0.12% ± 0.03%	5.4% ± 0.71%
SML-C-FR	0.41% ± 0.2%	0.15% ± 0.04%	4.48% ± 0.65%
SML-MI	0.82% ± 0.29%	0.06% ± 0.02%	7.35% ± 0.82%
SML-MI-FR	0.55% ± 0.24%	0.09% ± 0.03%	6.45% ± 0.77%
SMC-C	0.68% ± 0.26%	0.54% ± 0.53%	5.17% ± 0.69%
SMC-C-FR	0.55% ± 0.24%	0.57% ± 0.53%	4.37% ± 0.64%
SMC-MI	0.82% ± 0.29%	0.59% ± 0.53%	8.49% ± 0.87%
SMC-MI-FR	0.55% ± 0.24%	0.57% ± 0.53%	8.19% ± 0.86%

Table 9.3: Evaluation of the proposed solution in comparison to other comparison strategies in equal error rates (EER) and the error margin around the EER at a confidence interval of 90%. †Modified Hausdorff distance as proposed in [50, 242]. ⊢Similarity-based Mix-matching [30].

Comparison	SNIR	SFIR-GT	UC3M
Hausdorff	95.77% ± 0.87%	93.45% ± 3.14%	93.45% ± 0.98%
MHD†	3.56% ± 1.13%	7.14% ± 3.27%	23.1% ± 2.35%
SMM⊢	0.27% ± 0.32%	0% ± 0%	1.72% ± 0.73%
SML-C	1.23% ± 0.67%	0.59% ± 0.96%	10.23% ± 1.69%
SML-C-FR	1.09% ± 0.63%	1.18% ± 1.36%	8.05% ± 1.52%
SML-MI	1.64% ± 0.77%	0.59% ± 0.96%	14.14% ± 1.94%
SML-MI-FR	1.37% ± 0.71%	0.59% ± 0.96%	11.95% ± 1.81%
SMC-C	0.96% ± 0.59%	1.18% ± 1.36%	10.69% ± 1.72%
SMC-C-FR	0.82% ± 0.55%	1.18% ± 1.36%	9.31% ± 1.62%
SMC-MI	1.37% ± 0.71%	1.18% ± 1.36%	16.55% ± 2.07%
SMC-MI-FR	0.96% ± 0.59%	1.18% ± 1.36%	15.63% ± 2.03%

Table 9.4: False non-match rate (FNMR) at a fixed rate of 0.1% false match rate (FMR) and the error margin around the FNMR at a confidence interval of 90%. †Modified Hausdorff distance as proposed in [50, 242]. ⊢Similarity-based Mix-matching [30].

9.4.3.1 Minutiae Statistics

In addition to the performance evaluation, statistical information regarding the number of extracted minutiae, as well as the skeletons are summarized in Table 9.5.

9.4.3.2 Computation Statistics

Statistics about the execution time necessary to compute the spectral minutiae and to compare them with the different approaches were collected to give an idea about the general execution-time-wise performance. The test system features an Intel Core i7 processor and 6 GB of RAM, Windows 7 as well as MATLAB are 64 bit versions. The majority of the code is executed within MATLAB, only the MI comparison is based on a C++ implementation from [175], using the MEX system to integrate it into the MATLAB pipeline.

Property	SNIR	SFIR/SFIR-GT	UC3M
Bifurcations	56.93	28.82	87.21
Endpoints	16.42	18.32	62.01
Skeleton length	3146.23	2157.4	3594.62

Table 9.5: Statistics about the average number of end and bifurcation points, as well as the average skeleton length (in pixels) for the different datasets.

The code is not optimized for fast runtime and despite the programming language, the times for generating a spectral minutiae representation from a skeletonized image can be approximated around 250-630 ms depending on the number of minutiae points. It seems there is a linear relation between the number of minutiae Z and the time T for the computation of the spectra, which can be approximated by: $T \approx 225ms + Z \cdot 2.65ms$. The results are summarized in Figures 9.13 and 9.14.

9.4.3.3 Minutiae-Type Sets

It is interesting to investigate how reliable the different types of minutiae can be extracted from the samples. A direct measurement is only possible with a ground truth set of minutiae that is not available, therefore we investigated the algorithm performance by means of EERs.

For the simulations, we distinguished three sets of minutiae types as input for the spectral transformation: (i) using all minutiae points as one concatenated feature vector, not distinguishing between end- or branch points, (2) only endpoints, (3) only bifurcations.

The results are summarized in Tables 9.6 and 9.7, also indicating the confidence interval of 90%. In general the SML performance seems to peak when all of the minutiae types are considered. Only in case of the SNIR dataset the performance difference is significant although. The latter holds true for the trend that bifurcations perform better than endpoints.

Considering all minutiae types in one concatenated feature vector can be seen as feature level fusion. In the next subsection, we compare the results against a score level fusion approach.

The proposed orientation estimation algorithm seems to produce minutiae orientations of reasonable quality. The difference in biometric performance of the SML approach (considering only the location of the minutiae) and the SMC approach (considering also the orientation) regarding the different minutiae type sets is statistically insignificant.

Type	SNIR	SFIR-GT	UC3M
All minutiae	$0.41\% \pm 0.2\%$	$0.15\% \pm 0.04\%$	$4.48\% \pm 0.65\%$
Bifurcation	$0.55\% \pm 0.24\%$	$0.59\% \pm 0.53\%$	$4.14\% \pm 0.62\%$
Endpoints	$1.89\% \pm 0.44\%$	$0.62\% \pm 0.54\%$	$4.82\% \pm 0.67\%$

Table 9.6: Evaluation of the SML-C-FR method for the different minutiae types (in EER $\pm$ 90% confidence interval).

9.4.3.4 Score Level Fusion

Different experiments were designed to investigate the potential performance increase that can be achieved using a normalized score fusion approach with equal weighting. The first two experiments are focused on the combination of comparison scores generated using

Type	SNIR	SFIR-GT	UC3M
All minutiae	0.55% ± 0.24%	0.57% ± 0.53%	4.37% ± 0.64%
Bifurcation	0.68% ± 0.26%	0.62% ± 0.54%	4.83% ± 0.67%
Endpoints	2.73% ± 0.52%	0.59% ± 0.53%	4.95% ± 0.68%

Table 9.7: Evaluation of the SMC-C-FR method for the different minutiae types (in EER ± 90% confidence interval).

Experiment	SNIR	SFIR-GT	UC3M
Exp1	0.55% ± 0.24%	0.45% ± 0.52%	3.11% ± 0.54%
Exp2	0.41% ± 0.2%	0.07% ± 0.03%	3.33% ± 0.56%
Exp3	0.27% ± 0.17%	-	-
Exp4	-	0.03% ± 0.02%	-
Exp5	-	-	1.15% ± 0.33%
Exp6	0.41% ± 0.2%	0.08% ± 0.03%	4.48% ± 0.65%

Table 9.8: Evaluation of score level fusion approaches using different minutiae types and comparison strategies (in EER ± 90% confidence interval). Experiment description in Section 9.4.3.4.

separate spectral minutiae for the different minutiae type sets. The following three simulations focus on combining the two best performing approaches for each dataset. Experiment 6 fuses the location and complex spectral minutiae scores. In more detail:

- Experiment 1: Bifurcation + endpoints using SML-C-FR;
- Experiment 2: All minutiae + bifurcation + endpoints using SML-C-FR;
- Experiment 3: SNIR – all minutiae SML-C-FR + All minutiae SMM;
- Experiment 4: SFIR-GT – all minutiae SML-MI + All minutiae SMM;
- Experiment 5: UC3M – Experiment 1 + all minutiae SMM;
- Experiment 6: All minutiae SML-C + all minutiae SMC-C.

Experiment 1 shows that the different datasets are behaving in completely different ways when comparing the feature fusion level with the score fusion approach: the performance of the SNIR database stays constant, in SFIR-GT the performance of score fusion lowers slightly the EER, whereas the performance of the UC3M dataset strongly improves. In experiment 2, the redundancy of a feature level fused score plus scores of the separate features increases the biometric performance for all datasets. Experiments 3-5 show that the classification performance of the most reliable method, the SMM method, can only slightly be improved in case of the SFIR-GT and the UC3M databases. In experiment 6 a slight performance increase compared to the separate evaluations can be noticed using scores from both the SML and SMC approaches with the simple direct correlation comparison. Since no dedicated comparison strategies can be used in case of a helper data-based template protection system, this results is valuable for the selection of features.

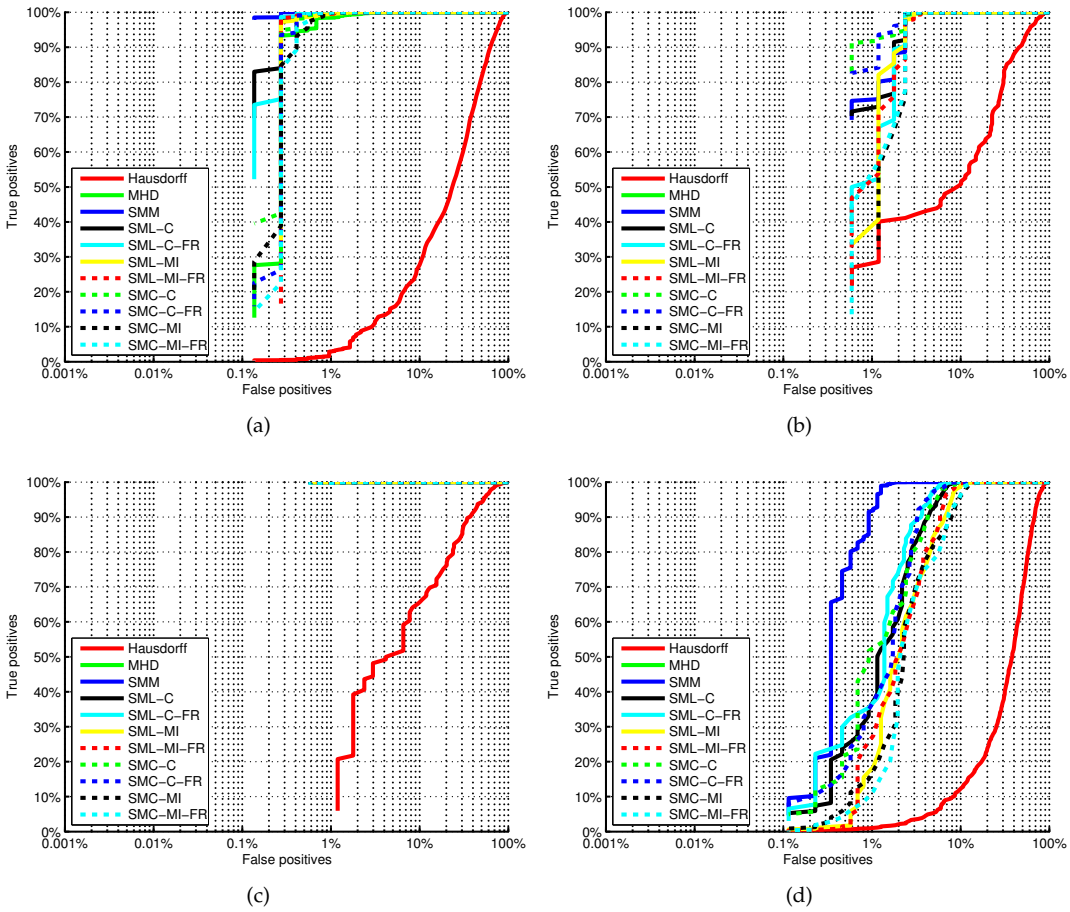


Figure 9.12: Receiver operating characteristics (ROC) from the databases: (a) SNIR, (b) SFIR, (c) SFIR-GT, (d) UC3M.

9.5 Conclusions

The paper has extended the work on spectral minutiae representations for vein [77]. The complex spectral minutiae are introduced which utilize the orientation in addition to the minutiae location; therefore a minutiae orientation extraction algorithm based on a fast convolution approach is proposed. Furthermore, mutual information as a comparison method is investigated with promising biometric performances in case of the SFIR-GT database using the SML method.

Two different approaches for the normalization of the spectra are investigated: the complex magnitude approach and the proposed real-valued method. An evaluation revealed: the latter method performs better in terms of EERs for the selected databases. Since this representation is not translation and rotation invariant the following assumptions can be made: (i) the samples of the datasets are only slightly translated and rotated, and (ii) the real-valued part of the spectra has higher capabilities for classification.

The fast rotation comparison improves the performance compared to the direct correlation measure utilizing the SNIR and the UC3M datasets, although not statistically significant. In SFIR-GT the direct comparison yields in a superior performance, thus it can be assumed that the samples are less rotated.

Statistics about the computation time for the spectra generation and the comparisons are provided, proving its applicability.

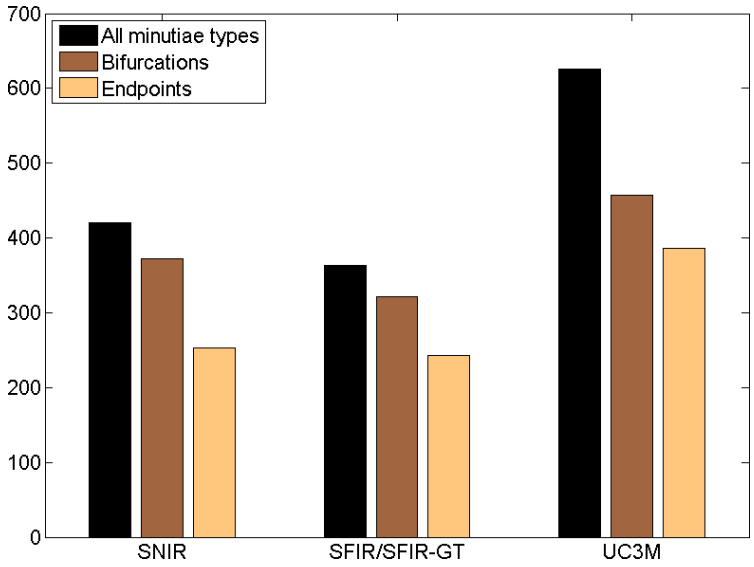


Figure 9.13: Statistics on the average time (in milliseconds) for computing one spectral minutiae representations for the different datasets.

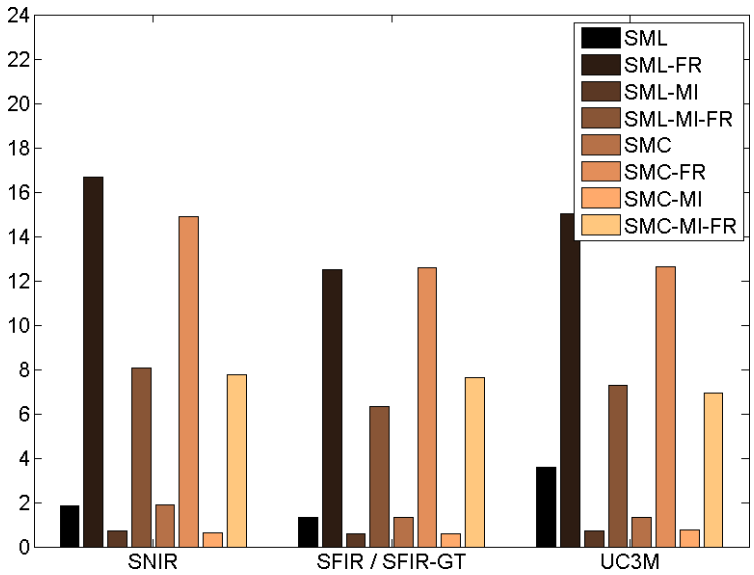


Figure 9.14: Statistics on the average comparison time (in milliseconds) for the location and complex minutiae (SML/SMC) using comparison based on correlation (C), correlation fast rotation (C-FR), the mutual information (MI) as well as MI in combination with the fast rotation (MI-FR) for the different datasets. Details in Section 9.4.3.2.

The reliability is further increased using algorithm fusion. Analyzing the performance of different vein minutiae type sets (bifurcation and endpoints) show diverse results, bifurcations seem to be more stable than endpoints. Fusion at feature level of the two type sets leads to significantly better performance in some cases.

Score level fusion between location and complex spectral minutiae seems to increase recognition performance slightly. Fusing scores from the two best performing algorithms is not improving accuracy significantly.

Summarizing it can be stated, that the proposed solution yields in most cases a significantly improved performance in comparison with other point-to-point-based approaches. In addition, it produces fixed-length and structure feature vectors, that are compatible with state-of-the-art template protection systems. Depending on the normalization of the spectra, a trade-off between an improved biometric performance (outperforming all other presented point-to-point-based approaches) and the property of translation invariance can be made.

Future work focuses on combining the advantages of the normalization approaches – high classification performance and translation invariant representation – into a single one.

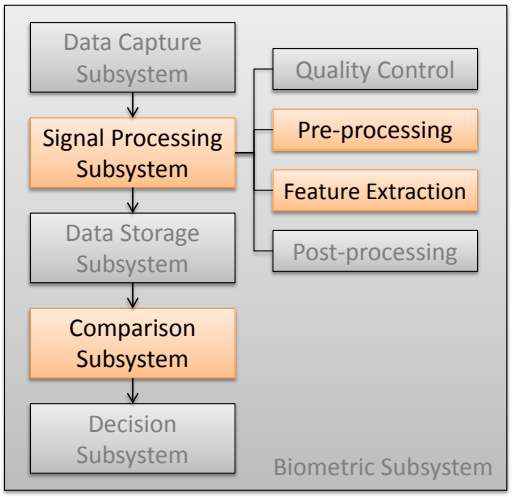
The next step is to combine the proposed approach for vein recognition, where the sensitive information is hidden inside the body, with the HDS – as a privacy enhancing technology – resulting in a secure system fulfilling strict legislative requirements and user expectations regarding privacy.

9.6 Acknowledgments

The authors would like to thank the Nanyang Technological University and University Carlos III of Madrid for making their vein pattern datasets available to the research community.

Chapter 10

Dorsal Finger Texture Recognition: Investigating Fixed-Length SURF



Multimodal biometric systems can help to improve the biometric performance and can at the same time strengthen liveness detection. Here, a biometric pipeline for dorsal finger skin texture information (including finger knuckle information) is proposed based on data from the multimodal database GUC45 introduced in Appendix E. The project instigates how SURF, as a prominent feature descriptor, can be utilized to generate fixed-length features for the fusion with vein data inside the helper data (HDS) template protection scheme.
The paper is accepted for publication in: [75] HARTUNG, D., AND KÜCKELHAHN, J. Dorsal finger texture recognition: Investigating fixed-length surf. In Proceedings of the IEEE International Conference on Systems, Man and Cybernetics, Seoul, Korea, October 14-17, 2012 (2012).

Abstract

We seek to create fixed-length features from dorsal finger skin images extracted by the SURF interest point detector to combine it in the privacy enhancing helper data scheme. The source of the biometric samples is the GUC45 database which features finger vein, fingerprint and dorsal finger skin images for modality fusion. First, the region of interest (ROI) is extracted, after which SURF features are extracted, and finally two different approaches for creating fixed length feature vectors are applied. SURF performance on the ROI is comparable to the PolyU database reported in the literature, namely an equal error rate of 0.74%. Of the two explored approaches for fixed-length features creation, averaging the descriptor components proved the most successful, achieving an equal error rate of 11.72%. Potential run-time performance increases were discovered as a side-effect. Without changing the complexity of the SURF matching scheme, a reduction in run-time of 75%-80% has been achieved, with only minimal precision loss; EER increases from 0.74% to 1%. The complexity of the matching can be reduced from $O(n^2)$ to constant time, but at a higher precision cost and resulting in an EER of 16.51%.

10.1 Multimodal and Privacy Enhancement

Much of the recent work in the field of biometric recognition systems has been focusing on fusing multiple biometric modalities, as this has shown to improve the performance in terms of verification rate. As biometric systems have become more popular and more information is stored about the subjects of systems, privacy issues have become a significant threat. Different approaches have been suggest, which seek minimize the privacy risks, one of which is the helper data system. This particular scheme requires the biometric templates to be of fixed-length.

We seek to create such fixed-length features from the features extracted by the SURF interest point detector and descriptor. Two main approaches will be explored; setting a global limit on the amount of interest points detected, and various methods of averaging the descriptor components themselves. The source of the biometric samples is the GUC45 database which features finger vein, fingerprint and dorsal finger skin images for modality fusion. For this work the focus is on the finger dorsal of the left middle finger. First, the region of interest has to be extracted from these samples, after which SURF features are extracted, and finally two different approaches for creating fixed length feature vectors are applied. Example images for the finger extraction can be found in Figures 10.1 (a-f), details are given in [125].

By fusing two or more of these modalities, it is possible to make the final biometric system more robust. As this work is focusing on modalities from the hand, a fusion system could be based on finger, knuckle and palm prints along with hand veins. If a user were to pass verification, the chance of a false acceptance would be extremely low. This is one of the advantages of relying on more than one modality for user verification. Another advantage of such a system is that faking a users biometric characteristics also becomes more difficult, as each and every modality will have to be captured and reproduced. There are numerous examples of fake finger print replication, mainly because obtaining a latent finger print is relatively easy. But if the attacker also needs to obtain the knuckle print or vein pattern, the task of defeating the biometric system becomes more improbable.

One of the challenges of fusion systems is that a lot of information needs to be kept about the user. If the system were to be compromised, the attacker could obtain much information about the user, and might even be able to use the data to produce fakes. Another attack vector could also be tracking the users behavior by comparing enrolment samples across different biometric systems. If a user's biometric templates is compromised, it is not possible to reissue this template, since the subject cannot change it's biometric characteristics. Privacy enhancement of the biometric templates is an approach to migrate these challenges, and much research has been done in this field. Common for the approaches

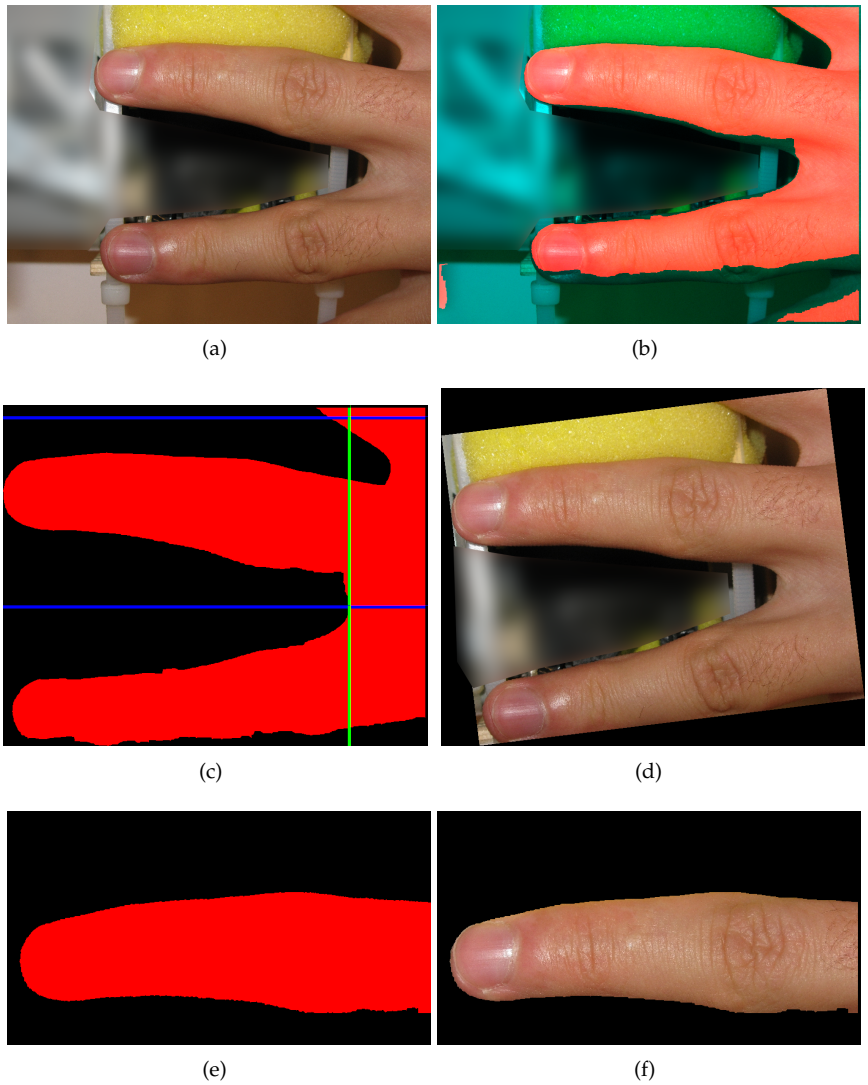


Figure 10.1: Examples for finger extraction, background obfuscated for NDA: finger vein sensor. (a) Original image, (b) Skin detection, (c) Finger root and tip detection, (d) Orientation correction, (e) Extraction mask, (f) Final extracted dorsal finger skin image.

is that either transform the input data or seek to encrypt or hash the templates stored of the subject's biometric characteristics, such that it is not feasible to obtain the user's original template. This helps prevent privacy issues such as identity theft and subject tracking. To solve these issues multiple approaches have been suggested, this work focuses on the helper data system described in [118], which requires a fixed length feature vector.

10.2 State of the Art

Research in finger knuckle prints (FKP) is still fairly new. In 2009 Zhang et al. [280] claim that finger knuckle prints can be used as an biometric trait. The article describes a complete process and setup for a FKP recognition system; capturing a sample, identifying the region of interest and extracting and encoding the features. The system proposed by the authors uses a specially built capturing device, that captures a specific area of the finger dorsal.

This makes multiple sample captures very similar, which almost negates the need for preprocessing, since there is practically no rotation, scale or other dynamic properties between sample captures. This database, the PolyU FKP Database [13], is a very interesting tool for researchers as it allows for a consistent performance measurement of different extraction methods. The following articles use this database to experiment with different approaches to finger knuckle print recognition: [115, 134, 150, 161, 245]. An obvious disadvantage of the described capturing method is that there is not much flexibility in the area that can be analyzed, as the area extracted is very local.

In [128], the authors use a different capturing set-up, where the sample image is also captured in a specially built device, but it allows for flexibility since the device can capture a sample of the whole hand, except for the thumb. This gives better flexibility, but as the authors also note, poor performance can be an issue in the case of too much rotation of the sample.

If not using a specially built device for capturing a local area, methods are needed that can extract regions in the image, from which feature extraction needs to be performed. Different methods are suggested for segmenting the image into the two classes, foreground (the hand/finger) and background (everything else). In [128] a thresholding technique is used which seeks to optimize the measure of separability in the classes. In [139] conversion of RGB color space to HSV color space is suggested along with a *k-means* clustering algorithm. Other methods require complete knowledge of the background before a sample image is captured, such that the difference in these two images can be measured [146]. The authors of [36], have developed a system that seeks to optimize skin detection values (thresholding values) by capturing images in human visible lighting and infra-red lighting. This makes it possible to fairly accurate segment an image into foreground and background.

For actual finger detection the authors of [128] capture a large and consistent portion of the back of the hand, which is used for calculating the finger placements, based on valleys and peaks in the euclidean distance between the middle of the hand-back and the contour of the hand. This is possible because, even though some flexibility in the capture method is possible, there is still a large similarity in the captured sample images. In [139] the fingers are extracted based on knowledge of the placement of the wrist and finger tip and valley localization is done via corner detection.

In [280, 281, 283, 284] the region of interest (ROI) extraction process involves detection of curvatures in the wrinkles of the finger knuckle print. By classifying the wrinkles as either left-ward or right-ward it is possible to detect the center of this region (the middle of the knuckle) as the fixed size area where there is an (almost) equal amount of opposite going wrinkles on either side of the region center line. This is used for defining a coordinate system that has its center in the middle of the knuckle, both vertical and horizontal. In [115] another method is presented that also uses direction to determine the center point of the region of interest, but uses gradient fields instead of edge detection (as in [280]). In [128] the authors present two methods for region of interest detection. The first method uses the finger length only, to determine the placement of the ROI (the ROI is extracted $\frac{1}{3}$ of the way from the finger base to the finger tip). The second method uses edge density to pin point the ROI, since wrinkles will appear as edges in the edge image.

To extract features from the detected ROIs, [280] use *CompCode* (competitive coding). The encoding uses the response values from a bank of Gabor filters, in which the dominating pixel response is used in the final encoding. In [283] this encoding method is improved (*ImCompCode*) by verifying that there actually is a dominating response value. If there is no dominating response value in the responses, the authors claim that the corresponding pixel value is irrelevant, and encoding an orientation value for it, will decrease the precision in the matching process. In [281] the *monogenicCode* is presented, which provides better performance compared to *CompCode*. This approach is based on the Hilbert transform instead of Gabor filtering. Common for the above methods are that the resulting encoding is fixed

length, with a size that is linear in the size of the region of interest.

In [129], Kumar et al. use a similar approach based on Radon transformations to identify knuckle lines and creases; the resulting encoding is named *AjayKumar2009* by the authors. As CompCode, the resulting KnuckleCode is of fixed length and number of dimensions is linear in the size of the region of interest. Both CompCodes and AjayKumar2009 rely on texture information from localized areas.

In [161] the authors use SIFT [142] to extract the ROI features, by detecting interest points in the region of interest and describing the local area around these points. SURF [11], which is another interest point detector and descriptor inspired by SIFT, is used in [134]. Both of these methods' strengths are that they are invariant to image translation, rotation and scaling, since they are not reliant on the geometric locations of the interest points. This feature makes the algorithms suited for feature recognition and extraction in uncontrolled environments. SURF's use of integral images and box-filters makes it more efficient than SIFT, which makes it a good candidate for on-line feature extraction. Furthermore SURF does not detect as many interest points as SIFT, which speeds up the algorithm even more in the interest point matching phase.

10.3 Goals

This work focuses on recognition of biometric samples taken in an environment where scaling, rotation, orientation and amount of sample captured is not fixed. This limits the types of feature extraction methods, since these must be invariant, or at least robust, to such variations in the samples. Feature extraction methods presented in [280] and [129], seem interesting since they produce a fixed length feature, are fast to compute and produce good results, but do not seem applicable under such conditions.

Interest point detectors and descriptors, such as SIFT [142] and SURF [11] are able to detect correlating interest points in different samples, but do not produce a fixed length feature vector. The goal of this work, is to examine the possibility of creating fixed length feature vectors using SURF as a detector and descriptor. The focus will not only be on finger knuckle prints but on the finger dorsal, as the finger dorsal should contain more information. Furthermore, the database used for testing, GUC45 [73], includes samples in which not all of the knuckle is contained, which would exclude such samples from being used. The samples are captured utilizing an out of the shelf consumer camera (Canon Powershot G9). The database features in addition to the finger dorsal skin images also fingerprint and finger vein images from 45 data subjects, making it an interesting set for modality fusion approaches. The final goal is to utilize the different modalities to create secure templates with the helper data scheme.

To evaluate the results obtained, the final method will be applied to the PolyU [13] finger knuckle print database, as many of the papers on finger knuckle print recognition uses this database ([115, 134, 150, 161, 245, 280, 281, 283, 284]).

As seen from Section 10.2 there are many approaches to extract and match finger knuckle prints. The feature extraction techniques suggested by Zhang et al. [280, 281, 283] are interesting in the context of privacy enhancement, since the length of the extracted features can easily be fixed, simply by ensuring that the size of the captured sample is always the same. However, this restricts the capturing environment, as the extracted features are dependent on the scale, orientation, resolution etc. being the same. While these conditions are met in the PolyU database, this is not guaranteed to be true for other capturing techniques, which is the case of GUC45.

Based on the observation that the samples in the GUC45 database range in both scale and orientation, SURF has been selected as the feature extractor. Zhu showed in [134] that SURF can achieve good results when applied to the finger knuckle prints found in the PolyU database. The challenge now becomes to create a fixed length feature vector

based on resulting SURF descriptors. Due space limitations we refer for details of the SURF algorithm to [11].

10.4 Modifications to SURF

The SURF descriptor is a collection of all the interest point descriptors. Since the number of interest points is likely to vary between different samples, the length of the SURF feature vector will also vary. The internal order the interest points in the SURF descriptor is not relevant for SURF matching, since this often involves an exhaustive search for the best matching interest points between two sets. However, in order to apply the helper data scheme (HDS) ordering of the interest points is crucial for achieving usable results. These are the two issues that have to be solved for utilizing SURF in conjunction with HDS.

The information produced by SURF is summarized in the following:

- Location – The (x,y) coordinates of the interest point in the sample image is known
- Orientation – The orientation at which the descriptor has been extracted
- Laplacian – The Laplacian value which indicates the contrast relationship between the blob (detected point of interest) and its background/surroundings.
- Scale – The size of the area around the interest point
- Octave – The octave at which the interest point was detected
- Response – The Fast-Hessian response value
- Descriptor – The description of the area around the interest point; orientation and scale normalized. This is of fixed size and internal ordering of the elements is consistent.

The most naive approach to fix the length of the SURF feature vector, is to set a limit on the amount of interest points that are included in the final collection. This would create a fixed-length feature vector, since the length of a single interest point descriptor is constant. However, a method of ordering the interest points consistently is still needed.

The descriptor for a single SURF interest point contains 64 elements, which are consistently ordered. By averaging each of the elements in the same position of the descriptor across all interest point detected, a feature vector of fixed length and ordered elements can be obtained. This will reduce the SURF feature vector to the size of a single interest point descriptor, but much information will be lost in the process.

In order to reduce the amount of information lost in the above averaging process, more information most be kept. Two methods are examined in this work, both seek to identify groups in a interest point collection, before calculating the average. Then the average is calculated for each group, such that the final feature vector has a length equal to the number of groups (multiplied by the descriptor length).

10.4.1 Fixed number of sorted interest points

In its current form, SURF does not directly implement setting a threshold on the amount of interest points. It is possible to set a response threshold, which limits the amount of interest points by setting a minimum requirement on the response value used in the Fast-Hessian interest point detection step. However, there is no guarantee that the detected amount of points is fixed, as the amount of response values above the threshold may vary.

If the number of interest points are to be limited to a fixed amount, the points that are chosen for this, is of high importance, since these points will have to be the most repeatable, e.g. if the points chosen are not the most distinctive, in terms of the features that are

identified by the Fast-Hessian, interest points from different samples will not be matchable. Another concern is that if a fixed limit is set, the total amount of interest points detected in the sample must at least be the same as the set limit. Therefore this limit will become directly dependent on the Fast-Hessian response value threshold, since a higher threshold produces less points and this amount of points might vary from sample to sample.

In the process of detecting interest points, the Fast-Hessian searches for blob-like objects in the image, and the higher the octave number is, the larger the blob-like object is. If it is assumed, that larger objects are more repeatable (since they are less likely to be the result of noise), it makes sense to chose interest points detected at a high octave level. By setting a fixed amount of interest points to be selected from each octave, favoring the higher levels, a rough ordering of the interest points is possible. Table 10.1 show an example of such a

		Octave number				
	#Ipts	1	2	3	4	5
Original SURF	647	382	200	45	15	5
Limited to 250 Ipts	250	105	80	45	15	5

Table 10.1: Example of interest point based on octave

selection. To order interest points belonging to the same octave either the scale, response value or a combination could be used as in the aforementioned proposed ordering. Such a structure will limit the amount of shifting that is possible, as the ordering will be "reset" at every octave. However, since the number of interest points is fixed for a given octave, it is necessary to introduce "blank" interest points, if there are not enough interest points in an octave. This could potentially introduces errors in the matching phase, decreasing the performance of this approach.

10.4.1.1 Averaging the descriptor

A simple way of obtaining a single descriptor for all interest points detected, is to calculate the averages of all interest points' descriptors. While simple, this might causes loss of detail in the process, but has the advantage that the feature vector is ordered. Three methods of averaging the descriptors are examined.

If the descriptor component is viewed as a vector with 64 elements, the simplest method of averaging all the descriptors, is to create a new vector in which each element is the average of the elements in the same position in the interest point descriptors:

$$v = [\text{avg}(d_{1...n}[1]), \text{avg}(d_{1-n}[2]), ..., \text{avg}(d_{1-n}[64])] \tag{10.1}$$

where d is the collection of descriptors and n is the number of interest points. Though this is simple, a lot of information is lost during this process. The following averaging methods, try to keep more information by grouping the interest points, and then applying this averaging method to each of the groups. For each group a feature vector of 64 elements is created, which reduce the information loss. However, in order for this to be applicable in regards to HDS, it most be possible to consistently order the groups.

10.4.1.2 Binning the descriptors

Some considerations have to be done in regards to the amount of bins and the assignment of a descriptor to a bin. The more bins that are used, the more likely it is for some bins to be empty, which could lead to poor matching results. However, the less bins that are used, the more information will be lost; if only one bin is used, the results will be the same as averaging all the descriptors. The bin assignment criteria also has a major influence on the results, and many different criteria could be used such as:

- Fast-Hessian response value – The Fast-Hessian detects blob-like structures in the image, and the response value indicates the significants of this structure. Grouping by response value could group blobs that have resemble each other texture-wise. This would minimize the amount of information loss during averaging. However, the opposite might also prove true, which would significantly decrease the comparison scores.

- The $dax : day$ ratio – Averaging these ratios would described the overall direction of the sub-regions in the descriptor. If there exists a strong general direction in all the descriptors this approach could prove successful, since the binning would be very distinct. However, if the identified directions in sub-regions of a descriptor are very different, i.e. like a circle, many descriptors that overall do not resemble each other could be grouped, which would lead to information loss.

- The average mdx or mdy only – Binning based on these values could minimize some of the disadvantages mentioned about, but new ones arise as the value used might not be the dominant of the two.

In the above dax, day, mdx, mdy refer to elements in a SURF interest point descriptor. More information about this can be found in [53].

Each of these binning criteria focus on different features of the descriptor, but it has to be recognized that the descriptors are meant to be as unique and distinctive as possible, such that interest points across different images can be compared.

10.4.1.3 Clustering

Another method of dividing the interest points into groups is to use a clustering algorithm. The clustering can be done in various feature spaces, such as those previously described, but clustering based on interest point locations, gives the best results on the GUC45 dataset.

10.5 Results

10.5.1 Averaging the descriptor

As the descriptors already are represented as an ordered fixed length structure, it might be possible to condense all the descriptors into a single vector by averaging all the descriptors created for a sample image. Table 10.2 shows the results of creating such a single feature vector. As the table shows, the best results in terms of equal error rate is achieved by averaging all the interest points' descriptors, by which an equal error rate of **20.82%** is achieved for the test database. It is interesting to note, that while some distinctiveness is lost during the averaging, enough information is kept to partially match samples from the same subject.

	Number of interest points						
Method	all	300	200	100	50	25	10
Octave (desc)	20.8	23.2	23.8	30.3	34.5	33.6	42.4
Response (desc)	20.8	22.2	21.3	18.1	23.9	28.4	32.5
Scale	20.8	24.1	28.2	31.7	37.7	43.2	44.1
Octave, response	20.8	23.5	23.9	25.9	26.1	31.3	37.9
OSR	20.8	23.1	22.7	24.9	34.3	35.6	36.6

Table 10.2: EERs (%) for average descriptor.

10.5.2 Binning

If more information were to be kept, it might be possible to improve the results. One way of attempting to keep more information, is to create a fixed number of bins which contain averages of the descriptors assigned to them. Table 10.3 shows the results of several binning methods: using information from the descriptors prove much more reliable compared to features of the interest point (octave, response etc.), and that binning by such features produce better results than just averaging the descriptors. This is likely due to the fact that more information is kept, but as the results also show, the EER declines when too many bins are used.

