Biometrics in a Glimpse

Shireen Y. Elhabian and Aly A. Farag

Computer Vision and Image Processing Laboratory

Department of Electrical and Computer Engineering

University of Louisville

Louisville, Kentucky

September, 2007

Abstract

Biometrics is a science concerned with automating people recognition, either for verification or identification, based on physiological and behavioral characteristics. But what is verification? How it differs from identification? What are physiological characteristics used for people recognition, and what is meant by behavioral characteristics, what are the most commonly used biometrics. Is their other new biometrics in their early stage of development? What are the advantages and disadvantages of each biometric? How can we measure the performance of a biometric system? The answers of all those questions can be found in this report, whose objective is to introduce the reader to biometric science. This report can be considered as a seed point to begin with. By anyway, we do not claim exhaustive coverage of the topic, but at least the general framework of a biometric science can be cleared throughout the following pages.

Table of Contents

Table of Figures **5**
Table of Tables **6**
1. Introduction 7
1. Introduction 7
2. What is Biometrics? **8**
3. Why do we use Biometrics? **9**
4. Person Authentication **10**
4.1 Modes of authentication 10
4.2 Biometric prerequisites 10
5. Biometrics in a glimpse **11**
5.1 Biometric identifiers 11
5.2 Generic framework of a biometric authentication 13
5.3 System performance and design issues. 16
5.4 Competing system design 17
6. Biometric myths **18**
7. Common Biometrics **21**
7.1 Fingerprint Recognition 22
What is it? 22
Advantages and disadvantages 22
Acquisition devices 23
Recognition approaches 24
Fingerprint characteristics 25
7.2 Face Recognition 25
What is it? 25
Advantages and disadvantages 26
Acquisition devices 27
Recognition systems 27
Challenge issues 28
7.3 Speaker Recognition 30
What is it? 30
Advantages and Disadvantages 30
Recognition approaches 31
Characteristics extracted 32
Challenge issues 32
7.4 Iris Recognition 32
What is it? 32
Advantages and Disadvantages 33
Acquisition devices 34
Recognition approaches 34
Iris characteristics 34
7.5 Hand geometry; 35
What is it? 35

Advantages and disadvantages 35
Application challenges 36
Acquisition devices 36
Matching approaches 37
7.6 Signature verification 38
Advantages and Disadvantages 38
Acquisition devices 39
Verification approaches 40
8. Non Common Biometrics 43
8.1 DNA 43
8.2 Retina recognition 44
8.3 Thermograms 45
8.4 Gait 46
8.5 Keystroke 47
8.6 Ear recognition 48
8.7 Skin reflectance 48
8.8 Lip motion 48
8.9 Body odor 49
8.10 Writer recognition 49
9. Multimodal Biometrics 50
10. Performance Evaluation 53
A Final Word 54
References 55

Table of Figures

Figure 1 - Architecture of a typical biometric authentication system 14
Figure 2 - Points of attacking a biometric authentication system 21
Figure 3 - Different ridge patterns 26
Figure 4 - Rapid changes in expression [3] 28
Figure 5 - Face changes over time (aging) [4] 29
Figure 6 - Makeup really makes difference [5] 29
Figure 7 - Different hair styles has an impact over face recognition [6] 29
Figure 8 - Eye illustration 33
Figure 9 - Iris images acquired under ideal circumstances 33
Figure 10 - Iris patterns (iriscodes) [7,8] 35
Figure 11 - Hand geometry challenge issues [10] 36
Figure 12 - Hand-scan device [9] 37
Figure 13 - Visual image of the hand [10] 37
Figure 14 - Examples of signature 38
Figure 15 - Examples of signature acquisition devices 39
Figure 16 - Human retina 44
Figure 17 - Retina scan [11,12] 45
Figure 18 - Visible photograph and two infrared thermograms (with different color pallets), [13] 46
Figure 19 - Walking silhouette [14] 46
Figure 20 - Model-based approaches (left- structural information, right – modeling information) [16] 47
Figure 21 - Examples of lip motion [15] 49
Figure 22 - Examples of multimodal biometrics 51

Table of Tables

Table 1 - Examples of authentication modes 11
Table 2 - Biometric Identifiers 12
Table 3 - Commonly used biometrics 41

1. Introduction

One day, a mother had to go to buy some groceries, but she had to leave her young children on their own in the house without any elder person who might take care of them. Before she came out of the door she told them "*do not open the door to anybody except you are sure that it's me who is knocking …",* and she agreed with them upon a sign in order to know whether the knocking person is their mother or someone strange who might hurt them.

Such a situation might happen in any family during everyday life. When scrutinizing the situation, the mother wants her children to recognize the knocking person depending on predefined sign in order to take a decision whether such person is their mother or an intruder. Moreover the knocking person might not be a strange person, he might be their uncle for example, but perhaps the mother did not want for their uncle to enter the house especially when she is out. So the situation does not only include people recognition (to know exactly who is knocking) but also it includes authentication (verification) of the knocking person and deciding whether he is authorized to enter the house or not.

To be more precise, *recognition* is a generic term, it does not necessarily imply either verification or identification, and simply it is concerned about *again knowing* a person who has been previously known. While *verification/authentication* is a task of attempting to confirm an individual's claimed identity by comparing what is presented by that person with what is stored about such a person (referring to the mother's story, it is a process to verify that the knocking person is the mother through asking him to present the predefined sign and comparing it with the sign of their mother). *Identification* is the task of determining the identity of an individual, where the individual does not claim anything here.

So methods of recognizing people have existed for centuries, moreover it is a process possessed by human beings since they were born. People can recognize each other through different signs, or scientifically speaking lets refer to it as features or characteristics, such characteristics might include the face, the eyes, the pattern of walking, the voice and other characteristics that allow a person recognize others in a very

intuitive way. Nevertheless the applications of such recognition are not limited to just recognize that the knocking person is my mother, the spectrum of application become wider everyday, ranging from logical access to a personal computer to controlling the access of physical locations (laboratories, buildings, … etc).

However, the means for automating such process is fairly new, dating only to the early of 1960's. Automated people recognition became possible within the last few decades with the advancement of computer processing capabilities. This is when the science of *biometrics* came into existence.

In this report, we present a quick glimpse to biometrics, starting with what is it in the first place (section 2), why it is necessary such that we can not rely on just IDs and passwords (section 3). Section 4 introduces the concept of authentication along with its modes and what are the necessary conditions to be satisfied in a feature to be denoted as a biometric. Biometrics science is surrounded by a lot of myths, section 6 is devoted to summarizing and discussing some of those myths. Common biometrics, such as fingerprint, face recognition, iris, voice, hand geometry and signature, are covered in section 7, while section 8 presents other non common biometrics which are in various stages of development and maturity. A biometric system can be based on single or multiple biometrics, section 9 introduces the concept of multimodal biometrics, giving a general discussion of commonly used approach for biometric fusion. Section 10 covers the general ideas of performance evaluation of biometric systems including the definitions of common performance metrics used in such application.

2. What is Biometrics?

Biometrics is a general term used to describe a characteristic and a process. *A biometric* is a measurable biological/physiological and behavioral characteristic that can be used for automated recognition. While as a process, *biometrics* is a process of recognizing an individual based on his or her distinguishing characteristics (biometrics).

Biometrics is the science of identifying or verifying the identity of a person based on his own physiological and/or behavioral characteristics.

Physiological biometrics includes God created characteristics *possessed* by the individual such as fingerprints and hand geometry. While behavioral biometrics refer to characteristics *acquired* by the individual throughout his life time, such as signature and pattern of walking (gait), in other words they refer to a way of some action carried out by the individual and extend over time, so they are dependent on one's state of mind or even subject to deliberate alteration.

Physiological biometrics (e.g., iris, fingerprint, hand geometry, retinal blood vessels, DNA) are strong modalities for person identification due to the reduced variability and high complexity of the biometric templates used. However, these physiological modalities are usually more invasive and require cooperating subjects. On the contrary, behavioral biometrics (e.g., voice, gait, keystroke dynamics, signature, handwriting) are less invasive, but the achievable identification accuracy is less impressive due to the large variability of the behavior-derived biometric templates.

However, one might ask what is the difference between biometrics and forensics? Both involve people recognition, so why they are considered different!!! Biometrics is automated people recognition process which takes place to the pre-event situation, such as gaining access to sensitive information or to a secured facility. While forensic applications typically occur after a crime has occurred, and may not use fully automated methods. Forensic methods are often used to assist in the adjudication/legal process which requires days of processing compared to seconds for biometrics, and are held to much higher accuracy requirements.

3. Why do we use Biometrics?

But in the first place, why do we use biometrics and not just use IDs and passwords to identify people!!! Passwords might be forgotten or compromised, IDs might be lost, and cards might be lost, forged or even misplaced. So identification of people based on what they know or what they have is insufficient. *Normally* people do not loose their

fingerprints, their faces or their voice, or even they wo not forget their gait in their home, so it is obvious that any reliable person identification should include biometric identification. It has been agreed on by the government and the industry that biometric identification is now becoming a fact of life [1, ch1]. However, such an emerging technology is surrounded with great expectations, but also by myths and misunderstandings. It is probable that such technology might die before being completely matured because of its failure to live up with such high expectations introduced by its strongest proponents.

4. Person Authentication

4.1 Modes of authentication

Verifying the identity of a person, i.e. person authentication, can be achieved either by what a person physically have, i.e. *possessions*, such as keys, passports and smartcards, or by what a person knows, i.e. *knowledge*, such as passwords and pass phrases, or by what a person is, i.e. *biometrics*, such as physiological and behavioral characteristics of an individual that discriminate a person from another. Possessions, knowledge, and biometrics are called *modes of authentication*

Authentication modes can be used in combination to impose higher levels of accuracy. For example, a passport which is a possession can be used with a face and signature biometrics to verify the identity of an individual. On the other hand, individual identification is only based on biometric measurements by comparing such measurements to the entire database of the previously enrolled individuals. Table 1 shows some of the existing user authentication modes (methods) with some advantages and disadvantages of their use.

4.2 Biometric prerequisites

The effectiveness of a biometric, and therefore, the effectiveness of a biometric authentication system are affected by several attributes as outlined by Bolle et al [1, ch1]. Every person should have the biometric characteristic, *(universal biometric)*, in the mean time, no two persons have the same biometric measurement, i.e. using discriminative

features *(unique biometric)*. The biometric should be invariant over time, or how could we identify an individual with variable measurement!!! *(permanence)*. The biometric should be collectable in the sense of being measured with some practical sensing device. Moreover, the biometric should be acceptable among people; a particular population might have strong objections to measuring certain biometrics.

