FI MU

**Faculty of Informatics**
**Masaryk University**

# Biometric Authentication Systems

**by**

**Zdeněk Říha**
**Václav Matyáš**

**FI MU Report Series** **FIMU-RS-2000-08**

**November 2000**

# Biometric Authentication Systems

Václav Matyáš Jr.
Zdeněk Říha

# Contents

# 1 Introduction

Humans recognize each other according to their various characteristics for ages. We recognize others by their face when we meet them and by their voice as we speak to them. Identity verification (authentication) in computer systems has been traditionally based on something that *one has* (key, magnetic or chip card) or *one knows* (PIN, password). Things like keys or cards, however, tend to get stolen or lost and passwords are often forgotten or disclosed.

To achieve more reliable verification or identification we should use something that really characterizes the given person. Biometrics offer automated methods of identity verification or identification on the principle of measurable physiological or behavioral characteristics such as a fingerprint or a voice sample. The characteristics are measurable and unique. These characteristics should not be duplicable, but it is unfortunately often possible to create a copy that is accepted by the biometric system as a true sample. This is a typical situation where the level of security provided is given as the amount of money the impostor needs to gain an unauthorized access. We have seen biometric systems where the estimated amount required is as low as $100 as well as systems where at least a few thousand dollars are necessary.

*biometrics*

This paper presents our conclusions* from a year-long study of biometric authentication techniques and actual deployment potential, together with an independent testing of various biometric authentication products and technologies. We believe that our experience can help the reader in considering whether and what kind of biometric authentication should or should not be used in a given system.

Biometric technology has not been studied solely to authenticate humans. A biometric system for race horses is being investigated in Japan and a company that imports pedigree dogs into South Africa uses a biometric technique to verify the dogs being imported.

*Conclusions and opinions as expressed are those of the authors as individual researchers, not of their past or present employers.

Biometric systems can be used in two different modes. Identity *verification* occurs when the user claims to be already enrolled in the system (presents an ID card or login name); in this case the biometric data obtained from the user is compared to the user's data already stored in the database. *Identification* (also called *search*) occurs when the identity of the user is a priori unknown. In this case the user's biometric data is matched against all the records in the database as the user can be anywhere in the database or he/she actually does not have to be there at all.

*verification*

*identification*

It is evident that identification is technically more challenging and costly. Identification accuracy generally decreases as the size of the database grows. For this reason records in large databases are categorized according to a sufficiently discriminating characteristic in the biometric data. Subsequent searches for a particular record are searched within a small subset only. This lowers the number of relevant records per search and increases the accuracy (if the discriminating characteristic was properly chosen).

*identification*

Before the user can be successfully verified or identified by the system, he/she must be registered with the biometric system. User's biometric data is captured, processed and stored. As the quality of this stored biometric data is crucial for further authentications, there are often several (usually 3 or 5) biometric samples used to create user's master template. The process of the user's registration with the biometric system is called *enrollment*.

*enrollment*

## 1.1 What to measure?

Most significant difference between biometric and traditional technologies lies in the answer of the biometric system to an authentication/identification request. Biometric systems do not give simple yes/no answers. While the password either is 'abcd' or not and the card PIN 1234 either is valid or not, no biometric system can verify the identity or identify a person absolutely. The person's signature never is absolutely identical and the position of the finger on the fingerprint reader will vary as well. Instead, we are told how similar the current biometric data is to the record stored in the database. Thus the biometric system actually says what is the

*not always the same*

probability that these two biometric samples come from the same person.

Biometric technologies can be divided into 2 major categories according to what they measure:

* Devices based on physiological characteristics of a person (such as the fingerprint or hand geometry).

* Systems based on behavioral characteristics of a person (such as signature dynamics).

Biometric systems from the first category are usually more reliable and accurate as the physiological characteristics are easier to repeat and often are not affected by current (mental) conditions such as stress or illness.

One could build a system that requires a 100% match each time. Yet such a system would be practically useless, as only very few users (if any) could use it. Most of the users would be rejected all the time, because the measurement results never are the same[†].

*variability*

We have to allow for some variability of the biometric data in order not to reject too many authorized users. However, the greater variability we allow the greater is the probability that an impostor with a similar biometric data will be accepted as an authorized user. The variability is usually called a (security) threshold or a (security) level. If the variability allowed is small then the security threshold or the security level is called *high* and if we allow for greater variability then the security threshold or the security level is called *low*.

*security threshold*

## 1.2 Error rates and their usage

There are two kinds of errors that biometric systems do:

* False rejection (Type 1 error) – a legitimate user is rejected (because the system does not find the user's current biometric data similar enough to the master template stored in the database).

[†] A hundred percent similarity between any two samples suggests a very good forgery.

- * False acceptance (Type 2 error) – an impostor is accepted as a legitimate user (because the system finds the impostor's biometric data similar enough to the master template of a legitimate user).

In an ideal system, there are no false rejections and no false acceptances. In a real system, however, these numbers are non-zero and depend on the security threshold. The higher the threshold the more false rejections and less false acceptances and the lower the threshold the less false rejections and more false acceptances. The number of false rejections and the number of false acceptances are inversely proportional. The decision which threshold to use depends mainly on the purpose of the entire biometric system. It is chosen as a compromise between the security and the usability of the system. The biometric system at the gate of the Disney's amusement park will typically use lower threshold than the biometric system at the gate of the NSA headquarters.

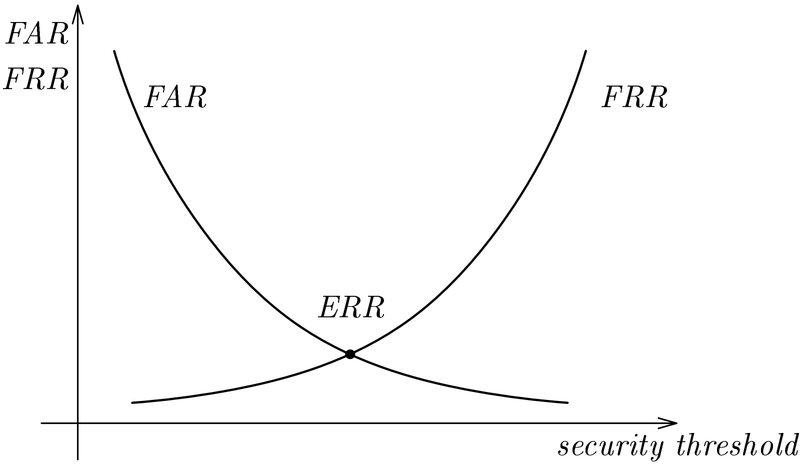
*trade-off*

The number of false rejections/false acceptances is usually expressed as a percentage from the total number of authorized/unauthorized access attempts. These rates are called the *false rejection rate (FRR)/false acceptance rate (FAR)*. The values of the rates are bound to a certain security threshold. Most of the systems support multiple security thresholds with appropriate false acceptance and false rejection rates.

Some of the biometric devices (or the accompanying software) take the desired security threshold as a parameter of the decision process (e.g. for a high threshold only linear transformations are allowed), the other devices return a score within a range (e.g. a difference score between 0 and 1000, where 0 means the perfect match) and the decision itself is left to the application.

*decision process*

If the device supports multiple security levels or returns a score we can create a graph indicating the dependence of the FAR and FRR on the threshold value. The following picture shows an example of such a graph:



The curves of FAR and FRR cross at the point where FAR and FRR are equal. This value is called the *equal error rate (ERR)* or the *crossover accuracy*. This value does not have any practical use (we rarely want FAR and FRR to be the same), but it is an indicator how accurate the device is. If we have two devices with the equal error rates of 1% and 10% then we know that the first device is more accurate (i.e., does fewer errors) than the other. However, such comparisons are not so straightforward in the reality. First, any numbers supplied by manufacturers are incomparable because manufacturers usually do not publish exact conditions of their tests and second even if we have the supervision of the tests, the tests are very dependent on the behavior of users and other external influences.