	Number of bins			
	2	3	4	5
Octave	33.59	44.57	37.24	35.88
Response	38.48	42.37	44.96	41.64
Scale	40.85	45.64	46.17	43.14
Octave, response	40.55	42.54	40.23	39.31
OSR	41.78	42.39	44.28	46.71
Ratios				
$mdx : mdy$	20.43	18.93	18.56	22.81
$dx : dy$	49.99	49.82	46.72	50.00
$dx : mdx$	24.45	23.95	22.04	24.12
$dy : mdy$	34.37	29.35	27.91	33.09
Averages				
mdx	15.98	17.57	18.47	21.25
mdy	20.66	22.70	24.44	25.63
dx	34.21	27.00	31.80	32.17
dy	31.64	25.77	25.79	28.75
descriptor	26.54	28.57	30.65	33.14

Table 10.3: EERs (%) from different binning methods.

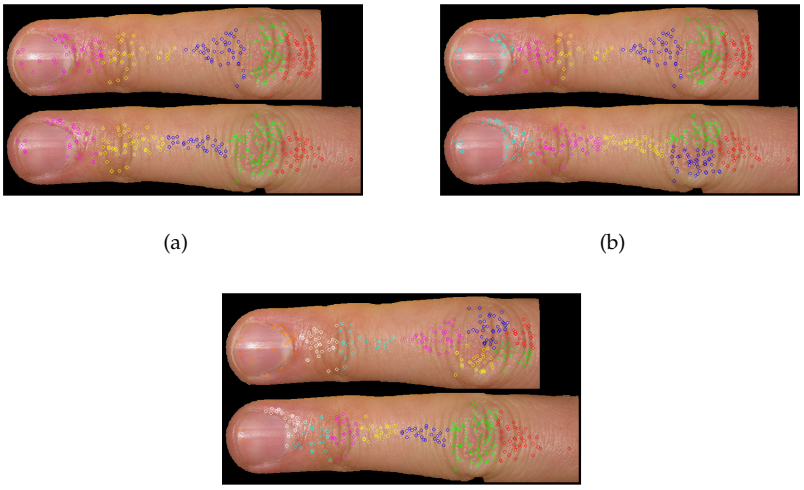
10.5.3 Clustering

Finding clusters is another way of dividing the interest points/descriptors into smaller groups. This method is interesting because it allows for the use of the interest points coordinates, since the location of the coordinates are not of interest, but only the relationship between them. However, there are some issues with using clusters, such as ordering the clusters and identifying the same clusters. As seen, the results of creating 2 clusters resemble those of binning. However, as the figures above show, clustering has the disadvantage of not creating robust clusters, which makes the matching phase error prone. Thus, when creating more than two clusters, it is important to 1) find a robust method of clustering and 2) a method of ordering the clusters. The clustering method used in this work is *k-means* which is a much used clustering approach. Different methods of ordering the clusters has been attempted, such as size of the cluster, average response value for interest points in a cluster etc, but none order the clusters robustly enough. An option in the case where clustering is done in the geometric space, is to order the clusters according to the location of the center. While this maintains scale invariance, it is not robust to orientation changes, as there would not be any fixed starting point. Table 10.4 shows the results of ordering clusters found in the geometric space by the location of their center point, which gives an indication of a best case scenario where orientation invariance is not a requirement. It can be seen that ordering by geometric location does provide a more stable ordering even with a high number of clusters, but at the cost of removing orientation invariance. Using the

center of the cluster as an ordering criteria makes it possible to utilize more clusters while still maintaining a low EER. It is possible to use up to 5 clusters, while maintaining an EER of approx. 20% or less, and the best results were obtained when partitioning the points into 4 clusters with an average EER of 17.37%.

	Number of clusters					
	2	3	4	5	6	8
Average	17.58	17.49	17.37	20.50	31.42	36.90
Standard deviation	0.71	0.44	0.97	0.77	1.31	2.40

Table 10.4: EERs (%) obtained by clustering by (x, y), ordered by location of the cluster centers



(a) (b)

(c)

Figure 10.2: Clustering SURF interest points. Interest points marked with the same color belong to the same cluster. Number of clusters: (a) 5, (b) 6, (c) 8

Figure 10.2 depicts the issues that arise, when creating more than five clusters. As shown in 10.2(b) and 10.2(c), the interest points have not been clustered similarly in the samples with the same amount of clusters.

From the visualizations of the clusters, it is clear that ordering by the clusters' center location works, because the finger dorsal is used, and not only the knuckle area. Clusters are therefore typically spread out along the finger, such that the clusters divide the finger into sections. If only the knuckle area were to be used (as in the PolyU database), it is likely that the ordering suggested would not achieve the same results, as the area where interest points are to be detected is more quadratic.

10.5.4 Fusion

By fusing the three comparison methods based on binning, clustering and averaging all, better performance might be obtained. The fusion is done by calculating the scores for each method, after which a weighted sum of the 3 scores is used as the final fused score. The weights that are assigned to each of the scores has a significant impact on the final results, and to determine the most robust and optimal weighting, exhaustive search is used.

To determine the actual EER for a fusion based system with the above parameters, the average EER over ten runs is calculated with an average EER of 11.77% (weighting

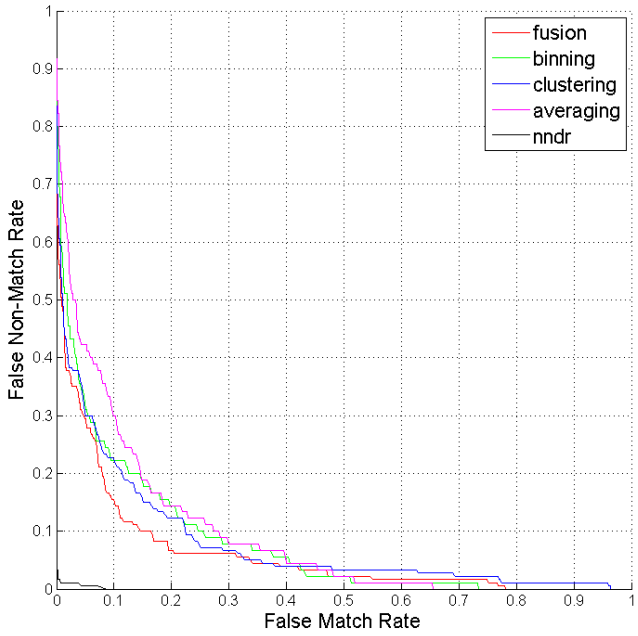


Figure 10.3: DET plot of GUC45 results

43%,56%,1% for binning, clustering and averaging). Results are summarized in Figure 10.3.

10.5.5 Results on the PolyU database

For comparison reasons the averaging methods, averaging all, clustering, binning and fusion have been applied to subset of the PolyU database. The subset has been created by randomly selecting 3 ROI samples (left index finger) from 30 subjects (subjects 1-30). The list shows the EERs obtained by extracting the U-SURF-128 descriptors and using different matching schemes:

- NNDR – 1.10%
- Averaging All – 24.12%
- Binning (4 bins) – 26.42%
- Clustering (3 clusters) – 28.88%
- Fusion (3 bins, 2 clusters) – 19.47%

When using the NNDR and averaging all matching schemes, the EERs are similar to those obtained from the GUC45 database. However, binning and clustering provide better results on the GUC45 dataset. A likely explanation for this deviance is that the number interest points detected in the PolyU database is much lower than the amount detected in the GUC45 samples (approx 100 vs 500 detected interest points), which means that individual descriptors have a much higher influence on the average values created in the bins and clusters. Furthermore, detecting clusters by interest point location is more prone to errors when ordering by the x-coordinate value, when more than 2 clusters are used, because of the height:width ratio of the PolyU ROI image samples. Fusing the 3 methods, still provides better results compared to the results of the individual matching schemes.

PolyU database [13]	
CompCode [280]	1.09
MonogenicCode [281]	1.72
SURF [9]	0.83
SIFT [161]	2.02
Enh-FUSE [9]	0.22
OE-SIFT [161]	0.85
LFI [282]	1.27
LGIC [284]	0.40
$LGIC_2$ [282]	0.36
Fixed-length SURF	19.47

IIT Delhi Database [129]	
AjayKumar2009 [129]	1.08

GUC45 [73]	
SURF	0.74
Fixed-length SURF	11.77

Table 10.5: EERs (%) reported in the literature and *in this work*. Fixed-length SURF refers to the fusion matching method.

.

10.6 Conclusions

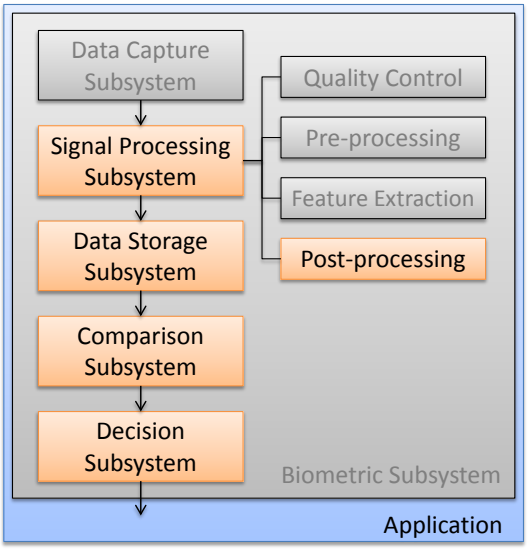
SURF has previously been used in finger knuckle-print recognition systems in [9] an EER of 0.83% on the PolyU dataset was achieved. During this work an EER of 0.74% was achieved on a subset of GUC45 data using the standard SURF matching scheme, suggesting that finger dorsal skin texture recognition using standard consumer cameras is feasible.

Experiments regarding the creation of a fixed-length (FL) feature vectors from SURF descriptors have been conducted. By finding a FL feature vector, it is possible to apply the HDS privacy enhancement to the extracted features. Two main approaches for FL creation have been researched, resulting in an fused equal error rate of 11.77% (Table 10.5). Future work needs to focuse on improving the recognition accuracy.

It has been discovered that it is possible to limit and order the amount interest points, whereby minimal recognition accuracy is measured. This result obtained on the GUC45 database indicates a possible speed-up of the comparison phase for SURF in general. The average amount of interest points detected in GUC45 samples were approx. 650, and it was possible to set a fixed limit of 300 points with minimum impact on the EER. The nearest neighbor distance ratio (NNDR) comparison times could be reduced by between 75% and 80%. The comparison schemes based on averaging the descriptors are able to distinguish individuals, but at a high cost of precision. In the simplest scenario of averaging all the descriptors the matching complexity is reduced from $O(n * m)$ (n and m are the amount of interest points detected in the samples to be compared) to constant time. The loss of precision is rather high, as an EER of 0.74% becomes 16.51%. However the amount of information compression, in terms of vector length, is on average 99.85% (the 650 descriptors are reduced to one).

Chapter 11

Biometric Transaction Authentication Protocol



The chapter extends the focus to the application of biometric systems. The approach that is sketched here, merges protected templates with information from the application to constitute an authentication system for online banking transactions. Such a system could prove to be useful in real life since a strong authentication overcomes repudiation problems for the service provider while offering improved convenience to a customer without introducing privacy issues.

Although designed modality-independent, a biometric vein system based on Chapter 9 with the improvements presented in Chapter 3 could be used.
The paper was published in: [72] HARTUNG, D., AND BUSCH, C. Biometric transaction authentication protocol. In Proceedings of the 2010 Fourth International Conference on Emerging Security Information, Systems and Technologies (Washington, DC, USA, 2010), SECURWARE 10, IEEE Computer Society, pp. 207-215. The ideas are patented in: [21] BUSCH, C., AND HARTUNG, D. (EN) AUTHENTICATED TRANSMISSION OF DATA, June 2011. (WO/2011/063992).

Abstract

The threat of phishing or malicious software (malware)-based attacks is significant and growing, at the same time online banking gets more and more popular. Financial loss may be one of the consequences if credentials get stolen. In many protocols, the transaction information is not secured properly. The proposed *Biometric Transaction Authentication Protocol (BTAP)* is based on the one hand on the helper data scheme for biometric template protection and on the other hand on a trusted biometric transaction device. BTAP provides data- and person authentic transactions since the relevant information in financial online transactions is fused with a secure biometric template from a verified natural person in a way that it is proven to the executing party, that the transaction, as it is received, was in fact initiated and confirmed by an identified natural person.

11.1 Introduction

An identity fraud can be defined as the exploit of an identity theft or more precisely a theft of an identity attribute with the intent to harm the affected person. The goal of an attacker is in most cases financial gain. The risk of being a victim of such an event has increased dramatically over the last years. The Identity Theft Resource Center (IDTRC) recorded recently a yearly increase of 46%. In the first three weeks of 2010 the IDTRC [90] registered 1,255,092 data records that were exposed whithin the reported breaches in the U.S. (where numbers were made available), not considering exposed encrypted data records. The list covers incidents of credit card misuse, bank account theft and banking defraud. Manipulated card readers, phishing attacks as well as sophisticated social engineering attacks were tracked. One of the reasons of increasing incidents is seen in the more and more widespread usage of online banking. According to the Federal Association of German Banks, the number of online bank accounts in Germany has increased from 15 Million in 2000 to 39 Million in 2008. The amount of online transactions is expected to increase even more within Europe with the implementation of the Single Euro Payments Area (SEPA) transaction initiative. A study of the Federal Association for Information Technology, Telecommunications and New Media (BITKOM) states that seven percent of all internet users above 14 years already experienced finicial loss through viruses, in online auctions or in online banking [17]. The vulnerability of knowledge-based finiancial transaction system became again obvious as hundred of thousand credit cards of German bank customers had to be re-issued after a data theft in a Spanish credit card processor in November 2009. Furthermore a year 2009 report from the German Federal Office for Information Security (BSI) claims that the threat from phishing attacks is still small but incidents related to online banking fraud will increase through the improved and technically mature mechanisms of malware [20]. Viruses and Trojan horses are representatives of malware. This kind of software is spread over various channels on private computers and is able to gather information like financial transactions. Without being noticed, this information can be sent to remote machines. The user will experience dramatical loss, if credentials like bank account numbers, passwords and valid transaction numbers will be used by the operator of the remote machine. The responsible software is often not detectable, since elaborate technologies like self-encryption and mutation make it impossible to match the malware against patterns used by anti-virus programs. On the other hand rootkits are used to infiltrate the whole operation system itself – this malware can hardly be detected with todays methods [193].

In consequence, a reliable transaction protocol is needed that securely links 1) Receiver-Account-Number, 2) Ordered Amount, 3) Sender-Account-Number, 4) Initiator and optionally various additional information like transaction number and time stamp in a reliable manner.

The paper is organized as follows: after introducing to the state of the art in biometric template protection and authentication in online transactions, the proposed protocol will be described in detail covering design objectives, sketching the use scenario, describing

the components and their interaction. Furthermore the enrolment and the verification / authentication process are shown followed by a brief discussion of security considerations. The paper concludes after further research directions are identified.

11.2 State of the Art

The state of the art of the two main building blocks of the proposed protocol – biometric template protection and online authentication approaches – are described in this section.

11.2.1 Biometric Template Protection

Biometric systems determine whether the observed biometric characteristic of a subject and the previously recorded representation in the reference data match. In contrary to knowledge or token-based authentication methods a biometric characteristic is bound to a natural person and such the likelihood that a security policy is violated by unauthorized delegation of the authentication factor can be minimized. However the limited number of biometric characteristics for a natural person and privacy regulations do require protection of the biometric data. It is not sufficient to simply encrypt biometric templates with classic cryptographic functions since they can not be compared in the encrypted domain. Furthermore requirements on template protection systems are: **Revocability** – pseudonymous identifiers can be revoked, multiple identifiers can be constructed from the same biometric trait. **Unlinkability** – pseudonymous identifiers cannot be tracked back to the data subject and multiple pseudonymous identifiers of the same data subject cannot be linked against each other. **Removal of additional information** like medical information.

A recent overview of existing biometric template protection systems is given in Breebaart [18]. The described harmonized reference architecture is integrated in the international standard ISO/IEC CD 24745 *Biometric Template Protection* and its nomenclature is used throughout this paper. The Fuzzy Commitment Scheme [109] is one of the systems for template protection, it introduced shielding functions to secure biometric data. An essential building block of our proposed protocol is the helper data scheme (HDS) [226] that uses the principle of fuzzy commitments to privacy protect biometric features and satisfy the above-mentioned requirements.

11.2.2 Authentication in Online Transactions

Up to now, many different systems are being used for online transactions that are, depending on the threat assessment, not adequately secure [1].

PIN/TAN – Since 1990 international banks were using two dynamic factor authentication based on personal identification number (PIN) and transaction number (TAN), which are pre-shared secrets between the customer and the bank. A list of a certain number of TANs is in the possession of the customer. To authenticate a transaction, the next valid TAN in the list is used and it gets invalid automatically. A new list can be sent via post. Due to the increasing threat posed through phishing attacks, the PIN/TAN approach is nowadays rarely in use.

PIN/iTAN In response to phishing attacks a new attempt of online transaction authentication, the iTAN, is used since 2006. It is based on the PIN/TAN approach, but in contrast it uses indexed TANs. For a certain transaction a TAN with a specific index is requested from the customer, therefore iTAN. Still, phishing is not prevented. If malware is on the customers computer, a man-in-the-middle attack is possible and the transaction can be manipulated (rerouting to a new beneficiary).

Mobile TAN (mTAN) This concept introduces a second channel towards the banking customer, through which relevant transaction data is sent. The channel is realized as a *Short Message Service* (SMS) towards the customers mobile phone. In this way the receiver is able to check the integrity of the transaction through visual comparison and is furthermore able

to confirm the transaction with a one time password (mTAN) that was also sent within the SMS. The mTAN has a limited validity and needs to be typed into the online banking software. Compared to the TAN and iTAN method mTAN is considered to be more secure. Man-in-the-middle attacks that intend to re-route the transaction fail. The mTAN-method requires a trusted platform (mobile phone) that can not be manipulated at the same time as the client computer of the customer. The method met with criticism because SMS messages can be traced [251]. During the next years the line between mobiles and web clients is blurring more and more, with the consequence of loosing this independent communication channel.

TAN Generators – Mobile tokens are used as TAN generators that produce sequentially new TANs. Some tokens like the RSA-token work on a timer basis. The different approaches are described below. **sm@rt-TAN** – a TAN can be generated if the banking card with chip and EMV TAN generator is inserted into the token. This approach is vulnerable to phishing and transaction monitoring through malware. **eTAN generator** – TANs are generated with the time and receiver bank account number as parameters. As the receiver number has to be typed into the token the approach is less convenient for customers but it is phishing proof. **chipTAN manual** – the banking cards needs to be inserted in order to generate a TAN. The transaction data (receiver account number, ordered amount) that needs to be secured has to be typed manually into the token. The device computes a transaction specific TAN. The approach results in a high level of security but also in inconvenience for the customer. **chipTAN comfort** – extension of the before mentioned approach. The transaction data is read through optical sensors into the generator. Furthermore the token is able to display the transaction data. With the activation of the generator the customer confirms the transaction. An assumption is that man-in-the-middle attacks are not possible because a generated TAN is only valid for one transaction. One comfort features make this assumption invalid: collective transfers are possible. In this case the receiver account number is not displayed by the device any more, which allow attacks that – assuming carelessness of a customer – can also effect single transactions. This online protocol and the interface to the used *Hand Held Device* (HHD) are standardized through the German Central Credit Committee (ZKA) as *HHD 1.3.2 with optical interface*.

photo TAN – *photoTAN* equates to the HHD 1.3.2 standard with optical interface, even though the transaction data is displayed as a two dimensional bar code from the banking server and captured with the mobile phone of the bank customer.

Digital Signature / HBCI – Digital signatures can also be used for online banking authentication. Its application was standardized with the *Home Banking Computer Interface* (HBCI) that was developed since 1996 from several German banking groups and standardized through the ZKA. This interface supports chip card based online transaction protocols. The protocol was further developed by the ZKA under *Financial Transaction Services* (FinTS) [279]. HBCI / FinTS render TAN lists unnecessary with a security assessed chip card and reader in the possession of the customer. HBCI establishes a secure tunnel from the client computer to the banking server and uses a public key infrastructure to digitally sign the transaction data with the private keys of the customer (signing key pair). This key pair is stored securely inside the chip card. The transaction data with the signature is then send to the banking server. As with all signature based approaches, also the HBCI suffers from the modification of the transaction data before the signature is done. The deployment of secure signature units can minimize this risk. A manipulation could nevertheless been performed by malware on the client computer before the signature is done by the chip card. The assumption that the client computers are malware free is not firm, in fact it is very improbably. Online banking based on digital signatures therefore requires a secure visualization concept for the transaction data that should be signed, as implemented in the *Secoder*.

Online-Banking with USB-Token – A token-based approach is followed by KOBIL with the *mIDentity*-USB-token, where the URL of the banking server is cast in hardware

to avoid rerouting to an attacker URL. In addition secure communication channels can be established. One drawback: authentication against the stick is based on on knowledge (PIN) typed into a (probably) insecure client program. Another provider for USB-token-based transaction security is Novosec: here not the communication itself is secured but the approach is based on digital signatures of the transaction data. Weigold et al. presented the *Zurich Trusted Information Channel (ZTIC)*, which is especially designed for insecure environments like malware-infected client computers [251]. The token establishes a secure connection to the banking server and displays the received transaction information, which can be accepted or denied on this dedicated piece of hardware.

11.3 Biometric Transaction Authentication Protocol

This section describes the proposed *Biometric Transaction Authentication Protocol* in detail. The abstract pipeline of the helper data scheme (HDS) as a building block and the BTAP are sketched in Figure 11.3. The acronyms are described in Table 11.2.

11.3.1 Design Objectives

We designed a new protocol, which addresses the two main requirements for online banking transactions. **Reliable Person Authentication**: the enrolled banking customer and only this natural person has initiated and confirmed the transaction. Repudiation of de facto executed transactions should be impossible. **Reliable Data Authentication**: The enrolled banking customer has checked the transaction within a trustworthy environment and confirmed the data with the supported biometric modality. The authentication data is send via a second autonomous and secure channel to a banking server.

11.3.2 Assumptions

The scenario in which the BTAP might be used can be described as follows: on a potentially insecure and malware infected client computer an Online Banking Software (BSW) is running, which communicates with a secure Online Banking Server (OBS). The BSW transmits the transaction data to the OBS and to a secure dedicated token, the Biometric Transaction Device (BTD). On the BTD the transaction is confirmed through the customer, a seal is created over the transaction data (the Transaction Order Seal (TOS)), which fuses the transaction data with the biometric data of the customer. The threat scenario for the BTAP is illustrated in Figure 11.1.

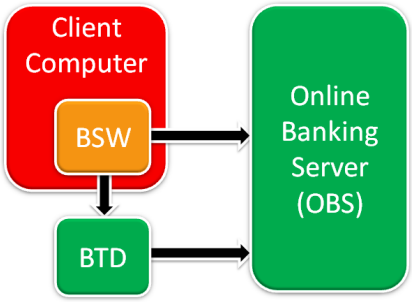


Figure 11.1: Sketch of threat scenario for the BTAP components. Green: trustworthy, tamper-proof (OBS, BTD); red/orange: probably insecure, malware infected (BSW)

The following list identifies components that are interacting for secure online transactions (Figures 11.4 / 11.5) and outlines their individual properties:

- **Secure Online Banking Server (OBS)**: has access to customer data; establishes communication with the Online Banking Software (BSW); conducts capital transactions; is able to identify a Biometric Trusted Device (BTD) as communication partner and preferably establishes a secure connection.
- **Online Banking Software (BSW) on insecure client computer**: executed on client computer that is threatened by Trojan horses, root kits, etc.; implemented as client software or browser based application; communicates with OBS and transfers transaction data as Transaction Order Records (TOR); TOR consist of: Transaction Identifier (TID), Sender Account Number (SAN), Receiver Account Number (RAN) and Ordered Amount (ORA); connected to the client computer is a trusted Biometric Transaction Device (BTD)
- **Secure Biometric Transaction Device (BTD)**: trusted piece of hardware, ideally with assessed security (e.g., common criteria), minimal and provable secure functionality; cannot be manipulated by malware; captures a biometric modality through Biometric Capture Device (BCD) as a fake resistant sensor, which is qualified for unsupervised operation in home and office environments; is able to connect to an Online Banking Server (OBS); is able to receive a TOR and visualize it on the trusted display (elements of a TOR are TID, SAN, RAN and ORA).

11.3.3 Enrolment Protocol

The enrolment process for the Biometric Transaction Authentication Protocol (BTAP) is sketched in Figure 11.4. The enrolment process of the helper data scheme (HDS) is modified for BTAP – the necessary steps are the following (executed operations are highlighted in *italic*, numbers in brackets indicate the time of execution and refer also to Figure 11.4):

11.3.3.1 Enrolment on the Online Banking Server (OBS)

- Generate shared Secret SBV, send it to customer(secure mail)/BTD(secure connection) (1)
- Create user record with: Account Number (AN) and Pseudo Identifier PI $= h(\text{SBV})$, which is derived from pre-shared secret SBV (2)

11.3.3.2 Enrolment steps inside the Biometric Transaction Device (BTD)

- Data subject (i.e., bank customer) presents the biometric characteristic (3)
- Capture multiple biometric (enrolment) samples (4)
- Extract real number reference feature vectors RRV (5)
- Binarize biometric features into quantized form QBV (6)
- Derive Auxiliary Data 1 (AD1) from biometric samples in the Reliable Bit Selector (RBS) block (7)
- Keep Robust Binarized Feature Vector RBV extracted from enrolment samples and AD1 (7)
- Insert shared Secret Bit Vector (SBV), e.g., sent via secure mail and typed in (8)
- Calculate Codebook Vector (CBV): CBV $= \mathit{ENC}(\text{SBV})$ (9) (e.g., using an error correction code like BCH)
- Calculate Auxiliary Data 2 (AD2) from CBV and RBV: AD2 $=$ CBV *XOR* RBV (10)
- Store non-sensitive data AD1 and AD2 into BTD or on personal chip card (11)

11.3.4 Transaction Authentication Protocol

To confirm an online transaction initiated by a bank customer, the Biometric Transaction Authentication Protocol (BTAP) extends the authentication with a biometric verification system. This protocol therefore follows a new approach, where a Transaction Order Seal (TOS) is computed locally and is sent instead of a TAN (sketched in Figure 11.5). The exchanged messages are sketched in Figure 11.2.

11.3.4.1 Operations executed by the insecure Online Banking Software (BSW)

- Creates through interaction with banking customer a Transaction Order Record (TOR), that contains: Transaction Identifier (TID), Sender Account Number (SAN), Receiver Account Number (RAN) and Ordered Amount (ORA)
  $\text{TOR} = (\text{TID}, \text{SAN}, \text{RAN}, \text{ORA})$ (1)
- Transmits TOR to Online Banking Server (OBS) (2)
- Transmits TOR to Biometric Transaction Device (BTD), which is connected to client computer (3)

11.3.4.2 Operations executed within the Biometric Transaction Device (BTD)

- Displays relevant information from TOR (at least RAN, ORA) on trusted display (4)
- Initiator and banking customer presents unforgeable biometric characteristic to the Biometric Capture Device (BCD) (5) for the transaction confirmation, that is further on processed as the probe sample image (6)
- Extract features from probe (7)
- Binarize features (8)
- Load Auxiliary Data AD1 from BTD memory or smart card (9)
- Compute binarized probe vector XBV from probe sample and AD1 (9)
- Compute codebook vector CBV′ from stored Auxiliary Data 2 (AD2) and XBV: $\text{CBV}' = \text{AD2}\ \mathit{XOR}\ \text{XBV}$ (10)
- Decode CBV′ into SBV′: $\text{SBV}' = \mathit{DEC}(\text{CBV}')$ (11)
- Compute Pseudo Identifier (PI′) from SBV′: $\text{PI}' = h(\text{SBV}')$ (12)
- Compute Transaction Order Seal (TOS′) from Transaction Order Record and reconstructed PI′: $\text{TOS}' = \mathit{MAC}(h(\text{TOR}), \text{PI}')$ (13)
- Transmit Transaction Order Seal (TOS′) to Online Banking Server (13)

11.3.4.3 Operations executed on the Online Banking Server (OBS)

- Received the Transaction Order Record (TOR) from the Online Banking Software (BSW) (2)
- Received also the Transaction Order Seal (TOS′) from the Biometric Transaction Device (BTD) (13)
- Hash the received TOR (14)
- Load stored Pseudo Identifier (PI) in the database for the customer ($\text{PI} = h(\text{SBV})$) (15)
- Reconstructs TOS: $\text{TOS} = \mathit{MAC}(h(\text{TOR}), \text{PI})$ (15)

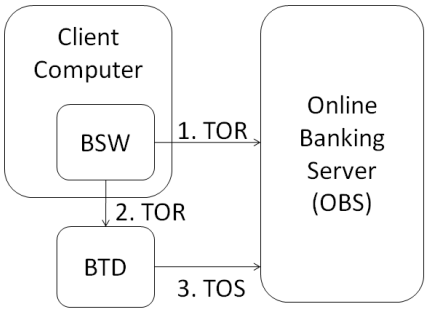


Figure 11.2: Arrows indicate messages exchanged between the different entities. Transaction Order Record TOR $=$ (TID, SAN, RAN, ORA), Transaction Order Seal TOS $=$ $MAC(h(\text{TOR}), \text{PI})$

Attack	Authentication Method TAN	iTAN	mTAN	Electr. Signature	Security Token	BTAP
Password Phishing	1	1	0	0	0	0
Visual Spoofing	1	1	0	1	0	0
Malware	1	1	1	1	0	0
Man-in-the-Middle	1	1	1	0	0	0
Denial of Service	1	1	1	1	1	1
Human Factor	1	1	1	1	1	1
Delegation / Repudiation	1	1	1	1	1	0

Table 11.1: Vulnerability of authentication methods (strongest representative) in online banking based on threats as categorized in [1].

- Compares TOS with the received TOS′ from the BTD: TOS == TOS′ (16)

The transaction is person and data authentic if, and only if, TOS and TOS′ are identical. In this case the transaction, encoded into the Transaction Order Record (TOR), is considered authentic and confirmed and thus the order will be conducted by the OBS. The various steps of the protocol that are executed in the BTD and on the OBS to confirm a transaction and to validate the authenticity of the data and the initiator are sketched in Figure 11.5. The BTAP Protocol operates on a minimal number of message that are transferred between the components as illustrated in Figure 11.2.

11.3.5 Security Considerations

The proposed BTA-protocol is based on the helper data scheme for Template Protection and on generic standard cryptographic primitives. The following primitives are used: Hash Function, Message Authentication Code, Error Correction Code and the XOR-operation used as a Vernam pad (where the key and the message are of the same length). The Biometric Transaction Device (BTD) is considered to be a tamper-proof trusted environment that cannot be modified nor eavesdropped. Assuming a secure enrolment process the following attacks aiming at gaining control over the transactions are identified according to the pipeline of BTAP and the exchanged messages (Figures 11.2 / 11.3(b)).

11.3.5.1 Attacks on the helper data scheme (HDS)

The helper data scheme is not leaking information about the secret nor the biometric features if the biometric information can be modeled as independent and identically-distributed (i.i.d.) random variables [226]. Further research on the security of template protective sys-

tems can be found in Ignatenko et al. [91] and Zhou et al. [290]. The main requirements of the HDS are in fact requirements on the entropy of the underlying biometric system[1].

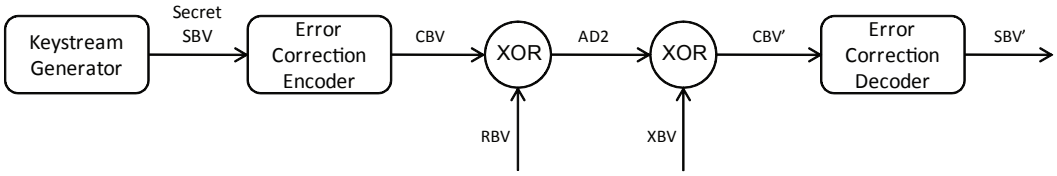
11.3.5.2 Modification of Transaction Data

The transaction data encoded in the Transaction Order Records (TOR) can easily be modified inside the potentially insecure client computer. There are two possibilities how to proceed an attack if the transaction data (e.g., the Receiver Account Number (RAN) and the Ordered Receiver Amount (ORA)) has been modified by malware.

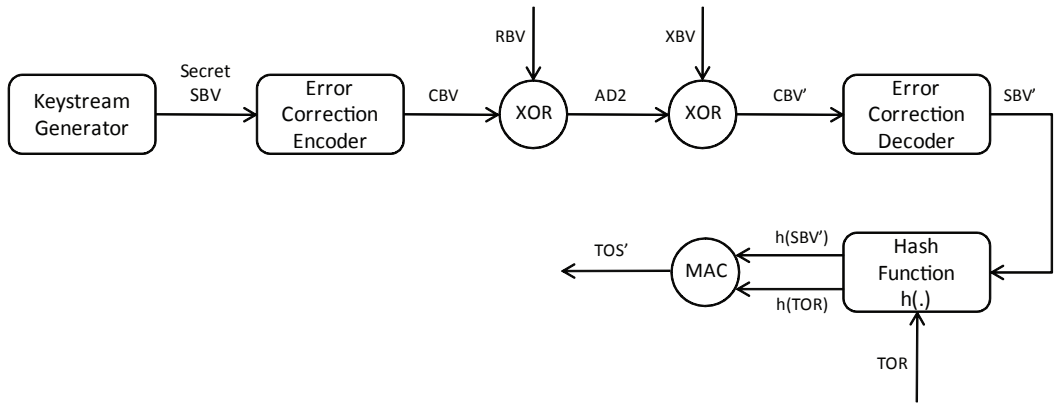
The first approach is modifying the data that is sent to the Online Banking Server (OBS) and to the Biometric Transaction Device (BTD) in the same way. This attack focuses on the human factor, since the initiator of the transaction has to check and confirm the transaction data that is displayed on the trusted display of the BTD. If the transaction is confirmed the attacker succeeded.

The second approach attacks the protocol itself. The transaction data forwarded to the BTD is not changed but the data sent to the OBS is modified. In this scenario the initiator would confirm the intended transaction. The comparison on the server site would result in a negative authentication if the Transaction Order Seals (TOS and TOS') are not equal. The TOR sent to the BTD could be constructed by choice. Assuming that a transaction initiated and authenticated by the customer will always be positively authenticated by the system, the secret SBV has to be error free when inputted to the MAC block. What follows directly: h(TOR) has to be the same on both sides, in the BTD as well as in the OBS. A construction attack on TOR turns out to be an attack on the full hash space (assuming the MAC block is

[1]The entropy of the biometric features in the information theoretic sense is not an issue, rather the reliable extraction of the core information that is invariant to noise and that could be described as *biometric entropy*.



(a) Building block HDS. Input: RBV/XBV (robust reference/probe bit vectors of the biometric subsystem for enrolment/verification), Output: SBV'



(b) BTAP. Input: RBV/XBV, TOR (Transaction Order Record); Output: TOS' (Transaction Order Seal).

Figure 11.3: Abstract pipelines of the helper data scheme (HDS) and the Biometric Transaction Authentication Protocol (BTAP).

secure, completely random guesses for the TOS' have to be made that could fit the chosen TOR). By replacing the hash function the protocol would still be secure.

11.3.5.3 Replay Attacks

Since the Transaction Identifier (TID) is included within the transaction information, which is hashed afterwards, a replay attack cannot succeed. A modification of the TOR results in a different hash value h(TOR) and therefore the value of the Transaction Order Seal (TOS) results in a not foreseeable different value.

11.3.5.4 Attack on the Transaction Order Seal (TOS)

If the independent and preferably secure channel between the BTD and the OBS is broken or an attacker gets hold of the communication between the parties (Man-in-the-Middle Attack), the Transaction Order Seal (TOS) can be attacked, since there is the possibility to extract information about the Pseudo Identifier (PI) from the TOS. The TOS is the result of a Message Authentication Code (MAC) that is applied with the hash value of TOR as message and the Pseudo Identifier (PI) as key. If the MAC is broken, PI could be extracted. In this scenario the security of the TOS depends on the MAC, which has to be exchanged if broken.

Another approach would be a brute force attack on the key (PI) when TOS and TOR are known to an attacker. To solve this issue the size of the key has to be sufficiently large to make this attack too expensive considering the computational effort.

Assuming the BTD to be powerful enough to perform asymmetric cryptography, TOS can be encrypted with the public key of the OBS to secure the link.

11.3.5.5 Limitations and Attacks on Biometric Subsystem

Limitations and potential attacks on the biometric subsystem need to be considered, as this is an essential component in the BTAP:

- Imposter Authentication – an attacker could try to authenticate a transaction, this would refer to an attack on the biometric system in combination with the helper data scheme (HDS). If the reliable bit vector (XBV) consists of equally distributed bits (over the population and inside each feature vector) and the RNG block generates also equally distributed secrets, the chances of having the same two reliable bit vectors from two different data subjects depends on the length of the XRV. The next points resumes this issue.

- Limited biometric performance – it has to be clearly stated that the error correction capability should be chosen as small as possible to add as less as possible redundancy to the secret. This is in fact a challenge of the underlying biometric system, the feature extraction has to be accurate in order to render the need for error correction unnecessary.

- Aging and Changes in the biometric characteristic – the biometric modality should be chosen in a way that aging can be neglected and that changes in the characteristic can be handled by the feature extraction. In the worst case the biometric characteristic has to be re-enrolled.

- Attacks on the Biometric Capture Device – the sensor - as part of the BTD - is considered to be trusted, non-attackable and also qualified for unsupervised biometric verification.

- Hill Climbing – cannot be conducted since the output of the system is not a comparison score but a binary decision.

11.3.5.6 Attacks on Privacy

- If TOR can be read by an attacker, transactions can be tracked. This could happen through malware on the client computer or weak links between either the BSW and the OBS or between the BSW and the BTD.
- Cross-Matching attacks cannot succeed if different Pseudonymous Identifiers (PI) are used in different application scenarios. To achieve this, different secrets have to be created and merged with the biometric information.
- Biometric Additional Information cannot be extracted if the BTD is secure and the used helper data scheme for privacy protection is not broken.

11.3.5.7 The Human Factor

As mentioned earlier the system can only operate in a secure manner, if the human factor is not exploited. A risk that could be foreseen is that to much information (e.g., long IBAN numbers) is displayed to the natural person. In such a case the likelihood that the subject approves that information without carefully comparing displayed information to the intended information is high (this happens widely, when users accept ”blindly” software license conditions). This risk of information overflow is in no way specific to the BTA-protocol.

A comparison of BTAP with standard approaches for transaction authentication is shown in Table 11.1 indicating that BTAP show robustness against more attacks than current alternative protocols.

As long as the building blocks of the Biometric Transaction Authentication Protocol are not broken, the protocol is secure against various attacks. The modular design provides the possibility to exchange most of the cryptographic primitives with limited effort in the case of an incident. The knowledge about the correct implementation of the system is a root of trust. Thus in order to increase trust of operators and users in the system, components and desirably the whole system should be subject to Common Criteria security analysis and its trustworthiness should be certified by an independent institution.

11.4 Future Work

The proposed protocol for transaction authentication can be used also in a more general context, since the biometric information can be fused with any kind of information. The resulting biometric signature system can be used in various applications. A future extension will handle multiple person transaction authentication to reach a higher level of security e.g., confirm transaction of large volumes in the cooperate and inter-banking sector or to satisfy regulations like the four-eyes principle. The BTAP can be hardened using multi-factor authentication adding also knowledge and/or possession factors.

