NTNU

Norwegian University of
Science and Technology

Biometric Solutions for Personal Identification

Tormod Emsell Larsen

Master of Science in Communication Technology

Submission date:	May 2008
Supervisor:	Svein Johan Knapskog, ITEM
Co-supervisor:	Danilo Gligoroski, ITEM

Norwegian University of Science and Technology
Department of Telematics

Problem Description

Establishing identity is becoming critical in the today's highly interconnected society and foolproof secure authentication solutions are desired. Biometrics, described as the science of recognizing individuals based on physical and behavioral traits, is gaining more popularity and acceptance as a legitimate method for determining identities. Some biometric methods are quite mature and considered reliable, while research on new and novel methods, which could be able to substitute or assist existing methods, is ongoing.

The student will have to give a broad picture of the biometric technology today and related issues and challenges. In addition, one novel type of biometrics shall be elaborated in detail and its potential shall be explored.

Assignment given: 15. January 2008
Supervisor: Svein Johan Knapskog, ITEM

Preface

This thesis is written by Tormod Emsell Larsen, a student in the 10th and last semester of the Master's program in Communication Technology at the Norwegian University of Science and Technology (NTNU). It marks off the end of his specialization within the field of information security and the Master's degree.

The thesis was written during the spring semester of 2008 under the supervision of professor Svein Knapskog who deserves acknowledgement for his help and motivation throughout the whole semester. I am also very thankful to my co-supervisor, post doctor Danilo Gligoroski, for his useful input and ideas on the topic. I thank Steinar Watne and Patrick Bours from Gjøvik University College, who have worked on the same topic as me, for great discussions and exchange of ideas.

I would like to express my gratitude to Aage Aune from Omega Termografering NE A/S for providing me an infrared camera and helping me with the data collection for my experiment. I also thank the camera distributor Presisjons Teknikk A/S who helped me with the image analyzing software.

Without the 14 volunteers constituting the test personnel, the experiment would not have been feasible, so thank you very much!

Trondheim, May 2008
Tormod Emsell Larsen

Abstract

With a high level of accuracy and ease of use, the technology of biometrics has the recent years gained popularity and in many cases replaced traditional identification methods based on passwords or tokens. While fingerprint matching is the most mature and most widely used technique of today, several others exist. Among these is ear recognition, which so far has received scant attention, but still has showed good results in performance. The thesis gives a general presentation of the biometric technology, with its advantages and challenges. In addition, the new and novel technology of ear recognition using thermal imagery is elaborated and discussed. An experiment of small scale, aiming to test the ability of thermal ear recognition as a method for identification, was performed. The test also considers the affect on the performance when the ear temperature varies. An EER of 20.7 % with a corresponding detection rate of 78 % was achieved when considering only ears with the same temperature. By including the applied temperature changes, an increase in the EER to 31.5 % with a corresponding detection rate of 72 % was observed. The results indicate that thermal images of the ears are not sufficiently distinguishable for use in establishing identity by itself, but it might be suitable as a supplement to other biometric techniques.

Contents

Abbreviations

2D	2-dimensional
3D	3-dimensional
AFIS	Automated Fingerprint Identification System
DNA	Deoxyribonucleic Acid
EER	Equal Error Rate
FAR	False Acceptance Rate
FBI	Federal Bureau of Investigation
FRR	False Rejection Rate
ICA	Independent Component Analysis
ID	Identification
IR	Infrared
LDA	Linear Discriminant Analysis
LFA	Local Feature Analysis
LWIR	Long-wave Infrared
MWIR	Mid-wave Infrared
NTNU	Norwegian University of Science and Technology
PCA	Principal Components Analysis
PIN	Personal Identification Number

List of Figures

List of Tables

Chapter 1

Introduction

The term *biometric* is derived from the Greek words *bios* and *metros*, meaning life and measure. Hence it refers to the measurement of life and is the study of recognizing the identity of a person based on physical and behavioral characteristics. Examples are fingerprints, hand geometry, iris, retina and voice.

The first known use of biometrics goes back to the 14th century where the Chinese merchants were stamping the children's palm prints and footprints to be able to distinguish the children from each other. In the 1880's the French police officer Alphonse Bertillon used body measurements, such as length and breadth of head and ear, length of fingers and feet and so on, to identify criminals. The system was quickly adopted by American and British police forces, but it was later discarded as it was discovered that several people could have the same measurements and that the characteristics could also change over time. It was then shortly after replaced by fingerprint identification, which is still being used by the police worldwide today. [24] [18]

Biometrics is suitable within a variety of fields and applications. Its use in the forensics dates back to the turn of the 20th century where it has been used for tasks as corpse identification, criminal investigation, terrorist identification and missing children, but it has not always been a part of an automated system as exists today. Government, which traditionally has relied on token-based identification (e.g. ID-cards) has now extended the use to include biometric applications in combination with national ID cards, driver's license, border and passport control. Also the commercial actors have recently entered the field of biometrics and developed applications for computer login, electronic data security, ATM authentication, physical access control, medical records management and the like. An industry report performed by International Biometric Group shows that the total biometric revenues are expected to grow in the next years, as illustrated in Figure 1.1.

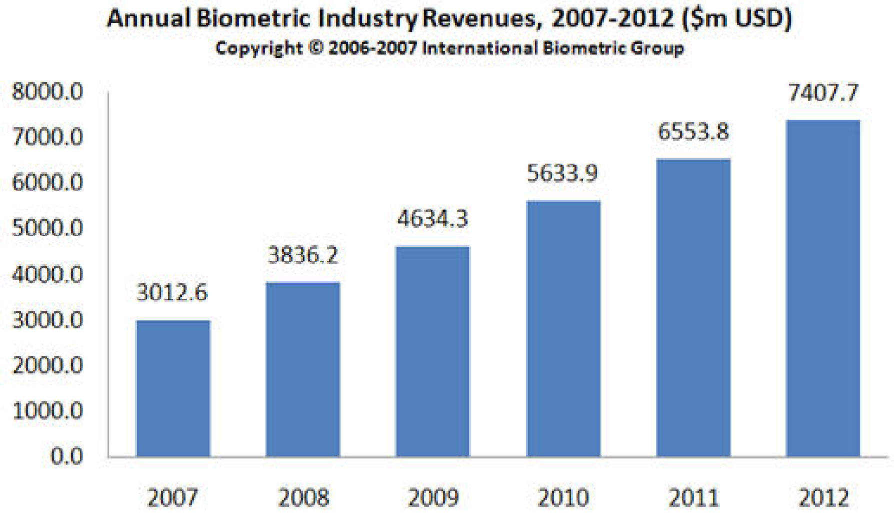

Figure 1.1: Biometric Revenues from 2007-20012, reported by International Biometric Group's "Biometrics Market and Industry Report 2007-2012" [10]

Even though fingerprinting is the most used and mature biometric technique today, other techniques are also being implemented and the research is proceeding. As an example, at the Pictet and Cie Swiss bank in Geneva, registered employees need only look at the camera on the security turnstiles to be allowed into the building. The authentication is done by face recognition at the entrance and iris scanning for access to the inner high security areas of the bank.

After the tragedy of 9/11 in the United States, the field of biometrics has been given more attention and become a part of the airport security, especially in the United States. Under their new border control system, foreigners entering the United States on visas, must have their two index fingers scanned and digital photographs taken.

1.1 Background and Motivation

In the search for better security solutions and authentication techniques, the use of biometrics as a means to establish identity has been considered a good candidate with much potential. By complementing the existing authentication methods, using a password or a personal token, with unique characteristics of the individual, the level of security is enhanced. This, in addition to the increased convenience, makes biometrics a promising technique for authentication in the future.

Many different techniques, using different characteristics of the human body or behavior, have been suggested. Some techniques have achieved much attention and successfully been implemented in security solutions worldwide while others, newer and less explored, still requires much remaining research. Face recognition is one of these newer discussed techniques which has proved to give good results [45]. Another, even newer and less explored technique is ear recognition. It resembles face recognition in several ways, in that it is non-intrusive, measured with similar devices and similar data processing. Hygienic concerns, as implied by fingerprints, are not present and there is no fear of being exposed to techniques dangerous to your body (as many falsely believe iris and retina scan is). Therefore, there should be reason to give more attention to this field, as the author believes it could be a biometric of the future.

As thermal imagery can give liveness to the captured data as well as eliminate several problems observed with visual cameras, there is reason to examine the use of it further. The promising results from thermal face recognition, [45], support the use also in ear recognition.

1.2 Scope

The report will first give a broad presentation of biometrics. Both its different techniques and related issues and challenges will be enlightened. Then one specific type of biometric will be presented, namely thermal infrared ear recognition. Tests will be performed to evaluate the possibilities for using thermal infrared images for ear recognition, but because of the amount of available resources, the test will be of a small scale. The type of experiment can be characterized as a feasibility study with the purpose and aim to indicate the suitability of the technique.

For the comparison of ears, a general image recognition tool will be used, not designed specially for recognizing ears due to limited capacity in time and resources. The main purpose is to state whether the images taken are unique enough to make them distinguishable and not to evaluate any recognition algorithm.

1.3 Related Work and Contributions

A vast amount of articles exist on the topic of biometrics, but there is also a vast amount of fields of interests within the biometrics. Related work to ear recognition is presented in Chapter 4.

A major part of this report will focus on ear recognition, in which the amount of already published work is limited. The report will further look into the special case of thermal infrared ear recognition, which has received very little attention so far. This report will present tests performed using a thermal infrared camera and indicate the suitability of this for the purpose of establishing identity. There is no published material on this specific topic as far as the author knows, but its promising potential is mentioned briefly in [5]. Hopefully, the report will contribute in making ear recognition a topic for further discussion and producing results that are of interest for future research.

1.4 Methodology

To answer the problem description, the research methodology needed to be two-sided. The first part consisted of presenting the biometric technology of today and required a broad literature study. For this, books about biometrics gathering many kinds of biometrics including related issues and aspects, were used as well as single topic specific papers.

In the other part, one specific type of biometric technique was to be chosen and explored. For this an experimental type of research was conducted.

1.5 Report Outline

Chapter 2

Chapter 2 follows with theoretical background and a presentation of biometric system types and solutions.

Chapter 3

Chapter 3 gives a presentation of privacy and security issues related to the use of biometrics.

Chapter 4

Chapter 4 presents the specific type of ear used as a biometric. Solutions and previous work in this field are presented as well as related advantages and problems.

Chapter 5

The special case of thermal ear recognition is treated in Chapter 5 and advantages and challenges are covered.

Chapter 6

Chapter 6 presents a test performed on thermal ear recognition.

Chapter 7

Ear recognition technology and the test results will be discussed in Chapter 7.

Chapter 8

Chapter 8 concludes the work.

Chapter 2

Biometrics: Overview

Biometrics used as an authentication scheme has been more widespread and gained more popularity the recent years, along with the increased funds given to research and development [44]. Authentication is the process of verifying the identity of an individual and is traditionally done using either a token, a password or both. These techniques guarantee that the person authenticating either is in the possession of the token or know the password, but they cannot actually guarantee for the identity of the person. Tokens can be stolen and passwords can be compromised. This can be improved using biometrics, which constitutes the last type of authentication. The three methods of authentication can hence be classified as:

- What you know (i.e. passwords)
- What you have (i.e. tokens, cards)
- What you are (i.e. fingerprint)

Using the physical and behavioral characteristics requires the person to be present at the time and point of authentication. It is difficult to forge biometrics and it requires more effort, time and money [15]. To enhance the security further and to complicate the possibilities of forgery, the three types can also be combined.

Today, biometrics is not only used as a system for verification, but also for identification. While a verification system conducts a one-to-one (1:1) comparison to determine whether the identity claimed by an individual is true, an identification system conducts a one-to-many (1:N) comparison to establish the identity of an individual. The first is used as an authentication technique in various applications today and it is by many predicted an increased use in the future.

For any characteristic to be used as a biometric identifier it needs to satisfy the following requirements, according to Jain et al. [14]:

- Universality: Each person should have the characteristic.
- Distinctiveness: The characteristics of two different people should be sufficiently different.
- Permanence: The characteristic should be sufficiently invariant over a period of time.
- Collectability: The characteristic should be quantitatively measurable.

