A

Seminar report

On

Biometric Authentication Technology

Submitted in partial fulfillment of the requirement for the award of degree
Of Computer Science

SUBMITTED TO: **SUBMITTED BY:**

www.studymafia.org www.studymafia.org

Preface

I have made this report file on the topic **Biometric Authentication Technology;** I have tried my best to elucidate all the relevant detail to the topic to be included in the report. While in the beginning I have tried to give a general view about this topic.

My efforts and wholehearted co-corporation of each and everyone has ended on a successful note. I express my sincere gratitude to ……..who assisting me throughout the preparation of this topic. I thank him for providing me the reinforcement, confidence and most importantly the track for the topic whenever I needed it.

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 behavioural 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.

In this computer-driven era, identity theft and the loss or disclosure of data and related intellectual property are growing problems. We each have multiple accounts and use multiple passwords on an ever-increasing number of computers and Web sites. Maintaining and managing access while protecting both the user's identity and the computer's data and systems has become increasingly difficult. Central to all security is the concept of authentication - verifying that the user is who he claims to be.

We can authenticate an identity in three ways: by something the user knows (such as a password or personal identification number), something the user has (a security token or smart card) or something the user is (a physical characteristic, such as a fingerprint,called a biometric).

Passwords are cheap, but most implementations offer little real security. Managing multiple passwords for different systems is a nightmare, requiring users to maintain lists of passwords and systems that are inevitably written down because they can't remember them. The short answer, talked about for decades but rarely achieved in practice, is the idea of single sign-on.Using security tokens or smart cards requires more expense, more infrastructure support and specialized hardware. Still, these used to be a lot

cheaper than biometric devices and, when used with a PIN or password, offer acceptable levels of security, if not always convenience.

Biometric authentication has been widely regarded as the most foolproof - or at least the hardest to forge or spoof. Since the early 1980s, systems of identification and authentication based on physical characteristics have been available to enterprise IT. These biometric systems were slow, intrusive and expensive, but because they were mainly used forguarding mainframe access or restricting physical entry to relatively few users, they proved workable in some high-security situations. Twenty years later, computers are much faster and cheaper than ever. This, plus new, inexpensive hardware, has renewed interest in biometrics.

Who are you? Do you belong here? What rights do you have? And how do I know you're who you say you are? Those are the essential questions that any effective security system must answer before a user can access a computer system, network or other protected resource. We think this is what a password system does, but passwords are only one part of an effective security system. That security system requires three separate elements - identification, authentication and authorization - that together make up what's called access control.When you log into a computer or network, the first thing you're asked for is a user name or account name. But a user name offers little protection to the system. Therefore, the system also usually prompts you for a password, a form of authentication.

1.1 Authentication

The question, "How do I know you're who you say you are?," is in many ways, the most important one. Unless it's answered satisfactorily, identification is incomplete and no authorization can or should take place. But how does a system verify that a user is who he says he is? Simply entering your password doesn't prove it's you. Someone else could know your password. The answer lies in a strong authentication process. Basically, the following three factors can be used to authenticate an individual:

1. **Something the user knows**. This is a reusable password, passphrase, personal identification number or a fact likely to be known only to the user, such as his mother's maiden name.

2. Something the user has. This could be a key, a magnetic-stripe card, a smart card or a specialized authentication device (called a token) that generates a one-time password or a specific response to a challenge presented by the server.

3. Something the user is. This depends on some inherent physical trait or characteristic. Often called biometrics, examples of this form of authentication include: fingerprints, retinal (eye) patterns, hand geometry, voice recognition, facialrecognition, typing pattern recognition and signature dynamics (speed and pressure, not just the outline).

These authentication factors are listed here from weakest to strongest as determined by how difficult they are to forge or fake. By themselves, each of these methods offers some security. However, each has its own problems or weaknesses.