*crossover accuracy*

The manufacturers often publish only the best achievable rates (e.g., FAR $<$ 0.01% and FRR $<$ 0.1%), but this does not mean that these rates can be achieved at the same time (i.e., at one security threshold). Moreover, not all the manufacturers use the same algorithms for calculating the rates. Especially the base for computation of the FAR often differs significantly. So one must be very careful when interpreting any such numbers.

*comparisons*

The following table shows real rounded rates (from real tests) for three devices set the lowest security level possible[‡]:

[‡] These numbers serve as an example only. Any such numbers depend heavily upon the conditions of the test and are subject to exhaustive discussions. Our numbers were collected during a two week trial in an office environment.

| Rates/devices | A | B | C |
|---|---|---|---|
| FAR | 0.1% | 0.2% | 6% |
| FRR | 30% | 8% | 40% |

This table shows rates (again rounded) for three devices set to the highest security level possible:

| Rates/devices | X | Y | Z |
|---|---|---|---|
| FAR | 0% | 0.001% | 1% |
| FRR | 70% | 50% | 60% |

*not error-free*

Although the error rates quoted by manufactures (typically ERR $<$ 1%) might indicate that biometric systems are very accurate, the reality is rather different. Namely the false rejection rate is in reality very high (very often over 10%). This prevents the legitimate users to gain their access rights and stands for a significant problem of the biometric systems.

# 2 Biometric techniques

There are lots of biometric techniques available nowadays. A few of them are in the stage of the research only (e.g. the odor analysis), but a significant number of technologies is already mature and commercially available (at least ten different types of biometrics are commercially available nowadays: fingerprint, finger geometry, hand geometry, palm print, iris pattern, retina pattern, facial recognition, voice comparison, signature dynamics and typing rhythm).

## 2.1 Fingerprint technologies

Fingerprint identification is perhaps the oldest of all the biometric techniques. Fingerprints were used already in the Old China as a means of positively identifying a person as an author of the document. Their use in law enforcement since the last century is well known and actually let to an association fingerprint = crime. This caused some worries about the user acceptance of fingerprint-based systems. The situation improves as these systems spread around and become more common.

*the oldest*

Systems that can automatically check details of a person's fingerprint have been in use since the 1960s by law enforcement agencies. The U.S. Government commissioned a study by Sandia Labs to compare various biometric technologies used for identification in early seventies. This study concluded that the fingerprint technologies had the greatest potential to produce the best identification accuracy. The study is quit outdated now, but it turned the research and development focus on the fingerprint technology since its release.

*Sandia study*

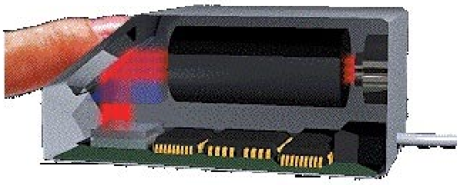
### Fingerprint readers

Before we can proceed any further we need to obtain the digitalized fingerprint. The traditional method uses the ink to get the fingerprint onto a piece of paper. This piece of paper is then scanned using a traditional scanner. This method is used only rarely today when an old paper-based database is being digitalised, a fingerprint found on a scene of a crime is being processed or in

*scanning*

law enforcement AFIS systems. Otherwise modern live fingerprint readers are used. They do not require the ink anymore. These live fingerprint readers are most commonly based on optical, thermal, silicon or ultrasonic principles.

Optical fingerprint readers are the most common at present. They are based on reflection changes at the spots where the finger papilar lines touch the readers surface.



Source: I/O Software [6]
All the optical fingerprint readers comprise of the source of light, the light sensor and a special reflection surface that changes the reflection according to the preassure. Some of the readers are fitted out with the processing and memory chips as well.

The size of the optical fingerprint readers typically is around 10 × 10 × 5 centimeters. It is difficult to minimize them much more as the reader has to comprise the source of light[§], reflection surface and the light sensor.

This is a fingerprint bitmap obtained by an optical fingerprint reader (Securetouch 99 manufactured by the Biometric Access Corporation)

The optical fingerprint readers work usually reliably, but sometimes have problems with dust if heavily used and not cleaned. The dust may cause latent fingerprints, which may be accepted by the reader as a real fingerprint. Optical fingerprint readers cannot be fooled by a simple picture of a fingerprint, but any 3D fingerprint model makes a significant problem, all the reader checks is the pressure. A few readers are therefore equipped with additional detectors of finger liveness.

[§] It actually need not be and often is not *visible* light.

Optical readers are relatively cheap and are manufactured by a great number of manufacturers. The field of optical technologies attracts many newly established firms (e.g., American Biometric Company, Digital Persona) as well as a few big and well-known companies (such as HP, Philips or Sony). Optical fingerprint readers are also often embedded in keyboards, mice or monitors.

Source: ABC [1]
This is an example of the optical fingerprint reader. The “Biomouse Plus” integrated with a smart card reader is able to capture the fingerprint at 500 DPI. It is connected to the paralel port of a computer and costs between $100 and $200.

*silicon*

Silicon technologies are older than the optical technologies. They are based on the capacitance of the finger. The dc-capacitive fingerprint sensors consist of rectangular arrays of capacitors on a silicon chip. One plate of the capacitor is the finger, the other plate is a tiny area of metallization (a pixel) on the chip’s surface. One places his/her finger against the surface of the chip (actually against an insulated coating on the chip’s surface). The ridges of the fingerprint are close to the nearby pixels and have high capacitance to them. The valleys are more distant from the pixels nearest them and therefore have lower capacitance.

Source: Veridicom [18]
Beneath the surface passivation layer is a 300 × 300 array of capacitor plates. The ridges and valleys of a finger are different distances from the capacitor plates. That difference corresponds to a capacitance difference which the sensor measures. The analog-to-digital converter translates that capacitance to into an 8-bit digital value. The resolution of the image is 500 DPI.

Such an array of capacitors can be placed onto a chip as small as 15 × 15 × 5 mm and thus is ideal for miniaturization. A PCMCIA card (the triple height of a credit card) with a silicon fingerprint reader is already available. Integration of a fingerprint reader on a credit card-sized smartcard was not achieved yet, but it is expected in the near future. Silicon fingerprint readers are popular also in mobile phones and laptop computers due to the small size.

This is an example of a fingerprint bitmap image obtained by a silicon fingerprint reader (captured using the “Precise 100 SC” manufactured by the Precise Biometrics) The resolution of the image is 300 × 300 points, 8-bit grayscale.

The fingerprint bitmap obtained from the silicon reader is affected by the finger moisture as the moisture significantly influences the capacitance. This often means that too wet or dry fingers do not produce bitmaps with a sufficient quality and so people with unusually wet or dry fingers have problems with these silicon fingerprint readers.

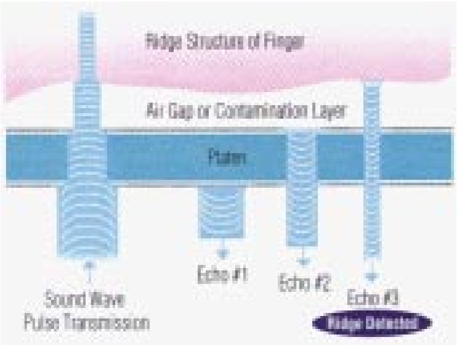
Both optical and silicon fingerprint readers are fast enough to capture and display the fingerprint in real time. The typical resolution is around 500 DPI.

Source: UltraScan [17] This is an example of a fingerprint bitmap image obtained by an ultrasonic fingerprint reader. This image was obtained using the Model 703 ID Station at 250 DPI.

Ultrasonic fingerprint readers are the newest and least common. They use ultrasound to monitor the finger surface.

The user places the finger on a piece of glass and the ultrasonic sensor moves and reads whole the fingerprint. This process takes one or two seconds. Ultrasound is not disturbed by the dirt on the fingers so the quality of the bitmap obtained is usually fair.

Ultrasonic fingerprint readers are manufactured by a single company nowadays. This company (UltraScan Inc.) owns multiple patents for the ultrasonic technology. The readers produced by this company are relatively big (15 × 15 × 20 centimeters), heavy, noisy and expensive (with the price around $2500). They are able to scan fingerprints at 300, 600 and 1000 DPI (according to the model).