When biometrics is used in a practical enterprise system, such as an authentication system, other features should also be considered:

- Performance: The recognition accuracy and speed.
- Acceptability: The extent to which people are willing to accept the use of the characteristic as a biometric identifier in their daily lives.
- Circumvention: The hardness of fooling the system using fraudulent methods.

2.1 Why use Biometrics?

Today there exist methods for identifying an individual that have been used for a long time. A very common means for identification is an ID-card and for automated systems this is often combined with a password or a code to verify the identity. So why should we include biometrics?

There are weaknesses of the existing methods using tokens or passwords as already mentioned. They are vulnerable against stealing and forgery and they can be forgotten and lost. Biometrics can eliminate or reduce these vulnerabilities and can also provide for additional benefits. For example, in an enterprise authentication system, both the employer and the employees will benefit. The employer can eliminate the work with password maintenance and buddy punching (since the employee has to be there in person), which will lead to reduced costs. The security can be improved if using the right biometrics in the right way reducing the vulnerabilities mentioned above. The login for the employees becomes more convenient as they do not need to remember a password and the login can be done faster.

2.2 How a Biometric System Works

Even though there are many different kinds of biometrics, most biometric authentication systems work in the same way seen at a high system level. Firstly, the system can be divided in two parts consisting of the enrollment phase and the verification phase. During the enrollment phase the user presents the biometric to a sensor. The raw biometric data gets captured and the relevant features are extracted. A quality check is conducted before the data is being further processed and the signature is generated. The resulting record, or template, is then securely stored for future matching. The user is then registered and can use the system for verification. The verification phase is almost the same except that the biometric features are matched against the previously recorded template to determine whether access should be granted and the quality check is then implicitly present.

When the two records are compared, a level of similarity is determined which indicates the probability that the samples came from the same person. This is represented by a matching score and the user is given access if he or she has a score above a certain preset threshold.

2.2.1 Components in a Biometric System

The elements included in a biometric system is illustrated in Figure 2.1 and described below.

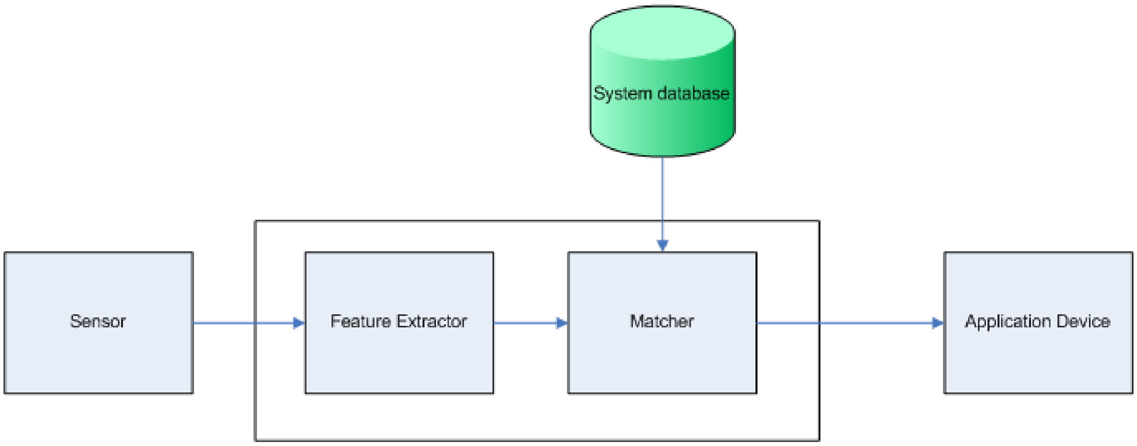

Figure 2.1: Elements of a Biometric System

Sensor

The sensor is the device capturing the biometric data of an individual. Different systems use different devices to get the samples. Examples are fingerprint scanner, voice recorder, on-line writing board, camera for face recognition and retinal scanner.

Feature Extractor

In the feature extraction module, the captured biometric data is processed to extract a set of distinguishable features. For fingerprints, the key parameters defining the fingerprint pattern are used, such as ridge positions and orientations. A template is created which should be different for any two persons.

Two approaches are being used. The first uses some meaningful sole features which are predefined and proved. The features are extracted and changed into mathematical code. The second approach is used when no meaningful sample is found. The sample is transformed into another dimension and the noise is then levered to get a refined sample and the overall data quantity is decreased. After tests it is proved and can be used as a template. [44]

Matcher

The matcher module compares the extracted features with the features from the registered template to generate matching scores. The matching scores are being used for the decision of whether the person is who he claims to be. Samples from the same person may also vary, so the comparison algorithm should tolerate these tiny variations from the same person yet distinguish different people. [16]

In an identification system, the new template is compared to all registered templates in the system, while in a verification system the new template is only compared to a particular registered template. There is also another variation of identification, referred to as negative identification or screening, where it should be determined whether the feature is in some negative database. That could for instant be a ”most wanted” database containing terrorists. [3]

System Database

The system database is where the biometric templates of the enrolled users are stored. It could be a central database or several distributed databases of the biometric system or the templates can simply be stored on a smart card issued to the user.

2.3 Types of Biometrics

Biometrics can be divided into two main types; physical and behavioral biometrics. The physical features of a person are related to the shape and characteristics of the body such as fingerprints, iris and hand geometry. The behavioral features relate to how or in which manner a person acts, for example voice, signature and gait. Some features can be both physical and behavioral. Each person's voice has a different pitch, making it a physical characteristic, but voice recognition is mainly based on the study of the way a person speaks, making it behavioral. While the fingerprint technology is the most mature and most used biometric technology of today, the Biometrics Market and Industry Report 2007-2012 performed by International Biometric Group, shows that some of the other techniques are catching up (see Figure 2.2). The following will present instances of both physical and behavioral biometrics. Figure 2.3.1 illustrates some of the biometric techniques.

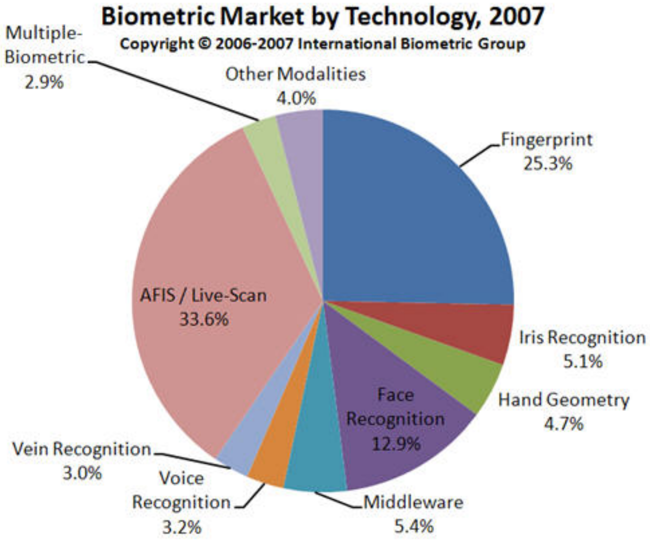

Figure 2.2: Comparative biometrics market share, reported by International Biometric Group's "Biometrics Market and Industry Report 2007-2012"

2.3.1 Physical Features

Fingerprints

Fingerprint identification is the most mature and most widely used type of biological identification technique. By measuring patterns on the fingertips, one can identify a person because of the uniqueness of the fingertip. The pattern is made up by friction ridges which every person has on the palms, the fingers, the soles and the toes. The technique analyzes small unique marks made up of the ridges, called minutiae. The relative positions of these are used for comparison. While fingerprint identification mostly has been associated with the field of forensics, there is now a tendency of increased use in civilian applications as well. [24]

Hand Geometry

Features related to the hand are relatively peculiar to a person. The shape and length of fingers and the knuckles are measured. The problem of hand geometry identification is the limited distinctiveness and is therefore normally not used for identification, but only verification, and often in combination with other identification techniques. An advantage is the small template size, which is only 9 bytes [17].

Retina Scanning

The retina is located at the posterior portion of the eye. The capillaries that supply the retina with blood have a very complex structure and make the retina unique and suitable for identification. The scanning process is performed using a low intensity light through a coupler to scan to unique pattern of the retina. It is the most accurate and reliable known biological identification technique today. The drawback is that the user needs to look into a receptacle, focus on a given point and remove glasses which decreases the convenience. [17]

Iris Scanning

The iris is the colored ring of tissue surrounding the pupil and is distinctive for each person and each eye. An iris scan analyzes the visual texture of the iris by making an image using a camera element. It does not require close contact with the user and it works with persons wearing glasses. [18]

Face Recognition

Facial characteristics may be the most common way of recognizing people in the daily life and is therefore also one of the most accepted forms of biometrics. A photo of your face in combination with your signature is common on todays identification cards. The difference when used in biometrics is the automated fashion in which the recognition is done, with algorithms extracting the face characteristics and comparing them to the template. There exists 3D facial scanning as well. This is considered more accurate, but it requires more advanced equipment as for instant a range camera, increasing the expenses. Also thermal face recognition, where infrared images are used, have recently received focus. [18]

DNA

Every cell in the human body contains a copy of the DNA (Deoxyribonucleic acid), which carries the genetic information necessary for the organization and structuring of most living cells and control the inheritance of characteristics. A small part of the entire genome, about 0.1 percent, is unique to each individual.

DNA signatures, used for recognition in the forensics, have proved that people can be identified with very high accuracy. The problems when using DNA in other applications such as authentication systems is that there is no automated process of analyzing the DNA and comparing them. A lot of time and resources are required for sequencing and processing, even though research indicates that this can be done real time with future technology [36]. Due to this, many say that it can not be considered a biometric technology. As opposed to the other known biometrics, DNA biometrics actually needs a physical sample from the person, which could be for example a single hair. [17]

Vascular Patterns

Researchers have determined that the vascular pattern of the human body is unique and does not change over time. By using near infrared light, reflected images of blood vessels from hands and fingers are derived and can be used for recognition. [18]

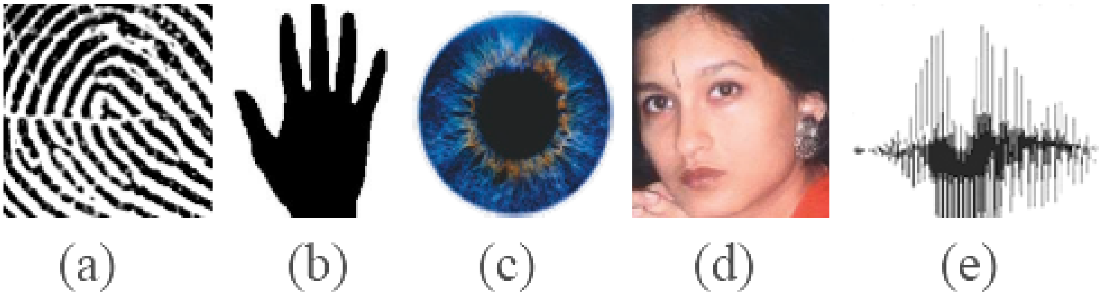

Figure 2.3: Biometrics Technologies: (a) Fingerprint, (b) Hand Geometry, (c) Iris Scanning, (d) Face Recognition, (e) Voice Recognition. Images found in [29].

2.3.2 Behavioral Features

Voice Recognition

The features of a person's voice are based on the shape and size of factors such as vocal tracts, mouth, lips and nasal cavities, which are used in the synthesis of the sound. These physiological characteristics do not change over time, but the behavioral part of the speech varies as a cause of aging, medical conditions and emotional state. So the voice is a combination of both physiological and behavioral biometric.

