



Gjøvik University College
*Faculty of Computer Science and Media Technology*

# Multimodal Biometric Authentication using Fingerprint and Iris Recognition in Identity Management

**Master's Thesis (30 ECTS)**

by

**Kamer Vishi**

*A dissertation submitted in partial fulfillment of the requirements for the degree*
of
**Master of Science in Information Security (MSc.)**

Supervisor: Prof. Dr. Şule Yildirim Yayilgan
Co-supervisor: Mohammad O. Derawi, PhD
External supervisor: Asbjørn Hovstø, (PortAhead)

Gjøvik, Norway 2012

*(Submitted on July 1st, 2012)*

Avdeling for
informatikk og medieteknikk
Høgskolen i Gjøvik
Postboks 191
2802 Gjøvik

Department of Computer Science
and Media Technology
Gjøvik University College
Box 191
N-2802 Gjøvik
Norway

# Multimodal Biometric Authentication using Fingerprint and Iris Recognition in Identity Management

Kamer Vishi

1st of July 2012

*I dedicate this work to my fiancée Blerta and my dearest parents, Hajrush (dad) and Habibe (mom - passed away on 20.07.2003)*

# Declaration of Authorship

I, **Kamer Vishi**, hereby declare that the work presented in this master's thesis is completely my own work, and it is not submitted nor any degree awarded by universities anywhere else. Experiment analysis and results are not previously published or written by another researcher nor any other thesis.

I have cited and acknowledged all sources when were used during this work, in a proper and academic honesty manner.

Place, Date:
*-Gjøvik, July 1, 2012*

Signature:

# Abstract

The majority of deployed biometric systems today use information from a single biometric technology for verification or identification. Large-scale biometric systems have to address additional demands such as larger population coverage and demographic diversity, varied deployment environment, and more demanding performance requirements. Today's single modality biometric systems are finding it difficult to meet these demands, and a solution is to integrate additional sources of information to strengthen the decision process.

A multibiometric system combines information from multiple biometric traits, algorithms, sensors, and other components to make a recognition decision. Besides improving the accuracy, the fusion of biometrics has several advantages such as increasing population coverage, deterring spoofing activities and reducing enrolment failure. The last 5 years have seen an exponential growth in research and commercialization activities in this area, and this trend is likely to continue. Therefore, here we propose a novel multimodal biometric authentication approach fusing iris and fingerprint traits at score-level. We principally explore the fusion of iris and fingerprint biometrics and their potential application as biometric identifiers. The individual comparison scores obtained from the iris and fingerprints are combined at score-level using three score normalization techniques (Min-Max, Z-Score, Hyperbolic Tangent) and four score fusion approaches (Minimum Score, Maximum Score Simple Sum and User Weighting). The fused-score is utilized to classify an unknown user into the genuine or impostor.

The proposed method is evaluated using two fingerprint databases (in total 2000 fingerprint images) and two iris databases (in total 2000 iris images). Fingerprint databases and one of the iris databases are collected by Machine Learning and Applications (MLA) Group at Shandong University in China (SDUMLA-HMT). Fingerprint and iris images are collected by FPR620 optical fingerprint scanner, capacitive fingerprint scanner and an iris acquisition device, respectively. While the other iris database is collected by Institute of Automation, Chinese Academy of Sciences called CASIA-Iris-Lamp. One hundred (100) subjects, 2 fingers, 2 irises and 5 attempts are chosen for our fingerprint and iris experiments. We demonstrated also that the proposed approach improves the performances, considerably.

In parallel with the thesis, another paper was written and submitted to *The International Conference of the Biometrics Special Interest Group - BIOSIG 2012* in Darmstadt, Germany. This article is attached and can be read in Appendix I.

**Kamer Vishi,**
*June 2012, Gjøvik, Norway*

# Acknowledgements

*It took me 6 months or about 1210 effective working hours to finish this report!...*

and today I want to thank the people who supported me to complete the MSc. studies.

First and foremost, I would like to express my deepest appreciation to my supervisor, Prof. Dr. Şule Yildirim Yayilgan for her help and guidance during my thesis work, whose feedback, input and critique has been very inspiring during the course of this research. Additionally, I would like to extend my gratitude to my co-supervisor PhD student Mohammad O. Derawi who has given so much help and advices during the thesis work. I highly appreciate the cooperation with Prof. Dr. Yayilgan and Derawi even though they were very busy with their academic and private life!

The research in this thesis was supported by external supervisor Asbjørn Hovstø(PortAhead AS), *Regionale Forskningsfond Innlandet (RFF Innlandet)* and Birkebeiner AS, to whom I am very thankful.

Next, I would like to thank Prof. Dr. Christoph Busch, Dr. Bian Yang and Prof. Dr. Patrick Bours for teaching me the basics of biometrics and authentication systems and not less, who always took the time to answer my questions. In addition, I would like to thank all professors that have taught me the basics of *information security* during these years of Master's studies. Thank you very much for all the nice fruitful discussion we have had.

I would like to give a special thanks to PhD students Daniel Hartung and Martin Astrup Olsen for supporting me with articles, suggestions and valuable advices during my work. I am grateful to all my colleagues and friends at Gjøvik University College. The atmosphere has always been a perfect source of motivation, even though when the weather reached -20 degrees Celsius outside. The work on my master's thesis on Gjøvik University College served as good basis for my future work.

I want to express my gratitude to Machine Learning Group, Shandong University in Jinan-China, mainly Prof. Dr. Yilong Yin, Lili Liu and Feifei Cui MSc. candidates, who supported with fingerprint and iris databases (SDUMLA-HMT), articles and all answers to my requests regarding to database issues. Furthermore, I would like to thank Center for Biometrics and Security Research Institute of Automation, Chinese Academy of Sciences by providing me the access to their databases, in particular CASIA-Iris-Lamp database.

Next I would like to thank my family back home, father, brothers and sisters, as well as my dearest nieces and nephews for their continuous support and love throughout these years abroad. My father, Hajrush deserves a special thanks for his support, financially and morally. He taught me the value of hard work and education. Next I would like to express my gratitude to my relatives here in Vestby, Rasim, Jetta, Diona and Dion, for their support and advices that they given to me to integrate in Norwegian society.

Last, but not least I would like to thank my fiancée and my colleague, Blerta Lufaj, for her encouragement and support for everything I aspire to.

# Contents

# List of Figures

# List of Tables

# 1 Introduction

In this newly complicated world of terrorism, identity theft, and rampant consumer fraud, biometrics has been heralded as a key technology for identity management, and hence security. As never before has identity management been so important. Governments and enterprises of all sizes have become much more vigilant regarding security. There is always a need to re-examine and potentially improve security, and biometrics is attracting growing interest as fraud increases and the conventional authentication methods - PINs, passwords, and identity cards - prove inadequate to counter the growing threats [14].

Biometric tools have become prominent differentiators for multiple applications in a variety of markets. The use of biometrics offers no panacea to completely remedy society's threats, and it provides no guarantee against terrorist activities. However, biometric technologies remain a critically important component of the total solution. The biometric authentication market has emerged and is expanding at an increasing rate.

Biometric systems are proliferating. The diversity of the various modalities and the many false claims of their promoters and detractors alike have somewhat clouded the market with at best some misinformation and at worst a public concern that this new technology is somehow menacing and will restrict freedoms. Unfortunately, many of the key benefits of biometrics have become obfuscated due to unfortunate sensationalism and myths that have surrounded biometric solutions [15].

Biometric technologies vary in capability, performance, and reliability. The success of a given biometric modality depends not only on the effectiveness of the technology and its implementation, but also on the total security solution for which any biometric system comprises only a part. The next several years will be exciting for the biometric market. We can expect increased user acceptance and demand as biometrics continue to become more user friendly and more reliable. Improved technology and biometric need are converging. There should be significant growth in each of the various biometric modalities, as well as in multimodal biometrics [16].

Because of their security, speed, efficiency, and convenience, biometric authentication systems have the potential to become the new standard for access control. Biometrics replaces or supplements knowledge and possession authentication with a person's physical or behavioral characteristics. Biometrics can be used in any situation where identity badges, PINs/passwords, or keys are needed. Biometrics offers some clear advantages over traditional identity methods:

- Biometric traits cannot be lost, stolen, or borrowed.
- Generally, physical human characteristics are much more difficult to forge than security codes, passwords, badges, or even some encryption keys.
- Biometrics guard against user denial - the principle of nonrepudiation - by providing definitive recognition of an individual.

- Biometrics cannot be delegated or shared. Its use proves that the individual in question was present for a given transaction.
- Identity verification can eliminate the need to carry a token or remember a password, although all three can be used.
- Biometrics is the only technique available today that can determine if a person is who he *denies* he is or if he has pre-enrolled.

Moreover, with the greater demand on biometrics in everyday life, governments are expected to enact statutes that help administer biometric solutions while maintaining privacy and legal support. Indeed, it has been the use of biometric solutions by government agencies and by mainstream industries such as banking and health care that has increased public awareness and acceptance of the technology.

Biometric technologies will play an increasingly larger role in our daily lives, and the following chapters of this research work discuss its various technical aspects, potential applications, challenges, and solutions.

## 1.1 Keywords

Biometrics, Multi-modal Biometrics, Authentication, Fingerprint Recognition, Iris Recognition, Identity Management, Image Quality, Score-level Fusion, Score Normalization, NFIQ, Neurotechnology, VeriFinger, VeriEye.

## 1.2 Thesis Motivation

Unimodal biometric systems face several challenges in today's implementations. The increasingly large enrolment population brings with it a range of issues such as missing biometric traits, the inability to provide good quality samples, and the refusal to use certain biometric traits due to religious and cultural concerns. For instance, there is a certain subset of the population that is incapable of providing fingerprint images due to a genetic disorder called *dermatopathia pigmentosa reticularis* (DPR) [17]. Demographics and occupation have more of an impact on certain biometrics such as fingerprint recognition than others such as iris recognition.

The capability of capturing another biometric trait can reduce the number of failure to enrol cases. Multibiometric systems are capable of capturing samples from multiple sensors. Environmental conditions have an impact on the ability of sensors and on the quality of captured data, and using multiple sensors increases the probability of acquiring good quality samples from at least one of the sensors. Spoofing of biometric systems is a growing concerns, and a layered biometric system can improve security of the overall system. For a spoofing attack to be successful on a multibiometric systems, all the biometric components would need to be successfully attacked [16].

Multibiometric systems can be designed intelligently so that the comparison (matching) performance of the system is better than a unimodal system. The multiple sources of information can be used to increase interclass variability and reduce intraclass variability. This is particularly useful for large-scale biometric systems, but this performance boost depends largely on the statistical independence of the biometric data. The decision process can be tuned at the individual

level to give more weight to the better performing component of the multibiometric system. At a higher level, multibiometric systems provide additional information to resolve cases that are on the boundary of the decision policy.

In this project work, we essentially limit our desire to two biometric traits such as fingerprint and iris. To the best of our knowledge, there is no published research on this field that fused fingerprint and iris recognition at score-level, particularly normalization by minmax, z-score and hyperbolic tangent, and fusion of scores by combination approaches such as minimum score, maximum score, simple sum and user weighting. There are many researches that have fused fingerprint and iris at feature-extraction (template) level, in particular application of multimodal biometrics in cryptography [18] [19] [20] [21].

The main motivation behind this choice of fingerprint and iris characteristics for a multibiometric authentication system is that fingerprint is the oldest and most widely adopted biometric technology and, as a result, is the most mature of all biometric technologies [1], iris recognition is proofed that it is most accurate and hygienic biometric technology among others, this is reported in *"Biometric Product Testing Final Report"* [22] and in figure 1 are shown the biometric performances of some modalities by Detection Error Trade-off (DET) curves.

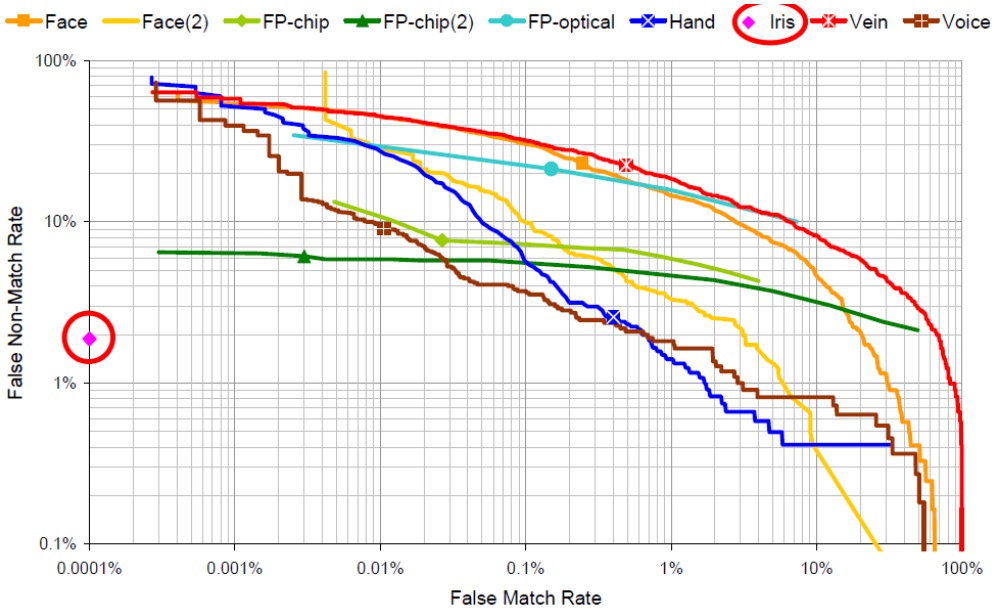



Figure 1: Detection Error Trade-off (DET): False Match rate (FMR) vs. False Non-Match Rate (FNMR) [22].

## 1.3 Trends and Applications

"*India is creating the biggest fingerprint and iris database in the world*"

A multibiometric system, because of the nature of the problems that is trying to solve, is better suited to large-scale identity management systems such as national ID programs and border control applications. The Unique Identification Authority (UIDAI) has initiated a project to provide all Indian residents, on a voluntary basis, currently numbering around 1.2 billion, with a unique 12 digit number. This unique number will be associated with the user's 10 fingerprint images, two iris images, and a face image. This is an example of multimodal and multi-instance type of biometric system [23].

The Biometric Automated Toolset (BAT) used by the U.S. military in Iraq and Afghanistan is a successful real-world deployment of multibiometrics. The BAT system includes a laptop, a fingerprint scanner, an iris scanner, a camera, and an ID card printer. The BAT system is used to create records of residents, wanted individuals, and detainees and it shared across multiple military posts across the Iraq. This allows a biometric identification check of individuals when they move from one region to another and determination of their civilian status [24].

The Next Generation Identification (NGI) program being developed by the FBI will replace the current IAFIS (Integrated Automated Fingerprint Identification System) program. One of the key goals of this program is to provide the capability of integrating multimodal biometric technologies into new system. Although fingerprint recognition will still serve as the basis of all matching operations, it is likely that iris recognition will be used increasingly in NGI [25].

Furthermore, in the U.S. passports face, iris and fingerprint images are stored in order to provide identity verification through identity documents. Hence, this is one example of multimodal biometric system [3].

## 1.4 Thesis Scope and Research Questions

As the core of our work throughout this thesis revolves around examining whether the performance of a biometric-based authentication system can be improved through integrating complementary biometric features which comes primarily from two different and independent modalities. Therefore, the main aim of the research will be to investigate the effectiveness of the suggested fusion techniques for multimodal biometrics, with the following specific objectives:

- Explore existing multimodal approaches.
- Evaluate fingerprint-based authentication performance.
- Evaluate iris-based authentication performance.
- Evaluate multimodal score-level fusion approach.
- Study the effectiveness of fusion of fingerprint and iris biometrics into the various comparison score fusion approaches in both unimodal and multimodal biometrics thorough experimental investigation.

All in all, the purpose of this work is to investigate whether the performance of a biometric system can be improved by integrating complementary information which comes primarily from the selected modalities.

> *"A question well-asked is a question well-answered."* [26]

Based on the previous discussions the following main research question is formulated:

> *"Can we improve security of biometric authentication systems by combining two different and independent modalities such as fingerprint and iris?"*

and should lead to contributions, relevant to improve the identified challenges.
To be able to answer the main research question, we need to address the following sub-questions:

1. How does quality of images affect the biometric performance?
2. What is the security performance of uni-modal biometrics fingerprint recognition and iris recognition?
3. What is the security performance of multi-modal biometrics using fingerprint and iris?
4. What is the most effective and robust score normalization and fusion technique?

## 1.5 Summary of Contributions

We propose a new multi-modal biometric authentication approach using iris and fingerprint images as biometric traits in this thesis. We fuse these two modalities at score-level by fusing different comparison scores from fingerprint and iris traits into a single score by combination approach. Since comparison scores that are generated from these uncorrelated and independent modalities are not homogeneous, score normalization step is essential to transform comparison scores into a common scale before fusing them.

The individual comparison scores obtained from the iris and fingerprints are combined at score-level using three normalization methods (Min-Max, Z-Score, Hyperbolic Tangent) and four fusion approaches (Minimum Score, Maximum Score Simple Sum and User Weighting). The fused-score is utilized to classify an unknown user into the genuine or impostor. We demonstrate that fusion based at score-level achieves high performance on different multimodal biometric databases involving fingerprint and iris modalities. In addition, we have analyzed the properties (performance, robustness and efficiency) of score normalization and fusion methods. Furthermore, we have analyzed the quality of fingerprint and iris databases.

Finally, we show that fusion of uncorrelated modalities such as fingerprint and iris achieves better accuracy and security compared to unimodal biometric systems.

## 1.6 Reading Instructions - Thesis Outline

This thesis is structured into nine chapters including this chapter (Introduction). The content of each chapter is summarized below:

**Chapter 2** describes the main components of identity management and basics of biometric authentication systems that are required when apprehending such a field.

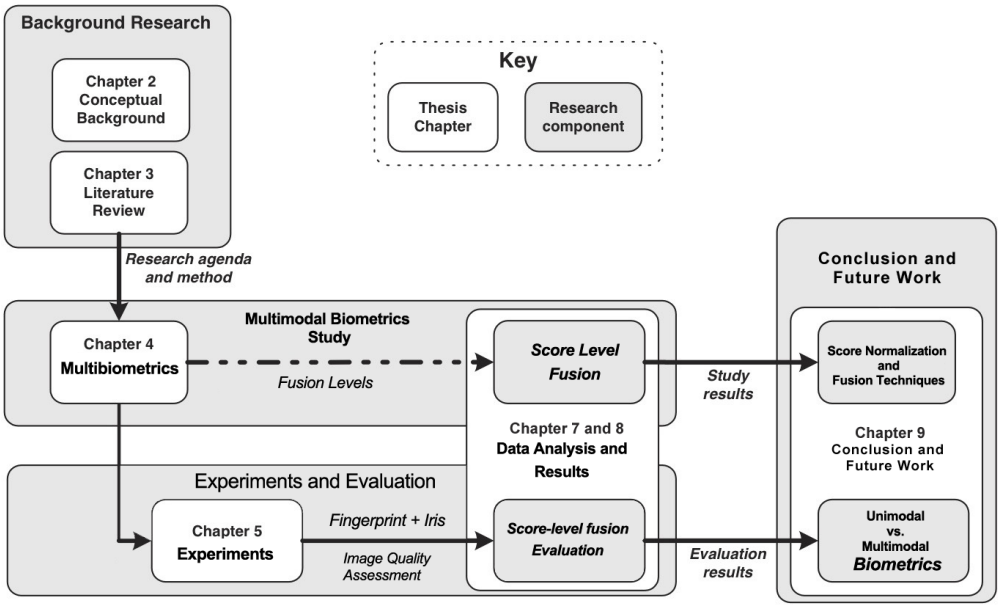



Figure 2: The general structure of the thesis, in outline.

**Chapter 3** in this chapter the state of the art of fingerprint and iris recognition is given.

**Chapter 4** presents a description of multi-modal biometrics, and how it works. It focuses on how it is possible to fuse (combine) two biometric modalities together to be used into an authentication system e.g. border control, financial institutions, government etc.

**Chapter 5** gives an overview of the system and the experiments performed during this project, focus on fingerprint and iris experiments.

**Chapter 6** In order to assess the performance of the biometric system there is a need for some metrics which can describe how the system behaves under several conditions. The work implemented in this thesis is assessed by the metrics discussed in this chapter.

**Chapter 7** gives a detailed description of how the experimental data have been analyzed. Furthermore it shows how performances are affected by quality of images the biometric performance and how to apply fingerprint and iris data in multi-modal biometrics.

**Chapter 8** gives an overview of the results for fingerprint recognition, iris recognition, as well as the main results of score-level fusion.

**Chapter 9** contains the summary of our work as well as are given answers to the research questions that are presented in Chapter 1, particularly in section 1.4, and than a discussion for future work is given.

# 2 Biometric Authentication Systems

This chapter is meant for those relatively new to identity management, authentication and biometrics, and will give a brief introduction to these subjects. In order to understand terms used later in the thesis, it is important to be familiar with the terms and explanations introduced in the following sections.

## 2.1 Identity Management

Identity management (IdM) is an important factor in many different contexts, representing a solid foundation for increasing the security of certain processes and services, while enabling digital interactions and transactions [27].
According to [28] main components of identity management are:

- User Authentication
- Enterprise Information Architecture
- Permission and Policy Management
- Enterprise Directory Services
- User Provisioning and
- Identity Management it self.

Brian Mizelle [28] claims that: **"Strong authentication is the key to successful identity management"** based on this claim and our goals, we are going to analyse the first and most critical component of identity management which is: *"User Authentication"*. Therefore, in following sections we are going to examine biometrics modalities as user authentication method.
Before starting the examination of individual biometric and multi-modal biometrics recognition system, first we need to explain some of the main definitions about biometric authentication systems.

There are three fundamental methodologies of human authentication (recognition):

1. **Something we know**: based on secret-knowledge authentication (passwords, PINs and cognitive knowledge)
2. **Something we have**: based on what the individuals possess (smartphones, IC cards or tokens)
3. **Something we are**: which refers to biometric authentication: physical or behavioural traits (fingerprint, iris, gait etc.).

These methodologies are illustrated in figure 3.

Biometrics is arguably the only technology that can bind a person to an authentication event. Knowledge and physical tokens cannot do that. Moreover, the person to be verified must be


Figure 3: Types of recognition methodologies.

physically present at the point of identity submission. A biometric template could also be stored on a smart card, access to which generally requires a PIN; and together, they would provide three-factor security. When strong three-factor security is used in a transaction, the risk of fraud significantly declines and assurance of legitimacy substantially increases. Figure 4 illustrates the relative power of three-factor security. The presence of a biometric template and PIN on a card

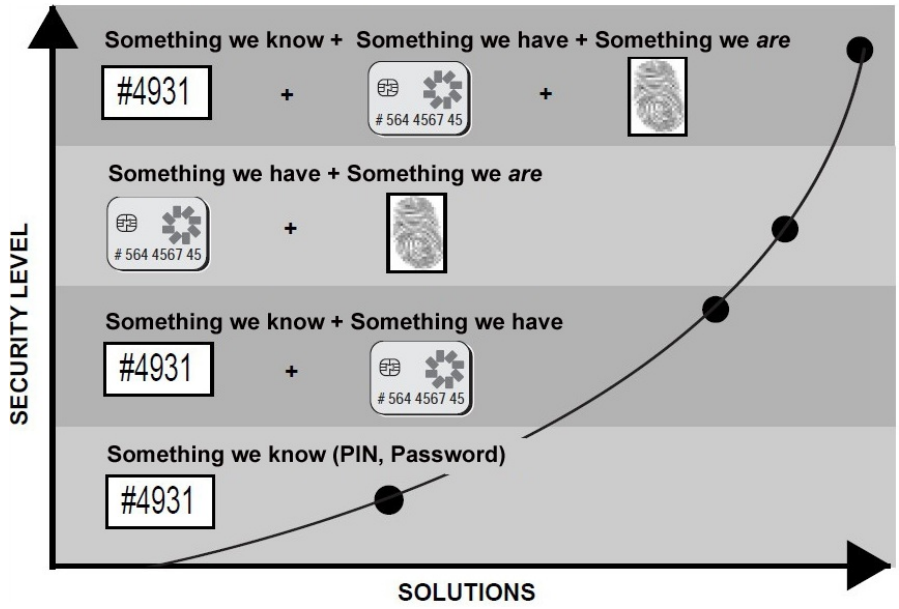



Figure 4: Relationship of three-factor security.

badge with a smart IC (Integrated Circuit) chip does not mean that every application or even every transaction would necessarily have three-factor security. For convenience or practicality, some applications might use only the biometric or use only the PIN with the card. For example, a financial institution might require a user to use only his biometric identifier for access to the

bank's own ATMs, but it might require the user to use both his biometric identifier and his PIN when remotely accessing financial records such as with home banking.

## 2.2 Characteristics of Biometric Features

The etymology of *"biometrics"* is derived from Greek words *"bios"*, which means *"life"* and *"metron"*, which means *"to measure"*, thus *"biometrics"* means *"life measurement"* [29]. The use of biometric was first known in the 14th century in China where *"Chinese merchants were stamping children's palm- and foot prints on paper with ink in order to distinguish young children from one another*"[30].

Biometric technologies are based on several biometric features (called characteristics) that can identify (verify) humans. Biometric modalities are divided into two basic groups:

- **Biological (or physiological)** - these biometric technologies use anatomical features, most known modalities are [29]: face, fingerprint, iris, hand geometry, hand veins, palm print, palm veins, finger veins, finger knuckle, DNA, retina, ear, tongue recognition etc.
- **Behavioural** - the primary biometric modalities based on persons' behavioural characteristics which use actions or mannerisms that are captured or learned over the time such as[29]: signature, keystroke, voice and gait recognition.

The biometric traits are illustrated in figure 5 and modified with current most used modalities such as vein recognition including (hand veins, finger veins, palm veins) and finger knuckle.

### 2.2.1 What Makes a Good Biometric?

Ross et. al. claim that [31] ***"There is no single biometric modality that is the best."***. According to the course IMT4621-Biometrics [3] and references [1] [32, 33, 34, 35, 36] , to define a good biometric trait, exist seven evaluation criteria which are:

1. **Uniqueness** - Every person has its own unique feature (characteristic) that means it should be different from any person. Moreover, *uniqueness* is known as *distinctiveness* which refers to the degree of variation of biometric trait across a population. The higher degree of distinctiveness the more the individual the identifier is, the lower degree of distinctiveness indicates that the biometric features can be found throughout the entire population.
2. **Permanence** - The characteristic should be invariant over time and features extracted thereof should be persistent and not be mutable over time. The ageing of the individual should not affect the feature vector.
3. **Universality** - Every individual in entire population should have a characteristic.
4. **Collectability** - The characteristic is measurable and the quantitative result is reproducible. Furthermore, the attribute should be convenient for an individual to capture, measurement and suitable to present to the biometric sensor.
5. **Acceptability** - The capture process provides a convenient measurement at low cost and is considered unobtrusive for the data subjects.
6. **Performance** - Does a recognition system based on this biometric characteristic provide a reasonable biometric performance (low errors). Furthermore this property is associated with

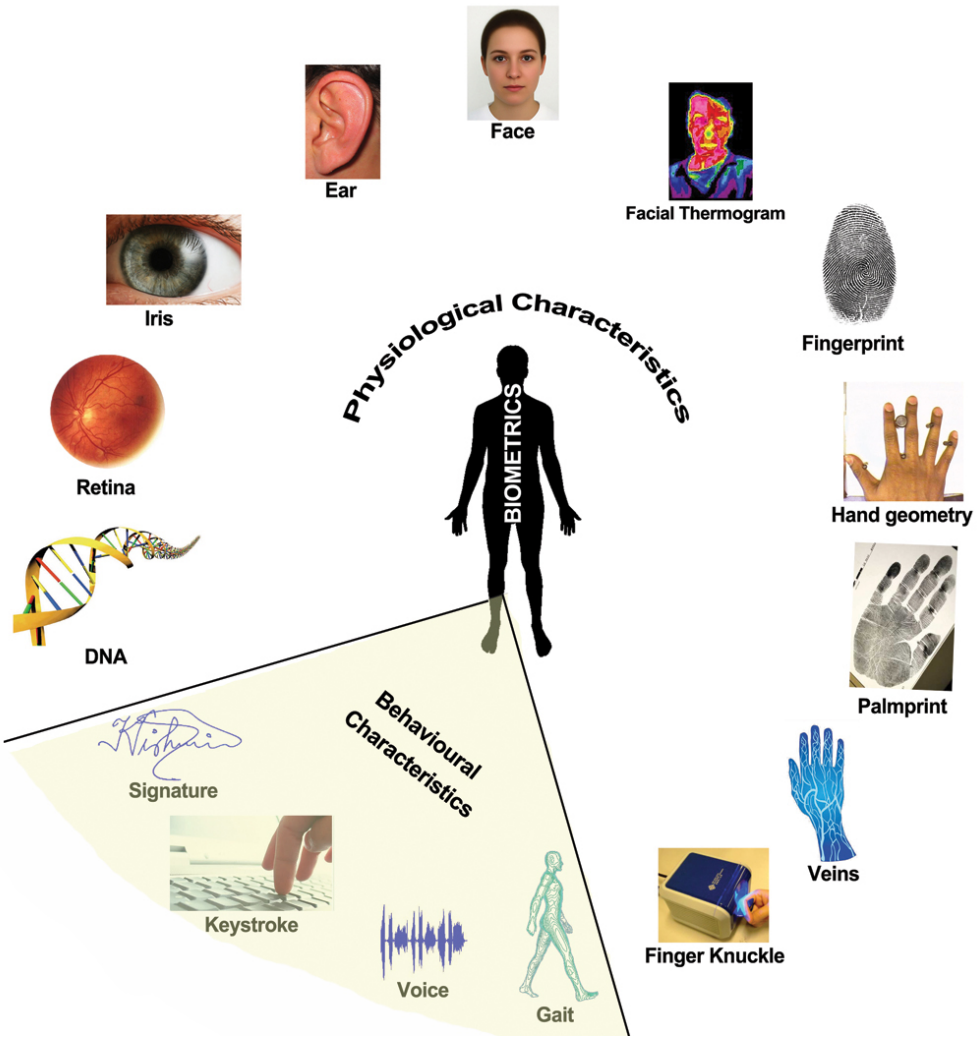



Figure 5: Examples of biometric traits that can be used for authenticating an individual (modified from [16]).

the throughput time (how does it take to capture the biometric characteristic and to extract features from the captured sample.

7. **Resistance to Circumvention** - How hard can the system be fooled or otherwise defeat a biometric system using fraudulent methods (i.e fake fingerprints).

The first four (1,2,3,4) criteria are the main properties to distinguish any person. The last three (5,6,7) criteria are needed to make the system practical [35].

### 2.2.2 Comparison of Traditional Biometric Traits

Based on seven properties of biometric modality's explained above (section 2.2.1), in table 1 is given a comparison of traditional biometric modalities. Honestly, this is a subjective evaluation of what is a good biometric modality [32, 33]. A long table with full comparison of main biometric modalities by seven evaluation criteria is given in Appendix B, based on previous different literatures that we have examined.

Fingerprinting is very widespread because of the existence of small sensors and it has a long history of research and usage within the police as a tool for investigation of crime. Despite of this fingerprinting has a high risk of forgery and theft as fingerprints are on the exterior of the body and latent fingerprints are often left on various objects handled throughout the day.

Moreover, the fingerprints are susceptible to be worn out or sweaty with a failure to enroll or authenticate as result. Even though humans normally use faces as a means to recognize each other during the day it is currently quite difficult to use as a biometric. Reasonable results are very hard to achieve when pose and environmental conditions such as lighting and background are not strictly controlled. 2D-face recognition is very susceptible to forging as sensors can be fooled using nothing more than a piece of paper with a print of a face. Iris recognition is very accurate and robust method. Eye is well protected by eyelashes and eyelids, thus to forge or damage it is very unlikely.

Table 1: Comparison of traditional biometric modalities [32, 33].

| Modality | Acceptability | Resistance to Circumvention | Collectability | Permanence | Performance | Uniqueness | Universality |
|---|---|---|---|---|---|---|---|
| DSV | H | M | H | L | L | M | L |
| Facial | H | L | H | L | L | M | H |
| Fingerprint | M | L | M | M | M | H | M |
| Hand geometry | M | L | H | M | L | L | H |
| Iris | M | H | M | H | H | H | H |
| Keystroke | M | L | M | L | L | L | L |
| Retina | L | H | L | H | H | H | H |
| Vein pattern | H | H | H | M | M | H | H |
| Voice | H | L | M | L | L | L | M |

*Note:* L, Low; M, Moderate; H, High.

According to this table from fingerprint and iris strengths, our aims and experimental environment at GUC [1], we have decided to analyse these two modalities in this report.

[1] GUC-Gjøvik University College

## 2.3 Biometric System Processes

The international standards committee on biometrics (ISO/IEC JTC1 SC37) defines biometrics as:

> ***"Automated recognition of individuals based on their behavioral and biological characteristics"***[37].

There are many real-world applications where security is a strong requirement, and reliable identity authentication is critical to that security. Token-based methods, including badges or passwords and personal identification numbers (PINs), tend to rely on surrogate representations of personal identities. Biometrics is considered a more natural and reliable solution for identity verification situations. Therefore, a biometric component for identity verification has become a critical enhancement for many security systems.

Any pattern recognition system that authenticates a user by determining the authenticity of a specific physiological or behavioral characteristic is basically a biometric system. With so many differing biometric modalities, it would seem that each biometric system supporting those modalities would be unique. However, biometric systems have much in common with one another. The biometric components are generically similar in terms of function. Moreover, all biometric systems share similar concerns with regard to acceptance, fraud, data storage, and privacy.

Biometric samples are not matched from raw data. Biometric systems acquire raw data from which they extract key features, which are then digitized, compressed, and encrypted to produce templates. A sample template is stored and compared to a reference template that was created during the enrollment process. This is an important privacy aspect of which much of the public remains unaware. The templates that most biometric systems store are simply digitized representatives of one's biometric traits. In most non-law enforcement applications, there are no repositories of individual biometric traits.

Components of biometric systems may varies from system to system, however, a generalized biometric system is functional combination of five main following components or subsystems as shown in Figure 6: (1) sensor/data capture (acquisition), (2) signal processing, (3) data storage (also called template storage), (4) comparison (matching) algorithm, (5) decision making.

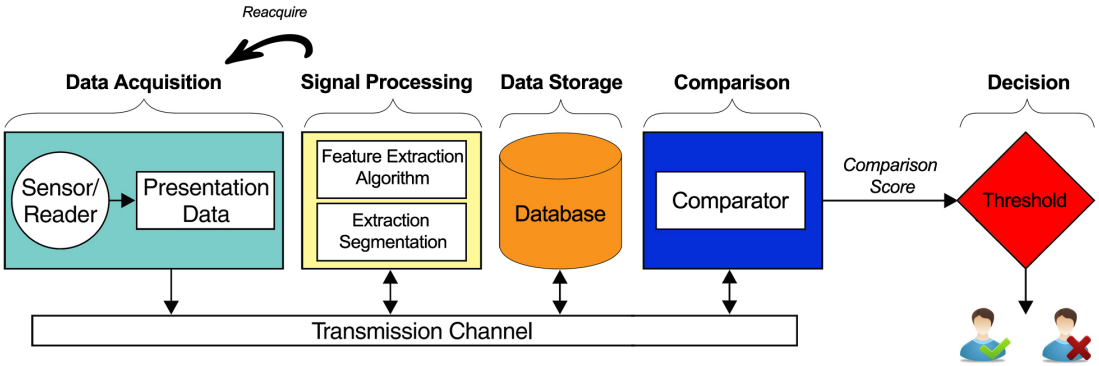



Figure 6: Components of Biometric System and Process Flow Diagram.

1. **Data Acquisition:** This subsystem is responsible to capture the sample of biometric characteristic (e.g. image or signal) from individual. This biometric sample is an uncompressed data and it is called *raw biometric data* and is captured by so called *sensor*[10]. This component is the only point where interaction between user and biometric system takes place and this process is also referred as *biometric presentation* [29].
   Quality of biometric sample and the manner in which the user presents biometric characteristic to a system has a significant impact in long-term performance of biometric system. Low-quality acquisition data will propagate through the rest of system and will lead to high error rates, including false match rate and false non-match rate explained in chapter 6. In fairness, one could argue that *"the sensor is the most relevant component (subsystem) of a biometric system"* [32]. Biometric data acquisition takes place during enrolment and precedes identification and verification.

2. **Signal Processing:** This subsystem is responsible to extract the features from biometric sample in order to generate digital representation called *biometric template* or *reference* which represent the uniqueness of the sample as well as be somewhat invariant related to multiple samples created from the same individual over the time [32, 33]. The signal processing process include: *sample enhancement, quality assessment (segmentation), and feature extraction*. The output of quality control checks (segmentation and feature extraction) is a *quality score*, reflecting the quality of the sample by how successful was the feature extraction algorithm [10].
   The signal processing component is extremely important to the accuracy of a biometric system, therefore quality of feature extraction has effect to the template generation process. If the quality score from feature extraction algorithm is low, the *signal processing* component does not accept the captured sample, then the sensor/data acquisition subsystem capture another biometric sample. If the signal processing subsystem accepts the biometric sample, it then generate a biometric template (reference) from the extracted data [32, 33].
   The signal processing takes place during enrollment, identification and verification - any time a template is created.

3. **Data Storage:** This subsystem stores the biometric template, this template that is housed for future processes is also called *reference* in the biometrics domain [38]. Those templates are generated and stored during the enrolment process into enrolment database.
   There are three main data storage methods to store the reference template [10, 32]:

   - ***Locally store*** - the templates can be stored on the biometric device itself or in another localized database.
   - ***Remotely store*** - the templates can be stored in a centralized database on a server or central data repository and available remotely over data network.
   - ***Securely store*** - the templates can be stored on a portable device (token) such as: *smart card, personal storage media etc.*

   Normally, a smart card can hold data from 8K size of memory up to 64K or more, thus this is sufficient to store a biometric template. Biometric template's size variate approximately: from 9 bytes (i.e. hand geometry template) to roughly 2000 bytes such as face or voice recognition

template (see table 2, page 16) [10].
If data capture arise at a remote location from the signal processing, the template should be stored in an altered format, compressed and encrypted prior to transmission [32].

4. **Comparison (Matching)**[2]**. Algorithm:** This subsystem depending on the application, each new created sample template is then compared with one or more reference templates by comparison algorithm. The result of the comparison algorithm is a *comparison score* or similarity (dissimilarity) score, indicating how similar are the templates [10]. The comparison score is then transferred to a decision making module.

5. **Decision Policy:** This subsystem uses score as input from the comparison component to compare with verification or identification attempts *threshold*. The *threshold* is a predefined value, normally chosen by biometric system administrator. If the score resulting from comparator (template comparison) exceeds the threshold the compared templates are *match*, if the score falls below the threshold value the compared templates are *not-match* [29]. According to [33] the threshold plays an important role in security of systems: "*Systems can be either highly secure or not secure at all, depending on their threshold settings.*"
The decision component outputs the result also called *decision* from comparison between the comparison (matching) score and the threshold value. The result of decision subsystem of biometric recognition could be *match, non-match* and *inconclusive*. These outputs are related to threshold value and comparison score, match might lead to successful authentication, a non match might lead to unsuccessful authentication, while inconclusive decision policy may require from the subject to present another sample to the system [32].

***Transmission Channel:*** is also a subsystem (component) of biometric recognition system (portrayed in diagram-figure 6) and it refers to the communication channels (paths) between the fundamental components. This subsystem is not present to all biometric systems, because those systems are self-contained and the transmission channels are inside to the device. The transmission channel for remotely and locally systems can be a LAN (Local Area Network), Intranet or even the Internet [38, 10].

### 2.3.1 Stages of the Biometric Process

Besides, of fact that there are many types of biometrics authentication methods, the biometric systems work in the same procedure. Biometric recognition systems have two key stages of operation: (1) enrollment and (2) ongoing transactions (both identification and verification), illustrated in figure 7 and 8 respectively.

- **Enrollment**: During *enrollment* process an individual present the biometric data into acquisition (capture) device and then these data are assessed, processed, and stored into data storage such as smart card, mobile phone, database etc. in set of biometric features known as *template* which is used in future stages of biometric system.
  Typically, an enrollment process includes the following steps [32, 31]:

  1. Acquisition (capture) of a biometric data.

[2]NOTE: match / matching is deprecated as a synonym for comparison!

2. Signal Processing which includes:
   - Sample Enhancement.
   - Quality Assessment: this module checks the quality of captured sample and it may reject or accept based on quality score, if quality score is low it requires reacquisition of biometric sample, otherwise it transmits the sample to feature extraction module.
   - Feature Extraction.
3. Reference template creation (which may require multiple samples).
4. Potential conversion of a template in a data interchange format and storage.
5. User test of a verification or identification attempt to ensure that the resulting enrollment is usable.

Enrollment takes place into both processes identification and verification. Enrollment is the most critical process of the biometric system. Nothing else can affect the successful use of the biometric technologies more than enrollment.
Enrollment quality is a critical factor in the long-term accuracy of biometric technologies. Low-quality enrollments (low quality of templates) the less accurate will be the system in general, and it leads to high error rates, including false match rate (FMR) and false non-match rate (FNMR). Avoiding impaired images generated during enrollment process should actually improve the accuracy of the biometric system [32, 31]. For this reason, in our experiments we have made the quality assessment of fingerprint and iris images by NIST Fingerprint Image Quality checker (NFIQ), and quality checking module from Neurotechnology VeriEye SDK, respectively. For more details please refer to chapter 5, respectively to section 5.2.2.
Figure 7 graphically illustrates the sub-processes involved in enrollment stage.

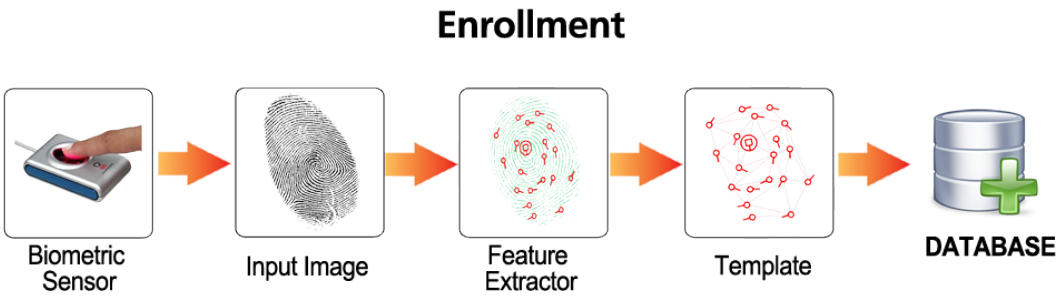



Figure 7: Enrollment Process.

**Biometric Template Creation**
From ISO Harmonized Vocabulary [37] *biometric template* is: *"set of stored **biometric features** comparable directly to biometric features of a **probe** biometric sample*", and often the biometric template is called *reference*. A *template* is a small file in size, most templates allocate less than 1 kilobyte. The small file sizes allow us to store it in mediums like smart cards and tokens

and to encrypt it for transmission. In table 2 are presented some of most used modalities and their template's size in Bytes (B). One of the most important matter about most biometric

Table 2: Approximate Biometric Template Sizes [10]

| Biometric Trait | Approx. Template Size in Bytes (B) |
|---|---|
| Fingerprint | $256 - 1200$ |
| Palmprint | $256 - 1000$ |
| Fingervein | 512 |
| Palmvein | 800 |
| HandGeometry | 9 |
| Face | $84 - 2000$ |
| Iris | $256 - 512$ |
| Retina | 96 |
| Voice | $70 - 80/second$ |
| Signature | $500 - 1000$ |

systems is that unique templates are generated every time an individual presents biometric data in acquisition device. Generally, two immediately successive impressions of a finger on a biometric capture device generate totally different templates. Depending on when they are created, templates can be referred to as *enrollment templates* or *comparison templates*. In most biometric technologies, enrollment and verification templates **should never** be *"the same"* [32].

An *identical comparison* is an indicator that some kind of attack is taking place (e.g. fingerprint reconstruction from latent prints), such as the resubmission of an intercepted or otherwise compromised template.

According to [32, 31]: *"potential enrollment problems exist with each biometric modality, and there are trade-offs that must be addressed, hence there is no biometric modality that works 100%"*.

- **Verification versus Identification:**
  During ***VERIFICATION*** process, system provide the answer for question: "*Am I who I claim to be?*" by requiring that an individual makes a claim to an identity in order for a biometric comparison (matching) to be completed.
  The biometric system acquire an individual's biometric data, and then extracts the features from biometric sample in order to generate the individual's sample template, also referred to as a probe template, trial template or a live template.
  The biometric verification system then compares the probe template to the template stored at enrollment (the reference template), and in most systems, numerical value (or set of values) - comparison score is generated resulting from comparison module on the percentage of similarity or dissimilarity between the probe and reference templates. Depending on the decision policy (threshold value), the identity verification score if the score meet or exceed the decision threshold the answer returned by verification system is **match** or the claimed identity is accepted (an individual is considered as*"genuine"*), otherwise the answer is **non-match** or claimed identity is rejected (an individual is considered as *"impostor"*). Verification process

is often referred to as *"one-to-one"* (1:1) search (comparison). *Authentication*[3] is verification system by providing biometric characteristic and username.
In general, verification system is used for *"positive recognition"*, where the goal is to prevent multiple people from using the same identity or to prevent accessing the system from unauthorized persons [31]. The verification decision outcome is considered to be erroneous if either a false claim (impostor) is accepted *(false accept)* or an authentic (genuine) claim is rejected *(false reject)*.
Typically, a verification process involves the following steps [32, 33]:

- Acquisition (capture) of a biometric data.
- Signal Processing which includes:
  - Sample Enhancement.
  - Quality Assessment: this module checks the quality of captured sample and it may reject or accept based on quality score, if quality score is low it requires reacquisition of biometric sample, otherwise it transmits the sample to feature extraction module.
  - Feature Extraction.
- Comparison of the sample template against the reference template for the claimed identity producing a matching score.
- A review on whether the sample template matches the reference template as it relates to the threshold score (no match is ever perfect because of the relative uniqueness of each template).
- A verification decision based on the *"one-to-one"* (1:1) comparison result of one or more attempts, depending on system's policy.

During ***IDENTIFICATION*** process, system provide the answer for question: "*Who am I?*" without claiming for an identity, but here the system reveals the identity associated with biometric characteristic (modality), before comparison is initiated. Identification process is usually referred to as *"one-to-many"* or *"one-to-N"* (1:N) search (comparison), because provided biometric data (1) is compared against every record or template (N) in the enrollment database.
Typically, identification process involves the following steps [32, 33]:

- Acquisition (capture) of a biometric data.
- Signal Processing which includes:
  - Sample Enhancement.
  - Quality Assessment: this module checks the quality of captured sample and it may reject or accept based on quality score, if quality score is low it requires reacquisition of biometric sample, otherwise it transmits the sample to feature extraction module.
  - Feature Extraction.

[3] In practice, authentication usually is used as synonym for verification

- Comparison against some or all templates in the enrollment database, producing a matching score for each comparison.
- A review on whether each matched template is a potential candidate identifier for the user, based on whether the similarity score exceeds a threshold or is among the highest similarity scores returned.
- A verification decision based on the candidate list *"one-to-many"* (1:N) search from one or more attempts, depending on system's policy.

Identification process can be classified in two different modes: *positive* and *negative* identification [31, 32, 39].
*Positive identification* system, search for individuals without explicitly claiming an identity, and ensure that a given biometric data is in identification database.
*Negative Identification*, the purpose of negative identification system is to confirm that a person is not enrolled using another identity or prevents an individual using multiple identities into system. This kind of systems are relevant for large-scale public applications such as: government, welfare, border control etc.
Positive identification system is in analogy with personal recognition like passwords, PINs, smart cards etc, while negative identification is performed only by biometrics.

Verification and identification processes have similarities, but their differences are *"stark"* [40]. Figure 8 shows the basic biometric process flow of verification and identification system.

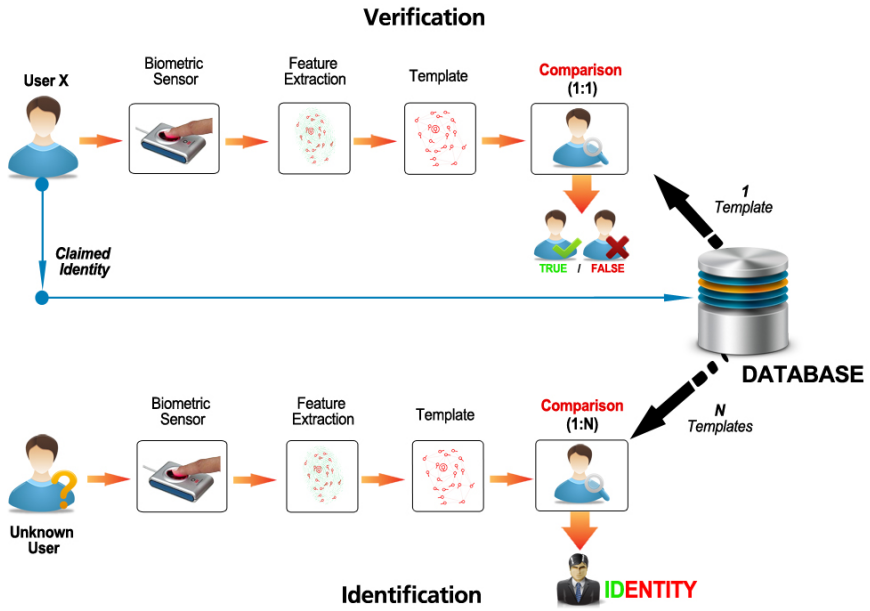



Figure 8: Schematic representation of the processing steps of a biometric system (verification and identification stage respectively).

## 2.4 Summary

Recognition methods that enhance the security of the system and convenience of users have acquired increased importance in today's digital world. Traditional recognition methods based on memorizing secrets or possession of tokens, although still used predominantly, and are facing serious operational challenges. Biometric technologies provide an additional level of security and convenience, but this should not be interpreted as biometrics being the perfect solution or silver bullet. Biometric technologies also have limitations.

Human interaction plays a significant role in determining the performance of biometric systems, and it has only lately started receiving the attention it deserves. Social acceptance based on geocultural conditions will challenge the user confidence in the technology. Ensuring user privacy is a key factor in increasing the adoption of biometric systems. Biometric systems are not immune to mismatch errors, which are influenced by variety of factors, including deployment environment, user interaction, and the strength of the underlying biometric comparison (matching) algorithm. A perfectly secure system has never existed and never will. All systems have vulnerabilities, and a well-designed system should use appropriate combination of knowledge-based, token based, and biometric technologies to reduce these vulnerabilities.

# 3 Literature Review

This chapter aims to illustrate the development of research in biometric authentication systems, particularly in fingerprint and iris recognition. It will show progressively the different approaches that have been done in the past years in fingerprint and iris recognition. All the work explained in this chapter initiated the idea of the work in this thesis and serves as the literature review which was done as the first step of this research.

## 3.1 Fingerprint Recognition System

If we look closely at our fingers and palm friction ridge skin, we will notice that skin forms a pattern of ridges and valleys, as shown in figure 9. As we can see from figure, these ridges are not continuous lines, they might end or diverge. These points where ridges are not continuous are called *minutiae points (features)* and today the major of fingerprint recognition algorithms use minutiae features to compare similarity or dissimilarity between two fingerprint templates. Fingerprint ridges are completely created by the seventh month of an individual fetus development, remain the same for whole lifespan [41], and are the last recognizable characteristics to disappear after death [3]. The form of this ridge patterns is randomly and given that even monozygotic twins have different pattern of fingerprints [42]. Two main layers of skin are: *epidermis* (outer layer) and *dermis* (inner layer), where ridges belong to epidermis, meanwhile sweat glands, blood vessels (veins), nerves and other cellular structures are inside the dermis. When ridges are injured or other damage of our finger skin, they will recover and retain original with time, thus the property of permanence and uniqueness makes fingerprint leader to the biometric recognition technologies.