Table 1 - Examples of authentication modes

Authentication Mode	Examples	Pros and Cons [1]
What you have (Possession – *P)*	User IDs, Cards, Badges, Keys	Can be shared Can be duplicated May be lost or stolen
What you know (knowledge – *K)*	Password, PIN code, Personal knowledge	Passwords easy to guess Can be shared May be forgotten
What you have and what you know (*P,K*)	User ID + Password ATM card + PIN code	Can be shared PIN is a weak link especially when written on the cards
What you are (Biometric – *B)*		Not possible to share Forging is difficult Can not be stolen or even forgotten

5. Biometrics in a glimpse

5.1 Biometric identifiers

Biometric identifier is a commonly used term to refer to biometric characteristics which are used to automatically identify people. As mentioned before, biometric characteristics/identifier can be divided into two broad categories according to the nature of the characteristic, either physiological or behavioral characteristic. However there is another way of classification according to the way of its extraction from the individual, either *extra venous* or *intra venous* characteristics, where intra venous characteristics extraction requires certain purpose devices to enter the human body, which is not acceptable by many people either from the health or social point of view. In this report we are mainly concerned about extra venous characteristics which can be acquired with minimal contact with sensors. Table 2 shows the most six commonly used biometrics and other biometric identifiers which are either used less frequently or that are still in the early stages of research.

Table 2 - Biometric Identifiers

Biometric Identifier	Physiological	Behavioral	Extra venous	Intra venous	Common	Uncommon
Face	√		√		√	
Fingerprint	√		√		√	
Hand Geometry	√		√		√	
Iris	√		√		√	
Signature		√	√		√	
Voice		√	√		√	
DNA	√			√		√
Ear Shape	√		√			√
Odor	√		√			√
Retina	√			√		√
Skin Reflectance	√		√			√
Thermogram	√					√
Gait		√	√			√
Key Stroke		√	√			√
Lip Motion		√	√			√

The retina biometric is often confused with the iris, while in reality, the iris and retina require different sample acquisition. The latter requires the image of inside the eye which needs medical doctor examination, while the former requires less intrusive sensing devices.

But the question now why is there so many different biometric modalities (technologies)?!! Why do not we identify people by just using their face or fingerprint?!! The most straight answer would be with different applications and environments, having different constraints forces the use of different biometric technologies. For instance, fingerprint samples require user cooperation; whereas, a face image can be captured by surveillance camera. Furthermore, fingerprints are not available for many of the suspects on watchlists. There are also multiple biometric modalities for technical and financial reasons. Therefore, wide varieties of biometrics are being researched and are available on the market.

5.2 Generic framework of a biometric authentication

Any biometric authentication system can be viewed as a pattern recognition system, following four basic processes; collection (acquisition), extraction, comparison and decision. *Collection* involves using a sensor (biometric reader) to capture traits and convert them to a digital form. *Extraction* (feature extractor) takes the digital data and compute salient attributes from the input signal, converting the distinctive features into a compact template, usually referred to as biometric template. *Comparison* (feature matcher) measures the likeness of the template to those in the database. Based on the likeness, the system *decides* whether or not the submitted biometric matches one of the templates in the database.

Basically, an authentication system consists of two subsystems; one for *enrollment* and one for *authentication*. During enrollment, biometric measurements are captured by the acquisition sensor (biometric reader) and converted to a digital form from which discriminative features are extracted to form the biometric template which is stored in a database along with some form of ID of the subject. While during authentication, a recognition of a subject at a later stage is performed, whether in context of identification of one person from among many (one-to-many matching), or verification that a person biometric matches a claimed identity (one-to-one matching). Figure 1 shows the architecture of a typical biometric authentication system consisting of the enrollment subsystem and the authentication subsystem which can be used either for identification or verification. Taking into account that the biometric reader differs according to the biometric identifier at hand.

Biometric identification

It is only based on biometric characteristics. This system has a direct access to a database containing biometric templates (representations) which are previously enrolled in the system. Biometric templates may contain representations of multiple biometric samples per individual. Furthermore, biometric identification system has the capability of searching the database, through feature (biometric) matcher, for entries that resemble the

incoming biometric measurements, resulting in a candidate list of subject identifiers form the database that have major likeness to the input biometric.

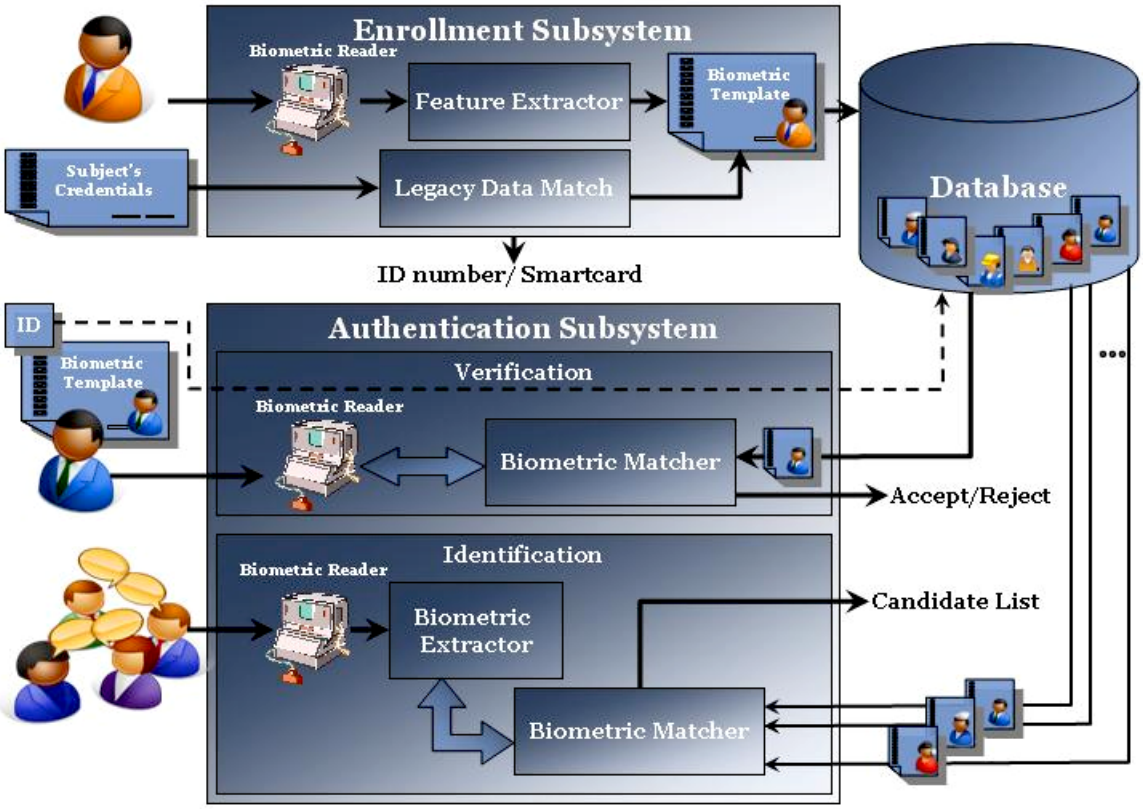

Figure 1 - Architecture of a typical biometric authentication system

Biometric identification system can be used in two different modes; *Positive identification* – determining that a given individual is a member of the biometric database. *Negative identification* – determining that a given individual is *not* a member of some negative database (watchlist), such database could be, for instance, the "most wanted" database, negative identification is commonly referred to as *screening*. Different modes of operation imply different performance measures to be taken into account. Furthermore, each mode requires different conditions regarding the size of the candidate list returned by the matching engine, for example, in case of positive identification, the size is required to be just one candidate, While in case of negative identification, the list size is required to be as small as possible to be examined by human operators.

Biometric verification

Biometric verification differs from identification in the sense of the matching strategy where the presented biometric is only compared with a single previously enrolled biometric template, the use presents a token which indicate one template from the database for comparison, an ID for example. Likewise the identification system, a verification system has a direct access to the biometric database, however a distinct identifier (ID number) is associated with each template in order to facilitate the retrieval process.

For verification systems, there are two possible configurations of the biometric database; *Centralized database* – where a central database stores the biometric information of all enrolled subjects, so the user presents some identify token allowing the retrieval of the corresponding biometric template to be compared with the newly presented biometric sample. *Distributed database* – where the user presents some biometric device containing a single biometric template directly to the system, e.g. smart card. The system compares the biometric information stored on the device with the biometric sample newly presented from the user. In practice, many systems may use both kinds of database; a distributed database for off-line day-to-day verification and a central database for card-free, online verification, or simply to allow lost cards to be reissued without having to re-enroll the subject.

Biometric enrollment

Biometric enrollment can be viewed as a registration process where subjects are presented to the enrollment system and biometric templates are extracted to be stored in the biometric database for future identification/verification.

Enrollment system can be used to achieve different objectives; *Positive enrollment* is used for to perform verification and positive identification. The main objective here is to construct a database of eligible subjects where criteria of subject eligibility should be predefined, e.g. a peaceful subject with no crime records. Biometric samples and other credentials (such as age, gender, race … etc) are stored in the database which in case of

verification might be a distributed database. The subject is issued an ID number or some possession that contains the biometric template. *Negative enrollment,* however is essentially used for negative identification. The main objective here is to construct a database of ineligible subjects for some application where the ineligibility criteria mainly depend on the application itself. The database is centralized by definition; it will be nonsense for someone to have a card proving that he is ineligible. Biometric samples and other credentials are stored in negative identification databases, where the enrollment process is usually done in a covert fashion, i.e. without the subject's cooperation or even knowledge.

The legacy data match module is mainly concerned about matching an input subject to these so-called "seed document" and other legacy data, this involves most likely manual labor and hence human visual matching, which is a potential source of error due to imperfections of humans and their procedures.

5.3 System performance and design issues.

The design of a biometric authentication system should satisfy the basic design specifications of any pattern recognition system. Bolle et al. [1, ch1] summarize them into four points; system accuracy, computational speed, exception handling and system cost.

System accuracy; in a verification system, does the system correctly accept a previously enrolled individual and correctly reject an intruder? However in an identification system, the system accuracy can not be exactly measured, it can be only estimated.

Computational speed; how fast the system makes a decision? Usually it is important to know if the system is scalable from small populations to large ones.

Exception handling; which involves a manual matching process, either due to the choice of the user not to use the biometric system or due to failure to enroll/acquire events. The exception rate is usually hard to estimate a priori. Somehow in the design, it should be

specified what exception rate is acceptable and how the exception process is implemented.

System cost; including the costs of the authentication system components, the operating personnel, routine operation and system maintenance.

There are other specifications that ca not be defined precisely due to the sensitivity of biometric data, among of them which are *security* and *privacy;* where security is mainly concerned about how much secure is the biometric data, in what ways can the biometric system be attacked and what is the system reaction when attack happened. Provided that the biometric data is not used as a tool for abuse, biometric system is supposed to provide privacy for individuals, persevering ones anonymity.

There are a variety of design questions can be arisen here, such as how to achieve the lowest exception handling rate? How to acquire biometric measurements with minimal user contact? What behavioral and physiological characteristics that can be extracted from the acquired measurements which guarantee a high level of discrimination among individuals? How to choose the internal representation of the data (data structure) to facilitate the feature matching procedure and to minimize storage requirements? And in the first place how to choose the feature matching procedure to guarantee high level of accuracy?

5.4 Competing system design

With scrutinizing the abovementioned requirements, we will find that the biometric authentication system has to satisfy contradicting requirements. A biometric system has to guarantee security, which implies accuracy, without compromising too much on the convenience of its uses, and it has to do this cost effectively.