There are two types of voice recognition, text-independent and text-dependent. The text-independent recognition is based on recognizing the speaker independent of what he or she speaks. This system is more complex than the text-dependent which is based on the utterance of a fixed predetermined phrase. [16]

Signature

Signatures have been used as identification since ancient times and are commonly used on credit cards and ID-cards as a form of authentication. In later years the signature verification technology has evolved and there are systems that not only examine the static shape of the signature, off-line verification, but also include behavioral characteristics, on-line verification, such as speed, acceleration, deceleration, pen pressure and position trajectory. [18]

As people are used to signatures as means of transaction related verification, the acceptance level of signatures used as biometrics is high. The signature can be influenced by emotional states and can change over time, which can affect the error rate. [15]

Keystroke

Keystroke biometrics is based on recognizing habitual and unique patterns in the typing rhythm of a computer user. Features such as latencies between successive keystrokes, keystroke durations, finger placement and pressure on the keys may be used to construct a personal and unique signature of a user [6]. This type of biometric permits ”continuous verification” over a session after the person has logged in using another, stronger authentication, but can also be used to enhance a password based authentication system.

Gait Recognition

As a new probing research field, gait recognition has recently gained many research results. It utilizes the manner in which a person walks for identification. It is one of the few biometrics that can be used at a distance and is therefore suitable for surveillance scenarios, for instant at an airport.

One of the challenges is to find motion patterns that are sufficiently distinguishable that can be extracted reliably and consistently from video. Several factors, both psychological and physiological, can lead to failure of recognition such as footwear, clothing, surface of walking, mood, illness and fatigue. [42]

2.3.3 Future Features

The human body has an enormous number of details and characteristics that could have good potential for biometric use. Despite that most of the visible and audible traits have already been explored, the research is still going on. There are many technologies which are in the research phase and not ready for commercial implementation. Among these are for instant ear recognition, where characteristics and shape of the ear are measured, and body odor that is based on measurements of the odor and analyses of the chemical pattern.

2.3.4 AFIS and Live Scan

Fingerprint databases used in the forensic field grew so large that manual fingerprint identification became infeasible to handle. Databases with a number of fingerprint cards exceeding 200 million, as the case of the FBI fingerprint database, require unreasonable many fingerprint experts to examine all the fingerprint requests each day in a reasonable amount of time [18]. With the introduction of the computer technology a solution to the challenge was developed. It was in the late sixties the first efforts to digitize and automatically process fingerprint images were made and formed the basis of the modern Automated Fingerprint Identification System (AFIS). It is a system used for automatically matching of fingerprints against a database of prints, with the help of computerized power. The system provides a list of best candidates and leaves the final identification to an expert.

The AFIS obtains the fingerprints with the help of live scan devices which replaces the process of recording the fingerprint patterns using ink. Digitizing the fingerprints make it possible to electronically send and compare fingerprints to databases located elsewhere in a short time.

AFIS was initially used mainly in criminal investigations and today almost all law enforcement agencies use it. Now, the use of AFIS has grown also into civilian applications in addition to the forensic use.

Chapter 3

Privacy and Security Issues in Biometrics

With powerful computer resources as we have today, great amounts of digital information can be processed and lead to greater efficiency than could have been performed manually by humans. This is one of the factors making security systems of today as efficient as they are. With the introduction of biometrics, it can for instant be possible to apply face recognition identification systems for use in surveillance. Such a possibility can improve police work in their search for criminals and makes places more secure, but on the other hand it implies collection of unique (or nearly unique) information about individuals without their knowledge nor consent. It degrades the level of personal privacy. This introduces the importance of privacy versus security. Which is more important and in which situations?

3.1 Privacy Aspects

It is claimed that privacy is enhanced by biometrics in the way that your personal information is protected by strong biometric mechanisms which are almost impossible to bypass by attackers. But seen from another perspective, the privacy is degraded because of the biometric technology.

The term privacy comprises the ability to live your life free of intrusions, to remain autonomous, and to control access to your personal information [29]. As computer science has evolved and the extensive use of large databases in a more and more interconnected world has increased, the personal privacy is getting an important factor to preserve.

Concerns related to privacy regarding biometrics can be divided into physical privacy and informational privacy.

3.1.1 Physical Privacy

Physical privacy is the ability to have spatial seclusion and solitude. Biometrics can interfere with this in two ways [40]:

- The use of biometrics can have an effect of stigmatization as for instant fingerprints which can be associated with criminals.
- Biometrics can cause hygienic concerns. This regards only the biometric types where physical contact is required.

There is also a segment of the population for whom the use of biometric technology is inherently offensive, distasteful, invasive or embarrassing. This may be due to a variety of cultural, religious, or personal beliefs.

3.1.2 Informational Privacy

Informational privacy is the ability of the individuals to control information about himself. Biometrics can interfere with this in the following related ways [40]:

- The biometric information are used for a different purpose than intended without the consent from the users. Additional purposes can be useful for the society, but ethical concerns arise when the biometric information is used beyond the original purpose. That is known as function creep.

- The biometric information is used for tracking activities of individuals. If a user must use the same biometric to participate in life's everyday activities, he or she can leave a detailed track behind. If all these tracks are linked by an entity, there can be made detailed profiles of each individual. If this is done without the consent or knowledge from the user, it poses a major threat to the privacy.

- The biometric information is misused. Even if it is considered hard to spoof biometrics, there are other ways to steal the identity (e.g., during the transaction or from the template). The consequences of an identity theft are more grave than for previously identification methods. If your biometric identifier gets compromised, you can not simply replace it as with a password or a card. So without the proper safeguards, personal information can be misused in numerous ways.

3.1.3 How Biometrics Implies Privacy Concerns

Biometrics can lead to loss of anonymity and autonomity [39]. When biometrics is used, truly unique information about one's identity is disclosed. If the technology becomes a widespread success, the use and application of it might expand. Biometric identifiers can be required in new and unexpected circumstances where it might not be actually necessary. This can create a fear of the fact that you do not any longer have control over who have this unique information about yourself.

Another great fear is a society of surveillance, where the state can monitor each individual's single move. If this is being abused or exposed to function creep (i.e., it is used for other purposes than intended), it makes a big threat to the privacy. Different databases can be cross-linked and detailed information about each person can be obtained. This is however counter-argued by [39] in that the real issue here is not the use of biometrics, but the controlling of information systems.

It is found that additional information can be obtained from some types of the biometrics. The voice and face can for instant reveal emotions and iris and retinal scans can also reveal health conditions [29]. There are also done research indicating that the fingerprints can reveal medical informations as

Downs syndrome, leukemia, and breast cancer [24], but this is not proved.

Other fears are due to religious, cultural and philosophical beliefs. There can for example be reasons from religious writings indicating the aversion of similar cases and there can be the stigmatization effect.

3.1.4 How Biometrics Protect the Privacy

Biometrics does not only have the ability to harm the personal privacy. It can also protect it [39]. Since biometrics requires each individual to be present to prove the identity, it works as a strong security safeguard which prevents fraud and thereby protects the identity and informational integrity.

When biometrics is used for access control purposes, it restricts unauthorized personnel from gaining access to personal and sensitive information. Instead of using PINs and passwords which can easily be compromised, a biometric identifier is required. In this way, it is used to limit access to information and consequently protects the privacy.

In addition to protect the privacy, biometrics also enhance the privacy [39]. This is explained by the fact that biometric systems normally do not store the actual biometric characteristic, but a digital code derived from the characteristic. The code can not be reversed back to the actual characteristic and the code itself does not contain information about the individual.

3.2 Security and Vulnerabilities of a Biometric System

Traditionally, users have been given access to computer systems, physical buildings or equipment by using passwords, keys, codes, secure tokens, identification cards or combinations of these. They all are authentication mechanisms based on something you know or something you have. The weaknesses with those types of authentication mechanisms are that they can be lost, stolen, forged or forgotten. By using the newer third option, something you are, i.e. biometrics, the mentioned weaknesses can hopefully be eliminated or at least the security will be improved. Biometric authentication sets higher requirements of the user presence, since it obviously is a much more demanding task to copy a biometric characteristic of a person than stealing an access card or password. With that said, it is not impossible to fool a biometric system and some attacks and methods for defeating them will be presented below.

Several elements of a biometric system can be vulnerable against attacks if not implemented in a sufficiently secure way. Some elements that can be attacked or exploited in an attack of the system are:

- Sensor:
  The sensor needs to be accurate enough to distinguish between the users and detect spoof attempts, but also allow for natural variations of each sample from the same user.
- Feature Extractor:
  Knowledge of the feature extractor algorithm can be used to escape detection.
- Network:
  The data are sent between the different elements using a network and can be eavesdropped by a non-legitimate user.
- Database:
  Access to the biometric templates may be exploited by non-legitimate users.
- Matcher:
  Any access to modifying the matching score can be critical.

3.2.1 Attacks and Circumventions

Spoof Attack

A spoof attack is when a malicious person pretends to be a legitimate user in order to pass the authentication system. In a biometric system, this can be done by presenting a copy of the biometric feature to the sensor, as for instant a fake finger with a copy of a legitimate fingerprint. It is demonstrated successful spoofing attacks which have not been too hard to perform [37]. Common for all types of physical characteristic spoofing attacks is first to capture the biometric sample belonging to the legitimate user and then to create a copy of the sample.

Spoofing Fingerprints

By simply using molding plastic and gelatin, it has been showed that it is possible to make gummy fingers that can bypass a fingerprint authentication system [37]. Fingerprints can be obtained by copying fingerprints left on a object, such as a glass. Some post treatment can be performed to enhance the quality. [31]

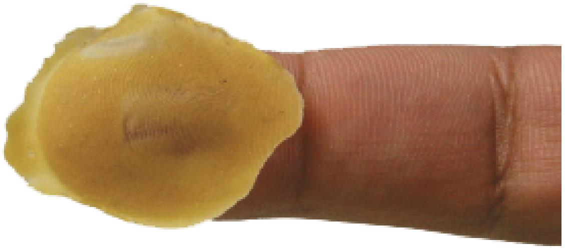

Figure 3.1: Fingerprint spoofing: Wafer-thin plastic sheet housing a three-dimensional replication of a fingerprint. Image found in [29].

Spoofing the Face

2D face recognition systems have been shown to be vulnerable to spoofing using a simple photograph of the face of a legitimate user. There are techniques to guard against this kind of spoofs, such as detection of movements in the face, for instant eye blinking, and also thermal images of the face.

To spoof a 3D recognition system requires more effort as a 3D-model of the face need to be fabricated. Such spoofs have, despite that, been carried out with success. [18]

Spoofing the Iris

As with 2D face recognition systems, iris scan systems have been fooled using a high-resolution photograph. Contact lenses on which an iris pattern is printed and also three-dimensional artificial irises can be produced. [18]

Spoofing the Voice

Some speaker verification systems are susceptible to spoofing attacks through the use of recorded voice and replay attacks. Human mimic can also be used, but this is rare and much more difficult [25].

Spoofing the Gait

Results from an experiment on spoofing the gait [8], shows that mimicking the gait is a threat, especially if the attacker has some knowledge of the closest target in the database. With no knowledge, on the other hand, using a minimal-effort impersonation attack does not necessarily improve the chances of an impostor being accepted as a legitimate user.

Replay Attack

By using a sniffer device or sniffer software during a legitimate authentication, the sent data can be captured and replayed later. This method requires the sensor to be bypassed, and it could be difficult to access the transmission medium as this often is protected in some way depending on the application and type of system.

Transmission Attack

If an impostor has access to the transmission medium between different components in the biometric system, he or she can act as a man-in-the-middle. Enrolled user data can be stopped, manipulated or replaced, and even matching scores can be manipulated with access to the right transmission mediums. [31]

Template Attack

Attacks on biometric templates include modifying, deleting or stealing stored templates or adding new ones. By stealing a template, the biometric system can be reverse engineered and synthetic biometrics can be made to bypass the authentication and it is therefore considered amongst the most dangerous. [31]

Trojan Horse Attack

The feature extractor can be attacked so that it will produce a pre-selected feature set at a given time or under some specific conditions. Thus, the extracted features can be replaced with a different synthesized feature set. This is called a Trojan Horse attack since the feature extractor module is replaced in a hidden manner. The matcher can also be vulnerable against this attack, as an artificially high or low matching score can be produced. [4]

3.2.2 Defeat Attacks

Encryption

Secure channel and encryption are suitable means for defeating transmission based attacks. Templates can also be protected using encryption whether they are stored in central databases, local storages or on smart cards.

Smart Cards

There are different architectures and design models for a biometric system and with respect to the privacy, the treatment and storage of the personal information is specially important. The biometric data may be stored in a central database, a local point of access or on a smart card.