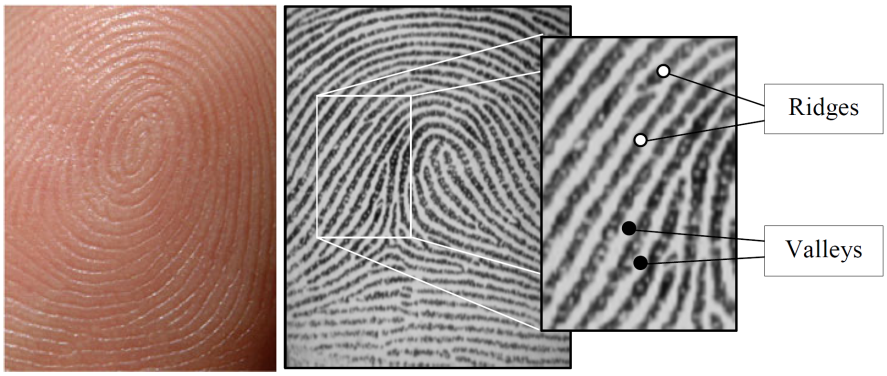



Figure 9: a) Raw fingerprint image, b) Ridge-valley structure of fingerprint image [1].

### 3.1.1 Fingerprint Acquisition

Fingerprint image acquisition is the first step in fingerprint recognition, the capturing process can be performed by different types of technologies, starting from so called *off-line methods*, such as *inked-paper fingerprint image* and *latent fingerprint image*, followed by *on-line (live-scan)* capturing methods such as *optical sensor, solid state capacitive sensor, RF sensor, thermal fingerprint sensor, electro-optical sensor, multispectral imaging sensor, ultrasound sensor* and *touchless sensor*. Off-line technologies were invented more than four decades ago [1], and are still used in forensic applications. These technologies do not generate any fingerprint image into digital format, whereas, on-line technologies produce fingerprint image into digital format. The sensing technologies are well described in *"Handbook of Fingerprint Recognition"* [1], but below is given a short description for three main families of on-line (live-scan) sensing technologies, such as optical, solid-state and ultrasound, their advantages and disadvantages.

**Optical Sensing [43][44][45]** this is the first and still used live-scan fingerprint image capture technology. Earlier types of optical sensors have used CCD (Charge-Coupled Device) cameras to capture the image, but newer optical sensing technologies used CMOS (Complementary Metal-Oxide Semiconductor) cameras. The resolution of fingerprint images acquired by this type of sensors varies from 256 dpi (dots per inch) up to 1000 dpi. Moreover, older optical sensors could not differentiate ridges and valleys, while by introducing Frustrated Total Internal Reflection (FTIR) this problem is solved, when we put the finger over the optical sensor light on valleys is totally reflected and light on ridges is not reflected, thereby ridges are resulted as dark lines in fingerprint image like in figure 9. Another issue related to optical sensing technology is for instance if the finger is wet, dirty or oily, this result in bad images as well as bad performance. Nevertheless, these issues are avoided by using multispectral light, rather than visible light. As optical sensor are accounted the following types: *FTIR, FTIR with a sheet prism, optical fibers, electro-optical, direct reading* and *multispectral imaging* [1]. The optical sensor by FTIR is illustrated in figure 10.

**Solid-State Sensing [46] [47]** this type of sensors is more used than optical FTIR sensors today, because they are very small in size and cheaper than others. These sensors are built by two-dimensional array of conductive plates. For instance, when the finger is places over a CMOS chip surface, the electrical capacitance is affected by ridges and valleys and such they create different capacitive charge and these charges are converted into pixels by different methods like: *AC, DC* and *RF*. Capacitive sensors acquired fingerprint image by two interaction mechanisms, such as *touch* and *swipe*. *Swipe (line)* sensors are very common these days, and are embedded into laptops, smartphones etc. Furthermore, as solid-state sensors are considered: *capacitive, thermal, electric field* and *piezoelectric* [1]. In figure 11 is given an illustration for touch capacitive sensor.

**Ultrasound Sensing [48]** this technology may be viewed as *echography*, which is based on reflected sound waves by ridges and valleys. Ultrasound sensor has two main components: *transmitter*, which creates short sound waves, and *receiver*, which detects the reflected pulses when they contact the finger skin. This type of sensors, sometimes are called as touchless

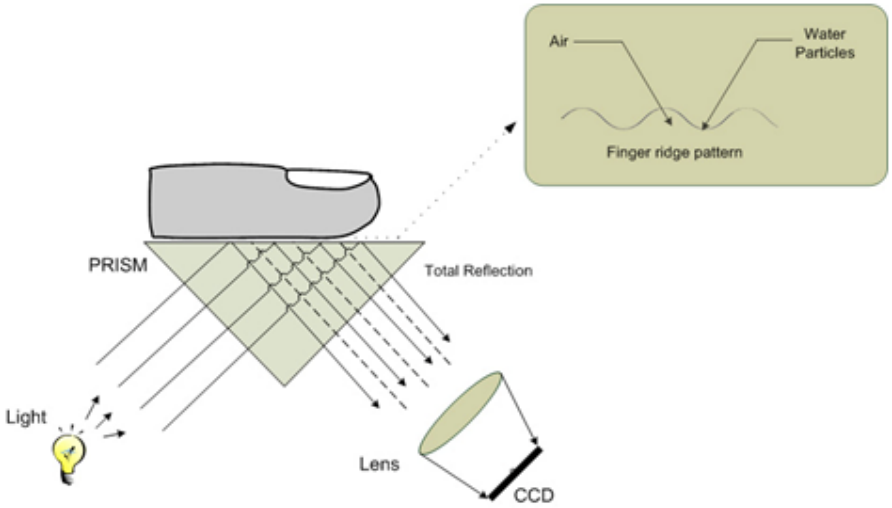



Figure 10: Optical fingerprint capture by FTIR (Frustrated Total Internal Reflection) [2].

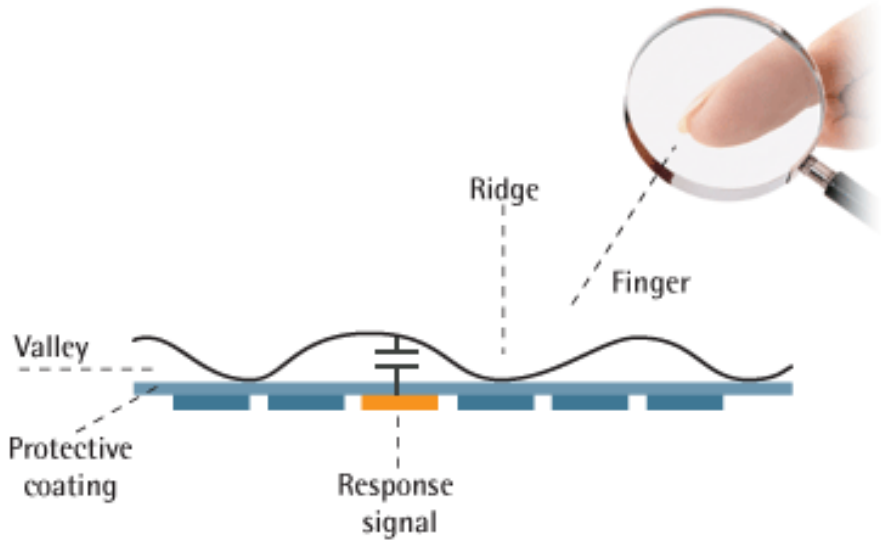



Figure 11: Touch capacitive sensor.

fingerprint sensors, which do not require any physical interaction, thereby wet and dirty fingers does not affect quality of images. Although, this family of sensors are quite expensive, bulky and takes longer capturing time than optical sensors [1]. Figure 12, shows a generic principle of ultrasound fingerprint sensor.

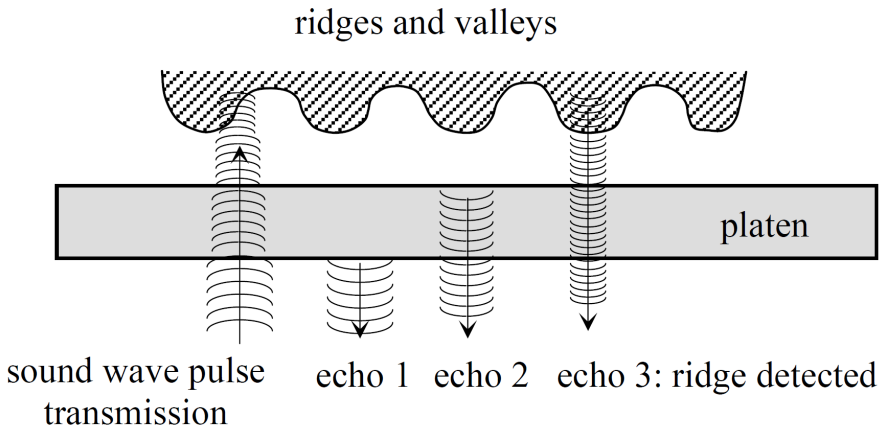



Figure 12: Ultrasound sensor (basic principle) [1].

The main challenges of fingerprint image acquisition techniques are:

1. Captured images should be invariant to:
   - translation – varying positions of the finger on the sensor,
   - rotation – varying orientation of the finger on the sensor and
   - scaling – non-linear deformation of the fingerprint [3].

   These three basic challenges are illustrated in figure 13, respectively.

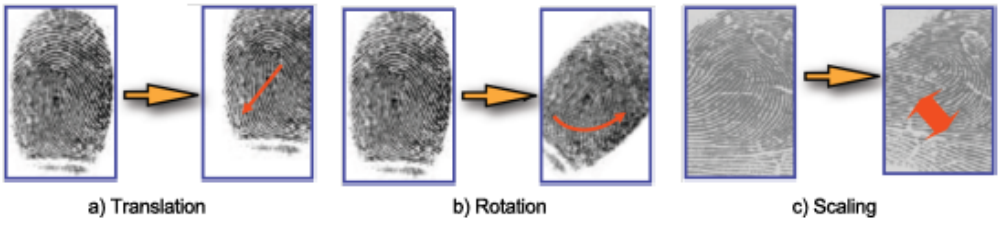



Figure 13: Challenges at image acquisition due to translation, rotation and scaling [3].

2. Poor image quality is another challenge of image acquisition, this is due to:
   - finger is too dry, wet, worn-out, dirty,
   - pressure too high or too low,
   - scratches (temporarily missing ridges) etc.

Consequences from mentioned problems are that real minutiae are overlooked and false minutiae points (also called spurious minutiae) are added, typically at border or background of the fingerprint image [3], illustrated in figure 14.

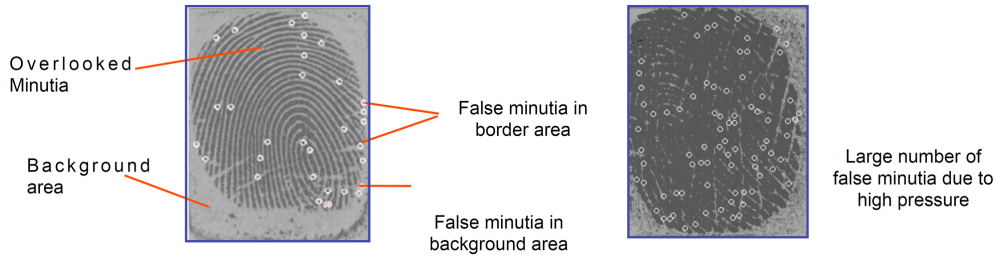



Figure 14: Poor image quality fingerprint image acquisition challenge [3].

### 3.1.2 Fingerprint Pre-processing and Feature Extraction

Second step after image acquisition in fingerprint recognition is image pre-processing, followed by feature extraction step. In general feature extraction belongs to pre-processing step, thus, when we talk about fingerprint image pre-processing it is usually accounted as feature extraction. Below are described main steps of feature extraction process.

The fingerprint image has two singularities or singular points called *core* and *delta*, illustrated in figure 15. Core and Delta are well defined by ISO/IEC 19794-8, as follows:

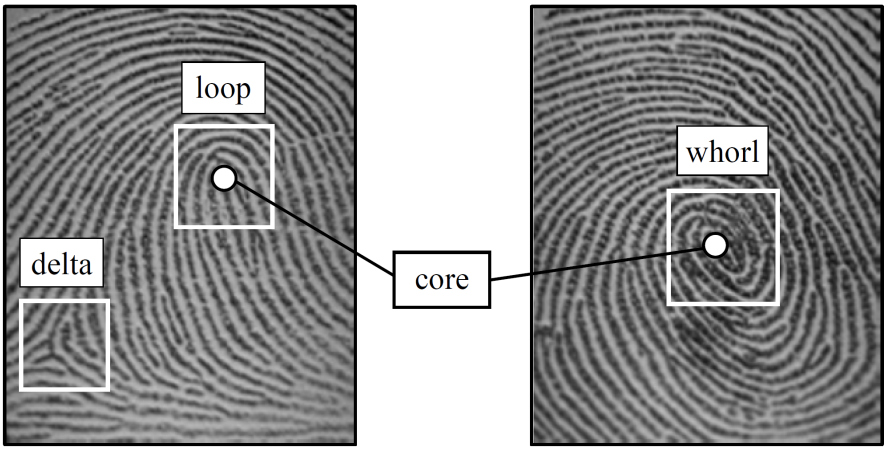



Figure 15: Singular points: core (white dots) and delta in fingerprint images [4].

**Core** is *"a singular point in the fingerprint, where the curvature of the ridges reaches a maximum"*. Can be considered as U-turn that includes a number of ridges and is approximation for the centre of the fingerprint pattern [3].

**Delta** is *"structure where three fields of parallel ridge lines meet"*, or the point where two parallel lines divert [3].

The significant information in fingerprint patterns are classified into three different levels:

- **Global level features**: this level is also called as classification of fingerprints according to global ridge patterns. In this level only ridge flow and ridge frequency are treated, hense even images acquired from sensors with low-resolution e.g. 250 pixels per inch (ppi) can be examined by Level 1 details. Examples of Level 1 fingerprint details are FBI and Hanry classification schemes. Edward Henry was a police officer in India and he worked on fingerprint recognition system to identify criminals. This classification system is published in 1900 "The Classification and Use of Finger Prints" and described in details in [1]. Henry's classification was a watershed moment for fingerprint recognition in identification technologies and base for mainly law enforcement applications. This system categorizes the fingerprints into four major classes, such as: arches, loops, whorls and compounds, from statistics loops and whorls are most common patterns in fingerprints: loop-type 65%, whorl-type 24%, while arch and twin loop approximately 4% and tented arch 3% [1]. In figure 16 are illustrated some combinations of fingerprint classification based on Hanry's scheme.

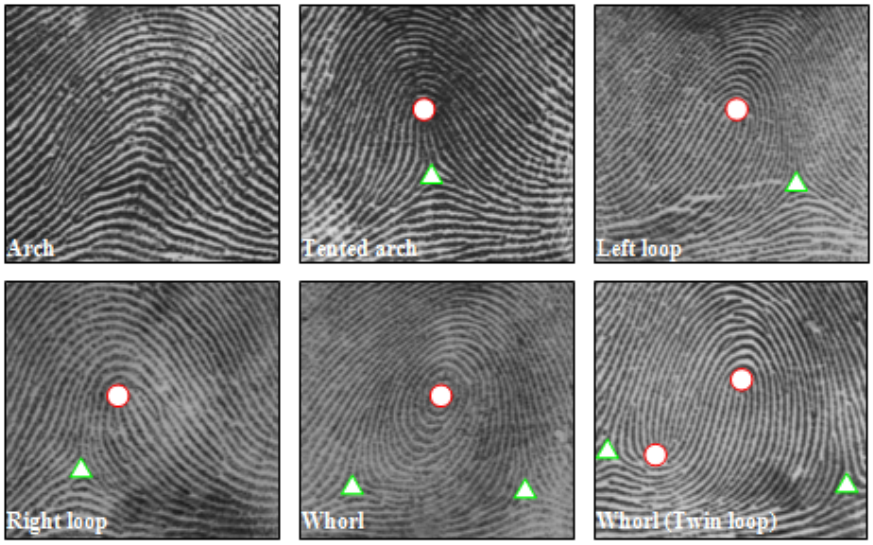



Figure 16: An example of first level classification features (Hanry classification). Where white-red dots constitute to core point and white-green triangle constitute to delta point [39].

- **Minutiae-based features (Galton details)**: this level is also called second-level features *(edgeoscopy)*, what means that in this level only minutia points are analysis. The main two types of minutia points are: endings or termination and bifurcation, all other points are presented as combinations from endings and bifurcations. In figure 17 are illustrated seven most commonly used minutiae points in fingerprint recognition system.
  Minutiae points are named by Francis Galton in 1880 and he proposed that *"two fingerprints could be matched by comparing the ridge discontinuities (minutiae points)"* [29]. Minutiae point is considered a four tuple $\mathbf{m = \{x, y, \theta, t\}}$, where *(x,y)* is absolute position and represent the

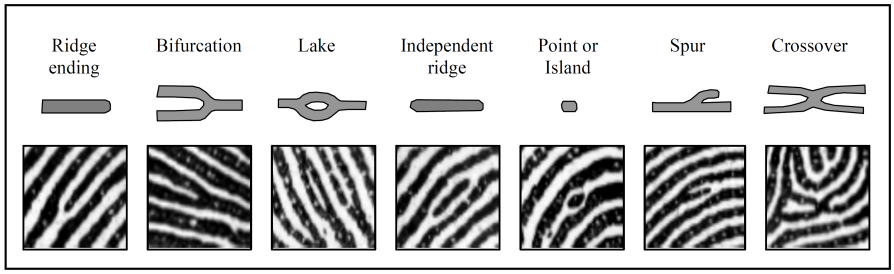



Figure 17: The most common fingerprint minutiae features (Galton classification) [1].

location of minutiae point in spatial domain of fingerprint image (origin point of system is ), angle θ is orientation and represent direction of minutiae point and t stands for minutia type {*ridge ending (re), bifurcation(bf)*}. Figure 18 shows a typical example of minutiae feature extraction by CUBS Fingerprint Feature Extraction Tool and image is from FVC2002 fingerprint database. This file is called as *minutiae template* of given fingerprint image. Minimum 12

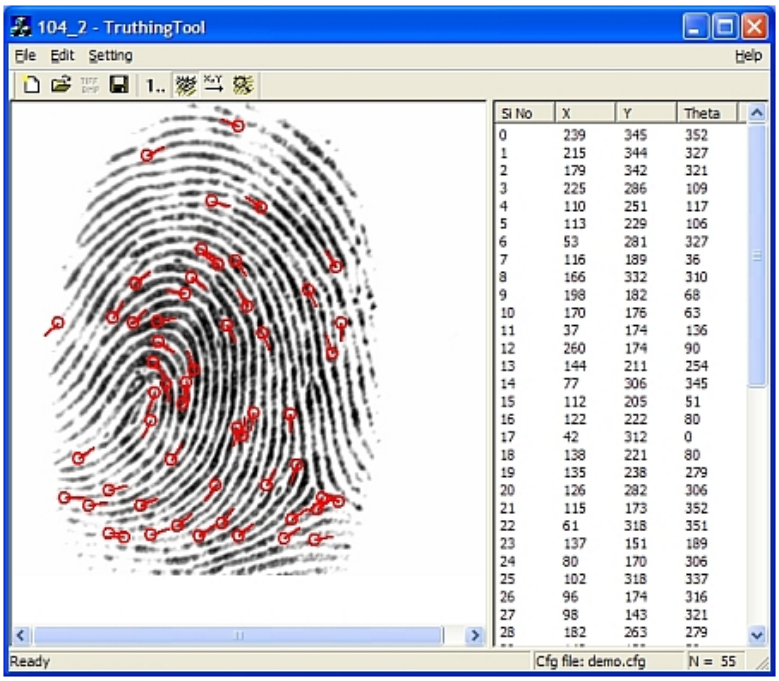



Figure 18: Example of fingerprint minutiae feature extraction. Where Si No is total number of minutiae features, X- Y are coordinates and Theta is the angle of minutiae points.

minutiae points in the overlapping area of fingerprint are required from ISO 19794-2 standard [11]. From live scans we can extract up to 40 minutiae points, while from *"rolled"* inked impression up to 150 minutiae points [3].

Most of automated fingerprint recognition systems today use minutiae comparison approach,

which is described into next sub-section 3.1.3.

- **Sweat pore-based features**: this level is also called third-level features *(poroscopy)*, what means that here only sweat pores are analysis, in normal finger exists up to 2700 sweat pores. This fingerprint classification method can extract very highly detailed features, wherefore it requires very advanced acquisition technology with 800 dpi or higher.

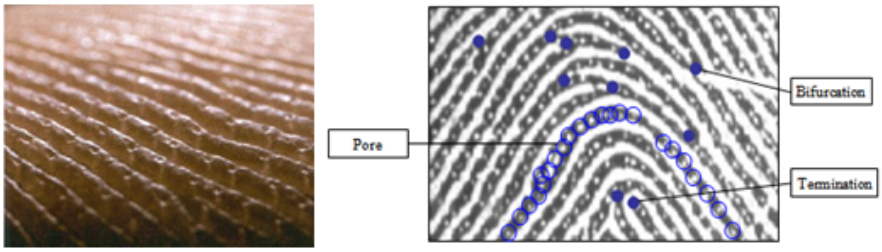



Figure 19: Fingerprint third level classification (pores).

### 3.1.3 Fingerprint Comparison Approaches

There are many researches on fingerprint comparison approaches and classified into three different families, such as minutia-based, correlation-based and ridge feature-based (hybrid) comparison [49][50][51][52]. Most of fingerprint recognition systems are based on main approaches:

- **Approach I**: Minutiae-based
- **Approach II**: Correlation-based

These two fingerprint comparison techniques are described briefly below. Furthermore, the fingerprint comparison in details is presented in *"Handbook of Fingerprint Recognition"* [1], chapter 4 – Fingerprint Matching.

**Minutiae-based comparison:** this is the most popular comparison method and most available on commercially fingerprint comparison systems. This method analysis Galton details or minutia information (second level features) described previously. As we discussed in section fingerprint pre-processing and feature extraction (minutia-based feature extraction) this process provides minutiae details like: x,y coordinates, angle and type of minutiae point, that are stored as template in database, file or other form of storage, these details are used for fingerprint comparison. An acquisition image of fingerprint from the same finger on the same acquisition device will never be exactly the same. This is due to one of several reasons: finger impression, finger orientation, any external factor such as damages etc. Given that, minutiae sets of two fingerprints compared will never have the same number, nor will they have same alignment. One of the major advantages of minutiae-based comparison approach is that it is invariant with above mentioned fingerprint sensing challenges like rotation, translation, scaling etc. Figure 20 summarizes the pre-processing flow of minutiae feature extraction from fingerprint image and will generally follow these steps: *quality assessment, segmentation, image enhancement, binarization, skeletisation (thinning)* and *minutiae extraction*.

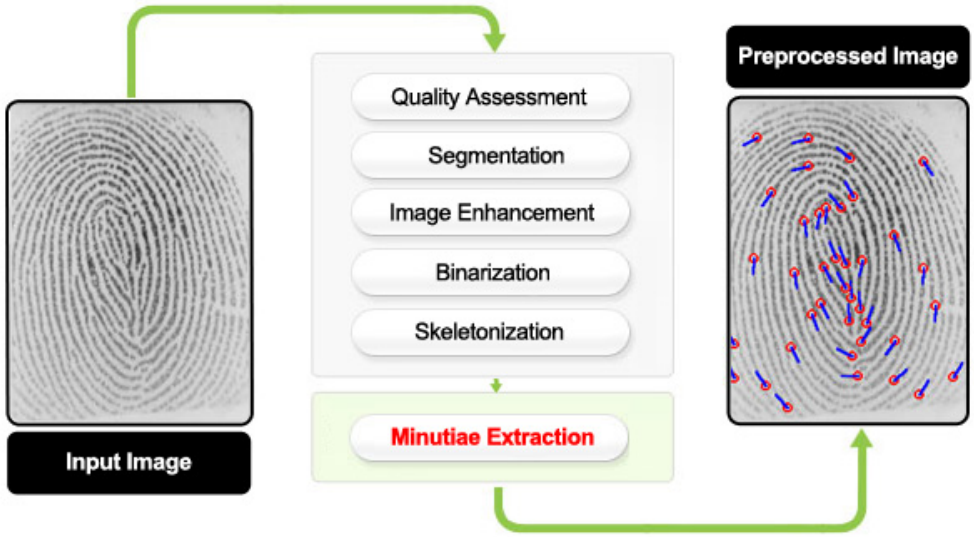



Figure 20: Flow diagram of the minutia-based pre-processing technique.

1. **Fingerprint input image**: a fingerprint image is captured from subject (user) by any type of fingerprint sensors, it worth mentioned that in this step is created digital gray scaled image, and all followed steps are performed on gray level fingerprint image.
2. **Quality Assessment**: fingerprint image quality has important impact on performance and in this stage the quality of captured image is assessed and checked if the image fulfils requirements to be accepted or if it is rejected another attempt is required from user. Hence, in our experiment we have used NFIQ (NIST Fingerprint Image Quality) tool, which is based on neural network method to check the quality of fingerprint images, all details are given in experimental section.
3. **Segmentation**: this step the region of interest known as ROI is extracted from fingerprint image, thus it separates fingerprint from background. Furthermore, as we described earlier from background can generate spurious (false) minutiae points from scars, cuts and other artefacts that impair quality of feature extracted. Some of segmentation techniques are described in [1].
4. **Image Enhancement**: in this stage some of standard image pre-processing routines such as normalization, filtering (like Gabor filtering), masking etc., are applied to enhance contrast between ridges and valleys, smooth, sharpen and remove noise from fingerprint image.
5. **Binarization**: in this step grey-scale representation (image) is converted into a black and white pixels image or binarized image, where white pixels represent valleys, and black pixels represent ridges.
6. **Skeletonization (Thining)**: here skeletonization or thining is made by erosion. From

binary image, ridgelines are crumbled (removing) pixel by pixel until line structures are one pixel wide. This operation is achieved by applying: distance transform or morphological operations. In this step the skeletonized image is created.

7. **Minutiae Extraction**: when skeletonised image is created from step 6, minutiae extraction is relatively simple step. Line structures are traced until a discontinuity is reached and this point is stored as minutia point (minutia position, type and angle).
   Identification of all minutiae points can be made through different methods: neighbourhood investigation, crossing numbers and pattern matching. From this step a fingerprint minutiae template is created and we are ready to perform comparison process.

Moreover, these steps have been studied from many researchers and some of fingerprint feature extraction algorithms are described in [1] and [31].

Our fingerprint comparison experiment is performed by Neurotechnology- VeriFinger SDK 6.5 which is commercial comparator discussed in experimental section. In figure 21 are given two examples of a genuine comparison and an imposter comparison by VeriFinger SDK 6.5 and flowchart of fingerprint minutiae-based comparison algorithm, just to have an idea how minutiae-based comparison technique works.

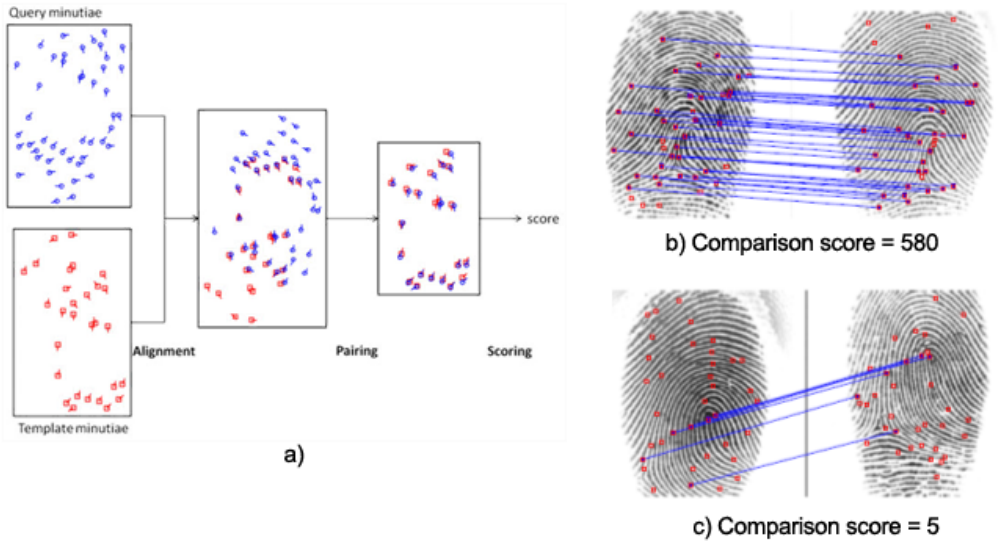



Figure 21: Fingerprint comparison by VeriFinger SDK 6.5. a) Flow diagram of a minutiae-based comparison algorithm. b) A genuine comparison of fingerprints with 30 matched minutiae, and c) an imposter comparison with 5 matched minutiae. Matched minutiae are connnected by blue lines. The comparison score (is calculated based on matched minutiae and some other functions that are defined by Neurotechnology.

**Correlation-based comparison:** The first or global level features described previously are analyzed by the correlation-based approach. This type of comparison approach uses correlation pixels of fingerprint image to measure the degree of similarity between two images. This approach overtakes some of the disadvantages of minutiae-based technique, but still it has

some drawbacks since it is sensitive to global transformations like rotation, orientation etc., given that size and orientation normalization of image is required. If we use this comparison technique a good fingerprint image quality is required, because comparison is performed with grey-scale images. Figure 22 gives an overview of pre-processing process based on [53]. Flow diagram of correlation-based technique involve: *quality assessment, image enhancement (normalization), low frequency filter, orientation field frequency map, filtering* and at the end *equalization*.

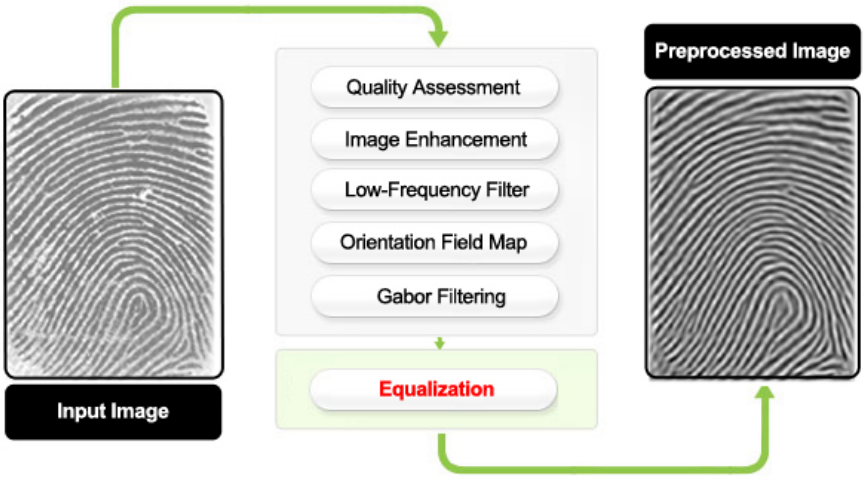



Figure 22: Flow diagram of the correlation-based pre-processing technique.

## 3.2 Iris Recognition

Iris Recognition uses the texture pattern on the surface of the iris for human identification or verification [34]. A person's iris contains approximately six times as many unique, measurable characteristics as fingerprints [54]. The probability that two persons have the same iris pattern is at 1 to $10^{78}$, while the number of people on the Earth is approximately $10^{10}$ [40], as we can see the *uniqueness* property of iris modality is fulfilled. Iris-based systems are relatively nonintrusive and hygienic. There are many literature sources for iris recognition such as Libor Masek "Recognition of Human Iris Patterns for Biometric Identification" [55] and implementation in Matlab, Arun Ross et.al. "Introduction to Biometrics" [34], John Daugman: "How Iris Recognition Works" [54] etc. Although, in order to understand iris recognition system, in this section we are going to give an overview of human's iris anatomy, followed by history of iris recognition and the iris recognition process.

### 3.2.1 The Anatomy of Human Eye

In this section is given a simplified view of a human eye, how it is built up and the way it works. Each eye is roughly a sphere and it is situated in its socket with the assistance of six small extra ocular muscles attached to it. The motion of an eye is supplied by shortening of appropriate muscles. These motions are guaranteed by a part of human brain called brainstem [56]. In a simplified way, the human eye can be categorized in three basic layers [5]. First layer consists of

cornea and sclera, middle layer is composed of choroid, ciliary body and iris and the innermost third layer is made up of retina. These main components with other eye's parts are shown in figure 23.

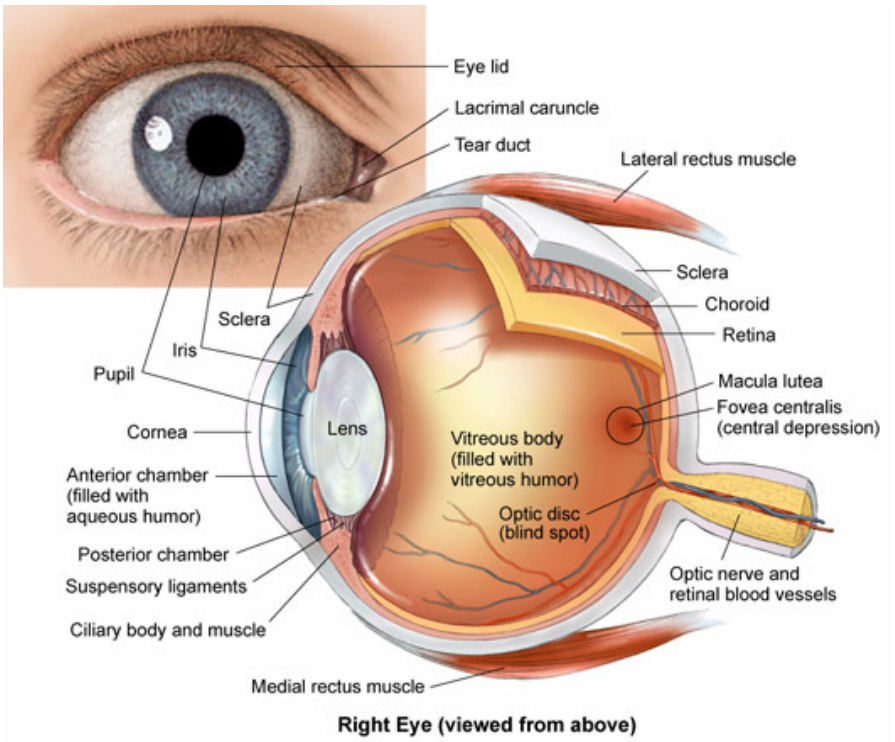



Figure 23: Representation of the human's eye structure [5].

As shown in the figure 23, the eye has many different parts with many different functions. Below is a short description of each part of the eye. Furthermore, in this thesis we will considerate only the *"iris"*.

**Cornea:** the outer coat of eye composes of two units, cornea and sclera. The cornea is smaller frontal unit that is more curved. Because of cornea's transparency, iris and pupil can be seen instead of the cornea and light can easily enter through it, the diameter of cornea to human eye is about 11 mm – 12 mm.

**Sclera:** is larger unit and it is connected to the cornea by a ring called limbus [57] [56]. Main task of the sclera is keeping the eye's shape and it is used as a point of attaching of the extra ocular muscles.

**Pupil:** absorbs almost all light entering into the eye through it, so it seems to be black. For illustrative reasons, let's imagine the pupil as an entrance gate for light into the eye. The iris surrounding this gate is a guardian that permits or forbids rays of light to enter the eye. In a more accurate manner it can be said that the essential task of the iris is to regulate intensity of light by changing size of the pupil [57].

**Lens:** the cornea (transparent frontal part of the eye) and lens together create the equivalent of camera lens. Unlike the focusing of the camera that is reached by changing the distance between lens and film, the focusing of the eye is accomplished by changing the shape of lens and this change is called accommodation. After accommodation the cornea and the lens can focus light rays onto the back of the eye [56]. The lenses in human eyes are created by a transparent protein called crystalline. It assumes that crystalline enables the appropriate accommodation of the eye and is responsible for releasing the right amount of light into the eye.

**Retina:** a light sensitive panel of cells located at the rear of the eye is known as the retina. The retina appears as a thin transparent membrane that covers the internal surface of the ocular globe. It has a shape of plate and it is approximately a quarter millimetres thick. Unlike the other parts of the eye, the retina belongs to the central nervous system and it is directly connected to the brain via optic nerve. The darker red pigmented region represents the macula, which is also known as a yellow spot. In reality, the macula does not have yellow colour in the retina of living individual but it becomes yellow after death.

**Iris:** the coloured part of the eye is called *"iris"* and is the most beautiful part of the eye, which is visible with the naked eye, some of the iris patterns are shown in figure 24. Melanin is a pigment that can be found in human's iris and determines the colour of one's eye. The amount of melanin in iris dictates how dark one's eye will be. More melanin in the eyes means darker eyes. Melanin is also used to block light noise from projecting it onto the retina. Due to this fact, people with light coloured eyes can have problem in bright light conditions [58]. In the centre of the iris the pupil is located. From biometric point of

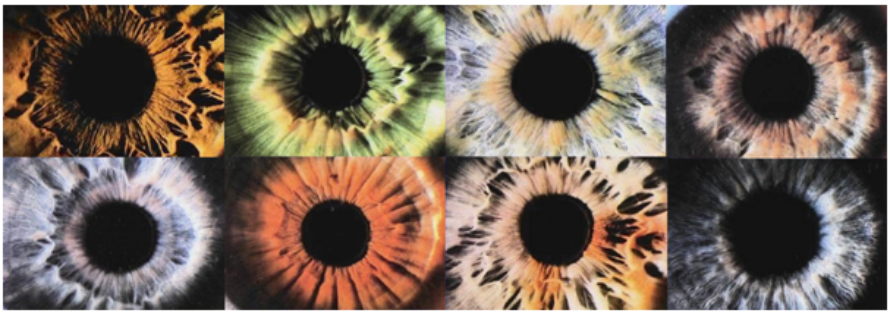


Figure 24: Illustration of some iris patterns (beauty and complexity of iris).

view, the iris is extremely rich in texture. It is unique to every individual, there are even differences between the left and the right eye. This intricate structure can also be used to distinguish identical twins because they have different texture in their iris. For the sake of its accuracy, it represents a universal biometric identifier and can be used for verification or identification [59]. The human iris begins forming during the third month of pregnancy, and it is completely formed by the eighth month after birth and it stays changeless during the whole life, with the exception of several diseases.

### 3.2.2 History of Iris Recognition

In 1886, anthropometrist Alphonse Bertillon proposed the concept of using iris patterns to distinguish (recognize) individuals, meanwhile, in 1936 ophthalmologist Frank Burch proof the similar conclusion [60]. In 1987 two ophthalmologists Dr. Leonard Flom and Aran Safir have published the first patent on iris recognition by proposing the concept that no two irises[1] are alike [61]. On March 1st, 1994 Dr. John G. Daugman was awarded for iris recognition algorithm or as is called *"IrisCode"* comparison and the algorithm is described in details in his patent *"Biometric personal identification system based on iris analysis"* [62]. This algorithm is base for all commercial iris recognition systems that are available today. The Daugman's patent is expired in 2011 [62], some biometric experts thoughts that the number of iris recognition system manufacturers will be increased during this decade [29].

A well known history of iris recognition is the identification of an afghan refugee known all around the world on National Geographic magazine cover page as *"the Afghan Girl"*.

**History of "Afghan Girl":** She was photographed by National Geographic Channel journalist Steve McCurry in December 1984, she was only 12 years old. The Identity of Afghan girl was unknown for roughly 18 years. In January 2002, he traveled to Afghanistan to find her and after about three weeks seeking, he found her and all information about her was revealed, name is *Sharbat Gula* and born around 1972. She was photographed again, but all people could not believe that she was the same person. National Geographic Channel required help from Dr. John Daugman, known for his contribution in iris recognition described above. First, he computed IrisCodes from both eyes captured in 1984, than he computed IrisCodes from both of her eyes captured in 2002. When he conducted the experiment by his own comparison algorithm he got Hamming Distances: 0.24 and 0.31 from the left and right eye, respectively. After these calculations Dr. Daugman concluded that the girl is the same, National Geographic accepted and published this conclusion [63].

Figure 25 shows an image of the refugee in captured in 1984 and 2002, respectively, while on the right side are her iris images and iris codes.

### 3.2.3 Iris Recognition Process

The process of iris recognition is constructed mainly from five different components (subsystems): acquisition, segmentation, normalization, feature extraction (iris code generation) and comparison of iris codes, illustrated in figure 26. All iris recognition steps are explained below.

**Iris Image Acquisition:** most of current iris recognition systems use near-infrared (NIR) spectral band illumination in the 700-900 nanometer (nm) range, illumination should be minimum 5 degree from the eye axes to avoid *"red eye"* effect [12] [39], by NIR illumination we can capture iris images at a distance up to 1 meter. The use of NIR light has many advantages over visible light (400-700 nm), which are:

- NIR light is not visible and it is harmless to the human eye.

[1] Two irises are called irides in biometrics.


Figure 25: "The Afghan Girl", the left side image is photographed in 1984 and 2002, respectively by National Geographic photographer Steve McCurry [64], while on the right side are her iris images and iris codes [63] conducted by Dr. John Daugman.

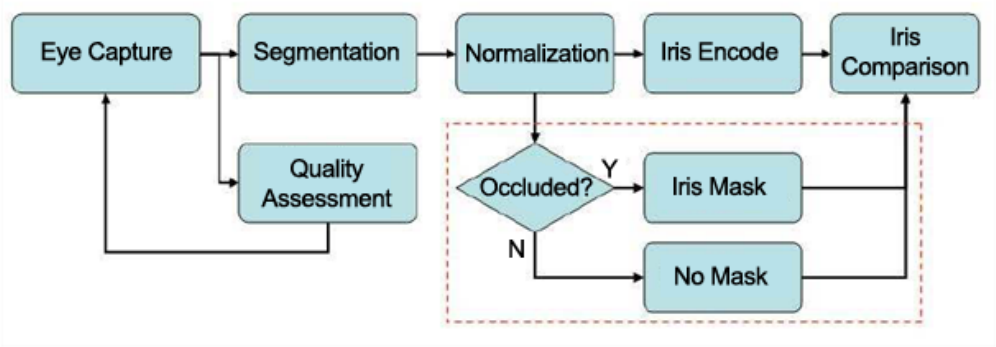



Figure 26: The block diagram of a generic iris recognition system [6].

- Melanin is a pigment that can be found in human's iris and determines the colour of one's eye. The amount of melanin in iris dictates how dark eye will be. It is difficult to capture image iris texture from strong (dark) pigmented irides via visible light. Hence, through NIR we are able to capture iris texture information of dark pigmented irises, while melanin reflect NIR and absorbs visible light.
- NIR light provides better control over the capture device than visible (ambient) light.

According to ISO standard contrast between sclera and iris, iris and pupil should be minimum 70 - 50 grey levels, respectively. Another challenge regarding iris image acquisition defined by ISO is that 70 % of the iris needs to be visible, e.g., not obscured by specular reflections, eyelids, eyelashes, or other obstructions [12] [3]. The image scale should be such that an iris with naturally occurring iris diameter range of 9,5 mm to 13,7 mm has a minimum digital iris diameter of at least 100 pixels. The image should be large enough to include at


Figure 27: Iris image. a) iris with visible light, b) iris with NIR illumination (image from CASIA-Iris-Lamp database version 4.)

Figure 28: Some of iris acquisition devices.

least 70 pixels between the left or right edge of the iris and the closest edge of the image, and at least 70 pixels between the upper or lower edges of the iris and the closest edge of the image as shown in figure 29 [12].

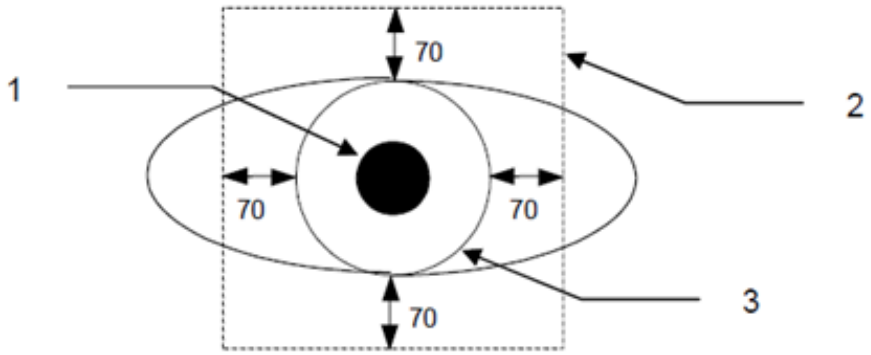



Figure 29: Iris image size specifications by ISO/IEC FDIS 19794-6. 1) pupil boundary, 2) image border, 3) iris boundary. Dimensions are in pixels [12].

**Iris Segmentation:** after image acquisition, the second and most important and critical step in iris recognition systems is to isolate or segment iris region from artefacts such as *sclera*, *pupil*,

*eyelids* and *eyelashes*. Iris segmentation starts with detection of edges by two circles, between sclera and iris, referred as *outer boundary* or *limbus boundary* and iris and pupil referred as *inner boundary* or *pupillary boundary*. An example of iris segmentation is illustrated in figure 30. There are many sources of iris segmentation errors:

- quality of captured image has important role to segmentation,
- iris region is occluded by eyelids and eyelashes,
- inconsistent illumination at acquisition step by low or high contrast between, sclera, iris and pupil,
- high dark pigmented irides may lead to difficulties differentiating iris from pupil.

All challenging problems mentioned above that leads to incorrectly segmented iris, have critical impact in iris comparison accuracy (false match or false non-match). There are many

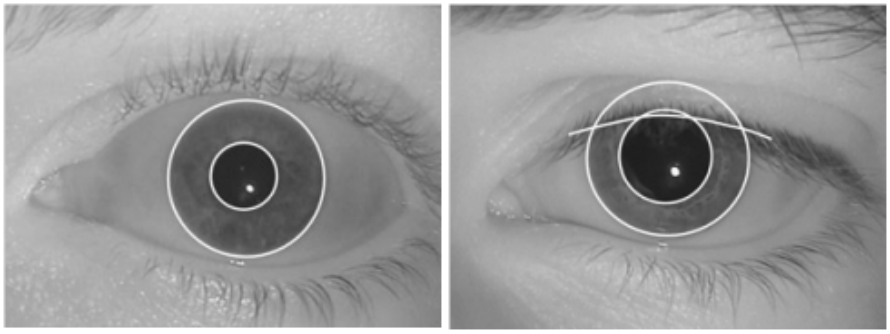



Figure 30: Example of iris segmentation. a) Iris region is not occluded by eyelids and eyelashes; b) iris is occluded by upper eyelid and eyelashes.

algorithms that are used to segment or localize the iris from captured image:

- **Segmentation using Hough Transform model:** This segmentation method is used and well described in following publications: Wildes et al. [65], Kong and Zhang [66], Tisse et al. [67], and Ma et al. [68].
- **Segmentation using Active Contour model:** Ritter et al. [69], and Arun Ross et. al. [70]
- **Segmentation using Eyelash and Noise Detection:** Kong and Zhang Model [66], and new method for eyelash detection using wavelet transform [71].

Furthermore, the first and most used algorithm for iris segmentation is: Daugman's Integro-Differential Operator (IDO) that detect the maximum of the partial derivative developed by John Daugman [54], this algorithm is also called as *Iris2pi*, which is shortly described below.

For segmentation of inner and outer regions Daugman proposed the following optimized equation as definition for IDO:

$$max(r, x_0, y_0) = | G_\sigma(r) * \frac{\partial}{\partial r} \oint_{r,x_0,y_0} \frac{I(x,y)}{2\pi r} \, ds | \tag{3.1}$$

Where *max* is order statistic, *I(x,y)* is an acquired image that contain the eye, *r* is radius to search for, $(x_0, y_0)$ are centre coordinates. The symbol (*) is convolution and $G_\sigma(r)$ is Gaussian smoothing function or filter of scale σ. IDO searches for radius r on image domain (x,y), where is the maximum change in pixel values. This algorithm is type of Hough transform model, but it works with raw derivative data, thus it overcomes the Hough transform limitations, nevertheless it is not appropriate when we have noise in images, such as reflection, low contrast etc., because it is applied only on a local scale [31] [55] [54]. It is to be noted that"*internal details of the IDO algorithm are not publicly available*" [29].

**Iris Normalization:** after correctly segmented iris, a normalized template is generated [29]. Same iris image captured over multiple attempts, will not be the same size due to variety of sources: imaging distance between iris and acquisition device will never be exactly the same, rotation of camera or head, size of pupil due to ambient illumination will indirectly affect the size of iris (e.g. number of iris pixels), moreover in bright light our pupil's size decreases and in low light the pupil's size increases to avoid these factors a normalized (rectangular) image is generated and sometimes is called as unwrapped images with fixed dimensions (size) [72], in order to compare two iris samples. There are many algorithms for iris normalization as follows:

- Image Registration [73],
- Virtual Circles [74],
- Daugman's Rubber Sheet Model [54].

Nevertheless, the most used approach for iris normalization today is Daugman's Rubber Sheet Model [54] and is described below. Daugman's iris normalization approach convert iris image to unwrapped image as mentioned previously and converts it from Cartesian coordinates to a normalized pseudo-polar coordinate system. Goal of this model is to transformation the iris pattern to flat area. Daugman's rubber sheet model re-maps every point of segmented iris region to a couple of polar coordinates $(r, \theta)$, where *r* is radial parameter [0,1] and θ is angular parameter between 0 and $360^o(2\pi)$. This model is illustrated in figure 31.

The re-mapping of the segmented iris I from Cartesian coordinates *(x,y)* to normalized pseudo-polar coordinates $(r, \theta)$ is defined as:

$$I(x(r,\theta), y(r,\theta)) \rightarrow I(r,\theta) \tag{3.2}$$

with

$$x(r,\theta) = (1-r)x_p(\theta) + rx_l(\theta)$$

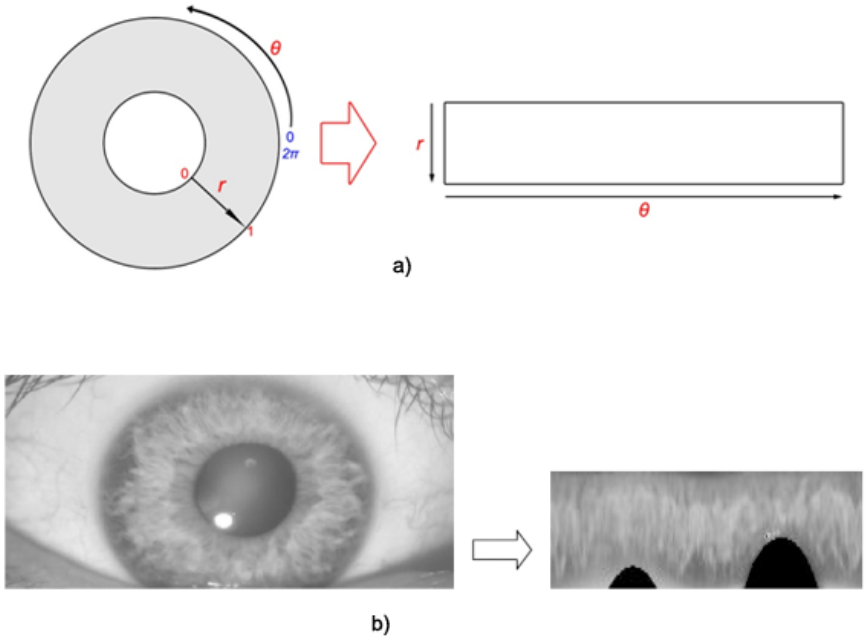



Figure 31: Iris Normalization. a) Daugman's Rubber Sheet Model, b) Example of iris image and normalized iris.

and

$$y(r,\theta) = (1-r)y_p(\theta) + ry_l(\theta)$$

where $x_p, y_p$ are coordinates of pupil boundary and $x_l, y_l$ are coordinates of iris boundary [55] [34].