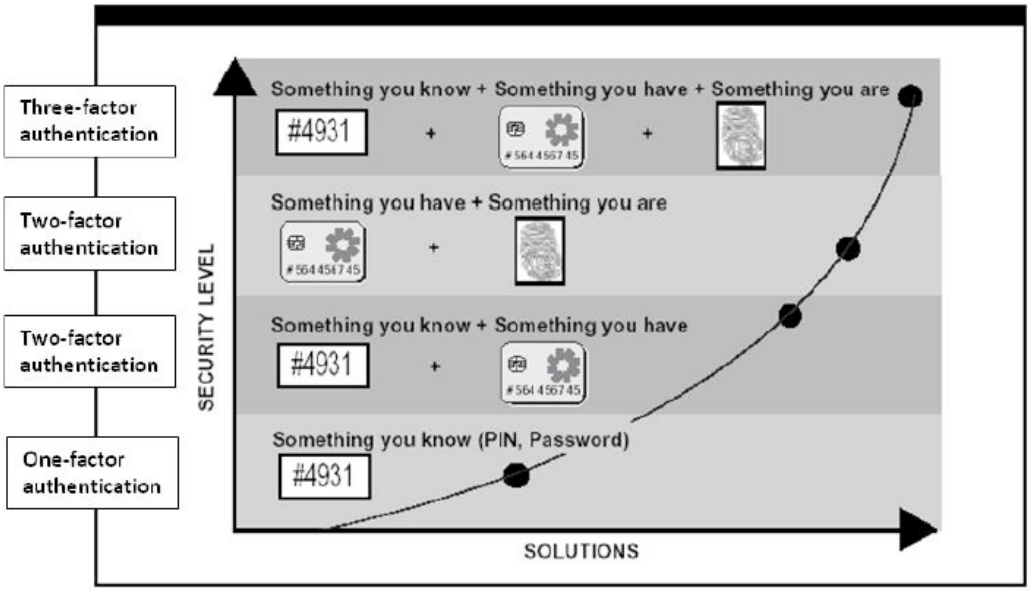
Anyone can enter a password and, historically, reusable passwords have been vulnerable to guessing, brute force and dictionary-based attacks.The second means of authentication - something the user has - requires the user to possess an often difficult-to-replicate device. However this stronger protection also costs more (typically tens of dollars per device), and it requires contingency procedures in case a device is left at home, lost or stolen. The third type of authentication - something the user is - is the most difficult to defeat, but it has other problems. Biometric identification methods are subject to two types of errors: false positives and false negatives. The first erroneously authenticates an individual who shouldn't be authenticated; the second denies an individual who should be authenticated. Error are not desirable, and it's important to know and verify error rates when considering such a system. [1]

Another problem is that permanent physical changes or temporary ailments or accidents can alter or render unreadable the measured characteristic. If you cut part of your fingertip, you've changed what the fingerprint reader sees. Put on a Band-Aid, and the reader can't see the fingerprint at all.

Finally, if the method is compromised, there's no way to give an individual a new identifying characteristic. You can issue a new password or security token, but you can't change his fingerprints or eye pattern.

1.2 Two-Factor Authentication

For greatly increased security, the approach preferred by experts is to use two of the three methods in combination - a process called two-factor authentication. For example, to use a security token that generates a one-time password, you may need to enter a personal identification number into the token itself. Similarly, a card-key can be used in combination with a biometric system.



This is essentially what happens when you check in at an airport ticket counter. You hand over your ticket, which identifies you. Then you show a photo ID of some kind. This is something you have with you, and it's biometric (something you are) in that the clerk has to determine that the photo on the card matches you.

Once a user has been identified and authenticated, what remains is to grant him access to whatever specific system resources have been approved. This authorization is usually accomplished by looking up that user's entry in an access control list that delineates specific rights and permissions. These can be based, among other things, on an individual's identity or job function, membership in a workgroup or other classification or time of day or day of week.

Authentication via Security Token

Security Token like Secure ID, a hardware authentication device, or security token, provides greatly increased protection against spoofing or brute-force attacks. The time-synchronized SecurID card from RSA Security Inc. in Bedford, Mass., has an LCD screen that shows a string of numbers that changes every minute. The user types in his user name at log in, then the number shown on the card. The host system knows what that

number is supposed to be for that user at that particular time. Some tokens don't show a number continuously but require the user to enter a PIN on the card itself before the number is displayed, thus providing two-factor authentication.