From the biometrics perspective further research has to focus on unsupervised biometric capture devices that generate biometric samples with sufficient entropy to make the proposed protocol strong against brute force attacks on the secret.

An interesting aspect is also the concrete implementation using existing technologies and products available on the market to realize the BTAP.

From an economic point of view the question has to be solved if the return of investment is guaranteed with the usage of the BTAP and the BTD. Considering not only that BTAP would prevent online transaction frauds but also the fact that the quantity of incidents is increasing rapidly one could assume that the investment is amortized after a rather short time span depending on the costs of the device and changes in the infrastructure.

A more formal security analysis is needed in order to prove the properties of the protocol – it is in preparation.

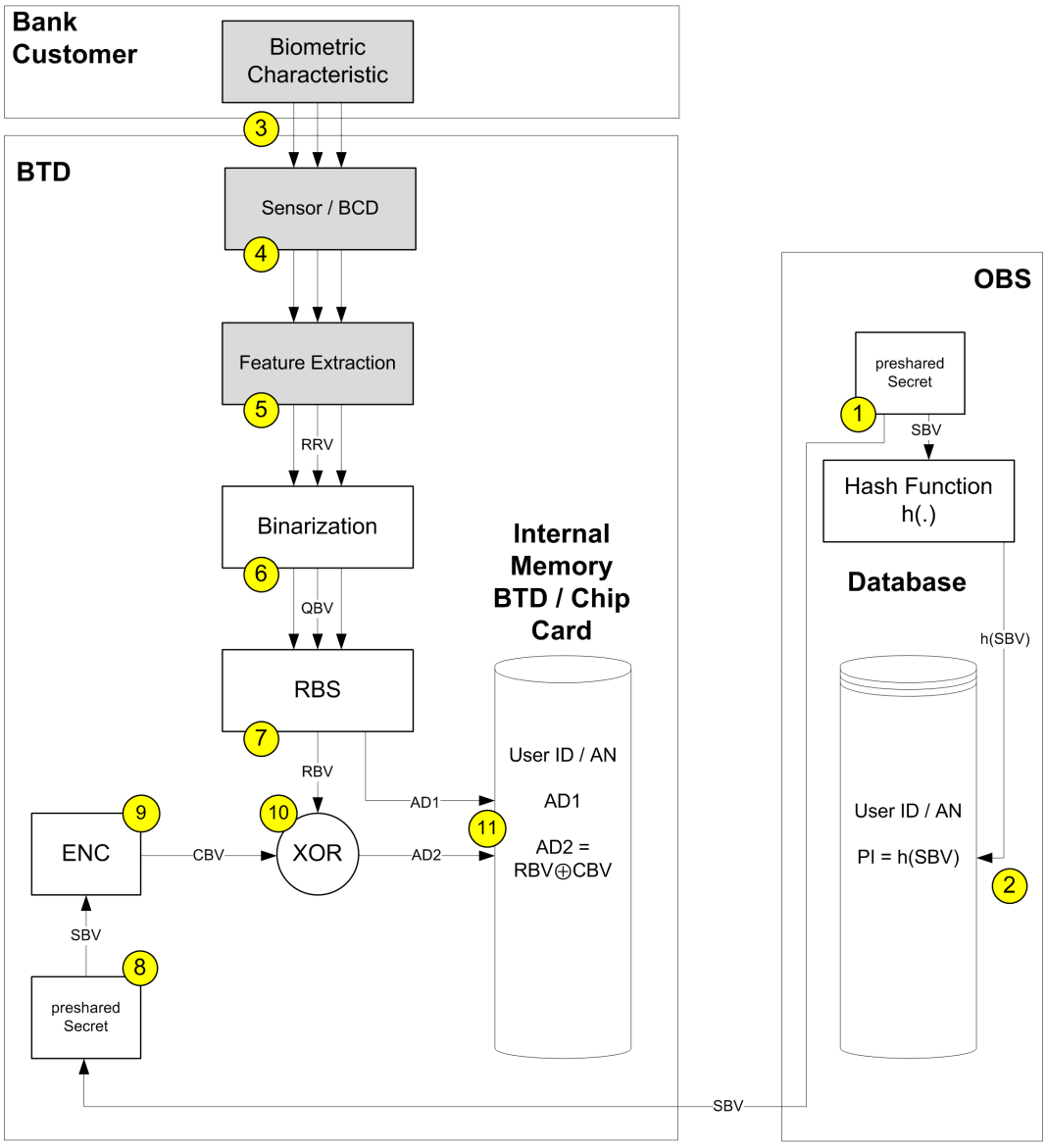


Figure 11.4: Process flow of the enrolment protocol

Name	Description
AD1	Auxiliary Data 1: Reliable Bit Indexes from RBS block
AD2	Auxiliary Data 2: AD2 = CBV *XOR* RBV
AN	Account Number
BCD	Biometric Capture Device
BSW	Online Banking Software
BTAP	Biometric Transaction Authentication Protocol
BTD	Biometric Transaction Device
CBV	Codebook Vector: CBV = $ENC(\text{SBV})$
ENC	Error Correction Encoding Block
DEC	Error Correction Decoding Block
HDS	Helper Data Scheme
OBS	Online Banking Server
ORA	Ordered Amount
PI	Pseudo Identifier: PI = $h(\text{SBV})$
QBV	Quantized Binary Vector
RAN	Receiver Account Number
RBV	Robust binarized feature vector from enrolment process (derived from QBV at positions AD1)
RBS	Reliable Bit Selector block (identifies stable positions in feature vectors)
SAN	Sender Account Number
SBV	Pre-shared Secret (Binary Vector)
TID	Transaction Identifier
TOR	Transaction Order Record: TOR = $(\text{TID}, \text{SAN}, \text{RAN}, \text{ORA})$
TOS	Transaction Order Seal: TOS = $MAC(h(\text{TOR}), \text{PI}) =$ $MAC(h(\text{TID, SAN, RAN, ORA}), h(\text{SBV}))$
XBV	Robust binarized probe vector for the verification process: XBV = RBV′

Table 11.2: Acronyms of the used variables and components in BTAP.

11.5 Conclusions

The proposed Biometric Transaction Authentication Protocol solves a basic problem of nowadays online banking: how to realize a person and transaction data authentic protocol in a potentially insecure environment. Furthermore the requirement to use biometrics in online banking scenarios to reach a binding of the biometric trait with the intended transaction data, is fulfilled in BTAP. At the same time the biometric information is sealed in a privacy preserving way and cannot be extracted by any party. BTAP offers two important features of a security protocol: low complexity and strong modularization.

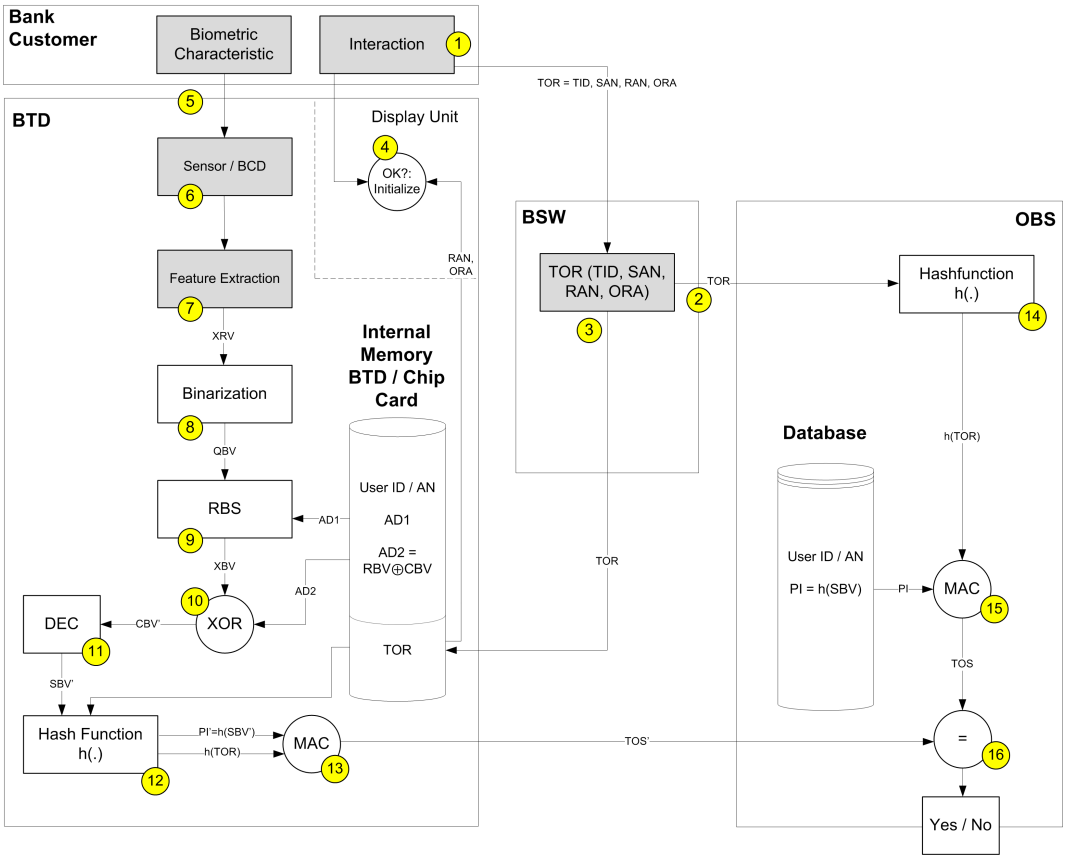
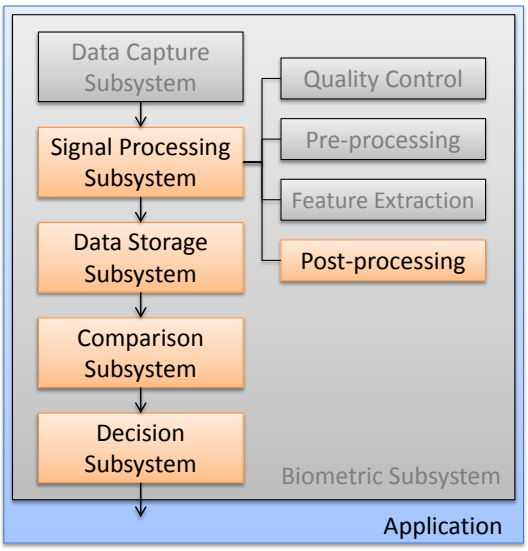


Figure 11.5: Process flow of the transaction verification protocol

Chapter 12

Biometric Transaction Authentication Protocol: Formal Model Verification and "Four-Eyes" Principle Extension



The BTAP, for biometric authentication of banking transactions, introduced in Chapter 11, is further specified in this chapter. A formal analysis in the applied pi calculus proves security properties of the core protocol. Additionally extensions are sketched to expand the transaction authentication to allow for multiple persons and for the encryption of exchanged messages.
The paper was published in: [74] HARTUNG, D., AND BUSCH, C. Biometric Transaction Authentication Protocol: Formal Model Verification and "Four-Eyes" Principle Extension. In LNCS 7126, Financial Cryptography and Data Security (2012). The ideas are patented in: [21] BUSCH, C., AND HARTUNG, D. (EN) AUTHENTICATED TRANSMISSION OF DATA, June 2011. (WO/2011/063992).

Abstract

The BTA protocol for biometric authentication of online banking transactions is extended to allow for multiple person authenticated transactions. In addition a formal specification is given, the protocol is modelled in the applied pi calculus and the security properties of data and person authentication as well as non-repudiation are verified using the tool ProVerif.

12.1 Introduction

The need for secure authentication methods is evident when looking at the assets transferred over the Internet, the level of interconnectedness and the posed threats: a recent example of malware affecting vital, well-protected infrastructures is the Stuxnet computer worm. And even more, badly protected client computers are exposed to threats: malware on clients endanger especially online banking transactions, whose manipulation promise rapid financial gain to attackers. This has to be prevented. However from a service providers view, not only the integrity of the data, but also its origin is to be guaranteed, which will be referred to as data and person authentication throughout the paper. Until now, no method for online banking transactions features non-repudiation of origin (natural person). One reasonable solution to this problem is the use of biometric systems, but not without raising threats to the users privacy.

In [72] a protocol was proposed that addresses the aforementioned problems, it uses a system for biometric person authentication using so called Privacy Enhancing Technologies (PETs) or Template Protection to authenticate online banking transactions without revealing the sensitive biometric data. At the same time the transaction data has to be authentic in order to get executed by the banking server side. These properties hold true even if the client is considered to be insecure and possibly controlled by an attacker.

The BTA protocol – Biometric Transaction Authentication Protocol – is summarized in the next section. It is modelled in Section 12.3 using the applied pi calculus [154] and its security properties are verified using the tool ProVerif [14] in Section 12.4. Before concluding the paper, an extension of the protocol, enabling multi-user, multimodal as well as multi-factor authentication of single transactions, is given in Section 12.6.

12.2 BTAP Wrap-Up

The goal of BTAP [72] is to enable data and person authentic online banking transactions on insecure client computer environments. To reach this goal a biometric subsystem has to be combined with classic cryptographic functionality. The critical transaction authentication is sourced out on a tamper-proof biometric transaction device (*BTD*) with limited functionality that can be certified using information technology security evaluations. The other different parties that communicate in the protocol are shown in Figure 12.1: the customer using a potentially insecure client computer running a banking software (*BSW*) and a trusted online banking server (*OBS*).

Within the first phase of the protocol, the user is enrolled on the *BTD* using a biometric identifier and a pre-shared secret key (*SBV*). The user can afterwards conveniently initiate a transaction on the client as it is done nowadays using e.g. the online portal of the bank. The transaction information is then shared with the *OBS* and the *BTD*. On the *BTD* the information is displayed within the trusted environment, the user has to check and verify the data by presenting his or her biometric trait(s) to the sensor of the *BTD*. A seal *TOS'* is created within the *BTD* over the transaction data using the pre-shared key, that is released by the biometric sample. This seal is sent to the *OBS*, which can then check the authenticity of the transaction data as well as the authenticity of the transaction initiator – only in the case of a successful verification of the seal, the transaction is confirmed and executed.

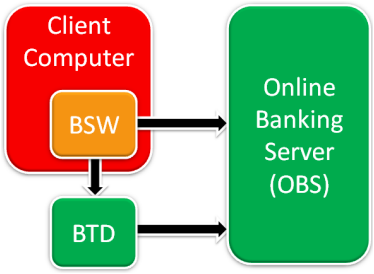


Figure 12.1: Threat scenario: online banking SW (*BSW*) resides on possibly malware controlled client environment and communicates with trusted online banking server (*OBS*) as well as with a secure biometric transaction device (*BTD*).

12.2.1 Information Flow Enrolment and Verification

The protocol involves more complex procedures inside the building blocks. Within the *BTD* the biometric subsystem is found, it covers the process of enrolment and verification that are inspired by the helper data scheme [226] for privacy protection, which performs a fuzzy commitment. For the enrolment, a biometric sensor inside the *BTD* captures the biometric sample multiple times, extracts a fixed-length bit feature vector, which is then analyzed for reliable positions. The resulting reliable bit vector (*RBV*) is fused using the XOR-function ($\oplus$) with an error-encoded version of a pre-shared key (*CBV* = ECC(*SBV*)) that has the same length. Correcting errors using the decoding DEC of the ECC makes it possible to cope with the noise caused by the variability in the biometric information. The information stored on the *BTD* are not revealing any sensitive biometric information: pseudo identifier *PI* = hash(*SBV*), auxiliary data *AD1* = indexes of reliable positions in the feature vector, auxiliary data *AD2* = $CBV \oplus RBV$. Figure 12.2 depicts the enrolment process of binding an identity to a pre-shared secret key, this process is modelled in a simplified way as described in Section 12.3.6. Note that the pseudo identifier can be renewed or exchanged to enable revocation in a biometric system, which is not possible if the biometric information itself was used for the verification of identity. Furthermore no cross-matching of different template protected biometric databases can succeed if the secret *SBV* is chosen independent from each other. Potentially sensitive biometric data is never stored or decrypted for comparison in its original form.

After this step, transactions can be authenticated as shown in Figure 12.3. Inverting the enrolment process is releasing the hash value of the pre-shared secret: the data subject presents the biometric trait, a biometric sample is generated, features are extracted. The helper data is loaded, so the system is able to extract the bits of the fixed-length feature vector at positions that should be reliable for the enrolled data subject. The resulting reliable bit vector *XBV* is releasing the key if the error correction capabilities ϵ (in bits) of the used code is higher than the amount of single bit errors $|(XBV \oplus RBV)|$ occurred during the feature extraction step:

$$\begin{aligned} AD2 \oplus XBV &= (CBV \oplus RBV) \oplus XBV \\ &= CBV \oplus (RBV \oplus XBV) = CBV' \\ &\text{with } |(RBV \oplus XBV)| < \epsilon \\ \Rightarrow SBV &= DEC(CBV) = DEC(CBV') = SBV' \end{aligned}$$

The hash value of the extracted secret bit vector *SBV'* is identical to the stored value *PI*=hash(*SBV*) if the enrolled biometric sample was presented and the noise could be compensated using the error correction decoder function DEC. The seal TOS'/TOS can be computed over the transaction data *TOR* (transaction identifier *TID*, sender account number *SAN*, receiver account number *RAN*, ordered amount *ORA*) using the keyed message authentication code

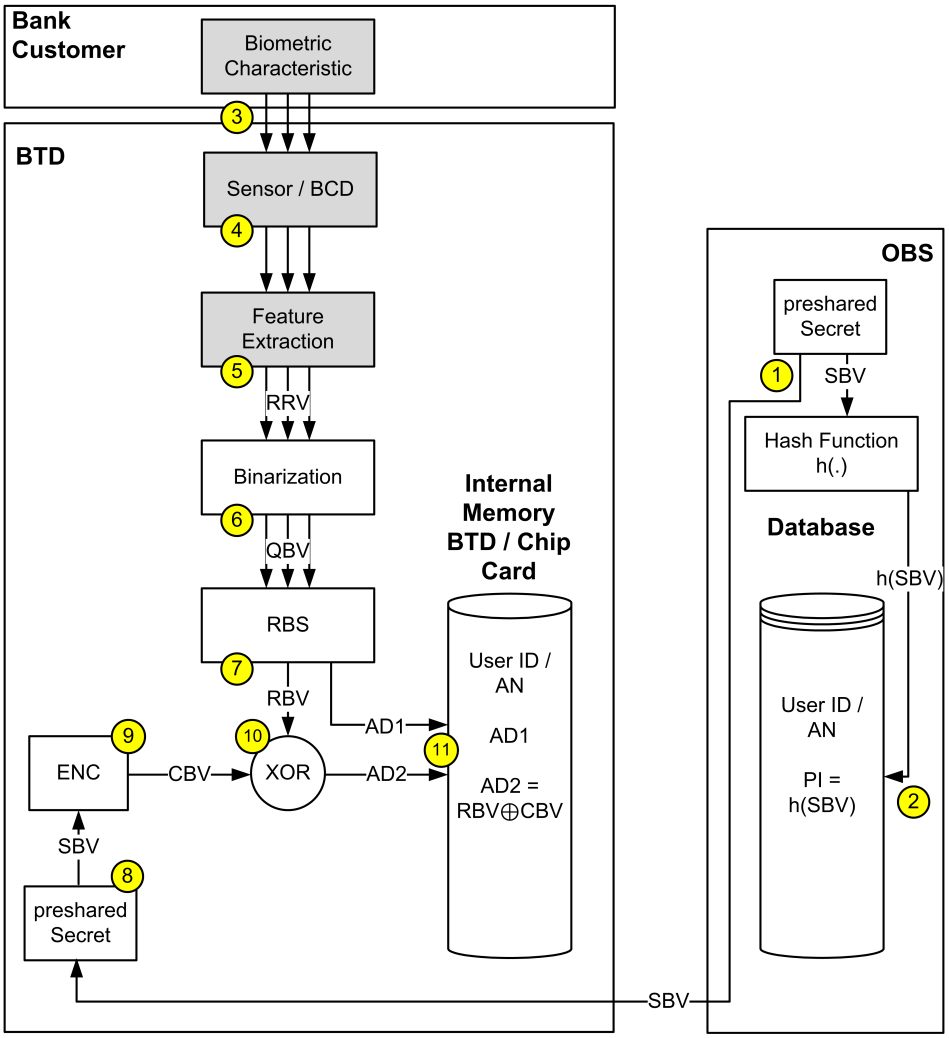


Figure 12.2: Information flow of the enrolment protocol.

function:

$$TOS' = mac(hash(TOR),\ hash(SBV'))$$

and accordingly on the server side

$$TOS = mac(hash(TOR),\ hash(SBV)).$$

12.2.2 Usage Scenario

The usage scenario of BTAP is seen in high value transactions like in the inter-banking sector, requiring a maximum level of security – the costs of enrolling the system in such an environment is negligible. Nonetheless since there is the need for secure authentication methods, BTAP could also be deployed in large scale, as in personal online banking transaction services, since the fixed cost for the *BTD* and the infrastructure would amortize considering the loss due to malware triggered false transactions over time.

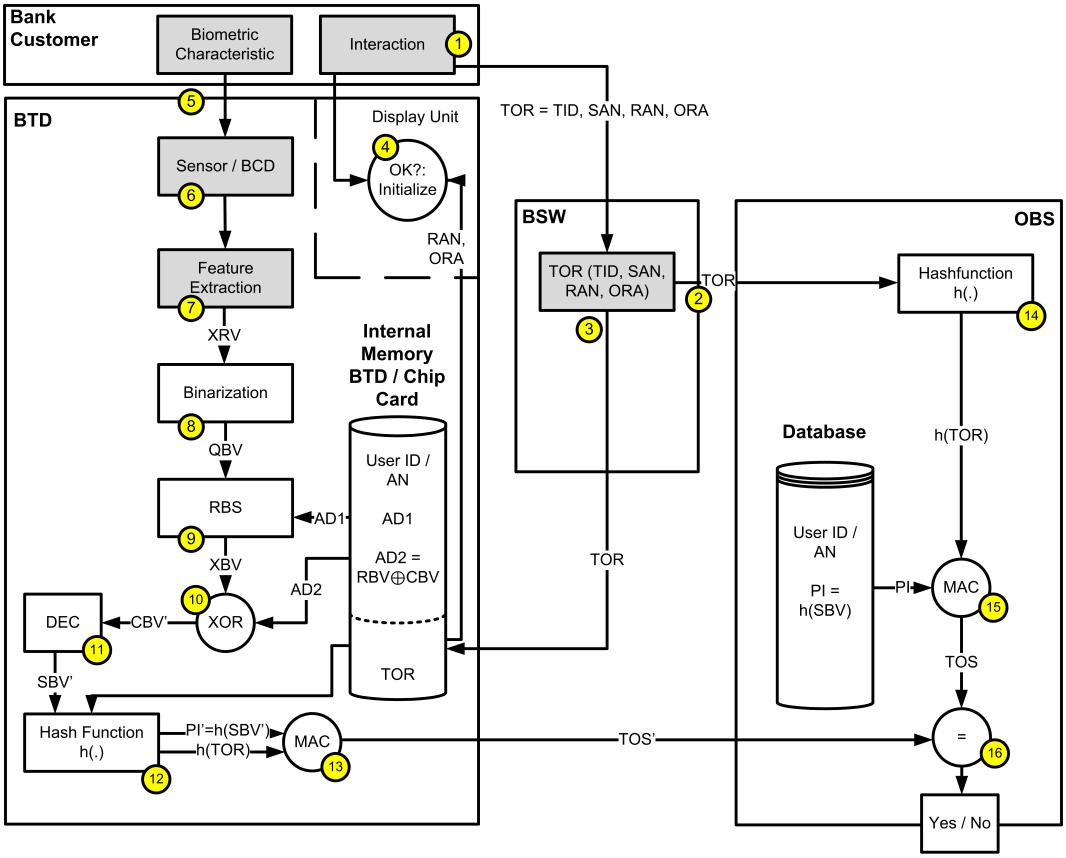


Figure 12.3: Information flow of the transaction verification protocol in the core BTAP.

12.3 Formal model

This section describes the formal method that was used to model BTAP and to analyse its security properties. The considered attacker model is sketched, the intended security properties are defined. Then the protocol is described using the exchanged messages as well as the applied pi calculus. The verification process based on the formal model is given in the end of this section.

12.3.1 Applied Pi Calculus and ProVerif

The applied pi calculus is a generalized version of the spi calculus [2], which itself is an extension of the pi calculus [154]. The pi calculus is a process calculus with the goal to formally describe concurrent systems, whose configuration may change during execution. Its variants are specifically designed to analyse and verify security properties of cryptographic protocols. The tool ProVerif was developed by Blanchet et al. [14] and it supports automated reasoning for applied pi calculus processes. It translates the protocol description into Horn clauses and acts upon them as a resolution prover. ProVerif fully automatically tries to prove security properties, its outcome can be either one of the following: robust safety can be proven, an attack as counter example is found, or it can neither prove or disprove robust safety according to the property. The protocol is modelled and verified using ProVerif, one advantage of using the tool: the Dolev-Yao attacker model, which is described in the next section, is specified and can be used directly.

12.3.2 Attacker Model

We assume the Dolev-Yao attacker model [47], which uses idealizations about the cryptographic primitives: an attacker can not learn from encrypted messages without the knowledge of the keys used for encryption. Changing an encrypted message without the knowledge of the key is detectable. Keys can not be guessed or learned from encrypted messages, also random numbers can not be guessed. Hash functions are collision free one-way functions. The attacker has full control over the communication channels, specifically he can: eavesdrop, inject and redirect messages. Furthermore he can generate keys and random numbers, as well as apply cryptographic primitives on what he learned.

12.3.3 Intended Security Properties

The intended properties of the BTA protocol are:

- *Authentication*: of the transaction data (integrity), the transaction initiator (proof of identity).
- *Non-Repudiation of Origin*: a valid transaction can not be repudiated by the initiator.
- *Secrecy*: the pre-shared secret and the sensitive biometric information stay secret.

Note: secrecy of the transaction data itself can not be assured if the client computer is compromised, and is therefore not covered in the core protocol. Additionally the internal *BTD* process is not modelled according to the applied pi calculus. Using the security assumptions, we model an idealized version of it.

12.3.4 Security Assumptions

The security assumptions for the verification of BTAP are listed below:

- *BTD* (in the model *B*) is tamper proof: no malware infection or manipulation of the processes and the storage of the *BTD* are possible (Note the advantages of using the privacy enhancing technology: revocation is enabled, the templates are protected additionally, only nonsensitive data is stored, storage capacity is negligible, efficient processing of the bitstrings, no hill climbing attacks possible). *BTD* supports secure I/O.
- Biometric subsystem: the biometric sensor can only be spoofed with unreasonable effort (suitable for unsupervised authentication). Biometric traits are unique and can not be replicated. The feature extraction system is able to extract a feature vector close to the enrolled sample, in a way that the shared key is released correctly (see Section 12.2.1).
- Enrolment phase is completed by the authentic person, the process is not tampered.
- Helper data scheme (HDS) is not leaking private information about the extracted biometric feature vector nor the pre-shared secret. The biometric entropy is high enough to enable reasonable long pre-shared secrets to avoid brute force attacks.
- Online banking server *OBS*, or short *S* in the model: trusted and secure environment. Its public key *pkEncS* for encryption and pkSignS for signatures are publicly available.
- Client computer is considered untrusted and can be manipulated by malware.
- Secret keys are secret: pre-shared key *SBV* is shared[1] between server *OBS* and *BTD*, extracted biometric feature vector is also secret.

[1] In a real-life scenario the key could be shared using a secure independent channel. Personalized confidential (physical) mails or credentials could serve as a direct input to the *BTD*.

- Computational limitations are: none for the client and server, no public-key crypto for *BTD*.
- Communication channel between server *S* and client *C* (running the banking software *BSW*), unidirectional channels from *C* to the *BTD* and from *BTD* to the server.

12.3.5 BTAP: Message Sequence

Informally a protocol can be described by the messages that are exchanged, the core message sequence for BTAP [72] is given below, where {} indicate an encryption with a symmetric key `Kxy`, a public key `pkEncX` from X for encryption, or a signature using the private key `prSignX` from X. `X->Y` stands for a message from X to Y. The four parties are client `C`, server `S`, biometric transaction device `B` and user `U`:

```
Message 1:  C->S: {(Nonce1, AN, ORA, RAN)}pkEncS
Message 2:  S->C: {(Nonce1, Nonce2, AN, ORA, RAN)}prSignS
Message 3:  C->B: (Nonce2, AN, ORA, RAN)
Message 4:  U->B: (Ok)
Message 5:  B->S: (mac(hash(Nonce2, AN, ORA, RAN), hash(SBV')))
Message 6:  S->C: {hash(true, Nonce2, AN, ORA, RAN)}prSignS
```

The transaction information consists of the sender account number *AN*, ordered amount of money to be transferred *ORA*, and the receiver account number *RAN*. Nonces are random numbers that are used only once for proof of freshness. *Nonce1* in message 1 and 2 serve as server authentication, only the owner of the private signature key *prSignS* (server *S*) can decrypt message 1 and reply the correct *Nonce1* (*Nonce1* should include a simple time stamp besides the random part, that has to be checked for freshness on the server side before sending message 2). Message 1 is encrypted with the public encryption key of the server. *Nonce2* is included for the freshness of the transaction data, to avoid replay attacks and to limit the validity using a timestamp part. The transaction data received by the server as well as *Nonce1* and *Nonce2* are signed and send back to the client as message 2. The client forwards the information in message 3 to the *BTD*. The user has to check and verify the transaction data displayed on the *BTD* with his or her biometric trait(s), which is modelled simplified as message 4. The pre-shared key *SBV* is released and used to create a seal *TOS'=mac(hash(Nonce2, AN, ORA, RAN), hash(SBV'))* using a message authentication code (MAC) mechanism in message 5 with *hash(Nonce2, AN, ORA, RAN)* as the message and *hash(SBV')* as the secret key. The server confirms the transaction in message 6 only if the seal from message 5 is identical to the seal *TOS* that can be created on the server side with the information from message 1, *Nonce2*, and the pre-shared key *SBV'*.

12.3.6 BTAP: Model in the Applied Pi Calculus

The internal processes of the biometric key release inside the *BTD* are not modelled here, since we are assuming a secure and tamper-proof environment and an idealized biometric subsystem. An attacker has no access per definition on the internal variables and processes. In order to model the process of checking and verification of the authentic transaction data by the user, we use the following approximation: the authentic transaction data is modelled as data signed with the secret key (the reliable biometric information *XBV* or equivalently *RBV* (see Section 12.3.4)) of a "public-key biometric" system only known to the user and verifiable by, among others, the *BTD*.
The attacker can create an arbitrary number of transaction information, which is modelled as *evilRAN* and *evilORA*. As we will see in Section 12.4, this is interesting for proving if such transaction information can be falsely authenticated.

All other protocol steps are modelled straightforward according to the message sequence shown in Section 12.3.5. The ProVerif code for the definition of functions, reductions

and free names is given below. The number behind a function name is its cardinality. As primitives we need the hash-, mac-function as well as public-key crypto in this model, the destructors describe the behaviour of the abstract functions:

```
(* Constants *)
data true/0.

(* Functions *)
fun hash/1.
fun mac/2. (* with destructor checkmac/2.*)

(* Asymmetric Encryption *)
fun pencrypt/2. (* with destructor pdecrypt/2 *)
fun prv/1. (* private part of a key pair *)
fun pub/1. (* public part of a key pair *)

(* Reductions *)
reduc  pdecrypt(pencrypt(x, prv(y)), pub(y)) = x;
   pdecrypt(pencrypt(x, pub(y)), prv(y)) = x.
reduc  checkmac(mac(y, x), x) = y.

(* Security Assumptions *)
(* Public Channels / Free Names *)
free c, cs, sb, cb, ub, uc, ORA, RAN, m, m2, m3.
```

The core of the protocol model are the processes, which define the behaviour of the communicating parties using the applied pi calculus. The processes are behaving like the user (processU), the client (processC), the server (processS), the *BTD* (processB) as well as the attacker (processAttacker). If a message is not as expected, the 0.-process is executed (process stops).

ProcessC receives a message *m* on the open channel *uc*. *m* is expected to have the form of a 2-tuple, the two elements are defined as *ORA* and *RAN* in the rest of the process. A nonce (*Nonce1*) is created and send on the open channel *cs* (to the server) with the transaction data received in *m* as well as the fixed account number, all encrypted with public encryption key of *S*. A reply is expected on *cs* in the form of a 5-tuple. The values received should be signed with the private signature key of the server, and they are expected to be equal to *Nonce1*, *AN*, *ORA* and *RAN*. On the second position a new nonce is received, which is defined *Nonce2*. The new nonce (used as a transaction identifier) as well as the transaction data is send on the open channel *cb* (also to the *BTD B*). The last line indicates the process to be waiting for the decision of the server (without function in the model, for the notification if a transaction was successful):

```
let processC =
 in(uc, m); (* user interaction: transaction data generated *)
 let (ORA, RAN) = m in
  (new Nonce1;
  out(cs, pencrypt((Nonce1, AN, ORA, RAN), pub(secretEncS))); (* Message 1 *)
  in(cs, reply); (* Message 2 *)
  let (= Nonce1, Nonce2, = AN, = ORA, = RAN) = pdecrypt(reply, pub(secretSignS)) in
   (out(cb, (Nonce2, AN, ORA, RAN)); (* Message 3 *)
   in(cs, decision))).
```

ProcessS describes the server behaviour. It receives a message on channel *cs*, which is encrypted with the public encryption key of *S*. Its decrypted form is expected to be a 4-tuple (*Nonce1*, *SAN*, *ORA*, *RAN*). If *Nonce1* is fresh (was not received before) and its timestamp is valid, a fresh and random number is generated (*Nonce2*) and send on *cs* with *Nonce1* as proof of authenticity as well as *SAN*, *ORA* and *RAN*, all signed with the private signature key from *S*. Note: in the model the freshness check of *Nonce1* is not performed due to limitations in the abstraction of memory in the applied pi calculus. The next expected message

is the seal sent on channel *sb* (from the *BTD B*). If the MAC was created using the secret pre-shared key *hash(SBV)* and using the transaction data received earlier in *m*, then the server accepts the transaction and creates a signed authentication reply over the transaction data including the nonce.

```
let processS =
 in(cs, m);
 let (Nonce1, SAN, ORA, RAN) = pdecrypt(m, prv(secretEncS)) in (* Message 1 *)
  (new Nonce2;
  out(cs, pencrypt((Nonce1, Nonce2, SAN, ORA, RAN), prv(secretSignS))); (* Message 2 *)
  in(sb, m2); (* Message 5 *)
  if checkmac(m2, hash(SBV)) = hash((Nonce2, SAN, ORA, RAN)) then
   (* Message 6 *)
   out(cs, pencrypt(hash((true, Nonce2, SAN, ORA, RAN)), prv(secretSignS)))).
```

ProcessB describes the biometric transaction device (*BTD*, here short: *B*). It receives message *m3* on channel *ub* (from the user). The message is expected to be a signed hash value of the authentic transaction data, only the party in possession of the private signature key can sign. This is a simplified model of the biometric subsystem. Message 3 is received from the (possibly malware infected) client *C*. Only if the hash of this transaction data is equal to the received signed hash, the seal (keyed MAC) is created over the message *m*:

```
let processB =
 (* reliable and authentic RAN, ORA from the user *)
 in(ub, m3);
 let hashvalue = pdecrypt(m3, pub(XBV)) in
  (* possibly UNreliable and UNauthentic RAN, ORA from the client *)
  (in(cb, m); (* Message 3 *)
  (let (Nonce, = AN, ORAin, RANin) = m in
   (if hashvalue = hash((ORAin, RANin)) then
    out(sb, mac(hash(m), hash(SBV))))))). (* Message 5 *)
```

ProcessU models the user, which is creating new authentic ordered amount and receiver account numbers (a new transaction). It signs these values with the secret private key (check and verify with biometric trait) and sends it on channel *ub*. The transaction data is not considered to be private (guessable + insecure client) and needs to be submitted to the client *C*, so it is made available on channel *uc*:

```
let processU =
 (* user creates new transaction *)
 new authORA;
 new authRAN;
 (* user checks and verifies authentic transaction data *)
 out(ub, pencrypt(hash((authORA, authRAN)), prv(XBV)));
 out(uc, (authORA, authRAN)).
```

The last process, the attacker, is simply creating evil (non-authentic) transaction information and makes it available on channel *c*. The idea behind this is to check later, if non-signed transaction data can be authenticated:

```
let processAttacker =
     new evilORA;
     new evilRAN;
     out(c, (evilORA, evilRAN)).
```

The following steps are modelled in the main process that is executed initially: create a new secret biometric feature vector *XBV* and make its public part available for verification. This is for the simulation of the checked and verified transaction data. A new secret pre-shared key *SBV* is created, as well as a sender account number *AN*, which is made public. *secretEncS* and *secretSignS* are the secrets for generating the servers key-pairs, again, the public keys are made available to all parties on channel *c*. The last part describes the

processes that can run after this initialization in parallel. Note: an unlimited number of processes is indicated by $!process$. A parallel execution of two processes X and Y is defined by $(processX) \mid (processY)$. That means any number of process instances of the user (*processU*), the client (*processC*), the server (*processS*), the *BTD* (*processB*) and the attacker (*processAttacker*) can run in parallel. The client and server are running by purpose with an unbound number of instances in this model, this may be counter intuitive but can be understood when looking at the specific processes:

process
new XBV;
out(c, pub(XBV));
new SBV;
new AN;
out(c, AN);
new $secretEncS$;
new $secretSignS$;
out(c, pub($secretEncS$));
out(c, pub($secretSignS$));

$((!processAttacker) \mid (!processU) \mid (!processC) \mid (!processS) \mid (!processB))$

12.4 Verification of security properties

In order to verify security properties, queries have to be formalized that are checked by ProVerif. A query of the form query $attacker{:}x.$, checks if the attacker gets to know x during the execution of the processes. The attacker model is set to active.

(Queries *)*
(Query 1: reliable bit vector extracted from biometric trait(s) *)*
query $attacker{:}XBV.$
(Query 2: modelled as public-key system *)*
query $attacker$:prv(XBV).
(Query 3: pre-shared secret key *)*
query $attacker{:}SBV.$
(Query 4: *)*
query $attacker$:hash(SBV).
(Query 5: encryption secret for public-key server construction *)*
query $attacker{:}secretEncS.$
(Query 6: private encryption server key *)*
query $attacker$:prv($secretEncS$).
(Query 7: signature secret for public-key server construction *)*
query $attacker{:}secretSignS.$
(Query 8: private signature server key *)*
query $attacker$:prv($secretSignS$).
(Query 9: seal over authentic transaction data *)*
query $attacker$:mac(hash(($Nonce2, AN, authORA, authRAN$)), hash($SBV$)).
(Query 10: seal over arbitrary transaction data *)*
query $attacker$:mac(hash(($Nonce2, AN, evilORA, evilRAN$)), hash($SBV$)).
(Query 11: server reply over authentic transaction data *)*
query $attacker$:pencrypt(hash((true, $Nonce2, AN, authORA, authRAN$)), prv($secretSignS$)).
(Query 12: server reply over arbitrary transaction data *)*
query $attacker$:pencrypt(hash((true, $Nonce2, AN, evilORA, evilRAN$)), prv($secretSignS$)).