**Iris Encoding (computing the IrisCode):** Once the normalized iris pattern is produced, it is divided into a grid of 128x8 blocks this process is called iris encoding. A complete iris recognition system is developed by Dr. John Daugman, and this encoding algorithm is based on Daugman's approach [54], illustrated in figure 32 together with iris 8 rings sample.

Each block in grid 128x8 of segmented iris pattern is then projected onto quadrature 2D Gabor filter to extract the pattern information and the filter's phase response is measured [54] [29]. Only phase information is took into consideration, because it provides discriminating information of iris and is invariant than amplitude information, which suffer from illumination or contrast information in image [75]. The quadrature 2D Gabor wavelets proposed by [54] generate complex number or phase angle that contains real part and imaginary part, where real and imaginary parts specify the coordinates of the phasor in the complex plane. The expression for demodulation and phase quantization is:

$$h_{Re,Im} = sign_{Re,Im} \int_{\rho}\int_{\phi} I(\rho,\phi) e^{-i\omega(\theta_0-\phi)} e^{-(r_0-\rho)^2/\alpha^2} e^{-(\theta_0-\phi)^2/\beta^2} \rho d\rho d\phi \qquad (3.3)$$

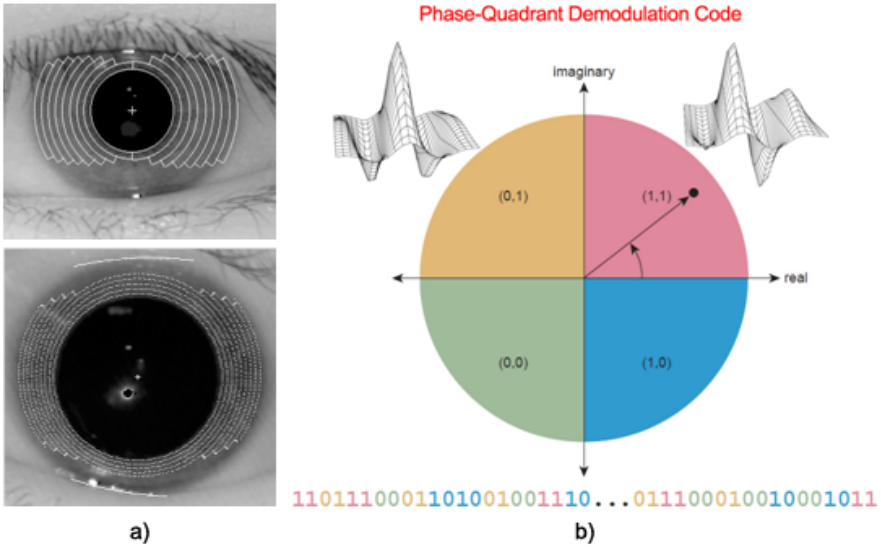



Figure 32: Iris Encoding Process. a) 8 rings at normal size pupil and extended pupil, b) quadrature 2D Gabor wavelets used to extract iris code [54].

where, $h_{Re,Im}$ is complex valued bit, $I(\rho,\phi)$ is normalized iris image in pseudo-polar coordinate, $\alpha,\beta$are parameters of the wavelet function and $\omega$ is frequency of wavelet band. The output of this equation is binary value containing two bits depending on which quadrant they are (2 bit - Re, Im) to facilitate the comparison [62]:

$$h_{Re} = 1 \text{ if } Re \int_{\rho}\int_{\phi} e^{-i\omega(\theta_0-\phi)} e^{-(r_0-\rho)^2/\alpha^2} e^{-(\theta_0-\phi)^2/\beta^2} I(\rho,\phi)\rho d\rho d\phi \geq 0 \tag{3.4}$$

$$h_{Re} = 0 \text{ if } Re \int_{\rho}\int_{\phi} e^{-i\omega(\theta_0-\phi)} e^{-(r_0-\rho)^2/\alpha^2} e^{-(\theta_0-\phi)^2/\beta^2} I(\rho,\phi)\rho d\rho d\phi < 0 \tag{3.5}$$

$$h_{Im} = 1 \text{ if } Im \int_{\rho}\int_{\phi} e^{-i\omega(\theta_0-\phi)} e^{-(r_0-\rho)^2/\alpha^2} e^{-(\theta_0-\phi)^2/\beta^2} I(\rho,\phi)\rho d\rho d\phi \geq 0 \tag{3.6}$$

$$h_{Im} = 1 \text{ if } Im \int_{\rho}\int_{\phi} e^{-i\omega(\theta_0-\phi)} e^{-(r_0-\rho)^2/\alpha^2} e^{-(\theta_0-\phi)^2/\beta^2} I(\rho,\phi)\rho d\rho d\phi < 0 \tag{3.7}$$

From expressions above we can conclude that: if the real part of equation is positive, it is represented as 1 or otherwise as 0. If imaginary part of equation is positive, it is represented as 1 or otherwise as 0. The phase angle is thus represented using 2 bits: (128x8) x 2 bits= 2048 phase bits equal to 256 bytes. This 256 byte template is called **IrisCode**, this process is shown in figure above. Furthermore, a 256 byte array is computed together with iris code, which is called *iris mask*. Masking bits indicate whether any iris region is usable or obscured by eyelids, contains any eyelash occlusions, specular reflections, boundary artefacts, hard contact lenses, poor signal-to-noise ratio this unusable regions (not contained in the mask) are ignored in the demodulation code as artefact during comparison process. In figure 33,


Figure 33: An example of a) iris code and b) iris mask. Calculated by Matlab (from CASIA DB image sample).

is given an example of iris code and iris mask. Other iris feature encoding algorithms are publicly available, such as: wavelet encoding, Log-Gabor filters [55], zero-crossings of the 1D wavelet [74], Haar wavelet [76] and Laplacian of Gaussian filters [73].

**Iris Code Comparison:** after iris code creation, we are able to perform iris comparison that results the similarity between two iris codes. Set of comparison values from the same irides is known as *intra-class comparison*, and comparison from different irides is known as *inter-class comparison*. There are three main metrics for iris comparison: Hamming distance (HD), weighted Euclidean distance (WED) and normalised correlation (NC) which are described below. The most used comparison method is Hamming distance.

- **Hamming distance:** Daugman's iris recognition approach [54] calculates a metric called the *normalized Hamming distance* (HD) for comparison of dissimilarity between two iris codes. The HD between two iris codes is calculated by:

$$\mathrm{HD} = \frac{|\,(\mathrm{codeQ} \otimes \mathrm{codeR}) \cap \mathrm{maskQ} \cap \mathrm{maskR}\,|}{|\,\mathrm{maskQ} \cap \mathrm{maskR}\,|} \tag{3.8}$$

Where codeQ is iris code of captured sample (Q) referred as probe iris code, codeR is iris code stored in database (R) referred as reference iris code, while maskQ and maskR are masks of Q and R, respectively. For each corresponding bits in the two iris codes, their corresponding mask bits are checked for quality. If both mask bits indicate that the iris code bits are usable (significant), they are compared. Operation $\otimes$ is Boolean Exclusive-OR (XOR) that provides a comparison between codeQ and codeR, to find differences between given iris codes. The result of this operation is 1 if two bits of code are different, and 0 if they are equal. Each bit of XOR operation is to be compared with the corresponding masks of Q and R by Booleand AND $\cap$ operation. This is done as said previously in order to ignore disturbed areas of the image such as: reflection, eyelids, eyelashes etc. To sum the bits that are true the operation ($||$) is used, it counts the differences (in the numerator) and the compared bits (denominator). In theory, two same irises will have HD=0.0 and it is known as *"perfect match"*, but in practise this is unreached due to normalization undetected noise. With decreasing of HD, the similarity of the two iris codes increases. The smaller the HD criterion the smaller the likelihood of a false accept case is, and vice-versa the higher the HD criterion, the higher the likelihood of a false reject case is, this is presented in table 3. Image of the iris could be rotated (tilted head) and this is to be accounted only in comparison stage. As we can see from table 3, the most Daugman-based systems have the threshold around 0.33, and a successful match is for similarity score less than 0.33. Large-scale and

Table 3: Error probabilities [3].

| HD Criterion | Likelihood of a false accept rate (FAR) |
|---|---|
| 0.26 | 1 in $10^{13}$ |
| 0.27 | 1 in $10^{12}$ |
| 0.28 | 1 in 84 billion |
| 0.29 | 1 in 8.6 billion |
| 0.31 | 1 in 127 million |
| 0.32 | 1 in 18 million |
| 0.33 | 1 in 2.9 million |
| 0.34 | 1 in 527.000 |
| 0.35 | 1 in 105.000 |

statistical analysis has shown that this threshold is acceptable for operational systems [77]. Daugman's iris comparison technique has many advantages. It is extremely quick, since the comparison between two iris codes is made by bitwise operation [29].

**Weighted Euclidean Distance (WED):** is iris recognition comparison method that has been used by Zhu et al. [78], and it compares two iris codes, particularly if the iris codes are represented as integer numbers. The WED outputs a measure of how similar are the sets of integer scores between two iris codes. The expression for this method is as following:

$$WED(k) = \sum_{i=1}^{N} \frac{(f_i - f_i^{(k)})^2}{(\delta_i^{(k)})^2} \tag{3.9}$$

Where $f_i$ is the i-th distinguished feature of unknown iris code, $f_i(k)$ and $\delta_i(k)$ are the i-th distinguished feature of stored iris code k, respectively. Two compared iris codes (unknown iris code and stored iris code k) are *match*, when WED reaches a minimum at k.

**Normalised Correlation (NC):** is a comparison method that has been implemented by Wilde [73] for iris recognition. The method tries to find a normalized correlation between the unknown iris code and stored iris code in the data storage. The method is defined as following:

$$\frac{\sum_{i=1}^{n}\sum_{j=1}^{m}(p_1[i,j]-\mu_1)(p_2[i,j]-\mu_2)}{nm\sigma_1\sigma_2} \tag{3.10}$$

where $p_1$ and $p_2$ are two iris codes with image size $n_x m$, $\mu_{1,2}$ and $\sigma_{1,2}$ are the mean and standard deviation of $p_1$ and $p_2$, respectively. Normalized correlation overcomes one of the main drawbacks of standard correlation that is: local variations of image intensity.

In table 4 is given a comparison of EER (Equal Error Rates) from previous researches and our approach only for iris recognition process for CASIA-IrisV4-Lamp.

As one can see from table 4 our iris comparison process by VeriEye 6.5 SDK for database CASIA-IrisV4-Lamp we have received EER equal to 0.71 %, which is lower than previous approaches based on He et.al. work published in 2009 [79].

Table 4: Comparison of performances provided by [79] with our iris recognition performance on CASIA-IrisV4-Lamp database.

| Study | Performance | CASIA-IrisV4-Lamp |
|---|---|---|
| Wildes [73] | EER(%) | 1.05 |
| John Daugman [80] | EER(%) | 0.86 |
| He et. al. [79] | EER(%) | 0.75 |
| Our Approach (VeriEye) | EER(%) | 0.71 |

## 3.3 Summary

Fingerprint is the oldest and most widely adopted biometric technology, but, as discussed in this chapter, it is by no means a fully mature technology. The improvement of fingerprint recognition requires research into issues that arise from real-world deployments, such as user interaction, system security and policies, along with image processing algorithms. The increase in the use of mobile and small-scale devices for fingerprint recognition is the next frontier. This will introduce a variety of challenges including user interaction, quality assessment in the field, remote connectivity, policies and procedures to support a mobile infrastructure. Fingerprint still is relatively cheaper than most other biometric solutions and will continue to enjoy broad acceptance in commercial and government implementations. The success of fingerprint recognition in operational deployments will depend on creating solutions that include the user, the system, and the organizational policies.

Iris recognition has made great strides in the last decade and the iris texture has shown high distinctiveness for use in large-scale applications. The evaluation of iris images has shown that different color irises provide better quality images in different wavelengths. Future iris systems could use multispectral imaging and choose the best quality iris images. Iris segmentation still remains the most studied area of iris recognition, although research in user interface and iris capture at a distance will likely become important in the near future. Iris recognition has already established itself as the biometric of choice for large-scale systems, and its proliferation will continue in the near future.

# 4 Multi-modal and Multi-instance Biometrics using fingerprint and iris

Security systems are not perfect, neither are biometric solutions[31]. The concept of multiple layering continues to gain traction as the biometrics industry is faced with imperfect systems and imperfect solutions. Whether the focus is on a security system in general or on a specific biometric solution, using a combination of proven techniques has the potential to make any system more robust and alleviates many of its limitations.

A multisystem security strategy is basically the use of two or more levels or types of security techniques. So waving an identity badge (something we have) and entering a personal identification number (PIN) or password (something we know) could be considered multisystem security. The concept is to use multiple techniques or technologies in a layered approach. No single system is foolproof, for that matter, multiple systems are not foolproof either. Nevertheless, multiple security systems used together are generally more resistant to fraud since they employ different techniques or technologies and process information through different algorithms. Similarly, using a multibiometric system (something we are) increases security (e.g., by improving accuracy) and broadens support for and acceptance by the user population by offering alternatives.

This chapter explains the limitations of unimodal biometric systems, describes multiple biometric integration strategies and clarifies how multibiometric systems work.

## 4.1 Limitations of Unimodal Biometric Systems

Nowadays, the biometric systems running in real world applications are primarily uni-modal. These systems use only one of the single biometric markers with purpose of identifying personal authentication (e.g fingerprint or iris). Unimodal biometrics are limited, because none of biometrics alone are not considered strong enough to deal with hindrances caused by any external factor [16]. Some of the biggest concerns that these systems try to deal with, are as following:

- **Noise**: made in the gained data due to differences in the biometric marker (e.g. surgically modification of the finger) [33]. Fingers with cuts across the fingerprinting areas or voices altered by bad colds are examples of noise. The issue with noisy biometric data is that it may cause an incorrect match or deny a genuine match [16].
- **Intraclass variation**: that could happen when a user contact with the sensor or with transformations caused by physiological factor that occurs with ageing [33].
- **Interclass similarities**: appears when a biometric database contains a large number of users, appearing the need to increase the complexity in order to make differences between the users [33].
- **Non-universality**: The biometric system may not get clear biometric data from some of the

users. *" The lack of universality is the primary reason for Failure-To-Enroll (FTE) situations"* [16].

- **Resistance to circumvention**: is the case when a user in the successful way masquerades as another person by falsifying biometric data taken from other person [33].

Some of the limitation of unimodal biometric may be resolved by combining multiple biometric markers in order to perform authentication. These systems are called multimodal biometric system, and are expected to be more secure because of the integration of multiple independent pieces of evidence [81]. Such a system is able to address those issues mention above shortcomings inherent to unimodal biometrics. For instance, the chance to get valuable biometric increases with the number of involved biometric markers. They also prevent data spoofing because it is more difficult to spoof multiple biometric markers of real users[33].

In most situations, the deployment of biometric systems is a superior solution to its precursor technologies—badge tokens, keys, PINs, and passwords. However, biometric solutions almost always have a need for improved performance or a broadening of their usability. The degree of needed improvement depends on the application and on the population using the biometric system. In some situations, it may be prudent to consider multiple integration strategies.

## 4.2 Multiple integration strategies

In general there are six types of multibiometric authentication systems based on the number of different modules or type of acquisition input. The definitions for these scenarios (types) are based on different sources [16, 1, 34]. In figure 34 we started from the top and moving clockwise to explain these types of multibiometrics:

1. **Multiple Sensors**: In these systems multiple samples are produced for a single biometric trait to assuage noisy sensor data, therefore different sensors might be used to improve performance for the same biometric identifier such as fingerprinting (e.g., optical and capacitance sensors).
2. **Multiple Samples**: A single sensor might be used to capture the same biometric modality using the same instance (e.g., two attempts or templates of a person's right index finger vein).
3. **Single Biometric-Multiple Matchers**: In these systems, the same biometric trait is processed using different algorithms (approaches) for feature extraction and matching module (e.g., minutiae vs. non-minutiae based, like filter-based) matcher or algorithm.
4. **Multiple Biometric fusion**: usually referred as multimodal biometric system using different body traits of the same person (e.g., using finger vein and fingerprint together, or gait and fingerprint, face, iris and fingerprint etc.)
5. **Multiple Instances**: These systems combine multiple instances from the same biometric trait (this is also called as multi-unit or intramodal system in the literature) such as five fingers, ten fingers or both palms for vein recognition.
6. **"Soft Biometrics"**: These systems are rarely deployed, but worth noting here as *"soft biometrics"* are considered all those characteristics that have lack of the distinctiveness and permanence to identify an individual, on the other hand they provide complementary information for

primary biometric traits. ”Soft biometrics” are: gender, age, eye color, hair color, height, weight, ethnicity etc.

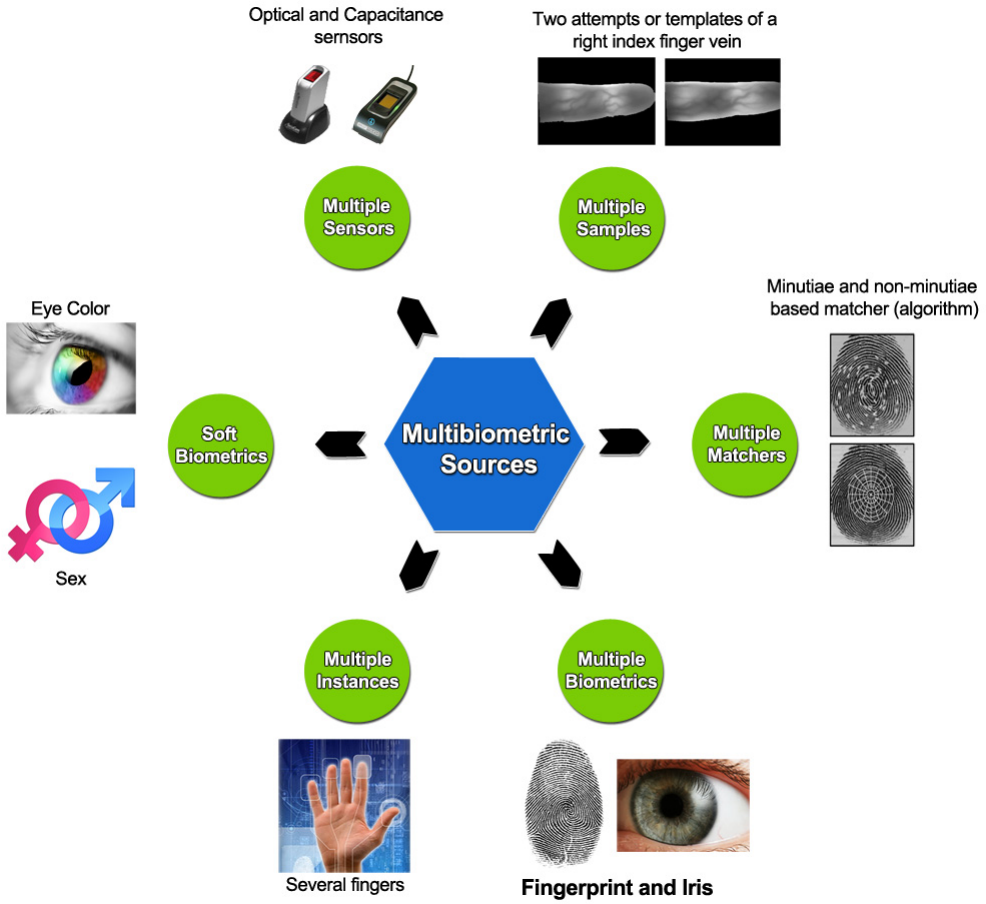



Figure 34: Types of multibiometric authentication systems [16].

The choice of multiple integration strategies depends primarily on an enterprise’s requirements as well as the type of applications supported, the correlations among the biometric identifiers, and, of course, the costs incurred. These techniques provide multiple corridors of security checks that can be performed simultaneously or sequentially. Multiple biometric techniques combine multiple factors of evidence to enable better decisions. By combining the evidence obtained from different sources, biometric systems can overcome some of the limitations of unimodal biometrics and generally improve recognition performance.

When the topic of multibiometric systems surfaces, most people think of multimodal biometric systems that use more than one physiological or behavioral trait for enrollment and identity verification (1:1 comaprison) or identification (1:n comparison). Multimodal systems are arguably the most powerful type of multibiometric system, and they hold great promise for significant performance improvements over unimodal systems. Indeed, multimodal systems analyze the

evidence from multiple sources for verifying an individual's identity or for identifying an individual from a database. Generally, multimodal systems provide superior recognition performance over unimodal biometric systems. Multimodal systems offer an extensive set of advantages:

- Reduce the number of false acceptances and false rejections, and thus significantly improve the matching accuracy and the overall performance of the biometric system, often providing a substantial reduction in the error rate.
- Better thwart attempts to spoof a biometric system, as it is difficult to spoof multiple traits simultaneously.
- Extend the range of acceptable environmental conditions (e.g., noise reduction) with which authentication or identification can occur.
- Provide a secondary means for enrollment, verification, and identification, increasing the availability of the biometric system, broadening its population coverage, and minimizing the effects of intra- and interclass variation.

Despite the advantages of multimodal biometrics, there are also some disadvantages such as high cost, complexity and longer processing time. These disadvantages are overcome by advantages.

## 4.3 Levels of Fusion

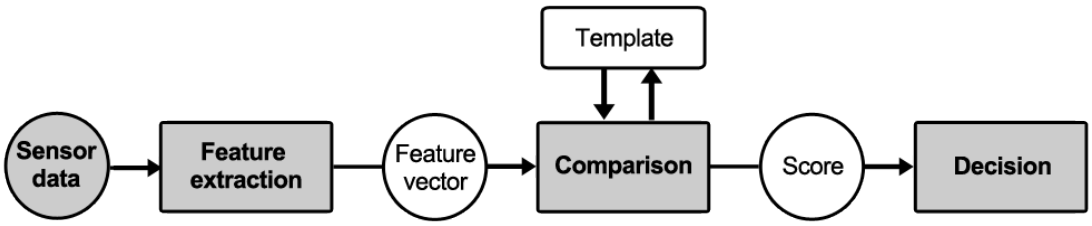



Figure 35: General biometric authentication process flow.

In most biometric systems, there are four key processes, as illustrated in figure 35: (1) capturing the biometric trait to be measured in the form of raw data; (2) processing the data extracted into a compressed representation of the trait; (3) comparing the extracted feature set with the reference data, generating a matching score; and (4) using the matching scores to either make an identification decision or to verify a claimed identity.

The use of multiple biometric techniques increases the likelihood of a successful match. Fusion levels can be categorized based on these biometric system components to fuse the biometric information. These fusion levels are described in following sections. According to [16] fusion can be performed at two basic stages:

- **Fusion before comparison** - Integration of information from multiple biometric sources can take place either at the sensor level or at the feature level.
- **Fusion after comparison** - Schemes for integration of information after the comparison stage

can be divided into four categories: dynamic classifier selection, fusion at the comparison score level, fusion at the decision level and fusion at the rank level.

### 4.3.1 Sensor Level Fusion

Figure 36 illustrates fusion at the sensor level. The sensor module reads the biometric attribute (e.g., a hand or finger), and then compiles raw data that is sent to the feature extraction module. In sensor level fusion, the raw data from the sensors are combined. As an example, this consolidation of data could occur if there are multiple reads of the same biometric trait from multiple compatible sensors (e.g., multiple images of same fingerprint, of the same iris etc.). With sensor level fusion, the data obtained must be compatible. For instance, reads from multiple sensors of differing quality and manufacture may not be compatible. Theoretically , data obtained from different sensors would be combined into a joint sensor vector prior to being sent out to the feature extraction module.

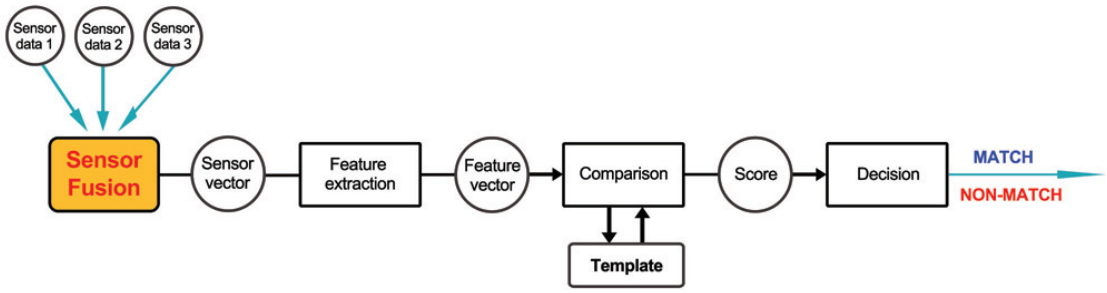



Figure 36: Fusion at sensor level [7].

### 4.3.2 Feature-extraction Level Fusion

Refers to combining different target features to produce a new feature set. Figure 4 illustrates the process of feature extraction fusion. In feature extraction fusion, feature vectors are combined. An example of fusion at the feature extraction level might occur with features extracted with multiple sensors. When feature vectors are homogeneous, such as multiple finger images, a weighted average of the individual features can calculate a single feature vector. However, this is rarely the case with true multimodal systems. Feature extraction fusion may not be practical or feasible in many situations, and most attempts to fuse multiple modalities at this level have met only limited success.

Additionally, most vendors do not wish to release the feature values computed by their systems, rendering feature level fusion problematic. *"Vendors' feature extraction processes are generally patented and are always held secret"* [32]. Although it is intuitively appealing to integrate information prior to matching the biometric data, it is difficult to achieve such integration in practice.

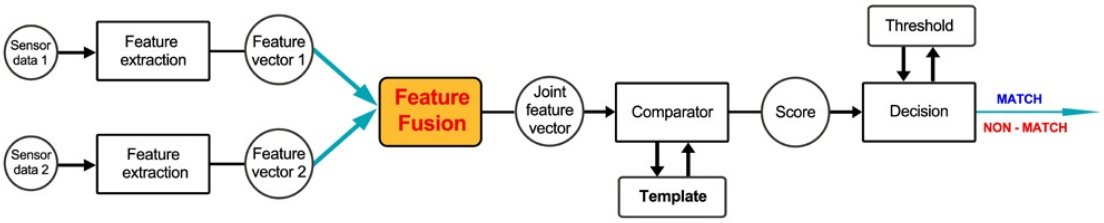



Figure 37: Fusion at feature-extraction level [7].

### 4.3.3 Score Level Fusion

Although there are many fusion scenarios, most multimodal biometric systems integrate data at the comparison score level because it offers a strong compromise between the ease in combining the data and better information content, and because it is a relatively straightforward way to combine the scores generated by different matchers. Therefore, comparison score fusion is generally the preferred approach for integrating data. Figure 38 illustrates this process. In comparison score fusion, scores produced by each modality are combined by a variety of techniques to produce a new score for comparison to the threshold. There are two key approaches in use today for consolidating comparison scores: classification and combination. In the classification approach, one can construct a feature vector with individual comparison scores, and it is then classified into accept or reject classes. A classification approach might use a decision tree, Support Vector Machine (SVM) or Linear Discriminate Analysis (LDA) algorithm to classify the vector as imposter or genuine. With the combination approach, one combines individual comparison scores to generate a single scalar score to render the final decision. The combination approach for consolidating comparison scores has compiled a superior performance record versus the other levels.

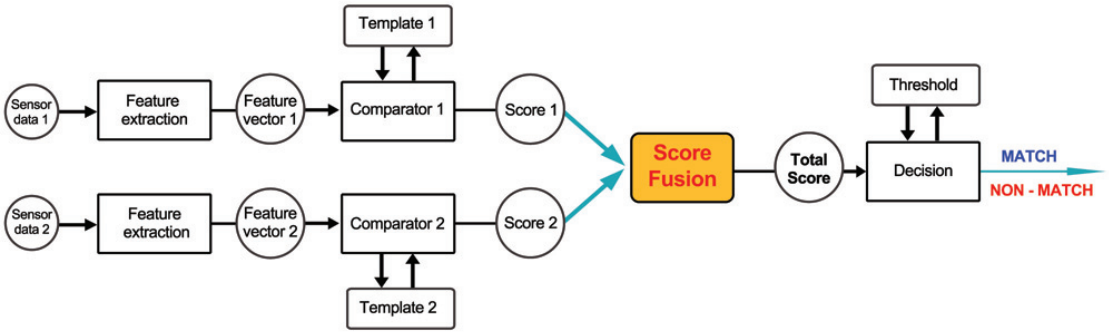



Figure 38: Fusion at comparison score level [7].

### 4.3.4 Decision Level Fusion

Let us briefly skip ahead to decision level fusion, which is depicted in figure 39. At the decision level, each biometric modality renders a separate authentication decision, and then those decisions are integrated using techniques similar to majority-voting schemes. The fusion effort at this level is commensurate to two separate verification processes joined together at their yes/no decision levels. Fusion at the decision level is commonly used but is seen as rigid and somewhat simplistic due to the limited content information available. Indeed, it has acquired some popularity as "layered biometrics". Nevertheless, the limited value of decision level fusion may not merit the added overhead that an organization would incur in implementing it. However, for certain implementations its use could be quite feasible.

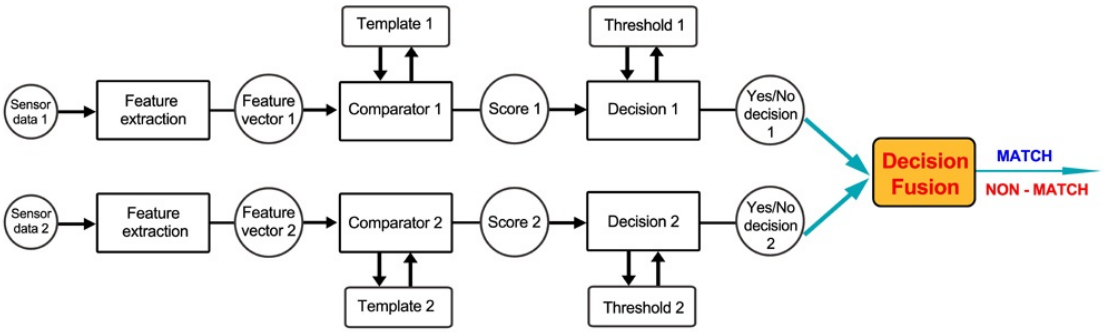



Figure 39: Fusion at decision level [7].

## 4.4 Literature Review - Fusion of Multimodal Biometrics

An overview of several modality fusion approaches is given in table 5. To the best of our knowledge and from table 5 fusion of fingerprint and iris at score level is not treated or better saying less studied. Fusion of these two modalities is studied at feature-extraction level as is highlighted in table 5 for cryptographic key generation purposes.

## 4.5 Score Level Fusion of Fingerprint and Iris: Normalization and Fusion Methods

As discussed previously in this chapter in biometric systems there are several types of fusion levels such as: sensor (sample) level, feature (template) level, score level or decision level. Many researches and industrial statistics have shown that comparison score level fusion is more accurate and effective than others [16]. The score level fusion that is scope of this thesis has two main steps. The first step of fusion at this level is called *"score normalization"*, what means that calculated comparison scores by certain comparator (algorithm) $S_i$ are mapped onto a new score scale or domain $S_i^{'}$. For instance, if comparator X produces scores on a domain of $[1, 100]$ and comparator Y generates scores on a domain of $[1, 2500]$, in these cases score normalization is required to map them to a common domain. The second step of fusion at score level is *fusion* itself. Exist many way of score fusion, but in this master project we are going to follow ISO standard on multibiometrics:

Table 5: Previous multimodal fusion approaches.

| Study | Fused Modalities | Fusion Level |
|---|---|---|
| Brunelli et.al. (1995) [82] | Face and voice | Score Level |
| Kittler et.al. (1998) [83] | Face and voice | Score Level |
| Ben-Yacoub et.al. (1999) [84] | Face and voice | Score Level |
| Bigun et.al. (1997) [85] | Face and voice | Score Level |
| Frischholz et.al. (2000) [86] | Face, voice and lip | Score Level |
| Hong et.al. (1998) [87] | Face and fingerprint | Score Level |
| Snelick et.al. (2005) [88] | Face and fingerprint | Score Level |
| Conti et.al. (2010) [21] | Fingerprint and iris | Feature Level |
| Jagadeesan et.al. (2010) [18] | Fingerprint and iris | Feature Level |
| Jagadeesan et.al. (2011) [20] | Fingerprint and iris | Feature Level |
| Derawi (2009) [30] | Fingerprint and gait | Score Level |
| Wang et.al. (2003) [89] | Face and iris | Score Level |
| Zhou et.al (2007) [90] | Face and gait | Score Level |
| Jafri et.al. (2008) [91] | Face and gait | Score Level |
| Chang et.al. (2003) [92] | Face and ear | Sensor Level |
| Feng et.al (2004) [93] | Face and palmprint | Feature Level |
| Cui et.al. (2011) [94] | Fingerprint and vein | Score Level |
| Toh et.al. (2003) [95] | Fingerprint and hand | Score Level |
| Camlikaya et.al. (2008) [96] | Fingerprint and voice | Feature Level |
| Fierrez-Aguilar et.al. (2005) [97] | Fingerprint and signature | Score Level |
| Krawczyk et.al. (2005) [98] | Voice and signature | Score Level |

*"ISO/IEC TR 24722:2007 – Multimodal and other Multibiometric Fusion"* [7]. In figure 40 is given a score level fusion framework of our approach (fingerprint + iris).

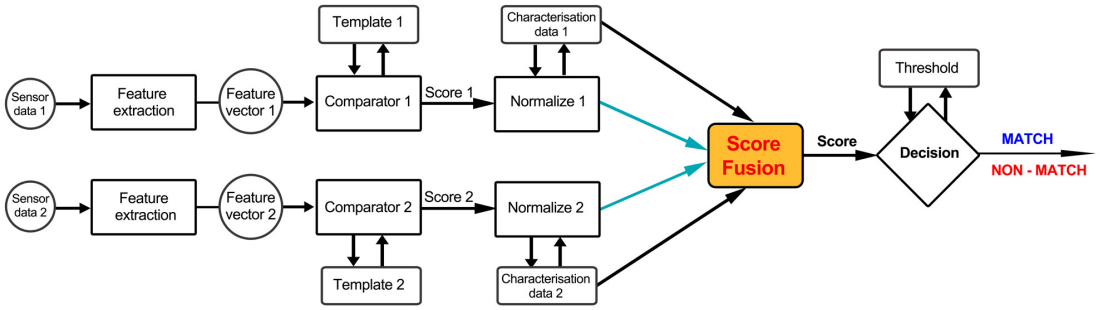



Figure 40: Advanced framework for score-level fusion approach [7].

### 4.5.1 Score Normalization

The Score Normalization process is research area onto itself [99], even though in this section are described fundamental points in order to understand this thesis [16] [7]. This process is performed to change the comparator's parameters and data types to map comparison scores to a

common scale (domain). Commonly, score normalization techniques are evaluated on the bases of robustness and efficiency.

The most used score normalization techniques that are employed in this thesis are: Min-Max (MM), Z-Score (ZS), and Hyperbolic Tangent (TanH). These methods are discussed below and in Appendix C are given in table of score normalization methods from ISO standard.

Table 6: Symbols used for score normalization expressions.

| **Statistical measrues** | **Genuine distribution** | **Impostor distribution** | **Both** |
|---|---|---|---|
| Minimum score | $S^G_{Min}$ | $S^I_{Min}$ | $S^B_{Min}$ |
| Maximum score | $S^G_{Max}$ | $S^I_{Max}$ | $S^B_{Max}$ |
| Mean | $S^G_{Mean}$ | $S^I_{Mean}$ | $S^B_{Mean}$ |
| Score standard deviation | $S^G_{SD}$ | $S^I_{SD}$ | $S^B_{SD}$ |

**Min-Max Normalization (MM):** performs a linear transformation of the original data. This is one of the simplest normalization techniques; it is most useful when the limits of the scores produced are known. It is generally efficient and provides adequate performance, but it may not yield completely accurate results if the data used contains outliers. MM maps raw scores to the [0,1] range, and given comparison scores such that $S^B_{Max}$ and $S^B_{Min}$ designate the end points of the score range.

$$S' = \frac{S - S^B_{Min}}{S^B_{Max} - S^B_{Min}} \tag{4.1}$$

**Z-Score Normalization (ZS):** is one of the more commonly used normalization techniques. It uses an arithmetic mean and standard deviation to normalize data; therefore, a priori knowledge regarding the average score and score variances of the matcher is needed. It is considered generally efficient and tends to work exceptionally well if the scores of each modality used follow a Gaussian distribution, but this technique may not achieve similar accuracy if the data used contains outliers since the mean and standard deviation are sensitive to outliers. ZS normalization transforms the scores to a normal distribution with an arithmetic mean $S^I_{Mean}$ of 0 and a standard deviation $S^I_{SD}$ of 1.

$$S' = \frac{S - S^I_{Mean}}{S^I_{SD}} \tag{4.2}$$

**Hyperbolic Tangent Normalization (TanH):** is generally efficient and provides adequate performance. It is very robust in handling outliers; however, it has been demonstrated that to work efficiently the parameters must be selected carefully. TanH maps the raw scores to the (0,1) range, where $S^G_{Mean}$ and $S^B_{SD}$ are the mean and standard deviation estimation of the score distribution, respectively.

$$S' = 0.5 \cdot \tanh \cdot \frac{0.01(S - S^G_{Mean})}{S^B_{SD}} + 1 \tag{4.3}$$

### 4.5.2 Score Fusion Techniques

In general, score fusion techniques fall into two categories: classification and combination approaches. Classification approaches formulates the problem as dividing the decision space into two classes: genuine and impostor. The reliability and effectively of this method is dependent on the large amount and quality of input data that are available to train the classifier and this is one of the disadvantages of this approach. Although, comparison scores need not to be homogeneous and hence normalization step here is not required. Some of the classification methods that have been researched are: neural network, nearest neighbourhood algorithms and tree-based classifiers.

Combination approach is most common and effective method for comparison score fusion. This method combines comparison scores from multiple comparators and generates single comparison score. It is obvious that this technique require score normalization in advance to fuse the comparison scores. The most used score level combination fusion techniques that are used in this thesis are: minimum score, maximum score, simple sum and user weighting. These fusion techniques are discussed below and in Appendix C, respectively in Table 28 are given several fusion methods from ISO standard.

**Minimum Score:** the max rule estimates the mean of the posteriori probabilities by the maximum value.

$$min(i = 1 \text{ to } N)\ S_i' \tag{4.4}$$

**Maximum Score:** the min rule sets the minimum value of posteriori probabilities.

$$max(i = 1 \text{ to } N)\ S_i' \tag{4.5}$$

**Simple Sum:** this is basically a weighted average of the raw scores. Matcher scores are summed without benefit of normalization routines. It simplistically assumes that the raw scores supplied by the biometric methods used have a comparable scale, distribution, and strength; there is no rescaling or reweighting to account for matcher accuracy variability. It can be used when there is a high level of noise resulting in some ambiguities in classification.

$$\sum (i = 1 \text{ to } N)\ S_i' \tag{4.6}$$

**User Weighted Sum:** this method computes the combined matching score as a weighted sum of the matching scores. The motivation behind the idea of user-specific weights for computing the weighted sum of scores is that some biometric traits cannot be reliably obtained from some people (e.g., individuals with faint fingerprints). Assigning a lower weight to the fingerprint score and a higher weight to other modalities reduces the probability of a false rejection.

$$\sum (i = 1 \text{ to } N)\ W_i^* \cdot S_i' \tag{4.7}$$

If implemented correctly, matching score fusion can improve accuracy, better thwart fraudsters, and increase usability. Implemented incorrectly, a multibiometric system might actually experience performance degradation in comparison to a unimodal solution. Further, multimodal systems potentially have a higher cost of ownership, can increase user inconvenience, can decrease user acceptance, and can exacerbate privacy issues.

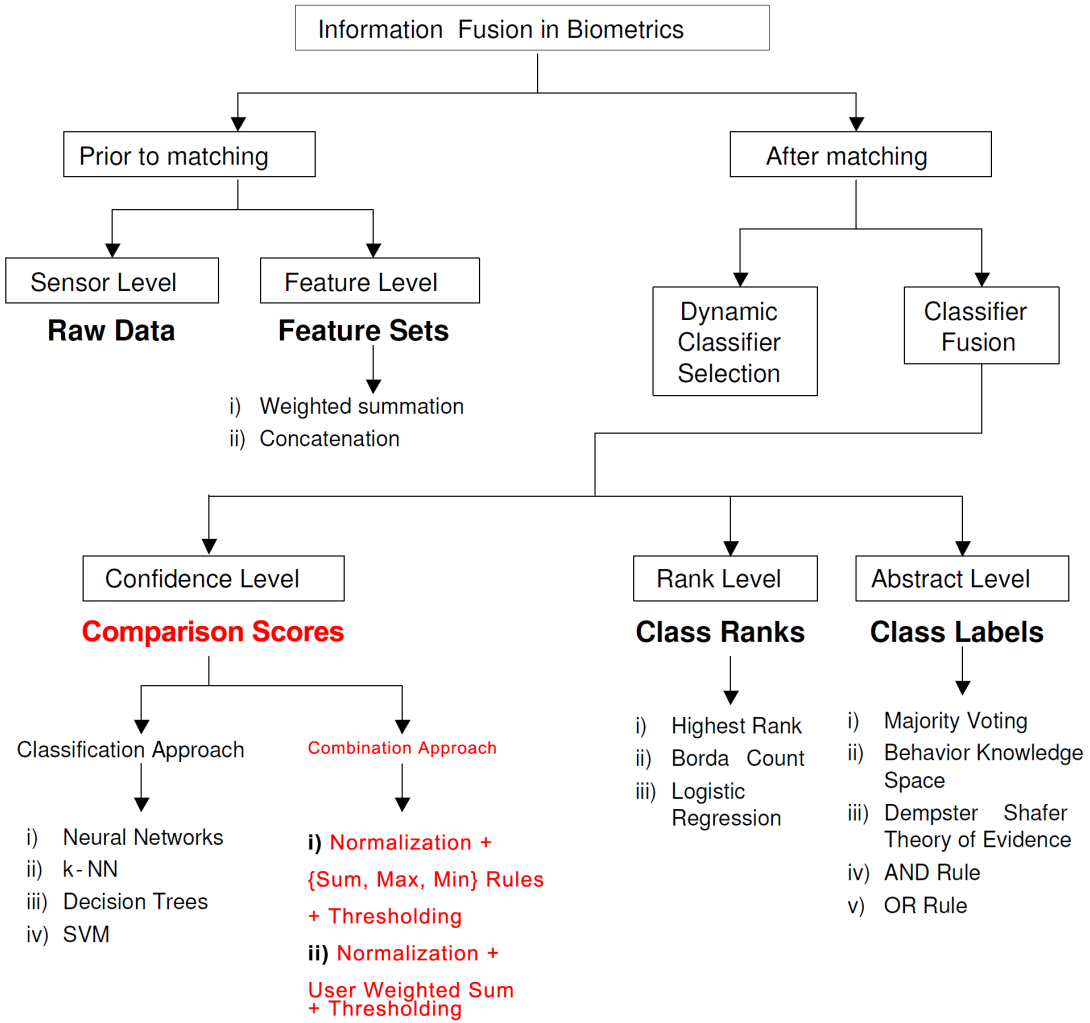



Figure 41: Summary of fusion levels and techniques in multi-modal biometrics.

## 4.6 Summary

Multibiometric systems are the new frontier and this is evident from th number of ongoing efforts in the research and commercial domains. They are an answer to the deficiencies of unimodal biometric systems, namely, the improvement of performance and the reduction of failure to enroll rates. Theoretically, they presents a huge potential, but research and commercial systems have yet to reflect this promise. The lack of standards also indicates that more work is required before it reaches an acceptable level of maturity.

Current operational multibiometric systems are designed to capture multiple traits and store the raw data separately and use it in a layered decision process, and this practise is unlikely to change in the near future. Multibiometric systems can use existing technology and improve the performance of large-scale databases, and these advantages will drive the development of multibiometric systems.

# 5 EXPERIMENTS

There are several approaches to study multimodal biometric fusion. One approach is to use heterogeneous database [100], i.e., combine biometric trait (e.g. fingerprint) from a database with biometric trait (e.g. iris) from another database. From the experiment point of view, these combined biometric traits belong to the same person. And the resultant person is called as *chimeric user* or *virtual user* (refer to section 5.5.1, page 71). Although this approach has been widely used in multimodal literature, it was questioned that whether this approach was reasonable during the 2003 Workshop on Multimodal User Authentication.

Poh et al. [101] studied this problem and showed that the performance measured with experiments carried out on chimeric users does not necessarily reflect the performance with real multimodal users. Obviously, the best way to study biometrics fusion is to use homologous multimodal biometric databases, which means the different biometric traits are truly come from the real same person. However, there are only a few multimodal biometric databases publicly available. And most of the existing multimodal databases are composed two modalities. BANCA [102] and XM2VTS [103] include *face* and *voice*; MYCT [104] includes fingerprint and signature.

Besides, there are also several databases including more than two modalities, such as BIOMET [105] which includes *face*, *voice*, *fingerprint*, *hand* and *signature*, and BioSec [106] including *fingerprint*, *face*, *iris* and *voice*. These existing databases have several limitations, e.g., lack of import traits or lack of diversity of sensors/traits. Therefore, for our experiments we have chosen two fingerprint and two iris databases described below.

## 5.1 Databases

Fingerprint and Iris experiments in this master thesis are made over four different databases (DB) collected from two different institutions.

1. Fingerprint databases and an iris database are collected by Machine Learning and Applications (MLA) Group at Shandong University in China (SDUMLA-HMT) [8].
2. Another iris database is collected by Institute of Automation, Chinese Academy of Sciences (CASIA-Iris-Lamp) [9].

### 5.1.1 SDUMLA-HMT Databases

The fingerprint (DB2 and DB3) and first iris database images used in this master project as we mentioned earlier are collected by Machine Learning and Applications (MLA) Group at Shandong University in China for what we appreciate their support during this project. We have been in contact with one of MLA member MSc. candidate Lili Liu all the time. MLA group called this database *"SDMLA- HMT: A Multimodal Biometric Database"*, the data was collected during the summer 2010, where 106 subjects in total: 61 males and 45 females with age between 17 and 31, participated in the data collecting process [8]. This database consists of face images captured from

7 different view angles, finger vein images of 6 fingers, gait videos from 6 view angles, iris images from an iris sensor and fingerprint images acquired with 5 different sensors [8]. In figure 42 are shown some of sample images from SDUMLA-HMT database. We have traced to this database by the help of Prof. Christoph Busch and PhD student Daniel Hartung.

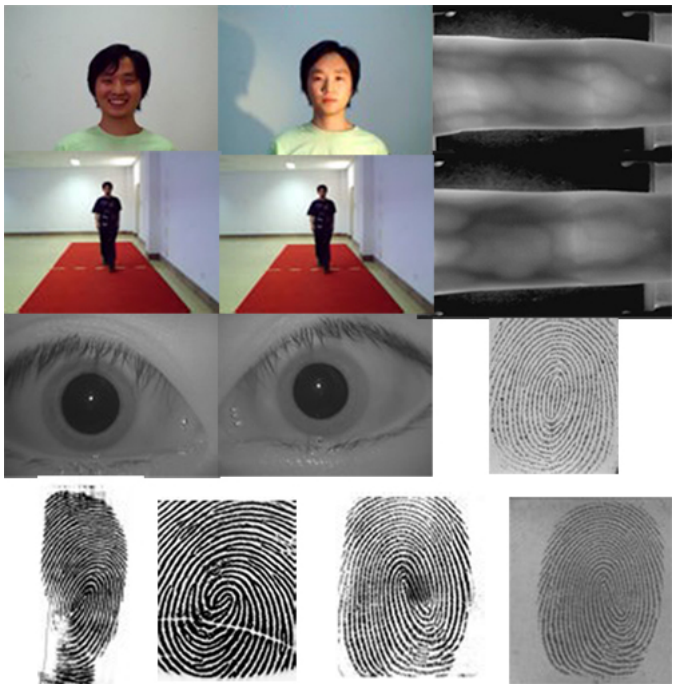


Figure 42: Some of the sample images of face, finger vein, gait, iris and fingerprint from SDUMLA-HMT Database [8].

Before we downloaded the SDUMLA-HMT database, we have filled and signed the ***SDUMLA-HMT Database Release Agreement*** and sent the scanned copy to Prof. Yilong Yin. The signed form and e-mail from Prof. Yilong Yin are attached in Appendix H, which proves that we have all rights, and due to ethical and legal aspects, we are able to perform experiments over SDUMLA-HMT database.

## 5.2 Fingerprint Recognition Experiment

### 5.2.1 Databases

The fingerprint images on SDUMLA-HMT database [8] are collected with five different sensors (multi-sensor database), such as:

**a) AES2501** swipe fingerprint scanner developed by Authentec Inc,

**b) FPR620** optical fingerprint scanner and

**c) FT-2BU** capacitive fingerprint scanner both developed by Zhongzheng Inc,

**d) URU4000** optical fingerprint scanner developed by Zhongkong Inc,

**e) ZY202-B** optical fingerprint scanner developed by Changchun Institute of Optics, Fine Mechanics and Physics, China Academy of Sciences

A visual view of these sensors is given in figure 43. MLA Group has selected these five sensors in

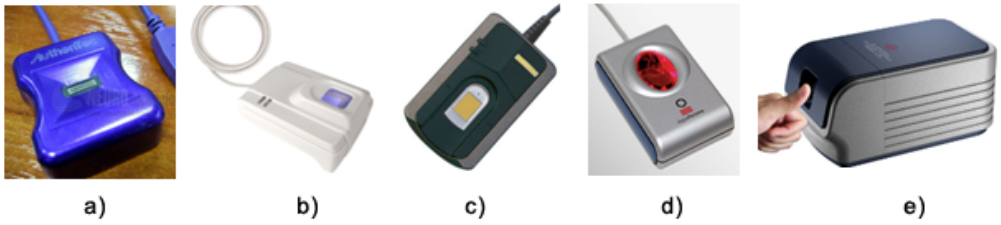



Figure 43: Five different fingerprint sensors from SDUMLA-HMT Fingerprint database.

order to do research on *"fingerprint sensor interoperability"* of fingerprint recognition, which is very popular topic recently. Fingerprint images in SDUMLA-HMT database are acquired from six fingers such as: *thumb finger, index finger* and *middle finger*, of both hands. It is worth mentioning that MLA Group has requested from participants eight impressions (attempts) for each of six fingers to five previous mentioned sensors. Some of fingerprint images are shown in figure 44. Fingerprint database (DB) consist of $6(\mathrm{fingers})\mathrm{x}5(\mathrm{sensors})\mathrm{x}8(\mathrm{attempts})\mathrm{x}106(\mathrm{subjects}) =$

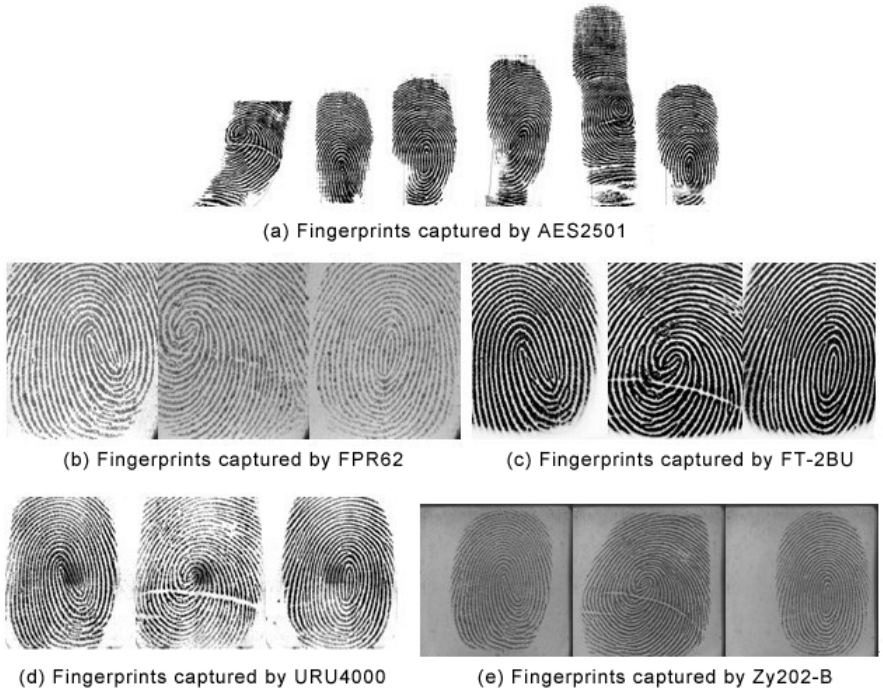



Figure 44: Fingerprint sample images from SDUMLA-HMT database [8].