Challenge-Response Systems with a token-based Challenge-Response system, the system displays a number (the challenge) when you log in. The user types this number into his token, which encrypts that to produce a second number (the response). The user enters the response into the computer. The host performs the same operation on the challenge, then compares its result to the user's response. If they match, the user is authenticated.

1.3 What is Biometric?

The term biometrics is derived from the Greek words Bio & Metric. The term Biometrics relates to the measurement (metric) of characteristics of a living (Bio) thing in order to identify a person. Biometrics uses various physiological or behavioural characteristics. Common physiological biometric measurements include fingerprints, hand geometry, retina, iris, facial images etc. While common behavioural biometric measurements include signatures, voice recordings, keystroke rhythms etc. With an increasing importance of security, there is a need to guaranty that only authenticated users have access to the system. In recent years, biometrics authentication has seen considerable improvements in reliability and accuracy, with some of the traits offering good performance. However, even the best biometric traits till date are facing numerous problems some of them are inherent to the technology itself. Biometric authentication systems generally suffer from enrolment problems due to non-universal biometric traits, insufficient accuracy caused by noisy data acquisition in certain environments. Biometric measurements are inherently varied because of the existence of back-ground noise, signal distortion, biometric feature changes and environmental variations. Identification based on a single bio-metric trait may not be sufficiently robust and it has a limited ability to overcome spoofing.

One way to overcome these problems is the use of multi-biometrics. A multi biometric system uses multiple sensors for data acquisition. This allows capturing multiple samples of a single biometric trait and/or samples of multiple biometric traits. This approach is enables to provide significant improvement over unimodal biometric system in terms of higher accuracy.

Biometric System Components and Process

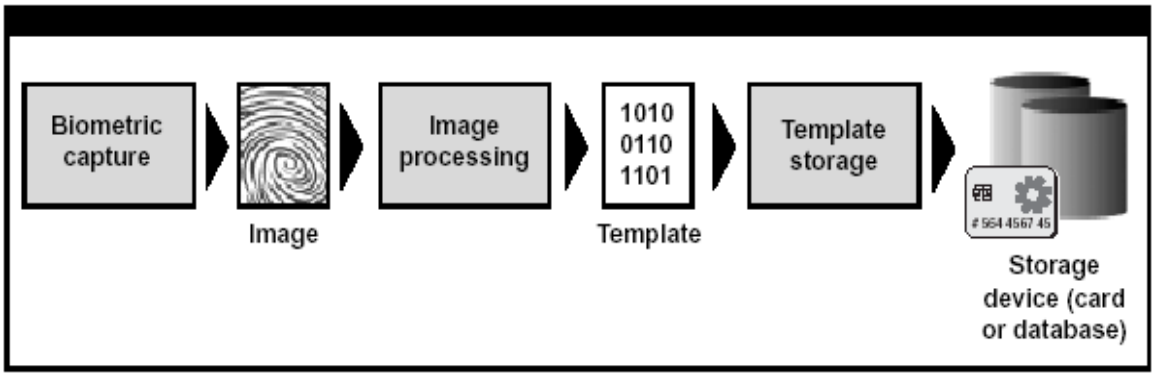
Four major components are usually present in a biometric system:

- A mechanism to scan and capture a digital representation of a living person's biometriccharacteristic.
- Software to process the raw data into a format (called a template) that can be used forstoringand matching.
- Matching software to compare a previously stored biometric template with a templatefrom a livesample.
- An interface with the application system to communicate the match result.

Two different stages are involved in the biometric system process – enrollment and matching.