Execution of the queries in ProVerif shows: query 9 (authentic seal) and query 11 (authentic reply from the server) are true. That means, the attacker gets to know information that is available on the channels after a successful run of the transaction authentication protocol using authentic transaction data on the server as well as in the *BTD*. The fresh nonce with

limited time validity inside the seal and the server reply avoid replay and delayed-play attacks, therefore the information can not be used to authenticate another transaction.

To wrap up the ProVerif simulation we could show, that the attacker does not get knowledge about the secret keys and the biometric feature vector. Non-authentic transaction data does not get sealed because of the process of checking and verifying inside the secure environment. If the integrity of a verified transaction is compromised, the two generated seals, the one inside the *BTD* and the one inside the server will differ, in this case the transaction is dropped. Non-repudiation of origin is ensured using the biometric subsystem, which only releases the key that is used to generate the seal, if the enrolled person is verifying the transaction. The private server keys stay secret, therefore the authenticity of the server towards C is guaranteed in the protocol, since only the owner of the private encryption key can respond with the correct nonce from message 1 (S only responds to message 1 if *Nonce1* is fresh). Attacks on availability are possible in our model if the attacker drops messages from the channels.

The security properties from Section 12.3.3 hold if the security assumptions from Section 12.3.4 hold true. Especially the assumption, that the authentic user is completing the enrolment phase correctly, is necessary for the non-repudiation of origin property. In a real-life scenario the enrolment of a user could be performed under controlled conditions to satisfy the assumption.

A drawback of the core protocol is that the user is incapable of deciding if the transaction was successfully executed, since a malware infected client can compromise / drop the result from the server, this issue and new features are addressed in the next section.

12.5 BTAP Extension: Secret Message Exchange

[2] Even though an attacker can not gain information from the seal, it is desirable to encrypt all exchanged messages to ensure privacy of the banking information. Note that the seal in message 5 does not need to be encrypted, since an attacker can not get any information about the key, nor the message from the MAC value. The best known forgery attacks for an MAC based on iterated keyed hash functions are birthday attacks, that are also used to find collisions in hash functions [12, 183]. Note also that the property of secrecy of the messages can not hold when the client is compromised, since for convenience reasons the client is still used to generate the transactions and to communicate with the server.

```
Message 1:  C->S: {(Nonce1, Ksc, AN, ORA, RAN)}pkEncS
Message 2:  S->C: {{(Nonce1,Nonce2,Nonce3,AN,ORA,RAN, ...
                ({(Nonce2, AN, ORA, RAN)}Kbs))}prSignS}Ksc
Message 3:  C->B: (Nonce3,AN,ORA,RAN,{(Nonce2, AN, ORA, RAN)}Kbs)
Message 4:  U->B: (Ok)
Message 5:  B->S: {(mac(hash(Nonce2, AN, ORA, RAN), hash(SBV)))}Kbs
Message 6:  S->C: {{hash(true, Nonce2, AN, ORA, RAN), ...
                ({hash(true, Nonce2, AN, ORA, RAN)}Kbs)}prSignS}Ksc
Message 7:  C->B: {hash(true, Nonce2, AN, ORA, RAN)}Kbs
```

Message 1 carries a symmetric session key Ksc, encrypted with the server's public encryption key pkEncS for an encrypted communication between S and C (PKI key verification required). Another symmetric session key, derived from the pre-shared secret SBV, is securing the communication for message 5, 6 and 7:

$$Kbs = onewayfunction(hash(Nonce3), hash(SBV)).$$

Since hash(SBV) is known to S and B, Kbs can only be computed within the two parties (on B after the enrolled user presents his or her biometric trait to release SBV).

[2] One parenthesis in message 2 was erroneous and is updated.

After releasing Kbs on the *BTD*, it is ensured to the device, that S has received the information (Nonce2, AN, ORA, RAN), since it is forwarded encrypted with Kbs in message 3 from the client. The *BTD* can check if the same transaction information was also send from the client and displayed to the user. Only if the two sets are identical, the transaction seal is created, otherwise a warning is shown on the secure display. When receiving message 7, it is proven to the *BTD*, that the server executed the transaction encoded in the authentic transaction data. On the secure display of the *BTD* the decision can be shown to the user.

The extended protocol does not send any transaction data in an unencrypted form over the channels, without the need for public-key crypto on the *BTD*. This extension ensures that the transaction data stays private and that the execution of the authentic transaction can be verified.

12.6 BTAP Extension: Online Banking Transactions Using the "Four-Eyes" Principle

Authentication of transaction data through multiple persons might be part of a policy if the ordered amount succeeds the liability of a single person or role. This procedure might help to prevent financial frauds. BTAP is extendible without much effort to comply with this requirement. Three different scenarios of a multiple-person authentication are identified, the pros and cons are discussed thereafter: 1.) one local *BTD*, one shared secret, 2.) one local *BTD*, multiple shared secrets, 3.) multiple remote *BTDs*, multiple shared secrets.

12.6.1 One local BTD, one shared secret

The enrolment process of the helper data scheme subsystem (Figure 12.2) has to be adapted, the shared secret has to be binded to n different data subjects. Therefore n different auxiliary-data-1 (*AD1*) sets have to be generated that define the reliable positions in the fixed length biometric feature vectors of each biometric trait. The pseudo identifier is created as in the original enrolment: $PI = hash(SBV)$. Only one auxiliary-data-2 (*AD2*) is generated during the process using the following formula for the error correction encoded pre-shared secret $CBV = ECC(SBV)$ and the data subjects reliable boolean biometric feature vectors RBV_i for $i = 2...n$ and $n \geq 2$:

$$AD2 = CBV \oplus (\bigoplus_{i=1...n} RBV_i)$$

The result of this adapted enrolment: the shared secret can only be released and therefore the transaction seal can only be generated over the transaction data, if all enrolled biometric feature vectors RBV_i can be extracted during the authentication phase. This means, every enrolled person must verify the transaction data locally with his or her biometric trait. Advantage: the order of presenting the biometric traits is negligible since the XOR-operation is commutative (still *AD1* is person specific and therefore an ID claim like a token is needed); a data subject k could be revoked, by just presenting the biometric trait (where RBV_k can be extracted from), *AD2* could be updated accordingly:

$$\begin{aligned} AD2' &= AD2 \oplus RBV_k \\ &= CBV \oplus (\textstyle\bigoplus_{i=1...n} RBV_i) \oplus RBV_k \\ &= CBV \oplus (\textstyle\bigoplus_{i=1...(k-1),(k+1)...n} RBV_i) \oplus (RBV_k \oplus RBV_k) \\ &= CBV \oplus (\textstyle\bigoplus_{i=1...(k-1),(k+1)...n} RBV_i) \end{aligned}$$

The drawback in this operation mode is that the amount of bit errors that can be corrected stays limited – only CBV carries the error-correction code. Evenly distributed bit errors in the feature vectors RBV_i would affect all positions of the codeword.

Alternatively the XOR-operation is applied to the concatenation of all RBV_i vectors and *CBV*. The entropy of the concatenated feature vector will be increased compared to a single feature vector, a longer key *SBV* and a longer resulting *CBV* could be used for high

security demands:

$$AD2 = CBV \oplus (RBV_1, \ldots RBV_k, \ldots, RBV_n)$$

Advantage: Higher level of security against brute force attacks on the secret *SBV*. Disadvantage: the system is inflexible, a re-enrolment is needed if data subject k is not allowed to authenticate online banking transactions anymore.

12.6.2 One local BTD, multiple shared secrets

When using multiple shared secrets, again an ID claim like a token is needed to distinguish between the enrolled data subjects. A binding of a pre-shared secret key and each extracted reliable boolean biometric feature vector (RBV_i) has to be conducted. This relates to n different enrolments on the same biometric transaction device (*BTD*) as described in the core BTAP. In this scenario, it is possible to create n different transaction order seals (TOS_i) over the same transaction order record *TOR = (TID, SAN, RAN, ORA)* using a keyed MAC-function:

$$TOS_i = mac(hash(TOR),\ hash(SBV_i))$$

The seals are send independently from each other to the server, which knows all the enrolled subject for a specific banking account. Advantage: Flexible solution for the user enrolment; Fine-grained policies on the server side enable different levels of security and flexible requirements (number of seals, seals from specific persons) for a transaction based on the ordered amount or the receiver account number, or other metadata. And the non-repudiation property is hold in this scenario, since a unique pre-shared key is bind to a natural person.

12.6.3 Multiple remote BTDs, multiple shared secrets

As seen in the previous case, a flexible system could be constructed using multiple shared secrets and one local *BTDs*. The same description applies to this case, with the difference that different *BTDs* could be used independent from each other, no ID claim is needed if every data subject is enrolled on a different *BTD* using a different pre-shared secret. This case enables time-shifted transaction authentication but it requires the distribution of pending transactions to the client, which could be done by using the online banking portal, simple e-mail transfer or a dedicated software.

12.6.4 Additional Authentication Factors and Multiple Biometric Modalities

BTAP can be extended to a multiple factor authentication system, adding possession as well as knowledge authentication factors that are given as input to the *BTD*. Including this information, which is shared with the server side, the transaction seal *TOS* would be computed as:

$$TOS = mac(hash(TOR),\ (hash(SBV),\ hash(Password),\ hash(TokenSecret)))$$

with the keyed mac-function. Adding additional authentication factors would strengthen the BTAP even more.

Extracted reliable biometric feature vectors RBV_i originating from multiple biometric modalities M_i with $i = 2...n$ and $n \geq 2$ of the same person, like e.g. fingerprint and finger vein data, can be used to generate a concatenated biometric feature vector $RBV' = (RBV_1, \ldots, RBV_n)$ that is used to release the pre-shared key in the BTA protocol.

12.7 Conclusions

The proposed security properties could be proven using a formal model of the core BTA protocol message exchanges and the protocol verification tool ProVerif. The protocol enables non-repudiable person and data authentic online banking transaction. The extensions enable privacy of the transaction data and in addition new security features: transactions can be sealed by multiple individuals to comply with restrictive policies. BTAP supports multiple biometric modalities and can be extended for multi-factor authentication as well. In the near future the pi-calculus must be extended in order to be able to deal with noisy biometric data as part of security protocols – then also the internal processes of the biometric transaction device could be modelled and verified.

Part III

Appendix

Appendix A

Biometric Systems

A.1 Introduction

We tried to stick to the ISO SC37 Harmonized Biometric Vocabulary throughout the thesis and according to their specification, biometrics is the field of "automated recognition of individuals based on their behavioral and biological characteristics". Examples for behavioral biometrics are signature, keystroke dynamics and gait, biological modalities are fingerprint, face, DNA, iris and vein. Many more characteristics can be used though and the list is continuously extended.

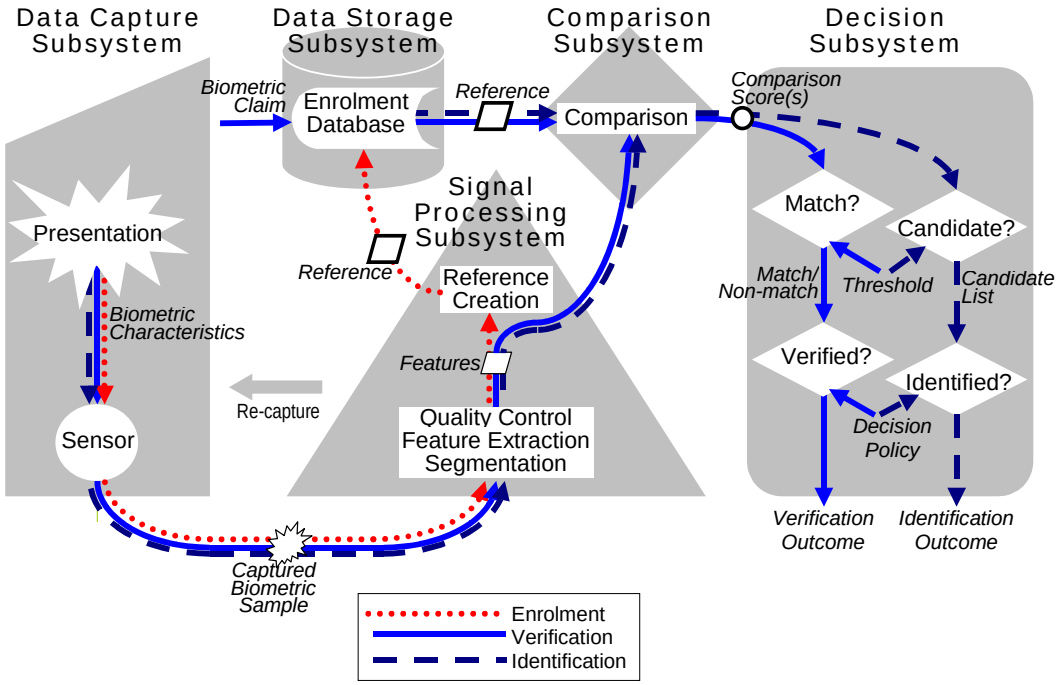


Figure A.1: Biometric pipeline obtained from [95].

The structure of a classic biometric system is shown in Figure A.1. In particular it describes the two stages of every biometric system (*enrolment* vs. operation), the basic modes that a biometric system can operate (*identification* vs. *verification*), the interaction of single functional blocks and the standardized nomenclature.

Before the automated recognition of a human can take place, its characteristics have to be known to the system. This process is referred to as *enrolment*, an entry in the data storage subsystem is created filled with a *reference*, also known as *template*, that represents the bodily characteristics in a compact form and that can later be used for comparisons. The template creation is based on the sensor information of a biometric characteristic from a *capture subject* that is further processed within the signal processing subsystem.

Two basic modes of a biometric system are distinguished, in an *identification* scenario no additional information is associated with a *probe* (biometric characteristic presented during operation), a *candidate list* is chosen from the enrolment database that is most similar to the probe (often referred to as 1:N comparison). The *similarity score* of two templates is decided by the comparison subsystem.

In a *verification* scenario a *biometric claim* has to be made, e.g. in form of a user ID or a token. Based on the claim a 1:1 comparison between the *reference* and the *probe* is performed. Depending on the similarity score from the *comparison subsystem* and a *threshold* that balances the the behaviour of the system, a *match* or a *non-match* is the result of the comparison.

A.2 Performance Evaluation

Biometric systems are error-prone probabilistic systems. To evaluate the biometric performance error rates are calculated at different stages of the pipeline, lower recognition errors correspond to a better biometric performance. *System performance* values for *scenario testing* reflect errors that may occur during the whole process depicted in Figure A.1, whereas *algorithm performance* for *technology testing* only considers errors that occur in the decision subsystem. We will focus in the following of verification scenarios only, identification scenarios require centralized databases and are often privacy intrusive and can be performed without consent of the capture subjects.

Commonly used as *system performance* measures are *false accepts*, that ISO defines as an "error of accepting a biometric claim that should have been rejected in accordance with ground truth". Its counterpart, the *false reject* is defined as "error of rejecting a biometric claim that should have been accepted in accordance with ground truth". The fraction of misclassifications including errors during the capturing process, the extraction of features that are observed are referred to as *false accept rate (FAR)* and *false reject rate (FRR)*.

The equivalents for the algorithm performance are *false matches*, that are defined as "comparison decision of "match" for a biometric probe and a biometric reference that are from different biometric capture subjects" and *false non-matches*, "comparison decision of "non-match" for a biometric probe and a biometric reference that are from the same biometric capture subject and of the same biometric characteristic". The error rates are defined as successfully completed comparison trials that result in a misclassification: *false match rate (FMR)* and *false non-match rate (FNMR)*.

A *receiver operating characteristic curve (ROC)* plots the FMR on the x-axis against 1-FNMR on the y-axis to visualize and compare the performances of different algorithms. Perfect biometric classification is indicated with the constant value of 1.

The *equal error rate (EER)* is often used as a scalar value indicating the performance of an algorithm or system. It is defined as the point where FMR/FNMR or FAR/FRR are equal or have the least distance for a fixed threshold.

A.2.1 Discussion

As indicated in Figure A.1, biometric systems are still considered to solely make decisions for authentication. However, with recent developments as shown in Chapters 11 and 12, it is possible to fuse information from the application, in which the biometric sub-system is integrated, with the released or extracted keys derived from biometric templates. This leads to new primitives and protocols, extending the intended use of biometric systems, and the need for standardization of those new scenarios.

Appendix B

Vein Minutia Cylinder-Codes[1]

Abstract

Vein recognition has been extensively studied in the past. The topology of the vein patterns allows to adopt simple representations, based on edges and their endings, which are quite similar to the fingerprint minutiae. In this paper, the Minutia Cylinder-Codes (MCC), developed for the comparison of fingerprint minutiae, are adapted to characterize vein minutiae. The algorithm adaptation requires to understand the vein topology and how to consequently define the parameter sets. Toward this end, an optimization problem is defined and solved using a genetic algorithm (GA) approach. The experimental results prove the applicability of MCC on three extended vein data sets of wrist and palm dorsal. The performance of the reference parameter set is improved and can compete with other state-of-the-art algorithms for vein-based verification.

B.1 Introduction

The key to successful biometric classification is often related to the choice of the representation (or template) adopted for the sampled biometric data. This, in turn, depends upon the choice of the features which are extracted from the raw data. For example, features with a fixed-length and structure can be further processed to improve a biometric system: in [225,226] a system for privacy protection was proposed that seals the biometric data from being extracted and reconstructed. It enables revocation and renewal of secure biometric templates with the inclusion of random keys into the secure template. It also hinders profiling the data subject over several databases. Therefore, it is very important to develop a feature representation which can cope with the limitations of a fixed length and order.

In the past several algorithms for extracting minutiae for vein pattern images have been proposed [127, 242]. However, the representation and comparison of such point clouds in a fixed-length form is not a trivial task if high biometric accuracy should be maintained. The spectral minutiae proposed in [264] is such a representation method that offers a fixed structure of the features and is invariant to translation and scaling of the input, rotations can be easily compensated. The original parameter set was utilized for vein data [77, 78]. However, for the investigated datasets representing different vein modalities, the recognition performance was deviating strongly.

Still, the reported biometric performance cannot compete with other state-of-art comparison methods, like the Similarity-based Mix-matching algorithm [30], that is using segmented and skeletonized versions of the input vein image. To resolve the currently limited biometric performance of fixed-length feature extractors in vein pattern recognition, this paper presents the investigation of the MCC algorithm to compare minutiae information extracted from different vein modalities, like the wrist area as well as the dorsal back areas. The MCC algorithm is one promising candidate that achieved solid recognition performance for fingerprint data while creating fixed-length features. It offers a variety of parameters, which makes it potentially an adaptable and flexible solution for the comparison

[1] submitted for publication

of various kinds of feature points with spatial and orientational information. The main focus of the work is to customize the MCC algorithm to improve the accuracy and robustness of biometric vein recognition.

B.2 MCC: the Minutia Cylinder-Code

The MCC algorithm, originally proposed in [22], it was designed to compare fingerprints minutiae according to the ISO/IEC 19794-2 template standard [102]. The location and orientational information of single minutia points is utilized to create a new representation. The MCC comparison of such a representation can be categorized as a local, fixed radius-based approach, which is in incorporating strong points of the alternative nearest neighbor-based approach: the descriptors are of fixed-length and can be efficiently compared. In the next sections the basic working principles of the algorithm are sketched.

B.2.1 Encoding

For each minutia m a cylinder is generated that has different layers and that is normalized according to m's orientation. The quantized orientation is encoded in the layer structure: all neighboring minutiae sharing the same quantized orientation are coded in the same layer.

Each layer is organized in cells that represent the quantized location around m in a fixed-length radius. Neighboring minutiae influence the cell's value that is corresponding to the distance and position towards m.

The encoding is invariant to translations and orientational changes of the minutiae points since it utilizes distances and locally normalized orientations.

B.2.2 Comparison

The global comparison score between two minutiae sets is composed of local, cylinder-based comparison scores. Whereas the local scores are defined as normalized Euclidean distances between two linearized cylinders. Finding minutiae pairs that will be compared is controlled based on a purely local manner or in a more complex way pre-selecting pairs based on local similarities, relaxing based on global relationships and optimizing for efficiency in the end.

B.2.3 Discussions

In [23] the algorithm was extended including enhanced techniques to improve the comparison: a new minutiae pair pre-selection method and a new relaxation method are proposed. In addition a reference parameter set was specified. With these parameters, MCC is defined as a baseline algorithm for the fingerprint verification competition *FVC-onGoing* introduced in 2009 in [48].

The MCC algorithm is highly parametrized: 7 parameters control the cylinder creation, 4 the local similarity and 12 the global similarity score computation. This extended parametrization makes the algorithm very adaptable and flexible. Yet, at the same time, finding the best parameter set according to some quality criteria is not trivial. Even though in [23] the parameters were *tuned* and *optimized*, the employed methodology is not described.

This paper aims to adapt and optimize the MCC algorithm (parameters) for minutiae from vein pattern images. It can be defined as an optimization or search problem, where the MCC parameters span the search space.

B.3 MCC for Vein Data

B.3.1 Problem Description

In biometric systems the performance – often reported as the equal error rate (EER) – is an essential measure in algorithm testing to determine the ability to distinguish genuine from imposter comparisons. The EER is defined as the operation point of a biometric system where a chosen threshold t yields an identical error rate for genuine and imposter attempts. The two error rates are often referred to as false non-match rate (FNMR) and false match rate (FMR). Utilizing normalized similarity score values $s \in [0, 1]$ and the probability density distributions (pdf) $\Phi_g(s)$ of genuine comparisons and $\Phi_i(s)$ of imposter comparisons. We can define the false non-match rate (FNMR) and the false match rate (FMR) for threshold t more formally as

$$\text{FNMR}(t) := \int_0^t \Phi_g(s)ds \text{ and } \text{FMR}(t) := \int_t^1 \Phi_i(s)ds. \tag{B.1}$$

The equal error rate can then be defined as:

$$\text{EER} := \text{FNMR}(t_{\text{EER}}), \text{with } \text{FNMR}(t_{\text{EER}}) = \text{FMR}(t_{\text{EER}}) \tag{B.2}$$

The classical optimization problem in biometric system is defined as: $\min \text{EER}$. In case of the MCC algorithm, the error rates depend on the parameter set $P = \{p_1, ..., p_n\}$ and the biometric minutiae training set T, therefore the search problem can be defined as:

$$\arg_P \min \text{EER}_{\text{MCC}}(P, T), \tag{B.3}$$

which translates to finding the MCC-algorithm parameter set P that minimizes the classification error measured in the equal error rate EER of the MCC algorithm applied to a training set T.

B.3.2 (Fingerprint vs.) Vein Pattern Recognition

Since the originally proposed MCC algorithm was designed for minutiae extracted from fingerprints, we briefly discuss similarities and differences between the two modalities.

Generally the samples captured for vein recognition are blood vessel images acquired from the hand area. Current research mainly focuses on palm and finger vein images, also palm dorsal and wrist vein patterns have been exploited.

Vein data features advantages compared to fingerprint-based biometric systems: no latent prints are left, there is no relation to crime investigation and therefore the acceptance in the population can be increased. It can be implemented touchless and is particularly suited for public applications. In addition it is considered to be more robust to fake attacks and liveness detection mechanisms possibilities are extended. But also drawbacks are inherent to this technology: the capturing devices are as of now more costly and voluminous. Reported error rates are often not reproducible, large-scale standardized datasets are not available and in general fingerprint recognition is considered more mature. However, in the last years vein recognition became more popular as an alternative to fingerprints.

Following a recent trend in biometric systems, vein data is captured to complement existing fingerprint systems. This fusion approach is recently being investigated and also products are being developed for the market. In the future, combined fingerprint and finger vein sensors can be expected as well as combined palm vein and multiple-fingerprint sensors.

Feature extraction in vein recognition can be categorized according to different criteria: (i) abstraction level for feature extraction; (ii) extracted features; (iii) comparison methods.

Criteria (i) covers different levels of abstraction with the need for different image processing stages (in ascending order of abstraction): raw sensor data, gray-scale image, contrast-enhanced image, segmented vein image and the skeletonized vein pattern. Further

abstractions are often based on the skeletonized vein pattern version and extract points describing the topography of the skeletonized vein pattern.

Criteria (ii) is based on the topology of the veins and can include: the vein image itself, local texture descriptors, the vein skeleton, minutiae points of vein skeletons, curvature information about the vein pattern, geometrical relations between veins and many more.

The comparison methods (iii) are derived from the field of research the features fall into. In consequence correlation-based, texture-based, graph-theory-based and point cloud-based strategies are feasible. The advantage of using minutiae points extracted from the vein skeletons is that the huge knowledge base from fingerprint-based minutiae comparators is available.

The main perceivable differences between fingerprint images and vein pattern images, that may influence the parameter selection and challenge the algorithm, are:

- Contrast in vein pattern images is in general low.
- Variation in contrast throughout the image.
- Sparsity of the veins, orientational field computation infeasible. Quality of orientation and angle extraction may suffer.
- Varying diameter of the blood vessels.
- Background diversity.
- In case of finger veins: shape of region of interest is rectangular.
- Angles may be highly correlated.
- Statistics of minutiae may differ from fingerprint and for different vein modalities.

B.3.3 Hypotheses

Due to the inherent differences between the modalities mentioned in Section B.3.2, it is expected that the reference parameter set of the MCC algorithm will not be suited to the vein data and will not result in lower biometric performance compared to state-of-the-art algorithms. The hypotheses **H1** hence formulates for falsifiability testing as: *MCC using the reference parameter set results in state-of-the-art performance*.

It is also expected that optimal parameter sets for different vein modalities will differ as they have particular properties. Hence hypothesis **H2**: *Optimal parameter sets will be equal for all vein modality datasets*.

As a last hypotheses we state that due to the variability of the MCC algorithm, parameter sets that result in state-of-the-art performance, can be found. Which leads to falsifiable hypothesis **H3**: *State-of-the-art performance using MCC for vein cannot be reached*.

B.3.4 MCC Parameterization

As mentioned earlier, a variety of parameters, overall 23, influence the behaviour of the algorithm regarding two main aspects: (i) generation of templates and (ii) comparison of templates. Within (ii), we can distinguish between (ii a) the local comparison computation and (ii b) the global score composition.

Please find an overview of all parameters in Table B.1.

The search space spanned by the 23 parameters is too large for a reasonable exhaustive search.If there are $x \in \mathbb{N}$ values for each parameter $p_{i=1,\ldots,N_{\text{param}}} \in P$, there are $x^{N_{\text{param}}}$ different parameter combinations. Even a small value for x, and therefore a strong quantization of the parameter value range, leads to large search spaces: with the MCC parameter cardinality of $N_{\text{param}} = |P| = 23$ and $x = 5$ we have $5^{23} \geq 10^{16}$ possible combinations, if no limitations are assumed for the parameter selection. Since every parameter set P needs to

be evaluated, e.g. according to Equation B.3, this leads to infeasible search times. However this approach will return the globally best parameter set for the training data.

The other naive approach, is to optimize each parameter independently of the others, which relates to a greedy search where local optima are chosen with the goal to find a global optimum. Unfortunately the assumption that the parameters are independent from each other is not necessary given here. To give an example, it is unlikely that the parameters that influence the generation of the templates are independent from the comparison parameters. In consequence the solution can be found efficiently, but it is most likely not finding the globally best solution.

Our approach to this optimization problem is to utilize the principles of Genetic Algorithms (GA) to find reasonable parameters for the MCC algorithm on the vein data. In the next section we are introducing the basics and the specific design for this designated problem.

Parameter	**Description**
R	Cylinder radius (in pixel)
N_S	Number of cells along the cylinder sections
N_D	Number of cylinder section
σ_S	Standard deviation in Gaussian for spatial contribution
σ_D	Standard deviation in Gaussian for directional contribution
μ_Ψ, τ_Ψ	Sigmoid parameter for function Ψ
Ω	Offset applied to enlarge the convex hull (in pixel)
$\min_{VC}$	Minimum number of valid cells for a cylinder to be valid (fraction of max number)
$\min_M$	Minimum number of minutiae for a cylinder to be valid
$\min_{ME}$	Minimum number of matching elements in two matchable cylinders (fraction of max number)
σ_Θ	Maximum global rotation allowed between two templates
μ_P, τ_P	Sigmoid parameters for LSS technique
$\min_{n_p}, \max_{n_p}$	Minimum and maximum number of minutiae in LSS
w_R	Weight parameter for LSS relaxation
μ_1^ρ, τ_1^ρ	Sigmoid parameters for d_1
μ_2^ρ, τ_2^ρ	Sigmoid parameters for d_2
μ_3^ρ, τ_3^ρ	Sigmoid parameters for d_3
n_{rel}	Number of relaxation iterations for LSS-R and LSA-R

Table B.1: Parameters of the MCC algorithm according to [22]. Separation between parameters for (i) template generation, (ii a) local comparison score computation and (ii b) global score composition.

B.4 Genetic Algorithms

Genetic algorithms (GA) are heuristic optimization or search strategies that are often used for problems where a solution cannot efficiently be computed. The basic principles are inspired from the natural evolution and from genetics – hence the name.

The idea is to create a population of candidate solutions for a problem and to select those individuals which comply best to a specified quality criteria (natural selection, survival of the fittest). The properties (genes) of the selected individuals are slightly modified (mutation) and recombined to generate a new generation of solutions (recombination/crossover).

The evaluation of GA is sometimes slow, but it improves the solutions from generation to generation until it converges without any knowledge about the problem itself. The design of a GA is specific to the application, the expert knowledge and problem description are encoded within the system. This is the crucial step for the effectiveness and efficiency. The main design decisions for the MCC parameter optimization are discussed in the next section.

B.5 GA MCC Parameter Optimization

Since the MCC, designed for fingerprints, uses minutiae locations and angles and this data is used for vein recognition already e.g. in [77, 78], we can apply it directly to vein data. However, the parameters of the algorithm might not fit the data. Therefore we decided to use GA as a search strategy to find optimal parameters in the vast search space for the MCC algorithm applied to vein data.

For the extend of this work, we restrict the optimization of the parameters to those 16 influencing the comparison behaviour of MCC (translating to the last two parameter groups (ii a) and (ii b) in Table B.1). The motivation for this decision is that the creation of templates takes space and computational time, which is restricting the iterations and population size of the genetic algorithm. In consequence the results may not be optimal and a re-consideration after the initial evaluation could be necessary. The design of the GA is described in this section.

B.5.1 How to represent genomes?

The genome of an individual is defined as a fixed-size array G of float values ranging in $[0, 1]$. Each element of the genome (gene $g_i \in G$) is coding exactly one parameter $p_i \in P$ of the MCC algorithm with $i = 1, ..., N_{\text{genes}}$. The order of the genes relates to the order of the parameters in Table B.1. It starts with parameter $p_1 := \min_{VC}$, as the first parameter coding the comparison part of MCC, and ends with $p_{16} := n_{\text{rel}}$.

The initialization of genomes G_s of the first population is done using a seeded random generator using parameter seed. Each element $g_i \in G_s$ for each individual s in the population with population size N_{pop} is assigned a random value within the defined range $[0, 1]$:

$$G_s := g_i, \forall s = 1, ..., N_{\text{pop}}, i = 1, ..., N_{\text{genes}}, \tag{B.4}$$

$$\text{with: } g_i := \text{rand}_{\text{seed}}([0, 1]), \tag{B.5}$$

and random generator rand that returns a value in $[0, 1]$.

The range $[0, 1]$ is equal for all genes to guarantee that mutations and recombinations are resulting in the same range. However, that indicates that genes cannot directly be utilized as parameters since they may have different ranges and may even be of different number

i	1	2	3	...	14	15	16
g_i	0.28	0.34	0.74	...	0.56	0.66	0.33
p_i	0.28	3	0.74	...	1.74	-28	4

Figure B.1: Sample genome with genes g_i and the parsed parameters p_i. Rounded to 2 digits after decimal point.

sets. E.g. parameters describe integer pixel values, whereas others describe angles in certain ranges. First, a definition of the number set a parameter belongs to, has to be defined. The two possibilities are:

$$\forall p_i \in P : p_i \in \mathbb{Z} \vee p_i \in \mathbb{R}. \tag{B.6}$$

A function $f : \mathbb{N} \rightarrow \{0, 1\}$ maps an index i into a binary value indicating the number set:

$$f(i) := \begin{cases} 0, \text{if } p_i \in \mathbb{Z} \\ 1, \text{if } p_i \in \mathbb{R} \end{cases}, \forall i = 1, ..., N_{\text{genes}}. \tag{B.7}$$

Secondly, upper ζ_i^U and lower boundaries ζ_i^L for each parameter $p_i \in P$ are defined:

$$\forall p_i \in P : \zeta_i^L \leq p_i \leq \zeta_i^U. \tag{B.8}$$

A parsing of the genes is performed based on Equations B.7 and B.8, only then the parameter set coded in the genome of an individual can be evaluated using the MCC algorithm. The parsing algorithm is a function $h : [0, 1] \times \mathbb{N} \rightarrow \mathbb{Z} \vee \mathbb{R}$, that maps a gene $g \in [0, 1]$ depending on the position in the genome $i \in 1, ..., N_{\text{genes}}$ to a parameter value $p \in \mathbb{Z} \vee \mathbb{R}$. The algorithm works as follows:

$$p_i = h(g_i, i) := \begin{cases} \text{rnd}(t(g_i, i)), \text{if } f(i) = 0 \\ t(g_i, i) \text{if } f(i) = 1 \end{cases} \tag{B.9}$$

$$\text{with} \quad t(g_i, i) := ((g_i | \zeta_i^U - \zeta_i^L|) + \zeta_i^L), \tag{B.10}$$

with rnd rounding a real value towards the closest integer number. Parsing a whole genome is equivalent to mapping all genes into their according parameter values, and it is defined as:

$$P = H(G) := h(g_i, i), \forall g_i \in G. \tag{B.11}$$

The selection of ζ_i^L and ζ_i^U is shown in Table B.2, it is based on the standard parameter p_i^{std} defined in [23]. In general, if not restricted otherwise, at least a range of $2p_i^{\text{std}}$ centered around p_i^{std} is defined as range for parameter p_i. An analysis of the best genomes after the simulation may reveal that the ranges have to be adapted. Example genomes and parameter sets are given in Figure B.1.

B.5.2 How to define the fitness function?

The fitness functions is the second key building block of the genetic algorithm. It defines a quality criteria based on the genome of an individual. High fitness results in a high probability of individuals for mating and therefore in maintaining (parts of) the genome for the next generation. Low quality results in a high probability for extinction of the genome which directly relates to Darwin's evolution theory of the natural world and the natural selection.

i	Parameter	p_i^{std}	Range (ζ_i^L, ζ_i^U)	$\in$
1	min_{VC}	$\frac{1}{5}$	$[0, 1]$	$\mathbb{R}$
2	min_{M}	1	$[0, 10]$	$\mathbb{Z}$
3	min_{ME}	$\frac{1}{5}$	$[0, 1]$	$\mathbb{R}$
4	σ_Θ	$\frac{3}{4}\pi$	$[0, 2\pi[$	$\mathbb{R}$
5	μ_P	30	$[0, 60]$	$\mathbb{R}$
6	τ_P	$\frac{2}{5}$	$[0, 5]$	$\mathbb{R}$
7	min_{n_p}	3	$[1, 5]$	$\mathbb{Z}$
8	max_{n_p}	10	$[\text{min}_{n_p} + 1, 15]$	$\mathbb{Z}$
9	w_R	$\frac{3}{10}$	$[0, 1]$	$\mathbb{R}$
10	μ_1^ρ	$\frac{1}{30}$	$[0, \pi[$	$\mathbb{R}$
11	τ_1^ρ	-150	$[-300, 0]$	$\mathbb{Z}$
12	μ_2^ρ	$\frac{\pi}{4}$	$[0, \pi[$	$\mathbb{R}$
13	τ_2^ρ	-15	$[-30, 0]$	$\mathbb{Z}$
14	μ_3^ρ	$\frac{\pi}{18}$	$[0, \pi[$	$\mathbb{R}$
15	τ_3^ρ	-40	$[-80, 0]$	$\mathbb{Z}$
16	n_{rel}	3	$[0, 10]$	$\mathbb{Z}$

Table B.2: Parameters boundaries for the MCC algorithm. Standard parameter p_i^{std} as in [23].

This method has the advantage that the functionality of the fitness function can be a black-box approach – no knowledge about the internals is needed. As long as the fitness function returns a fitness score for a given individual, the GA will find better and better solutions if possible and until convergence. In case of biometric systems the obvious singular value that can be utilized as a quality criteria and fitness value is the equal error rate. Since the rate should be minimized, the fitness function is defined according to Equations B.2 and B.11 as:

$$\mathcal{W}(G) := 1 - \text{EER}_{\text{MCC}}(H(G), T), \tag{B.12}$$

using minutiae training set T.

Evaluating the GA using the fitness function leads to increasing values for $\mathcal{W}$ and therefore decreasing values for the equal error rate: the search problem of Equation B.3 is encoded in the GA.

In some cases, the selection of parameters leads to extremely small genuine comparison scores. This makes not only the EER computation costly, but also only a fraction of the normalized score range $[0, 1]$ of the MCC algorithm is utilized. Average genuine score values smaller than 10^{-8} are punished with a fitness score of 0.

Alternatively, additional statistical information about the genuine and imposter comparisons can be incorporated into the fitness function. Also an optimization for minimal computational effort can be incorporated, e.g. when low values for parameter σ_Θ are chosen, that control the maximum global rotation allowed between two templates.

B.5.3 How to choose the population size?

The larger the population size, the larger the genetic material of a population due to the random initialization for the first generation described in Section B.5.1. Since every individual is evaluated as described in Section B.5.2, and therefore comparable to one search in the search space, it is advantageous to choose a large population. It also directly influences the resulting best fitted solutions since recombination mixes the best genomes of the population. However, an evaluation takes time, a trade-off has to be found.

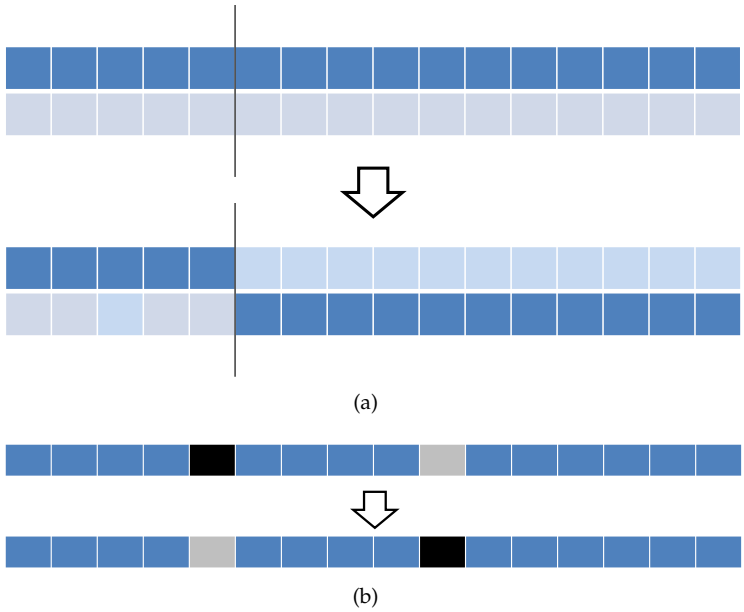
In the experiments the population size is chosen as $N_{\text{pop}} = 1000$.

B.5.4 How to generate the next generation?

The next generation of individuals is created using a mating probability according to the fitness function and according to the crossover and mutation operators describes next. The probabilities for crossover and mutation is set to $p(\text{cross}) = 0.8$ and $p(\text{mut}) = 0.05$.