25,440 fingerprint images, were all images are saved in 256 gray-scale *".bmp"* format and the size

Table 7: Fingerprint image size for five sensors [8].

| Sensor type | Image Size (in pixels) |
|---|---|
| **AES2501** swipe fingerprint scanner | varies (not fixed) |
| **FPR620** optical fingerprint scanner | 256x304 |
| **FT-2BU** capacitance fingerprint scanner | 152x200 |
| **URU4000** capacitance fingerprint scanner | 294x356 |
| **ZY202-B** capacitance fingerprint scanner | 400x400 |

of each images is different according to the sensor used. The size of fingerprint DB is about 2.2 Gigabytes. In table 7 are given the sizes of images from five different sensors.

### 5.2.2 Fingerprint Image Quality Assessment (NFIQ)

In this master project, in order to provide the answer to first research question (given in section 1.4), we have selected only two fingerprint databases. Our aim was to conduct experiments over the best and the worst fingerprint database to compare the biometric performances of these two databases. In order to check the quality of images, we have used an algorithm created by National Institute of Standards and Technology (NIST) called *NIST Fingerprint Image Quality version 1.0*" shortly ***NFIQ v.1.0*** [1].

NFIQ is a fingerprint image quality algorithm, developed by NIST in 2004. NFIQ is based on a machine learning algorithm, particularly *artificial neural networks*, which analyses a fingerprint image using a predictor of separation between match and nonmatch scores [107] [29]. NFIQ is trained using a large number of input vectors consisting of 11 - dimensional fingerprint features such as total number of minutiae, size of foreground, number of minutiae at different quality levels ranging between [0.5 - 0.9], and quality of different zones of a fingerprint image. NFIQ fingerprint feature extractor uses NIST Minutiae detector (mindtct) [107]. The output of NFIQ is an integer number, mapped to a score between 1 and 5, where 1 indicates the highest (best) quality of image, and 5 indicates the poorest (worst) quality of image. In 2010, NIST announced a call to enhance the *NFIQ v1.0* to *NFIQ v2.0*, hence our Prof. Busch and PhD student Martin Olsen are involved in developing the new version of NFIQ. The basic concept of NFIQ is illustrated in figure 45.

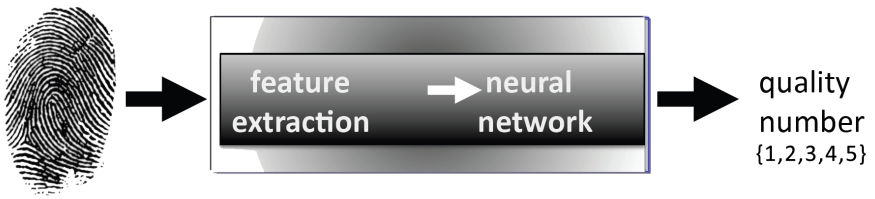



Figure 45: NIST Fingerprint Image Quality (NFIQ).

The answer to our first research question is that: high quality images (q=1) result in high

[1] More details about NFIQ: http://biometrics.nist.gov/cs_links/ibpc2010/workI/TabassiB_future_of_NFIQ.pdf

performance (low FMR and/or FNMR), while low quality images (q=5), result in low performance (high FMR and/or FNMR). NFIQ is based on a framework from ISO/IEC TR 29794-1:2009: Biometric Sample Quality [108].

### 5.2.3 Experiments on Fingerprint Image Quality Assessment

Our experiment of fingerprint recognition started by checking the quality of images from five different sensors, which is *the first challenge in experimental part*.

In order to run NFIQ we need two files from NIST: a library *cygwin1.dll* and *nfiq.exe* program. The NFIQ need to be executed from command line by following command:

```
<fingerprint_image> nfiq.exe -d
```

This command gives a quality score for certain image. The details for image quality checking will not be described in this section, but for more details about batch scripting or other programming part for bulk image quality assessment please feel free to contact the author of the thesis. After the quality of images is checked (see figure 46), we have calculated the mean and standard deviation for each database as given in table 8. This helped us to define which database has the best quality images and which one has the worst quality images.

| DB1 | | DB2 | | DB3 | | DB4 | | DB5 | |
|---|---|---|---|---|---|---|---|---|---|
| Filenames | Quality Scor | Filenames | Quality Scor | Filenames | Quality Scor | Filenames | Quality Scor | Filenames | Quality Scor |
| 1_001_1_1_p.jpg | 2 | 2_001_1_1_p.jpg | 3 | 3_001_1_1_p.jpg | 3 | 4_001_1_1_p.jpg | 3 | 5_001_1_1_p.jpg | 2 |
| 1_001_1_2_p.jpg | 2 | 2_001_1_2_p.jpg | 2 | 3_001_1_2_p.jpg | 3 | 4_001_1_2_p.jpg | 2 | 5_001_1_2_p.jpg | 2 |
| 1_001_1_3_p.jpg | 2 | 2_001_1_3_p.jpg | 2 | 3_001_1_3_p.jpg | 3 | 4_001_1_3_p.jpg | 2 | 5_001_1_3_p.jpg | 2 |
| 1_001_1_4_p.jpg | 2 | 2_001_1_4_p.jpg | 2 | 3_001_1_4_p.jpg | 3 | 4_001_1_4_p.jpg | 2 | 5_001_1_4_p.jpg | 2 |
| 1_001_1_5_p.jpg | 2 | 2_001_1_5_p.jpg | 2 | 3_001_1_5_p.jpg | 3 | 4_001_1_5_p.jpg | 2 | 5_001_1_5_p.jpg | 2 |
| 1_001_1_6_p.jpg | 2 | 2_001_1_6_p.jpg | 2 | 3_001_1_6_p.jpg | 3 | 4_001_1_6_p.jpg | 2 | 5_001_1_6_p.jpg | 2 |
| 1_001_2_1_p.jpg | 1 | 2_001_2_1_p.jpg | 2 | 3_001_2_1_p.jpg | 3 | 4_001_2_1_p.jpg | 2 | 5_001_2_1_p.jpg | 2 |
| 1_001_2_2_p.jpg | 1 | 2_001_2_2_p.jpg | 2 | 3_001_2_2_p.jpg | 3 | 4_001_2_2_p.jpg | 2 | 5_001_2_2_p.jpg | 2 |
| 1_001_2_3_p.jpg | 2 | 2_001_2_3_p.jpg | 2 | 3_001_2_3_p.jpg | 3 | 4_001_2_3_p.jpg | 2 | 5_001_2_3_p.jpg | 2 |
| 1_001_2_4_p.jpg | 2 | 2_001_2_4_p.jpg | 2 | 3_001_2_4_p.jpg | 2 | 4_001_2_4_p.jpg | 2 | 5_001_2_4_p.jpg | 3 |
| 1_001_2_5_p.jpg | 2 | 2_001_2_5_p.jpg | 2 | 3_001_2_5_p.jpg | 3 | 4_001_2_5_p.jpg | 2 | 5_001_2_5_p.jpg | 2 |
| 1_001_2_6_p.jpg | 2 | 2_001_2_6_p.jpg | 2 | 3_001_2_6_p.jpg | 3 | 4_001_2_6_p.jpg | 2 | 5_001_2_6_p.jpg | 2 |
| 1_001_3_1_p.jpg | 2 | 2_001_3_1_p.jpg | 2 | 3_001_3_1_p.jpg | 3 | 4_001_3_1_p.jpg | 2 | 5_001_3_1_p.jpg | 2 |
| 1_001_3_2_p.jpg | 2 | 2_001_3_2_p.jpg | 2 | 3_001_3_2_p.jpg | 3 | 4_001_3_2_p.jpg | 2 | 5_001_3_2_p.jpg | 2 |
| 1_001_3_3_p.jpg | 2 | 2_001_3_3_p.jpg | 2 | 3_001_3_3_p.jpg | 3 | 4_001_3_3_p.jpg | 2 | 5_001_3_3_p.jpg | 2 |
| 1_001_3_4_p.jpg | 2 | 2_001_3_4_p.jpg | 2 | 3_001_3_4_p.jpg | 3 | 4_001_3_4_p.jpg | 2 | 5_001_3_4_p.jpg | 2 |
| 1_001_3_5_p.jpg | 2 | 2_001_3_5_p.jpg | 2 | 3_001_3_5_p.jpg | 3 | 4_001_3_5_p.jpg | 2 | 5_001_3_5_p.jpg | 3 |
| 1_001_3_6_p.jpg | 2 | 2_001_3_6_p.jpg | 2 | 3_001_3_6_p.jpg | 3 | 4_001_3_6_p.jpg | 2 | 5_001_3_6_p.jpg | 2 |

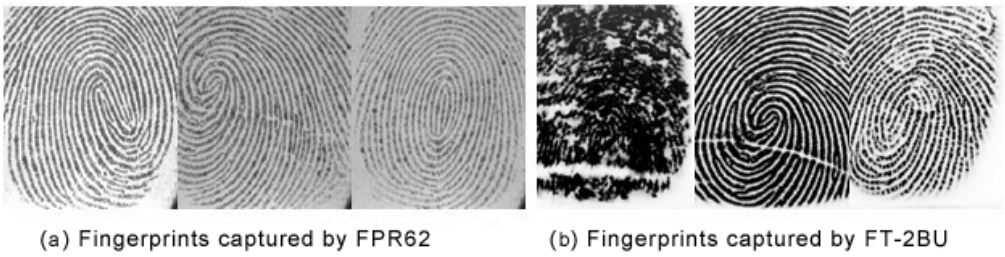
Figure 46: Some of quality scores of five fingerprint databases.

We have assign names of databases (DB1, ..., DB5) according to sensors, such as images from sensor AES2501 as DB1, FPR620 as DB2, FT-2BU as DB3, URU4000 as DB4, ZY202-B as DB5.

In Table 8 are given results for image quality assessment. As one can see from table 8, DB2 or images collected by optical sensor FPR620 has the best quality images with q = 1.3, and DB3 or images collected by capacitive sensor FT-2BU has bad quality images with q = 3.9 in our case the worst DB. Therefore, fingerprint experiments conducted in this thesis will only use DB2 and DB3, best and worst databases, respectively. In Figure 47 are given some image samples from these two databases.

Table 8: Image quality assessment (1 best, 2 good, 3 bad, 4 very bad and 5 worst quality).

| Database name | Mean (q) | Standard Deviation |
|---|---|---|
| DB1 [1] AES2501 | 2.3880 | 0.8858 |
| DB2 [2] FPR620 | 1.2813 | 0.8385 |
| DB3 [3] FT-2BU | 3.8729 | 0.9600 |
| DB4 [4] URU4000B | 2.1187 | 1.0094 |
| DB5 [5] ZY202-B | 1.9894 | 0.8881 |



(a) Fingerprints captured by FPR62 (b) Fingerprints captured by FT-2BU

Figure 47: Fingerprint image samples from a) DB2 (best db) and b) DB3 (worst db).

### 5.2.4 Experiment details

It is to be noted that we have reduced the number of participants, fingers and impressions as following: 2 fingers, in particular index fingers of both hands from 100 participants out of 106, and from 8 impressions we have used only first 5 impressions for finger in order to correlate fusion with 2 irides and 5 iris attempts (1000 iris images). After this modification we do have $2(\mathrm{fingers})\mathrm{x}100(\mathrm{subjects})\mathrm{x}5(\mathrm{attempts}) = 1000\ \mathrm{images}$ per database in total 2000 fingerprint images from two databases (DB2 and DB3) out of 25,440 fingerprint images. In our fingerprint experiment we have assigned *DB2* as ***FP_DB1*** (for best quality database) and *DB3* as ***FP_DB2*** (for worst quality database).

*The second challenge* in experimental part was filename convention or renaming the filenames from original to new names for our convenience and according to standards. At the beginning of our experiment Machine Learning and Applications (MLA) Group have not published finger position codes, and consequently we have requested help from them on finger position codes. Then they have updated the website based on our request.

Citation for finger position codes from MLA Group on their official website [2] is:

> *"The fingerprint images are named in the format of "fingeridx_n.bmp", where fingeridx = (1, 2, . . . , 6) is the finger index (i.e., 1 for left thumb, 2 for left index, 3 for left middle, 4 for right thumb, 5 for right index, and 6 for right middle), and n is the repeated impression index ranging from 1 to 8."*

As one can see from finger codes, MLA Group did not follow finger coding from ISO 19794-2 [11]. We have converted the existing finger codes according to ISO 19794-2 for two fingerprint databases, namely DB2 and DB3, given in table 9.

[2] Official website for SDUMLA-HMT Database: http://mla.sdu.edu.cn/sdumla-hmt.htm

Table 9: Finger position codes (names) according to ISO 19794-2 [11].

| Finger position (name) | Finger Code |
|---|---|
| Unknown finger | 0 |
| Right thumb | 1 |
| Right index finger | 2 |
| Right middle finger | 3 |
| Right ring finger | 4 |
| Right little finger | 5 |
| Left thumb | 6 |
| Left index finger | 7 |
| Left middle finger | 8 |
| Left ring finger | 9 |
| Left little finger | 10 |

An illustration of finger position codes (names) from MLA Group and ISO is given in figure 48, respectively. To rename all fingerprint images for our experiment, we have used a tool called *Bulk*

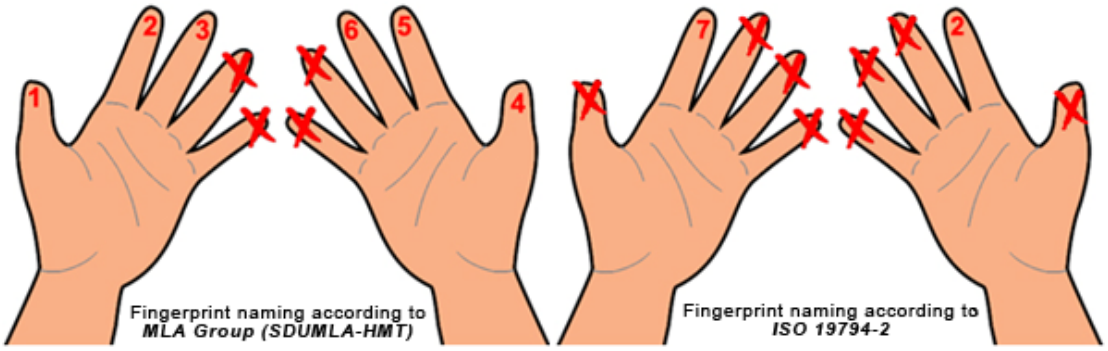



Figure 48: Illustration of finger position codes (names): to the right side MLA Group and to the left side ISO 19794-2.

*Rename Here"*, and a screen-shot from renaming phase of *subject_id=001* or first participant and his/her two fingers is given in figure 49. For more details about filenames and finger codes, please refer to Appendix A: Filename Convention.

## 5.3 Iris Recognition Experiment

### 5.3.1 Iris Databases

Iris experiments in this master thesis are conducted on two different databases (DB) collected from different institutions.

1. First iris database (named as Iris_DB1) is collected by Institute of Automation, Chinese Academy of Sciences (CASIA-Iris-Lamp) [9].
2. Second iris database (named as Iris_DB2) collected by Machine Learning and Applications

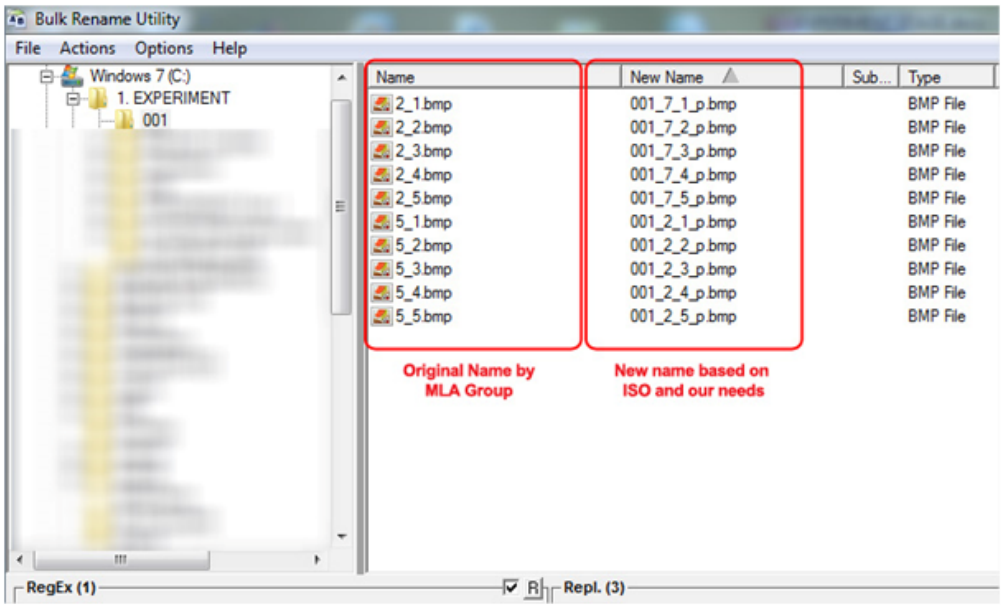



Figure 49: Filename Convention based on ISO 19794-2 finger position codes.

(MLA) Group at Shandong University in China (SDUMLA-HMT Iris) [8].

### 5.3.2 CASIA-Iris-Lamp Database

CASIA-IrisV4 iris database is collected by Institute of Automation, Chinese Academy of Science and consists six different sub-databases, in total of 54601 iris images from more than 1800 genuine users and 1000 virtual users [9]. Three sub-databases from CASIA-IrisV3 are:

1. CASIA-Iris-Interval,
2. CASIA-Iris-Lamp and
3. CASIA-Iris-Twins.

While three following sub-databases are new in CASIA-IrisV4:

1. CASIA-Iris-Distance,
2. CASIA-Iris-Thousand and
3. CASIA-Iris-Syn.

In our research work we have selected CASIA-Iris-Lamp database, details for this database are given below.

**CASIA-Iris-Lamp** is collected by capturing device OKI IRISPASS-h, which is handheld unit developed by OKI Group [9]. All images in CASIA-Iris-Lamp are collected under different illumination conditions which are the main challenge in iris recognition systems as we described in chapter 3, section *Iris Recognition*. Lamp was turned on/off to create more intra-class variations, elastic deformation of iris patterns due to pupil expansion and con-

traction [9]. This database is collected in indoor environment, and most of participants were graduate students of Automation Institute (CASIA). The total size of the database is about 390 Mega Bytes. In figure 50 are given some sample images of CASIA-Iris-Lamp, as well as a visual view of OKI device.

Figure 50: Some sample images from CASIA-Iris-Lamp database [9].

In table 10 are shown all necessary characteristics for CASIA-iris-Lamp. The filenames of CASIA-

Table 10: Characteristics of CASIA-Iris-Lamp database.

| Database (Sensor) | Session | Subjects | No. of classes | Images | Resolution (px) |
|---|---|---|---|---|---|
| CASIA-Iris-Lamp (OKI) | 1 | 411 | 819 | 16212 | 640x480 |

Iris-Lamp images are stored in *".jpg"* gray-scale level format, as [9]:

*root path/CASIA-Iris-Lamp/YYY/E/S2YYYENN.jpg*

where:
***S2***: stands for sub-database number 2 in CASIA-IrisV4, which is CASIA-Iris-Lamp
***YYY***: the unique identifier of the participant in the sub-database from 001 to 411
***E***: 'L' and 'R' stands for left and right eye, respectively.
***NN***: stands for number of attempts from 1 to 20.

### 5.3.3 Iris SDUMLA-HMT Database

All necessary details for SDUMLA-HMT fingerprint and iris databases are given in section 5.1.1, here we are going to give in particular SDUMLA-HMT iris database details.

SDUMLA-HMT Iris database is collected by an iris acquisition device which is developed by China University of Science and Technology using NIR (Near Infra-Red) illumination wavelength [8] as described in chapter 3, section *Iris Recognition*.

All participants in this experiment were required to take off their glasses and to keep the distance between device and their eye in range of 6 cm to 32 cm. MLA Group collected 10 iris

images for each subject, that means 5 images (attempts) per eye. The SDUMLA-HMT iris database consists of $2(irides)$x$5(irisimages)$x$106(participants) = 1060\ iris\ images$. These images are stored in *".bmp"* 256 grey-scale level format with size 768x576 pixels. The total size of the iris database is about 500 Mega Bytes. In figure 51 are given some iris images from this database. The

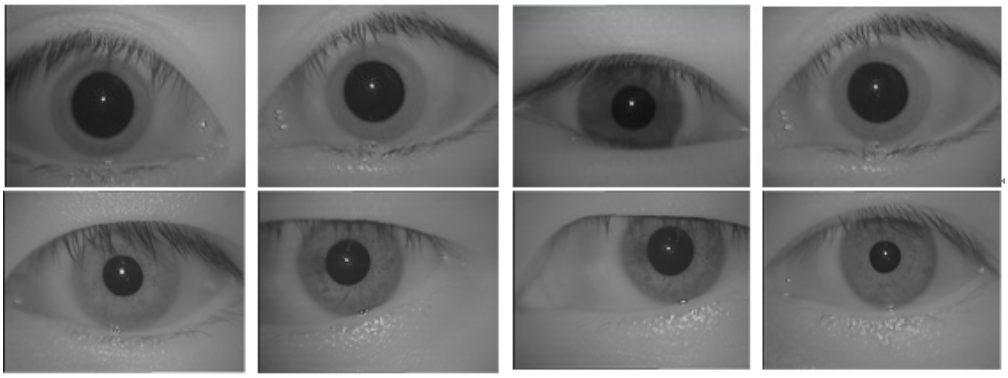


Figure 51: Some sample images from SDUMLA-HMT iris database [8].

filenames of SDUMLA-HMT iris images are stored as [8]:

*SDUMLA-HMT/Iris/YYY/E/YYY_E_NN.bmp*

where:
***YYY***: the unique identifier of the participant in the iris database from 001 to 106
***E***: 'L' and 'R' stands for left and right eye, respectively.
***NN***: stands for number of attempts from 1 to 5.

### 5.3.4 Experiment details

In our iris experiments we have reduce the number of participants (images) in order to perform fusion with fingerprint databases.

- From SDUMLA-HMT iris database we have chosen only 100 subjects out of 106 in total 1000 iris images: $2(irises)$x$5(irisimages)$x$100(subjects) = 1000\ iris\ images$
- From CASIA-Iris-Lamp we have used also only 100 subjects out of 411 and it is to be noted that we have reduced the number of attempts from 20 to 5, in order to comply with 1000 images in total: $2(irises)$x$5(irisimages)$x$100(subjects) = 1000\ iris\ images$

Quality of Iris images is checked by our C# console application which is developed in accordance with FDIS 19794-6, Information technology: Biometric data interchange formats – Part 6: Iris image data standard [12] and IREX (Iris Exchange) project established by NIST [109]. The Quality assessment is based on iris image properties shown in table 12. Refer to Appendix E for iris quality assessment function. While in table 11 are given image quality levels based on ISO standard [12].

In table 12 are given two examples of image quality assessment and properties for certain images from SDUMLA-HMT iris database (2_100_7_5_i.jpg) [3] and CASIA-Iris-Lamp iris database

[3] 2 in iris filenames stands for *right eye*, while 7 stands for *left eye*.

Table 11: Iris image quality levels [12].

| Image quality level | Image quality value |
|---|---|
| Poor | 0-25 |
| Low | 26-50 |
| Medium | 51-75 |
| High | 76-100 |

(1_035_7_1_i.jpg), these images are chosen randomly. For more details of filename convention refer to Appendix A.

Table 12: Iris image properties for SDUMLA-HMT iris.

| Property | Value |
|---|---|
| **Quality** | **33** |
| Iris Size | 81 |
| Pupil Iris Ratio | 155 |
| Usable Iris Area | 236 |
| Gray Level Spread | 77 |
| Iris Sclera Contrast | 18 |
| Iris Pupil Contrast | 51 |
| Iris Sclera Boundary | 216 |
| Iris Pupil Boundary | 190 |
| Sharpness | 254 |
| Signal to Noise Ratio | 254 |
| Interlance | 116 |
| Margin | 124 |

Table 13: Iris image properties for CASIA-Iris-Lamp.

| Property | Value |
|---|---|
| **Quality** | **72** |
| Iris Size | 78 |
| Pupil Iris Ratio | 133 |
| Usable Iris Area | 136 |
| Gray Level Spread | 88 |
| Iris Sclera Contrast | 18 |
| Iris Pupil Contrast | 65 |
| Iris Sclera Boundary | 213 |
| Iris Pupil Boundary | 98 |
| Sharpness | 267 |
| Signal to Noise Ratio | 121 |
| Interlance | 109 |
| Margin | 154 |

As one can see from table 12 the quality for SDUMLA-HMT given iris image is 33, and based on ISO iris data format belongs to low quality images (table 11). Whereas as can be seen from table 13 the quality for CASIA-Iris-Lamp given iris image is 72, and based on ISO iris data format belongs to medium to high quality images (table 11).

Quality of images from SDUMLA-HMT iris database is $\mathrm{Quality}_{average} = 47.2$ (LOW quality), while quality of images from CASIA-Iris-Lamp is $\mathrm{Quality}_{average} = 70.7$ (MEDIUM quality), illustrated in figure 52.

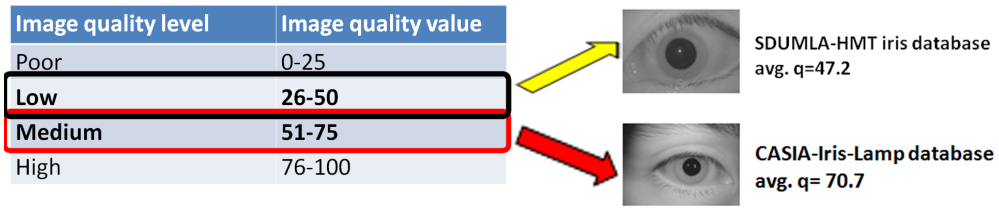



Figure 52: Quality of iris images in average.

### 5.3.5 Iris Segmentation

As we have discussed in chapter 3, the iris segmentation is key and the most critical step in iris recognition process. After quality assessment process we have discovered that iris images from SDUMLA-HMT database have very low contrast between *sclera* and *iris* and due to the low quality of images Neurotechnology comparator (VeriEye SDK) failed to segment the iris correctly (comparison score=8.9110), this is shown in figure 53. Segmentation of iris images by

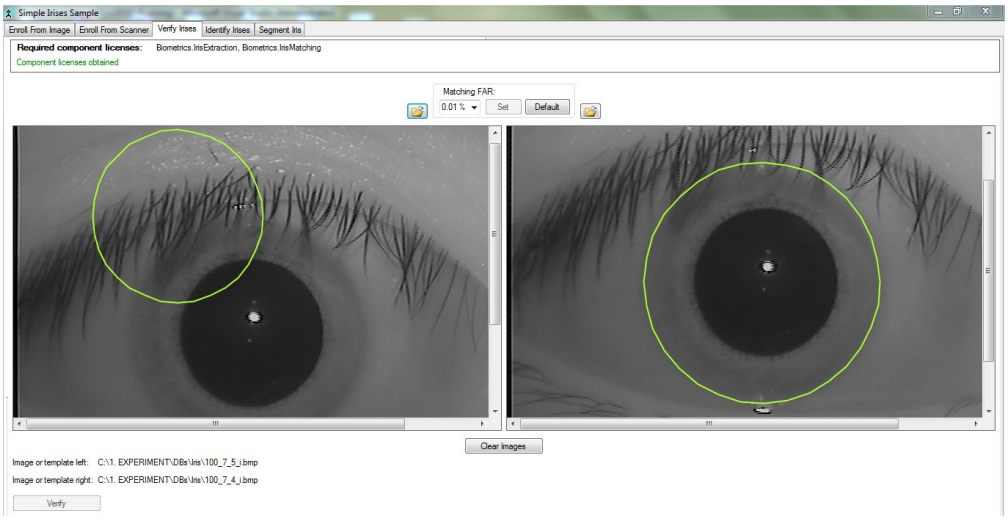



Figure 53: Iris image without segmentation. VeriEye has incorrectly segmented the iris (same iris comparison score=1.1120).

Neurotechnology VeriEye comply with ISO/IEC 19794-6 Iris Image Data [12] and NIST IREX-I (Iris Exchange and Interoperability: test reports 2009, 2010). This segmentation format is called **IREX FORMAT B**: *Cropped and masked image* [109], and is illustrated in figure 54.

After we have performed the segmentation over all iris images the VeryEye SDK has correctly segmented the iris. In figure 55 is shown a screen shot of correctly segmented iris after segmentation for the same image displayed in figure 53, we have received comparison score=327 for the same iris image. In our iris experiments all images are segmented by **IREX FORMAT B**: *Cropped and masked image* approach.

## 5.4 Fingerprint and Iris Comparisons

In this master project, for fingerprint and iris comparisons we have used a commercial comparator Software Development Kit (SDK) from Neurotechnology called MegaMatcher 4.3 SDK [110]. For fingerprint comparisons VeriFinger 6.5 Extended SDK is used [111], whereas for iris comparisons VeriEye 6.5 Extended SDK is used [112].

Mohammad Derawi, has concluded that Neurotechnology achieved best results for all types of fingerprint comparisons [30]. As well as, it is recognized by NIST as MINEX (The Minutiae Interoperability Exchange Test) compliant algorithm. Furthermore, in the Fingerprint Verification Competition 2006 (FVC2006), Neurotechnology VeriFinger algorithm (known as P058) has

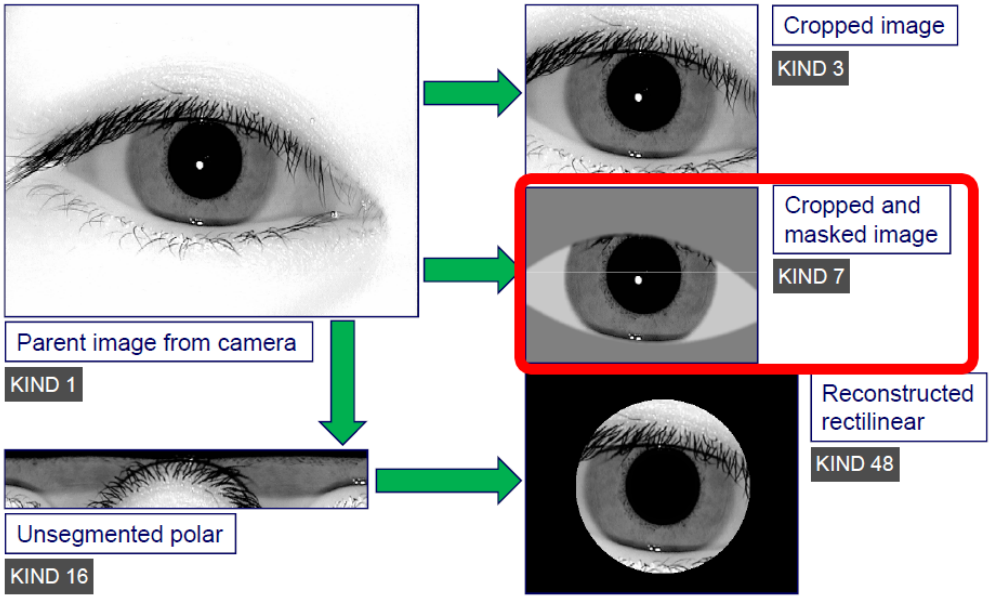



Figure 54: IREX Format B segmentation: Cropped and masked image (KIND 7). *"The KIND 7 record requires detection of the iris-eyelid and iris-sclera boundaries and a pixel-replacement masking operation"* [109].

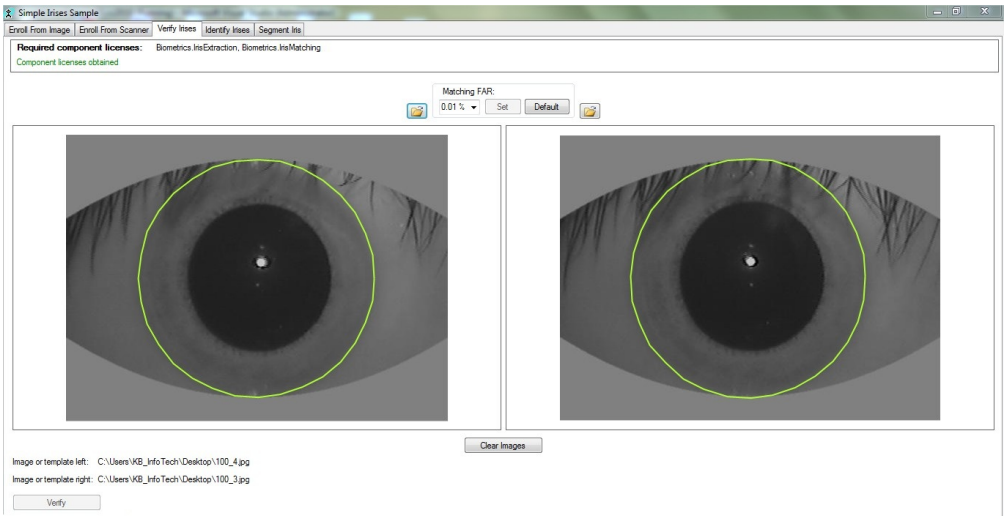
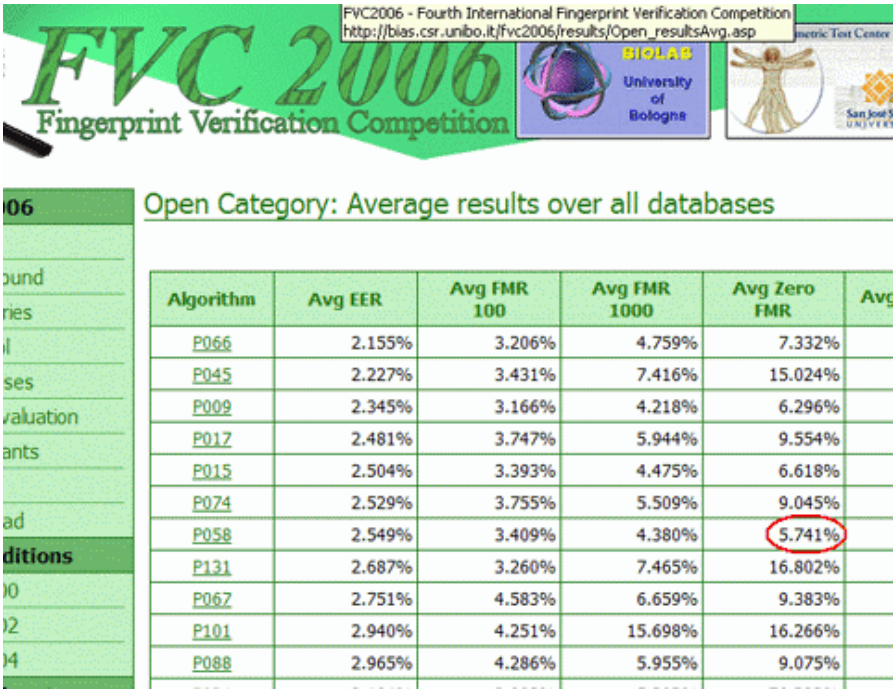



Figure 55: Iris image with segmentation. VeriEye has correctly segmented the iris (same iris comparison score=327).

achieved the lowest so called *"Average Zero FMR"* in Open Category results [4] [5], given in figure 56. These are one of the facts why we have chosen Neurotechnology as comparator as well as with licensing rights that we have as Gjøvik University College (Biometric Laboratory).

[4] Official website of FVC2006 Open Category results: http://bias.csr.unibo.it/fvc2006/results/Open_resultsAvg.asp
[5] Neurotechnology awards: http://www.neurotechnology.com/awards.html




| Algorithm | Avg EER | Avg FMR 100 | Avg FMR 1000 | Avg Zero FMR | Avg |
|---|---|---|---|---|---|
| P066 | 2.155% | 3.206% | 4.759% | 7.332% | |
| P045 | 2.227% | 3.431% | 7.416% | 15.024% | |
| P009 | 2.345% | 3.166% | 4.218% | 6.296% | |
| P017 | 2.481% | 3.747% | 5.944% | 9.554% | |
| P015 | 2.504% | 3.393% | 4.475% | 6.618% | |
| P074 | 2.529% | 3.755% | 5.509% | 9.045% | |
| P058 | 2.549% | 3.409% | 4.380% | 5.741% | |
| P131 | 2.687% | 3.260% | 7.465% | 16.802% | |
| P067 | 2.751% | 4.583% | 6.659% | 9.383% | |
| P101 | 2.940% | 4.251% | 15.698% | 16.266% | |
| P088 | 2.965% | 4.286% | 5.955% | 9.075% | |

Figure 56: Neurotechnology algorithm results in FVC2006.

Neurotechnology VeriEye iris recognition algorithm is judged on the IREX-III report to be one of the fastest and most accurate algorithm among the others. IREX-III Evaluation and Interoperability test report is published on April 5$^{th}$, 2012 by the The National Institute of Standards and Technology (NIST) [6]. In this report the VeriEye algorithm is denoted as N02A, N03A and N02B at low, medium and high speed, respectively.

Neurotechnology comparator (VeriFinger and VeriEye) does not support bulk comparisons, therefore, we have developed a C#.NET console application to compare all fingerprint and iris images (bulk comparison). In this application we have used all libraries from Neurotechnology that are necessary to compare fingerprint and iris images. For more details about fingerprint and iris comparison process, refer to chapter 7 *Data Analysis*, as well as for C# console application, refer to Apppendix E: Source code of our console application for bulk comparison in C#.NET.

## 5.5 Fusion Experiments

Fusion is performed over four previously mentioned databases. Based on quality assessment results that we have conducted over databases, the best databases are named with suffix 1, while the worst databases are named with suffix 2 such as:

- **Fingerprint Databases:**
  - Fingerprint best quality database SDUMLA-HMT DB2 is named as FP_DB1,

[6] IREX-III site: http://www.nist.gov/itl/iad/ig/irexiii.cfm

  - Fingerprint worst quality database SDUMLA-HMT DB3 is named as FP_DB2.
- **Iris Databases:**
  - Iris best quality database CASIA-Iris-Lamp is named as Iris_DB1,
  - Iris worst quality database SDUMLA-HMT iris database is named as Iris_DB2.

We have defined four fusion scenarios, fusion with the best and the worst databases as following:

1. Fusion of *FP_DB1* and *Iris_DB1*
2. Fusion of *FP_DB1* and *Iris_DB2*
3. Fusion of *FP_DB2* and *Iris_DB1*
4. Fusion of *FP_DB2* and *Iris_DB2*

As we have mentioned earlier, fusion in this thesis is performed at score level. First we have normalized all scores by three normalization techniques such as *MinMax, Z-Score* and *Tangent Hyperbolic*. After normalization, fusion stage is performed by four most used fusion techniques such as *Minimum score, Maximum Score, Simple sum* and *User weighted sum*. All details about fusion process are given in chapter 7, respectively in section 7.5 (*Normalization and Fusion*), and performance results are shown in chapter 8, respectively in section 8.6 (*Fingerprint and Iris Fusion Results*).

### 5.5.1 Real vs. Virtual Users

For fusion scenarios 1 and 3 we have used heterogeneous databases for fingerprint and iris, thus we have created so called *"virtual users"*, while for fusion scenarios 2 and 4 we have used modalities (fingerprint and iris) from homogeneous databases or *"real users"* [113], methodology of real and virtual users is illustrated i figure 57. A *"real user"* denoted as **A** subject has provided both required modalities to the database, iris and fingerprint, this case is for SDUMLA-HMT database (same subjects for both iris and fingerprint). While a participant B, donated only one biometric modalities, either iris data **($B_I$)** or fingerprint data **($B_F$)**, therefore these modalities are combined from different users in order to create another user [113]. In this case we have combined iris modality from CASIA-Iris-Lamp and fingerprint modality from SDUMLA-HMT fingerprint database, and thus we have created so called a *"virtual user"*.

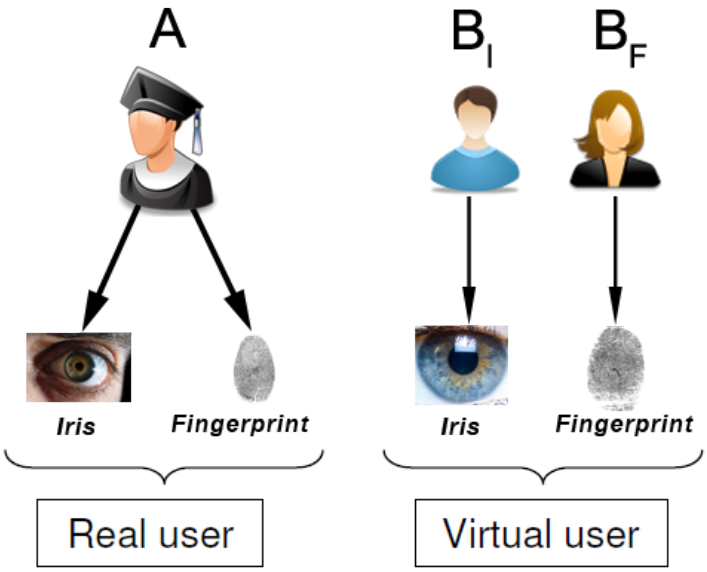



Figure 57: Methodology of real and virtual users.

## 5.6 Summary

This chapter introduced the experiments performed for fingerprint and iris databases. Two fingerprint databases and two iris databases are chosen and used in this work. The fingerprint databases and an iris database are collected by The Group of Machine Learning and Applications, Shandong University (SDUMLA) in China. The other iris database (CASIA-Iris-Lamp) was conducted by Institution of Automation, China Academy of Science (CASIA). As these biometric samples from both databases (fingerprint and iris) are in its digital form, in chapter 7 *Data Analysis* we will start to perform signal processing techniques for analyzing the data to be used for comparison of the individuals. This involves processing the data to remove noise or unnecessary background and extracting features. In table 14 is given summary of details for used fingerprint and iris databases.

Table 14: Details of used fingerprint and iris databases.

| Database (Sensor) | Images | Users | No. of Finger/Iris | Attempts | Image Size (in px) |
|---|---|---|---|---|---|
| FP_DB1 (FPR620) | 1000 | 100 | 2 | 5 | 256x304 |
| FP_DB2 (FT-2BU) | 1000 | 100 | 2 | 5 | 152x200 |
| Iris_DB1 (OKI) | 1000 | 100 | 2 | 5 | 640x480 |
| Iris_DB2 (N/A) | 1000 | 100 | 2 | 5 | 768x576 |

All unimodal and multimodal experiments have been implemented in Microsoft Visual C#.NET environment, running on PC Intel Pentium 4 2.10 GHz Dual-Core CPU, with 4 GB RAM memory and Windows 7 64-bit Operating System.

# 6 Performance Evaluation of Biometric Systems

No biometric system is perfect - there are varying levels of how well a biometric system performs its task of recognizing users. Evaluating biometric systems requires analyzing a number of different variables such as mismatch error rates, throughput rates, reliability, consistency, cost, and target population. In order to assess the performance of the biometric system there is a need for some metrics which can describe how the system behaves under several conditions. Before starting the description of biometrics performance metrics, first we need some main definitions of comparison scores adopted from ISO:

- **comparison score c(Q,R)**[1]**:** numerical value (or set of values) resulting from a comparison
- **similarity score s(Q,R):** is comparison score that increases with similarity of compared samples
- **distance score / dissimilarity score d(Q,R):** is comparison score that decreases with similarity of compared samples

where: **Q** - stands for *query*, *probe* or *sample*.
**R** - stands for *reference* or *template*.

Two other important concepts in order to calculate the error rates correctly, as well as differentiating system errors from algorithm errors are those of *genuine attempt* and *impostor attempts*. In a genuine attempt a user tries to compare his or her sample against his or her own enrollment template. While in an impostor attempt a user tries to compare his or her sample against another user's enrollment template. The similarity score generated from genuine transactions are called *genuine comparison scores* and similarity score generated from impostor transactions are called *impostor comparison scores*.

## 6.1 Biometric Failures

There are multiple failure associated with a acquisition of a biometric sample or with its processing. In Sections 6.1.3 to 6.1.4 we will discuss the failures that are associated with the deficiency of a biometric system to create a biometric reference for a data subject and subsequently in Section 6.3 will consider errors that are attributed to biometric verification systems.

### 6.1.1 Failure to Capture Rate

Failure to Capture Rate (FTC) is constituted, when the capture process could not generate a biometric sample of sufficient quality. This can be caused due to one of the following reasons:

1. The sample is not generated, as the characteristic is not placed properly on the capture device (e.g finger not covering the sensor area)
2. The captured signal is rejected by the automatic sample quality control algorithm.

[1]NOTE: the term *"matching score"* is deprecated by ISO for *"comparison"*

3. The captured signal is stored as file, but rejected by the operator (staff expert) subsequent to visual inspection as it is not of sufficient quality

The ISO-definition [114] for the FTC is given by:

**Failure-to-Capture Rate:** *proportion of failures of the biometric capture process to produce a captured biometric sample that is acceptable for use.*

The expression to calculate the FTC is as follows:

$$FTC = \frac{N_{tca} + N_{nsq}}{N_{tot}} \tag{6.1}$$

where $N_{tca}$ is the number of terminated capture attempts, $N_{nsq}$ is the number of images created with insufficient sample quality and $N_{tot}$ is the total number of capture attempts. In consequence of a Failure-to-Capture are new capture attempt is initiated.

### 6.1.2 Failure to eXtract

Failure to eXtract (FTX) is constituted, when the feature extraction process was not able to generate a biometric template. This can be caused due to one of the following reasons:

1. The algorithm itself declares that it cannot create a template from the input sample. This could be caused by a insufficient number of features that were identified e.g. only five minutia could be extracted from a fingerprint image.
2. Processing time of feature extraction algorithm exceeds the specified limit and thus the feature extraction is terminated.
3. The feature extraction algorithm might suddenly crash during processing. In this case, some actions will be undertaken (e.g. start over application, repeat process, etc.) but if the crash happens all the time with the same sample then for this image a failure to extract feature will be constituted. There is currently no ISO-definition for the Failure-to-eXtract Rate.

The expression to calculate the FTX is as follows:

$$FTX = \frac{N_{ngt}}{N_{sub}} \tag{6.2}$$

where $N_{ngt}$ is the number of cases, where no template was generated and $N_{sub}$ is the total number of biometric samples being submitted to the feature extraction component (i.e. the template generator). In an operational scenario the consequence of a Failure-to- eXtract is a new attempt including a new biometric sample creation and it subsequent processing.

### 6.1.3 Failure to Enrol

A Failure-to-Enrol (FTE) is constituted, when the biometric system is not capable to create for data subject a biometric reference. Thus the Failure-to-Enrol Rate (FTE) expresses the proportion of the population, for which the system fails to complete the enrolment process. This can be caused due to one of the following reasons:

1. The biometric characteristic of the subject (e.g. its fingerprint images) can not be captured at all.

2. For each evaluation setting, and if required instances of the same characteristic (e.g. left index finger instead right index finger) it is not possible to create for this subject a template of sufficient quality (e.g. a feature set with minimum number of minutia).

There are currently two ISO-definitions for the FTE. The original definition in the performance testing standard [115] and the more recent one from the harmonized biometric vocabulary [114]:

**Failure-to-Enrol Rate (ISO 19795-1):** *proportion of the population for whom the system fails to complete the enrolment process.*

**Failure-to-Enrol Rate (ISO SC37 SD2):** *proportion of biometric enrolment (that did not fail for non-biometric reasons), that resulted in a failure to create and store an enrolment data record for an eligible biometric capture subject, in accordance with an enrolment policy.*

The expression to calculate the FTE is as follows:

$$\mathrm{FTE} = \frac{\mathrm{N}_{\mathrm{nec}}}{\mathrm{N}} \tag{6.3}$$

where $\mathrm{N}_{\mathrm{nec}}$ is the number of cases, where we meet one of the two Failure-to-Enrol criteria and N is the total number of subjects, intended to be enrolled in the biometric application. The consequence of a Failure-to-Enrol In an operational scenario is that for the capture subject a fall-back procedure must be activated that should treat the individual in a non-discriminatory manner. In figure 58 are illustrated these three basic metrics of biometric process pipeline.

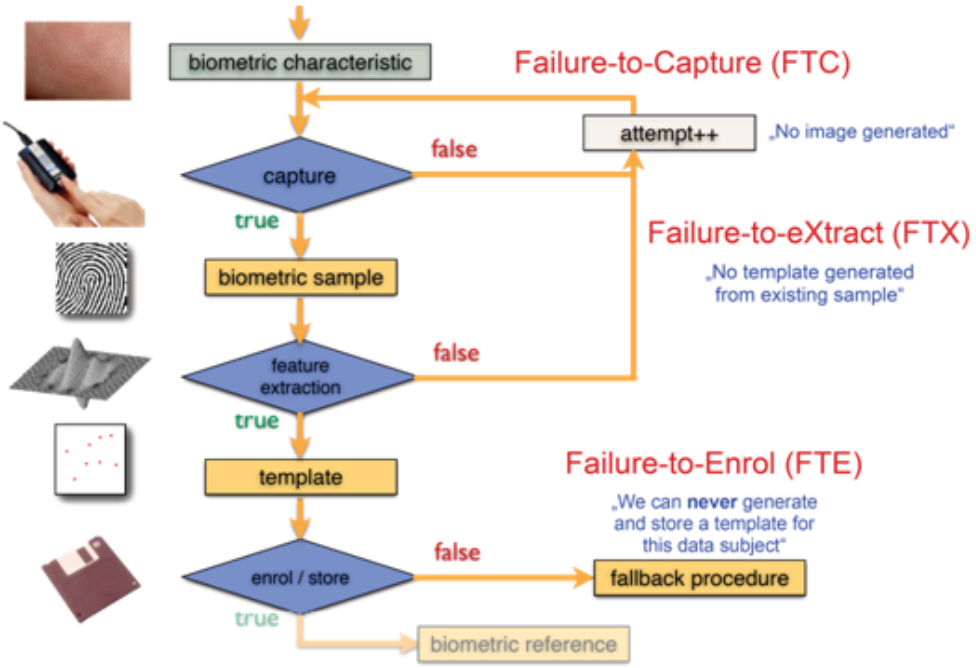



Figure 58: Potential failures in a biometric processing pipeline.