Source: UlstraScan [17] Ultrasound has the ability to penetrate many materials. Ultrasonic fingerprint scanner is based on the difference in the acoustic impedance of skin, air and the fingerprint platen. At each interface level, sound waves are partially reflected and partially transmitted through. This penetration produces return signals at successive depths. Low propagation velocities allow pulse-echo processing of return echoes, which can be timed to vary the depth at which the image is captured.

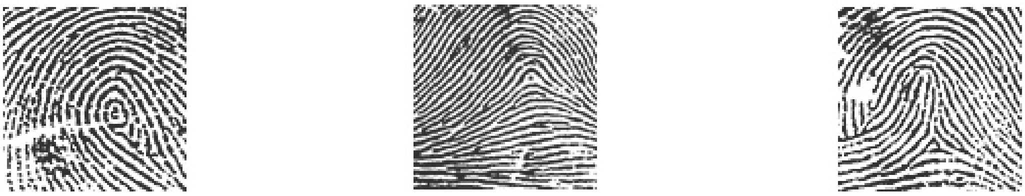
### Fingerprint processing

Fingerprints are not compared and usually also not stored as bitmaps. Fingerprint matching techniques can be placed into two categories: minutiae-based and correlation based. Minutiae-based techniques find the minutiae points first and then map their relative placement on the finger. Minutiae are individual unique characteristics within the fingerprint pattern such as ridge endings, bifurcations, divergences, dots or islands (see the picture on the following page). In the recent years automated fingerprint comparisons have been most often based on minutiae.

*minutiae*

The problem with minutiae is that it is difficult to extract the minutiae points accurately when the fingerprint is of low quality. This method also does not take into account the global pattern of ridges and furrows. The correlation-based method is able to overcome some of the difficulties of the minutiae-based approach. However, it has some of its own shortcomings. Correlation-based techniques require the precise location of a registration point and are affected by image translation and rotation.

*correlation-based*



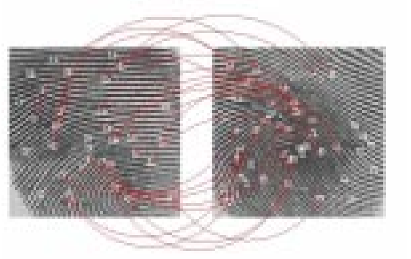
**Loop** **Arch** **Whorl**

Source: Digital Persona [4]
The loop is the most common type of fingerprint pattern and accounts for about 65% of all prints. The arch pattern is a more open curve than the loop. There are two types of arch patterns: the plain arch and the tented arch. Whorl patterns occur in about 30% of all fingerprints and are defined by at least one ridge that makes a complete circle.

The readability of a fingerprint depends on a variety of work and environmental factors. These include age, gender, occupation and race. A young, female, Asian mine-worker is seen as the most difficult subject. A surprisingly high proportion of the population have missing fingers, with the left forefinger having the highest percentage at 0.62% (source: [10]).

Source: PRIP MSU [11]
Fingerprint ridges are not continuous, straight ridges. Instead they are broken, forked, changed directionally, or interrupted. The points at which ridges end, fork and change are called minutia points, and these minutia points provide unique, identifying information. There are a number of types of minutia points. The most common are ridge endings and ridge bifurcations (points at which a ridge divides into two or more branches).

There are about 30 minutiae within a typical fingerprint image obtained by a live fingerprint reader. The FBI has shown that no two individuals can have more than 8 common minutiae. The U.S. Court system has allowed testimony based on 12 matching minutiae. The number and spatial distribution of minutiae varies according to the quality of the fingerprint image, finger pressure, moisture and placement. In the decision process, the biometric system tries to find a minutiae transformation between the current distribution and the stored template. The matching decision is then based on the possibility and complexity of the necessary transformation. The decision usually takes from 5 milliseconds to 2 seconds.



Source: PRIP MSU [11]
The minutiae matching is a process where two sets of minutiae are compared to decide whether they represent the same finger or not.

The speed of the decision sometimes depends on the security level and the negative answer very often takes longer time than the positive one (sometimes even 10 times more). There is no direct dependency between the speed and accuracy of the matching algorithm according to our experience. We have seen fast and accurate as well as slow and less accurate matching algorithms.

*templates*

The minutiae found in the fingerprint image are also used to store the fingerprint for future comparisons. The minutiae are encoded[¶] and often also compressed. The size of such a master template usually is between 24 bytes and one kilobyte.

*AFIS*

Fingerprints contain a large amount of data. Because of the high level of data present in the image, it is possible to eliminate false matches and reduce the number of possible matches to a small fraction. This means that the fingerprint technology can be used for identification even within large databases. Fingerprint identification technology has undergone an extensive research and development since the seventies. The initial reason for the effort was the response to the FBI requirement for an identification search system. Such systems are called Automated Fingerprint Identification Systems (AFIS) and are used to identify individuals in large databases (typically to find the offender of a crime according to a fingerprint found at the crime scene or to identify a person whose identity is unknown). AFIS systems are operated by professionals who manually intervene the minutiae extraction and matching process and thus their results are really excellent. In today's criminal justice applications, the AFIS systems achieve over 98% identification rate while the FAR is below 1%.

[¶] Software suppliers never publish their exact encoding methods. They are usually based on the type of minutiae, its location, the direction and the number of ridges between the minutiae *access control systems*

The typical access control systems, on the other side, are completely automated. Their accuracy is slightly worse. The quality of the fingerprint image obtained by an automated fingerprint reader from an unexperienced (non-professional) user is usually lower. Fingerprint readers often do not show any fingerprint preview and so the users do not know if the positioning and pressure of the finger is correct. The automatic minutiae extraction in a lower quality image is not perfect yet. Thus the overall accuracy of such a system is lower.

*pores*

Some newer systems are based not only on minutiae extraction, they use the length and position of the papilar lines as well. A few system take into account even pores (their spatial distribution), but the problem with pores is that they are too dependent on the fingerprint image quality and finger pressure.

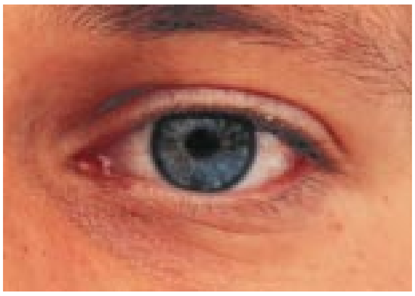
*processing*

Most of the biometric fingerprint systems use the fingerprint reader to provide for the fingerprint bitmap image only, whole the processing and matching is done by a software that runs on a computer (the software is often available for Microsoft Windows operating systems only). There are currently only very few fingerprint devices that do all the processing by the hardware.

*software*

The manufacturers of the fingerprint readers used to deliver the fingerprint processing software with the hardware. Today, the market specializes. Even if it is still possible to buy a fingerprint reader with a software package (this is the popular way especially for the low-end devices for home or office use) there are many manufacturers that produce fingerprint hardware only (e.g. fingerprint silicon chips by Thomson) or software companies that offer device-independent fingerprint processing software (e.g. Neurodynamics). Device-independent software is not bound to images obtained by one single input devices, but their accuracy is very low if various input devices are mixed.