Combining both smart card and biometric technology can provide a very high level of confidence in the verification of the identity of an individual and provide a secure system solution, while still protecting the privacy. A smart card is a card which is embedded with either a microprocessor and a memory chip or only a memory chip with non-programmable logic. Because the cards can carry all necessary functions and information on the card, they normally do not require access to remote databases, but the small memory capacity will limit the use. Parts of the memory are tamper resistant while other parts can be accessible to any application that can talk to the card.

There are some different solutions when using biometric technology in combination with smart cards and the place of processing is maybe the most critical factor. First, the verification template must be extracted and preprocessed, and second, the verification template must be compared to the trusted, stored template. The first task needs much more processing than the second, but cards that are able to process the template extraction itself are under development [2]. Cards that are able to do the matching already exist. One system solution is where the template extraction process is done at the reader and then sent to the smart card for comparison in the card's secure processing environment. The cardholders' stored template will then never leave the card. [2]

Liveness

Even though biometric devices provide physical characteristics of the users, these measurements do not guarantee for the liveness (i.e. the fact that there is a real living person and not some kind of spoof attack being performed). Liveness detection is hence techniques that aim to discover if the biometric measured is from an actual, live person and can thereby detect spoof attacks. It is based on physiological information as signs of life:

- from liveness information inherent to the biometric
- from additional processing of data captured from the sensor
- using additional hardware.

[33]
Examples are temperature measurements, infrared measurements of hand vein patterns, pulse measurements, facial thermograms. In addition one can use a challenge-response technique, where the user hear, feel or see something and must respond accordingly.

Multimodal Fusion

Most of the biometric systems in use today are using a single biometric trait for the identification or verification process. Due to vulnerabilities such as noisy data, non-universality of the trait, high error rates and spoof attacks, these single mode biometric systems may not provide sufficient reliability. Some of these problems and limitations can be addressed by using what is called a multimodal biometric system. That is a biometric system that combines multiple sources of biometric information and hence provides multiple evidences of the same identity.

An effective fusion scheme is needed to combine the data in order to maximize the performance and accuracy of the system. There are three possibilities of where the fusion takes place [32] when combing two biometric techniques:

- feature extractor level
- matching score level
- decision level

One example of multimodal biometrics is combining face recognition, voice recognition and lip movement as described in [7].

Chapter 4

Ear as a Biometric

After having presented basic principles of biometrics, the most common methods including related issues and challenges, the report will now focus on one specific biometric, namely ear recognition. This technique is still in a research phase and there are still unexplored and unsolved problems related to the topic.

Alphonse Bertillon, also mentioned in Chapter 1, examined the possibility of using the ear as a biometric as early as in 1890. It has been used in the forensics for 40 years following a system developed by Alfred Iannarelli, but then mostly by manual techniques [18]. Earprints found on a crime scene have in fact been used as proof in a few hundred cases in the Netherlands and the United States [11], but is no longer considered as legal proof in the Netherlands[1]. In more recent times attempts have been made to automate the system of Iannarelli, but compared to the more popular techniques of automatic fingerprint, eye and face recognition, the attention has been scant.

[1] In Case No. 23-001847-99, verdict No. 948/00, Court of Appeal of Amsterdam, 8 May 2000, earprint was rejected as a valid proof

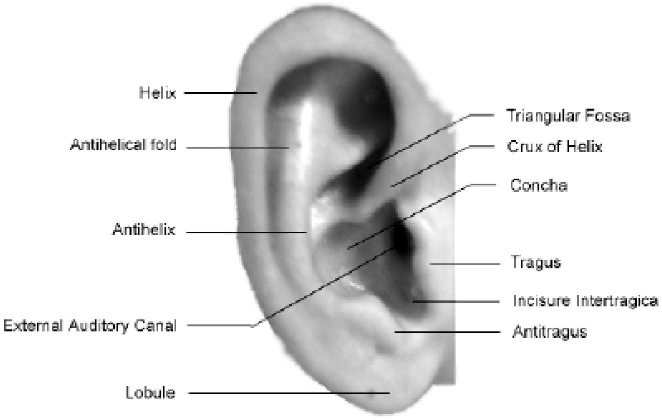

Figure 4.1: The topographic anatomy of the human ear, found in [30].

4.1 Why Use the Ear?

In 1989, Iannarelli gathered up over 10.000 ears and found in his work that they were all different. One of the fundamental requirements for a characteristic to be used as a biometric is exactly the uniqueness factor. It has several advantages over the more established biometrics such as the rich and stable structure of the ear, showed in Figure 4.1. While face biometrics suffer from changes in facial expression and changes with time, the ear remains the same. The quality of the face recognition also depends on the varying background, while the background of ear recognition remains almost the same. The size of the ear does not require high precision from the capture device as with iris recognition. No contact between the user and the capture device is necessary which avoids hygiene related concerns. It will probably not have the user anxiety effect as can be the case with iris and retina scan, because of its harmless capture method and low intrusiveness.

4.2 Problems With Ear Recognition

While ear recognition has some advantages over face recognition, it also have some of the same weaknesses. The ears can be covered by the hair (see Figure

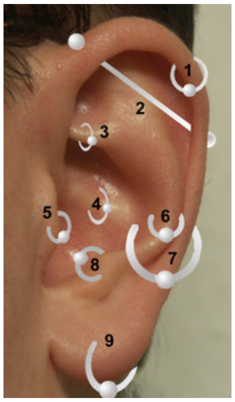

Figure 4.2: Possible earrings placements: 1) Helix/Cartilage, 2) Industrial, 3) Rook, 4) Daith, 5) Tragus, 6) Snug, 7) Conch, 8) Anti-Tragus, 9) Lobe. The image is a copy from Wikimedia Commons database, http://commons.wikimedia.org

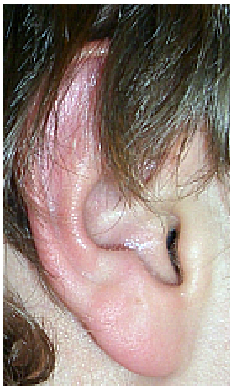

Figure 4.3: Ear partially covered by hair

4.3), a scarf, a cap and the like. This can of course be removed from the ear by the persons themselves, but this will hence introduce the factor of active help from the user. It is not very uncommon with people using earrings (see Figure 4.2) and this can affect the pattern recognition process. It also faces problems caused by illumination and head rotation. As one can see, face recognition also faces these problems. The ear can get stretched due to gravity over time, but this mainly affects the lobe. [18]

4.3 Approaches

In the sections above, the ear recognition using 2-dimensional images have been considered. Researchers have also examined a variety of other techniques for using the ear as a biometric identifier and some of them are presented below.

4.3.1 2D Recognition

For ear recognition based on 2-dimensional images, there have been suggested many different methods. Iannarelli developed a system based upon 12 measurements, but this was not suited for machine vision because of difficulties localizing the anatomical points.

Inspired by the work of Iannarelli, Burge and Burger conducted a proof of concept study through an implementation of a computer vision based system [5]. They modeled each subject's ear as an adjacency graph build from the Voronoi diagram of its Canny extracted curve segments and used graph matching techniques for authentication.

Hurley et al. used a force field feature extraction to map the ear to an energy field which highlights potential energy wells and channels as features as described in more detail in [13]. Using a dataset of 252 images, this method achieved a recognition rate of 99.2 %.

However, the most popular technique has proved to be Principal Components Analysis (PCA). The functionality of this is described in [18]. PCA was used in a study by Chang, where he concludes that ear and face do not have significant differences on recognition rate [22].

4.3.2 3D Recognition

Because of the rich and deep three-dimensional structure of the ear, some researchers have searched for solutions using these characteristics. 3D data offer resilience to problems known in 2D data such as illumination and pose and has been successfully deployed in face recognition.

Bhanu and Chen have presented a solution using range sensors to directly obtain 3D geometric data. A new local surface shape descriptor for 3D ear recognition was proposed and is described in detail in [12].

Another approach was presented by Yan and Bowyer using a range scanner to capture the data where the depth is calculated using triangulation. For the recognition process they use an iterative closest point (ICP) based 3D shape matching. They reported a performance of 98% for the 302 subjects and it was proved to be better than PCA [27].

4.3.3 Thermal Infrared

In face recognition, one has examined the possibility of using thermal images for recognition. This eliminates the problems with illumination and different skin colors that is observed in visual face recognition. As far as the author know, no material have been published on thermal ear recognition. Some articles, [5][43], briefly mention the use without going into details. Because of the promising use of thermal imagery in face recognition, it should be reason to believe that it could have good potential also in ear recognition. Therefore the next chapter will look into this field in detail.

4.3.4 Acoustic

Another novel and interesting method is to use the acoustic properties of the ear for recognition. This is exploited by Akkermans et al. [1]. His idea is based on the special shape of the ear that will behave as a filter so that a sound signal played into the ear is reflected back in a modified form constituting a personal signature for the person (as illustrated in Figure 4.4). They tested this in different applications (ear phone, head phone and mobile phone) which resulted in equal error rate in the order of 1-5%.

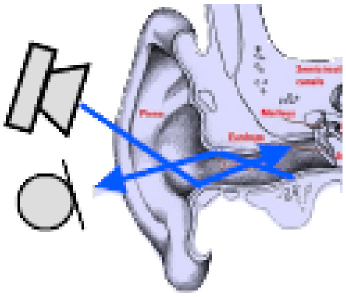

Figure 4.4: Functionality of acoustic ear recognition: A sound signal is probed into the ear which is reflected and picked up by a microphone, thereby generating an ear signature. The figure is found in [1].

4.4 Spoofing the Ear

Little effort has been made on the research of spoofing the ear, but as with all authentication or security systems, it is important to map out vulnerabilities that may be exploited. Hence, if ear recognition system will be implemented, there will be of great importance to have anti-attack methods to prevent spoofing.

By looking at spoofing methods from the other types of biometrics, one could possibly identify methods that also fit for ear recognition. A method for spoofing the face and the iris, is to simply use a high resolution photograph and present it to the capture device. For a 2D ear recognition system, this method could probably be used.

It may also be feasible to make a three dimensional model of an ear, but it is obviously more difficult and will require equipment for this. It will however be a threat to 3D recognition systems.

4.5 Ear Recognition in a Multimodal System

As already described, a multimodal biometric system, aim to combine two or more types of biometrics in order to increase the detection rate and thereby the security level. There exist combinations that give high detection rates, but nevertheless are inconvenient as combinations per se. As an example, it is more convenient combining fingerprint and palmprint as these can be captured in the same operation, than fingerprint and gait recognition, which requires you first to walk and then to register your finger.

One combination that has been given attention by researchers is the fusion of ear and face (e.g. [22]) and is proved to improve the recognition rate compared to only one of the methods alone.

Also the fusion of ear and profile face has been thought of and gives the advantage of capturing both characteristics from the same position and by the same device [23]. A recognition rate of 96.2 % on 79 subjects was achieved using this method.

Chapter 5

Thermal Ear Recognition

Minimal effort is spent on the field of using thermal ear recognition as a biometric measure. In face recognition, on the other hand, there have been conducted more studies, although neither this field has been subject to many researches. Since studies on thermal face recognition have produced promising results, known techniques from this field can probably also be applied to ear recognition.

5.1 The Infrared Spectrum

Electromagnetic spectral bands below the visible spectrum such as X-rays and ultraviolet radiation are harmful to the human body and are therefore unsuitable for ear recognition applications. The spectral bands above the visible spectrum, such as thermal IR imagery, has been suggested as an alternative source of information for the case of face recognition and ear recognition [5]. The visual spectrum ranges from 0.4 to 0.7 microns, which is the range in which a visual camera can measure the electromagnetic energy. Sensors in the IR camera, on the other hand, respond to thermal radiation in the infrared spectrum range at 0.7-Ű14.0 microns.