### 6.1.4 Failure to Acquire Rate

Failure to Acquire Rate (FTA) is essential for the verification process and estimates the likelihood that biometric comparison can not be completed due to potential deficiencies in the live sample that is submitted as a probe. If there is no feature vector that can be compared to a biometric reference this can be caused due to one of the following reasons:

1. The is no biometric sample generated, which is expressed by the FTC.
2. The feature extraction component failed to extract features as the number and/or quality of extracted features is not sufficient. This is expressed by the FTX.

There are currently two ISO-definitions for the FTA. The original definition in the performance testing standard [115] and the more recent one from the harmonized biometric vocabulary [114]:

**Failure-to-Acquire Rate (ISO 19795-1):** *proportion of verification or identification attempts for which the system fails to capture or locate an image or signal of sufficient quality.*

**Failure-to-Acquire Rate (ISO SC37 SD2):** *proportion of a specified set of probe acquisitions that failed to create a biometric probe.*

**Note** that in ISO SC37 SD2 a *probe* is defined as *biometric data input to an algorithm for comparison to a biometric reference(s)*. The expression to calculate the FTA is as follows:

$$FTA = FTC + FTX * (1 - FTC) \tag{6.4}$$

## 6.2 Algorithm Error Rates

Algorithm error rates are considered: *false match rate* and *false non-match rate*, which are described below.

### 6.2.1 False Match Rate (FMR)

For imposter comparisons a False-Match constitutes the undesired case that an imposter probe is matching a biometric reference, which has not been created for himself. There are currently two ISO-definitions for the corresponding False-Match-Rate (FMR). The original definition in the performance testing standard [115] and the more recent one from the harmonized biometric vocabulary [114]:

**False-Match-Rate (ISO 19795-1):** *proportion of zero-effort impostor attempt samples falsely declared to match the compared non-self template.*

**False-Match-Rate (ISO SC37 SD2):** *proportion of the completed biometric non-match comparison trials that result in a false match.*

$$FMR(t) = \int_{t}^{1} p(s|H_0)dt \tag{6.5}$$

Together with the False-Non-Match-Rate (FNMR) the FMR is the key metric to be used in biometric technology testing and is understood to characterize a security property of a biometric system [2].

[2]Note that some literature is using the term False-Accept-Rate in the meaning of FMR

### 6.2.2 False Non-Match Rate (FNMR)

For genuine comparisons a False-Non-Match constitutes the undesired case that an genuine probe is not matching to biometric reference, which has been created for the same subject from the same source (e.g. same index finger). There are currently two ISO-definitions for the corresponding False-Non-Match-Rate (FNMR). The original definition in the performance testing standard [115] and the more recent one from the harmonized biometric vocabulary [114]:

**False-Non-Match-Rate (ISO 19795-1):** *proportion of genuine attempt samples falsely declared not to match the template of the same characteristic from the same data subject supplying the sample.*

**False-Non-Match-Rate (ISO SC37 SD2):** *proportion of the completed biometric match comparison trials that result in a false non-match.*

$$\mathrm{FNMR}(t) = \int_0^t p(s|H_1)\,dt \tag{6.6}$$

Together with the False-Match-Rate (FMR) the FNMR is the key metric to be used in biometric technology testing and is understood to characterize a security property of a biometric system [3]. Graphical illustration of these key metrics for biometric systems is given in figure 59. The

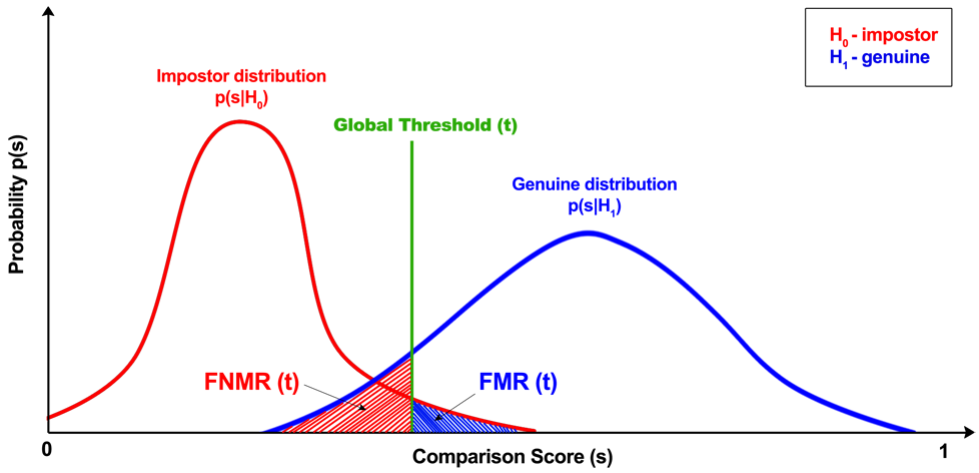



Figure 59: Biometric system comparison score distributions.

simplify equations for calculating the FMR and FNMR values are given in Equations 6.7 and 6.8, respectively.

$$\mathrm{FMR} = \frac{\text{Number of impostor comparisons}}{\text{Total number of impostor comparisons}} \tag{6.7}$$

**False Match Rate (FMR)** *is calculated as the proportion of samples from impostor attempts that cannot be matched against the enrolled templates of genuine users* [29].

[3] Note that some literature is using the term False-Reject-Rate in the meaning of FNMR

$$\text{FNMR} = \frac{\text{Number of rejected genuine comparisons}}{\text{Total number of genuine comparisons}} \tag{6.8}$$

**False Non-Match Rate (FNMR)** *is calculated as the proportion of samples from genuine attempts that are successfully matched against the enrolled templates of genuine users* [29].

### 6.2.3 Equal Error Rate (EER)

EER is calculated as the point where the FMR(t) and FNMR(t) are equal: *FMR(t)=FNMR(t)*, illustrated in figure 60. This rate is also called the crossover error rate. A lower EER indicates a better overall biometric system performance. To obtain the ERR from the Detection Error Trade-off curve, simply we need to draw a line that forms an angle of 45 degree from the origin of coordinate system (x, y) = (0, 0). The EER rate line is illustrated below in figure 61.

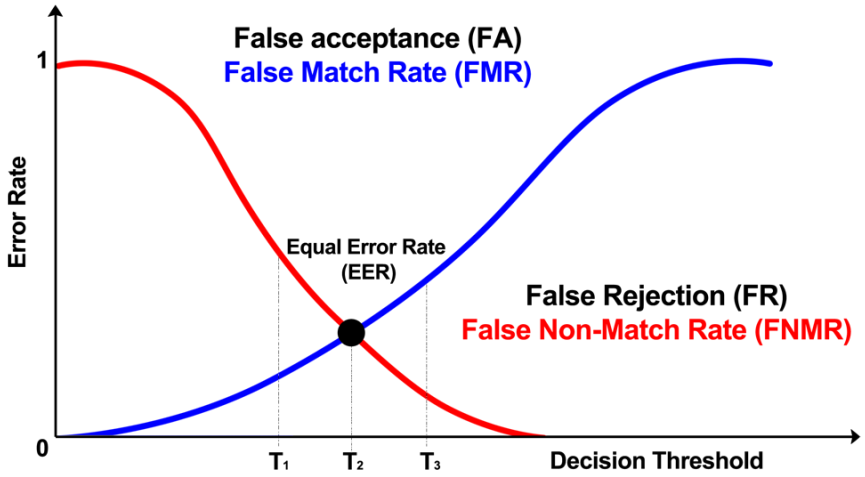



Figure 60: An example of EER point.

## 6.3 Performance Metrics for Verification System

The first order estimation of the performance for a verification system that is based on transactions allowing multiple attempts can be derived from the detection error trade- out curve. However if this is applied the potential correlations between the attempts are neglected. Such correlations could be due to habituation of the capture subject with the human- computer interface of the biometric system. The relevant measures for a verification system are the False-Accept-Rate (FAR) and the False-Reject-Rate (FRR). The ISO-definition [115] for both metrics are the following:

**False-Accept-Rate (ISO 19795-1):** *proportion of verification transactions with wrongful claims of identity that are incorrectly confirmed.*

**False-Reject-Rate (ISO 19795-1):** *proportion of verification transactions with truthful claims of identity that are incorrectly denied.*

For the simplified case that the verification system does allow only a single attempt per transaction then the FAR and FRR can be estimated as follows:

$$FAR = FMR * (1 - FTA) \tag{6.9}$$

and

$$FRR = FTA + FNMR * (1 - FTA) \tag{6.10}$$

If the biometric application is likely to be confronted with a large number of failure to enrol cases (e.g. as it is a fingerprint system for mine workers) and the biometric performance shall be predicted based on a gallery that was collected for a technology testing then the equations 6.9 and 6.10 do not sufficiently express the performance to be expected. The reason for this is that in a technology evaluation biometric references are generated from the gallery that do not cause a failure-to-enrol and probes that do not cause a failure-to-acquire. For such a case the generalized versions of the above equations are more appropriate, which are given by:

$$GFAR = FMR * (1 - FTA) * (1 - FTE) \tag{6.11}$$

and

$$GFRR = FTE + (1 - FTE) * FTA + (1 - FTE) * (1 - FTA) * FNMR \tag{6.12}$$

## 6.4 DET and ROC curves

Detection Error Trade-off (DET) curve is a modified Receiver Operating Characteristic (ROC) curve which plots FMR (in the x-axis) against FNMR (in the y-axis). Whereas ROC curve plots FMR (in the x-axis) and 1-FNMR (in the y-axis). DET curve is usually used to measure the performance of biometric system and provides a more direct view of the error-vs-error trade-off [1].

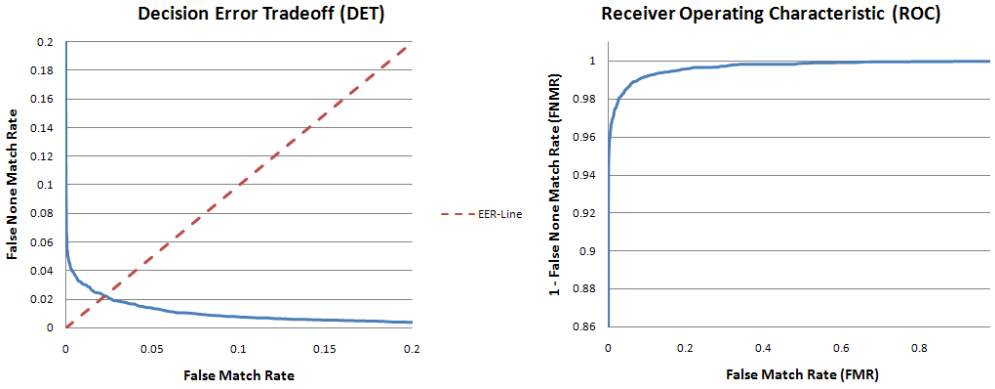



Figure 61: An example of Decision Error Trade-off (DET) and Receiver Operating Characteristic (ROC) curves [30].

## 6.5 Security versus Convenience

A biometric system is developed to increase *security* and *convenience*. For a biometric system security is the ability of the system to detect impostor attempts reliably and accurately, meanwhile convenience is the ability of the system to detect genuine attempts reliably and accurately [29].

For instance, in forensic applications the FNMR is more important than FMR (a very low FNMR is required), given that we do not want to miss a criminal. On the other hand, in access control environments where the high security is required most important factor is FMR than FNMR (here very low FMR is required), thus we don not want to let in any impostor, such environments are: border control, nuclear power plant, accessing restricted zones by the public etc.

It is extremely important to understand the difference between FMR (FAR) and FNMR (FRR) error rates, as these two factors are inversely related, lowering one of them often results in increasing the other, so it's common to describe the performance by another error rate that we have described previously EER.

***Example:*** *a very low FMR will cause inconvenience to genuine users, because this leads to high FNMR.* Biometric systems in commercial application such as banks (ATMs) where FMR and FNMR are very important factors. In figure 62 are illustrated a) applications of biometric systems and b)security vs. convenience.

***Example:***
*Border control, Nuclear power plant (high security):*

$$\mathrm{FNMR} > \mathrm{FMR}(\mathrm{FMR} \cong 0) \quad | \quad \textbf{Security = 1 - FMR} \tag{6.13}$$

*Season ticket control (low security):*

$$\mathrm{FMR} > \mathrm{FNMR} \quad | \quad \textbf{Convenience = 1 - FNMR} \tag{6.14}$$

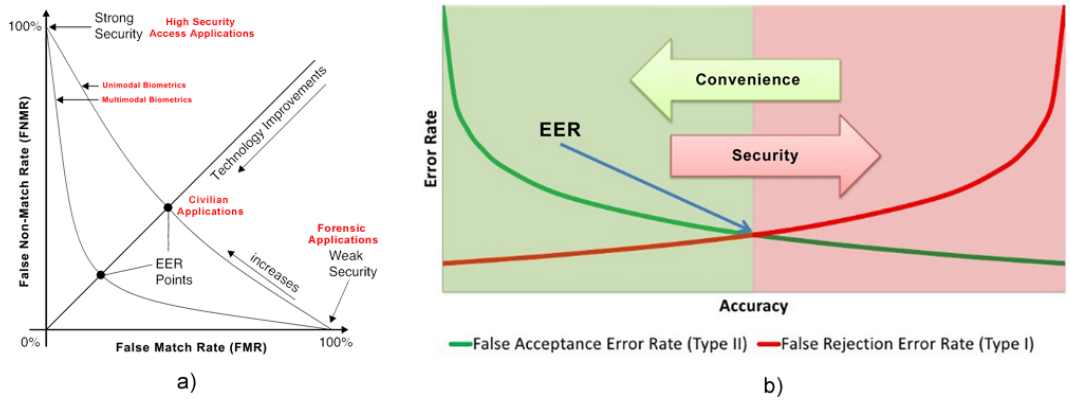



Figure 62: Security vs. Convenience a) Unimodal and multimodal biometrics in different applications. b) Illustration of Security vs. Convenience.

## 6.6 Summary

This chapter introduces various topics related to the performance evaluation of biometric systems including fundamental system errors and error rates, transactional error rates, graphical techniques for analyzing these error rates, and system evaluation methodologies. Performance evaluations are critical for successful deployments, it gives decision-makers information at their disposal to make educated decisions about procurement, system administrators can fine-tune performance based on specific application context and predict future performance, and vendors can identify performance issues that need to be addressed.

The goal of this chapter is to lay a solid foundation for conducting performance evaluations of specific biometric modalities. Biometric technologies have advanced significantly in the last decade and their use in specific applications will increase in the near future. The ability to conduct meaningful comparisons and assessments will be crucial to successful deployments and increasing biometric adoption.

# 7 Data analysis

In chapter 5 we have seen how raw biometric information (or biometric sample) was gathered directly from the sensor before any processing has been carried out. The biometric acquisition techniques gathering these samples were fingerprint and iris images. This chapter provides a description of analysis techniques used for fingerprint and iris. The first sections give a sketch of how a template is extracted and which comparison methods have been applied. Furthermore it covers the topic of comparison tables that gives a clear overview of how the comparison scores are matched against each other. The last two sections illustrate practical examples of how fusion is performed between fingerprint and iris scores. In addition it also exemplify how False Match Rate (FMR), False None-Match Rate (FNMR), Equal Error Rate (EER) and Decision Trade-off (DET) curves are computed (refer to previous chapter 6, section 6.2)

## 7.1 Creation of biometric templates

Before we are capable of calculating the comparison (distance or similarity) score we must first create templates for each fingerprint and iris image. The template is a processed and stored representation of the distinguishing characteristics of a subject. It gets stored during an enrollment (fingerprint and iris experiment) and which we later will use it for comparison. Due to variations in the way of biometric sample is captured; two templates from the same biometric will never be identical [30]. This is the origin of the probabilistic nature of biometrics, as the comparison process can only give a decision confidence and not an absolute assurance (refer to chapter 3). This project does, however, not give a detailed description of how the low level pre-processing is performed, since it is not a part of this research.

### 7.1.1 Creation of Fingerprint Template

We will now describe how to determine the feasibility of creating minutiae data (templates). These templates are used as the interchange medium for fingerprint information between dissimilar fingerprint comparison systems or similar fingerprint system, which in other words are known as the sensor interoperability. Most biometric systems are designed to compare data originating from the same sensor (using their own algorithms). In some cases the classifiers are trained on data obtained using a single sensor alone thereby restricting their ability to act on data from other sensors. In this thesis is used following comparator:

**Neurotechnolgy [111]** :

**SDK name:** MegaMatcher 4.3 SDK (VeriFinger 6.5 Extended SDK).

**Possible Template Formats:** ISO, ANSI and NT Template.

**Used Template Format:** NT Template, particularly NFTemplate for fingerprint images.

Neurotechnology MegaMatcher SDK includes functionality to extract a set of minutiae data from an individual fingerprint image and compute a comparison-score by comparing one set of

minutiae data with another. The image processing of obtaining the templates can be found in the SDK documention report [111]. Neurotechnolgy supplier provide ISO and ANSI interoperability due to the standardized template formats they offer. These are therefore known as standards. Looking into further details of how interoperability is performed, Neurotechnology offers a Biometric Standards Support (BSS) feature for its SDK. What is special about this is that it allows conversion for fingerprint template to existing biometric systems based on VeriFinger SDK. A list of standards that are supported for conversion with the use of Neurotechnolgy VeriFinger SDK:

- BioAPI 2.0 (ISO/IEC 1978-1:2006) (Framework and Biometric Service Providers for fingerprint identification engines)
- ISO/IEC 19794-2:2005 (Finger Minutiae Data).
- ISO/IEC 19794-4:2005 (Finger image data).
- ANSI/INCITS 378-2004 (Finger Minutiae Format for Data Interchange).
- ANSI/INCITS 381-2004 (Finger Image-Based Data Interchange Format).
- ANSI/NIST-ITL 1-2000 (Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information).

## 7.2 Creation of Iris Template

The same comparator (Neurotechnology) but different algorithm is used for iris comparison process called VeriEye SDK. All core modules that we have mentioned earlier for VeriFinger SDK are part of VeriEye SDK comparator. A list of standards that are supported in addition to above list for conversion with the use of Neurotechnolgy VeriEye SDK [112]:

- BioAPI 2.0 (ISO/IEC 1978-1:2006) (Framework and Biometric Service Providers for fingerprint identification engines)
- ISO/IEC 19794-6:2005 (Iris Image Data).
- ANSI/INCITS 379-2004 (Iris Image Interchange Format).

*"Iris BSS component also allows to integrate JPEG 2000 image format support into applications based on VeriEye SDK or MegaMatcher SDK"* [112].

Iris templates are created by Neurotechnology VeriEye module called *NETemplate* The iris template creation process, known as *"IrisCode"* creation is described in Chapter 3, section 3.2 (Iris Recognition).

## 7.3 Calculation of Comparison Scores

When all templates are created for each fingerprint/iris, a biometric algorithm will take the features from one stored reference template, along with the features extracted from the rest of the templates, and compare them to generate scores which indicates the likelihood that both are

from the same person. The output comparison score may come in a variety of forms, as from zero to hundred (similarity score), unbounded, or such that the closer the score is to zero, the more likely the match (dissimilarity/distance score). This score is the fundamental building block to be used in the comparison score level extraction (refer to section 4.3). In figure 63 is given an illustration of our fusion approach (fingerprint + iris) that we have followed.

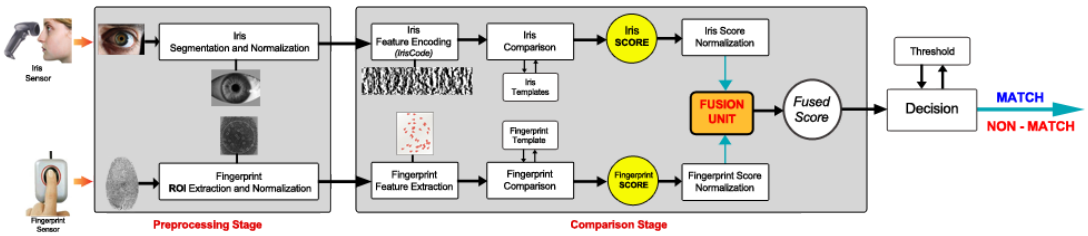



Figure 63: Our Approach: Score-Level Fusion of Fingerprint and Iris Recognition.

It is to be noted that we have optimized our program by creating a function that stores all extraction templates for fingerprint and iris images in a dictionary or hash list in order to speed up the comparison process. The pseudo-code of this function is given in listing 7.1.

Listing 7.1: Pseudo-code that stores all fingerprint and iris templates.

```
public void storeTemplate() //This function stores all templates.
{
        string[] files = Directory.GetFiles(@"path");
        for (int i = 0; i < files.Length; i++)
        {
                string currentFilenamePath = files[i];
                NBuffer currentTemplate =
                   readTemplate(currentFilenamePath);
                templates.Add(Path.GetFileName(currentFilenamePath),
                   currentTemplate);
        }
}
```

### 7.3.1 Fingerprint and Iris Comparison Scores

The comparison score retrieved for the fingerprint and iris were executed from comparison algorithm which is based on similarity and dissimilarity metrics, respectively. This algorithm was executed by the following SDK:

**Neurotechnolgy [110]:** MegaMatcher 4.3 Standard SDK (VeriFinger and VeriEye).

The fingerprint comparison scores are either genuine matches, which should be high scores, or impostor matches which should be lower scores. While the iris comparison scores are either genuine matches, which should be low scores, or impostor matches which should be higher scores. A system's performance is based on these scores, and the biometric graphs (DET-curves) summarize this information in a useful way (refer to section 6.4).

## 7.4 Creating Comparison Score Table

The section deals with the so-called comparison matrix or similarity matrix. The comparison matrix stores the comparison score of every query image versus target image pair. So the size of the comparison matrix is R Q C, where R is the number of targets images, Q is the number of query images and C is comparison score. This, however, depends on the databases given as input that are to be compared against each other. When comparing images from the same database, one will get half as many scores if as comparing two different databases against each other. This is due to the fact that two identical images must not be compared to each other.

### 7.4.1 Comparison Tables

**Fingerprint comparison tables:** Listing 7.2 and 7.3 shows a small excerpt of how the output files from fingerprint comparison process looks like, for fingerprint best database (FP_DB1) and worst database (FP_DB2), respectively.

Listing 7.2: An excerpt of the scores as it is stored for fingerprint database (FP_DB1)

```
1  <1_001_2_1_p.jpg>  <1_001_2_2_p.jpg>  1142  (G)
2  <1_001_2_1_p.jpg>  <1_001_2_3_p.jpg>  1079  (G)
3  <1_001_2_1_p.jpg>  <1_001_2_4_p.jpg>  993   (G)
4  <1_001_2_1_p.jpg>  <1_001_2_5_p.jpg>  1172  (G)
5  <1_001_2_1_p.jpg>  <1_001_7_1_p.jpg>  12    (I)
6  <1_001_2_1_p.jpg>  <1_001_7_2_p.jpg>  17    (I)
7  <1_001_2_1_p.jpg>  <1_001_7_3_p.jpg>  11    (I)
8  <1_001_2_1_p.jpg>  <1_001_7_4_p.jpg>  23    (I)
9  <1_001_2_1_p.jpg>  <1_001_7_5_p.jpg>  9     (I)
.
.
```

Listing 7.3: An excerpt of the scores as it is stored for fingerprint database (FP_DB2)

```
1  <2_001_2_1_p.jpg>  <2_001_2_2_p.jpg>  1341  (G)
2  <2_001_2_1_p.jpg>  <2_001_2_3_p.jpg>  1220  (G)
3  <2_001_2_1_p.jpg>  <2_001_2_4_p.jpg>  1208  (G)
4  <2_001_2_1_p.jpg>  <2_001_2_5_p.jpg>  858   (G)
5  <2_001_2_1_p.jpg>  <2_001_7_1_p.jpg>  15    (I)
6  <2_001_2_1_p.jpg>  <2_001_7_2_p.jpg>  23    (I)
7  <2_001_2_1_p.jpg>  <2_001_7_3_p.jpg>  0     (I)
8  <2_001_2_1_p.jpg>  <2_001_7_4_p.jpg>  9     (I)
9  <2_001_2_1_p.jpg>  <2_001_7_5_p.jpg>  27    (I)
.
.
```

**Iris comparison tables:** Listing 7.4 and 7.5 shows a small excerpt of how the output files from iris comparison process looks like, for iris best database (iris_DB1) and worst database (Iris_DB2), respectively.

Listing 7.4: An excerpt of the scores as it is stored for iris database (Iris_DB1)

```
1   <1_001_2_1_i.jpg>   <1_001_2_2_i.jpg>   1.1645   (G)
2   <1_001_2_1_i.jpg>   <1_001_2_3_i.jpg>   2.0204   (G)
3   <1_001_2_1_i.jpg>   <1_001_2_4_i.jpg>   1.4000   (G)
4   <1_001_2_1_i.jpg>   <1_001_2_5_i.jpg>   1.2683   (G)
5   <1_001_2_1_i.jpg>   <1_001_7_1_i.jpg>   9.2723   (I)
6   <1_001_2_1_i.jpg>   <1_001_7_2_i.jpg>   8.5758   (I)
7   <1_001_2_1_i.jpg>   <1_001_7_3_i.jpg>   8.2624   (I)
8   <1_001_2_1_i.jpg>   <1_001_7_4_i.jpg>   8.3801   (I)
9   <1_001_2_1_i.jpg>   <1_001_7_5_i.jpg>   6.1645   (I)
.
.
```

Listing 7.5: An excerpt of the scores as it is stored for iris database (Iris_DB2)

```
1   <2_001_2_1_i.jpg>   <2_001_2_2_i.jpg>   1.1341   (G)
2   <2_001_2_1_i.jpg>   <2_001_2_3_i.jpg>   1.1220   (G)
3   <2_001_2_1_i.jpg>   <2_001_2_4_i.jpg>   1.1208   (G)
4   <2_001_2_1_i.jpg>   <2_001_2_5_i.jpg>   1.8580   (G)
5   <2_001_2_1_i.jpg>   <2_001_7_1_i.jpg>   8.2624   (I)
6   <2_001_2_1_i.jpg>   <2_001_7_2_i.jpg>   8.3801   (I)
7   <2_001_2_1_i.jpg>   <2_001_7_3_i.jpg>   7.2723   (I)
8   <2_001_2_1_i.jpg>   <2_001_7_4_i.jpg>   6.2887   (I)
9   <2_001_2_1_i.jpg>   <2_001_7_5_i.jpg>   8.1144   (I)
.
.
```

From listings 7.2, 7.3, 7.4 and 7.5, the first column indicates the index/comparison number. Column two and three are the images (or templates) that are compared against each other. Column four indicates the score of the two files compared against each other and the last column tells whether it is a *"genuine"* (G) or an *"impostor"* (I) attempt. As one can see, the filename has a special convention and its context description is shown in Appendix A.

When comparing templates from the same database, for example; if we want to compare iris images from Iris_DB1 with images of the same database Iris_DB1, it will not be applicable to compare the same image against each other as they are identical and in the same time gives an perfect score of 100 % match. However, if the database sets were dissimilar, for example: Iris_DB1 templates against Iris_DB2 templates, then here it would be necessary to compare all templates against each other, since no template in this scenario is the same. The templates that are matched against all the other samples produced by the same subject are indicated as genuine attempts and the templates matched against others are indicated as the impostor or fraudulent attempts. In Table 15 is a small excerpt of a comparison score table for when comparing images of the from the same Database ($DB_x = DB_x$) and Table 16 is when the databases differs ($DB_x \neq DB_x$). [1].

[1] x represent the index-number of a database , so x = (1, 2, 3, 4), because we have four different databases (two for iris two for fingerprint).

Table 15: Comparison scores from the same eye (iris) and same database ($DB_x = DB_x$). G = [genuine], I = [impostor], S = [subject-ID] and A = [attempt-ID].

| | $S_1A_1$ | $S_1A_2$ | ... | $S_1A_K$ | $S_2A_1$ | $S_2A_2$ | ... | $S_NA_K$ |
|---|---|---|---|---|---|---|---|---|
| $S_1A_1$ | - | - | ... | - | - | - | ... | - |
| $S_1A_2$ | G | - | ... | - | - | - | ... | - |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| $S_1A_K$ | G | G | ... | - | - | - | ... | - |
| $S_2A_1$ | I | I | ... | I | - | - | ... | - |
| $S_2A_2$ | I | I | ... | G | G | - | ... | - |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| $S_NA_K$ | I | I | ... | I | I | I | ... | - |

Table 16: Comparison scores from the same eye (iris) and different databases ($DB_x \neq DB_x$). G = [genuine], I = [impostor], S = [subject-ID] and A = [attempt-ID].

| | $S_1A_1$ | $S_1A_2$ | ... | $S_1A_K$ | $S_2A_1$ | $S_2A_2$ | ... | $S_NA_K$ |
|---|---|---|---|---|---|---|---|---|
| $S_1A_1$ | G | G | ... | G | I | I | ... | I |
| $S_1A_2$ | G | G | ... | G | I | I | ... | I |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| $S_1A_K$ | G | G | ... | I | I | I | ... | I |
| $S_2A_1$ | I | I | ... | I | G | G | ... | I |
| $S_2A_2$ | I | I | ... | I | G | G | ... | I |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| $S_NA_K$ | I | I | ... | I | I | I | ... | G |

Assuming that we have N number of participants (subjects) and A number of images (attempts) per iris/fingerprint. When comparing two templates the total number of genuine attempts in the same-sensor and different-sensor context will be:

$$(DB_x = DB_x) \quad G_{tot} = \frac{A \cdot (A-1) \cdot N}{2}, \quad x = 1,2 \tag{7.1}$$

$$(DB_x \neq DB_x) \quad G_{tot} = N \cdot A^2, \quad x = 1,2 \tag{7.2}$$

, whereas total number of impostor attempts will be:

$$(DB_x = DB_x) \quad I_{tot} = \frac{A^2 \cdot (N-1) \cdot N}{2}, \quad (x) = 1,2,3,4 \tag{7.3}$$

$$(DB_x \neq DB_x) \quad I_{tot} = N \cdot (N-1) \cdot A^2, \quad x = 1,2,3,4 \tag{7.4}$$

Each algorithm is tested by performing the following comparisons:

**Genuine recognition attempts:** The template of each fingerprint image is compared to the

remaining images of the same finger, but avoiding symmetric matches (i.e. if the template of image j is matched against image k, template k is not matched against image j);

**Impostor recognition attempts:** The template of each fingerprint image is compared to the remaining images of the same finger, but different subject and avoiding symmetric matches.

**Alternative Impostor recognition attempts** the template of each fingerprint image is compared to the remaining images, avoiding symmetric matches.

Then, for each database:

- A total of 1000 enrollment attempts are performed for iris and a total of 1000 enrollment attempts are performed for fingerprint.
- If all the enrollments are correctly performed (no enrollment failures) for iris or fingerprint database, the total number of genuine and impostor comparison attempts is:

| | $DB_x = DB_x$ | $DB_x \neq DB_x$ |
|---|---|---|
| Genuine | 2000 | 5000 |
| Impostor | 497500 | 995000 |

Table 17: Expected values of genuine and impostor attempts when: subjects N = 100, attempts A = 5 and use of 2 fingers (irises) per subject. Furthermore, x belongs to index-numbers 1, 2, 3 and 4.

It is worth mentioning that for three databases FP_DB1, FP_DB2 and Iris_DB2 we have received a lot of enrolment failures (failure to extract), these failures are presented in chapter 8, particularly in tables 18 and 20 (page 100). While for CASIA-Iris-Lamp we have received 0 extraction failures. This is due to the high quality of iris images and VeriEye algorithm did not fail to extract the iris code for images in this database. On the other hand from these failures we can get indirectly the answer for our research question: How does the quality of images affect the biometric performance? For bad databases X_DB2 (X is for FP or Iris), the VeriFinger and VeriEye failed to extract the templates from images more than for good quality databases X_DB1 (X is for FP or Iris), and this leads to bad biometric performance (high FMR and(or) FNMR).

## 7.5 Normalization and Fusion

### 7.5.1 Normalization

When using the method of fusion at the comparison-score level a normalization step is generally required for the following reasons (refer to 4.5):

1. The comparison scores at the output of the matchers for different modalities can be represented in different ways. For example, one matcher may output distances (as a measure of dissimilarity), while the others may output proximities (as a measure of similarity).
2. The matcher outputs can be in different numerical ranges.

3. The genuine and impostor comparison scores from different modalities might not follow the same statistical distributions.

The output scores for within our experiment resulted in:

**Fingerprint scores:** Similarity measure. Listings 7.2 and 7.3 shows a higher score for a genuine attempt and a low score for an impostor attempt.

**Iris scores:** Dis-similarity or distance measure (Hamming Distance - HD) as we described in chapter 3, sub-section 3.2.3. The Hamming Distance is calculated between two iris codes by following expression:

$$\mathrm{HD} = \frac{|\,(\mathrm{codeQ} \otimes \mathrm{codeR}) \cap \mathrm{maskQ} \cap \mathrm{maskR}\,|}{|\,\mathrm{maskQ} \cap \mathrm{maskR}\,|} \tag{7.5}$$

This distance metric will give us the distance score between the two iris images, $\underline{\mathrm{Q}}$ (Query image) and $\underline{\mathrm{R}}$ (Reference image), meaning that the score should be smaller for genuine attempts than for impostor attempts. But to get the same comparison type as the fingerprint, we simple calculate the multiplicative inverse or reciprocal for the distance score like shown in Equation 7.6.

$$\mathrm{Score}_{\mathrm{similarity}} = \frac{1}{\mathrm{Score}_{\mathrm{distance}}} \cdot \mathrm{factor} \tag{7.6}$$

The $\mathrm{factor}$ is a constant of all natural numbers except zero.

Listing 7.6 shows a lower score for genuine attempts and higher score for impostors.

Listing 7.6: An excerpt of the scores as it is stored for iris database (Iris_DB1)

```
1  <1_001_2_1_i.jpg>  <1_001_2_2_i.jpg>  1.1645  (G)
2  <1_001_2_1_i.jpg>  <1_001_2_3_i.jpg>  2.0204  (G)
3  <1_001_2_1_i.jpg>  <1_001_2_4_i.jpg>  1.4000  (G)
4  <1_001_2_1_i.jpg>  <1_001_2_5_i.jpg>  1.2683  (G)
5  <1_001_2_1_i.jpg>  <1_001_7_1_i.jpg>  9.2723  (I)
6  <1_001_2_1_i.jpg>  <1_001_7_2_i.jpg>  8.5758  (I)
7  <1_001_2_1_i.jpg>  <1_001_7_3_i.jpg>  8.2624  (I)
8  <1_001_2_1_i.jpg>  <1_001_7_4_i.jpg>  8.3801  (I)
9  <1_001_2_1_i.jpg>  <1_001_7_5_i.jpg>  6.1645  (I)
.
.
```

Listings 7.2, 7.3, 7.4 and 7.4 shows clearly that individual matchers in our experiment was homogeneous, meaning that the scores for fingerprint and iris are represented in a different way to each other (refer to point 1). Furthermore, it is also observed a difference in range and a difference in the numbers; the fingerprint scores are integers while iris scores are decimal points (refer to point 2). To solve point 1, that means: to gain a non-homogeneous system, we use Equation 7.6 for the iris scores. This conversion ensures that we translate the distance scores into similarity cores. Listing 7.7 shows a small excerpt of the result when converting the iris distance score into similarity scores by having a factor 10 in Equation 7.6.

Listing 7.7: Conversion from dis-similarity to similarity for iris database (Iris_DB1)

```
1  <1_001_2_1_i.jpg>  <1_001_2_2_i.jpg>  1.8772  (G)
2  <1_001_2_1_i.jpg>  <1_001_2_3_i.jpg>  2.4872  (G)
3  <1_001_2_1_i.jpg>  <1_001_2_4_i.jpg>  4.1667  (G)
4  <1_001_2_1_i.jpg>  <1_001_2_5_i.jpg>  2.3428  (G)
5  <1_001_2_1_i.jpg>  <1_001_7_1_i.jpg>  1.1002  (I)
6  <1_001_2_1_i.jpg>  <1_001_7_2_i.jpg>  1.1660  (I)
7  <1_001_2_1_i.jpg>  <1_001_7_3_i.jpg>  1.2103  (I)
8  <1_001_2_1_i.jpg>  <1_001_7_4_i.jpg>  1.1932  (I)
9  <1_001_2_1_i.jpg>  <1_001_7_5_i.jpg>  1.2316  (I)
.
.
```

Once the conversion from homogeneous to non-homogeneous is processed, normalization can now be applied for fingerprint and iris scores. In sub-section 4.5.1, page 52 are given the normalization methods used for the fingerprint and iris scores. The approaches are MinMax, Z-score and Hyperbolic Tangent. Listing 7.8 shows an excerpt of scores that have been normalized. The normalization approach applied was the MinMax, and it was applied from the data of Listing 7.2 and 7.4 (column 4) [2].

Listing 7.8: Example of using MinMax Approach from section 4.5.1, page 4.5.1

```
1  <1_001_2_1_x.jpg> <1_001_2_2_x.jpg> [0.79526462] [0.6453333]  (G)
2  <1_001_2_1_x.jpg> <1_001_2_3_x.jpg> [0.75139275] [0.5973333]  (G)
3  <1_001_2_1_x.jpg> <1_001_2_4_x.jpg> [0.69150411] [0.6333333]  (G)
4  <1_001_2_1_x.jpg> <1_001_2_5_x.jpg> [0.81615539] [0.3266667]  (G)
5  <1_001_2_1_x.jpg> <1_001_7_1_x.jpg> [0.00835652] [0.0093333]  (I)
6  <1_001_2_1_x.jpg> <1_001_7_2_x.jpg> [0.01181420] [0.0240000]  (I)
7  <1_001_2_1_x.jpg> <1_001_7_3_x.jpg> [0.00766919] [0.0186667]  (I)
8  <1_001_2_1_x.jpg> <1_001_7_4_x.jpg> [0.01601622] [0.0173333]  (I)
9  <1_001_2_1_x.jpg> <1_001_7_5_x.jpg> [0.00626747] [0.0466666]  (I)
.
.
```

As can be seen on the normalized values for both the fingerprint and iris scores, we examine the numbers within the same domain [0 - 1] and numerical range (both are decimal points). In figure 64 are given some distribution examples of fingerprint score normalization by mentioned techniques.

### 7.5.2 Fusion

The fusion at the score-level is the most commonly discussed technique in the biometric literature primarily due to the ease of accessing and processing match scores. The process of fusing normalized data is quite simple. But can also be complex. The fingerprint-based and iris-based similarity scores were fused by four different methods, which are very popular fusion methods in multimodal biometrics and has the advantage of being very fast and simple (refer to section 4.5.2, page 54):

[2] x is for _i or _p, iris and fingerprint images, respectively).

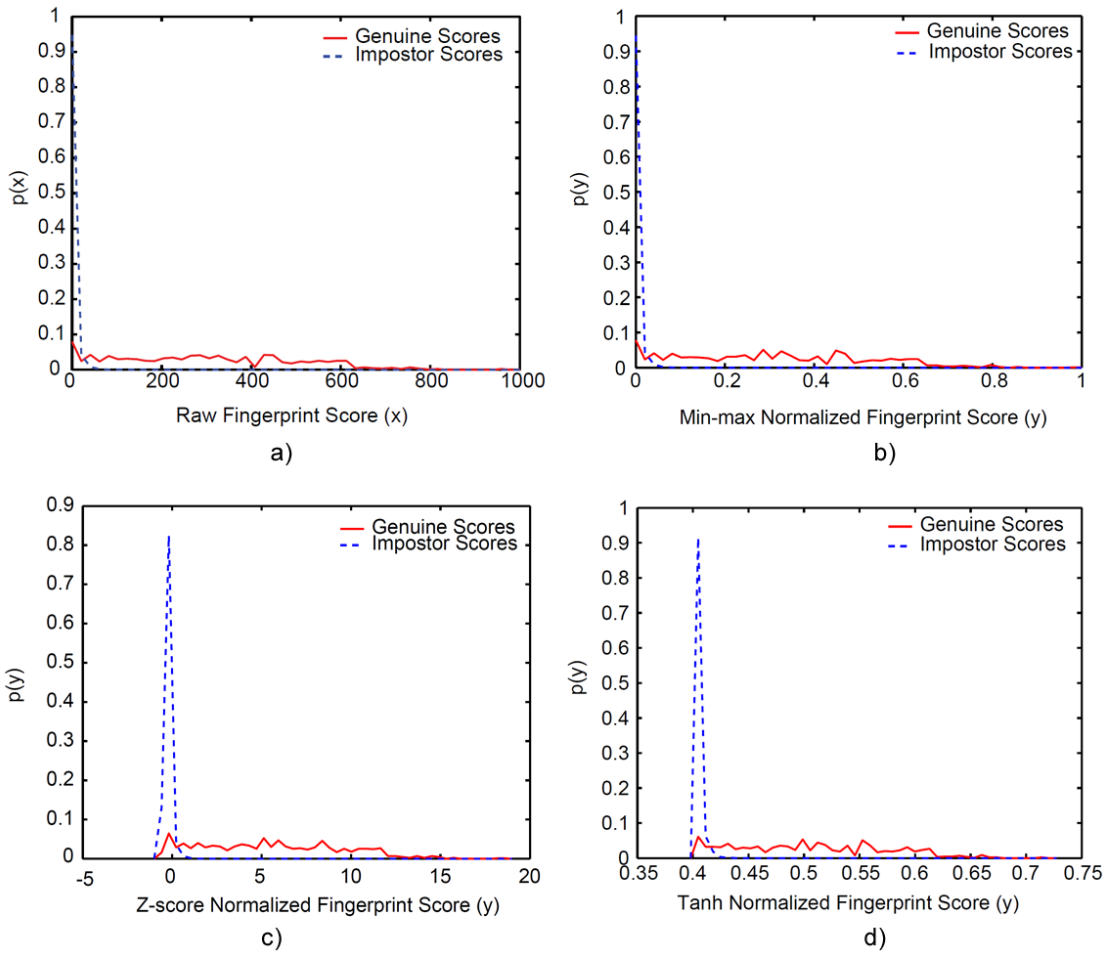



Figure 64: Distributions of genuine and impostor comparison scores. a) Fingerprint un-normalized scores b) MinMax normalization, c) Z-Score normalization and d) TanH normalization.

**Simple Sum:** Adds the fingerprint score with the normalized iris.

**Maximum score:** Applies the maximum score as the fused score between the normalized fingerprint and normalized iris score.

**Minimum score:** Applies the minimum score as the fused score between the normalized fingerprint and normalized iris score.

**User Weighting:** This fusion is based on two weights that are multiplied to each normalized fingerprint-based and iris-based score. The weight denotes how much we trust in that modality, and the common way of assigning weights is according to the performances of the modalities. However, we have chosen to denote the weight for the fingerprint-based score

with 90% and 10 % to the iris:

$$\begin{aligned} S_{fused} &= W_{finger} \cdot S_{finger} + W_{iris} \cdot S_{iris} \\ S_{fused} &= 0.90\% \cdot S_{finger} + 0.10\% \cdot S_{iris} \end{aligned}$$

Listing 7.9 shows an excerpt of fused scores that are normalized with the MinMax approach and fused with the Simple Sum technique.

Listing 7.9: Fusion excerpt of using MinMax normalization and Simple Sum Approach

```
1  <1_001_2_1_x.jpg>  <1_001_2_2_x.jpg>  1.44059795  (G)
2  <1_001_2_1_x.jpg>  <1_001_2_3_x.jpg>  1.34872609  (G)
3  <1_001_2_1_x.jpg>  <1_001_2_4_x.jpg>  1.32483751  (G)
4  <1_001_2_1_x.jpg>  <1_001_2_5_x.jpg>  1.14282265  (G)
5  <1_001_2_1_x.jpg>  <1_001_7_1_x.jpg>  0.01768987  (I)
6  <1_001_2_1_x.jpg>  <1_001_7_2_x.jpg>  0.03583844  (I)
7  <1_001_2_1_x.jpg>  <1_001_7_3_x.jpg>  0.02632683  (I)
8  <1_001_2_1_x.jpg>  <1_001_7_4_x.jpg>  0.03335004  (I)
9  <1_001_2_1_x.jpg>  <1_001_7_5_x.jpg>  0.05293407  (I)
.
.
```

## 7.6 Calculation of FMR, FNMR, EER and DET-curves

After scores have been calculated for both the fingerprint and iris, we can now initiate the creation of Decision Error Trade-off (DET) curve for each score set (refer to section 6.2. The DET curve shows the trade-off between the rate of correct verification (FMNR) and chance of a false match (FMR). A curve from a good system will be located near the bottom of the graph (high verification rate for most false match rates (see Figure 65, right figure). The following describes how the different error rates and curves have been calculated. In Appendix F are some listings of how these rates were calculated in form of a programming aspect compared to the pseudo code that will be used here:

**Creation of List** :

$\text{List}_{gen}$ all genuine scores

$\text{List}_{imp}$ all impostor scores

$\text{List}_{all}$ both genuine and impostor scores

**Calculation of False Match Rate (FMR):** The False Match Rate are calculated as shown in the Pseudo code (Listing 7.10). By having a nested loop, we first count the number of scores which are *smaller* than all the different thresholds in the list of both genuine and impostor. The reason why we increment the smaller is because the data files are of similarity measures and not dissimilarity.

Listing 7.10: Pseudo-code for calculating False Match Rate (FMR)

```
foreach(score s in List_{all})
{
        threshold = s;
        foreach (score gs in List_{gen} )
        {
                genuine_score = gs;
                if (genuine_score < threshold)
                genuine_counter++;
        }
        fmr = genuine_counter / total_number_of_genuines;
}
```

**Calculation of False None Match Rate (FNMR):** There are two changes here from the previous FMR calculation. The first change is that we now look for if the chosen impostor score is *greater* than the threshold. And the other change is that we now divide by the total number of impostors for finding the FNMR value (Listing 7.11). Two small changes, but very important.

Listing 7.11: Pseudo-code to calculate False None Match Rate (FNMR)

```
foreach(score s in List_{all})
{
        threshold = s;
        foreach (score is in List_{imp} )
        {
                impostor_score = is;
                if (impostor_score > threshold)
                impostor_counter++;
        }
        fnmr = impostor_counter / total_number_of_impostor;
}
```

When the threshold, FMR and FNMR values are calculated, then they are outputted to a file as shown in Listing 7.12. In these files first columns indicate the threshold value, second and third column indicate FMR and FMNR, respectively.

Listing 7.12: Output file to create a DET-curve.

```
Threshold       FMR             FNMR
0.2050          0.0031453       0.0135271
0.6863          0.0000000       0.4762859
1.1379          0.0000000       0.9679359
0.6204          0.0000000       0.3700735
0.3299          0.0000000       0.0612892
0.0884          0.5516748       0.0001670
```

```
0.1132          0.2814693       0.0006680
0.1357          0.1219002       0.0016700
0.1126          0.2874137       0.0006680
0.1354          0.1233640       0.0016700
0.1524          0.0579226       0.0041750
0.1347          0.1270555       0.0015030
.
.
```

**Calculation of Error Equal Rate (EER) and Decision Error Trade:** The value indicates that the proportion of false match is equal to the proportion of false none-match. The lower the equal error rate value, the higher the accuracy of the biometric system. A sample graph would look like in Figure 65 (left figure) and as one can see from the graph, the EER occurs where the two lines crosses.

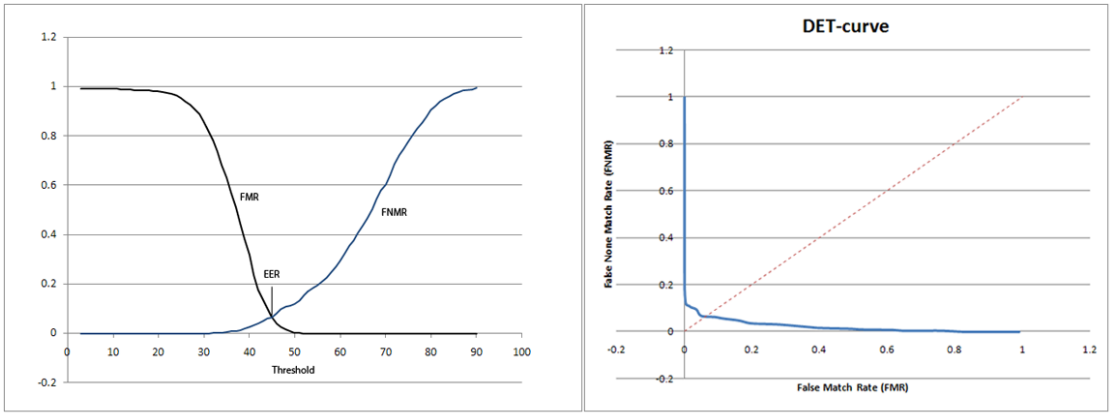



Figure 65: Calculating EER from FMR / FNMR intersection.

To calculate the DET of a biometric system, each corresponding FMR and FNMR point is plotted on a logarithmic scale or scale from 0 - 1 (Figure 65). The EER is then found by extending a 45-degree line from the point of origin (0,0). Where this line crosses the DET in that point we have the EER.

# 8 RESULTS

This chapter is divided into six sections and shows the results of the single biometric modalities (finger and iris) as well as the fusion results. The results are shown by the Decision Error Trade-off (DET) curves with their Equal Error Rates (EER).

First section describes some general information about the experiment plus the way of understanding the abbreviations used in the curves. Second section describes the failure-to-extract (FTX) rates for four used databases (fingerprint and iris). Third and fourth sections show the results from the fingerprint and iris experiment, respectively. While fifth section gives a graph which summarizes the performances for iris and fingerprint databases. And last section gives an overview of some of the fusion results by fusing finger scores with iris scores. Appendix D includes all of the Equal Error Rates for fingerprint, iris, and fusion results.

## 8.1 General Information and Assumptions

In section 7.6 we showed how to calculate the genuine and the impostor attempts. The definitions of these two comparison attempts were not obviously clear to know which one to apply and for that basis it gave us the opportunity to calculate the impostor genuine attempt in two different ways:

**Impostor recognition attempts:** The template of each fingerprint image is compared to the remaining images of the same fingerprint/iris, but different subject and avoiding symmetric matches.

**Alternative Impostor recognition attempts** The template of each fingerprint/iris image is compared to the remaining images, avoiding symmetric matches.

The two approaches are more or less similar. The merely difference is that the alternative approach will produce more impostor scores. And to see which affect it would provide, we consequently analyze and create two DET-curves to distinguish between the approaches in a general manner, see Figure 66.