## 2.2 Iris

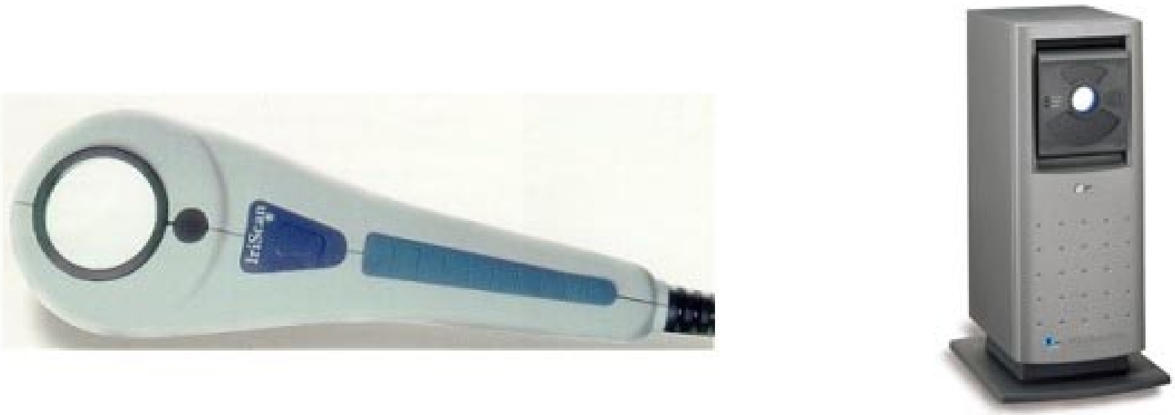


Each iris is a unique structure featuring a complex pattern. This can be a combination of specific characteristics known as corona, crypts, filaments, freckles, pits, furrows, striations. and rings.

The iris is the colored ring of textured tissue that surrounds the pupil of the eye. Even twins have different iris patterns and everyone's left and right iris is different, too. Research shows that the matching accuracy of iris identification is greater than of the DNA testing.

*scanning*

The iris pattern is taken by a special gray-scale camera in the distance of 10–40 cm from the camera (earlier models of iris scanners required closer eye positioning). The camera is hidden behind a mirror, the user looks into the mirror so that he/she can see his/her own eye, then also the camera can "see" the eye. Once the eye is stable (not moving too fast) and the camera has focused properly, the image of the eye is captured (there exist also simpler versions without auto-focus and with a capture button).



Source: Iridian Technologies [7]
The PC iris uses a hand-held personal iris imager that functions as a computer pheripheral. The user holds the imager in his hand, looks into the camera lens from a distance of 10 cm and presses a button to initiate the identification process. The Iris Access is more advanced. It is auto-focus and has a sensor that checks whether an individual has stepped in front of the camera. It is also able to guide the person audily into the correct position.

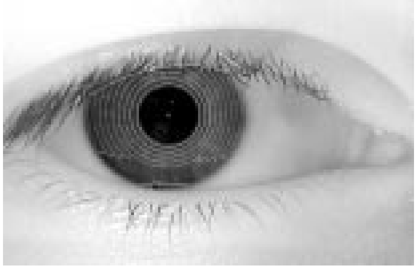
*lighting*

The iris scanner does not need any special lighting conditions or any special kind of light (unlike the infrared light needed for the retina scanning). If the background is too dark any traditional lighting can be used. Some iris scanners also include a source of light that is automatically turned on when necessary.

The iris scanning technology is not intrusive and thus is deemed acceptable by most users. The iris pattern remains stable over a person's life, being only affected by several diseases.

*iriscode*

Once the gray-scale image of the eye is obtained then the software tries to locate the iris within the image. If an iris is found then the software creates a net of curves covering the iris. Based on the darkness of the points along the lines the software creates the iriscode, which characterizes the iris. When computing the iriscode two influences have to be taken into account. First, the overall darkness of the image is influenced by the lighting conditions so the darkness threshold used to decide whether a given point is dark or bright cannot be static, it must be dynamically computed according to the overall picture darkness. And second, the size of the iris dynamically changes as the size of the pupil changes. Before computing the iriscode, a proper transformation must be done.



Source: Iridian Technologies [7]
The iriscode is computed very fast and takes 256 bytes. The probability that 2 different irises could produce the same iriscode is estimated as low as 1 : $10^{78}$ The probability of two persons with the same iris is very low (1 : $10^{52}$).

*speed*

In the decision process the matching software given 2 iriscodes computes the Hamming distance based on the number of different bits. The Hamming distance is a score (within the range 0 – 1, where 0 means the same iriscodes), which is then compared with the security threshold to make the final decision. Computing the Hamming distance of two iriscodes is very fast (it is in fact only counting the number of bits in the exclusive OR of the two iriscodes). Modern computers are able to compare over 4 000 000 iriscodes in one second.

An iris scan produces a high data volume which implies a high discrimination (identification) rate. Indeed the iris systems are suitable for identification because they are very fast and accurate. Our experience confirms all that. The iris recognition was the fastest identification out of all the biometric systems we could work with. We have never encountered a false acceptance (the database was not very large, however) and the false rejection rate was reasonably low. The manufacturer quotes the equal error rate of 0.00008%, but so low false rejection rate is not achievable with normal (non-professional) users.

*discrimination rate*

It is said that artificial duplication of the iris is virtually impossible because of the unique properties. The iris is closely connected to the human brain and it is said to be one of the first parts of the body to decay after death. It should be therefore very difficult to create an artificial iris or to use a dead iris to fraudulently bypass the biometric system if the detection of the iris liveness is working properly.

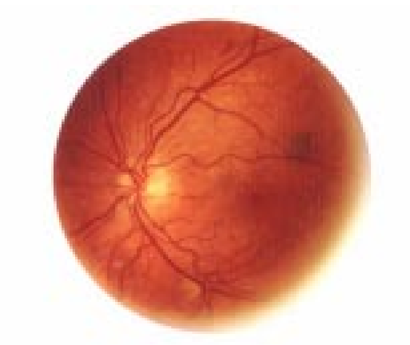
*not easy to forge*

We were testing an iris scanning system that did not have any countermeasures implemented. We fooled such a system with a very simple attack. The manufacturer provided us with a newer version of the system after several months. We did not succeed with our simple attacks then, but we wish to note that we did not have enough time to test more advanced versions of our attack.

A single company (Iridian Technologies, Inc.) holds exclusively all the world-wide patents on the iris recognition concept. The technology was invented by J. Daugman of Cambridge University and the first iris scanning systems were launched in 1995.

Source: Iridian Technologies [7]. Sensar used to be the only licensee, that used the iris recognition process in the financial sector. It signed agreements with ATM manufacturers and integrated its iris regognition products into ATMs. Such ATMs do not require bank cars anymore, the system identifies customers automatically. In 2000 Iriscan, Inc. merged with Sensar, Inc. and changed its name to Iridian Technologies, Inc.

## 2.3 Retina



Source: EyeDentify [5]

Retina is not directly visible and so a coherent infrared light source is necessary to illuminate the retina. The infrared energy is absorbed faster by blood vessels in the retina than by the surrounding tissue. The image of the retina blood vessel pattern is then analyzed for characteristic points within the pattern. The retina scan is more susceptible to some diseases than the iris scan, but such diseases are relatively rare.

Retina scan is based on the blood vessel pattern in the retina of the eye. Retina scan technology is older than the iris scan technology that also uses a part of the eye. The first retinal scanning systems were launched by EyeDentify in 1985.

The main drawback of the retina scan is its intrusiveness. The method of obtaining a retina scan is personally invasive. A laser light must be directed through the cornea of the eye. Also the operation of the retina scanner is not easy. A skilled operator is required and the person being scanned has to follow his/her directions.

*high discrimination rate*

A retina scan produces at least the same volume of data as a fingerprint image. Thus its discrimination rate is sufficient not only for verification, but also for identification. In the practice, however, the retina scanning is used mostly for verification. The size of the eye signature template is 96 bytes.

The retinal scanning systems are said to be very accurate. For example the EyeDentify's retinal scanning system has reputedly never falsely verified an unauthorized user so far. The false rejection rate, on the other side, is relatively high as it is not always easy to capture a perfect image of the retina.

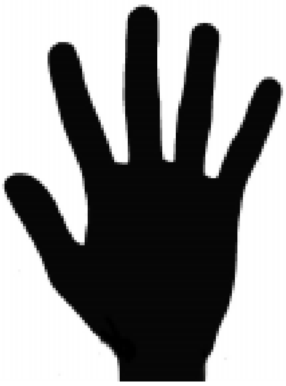
Retinal scanning is used only rarely today because it is not user friendly and still remains very expensive. Retina scan is suitable for applications where the high security is required and the user's acceptance is not a major aspect. Retina scan systems are used in many U.S. prisons to verify the prisoners before they are released.