The infrared spectrum comprises the reflected IR and the thermal IR wavebands. The thermal IR band is associated with thermal radiation emitted by the objects. The amount of emitted radiation depends on both the temperature and the emissivity of the material. There are two primary bands in the thermal IR spectrum: the mid-wave infrared (MWIR) of the spectral range 3.0-Ű5.0 microns and long-wave infrared (LWIR) from 8.0Ű-14.0 microns. Between these bands (5.0–8.0 microns), there is a strong atmospheric absorption band where imaging becomes extremely difficult. [21]

The human body emits thermal radiation in both these bands of the thermal IR spectrum in which thermal IR cameras can sense temperature variations at a distance. Thermograms can be produced and presented in the form of heatmapped 2D images.
[18]

5.2 Thermal Imagery Used In Face Recognition

Since no research exist on thermal ear recognition, it can be wise to look aside into thermal imagery when used in similar applications. Hence, a brief overview of its use in face recognition follows.

Recognition of faces using the infrared spectrum has become an area of growing interest. In 1996, initial results from a comparison study of visible and infra-red imagery for face recognition were presented [38]. It indicated that both visible and IR imagery perform similarly and that a fusion of the two enhances the performance further. This theory was later supported in both [35] and [41].

Flynn et al. points out that visible imagery performs better than thermal imagery when using time-lapse between gallery and probe sets, but equally good in a same session scenario [41]. A PCA based recognition algorithm was used.

A study by Socolinsky [35] performed tests using several algorithms: PCA (Principal Component Analysis), LDA (Linear Discriminant Analysis), LFA (Local Feature Analysis) and ICA (Independent Component Analysis). The LDA-based algorithm outperformed the others in both thermal and visible imagery. They concluded that visible imagery performs worse when illumination and facial expression differ while the thermal imagery performance does not change significantly.

Automated location of eyes is often used for reference points and is in visible imagery a well-studied problem. In thermal images, on the other hand, the eyes do not stand out in the same degree and thermal face images have fewer readily localizable landmarks. Suggested methods to overcome this is suggested in [18].

The use of eyeglasses poses a problem when using thermal imagery, both for eye localization and for the face recognition itself, as glass is completely opaque in this modality. A solution for this is presented in [19] where a method for detecting the eyeglasses and replacing them with a template is suggested.

5.3 Advantages of Thermal Infrared Imaging

Since the light in the thermal IR range is emitted rather than reflected, there is no need for light. Thermal emissions from skin are an intrinsic property, independent of illumination. Hence, the ear images captured by a thermal IR sensor will be invariant to changes in illumination. So compared to the visible spectrum cameras, the infrared spectrum cameras have the advantage of better performance under poor light conditions.

Burge and Burger proposed thermal imagery for overcoming the problem of hair occlusion [5], but this is not yet tested. However, in Chapter 6, this will be included as a part of the experiments with thermal imagery of ears.

Spoofing of biometrics based on visual imagery, can be, depending on the system, possible by presenting a high resolution photo to the camera [31]. A thermogram system cannot be fooled by such an approach. Making a fake that generate a right heat emission pattern is still not achieved (as far as the author know), and it will obviously be a difficult task because it requires information of the heat emission of a person. So, thermal imagery used in biometrics will also have the function as an anti-spoofing technique, providing liveness to the captured data.

5.4 Thermoregulation: Factors Effecting the Body Temperature

Thermoregulation is the process of keeping the body at a constant temperature, which normally is about 37 degrees Celsius. There are certain factors or affections that will make the body temperature deviate from what is normal. Such factors are [28]:

- Illness
- Physical activity
- Menstruation
- Day rhythm
- Environmental temperature
- Emotional variations
- Food and drink intake
- Time of day (related to activity and rest)

Due to these factors [20], the heat emission image from the body will vary. The body will always try to keep the inner body temperature constant and reacts differently to hot and cold conditions. The blood flow is one of the factors that is affected by the thermoregulation mechanisms. When the body is cold, the blood is routed away from the skin and towards the warmer core of the body, while when the body is warm the blood is routed towards the skin, thereby increasing heat loss by radiation and conduction. These changes in the blood flow can also change the thermal body image and consequently the ear image.

Chapter 6

Test of Thermal Infrared Ear Recognition

Since thermal imagery has successfully been applied to face recognition schemes [34], there is reason to believe that also ear recognition can take advantage of this technique. This chapter will present a feasibility study aiming to give an indication of the suitability of using thermal imagery as a means to biometric ear recognition.

6.1 Test Design

The experiment was undertaken at NTNU, performed by the author, with the help of a certified thermographer and test personnel from the university. The experiment consists of the following steps:

1. Data Collection
2. Data Processing
3. Result Analysis

Set name	Description
Target Set	The set of known ears taken under normal circumstances.
Query Set 1	The set of ears taken under normal circumstances.
Query Set 2	The set of ears partially occluded by hair.
Query Set 3	The set of wet ears.
Query Set 4	The set of ears heated up.

Table 6.1: Description of Test Sets

6.1.1 Data Collection

Two types of image sets were used: target set and query set. The target set is meant to be the set of known images given to the recognition system and would represent the enrolled, registered images in an authentication system. The query set consists of unknown images which are to be identified or verified by comparisons to the target set. There were one target set and several query sets taken in different settings. This is similar to the test design described in the FERET test model used in face recognition [26].

The test data set in this experiment was of a small scale and consisted of 14 persons. Several thermograms were taken of each person's right ear, all on the same day. One image of each ear under normal circumstances was taken for the target set. In addition several other images were taken, constituting the different query sets. Before a person was taken thermograms of, 5 minutes of acclimatization was required due to factors related to thermoregulations described in Chapter 5.

Query Sets

The query sets are described in Table 6.1. The first query set represented the person under normal circumstances and was most equal to the target set. The set consisted of 14 subjects which was the same as the target set.

Query Set 2 consisted of images taken where the ears are partially occluded by hair. The set consisted of 4 subjects.

The third query set aimed to represent a person that may have been out in the

Person ID \Test Set ID	**TS**	**QS1**	**QS2**	**QS3**	**QS4**
P01	P01-TS	P01-QS1		P01-QS3	
P02	P02-TS	P02-QS1		P02-QS3	
P03	P03-TS	P03-QS1	P03-QS2	P03-QS3	
P04	P04-TS	P04-QS1		P04-QS3	
P05	P05-TS	P05-QS1		P05-QS3	
P06	P06-TS	P06-QS1	P06-QS2	P06-QS3	
P07	P07-TS	P07-QS1	P07-QS2	P07-QS3	
P08	P08-TS	P08-QS1			P08-QS4
P09	P09-TS	P09-QS1	P09-QS2		P09-QS4
P10	P10-TS	P10-QS1			P10-QS4
P11	P11-TS	P11-QS1			P11-QS4
P12	P12-TS	P12-QS1			P12-QS4
P13	P13-TS	P13-QS1			P13-QS4
P14	P14-TS	P14-QS1			P14-QS4

Table 6.2: Test subject IDs and query set IDs. The leftmost column represents the subjects and the other columns represent the target and query sets.

rain and therefore has a wet ear. This was achieved by simply moisturizing the ear. It was done on the first half of the subjects (i.e., the first 7 subjects). The effect of this is showed in the thermal image in Figure 6.1[1].

The fourth query set represents a person with a heated ear. This was achieved using a hair dryer and was suppose to simulate a person that has been physical active and therefore is warmer than normal. It was done on the second half of the subjects (i.e., the 7 last subjects). The effect is showed in Figure 6.2

Thus, the Target Set and Query Set 1 consist each of the whole test set. Query Set 2 consists of the persons with sufficient hair length. Query Set 3 consists of the first half of the test set and Query Set 4 consists of the last half. This is also presented in Table 6.2.

[1] The images are best viewed digitally or in a color printout

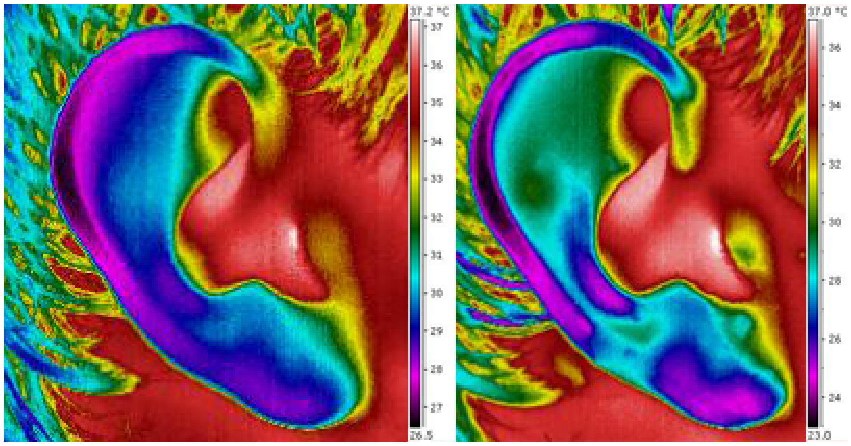

Figure 6.1: Two IR images of the same subject from the Target Set and Query Set 3 where a rainbow palette is applied.

Conditions and Surroundings

The thermograms were taken with a thermal infrared camera with the help of a certified thermographer. All the thermograms were taken under the same conditions such as the temperature of the environment and using the same background. The test was in this respect more of a best case scenario than a worse case, but the author found it appropriate as initial test conditions, and leaves other scenarios to future studies.

The thermal infrared camera being used was ThermaCAM P640 from FLIR Systems, that works in the range between 7.5 and 13 microns (i.e., the LWIR spectra) and provides for images with a resolution of 640x480 pixels. The distance from the camera lens to the ear was approximately 20 cm.

6.1.2 Data Processing

A complete ear recognition system would have the ability to locate the ear, extract the right features and do the comparisons in an automatic manner. No such system was found and since the focus of this report is to investigate the ability of using thermal images of the ear for recognition, there was no time for implementing a new system. Instead, a complete system was

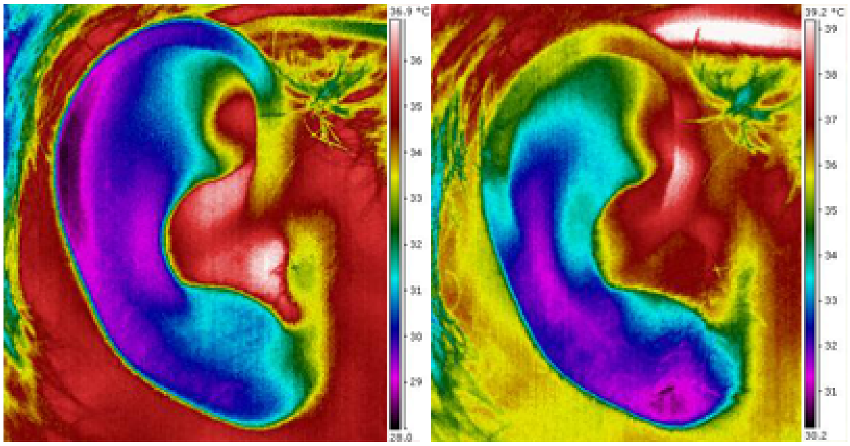

Figure 6.2: Two IR images of the same subject from the Target Set and Query Set 4 where a rainbow palette is applied.

emulated with manual help and third party software, but without automating all the processes which may would have been necessary in an experiment of a larger scale. The tool used for the image recognition process was Attrasoft Imagefinder 7.01.

Preprocessing

The first image preprocessing step was to apply a color palette to the image, which visually represents the temperature differences using colors. ThermaCAM Quickview 2.0 is free software provided by FLIR Systems and was used for this task.

To achieve a color distribution as detailed as possible, a rainbow palette was used. To apply the whole color spectrum to the ear, the ear's maximum and minimum temperature of each image were measured (using ThermaCAM Quickview 2.0) and used as the temperature scale for the image.

Since no software was found to localize and mask out the ear, this was done manually, using Adobe Photoshop CS2. The result was the ear masked out on a black background. In addition all images were resized to the same resolution. As all the ears were captured in the same position, no rotation normalization was applied.

Recognition and Matching using Attrasoft ImageFinder 7.01

For the recognition process, Attrasoft ImageFinder 7.01 was used, which is capable of analyzing the images, comparing them and find matches. It first extracts the features of the image by applying a filter. It is here critical to choose the right filter as this will be important for the results. The aim is to make the right features to stand out. The configured parameters are documented in Appendix A.