Usually, when someone is assigned to a task of designing a biometric system, a lot of questions pop up; which biometric is the best for the given application? When measuring the system performance in terms of error rates, how to interpret such errors in a qualitative manner according to the biometric used? And how to set thresholds of error

acceptance? Additionally, biometrics is surrounded by a lot of myths and misconceptions, of which are outlined in the next section.

6. Biometric myths

Bolle et al [1, ch8] has outlined some of the most prevalent myths surrounding biometrics, we take the advantage to summarize them here before into deep discussion of the biometric technologies (modalities):

Biometric X is the best for all applications; there is not single biometric so-called the best one for all applications, there are many factors that should be taken into consideration when selecting the most appropriate biometric for the application at hand, among of them user circumstances, size of user population, society acceptance, and system cost. Therefore the effectiveness of a biometric technology is dependant on the how and where it is used. Each biometric technology has its own strengths and weaknesses that should be evaluated in relation to the application before implementation.

It is also important to note that biometric technologies are in varying stages of maturity. For example, fingerprint recognition has been used for over a century while iris recognition is a little more than a decade old. It should be considered that maturity level has nothing to do with which technology is the best, i.e. less mature biometric does not mean at all that this technology is not good, but such level might be used as an indicator of which technology has more implementation experience.

Biometric X is unique for each individual; it is true that each person's biometric is unique if and only if analyzed with sufficient detail. However, with resolution and data storage limitations, in addition to practical limitations on the ability to compare the sensed data, as well as inherent intra-personal variations over time due to aging, all these limitations make this statement not fully true in all conditions. On the other hand, in any reasonable biometric system, it is rare for any two people to have identical biometric representations, it is also extremely unlikely that two measurements of the same person would give identical representations. Consequently, tolerance should be an important feature of a

practical biometric system to overcome such problems, allowing matching of biometrics despite measurement noise and temporal variation.

A single number quantifies system accuracy; if this were true, it will be a piece of cake to compare matchers and give a precise decision regarding which matcher to use. However, this is not the case, the error rates which are merely numbers should be interpreted in the context of the biometric technology in use along with the application at hand.

Our system is "plug and play"; a biometric authentication system is mainly dependent on the database of biometric templates, in the system design phase, the system is trained using training samples, which could be limited in terms of size and actual variety, so when the system firstly installed it should take its time to adapt to the actual operating environment, to be tuned to the sensing devices and acquisition circumstances.

Real accuracy performance can be predicted; real accuracy prediction means that the system is trained using the actual population, or at least the actual user population and the acquisition environment are precisely modeled a priori, which is not the typical case in many biometric systems. Therefore, real accuracy performance can not be predicted in the design phase, it can be merely estimated.

The vendor reporting best error rates has the most accurate system; vendors might report system accuracy results which may be misleading. First of all, the data used for evaluation may be collected under unrealistic and controlled conditions. So it would be much better to compare different systems on standard public domain databases to establish realistic performance evaluation. Second, even if standard databases are used in the evaluation phase, there is no guarantee that such reports were for the entire set, it might be reported for a subset of the data or without following a standard testing protocol.

Multiple biometrics outperform single biometrics; intuitively, using multiple biometrics per individual and moreover using multiple samples per biometric might be beneficial, however there is no guarantee that this actually outperform single biometrics, this might impose much overhead with no significant impact to the system performance.

Our biometric system does not use a decision threshold; any biometric authentication system should include a decision phase to decide whether the incoming individual is accepted or not. Such decision is mainly dependent on the result of feature matcher, so how such decision could be taken without defining a threshold to indicate the acceptance level of matching!!!

Our feature extractor can be used with any match engine; different features might have common representation, but they are different in terms of their physical meaning and their nature. A matching engine mainly concerned about measuring the distance between features in the context of their feature spaces. So having different features derived from different feature spaces will inherently impose using different matching engine, even if apparently features have common representation and different matchers have common base (measuring distance).

Large templates mean better accuracy; system accuracy by no way a function of the biometric template. Moreover, large templates might deteriorate system performance, since having large template means more precise details for an individual; this might affect the system tolerance to biometric variation for an individual. Therefore large templates are not necessarily a merit.

Face recognition prevents terrorism; no technology can provide 100% guarantee, the current state of face recognition is still far from being completely matured. Lots of research is still being conducted to reach to acceptable level of maturity. In fact, there have been several face recognition test at US airports and public place which show that the face biometric still needs much further study.

Biometrics means 100 percent security; no system is 100 percent foolproof, especially when taking into account the attacks of professional hackers. Figure 2 shows stages of authentication system and enrollment system and points of possible attack in a generic biometric system. The reader is encouraged to refer to chapter 12 [1] for more elaboration of possible attack points and some offered solutions.

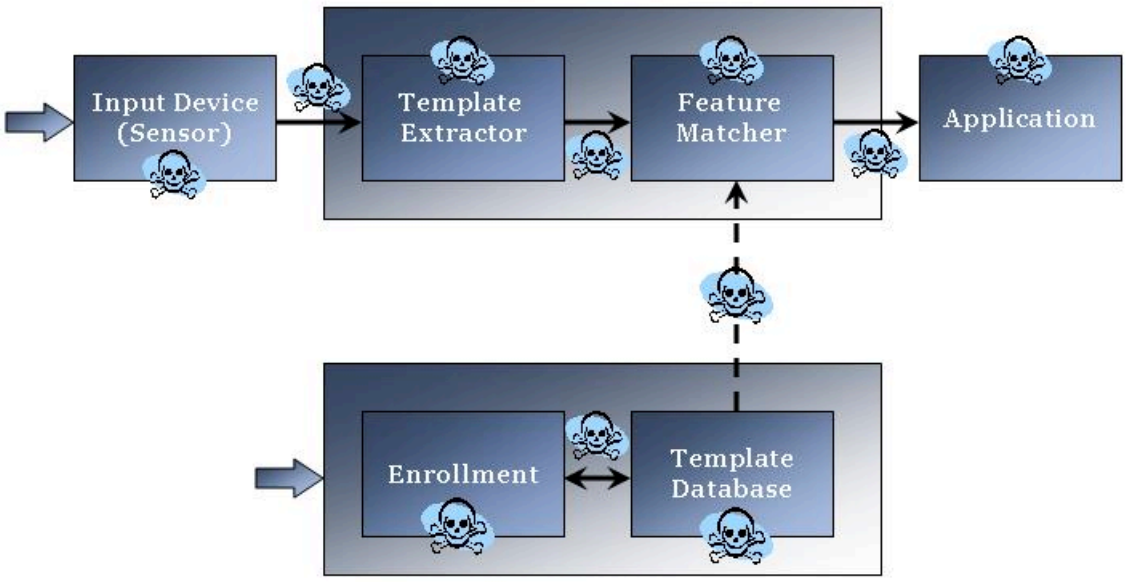

Figure 2 - Points of attacking a biometric authentication system

Biometric systems invade our privacy; many Supreme Court findings imply that the use of biometrics does not invade an individual's civil liberties or privacy, although personal viewpoints are subjective and may differ. A well thought biometric system implementation should consider those issues in the design phase.

Biometric sensors are unhygienic or otherwise harmful; most of biometric acquisition devices require human contact. Most stated health concerns are actually similar to those encountered in everyday life (touching a fingerprint sensor is roughly equivalent to touching a doorknob). Retina and iris scanners do not shine lasers into the eye, and in those systems that do provide illumination there is no indication that this is in anyway harmful [1, ch8].

7. Common Biometrics

In this section we provide a brief description of the six most widely used/discussed biometric. These most commonly used automated biometric identifiers are (1) fingerprint, (2) face, (3) voice, (4) hand geometry, (5) iris and (6) signature. For these six biometrics, we describe the characteristics (behavioral/physiological) that is being measured, pointing to the advantages and disadvantages of using such biometric identifier, the

devices used to measure the biometric, the features which are extracted to represent it, as well as a brief indication of the algorithms used to compare two samples of the biometrics. Table 3 summarizes the commonly used biometrics discussed in the following subsections.

7.1 Fingerprint Recognition

What is it?

The skin structure of the inside surface of human hands contain minute ridges of skin with furrows between each ridge, in order to facilitate the perspiration process and provide a gripping surface. One can not imagine if we were created with hands of flat inside surface, how we could sense things by touching. Fingerprints are weakly determined by genetics, which explains different fingerprints for twins. Within the forensic community, it is believed that no two people have identical ridge details, which is the main reason behind using fingerprints as a discriminative feature to identify people, especially in law-enforcement identification applications.

Advantages and disadvantages

Fingerprint is being used for a long time for identification in law enforcement. However, there are some recent challenges to the premise of uniqueness. The two fundamental premises on which fingerprint identification is based are (i) fingerprint details are permanent; and (ii) fingerprints of an individual are unique. The validity of the first premise has been established by *empirical* observations and is based on the anatomy of ridge skin. However it is the second premise that is being challenged in recent court case. The individuality of fingerprint has been widely accepted based on manual inspection, however such individuality assumption has not been rigorously proved in a scientific way. The reader is encouraged to refer to chapter 14 in [1] for more details regarding fingerprint individuality.

Due to its widespread, there exist large legacy databases of fingerprints, in the meantime, a number of US states are working to establish a fingerprint biometric system for driver's licenses.

Fingerprint lends itself to forensic investigation where criminals most probably leave a trail of fingerprints that allows reconstruction of facts after the events take place.

A major advantage of such biometric identifier is the low cost needed for its acquisition using low-tech means requiring little space. Moreover, the conversion of fingerprints into digital images is getting easier, better and cheaper with the continuous advance in digital scanners.

However, fingerprints suffer from bad reputation due to its apparent relationship to the individual criminal history. In addition to health concerns considered when touching a sensor used by countless individuals. Besides in some countries, fingerprints are associated with illiterate people who use them instead of signatures.

The quality of the fingerprint itself is dependant on the age, occupation and lifestyle of the individual. Technical problems also exist due to the sampling process which is a matter of pressing the finger against the platen of a fingerprint reader. For those who are without fingers or without a full set of them, fingerprints can not be used for their identification, but such a case is very rare.

Acquisition devices

Fingerprint acquisition has been possible for centuries in the form of impression of inked fingers on paper and direct impressions in materials like clay or paper. However over the last decade, many novel techniques have been developed to acquire fingerprint without the use of ink. The main theme of ink-less methods is sensing the ridges on a finger which are in contact with the surface of a scanner, usually called “livescan” fingerprint scanner. Such systems are mainly based on four main technologies, summarized as follows;

Frustrated total internal reflection (FTIR) and other optical methods; such technology is the oldest livescan method, where a camera acquires the reflected optical signal from the ridge as it touches the scanner surface. The main problem with such technology is that the reflected light is a function of skin characteristics. If the skin is wet or dry, the fingerprint

impression can be saturated or faint, consequently hard to process. However such problems can be diminished when using ultrasound instead of visible light, but the resulting system would be bulkier.