Source: EyeDentify [5]
The company EyeDentify is the only producer of the retinal eye scanners. It has been founded in the late seventies and since then has developped a number of retina scanners. The current model 2001 is equipped with the memory for 3300 templates and (after the image has been captured) is able to verify an individual in 1.5 seconds or run an identification (withing the stored 3000 templates) in less than 5 seconds.

The check of the eye liveness is usually not of a significant concern as the method of obtaining the retina blood vessel pattern is rather complicated and requires an operator.

## 2.4 Hand geometry

Hand geometry is based on the fact that nearly every person's hand is shaped differently and that the shape of a person's hand does not change after certain age. Hand geometry systems produce estimates of certain measurements of the hand such as the length and the width of fingers. Various methods are used to measure the hand. These methods are most commonly based either on mechanical or optical principle. The latter ones are much more common today. Optical hand geometry scanners capture the image of the hand and using the image edge detection algorithm compute the hand's characteristics. There are basically 2 sub-categories of optical scanners. Devices from the first category create a black-and-white bitmap image of



This is a 2D picture of the hand shape. Most modern systems use all three dimensions to measure the hand's characteristics.

the hand's shape. This is easily done using a source of light and a black-and-white camera. The bitmap image is then processed by the computer software. Only 2D characteristics of the hand can be used in this case. Hand geometry systems from the other category are more sophisticated. They use special guide markings to position the hand better and have two (both vertical and horizontal) sensors for the hand shape measurements. So, sensors from this category handle data from all the three dimensions.

*scanners*

Hand geometry scanners are easy to use. Where the hand must be placed accurately, guide markings have been incorporated and the units are mounted so that they are at a comfortable height for majority of the population. The noise factors such as dirt and grease do not pose a serious problem, as only the silhouette of the hand shape is important. The only problem with hand geometry scanners is in the countries where the public do not like to place their hand down flat on a surface where someone else's hand has been placed.

A few hand geometry scanners produce only the video signal with the hand shape. Image digitalization and processing is then done in the computer. On the other side there exist very sophisticated and automated scanners that do everything by themselves including the enrollment, data storage, verification and even simple networking with a master device and multiple slave scanners. The size of a typical hand geometry scanner is considerably big (30 × 30 × 50 cm). This is usually not a problem as the hand geometry scanners are typically used for physical access control (e.g. at a door), where the size is not a crucial parameter.

Source: Recognition Systems [14]
This is a hand geometry scanner HandKey II manufactured by the Recognition systems, Inc. Special guides use electrical conductivity to ensure that the fingers really touch the pins. Correct position of the fingers is indicated by a led diod on the front pannel.

Hand geometry does not produce a large data set (as compared to other biometric systems). Therefore, given a large number of records, hand geometry may not be able to distinguish sufficiently one individual from another. The size of the hand template is often as small as 9 bytes. Such systems are not suitable for identification at all. The verification results show that hand geometry systems are

*applications*

suitable for lower level security application. The hand geometry systems are used for example at the Disney Theme Parks in the US or were used at the 1996 Olympic Games in Atlanta.

The manufacturers advertise the crossover accuracy about 0.1%. These numbers are difficult to obtain in reality. FAR of 3% and FRR of 10% at the middle security threshold are more realistic.

*accuracy*

The verification takes takes about one second. The speed is not a crucial point because the hand geometry systems can be used for verification only.

## 2.5 Signature dynamics

The signature dynamics recognition is based on the dynamics of making the signature, rather than a direct comparison of the signature itself afterwards. The dynamics is measured as a means of the pressure, direction, acceleration and the length of the strokes, number of strokes and their duration. The most obvious and important advantage of this is that a fraudster cannot glean any information on how to write the signature by simply looking at one that has been previously written.

*dynamics*

Pioneers of the signature verification first developed a reliable statistical method in 1970s. This involved the extraction of ten or more writing characteristics such as the number of times the pen was lifted, the total writing time and the timing of turning points. The matching process was then performed using fairly standard statistical correlation methods. Newer sequential techniques treat the signature as a number of separate events, with each event consisting of the period between the pen striking the writing surface and lifting off again. This approach is much more flexible. If the majority of the signature is accurate and only one[||] event is missing or added then this event can be easily ignored.

There are various kinds of devices used to capture the signature dynamics. These are either traditional tablets or special purpose devices. Tablets capture 2D coordinates and the pressure.

This is a signature. It was captured using a tablet.

[||] Or another small number.

Special pens are able to capture movements in all 3 dimensions. Tablets have two significant disadvantages. First, the resulting digitalised signature looks different from the usual user signature. And second, while signing the user does not see what he/she has written so far. He/she has to look at the computer monitor to see the signature. This is a considerable drawback for many (unexperienced) users. Some special pens work like normal pens, they have ink cartridge inside and can be used to write with them on paper.

*input devices*

**E-pad** **Smartpen**

Source: PenOp [12], Smartpen [9]

These are special purpose devices used to capture the signature dynamics. Both are wireless. The E-pad devices shows the signature on the digital display while the Smartpen has got its own ink cartridge and can be used to write onto any paper.

A person does not make a signature consistently the same way, so the data obtained from a signature from a person has to allow for quite some variability. Most of the signature dynamics systems verify the dynamics only, they do not pay any attention to the resulting signature. A few systems claim to verify both (i.e. the signature dynamics as well as the resulting signature look itself). Our experience shows that if the system does not verify the resulting signature, then the signature that is accepted as a true match may look significantly different from the master template. The speed of writing is often the most important factor in the decision process, so it is possible to successfully forge a signature even if the resulting signature looks so different that any person would notice.

*dynamics vs. look*

We have tried simple attempts to sign as other users as well as simulation of attacks where the attacker has seen a user signing once or several times. Our results show that individuals' ability to fake signature dynamics substantially improves after they see the way the true signers sign.

The size of data obtained during the signing process is around 20 kB. The size of the master template, which is computed from 3 to 10 signatures, varies from around 90 bytes up to a few kilobytes. *size* Even if the size of the master template is relatively high the signature recognition has problems with match discrimination and thus is suitable for verification only.

The accuracy of the signature dynamics biometric systems is not high, the crossover rate published by manufacturers is around 2%, but according to our own experience the accuracy is much worse.

The leading companies in the signature systems are CyberSign, PenOp and Quintet.

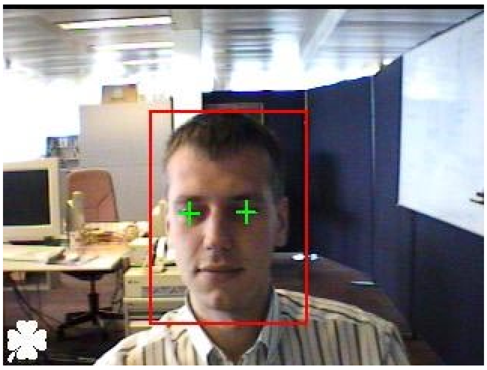
## 2.6 Facial recognition

Facial recognition is the most natural means of biometric identification. The method of distinguishing one individual from another is an ability of virtually every human. Until recently the facial recognition has never been treated as a science. *natural*

Any camera (with a sufficient resolution) can be used to obtain the image of the face. Any scanned picture can be used as well. Generally speaking the better the image source (i.e. camera or scanner) the more accurate results we get. The facial recognition systems usually use only the gray-scale information. Colors (if *image source* available) are used as a help in locating the face in the image only. The lighting conditions required are mainly dependent on the quality of the camera used. In poor light condition, individual features may not be easily discernible. There exist even infrared cameras that can be used with facial recognition systems.

Most of facial recognition systems require the user to stand a specific distance away from the camera and look straight at the camera. This ensures that the captured image of the face is within a specific size tolerance and keeps the features (e.g., the eyes) in as similar position each time as possible.

The first task of the processing software is to locate the face (or faces) within the image. Then the facial characteristics are extracted. Facial recognition technology has recently developed into two areas: *facial metrics* and *eigenfaces*.