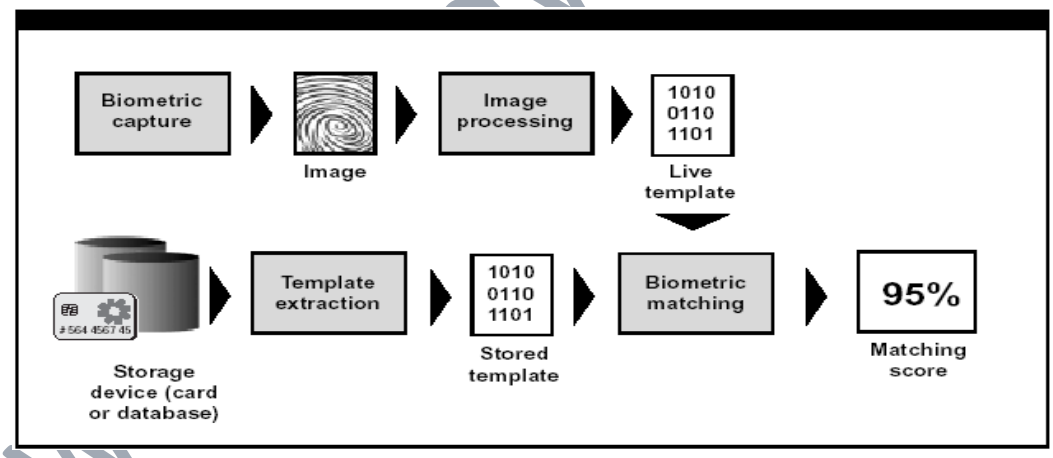
Enrollment. As shown in Figure 1, the biometric sample of the individual is captured during theenrollment process (e.g., using a sensor for fingerprint, microphone for speaker recognition, camera forface recognition, camera for iris recognition). The unique features are then extracted from thebiometricsample (e.g., image) to create the user's biometric template. This biometric template is stored in adatabase or on a machine-readable ID card for later use during a matching process.

Figure 1. Example Enrollment Process



Matching.Figure 2 illustrates the biometric matching process. The biometric sample is again captured. The unique features are extracted from the biometric sample to create the user's "live" biometrictemplate.This new template is then compared with the template(s) previously stored and a numeric matching(similarity) score(s) is generated based on a determination of the common elements between the twotemplates. System designers determine the threshold value for this verification score based upon thesecurity and convenience requirements of the system.

Figure 2. Example Matching Process



Biometrically enabled security systems use biometrics for two basic purposes: identification andverification.

Identification(one-to-many or 1: N comparison) determines if the individual exists within an enrolled population by comparing the live sample template to all stored templates in the system. Identification can confirm that the individual is not enrolled with another identity or is not on a predetermined list ofprohibited persons. The biometric for the individual being considered for enrollment should be comparedagainst all stored

biometrics. For some credentialing applications, a biometric identification process isused at the time of enrollment to confirm that the individual is not already enrolled.