B.5.5 How to define crossover/mutation operators?

Crossover is defined as a single point crossover, the mutations are defined as swappings of single genes. The application of the operators are depicted in Figures B.2(a) and B.2(b).



(a)

(b)

Figure B.2: Abstraction of the (a) single point crossover, (b) swap mutator operators of the GA.

B.5.6 How to define the stopping criteria?

Two stopping criteria are defined: (i) the number of generations is limited to 100 and (ii) a convergence rate of the best fitness score of 1 for 3 subsequent generations of the GA. The latter criteria translates to: if in three generations the best fitness score does not change, the algorithm terminates and reports accordingly this individual as best fitted and therefore its parameter interpretation as best set for the MCC algorithm on the training data.

B.6 Experimental Results

B.6.1 Implementation

For the GA system the *GAlib* library [232] is used. An MCC SDK was kindly supported by the authors of [22, 23]. The implementation languages for controlling GAlib and the MCC SDK are C respectively C++. Computation times for generating templates and for single comparisons using the MCC implementation are extremely fast (ms). However a large amount of comparisons is needed to get reliable fitness estimates for the GA subsystem.

B.6.2 Training Protocol

The minutiae points of all samples of the specific database are extracted according to the preprocessing introduced in [77]. As a first step, the minutiae information is encoded as MCC templates using the standard parameters as introduced in [23].

In the second phase the parameter optimization is performed. For this we introduce the rate of biometric samples of the hole dataset that are considered for the training phase as $R_{\text{train}} = 0.25$. The MCC templates are chosen from the first file of the database until the rate is reached, in this way the maximal possible genuine as well as imposter scores of the selected samples are generated. A random selection may lead to an insufficient amount of genuine comparisons: all datasets feature a limited amount of captures for a biometric source (Table B.3). The remaining templates are used as the testing data set.

The GA is set up according to Section B.5. For each call of the fitness function, an evaluation using the MCC SDK is launched using the parameters encoded in the genome.

B.6.3 Databases

Table B.3 summarizes the main characteristics of the datasets. The three sets cover different capturing wavelengths (near and far infrared), as well as different vein modalities (palm dorsal and wrist vein images), therefor providing a broad basis for conclusions about the proposed method for adapting the MCC algorithm to vein data.

The *SNIR* and *SFIR* databases were gathered in 2006 in Singapores Nanyang Technological University and contain a subset of samples that were used in several publications [240, 242]. The two parts contain 732 back hand vein samples in the near infrared and 173 in the far infrared spectrum from 122 respectively 34 data subjects. For comparison purposes the labeling-failure corrected version of SFIR, *SFIR-GT*, is used here.

The third database used for the experiment is referred to as *UC3M* [171]. It was collected in 2010 in the University Carlos III of Madrid. The dataset consists of 348 vein images in the near infrared spectrum from the wrist areas of 29 data subjects. The dataset was taken under different illumination intensities to optimize the capturing device and does not reflect an operational database.

One limitation of the datasets is that they were captured during only one session, which limits the variability in the signals. In addition the sizes of the databases limit the significance of the results. Example raw images are given in Figures B.3(a), B.3(b) and B.3(c). Statistical information regarding the number of extracted minutiae, as well as the skeletons are summarized in Table B.3.

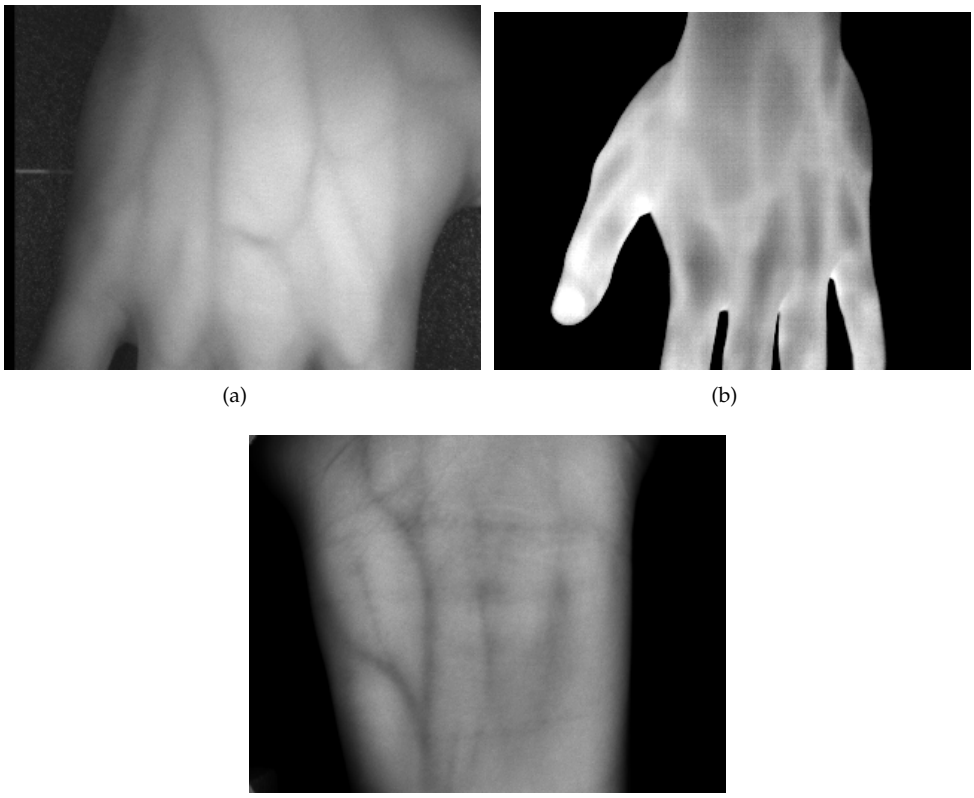
B.6.4 Best Individuals

For the extend of the paper the best individuals (MCC parameter configurations) for the experimental datasets are given in Table B.4. The individuals with best fitness score (1% of all individuals) are evaluated on the testing data and the best parameter set is given. In addition an evaluation using the standard MCC-parameters on the testing data is provided.

The biometric performance of the MCC algorithm with the defined standard parameter [23], is low for the SNIR and SFIR-GT data (2.06%/3.15% EER) and excelent for the UC3M data (0.31% EER). In the first two cases the equal error rate is reduced to 1.45% respectively 1.88% using the parameters optimization procedure introduced in this paper. However, in case of the UC3M data the excellent performance is maintained.

B.7 Discussions

In case of the UC3M data, many genomes were evaluated with the same maximum score of 0.999858. However, their performance on the testing data differed significantly. Also the distribution of parameters for this data set of individuals differs, further investigation is



(a) (b)

(c)

Figure B.3: Sample raw images of the datasets (a) SNIR, (b) SFIR, (c) UC3M.

Property	**SNIR**	**SFIR-GT**	**UC3M**
Frequency Band	NIR	FIR	NIR
Modality	Dorsal hand (2)	Dorsal hand (2)	Wrist (2)
Data Subjects	122	34	29
Sessions	1	1	1
Images per Session	2×3	$2\times \sim 3$	2×6
Images	732	173	348
Genuine Comparisons	732	170	870
Imposter Comparisons	266814	14708	59508
Resolution (px)	$(644 \times 492)^{\perp}$	320×240	$(640 \times 480)^{\perp}$
Depth	8 bit	8 bit	8 bit
Bifurcations	56.93	28.82	87.21
Endpoints	16.42	18.32	62.01
Skeleton length (px)	3146.23	2157.4	3594.62

Table B.3: Properties and statistics of the biometric vein datasets. $^{\perp}$Image size reduced by 50% in each spatial dimension for experiments.

Parameter	P_{std}	**SNIR**	**SFIR-GT**	**UC3M**
min_{VC}	$\frac{1}{5}$	0.84	0.84	0.48
min_{M}	1	9	9	3
min_{ME}	$\frac{1}{5}$	0.42	0.25	0.04
σ_{Θ}	$\frac{3}{4}\pi$	0.58	0.58	3.07
μ_P	30	28.53	28.53	23.86
τ_P	$\frac{2}{5}$	4.89	4.89	2.04
min_{n_p}	3	4	4	4
max_{n_p}	10	8	9	6
w_R	$\frac{3}{10}$	0.32	0.32	0.33
μ_1^ρ	$\frac{1}{30}$	0.02	0.02	0.04
τ_1^ρ	-150	-213	-213	-199
μ_2^ρ	$\frac{\pi}{4}$	1.07	1.07	2.62
τ_2^ρ	-15	-28	-28	-26
μ_3^ρ	$\frac{\pi}{18}$	0.12	0.12	0.09
τ_3^ρ	-40	-15	-15	-76
n_{rel}	3	4	5	3
Performance with P^1_{std}		2.06%	3.15%	0.31%
Fitness score		0.9805	0.9623	0.9999
Performance with P^2_{opt}		1.45%	1.88%	0.31%
Improvement		29.61%	40.32%	0%

Table B.4: Best parameters after evaluation of the GA. Performance measured in EER on the testing data. [1]Standard parameter as in [23]. [2]Optimized parameters according to this table.

needed. It may be caused by the limited size of the data set. Additional information for calculating the fitness function values could improve the results.

It can be useful to analyse the vast amount of tested parameters to eventually approximate the influence of all parameters on the performance and to find non-evaluated areas in the search space that may lead to even better biometric accuracy.

As can be seen from the evaluation, the standard parameter (chosen for fingerprint) perform surprisingly well on the vein data as well. In two cases the EER could even be improved with the GA parameter optimization. In one case, however, performance was not improved, and stayed constant. It is highly unlikely that the standard parameter set is the optimal one, considering the vast search space, a re-optimization of the parameter ranges centered around the best parameter sets and with a "higher resolution" could be one approach. Alternatively the population size of the GA can be adapted, which requires additional computational time.

The optimal parameter sets for the three vein datasets differ. However, a high correlation between parameters for SNIR and SFIR-GT data are visible with identical parameters for p_i with $i = \{1, 2, 4, 5, 6, 7, 9, 10, 11, 12, 13, 14, 15\}$. Also a correlation with the parameters of the UC3M data is evident for $i = \{5, 7, 9, 10, 11, 13, 14\}$ as can be seen in Table B.4.

If the performance results of the MCC algorithm are compared to Spectral Minutiae (SM) [77, 78] on the same data, the following observations can be noted: SM performs better on SNIR (0.41% vs. 1.45% EER) and SFIR-GT data (0.06% vs. 1.88% EER); MCC outperforms SM significantly on UC3M data (4.37% vs. 0.31% EER), MCC even outperforms the state-of-the-art Similarity-based Mix-matching algorithm (SMM) [30].

B.8 Conclusions and Future Work

Parameter optimization is a challenge, especially in high-dimensional search spaces. The proposed GA-based solution finds parameter sets that improve the biometric performance (EER) up to 40% compared to the standard parameter set. This result is promising and the proposed GA parameter optimization can be utilized for all parametrized biometric algorithms.

All hypotheses of Section B.3.3 could be falsified: performance of optimized parameter sets compared to the reference parameter set was at least at the same level if not improved (**H1**). Optimized parameter sets differ for the different vein datasets. However, the difference between SNIR and SFIR-GT parameters is marginal and a correlation of some parameters can be identified (**H2**). State-of-the-art algorithm performance could be reached for the UC3M data (**H3**).

As future work, the mapping function (genome to parameter) needs to be reconsidered. Additional information should be utilized for the fitness function, instead of focusing on the EER only. Also involving the parameters controlling the template creation is planned. As a next step, the MCC standard parameters for the fingerprint verification challenge *FVC-onGoing* will be re-optimized.

Appendix C

Entropy Estimator and Formal Model for Vascular Skeletons[1]

Abstract

Currently biometric systems are evaluated using performance measures like the equal error rate in database comparisons. The biometric performance can give an indication how good a certain system is suited to handle the biometric samples. However, there are more factors of reasoning: test data and simulations are always limited and the performance does not give any insight in how discriminating the features from a certain source are in theory. In this paper we propose a model for vein skeletons and an entropy estimator on the skeletonized representation of the vein patterns to overcome the before mentioned limitations. The results are compared to information theoretical entropy estimations on a specific finger vein database.

C.1 Introduction

Modeling formally the structure of biometric samples of a specific modality is a challenging but useful approach to get further insight in the data. It enables researches to optimize the feature extraction algorithms and comparison strategies, to estimate the discriminating power. It points out theoretical boundaries for large-scale scenarios like the number of data subjects that can be distinguished, or it helps to configure cryptographic template protection schemes based on e.g. the fuzzy commitment scheme [18, 226] or biometric enhanced security protocols [72, 74]. Some work has been done to describe the entropy for distinguishing individuals [3] and statistical randomness properties of irises [42]. This work is focused on modeling skeletons of vein patterns and estimating their entropy.

The paper is organized as follows: a brief introduction to vein pattern recognition is given in the next section. The main contribution can be found in Section C.3, where the model and the estimator are described, followed by Section C.4 describing a finger vein database which will be used later in the experimental part in Section C.5. There, the model is applied to the test database before the paper is concluded.

C.2 Vein Pattern Recognition

Vein pattern recognition has particular properties which makes it an interesting research area in the field of biometrics. This section introduces the physiological modality and discusses the applicability according to the following requirements:

- Universality - characteristic is available at every data subject.
- Uniqueness - biometric trait differs for different sources.
- Permanence - variance over time.

[1] [70] HARTUNG, D. Entropy estimator and formal model for vascular skeletons. In Biometric Measurements and Systems for Security and Medical Applications(BIOMS), 2011 IEEE Workshop on (September 2011), pp. 1-5.

- Collectability - ease of acquisition process.
- Performance - accuracy of decisions (biometric performance), decision delay and throughput (physical performance).
- Acceptability - degree of objections of population.
- Circumvention - ease of spoofing the system or successfully faking the biometric.

Vein patterns evolve during the embryonic vasclogenesis and their final structure is mostly influenced by random factors [52]. Even identical twins can be distinguished. The pattern is available and can be read from every healthy human.

Commercial applications evolved out of this research, nowadays many ATMs in Japan and Brazil are secured using this biometric modality, commercial sensors are available. With the upcoming changes of the liability situation in the Single Euro Payments Area (SEPA) it is likely that this biometric technology will also be widespread in Europe.

The patterns are commonly extracted from images of the palm, the back of the hand or fingers as seen in Figure C.1, also the wrist area can be used [171]. Yanagawa et al. showed that the diversity of finger vein patterns among different persons is competitive to iris-based systems [269]. The International Biometrics Group (IBG) 6th report 2006 confirms recognition rates fairly at the same level for two different vein and one iris-based authentication system [94]. An interesting aspect of vein recognition is the fact that the information is not visible, it is hidden inside the body. Unlike fingerprints it is not possible to leave a vein pattern representation unintentionally in public places and thus it is not possible for an attacker to acquire the pattern in daily life or to replicate it. Furthermore there is no relation to criminal prosecution, which is an argument for its acceptance in biometric systems.

Permanence of vein patterns is not studied in large scale since the research on this modality is relatively young. For now the vendors claim liveness detection mechanisms, on which there is no publicly available information. So far those sensors could not be spoofed, if an enrolment using the true biometric source was performed.

The imaging approach makes use of the absorption capacity of particular substances in the blood running through the veins. To capture the image, the region of interest is illuminated with a near-infrared (NIR) light source with wavelengths around 700 to 1,000 nm. A reflection or transmission technique can be used. Deoxygenized hemoglobin highly absorbs rays within this wavelength band while the surrounding tissue does not. NIR-sensitive optical sensors are used to capture the image of the vein pattern. Examples are shown in Figure C.1.

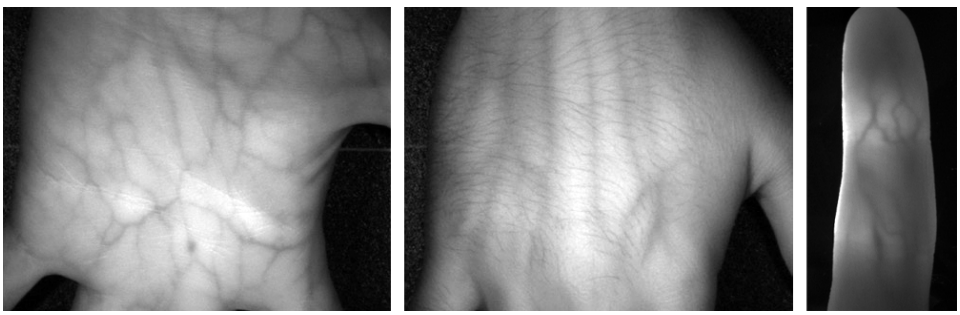


Figure C.1: Near infrared examples for vein pattern images taken from the palm, backhand [241] and finger [81].

C.3 Vein Model and Entropy Estimation

In this section a skeletal vein model is proposed and a entropy estimation is given for that model.

C.3.1 Entropy Estimation

The amount of information – or entropy – H, that can be extracted from K occurrences, each having the probability p_i with $i = 1, 2, ..., K$ can be computed using the Shannon-Entropy:

$$H = -\sum_{i=1}^{K} p_i \cdot log2(p_i), \tag{C.1}$$

In praxis the probabilities are not known, the concept of the maximum-likelihood estimator $\hat{p}_i$, that estimates the probabilities by using absolute frequencies n_i over N observations, can help out. Where occurrence i is approximated with: $\hat{p}_i = n_i/N$. The resulting formula is given by:

$$\hat{H} = -\sum_{i=1}^{N} \hat{p}_i \cdot log2(\hat{p}_i) \tag{C.2}$$

It will be used in Section C.5 to estimate the entropy for the test database.

C.3.2 Skeletal Model

In order to refine the entropy estimation we propose a model for the skeletonized form – where the structure of the vein pattern is reduced to a 1-pixel wide and 8-connected mesh representing the topology of the original data. The model is based on the following information of the data:

- P_x: Image size (pixel) in horizontal direction (in finger vein images: from finger root to finger tip)
- P_y: Image size (pixel) in vertical direction
- P: Number of pixels in the image ($P = P_x \times P_y$)
- P_{null}: Number of elements always classified as background
- P_{skel}: Average number of pixels describing the skeletal pattern
- N_{end}: Average number of endpoints
- N_{bra}: Average number of branch points
- N_d: Number of possible directions to a neighbor in the skeleton
- A_r: Average rate of angle changes in the skeleton
- A_c: Average change in the angles

The model is discussed and elaborated in detail during this subsection.

Starting with the idea that the amount S of different binary images I_{Skl} of size $P = P_x \times P_y$ – considering that there are P_{null} pixels which are always zero and therefore classified as background and not as vein, and that P_{skel} belong to a skeleton (are equal to one or are "active"), and that the pixels are independent from each other – can be expressed as:

$$S = \binom{P - P_{\text{null}}}{P_{\text{skel}}}. \tag{C.3}$$

This amount is tremendously large and not reflecting the nature of the vein patterns in detail.

If the vein skeletal structure is completely connected (not necessarily given in practice), the possible unique structures would be a tiny subset of the before mentioned expression from Equation C.3. If we consider a 8-connected structure of the skeleton (guaranteed by the skeletonization algorithm), the possible combinations could be approximated by:

$$S = (P - P_{\text{null}}) \cdot N_d^{(P_{\text{skel}})}, \tag{C.4}$$

assuming a given random start pixel and N_d positions in the 8-connected grid that the vein structure can follow for each of the following pixels, which is equal to 5 in a 8-connected structure for all but the starting, end point of a skeleton part or pixels at the borders of the image. Again this model is simplified, but it does consider bifurcation points – when the vein structure splits into two branches – it could loop, since the direction is chosen freely. But it could also visit the same location more than once.

To further analyze the amount of possible unique vein structures the amount of endpoints N_{end} is considered as well. If the vein segments between endpoints are of equal length we can approximate the possible unique structures with:

$$S = a \cdot (N_d)^b, \tag{C.5}$$

with

$$a = ((P - P_{\text{null}})! - (P - P_{\text{null}} - (N_{\text{end}}/2))!), \tag{C.6}$$

and

$$b = (P_{\text{skel}} - (N_{\text{end}}/2))/(N_{\text{end}}/2). \tag{C.7}$$

Considering a possible positions for $N_{\text{end}}/2$ start points resulting in sub vein patterns of length b.

The direction changes should also be considered, therefore we introduce A_r for the rate in percentage that an angle is changed and A_c for the actual average change in directions from the direction of the pre-visited pixel, which is zero for an unchanged direction, one for a one pixel change and two for the maximal change in direction. The estimation of the amount of possible vein patterns is then described by:

$$S = a \cdot c^b, \tag{C.8}$$

with

$$c = (1 - A_r) + (A_r \cdot 2A_c). \tag{C.9}$$

In the equation, $(1 - A_r)$ describes the case of no change of direction and $A_r \cdot 2A_c$ stands for the average changes in directions.

Database	GUC45
Frequency Band	NIR (850nm)
Sensor	non-commercial
Modality	Finger (10)
Data Subjects	45
Sessions	12
Images per Session	10×2
Images	10800
Resolution (px)	$512 \times 240^{\dagger}$
Depth	8 Bit gray-scale

Table C.1: Properties of the biometric vein dataset used for the entropy estimation. †For the experiment the images are cropped to size 401×111 pixel to eliminate most non-finger area.

C.4 Database

For the entropy estimation we use the database *GUC45*. Their main properties are summarized in Table C.1. The images contained in the finger vein database were collected from 45 subjects in 12 sessions at Gjøvik University College in Norway. Each finger was captured twice during each session, which results in 10800 unique vein images in total. The sensor used for gathering the finger vein data employed the transmission method [81]. It is composed of a CCD camera and an array of near infrared LED operating at a wavelength of 850nm. Because of the open structure, not only the light emitted by the LED but also ambient light reaches the sensor. Due to different size of the fingers the amount of ambient light and therefore the overall lightning is uneven among different fingers and users.

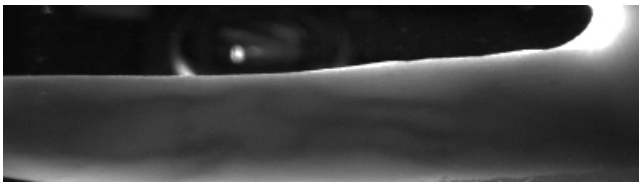
One example for a cropped raw image can be seen in Figure C.2(a). Its contrast is optimized using the STRESS algorithm [120], which uses a stochastic sampling strategy in the vicinity of each pixel to adapt its gray value to boost the local contrast (Figure C.2(b)). After this step the optimized image is segmented using a Laplacian of Gaussian approach, the outcome is shown in Figure C.2(c). To further remove unnecessary data, a skeletonization is applied using the algorithm from [133], also implemented in MATLAB as *bwmorph* with the *"thin"* option, the resulting image is shown in Figure C.2(d).

C.5 Experiment

In GUC45 the average entropy of each of the 111×401 components in the skeletal vein image database is approx. 0.199, which leads to a summed entropy of 8853.3 bits for one sample. That means according to a naive estimator approximately 8853.3 bits of information can be extracted in average from one processed vein pattern image.

Extracting the coordinates from the end and branch points from the skeletons using a fast convolution based approach [166], made it possible also estimate the entropy for this representation. Average entropy for the bi- and multifications is around 376 bits, the estimated entropy for the endpoints is slightly higher with approximately 416 bits. The results are summarized in Table C.2.

Each input image has a size of $P = P_x \times P_y = 401 \times 111 = 44511$ px and an average skeleton coverage of 3.47% of the image, which corresponds to approximately $P_{\text{skel}} = 1544$ pixels. $P_{\text{null}} = 3728$ pixels of the images are never active over all samples, the average active pixel is active appriximately 442 times with a standard deviation of 409 in the database of 10800 images originating from 45 datasubjects finger vein patterns (with 24 images per finger). The average amount of endpoints N_{end} in the database following the preprocess-



(a) Raw, cropped vein image I_{Raw}.

(b) Contrast enhanced image I_{Opt}.

(c) Segmentation of a vein pattern image I_{Seg}.

(d) Skeletonization of segmented image I_{Skl}.

Representation	**Average Entropy (bits)**
Skeletal Pattern	8853.3
Branch points	376.4254
End points	416.5209

Table C.2: Average entropy estimation for the different representations of the GUC45 finger vein data.

Property	GUC45
P_x	401
P_y	111
P	44511
P_{null}	3728
P_{skel}	1544
N_{end}	38.1746
N_{bra}	35.6757
N_d	5
A_r	0.3324
A_c	1.1639

Table C.3: Model properties for the GUC45 finger vein data.

ing described in Section C.4 is equal to approximately 38. The properties are listed in Table C.3, with the information about the direction changes, the estimator from Equation C.8 is applied here.

The Equation C.8 is then equal to:

$$S = a \cdot c^{((1544-(38.1746/2))/(38.1746/2))}$$

with

$$a = ((44511 - 3728)! - (4451 - 3728 - 38.1746/2))!)$$

and

$$c = (1 - 0.3324) + (0.3324 \cdot 2 \cdot 1.1639) = 1.4415$$

This leads to the following approximations:

$$\begin{aligned} S &= (40783! - 40764!) \cdot 1.4415^{79.89148} \\ &= 3.95624 \cdot 10^{87} \cdot 1.4415^{185.50227} \\ &= 1.142256 \cdot 10^{117} \approx 2^{388.8574} \end{aligned}$$

The model shows an entropy of approx. 388 bits for the GUC45 database in the model; not considering the angle information the entropy is estimated to approx. 476 bits. The modeled entropy is more close to the entropy measured for the minutiae points as can be seen in Table C.2, but not correspondent to the naive information theoretical estimated entropy, that is not considering correlations between the pixels.

C.6 Conclusions

We proposed a model for vein patterns skeletons. With this model the average entropy of a database can be estimated using statistical information about the vein pattern skeletons. We designed the model to be as generic as possible allowing to be applied to vein data gathered from various locations like the finger, the palm, the wrist or the back hand. The model is applied to the GUC45 database and a discrepancy between the estimated information theoretical entropy and the entropy estimated with the model is seen.

The model is describing the information in the finger vein skeletons more strict than the naive entropy estimation from Section C.3.1, since correlations between the pixels are considered. At the current state it does not contain any descriptors for noise in the image due to sensor noise, environmental changes and changes in the biometric characteristic as well as noise introduced by the contrast enhancement, segmentation and skeletonization

process. The model is aimed at describing the distinct information – maybe best described as biometric entropy — usable to distinguish individuals. It can be used to limit the information that is extracted from the vein pattern in the context of crypto-based template protection mechanisms like the approach in [226].

The model also allows to generate artificial vein skeletal patterns that correspond to the statistical properties of a training database. In that way large scale databases could be generated with little effort, with the additional bonus of avoiding privacy issues. Those databases could be used for the optimization of feature extraction algorithms or comparison strategies based on the skeletal representation.

In addition the entropy of different databases of the same vein modality or datasets containing different modalities (finger, hand, wrist or dorsal hand data) can be compared against each other.

Some question for the future work: How to consider noise issues in the model? How can information about line segments be used to overcome certain approximations in the model? How does the quality of the pre-processing correlates with the estimated entropy? Finally the stability of the features: what is the correlation between biometric performance and the entropy estimator.

Appendix D

Towards a Biometric Random Number Generator – A General Approach For True Random Extraction From Biometric Samples[1]

Abstract

Biometric systems are per definition used to identify individuals or verify an identity claim – one difficulty of getting reliable decisions is the inherent noise that makes it difficult to extract stable features from biometric data. This paper describes how biometric samples can be used to generate strong random numbers which form the basis of many security protocols. Independent from the biometric modality, the only requirement of the proposed solution are feature vectors of fixed length and structure. Each element of such a feature vector is analyzed for its reliability – only unreliable positions, that cannot be reproduced coherently from one source, are extracted as bits to form the final random bit sequences. Optionally a strong hash-based random extraction can be used. The practicability is shown testing vascular patterns against the NIST-recommended test suite for random number generators.

D.1 Introduction

One observation with biometric systems is that they deal with noisy physiological or behavioral data. Another observation is that the extraction of reliable features, which allows to discriminate between imposter and genuine attempts, is usually a non-trivial and difficult task. Both observations contribute to the motivation of this work. The common strategy in a biometric system is to extract a compact representation that includes only the most stable, reliable and distinctive information from the raw sensorial data.

On the other hand cryptographic protocols are used more and more widely in nowadays every-day applications as e.g. authentication in online banking. One major building block of those protocols is the proof of freshness. Such a proof is usually done by inserting a cryptographic nonce – a freshly generated random number that is only used once – in a message, which makes a simple message replay detectable. Such random numbers have to be unpredictable for an attacker in order to not compromise the whole protocol. Therefore strong random number generators are needed. The sources of true randomness are often physical processes while randomness from deterministic and highly non-chaotic systems like computers is often very limited. One example of a security protocol using a biometric transaction authentication with the need for strong random numbers for enrolment is the BTAP [72, 74].

In this paper, we present and evaluate the idea to use physical, biometric data to generate strong random numbers. This paper investigates how to combine biometric feature extraction and random number generation , how to generate the random numbers and how to verify the claimed randomness properties. Simulation results are presented before the paper concludes.

[1] [80] HARTUNG, D., WOLD, K., GRAFFI, K., AND PETROVIC, S. Towards a biometric random number generator - a general approach for true random extraction from biometric samples. In BIOSIG (2011), pp. 267-274.

D.1.1 Noise and Biometrics

Noise is inherently existent in biometric data – data from alive individuals. The term biometric noise is not yet clearly defined and it is often used to describe the variability in the signals due to changes in the biometric (e.g. dirty or torn off finger tips in fingerprint systems, different hair style in face recognition systems), inaccuracies of the sensorial subsystem (e.g. camera noise, dust on fingerprint sensor, pose towards camera), or varying environmental conditions (e.g. lighting, humidity). Here, we use these variations and the noise to generate random sequences.

D.1.2 Vein Patterns

Vein patterns evolve during the embryonic vasculogenesis and their final structure is mostly influenced by random factors [52]. Even identical twins can be distinguished. The pattern is available at every healthy human, making it an interesting research objective. Commercial applications evolved out of this research, nowadays many ATMs in Japan and Brazil are secured using this biometric modality. The patterns are commonly extracted from images of the palm, the back of the hand or fingers. The International Biometrics Group (IBG) 6th report 2006 confirms recognition rates fairly at the same level for two different vein and one iris-based authentication system [94]. An interesting aspect of vein recognition is the fact that the information is not visible, it is hidden inside the body. Unlike fingerprints it is not possible to leave a vein pattern representation unintentionally in public places and thus it is not possible for an attacker to acquire the pattern in daily life or to replicate it. Furthermore there is no relation to criminal prosecution.

The imaging approach makes use of the absorption capacity of particular substances in the blood running through the veins. To capture the image, the region of interest is illuminated with a near-infrared (NIR) light source with wavelengths around 700 to 1,000 nm. A reflection or transmission technique can be used. Deoxygenized hemoglobin highly absorbs rays within this wavelength band while the surrounding tissue does not. NIR-sensitive optical sensors are used to capture the image of the vein pattern.

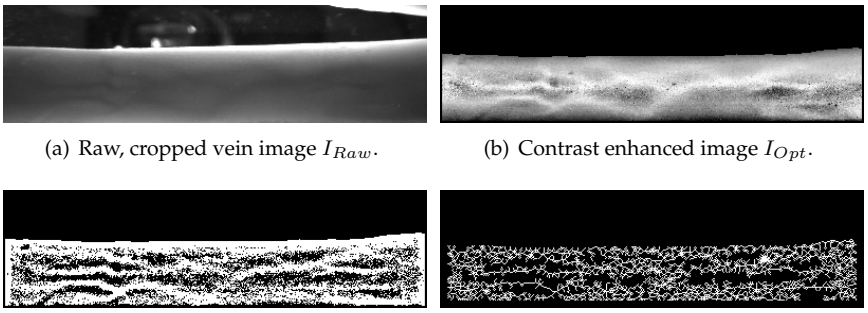
D.1.2.1 Feature Extraction Examples

The following images will be used during later stages of the random extraction: Figure D.1(a) shows an example vein pattern image and a STRESS [120] contrast enhanced version in Figure D.1(b), its segmented version in Figure D.1(c) produced using a local thresholding algorithm. The image is then transformed to a skeleton representing the topology of the vein pattern (Figure D.1(d)) by using morphological operators. The database consists of 10800 finger vein images from all 10 fingers of 45 data subjects acquired in 12 sessions, each image having a size of 111×401 pixels. Throughout the paper only the left middle fingers will be considered.

D.2 Biometric Random Number Generator

D.2.1 Random Number Generation

Random numbers have various important applications in computer science, from computer simulations, statistical sampling to cryptology. This section will describe some properties of randomness and the general classification into two distinctive classes: True random number generators (TRNG) are based on measurements of physical processes that are expected to be random like coin flipping, chemical processes including radioactive decay and atmospheric radio noise or processes based on quantum mechanics. Pseudo random number generators (PRNG) are based on deterministic computations where the output is predictable, but initialized with a true random seed or key makes the PRNG output difficult to predict.



(a) Raw, cropped vein image I_{Raw}.

(b) Contrast enhanced image I_{Opt}.

(c) Segmentation of a vein pattern image I_{Seg}.

(d) Skeletonization of segmented image I_{Skl}.

Figure D.1: A sample finger vein image and its representations within the pipeline. Note: an unstable segmentation and skeletonization method was chosen.

In order to verify the before mentioned and additional properties, statistical tests can be performed on random numbers. The NIST suite "A Statistical Test Suite for Random and Pseudo random Number Generators for Cryptographic Applications" based on [191] is a complete and commonly used test suite. It will be the basis for the evaluation of the generated random numbers in Section D.3.

D.2.2 State of the Art

Very limited work has yet been done on the field of biometric random generation. During the literature search only a hand full of papers was focusing on biometric random number generation. Often the terms were used incorrectly, in [26], the title indicated a random key generation from iris data, instead the extraction of non-random keys from the same biometric trait was discussed, related to a biometric key release or extraction. The research work in [123] was focusing on the sources of randomness in mobile devices, focusing on hardware sensorial noise from the camera or the microphone, not considering the use of the built-in sensors as sensors for biometric traits like voice or face recognition.

The work in [215], was closest to the scope of this paper. In there, the use of biometric data in the medical sense – in example animal neurophysical brain responses and human galvanic skin responses – were examined as sources of randomness. An approach was used, where physical measurement data was binarized and the last fluctuating digit was used as random bit sequence over time. Their true random generator passed successfully the NIST test suite as well as other statistical tests, whereas the brain signals come along with complex data measurement and the skin response did not show a sufficiently fast sampling rate.

Basis for the verification of the approach presented in this paper is a subsection of the database described in Section D.1.2.1.

D.2.3 Entropy Estimation

Entropy is an important measure in random number generators to estimate the quality of randomness. The amount of information – or entropy – H, that can be extracted from K occurrences, each having the probability p_i with $i = 1, 2, ..., K$ can be computed using the Shannon-Entropy:

$$H = -\sum_{i=1}^{K} p_i \cdot log_2(p_i), \tag{D.1}$$

Source	Entropy (bits)
I_{Raw}	25165
I_{Opt}	26930
I_{Seg}	19211
I_{Skl}	8003

Table D.1: Entropy estimation for the different stages of the pipeline.

In practice the probabilities are not known, the concept of the maximum-likelihood estimator $\hat{p_i}$, that estimates the probabilities by using absolute frequencies n_i over N observations, can help out. Where occurrence i is approximated with: $\hat{p_i} = n_i/N$. The resulting formula is given by:

$$\hat{H} = -\sum_{i=1}^{K} \hat{p_i} \cdot log_2(\hat{p_i}) \tag{D.2}$$

The entropy is estimated for our test database, the average entropy of the skeletal vein images is given in Table D.1, not considering the correlation between the single pixels. That means according to the estimator theoretically about that many bits of information can be extracted in average from one vein pattern image. A more refined estimation for the biometric entropy in finger vein images is currently under development and will be published soon.

D.2.4 Image Based Biometric Random Number Generation (BRNG)

Having discussed the motivation and requirements for a biometric random number generator, next, we present our approach for a BRNG. Data from different stages of a biometric pipeline are used as input to the proposed BRNG. The generic approach only requires a fixed length and a fixed structure of the feature vector. Here we will use images from the vein patterns, every other kind of features would also work. In order to find the most appropriate stage of the feature vector, first the raw image itself (I_{Raw}), followed by an enhanced and contrast optimized image is taken into account (I_{Opt}). After that the segmented and binarized representation (I_{Seg}) is considered as well as the skeletonized version (I_{Skl}).

The idea is that lower level features (in earlier stages of the pipeline) yield higher degrees of noise e.g. from the sensor, and recent work shows that using the Photo-Response Non-Uniformity (PRNU) of sample images the imaging sensors can be distinguished [57]. The randomness in higher level features is more and more based on the biometric information since unnecessary information is being removed during the preprocessing steps. One assumption is that these features have a better statistical quality and are more difficult to predict even though the amount of information in the images is reduced. The **hypothesis** that is tested later on: low level features produce lower quality random sequences than higher level features.

All real-valued feature vectors or images can be binarized using the interclass mean image ($\bar{I}$) of a training set (one / two dimensional case). One advantage of the binarization is that the amount of ones and zeros is approximately equal. The bit value $I^{Bin}(x, y)$ of every pixel $I(x, y)$ at position (x,y) in the source image I is computed as:

$$F^{Bin}(i) = \begin{cases} 0, & \text{if } F(i) < \overline{inter}(i) \\ \\ 1, & \text{if } F(i) \geq \overline{inter}(i) \end{cases} \tag{D.3}$$

Note the feature vector F is derived as concatenation from the image I's columns:

$$F = [I(1,1), I(2,1), \ldots, I(end,1), I(1,2), I(2,2), \ldots, I(end,2), \ldots, I(end,end)] \tag{D.4}$$

The binarized feature vector F^{Bin} is derived from I^{Bin} in the same way.

During the next step of the BRNG, every position in the feature vector F – which is defined in Equation D.4 – is analyzed for its reliability, meaning that single positions can be reproduced very accurately over many captures. The idea is based on work from Tuyls et al. [226], where the helper data scheme (HDS) is introduced that combines cryptography with biometrics to secure the privacy and the templates. Following this approach we could use the same mechanism used there to estimate the reliability of positions in the feature vector to estimate the inverse, the least reliable positions, and to use those bits for our random sequence. Using the inverse measure, we can select positions that are not reproduced accurately over many captures and that are being close to the mean value used for the binarization, resulting in random and flipping bits.

Reliability $R(i)$ (data subject specific) on position i of a fixed length and structured real-valued feature vector F, in the context of the HDS is estimated using the fraction of the inter-class var_{inter} and the intra-class var_{intra} variance:

$$R(i) = \frac{var_{inter}}{var_{intra}} = \frac{(F(i) - \overline{inter}(i))^2}{(F(i) - \overline{intra}(i))^2}, \tag{D.5}$$

using the mean value of the class $\overline{intra}$ (calculated from a fixed number of samples of the same biometric trait – called training set) and the mean value of the whole population $\overline{inter}$ (mean of all training sets together).

Here we introduce the unreliability measure:

$$U(i) = \frac{1}{R(i)}. \tag{D.6}$$

Border zones in the image that are always set to zero or one are resulting in high values for U, since they are very close to the inter class mean. Those positions are not interesting for the bit extraction since they are constant over the samples and occur in blocks, therefore $U(i)$ is set to zero for those positions.