After locating the face in the image the system locates eyes within the face region.

Facial metrics technology relies on the measurement of the specific facial features (the systems usually look for the positioning of the eyes, nose and mouth and the distances between these features).

*eigenfaces*

Another method for facial recognition has been developed in the past three years. The method is based on categorizing faces according to the degree of fit with a fixed set of 150 master eigenfaces. This technique is in fact similar to the police method of creating a portrait, but the image processing is automated and based on a real picture here. Every face is assigned a degree of fit to each of the 150 master eigenfaces, only the 40 template eigenfaces with the highest degree of fit are necessary to reconstruct the face with the accuracy of 99%.

The image processing and facial similarity decision process is done by the computer software at the moment, this processing requires quite a lot of computing power and so it is not easy to assemble a stand-alone device for face recognition. There are some efforts (by companies like Siemens) to create a special-purpose chip with embedded face recognition instruction set.

The face region is rescaled to a fixed pre-defined size (e.g. 150 × 100 points). This normalized face image is called the *canonical image*. Then the facial metrics are computed and stored in a face template. The typical size of such a template is between 3 and 5 kB, but there exist systems with the size of the template as small as 96 bytes.

The accuracy of the face recognition systems improves with time, but it has not been very satisfying so far. According to our experience there is still a potential for improving the algorithms for face location. The current software often does not find the face at all or finds “a face” at an incorrect place. This significantly makes the results worse. Better results can be achieved if the operator is able to tell the system exactly where the eyes are positioned. The systems also have problems to distinguish very similar persons like twins and any significant change in hair or beard style requires re-enrollment. Glasses can also cause additional difficulties. The quoted accuracy of facial recognition systems varies significantly, many systems quote the crossover accuracy of less then one percent. The numbers from real systems are not so pleasant, the crossover accuracy is much higher and indicates that these systems are not suitable for identification. If security is the main concern then even the verification accuracy may not be sufficiently good.

*accuracy*

Facial recognition systems are offered by a great number of suppliers nowadays, to name a few of them: Miros, Neurodynamics or Visionics.

The face recognition system does not require any contact with the person and can be fooled with a picture if no countermeasures are active. The liveness detection is based most commonly on facial mimics. The user is asked to blink or smile. If the image changes properly then the person is considered “live”. A few systems can simultaneously process images from two cameras, from two different viewpoints. The use of two cameras can also avoid fooling the system with a simple picture.

*liveness*

## 2.7 Speaker verification

The principle of speaker verification is to analyze the voice of the user in order to store a voiceprint that is later used for identification/verification. Speaker verification and speech recognition are two different tasks. The aim of speech recognition is to find *what* has been told while the aim of the speaker verification is *who* told that. Both these technologies are at the edge between research and industrial development. Texas Instruments reported their work in speech verification for access control already in the early 1970’s.

*principle*

There are many commercial systems available today, but their accuracy still can be improved.

Speaker verification focuses on the vocal characteristics that produce speech and not on the sound or the pronunciation of the speech itself. The vocal characteristics depend on the dimensions of the vocal tract, mouth, nasal cavities and the other speech processing mechanisms of the human body.

The greatest advantage of speaker verification systems is that they do not require any special and expensive hardware. A microphone is a standard accessory of any multimedia computer, speaker verification can also be used remotely via phone line. A high sampling rate is not required, but the background (or network) noise causes a significant problem that decreases the accuracy. The speaker verification is not intrusive for users and is easy to use.

*no special HW*

The system typically asks the user to pronounce a phrase during the enrollment, the voice is then processed and stored in a template (voiceprint). Later the system asks for the same phrase and compares the voiceprints. Such a system is vulnerable to replay attacks; if an attacker records the user's phrase and replays it later then he/she can easily gain the user's privilege. More sophisticated systems use a kind of challenge-response protocol. During the enrollment the system records the pronunciation of multiple phrases (e.g. numbers). In the authentication phase the system randomly chooses a challenge and asks the user to pronounce it. In this case the system not only compares the voiceprints, but also deploys the speech recognition algorithms and checks whether the proper challenge has really been said. There exist (very few) systems that are really text independent and can cope with the full vocabulary.

*challenge-response*

Speaker verification is quite secure from the professional mimics since the system make a comparison of the word stored in a different way than humans compare voices.

Currently there are three major international projects in the field of voice technology: PICASSO, CASCADE and Cost 250. There is a great number of commercially available voice systems as well. Keyware, VeriTel and International Electronics are a few of the leading companies.

Speaker verification is a biometric technique based on behavioral characteristic and as such can be negatively affected by the current physical condition and the emotional state. The accuracy of the speaker verification can also be affected by the background and network noise in the input signal. This increases the false rejection rate. During the tests of a speaker verification system in the Sandia Labs the false acceptance rate after a single attempt was 0.9% and the false rejection rate after *three* attempts was 4.3%. A trial at UBS's Ubilab achieved the equal error rate of 0.16% after a one attempt.

*accuracy*

## 2.8 Other biometric techniques

### Palmprint

Palmprint verification is a slightly different implementation of the fingerprint technology. Palmprint scanning uses optical readers that are very similar to those used for fingerprint scanning, their size is, however, much bigger and this is a limiting factor for the use in workstations or mobile devices.

### Hand vein

Hand vein geometry is based on the fact that the vein pattern is distinctive for various individuals. The veins under the skin absorb infrared light and thus have a darker pattern on the image of the hand taken by an infrared camera. The hand vein geometry is still in the stage of research and development. One such system is manufactured by British Technology Group. The device is called Veincheck and uses a template with the size of 50 bytes.

### DNA

DNA sampling is rather intrusive at present and requires a form of tissue, blood or other bodily sample. This method of capture still has to be refined. So far the DNA analysis has not been sufficiently automatic to rank the DNA analysis as a biometric technology. The analysis of human DNA is now possible within 10 minutes. As soon as the technology advances so that DNA can be matched automatically in real time, it may become more significant. At present

DNA is very entrenched in crime detection and so will remain in the law enforcement area for the time being.

### Thermal imaging

This technology is similar to the hand vein geometry. It also uses an infrared source of light and camera to produce an image of the vein pattern in the face or in the wrist.

### Ear shape

Identifying individuals by the ear shape is used in law enforcement applications where ear markings are found at crime scenes. Whether this technology will progress to access control applications is yet to be seen. An ear shape verifier (Optophone) is produced by a French company ART Techniques. It is a telephone-type handset within which is a lighting unit and cameras which capture two images of the ear.

### Body odor

The body odor biometrics is based on the fact that virtually each human smell is unique. The smell is captured by sensors that are capable to obtain the odor from non-intrusive parts of the body such as the back of the hand. Methods of capturing a person's smell are being explored by Mastiff Electronic Systems. Each human smell is made up of chemicals known as volatiles. They are extracted by the system and converted into a template.

The use of body odor sensors brings up the privacy issue as the body odor carries a significal ammount of sensitive personal information. It is possible to diagnose some diseases or activities in the last hours (like sex, for example) by analyzing the body odor.

### Keystroke dynamics

Keystroke dynamics is a method of verifying the identity of an individual by their typing rhythm which can cope with trained typists as well as the amateur two-finger typist. Systems can verify the user at the log-on stage or they can continually monitor the typist. These systems should be cheap to install as all that is needed is a software package.

### Fingernail bed

The US company AIMS is developing a system which scans the dermal structure under the fingernail. This tongue and groove structure is made up of nearly parallel rows of vascular rich skin. Between these parallel dermal structures are narrow channels, and it is the distance between these which is measured by the AIMS system.

# 3 Practical Issues

## 3.1 The core biometric technology

There are at least ten biometric techniques commercially available and new techniques are in the stage of research and development. What conditions must be fulfilled for a biological measurement to become a biometric? Any human physiological or behavioral characteristics can become a biometric provided the following properties are fulfilled (extended version of [8]).

*good biometrics*

∗ **Universality:** This means that every person should have the characteristics. It is really difficult to get 100% coverage. There are mute people, people without fingers or with injured eyes. All these cases must be handled.