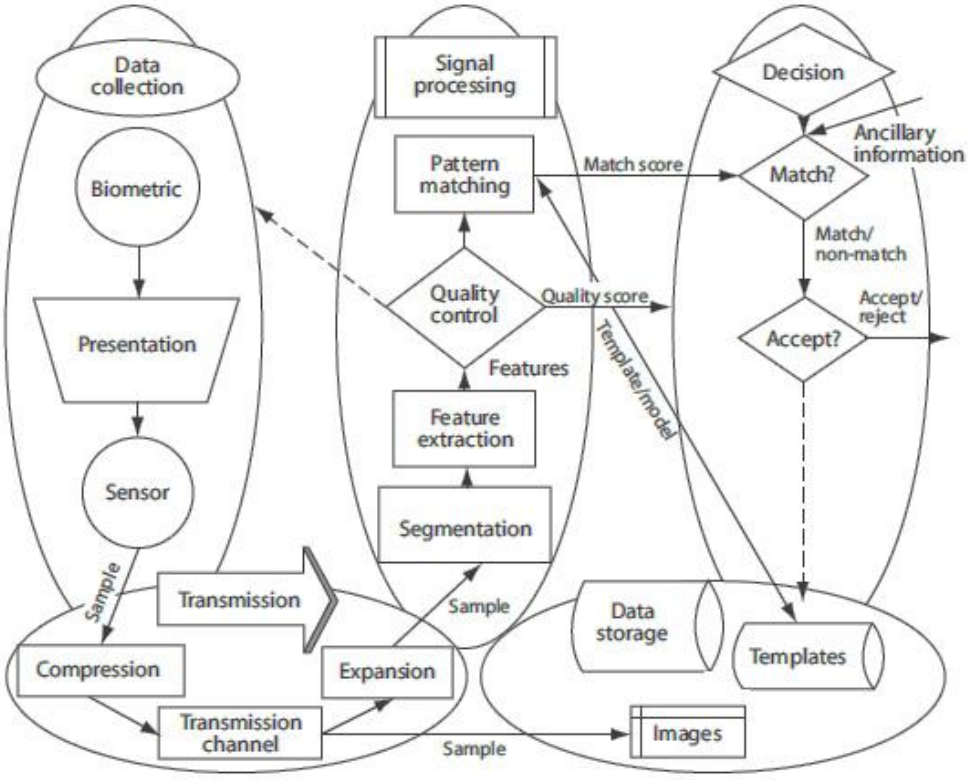
Verification(one-to-one or 1:1 comparison) determines whether the live biometric template matcheswith a specific enrolled template record. This requires that there be a "claim" of identity by the personseeking verification so that the specific enrolled template record can be accessed. An example would bepresentation of a smart card credential and matching the live sample biometric template with the enrolled template stored in the smart card memory. Another example would be entry of a user name or ID numberwhich would point to an enrolled template record in a database.

1.4 A System Model

Although these devices rely on widely different technologies, much can be said about them in general. Figure 1.1 shows a generic biometric authentication system divided into five subsystems: data collection, transmission, signal processing, decision and data storage. We will consider these subsystems one at a time.

1.4.1 Data Collection

Biometric systems begin with the measurement of a behavioural/physiological characteristic. Key to all systems is the underlying assumption that the measured biometric characteristic is both distinctive between individuals and repeatable over time for the same individual. The problems in measuring and controlling these variations begin in the data collection subsystem.



A generic biometric system.

The user's characteristic must be presented to a sensor. The presentationof any biometric characteristic to the sensor introduces a behavioural (and,consequently, psychological) component to every biometric method. This behavioural component may vary widely between users, between applications,and between the test laboratory and the operational environment.The output of the sensor, which is the input data upon which the system isbuilt, is the convolution of: (1) the biometric measure; (2) the way the measureis presented; and (3) the technical characteristics of the sensor. Boththe repeatability and the distinctiveness of the measurement are negativelyimpacted by changes in any of these factors. If a system is to be open, thepresentation and sensor characteristics must be standardized to ensurethat biometric characteristics collected with one system will match thosecollected on the same individual by another system. If a systemis to be usedin an overt, non-cooperative application, the user must not be able to wilfully change the biometric or its presentation sufficiently to avoid beingmatched to previous records.

1.4.2 Transmission

Some, but not all, biometric systems collect data at one location but store and/or process it at another. Such systems require data transmission. If a great amount of data is

involved, compression may be required before transmission or storage to conserve bandwidth and storage space. Figure shows compression and transmission occurring before the signal processing and image storage. In such cases, the transmitted or stored compressed data must be expanded before further use. The process of compression and expansion generally causes quality loss in the restored signal, with loss increasing with increasing compression ratio. The compression technique used will depend upon the biometric signal. An interesting area of research is in finding, for a given biometric technique, compression methods with minimum impact on the signal-processing subsystem.

If a system is to be open, compression and transmission protocols must be standardized so that every user of the data can reconstruct the original signal. Standards currently exist for the compression of fingerprints (Wavelet Scalar Quantization), facial images (JPEG), and voice data (Code Excited Linear Prediction). [5]

1.4.3 Signal Processing

Having acquired and possibly transmitted a biometric characteristic, we must prepare it for matching with other like measures. Figure divides the signal-processing subsystem into four tasks: segmentation, feature extraction, quality control, and pattern matching.