Attrasoft ImageFinder 7.01 supports three different types of filters named:

- Unsupervised filter
- Biofilter
- Neural filter

In this experiment the Biofilter was used as this have higher performance than the Unsupervised filter and requires less training that the Neural filter.

The Biofilter matching process consists of the following steps:

- Generation of signatures: Each image has a set of computed values (i.e., the features of the image). A collection of features are grouped into a signature. Attrasoft ImageFinder provided this functionality.
- Training: For the Biofilter, there is a need for training before the matching starts. Data is collected in advance to teach the recognition algorithm what to look for and how to match. Because of the amount of gathered data, there was not possible to make a disjoint training set. Therefore a subset of the test sets was used. This is documented in Appendix A.
- Matching: M:N matching compares all images in one directory with images in another directory. A score for each comparison is computed and indicates the similarity of the two images.

The tests were done using M:N comparisons. The output of the tool is a list of the matches and a number of matches found by Attrasoft ImageFinder, both correct and incorrect, in addition to a list of the correct matches found and the missing matches.

6.1.3 Result Analysis

The analysis produced parameters as False Acceptance Rate (FAR), False Rejection Rate (FRR) and Equal Error Rate (EER). The threshold, which determines the success of identification, was changed iteratively from 0 to 100%, with an increase of 5% each time. FAR and FRR were computed for each value of the threshold and finally the EER was determined.

$$FAR = \frac{\text{Na}}{\text{Nn}}$$

$$FRR = \frac{\text{Nb}}{\text{Nm}}$$

where Na is the number of all non-match comparisons that generate a score above the threshold, Nn is the number of all non-matches, Nb is the number of all genuine matches that generate a score below the threshold and Nm is the number of all genuine matches.

The intersection point of these two graphs is the EER (FAR=FRR). The EER defines at which threshold the system is working the best with respect to both FAR and FRR. Hence, the corresponding threshold will be a natural choice as the threshold in an verification or identification system. To have a stricter system, the threshold can be set higher to decrease the number of false acceptances, but this will correspondingly increase the number of false rejections.

Two analyses were performed:

1. Matchlist consisted of images from all query sets, each image having the respective match in the target set.

2. Matchlist consisted of images from Query Set 1, each image having the respective match in the target set.

The matchlist is the list which defines the correct matches and will affect the output of the test. The matchlist used is found in Appendix A.

6.2 Test Results

The results of the test are presented in this section and discussed in Chapter 7.

First, the results for the first ImageFinder test, where all matches (i.e., those between the target set and query set 1-4) were counted as correct matches, are presented. The results are given in Table B.1 in Appendix B and Figure 6.3. The EER with the corresponding threshold and detection rate is:

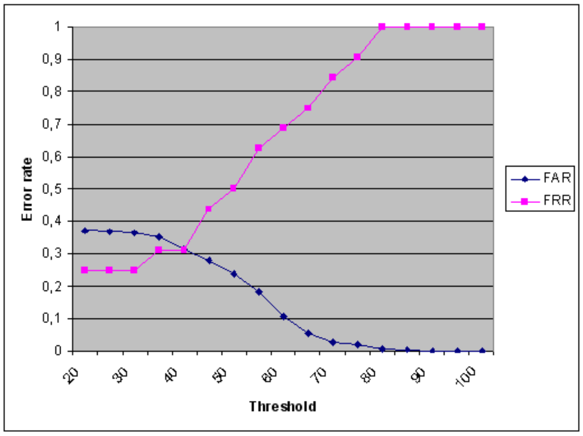

Figure 6.3: Chart of the first ImageFinder test including FAR and FRR graphs

EER = 0.315
Threshold = 40,09

Since ImageFinder only operates with natural numbers of the threshold, it is rounded off to the nearest whole number:

Threshold ≈ 40%
Detection rate with a threshold of 40% = 72%

Then in Table B.1 in the Appendix B and Figure 6.4, the results of the second test, where only matches between the target set and query set 1 were counted as correct matches, are presented. The EER with the corresponding threshold and detection rate for this test is:

EER = 0.207
Threshold = 52,24

Threshold ≈ 52%
Detection rate with a threshold of 52% = 78%

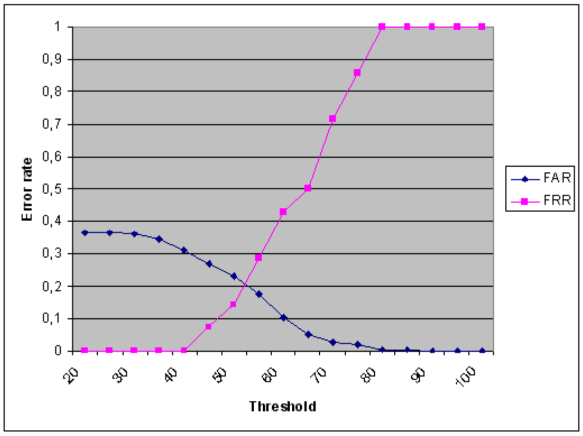

Figure 6.4: Chart of the second ImageFinder test including FAR and FRR graphs

As seen from the charts, the threshold starts at 20%. This is because of the way Attrasoft ImageFinder operates. For each matching process, there is a lower bound threshold and all image comparisons not generating a score above this threshold is simply considered a non-match without being given a score. Normally the line of the FAR starts at 1 and the line of the FRR starts at 0 with the threshold of 0.

Calculations of the parameters is presented in Appendix C.

6.3 Occlussion by Hair

In addition to the tests above, an examination of the temperature zones of the subjects was conducted. Each subject's target image was used for this. By using ThermaCAM QuickView, the maximum and minimum temperatures of the ear and the hair were separately observed. The result is shown in Table 6.3 and illustrated in Figure 6.5. None of the subjects have disjoint ear and hair temperature zones, which will cause difficulties in segmenting out just the hair that covers the ear. Then also parts of the ear will be segmented out. The registered maximum temperature of the hair may be too high as the skin temperature between the hair can have been captured when using ThermaCam QuickView. Anyhow, in many of the cases the lower temperature of the hair actually is higher than the lower temperature of the ear, which makes segmentation unsuitable.

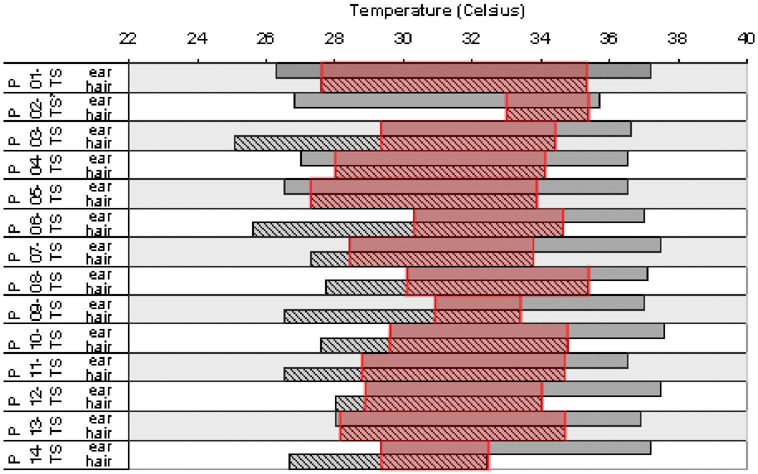

Figure 6.5: The intersected temperature zones of the ear and the hair marked in red

	Ear (° Celsius)		Hair (° Celsius)	
	Min	Max	Min	Max
P01-TS	26,3	37,2	27,6	35,3
P02-TS*	26,8	35,7	33	35,4
P03-TS**	29,3	36,6	25,1	34,4
P04-TS	27	36,5	28	34,1
P05-TS	26,5	36,5	27,3	33,9
P06-TS**	30,3	37	25,6	34,6
P07-TS	28,4	37,5	27,3	33,8
P08-TS	30,1	37,1	27,7	35,4
P09-TS**	30,9	37	26,5	33,4
P10-TS	29,6	37,6	27,6	34,8
P11-TS	28,8	36,5	26,5	34,7
P12-TS	28,9	37,5	28	34
P13-TS	28	36,9	28,2	34,7
P14-TS	29,3	37,2	26,7	32,4

Table 6.3: Overview of minimum and maximum temperatures of the ear and the hair of the subjects' target sets. *subject has very little hair. **subject has used a cap which can have influenced the temperature of the ear and the hair.

Chapter 7

Discussion

7.1 Potential of Ear Recognition

The research in ear biometrics is just rudimental, many methods remain to be explored and commenced studies need to be followed up. Compared to other, more mature techniques as fingerprints, there exists little literature on the field. The technique resembling ear recognition the most is face recognition which have been given much more attention and now seems to be one of the more promising contributors to the biometric market [10]. Hence, there should be reason to predict ear recognition a promising future as a means to personal identification.

Section 4.1 points out reasons for why ear recognition is a technique just as good as face recognition or maybe even better.

7.2 Using Thermography

The use of thermography has been applied in face recognition studies with promising results and gives therefore good motivations for applying it to ear recognition as well. With fewer problems caused by variations in illumination, a great obstacle is handled, but if other problems consequently are introduced, the situation may not have improved.

Other factors are costs and availability. Using 2-dimensional visible imagery requires a high resolution camera. This is not too costly and there exist many manufacturers. Cameras capable of taking thermal imagery, on the other hand, can be very costly and there are fewer manufacturers of these.

7.2.1 Test Results

The results from the experiment were presented in Chapter 6. The purpose of the small scale experiment was to indicate whether the ear could be used in personal identification. The results showed that images taken under the same conditions (i.e., Query Set 1) were not sufficiently distinguishable and the images taken under different conditions gave even worse results.

The first test showed that when considering all the query sets (i.e., all elements in the query sets had a match in the target set), the EER was 0.315 with a detection rate of 72%. The second test considered only the matches in query set 1. The result was then better than in the first test with an EER of 0.207, giving a detection rate of 78%. For comparison, a test performed by International Biometric Group [9], comparing biometric systems, reports equal error rates all below 0.015 for tests with authentication attempts within the same day.

By observing the two images in Figure 6.1, one can see that when the water is applied, the degree of details and accuracy is actually perceived to be higher, but the heat distribution is also changed from the original image. Figure 6.2 shows the effect of heating up the ear and one can see that the heat distribution also here is changed. These changes make it hard to find the corresponding registered image. An authentication system where the performance is affected by the temperature variations of the persons to be authenticated is not preferable. Persons entering a building from a cold, warm or rainy weather or people having a fever or have been exposed to stress will have less chance to pass the authentication. This would make the access system very little convenient. Even if the system would not have been sensitive to temperature variations, the performance is still too poor. Two of the main advantages with a biometric authentication system is suppose to be enhanced security and the ease of use, but neither of these are present in the results from this experiment.

Burge and Burger suggested to solve the problem of occlusion by hair by the use of thermal imagery [5]. Then the hair could be segmented out on temperature with the assumption that the temperature of the hair does not coincide with the temperature of the ear. The results from this report show that none of the subjects having their ear occluded by hair were recognized. Some of them might have been recognized by using algorithms specially designed for handling this kind of problem, but nevertheless, some would probably never have been recognized because of the high degree of occlusion. Thermography gives the capability of mapping temperatures to the image and thereby segment out the ear from the hair, but it will obviously not give any information about what is behind the hair. Hence, if the subject has the whole ear covered, either by hair, a cap or anything else, there will not be possible to perform the identification. Also, as observed using ThermaCam QuickView, the subjects' hair temperatures and ear temperatures are not disjoint, which will complicate the task of automatically segment out the hair.

As a suggestion to overcoming the problems with the temperature variations, several templates with different ear temperatures can be registered, instead of just one. This complicates of course the registration process and may not work as an access system for a large number of people as for instant a border control at an airport, but it could be applicable in a smaller environment, maybe within a company. With the use of machine learning, a self learning system can also be applied with a controlled training phase the first period. In this way the system can accept the differences in temperatures and hopefully without increasing the rate of false matches.

Possible Error Sources

The experiment conducted is not perfect and there could be several sources of errors.

In the data gathering part there are factors that can affect the results. One factor is the size of the data sets. Ideally this should be of a certain size, dependent of the experiment, to achieve accurate and representative results.