What we in fact perceive in Figure 66 is a very small dissimilarity; thus we created another zoomed version (see Figure 67), to see the main differences in the EER. What is observed from the figure is that there is a minor difference in of 0.02 %. What we furthermore exposed during the calculation analysis of the two approaches we realized that the alternative approach was more time consuming while calculating. And due to the minor differentiation of EER, we not chosen to apply this approach for the rest of the results shown in following sections

The extraction of features, creation of templates, calculations of comparison scores, FMR, FNMR and creating graphs were done by creating a C#/.NET application. The details of the

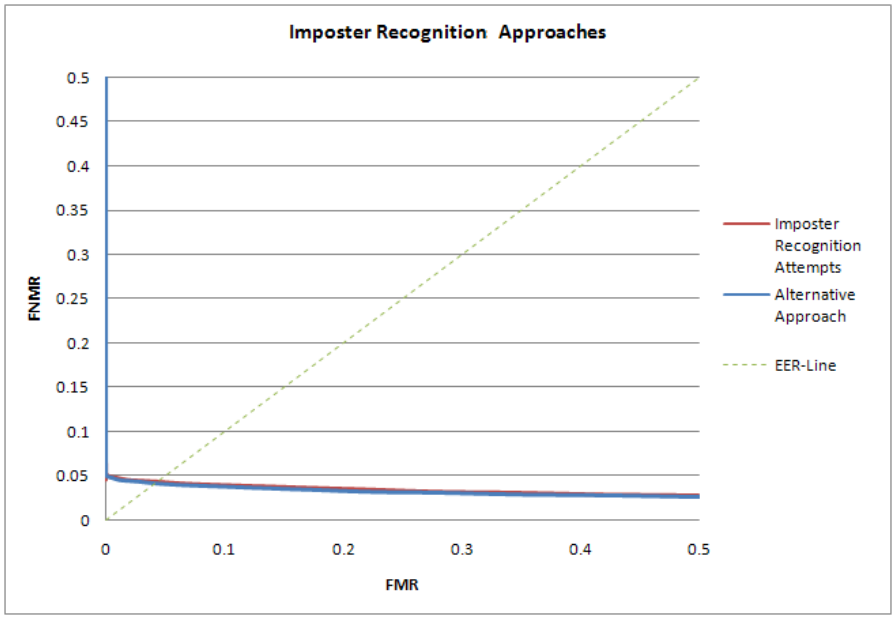



Figure 66: DET-curve illustrating impostor recognition and alternative impostor recognition.

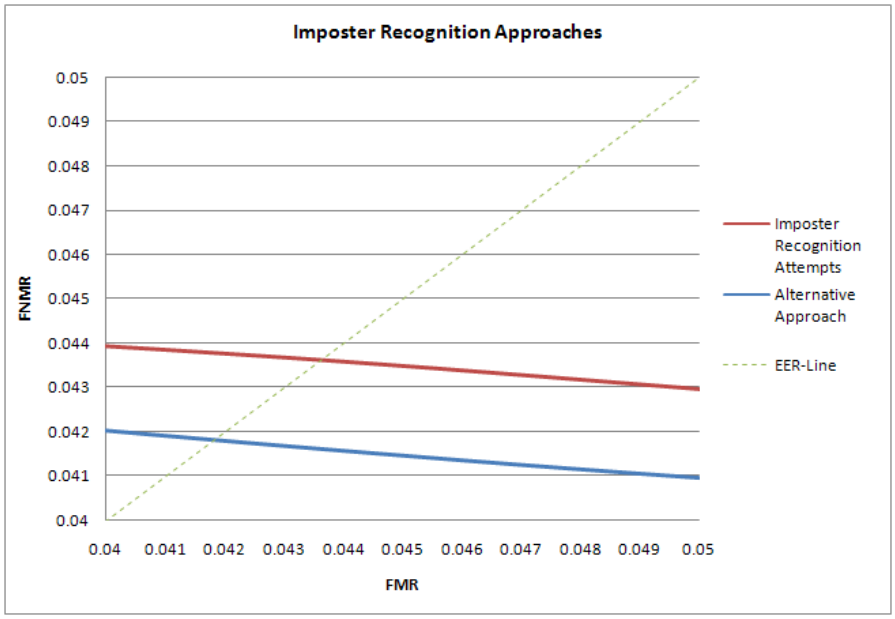



Figure 67: A zoomed version of figure 66.

customized created application will not be described in this section, but for more details about that program, please feel free to contact the author of the thesis.

Before moving into further details we will first introduce some abbreviations. These abbreviations are used to replace large names.

**FP_DB1, FP_DB2, Iris_DB1 and Iris_DB2:** Represent the images of fingerprint best DB (SDUMLA-HMT DB2), fingerprint worst DB (SDUMLA-HMT DB3), Iris best DB (CASIA-Iris-Lamp) and Iris worst DB (SDUMLA-HMT iris), respectively. Refer to Table 14, page 72).

**NT-VF:** Neurotechnology VeriFinger SDK.

**NT-VE:** Neurotechnology VeriEye SDK.

**NNN:** Neurotechnology template extractor, Neurotechnology template comparator, Neurotechnology template extractor.

**MM:** MinMax Normalization method.

**ZS:** Z-Score Normalization method.

**TanH:** Hyperbolic Tangent estimators Normalization method.

**MinS:** Minimum Score Fusion method (rule).

**MaxS:** Maximum Score Fusion method (rule).

**SS:** Simple Sum Score Fusion method (rule).

**UW:** User Weighted Sum score Fusion method.

For each database and for each algorithm/combination, the following performance indicators were measured and reported.

- Threshold, False Match Rate (FMR) and False Non-Match Rate (FNMR).
- Decision Error Trade-off (DET) graphs.
- Failure-to-eXtract (FTX) Rate.
- Equal Error Rate (EER)

Reporting results from all the subjects (100) on the four databases would require too much space for inclusion into this report, therefore, due to the large number of combinations we included all of the EER's in the Appendix D, and choose to describe some of the most *"exciting"* results.

## 8.2 Failure to eXtract (FTX)

An enrollment or comparison attempt can fail, thus resulting in a failure-to-compare (FTC), and Failure-to-eXtract (FTX). Failures can be reported by the algorithm (which declares itself to be unable to process a given fingerprint) in our fingerprint experiment Neurotechnology VeriFinger/VeriEye 6.5 Extended SDK.

The FTX (refer to section 6.1.3) is the error rate when it was unable to create template from fingerprint and iris image and the rates can be seen in Tables 18 and 20, respectively. In these cases feature extraction algorithm (VeriFinger or VeriEye) from Neurotechnology ended with an indication error NULL_TEMPLATE. The algorithm inside the mentioned extractor contain some kind of quality checking functions.

Table 18: Number of not-generated templates from Fingerprint Comparison (VeriFinger)

| **Images From Database** | No. of images | **FP_DB1** | **FP_DB2** | **All** |
|---|---|---|---|---|
| **# Not-generated Templates (NT-VF)** | 1000 | 17 | 31 | 48 |

Table 19: Failure-to-eXtract rates (FTX) in percentage (%).

| **Images From Database** | No. of images | **FP_DB1** | **FP_DB2** | **All** |
|---|---|---|---|---|
| **# Not-generated Templates (NT-VF)** | 1000 | 1.7 | 3.1 | 4.8 |

Table 20: Number of not-generated templates from Iris Comparison (VeriEye)

| **Images From Database** | No. of images | **Iris_DB1** | **Iris_DB2** | **All** |
|---|---|---|---|---|
| **# Not-generated Templates (NT-VE)** | 1000 | 109 | 0 | 109 |

Table 21: Failure-to-eXtract rates (FTX) in percentage (%).

| **Images From Database** | No. of images | **Iris_DB1** | **Iris_DB2** | **All** |
|---|---|---|---|---|
| **# Not-generated Templates (NT-VF)** | 1000 | 10.9 | 0 | 10.9 |

## 8.3 Fingerprint results

### 8.3.1 Comparison of Fingerprint Databases

At first we will be looking at the results when comparing two fingerprint databases collected by two different sensors (refer to chapter 5.2, page 58). Figure 68 illustrates that the fingerprint SDUMLA-HMT database *(FP_DB1)* is performing best and the other fingerprint SDUMLA-HMT database *(FP_DB2)* worst. This is due to bad quality of images that are in *(FP_DB2)*.

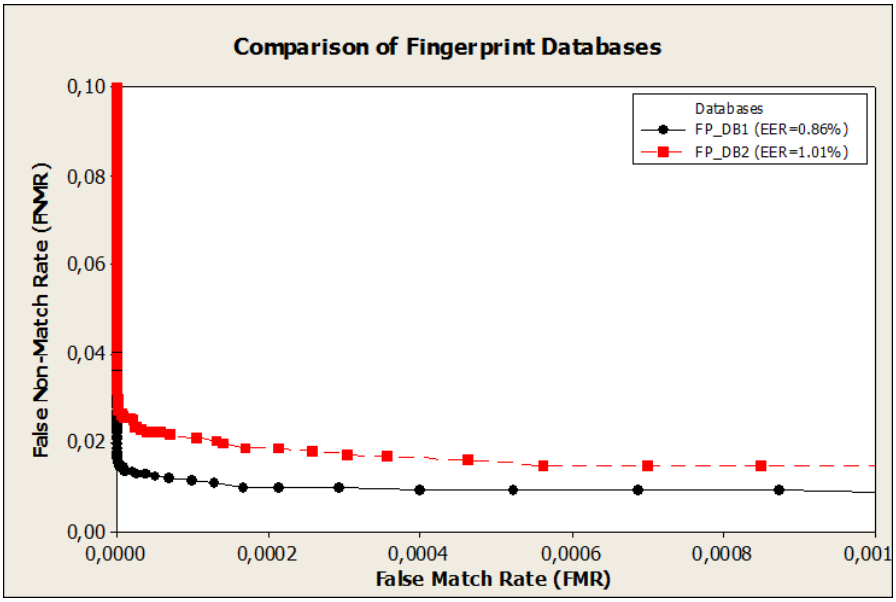



Figure 68: Comparison of Fingerprint Databases. $EER_{FP\_DB1}$ = 0.86 % and $EER_{FP\_DB2}$ = 1.01%.

## 8.4 Iris results

### 8.4.1 Comparison of Iris Databases

Secondly, we will be looking at the results when comparing two iris databases collected by two different sensors (refer to chapter 5.3, page 63).

Figure 69 illustrates that the CASIA-Iris-Lamp iris database *(Iris_DB1)* is performing best and SDUMLA-HMT iris database *(Iris_DB2)* worst. This is due to bad quality of images that are in *(Iris_DB2)*.

In table 22 is given a comparison of EER (Equal Error Rates) from previous researches and our approach only for iris recognition process for CASIA-IrisV4-Lamp (Iris_DB1), because for other databases (SDUMLA-HMT fingerprint and iris) based on our researches and to the best of our knowledge we are the only one who conducted experiments over SDUMLA-HMT fingerprint and iris databases. Thus we do not have other previous results to compare with ours.

Table 22: Comparison of performances provided by [79] with our iris recognition performance on CASIA-IrisV4-Lamp database.

| Study | Performance | CASIA-IrisV4-Lamp |
|---|---|---|
| Wildes [73] | EER(%) | 1.05 |
| John Daugman [80] | EER(%) | 0.86 |
| He et. al. [79] | EER(%) | 0.75 |
| Our Approach (VeriEye) | EER(%) | 0.71 |

As one can see from table 4 our iris comparison process by VeriEye 6.5 SDK for database CASIA-IrisV4-Lamp (Iris_DB1), we have received EER equal to 0.71 %, which is lower than

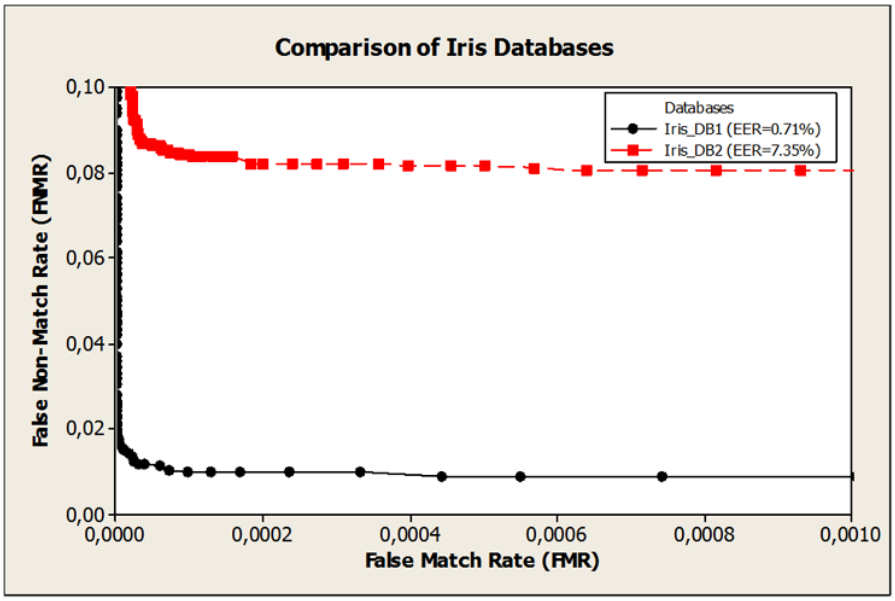



Figure 69: Comparison of Iris Databases. $\mathrm{EER}_{\mathrm{Iris\_DB1}}$ = 0.71 % and $\mathrm{EER}_{\mathrm{Iris\_DB2}}$ = 7.35%.

previous approaches based on He et.al. work published in 2009 [79].

## 8.5 Comparison of Fingerprint and Iris Databases

In Figure 70 is given a summary of comparison between fingerprint and iris databases.

In this case another DET-curve (orange color) is for SDUMLA-HMT iris database (Iris_DB2) that we have carried out some image enhancement, particularly we have enhance the contrast of iris images to 30 % and we have received EER=3.30 % lower than before (EEE=7.35 %), to proof that quality of images is the *key* factor in biometric systems.

## 8.6 Fingerprint and Iris Fusion Results

In the previous sections we saw the results from the fingerprint and iris in a separate manner. We retrieved both low and high EERs and in such cases when having unimodal biometric, then it is often affected by several practical problem like noisy sensor data, unacceptable error rates, spoof attacks etc. As described in Chapter 4 multi-modal biometrics overcome some of these problems. Biometric fusion can be performed in different levels,

1. Sensor level
2. Feature extraction level
3. Score level
4. Decision level

and in this project we conduct fusion at the score-level because it is the most popular and suitable way. Score-level fusion requires normalization of the fingerprint and iris scores as an

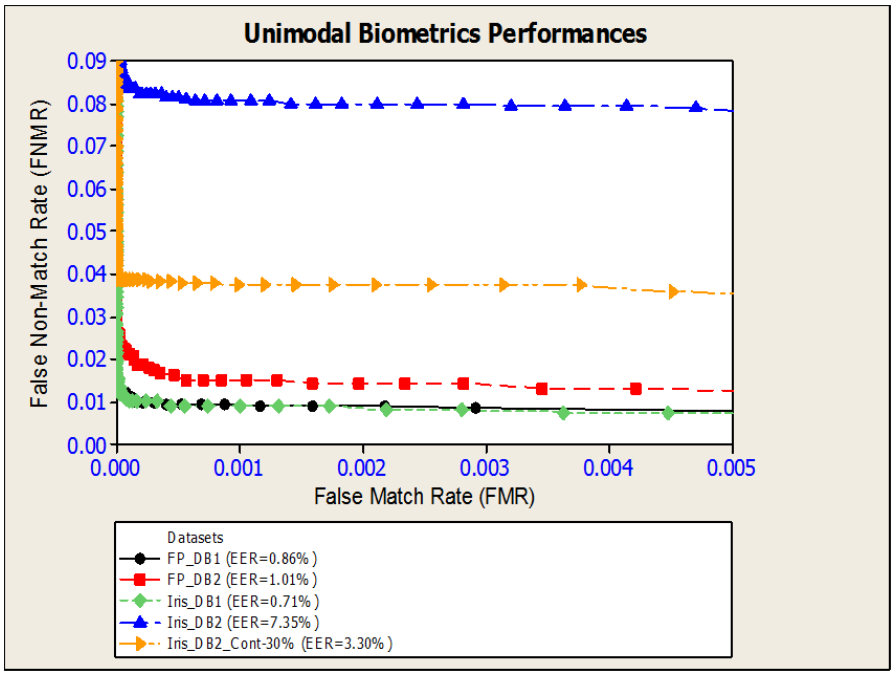



Figure 70: Comparison of Fingerprint and Iris Databases.

initial step. We have applied several normalization techniques such as *Min-Max*, *Z-score*, and *Tanh*. Afterwards, we used four fusion methods which are *Simple Sum*, *Maximum score*, *Minimum score* and *User Weighted sum*. All these normalization and fusion techniques are very known in multi-modal biometrics [116] [117].

### 8.6.1 Comparison of Uni-modal and Multi-modal Biometrics

In figures 71, 72, 73 and 74 we are going to show only one graph for normalization and fusion method per fusion scenario, instead of *3 (normalization methods) x 4 (fusion methods) x 4 (scenarios)* = ***48*** DET graphs in total for fusion scenarios.

**1st scenario:** ***Fusion of FP_DB1 and Iris_DB1***.

Figure 71 shows fusion performance of iris database *Iris_DB1* and fingerprint database *FP_DB1* using Hyperbolic Tangent estimators (TanH) normalization and Simple Sum rule fusion. As can been seen from the figure, EER of fingerprint, iris and fingerprint + iris are 0.86 %, 0.71 % and 0.00010 %, respectively.

**2nd scenario:** ***Fusion of FP_DB1 and Iris_DB2***.

Figure 72 shows fusion performance of fingerprint database *FP_DB1* and iris database *Iris_DB2* using Hyperbolic Tangent estimators (TanH) normalization and Maximum Score rule Fusion. As can been seen from the figure, EER of fingerprint, iris and fingerprint + iris are 0.86 %, 0.71 % and 0.0320 %, respectively.

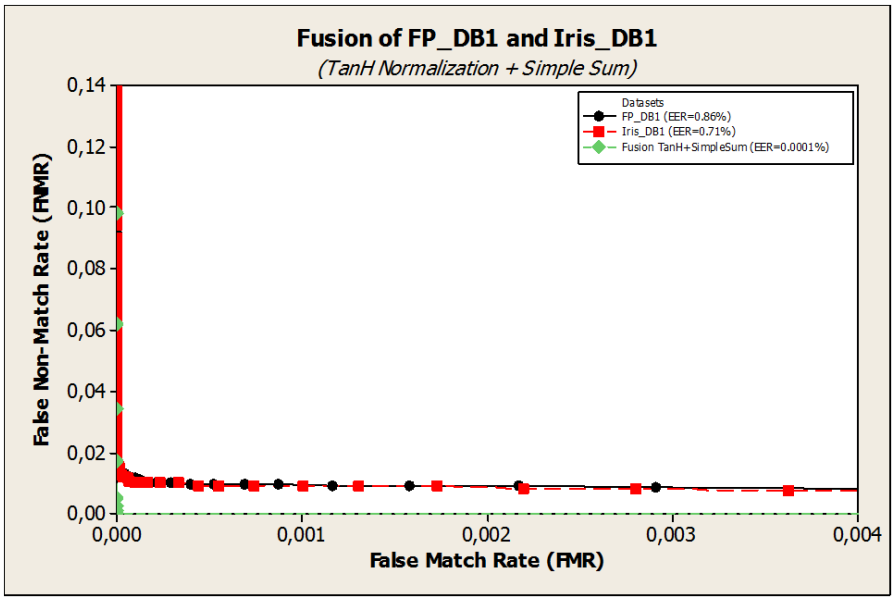



Figure 71: **Scenario 1:** Multi-modal Performance of Fingerprint and Iris using TanH Score Normalization + Simple Sum Score Fusion. $\mathrm{EER}_{\mathrm{FP\_DB1}} = 0.86\%$ , $\mathrm{EER}_{\mathrm{Iris\_DB1}} = 0.71\%$ , $\mathrm{EER}_{\mathrm{Finger+Iris}} = 0.00010\%$.

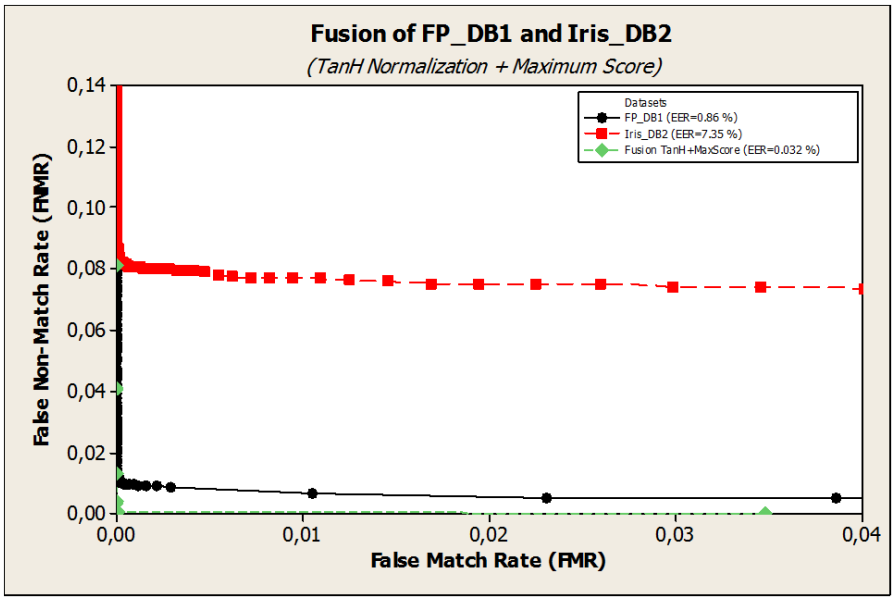



Figure 72: **Scenario 2:** Multi-modal Performance of Iris and Fingerprint using TanH Score Normalization + Maximum Score rule Fusion. $\mathrm{EER}_{\mathrm{FP\_DB1}} = 0.86\%$ , $\mathrm{EER}_{\mathrm{Iris\_DB2}} = 7.35\%$ , $\mathrm{EER}_{\mathrm{Finger+Iris}} = 0.0320\%$.

**3$^{rd}$ scenario:** ***Fusion of FP_DB2 and Iris_DB1***.

Figure 73 shows fusion performance of fingerprint database *FP_DB2* and iris database *Iris_DB1* using MinMax normalization and Maximum Score rule fusion. As can been seen from the figure, EER of fingerprint, iris and fingerprint + iris are 1.01 %, 0.71 % and 0.00015 %, respectively.

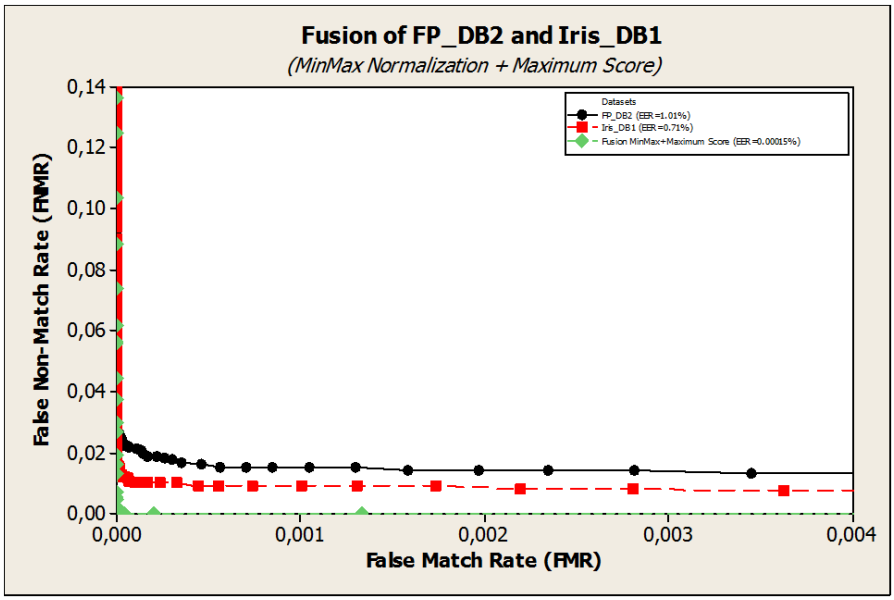



Figure 73: **Scenario 3:** Multi-modal Performance of Iris and Fingerprint using TanH Score Normalization + Simple Sum Score Fusion. $EER_{FP\_DB2} = 1.01\%$ , $EER_{Iris\_DB1} = 0.71\%$ , $EER_{Finger+Iris} = 0.00015\%$.

**4$^{th}$ scenario:** ***Fusion of FP_DB2 and Iris_DB2***.

Figure 74 shows fusion performance of fingerprint database *FP_DB2* and iris database *Iris_DB2* using Hyperbolic Tangent estimators (TanH) normalization and Maximum Score rule fusion. As can been seen from the figure, EER of fingerprint, iris and fingerprint + iris are 1.01 %, 7.35 % and 0.0038 %, respectively.

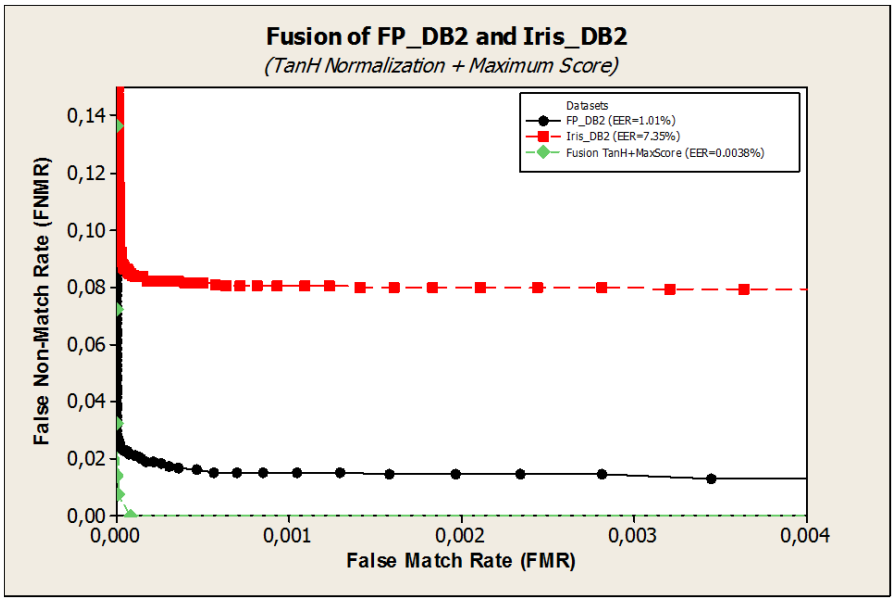



Figure 74: **Scenario 4:** Multi-modal Performance of Iris and Fingerprint using TanH Score Normalization + Simple Sum Score Fusion. $EER_{FP\_DB2} = 1.01\%$ , $EER_{Iris\_DB2} = 7.35\%$ , $EER_{Finger+Iris} = 0.0038\%$.

### 8.6.2 Comparison of Normalization and Fusion Techniques

In Figure 75 are given only four graphs to illustrate the comparison between normalization and fusion techniques.

As can be seen from figure 75 and table 23 Hyperbolic Tangent estimators score normalization technique gives better performance than two others (MinMax and Z-Score). Additionally, the Simple Sum rule fusion gives better results comparing with other fusion approaches.

Table 23: Some of comparison results for normalization and fusion techniques.

| EER (in %) | | | |
|---|---|---|---|
| ***Fusion technique*** | ***Normalization technique*** | | |
| | MinMax (MM) | Z-Score (ZS) | TANH (TH) |
| Minimum Score (MinS) | **3.81836** | **7.32851** | **1.01881** |
| Maximum Score (MaxS) | **0.11591** | **0.11206** | **0.07837** |
| SimpleSum (SS) | **0.08281** | **0.10955** | **0.00011** |
| User Weighting (UW) | **0.08949** | **0.15935** | **0.01763** |

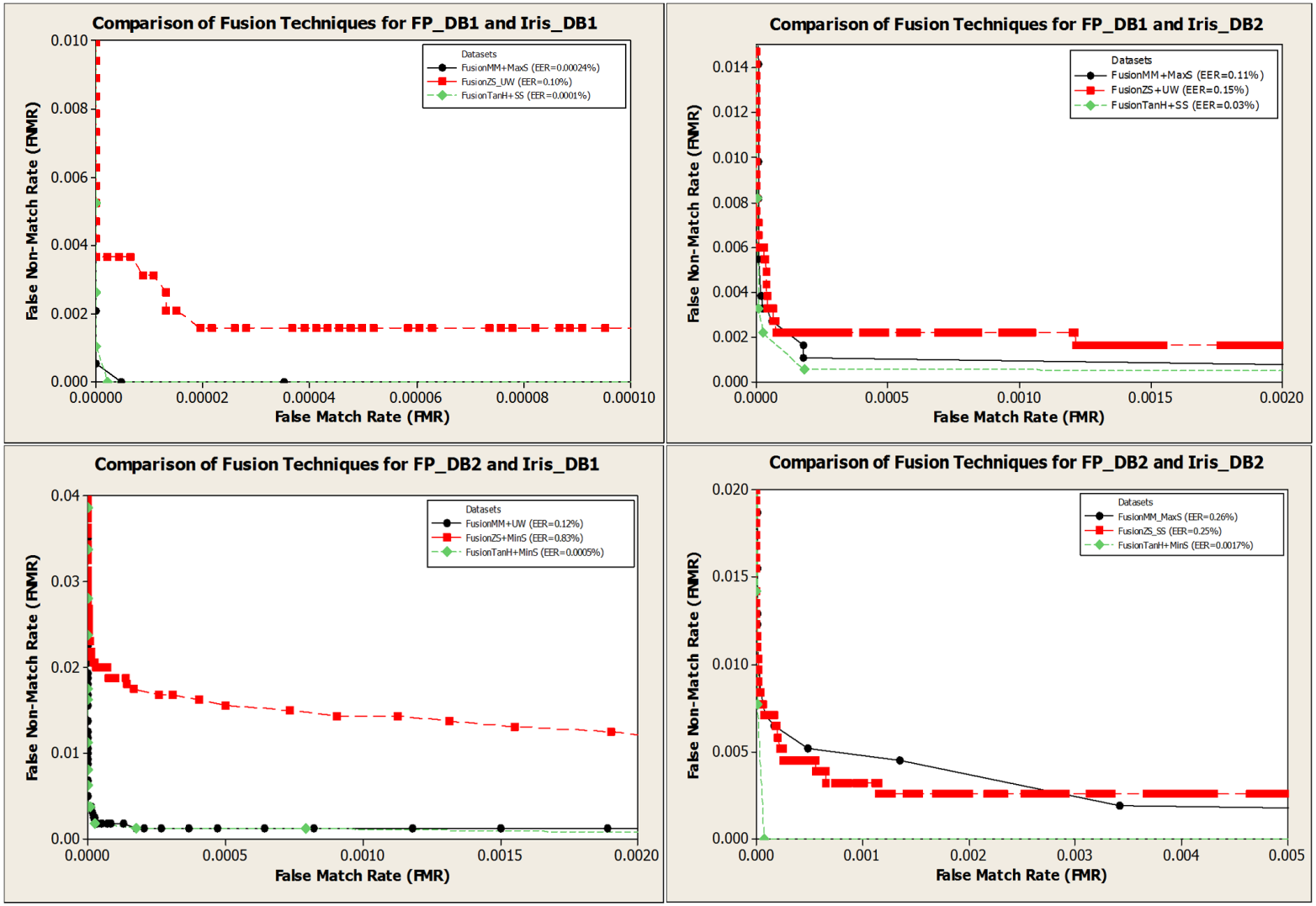



Figure 75: Comparison of Normalization and Fusion Techniques.

## 8.7 Summary

This section provides results obtained on a multi-modal biometric system that uses fingerprint and iris features for biometric verification purposes. As our analysis indicates fusion of iris and fingerprint can improve a performance. For example in Figure 71 we can see an improvement (defined as the percentage difference based on the lowest EER between finger and iris compared to the finger+iris EER) of:

$$\mathrm{Improvement} = \frac{\mathrm{EER}_{min(finger,iris)} - \mathrm{EER}_{finger+iris}}{\mathrm{EER}_{min(finger,iris)}} \cdot 100 \tag{8.1}$$

$$\mathrm{Improvement} = \frac{0.71 - 0.0001}{0.71} \cdot 100 \tag{8.2}$$

$$\mathrm{Improvement} = 99.98\,\%\ \mathrm{decrease} \tag{8.3}$$

Table 24 summarizes the performances shown in this section with their improvements. For more improvement results, refer to Appendix D.

| **Finger** | **Iris** | **Finger + Iris** | **Improvement (method)** |
|---|---|---|---|
| 0.86 % | 0.71 % | 0.0001 % | 99.98 (TanH+SS) % |
| 0.86 % | 7.35 % | 3.81 % | 48.10 (MM+MinS) % |
| 1.01 % | 0.71 % | 0.1872 % | 99.50 (TanH+SS) % |
| 1.01 % | 7.35 % | 0.0038 % | 99.62 (ZS+SS) % |

Table 24: Multimodal fusion improvements of fingerprint and iris recognition. The values in percentages indicate the EER.

Whereas in table 25 is given a comparison of our fusion approach with previous studies [118, 119, 120, 121]. As can be seen from table we have got better fusion performances compared with others.

Table 25: Comparison of our approach (fusion) recognition performances and other previous researches.

| System | Database | Feature | Approach | Level Fusion | FAR | FRR | EER |
|---|---|---|---|---|---|---|---|
| Nagar et al. [118] | FVC2002 DB2A subset | Fingerprint | Unimodal | --- | 0.01% | 5% | *N/A* |
| Li et al. [119] | FVC2002 DB2A | Fingerprint | Unimodal | --- | 0÷0.02% | 12÷8% | *N/A* |
| Mehrotra et al. [120] | BATH | Iris | Multi-algorithmic | Score Level | 0.36% | 8.38% | *N/A* |
| Khalifa et al. [121] | Proprietary DBs | Signature + Handwriting | Multimodal | Decision level | *N/A* | *N/A* | *3.80* |
| | | Signature + Handwriting | Multimodal | Score level | *N/A* | *N/A* | *2.65* |
| | | Signature + Handwriting | Multimodal | Feature Extraction Level | *N/A* | *N/A* | *2.60* |
| | | Signature + Handwriting | Multimodal | Signal level | *N/A* | *N/A* | *6.05* |
| Conti et. al. [21] | FVC2002 DB2B+BATH subset | Iris and Fingerprint | Multimodal | Template Level | 0 | 5.71% | 2.36 |
| | FVC2002 DB2A+BATH | Iris and Fingerprint | Multimodal | Template Level | 0 | 7.28÷9.7% | 3.17÷5.76 |
| **Our Approach** | **CASIA-Iris-Lamp + FP_DB1** | **Iris and Fingerprint** | **Multimodal** | **Score Level** | *N/A* | *N/A* | **0.0001** |
| | **SDUMLA-HMT Iris + FP_DB2** | **Iris and Fingerprint** | **Multimodal** | **Score Level** | *N/A* | *N/A* | **0.0038** |

# 9 Conclusion and Future Work

After the completion of the research presented in this report, there are some conclusions to be drawn. The work done in this thesis has provided some results and insight on multimodal biometric authentication systems. The score level fusion approach presented in this report must still be tested to different modalities and databases to determine its performance. Ultimately the goal is to create such authentication systems in order to increase population coverage, to reduce failure to enrol (FTE) rate and increase biometric systems security. This work shows the potential that can be done. Additionally, many improvements can also still be done on this subject. Therefore this chapter will also list some potential topics for future work in this field. The prospect of continuous research in this area seems to be promising in the future.

## 9.1 Conclusion

Fingerprint is the oldest and most widely adopted biometric technology, but, as discussed in this project (Chapter 3), it is by no means a fully mature technology. The improvement of fingerprint recognition requires research into issues that arise from real-world deployments, such as user interaction, system security and policies, along with image processing algorithms. The increase in the use of mobile and small-scale devices for fingerprint recognition is the next frontier. This will introduce a variety of challenges including user interaction, quality assessment in the field, remote connectivity, policies and procedures to support a mobile infrastructure. Fingerprint still is relatively cheaper than most other biometric solutions and will continue to enjoy broad acceptance in commercial and government implementations. The success of fingerprint recognition in operational deployments will depend on creating solutions that include the user, the system, and the organizational policies.

Fingerprint-based recognition resulted in different performances of using two different databases (FP_DB1 and FP_DB2) collected by two different sensors: *FPR620 optical fingerprint sensor* and *FT-2BU capacitive fingerprint sensor* both developed by Zhongzheng Inc., respectively. The general performance for best quality of fingerprint images (FP_DB1) resulted in *EER = 0.86 %*, while the general performance for worst quality of fingerprint images (FP_DB2) resulted in *EER = 1.01 %*, the difference of performance of these two fingerprint databases in percentage of 0.15 % is due to quality of captured images. Therefore, we conclude that Ft-2BU capacitive fingerprint sensor generates worse images than FPR620 optical fingerprint sensor.

Iris recognition has made great strides in the last decade and the iris texture has shown high distinctiveness for use in large-scale applications. The evaluation of iris images has shown that different color irises provide better quality images in different wavelengths. Future iris systems could use multispectral imaging and choose the best quality iris images. Iris segmentation still remains the most studied area of iris recognition, although research in user interface and iris

capture at a distance will likely become important in the near future. Iris recognition has already established itself as the biometric of choice for large-scale systems, and its proliferation will continue in the near future.

As well as, iris-based recognition resulted in different performances of using two different databases (Iris_DB1 and Iris_DB2) collected by two different sensors: OKI sensor and SDUMLA-HMT sensor, respectively. From the best quality of iris database (CASIA-Iris-Lamp or Iris_DB1) we have achieved the performance of *EER = 0.71 %*, whereas the performance of the worst quality iris database (SDUMLA-HMT iris databse) resulted in an *EER = 7.35 %*, the difference of performance of these two iris databases in percentage of 6.64 % is due to quality of captured iris image and failure of VeriEye to correctly segment the iris.

After we completed the iris experiment and achieved such distinction performances we have conducted iris image processing on SDUMLA-HMT iris database, particularly we have enhance the contrast of iris images about 30 %. We have repeated again the iris comparison process for SDUMLA-HMT iris database (Iris_DB2) and we achieved higher results than in first case and the EER = 3.30 % while without image processing EER was 7.35 %. As one can see we only by contrast enhancement we have increased the biometric performance about 55 % than before.

All achieved results lead to the answer of first research question *How does the quality of images affect biometric performance?*. High quality images result in high performance (low FMR and/or FNMR), while low quality images, result in low performance (high FMR and/or FNMR).

Multibiometric systems are the new frontier and this is evident from th number of ongoing efforts in the research and commercial domains. They are an answer to the deficiencies of unimodal biometric systems, namely, the improvement of performance and the reduction of failure to enroll rates. Theoretically, they presents a huge potential, but research and commercial systems have yet to reflect this promise. The lack of standards also indicates that more work is required before it reaches an acceptable level of maturity.

Current operational multibiometric systems are designed to capture multiple traits and store the raw data separately and use it in a layered decision process, and this practise is unlikely to change in the near future. Multibiometric systems can use existing technology and improve the performance of large-scale databases, and these advantages will drive the development of multibiometric systems.

Furthermore, experimental results show that in most cases fused performance (fingerprint + iris) was significantly improved compared to unimodal biometric performances fingerprint and iris, respectively. All results and improvements for multimodal recognition of fingerprint and iris are found in Appendix D. It is to be noted that the best fusion performance is fusion by *hyperbolic tangent estimators* score normalization technique and *simple sum* rule fusion: $\mathrm{EER}_{\mathrm{Finger+Iris}} = 0.00010$ %.

All in all, we have evaluated the effects on performance, robustness and efficiency of comparison score normalization techniques such as *MinMax*, *Z-Score*, and *Hyperbolic Tangent (TanH)* estimators and fusion approaches like *minimum score*, *maximum score*, *simple sum* rules and *user weighting*. TanH score normalization technique followed by a simple sum and maximum score rule fusion method result in a higher performance than all the other normalization and fusion techniques. What has been observed is that both MinMax and Z-Score methods are sensitive to outliers. On the other hand, the TanH score normalization method is both *robust* and *efficient*.

## 9.2 Future Work

The work done in this thesis can still be expanded in many ways. Score normalization techniques as we mentioned earlier belongs to combination approaches. Therefore, further research would also be: *fusion of fingerprint and iris recognition at score level by learning-based approaches or classification approaches* such as *Artificial Neural Networks (ANN)*, *K-Nearest Neighbourhood (K-NN)*, *Decision Tree* and *Support Vector Machines (SVM)*. And than to compare the recognition performances of score normalization techniques (classification vs. combination approaches).

Another interesting part that could be investigated is fusion of fingerprint and iris recognition at feature extraction level or template level, in order to secure biometric templates and enhance privacy by hiding the meaning of extracted features (points) from iris and fingerprint in the stored template.

It could be also interesting to do research on biometric-based cryptographic keys for identity documents and PKI (Public Key Infrastructure) by combination of fingerprint and iris at feature extraction level (fusion of fingerprint minutiae and iris codes) [18] [19] [20].

It is worth mentioning that we are working on another multimodal biometric authentication topic called: "*Multibiometric Authentication using Fingerprint and Finger Vein: Score Level Fusion Approach*", where we are comparing fusion approaches and performances of fingerprint and finger vein individually, as well as fused performances.

We are looking for possibilities to combine the results from this master thesis and future work on NFC (Near Field Communication) technology as new identity management means for "*Youth Olympic Games 2016*", that are going to be held in Lillehammer.

*I hope and believe that these future researches will be part of challenges to my further studies...PhD!*

# Bibliography

[1] Maltoni, D., Maio, D., Jain, A. K. A., & Prabhakar, S. 2009. *Handbook of Fingerprint Recognition*. Number ISBN: 978-1-84882-253-5. Springer-Verlag, 2nd edition.

[2] Derawi, M. O. *Multi-modal Biometric Authentication using Gait and Fingerprint on Mobile Devices*. Academic dissertation[master thesis], Technical University of Denmark, 2009.

[3] Busch, C. January 29th 2009. *IMT 4621-Biometrics Course: "Biometric Systems" - script*. Number Version 1.0. NISLab.

[4] Jain, A. K., Ross, A. A., & Nandakumar, K. 2011. *An Introduction to Biometrics*. Springer-Verlag.

[5] Smerdon, D. 2000. Anatomy of the eye and orbit. *Current Anaesthesia; Critical Care*, 11(6), 286 – 292.

[6] Guo, G. Face, expression, and iris recognition using learning-based approaches. Master's thesis, UNIVERSITY OF WISCONSIN–MADISON, 2006.

[7] *ISO/IEC TR 24722:2007, Information technology - Biometrics - Multimodal and other multi-biometric fusion, 2007.*

[8] Yin, Y., Liu, L., & Sun, X. 2011. SDUMLA-HMT: A Multimodal Biometric Database. *Biometric Recognition*, 260–268.

[9] Chinese Academy of Sciences Institute of Automation. CASIA-Lamp Image Database V4.0 (CASIA-IrisV4-Lamp). Technical report, 2009.

[10] Woodward, J., Orlans, N., & Higgins, P. 2003. *Biometrics: Identity Assurance in the Information Age*. McGraw-Hill and Osborne Media, Inc.

[11] *ISO/IEC 19794-2:2005, Information technology – Biometric data interchange formats – Part 2: Finger minutiae data, 2005*.

[12] *ISO/IEC 19794-4:2005, Information technology – Biometric data interchange formats – Part 6: Iris image data. 2005*.

[13] *ISO/IEC TR 24722:2007, Information technology - Biometrics - Multimodal and other multi-biometric fusion, 2007*.

[14] Whisenant, W. A. 2003. Using biometrics for sport venue management in a post 9-11 era. *The Emerald Research Register. Facilities*, 21(5/6), pp. 134–141.

[15] *CRS Report for Congress. Biometric Identifiers and Border Security: 9/11 Commission Recommendations and Related Issues*. http://www.au.af.mil/au/awc/awcgate/crs/rs21916.pdf.

[16] Ross, A. A., Nandakumar, K., & Jain, A. K. 2006. *Handbook of Multibiometrics*. Number ISBN-13: 978-0-387-22296-7. Springer-Verlag, 1st edition.

[17] *Brian Handwerk: Born Without Fingerprints: Scientists Solve Mystery of Rare Disorder. National Geographic News, 2006*. http://news.nationalgeographic.com/news/2006/09/060922-fingerprints_2.html.

[18] Jagadeesan, A. 2010. Secured Cryptographic Key Generation From Multimodal Biometrics: Feature Level Fusion of Fingerprint and Iris. *Arxiv preprint arXiv:1003.1458*, 7(2), 28–37.

[19] Lakshmi, A. J. & Ramesh, I. 2012. PKI Key Generation using Multimodal Biometrics Fusion of Fingerprint and Iris. *Matrix*, (2), 285–290.

[20] Jagadeesan, A. 2011. Protected Bio-Cryptography Key Invention from Multimodal Modalities : Feature Level Fusion of Fingerprint and Iris. *European Journal of Scientific Research*, 49(4), 484–502.

[21] Conti, V., Militello, C., Sorbello, F., & Vitabile, S. 2010. A Frequency-based Approach for Features Fusion in Fingerprint and Iris Multimodal Biometric Identification Systems. 40(4), 384–395.

[22] *Biometric Product Testing Final Report*.

[23] *James Corbett: India's Identity Scheme The Magic Number (over one billion people). 2012*. http://tv.globalresearch.ca/2012/01/india-fingerprinting-iris-scanning-over-one-billion-people.

[24] *Biometrics Task Force: Biometric Automated Toolset (BAT) and Handheld Interagency Identity Detection Equipment (HIIDE). 2007*. http://biometrics.nist.gov/cs_links/standard/archived/workshops/xmlandmobileid/Presentations-docs/Vermury-BAT-HIIDE.pdf.

[25] *Wikipedia: Next Generation Identification. 2011*. http://en.wikipedia.org/wiki/Next_Generation_Identification.

[26] Leuven, K. U. 2007. Defining a Research Question. *Seminaire Polibius, Granada*.

[27] Mont, M. C., Bramhall, P., & Pato, J. On Adaptive Identity Management: The Next Generation of Identity Management Technologies. Technical report, HPL, 2003.

[28] Mizelle, B. 2002. Biometrics and Single Sign-On: The Next Step in Identity Management. *BioNetrix Systems Corporation*.

[29] Modi, S. 2011. *Biometrics in Identity Management: Concepts to Applications*. Artech House Information Security and Privacy. Artech House.

[30] Derawi, M. O. Multi-modal biometric authentication using gait and fingerprint on mobile devices. Master's thesis, Technical University of Denmark, 2009.

[31] Flynn, P., Jain, A., & Ross, A. 2008. *Handbook of Biometrics*. Number ISBN-13: 978-0-387-71040-2. Springer-Verlag.

[32] Nanavati, S., Thieme, M., & Nanavati, R. 2002. *Biometrics: personal identification in networked society*. John Wiley and Sons, Inc.

[33] Bhanu, B. & Govindaraju, V. 2011. *Multibiometrics for Human Identification*. Cambridge Univ Pr.

[34] Jain, A. K., Bolle, R., Pankanti, S., Ross, A. A., & Nandakumar, K. 2011. *Introduction to biometrics*. Springer.

[35] Bours, P. A. H. September 2008. *IMT 4721-Authentication Course*. Number Version 1.0.2. NISLab.

[36] Chen, Y., Vinck, H., Gligoroski, D., & Knapskog, S. J. 2011. An overview of the information-theoretic perspective on biometric systems. *Norsk informasjonssikkerhetskonferanse - NISK*, 4(10), 31–42.

[37] Committee, I. S. 2007. Harmonized biometric vocabulary, iso/iec jtc1 sc37.

[38] *ISO/IEC JTC 1/SC 37 Biometrics: SC 37 Standing Document 11 (SD 11), Part 1 Harmonization Document*.

[39] Li, S. Z. & Jain, A. K., eds. 2009. *Encyclopedia of Biometrics*. Springer US.

[40] Vacca, J. 2007. *Biometric technologies and verification systems*. Butterworth-Heinemann.

[41] Babler, W. J. 1991. Embryologic development of epidermal ridges and their configurations. *Birth Defects Original Article Series*, 27(2), 95–112.

[42] Pankanti, S., Prabhakar, S., & Jain, A. aug 2002. On the individuality of fingerprints. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 24(8), 1010 – 1025.

[43] *D.T. Follette, E.B. Hultmark and J.G. Jordan. Direct optical input system for fingerprint verification. IBM Technical Disclosure Bulletin, April*.

[44] *N.J Harrick. Techniques to improve binary joint transform correlator performance for fingerprint recognition, Applied Optics, 1962*.

[45] *Harrick Scientific. Data sheet 8. Frustrated reflection fingerprinting, 1970*.

[46] *S. Jung, R. Thewes, T. Scheiter, K.F. Gooser, and W. Weber. A low-power and high-perfomance CMOS fingerprint sensing and encoding architecture. IEEE Journal of Solid-state Circuits, July 1999*.

[47] *J.-F. Mainguet, M. Pegulu and J.B. Harris. Fingerchip: Thermal imaging and finger sweeping in a silicon fingerprint sensor. In Proc. of AutoID 99, pages 91-94, October 1999*.

[48] *W. Bicz, Z. Gurnienny, and M. Pluta. Ultrasound sensor for fingerprint recognition. In Proc of SPIE, Vol. 2634. Optoelectronic and electronic sensors, pages 104-111, June 1995*.

[49] *B. Moayar and K.S. Fu. An syntactic approach to fingerprint pattern recognition. Pattern Recognition, 7:1-23,1975*.

[50] *B. Moayar and K.S. Fu. A tree system approach for fingerprint for fingerprint pattern recognition. In IEEE Trans. on Computers, C-25(3):262-274, 1976.*

[51] *C.V.K. Rao. Pattern Recognition Techniques applied to Fingerprints. PhD thesis, Linköping University, Sweden, 1977.*

[52] *J.H. Wegstein and J.F. Rafferty. Matching fingerprints by computer. Technical Report 466, National Bureau of Standards, 1969.*

[53] *Hong, L., Wan, Y., Jain, A.: Fingerprint image enhancement: algorithm and performance evaluation. IEEE Transactions on Pattern Analysis and Machine Intelligence 20(8), 777-789 (1998)*.

[54] Daugman, J. 2002. How iris recognition works. *IEEE Transactions on Circuits and Systems for Video Technology*, 14, 21–30.

[55] Masek, L. Recognition of human iris patterns for biometric identification. Technical report, The University of Western Australia, 2003.

[56] Hubel, D. H. 1988. *Eye, brain, and vision / David H. Hubel*. Scientific American Library : Distributed by W.H. Freeman, New York :.

[57] *Wikipedia - Eye. Last Visited: April 17th, 2012.* `http://en.wikipedia.org/wiki/Eye`.

[58] *Wikipedia - Human Eye. Last Visited: April 17th, 2012.* `http://en.wikipedia.org/wiki/Human_eye`.

[59] *Bolle R.M., Connell, J.H., Pankanti, S., Ratha, N.K., Senior, A.W., Guide to Biometrics. 2004, New York: Springer.*

[60] Bertillon, A. 1886. *La couleur de l'Iris: Exposé de la nomenclature des nuances de l'oeil*. Masson.

[61] *Biometrics.gov - NSTC Subcommittee in Biometrics. Iris Recognition. Last Visited: March 7th, 2012.* `http://www.biometrics.gov/Documents/irisrec.pdf`.

[62] Daugman, J. 1994. Biometric personal identification system based on iris analysis. *United States Patent No. 5,291,56. Washington DC: U.S. Government Printing Office. Issued on March*, 1, 1–30.

[63] *Dr. John Daugman - How the Afghan Girl was Identified by Her Iris Patterns.* http://www.cl.cam.ac.uk/~jgd1000/afghan.html.

[64] *NationalGeoraphic.com - A Perfect Match. Available: 12 May 2012.* http://ngm.nationalgeographic.com/static-legacy/ngm/0204/feature0/zoom8.html.