In order to make an extraction of bits more efficient the indexing vector U_{idx} contains the indexes i sorted in descending order of $U(i)$.

A variable $\kappa < |F|$ is introduced to define the amount of unreliable bits that are to be extracted from and used for the random sequence Δ:

$$\Delta = [F(U_{idx}(1), F(U_{idx}(2)), \ldots, F(U_{idx}(\kappa))], \tag{D.7}$$

A further degree of freedom is given when using the help of a hash function h as a random extractor. Depending on the needed length of the random bit vector and the quality of randomness a variable λ is introduced splitting the random sequence Δ into k chunks C_i of length $\lfloor \kappa/\lambda \rfloor$. If λ is set to one, the whole sequence is used as input to a hash function, the larger it gets, the more chunks are created. Each chunk itself can be used to create a new hashvalue $h(C_i)$. The length of each chunk C_i should be larger or equal to the output length of the hash function.

$$\Delta_h = [h(C_1), h(C_2), \ldots, h(C_k)]. \Delta = \Delta \oplus \Delta^{-1}. \tag{D.8}$$

The final sequences Δ and Δ_h are xor-ed with its inverse order version to enhance the distribution of biased features, since mainly positions containing logical zeros are selected as most unreliable bits.

Source	κ	λ	Length Bitstream	# Bitstreams	Result
I_{Raw}	25165	x	135000	100	5.6%
I_{Raw}	25165	157	135000	100	87.9%
I_{Raw}	25165	78	67000	100	93.4%
I_{Opt}	26930	x	145000	100	69.3%
I_{Opt}	26930	168	145000	100	98.2%
I_{Opt}	26930	84	72000	100	98.2%
I_{Seg}	19211	x	100000	100	66.9%
I_{Seg}	19211	120	100000	100	98.1%
I_{Seg}	19211	60	50000	100	97.2%
I_{Skl}	8003	x	43000	100	1.4%
I_{Skl}	8003	50	43000	100	95.3%
I_{Skl}	8003	25	21000	100	97.9%

Table D.2: Experimental results of NIST test suite (standard parameters) applied to the random sequences extracted from the vein database. Hash function used: SHA-1. x = no hashing. Result: ratio of how many of the NIST tests successfully passed.

D.3 Simulations

The simulations cover the statistical test of NIST based on the data that was extracted as described in Section D.2.1. The database was divided into two distinct sets each containing 540 samples – 12 samples from 6 sessions of each of middle left finger of 45 data subjects: the odd numbered sessions are taking as training set and the even numbered ones for verification. In order to run the NIST test suite several Mbit of data are needed, therefore the resulting random sequences will be concatenated and presented to the test suite. The maximal amount of unreliable bits κ extracted from the various samples is set to the estimated entropy value from Table D.1.

D.3.1 NIST Results

The unreliable bits from the raw images are not qualified for the random extraction, but after a strong random extraction using a hash function very good NIST test results are achieved. With more than 95% of successfully passed tests, hashed unreliable bits from higher level features (I_{Opt}, I_{Seg} and I_{Skl}) are especially qualified. The amount of successfully passed tests is peaking with more than 98% for the hashed unreliable bits extracted from the optimized or segmented images (see Table D.2). Lower values for λ, resulting in bigger chunks as input for the hash function, are not effective to improve the random properties for higher level features.

D.4 Conclusions And Future Works

The results are quite diverse – on the one hand the pure unhashed versions of the data are not useful as a basis for BRNG, as they pass only a minor amount of the tests . On the other hand, good randomness properties are seen in case of the hashed version of all images, in particular higher level images.

The hypothesis cannot be verified; the quality of the random sequence extracted, measured in successful runs over the NIST test suite, is increasing from the raw level to the more abstract ones ($I_{Raw}, I_{Opt}, I_{Seg}$), but the skeletonized features pass only few of the NIST test if unhashed. The influence of hashing on passing the NIST test is too large to

claim the hypothesis that abstract biometric information offers a higher entropy and thus better randomness characteristics.

Future works will focus on an improved quality of random bits generated from one biometric sample and on the statistical properties. In addition future research will focus on a more sophisticated model for the biometric finger vein entropy estimation which may lead to quality metric for single samples as well as for capturing devices and feature extraction algorithms.

Appendix E

GUC45 Dataset

The GUC45 was gathered to have a solid data basis for the experimental work of the project. It was intended to be a multimodal database featuring finger vein, finger knuckle and to some extend fingerprint images. The period of data acquisition was around 15 weeks (late August - mid December 2009) split in 12 sessions, fingerprint acquisition was added for the last four sessions.

The setup of the data gathering is shown in Figure E.1, five different sensors were used: two self-built transmittance setups with CCDs, NIR pass-filters and LED illumination of 850 and 940nm wavelength (finger vein sensors 1 and 2), one finger knuckle sensor based on a Canon Powershot G9 and two commercial optical fingerprint sensors.

The procedure for each session was the following:

- Experiment 1: capture finger veins and finger knuckles on finger vein sensor 1 (almost simultaneously)
- Experiment 2: capture finger veins in a 90 degrees rotated way on finger vein sensor 1
- Experiment 3: capture finger veins on finger vein sensor 2 (video and extracted frames)
- Experiment 4: capture fingerprints with Cross Match L SCAN 100
- Experiment 5: capture fingerprints with Lumidigm V 100

Each capturing process was performed following the following protocol:

- 1st round: capture one sample from each finger according to order shown in Figure E.2
- 2nd round: repeat the same procedure again

The procedure led to two samples for each finger for each sensor in each session. Since 45 volunteers completed all 12 sessions, the resulting amount of data is $45 \times 10 \times 12 \times 2 = 10800$ images for experiments 2-3, in experiment 1 additionally 10800 finger knuckle images are captured. In experiment 3 also a video clip of the whole process is stored. Experiments 4 and 5 cover only 4 sessions and only 44 volunteers (one refused due to privacy concerns), summing up to each 3560 fingerprints. The main facts are summarized in Table 2.1.

During the enrolment and the final session additional measurements of the fingers were performed at points defined in Figure E.3 and two questionnaires about the volunteers physiological features (age, gender, nationality, handedness) and specific habits (smoking, snus, regular sports, type of work) were acquired. Also one calibration image of the palm dorsal was taken to be able to extract the skin color under controlled conditions.

During each session the following meta-data besides data and time was recorded: temperature (in/out), humidity and atmospheric pressure. The statistical information is addressed in the next section.

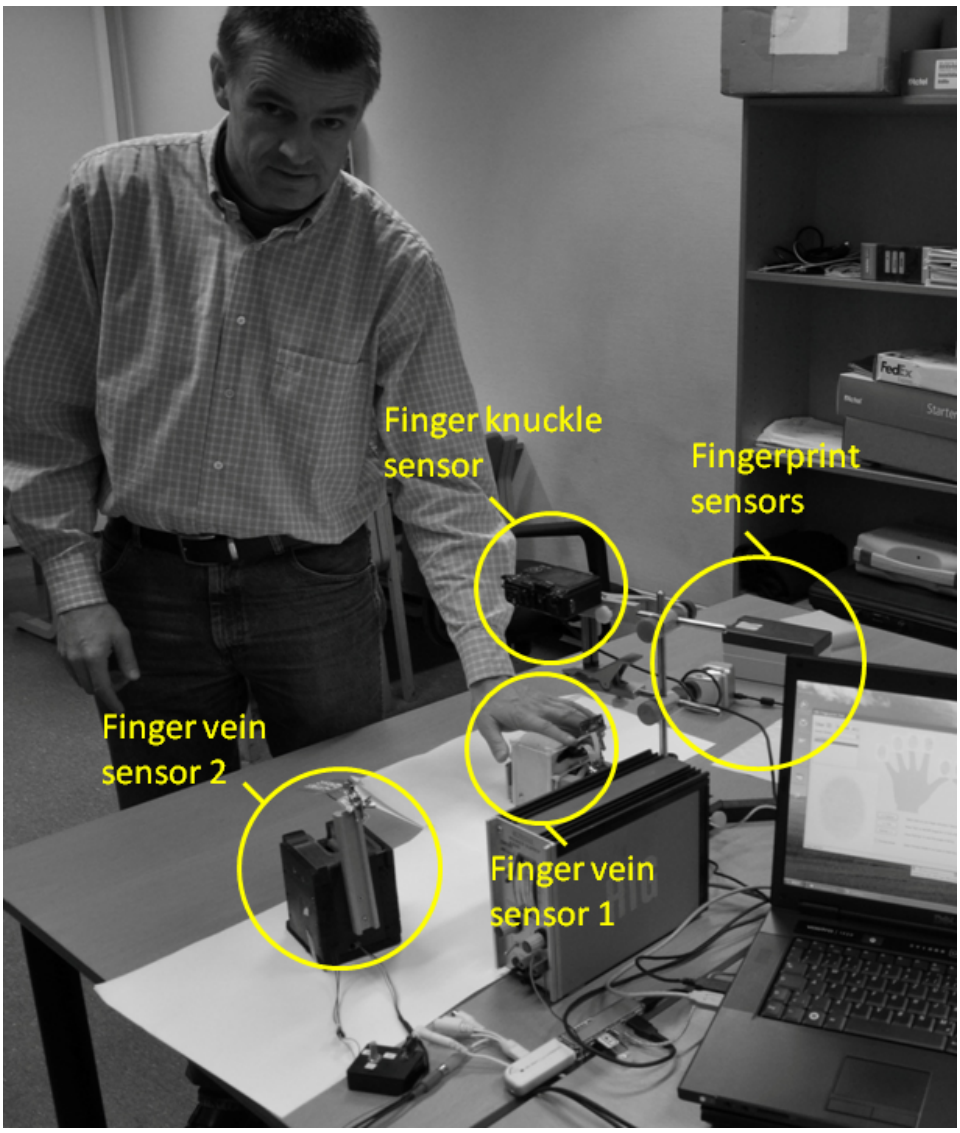


Figure E.1: GUC45 data acquisition setup.

E.1 Metadata Statistics

This section contains statistical information about the metadata describing the subjects, the fingers and session parameters of samples belonging to the GUC45 database. The statistics were generated in [148] and are extracted from Section 2.2 and Appendix B. First an overview is given in Tables and E.1 E.2 for the subjects respectively the session metadata. Details will be discussed in the following sections.

E.1.1 Subject Metadata

The subject properties are classified under different categories and displayed as bar charts. Figure E.4 displays the bar graphs of the number of subjects per gender, handedness, smokers, snus, sport, work and origin. Figure E.5 shows bar graphs of the number of subjects per age and per countries.

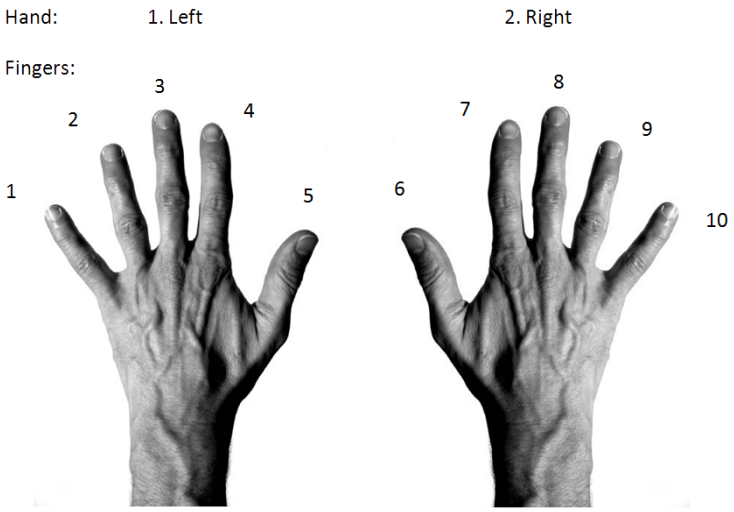


Figure E.2: GUC45 capturing order.

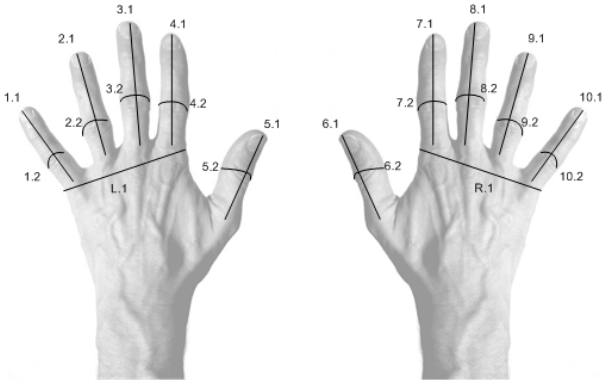


Figure E.3: GUC45 finger measurements.

Subject metadata		Total	Subject metadata		Total
Age range	[21-30[	18	Ethnicity	Asian	5
	[30-45[	14		Caucasian	37
	[45-66[	13		Indian	3
Gender	Male	35	Handedness	Left	6
	Female	10		Right	39
Smoker	Yes	7	Snus$^{d}agger$	Yes	3
	No	38		No	42
Sport	Regular	20	Work	Office	44
	Non-regular	25		Physical	1
Disease	Yes	-	Width and length of captured fingers		
	No	-	Height and weight of subjects		

Table E.1: Subject metadata of the GUC45 database. $^{d}agger$Snus is a moist tobacco powder especially consumed in Sweden and Norway.

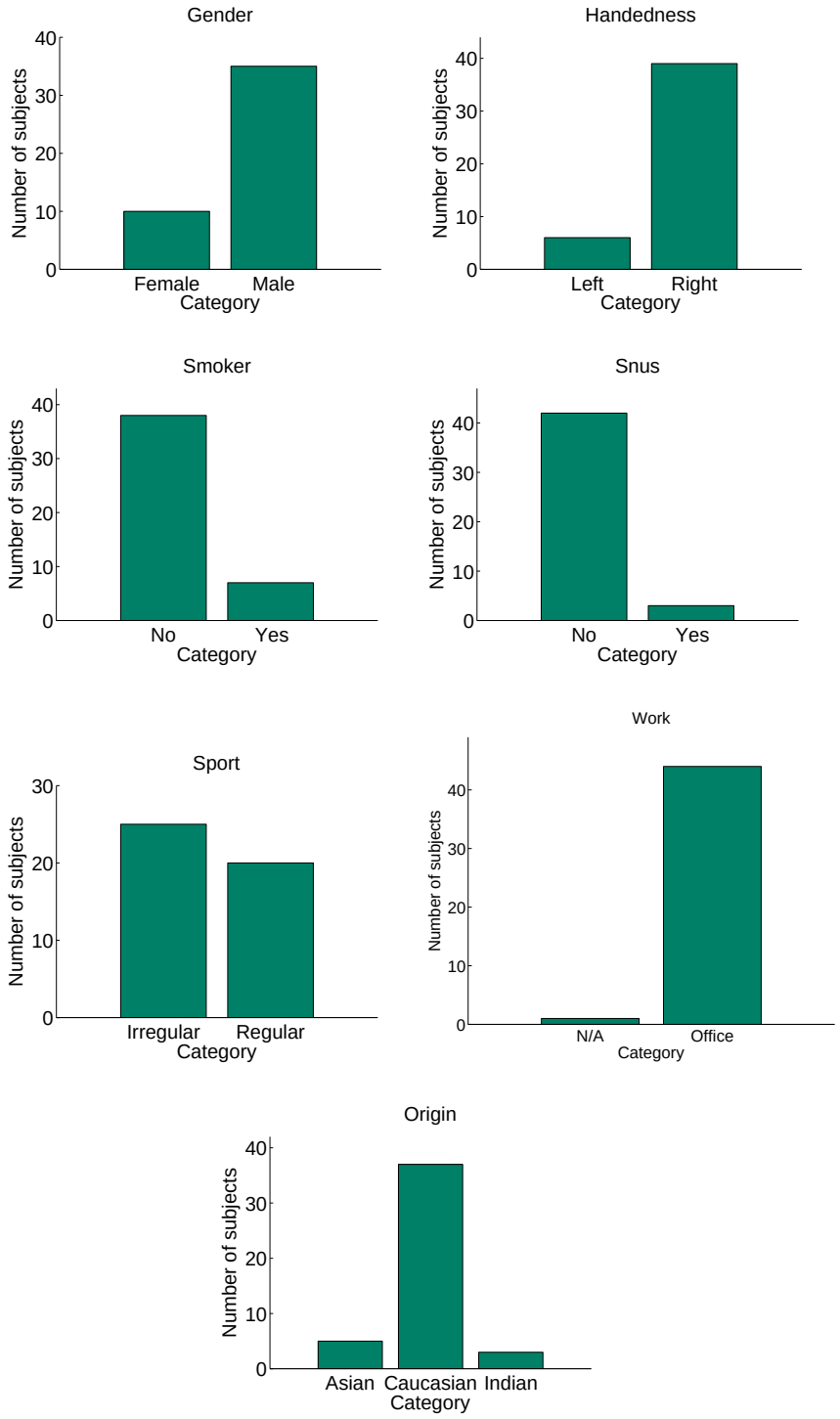


Figure E.4: Number of subjects for each category of the metadata (1/2).

Session metadata		Minimal	Maximal	Mean
Temperature in °C	Inside	18.5	28.5	23.3
	Outside	-10	26.5	6.4
Humidity in %	Inside	<15	61	28.1
	Outside	43	>95	81.4
Atmospheric pressure in hPa		968	1024	994.2

Table E.2: Session metadata of the GUC45 database.

Aus	Austria	Ita	Italy	Nor	Norway	Spa	Spain
Ban	Bangladesh	Jap	Japan	Pak	Pakistan	Swi	Switzerland
Chi	China	Lit	Lithuania	Pol	Poland	Taj	Tajikistan
Den	Denmark	Nep	Nepal	Rus	Russia	Tha	Thailand
Ger	Germany	Net	Netherlands	Ser	Serbia	Vie	Vietnam

Table E.3: Country abbreviations

E.1.2 Finger Metadata

The finger metadata consists of the width and length of each finger. A scattergraph is defined for each finger and plots the dimensions of each finger (Figure E.6). The scatter points are colored and indicate an occurrence range of finger dimensions. The x axis indicates the length of the finger while the y axis represents the width. The mean dimension of each finger is also plotted.

E.1.3 Session Metadata

The metadata of the sessions describes inside and outside temperature and humidity as well as the atmospheric pressure. The data is displayed through two graphical representations. The first plot is a bar charts which values are distributed within 6 bins. The second plot is a scattergraph which shows the value distribution for each session. The mean value of each session is also indicated.

Comment: The barometer used for the measurement of the humidity level gave values between 15% and 95%. Values below and above the maximal numeric values have “LOW” and “HIGH”, respectively. In the graphics, these extreme values were set to 10 for “LOW” and 96 for “HIGH”. In the graphs two lines were plotted to clearly delimite these extreme values from the numeric ones.

E.2 Sample Images

The image quality of the finger vein images is challenging due to the lack of experience in the setup of the capturing devices and technical difficulties. Sample images for for two fingers of two subjects are given in Figures E.12 and E.13. Images from all fingers were captured and the latter figure shows problems of the vein sensor for thick fingers like the thumb of the data subject. The vertical images of experiment 3 were designed to examine the potential to capture the finger veins from two side and to reconstruct a 3D model, however the visibility of the veins is very limited. Finger knuckle images are partly obfuscated to avoid conflicts with the organization lending parts of the vein sensor.

In conclusion, even though the dataset contains generally low quality vein images, interesting results could be achieved as the database is utilized in the experimental sections of several publications (e.g. those included in Chapters 6, 7 8, 10, C and Appendix D). It was as well the bases for several master theses [125, 148, 167, 177].

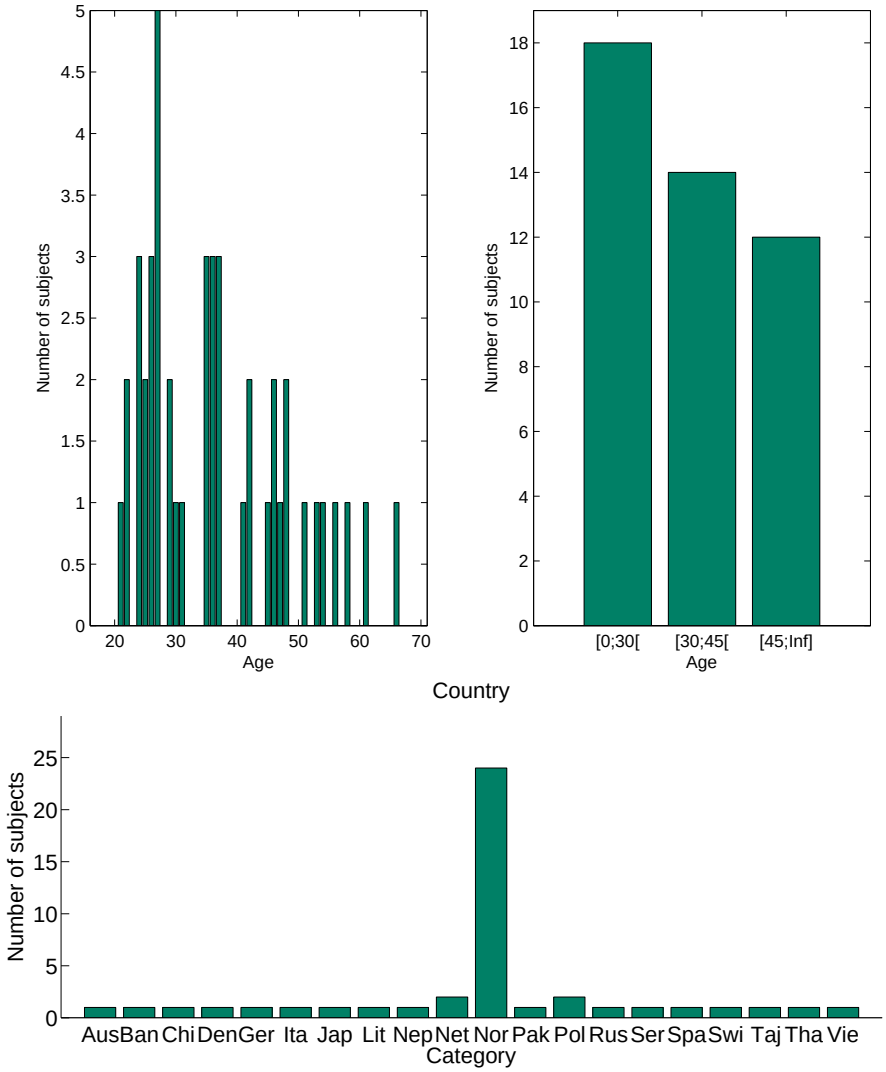


Figure E.5: Number of subjects for each category of the metadata (2/2).

Mostly data from experiment 1, 4 and 5 was utilized. To be able to continue the work on GUC45 and use its full potential the volunteers have to be contacted for their consent to extend the purpose of the data collection. In addition the Norsk samfunnsvitenskapelig datatjeneste AS (NSD) as official Norwegian institution responsible for database acquirements has to be contacted. Every scientific database gathering has to be registered with and approved by the NSD to ensure amongst others the privacy of data subjects. The extend of GUC45 was limited to the PhD project, hence it could not be made public.

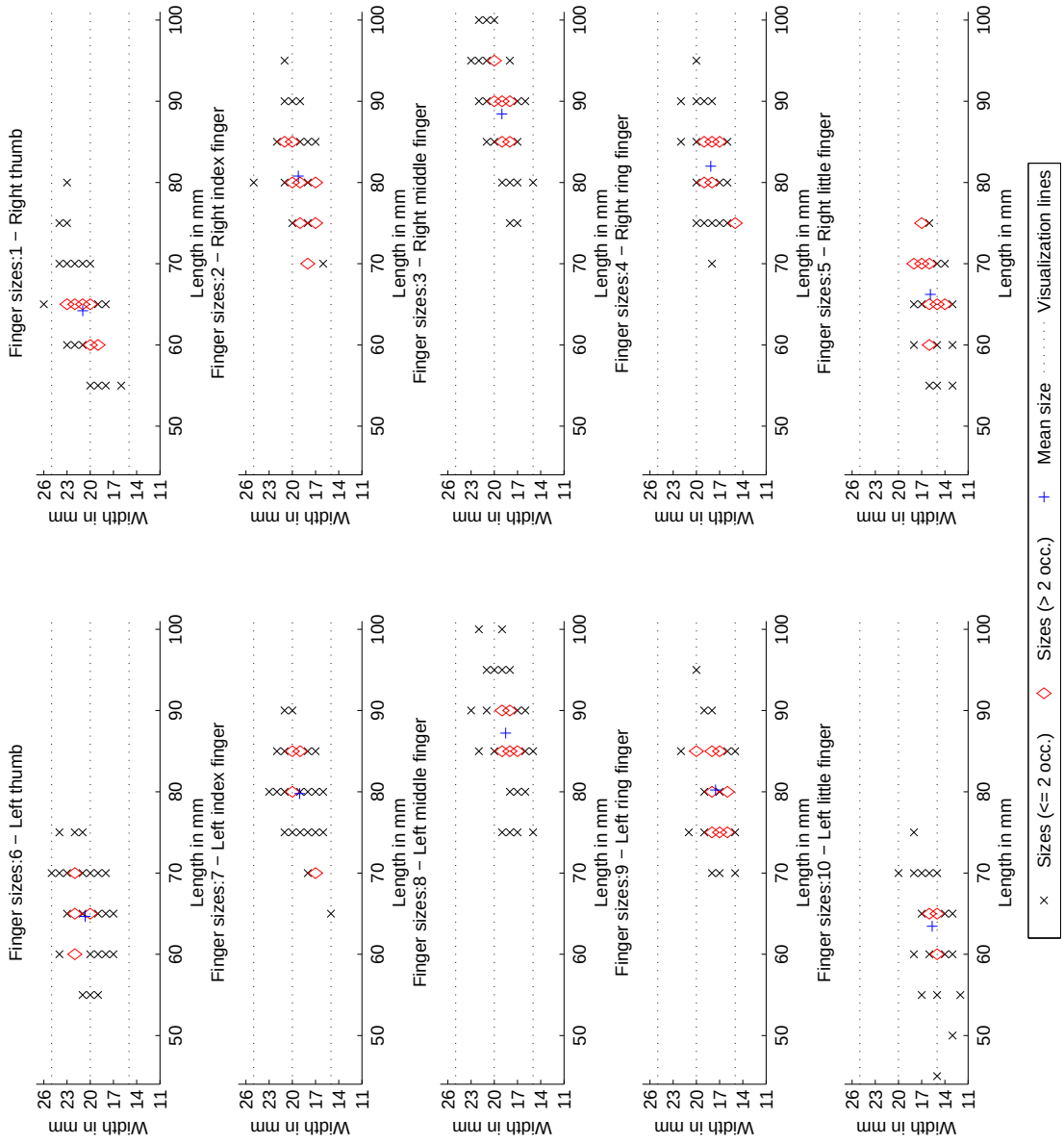


Figure E.6: Length and width of fingers (ISO finger code).

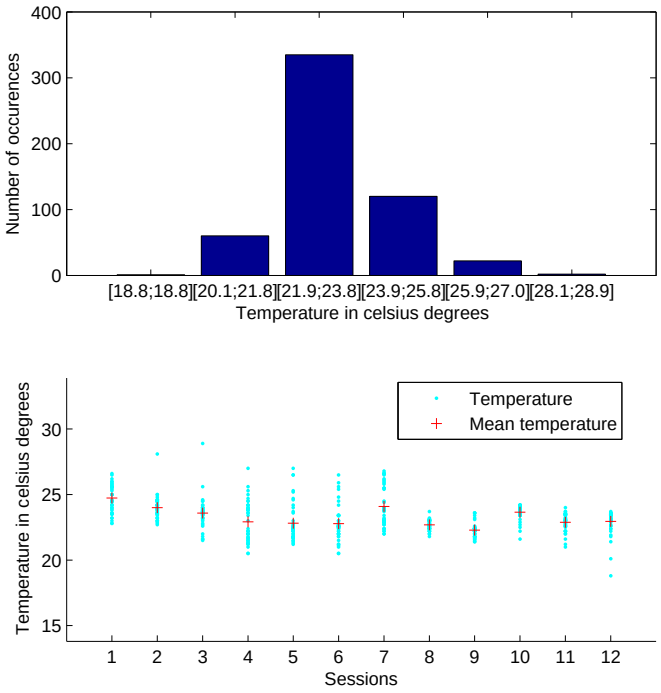


Figure E.7: Inside temperatures.

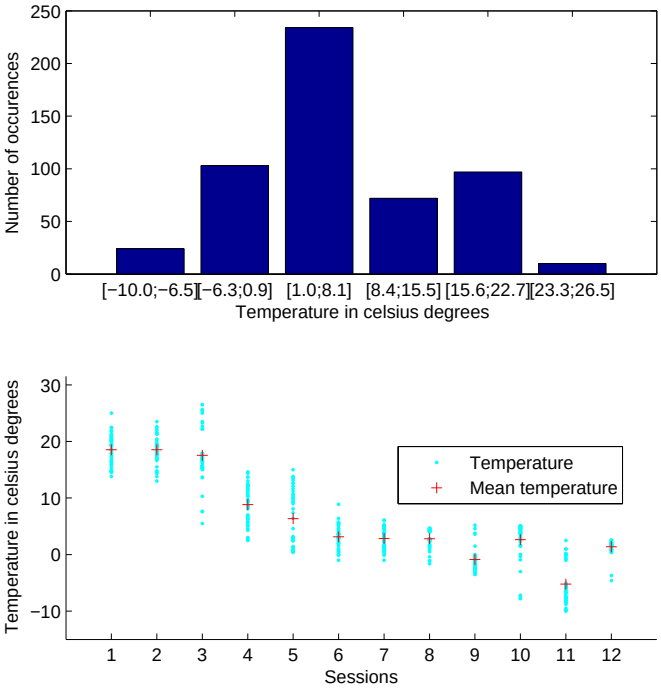


Figure E.8: Outside temperatures.

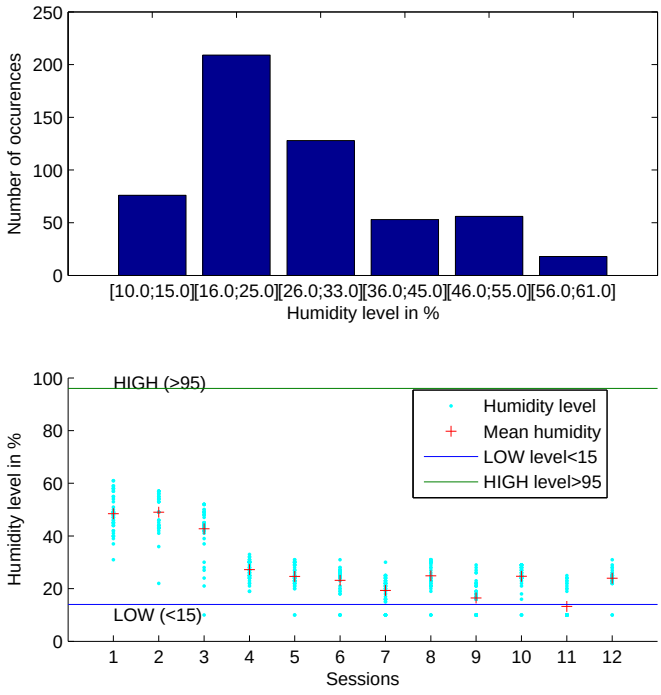


Figure E.9: Inside humidity.

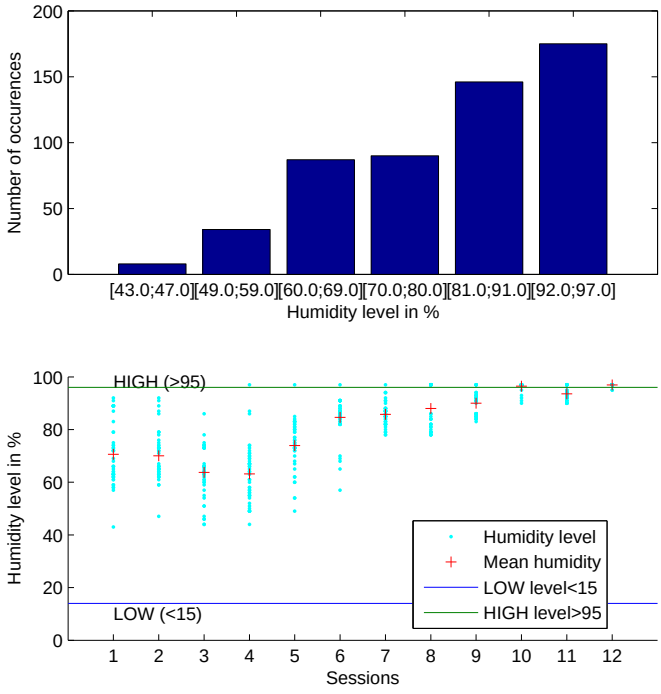


Figure E.10: Outside humidity.

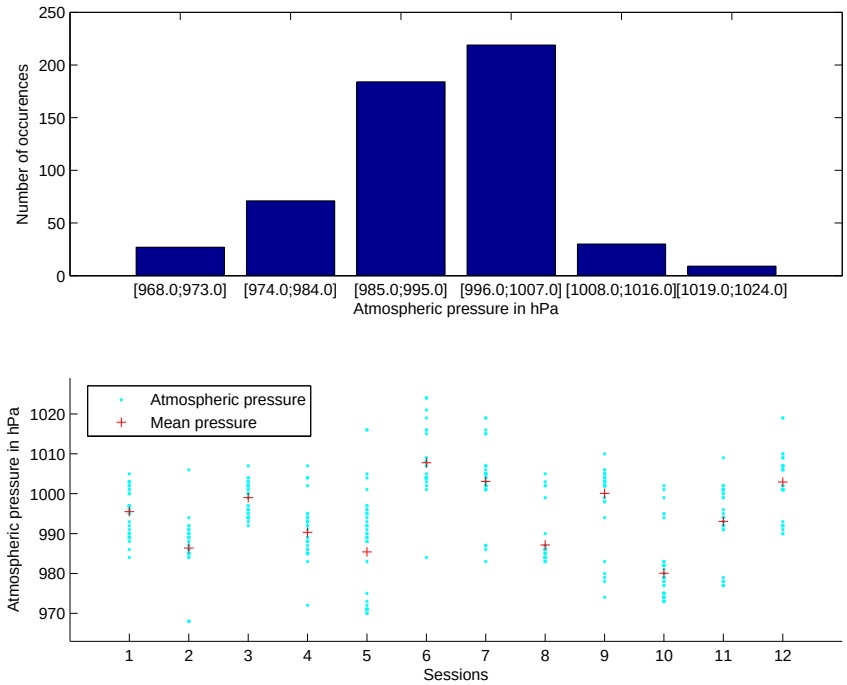
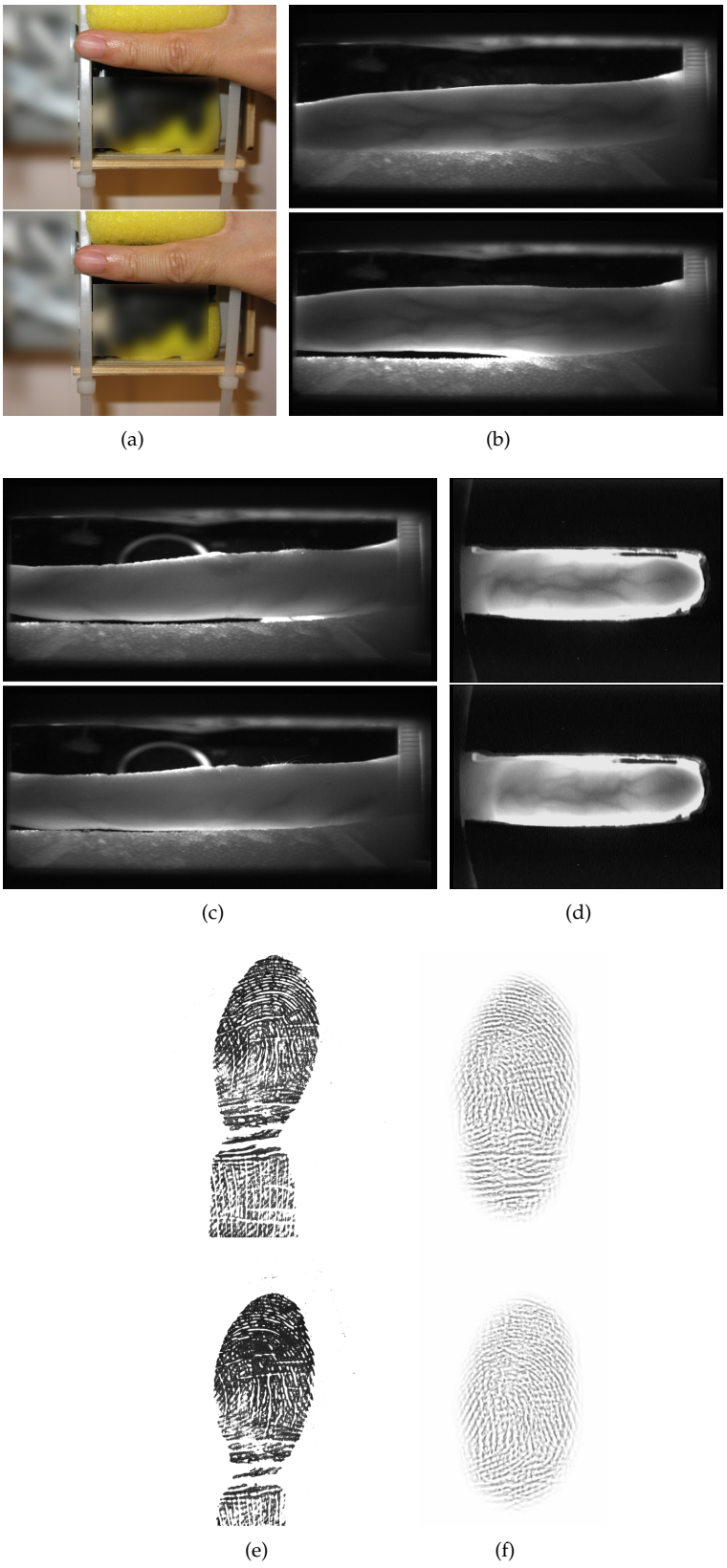


Figure E.11: Atmospheric pressure.



(a) (b) (c) (d) (e) (f)

Figure E.12: Sample image set from one session (2 attempts each) of a left little finger: (a) Exp 1: vein part sensor 1; (b) Exp 1: knuckle part (vein sensor obfuscated due to NDA); (c) Exp 2: vein side view sensor 1; (d) Exp 3: vein sensor 2; (e) Exp 4: fingerprints (Cross Match L SCAN 100); (f) Exp 5: fingerprints (Lumidigm V 100).