The data size of this experiment was of a relatively small size and the result can then be less accurate than it could have been.

There could also have been gathered a separate training set disjoint from the actual test data. To avoid bias associated with the training set, the test sets and training sets should be disjoint. By including images similar to those in the target set, the training set becomes more representative of the target set which can lead to a bias of too good performance. However, with the obtained results from the tests performed, it will in this case only strengthen the conclusion. Another aspect regarding the training set is in this case more relevant and that is the size of the training set. By using a small training set, it will have a degrading effect on the performance. Hence, better results could have been obtained by using a larger training set.

A third factor is the data capturing part. The equipment used in this test was a thermal IR camera. Factors relevant for the final results are the camera features (e.g., resolution) and configuration of the camera (e.g., emissivity level). The camera used, a FLIR ThermaCAM P640, has as of today, the best resolution for thermal IR cameras on the market and the camera configuration was done by a certified thermographer.

In the data processing part there are also certain factors that may affect the results. The algorithm used for comparison is maybe the most critical factor as this is the element deciding the equality between the images. Within the algorithm lays the feature extractor which determines the features to make up the signature and are used for the comparison. In this experiment, a closed-source software product was used. Hence, no knowledge of the actual algorithm is known, but the tool lets the user choose between different filters for making the objects stand out in the best way. Also other parameters were set and could be leading to poor results if not set correctly.

Challenges

One of the challenges by using thermal ear recognition, as seen from the test results, is overcoming the problem caused by the temperature variations in a human. As described in Chapter 5, there are several factors causing these variations and there is nothing to do about the temperature variations themselves.

If images are taken under uncontrolled surroundings, there might be a chance of radiation originated from the surroundings reflecting in the object. Hence, this will probably not be a problem in the controlled situation of an access control scenario, but it could pose a problem if the use is passive identification and surveillance. The fact that the camera needs calibration and that the resolution is low compared to a visual camera also complicates such a scenario.

Another possible challenge is the cost as briefly mentioned above. Since the price of a thermal camera is much higher than a normal visual camera, this can also be an important factor. The camera used in the test of this thesis, FLIR ThermaCAM P640, had a price of 382.000 Norwegian kroner (approximately 50.000 euro) as of 2007[1]. If a technology yields superior performance, a higher price can be acceptable, but if choosing between similar performance technologies, the price will play an important role.

7.2.2 Evaluation of Thermal Ear Recognition

A brief evaluation of thermal ear recognition with respect to the requirements listed in Chapter 2 follows.

Universality

Every human being is normally born with an ear. Some can be born with malformed or abnormal pinna (outer ear). This does not necessarily need to be a problem though, depending on the feature extractor and matching algorithm used. Even absence of the pinna can be possible, but this is very rare.

[1] According to Precision Technic Nordic, http://www.ptnordic.no

Distinctiveness

From the results obtained in this study, the ears' thermal image is not distinctive enough for use in verification or identification.

Permanence

The structure of the ear is preserved from birth into old age. Gravity can though cause the ear to undergo stretching, but this is mainly affecting the lobe [17]. When it comes to the thermal image of the ear, no study is yet performed to investigate whether the heat distribution of the ear changes with age. However, the body temperature can change slightly with age as mentioned in Chapter 5.

Collectability

It is easy to collect a thermal image of the ear as all needed is taking an image with an infrared camera, but there can be problems as already mentioned by hair occlusion. In active authentication scenarios with some help from the user this will not be a problem.

Performance

The process of recognition can be done reasonably fast in a verification scheme, but as seen from this study the recognition rates and error rates are not satisfactory.

Acceptability

As with normal ear recognition, thermal ear recognition does not require any physical contact and is non-invasive. There should therefore be reason to believe this technique will have a high level of acceptability, but as far as the author know, no qualitative study is performed on this.

Circumvention

In Section 4.4, spoofing techniques for ear recognition are discussed, but without mentioning thermal ear recognition. By taking infrared images of the ear, information from a person which is unobservable (i.e., information that one can not obtain without an infra-red camera) is gained. This feature yields a liveness property and works as an anti-spoofing technique which can be of great value.

If an attacker should be able to get a thermal image of a legitimate user, this could not be used to fool the capture device by presenting the obtained image (since the capture device only would take a thermal image of the image presented, containing no valuable information). However, the thermal image can be used in a transmission replay attack, but this requires access to the transmission medium.

7.3 The Future and Remaining Work

Biometrics is definitively a technology for the future, as seen from the trends the recent years. Ear recognition has still not reached the big market, but several studies have given promising results. Thermal ear recognition has from this study shown poor results in performance, so it will probably be unsuitable as a biometric technology per se. It could, however, be used in combination with another biometric technique.

Regarding future studies in thermal ear recognition, a similar test can be performed again, however utilizing another algorithm and a bigger training set. If better results are achieved, then one can look at scenarios where images are not taken in the same session, but with a time-lapse in between.

Another topic of current interest is the use of passive identification used in surveillance. Other techniques which are considered for this, as of today, are face recognition and gait recognition. It could be interesting to investigate the possibility of using thermal ear recognition or maybe localization of the ear in this setting.

Chapter 8

Conclusions

Finding new traits and characteristics of the human body for use in the biometric technology is becoming more and more difficult as so much are already thought of. Even so, this does not mean that the biometric evolution has reached its end. Focus is now on how to improve existing technologies and use the known characteristics in new ways.

This thesis gives a broad presentation of the biometric technology in general while also presenting ear recognition in detail. A novel approach of using thermal imagery combined with ear recognition is presented and its potential is explored.

An experiment, of a small scale, using thermal imagery for recognizing ears was conducted in order to give an indication of the usefulness of this novel biometric technology.

The results show that the thermal images of the ears are not sufficiently distinguishable if the body temperature (and consequently the ear temperature) has changed since the time of registration. Such temperature changes can be caused by stress, physical activity or the temperature of the surroundings. It will change the thermal image of the ear, which will generate new ear signatures, and it might lead to a high FRR, even at low thresholds.

Even the images of the ears that had maintained the same temperature since the registration did not give a sufficiently good result. The EER was 0.207, which is better than for the ears with different temperatures, but it is still too high for use in authentication.

The occlusion by hair will, depending on the degree of occlusion, cause a problem. If the ear is almost fully covered by hair, the problem is inevitable. If the ear is only partially covered, Burge and Burger suggested to segment out certain temperature zones to separate the ear and the hair from each other [5]. The experiment images showed that not all subjects have ears and hair in disjoint temperature zones, so their idea will not hold for everyone.

The results were not as promising as the author expected in advance. The experiment was performed on only 14 persons with 3-4 images of each person and the EER was high for this small number of participants, but it is still uncertain how a larger number of participants will affect the results. However, one can conclude based on this specific test that using only thermal imagery by itself is not suited as a biometric authentication technique, but it might work as a supplement to other biometric techniques.

References

[1] A. H. M. Akkermans, T. A. M. Kevenaar, and D. W. E. Schobben. Acoustic ear recognition for person identification. In T. A. M. Kevenaar, editor, *Automatic Identification Advanced Technologies, 2005. Fourth IEEE Workshop on*, pages 219–223, 2005.

[2] Smart Card Alliance. Smart cards and biometrics in privacy-sensetive secure personal identification systems. 2002.

[3] Ruud Bolle. *Guide to Biometrics*. Springer, 2004.

[4] I. R. Buhan and P. H. Hartel. The state of the art in abuse of biometrics. Technical report, Centre for Telematics and Information Technology, University of Twente, 2005.

[5] M. Burge and W. Burger. Ear biometrics in computer vision. In W. Burger, editor, *Pattern Recognition, 2000. Proceedings. 15th International Conference on*, volume 2, pages 822–826 vol.2, 2000.

[6] Monrose Fabian and D. Rubin Aviel. Keystroke dynamics as a biometric for authentication. *Future Gener. Comput. Syst.*, 16(4):351–359, 2000. 338359.

[7] R. W. Frischholz and U. Dieckmann. Biold: a multimodal biometric identification system. *Computer*, 33(2):64–68, 2000.

[8] D. Gafurov, E. Snekkenes, and P. Bours. Spoof attacks on gait authentication system. *Information Forensics and Security, IEEE Transactions on*, 2(3):491–502, 2007.

[9] International Biometric Group. Comparative biometric testing round 6 public report. Technical report, 2006.

[10] International Biometric Group. *Biometris Market and Industry Report 2007-2012*. 2007.

[11] A.J. Hoogstrate, H. Van Den Heuvel, and E. Huyben. Ear identification based on survaillance camera images. *Sci Justice*, 41:167–172, 2001.

[12] Chen Hui and Bhanu Bir. Human ear recognition in 3d. In Bhanu Bir, editor, *Workshop on Multimodal User Authentication*, 2003.

[13] D. J. Hurley, M. S. Nixon, and J. N. Carter. A new force field transform for ear and face recognition. In M. S. Nixon, editor, *Image Processing, 2000. Proceedings. 2000 International Conference on*, volume 1, pages 25–28 vol.1, 2000.

[14] A. K. Jain. Biometric recognition: how do i know who you are? In *Signal Processing and Communications Applications Conference, 2004. Proceedings of the IEEE 12th*, pages 3–5, 2004.

[15] A. K. Jain, A. Ross, and S. Pankanti. Biometrics: a tool for information security. *Information Forensics and Security, IEEE Transactions on*, 1(2):125–143, 2006.

[16] A. K. Jain, A. Ross, and S. Prabhakar. An introduction to biometric recognition. *Circuits and Systems for Video Technology, IEEE Transactions on*, 14(1):4–20, 2004.

[17] Anil K. Jain, Ruud Bolle, and Sharath Pankanti. *Biometrics: Personal Identification in Networked Society.* Springer Science+Business Media, Inc., Boston, MA, 2002. E-bok tilgjengelig for eierbibliotek via Internett.

[18] Anil K. Jain, Patrick Flynn, and Arun A. Ross. *Handbook of biometrics.* Springer, New York, 2007.

[19] Heo Jingu, G. Kong Seong, R. Abidi Besma, and A. Abidi Mongi. Fusion of visual and thermal signatures with eyeglass removal for robust face recognition, 2004. 1033013 122.

[20] Greg Kelly. Body temperature variability (part 1): A review of the history of body temperature and its variability due to site selection, biological rhythms, fitness, and aging. *Alternative medicine review*, 11(4):278–293, 2006.

[21] Seong G. Kong, Jingu Heo, Besma R. Abidi, Joonki Paik, and Mongi A. Abidi. Recent advances in visual and infrared face recognition–a review. *Computer Vision and Image Understanding*, 97(1):103–135, 2005.

[22] Chang Kyong, W. Bowyer Kevin, Sarkar Sudeep, and Victor Barnabas. Comparison and combination of ear and face images in appearance-based biometrics. *IEEE Trans. Pattern Anal. Mach. Intell.*, 25(9):1160–1165, 2003. 942780.

[23] Yuan Li, Mu Zhichun, and Liu Ying. Multimodal recognition using face profile and ear. In Mu Zhichun, editor, *Systems and Control in Aerospace and Astronautics, 2006. ISSCAA 2006. 1st International Symposium on*, page 5 pp., 2006.

[24] Davide Maltoni, Dario Maio, Anil K. Jain, and Salil Prabhakar. *Handbook of Fingerprint Recognition.* Springer-Verlag New York, Inc., New York, NY, 2003. E-bok tilgjengelig for eierbibliotek via Internett.

[25] Judith Markowitz. Anti-spoofing for voice. In *Biometric Consortium*, Washington, 2005.

[26] P. J. Phillips, Moon Hyeonjoon, P. Rauss, and S. A. A. Rizvi S. A. Rizvi. The feret evaluation methodology for face-recognition algorithms. In Moon Hyeonjoon, editor, *Computer Vision and Pattern Recognition, 1997. Proceedings., 1997 IEEE Computer Society Conference on*, pages 137–143, 1997.

[27] Yan Ping, W. Bowyer Kevin, and J. Chang Kyong. Icp-based approaches for 3d ear recognition. volume 5779, pages 282–291. SPIE, 2005. Biometric Technology for Human Identification II 1.