[65] Wildes, R., Asmuth, J., Green, G., Hsu, S., Kolczynski, R., Matey, J., & McBride, S. dec 1994. A system for automated iris recognition. In *Applications of Computer Vision, 1994., Proceedings of the Second IEEE Workshop on*, 121 –128.

[66] Kong, W. & Zhang, D. 2001. Accurate iris segmentation based on novel reflection and eyelash detection model. *Proceedings of 2001 International Symposium on Intelligent Multimedia, Video and Speech Processing, Hong Kong*, 1, 1–30.

[67] Tisse, C.-L., Martin, L., Torres, L., & Robert, M. 2002. Person identification technique using human iris recognition. In *Proc. of Vision Interface*, 294–299.

[68] Ma, L., Wang, Y., & Tan, T. 2002. Iris recognition using circular symmetric filters. 414–417.

[69] Ritter, N. & Owens, R. 1999. Location of the pupil-iris border in slit-lamp images of the cornea. In *Proceedings of the international Conference on Image Analysis and Processing*, 5–6.

[70] Ross, A. & Shah, S. 19 2006-aug. 21 2006. Segmenting non-ideal irises using geodesic active contours. In *Biometric Consortium Conference, 2006 Biometrics Symposium: Special Session on Research at the*, 1 –6.

[71] Aligholizadeh, M., Javadi, S., Sabbaghi-Nadooshan, R., & Kangarloo, K. sept. 2011. An effective method for eyelashes segmentation using wavelet transform. In *Biometrics and Kansei Engineering (ICBAKE), 2011 International Conference on*, 185 –188.

[72] Daugman, J. nov 1993. High confidence visual recognition of persons by a test of statistical independence. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 15(11), 1148 –1161.

[73] Wildes, R. sep 1997. Iris recognition: an emerging biometric technology. *Proceedings of the IEEE*, 85(9), 1348 –1363.

[74] Boles, W. & Boashash, B. apr 1998. A human identification technique using images of the iris and wavelet transform. *Signal Processing, IEEE Transactions on*, 46(4), 1185 –1188.

[75] Oppenheim, A. & Lim, J. may 1981. The importance of phase in signals. *Proceedings of the IEEE*, 69(5), 529 – 541.

[76] Lee, K., Lim, S., Lee, K., Byeon, O., & Kim, T. 2001. Efficient iris recognition through improvement of feature vector and classifier. *ETRI Journal*, 23, 61–70.

[77] Daugman, J. nov. 2006. Probing the uniqueness and randomness of iriscodes: Results from 200 billion iris pair comparisons. *Proceedings of the IEEE*, 94(11), 1927 –1935.

[78] Zhu, Y., Tan, T., & Wang, Y. 2000. Biometric personal identification based on iris patterns. In *Pattern Recognition, 2000. Proceedings. 15th International Conference on*, volume 2, 801 –804 vol.2.

[79] He, Z., Tan, T., Sun, Z., & Qiu, X. September 2009. Toward accurate and fast iris segmentation for iris biometrics. *IEEE Trans. Pattern Anal. Mach. Intell.*, 31(9), 1670–1684.

[80] Daugman, J. oct. 2007. New methods in iris recognition. *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*, 37(5), 1167 –1175.

[81] Kuncheva, L. I., Whitaker, C. J., Shipp, C. A., & Duin, R. P. W. 2000. Is independence good for combining classifiers? In *Pattern Recognition, 2000. Proceedings. 15th International Conference on*, volume 2, 168 –171 vol.2.

[82] Brunelli, R. & Falavigna, D. 1995. Person Identification Using Multiple Cues. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 17(10), 955–966.

[83] Kittler, J., Hatef, M., Duin, R. P. W., & Matas, J. 1998. On combining classifiers. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 20(3), 226–239.

[84] Ben-Yacoub, S., Abdeljaoued, Y., & Mayoraz, E. 1999. Fusion of face and speech data for person identity verification. *IEEE Transactions on Neural Networks*, 10(5), 1065–1074.

[85] Bigün, E., Bigün, J., Duc, B., & Fischer, S. 1997. Expert conciliation for multi modal person authentication systems by Bayesian statistics. *Biometric Person Authentication*, 291–300.

[86] Frischholz, R. W. & Dieckmann, U. 2000. BiolD: a multimodal biometric identification system.

[87] Hong, L. & Jain, A. 1998. Integrating faces and fingerprints for personal identification. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 20(12), 1295–1307.

[88] Snelick, R., Uludag, U., Mink, A., Indovina, M., & Jain, A. 2005. Large-scale evaluation of multimodal biometric authentication using state-of-the-art systems. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 27(3), 450–455.

[89] Wang, Y., Tan, T., & Jain, A. K. 2003. Combining Face and Iris Biometrics for Identity Verification. *Analysis*, 805–813.

[90] Zhou, X. Z. X. & Bhanu, B. 2007. Integrating Face and Gait for Human Recognition at a Distance in Video. *IEEE transactions on systems man and cybernetics Part B Cybernetics a publication of the IEEE Systems Man and Cybernetics Society*, 37(5), 1119–1137.

[91] Jafri, R. & Arabnia, H. R. 2008. Fusion of Face and Gait for Automatic Human Recognition. *Fifth International Conference on Information Technology New Generations iTNG 2008*, 167–173.

[92] Chang, K. C. K., Bowyer, K. W., Sarkar, S., & Victor, B. 2003. Comparison and combination of ear and face images in appearance-based biometrics.

[93] Feng, G., Dong, K., Hu, D., & Zhang, D. 2004. When Faces Are Combined with Palmprints : A Novel Biometric Fusion Strategy. *Proc ICBA*, 701–707.

[94] CUI, F. 2011. Score Level Fusion of Fingerprint and Finger Vein Recognition. *Journal of Computational Information Systems*, 16, 5723–5731.

[95] Toh, K.-A., Xiong, W., Xiong, W., Yau, W.-Y., & Jiang, X. 2003. Combining fingerprint and hand-geometry verification decisions. In *Proceedings of the 4th international conference on Audio- and video-based biometric person authentication*, AVBPA'03, 688–696, Berlin, Heidelberg. Springer-Verlag.

[96] Camlikaya, E., Kholmatov, A., & Yanikoglu, B. 2008. Multi-biometric templates using fingerprint and voice. *Proceedings of SPIE*, 6944, 69440I–69440I–9.

[97] Fierrez-Aguilar, J., Ortega-Garcia, J., Gonzalez-Rodriguez, J., & Bigun, J. 2005. Discriminative multimodal biometric authentication based on quality measures. *Pattern Recognition*, 38(5), 777–779.

[98] Krawczyk, S. & Jain, A. K. 2005. Securing Electronic Medical Records Using Biometric Authentication. *Audio and VideoBased Biometric Person Authentication*, 3546, 1110–1119.

[99] Jain, A., Nandakumar, K., & Ross, A. 2005. Score normalization in multimodal biometric systems. 38(12), 2270–2285.

[100] Ross, A. & Jain, A. 2003. Information fusion in biometrics. *Pattern Recognition Letters*, 24, 2115–2125.

[101] Poh, N. & Bengio, S. 2005. Can chimeric persons be used in multimodal biometric authentication experiments? In *IN: PROC. 2ND JOINT AMI/PASCAL/IM2/M4 WORKSHOP ON MULTIMODAL INTERACTION AND RELATED MACHINE LEARNING ALGORITHMS (MLMI). VOLUME LNCS 3869. (2005) 87–100*, 11–13.

[102] Bailly-baillire, E., Bengio, S., Bimbot, F., Hamouz, M., Kittler, J., Mariéthoz, J., Matas, J., Messer, K., Porée, F., & Ruiz, B. 2003. The banca database and evaluation protocol. In *In Proc. Int. Conf. on Audio- and Video-Based Biometric Person Authentication (AVBPA03*, 625–638. Springer-Verlag.

[103] Poh, N. & Bengio, S. 2004. Database, protocol and tools for evaluating score-level fusion algorithms in biometric authentication.

[104] Ortega-Garcia, J., Fierrez-Aguilar, J., Simon, D., Gonzalez, J., Faundez-Zanuy, M., Espinosa, V., Satue, A., Hernaez, I., Igarza, J. J., Vivaracho, C., Escudero, D., & Moro, Q. I. December 2003. MCYT baseline corpus: a bimodal biometric database. *Vision, Image and Signal Processing, IEE Proceedings -*, 150(6), 395–401.

[105] Garcia-Salicetti, S., Beumier, C., Chollet, G., Dorizzi, B., Jardins, J., Lunter, J., Ni, Y., & Petrovska-Delacrétaz, D. June 2003. BIOMET: A Multimodal Person Authentication Database Including Face, Voice, Fingerprint, Hand and Signature Modalities Audio- and

Video-Based Biometric Person Authentication. In *Audio- and Video-Based Biometric Person Authentication*, Kittler, J. & Nixon, M., eds, volume 2688 of *Lecture Notes in Computer Science*, chapter 98, 1056. Springer Berlin / Heidelberg, Berlin, Heidelberg.

[106] Fierrez-aguilar, J., Ortega-garcia, J., Torre-toledano, D., & Gonzalez-rodriguez, J. 2007. Biosec baseline corpus: A multimodal biometric database. *Pattern Recognition*, 1389–1392.

[107] *NIST Biometric Image Software (NBIS):Release 4.1.0.* http://www.nist.gov/itl/iad/ig/nbis.cfm.

[108] *ISO/IEC TR 29794-1:2009, Information technology – Biometric sample quality – Part 1: Framework. 2009*.

[109] *P. Grother and E. Tabassi and G. W. Quinn and W. Salamon: IREX I: Performance of Iris Recognition Algorithms on Standard Images. NIST Interagency Report 7629. 2005*. http://www.nist.gov/itl/iad/ig/irexi.cfm.

[110] *MegaMatcher 4.3 Extended SDK*.

[111] *Contents of VeriFinger 6.5 Standard SDK and Extended SDK*.

[112] *Contents of VeriEye 6.5 Standard SDK and Extended SDK*.

[113] Wolf, F., Scheidat, T., & Vielhauer, C. 2006. Study of applicability of virtual users in evaluating multimodal biometrics. In *Proceedings of the 2006 international conference on Multimedia Content Representation, Classification and Security*, MRCS'06, 554–561, Berlin, Heidelberg. Springer-Verlag.

[114] *ISO/IEC JTC1 SC37 Biometrics. ISO/IEC SC37 SD2 Version10 Harmonized Biometric Vocabulary.International Organization for Standardization, Aug. 2008.*

[115] *ISO/IEC TC JTC1 SC37 Biometrics. ISO/IEC 19795-1:2006. Information Technology Biometric Performance Testing and Reporting Part 1: Principles and Framework. International Organization for Standardization and International Electrotechnical Committee, Mar. 2006.*

[116] *Jain, A., Ross, A., Multibiometric Systems, Communications of the ACM, Special Issue on Multimodal Interfaces , Vol. 47, No. 1, pp. 34-40, January 2004*.

[117] *State-of-the-Art Report on Multimodal Biometric Fusion.* http://www.biosec.org/index.php.

[118] Nagar, A., Nandakumar, K., & Jain, A. dec. 2008. Securing fingerprint template: Fuzzy vault with minutiae descriptors. In *Pattern Recognition, 2008. ICPR 2008. 19th International Conference on*, 1 –4.

[119] Li, J., Yang, X., Tian, J., Shi, P., & Li, P. dec. 2008. Topological structure-based alignment for fingerprint fuzzy vault. In *Pattern Recognition, 2008. ICPR 2008. 19th International Conference on*, 1 –4.

[120] Sathish, G., S.V.Saravanan, D., Narmadha, D. S., & Maheswari, D. S. U. January 2012. Article: Multi-algorithmic iris recognition. *International Journal of Computer Applications*, 38(11), 13–21. Published by Foundation of Computer Science, New York, USA.

[121] Ben Khalifa, A. & Ben Amara, N. march 2009. Bimodal biometric verification with different fusion levels. In *Systems, Signals and Devices, 2009. SSD '09. 6th International Multi-Conference on*, 1 –6.

# APPENDIXES

# A Filename Convention

The image files are named as follows:

**sensorID_subjectID_modalityID_attemptID_modalityCHAR.jpg**

**sensorID:** is identification number of fingerprint and iris sensors (databases).

**1:** FPR620 optical fingerprint scanner.

**1:** OKI (CASIA-Iris-Lamp) iris scanner.

**2:** FT-2BU capacitive fingerprint scanner both developed by Zhongzheng Inc.

**2:** SDUMLA-HMT iris scanner.

**subjectID:** is identification number of participants (subject) from 001 to 100.

**modalityID:** is identification number for modalities (finger/iris).

**2:** right index finger and RIGHT EYE.

**7:** left index finger and LEFT EYE.

**attemptID:** is identification number for attempts of subjects in total 5: from 1 to 5.

**modalityCHAR:** is identification character for modalities.

**p:** for *fingerprint*.

**i:** for *iris*.

# B Comparison of Biometric Modalities

| Biometric Modality | Advantages | Limitations and Considerations |
|---|---|---|
| • Dynamic signature verification | • Readily integrates into e-business applications<br>• An accepted biometric in banking and financial applications | • Accuracy is affected by one's emotional state, fatigue, or illness |
| • Facial recognition | • Can operate without user interaction<br>• Only current technology capable of identification over distance<br>• Leverages existing image databases<br>• 3D offers increased precision as images capture surface texture of the face on three axes<br>• Can provide a record of potential imposters<br>• Easy for humans to verify the results | • Lighting, variations in pose, and camera inconsistency can reduce matching accuracy<br>• Changes in physiological characteristics or obstructions by hair, hats, glasses, etc., reduce matching accuracy<br>• 2D is susceptible to high false match rates<br>• Faces change over time<br>• Potential privacy concerns |
| • Fingerprint/ palm print | • Most widely used biometric system<br>• Ability to enroll multiple fingers<br>• Generally uses small, low-cost readers<br>• Uses moderate storage space for templates<br>• Many vendors to choose from<br>• Can be highly accurate<br>• An effective biometric for large-scale systems | • Negative public perception regarding the criminal association (e.g., law enforcement and forensics)<br>• Impaired, dirty, dry, or damaged fingers/palms affect use<br>• Not privacy enhancing; high level of latency<br>• Not considered hygienic<br>• Approximately 2% to 5% of a given population cannot be enrolled |

| Biometric Modality | Advantages | Limitations and Considerations |
|---|---|---|
| • Hand geometry | • Operates well in challenging environments; easy to capture<br>• Widely used; established<br>• Biometric is considered highly stable<br>• Very low storage requirements for its templates | • Not accurate for moderate to large populations; human hands are not unique<br>• Readers are bulky and can seem complicated<br>• Perception of passing germs; unhygienic<br>• Not intuitive; requires training |
| • Iris recognition | • Considered the most accurate modality<br>• High stability of characteristics over time<br>• Hands-free operation<br>• Moderate data storage requirements for templates<br>• Works well with either verification or identification applications | • Moderately expensive implementation costs<br>• Requires more training and attentiveness than other biometrics<br>• Can be obscured by eyelashes, eye lenses, and reflections from the cornea |
| • Keystroke dynamics | • Very ease to use and to implement<br>• No additional hardware required | • Only useful for applications that require keyboarding and with users capable of using keyboards |
| • Retina recognition | • Among the most accurate of biometrics<br>• Moderate storage requirements for templates | • Considered intrusive; public has never warmed up to it<br>• Not usable in populations with high incidence of eye disease (e.g., elderly)<br>• Can have high cost; special hardware is required<br>• Limited commercial availability |

*(Continued on next page)*

| Biometric Modality | Advantages | Limitations and Considerations |
|---|---|---|
| • Vein pattern recognition | • Highly private; no properties of latency<br>• Highly secure; not possible to lift or steal the vein pattern<br>• Very accurate<br>• Small to moderately sized readers<br>• Near contactless, hygienic<br>• High level of usability<br>• Difficult to circumvent<br>• No cultural stigmas to overcome | • Newer biometric; not yet widely used<br>• Can be impacted by bright ambient light and some anomalies such as tattooing |
| • Voice verification | • High public acceptance<br>• Readily available component parts (e.g., microphone, etc.)<br>• Contactless<br>• Relatively inexpensive; uses commonly available sensors (e.g., telephones, microphones) | • Not sufficiently distinctive for identification over large databases<br>• Generally large storage requirements for templates (e.g., 2 Kbytes to 10 Kbytes)<br>• Use is limited to those applications in which one's voice is being verified<br>• Somewhat difficult to control sensor and channel variances<br>• Influenced by temporary circumstances such as a sore throat, cold, or similar illnesses |

# C Score normalization and fusion

**ISO/IEC TR 24722**

| Statistical measures | Characterisation data | | |
|---|---|---|---|
| | Genuine distribution | Impostor distribution | Both genuine and impostor distributions |
| Minimum score | $S^G_{Min}$ | $S^I_{Min}$ | $S^B_{Min}$ |
| Maximum score | $S^G_{Max}$ | $S^I_{Max}$ | $S^B_{Max}$ |
| Mean score | $S^G_{Mean}$ | $S^I_{Mean}$ | $S^B_{Mean}$ |
| Median score | $S^G_{Med}$ | $S^I_{Med}$ | $S^B_{Med}$ |
| Score standard deviation | $S^G_{SD}$ | $S^I_{SD}$ | $S^B_{SD}$ |
| Constant | C | C | C |
| Probability density function | $PDF^G$ | $PDF^I$ | N.A. |
| Centre of PDF crossover | $S_{center}$ | | |
| Width of PDF crossover | $S_{width}$ | | |

NOTE S – represents Similarity score; Subscript G stands for Genuine; Subscript I stands for Impostor ; Subscript B stands for Both.



Table 26: Score normalization symbols [13].

**ISO/IEC TR 24722**

| Method | Formula | Data elements | Comment |
|---|---|---|---|
| Min-max (MM) | $S' = (S - S^B_{Min})/(S^B_{Max} - S^B_{Min})$ | $S^B_{Min}$<br>$S^B_{Max}$ | • Uses empirical data (or theoretical limit or vendor provided)<br>• No accounting for non-linearity |
| Z-score | $S' = (S - S^I_{Mean}) / S^I_{SD}$ | $S^I_{Mean}$<br>$S^I_{SD}$ | • Assumes normal distribution<br>• Symmetric about mean<br>• Assumes stability of both distributions across populations |
| Median absolute deviation (MAD) | $S' = (S - S^B_{Med}) / (C \cdot \text{median}\,\lvert S - S^B_{Med}\rvert)$ | $S^B_{Med}$<br>C | • Assumes stability of both distributions across populations |
| Hyperbolic tangent (Tanh) | $S' = 0.5(\tanh(C(S - S^G_{Mean})/ S^G_{SD})+1)$ | $S^G_{Mean}$<br>$S^G_{SD}$ | • Mean and variance of transformed data distribution<br>• Assumes stability of both distributions across populations |
| Adaptive (AD) [a]<br>a) Two-quadrics (QQ)<br>b) Logistic<br>c) Quadric-line-quadric (QLQ) | $n_{AD} = \begin{cases} \frac{1}{c} n_{MM}^2, & n_{MM} \le c \\ c + \sqrt{(1-c)(n_{MM} - c)}, & \text{otherwise} \end{cases}$<br>$n_{AD} = \frac{1}{1 + A \cdot e^{-B \cdot n_{MM}}}$<br>$n_{AD} = \begin{cases} \frac{1}{(c - \frac{w}{2})} n_{MM}^2, & n_{MM} \le (c - \frac{w}{2}) \\ n_{MM}, & (c - \frac{w}{2}) < n_{MM} \le (c + \frac{w}{2}) \\ (c + \frac{w}{2}) + \sqrt{(1 - c - \frac{w}{2})(n_{MM} - c - \frac{w}{2})}, & \text{otherwise.} \end{cases}$ | $c$<br>$w$<br>$\Delta$<br>$A = \frac{1}{\Delta} - 1$<br>$B = \frac{\ln A}{c}$ | • Assumes non-linearity<br>• 3 modeling methods<br>• Assumes stability of both distributions across populations<br>• $n_{AD}$ = adaptive normalisation score; $n_{MM}$ = min-max normalized score; $c$ = center of overlap of genuine and impostor score distributions; $w$ = width of the overlap; $\Delta$ = a small value (0.01 in [63]) |
| Biometric Gain against Impostors (BGI) | $P_{Si\|I} / P_{Si\|G}$, $P_{Si\|G}$ = Value of $PDF^G$ at score $S_i$<br>$P_{Si\|I}$ = Value of $PDF^I$ at score $S_i$ | $PDF^G$<br>$PDF^I$ | • Assumes stability of both distributions across populations |
| BioAPI | $S' = FAR_{(threshold = score)}$ | $PDF^I$ | • Assumes stability of imposter distribution |
| Borda count | N - Rank(S)<br>(Where *N* is the number of alternatives). | Rank | • Applicable only to 1:N matching |

NOTE This table lists two types of normalisation schemes: (i) schemes that modify the location and scale parameters of the score distribution; and (ii) schemes that consider only the overlap region of the genuine and impostor scores. Thus, the min-max, z-score, MAD and tanh techniques fall under category (i), while QQ and QLQ fall under category (ii). Typically, category (ii) techniques are used *after* having applied one of the category (i) schemes.

[a] Refer to document [63] in Bibliography.



Table 27: Score normalization methods [13].

**ISO/IEC TR 24722**

| Method | Score fusion equation | Characterisation data required | | | | | |
|---|---|---|---|---|---|---|---|
| | | None | $PDF_G$ | $PDF_I$ | EER | $V_G$, $V_I$ | Personal |
| Simple sum | $\sum (i=1 \text{ to } N)\ S_i'$ | O | | | | | |
| Minimum score | $\min (i=1 \text{ to } N)\ S_i'$ | O | | | | | |
| Maximum score | $\max (i=1 \text{ to } N)\ S_i'$ | O | | | | | |
| Matcher weighting | $\sum (i=1 \text{ to } N)\ W_i \cdot S_i'$ | | | | O | | |
| Matcher weighting with PDF fusion for decision [a] | $\sum (i=1 \text{ to } N)\ W_i' \cdot S_i'$ | | O | O | | | |
| User weighting | $\sum (i=1 \text{ to } N)\ W_i^* \cdot S_i'$ | | | | | | O |
| Weighted product | $\prod (i=1 \text{ to } N)\ W_i \cdot S_i'$ | | | | O | | |
| Sum of probabilities Genuine | $\sum (i=1 \text{ to } N)\ P_{G\|Si}$ | | O | | | | |
| Sum of probabilities Impostor | $\sum (i=1 \text{ to } N)\ P_{I\|Si}$ | | | O | | | |
| Product of probabilities Genuine | $\prod (i=1 \text{ to } N)\ P_{G\|Si}$ | | O | | | | |
| Product of probabilities Impostor | $\prod (i=1 \text{ to } N)\ P_{I\|Si}$ | | | O | | | |
| BGI [b] | $\prod (i=1 \text{ to } N)\ BGI_i$ | | O | O | | | |
| Likelihood ratio [c] | $PDF_G/PDF_I$ | | O | O | | | |
| K-nearest neighbour | - | | | | | O | |
| Decision trees | - | | | | | O | |
| Support vector machines | - | | | | | O | |
| Discriminant analysis | - | | | | | O | |
| Neural network | - | | | | | O | |

NOTE The following symbols and abbreviations are used in the table.

i = i-th biometric score

N = Number of fusion inputs

$S_i'$ = i-th normalized match score

$W_i$ = i-th matcher weight factor

$W_i^*$ = i-th user weight factor

Wi' = i-th matcher weight factor in case of PDF fusion

BGI = Biometric gain against impostors

$PDF_G$ = Probability density functions of scores from genuine users for each dimension

$PDF_I$ = Probability density functions of scores from impostors for each dimension

EER = Equal error rate

$V_G$ = N-dimensional genuine score vector; N is the number of modalities

$V_I$ = N-dimensional impostor score vector; N is the number of modalities

$P_{G|Si}$ = Value of $PDF_G$ at score $S_i$

$P_{I|Si}$ = Value of $PDF_I$ at score $S_i$

[a] Refer to document [64] in Bibliography.

[b] Refer to documents [60, 61] in Bibliography.

[c] Refer to documents [51] in Bibliography.



Table 28: Score fusion methods [13].

# D Improvements

## D.1 Fusion Recognition Performances (EER in %) - Iris_DB1 and FP_DB1

| Table 1: Fusion with Iris_DB1 and FP_DB1 | | | |
|---|---|---|---|
| EER (in %) | | | |
| ***Fusion technique*** | ***Normalization technique*** | | |
| | MinMax (MM) | Z-Score (ZS) | TANH (TH) |
| Minimum Score (MinS) | **0.49241** | **0.76172** | **1.01881** |
| Maximum Score (MaxS) | **0.00024** | **0.00011** | **0.07837** |
| SimpleSum (SS) | **0.00012** | **0.00011** | **0.00011** |
| User Weighting (UW) | **0.10415** | **0.10462** | **0.01763** |

### D.1.1 Calculated Improvements

| Normalization+Fusion | FP_DB1 | Iris_DB1 | Fingerprint+Iris | Improvement |
|---|---|---|---|---|
| MM+MinS | 0.86 | 0.71 | 0.4924 | **31.04** |
| MM+MaxS | 0.86 | 0.71 | 0.0002 | **99.97** |
| MM+SS | 0.86 | 0.71 | 0.0001 | **99.98** |
| MM+UW | 0.86 | 0.71 | 0.1041 | **85.41** |

| Normalization+Fusion | FP_DB1 | Iris_DB1 | Fingerprint+Iris | Improvement |
|---|---|---|---|---|
| ZS+MinS | 0.86 | 0.71 | 0.76172 | **-6.68** |
| ZS+MaxS | 0.86 | 0.71 | 0.00011 | **99.98** |
| ZS+SS | 0.86 | 0.71 | 0.00011 | **99.98** |
| ZS+UW | 0.86 | 0.71 | 0.10462 | **85.35** |

| Normalization+Fusion | FP_DB1 | Iris_DB1 | Fingerprint+Iris | Improvement |
|---|---|---|---|---|
| TH+MinS | 0.86 | 0.71 | 1.0188 | **-42.69** |
| TH+MaxS | 0.86 | 0.71 | 0.0784 | **89.02** |
| TH+SS | 0.86 | 0.71 | 0.0001 | **99.98** |
| TH+UW | 0.86 | 0.71 | 0.0176 | **97.53** |

## D.2 Fusion Recognition Performances (EER in %) - Iris_DB1 and FP_DB2

| Table 2: Fusion with Iris_DB1 and FP_DB2 | | | |
|---|---|---|---|
| EER (in %) | | | |
| ***Fusion technique*** | ***Normalization technique*** | | |
| | MinMax (MM) | Z-Score (ZS) | TANH (TH) |
| Minimum Score (MinS) | **0.46782** | **0.83031** | **0.00055** |
| Maximum Score (MaxS) | **0.00015** | **0.00014** | **0.18715** |
| SimpleSum (SS) | **0.00045** | **0.00014** | **0.03119** |
| User Weighting (UW) | **0.12156** | **0.12248** | **0.10199** |

### D.2.1 Calculated Improvements

| Normalization+Fusion | FP_DB2 | Iris_DB1 | Fingerprint+Iris | Improvement |
|---|---|---|---|---|
| MM+MinS | 1.02 | 0.71 | 0.4678 | **34.48** |
| MM+MaxS | 1.02 | 0.71 | 0.0002 | **99.98** |
| MM+SS | 1.02 | 0.71 | 0.0004 | **99.94** |
| MM+UW | 1.02 | 0.71 | 0.1216 | **82.98** |

| Normalization+Fusion | FP_DB2 | Iris_DB1 | Fingerprint+Iris | Improvement |
|---|---|---|---|---|
| ZS+MinS | 1.02 | 0.71 | 0.83031 | **-16.29** |
| ZS+MaxS | 1.02 | 0.71 | 0.00014 | **99.98** |
| ZS+SS | 1.02 | 0.71 | 0.00014 | **99.98** |
| ZS+UW | 1.02 | 0.71 | 0.12248 | **82.85** |

| Normalization+Fusion | FP_DB2 | Iris_DB1 | Fingerprint+Iris | Improvement |
|---|---|---|---|---|
| TH+MinS | 1.02 | 0.71 | 0.0005 | **99.92** |
| TH+MaxS | 1.02 | 0.71 | 0.1872 | **73.79** |
| TH+SS | 1.02 | 0.71 | 0.0312 | **95.63** |
| TH+UW | 1.02 | 0.71 | 0.1020 | **85.72** |

## D.3 Fusion Recognition Performances (EER in %) - Iris_DB2 and FP_DB1

| Table 3: Fusion with Iris_DB2 and FP_DB1 | | | |
|---|---|---|---|
| EER (in %) | | | |
| ***Fusion technique*** | ***Normalization technique*** | | |
| | MinMax (MM) | Z-Score (ZS) | TANH (TH) |
| Minimum Score (MinS) | **3.81836** | **7.32851** | **4.39651** |
| Maximum Score (MaxS) | **0.11591** | **0.11206** | **0.03264** |
| SimpleSum (SS) | **0.08281** | **0.10955** | **0.03650** |
| User Weighting (UW) | **0.08949** | **0.15935** | **0.04763** |

### D.3.1 Calculated Improvements

| Normalization+Fusion | FP_DB1 | Iris_DB2 | Fingerprint+Iris | Improvement |
|---|---|---|---|---|
| MM+MinS | 0.86 | 7.36 | 3.8184 | **48.10** |
| MM+MaxS | 0.86 | 7.36 | 0.1159 | **98.42** |
| MM+SS | 0.86 | 7.36 | 0.0828 | **98.87** |
| MM+UW | 0.86 | 7.36 | 0.0895 | **98.78** |

| Normalization+Fusion | FP_DB1 | Iris_DB2 | Fingerprint+Iris | Improvement |
|---|---|---|---|---|
| ZS+MinS | 0.86 | 7.36 | 7.32851 | **0.38** |
| ZS+MaxS | 0.86 | 7.36 | 0.11206 | **98.48** |
| ZS+SS | 0.86 | 7.36 | 0.10955 | **98.51** |
| ZS+UW | 0.86 | 7.36 | 0.15935 | **97.83** |

| Normalization+Fusion | FP_DB1 | Iris_DB2 | Fingerprint+Iris | Improvement |
|---|---|---|---|---|
| TH+MinS | 0.86 | 7.36 | 4.3965 | **40.24** |
| TH+MaxS | 0.86 | 7.36 | 0.0326 | **99.56** |
| TH+SS | 0.86 | 7.36 | 0.0365 | **99.50** |
| TH+UW | 0.86 | 7.36 | 0.0476 | **99.35** |

## D.4 Fusion Recognition Performances (EER in %) - Iris_DB2 and FP_DB2

| Table 4: Fusion with Iris_DB2 and FP_DB2 | | | |
|---|---|---|---|
| EER (in %) | | | |
| ***Fusion technique*** | ***Normalization technique*** | | |
| | MinMax (MM) | Z-Score (ZS) | TANH (TH) |
| Minimum Score (MinS) | **3.38837** | **7.09106** | **0.00170** |
| Maximum Score (MaxS) | **0.26764** | **0.19362** | **0.00381** |
| SimpleSum (SS) | **0.37123** | **0.19376** | **0.07143** |
| User Weighting (UW) | **0.07957** | **0.25806** | **0.04390** |

### D.4.1 Calculated Improvements

| Normalization+Fusion | FP_DB2 | Iris_DB2 | Fingerprint+Iris | Improvement |
|---|---|---|---|---|
| MM+MinS | 1.02 | 7.36 | 3.3884 | **-233.24** |
| MM+SS | 1.02 | 7.36 | 0.3712 | **63.49** |
| MM+MaxS | 1.02 | 7.36 | 0.2676 | **73.68** |
| MM+UW | 1.02 | 7.36 | 0.0796 | **92.17** |

| Normalization+Fusion | FP_DB2 | Iris_DB2 | Fingerprint+Iris | Improvement |
|---|---|---|---|---|
| ZS+MinS | 1.02 | 7.36 | 7.0911 | **-597.40** |
| ZS+SS | 1.02 | 7.36 | 0.1938 | **80.94** |
| ZS+MaxS | 1.02 | 7.36 | 0.1936 | **80.96** |
| ZS+UW | 1.02 | 7.36 | 0.2581 | **74.62** |

| Normalization+Fusion | FP_DB2 | Iris_DB2 | Fingerprint+Iris | Improvement |
|---|---|---|---|---|
| TH+MinS | 1.02 | 7.36 | 0.0017 | **99.83** |
| TH+SS | 1.02 | 7.36 | 0.0714 | **92.97** |
| TH+MaxS | 1.02 | 7.36 | 0.0038 | **99.63** |
| TH+UW | 1.02 | 7.36 | 0.0439 | **95.68** |

# E Source code of our console application for bulk comparison in C#.NET

## E.1 Comparison of Fingerprint Images

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using Neurotec.IO;
using Neurotec.Images;
using Neurotec.Biometrics;
using System.IO;

namespace HIG_VeriFinger
{
    class Neurotechnology
    {
        private NFExtractor _extractor;  // They were "private"
        private NMatcher _matcher;
        private Dictionary<string, NBuffer> templates;
        private DateTime currTime;

        public Neurotechnology()
        {
            _extractor = new NFExtractor();
            _matcher = new NMatcher();
            _matcher.MatchingThreshold = 0;
            templates = new Dictionary<string, NBuffer>();
        }

        public void SetMatchingThreshold()
        {
            //_matcher.MatchingThreshold = 48;
            //_matcher.MatchingThreshold =
               Utils.MatchingThresholdFromString("0.01");
        }

        public NBuffer readTemplate(string fileLocation)
        {

            //NImage image = null;
            NBuffer template = null;

            // Check if given file is a template
```

```
NBuffer fileData = new
    NBuffer(File.ReadAllBytes(fileLocation));
try
{
     NTemplate.Check(fileData);
     template = fileData;
}
catch { }

// If file is not a template, try to load it as image

if (template == null)
{
     try
     {

          // read image
          using (NImage image =
              NImage.FromFile(fileLocation))
          {


               // convert image to grayscale
               using (NGrayscaleImage grayscaleImage =
                   image.ToGrayscale())
               {
                    if
                        (grayscaleImage.ResolutionIsAspectRatio
                             || grayscaleImage.HorzResolution
                                < 250
                             || grayscaleImage.VertResolution
                                < 250)
                    {
                         grayscaleImage.HorzResolution = 500;
                         grayscaleImage.VertResolution = 500;
                         grayscaleImage.ResolutionIsAspectRatio
                             = false;
                    }


                    // extract a fingerprint template from
                        the image for showing
                    NfeExtractionStatus extractionStatus;

                    NFRecord record =
                        _extractor.Extract(grayscaleImage,
                        NFPosition.Unknown,
                        NFImpressionType.LiveScanPlain, out
                        extractionStatus);
```

```
                    if (extractionStatus ==
                        NfeExtractionStatus.TemplateCreated)
                    {
                        // save record to byte array
                        template = record.Save();
                    }
                    else
                    {

                    }
                }
            }
        }
        catch (Exception exp) { }

    }

    return template;

}

public void storeTemplate()
{

    string[] files = Directory.GetFiles(@"path");


    for (int i = 0; i < files.Length; i++)
    {
        string currentFilenamePath = files[i];
        NBuffer currentTemplate =
            readTemplate(currentFilenamePath);
        templates.Add(Path.GetFileName(currentFilenamePath),
            currentTemplate);

    }




}


public int compare(NBuffer _template1, NBuffer _template2)
{
    int score = -1;
    //SetMatchingThreshold();
    if (_template1 != null && _template2 != null)
    {
```

```
            try
            {
                //_matcher.MatchingThreshold = 0;
                return score = _matcher.Verify(_template1,
                    _template2);
            }
            catch (Exception ex)
            {
                // Could not compare two templates -> -2
                return -2;
            }
        }

        return score;
    }

    public void SimalarityScores()
    {

        string output = @"path";
        TextWriter tw = new StreamWriter(output);

        int counter = 0;
        int genuine = 0, imposter = 0;
        int nullTemplates = 0;

        string userID1, userID2;
        string fingerID1, fingerID2;
        string attemptID1, attemptID2;

        for (int i = 0; i < templates.Count; i++)
        {
            var item1 = templates.ElementAt(i);
            string file1 = item1.Key;
            NBuffer tmp1 = item1.Value;

            string[] fileInfo1 = file1.Split('_');
            userID1 = fileInfo1[0];
            fingerID1 = fileInfo1[1];
            attemptID1 = fileInfo1[2];

            if (!file1.EndsWith(".jpg"))
                continue;

            for (int j = i + 1; j < templates.Count; j++)
            {
                var item2 = templates.ElementAt(j);
                string file2 = item2.Key;
                NBuffer tmp2 = item2.Value;
```

```
if (!file2.EndsWith(".jpg"))
    continue;

string[] fileInfo2 = file2.Split('_');
userID2 = fileInfo2[0];
fingerID2 = fileInfo2[1];
attemptID2 = fileInfo2[2];


if (tmp1 != null && tmp2 != null)
{
    counter++;
    //string verified = "";

    //int score = Matcher(tmp1, tmp2,
        verification, ref verified);
    int score = compare(tmp1, tmp2);

    if (userID1.Equals(userID2) &&
        fingerID1.Equals(fingerID2))
    {
        // Genuine
        tw.WriteLine(counter + "\t" + "<" +
            file1 + ">\t" + "<" + file2 + ">\t" +
            "[" + score + "]\t" + "(G)");
        genuine++;
    }
    //else if (sessionID1.Equals(sessionID2))
    else
    {
        // Imposter
        tw.WriteLine(counter + "\t" + "<" +
            file1 + ">\t" + "<" + file2 + ">\t" +
            "[" + score + "]\t" + "(I)");
        imposter++;
    }
}
else
{
    nullTemplates++;
    if (userID1.Equals(userID2) &&
        fingerID1.Equals(fingerID2))
    {
        // Genuine
        tw.WriteLine(counter + "\t" + "<" +
            file1 + ">\t" + "<" + file2 + ">\t" +
            "[" + -1 + "]\t" + "(G)");
        genuine++;
```

```
                    }
                    //else if (sessionID1.Equals(sessionID2))
                    else
                    {
                        // Imposter
                        tw.WriteLine(counter + "\t" + "<" +
                            file1 + ">\t" + "<" + file2 + ">\t" +
                            "[" + -1 + "]\t" + "(I)");
                        imposter++;
                    }

                    counter++;
                }


            }

        }



        // Information about the data:
        tw.WriteLine(); tw.WriteLine();
        tw.WriteLine("In Total:\t" + counter);
        tw.WriteLine("Genuines:\t" + genuine);
        tw.WriteLine("imposters:\t" + imposter);
        tw.WriteLine("Template err:\t" + nullTemplates);

        tw.Close();

        currTime = DateTime.Now;
        Console.WriteLine("Finished:  / 24 : {0:f}", currTime);

    }

    #region Public properties

    public NFExtractor Extractor
    {
        get
        {
            return _extractor;
        }
        set
        {
            _extractor = value;
        }
    }
```

```
        public NMatcher Matcher
        {
            get
            {
                return _matcher;
            }
            set
            {
                _matcher = value;
            }
        }

        #endregion
    }
}
```

## E.2 Comparison of Iris Images

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using Neurotec.IO;
using Neurotec.Images;
using Neurotec.Biometrics;
using System.IO;
using Neurotec.Biometrics.Tools;

namespace IrisRecognition
{
    class Neurotechnology
    {
        private NEExtractor _extractor;  // They were "private"
        private NMatcher _matcher;
        private Dictionary<string, NBuffer> templates;
        private DateTime currTime;
        private NESegmenter _segmenter;

        public Neurotechnology()
        {
            _extractor = new NEExtractor();
            _matcher = new NMatcher();
            //_matcher.IrisesMatchingThreshold = 0;
            templates = new Dictionary<string, NBuffer>();
            _segmenter = new NESegmenter();
            _matcher.MatchingThreshold = 0;
            //_matcher.IrisesMatchingThreshold = 0;

        }
```

```
#region ReadTemplate function with SEGMENTATION
public NBuffer readTemplate(string fileLocation)
{

    //NImage image = null;
    NBuffer template = null;

    // Check if given file is a template
    NBuffer fileData = new
        NBuffer(File.ReadAllBytes(fileLocation));
    try
    {
        NTemplate.Check(fileData);
        template = fileData;
    }
    catch { }

    // If file is not a template, try to load it as image

    if (template == null)
    {
        try
        {

            // read image
            using (NImage image =
                NImage.FromFile(fileLocation))
            {


                // convert image to grayscale
                using (NGrayscaleImage grayscaleImage =
                    image.ToGrayscale())
                {

                    NeeExtractionStatus extractionStatus;
                    NESegmenterAttributes attributes;
                    byte quality;
                    NImage _resultImage =
                        _segmenter.Process(grayscaleImage,
                        NeeImageKind.CroppedAndMasked, out
                        attributes, out quality, out
                        extractionStatus);


                    NeeExtractionStatus extractionStatus2;
                    NeeSegmentationDetails
                        segmentationDetails;
```

```
                        NERecord record =
                            _extractor.Extract(_resultImage.ToGrayscale(),
                            NEPosition.Unknown, out
                            segmentationDetails, out
                            extractionStatus2);

                        if (extractionStatus2 ==
                            NeeExtractionStatus.TemplateCreated)
                        {
                            // save record to byte array
                            template = record.Save();
                        }
                        else
                        {

                        }
                    }
                }
            }
            catch (Exception exp) { }

        }

        return template;

    }
    #endregion

    public void storeTemplate()
    {

        string[] files = Directory.GetFiles(@"path");


        for (int i = 0; i < files.Length; i++)
        {
            string currentFilenamePath = files[i];
            NBuffer currentTemplate =
                readTemplate(currentFilenamePath);
            templates.Add(Path.GetFileName(currentFilenamePath),
                currentTemplate);

        }
    }

    public int compare(NBuffer _template1, NBuffer _template2)
    {
        int score = -1;
```

```
        if (_template1 != null && _template2 != null)
        {
            try
            {
                //_matcher.MatchingThreshold = 0;
                return score = _matcher.Verify(_template1,
                    _template2);
            }
            catch (Exception ex)
            {
                // Could not compare two templates -> -2
                return -2;
            }
        }

        return score;
    }

    public void SimalarityScores()
    {

        string output = @"path";
        TextWriter tw = new StreamWriter(output);

        int counter = 0;
        int genuine = 0, imposter = 0;
        int nullTemplates = 0;

        string userID1, userID2;
        string irisID1, irisID2;
        string attemptID1, attemptID2;

        for (int i = 0; i < templates.Count; i++)
        {
            var item1 = templates.ElementAt(i);
            string file1 = item1.Key;
            NBuffer tmp1 = item1.Value;

            string[] fileInfo1 = file1.Split('_');
            userID1 = fileInfo1[0];
            irisID1 = fileInfo1[1];
            attemptID1 = fileInfo1[2];

            if (!file1.EndsWith(".jpg"))
                continue;

            for (int j = i + 1; j < templates.Count; j++)
            {
                var item2 = templates.ElementAt(j);
```

```
string file2 = item2.Key;
NBuffer tmp2 = item2.Value;

if (!file2.EndsWith(".jpg"))
    continue;

string[] fileInfo2 = file2.Split('_');
userID2 = fileInfo2[0];
irisID2 = fileInfo2[1];
attemptID2 = fileInfo2[2];


if (tmp1 != null && tmp2 != null)
{
    counter++;
    //string verified = "";

    //int score = Matcher(tmp1, tmp2,
        verification, ref verified);
    int score = compare(tmp1, tmp2);

    if (userID1.Equals(userID2) &&
        irisID1.Equals(irisID2))
    {
        // Genuine
        tw.WriteLine(counter + "\t" + "<" +
            file1 + ">\t" + "<" + file2 + ">\t" +
            score + "\t" + "(G)");
        genuine++;
    }
    //else if (sessionID1.Equals(sessionID2))
    else
    {
        // Imposter
        tw.WriteLine(counter + "\t" + "<" +
            file1 + ">\t" + "<" + file2 + ">\t" +
            score + "\t" + "(I)");
        imposter++;
    }
}
else
{
    nullTemplates++;
    if (userID1.Equals(userID2) &&
        irisID1.Equals(irisID2))
    {
        // Genuine
        tw.WriteLine(counter + "\t" + "<" +
            file1 + ">\t" + "<" + file2 + ">\t" +
```

```
                        -1 + "\t" + "(G)");
                    genuine++;
                }
                //else if (sessionID1.Equals(sessionID2))
                else
                {
                    // Imposter
                    tw.WriteLine(counter + "\t" + "<" +
                        file1 + ">\t" + "<" + file2 + ">\t" +
                        -1 + "\t" + "(I)");
                    imposter++;
                }

                counter++;
            }


        }

    }



    // Information about the data:
    tw.WriteLine(); tw.WriteLine();
    tw.WriteLine("In Total:\t" + counter);
    tw.WriteLine("Genuines:\t" + genuine);
    tw.WriteLine("Imposters:\t" + imposter);
    tw.WriteLine("Template err:\t" + nullTemplates);

    tw.Close();

    currTime = DateTime.Now;
    Console.WriteLine("Finished:  / 24 : {0:f}", currTime);

}

#region Public properties

public NEExtractor Extractor
{
    get
    {
        return _extractor;
    }
    set
    {
        _extractor = value;
    }
```

```
        }

        public NMatcher Matcher
        {
            get
            {
                return _matcher;
            }
            set
            {
                _matcher = value;
            }
        }

        #endregion
    }
}
```

# F Source Code to Calculate FMR, FNMR and EER IN C#.NET

## F.1 Calculation of FMR and FNMR

```
public void CalculateFMR_FNMR(string path)
{
                resultsFiles = new DirectoryInfo(path).GetFiles();

    List<double> all;
    List<double> genuines;
    List<double> imposters;

    TextReader tr, trc;
    TextWriter tw;

    foreach (FileInfo file in resultsFiles)
                {
            genuines = new List<double>();
            imposters = new List<double>();
            duplicates = new List<double>();
            all = new List<double>();

            tr = new StreamReader(file.FullName);
      tw = new StreamWriter(path + "output" + file.Name);

      try
      {
          using (tr = new StreamReader(file.FullName))
          {
              string line "";
              string[] lineInfo;
              int score = -1;
              string type = "";

              while ((line = tr.ReadLine()) != null)
              {
                  lineInfo = line.Split("\t");

                  type = lineInfo[4].Substring(1, 1);
                  score = Double.Parse((lineInfo[3].Trim("[", "]")));
                  score = Double.Parse(score.ToString(".####"));

                  all.Add(score);

                  if (type.Equals("G"))
```

```
                {
                    genuines.Add(score);
                }
                else if (type.Equals("I"))
                {
                    imposters.Add(score);
                }
                else
                    Console.Out.WriteLine("Error state;");
            }
        }
    }
    catch (Exception e)
    {
        Console.WriteLine("Error Message: {0}", e.Message);
    }

    List<double> FAR = new List<double>();
    List<double> FRR = new List<double>();

    double genSmaller = 0;
    double impGreater = 0;

    for (int i = 0; i < all.Count; i++)
    {
        double currentScore = all[i];

        if (currentScore == -1 || checkDuplicates(currentScore))
            continue;
        else duplicates.Add(currentScore);

        for (int j = 0; j < genuines.Count; j++)
        {
            double genScore = genuines[j];

            if (genScore < currentScore)
                genSmaller++;
        }

        for (int k = 0; k < imposters.Count; k++)
        {
            double impScore = imposters[k];

            if (impScore > currentScore)
                impGreater++;
        }

        float frr = (float)genSmaller /
            (float)(Convert.ToDouble(genuines.Count));
```

```
            float far = (float)impGreater /
                (float)(Convert.ToDouble(imposters.Count));

            if (!(far == 0.0 && frr == 0.0))
            {
                tw.WriteLine(currentScore + "\t" + "{0:F7}" + "\t" +
                    "{1:F7}", far, frr);
            }

            genSmaller = 0;
            impGreater = 0;
        }

        tw.Flush(); tr.Close(); tw.Close();
                  }
}
```

## F.2 Calculation of Equal Error Rate (EER)

```
public void CalculateEER(string path, string outputname)
{
    resultsFiles = new DirectoryInfo(path).GetFiles();

    TextReader tr;
    TextWriter tw;
    string output = @"..\EER_" + outputname ;
    tw = new StreamWriter(output);

    foreach (FileInfo file in resultsFiles)
    {
        tr = new StreamReader(file.FullName);

        try
        {
            using (tr = new StreamReader(file.FullName))
            {
                string line;
                string[] lineInfo;
                double minimum = 100.0;
                double eer = -2;

                while ((line = tr.ReadLine()) != null)
                {
                    lineInfo = line.Split("\t");

                    if (lineInfo.Length != 2 || lineInfo == null)
                        continue;

                    double fmr = Convert.ToDouble(lineInfo[1]);
                    double far = Convert.ToDouble(lineInfo[0]);
```

```
                    if (Math.Abs(fmr - far) < minimum)
                    {
                        eer = (((fmr + far) / 2.0) * 100.0);
                        minimum = Math.Abs(fmr - far);
                    }
                }

                tw.WriteLine("{0}\t{1}", file.Name, eer);
            }
        }
        catch (Exception e)
        {
            Console.WriteLine("The file could not be read:");
        }
        tr.Close();
    }

    tw.Flush();

}
```

# G Some of FMR and FNMR values Generated by our Program

## G.1 Fingerprint FMR and FNMR

Table 29: FMR and FNMR for FP_DB1

| Threshold | FMR | FNMR |
|---|---|---|
| 1142 | 0.00000 | 0.96813 |
| 1079 | 0.00000 | 0.96186 |
| 993 | 0.00000 | 0.95716 |
| 1172 | 0.00000 | 0.93730 |
| 12 | 0.00000 | 0.89864 |
| 17 | 0.00000 | 0.81557 |
| 11 | 0.00017 | 0.00993 |
| 23 | 0.00021 | 0.00993 |
| 9 | 0.00158 | 0.00888 |
| 0 | 0.00217 | 0.00888 |
| 8 | 0.00291 | 0.00836 |
| 5 | 0.01047 | 0.00679 |
| 24 | 0.03862 | 0.00522 |
| 21 | 0.02304 | 0.00522 |
| 14 | 0.05887 | 0.00470 |
| 29 | 0.08358 | 0.00470 |
| 3 | 0.15500 | 0.00418 |
| 6 | 0.11549 | 0.00418 |
| 15 | 0.20319 | 0.00366 |
| 18 | 0.26106 | 0.00366 |
| 32 | 0.38330 | 0.00313 |
| 26 | 0.31145 | 0.00313 |
| 20 | 0.46111 | 0.00209 |
| 2 | 0.55425 | 0.00209 |
| 27 | 0.60878 | 0.00209 |
| 44 | 0.70375 | 0.00104 |
| 42 | 0.72051 | 0.00104 |
| 30 | 0.66637 | 0.00104 |
| 1202 | 0.72451 | 0.00104 |
| 1184 | 0.72546 | 0.00000 |

Table 30: FMR and FNMR for FP_DB2

| Threshold | FMR | FNMR |
|---|---|---|
| 1341 | 0.61802 | 0.00000 |
| 1220 | 0.61669 | 0.00312 |
| 1208 | 0.61222 | 0.00312 |
| 858 | 0.60202 | 0.00312 |
| 15 | 0.58503 | 0.00312 |
| 23 | 0.56417 | 0.00312 |
| 0 | 0.52954 | 0.00312 |
| 9 | 0.48853 | 0.00374 |
| 27 | 0.44157 | 0.00374 |
| 17 | 0.39935 | 0.00374 |
| 18 | 0.34699 | 0.00374 |
| 21 | 0.29482 | 0.00437 |
| 29 | 0.24472 | 0.00499 |
| 20 | 0.19751 | 0.00499 |
| 8 | 0.15999 | 0.00499 |
| 14 | 0.12083 | 0.00499 |
| 24 | 0.08572 | 0.00561 |
| 12 | 0.05508 | 0.00561 |
| 11 | 0.03192 | 0.00686 |
| 26 | 0.02639 | 0.00811 |
| 6 | 0.02169 | 0.00873 |
| 36 | 0.01786 | 0.00936 |
| 5 | 0.01464 | 0.00936 |
| 32 | 0.01193 | 0.00998 |
| 45 | 0.00973 | 0.01061 |
| 30 | 0.00801 | 0.01123 |
| 33 | 0.00643 | 0.01185 |
| 1488 | 0.00422 | 0.01310 |
| 1121 | 0.00345 | 0.01310 |
| 996 | 0.00000 | 0.95134 |

## G.2 Iris FMR and FNMR values

Table 31: FMR and FNMR for Iris_DB1

| Threshold | FMR | FNMR |
|---|---|---|
| 0.26810 | 0.00000 | 0.73600 |
| 0.29070 | 0.00000 | 0.64500 |
| 0.28986 | 0.00000 | 0.64750 |
| 0.42735 | 0.00000 | 0.34500 |
| 5.00000 | 0.01158 | 0.00550 |
| 4.76190 | 0.00922 | 0.00600 |
| 7.69231 | 0.23475 | 0.00200 |
| 6.25000 | 0.13845 | 0.00250 |
| 5.88235 | 0.11431 | 0.00250 |
| 9.09091 | 0.36289 | 0.00000 |
| 8.33333 | 0.27410 | 0.00150 |
| 6.66667 | 0.16680 | 0.00250 |
| 8.33333 | 0.03904 | 0.00450 |
| 11.1111 | 0.07597 | 0.00250 |
| 0.90090 | 0.31729 | 0.00150 |
| 1.13636 | 0.09348 | 0.00250 |
| 2.94118 | 0.00033 | 0.01000 |
| 9.09091 | 0.04914 | 0.00400 |
| 2.22222 | 0.19902 | 0.00250 |
| 4.16667 | 0.00448 | 0.00750 |
| 10.0000 | 0.06125 | 0.00350 |
| 7.69231 | 0.03094 | 0.00450 |
| 5.26316 | 0.01425 | 0.00500 |
| 5.55556 | 0.01720 | 0.00500 |
| 7.14286 | 0.02445 | 0.00500 |
| 4.00000 | 0.00362 | 0.00750 |
| 6.66667 | 0.02278 | 0.00500 |
| 4.34783 | 0.00572 | 0.00700 |
| 4.54545 | 0.00728 | 0.00700 |
| 3.70370 | 0.00219 | 0.00800 |

Table 32: FMR and FNMR for Iris_DB2

| Threshold | FMR | FNMR |
|---|---|---|
| 0.20661 | 0.00000 | 0.88761 |
| 0.22321 | 0.00000 | 0.82331 |
| 0.21053 | 0.00000 | 0.87036 |
| 0.40816 | 0.00000 | 0.29117 |
| 1.29870 | 0.23301 | 0.06952 |
| 5.55556 | 0.06762 | 0.07371 |
| 7.14286 | 0.08409 | 0.07318 |
| 7.69231 | 0.09815 | 0.07318 |
| 2.85714 | 0.00622 | 0.07737 |
| 5.00000 | 0.05289 | 0.07371 |
| 8.33333 | 0.11405 | 0.07266 |
| 2.94118 | 0.00721 | 0.07684 |
| 1.51515 | 0.26553 | 0.06900 |
| 4.54545 | 0.04010 | 0.07371 |
| 9.09091 | 0.50667 | 0.00000 |
| 3.03030 | 0.37972 | 0.06587 |
| 10.0000 | 0.15336 | 0.07214 |
| 4.00000 | 0.02592 | 0.07527 |
| 1.13636 | 0.20376 | 0.07005 |
| 9.09091 | 0.13284 | 0.07214 |
| 5.26316 | 0.06024 | 0.07371 |
| 3.57143 | 0.01683 | 0.07527 |
| 5.88235 | 0.07395 | 0.07318 |
| 3.22581 | 0.01087 | 0.07684 |
| 4.34783 | 0.03458 | 0.07423 |
| 1.81818 | 0.30113 | 0.06848 |
| 4.54545 | 0.42142 | 0.06221 |
| 4.16667 | 0.02986 | 0.07423 |
| 3.44828 | 0.01452 | 0.07580 |
| 3.70370 | 0.01943 | 0.07527 |

# H SDUMLA-HMT and CASIA Database Release Agreements

# SDUMLA-HMT DATABASE RELEASE AGREEMENT

**Introduction**

Biometrics fusion recognition is a newly arisen and active research topic in recent years. In 2010, the Group of Machine Learning and Applications, Shandong University (SDUMLA) set up the Homologous Multi-modal Traits Database which is named SDUMLA-HMT Database. SDUMLA-HMT Database includes 5 biometric traits, i.e., face, finger vein, gait, fingerprint and iris. SDUMLA will provide the SDUMLA-HMT Database freely of charge to biometrics recognition researchers in order to promote research.