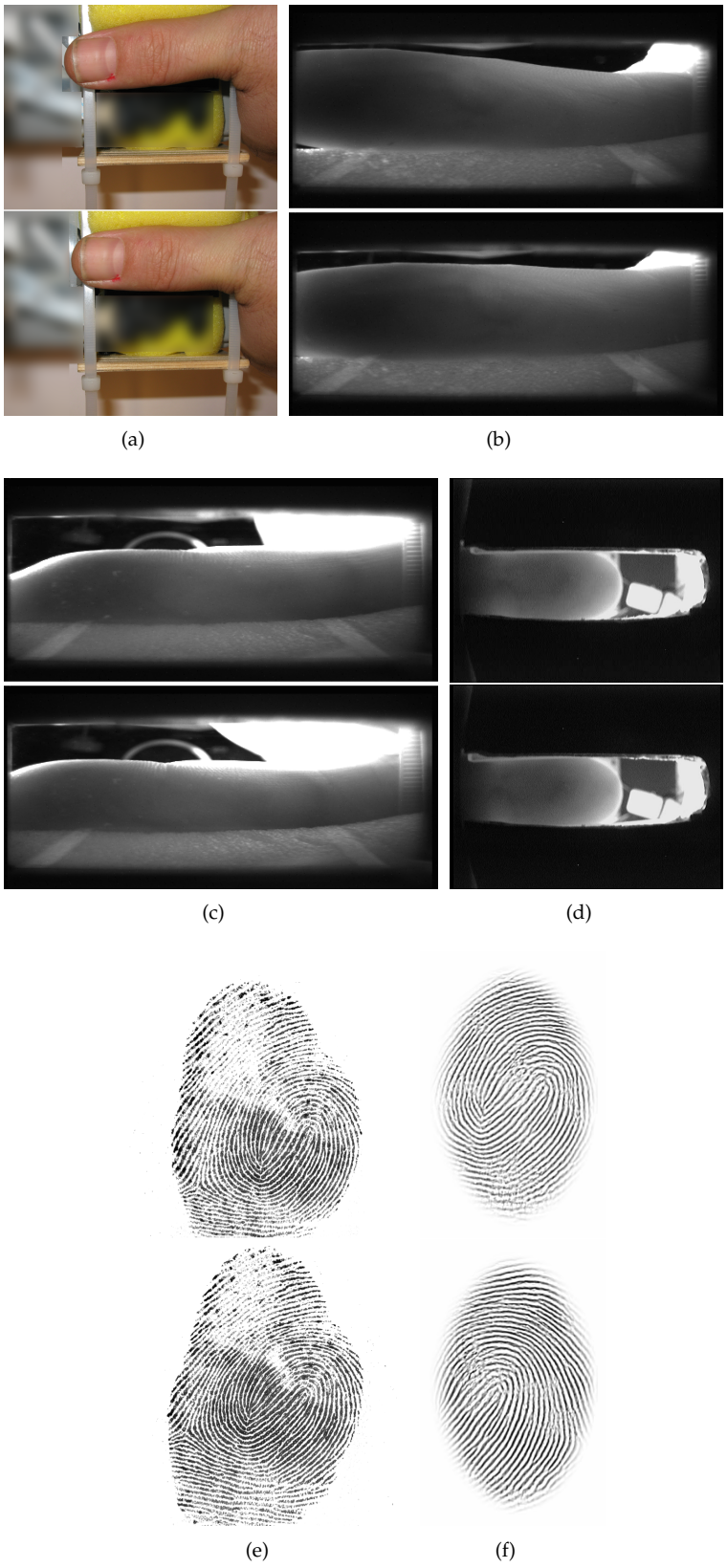


Figure E.13: Sample image set from one session (2 attempts each) of a left thumb: (a) Exp 1: vein part sensor 1; (b) Exp 1: knuckle part (vein sensor obfuscated due to NDA); (c) Exp 2: vein side view sensor 1; (d) Exp 3: vein sensor 2; (e) Exp 4: fingerprints (Cross Match L SCAN 100); (f) Exp 5: fingerprints (Lumidigm V 100).

Bibliography

[1] A-SIT: SECURE INFORMATION TECHNOLOGY CENTER AUSTRIA, ÖSTERREICHISCHENATIONALBANK. Risikoanalyse - E-Banking Angebote österreichischer Kreditinstitute. http://www.oenb.at/de/img/20080613_studie_sicherheit_im_e-banking_nach_feedback_durch_die_wko_tcm14-86337.pdf, May 2008. 151, 156

[2] ABADI, M., AND GORDON, A. D. A calculus for cryptographic protocols: the spi calculus. In *CCS '97: Proceedings of the 4th ACM conference on Computer and communications security* (New York, NY, USA, 1997), ACM, pp. 36–47. doi:http://doi.acm.org/10.1145/266420.266432. 167

[3] ADLER, A., YOUMARAN, R., AND LOYKA, S. Towards a measure of biometric feature information. *Pattern Analysis and Applications 12* (2009), 261–270. 10.1007/s10044-008-0120-3. doi:10.1007/s10044-008-0120-3. 195

[4] AI LAB, PEKING UNIVERSITY. Pku finger vein database (v2-v4). 37, 40

[5] ANDERSON, R. R., AND PARRISH, J. A. The optics of human skin. *J. Invest. Dermatol. 77*, 1 (July 1981), 13–19. 21

[6] ANTONELLI, A., CAPPELLI, R., MAIO, D., AND MALTONI, D. Fake finger detection by skin distortion analysis. *Information Forensics and Security, IEEE Transactions on 1*, 3 (September 2006), 360 –373. doi:10.1109/TIFS.2006.879289. 32

[7] ARCELLI, C., AND DI BAJA, G. S. A width-independent fast thinning algorithm. *IEEE Trans. Pattern Anal. Machine Intell.*, 4 (1985), 463–474. doi:10.1109/TPAMI.1985.4767685. 93

[8] BADAWI, A. M. Hand vein biometric verification prototype: A testing performance and patterns similarity. IPCV, pp. 3-9, 2006. 22, 41, 43

[9] BADRINATH, G., NIGAM, A., AND GUPTA, P. An efficient finger-knuckle-print based recognition system fusingsift and surf matching scores. In *Information and Communications Security*, vol. 7043 of *Lecture Notes in Computer Science*. Springer Berlin / Heidelberg, 2011, pp. 374–387. 148

[10] BARANCZUK, Z., ZOLLIKER, P., AND GIESEN, J. Image quality measures for evaluating gamut mapping. In *17th Color Imaging Conference* (Albuquerque, NM, USA, November 2009), pp. 21–26. 73

[11] BAY, H., TUYTELAARS, T., AND GOOL, L. V. Surf: Speeded up robust features. In *9th European Conference on Computer Vision* (May 2006), pp. 404–417. 49, 141, 142

[12] BELLARE, M., CANETTI, R., AND KRAWCZYK, H. Pseudorandom functions revisited: the cascade construction and itsconcrete security. *Foundations of Computer Science, Annual IEEE Symposium on 0* (1996), 514. doi:http://doi.ieeecomputersociety.org/10.1109/SFCS.1996.548510. 173

[13] BIOMETRIC RESEARCH CENTRE (UGC/CRC) AT THE HONG KONG POLYTECHNIC UNIVERSITY. PolyU FKP database. http://www4.comp.polyu.edu.hk/ biometrics/FKP.htm, July 2012. 140, 141, 148

[14] BLANCHET, B. An Efficient Cryptographic Protocol Verifier Based on PrologRules. In *14th IEEE Computer Security Foundations Workshop (CSFW-14)* (Cape Breton, Nova Scotia, Canada, June 2001), IEEE Computer Society, pp. 82–96. 164, 167

[15] BOGAZICI UNIVERSITY. Bosphorus hand vein database. 39, 40

[16] BOLLE, R., AND PANKANTI, S. *Biometrics, Personal Identification in Networked Society: PersonalIdentification in Networked Society*. Kluwer Academic Publishers, Norwell, MA, USA, 1998. 116

[17] BRANCHENVERBAND BITKOM. Fast 4 Millionen Opfer von Computer- und Internet-Kriminalität. http://www.bitkom.org/de/presse/56204_53100.aspx, July 2008. 150

[18] BREEBAART, J., BUSCH, C., GRAVE, J., AND KINDT, E. A reference architecture for biometric template protection basedon pseudo identities. In *BIOSIG* (2008), pp. 25–38. 34, 116, 151, 195

[19] BRINGER, J., CHABANNE, H., POINTCHEVAL, D., AND QIANGTANG. Extended private information retrieval and its application in biometricsauthentications. In *Cryptology and Network Security* (2007), vol. 4856 of *Lecture Notes in Computer Science*, Springer Berlin / Heidelberg, pp. 175–193. doi:10.1007/978-3-540-76969-9_12. 35

[20] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK. Die Lage der IT-Sicherheit in Deutschland 2009. https://www.bsi.bund.de/cae/servlet/contentblob/476182/publicationFile/30725/Lagebericht2009_pdf.pdf, January 2009. 150

[21] BUSCH, C., AND HARTUNG, D. (EN) AUTHENTICATED TRANSMISSION OF DATA, June 2011. http://www.wipo.int/patentscope/search/en/WO2011063992. 8, 149, 163

[22] CAPPELLI, R., FERRARA, M., AND MALTONI, D. Minutia cylinder-code: A new representation and matching technique for fingerprint recognition. *IEEE Trans. Pattern Anal. Mach. Intell. 32*, 12 (2010), 2128–2141. xiv, 182, 185, 189

[23] CAPPELLI, R., FERRARA, M., MALTONI, D., AND TISTARELLI, M. Mcc: A baseline algorithm for fingerprint verification in fvc-ongoing. In *ICARCV* (2010), IEEE, pp. 19–23. 182, 187, 188, 189, 190, 192

[24] CARO, J. J., TRINDADE, E., AND MCGREGOR, M. The risks of death and of severe nonfatal reactions with high- vs low-osmolality contrast media: a meta-analysis. *AJR Am J Roentgenol 156*, 4 (April 1991), 825–832. 16

[25] CARSTENSEN, J. M. *Image analysis, vision and computer graphics*. Technical University of Denmark, 2002. 93

[26] CASTAN, L., REIGOSA, M., AND NOLAZCO-FLORES, J. Biometric-iris random key generator using generalized regression neural networks. In *Advances in Applied Artificial Intelligence*, M. Ali and R. Dapoigny, Eds., vol. 4031 of *Lecture Notes in Computer Science*. Springer Berlin / Heidelberg, 2006, pp. 530–539. 205

[27] CHAN, T. F., AND VESE, L. A. Active contours without edges. *IEEE Transactions on Image Processing 10*, 2 (February 2001), 266–277. 86, 102, 104, 110

[28] CHEN, C., VELDHUIS, R., KEVENAAR, T., AND AKKERMANS, A. Biometric binary string generation with detection rate optimized bit allocation. In *2008 IEEE Computer Society Conference on Computer Vision and Pattern Recognition. Workshop on Biometrics* (Los Alamitos, June 2008), IEEE Computer Society Press, pp. 1–7. 54

[29] CHEN, C., VELDHUIS, R., KEVENAAR, T., AND AKKERMANS, A. Biometric quantization through detection rate optimized bit allocation. *EURASIP Journal on Advances in Signal Processing 2009*, 1 (2009), 784834. doi:10.1155/2009/784834. 54

[30] CHEN, H., LU, G., AND WANG, R. A new palm vein matching method based on icp algorithm. In *Proceedings of the 2nd International Conference on Interaction Sciences: Information Technology, Culture and Human* (New York, NY, USA, 2009), ICIS '09, ACM, pp. 1207–1211. 22, 41, 42, 48, 86, 102, 103, 110, 111, 128, 129, 130, 181, 192

[31] CHENGBO, Y., HUAFENG, Q., AND LIAN, Z. A research on extracting low quality human finger vein pattern characteristics. In *Bioinformatics and Biomedical Engineering, 2008. ICBBE 2008. The 2nd International Conference on* (May 2008), pp. 1876 –1879. doi:10.1109/ICBBE.2008.798. 22

[32] CHEONG, W. F., PRAHL, S. A., AND WELCH, A. J. A review of the optical properties of biological tissues. *IEEE Journal of Quantum Electronics 26* (1990), 2166–2185. doi:10.1109/3.64354. 21

[33] CHINESE ACADEMY OF SCIENCES' INSTITUTE OF AUTOMATION (CASIA). Casia multi-spectral palmprint database v1.0. ix, 37, 38, 40

[34] COLI, P., MARCIALIS, G., AND ROLI, F. Analysis and selection of features for the fingerprint vitality detection. In *Structural, Syntactic, and Statistical Pattern Recognition*, D.-Y. Yeung, J. Kwok, A. Fred, F. Roli, and D. de Ridder, Eds., vol. 4109 of *Lecture Notes in Computer Science*. Springer Berlin / Heidelberg, 2006, pp. 907–915. 10.1007/11815921_100. 29

[35] COLI, P., MARCIALIS, G., AND ROLI, F. Vitality detection from fingerprint images: A critical survey. In *Advances in Biometrics*, S.-W. Lee and S. Li, Eds., vol. 4642 of *Lecture Notes in Computer Science*. Springer Berlin / Heidelberg, 2007, pp. 722–731. 10.1007/978-3-540-74549-5_76. doi:10.1007/978-3-540-74549-5_76. 27

[36] CONAIRE, C. O., O'CONNOR, N. E., AND SMEATON, A. F. Detector adaptation by maximising agreement between independent datasources. In *CVPR* (2007). doi:10.1109/CVPR.2007.383448. 140

[37] CORTS, F., ARANDA, J., AND SACHEZ-REILLO, R. Spectral selection for a biometric recognition system based on hand veins detection through image spectrometry. *BIOSIG* (2009). 22

[38] COVER, T. M., AND THOMAS, J. A. *Elements of information theory*. Wiley-Interscience, New York, NY, USA, 1991. 127

[39] CROSS, J., AND SMITH, C. Thermographic imaging of the subcutaneous vascular network of the back of the hand for biometric identification. In *Security Technology, 1995. Proceedings. Institute of Electrical and Electronics Engineers 29th Annual 1995 International Carnahan Conference on* (October 1995), pp. 20 –35. doi:10.1109/CCST.1995.524729. 22, 43

[40] DAI, Y., HUANG, B., LI, W., AND XU, Z. A method for capturing the finger-vein image using nonuniform intensity infrared light. In *Image and Signal Processing, 2008. CISP '08. Congress on* (May 2008), vol. 4, pp. 501 –505. doi:10.1109/CISP.2008.654. 22, 37

[41] DAPP, T. Growing need for security in online banking - Biometrics enjoy remarkable degree of acceptance. White Paper, Deutsche Bank Research, 2012. 47

[42] DAUGMAN, J. The importance of being random: statistical principles of iris recognition. *Pattern Recognition 36*, 2 (2003), 279 – 291. doi:DOI:10.1016/S0031-3203(02)00030-4. 195

[43] DAVIS, H., RUSSELL, S., BARRIGA, E., ABRAMOFF, M., AND SOLIZ, P. Vision-based, real-time retinal image quality assessment. In *Computer-Based Medical Systems, 2009. CBMS 2009. 22nd IEEE International Symposium on* (August 2009), pp. 1 –6. doi:10.1109/CBMS.2009.5255437. 82

[44] DEEPALMAR, M., AND MADHESWARAN, M. An Improved Multimodal Palm Vein Recognition System Unsing Shape and Texture Features. *International Journal of Coputer Theory and Engineering 2*, 3 (June 2010), 1793–8201. 102

[45] DEEPIKA, C. L., AND KANDASWAMY, A. An Algorithm for Improved Accuracy in unimodal Biometric Systems Through Fusion of Multiple Feature Sets. *ICGST-GVIP Journal 9*, 3 (June 2009), 33–40. 102

[46] DERAKHSHANI, R., ROSS, A., AND CRIHALMEANU, S. A New Biometric Modality Using Concunctival Vasculature. In *Proceedings of Artificial Neural Networks in Engineering* (November 2006). 116

[47] DOLEV, D., AND YAO, A. C. On the security of public key protocols. In *SFCS '81: Proceedings of the 22nd Annual Symposium on Foundations of Computer Science* (Washington, DC, USA, 1981), IEEE Computer Society, pp. 350–357. doi:http://dx.doi.org/10.1109/SFCS.1981.32. 168

[48] DORIZZI, B., CAPPELLI, R., FERRARA, M., MAIO, D., MALTONI, D., HOUMANI, N., GARCIA-SALICETTI, S., AND MAYOUE, A. Fingerprint and on-line signature verification competitions at icb 2009. In *Proceedings of the Third International Conference on Advances in Biometrics* (Berlin, Heidelberg, 2009), ICB '09, Springer-Verlag, pp. 725–732. doi:10.1007/978-3-642-01793-3_74. 182

[49] DRAHANSK, M. *Liveness Detection in Biometrics*. InTech - Open Access Publisher, 2011, pp. 179–198. 27

[50] DUBUISSON, M.-P., AND JAIN, A. A modified hausdorff distance for object matching. In *Pattern Recognition, 1994. Vol. 1 - Conference A: Computer Vision Image Processing., Proceedings of the 12th IAPR International Conference on* (October 1994), vol. 1, pp. 566 –568 vol.1. doi:10.1109/ICPR.1994.576361. 48, 128, 129, 130

[51] ECONOMOPOULOS, T., ASVESTAS, P., AND MATSOPOULOS, G. Contrast enhancement of images using partitioned iterated function systems. *Image and Vision Computing 28*, 1 (2010), 45 – 54. doi:10.1016/j.imavis.2009.04.011. 71, 72

[52] EICHMANN, A., YUAN, L., MOYON, D., LENOBLE, F., PARDANAUD, L., AND BRANT, C. Vascular Development: From Precursor Cells to Branched Arterial and Venous Networks. *International Journal of Developmental Biology 49* (2005), 259–267. doi:10.1387/ijdb.041941ae. 11, 100, 116, 196, 204

[53] EVANS, C. Notes on the opensurf library. Tech. Rep. CSTR-09-001, University of Bristol, January 2009. 144

[54] FAN, K.-C., LIN, C.-L., AND LEE, W.-L. Biometric Verification Using thermal Images of Palm-Dorsa Vein-patterns. In *16th IPPR Conference on Computer Vision, Graphics and Image Processing* (2003). 17, 43, 104

[55] FERRER, M., MORALES, A., AND ORTEGA, L. Infrared hand dorsum images for identification. *Electronics Letters 45*, 6 (12 2009), 306 –308. doi:10.1049/el.2009.0136. 22, 39, 43

[56] FIDIS CONSORTIUM, WP6. Deliverable D6.1: Forensic Implications of Identity Management Systems. *Future of Identity in the Information Society*, 1 (January 2006). 32, 100

[57] FILLER, T., FRIDRICH, J. J., AND GOLJAN, M. Using sensor pattern noise for camera model identification. In *ICIP* (2008), pp. 1296–1299. doi:10.1109/ICIP.2008.4712000. 206

[58] FRANGI, R. F., NIESSEN, W. J., VINCKEN, K. L., AND VIERGEVER, M. A. Multiscale Vessel Enhancement Filtering. In *Medical Image Computing and Computer-Assisted Intervention*. Springer-Verlag, 1998, pp. 130–137. 102, 104, 110, 121

[59] FRONTHALER, H., KOLLREIDER, K., AND BIGUN, J. Automatic image quality assessment with application in biometrics. In *2006 Computer Vision and Pattern Recognition Workshop (CVPRW '06) Conference on* (June 2006), p. 30. doi:10.1109/CVPRW.2006.36. 82

[60] FUJITSU COMPUTER PRODUCTS OF AMERICA, INC. Palm Vein Pattern Authentication Technology. White Paper, Fujitsu Computer Products of America, Inc., 2006. 24

[61] FUJITSU LABORATORIES LTD. Fujitsu Develops World's Smallest and Slimmest Palm Vein Biometric Authentication Sensor Deployable in Tablet Devices – Able to handle slim mobile device integration through a 5mm optical sensor. http://www.fujitsu.com/global/news/pr/archives/month/2012/20120501-01.html, March 2012. 27, 28

[62] FUKSIS, R., KADIKIS, A., AND GREITANS, M. Biohashing and fusion of palmprint and palm vein biometric data. In *Hand-Based Biometrics (ICHB), 2011 International Conference on* (November 2011), pp. 1 –6. doi:10.1109/ICHB.2011.6094334. 22, 42

[63] GRAY, H. *Anatomy of the Human Body*, 20 ed. Lea and Febiger, 1918. Retrieved from Wikimedia Commons. ix, 11, 13, 14

[64] GROUP OF MACHINE LEARNING AND APPLICATIONS, SHANDONG UNIVERSITY (SDUMLA). Sdumla-hmt database. ix, 37, 38, 40

[65] GUAN, F., WANG, K., AND WU, Q. Bi-directional weighted modular b2dpca for finger vein recognition. In *Image and Signal Processing (CISP), 2010 3rd International Congress on* (October 2010), vol. 1, pp. 93 –97. doi:10.1109/CISP.2010.5646294. 42, 103

[66] GUAN, F., WANG, K., AND YANG, Q. A study of two direction weighted (2d)2lda for finger vein recognition. In *Image and Signal Processing (CISP), 2011 4th International Congress on* (October 2011), vol. 2, pp. 860 –864. doi:10.1109/CISP.2011.6100257. 42, 103

[67] HAO, Y., SUN, Z., AND TAN, T. Comparative studies on multispectral palm image fusion for biometrics. In *Computer Vision ACCV 2007*, Y. Yagi, S. Kang, I. Kweon, and H. Zha, Eds., vol. 4844 of *Lecture Notes in Computer Science*. Springer Berlin / Heidelberg, 2007, pp. 12–21. 10.1007/978-3-540-76390-1_2. doi:10.1007/978-3-540-76390-1_2. 22, 24, 37

[68] HAO, Y., SUN, Z., TAN, T., AND REN, C. Multispectral palm image fusion for accurate contact-free palmprint recognition. In *Image Processing, 2008. ICIP 2008. 15th IEEE International Conference on* (October 2008), pp. 281 –284. doi:10.1109/ICIP.2008.4711746. 22, 24, 37, 42

[69] HARALICK, R. M., SHANMUGAM, K., AND DINSTEIN, I. Textural features for image classification. *IEEE Transactions on Systems, Man and Cybernetics 3*, 6 (November 1973), 610 –621. doi:10.1109/TSMC.1973.4309314. 83

[70] HARTUNG, D. Entropy estimator and formal model for vascular skeletons. In *Biometric Measurements and Systems for Security and Medical Applications(BIOMS), 2011 IEEE Workshop on* (September 2011), pp. 1 –5. doi:10.1109/BIOMS.2011.6053681. 6, 195

[71] HARTUNG, D., AND BUSCH, C. Why vein recognition needs privacy protection. In *Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP '09)* (September 2009), pp. 1090 –1095. doi:10.1109/IIH-MSP.2009.132. 6, 43, 47, 59, 116

[72] HARTUNG, D., AND BUSCH, C. Biometric transaction authentication protocol. In *Proceedings of the 2010 Fourth International Conference on Emerging Security Information, Systems and Technologies* (Washington, DC, USA, 2010), SECURWARE '10, IEEE Computer Society, pp. 207–215. doi:10.1109/SECURWARE.2010.41. ix, 6, 47, 50, 149, 164, 169, 195, 203

[73] HARTUNG, D., AND BUSCH, C. Biometrische Fingererkennung - Fusion von Fingerabdruck, Fingervenen- und Fingergelenkbild. In *12. Deutscher IT-Sicherheitskongress des BSI: Sicher in die digitale Welt von morgen* (May 2011), SecuMedia-Verlag. 7, 36, 86, 141, 148

[74] HARTUNG, D., AND BUSCH, C. Biometric Transaction Authentication Protocol: Formal Model Verification and "Four-Eyes" Principle Extension. In *LNCS 7126, Financial Cryptography and Data Security* (2012). doi:10.1007/978-3-642-29889-9_8. ix, 7, 47, 50, 163, 195, 203

[75] HARTUNG, D., AND KÜCKELHAHN, J. Dorsal finger texture recognition: Investigating fixed-length surf. In *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics, Seoul, Korea, October 14-17, 2012* (2012). 7, 49, 137

[76] HARTUNG, D., MARTIN, S., AND BUSCH, C. Quality estimation for vascular pattern recognition. In *Hand-Based Biometrics (ICHB), 2011 International Conference on* (November 2011), pp. 1 –6. doi:10.1109/ICHB.2011.6094332. 7, 48, 80

[77] HARTUNG, D., OLSEN, M. A., XU, H., AND BUSCH, C. Spectral minutiae for vein pattern recognition. In *Biometrics (IJCB), 2011 International Joint Conference on* (October 2011), pp. 1 –7. doi:10.1109/IJCB.2011.6117549. 7, 41, 43, 44, 110, 115, 117, 118, 119, 133, 181, 186, 190, 192

[78] HARTUNG, D., OLSEN, M. A., XU, H., NGUYEN, H. T., AND BUSCH, C. Comprehensive analysis of spectral minutiae for vein pattern recognition. In *IET Biometrics* (March 2012), vol. 1, pp. 25–36. doi:10.1049/iet-bmt.2011.0013. ix, 7, 41, 43, 44, 48, 50, 51, 115, 181, 186, 192

[79] HARTUNG, D., PFLUG, A., AND BUSCH, C. Vein pattern recognition using chain codes spatial information andskeleton fusing. In *Sicherheit* (2012), pp. 245–256. 7, 41, 42, 44, 99, 101

[80] HARTUNG, D., WOLD, K., GRAFFI, K., AND PETROVIC, S. Towards a biometric random number generator - a general approach for true random extraction from biometric samples. In *BIOSIG* (2011), pp. 267–274. 7, 203

[81] HASHIMOTO, J. Finger vein authentication technology and its future. *VLSI Circuits, 2006. Digest of Technical Papers. 2006 Symposium on* (2006), 5–8. doi:10.1109/VLSIC.2006.1705285. ix, xi, 22, 27, 60, 196, 199

[82] HAXTHAUSEN, H. "infrarotes" photographieren in der dermatologie. *Derm. Wschr. 97*, 1289 (1933). 21

[83] HEENAYE-MAMODE KHAN, M., SUBRAMANIAN, R., AND ALI MAMODE KHAN, N. Representation of hand dorsal vein features using a low dimensional representation integrating cholesky decomposition. In *Image and Signal Processing, 2009. CISP '09. 2nd International Congress on* (October 2009), pp. 1 –6. doi:10.1109/CISP.2009.5304218. 22, 43

[84] HERMOSILLA, G., DEL SOLAR, J. R., VERSCHAE, R., AND CORREA, M. A comparative study of thermal face recognition methods in unconstrained environments. *Pattern Recognition 45*, 7 (2012), 2445 – 2459. doi:10.1016/j.patcog.2012.01.001. 17

[85] HIRZEL, J., HARTUNG, D., AND BUSCH, C. Fingerprint recognition with cellular partitioning and co-sinusoidal triplets. In *BIOSIG* (2010), pp. 109–114. 7

[86] HITACHI, LTD. Hitachi develops grip-type finger vein authentication technology. Press release, 2005. 27

[87] HITACHI, LTD. Finger vein authentication: White paper, 2006. http://www.hitachi.co.jp/products/it/veinid/global/introduction/pdf /finger_vein_authentication_white_paper.pdf, Visited on 06/07/2011. 24

[88] HITACHI LTD. Finger vein authentication technology. http://www.hitachi-america.us/products/business/smart_solutions/finger_vein/index.html, 2009. 24

[89] HITACHI, LTD. Hitachi develops a 3mm thin-type finger vein authentication module. http://www.hitachi.com/New/cnews/090826.html, August 2009. ix, 27, 28

[90] IDENTITY THEFT RESOURCE CENTER. 2009 ITRC Breach Report. http://www.idtheftcenter.org/artman2/publish/lib_survey/ITRC_2008_Breach_List.shtml, February 2010. 150

[91] IGNATENKO, T., AND WILLEMS, F. Biometric systems: Privacy and secrecy aspects. *Information Forensics and Security, IEEE Transactions on 4*, 4 (December 2009), 956 –973. doi:10.1109/TIFS.2009.2033228. 157

[92] IM, S.-K., CHOI, H. S., , AND KIM, S.-W. A direction-based vascular pattern extraction algorithm for hand vascular pattern verification. In *ETRI Journal* (2003), vol. 25, pp. 101–108. 22

[93] IM, S.-K., PARK, H.-M., KIM, Y.-W., HAN, S.-C., KIM, S.-W., AND KANG, C.-H. An biometric identification system by extracting hand vein patterns. In *Journal of the Korean Physical Society* (2001), vol. 38, pp. 268–272. 22

[94] INTERNATIONAL BIOMETRICS GROUP (IBG). *Comparative Biometric Testing Round 6 Public Report*, September 2006. 44, 60, 196, 204

[95] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). General biometric system (sc37 sd11 document). xi, 179

[96] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). Iso/iec tr 29794-4:2010 biometric sample quality - part 4: Finger image (iso/iec tc jtc1/sc37). 81, 82

[97] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). Iso/iec tr 29794-5:2010 biometric sample quality – part 5: Face image data (iso/iec tc jtc1/sc 37). 82

[98] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). Iso/iec wd 29794-6 biometric sample quality - part 6: Iris image (iso/iec tc jtc1/sc37). 82

[99] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). Biometric performance testing and reporting. part 1: Principles and framework (iso/iec 19795-1:2005), 2005. 82

[100] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). Iso/iec 29794-1:2009 biometric sample quality - framework, October 2009. 82

[101] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). Information technology – security techniques – biometric information protection (iso/iec 24745:2011), 2011. 34

[102] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO), ISO/IEC JTC1 SC37 BIOMETRICS. ISO/IEC 19795-1:2006 Information Technology *Biometric Data Interchange Formats - Part 2: Finger Minutiae Data*, 2005. 112, 182

[103] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO), ISO/IEC JTC1 SC37 BIOMETRICS. Information technology - biometric data interchange formats - part 9: Vascular image data. *19794-9:2007* (2007). 62

[104] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO), ISO/IEC JTC1 SC37 BIOMETRICS. ISO/IEC 19794-9:2011 Information Technology - Biometric Data Interchange Formats - Part 9: Vascular image data, 2011. 9, 53

[105] JAIN, A. K., BOLLE, R. M., AND PANKANTI, S. *Biometrics: Personal Identification in Networked Society*. Springer, October 2005. 9

[106] JAIN, A. K., NANDAKUMAR, K., AND NAGAR, A. Biometric template security. *EURASIP J. Adv. Signal Process 2008* (January 2008), 113:1–113:17. doi:10.1155/2008/579416. 34, 116

[107] JOUSSEN, A. M. Vascular plasticity–the role of the angiopoietins in modulating ocular angiogenesis. *Graefes Arch Clin Exp Ophthalmology 239*, 12 (December 2001), 972 – 975. 100

[108] JUELS, A., AND SUDAN, M. A fuzzy vault scheme. *Des. Codes Cryptography 38*, 2 (2006), 237–257. doi:10.1007/s10623-005-6343-z. 34, 41, 56

[109] JUELS, A., AND WATTENBERG, M. A fuzzy commitment scheme. In *ACM Conference on Computer and Communications Security* (1999), pp. 28–36. doi:10.1145/319709.319714. 34, 117, 151

[110] KANADE, S., PETROVSKA-DELACRÉTAZ, D., AND DORIZZI, B. Multi-biometrics based crypto-biometric session key generation and sharing protocol. In *Proceedings of the thirteenth ACM multimedia workshop on Multimedia and security* (New York, NY, USA, 2011), ACM, pp. 109–114. doi:10.1145/2037252.2037272. 56

[111] KANADE, S. G., PETROVSKA-DELACRETAZ, D., AND DORIZZI, B. A novel cryptobiometric scheme for establishing secure communication sessions between two clients. In *BIOSIG* (September 2012), pp. 1 –6. 56

[112] KANG, B., PARK, K., YOO, J., AND KIM, J. Multimodal biometric method that combines veins, prints, and shape of a finger. *Optical Engineering 50* (2011), 017201. 22, 24

[113] KANG, W.-X., CHEN, Z.-Y., AND YANG, Q.-Q. A hand vein recognition system based on dsp and cpld. *Optoelectronics Letters 6* (2010), 477–480. doi:10.1007/s11801-010-8098-7. 22

[114] KANUKURTHI, B., AND REYZIN, L. An Improved Robust Fuzzy Extractor. *ArXiv e-prints* (July 2008). 35

[115] KEKRE, H. B., AND BHARADI, V. A. Finger-knuckle-print region of interest segmentation using gradient field orientation and coherence. *Third International Conference on Emerging Trends in Engineering and Technology* (2010). 140, 141

[116] KELKBOOM, E. J. C. *On the performance of helper data template protection schemes*. Ph.D. thesis, University of Twente, Enschede, the Netherlands, October 2010. 34, 35, 55

[117] KELKBOOM, E. J. C., DE GROOT, K. T. J., CHEN, C., BREEBAART, J., AND VELDHUIS, R. N. J. Pitfall of the detection rate optimized bit allocation within template protection and a remedy. In *Proceedings of the 3rd IEEE international conference on Biometrics: Theory, applications and systems* (Piscataway, NJ, USA, 2009), BTAS'09, IEEE Press, pp. 230–237. 54

[118] KELKBOOM, E. J. C., ZHOU, X., BREEBAART, J., VELDHUIS, R. N. S., AND BUSCH, C. Multi-algorithm fusion with template protection. In *Proceedings of the 3rd IEEE international conference on Biometrics: Theory, applications and systems* (Piscataway, NJ, USA, 2009), BTAS'09, IEEE Press, pp. 222–229. 139

[119] KHAN, M. H.-M., AND KHAN, N. M. Feature Extraction of Dorsal hand- Vein Pattern Using a Fast Modified PCA Algorithm Based on Cholesky Decomposition and Lanczos Technique. *International Journal of Mathematical and Computer Sciences 5*, 4 (2009), 230–234. 43, 103

[120] KOLÅS Ø., FARUP, I., AND RIZZI, A. Stress: A framework for spatial color algorithms. In *Journal of Imaging Science and Technology* (2011), vol. 55,4. 70, 98, 102, 199, 204

[121] KONO, M., H, H. U., AND UMEMURA, S. A new method for the identification of individuals by using vein pattern matching of a finger. In *Proceedings of the 5th symposium on pattern measurement* (Yamaguchi, Japan, 2000), pp. 9–12. 102

[122] KONO MIYUKI ET AL. Personal identification system. US Patent (Patent no. 7352448), 2008. 24

[123] KRHOVJÁK, J., ŠVENDA, P., AND MATYÁŠ, V. The sources of randomness in mobile devices. *In Proceeding of the 12th Nordic Workshop on Secure IT Systems, Reykjavik* (2007), 73–84. 205

[124] KRYSZCZUK, K., AND POH, N. Handling high dimensionality in biometric classification with multiple quality measures using locality preserving projection. In *2010 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)* (June 2010), pp. 146 –153. doi:10.1109/CVPRW.2010.5544619. 82

[125] KÜCKELHAHN, J. Dorsal finger skin texture recognition with fixed-length feature extraction based on SURF for multimodal privacy enhanced biometric systems. Master's thesis, Technical University of Denmark, DTU Informatics, E-mail: reception@imm.dtu.dk, Asmussens Alle, Building 305, DK-2800 Kgs. Lyngby, Denmark, 2012. Supervised by Professor Rasmus Larsen, rl@imm.dtu.dk, DTU Informatics. Thesis not publicly available. 138, 215

[126] KUMAR, A., HANMANDLU, M., AND GUPTA, H. Online biometric authentication using hand vein patterns. In *Computational Intelligence for Security and Defense Applications, 2009. CISDA 2009. IEEE Symposium on* (July 2009), pp. 1 –7. doi:10.1109/CISDA.2009.5356554. 19, 43

[127] KUMAR, A., AND PRATHYUSHA, K. V. Personal authentication using hand vein triangulation and knuckle shape. *Trans. Img. Proc. 18* (September 2009), 2127–2136. doi:10.1109/TIP.2009.2023153. 22, 24, 41, 43, 117, 181

[128] KUMAR, A., AND RAVIKANTH, C. Personal authentication using finger knuckle surface. *Information Forensics and Security, IEEE Transactions on 4*, 1 (March 2009), 98 –110. doi:10.1109/TIFS.2008.2011089. 140

[129] KUMAR, A., AND ZHOU, Y. Human identification using knucklecodes. In *Proceedings of the 3rd IEEE international conference on Biometrics: Theory, applications and systems* (Piscataway, NJ, USA, 2009), BTAS'09, IEEE Press, pp. 147–152. 141, 148

[130] KUMAR, A., AND ZHOU, Y. Human identification using finger images. *Image Processing, IEEE Transactions on 21*, 4 (April 2012), 2228 –2244. doi:10.1109/TIP.2011.2171697. 22, 36

[131] LA BERGE ET. AL. *Interventional Radiology Essentials*. Lippincott Williams and Wilkins, 2000. x, 34, 62, 63

[132] LADOUX, P.-O., ROSENBERGER, C., AND DORIZZI, B. Palm vein verification system based on sift matching. In *ICB* (2009), pp. 1290–1298. doi:10.1007/978-3-642-01793-3_130. 22, 42

[133] LAM, L., LEE, S.-W., AND SUEN, C. Y. Thinning methodologies-a comprehensive survey. *IEEE Trans. Pattern Anal. Mach. Intell. 14* (September 1992), 869–885. doi:10.1109/34.161346. 93, 199

[134] LE-QING, Z. Finger knuckle print recognition based on surf algorithm. *Eighth International Conference on Fuzzy Systems and Knowledge Discovery* (2011). 140, 141

[135] LEE, C.-J., YANG, T.-N., JENG, I.-H., CHEN, C.-J., AND LIN, K.-L. Singular points and minutiae detection in fingerprint images using principal gabor basis functions. In *IPCV* (2006), pp. 29–34. 94

[136] LEE, E., AND PARK, K. Restoration method of skin scattering blurred vein image for finger vein recognition. *Electronics Letters 45*, 21 (8 2009), 1074 –1076. doi:10.1049/el.2009.1231. 22, 42

[137] LEE, E. C., LEE, H. C., AND PARK, K. R. Finger vein recognition using minutia-based alignment and local binary pattern-based feature extraction. *International Journal of Imaging Systems and Technology 19* (September 2009), 179–186. doi:10.1002/ima.v19:3. 82, 117

[138] LEE, H. C., PARK, K. R., KANG, B. J., AND PARK, S. J. A new mobile multimodal biometric device integrating finger vein and fingerprint recognition. In *Ubiquitous Information Technologies Applications, 2009. ICUT '09. Proceedings of the 4th International Conference on* (December 2009), pp. 1 –4. doi:10.1109/ICUT.2009.5405686. 22, 24

[139] LI, K., YUAN, H., AND LIU, M. A novel preprocessing algorithm of knuckleprint. *International Conference on Artificial Intelligence and Computational Intelligence* (2010). 140

[140] LIN, C.-L., AND FAN, K.-C. Biometric verification using thermal images of palm-dorsa vein patterns. *Circuits and Systems for Video Technology, IEEE Transactions on 14*, 2 (February 2004), 199 – 213. doi:10.1109/TCSVT.2003.821975. ix, 17, 19, 21, 34, 43

[141] LINNARTZ, J.-P. M. G., AND TUYLS, P. New shielding functions to enhance privacy and prevent misuse ofbiometric templates. In *AVBPA* (2003), pp. 393–402. 34

[142] LOWE, D. G. Distinctive image features from scale-invariant keypoints. *Int. J. Comput. Vision 60*, 2 (November 2004), 91–110. doi:10.1023/B:VISI.0000029664.99615.94. 42, 43, 141

[143] LUNNON, R. J. Some observations on the photography of the diseased skin. *Med Biol Illus 11* (April 1961), 98–103. 21

[144] LUO, H., YU, F.-X., PAN, J.-S., CHU, S.-C., AND TSAI, P.-W. A survey of vein recognition techniques. *Information Technology Journal 9*, 6 (2010), 1142–1149. 41

[145] MACKAY, D. Fountain codes. *Communications, IEE Proceedings- 152*, 6 (December 2005), 1062 – 1068. doi:10.1049/ip-com:20050237. 55