[28] C. Polk and E. Postow. *Handbook of biological effects of electromagnetic fields.* CRC Press Inc.,Boca Raton, FL, United States, 1986. System Entry Date: 05/13/2001 Availability: CRC Press Inc., 2000 Corporate Blvd. NW, Boca Raton, FL 33431. Source: NOV-88-008219;EDB-88-108413; NOV (DOE contractor) Language: English.

[29] S. Prabhakar, S. Pankanti, and A. K. Jain. Biometric recognition: security and privacy concerns. *Security & Privacy, IEEE*, 1:33–42, 2003.

[30] K. H. Pun and Y. S. Moon. Recent advances in ear biometrics. In Y. S. Moon, editor, *Automatic Face and Gesture Recognition, 2004. Proceedings. Sixth IEEE International Conference on*, pages 164–169, 2004.

[31] Xiao Qinghan. Security issues in biometric authentication. In *Information Assurance Workshop, 2005. IAW '05. Proceedings from the Sixth Annual IEEE SMC*, pages 8–13, 2005.

[32] Arun Ross and Anil Jain. Information fusion in biometrics. *Pattern Recognition Letters*, 24(13):2115–2125, 2003.

[33] Stephanie A. C. Schuckers. Spoofing and anti-spoofing measures. *Information Security Technical Report*, 7(4):56–62, 2002.

[34] D. A. Socolinsky and A. Selinger. Thermal face recognition over time. In A. Selinger, editor, *Pattern Recognition, 2004. ICPR 2004. Proceedings of the 17th International Conference on*, volume 4, pages 187–190 Vol.4, 2004.

[35] Diego A. Socolinsky, Andrea Selinger, and Joshua D. Neuheisel. Face recognition with visible and thermal infrared imagery. *Computer Vision and Image Understanding*, 91(1-2):72–114, 2003.

[36] N. Yanushkevich Svetlana, Stoica Adrian, P. Shmerko Vlad, and V. Popel Denis. *Biometric Inverse Problems.* CRC Press, Inc., 2005. 1211719.

[37] K. Yamada S. Hoshino T. Matsumoto, H. Matsumoto. Impact of artificial gummy fingers on fingerprint systems. In *SPIE Optical Security and Counterfeit Deterrence Techniques IV*, volume 4677, 2002.

[38] J. Wilder, P. J. Phillips, Jiang Cunhong, and S. Wiener. Comparison of visible and infra-red imagery for face recognition, 1996. 796044 182.

[39] J. D. Woodward. Biometrics: privacy's foe or privacy's friend? *Proceedings of the IEEE*, 85(9):1480–1492, 1997.

[40] J. D. Woodward. *Army Biometric Applications: Identifying and Addressing Sociocultural Concerns.* 2001.

[41] Chen Xin, J. Flynn Patrick, and W. Bowyer Kevin. Ir and visible light face recognition. *Comput. Vis. Image Underst.*, 99(3):332–358, 2005. 1099056.

[42] Li Yi-Bo, Jiang Tian-Xiao, Qiao Zhi-Hua, and A. Hong-Juan Qian Hong-Juan Qian. General methods and development actuality of gait recognition. In Jiang Tian-Xiao, editor, *Wavelet Analysis and Pattern Recognition, 2007. ICWAPR '07. International Conference on*, volume 3, pages 1333–1340, 2007.

[43] Lee Yuan, Zhichun Mu, and Zhengguang Xy. Using ear biometrics for personal recognition. pages 221–228, 2005.

[44] David Zhang. *Automated Biometrics: Technologies and Systems.* Springer, 2000.

[45] W. Zhao, R. Chellappa, P. J. Phillips, and A. Rosenfeld. Face recognition: A literature survey. *ACM Comput. Surv.*, 35(4):399–458, 2003. 954342.

Appendix A

Software Parameters and Files

These are the files and parameters used by Attrasoft ImageFinder 7.01:

The training set is defined in match.txt:

```
match.txt:
7
1 P01-TS P01-QS1
2 P02-TS P02-QS1
3 P03-TS P03-QS1
4 P04-TS P04-QS1
5 P05-TS P05-QS1
6 P06-TS P06-QS1
7 P08-TS P08-QS1
```

For the first test, this matchlist was used:

```
b1_matchlist.txt:
32
1 P01-TS P01-QS1
2 P02-TS P02-QS1
3 P03-TS P03-QS1
4 P04-TS P04-QS1
5 P05-TS P05-QS1
6 P06-TS P06-QS1
7 P07-TS P07-QS1
8 P08-TS P08-QS1
```

```
9 P09-TS P09-QS1
10 P10-TS P10-QS1
11 P11-TS P11-QS1
12 P12-TS P12-QS1
13 P13-TS P13-QS1
14 P14-TS P14-QS1
15 P03-TS P03-QS2
16 P06-TS P06-QS2
17 P09-TS P09-QS2
18 P07-TS P07-QS2
19 P05-TS P05-QS3
20 P04-TS P04-QS3
21 P01-TS P01-QS3
22 P02-TS P02-QS3
23 P03-TS P03-QS3
24 P06-TS P06-QS3
25 P07-TS P07-QS3
26 P08-TS P08-QS4
27 P09-TS P09-QS4
28 P10-TS P10-QS4
29 P11-TS P11-QS4
30 P12-TS P12-QS4
31 P13-TS P13-QS4
32 P14-TS P14-QS4
```

For the second test, this matchlist was used:

```
b1_matchlist.txt:
14
1 P01-TS P01-QS1
2 P02-TS P02-QS1
3 P03-TS P03-QS1
4 P04-TS P04-QS1
5 P05-TS P05-QS1
6 P06-TS P06-QS1
7 P07-TS P07-QS1
8 P08-TS P08-QS1
9 P09-TS P09-QS1
10 P10-TS P10-QS1
11 P11-TS P11-QS1
12 P12-TS P12-QS1
13 P13-TS P13-QS1
14 P14-TS P14-QS1
```

The following parameters in Attrasoft ImageFinder were set:

```
Filter: BioFilter
[ImagePreProcessing]
BorderCut=0
MaskX=0
MaskY=0
MaskW=0
MaskH=0
MaskType=0
StickShift=0
SkipEmptyBorder=0
SkipEmptyBorderPercent=0
SkipEmptyBorderEdgeFilter=0
SkipEmptyBorderThresholdFilter=5
Parameter12=0
Parameter13=0
Parameter14=0
Parameter15=0
[Image Processing Filters]
EdgeFilter=4
ThresholdFilter=1
CleanUpFilter=2
DoubleProcessing=0
R1=0
R2=128
R3=2
G1=0
G2=128
G3=2
B1=0
B2=128
B3=2
Parameter14=0
Parameter15=0
Parameter16=0
Parameter17=0
Parameter18=0
Parameter19=0
[Reduction Filter]
ReductionFilter=0
SegmentCut=0
SizeCut=0
BorderCut=0
lookAtX=0
lookAtY=0
lookAtXLength=0
```

```
lookAtYLength=0
[Signature Filter]
SignatureFilter=0
[BioFilter]
bioFilter=0
FaultToleranceScale=20
Mode=0
Threshold=90
OutputType=0
ShowFile=1
Blurring=2
Sensitivity=4
UseRelativeScore=1
ShowScore=1
AutoSegment=0
Parameter12=0
Parameter13=0
Parameter14=0
Parameter15=0
Parameter16=0
Parameter17=0
Parameter18=0
Parameter19=0
```

Appendix B

Test Tables

The results of the two tests done using Attrasoft ImageFinder 7.01 follows on the next page. The parameters included are:

Threshold The threshold is incremented with a value of 5 from 20 to 100. The thresholds below 20 would yield the same corresponding values as 20. This is because of the way Attrasoft ImageFinder operates as described in section 6.1.3.

Total matches found The number of all matches found by Attrasoft ImageFinder. These matches can be both correct and incorrect.

Genuine matches found The number of the genuine (true) matches found by Attrasoft ImageFinder.

Na The number of all non-match comparisons that generate a score above the threshold.

Nb The number of all genuine matches that generate a score below the threshold.

Nn The number of image pair comparisons which are non-matches.

Nm The number of all genuine matches.

FAR The rate of which the system will wrongly accept a matching attempt.

FRR The rate of which the system will wrongly deny a matching attempt.

Table B.1: Attrasoft ImageFinder Test Results: (a)First test (b)Second test

(a)

Threshold	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
Total matches found	253	252	250	240	219	193	169	132	86	52	34	28	17	16	14	14	14
Genuine matches found	24	24	24	22	22	18	16	12	10	8	5	3	0	0	0	0	0
Na	215	214	212	204	183	161	139	106	62	30	15	11	3	2	0	0	0
Nb	8	8	8	10	10	14	16	20	22	24	27	29	32	32	32	32	32
Nn	580	580	580	580	580	580	580	580	580	580	580	580	580	580	580	580	580
Nm	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
FAR	0,371	0,369	0,366	0,352	0,316	0,278	0,240	0,183	0,107	0,052	0,026	0,019	0,005	0,003	0	0	0
FRR	0,250	0,250	0,250	0,313	0,313	0,438	0,500	0,625	0,688	0,750	0,844	0,906	1	1	1	1	1
Detection Rate	0,75	0,75	0,75	0,688	0,688	0,563	0,500	0,375	0,313	0,250	0,156	0,094	0	0	0	0	0

(b)

Threshold	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
Total matches found	253	252	250	240	219	193	169	132	86	52	34	28	17	16	14	14	14
Genuine matches found	14	14	14	14	14	13	12	10	8	7	4	2	0	0	0	0	0
Na	225	224	222	212	191	166	143	108	64	31	16	12	3	2	0	0	0
Nb	0	0	0	0	0	1	2	4	6	7	10	12	14	14	14	14	14
Nn	616	616	616	616	616	616	616	616	616	616	616	616	616	616	616	616	616
Nm	14	14	14	14	14	14	14	14	14	14	14	14	14	14	14	14	14
FAR	0,365	0,364	0,360	0,344	0,310	0,269	0,232	0,175	0,104	0,050	0,026	0,019	0,005	0,003	0	0	0
FRR	0	0	0	0	0	0,071	0,143	0,286	0,429	0,500	0,714	0,857	1	1	1	1	1
Detection Rate	1	1	1	1	1	0,929	0,857	0,714	0,571	0,500	0,286	0,143	0	0	0	0	0

Appendix C

Calculations

C.1 Calculation of EER

When the intersection of FAR and FRR lays between two sample values, the exact value of the EER needs to be calculated. This is done by simple linear equations:

First test:
The intersection of FAR and FRR is between the X-values 35 and 40. Functions for FAR and FRR for the first test is calculated:

FAR(X) = aX + b

a = $\frac{FAR(40)-FAR(35)}{40-35}$ = -0,007586207

b = FAR(35)-a×35 = 0,618965517

FRR(X) = a'X + b'

a' = $\frac{FRR(40)-FRR(35)}{40-35}$ = 0,025

b' = FRR(35) - a'×35 = -0,6875

where X is the threshold. The point of intersection is found:

FAR(X*)=FAR(X*)

⇒ X* = 40,09259259, Y(X*) = 0,314814815 = EER

Second test: The intersection of FAR and FRR is between the X-values 50 and 55. Functions for FAR and FRR for the second test is calculated:

FAR(X) = aX + b

a = $\frac{FAR(55)-FAR(50)}{55-50}$ = -0,011363636

b = FAR(50)-a×50 = 0,800324675

FRR(X) = a'X + b'

a' = $\frac{FRR(55)-FRR(50)}{55-50}$ = 0,028571429

b' = FRR(35) - a'×35 = -1,285714286

where X is the threshold. The intersection is found:

FAR(X*)=FAR(X*)

⇒ X* = 52,23577236, Y(X*) = 0,206736353 = EER

C.2 Verification of the Number of Comparisons

Total number of comparisons:	
N-target =	14
N-allsets =	46
N-target x N-allsets =	**644**

where N-target is the number in the target set and N-allsets is the number in the target set and all of the query sets.

Comparisons	Test 1	Test 2
Nn	616	580
+ Nm	14	32
+ Self comparisons	14	32
= Total comparisons	**644**	**644**

As seen, the numbers add up right.