∗ **Uniqueness:** This means that no two persons should be the same in terms of the biometric characteristics. Fingerprints have a high discrimination rate and the probability of two persons with the same iris is estimated as low as $1 : 10^{52}$. Identical twins, on the other side, cannot be easily distinguished by face recognition and DNA-analysis systems.

∗ **Permanence:** This means that the characteristics should be invariant with time. While the iris usually remains stable over decades, a person's face changes significantly with time. The signature and its dynamics may change as well and the finger is a frequent subject to injuries.

∗ **Collectability:** This means that the characteristics must be measured quantitatively and obtaining the characteristics should be easy. Face recognition systems are not intrusive and obtaining of a face image is easy. In the contrast the DNA analysis requires a blood or other bodily sample. The retina scan is rather intrusive as well.

∗ **Performance:** This refers to the achievable identification/verification accuracy and the resources and working or environmental conditions needed to achieve an acceptable accuracy. The crossover accuracy of iris-based systems is under 1% and the system is able to compare over $4 \cdot 10^6$

iriscodes in one second. The crossover accuracy of some signature dynamics systems is as high as 25% and the verification decision takes over one second.

∗ **Acceptability:** This indicates to what extend people are willing to accept the biometric system. Face recognition systems are personally not intrusive, but there are countries where taking pictures of persons is not viable. The retina scanner requires an infrared laser beam directed through the cornea of the eye. This is rather invasive and only few users accept this technology.

∗ **Circumvention:** This refers to how difficult it is to fool the system by fraudulent techniques. An automated access control system that can be easily fooled with a fingerprint model or a picture of a user's face does not provide much security.

## 3.2 The layer model

Although the use of each biometric technology has its own specific issues, the basic operation of any biometric system is very similar. The system typically follows the same set of steps. The separation of actions can lead to identifying critical issues and to improving security of the overall process of biometric authentication. The whole process starts with the enrollment:

*typical steps*

### First measurement (acquisition)

This is the first contact of the user with the biometric system. The user's biometric sample is obtained using an input device. The quality of the first biometric sample is crucial for further authentications of the user, so the quality of this biometric sample must be particularly checked and if the quality is not sufficient, the acquisition of the biometric sample must be repeated. It may happen that even multiple acquisitions do not generate biometric samples with sufficient quality. Such a user cannot be registered with the system. There are also mute people, people without fingers or with injured eyes. Both these categories create a ”failed to enroll“ group of users. Users very often do not have any previous experiences with

*quality is crucial*

the kind of the biometric system they are being registered with, so their behavior at the time of the first contact with the technology is not natural. This negatively influences the quality of the first measurement and that is why the first measurement is guided by a professional who explains the use of the biometric reader.

### Creation of master characteristics

The biometric measurements are processed after the acquisition. The number of biometric samples necessary for further processing is based on the nature of the used biometric technology. Sometimes a single sample is sufficient, but often multiple (usually 3 or 5) biometric samples are required. The biometric characteristics are most commonly neither compared nor stored in the raw format (say as a bitmap). The raw measurements contain a lot of noise or irrelevant information, which need not be stored. So the measurements are processed and only the important features are extracted and used. This significantly reduces the size of the data. The process of feature extraction is not lossless and so the extracted features cannot be used to reconstruct the biometric sample completely.

*noise elimination*

### Storage of master characteristics

After processing the first biometric sample and extracting the features, we have to store (and maintain) the newly obtained master template. Choosing a proper discriminating characteristic for the categorization of records in large databases can improve identification (search) tasks later on. There are basically 4 possibilities where to store the template: in a card, in the central database on a server, on a workstation or directly in an authentication terminal. The storage in an authentication terminal cannot be used for large-scale systems, in such a case only the first two possibilities are applicable. If privacy issues need to be considered then the storage on a card has an advantage, because in this case no biometric data must be stored (and potentially misused) in a central database. The storage on a card requires a kind of a digital signature of the master template and of the association of the user with the master template. Biometric samples as well as the extracted features

*template must be encrypted*

are very sensitive data and so the master template should be stored always encrypted no matter what storage is used.

As soon as the user is enrolled, he/she can use the system for successful authentications or identifications. This process is typically fully automated and takes the following steps:

### Acquisition(s)

The current biometric measurements must be obtained for the system to be able to make the comparison with the master template. These subsequent acquisitions of the user's biometric measurements are done at various places where the authentication of the user is required. This might be user's computer in the office, an ATM machine or a sensor in front of a door. For the best performance the kind of the input device used at the enrollment and for the subsequent acquisitions should be the same. Other conditions of use should also be as similar as possible with the conditions at the enrollment. These includes the background (face recognition), the background noise (voice verification) or the moisture (fingerprint). While the enrollment is usually guided by trained personnel, the subsequent biometric measurements are most commonly fully automatic and unattended. This brings up a few special issues. Firstly, the user needs to know how to use the device to provide the sample in the best quality. This is often not easy because the device does not show any preview of the sample obtained, so for example in the case of a fingerprint reader, the user does not know whether the positioning of the finger on the reader and the pressure is correct. Secondly, as the reader is left unattended, it is up to the reader to check that the measurements obtained really belong to a live persons (the liveness property). For example, a fingerprint reader should tell if the fingerprint it gets is from a live finger, not from a mask that is put on top of a finger. Similarly, an iris scanner should make sure that the iris image it is getting is from a real eye not a picture of an eye. In many biometric techniques (e.g. fingerprinting) the further processing trusts the biometric hardware to check the liveness of the person and provide genuine biometric measurements only. Some other systems (like the face recognition) check the user's liveness in software (the proper change of a characteristic with time). No matter whether hardware or software is used,

*no guide available*

*liveness test*

ensuring that the biometric measurements are genuine is crucial for the system to be secure. Without the assumption of the genuine data obtained at the input we cannot get a secure system. It is not possible to formally prove that a reader provides only genuine measurements and this affects also the possibility of a formal proof of the security of whole the biometric system. The liveness test of a person is not an easy task. New countermeasures are always to be followed by newer attacks. We do not even know how efficient the current countermeasures are against the attacks to come. Biometric readers are not yet the main target of sophisticated criminals. But then we can expect a wave of professional attacks. We have seen a few biometric readers where the estimated cost of an attack is as low as a few hundred dollars. The security of such a system is really poor.

*attacks and countermeasures*

### Creation of new characteristics

The biometric measurements obtained in the previous step are processed and new characteristics are created. The process of feature extraction is basically the same as in the case of the enrollment. Only a single biometric sample is usually available. This might mean that the number or quality of the features extracted is lower than at the time of enrollment.

### Comparison

The currently computed characteristics are then compared with the characteristics obtained during enrollment. This process is very dependent on the nature of the biometric technology used. Sometimes the desired security threshold is a parameter of the matching process, sometimes the biometric system returns a score within a range. If the system performs verification then the newly obtained characteristics are compared only with one master template (or with a small number of master templates, e.g. a set of master templates for a few different fingers). For an identification request the new characteristics are matched against a large number of master templates (either against all the records in the database or if the database is clustered then against the relevant part of the database)

*similarity score*

### Decision

The final step in the verification process is the yes/no decision based on the threshold. This security threshold is either a parameter of the matching process or the resulting score is compared with the threshold value to make the final decision. In the case of identification the user whose master template exceeds the threshold is returned as the result. If multiple master templates exceed the threshold then either all these users are returned as the result or the template with the highest score is chosen. Although the error rates quoted by manufactures (typically ERR $< 1\%$) might indicate that biometric systems are very accurate, the reality is rather different. The accuracy of biometric systems used by non-professional users is much lower. Especially the false rejection rate is in reality very high (very often over 10%). This prevents the legitimate users to gain their access rights and stands for a significant problem of the biometric systems.

*high error rates*

## 3.3 Biometrics and cryptography

Is cryptography necessary for the secure use of biometric systems? The answer is quite clear: Yes.