[146] MALIK, S. Real-time hand tracking and finger tracking for interaction, 2003. 140

[147] MALTONI, D., MAIO, D., JAIN, A. K., AND PRABHAKAR, S. *Handbook of Fingerprint Recognition*, 2nd ed. Springer Publishing Company, Incorporated, 2009. 17, 27, 29, 93

[148] MARTIN, S. E. M. Quality assessment in vein recognition systems. Master's thesis, Technical University of Denmark, DTU Informatics, E-mail: reception@imm.dtu.dk, Asmussens Alle, Building 305, DK-2800 Kgs. Lyngby, Denmark, 2011. Supervised by Professor Rasmus Larsen, rl@imm.dtu.dk, DTU Informatics. Thesis not publicly available. 79, 212, 215

[149] MEINTS, M., BIERMANN, H., BROMBA, M., BUSCH, C., HORNUNG, G., AND QUIRING-KOCK, G. Biometric systems and data protection legislation in germany. In *IIH-MSP '08: Proceedings of the 2008 International Conference on Intelligent Information Hiding and Multimedia Signal Processing* (Harbin, China, 2008), IEEE Computer Society, pp. 1088–1093. doi:10.1109/IIH-MSP.2008.314. 62

[150] MERAOUMIA, A., CHITROUB, S., AND BOURIDANE, A. Fusion of finger-knuckle-print and palmprint for an efficient multi-biometric system of person recognition. In *Communications (ICC), 2011 IEEE International Conference on* (June 2011), pp. 1 –5. doi:10.1109/icc.2011.5962661. 140, 141

[151] MICHAEL, G. K. O., CONNIE, T., HOE, L. S., AND JIN, A. T. B. Design and implementation of a contactless palm vein recognition system. In *Proceedings of the 2010 Symposium on Information and Communication Technology* (New York, NY, USA, 2010), (SoICT '10), ACM, pp. 92–99. 79, 82, 83

[152] MICHELSON, A. A. *Studies in Optics*. University of Chicago Press, 1927. 73

[153] MILLIKAN, G. A. The oximeter, an instrument for measuring continuously the oxygen saturation of arterial blood in man. *Review of Scientific Instruments 13*, 10 (October 1942), 434 –444. doi:10.1063/1.1769941. 30

[154] MILNER, R., PARROW, J., AND WALKER, D. A calculus of mobile processes, i. *Information and Computation 100*, 1 (1992), 1 – 40. doi:10.1016/0890-5401(92)90008-4. 164, 167

[155] MIRMOHAMADSADEGHI, L., AND DRYGAJLO, A. Palm vein recognition with local binary patterns and local derivative patterns. In *Biometrics (IJCB), 2011 International Joint Conference on* (October 2011), pp. 1 –6. doi:10.1109/IJCB.2011.6117804. 22, 37, 39, 42, 103, 117

[156] MIURA, N., NAGASAKA, A., AND MIYATAKE, T. Automatic feature extraction from non-uniform finger vein image and its application to personal identification. In *MVA* (2002), pp. 253–256. 22, 42

[157] MIURA, N., NAGASAKA, A., AND MIYATAKE, T. Feature extraction of finger-vein patterns based on repeated line tracking and its application to personal identification. *Machine Vision and Applications 15* (2004), 194–203. doi:10.1007/s00138-004-0149-2. 22, 42, 61, 102

[158] MIURA, N., NAGASAKA, A., AND MIYATAKE, T. Extraction of finger-vein patterns using maximum curvature points in image profiles. In *MVA'05* (2005), pp. 347–350. 22, 42

[159] MIURA, N., NAGASAKA, A., AND MIYATAKE, T. Extraction of Finger-Vein Patterns Using Maximum Curvature Points in Image Profiles. *IEICE Trans Inf Syst E90-D*, 8 (2007), 1185–1194. doi:10.1093/ietisy/e90-d.8.1185. ix, 22, 42, 61, 102

[160] MONIZ, E. *Die cerebrale Arteriographie und Phlebographie*. Handbuch der Neurologie. Ergänzungsserie. Springer, 1940. 12

[161] MORALES, A., TRAVIESO, C., FERRER, M., AND ALONSO, J. Improved finger-knuckle-print authentication based on orientation enhancement. *Electronics Letters 47*, 6 (17 2011), 380 –381. doi:10.1049/el.2011.0156. 140, 141, 148

[162] MULYONO, D., AND JINN, H. S. A study of finger vein biometric for personal identification. In *2008 International Symposium on Biometrics and Security Technologies (ISBAST 2008)* (April 2008), pp. 1 –8. doi:10.1109/ISBAST.2008.4547655. 22, 42

[163] NADORT, A. The hand vein pattern used as a biometric feature. Master's thesis, Universiteit Amsterdam, 2007. 9

[164] NANYANG TECHNOLOGICAL UNIVERSITY. *http://www.ntu.edu.sg*, March 2009. 64

[165] NARAYANASAMY, G. *Advances in Biomedical Applications and Assessment of Ultrasound Nonrigid Image Registration*. Ph.D. thesis, University of Michigan, 2009. 17

[166] OLSEN, M., HARTUNG, D., BUSCH, C., AND LARSEN, R. Convolution approach for feature detection in topological skeletons obtained from vascular patterns. In *IEEE Symposium Series on Computational Intelligence 2011* (April 2011). doi:10.1109/CIBIM.2011.5949223. 7, 48, 91, 122, 199

[167] OLSEN, M. A. Vein pattern recognition - a rotation, translation and scale invariant approach. Master's thesis, Technical University of Denmark, DTU Informatics, E-mail: reception@imm.dtu.dk, Asmussens Alle, Building 305, DK-2800 Kgs. Lyngby, Denmark, 2010. Supervised by Professor Rasmus Larsen, rl@imm.dtu.dk, DTU Informatics. Thesis not publicly available. 215

[168] OLSEN, M. A., HARTUNG, D., BUSCH, C., AND LARSEN, R. Contrast enhancement and metrics for biometric vein pattern recognition. In *Advanced Intelligent Computing Theories and Applications*, D.-S. Huang, M. McGinnity, L. Heutte, and X.-P. Zhang, Eds., vol. 93 of *Communications in Computer and Information Science*. Springer Berlin Heidelberg, 2010, pp. 425–434. doi:10.1007/978-3-642-14831-6_56. 7, 48, 69, 102

[169] OTSU, N. A Threshold Selection Method from Grey-Level Histograms. *Systems, Man and Cybernetics, IEEE Transactions 9* (January 1979), 62–66. doi:10.1109/TSMC.1979.4310076. 86, 102, 104, 110

[170] PARTHASARADHI, S., DERAKHSHANI, R., HORNAK, L., AND SCHUCKERS, S. Time-series detection of perspiration as a liveness test in fingerprint devices. *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on 35*, 3 (August 2005), 335 –343. doi:10.1109/TSMCC.2005.848192. 31

[171] PASCUAL, S., J.E., URIARTE-ANTONIO, J., SANCHEZ-REILLO, R., AND LORENZ, M. Capturing Hand or Wrist Vein Images for Biometric Authentication Using Low-Cost Devices. In *Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2010 Sixth International Conference on* (October 2010), pp. 318 –322. doi:10.1109/IIHMSP.2010.85. 22, 35, 36, 48, 82, 86, 109, 120, 121, 128, 190, 196

[172] PAUL MACGREGOR, R. W. Veincheck: Imaging for security and personnel identification. *Advanced Imaging 6*, 7 (1991), 25–56. 13, 22

[173] PAUL MACGREGOR, R. W. Veincheck lends a hand for high security. *MCB UP Ltd: Sensor Review 12*, 3 (1992), 19–23. 22

[174] PELI, E. Contrast in complex images. *Journal of the Optical Society of America A 7* (1990), 2032–2040. 73

[175] PENG, H., LONG, F., AND DING, C. Feature selection based on mutual information: criteria of max-dependency, max-relevance, and min-redundancy. *IEEE Transactions on Pattern Analysis and Machine Intelligence 27* (2005), 1226–1238. 130

[176] PERSSON, A. B., AND BUSCHMANN, I. R. Vascular growth in health and disease. *Frontiers in Molecular Neuroscience 4*, 00014 (2011). doi:10.3389/fnmol.2011.00014. 10

[177] PFLUG, A. Finger vein recognition - extraction and comparison of vein patterns for biometric purposes. Master's thesis, Department of Computer Science, Hochschule (Darmstadt) - CASED, Center for Advanced Security Research (Darmstadt), 2011. 215

[178] PFLUG, A., HARTUNG, D., AND BUSCH, C. Feature extraction from vein images using spatial information and chain codes. *Information Security Technical Report*, 0 (2012), –. doi:10.1016/j.istr.2012.02.003. 7, 41, 42, 44, 48, 99

[179] POH, N., BOURLAI, T., AND KITTLER, J. Quality-based score normalisation with device qualitative information for multimodal biometric fusion. *IEEE Trans. on Systems, Man, and Cybernatics (part B) 40*, 539–554 (2010). 82

[180] POH, N., AND KITTLER, J. A unified framework for biometric expert fusion incorporating quality measures. *IEEE Trans. on Pattern Analysis and Machine Intelligence* (2010). 82

[181] PRAHL, S. *Molar extinction coefficients of oxy and deoxyhemoglobin*, July 2012. 23

[182] PRAHL, S. *Molar extinction coefficients of variation of melanin*, July 2012. 23

[183] PRENEL, B., AND OORSCHOT, P. C. V. Mdx-mac and building fast macs from hash functions. In *CRYPTO '95: Proceedings of the 15th Annual International Cryptology Conference on Advances in Cryptology* (London, UK, 1995), Springer-Verlag, pp. 1–14. 173

[184] RAGHAVENDRA, R., IMRAN, M., RAO, A., AND KUMAR, G. H. Multimodal biometrics: Analysis of handvein & palmprint combination used for person verification. *Emerging Trends in Engineering & Technology, International Conference on 0* (2010), 526 –530. doi:10.1109/ICETET.2010.14. 82

[185] RATHA, N., CHIKKERUR, S., CONNELL, J., AND BOLLE, R. Generating cancelable fingerprint templates. *Pattern Analysis and Machine Intelligence, IEEE Transactions on 29*, 4 (April 2007), 561–572. doi:10.1109/TPAMI.2007.1004. 34

[186] RATHA, N., CONNELL, J., AND BOLLE, R. Enhancing security and privacy of biometric-based authentication systems. *IBM Systems Journal 40* (2001). 63

[187] RATHGEB, C., AND UHL, A. A survey on biometric cryptosystems and cancelable biometrics. *EURASIP Journal on Information Security 2011*, 1 (2011), 3. doi:10.1186/1687-417X-2011-3. 34

[188] REDDY, P., KUMAR, A., RAHMAN, S., AND MUNDRA, T. A new antispoofing approach for biometric devices. *Biomedical Circuits and Systems, IEEE Transactions on 2*, 4 (December 2008), 328 –337. doi:10.1109/TBCAS.2008.2003432. 30

[189] RÖNTGEN, W. *Eine neue Art von Strahlen*. Verlag und Druck der Stahel'schen K. Hof- und Universitäts-Buch- und Kunsthandlung, 1896. 12

[190] ROWE, R., NIXON, K., AND BUTLER, P. Multispectral fingerprint image acquisition. In *Advances in Biometrics*, N. K. Ratha and V. Govindaraju, Eds. Springer London, 2008, pp. 3–23. 10.1007/978-1-84628-921-7_1. doi:10.1007/978-1-84628-921-7_1. 30

[191] RUKHIN, A., SOTO, J., NECHVATAL, J., SMID, M., BARKER, E., LEIGH, S., LEVENSON, M., VANGEL, M., BANKS, D., HECKERT, A., DRAY, J., AND VO, S. National Institute for Standards and Technology, NIST Special Publication 800-22 Revision 1a. Revised: April 2010. 205

[192] RUSINKIEWICZ, S., AND LEVOY, M. Efficient Variants of the ICP Algorithm. Tech. rep., Stanford University, 2001. 105

[193] RUTKOWSKA, J. Introducing Stealth Malware Taxonomy. http://www.invisiblethings.org/papers/malware-taxonomy.pdf, November 2006. 150

[194] SANCHEZ-REILLO, R., FERNANDEZ-SAAVEDRA, B., LIU-JIMENEZ, J., AND SANCHEZ-AVILA, C. Vascular biometric systems and their security evaluation. In *2007 41st Annual IEEE International Carnahan Conference on Security Technology* (October 2007), pp. 44–51. 22, 82

[195] SCHEIRER, W. J., BISHOP, B., AND BOULT, T. E. Beyond pki: The biocryptographic key infrastructure. In *The IEEE International Workshop on Information Forensics and Security (WIFS)* (December 2010). 56

[196] SCHEIRER, W. J., BISHOP, B., AND BOULT, T. E. Beyond pki: The biocryptographic key infrastructure. In *Security and Privacy in Biometrics*, P. Campisi, Ed. Springer-Verlag, 2012. 56

[197] SCHEIRER, W. J., AND BOULT, T. E. Bio-cryptographic protocols with bipartite biotokens. In *The Biometrics Symposium, held in conjunction with the Biometrics Consortium Conference (BCC)* (September 2008). 56

[198] SCHEIRER, W. J., AND BOULT, T. E. Bipartite biotokens: Definition, implementation, and analysis. In *The 3rd IAPR/IEEE International Conference on Biometrics (ICB)* (June 2009). 56

[199] SCHUCKERS, S., AND ABHYANKAR, A. Detecting liveness in fingerprint scanners using wavelets: Results of the test dataset. In *Biometric Authentication*, D. Maltoni and A. Jain, Eds., vol. 3087 of *Lecture Notes in Computer Science*. Springer Berlin / Heidelberg, 2004, pp. 100–110. 31

[200] SCHULZ, K. *Spectrometric analyses on reoxygenation of haemoglobin in livores after post-mortem exposure to a cold environment*. Ph.D. thesis, Universitt Freiburg, June 2009. 31, 33

[201] SEIGWORTH, G. R. Bloodletting over the centuries. *N Y State J Med 80*, 13 (December 1980), 2022–2028. 12

[202] SETHIAN, J. A. A fast marching level set method for monotonically advancing fronts. In *Proc. Nat. Acad. Sci* (1995), pp. 1591–1595. 104

[203] SHAHIN, M., BADAWI, A., AND KAMEL, M. Biometric authentication using fast correlation of near infrared hand vein patterns. *International journal of Biomedical sciences 2*, 3 (2007), 1306–1216. 22, 43

[204] SHAHIN, M., BADAWI, A., AND RASMY, M. A multimodal hand vein, hand geometry, and fingerprint prototype design for high security biometrics. In *Biomedical Engineering Conference, 2008. CIBEC 2008. Cairo International* (December 2008), pp. 1 –6. doi:10.1109/CIBEC.2008.4786038. 22, 24

[205] SHAO, X., XU, H., VELDHUIS, R., AND SLUMP, C. A 3-layer coding scheme for biometry template protection based on spectral minutiae. In *Acoustics, Speech and Signal Processing (ICASSP), 2011 IEEE International Conference on* (May 2011), pp. 1948 –1951. doi:10.1109/ICASSP.2011.5946890. 55

[206] SHIMOOKA, T., AND SHIMIZU, K. Artificial immune system for personal identification with finger vein pattern. In *Knowledge-Based Intelligent Information and Engineering Systems*, M. Negoita, R. Howlett, and L. Jain, Eds., vol. 3214 of *Lecture Notes in Computer Science*. Springer Berlin / Heidelberg, 2004, pp. 511–518. 10.1007/978-3-540-30133-2_67. doi:10.1007/978-3-540-30133-2_67. 22, 42

[207] SHIN, J.-H., HWANG, H.-Y., AND CHIEN, S.-I. Detecting fingerprint minutiae by run length encoding scheme. *Pattern Recogn. 39*, 6 (2006), 1140–1154. doi:10.1016/j.patcog.2005.12.013. 94

[208] SIMONE, G., PEDERSEN, M., AND HARDEBERG, J. Y. Measuring perceptual contrast in digital images. *Journal of Visual Communication and Image Representation 23*, 3 (2012), 491 – 506. doi:10.1016/j.jvcir.2012.01.008. 73

[209] SONI, M., GUPTA, S., AND RAO, M. A New Vein Pattern-based Verification System. *International Journal of Computer Science and Information Security 8*, 1 (2010), 58–63. 22, 43, 102

[210] SOUTAR, C., ROBERGE, D., STOIANOV, A., GILROY, R., AND VIJAYA KUMAR, B. V. K. Biometric Encryption using image processing. In *Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series* (April 1998), R. L. van Renesse, Ed., vol. 3314 of *Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series*, pp. 178–188. 34

[211] STANDRING, S., AND GRAY, H. *Gray's anatomy : the anatomical basis of clinical practice / editor-in-chief, Susan Standring*, 40th ed. ed. Churchill Livingstone, Edinburgh :, 2008. 9

[212] STRUC, V., AND PAVESIC, N. Illumination Invariant Face Recognition by Non-local Smoothing. In *Proceedings of the BIOID Multicomm* (September 2008). 104, 110, 119

[213] STUCKER, M., STRUK, P. A., HOFFMANN, K., SCHULZE, L., ROCHLING, A., AND LUBBERS, D. W. The transepidermal oxygen flux from the environment is in balance with the capillary oxygen supply. *J. Invest. Dermatol. 114*, 3 (March 2000), 533–540. 33

[214] SWEENEY, E. Veincheck a technical perspective. *Information Security Technical Report 3*, 1 (1998), 47 – 51. doi:10.1016/S1363-4127(98)80018-6. 22

[215] SZCZEPANSKI, J., WAJNRYB, E., AMIG, J. M., SANCHEZ-VIVES, M. V., AND SLATER, M. Biometric random number generators. *Computers & Security 23*, 1 (2004), 77 – 84. 205

[216] T. MATSUMOTO, H. MATSUMOTO, K. Y., AND HOSHINO, S. Impact of artificial gummy fingers on fingerprint systems. *Proc. SPIE, Optical Security and Counterfeit Deterrence Techniques IV 4677* (January 2002), 275–289. 27

[217] TAN, B., AND SCHUCKERS, S. A. C. New approach for liveness detection in fingerprint scanners based on valley noise analysis. *J. Electronic Imaging 17*, 1 (2008), 011009. doi:10.1117/1.2885133. 29

[218] TANAKA, T., AND KUBO, N. Biometric authentication by hand vein patterns. In *SICE 2004 Annual Conference* (August 2004), vol. 1, pp. 249 –253 vol. 1. 22, 41, 43

[219] TANG, C., KONG, A. W. K., AND CRAFT, N. Uncovering vein patterns from color skin images for forensic analysis. In *Proceedings of the 2011 IEEE Conference on Computer Vision and Pattern Recognition* (Washington, DC, USA, 2011), CVPR '11, IEEE Computer Society, pp. 665–672. doi:10.1109/CVPR.2011.5995531. 24, 53

[220] TELEA, A., AND VAN WIJK, J. J. An Augmented Fast Marching Method for Computing Skeletons and Centerlines. In *Joint Eurographics - IEEE TCVG Symposium on vizalization* (2002). 104, 105, 110, 121

[221] THE HONG KONG POLYTECHNIC UNIVERSITY. The hong kong polytechnic university finger image database (version 1.0). ix, 36, 37, 40

[222] TOTH, B. Biometric liveness detection. *Information Security Bulletin 10* (2005), 291–297. 27

[223] TSOKOS, M. Postmortem changes and artifacts occurring during the early postmortem interval. In *Forensic Pathology Reviews*, M. Tsokos and M. Tsokos, Eds., vol. 3 of *Forensic Pathology Reviews*. Humana Press, 2005, pp. 183–238. 10.1007/978-1-59259-910-3_5. doi:10.1007/978-1-59259-910-3_5. 33

[224] TSUTOMU, M., TAKUJI, H., TAKEHIRO, T., TOMOKI, M., AND KENJI, S. Liveness detection and failure to enroll in biometrics (2) : A research on vein pattern based authentication, part 1. *Technical report of IEICE. ISEC 105*, 51 (2005), 29–33. 32

[225] TUYLS, P., AKKERMANS, A. H. M., KEVENAAR, T. A. M., SCHRIJEN, G.-J., BAZEN, A. M., AND VELDHUIS, R. N. J. Practical biometric authentication with template protection. In *5th Int. Conf. on Audio- and Video-Based Personal Authentication (AVBPA), Rye Brook, New York* (Heidelberg, July 2005), T. Kanade, A. K. Jain, and N. K. Ratha, Eds., vol. LNCS 3546, Springer-Verlag Berlin, pp. 436–446. doi:10.1007/11527923_45. 34, 40, 47, 51, 63, 64, 117, 181

[226] TUYLS, P., AND GOSELING, J. Capacity and examples of template-protecting biometric authentication systems. In *Biometric Authentication* (2004), vol. 3087 of *Lecture Notes in Computer Science*, Springer Berlin / Heidelberg, pp. 158–170. doi:10.1007/b99174. 117, 151, 156, 165, 181, 195, 202, 207

[227] UNIVERSIDAD DE LAS PALMAS DE GRAN CANARIA. Gpds100veinsccdcylindrical / gpds100veinscmoscylindrical database. 39, 40

[228] URIARTE-ANTONIO, J., HARTUNG, D., PASCUAL, J., AND SANCHEZ-REILLO, R. Vascular biometrics based on a minutiae extraction approach. In *Security Technology (ICCST), 2011 IEEE International Carnahan Conference on* (October 2011), pp. 1 –7. doi:10.1109/CCST.2011.6095927. 7, 41, 43, 44, 103

[229] VIDEOMETER A/S. Videometerlab. http://www.videometer.com/products/videometerlab/videometerlab.html. ix, 22, 25, 26

[230] VLACHOS, M., AND DERMATAS, E. Vein Segmentation in Infrared Images Using Compound Enhancing and Crisp Clustering. *Lecture Notes in Computer Science 5008/2008* (2008), 393–402. doi:10.1007/978-3-540-79547-6_38. 22, 102

[231] VO-DINH, T. *Biomedical Photonics Handbook*. CRC Press, 2003. 21

[232] WALL, M. GAlib: A C++ library of genetic algorithm components. *Mechanical Engineering Department, Massachusetts Institute of Technology* (1996). 189

[233] WANG, H.-B., TAO, L., AND HU, X.-Y. Novel algorithm for hand vein recognition based on retinex method and sift feature analysis. In *Electrical Power Systems and Computers*, X. Wan, Ed., vol. 99 of *Lecture Notes in Electrical Engineering*. Springer Berlin Heidelberg, 2011, pp. 559–566. 10.1007/978-3-642-21747-0_70. doi:10.1007/978-3-642-21747-0_70. 22, 43

[234] WANG, J.-G., YAU, W.-Y., SUWANDY, A., AND SUNG, E. Fusion of palmprint and palm vein images for person recognition based on "laplacianpalm" feature. In *Computer Vision and Pattern Recognition, 2007. CVPR '07. IEEE Conference on* (June 2007), pp. 1 –8. doi:10.1109/CVPR.2007.383386. 22, 24

[235] WANG, K., MA, H., POPOOLA, O., AND LI, X. A novel finger vein pattern extraction method using oriented filtering technology. In *Intelligent Control and Automation (WCICA), 2010 8th World Congress on* (July 2010), pp. 6240 –6244. doi:10.1109/WCICA.2010.5554393. 22, 42

[236] WANG, K., ZHANG, Y., YUAN, Z., AND ZHUANG, D. Hand Vein Recognition Based on Multi Supplemental Features of Multi-Classifier Fusion Detection. In *International Conference on Mechatronics and Automation* (June 2006). 22, 43, 103

[237] WANG, L., AND LEEDHAM, G. A Thermal Hand Vein Pattern Verification System. *LNCS: Pattern Recognition and Image Analysis 3687/2005* (2005), 58–65. doi:10.1007/11552499_7. 19, 43, 102, 104

[238] WANG, L., AND LEEDHAM, G. Gray-scale skeletonization of thermal vein patterns using the watershed algorithm in vein pattern biometrics. In *Computational Intelligence and Security, 2006 International Conference on* (November 2006), vol. 2, pp. 1597 –1602. doi:10.1109/ICCIAS.2006.295332. 19

[239] WANG, L., AND LEEDHAM, G. Near- and far- infrared imaging for vein pattern biometrics. In *Video and Signal Based Surveillance, 2006. AVSS '06. IEEE International Conference on* (November 2006), pp. 52–52. doi:10.1109/AVSS.2006.80. 19, 21, 22, 43

[240] WANG, L., AND LEEDHAM, G. A watershed algorithmic approach for gray-scale skeletonization in thermal vein pattern biometrics. In *Computational Intelligence and Security*, Y. Wang, Y.-m. Cheung, and H. Liu, Eds., vol. 4456 of *Lecture Notes in Computer Science*. Springer Berlin / Heidelberg, 2007, pp. 935–942. 10.1007/978-3-540-74377-4_98. doi:10.1007/978-3-540-74377-4_98. 19, 35, 128, 190

[241] WANG, L., LEEDHAM, G., AND CHO, D. Infrared imaging of hand vein patterns for biometric purposes. *Computer Vision IET 1*, 3-4 (December 2007), 113–122. ix, xi, 19, 20, 21, 22, 43, 60, 61, 63, 64, 196

[242] WANG, L., LEEDHAM, G., AND CHO, D. S.-Y. Minutiae feature analysis for infrared hand vein pattern biometrics. *Pattern Recognition 41*, 3 (2008), 920 – 929. Part Special issue: Feature Generation and Machine Learning for Robust Multimodal Biometrics. doi:10.1016/j.patcog.2007.07.012. 19, 35, 36, 43, 48, 70, 86, 116, 128, 129, 130, 181, 190

[243] WANG, Y., LI, K., CUI, J., SHARK, L.-K., AND VARLEY, M. Study of hand-dorsa vein recognition. In *Advanced Intelligent Computing Theories and Applications*, D.-S. Huang, Z. Zhao, V. Bevilacqua, and J. Figueroa, Eds., vol. 6215 of *Lecture Notes in Computer Science*. Springer Berlin / Heidelberg, 2010, pp. 490–498. 10.1007/978-3-642-14922-1_61. doi:10.1007/978-3-642-14922-1_61. 22, 43

[244] WANG, Y., LI, K., SHARK, L., AND VARLEY, M. Hand-dorsa vein recognition based on coded and weighted partition local binary patterns. In *Hand-Based Biometrics (ICHB), 2011 International Conference on* (November 2011), pp. 1 –5. doi:10.1109/ICHB.2011.6094331. 22, 43

[245] WANKOU, Y., CHANGYIN, S., AND ZHONGXI, S. Finger-knuckle-print recognition using gabor feature and olda. *Proceedings of the 30th Chinese Control Conference* (2011). 140, 141

[246] WATANABE, M. Palm vein authentication. In *Advances in Biometrics*, N. K. Ratha and V. Govindaraju, Eds. Springer London, 2008, pp. 75–88. doi:10.1007/978-1-84628-921-7_5. 24

[247] WATANABE, M., AND ENDOH, T. Palm Vein Authentication Technology and its Applications. In *Proceedings of the Biometric Consortium Conference* (September 2005). 22, 42, 100

[248] WATNE, K. S. Thermal imaging of ear biometrics for authentication purposes. Master's thesis, Gjøvik University College, 2008. 17

[249] WAYMAN, J. Technical testing and evaluation of biometric identification devices. In *Biometrics*, A. Jain, R. Bolle, and S. Pankanti, Eds. Springer US, 1996, pp. 345–368. doi:10.1007/0-306-47044-6_17. 35

[250] WEICKERT, J. Applications of nonlinear diffusion in image processing and computer vision. *Acta Math. Univ. Comenianae 70* (2001), 33–50. 104, 110, 119

[251] WEIGOLD, T., KRAMP, T., HERMANN, R., HÖRING, F., BUHLER, P., AND BAENTSCH, M. The zurich trusted information channel — an efficient defence against man-in-the-middle and malicious software attacks. In *Trust '08: Proceedings of the 1st international conference on Trusted Computing and Trust in Information Technologies* (Berlin, Heidelberg, 2008), Springer-Verlag, pp. 75–91. doi:10.1007/978-3-540-68979-9_6. 152, 153

[252] WIDMAIER, E., RAFF, H., AND STRANG, K. *Vander's human physiology: the mechanisms of body function*. McGraw-Hill, 2006. 9, 10, 16

[253] WILSON, C. *Vein Pattern Recognition: A Privacy-Enhancing Biometric*. CRC Press/Taylor & Francis, 2010. 9

[254] WITOPIL, K. Schutzmanahmen im Leipziger DHL-Hub. *Protector 6* (June 2008), 44–45. 100

[255] WOODWARD, J., ORLANS, N., AND HIGGINS, P. *Biometrics: Identity Assurance in the Information Age*. Rsa Press Series. McGraw-Hill/Osborne, 2003. 27

[256] WORLD HEALTH ORGANIZATION (WHO). *The world health report 2004 - changing history.*, 2004. 12, 34, 62

[257] WU, J.-D., AND LIU, C.-T. Finger-Vein Pattern Identification Using Principal Component Analysis ans the Neural Network technique. *Expert Systems with Applications 38* (2011), 5423–5427. 22, 42

[258] WU, J.-D., AND YE, S.-H. Driver identification using finger-vein patterns with radon transform and neural network. *Expert Systems with Applications 36*, 3, Part 2 (2009), 5793 – 5799. doi:10.1016/j.eswa.2008.07.042. 22, 42

[259] WU, X., GAO, E., TANG, Y., AND WANG, K. A novel biometric system based on hand vein. In *2010 Fifth International Conference on Frontier of Computer Science and Technology (FCST)* (August 2010), pp. 522 –526. doi:10.1109/FCST.2010.65. 82

[260] XU, H., VELDHUIS, R., KEVENAAR, T., AKKERMANS, A., AND BAZEN, A. Spectral minutiae: A fixed-length representation of a minutiae set. In *2008 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)* (June 2008), pp. 1–6. doi:10.1109/CVPRW.2008.4563120. 86, 103, 123, 127

[261] XU, H., VELDHUIS, R., KEVENAAR, T., AND AKKERMANS, T. A fast minutiae-based fingerprint recognition system. *Systems Journal, IEEE 3*, 4 (December 2009), 418 –427. doi:10.1109/JSYST.2009.2034945. 41, 54

[262] XU, H., AND VELDHUIS, R. N. Binary representations of fingerprint spectral minutiae features. *Pattern Recognition, International Conference on 0* (2010), 1212–1216. doi:10.1109/ICPR.2010.302. 41, 54

[263] XU, H., AND VELDHUIS, R. N. Complex spectral minutiae representation for fingerprint recognition. In *2010 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, CVPRW* (June 2010), IEEE Computer Society Press, pp. 1–8. 123, 125

[264] XU, H., VELDHUIS, R. N. J., BAZEN, A. M., KEVENAAR, T. A. M., AKKERMANS, T. A. H. M., AND GOKBERK, B. Fingerprint verification using spectral minutiae representations. *Trans. Info. For. Sec. 4* (September 2009), 397–409. doi:10.1109/TIFS.2009.2021692. 48, 117, 123, 125, 181

[265] XUEYAN, L., AND SHUXU, G. *Pattern Recognition Techniques, Technology and Applications*. InTech, November 2008, ch. 23: The Fourth Biometric - Vein Recognition, pp. 537–546. 41

[266] XUEYAN, L., SHUXU, G., FENGLI, G., AND YE, L. Vein pattern recognitions by moment invariants. In *Bioinformatics and Biomedical Engineering, 2007. ICBBE 2007. The 1st International Conference on* (July 2007), pp. 612 –615. doi:10.1109/ICBBE.2007.160. 22, 41, 42, 102

[267] YAMAKOSHI, K., AND YAMAKOSHI, Y. Pulse glucometry: A new approach for noninvasive blood glucose measurement using instantaneous differential near-infrared spectrophotometry. *J Biomed Opt 11*, 5 (2006), 054028. 31

[268] YAMAKOSHI, Y., OGAWA, M., YAMAKOSHI, T., SATOH, M., NOGAWA, M., TANAKA, S., TAMURA, T., ROLFE, P., AND YAMAKOSHI, K. A new non-invasive method for measuring blood glucose using instantaneous differential near infrared spectrophotometry. *Conf Proc IEEE Eng Med Biol Soc 2007* (2007), 2964–2967. 31

[269] YANAGAWA, T., AOKI, S., AND OHYAMA, T. E. A. Human finger vein images are diverse and its patterns are useful for personal identification. *2007-12, Kyushu University Preprint Series in Mathematics* (2007). 22, 42, 60, 196

[270] YANG, B., HARTUNG, D., SIMOENS, K., AND BUSCH, C. Dynamic random projection for biometric template protection. In *Biometrics: Theory Applications and Systems (BTAS), 2010 Fourth IEEE International Conference on* (September 2010), pp. 1 –7. doi:10.1109/BTAS.2010.5634538. 7

[271] YANG, J., AND LI, X. Efficient finger vein localization and recognition. In *Pattern Recognition (ICPR), 2010 20th International Conference on* (August 2010), pp. 1148 – 1151. 42, 103

[272] YANG, J., SHI, Y., AND YANG, J. Finger-vein recognition based on a bank of gabor filters. In *Computer Vision - ACCV 2009*, H. Zha, R.-i. Taniguchi, and S. Maybank, Eds., vol. 5994 of *Lecture Notes in Computer Science*. Springer Berlin / Heidelberg, 2010, pp. 374–383. 82

[273] YANG, J., AND WANG, W. Finger-vein image enhancement based on orientation field. In *Hand-Based Biometrics (ICHB), 2011 International Conference on* (November 2011), pp. 1 –6. doi:10.1109/ICHB.2011.6094322. 22

[274] YANG, W., RAO, Q., AND LIAO, Q. Personal identification for single sample using finger vein location and direction coding. In *Hand-Based Biometrics (ICHB), 2011 International Conference on* (November 2011), pp. 1 –6. doi:10.1109/ICHB.2011.6094318. 42

[275] YANG, W., XU, X., AND LIAO, Q. Personal Authentication Unsing Finger Vein Patterns and Finger-Dorsa Texture Fusion. In *MM '09 Proceedings of the 17th ACM international conference on Multimedia* (2009). 22, 42, 102

[276] YIN, Y., LIU, L., AND SUN, X. Sdumla-hmt: a multimodal biometric database. In *Proceedings of the 6th Chinese conference on Biometric recognition* (Berlin, Heidelberg, 2011), CCBR'11, Springer-Verlag, pp. 260–268. 22, 24, 38

[277] YOSHITOMI, Y., MIYAURA, T., TOMITA, S., AND KIMURA, S. Face identification using thermal image processing. In *Robot and Human Communication, 1997. RO-MAN '97. Proceedings., 6th IEEE International Workshop on* (September 1997), pp. 374 –379. doi:10.1109/ROMAN.1997.647015. 17

[278] YUKSEL A, A., AKARUN, L., AND SANKUR, B. Biometric identification through hand vein patterns. In *2010 IEEE 18th Signal Processing and Communications Applications Conference (SIU)* (April 2010), pp. 708 –711. doi:10.1109/SIU.2010.5652148. 82

[279] ZENTRALER KREDITAUSSCHUSS (ZKA). Financial Transactions Services (FinTS). http://www.hbci-zka.de/, February 2010. 152

[280] ZHANG, L., ZHANG, L., AND ZHANG, D. Finger-knuckle-print: a new biometric identifier. In *Proceedings of the 16th IEEE international conference on Image processing* (Piscataway, NJ, USA, 2009), ICIP'09, IEEE Press, pp. 1961–1964. 139, 140, 141, 148

[281] ZHANG, L., ZHANG, L., AND ZHANG, D. Monogeniccode: A novel fast feature coding algorithm with applications to finger-knuckle-print recognition. In *Emerging Techniques and Challenges for Hand-Based Biometrics (ETCHB), 2010 International Workshop on* (August 2010), pp. 1 –4. doi:10.1109/ETCHB.2010.5559286. 140, 141, 148

[282] ZHANG, L., ZHANG, L., ZHANG, D., AND GUO, Z. Phase congruency induced local features for finger-knuckle-print recognition. *Pattern Recognition 45*, 7 (2012), 2522–2531. doi:10.1016/j.patcog.2012.01.017. 148

[283] ZHANG, L., ZHANG, L., ZHANG, D., AND ZHU, H. Online finger-knuckle-print verification for personal authentication. *Pattern Recogn. 43* (July 2010), 2560–2571. doi:10.1016/j.patcog.2010.01.020. 140, 141

[284] ZHANG, L., ZHANG, L., ZHANG, D., AND ZHU, H. Ensemble of local and global information for finger-knuckle-print recognition. *Pattern Recogn. 44*, 9 (September 2011), 1990–1998. doi:10.1016/j.patcog.2010.06.007. 140, 141, 148

[285] ZHANG, T. Y., AND SUEN, C. Y. A fast parallel algorithm for thinning digital patterns. *Commun. ACM 27*, 3 (March 1984), 236–239. doi:10.1145/357994.358023. 93, 104

[286] ZHANG, Z., MA, S., AND HAN, X. Multiscale feature extraction of finger-vein patterns based on curvelets and local interconnection structure neural network. In *ICPR '06: Proceedings of the 18th International Conference on Pattern Recognition* (Washington, DC, USA, 2006), IEEE Computer Society, pp. 145–148. doi:10.1109/ICPR.2006.848. 22, 42, 61

[287] ZHANG, Z. B., WU, D. Y., MA, S. L., AND MA, J. Multiscale feature extraction of finger-vein patterns based on wavelet and local interconnection structure neural network. In *Neural Networks and Brain, 2005. ICNN B '05. International Conference on* (October 2005), vol. 2, pp. 1081 –1084. doi:10.1109/ICNNB.2005.1614805. 22, 42

[288] ZHOU, X. *Privacy and Security Assessment of Biometric Template Protection*. Ph.D. thesis, Technical University Darmstadt, Germany, February 2012. 35, 55

[289] ZHOU, X., KEVENAAR, T., KELKBOOM, E., BUSCH, C., VAN DER VEEN, M., AND NOUAK, A. Privacy enhancing technology for a 3d-face recognition system. In *BIOSIG: Biometrics and Electronic Signatures* (July 2007), vol. P-108 of *Lecture Notes in Informatics*, GI-Edition, pp. 3–14. 63

[290] ZHOU, X., WOLTHUSEN, S. D., BUSCH, C., AND KUIJPER, A. A security analysis of biometric template protection schemes. In *Image Analysis and Recognition* (2009), vol. 5627 of *Lecture Notes in Computer Science*, Springer Berlin / Heidelberg, pp. 429–438. doi:10.1007/978-3-642-02611-9_43. 157

[291] ZHOU, Y., AND KUMAR, A. Contactless palm vein identification using multiple representations. In *Biometrics: Theory Applications and Systems (BTAS), 2010 Fourth IEEE International Conference on* (September 2010), pp. 1 –6. doi:10.1109/BTAS.2010.5634470. 22, 37, 39, 42

[292] ZUIDERVELD, K. Contrast limited adaptive histogram equalization. In *Graphics gems IV*, P. S. Heckbert, Ed. Academic Press Professional, Inc., San Diego, CA, USA, 1994, pp. 474–485. 51, 72

[293] ZWIESELE, A., MUNDE, A., BUSCH, C., AND DAUM, H. Biois study. comparative study of biometric identification systems. In *Security Technology, 2000. Proceedings. IEEE 34th Annual 2000 International Carnahan Conference on* (2000), pp. 60 –63. doi:10.1109/CCST.2000.891168. 27