CMOS capacitance; based on the fact that the ridges and valleys of a finger create different charge accumulation when the finger touches a CMOS chip, with suitable electronics, such charges can be converted to intensity values. However CMOS devices are sensitive to electrostatic discharge and scratching. The image also tends to be affected by the skin dryness and wetness.

Thermal sensing; it measures temperature changes due to ridge-valley structure as the finger is swiped over the scanner and produces an image. Such technology is based on the fact that skin is considered a better thermal conductor than air; therefore there will be noticeable thermal change on the scanner surface when touched by the finger skin. Skin characteristics will not affect the scanner's output; however, the resultant image is not rich in gray scales, i.e. very narrow dynamic range.

Ultrasound sensing; an ultrasound beam is scanned across the finger surface to measure directly the depth of valleys from the reflected signal. Skin conditions do not affect the imaging process. However these devices tend to be very bulking and require longer scanning time than the optical scanners.

Recognition approaches

A fingerprint authentication system reports some sort of a distance measure between two fingerprint images, such a measure, whether similarity or dissimilarity measure, should be invariant to scaling, rotation, the pressure applied and elastic distortion between impressions due to the elasticity of the finger skin. Fingerprint matching has been studied over several decades by many researchers. However there are two broad classes of matching techniques; image-based and feature-based techniques. *Image-based techniques* include image correlation techniques using different image transformations. Such techniques become more important when the area of the finger that is sensed is small as with CMOS sensors [1, ch3]. While *feature-based techniques* are based on extracting

interesting landmarks (features) from the fingerprint image, and feature matching approaches are then employed. A third class of matching techniques is recently becoming widely used which combines both image- and feature-based techniques in a unified framework (*hybrid techniques)*.

Fingerprint characteristics

The biometric characteristics that can be extracted from a fingerprint image are classified as physiological characteristics. They are commonly referred to as *minutiae*; which are the points of interest in a fingerprint. Figure 3 illustrates different ridge patterns of individual fingers having minute details, know as minutiae, which distinguish one print from another.

Fingerprint contains special features (minutiae) such as [2]:

- *Rigdge ending;* a ridge that ends abruptly.
- *Ridge bifurcation;* a single ridge that divides into two ridges.
- *Short ridge, island of independent ridge;* a ridge that commenses, travels a short distance then ends.
- *Ridge enclosures;* a single ridge that bifurcates and reunits shortly afterward to continue as a single ridge.
- *Spur;* a bifurcation with a short ridge branching off a longer ridge.
- *Crossover or bridge;* a short ridge that runs between two parallel ridges.

7.2 Face Recognition

What is it?

Identifying people using their faces is used in every day's life nearly by all people. Due to its naturalness and availability (everyone has a face), it has become more acceptable than other biometrics and has been used as an identity guarantee in official documents such as passports and ID cards, and therefore there is a wide public acceptance for such biometric to be used for identification.

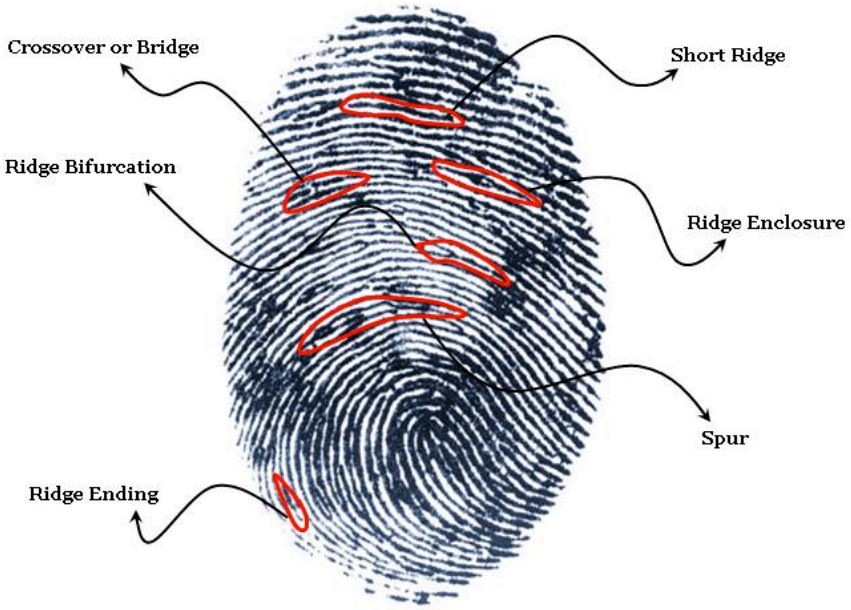

Figure 3 - Different ridge patterns

Advantages and disadvantages

One of its major advantages lies in the biometric sampling (acquisition) process, where contact-less devices are used, even the subject might be unaware of such process, i.e. covert sampling. Face biometric has a variety of information sources; it might be extracted from still images, legacy photograph databases or even videotape. Face recognition can be used for screening of unwanted individual in a crowd in real time (theoretical speaking) and it can be used for small-scale verification applications, where the verification process can be checked by normal humans, i.e. no experts needed for results verification.

However, there are disadvantages, and might be considered challenging issues, when using face as a biometric identifier. The face needs to be well lighted by controlled light sources in the first place in order to acquire high quality images. Face performs better in case of verification but poor results achieved when used as a pure identification biometric, since it can be obstructed by hair, glasses, hats, scarves … etc. Variances, such as disguising, makeup, change over time (aging), expression and pose, might have from minor to major negative impact on a face recognition system, decreasing its ability to recognize faces.

Acquisition devices

Faces could be acquired using different image acquisition modes; single image, video sequence, 3D image and near infrared.

Single image; optical methods, include digitizing hardcopy photographs using digital scanners, are important since legacy data is mostly available in the form of still images. Analog and digital cameras could also be using in the face acquisition process. In most cases, such process is done with user cooperation and under controlled lighting conditions to normalize the appearance of the samples in the database.

Video sequence; surveillance cameras (overtly or covertly used) can be used to acquired video sequences which include face information. However such cameras suffer from low resolution and low frame rate, and therefore no much information can be extracted from their output. Recent research in tracking algorithms taking the advantages of pan-tilt-zoom cameras improved the resolution by physically zooming on suspected faces.

3D image; such images can be used for face recognition techniques which are based on skin or skull geometry. There are various techniques for acquiring 3D face images among of them stereo imaging.

Near infrared; infrared illumination (low-power, i.e. invisible to human eye) can be used to obtain robust imaging under poor lighting conditions.

Recognition systems

Face recognition systems generally start with face localization procedure, where faces are detected in the scene based on weak models of the human face, where modeling is accomplished using facial texture, then face normalization takes place, where estimation for translation, scaling and in-plane rotation is performed.

Once prospective face has been localized, face recognition approaches start its journey; here approaches are mainly divided into two broad categories; face appearance-based and face geometry-based.

Face appearance-based; the main theme of such approaches is dealing the face as a whole, by capturing the distinctiveness of the face without being sensitive to noise such as illumination variation. To do this, a face image is transformed into a space of basis functions, know as eigenfaces.

Face geometry-based; here the face is viewed as a collection of components placed in a certain order following a certain geometry, so the face is not grossly dealt with, instead the face is modeled in terms of particular face features such as eyes, lips, nose … etc and the geometry of the layout of these features.

Challenge issues

Despite all research conducted in the area of face recognition, it still far away from being sufficiently accurate for large population identification when compared with fingerprint and iris recognition. There are still challenging issues that hinder identifying people using their faces. One clear issue here is the appearance similarity of an identical twin. In general the challenges for face recognition can be broken into four broad categories of variations which should be handled by any robust face recognition system.

Physical appearance; which include rapid changes in expression (figure 4), slow changes like aging (figure 5) and personal changes such as makeup (figure 6), changes in hairstyle (figure 7), glass wearing and intentional disguises.

Figure 4 - Rapid changes in expression [3]

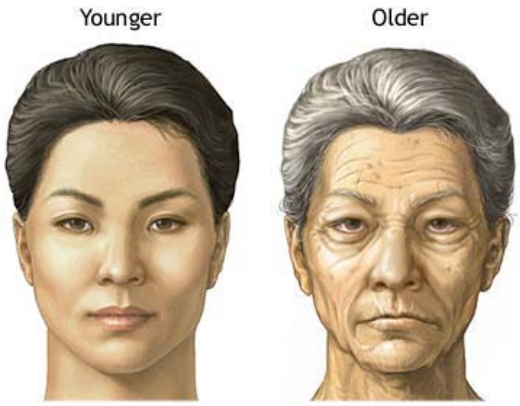

Figure 5 - Face changes over time (aging) [4]

Figure 6 - Makeup really makes difference [5]

Figure 7 - Different hair styles has an impact over face recognition [6]

Acquisition geometry; the general case is the face in the image is of unknown location, in-plane rotation, size (scale) and pose. All such variations introduce a host of differences of appearance of a face from one image to the next.

Image conditions; variances in lighting conditions and camera characteristics and parameters may further change the appearance of a face in an image.

Compression artifacts; image degradation might occur as a result of lossy image compression techniques utilized for efficient image storage/transmission and subsequent decompression. Commonly used image compression algorithms (e.g. JPEG) are not mainly designed to preserve the appearance of the human face. This can significantly impact the performance of face recognition algorithms on archived data such as legacy databases and broadcasted video.

There is not current face recognition system that can claim handling all those challenges, however research has been conducting to handle such challenges by imposing several constraints on the problem definition and using controlled image capturing environment. In practice, the performance is not yet high enough for a reasonable degree of automation without forcing constraints.

7.3 Speaker Recognition

What is it?

Speaker recognition, also referred to as voiceprint recognition or simply voice recognition, attempts to identify people by how they sound when speaking. Taking into consideration that this is totally different from speech recognition, despite using the same front-end processing, speech recognition is mainly concerned with what is spoken in terms of words not who is speaking. Like face recognition, using voice for identification is very attractive and popular due to its prevalence in human communication during day-to-day use. Naturally, the human brain is very good at exploiting the context to narrow down the possibilities.

Advantages and Disadvantages

Besides being a natural biometric like face, voice sampling can be accomplished quite unobtrusively. There exists great public acceptance of this biometric due to its naturalness and little association with identifying criminals. Voice biometric also requires

inexpensive, commonly used hardware for its acquisition which facilitates its deployment without a need for extra human training.

However the use of such biometric is threatened by imitations by skilled impersonators, unlike with signature, there is not much of a discipline for voice testing using real forgeries. With advances in the field of text-to-speech, it becomes possible to create nonexistent identities with machine voices especially when using remote enrollment and authentication. Like face, voice recognition is dependent on the acquisition conditions, such as background noise, channel noise (from phone lines, wireless transmission or severe compression) and unknown channel or microphone characteristics. Such biometric can not be used in case of people who can not talk due to injury, temporal loss of voice, physical or mental abnormalities or even deafness.