**Content**

The researcher agrees to the following restrictions and requirements on the SDUMLA-HMT database:

1. **Redistribution**: Without prior approval from SDUMLA, SDUMLA-HMT Database, in whole or in part, will not be further distributed, published, copied, or disseminated in any way or form whatsoever, whether for profit or not. This includes further distributing, copying or disseminating to a different facility or organizational unit within the requesting university, organization or company.
2. **Modification**: Without prior approval from SDUMLA, SDUMLA-HMT Database, in whole or in part, will not be modified.
3. **Commercial Use**: SDUMLA-HMT Database, in whole or in part, will not be used for commercial use whensoever.
4. **Publication Requirements**: In no case should the images/videos be used in a way that could reasonably cause the original subject embarrassment or mental anguish.
5. **Acknowledgment to SDUMLA**: In all documents and papers that report experimental results based on this database, SDUMLA-HMT Database should be acknowledged as "We would like to express our thanks to the Group of Machine Learning and Applications, Shandong University for SDUMLA-HMT Database".
6. **Publications to SDUMLA**: Authors of all reports and papers that are for public or general release that use the SDUMLA-HMT Database are kindly requested to send copies of these publications to the following:

Prof. Yilong Yin

The Group of Machine Learning & Applications

School of Computer Science and Technology

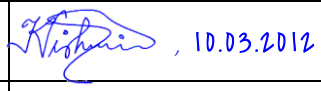
Shandong University

Jinan 250101

China

or send the electronic copy to **ylyin@sdu.edu.cn**.

7. **Indemnification**: Researcher agrees to indemnify, defend and hold harmless SDUMLA and its officers, employees and agents, individually and collectively, from any and all losses, expenses, damages, demands and/or claims based upon any such injury or damage (real or alleged) and shall pay all damages, claims, judgments or expenses resulting from Researcher's use of SDUMLA-HMT Database.

| | |
|---|---|
| **NAME (in capitals)** | KAMER VISHI |
| **SIGNATURE and DATE** |  , 10.03.2012 |
| **ORGNIZATION** | Gjøvik University College |
| **ADDRESS** | Teknologivegen 22, 2815 GJØVIK, NORWAY |
| **EMAIL** | kamer.vishi@hig.no |
| **TELEPHONE** | +47 94 25 91 72 |

*The table can be filled in English or Chinese.

*Send to Prof. Yilong Yin, the Group of Machine Learning & Applications, School of Computer Science and Technology, Shandong University, Jinan, 250101, China, or fax to above at +86-531-88391367, or scan and email **ylyin@sdu.edu.cn**.

**Kamer Vishi**

**From:** Yilong Yin [ylyin@sdu.edu.cn]
**Sent:** 11. mars 2012 11:09
**To:** Kamer Vishi
**Subject:** Re: SDUMLA-HMT Database

Dear Vishi,

I got the agreement.

Hope the datatbase will be helpful to your research.

Best,

Yilong

2012-03-11

Yilong Yin Professor

MLA Group
School of Computer Science and Technology
Shandong University, Mailbox 130
Shunhua Road
Jinan 250101, China

Tel: +86-531-8839-1367 Fax: +86-531-8839-1367
URL: http://mla.sdu.edu.cn/ylyin.html
Email: ylyin@sdu.edu.cn or ylyinsdu@gmail.com

**Granted access on CASIA databases**
*(Confirmation e-mail)*

Welcome to BIT (Biometrics Ideal Test) Inbox x

bitadmin@nlpr.ia.ac.cn May 7
to me

Dear Kamer Vishi,
I am glad to inform you that your registration information submitted to BIT (Biometrics Ideal Test) has been approved and you need to click the following link to activate your account so that you can login the website of BIT.

Please click here to activate your account!

Regards,
Administrator of BIT

Figure 76: SDUMLA-HMT and CASIA database releases (confirmation e-mails).

# Glossary

## A

**Access control** The process of granting or denying specific request to enter a physical facility or to access and use information.

**Accuracy** A computation indicating a biometric system's ability to correctly score a submitted template as a result of a matching process. FAR, FRR, and EER are computational proxies for accuracy.

**Acquisition** See *Capture*.

**Acquisition device** The hardware used to acquire biometric samples.

**Attempt** The submission of a biometric sample to a biometric system for identification or verification. A biometric system may allow more than one attempt to identify or verify.

**Authentication** The process of establishing confidence in a given claim. In biometrics, it is any systematic method of confirming the identity of an individual with confidence; it is used interchangeably with *Verification*.

**Authorization** The administration of person-specific rights, privileges, or access to data or corporate resources.

**Automated Fingerprint Identification System (AFIS)** A specialized fingerprint system that is used to determine the identity of individuals. It is predominantly used by law enforcement. It automatically matches one or many unknown fingerprints against a database of known prints.

## B

**Behavioral biometric** A biometric trait or characteristic that is learned and acquired over time rather than a physiological characteristic.

**Bifurcation** A branch made by more than one finger image ridge. It is a Y-shaped split of one ridge into two ridges.

**Biometric Application Program Interface (BioAPI)** It was designed to produce a standard biometric API aiding developers and consumers. It enables easier installation and integration of biometric devices within the overall system architecture.

**Biometric data** The extracted information taken from the biometric sample and used either to build a reference template or to compare against a previously created reference template. The term is sometimes used as a catch all phrase to refer to any data created during a biometric process to include samples, models, templates, or scores. However, it does not include personal information such as user name or demographic information.

**Biometric sample** The identifiable, unprocessed image or recording (raw data) of a physiological or behavioral characteristic, acquired during submission, and used to generate biometric templates.

**Biometric system** An automated system capable of capturing a biometric sample from an end user; extracting biometric data from that sample, comparing the biometric data with that contained in one or more reference templates, deciding how well they match, and indicating whether an identification or verification of identity has been achieved, and storing the biometric information.

**Biometric template** An encoded, formatted, digital representation of an individual's distinct characteristic(s). Templates are typically created by translating an individual's biometric characteristics using sophisticated algorithms. Templates can vary among biometric modalities and vendors.

**Biometrics** A technology that uses behavioral or physiological characteristics to automatically determine or verify identity. Also, it is a measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an enrollee.

## C

**Capture** The method of collecting a biometric sample from the end user via a sensor. It might be considered a "on-line capture" or an "off-line capture."

**Claim of identity** A claim that occurs when a biometric sample is submitted to a biometric system to verify a claimed identity.

**Comparison** The process of comparing a biometric reference or template with a previously stored template.

**Crossover Error Rate (CER)**

## D

**Decision threshold** The acceptance or rejection of biometric data is dependent on the match score falling above or below the threshold. The threshold is adjustable so that the biometric system can be more or less strict, depending on the requirements of any given biometric application.

**Delta** The point where two ridge-lines moving in parallel change direction and move away from each other.

**Detection Error Trade-off (DET ) curve** A graphical plot of decision error rates (e.g., false acceptance rates (x-axis) vs. false reject rates (y-axis) or matching error rates (false match rates (x-axis) vs. false non-match rates (y-axis).

**Difference score** A value returned by a biometric system that indicates the degree of difference between a biometric sample and a biometric reference.

## E

**Enrollee** A person who has a biometric reference template on file.

**Enrollment** The initial process of collecting biometric samples from an individual and the subsequent preparation and storage of biometric reference templates representing that person's identity.

**Enrollment template** A biometric template, or digital representation of a physical trait, created during the enrollment process.

**Equal Error Rate (EER)** A statistic used to measure biometric performance when operating in the verification task. EER occurs when the decision threshold of a system is set so that the proportion of false rejections will be approximately equal to the proportion of false acceptances. EER is a synonym to *crossover rate*.

**Extraction** The process of converting a captured biometric sample into biometric data so that it can be compared to a reference template.

## F

**Face recognition** A biometric modality that uses an image of the physical structure of an individual's face for recognition purposes.

**Failure to acquire (FTA)** Failure of a biometric system to capture and extract usable biometric data from a biometric sample. The failure to acquire situation might depend on adjustable thresholds for image or signal quality.

**Failure to acquire rate (FTAR)** The frequency (e.g., percentage of attempts) of a failure to acquire.

**Failure to enroll (FTE)** Failure of a biometric system to form a proper enrollment reference for an end user.

**Failure to enroll rate (FTER)** The proportion of a population of users that fail to enroll.

**False acceptance** When a biometric system incorrectly identifies an individual or incorrectly verifies an imposter against a claimed identity.

**False acceptance rate (FAR)** Measures how frequently unauthorized persons are accepted by the system due to erroneous matching. It is the probability that a biometric system will

incorrectly verify an individual's identity or will fail to reject an imposter's identity. It is stated as follows: FAR = NFA/NIIA or FAR = NFA/NIVA, where FAR is the false acceptance rate, NFA is the number of false acceptances, NIIA is the number of imposter identification attempts, and NIVA is the number of imposter verification attempts.

**False acceptance rate (FAR) curve** Graphic depiction of false acceptances plotted as a function of a decision threshold.

**False match rate (FMR)** The expected probability that a sample will be falsely declared a match of a single template.

**False nonmatch rate (FNMR)** The expected probability that a sample will be falsely declared not to match a template from the user supplying the sample.

**False rejection** When a biometric system fails to identify an enrollee or fails to verify the legitimate claimed identity of an enrollee.

**False rejection rate (FRR)** Measures how frequently registered users are rejected by the system. It is the probability that a biometric system will fail to identify an enrollee, or verify the legitimate claimed identity of an enrollee. It is stated as follows: FRR = NFR/NEIA or FRR = NFR/NEVA, where FRR is the false rejection rate, NFR is the number of false rejections, NEIA is the number of enrollee identification attempts, and NEVA is the number of enrollee verification attempts.

**False rejection rate (FRR) curve** Graphic depiction of false rejections as a function of the decision threshold.

**Feature** A distinctive mathematical characteristic derived from a biometric sample.

**Feature extraction** The automated process of locating and encoding distinctive characteristics from a biometric sample in order to generate a template.

## G

**Gait recognition** An individual's manner of walking; a behavioral biometric characteristic.

**Galton features** The features formed by discontinuities in the flow of ridges on finger skin, also called *minutiae*.

**Genuine attempt** A user tries to match his or her sample against his or her own enrollment template.

## H

**Hacking** The act of gaining illegal or unauthorized access to a computer system or network.

**Hamming distance** The number of non-corresponding digits in a string of binary digits, used to measure dissimilarity (eg. comparison of *iriscodes* in iris recognition).

**Henry classification** The classification system based on overall ridge flow created by Edward Henry for manual fingerprint identification.

## I

**Identification** The process by which the biometric system identifies a person by performing a one-to-many (1:n) search against the entire enrolled population. Identification systems are designed to determine identity based solely on biometric information.

**Identifying characteristics** Unique characteristics of an individual used for biometric processing.

**Identity** An assortment of information describing and individual's characteristics and uniqueness. *Note:* Identity is information concerning an individual, not the individual himself.

**Identity management** The process of establishing identities for individuals in a system and controlling their access to resources with that system by associating user rights and restrictions with the established identities.

**Identity theft** The appropriation of another's personal information to commit fraud, steal the person's assets, or pretend to be that person.

**Imposter attempt** A person who submits a biometric sample in either an intentional or inadvertent attempt to pass himself or herself off as another person who is an enrollee.

**Integrated Automated Fingerprint Identification System (IAFIS)** The Federal Bureau of Investigation's (FBI) large-scale 10-fingerprint identification system that is used for criminal history background checks and identification of latent prints discovered at crime scenes.

**Intraclass variation** A condition where data acquired from a user during verification differs significantly from the data acquired during enrollment by the same user.

**Interclass variation** Variation in feature representations of the same modality from different modality.

**Iris recognition** A biometric modality that uses an image of a physical structure of an individual's iris for recognition purposes.

**ISO/IEC** International Organization for Standardization/Internal Electrotechnical Commision, responsible for creating international standards.

**IrisCode** A 512-byte iris template created ny the algorithm designed by John Daugman.

## K

**Keystroke dynamics** A biometric modality that uses the cadence of an individual's typing pattern for recognition.

## L

**Latent fingerprint** These are "leftover" fragments left on a surface that was touched and are usually caused by the buildup of oily residues on a finger.

**Live capture** The process of capturing a biometric sample by an interaction between an end user and a biometric system.

**Liveness detection** A system determination if a collected biometric is presented by a living person for the purpose of thwarting a spoofing attack.

## M

**Match** A decision that a biometric sample and a stored biometric template originates from the same individual, based on the high set of similarity difference.

**Match score** A numeric value associated with a sample template derived from a comparison to a reference template. See also *Similarity score*.

**Matching** See *Comparison*

**Match-on-card** Storing and matching biometrics on smart cards. The smart card has built-in software that matches the template saved on the card against the input biometric image. As such, the template never leaves the secure environment of the smart card, protecting both the biometric information and the user's personal privacy.

**Minutiae** The unique, measurable physical characteristics scanned as input and stored for matching by biometric systems. For fingerprints, minutiae points include the starting and ending points of ridges, bifurcations, and ridge junctions among other features.

**Modality** A type or class of biometric systems, for example, vein pattern recognition or hand geometry.

**Multimodal biometric** A biometric device that uses information from two or more different biometric types, for example, a fingerprint and iris.

## N

**National Institute of Standards and Technology (NIST)** An agency of the U.S. federal government within the U.S. Department of Commerce that establishes standards and guidelines for private and public sector purposes.

**Near infrared** Light that lies outside the human visible spectrum at its low frequency end.

**Noise** Unwanted components in a signal that degrade the quality of data or interfere with the desired signals processed by the system.

**Nonrepudiation** The assurance that the authentication of parties to a transaction is so strong that they cannot later deny (repudiate) that they were the parties to that transaction.

**Normalization** An algorithm that brings dissimilarly scaled matching scores into a common alignment based on the concept of a normal probability distribution.

## O

**Off-line comparison** Process of creating an enrollment template and matching separate from the sample capture.

**On-line comparison** Process of creating an enrollment template and matching during the sample capture.

**One-to-Many (1:N comparison)** The process of comparing an input biometric sample to more than one template. See *Identification*.

**One-to-One (1:1 comparison)** The process of comparing an input biometric sample to only one template. See *Authentication* or *Verification*.

## P

**Palm print recognition** A biometric modality that uses the physical structure of an individual's palm print for recognition purposes.

**Performance criteria** Predetermined criteria established to evaluate the performance of the biometric system under testing.

**Physical/physiological biometric** A biometric that is characterized by a physical characteristic rather than a behavioral trait.

**Presentation** When the user physically presents to the biometric system the data required for capture, such as a finger, hand, or eye.

**Privacy** The assurance that data provided or used in a specific transaction will not be revealed or used by the recipient for purposes not authorized by the provider.

## R

**Receiver operating characteristic (ROC) curve** A method of showing measured accuracy performance of a biometric system by comparing graphically for a verification ROC a false accept rate with a verification rate; an open-set identification (watch list) ROC compares false alarm rates to detection and identification rates.

**Reference template** A biometric template for an individual for future comparisons.

**Ridge endings** Minutiae points at the ending of a fracture ridge.

## S

**Scenario evaluation** Used to measure performance of a biometric system operating in a specific application.

**Score** A number indicating the degree of similarity or correlation of a biometric match. Traditional authentication methods—passwords, PINs, keys, and tokens—are binary, offering only a strict yes/no response. However, biometric systems are based on matching algorithms that generate a probability of a match. This probability is converted to a score that represents the degree of correlation between the verification template and the enrollment template. There is no standard scale used for biometric scoring: for some vendors a scale of 1 to 100 might be used, others might use a scale of –1 to 1. Some vendors may use a logarithmic scale and others a linear scale. Regardless of the scale employed this verification score is compared to the system's threshold to determine how successful the potential biometric match is.

**Security** Protection from intended and unintended breaches that would result in the loss or dissemination of data or damage to the integrity, confidentiality, or authenticity of the system.

**Segmentation** The process of parsing the biometric signal (item) of interest from the entire acquired data set (e.g. iris segmentation).

**Sensor** See *Acquisition device*.

**Similarity score** A value returned by a biometric algorithm that indicates the degree of similarity or correlation between a biometric sample and a biometric reference.

**Smart card** A device that includes an embedded integrated circuit, memory, and a microcontroller. It can be contact based or contactless.

**Soft biometrics** Visual methods for identifying people based on traits that in themselves are not sufficiently distinct but assist in classification of individuals within a database. These traits include gender, eye color, ethnicity, and height.

**Speaker recognition** A biometric modality that uses an individual's speech, a feature that is influenced by both an individual's physical and behavioral characteristics, for recognition purposes. It is also called voice verification.

**Spoofing** The ability to fool a biometric sensor into recognizing an unauthorized user as a legitimate user (verification) or into missing an identification of someone in the database (identification).

## T

**Technology evaluation** Measures the performance of biometric systems in general tasks; typically, it reviews only the recognition algorithm component.

**Template** A digital representation of biometric data; a reference pattern of a person stored for matching. A biometric template can vary in size from 9 bytes for hand geometry to several thousand bytes for facial recognition.

**Threat** An intentional or unintentional potential event that could compromise the security and integrity of a system.

**Threshold** A predefined number or user setting, often controlled by a biometric system administrator, which establishes the minimum degree of correlation necessary for a comparison to be deemed a match. Most thresholds are adjustable to be stricter or less strict.

**Token** A physical device containing individual credentials that an authorized person carries to aid in authentication. Hardware tokens are often small enough to be carried in a pocket or purse. Some may store cryptographic keys, like a digital signature, or biometric template.

**Transaction** The completion of one or more attempts for the purpose of enrollment, verification, or identification.

## U

**Utility** The observed or predicted positive or negative contribution of a biometric sample to overall performance of a biometric sample.

## V

**Verification** It is the process of establishing the validity of a claimed identity by comparing a verification template to an enrollment template. Verification requires that an identity be claimed, after which the individual's enrollment template is located and compared with the verification template. Verification answers the question, "Am I who I claim to be?". It is used interchangeably with *authentification*.

**Vulnerability** The potential for a biometric system to be compromised by intent (e.g., fraudulent activity), by design flaw (including usage errors), by accident, by hardware malfunctions, or external environmental conditions.

## W

**Watch list** Refers to an open-set identification; a term to describe answers to the questions: Is this person in the database? If so, who is he?

**Whorl** A fingerprint pattern in which the ridges are circular or nearly circular.

## Z

**Zero effort imposter attempt** An attempt in which an individual presents his or her own biometric sample for verification against his or her own template, but the comparison is made against another individual's template.

# I Submitted Academic Paper During the Thesis Work

The following academic paper was written and submitted for publication to *The International Conference of the Biometrics Special Interest Group - **BIOSIG 2012*** in Darmstadt, Germany during the thesis work. BIOSIG 2012 is technically co-sponsored by IEEE and papers will be published to IEEE Xplore.

The paper is currently still under review of the committee and the authors hope to benefit from the feedback from the reviewers. It covers an analysis of Norwegian Sport Events including identity management needs.

The website of the conference can be accessed at:

**http://www1.gi-ev.de/fachbereiche/sicherheit/fg/biosig/biosig2012/**

# Evaluation Assurance Criteria in Sport Event Management

S. Yildirim Yayilgan[1], Elham Rajabian[1], Kamer Vishi[1], Asbjørn Hovstø[2]

[1]Department of Information Security
Gjøvik University College
Teknologiveien 22, Gjøvik
sule.yayilgan@hig.no, elham.nogondar@hig.no, kamer.vishi@hig.no

[2]PortAhead
Merkantilveien 2, Gjøvik
hovsto@online.no

**Abstract:** In this paper, we are presenting an analysis for a Norwegian Sport Event, Birken for needs including identity management needs. Our approach to the analysis is to propose an evaluation criteria for assessing the risks and the corresponding needs related to processes, people and technology in the event. We identify risks and corresponding needs not only resulting from vulnerabilities, threats, security holes, and hazards but also from the view point of improvement in technology, logistics and savings related to technology and logistics. Our research on state of the art has shown that there is not such criteria that can evaluate sport events using the three pillars (processes, people and technology) of sport events and that takes into account not only IT-services but services related to other technology and also logistics. We present our assesment results in terms of risks, and the needs.

## 1 Introduction

Major sport event management is a complex process, and in this paper, we will explain the steps we went through in order to analyze a Norwegian sport event for identity management needs as well as needs in general. Consequently we will suggest a methodology for analyzing sport events.

Birken is three annual sporting events comprise a run, ski race and a mountain bike race. It is to honor a historic fact in 1206 about rescuing of the 18 month old prince, **Håkon IV Håkonsson** from rivals in the Norwegian civil war area[1]. The athletes have to carry a weight of 3.5 kg that is equal to the baby weight. The ski and bike race begin in the city of Rena and end in Lillehammer. The length of the race is 56 kilometer. The individuals tend to participate have to enroll themselves through the internet and receive a token for time measuring aim. The athletes typically departure early morning from the starting point and will arrive at the end point a few hours after noon.

[1] http://en.wikipedia.org/wiki/Håkon_Håkonsson

Sport EvEnt iDentity management SPEED is a project funded by regional forskningsfondet, Innlandet and the main goal of the project is to evaluate the use of biometric information combined with RFID technology as a tool for identity management, pre- and post-event travel, Birken enrollment, the athletes/user profiling, housing arrangements, transfer of equipment and belongings (e.g. between Rena and Lillehammer), Individual preference in respect to medication and health risks, special diets, equipment e.g. skiing wax suitable for the weather, reduced interaction and waiting time in queues at enrollment desk and flexible identification at predefined slots in the race (during the ongoing event).

In order to be able to evaluate the use of such a technology, we chose to find out the needs in sport event management first including identity management needs and then we evaluated if there is actually a need for using biometric information combined with RFID technonology. The first big question in finding out the needs is "How to evaluate a sport event for needs" and "what are the existing techniques for such evaluations". It is common to share experiences related to managing sport events, for example what sport event managers are mostly occupied with, what they value the most as skills in sport event management. However, as to our best knowledge, there is not much literature on practices related to finding out the needs in general and identity management needs in particular. For that reason, we had to find out an evaluation technique for finding out the needs. Our results will be useful in future races e.g. Youth Olympics 2016 in Oppland Norway.

In [It08], a list of evaluaton techniques for evaluating IT systems is given. Evaluation has been the traditional means of gaining assurance, and is the basis of ISO/IEC 15408 approach. The list includes the following techniques, but are not limited to:

a) **analysis and checking of process(es) and procedure(s);**
b) checking that process(es) and procedure(s) are being applied;
c) analysis of the correspondence between TOE design representations;
d) analysis of the TOE design representation against the requirements;
e) verification of proofs;
f) analysis of guidance documents;
g) analysis of functional tests developed and the results provided;
h) independent functional testing;
i) **analysis for vulnerabilities (including flaw hypothesis);**
j) penetration testing.

Consequently, we adopted techniques a) and i) in the above list in order to understand the nature of sport event arrangements and for being able to find out the needs in order to provide solutions meeting those needs. It is also important to point out that our evaluation will not only consider IT (Information Technology) systems but also processes and people in sport event arragements, other technology than IT.

Sport event arrangements not only include technology aspect but also has the people and process dimension. As shown in Figure 1, the synergy among people, processes and technology brings out the business capability and is key to business excellence [Ke10]. It

is important to take this synergy into account while evaluating sport events for finding out needs to also ensure business excellence as an outcome of finding out and meeting the needs. As a result, we will not only evaluate the processes but also the people and technology aspects of sport event arragements.


Figure 1: Process, People and Technology Synergy, adopted from [Ju10]

As stated in [Ju10], business leadership is occupied with strategic planning oriented towards customer and market focus. Strategic planning results in a work core where on one hand management of processes is achieved and on the other hand human resources are managed. Consequently business results are obtained. In [Em10], a detailed list of management practices for sport event arragements are given. According to the report, sport event managements are mostly concerned with planning related to financial, marketing, technical, crowd control, master, time, human resources and crisis management issues.

In [Es2012], a list of guidelines is given for arranging safe sport events. Considering all these and the literature and the written experiences we surveyed, our project aims at examining the experiences, processes in the Birken sport races, interviewing involved people for their experiences, needs, and making a risk assessment for use in future sport arrangements in Norway, and an example for international sport event arragements.

In [Up08], it is stated that the basic principle of assessing risks were essentially identify hazards and then evaluate the risks, i.e. the likelihood of the hazard arising and the harm it could cause. In our project, we not only identity hazards and the risk arising subsequently, but also we want to find out the areas of improvement in technology, logistics, savings in order to offer better, preferenced based services. In [Up08], it is also stated that the key to risk assessment is a risk analysis process that considers the phases of arrival and queuing, ingress, attendance, egress and evacuation as separate activities. The potential for accidents during each activity should be acknowledged and the management actions taken to eliminate risk shown. In [Be09], a detailed cover of event management is given, from event models, to event management, strategy making in event managements, to various aspects related to marketing, logistics, financing, health, safety and risk assesment, etc. The book is also very useful in understanding different

phases of event planning. In [Ha08], a risk assessment model for sport venues is presented. According to the report:

"The risk assessment process is a way to determine risk and threat levels and identify vulnerabilities. "A good risk management approach includes three primary elements: a threat assessment, a vulnerability assessment, and a criticality assessment." [De01, p. 1]. These assessments provide vital information for the protection of critical assets against terrorist attacks and other threats. Sport venue managers are able to identify vulnerabilities and thus harden the facility and improve physical protection systems. This may include implementing access controls, using CCTV security cameras, adding lighting, encouraging background checks, credentialing, checking backpacks, enhancing communication networks, and developing or updating emergency response and evacuation plans. "

In this work, a ten-step risk assessment methodology criterion [Of03] issued by the Department of Homeland Security is given as follows:

- Clearly identify the infrastructure sector being assessed.
- Specify the type of security discipline addressed, e.g. physical, information, operations.
- Collect specific data pertaining to each asset.
- Identify critical/key assets to be protected.
- Determine the mission impact of the loss or damage of that asset.
- Conduct a threat analysis and perform assessment for specific assets.
- Perform a vulnerability analysis and assessment to specific threats.
- Conduct analytical risk assessment and determine priorities for each asset.
- Be relatively low cost to train and conduct.
- Make specific, concrete recommendations concerning countermeasures.

[Ha07] identified common vulnerabilities at collegiate sport venues as follows:

- Lack of emergency and evacuation plans specific to sport venue;
- Inadequate searching of venue prior to event;
- Inadequate searches of fans and belongings;
- Concessions not properly secured;
- Dangerous chemicals stored inside the sport venue;
- No accountability for vendors and their vehicles; and
- Inadequate staff training in security awareness and response to Weapons of Mass Destruction (WMD) attacks.

Also, in general risks are identified by a) conducting surveys of attendees, b) conducting inspections of the facility, and c) interviewing present employees, or ask experts in the field as also stated in [Am04].

Our risk assessment is an adaption from [Wh07] to recognize security breaches, threats, risks and hazards. The 7 steps of risk assesment in this paper are Risk identification, Risk Assessment: likelihood, consequence and risk map, Inventorying assets,

Information assets classification, Identifying threats, vulnerabilities and hazards, Risk control and Strategy selection and adapting controls. It is also stated in [Br12; Ta02] that size of crowd, size and nature of event, time of day, nature of event, consumables (food, water, alcohol), age of crowd, weather conditions, location of event venue (urban, rural) are the factors need to be taken in consideration in risk management.

## 2 The Methodology for Risk and Need Management in Birken

In this paper we will examine three main pillars, namely people, technology and processes to have a secured and highly well-quailified sport events while evaluating them for vulnerabilities, corresponding risks, and resulting needs and solutions. Our appoach to finding the eventual needs is summarized as follows:

Evaluate the processes to find out the threats, security holes, hazards and vulnerabilities. Define and use an evaluation criteria for such an evaluation. Then, identify the resulting/corresponding actual risks and the needs (See Table 2 for examples). Evaluate the technology and people separately in the same way (Figure 2).

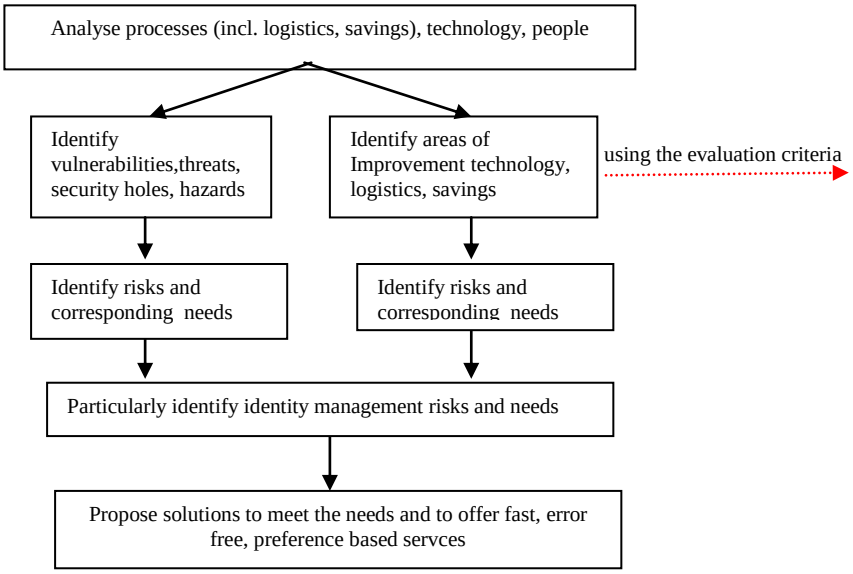



Figure 2: The Overall Methodology for Risk and Need Management

### 2.1 People in Birken

Birken is a associated sport event mostly for regular people, but there are different social social levels that attend to the race by today. The people involved in Birken races are organizers, athletes, spectators, voluntary workers, press, broadcasting company etc. As

a matter of fact, huge number of participants compete against themselves and the others to get to the end point as fast as possible.

### 2.2 Existing Technology in Birken

The technology currently in use in Birken sport event involves broadcasting network for live cameras and media coverage, participant management software that includes two main modules: producing of diplomas and timing control, central database which contains all participants' data, use of wireless technology, RFID for timing aims. Moreover, the latest ski race have taken place in March and has been followed by cameras both on the ground and by helicopter.

### 2.3 Processes in Birken

In order to find out what the required processes in Birken sport event are, first we introduce business objectives for event sports similar to our case study. After that we discuss reuired services and relevant processes to provide the services. The business objectives include:

- Economic purpose: regional economic deployment, impact on the regional outcomes via creating social capital, defining new source of income, etc.
- Social effects: creating social capital, community capacity, improve pubic tendency for terrain-cycling and health effects, optimal emotional and intellectual conditions for athletes, delivering high quality and well-priced social services, entertainment activity, etc.

The needed processes to support high-qualified services for the sport event are defined as follows:

- Compliance to standards and regulations
- Data handling and investigation of data leakage sources and mitigation methods
- Implementation of the best information technology practices and access control
- Recources and information risk management
- Analysis of functional rehearsals

There are five stages in Birken Processes as a result of our analysis of the event. These are pre-event travel arrangements (housing arrangements, SMS services, enrollment), the pre-event travel phase, at the Rena or Lillehammer site phase (luggage delivery to Birken, club controls, distribution of envelops, over-nighting, equipment maintenance, shopping in Rena/Lillehammer, food, interaction with local community, voluntary workers), the day of event/durign event phase (bus transportation from Rena to Lillehammer, transfer of luggage and equipment, racing, parking, race surveillance, ambulance services, diploma, luggage pickup, food), the after event travel phase (transportation to Oslo for flights back to home country, driving back to home city). Some of these process are related to logistics supply-chain.

### 2.4 The proposed evaluation criteria

We need certain criteria in order to evaluate the processes, people and technology pillars of sport events to find out the involved hazards, threats, security holes and vulnerabilities. Below we explain our proposal for 6 point evaluation criteria:

**Coping with Law Suits and reputation:** An organizational structure for sport event management should embody a role which is particularly responsible for complying with law suits. In two of the recent accidents [Tu12; Wc12], improper use of barriers was the cause. Complying with the law suits and revision of the law suits accordingly will decrease the number of accidents.

**Lack of police and security personnel:** Since terrorists follow the motto of mass casualities and mass exposure of humiliation, large scale sporting events provide a potential target for terrorist and violent activity [Ha08]. These are people with legal skills, and are necessary for discouraging from hazardous acts and preventing them.

**Attacks on Information system:** This criteria helps identify attacks against the Information system, e.g. Biometric Systems. The state of information management and information security refers to a well-structured framework for the information systems and information technology to safeguard the information systems. In order to provide the structured we need a clear knowledge about number of information systems, centralized and decentralized databases, backup storage, security controls for the information systems, whether to fit to the business needs, the technical countermeasures employed, expertise of the IT team in case of an security incident, etc.

**Information theft and mis-use – Non-data:** Mis use of athlete behaviour, preferences and interests. Unauthorized people might have access to sensitive information, e.g. unsatisfied staff can capture some sensitive information and share it with others. Such information might include a person's origin, ethnical and religious preferences, disease, which club he belongs to. Other sensitive information can be, in sport event management, atheles' food habits and their interests. It is possible to trace these kind of information, and share with marketing companies for different opportunities.

**Unable to control emergency situations:** There might occur situations that require immediate action in sport event arrangements as in the violence happened in a recent football game in Egypt [Egypt Game]. It should be possible to detect signs of rising emergency situation and there should be emergency plans ready in handling the rising emergency situations.

**Human Errors:** This criteria refers to conditions that a service interruption or information disclosure occur due to immature technology such as mobile systems and unexprienced staff. Human error and accidental incident can be discussed on the same category in the Table 2. The reason is that both are unintentional events. An example for human error is emailing the athletes' sensitive information to wrong receivers. Thus, an information disclosure happens that might raise law suits against the company responsiple for IT services. Athletes and the company's reputation are recognized as assets.

An evaluation using the given criteria will lead to finding out the vulnerabilities, threats, security holes and other areas of hazards such as natural disasters, and the corresponding needs.

### 2.5. Identifying Risks

This part of the paper covers the risk assessment procedure for the sport event project and provides appropriate authentication method and access control mechanisms regarding to the business and sport objectives and to maintaining good reputation for the sponsored organizations. We have used Risk IT framework [Rm10] as risk methodology for risk assessment indicated as "Identify risks and corresponding needs" in Figure 2 which displays our overall methodology for risk management and needs identification.

The risk assessment has been completed based on the objectives in section 2.3 and concentrate on the risk related to information security and incident management. The risk assessment plan consists of information collection and identifying business goals. The sport administrators are risk-averse – meaning that their tolerance for taking risk is low.

In [Hs11], a 5-steps approach to risk assessment in workplaces is given: 1) Identify the hazards, 2) Decide who might be harmed and how, 3) Evaluate the risks and decide on precautions, 4) Record your findings and implement them and 5) Review your assessment and update if necessary. In [Hs11], a hazard is defined as anything that may cause harm, such as chemicals, electricity, working from ladders, an open drawer, etc. in an office environment. In our approach, we extend hazards, to threats, security holes and vulnerabilities as shown in Figure 2. In [Hs11], the risk is defined as the chance, high or low, that somebody could be harmed by these and other hazards, together with an indication of how serious the harm could be.

In addition to the earlier mentioned risk analysis scope, we also consider risks and vulnerabilities due to other reasons, namely natural disasters, law suits, information theft for generating marketing opportunities, terrorism, hostage taking, etc. Using a similar approach, our first step is related to identifying the hazards, threats, security holes and vulnerabilities as shown in Figure 2. Our next step is to identify the resulting risks. Step1 of [Br12], which is identifying risks cover step1, step2, and step3 of the above list from [Hs11].

There are terms often used in the risk management frameworks consist of threat[2], event[3], asset, actor and risk level. We have defined the first three terms because those will be helpful to generalize to the similar case studies. The actor and risk level can assist the management committee of Biken which is avaiable in the risk analysis report for the

[2] Threat is a adversary action that results to a harm e.g. a virus infection, malware and illegal network penetration.

[3] The effect of occurring a risk. Where risk is the expection of a threat to be succeed and the potential harms that may happen.

management committe. We have considered two main risk factors based on the ISACA framework. These factors effect on the frequency and/or business influence of risk category/risk scenarios.

Table 1 illustrates the risk categories based on the six evaluation criteria for the Birken sport event. There are eight main risk events that threat the information assets, people, resources, sport equipments and infrastructure. The last column has been adapted from our six evaluation criteria, introduced earlier. The risk category in the table corresponds to the actual threats, vulnerabilities, security holes and hazards which have been identified for Birken by evaluating the three pillars using the six evaluation criteria [Is10].

### 2.6. Identifying Needs: Resulting from the Risk Category

The needs related to improving logistics, technology and savings and some of the needs resulting from risks related to the Law suits and emergency situation criteria fall under non-identity management needs. Others are, identity management needs which do require identity management solutions (Table 2).

## 3 Discussion and conclusions

In this paper, we proposed a methodology for identifying needs in sport event arragements. The methodology is given in Figure 2 and the evaluation of processes, technology and people are done using a 6 point evaluation criteria. This way we were able to capture and classify the needs particularly for Birken races, Norway. Table 1 presents a sample set of risk categories associated with the Birken event. Table 2 presents corresponding needs related to various risk categories.

The needs identified can be generalized into appropraite services for Birken sport event which encompass the points below but not limited to:

- Provide in an uninterrupted and continuous way, the sport event and social services such as public transportation, ticketing, media coverage, crowd control, portable facilities such as showers and changing cabins, food at the cantine, health supervision, first aid, event insurance; addresing financial issues, provide a safe sport event for the athletes and spectators by protecting the participants against violent activities, against unauthorized access to the athletes' sensitive and health information in terms of availability, confidentiality and integrity; provide technical error reduction, data leakage prevention, data handling, privacy and regulation compliance.
- Have a modern and up-to date administration using registration services, issuing (identity) ID cards, using timing control by use of RFID technology, involving event and crisis management, risk contingency planning and risk response.
- Emergency preparation from first aid and medicine team to high quality health care services like ambulance and helicopter.

Table1. A sample set of risk categories associated with the Birken event

| Risk Category | Threat Type | Event | Asset/Resource | EC |
|---|---|---|---|---|
| 1. Natural disaster: snow avalanche | Nature, external | Destruction(loss of availability) Interruption(loss of availability) | Infrastructure, information and people | Emergency situation |
| 2. Physical loss of the luggage | 2.1:Accidental/ human error 2.2: Malicious | Rules and regulations, Inappropriate use of fences, might interruption in the event sport process. | Sport equipments, information | Reputation |
| 3.Accidental risk e.g. not proper crowd control or inapporopraite fencing cause the athlete hit fence | Accidental, athletes error/ External requirement[4] | Rules and regulations, Inappropriate use of fences, might interruption in the event sport process. | People (spectators, athletes), reputation of the sponsored organizations. | Law Suits, Emergency situation |
| 4.Technological Incident<br><br>4.1 e.g, the mobile network capacity: failure<br><br>4.2 e.g. phishing attack | 4.1Accidental/human error | Interruption (availability, integrity), Disclosure sensitive information(confidentiality), Ineffective execution[5] (availability, integrity), Rules and regulations (confidentiality | People(athletes and staff information) and organization | Information System |
| | 4.2Malicious | Disclosure (confidentiality), Theft (identity, confidentiality), Destruction(availability, integrity) | People and organization, information, applications | Information Theft and misuse |
| 5. Smoldering incident e.g. lack of up to date anti virus | Failure | Disclosure (confidentiality), Theft (identity, confidentiality, integrity), Modification (malware, confidentiality, integrity) | Applications, People and organization (IT staff, spectators and athletes) | Information Theft and misuse |
| 6.Staff misconduct/data leakage e.g. an unsatified employee or a staff sells the athletes data to third party companies | Malicious | Disclosure (confidentiality), Destruction(availability, integrity), Modification (integrity), Rules and regulations (confidentiality, integrity) | People and organization( reputation), information, applications | Information Theft and misuse |
| 7.End point devices: Databases, PCs, USPs, external hards, etc. | 7.1Accidental | Disclosure (confidentiality), Rules and regulations (confidentiality) | Information, IT infrastructure, process: technology(bad use of implemented technology) | Information Theft and misuse, Law Suits |
| | 7.2Malicious | Ineffective IT design, disclosure, identity theft, information destruction, regulation | Information, IT infrastructure | Information System |
| 8. Radical and violent actions e.g. terrorist activities, hostage and kidnapping | Malicious | Interruption, destruction | People life and organization destruction | Lacking security personnel |

[4]E.g. first aid and medicine services.
[5] E.g. low capacity of the mobile network

Table 2. Risk Category and Corresponding Needs

| **Risk Category:** ***(Hazard, Vulnerability, Threat, Security Hole)*** | **NEEDS FOR** | **Evaluation Criteria** |
|---|---|---|
| Not being able to meet athlete preferences | offering the food and drink of preference to the athlete when the athlete asks for it. Now the approach is to tell the athlete that a certain kind of food can only be offered at the next rest point e.g. in 6 km but not at the current rest point. | Law Suit |
| 8. Radical and violent actions | crowd management in case of violence in sport events | Lack of Security Personnel |
| Accidents | in the organizational structure of Birken, it should be made clear whom/which role is responsible for sport accidents which have law dimension | Law Suits |
| 4.Technological Incident -- malicious | protecting the security and the safety of the information system. | Information System |
| 6.Staff misconduct/data leakage | protecting the athlete specific information | Information theft and mis-use |
| 3.Accidental risk | storing the personal identification number<br><br>identity management for Health using Wrist bands | Emergency Situation |
| Pick up wrong equip. | athetes to pickup own bike/ski at the repair butique | Reputation |
| 2. Physical loss of the luggage / exchnage of wrong luggegage | identity management for picking up the right luggage | Reputation |
| Antidoping | for detecting antidoping by using biometrics | Law Suits |
| persons racing in other people's name: picking up wrong envelop. | identity Management | Law Suits, Human Errors |
| Losing hotel door keys | RFID cards, cell phones, wrist bands for door access | Human Errors |
| Entering busses without tickets, failures in parking lot access | identity management for Transportation and for Parking lot access. Families and athletes, press park in different areas | Human Errors, Law Suits |
| Managing lot of cards, losing cards | using multi-purpose cards e.g. visa cards, or Birken card for payments, door access, other id management. | Human Errors |
| Hacking biometric profiles, personal identification numner | storing biometric profiles, re-use them, and this information is not hacked (authentication). | Information System |

## References


[Is10] ISACA, Risk IT Framework for Management of IT Related Business Risks, 2010

[IT08] Text of ISO/IEC FDIS 15408-3 -- Information technology --Security techniques -- Evaluation criteria for IT security - Part 3: Security assurance components

[Em10] Emery, P. Past, present, future major sport event management practice: The practitioner perspective, Sport Management Review, 2010.

[Egypt Game] http://www.guardian.co.uk/world/2012/feb/01/egypt-football-match-violence-dead

[ES12] Event Safety Plan, Risk Assessment and Management, http://www.sport.ox.ac.uk/sports-federation/safety/events-safety-plan-and-risk-assessment, last read 04.05.12

[Up08] Upton, M. Safe Event Management, Theatre Managers Association Conference Birmingham 10th June 2008

[Be09] Beloviene, A. et. Al. Event Management Handbook

[Ha08] Hall, S., Marciani, L., & Cooper, W.E, & Rolen, R., Introducing a Risk Assessment Model for Sport Venues, The Sport Journal, ISSN: 1543-9518 http://www.thesportjournal.org/article/introducing-risk-assessment-model-sport-venues

[De01] Decker, R.J. (2001). Key elements of a risk management approach. United States General Accounting Office. [On-line]. Available: http://www.gao.gov/new.items/d02150t.pdf

[Am04] Ammon, R., Southall, R. & Blair, D. (2004). Sport facility management: Organizing events and mitigating risks. Morgantown, WV: Fitness Information Technology, Inc.

[Ta02] Tarlow, P. E., Event Risk Management and Safety, John Wiley & Sons, 1. aug. 2002

[Br12] Brown, S. Risk Management of Events – Sport Event Management, Lecture Notes, last read 04.05.2012

[Of03] Office of Domestic Preparedness, U.S. Department of Homeland Security, Vulnerability Assessment Report. (July, 2003).. Retrieved May 7, 2012, from http://purl.access.gpo.gov/GPO/LPS53545

[Ha07] Hall, S., Marciani, L., & Cooper, W.E, & Rolen, R. (2007, August). Securing sport stadiums in the 21st century: Think security, enhance safety. Homeland Security Institute: Journal of Homeland Security. Retrieved from http://www.homelandsecurity.org/newjournal/Articles/displayArticle2.asp?article=162.

[Hs11] HSE, Five Steps to Risk Assessment, Health and Safety Executive, 2011

[Wh07] Michael Whitman and Herbert Mattord, Principles of Incident Response and Disatster Recovery. Thomson, 2007.

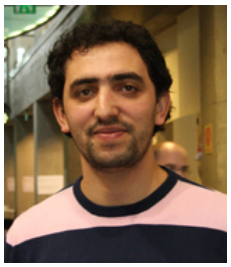
[Ju10] Joint Universities Computer Centre Limited (JUCC), Information Security Updates Data Leakage Prevention, 2010.

[Rm10] RISK MANAGEMENT GUIDE FOR COMMUNITY SPORT ORGANIZATIONS, 2010

[Tu12] http://www.hurriyetdailynews.com/turkish-national-skier-dies-in-training-accident--.aspx?pageID=238&nID=11317&NewsCatID=371

[Wc12] Nick Zoricic Dead: Ski Racer Dies During Skicross Crash In World Cup Event

# About the Author



**Kamer H. Vishi** is a master student in Information Security, Department of Computer Science and Media Technology, Gjøvik University College, Norway. Furthermore, he is currently engaged as *technology manager* in SPEED project (project number *ES 477262 RFF*) funded by Regionale Forsknings Fond (RFF) Innlandet. He received two BSc. (Honours) one in Computer and Electrical Engineering - 2008, thesis titled "*Skype Secuirty, analyzing the security level of communication protocol (MSN vs. Skype)*" and the other BSc. in Management and Informatics - 2009, thesis titled "*Managing the Computer Networks in Large-Scale Companies*".

Kamer has more than 8 years of working experience in web & software development, wireless communication security, network security and internet security certified by CISCO Networking Academy. His working experiences include research, design and development of many web application for government, secure information systems, and project management. His current research interests include: *identity management*, *biometrics*, *cryptography*, *cryptanalysis*, *ethical hacking*, *wireless communication security* and innovation concepts such as *Near Field Communication (NFC)*, *Cloud Computing* etc.

URL: `http://www.stud.hig.no/~091340/web/`

Media Coverage (article published on HiG's website):
`http://www.hig.no/nyheter/biometri`