There are basically two kinds of biometric systems:

- ∗ Automated identification systems operated by professionals. The purpose of such systems is to identify an individual in question or to find an offender of a crime according to trails left on the crime scene. The operators of these systems do not have any reason to cheat the system, so the only task for the cryptography is to secure the sensitive biometric data.
- ∗ Access control systems. These systems are used by ordinary users to gain a privilege or an access right. Securing such a system is much more complicated task.

Let us consider further the general-use systems of the latter type, as this report is devoted solely to the use of biometrics for the authentication.

### Biometrics are not secrets

Some systems incorrectly assume that biometric measurements are secret and grant access when matching biometric measurements are presented. Such systems cannot cope with the situations when the biometric measurements are disclosed, because the biometrics cannot be changed (unless the user is willing to have an organ transplant). Moreover, the user will not learn that his/her biometric is disclosed. People leave fingerprints on everything they touch, and the iris can be observed anywhere they look. Biometrics definitely are sensitive data and therefore should be properly protected, but they cannot be considered secret. So the security of the system cannot be based on knowledge of the biometric characteristics. When using secret keys or passwords for authentication, a common method to defeat replay attacks is to use a challenge-response protocol, in which the password is never transmitted. Instead, the server sends a challenge that can only be answered correctly if the client knows the correct password. Unfortunately, this method does not apply to biometric data. The difference between a password and a fingerprint is that the password is supposed to be secret, while the fingerprint is not. Hence, replaying attacks are inherent with biometric authentication schemes.

*no secrets*

*replay attack*

The only way how to make a system secure is to make sure that the characteristics presented came from a real person and were obtained at the time of verification.

### The liveness problem

So-called liveness problem is a closely related issue. One has to make sure that the authentication device is verifying a live person. The liveness test is dependent on the kind of biometric technology used and it is a task left up to the core biometric technology. Some biometric techniques (e.g. face recognition or voice verification) may use experiences with the challenge-response protocols used in cryptography. The user is then asked to pronounce a randomly chosen phrase or make a certain movement. The biometric system has to trust the input device it provides only genuine measurements. We cannot make a secure system if we do not trust the

*live person*

biometric input device. If a malicious party can easily tamper with a fingerprint scanner, the whole system is not secure no matter how secure the other parts of the system are. In terms of the hardware of the device, until now, only smartcard-based devices can provide certain level of tamper-resistance. (Note: Smartcards are hardly ever tamper-proof, rather tamper-resistant.) The trustworthiness of a device is also a relative concept that depends on how the device is used. For example, a removable optical finger scanner put in a public place may be treated as untrustworthy, while the same removable optical finger scanner may be treated as trustworthy in a place where there is a constant human supervision.

*input device trustworthiness*

### Authentication software

The biometric system must be convinced that the presented biometric measurements come from a trusted input device and were captured at a certain time. If the authentication is done on-device, the device itself should be trustworthy. If the authentication is done off-device, then the operating environment of the software and the communication link between the software and the device, have to be secure. For example, in a client-server application, if the client workstation is not trusted, then there is no point authenticating a user using that workstation. If one chooses to run the authentication software at the server side, then the communication link between the server and the device itself (not just the client workstation) has to be secured. Otherwise, a malicious party or even the workstation itself may intercept the communication and replay recorded biometric data. One way to defeat replaying attacks is to put a separate secret key in the device and use challenge/response protocol with this key. Obviously, the device has to be trustworthy.

*trust is crucial*

The best solution probably is to use a TLS-like protocol with mandatory authentication of both parties. In any case it is necessary to transmit the whole biometric measurements over the connection. Either the reader sends the biometric measurements to the workstation (or server or whatever grants the access right) to make the match or the workstation provides the master template to the reader that makes the matching. Hashing in the usual sense and sending only the hash over the link does not help here, because the biometric measurements never are the same. To make it work we

*solutions*

either would have to ensure that the biometric measurements are always the same (but see the warning below) or change the hash function not to depend on all the input.

One has to consider that 100% similarity of two samples from different biometric measurements implies a good forgery. This is true with almost 100% probability.

### Improving security with biometrics

Can biometrics help cryptography to increase the security? Here the answer is not so clear.

*key management*

Cryptography has been relatively successfully used without biometrics over decades. But it still can benefit from the use of biometrics. To put it simple, cryptography is based on keys. Secure storage of keys is a crucial non-trivial task. Key management often is the weakest point of many systems. Secret and private keys must be kept secret, and here the biometric technologies might help.

*secret key protection*

Indeed, one of the most promising applications of biometrics is the secret key protection. If a user's local workstation is trusted, then the problem of the authentication software is minor, but the input device must be trustworthy. The security concerns are the same no matter whether the secret (or private) keys are stored on a smartcard or on the hard disk of the workstation. If a user's workstation is not trusted, the private keys have to be stored in a separate secure place, usually a smartcard. Smartcard based solutions where the secret key is unlocked only after a successful biometric verification increase the overall security, as the biometric data does not need to leave the card. For smartcards the fingerprint techniques with a silicon fingerprint reader are most commonly used today.

*“biometric keys”*

It is necessary to distinguish securing a key with biometrics and generating a key from biometrics. The latter does not work. It must be pointed out that biometric data cannot be used as capability tokens in the same way as secret keys or passwords. In secret key or password based access control schemes, a key/password itself can be used as a capability. Knowing a secret key or a password can mean that the user has the right to use certain application. However, this does not apply to biometric data. As we already know biometrics are not secrets. One viable way is to use digital certificates.

Digital certificates can be used as capabilities or digital identities that allow users to access remote applications, while biometrics is used to secure the access/usage of the private keys associated with the digital certificates.

# 4 Conclusions

Even if the accuracy of the biometric techniques is not perfect yet, there are many mature biometric systems available now. Proper design and implementation of the biometric system can indeed increase the overall security, especially the smartcard based solutions seem to be very promising. Making a secure biometric systems is, however, not as easy as it might appear. The word biometrics is very often used as a synonym for the perfect security. This is a misleading view. There are numerous conditions that must be taken in account when designing a secure biometric system. First, it is necessary to realize that biometrics are not secrets. This implies that biometric measurements cannot be used as capability tokens and it is not secure to generate any cryptographic keys from them. Second, it is necessary to trust the input device and make the communication link secure. Third, the input device needs to check the liveness of the person being measured and the device itself should be verified for example by a challenge-response protocol.

*be careful*

# References

[1] American Biometric Company,
`http://www.abio.com/`

[2] Biometric Access Corporation,
`http://www.biometricaccess.com/`

[3] C. Calabrese: *The trouble with biometrics*, ;login:, Volume 24, Number 4

[4] Digital Persona, `http://www.digitalpersona.com/`

[5] EyeDentify, `http://www.eyedentify.com/`

[6] I/O Software, `http://www.iosoftware.com/`

[7] Iridian Technologies, `http://www.iriscan.com/`

[8] A. Jain et al: *BIOMETRICS: Personal Identification in Networked Society*, Kluwer Academic Publishers, 1999, ISBN 0-7923-8345-1

[9] LCI Smartpen, `http://www.smartpen.net/`

[10] E. Newham, *The biometric report*, SBJ Services, 1995

[11] Pattern Recognition and Image Processing Lab, Michigan State University,
`http://biometrics.cse.msu.edu/`

[12] PenOp, `http://www.penop.com/`

[13] Precise Biometrics,
`http://www.precisebiometrics.com/`

[14] Recognition Systems, `http://www.recogsys.com/`

[15] B. Schneier: *The Uses and Abuses of Biometrics*, Communications of the ACM, August 1999

[16] UBS, Ubilab, *internal company report*

[17] UltraScan, `http://www.ultra-scan.com/`

[18] Veridicom, `http://www.veridicom.com/`

Publications in the FI MU Report Series are in general accessible via WWW and anonymous FTP:

```
http://www.fi.muni.cz/informatics/reports/
ftp  ftp.fi.muni.cz (cd pub/reports)
```

Copies may be also obtained by contacting:

Faculty of Informatics
Masaryk University
Botanická 68a
602 00 Brno
Czech Republic