Recognition approaches

After speech signal acquisition takes place, the microphone output is first digitized, then feature extraction phase begins to separate the speech from non-speech portions, such as silence, in the signal. The recognition phase is then commenced. Speaker recognition approaches are generally divided into four broad classes. *Template-based* approaches which have template matching framework. They have the highest accuracy, however it can not be plugged and played, it should be trained first to generate the templates, and it is also limited to the words and phrases used in the training session, i.e. fixed-text-based systems. *Nearest neighbor* matcher computes the matching score as the sum of distances between the query vector (incoming speech signal) and the *k* nearest neighbors (reference templates) corresponding to the speaker's identity, it is mainly used in the verification systems. *Neural network* based matcher develop more precise decision boundaries but require extensive data driven training to discriminate the speakers. HMM based are commonly used in speech signal, encoding not only the features themselves but also the evolution of the features over the course of utterance, but again, require large amounts of training data.

Characteristics extracted

Voice is a behavioral biometric but is also dependent on the underlying physical traits, which govern the type of speech signals we are able to utter. Properties like the fundamental frequency (pitch period) which is a function of the vocal tract length can be explicitly estimated from the individual's speech signal. Other features such as nasal tone, inflection … etc are also speaker dependent.

Ideally, the features chosen for speaker recognition should have the minimum variability within an individual and the maximum variability within others, i.e. a discriminative feature. Features should be stable over time, difficult to disguise or mimic, robust to transmission and noise, relatively easy to extract and measure, and occur frequently in the speech samples.

Most speaker recognition systems extract some form of frequency-based features similar to those used in speech recognition systems, such as the use of spectral analysis and Fourier coefficients to generate cepstral features.

Challenge issues

A voice biometric can be corrupted by the physical and emotional state of the subject as well as by environmental issues. That's the main reason behind limiting the use of voice as a biometric. Like face recognition, speaker recognition is most likely used in the verification systems, while speaker identification still in its early stages of maturity.

7.4 Iris Recognition

What is it?

The colored part of the eye bounded by the pupil and sclera is the iris, which is extremely rich in texture (see figure 8 for illustration and figure 9 for examples). Like fingerprints, the appearance of the iris is weakly determined by genetics, even identical twins have different iris texture. However unlike fingerprints, there is no elastic distortion from one sample to the next. It is also believed that it is highly stable over lifetime.

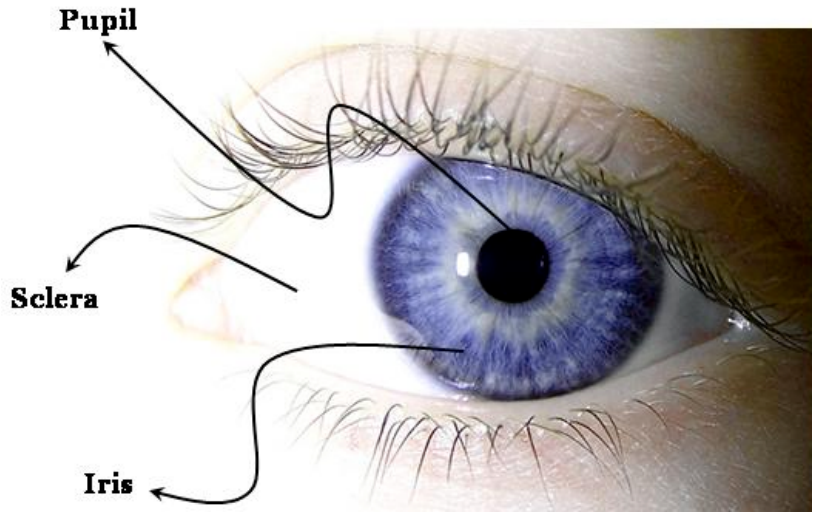

Figure 8 - Eye illustration

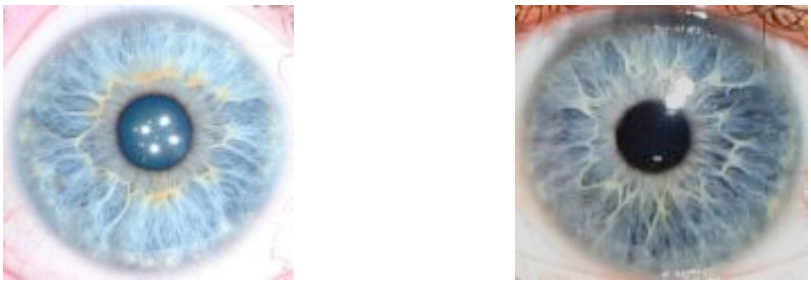

Figure 9 - Iris images acquired under ideal circumstances

Advantages and Disadvantages

Iris might be a good biometric for pure identification applications, since it currently claimed the most accurate biometric in terms of false accepts rate [1, ch8]. Unlike fingerprint, iris acquisition process does not require physical contact to the sensor, unobtrusive and distant cameras can be used. Iris as a biometric has received public acceptance since it has no relationship to the individual criminal history like fingerprints. Moreover it does not involve high training costs.

On the other hand, there are no or few legacy databases due to its recent use, thus there does not exist much legacy infrastructure. Though iris might be a good biometric for identification, however large-scale deployment is impeded by lack of installed base. User cooperation is needed in the sampling process, in addition to expensive input devices, so

covertly identifying people using their iris, if possible, will have high cost. Moreover, iris is easily obscured by eyelashes, eyelids, contact lenses and reflections from the cornea. In addition, it ca not be used for forensic applications since such biometric is not left as evidence on the crime scene. It would be difficult or even impossible for those who miss on or both eyes. Besides iris verification (ground truthing) can not be performed by human operators.

Acquisition devices

An iris image capture device has a lot of challenges to deal with; ideally it should be user friendly and yet capture the iris image with minimal variance to the lighting conditions. The iris device should further handle the specular reflection off the eyeballs. It should also deal with glasses and contact lenses. Capturing techniques are generally classified into two approaches; one of them is first to find the human face in the image then using pan-tilt-zoom camera capabilities to get high-quality image of the iris. While the majority of current commercial systems follow the second approach which require the user to position his/her own eyes within the field of view of a single narrow-angle camera.

Recognition approaches

Iris matcher computes a normalized Hamming distance, i.e. a simple count of bit differences, between two iris templates. The normalization factor uses the mask to discount the areas where the images have been observed to be noisy. Since hamming distance is fast (dealing with binary codes), it can be used in identification as well as verification applications.

Iris characteristics

In order to extract the physiological features from the iris image, iris itself should be located in the acquired image, typically by estimating the center of the pupil and the center of the iris over an image pyramid of different scales until the estimates converge to a single point. The isolated iris is then demodulated to extract its phase information. Phase is used instead of amplitude due to its invariance to imaging contrast and illumination. Then for each iris contrast independent 2k bits (256 bytes) are computed,

another 2k bits representing a mask for the noisy areas of the image is also computed to improve matcher accuracy (figure 10).

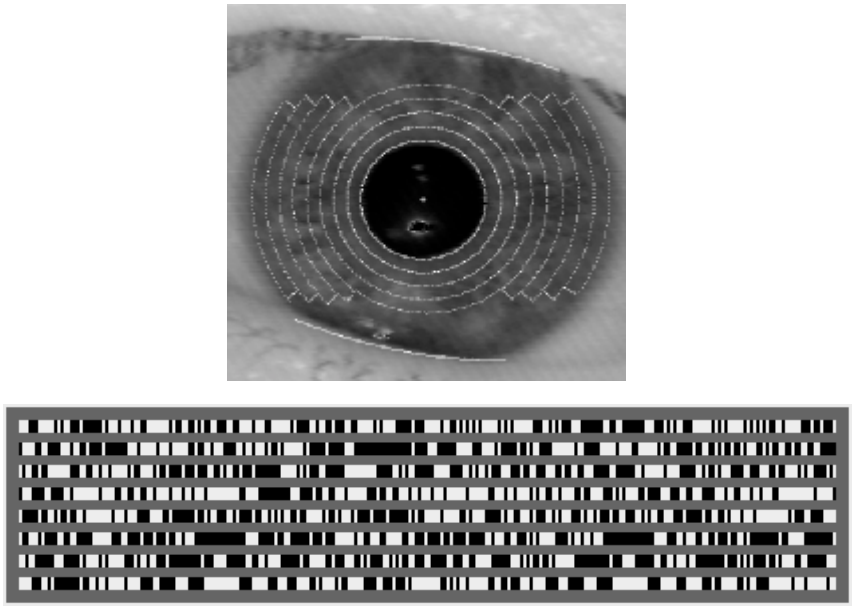

Figure 10 - Iris patterns (iriscodes) [7,8]

7.5 Hand geometry;

What is it?

Hand geometry refers to the geometric structure of human hand, including length and with of the fingers, aspect ratio of the palm or fingers, width and thickness of the palm. The existing commercial system does not take advantage of any other hand features other than the geometrical features, e.g. skin color [1, ch3]. Moreover, hand geometry biometric does not include any detailed features of the hand such as skin wrinkles which fall into the area of palm print verification and finger print recognition.

Advantages and disadvantages

Unfortunately hand features are not discriminative features for people authentication, yield high false accept and reject rates. Yet despite these error rates, hand recognition systems are surprisingly widespread due to its user-friendliness, however there is debate as to whether hand geometry is truly a biometric or not.

Hand geometry biometric is attractive due to its availability, i.e. every one has hands, except for those with disabilities. The sampling process is relatively easy (do-it-yourself operation) compared to that of iris and retina. It enjoys certain amount of public acceptance due to its use in Disney World.

It is suitable for verification especially when combined with other biometrics; however it can be used widely in identification applications due to its insufficient distinctiveness.

On the other hand, hand geometry, as with fingerprint, is measured through physical contact with the user, which causing public hygiene concerns. In addition, hand-scan devices usually occupy a large amount of physical space.

Application challenges

Hand geometry has major challenge issues that lend itself to be an exhaustive research area. First of them its variability over the lifespan of the individual especially due to age conditions. An individual jewelry may pose challenges in extracting correct features. The physical size of a hand geometry-based system is large thus can not be used in applications like laptop computers (figure 11).

Figure 11 - Hand geometry challenge issues [10]

Acquisition devices

Intuitively, hand images can be more reliably captured using other sensing modalities such as thermal devices (figure 12), however, the existing hand measurement acquisition devices typically rely on visual images of the hand (figure 13). To enroll a person in the

database, typically two snapshots of the hand are taken and the average of the resulting features is computed and stored.

Figure 12 - Hand-scan device [9]

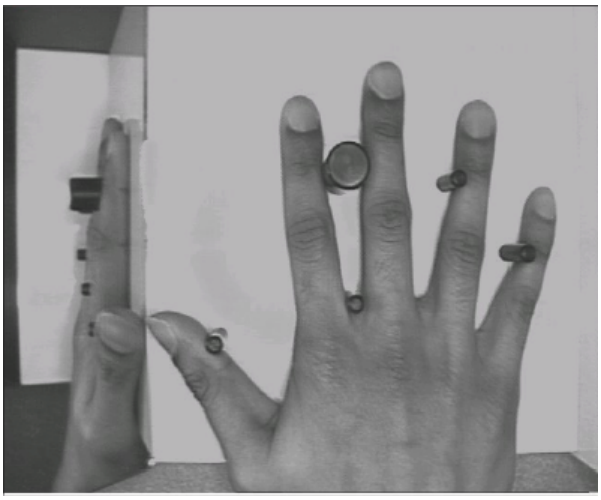

Figure 13 - Visual image of the hand [10]

Matching approaches

To match hands, a newly acquired hand measurements is compared with claimed identity (verification applications), four different distance metrics are commonly used which are absolute, weighted absolute, Euclidean and weighted Euclidean.

7.6 Signature verification

Signature is a behavioral biometric which was used even before the advent of the computers. It has been widely used in document authentication and transaction authorization such as checks and credit card receipts. It can be viewed as some sort of writer recognition. Figure 14 shows some examples of signature. The user (signatory) is the one who have the ability to choose the degree of distinctiveness and uniqueness of his signature. However, the permanence of signature is questionable since a person can change his or her signature at any time, even the signature itself might change according to illness, emotion or aging conditions.

False accept rate is the most important rate as far as the signature verification community is concerned. Unlike other biometrics, the level of impersonating sophistication is clearly defined by the false accept rate for signature biometric; they are broadly classified into zero-effort forgery, home-improved forgery, over-the-shoulder forger and professional forgery.

Figure 14 - Examples of signature

Advantages and Disadvantages

Signature is a man-made biometric, thus forgery can be detected even when the forger has managed to get a copy of the authentic signature. Since enrollment requires physical existence of the signatory, so impersonation of existing identities can be detected at the enrollment time. The need for training is intuitively known and accepted by public. Moreover, signature verification in general does not required high storage requirements and even it has a fast response compared to other biometrics. Signature verification is independent of the user's native language compared to voice recognition. Signature itself

has the merit of combining two modes of authentication, what you know (what is written) and what you are (how you write it), where both can be chosen and even changed by the user. Nevertheless very high compression rates do not affect the signature shape.

However, for more accurate results, expensive electronic devices needed for dynamic signature verification, in addition, the effectiveness of signature for access control using the state-of-art input devices is unknown [1, ch8]. Moreover, some people have difficulty in maintaining an stable signature throughout their lifetime due to insufficient capability of writing consistently.

Acquisition devices

Automated signature verification systems are divided into two branches; *offline* and *online* systems according to the sensing modality. *Offline* systems are used to verify static signatures from paper documents which are scanned using standard camera or scanner. While *online* systems acquire dynamic signatures written with an electronically instrumented device and the dynamic information (pen tip location through time) is usually available at high resolution, even when the pen is not in contact with the paper, see figure 15 for examples.

Figure 15 - Examples of signature acquisition devices

Verification approaches

Signature verification approaches are mainly based on features extracted from the signature to decrease the sensitivity of the system results to signature image variability due to minor changes, i.e. image-based matching approach will be more sensitive to such changes. However the features differ according to the sensing modality, where in case of offline (static) signature acquisition, the only available information is the signature images, so features like number of interior contours and number of vertical and horizontal slope components are used, which are very vulnerable to forgery. On the other hand, online (dynamic) signature acquisition offers more features to be extracted, especially the notion of time beyond just pen position; this is particularly useful in preventing forgery. Approaches to dynamic signature verification include measuring Euclidean distances between pen trajectories, regional correlation matching approaches and probabilistic temporal recognizers such as Hidden Markov Models.

Table 3 - Commonly used biometrics

Biometric Identifier	Features	Recognition Approaches	Devices	Challenge Issues	Pros	Cons
Fingerprint	Ridge patterns (Minutiae)	Image-based Feature-based Hybrid-based	Optical devices (FTIR) CMOS devices Thermal sensors Ultrasound sensors	Skin characteristics (wet or dry, scratched, wounds, age and discharge) affect the sampling process. Touching the sensor causes distortion during the acquisition process.	Widely used, however uniqueness is not proved scientifically. Large legacy databases exist. It lends itself to forensic investigation. Low-cost acquisition devices requiring little space.	Public perception (reputation, health concerns and relation to illiteracy). Quality depends on age, occupation and lifestyle of the individual. Technical problems due to the sampling process. Ca not be used for fingerless people (rare case).
Face	Global face models (gross recognition) Local face models (geometrical face layout)	Face appearance-based (eignfaces) Face geometry-based	Still images; optical devices (scanners for hardcopy, analog and digital cameras) Surveillance cameras for video sequence acquisition Stereo (multiple) cameras for 3D images Infrared devices for near infrared images.	Physical appearance (aging, expression, hairstyle, glasses, makeup, disguise … etc). Acquisition geometry (pose). Image conditions (illumination changes and camera characteristics) Compression artifacts.	Contact-less sampling process Commonly available sensors Large amount of existing data allowing watchlist checks Easy verified by humans	Controlled lighting conditions needed. Obstructed by hair, glasses, hats … etc. Sensitive to light changes, pose, expression and aging.
Voice	Frequency-based features	Template-based k-nearest neighbor neural networks hidden markov models	Inexpensive, commonly used voice sampling devices (microphone, telephony system …)	Background noise. Temporal change of voice due to health conditions and speaker emotional state. Unknown acquisition parameters (channel, microphone) Severe compression.	Public acceptance No contact required Commonly available sensors	Threatened by Impersonators Not sufficiently distinctive for identification over large databases. Possible fake identities enrollment and authentication using machine voice. Its performance depends on the acquisition conditions.

Biometric Identifier	Features	Recognition Approaches	Devices	Challenge Issues	Pros	Cons
Iris	Hamming distance (bit difference count)	Phase information	Distant cameras with PTZ capabilities. Narrow-angle camera.	Obscured by eyelashes, eyelids, contact lenses, glasses, reflections from the cornea. Temporarily changes due to health conditions Controlled lighting needed since iris naturally react differently according to light (its center get wider or narrower according to the intensity of light received)	More accurate biometric in terms of false accept rates. Contact-less sampling process Public acceptance Low training costs	Few legacy databases Expensive sensors User cooperation Easily obscured by eyelashes, lenses, reflections … etc Ca not be used in forensic applications Ca not be sampled for certain people (missing one or both eyes) Ca not be verified by human operators
Hand Geometry	Matching using distance measures (absolute, weighted absolute, Euclidean and weighted Euclidean)	Length and with of the fingers, aspect ratio of the palm or fingers, width and thickness of the palm	Hand-scan devices Commonly-used cameras	Not stable throughout individual lifetime Variant to jewelry Variant to hand orientation (way of positioning it on the sensor)	Availability except for those with disabilities Public acceptance Easy sampling process	Not sufficiently distinctive for identification. Physical contact with the sensor Health concerns Scanners require large physical spac.
Signature	Offline signatures (image-based features such as number of interior contours and number of vertical and horizontal slope components) Online signature (time notation is included in addition to position)	Offline signatures (standard feature matching algorithms can be used) Online signatures (Euclidean distances between pen trajectories, regional correlation matching approaches and probabilistic temporal recognizers such as Hidden Markov Models)	Cameras or scanners for offline or static signature acquisition Electronically instrumented device associated with an electronic pen for online or dynamic signature acquisition	Can be changed (signatory choice) Vulnerable to changes according to the individual emotional state, state of mind and muscle dexterity of the hand, i.e. affected by illness, emotion, and aging.	Man-made biometric so forgery can be detected. Enrollment needs signatory existence, so impersonation can be detected. Public acceptance especially for the training aspect. Fast response verification with low storage requirement. User's native language independent Signature is a combination of what you know and what you are Invariant to high compression rates	Dynamic signature needs expensive hardware. Training needed for using electronic signature devices. Not stable biometric especially for those who could not maintain consistent writing.

8. Non Common Biometrics

The most extreme case for person identification is just having the whole flesh stored in the authentication system, which is of course infeasible in all ways. However what we meant by this extreme is that the more details we know about the person, i.e. higher resolution, the easier and m0re accurate we can identify/verify him. In the preceding section, we have discussed the most commonly used biometrics, some are widely used long ago, others are relatively new, however they are common due to their naturalness, prevalence, public acceptance, and may be easiness. On the other hand, not all of them provide the absolute level of distinctiveness, uniqueness, stability over lifetime and high resolution, and in order to allow them provide such level, more user training is needed, much complicated and expensive devices are required … etc. Scientists began to think of other biometrics to satisfy higher levels of identification, however they are still uncommon and in their early stages of maturity. In this section we will highlight some of those biometrics, nevertheless we do not claim that this list is an exhaustive one, but we have included it just for the sake of completeness.

8.1 DNA

DNA is considered the ultimate biometric due to its absolute level of distinctiveness, since DNA codes identity information of the body cells in a digital form. However, its major drawback is being the same for identical twins. Moreover, practically it is still a slow (in terms of days and weeks), expensive and complex operation to compare identities using two DNA samples. Hence its use as a biometric is limited to forensic applications.

Generally, the basis of DNA matching is the comparison of alternate forms of DNA sequences found at predetermined point in nuclear genetic material. Intuitively, any difference between enrolled and test samples indicates a difference of identity.

Privacy is an important issue in DNA identification, since DNA encodes information that might be used for purposes other than identification, such as medical conditions and the individual vulnerability to certain diseases.

8.2 Retina recognition

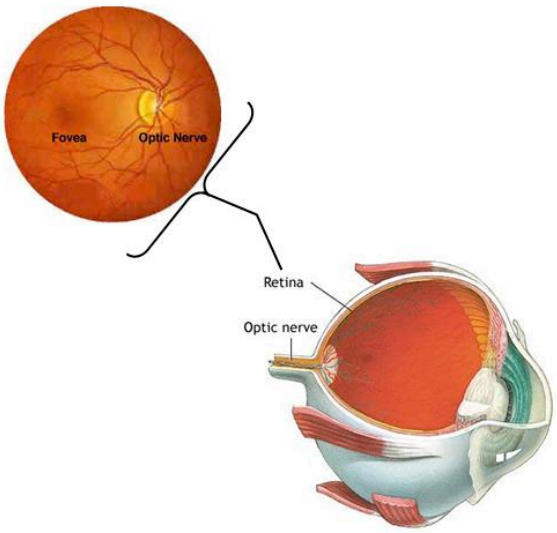

Figure 16 - Human retina

Retina recognition is mainly concerned with comparing images of the blood vessels in the back of the human eye to identify a person (figure 16). Retina image can be acquired using a low-intensity light source through an optical coupler and scans the unique pattern of the layer of blood vessels. Like iris scan, retina scanning is considered accurate in the sense of being unique to each individual, but unlike iris scan, it typically requires the user to look into a receptacle and focus on a given point (see figure 17), which is inconvenient for those who wear eyeglasses or are concerned about close contact to an optical device, in addition to the need of expensive sensors compared to those needed for other biometrics. As a result, retina scanning is not the most user-friendly process even though the biometric itself is very accurate for use in identification and verification. It is also important here to note that retina images can not be reliably formed for eyes suffer from strong astigmatism or very poor eyesight. A great advantage of the retina for identification is the fact that it is a permanent structure, unaffected by anything but the most traumatic accident, and can be considered impossible to alter. Moreover, the construction of a fake retina is extremely difficult due to its optical properties which are hard to be simulated.

Figure 17 - Retina scan [11,12]

8.3 Thermograms

Thermography is a technology that allows us to visualize the thermal energy emitted from the human body (figure 18). Note how the eyeglasses appear cool because the plastic lenses do not transmit IR energy at these wavelengths and are cooler than the face. In the context of biometry, thermal patterns can be used for people identification, in particular thermal images (infrared-based) of the face. The major advantage of thermograms as compared to visible light images for face recognition is their independence of ambient illumination, so no challenge issues regarding illumination changes and shadowing. Thermograms are invariant to disguise, or at least have the ability to detect certain kinds of disguises.

Like retina recognition, since what is being imaged is beneath the skin, so thermograms can not be forged or modified, they are also robust to aging and are unaffected except by traumatic accidents. However, it really needs expensive sensors.

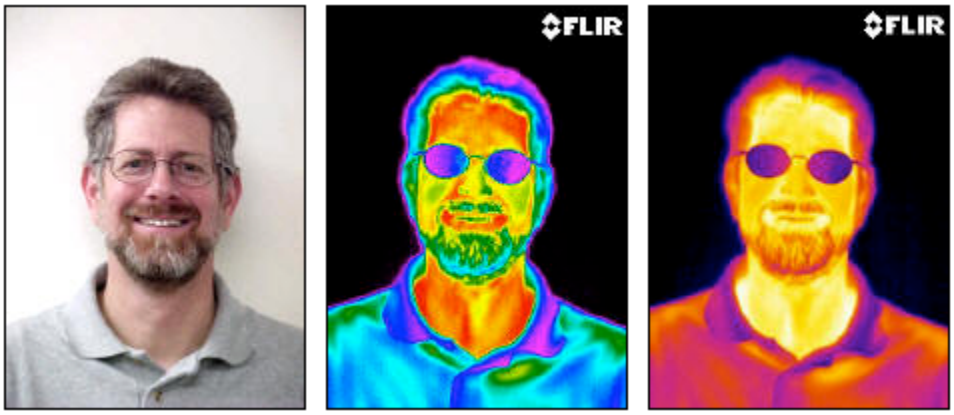

Figure 18 - Visible photograph and two infrared thermograms (with different color pallets), [13]

8.4 Gait

Gait recognition is mainly concerned about identifying people by their pattern of walk (figure 19), which is a behavioral biometric that is still in its development stage. Recognition by gait is actually one of the newest biometrics, since its development only started when computer memory and processing speed became sufficient to process sequences of image data with reasonable performance.

The major strength of such biometric is in its applicability to recognition of people at a distance in video images, so that covert identification might be feasible. In gait recognition, video images are processed to derive numbers that reflect the identity of the moving subject. By using a silhouette, a subject can be described not just by shape but also by motion; an alternative is to model features.

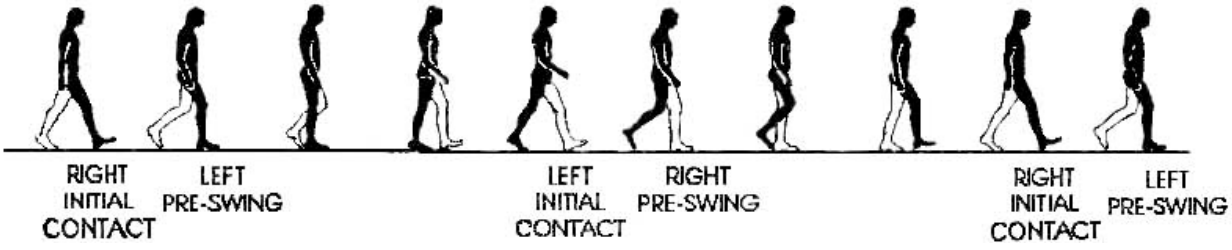

Figure 19 - Walking silhouette [14]

Motion capture equipments such as moving light displays or special marker were initially used, more recently research has been extended to tracking people in less constrained video, however, some work still used special clothing constrain. The main challenge issues in such biometric are

inherited from people tracking problem, where illumination changes, shadowing, occlusions …. etc really impact the performance of gait recognition systems. The current state of the art can achieve over 90% identification rate under situations where the training and test data are captured under similar conditions, while recognition rates with change of clothing, shoe, surface, illumination, and pose usually decrease performance and are the subject of much of the current literature [16]. Gait recognition approaches are roughly classified into two broad classed; *model-free* and *model-based* approaches. The approaches derive the human silhouette by separating the moving object from the background. Then, the subject can be recognized by measurements that reflect shape and/or movement. *Model-free* approaches (referred to as silhouette-based) have the frame work of feature matching (similarity measure) between observed walk patterns. On the other hand, *model-based* approaches impose a model of the gait sequence (figure 20), and process a period of gait information.

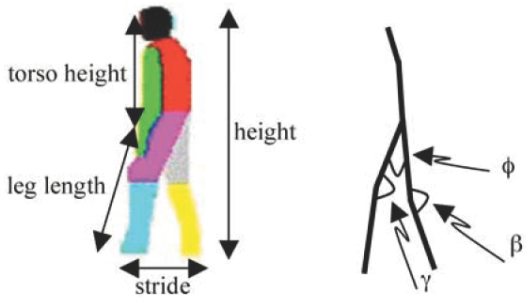

Figure 20 - Model-based approaches (left- structural information, right – modeling information) [16]

8.5 Keystroke

Keystroke identification is the identification of a person by his personal typing style, which is also a behavioral biometric. Features like time between keystrokes, the hold time of keys in certain contexts and commonly unmistaken keys (or using the backspace button) can be used for modeling the keystroke pattern of an individual, which might show less variation for a given typist than across the population in general. Like in speaker recognition, such systems can be fixed-text based, i.e. asking the user to type certain text and extract features from his typing style. However, such biometric is limited in its use; it ca not be generalized to all individuals, as far as computer literacy is in concern, but at least it has its own applications since it can be used with other biometrics or even other authentication modes, e.g. using password to login and at the same time, matching the keystroke style of the individual.

8.6 Ear recognition

Ear is a new class of biometrics, which has certain advantages over face and fingerprint, For example, its structure is stable throughout individual's lifetime and it does not change its shape with facial expressions. Furthermore, ear is larger in size compared to fingerprints but smaller as compared to face and it can be easily captured from a distance without a fully cooperative subject. However it can sometimes be hidden with hair, cap, turban, muffler, scarf, and earrings. Ear recognition approaches can be classified either 2D or 3D recognition, where 2D intensity images are used in 2D-based systems; however, their performance is greatly affected by the pose variation and imaging conditions. On the other hand, the ear can be imaged in 3D using a range sensor which provides a registered color and range image pair [17]. A range image is relatively insensitive to illuminations and it contains surface shape information related to the anatomical structure, which makes it possible to develop a robust 3D ear biometrics. In both approaches, the general framework of an ear recognition system is first ear detection followed by ear recognition (i.e. assigning it to an individual).

8.7 Skin reflectance

Light undergoes scattering and absorption in skin. The depth of light penetration depends on the wavelength of light and the level of pigmentation. Furthermore, the reflectance spectrum of skin provides information regarding the distribution and concentration of various chromophores present in the skin and is highly person dependant. Thus spectroscopic measurements can be successfully used as a biometric. While it can be used by itself, it is much likely used in combination with a fingerprint sensor to make forgery harder.

8.8 Lip motion

Lip motion is a behavioral biometric which captures the lip motion characteristics of people as they speak (figure 21). Like speaker recognition, it can be fixed text, text-dependent, or text independent. It can be used in combination with speaker identification and face recognition to make an accurate system which is extremely difficult to fake. Such biometric finds its application in physical access control, with a user speaking in front of a microphone and video camera. Under controlled lighting conditions, lip motion can be fairly well extracted. However, when the imaging conditions are less controlled, mouth detection in a face video is a difficult take in the

visual light, that's why non-visible bands (infrared and near infrared) are also used for lip-motion imaging.

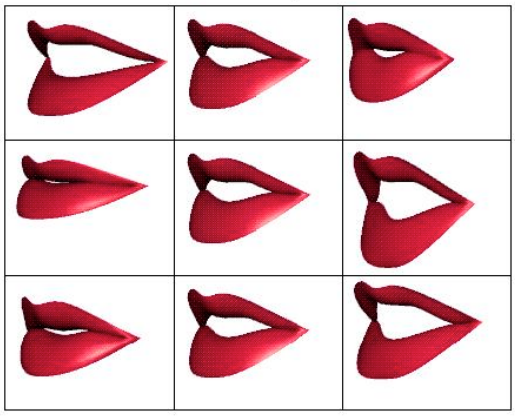

Figure 21 - Examples of lip motion [15]

8.9 Body odor

"I can smell him hundred miles away …" almost a common statement said regarding those having stink body odor. It is almost guaranteed that everyone has been in a situation of disliking somebody due to his body odor, to the extent that such a person is recognizable by such odor. Even such biometric is used by dogs to identify people. Recent advances in semiconductor-based chemical analyses have lead to the development of what so called *electronic noses* that can measure the concentrations of a spectrum of different chemicals. However such sensors do not yet have the range or the sensitivity of the human nose. Furthermore, they suffer from a range of problems such as the need for calibration; they might be fooled by personal change in the body odor due to diet, perfumes, deodorants and sometimes the emotional state. It is not yet clear whether such factors can be normalized away well enough to allow reliable identification of individuals.

8.10 Writer recognition

Scanned images of individual's handwriting can be viewed as a useful behavioral biometric modality to identify people. Such biometric has its own application in forensic and historic document analysis. The feasibility of writer identification and verification is gained from the fact that the variation in handwriting style between different writers exceeds the variations intrinsic to every single writer considered in isolation [18].

One might think of writer identification as some sort of automatic handwriting recognition, like speaker recognition versus speech recognition, handwriting recognition is mainly concerned about what is written by eliminating the variability in writing style which is individual dependent, while *who wrote it* is the main concern of writer identification systems by emphasizing the variability between writers. Handwriting recognition and writer identification therefore represent two opposing facets of handwriting analysis. It is important, however, to also mention the idea that writer identification could aid the recognition process if information on the writer's general writing habits and idiosyncrasies is available to the handwriting recognition system.

Writer identification and verification methods fall into two broad categories: text-dependent versus text-independent methods. The text-dependent methods are very similar to signature verification techniques and use the comparison between individual characters or words of known semantic content. These methods therefore require prior localization and segmentation of the relevant information, which is usually performed interactively by a human user. The text-independent methods for writer identification and verification use statistical features extracted from the entire image of a text block. A minimal amount of handwriting (e.g., a paragraph containing a few text lines) is necessary in order to derive stable features insensitive to the text content of the samples.

9. Multimodal Biometrics

The simplest and most straightforward framework to biometrics is sensing a single sample, e.g. image, of a biometric source, e.g. face, from an individual, such sensed sample is then processed to obtain a recognition result. Hence biometrics so far is concerned about having single sample from single source using single sensor. However, the term *multimodal biometrics* has come into existence, which is used in the literature with various meanings.

Multimodal biometrics would be viewed as two different biometric sources on a person, say face and fingerprint, sensed by different sensors. Two different properties, say infrared and reflected light, of the same biometric source, say the face, would be another example of multimodal. Another might be two different biometric sources, say face and ear, imaged by the same sensor. It might be viewed also as two different properties, say 3-D shape and reflected light, of the same source, say face, sensed by the same sensor. An expansive view would consider all of these

variations as multimodal and consider *multi-biometric* as an equivalent term. Figure 22 illustrates those examples.

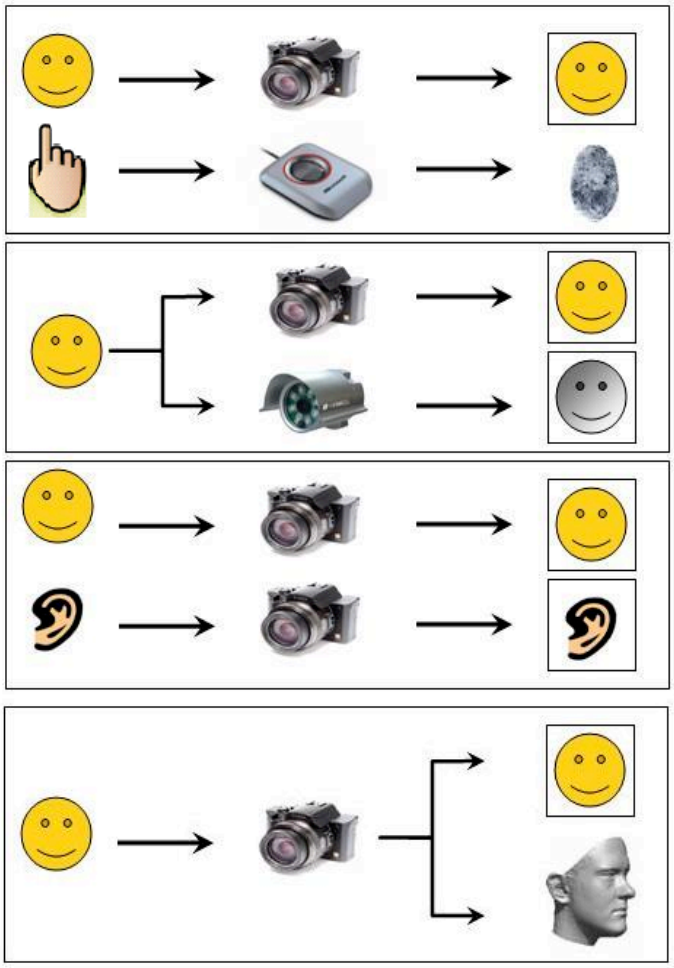

Figure 22 - Examples of multimodal biometrics

As far as simple single biometric is concerned, there is what so called a *multi-algorithm* approach which employs a single sensor, and acquires a single biometric sample. Two or more different algorithms process the single sample, and the individual results are fused to obtain an overall recognition result. The multi-algorithm approach would seem to be attractive, since there is only one sensor and only one sample sensed in order to obtain a recognition result, therefore it minimizes sensor and sensing cost. A variation of the multi-algorithm approach builds an ensemble of multiple instances of the same basic type of algorithm, with intentional random variation between instances.

Another approach might be called *multi-sample* or *multi-instance,* where multiple samples of the same biometric are sensed, the same algorithm processes each of the samples, and the individual results are fused to obtain an overall recognition result.

Compared to multi-algorithm approach, a multi-sample approach has its own advantages and disadvantages. The use of multiple samples may overcome poor performance due to one sample that has unfortunate properties. For example, a person might be blinking in one face image, and this might present problems for the recognition algorithm; if multiple samples in time are used, it is unlikely that the person is blinking in all of them. However, the acquisition of multiple samples requires either multiple copies of the sensor, or that the user be available for sensing over a longer period of time. When compared to multi-algorithm approaches, multi-sample techniques would seem to require either greater expense for sensors, greater cooperation from the user, or a combination of both.

However in case of multimodal biometrics, there should be a scientific approach towards combining multiple biometrics modalities in a unified framework. Bowyer et al [19] classify the multimodal approaches into three broad categories; orthogonal, independent, and collaborative.

The *orthogonal* approach uses biometric sources that involve different parts of the body, e.g. face and fingerprint, where there is little or no interaction between the individual biometrics. As a result, the individual biometrics are combined at the decision level or the score level. In decision-level fusion, a recognition decision is made for each individual biometric, and the individual decisions vote to obtain the overall decision. In score-level fusion, a matching score is obtained for each individual biometric, and the scores are combined to obtain the multimodal decision. In general, score-level fusion must involve a method to normalize the scores from the individual biometrics, followed by a method to combine the scores.

On the other hand, the *independent* approach indicates that the individual biometrics is processed independently of each other. It would seem that orthogonal biometrics is processed independently by necessity. But when the biometric source is the same and different properties are sensed, then the processing may be independent, but there is at least the potential for gains in performance through collaborative processing.

A less common approach to multimodal biometrics is called *collaborative*, which refers to the interaction between the intermediate results of processing the individual biometrics. These approaches are collaborative in the sense that intermediate results of processing in one modality are used to assist the processing in the other modality. In this way, the intermediate results of processing each modality might be used to improve the reliability and accuracy in processing the other.

10. Performance Evaluation

A biometric authentication system merely depends on biometric matching. A matcher is a system that takes two biometric samples and returns a score that indicates their similarity. In a verification system, i.e. one-to-one matching, this score is used as a mean of determining whether the two samples are from the same original "real world" biometric. While in an identification system, i.e. one-to-many matching, the scores are thresholded in order to extract the candidate list from the database.

For erroneous decisions there are two types of errors; false match and false non-match errors, while for correct decision there are other two types of errors; correct match and correct non-match errors, they are defined as follows.

False Match (FM): deciding that two biometrics samples are from the same identity, while they are from different identities; the frequency with which this occurs is called the False Match Rate (FMR).

False Non-Match (FNM): deciding that two biometrics are not from the same identity, while they are form the same identity; the frequency with which this occurs is called the False Non-Match Rate (FNMR).

Correct Match (CM): correctly deciding that two biometric samples match.

Correct Non-Match (CNM): correctly deciding that the samples do not match.

Up to this point we have phrased the errors in terms of matching or not matching biometric samples. However, one could use the more conventional pattern recognition terminology of *False Accept (FA)* and *False Reject (FR)* defined as follows.

False Accept (FA): deciding that a claimed identity is a legitimate one while in reality it is an imposter. The frequency at which false accept errors are made is called the False Accept Rate (FAR).

False Reject (FR): deciding that a claimed identity is not legitimate when in reality the person is genuine. The frequency at which false reject errors are made is called the False Reject Rate (FRR).

The receiver-operating-characteristics (ROC) curve is commonly used to plot the false accept rate versus the false reject rate to determine a desired level of performance. ROC analysis is often employed in verification applications due to it nature, i.e. one-to-one matching process, since ROC curves display the system sensitivity for verifying a particular biometric sample against a particular biometric template. These plots attempt to show the general performance of a matcher over the range of its possible threshold values. The quality of a particular algorithm can be inferred from its ROC plot in several ways. A common approach is to measure the area under the ROC curve. However, the ROC curve approach has several weaknesses. One significant problem is that once an ROC plot is generated, it is impossible to infer the amount or nature of the data considered when creating the plot-information that is clearly important for ascertaining the relevance of the curve. Another problem concerns threshold selection. Many different thresholds are used to generate an ROC plot. From these plots, one can infer to some extent the general behavior of the system in hand and can perhaps gain basic insight into which values may be good thresholds. These plots can vary widely from one application to another, though, and the optimal threshold may drastically change with the situation.

A Final Word

In this report, we have seen different biometrics in various stages of maturity. We have tried to highlight the advantages and disadvantages of each biometric (as far as we know). In fact, almost any physical property of the human being (density, reflectance, emission, absorption …), if it can be defined and measured with sufficient precision, could play the role of a biometric. As discussed throughout this report, there is not single biometric that claim absolute distinctiveness in all cases, each biometric has its own merits and demerits, so to answer what will be next in this field, two scenario might happen, the first one is multimodal biometrics, i.e. using one biometric to diminish the weakness of the other, while the second scenario is forcing each biometric to be

used in its specific application, such as fingerprints, face and signatures can be used in legacy systems while speaker recognition can be used in telephony systems.

Biometrics has many aspects to be covered, a report like that will not by any way claim the coverage of all its aspects, however, our main goal behind those pages is introducing the reader to the biometric science, to be familiar with terminologies, to have the general layout of such area in mind in a complete, yet not exhaustive, way. Our final here is that *we hope that such goal is achieved!!!*

References

[1] Ruud Bolle, Jonathan H. Connell, Sharath Pankanti, Nalini K. Ratha, Andrew W. Senior, "Guide to Biometrics", Springer-Verlag, New York, 2004.

[2] Wikipedia, Minutiae, http://en.wikipedia.org/wiki/Minutiae.

[3] Andriodblues website, http://www.androidblues.com/news.html

[4] Northwestern memorial hospital, http://www.nmh.org/nmh/adam/adamencyclopedia/Imagepages/8691.htm

[5] Flickr makeup site, http://www.flickr.com/photos/melaniumom/393617863/

[6] Curly-hair-styles magazine, http://www.curly-hair-styles-magazine.com/virtual-hair-styles-at-the-hair-style-editor.html

[7] The point group, http://www.thepointgroup.org/biometriciris.shtml

[8] Pictorial examples of iris codes, http://www.cl.cam.ac.uk/~jgd1000/examples.html

[9] www.recogsys.com

[10] http://www.cse.msu.edu/~cse891/Sect601/HandGeometry.pdf

[11] MURDOC online, http://www.murdoconline.net/archives/003620.html

[12] Lazyhorse website, http://www.lazyhorse.supanet.com/~lazyhorse/document/biometricmindcontrol

[13] ITC newsletter, http://www.itcnewsletter.com/Newitc/what_is_IR.htm

[14] www.furl.net

[15] http://www.icp.inpg.fr/~reveret/icp.html

[16] Nixon, M. S.; Carter, J. N., "Automatic Recognition by Gait," *Proceedings of the IEEE* , vol.94, no.11, pp.2013-2024, Nov. 2006

[17] Hui Chen; Bir Bhanu, "Human Ear Recognition in 3D," *Pattern Analysis and Machine Intelligence, IEEE Transactions on* , vol.29, no.4, pp.718-737, April 2007

[18] Marius Bulacu; Lambert Schomaker, "Text-Independent Writer Identification and Verification Using Textural and Allographic Features," *Pattern Analysis and Machine Intelligence, IEEE Transactions on* , vol.29, no.4, pp.701-717, April 2007

[19] Hugo Proenca; Luis A. Alexandre, "Toward Noncooperative Iris Recognition: A Classification Approach Using Multiple Signatures," *Pattern Analysis and Machine Intelligence, IEEE Transactions on* , vol.29, no.4, pp.607-612, April 2007