Segmentation is the process of finding the biometric pattern within the transmitted signal. For example, a facial recognition system must first find the boundaries of the face or faces in the transmitted image. A speaker verification system must find the speech activity within a signal that may contain periods of non-speech sounds. Once the raw biometric pattern of interest has been found and extracted from larger signal, the pattern is sent to the feature extraction process.

Feature extraction is fascinating. The raw biometric pattern, even after segmentation from the larger signal, contains non-repeatable distortions caused by the presentation, sensor and transmission processes of the system. These non-controllable distortions and any non-distinctive or redundant elements must be removed from the biometric pattern, while at the same time preserving those qualities that are both distinctive and repeatable. These qualities expressed in mathematical form are called “features”. In a text-independent speaker recognition system, for instance, we may want to find the features, such as the mathematical frequency relationships in the vowels that

depend only upon the speaker and not upon the words being spoken, the health status of the speaker, or the speed, volume and pitch of the speech. There are as many wonderfully creative mathematical approaches to feature extraction as there are scientists and engineers in the biometrics industry. You can understand why such algorithms are always considered proprietary. Consequently, in an open system, the “open” stops here.In general, feature extraction is a form of non-reversible compression, meaning that the original biometric image cannot be reconstructed from the extracted features. In some systems, transmission occurs after feature extraction to reduce the requirement for bandwidth.

After feature extraction, or maybe even before, we will want to check to see if the signal received from the data collection subsystem is of good quality. If the features “don’t make sense” or are insufficient in some way, we can conclude quickly that the received signal was defective and request a new sample from the data collection subsystem while the user is still at the sensor. The development of this “quality control” process has greatly improved the performance of biometric systems in the last few short years. On the other hand, some people seem never to be able to present an acceptable signal to the system. If a negative decision by the quality control module cannot be overridden, a “failure to enroll” error results.

The feature “sample”, now of very small size compared to the original signal, will be sent to the pattern matching process for comparison with one or more previously identified and stored feature templates or models. We use the term “template” to indicate stored features. The features in the template are of the same type as those of a sample. For instance, if the sample features are a “vector” in the mathematical sense, then the stored template will also be a “vector”. The term “model” is used to indicate the construction of a more complex mathematical representation capable of generating features characteristic of a particular user. Models and features will be of different mathematical types and structures. Models are used in some speaker and facial recognition systems. Templates are used in fingerprint, iris, and hand geometry recognition systems.

The term “enrollment” refers to the placing of a template or model into the database for the very first time. Once in the database and associated with an identity by external information (provided by the enrollee orothers), the enrollment biometric data is referred to as the template ormodel for the individual to which it refers.The purpose of the patternmatching process is to compare a presented featuresample to the stored data,and to

send to the decision subsystemaquantitativemeasure of the comparison. An exception is enrollment in systemsallowing multiple enrollments. In this application, the pattern matching processcan be skipped. In the cooperative case where the user has claimed anidentity or where there is but a single record in the current database (whichmight be a magnetic stripe card), the pattern matching process might onlymake a comparison against a single stored template. In all other cases, such aslarge-scale identification, the pattern matching process compares the presentsample to multiple templates or models from the database one at a time, asinstructed by the decision subsystem, sending on a quantitative "distance"measure for each comparison. In place of a "distance"measure, some systemsuse "similarity"measures, such as maximum likelihood values.

The signal processing subsystem is designed with the goal of yieldingsmall distances between enrolled models/templates and later samples fromthe same individual and large distances between enrolled models/templatesand samples of different individuals. Even for models and samplesfrom the same individual, however, distances will rarely, if ever, be zero, asthere will always be some non-repeatable biometric-, presentation-,sensor- or transmission-related variation remaining after processing. [5]

1.4.4 Storage

The remaining subsystem to be considered is that of storage. There will beone or more forms of storage used, depending upon the biometric system.Templates or models from enrolled users will be stored in a database forcomparison by the pattern matcher to incoming feature samples. For systemsonly performing "one-to-one"matching, the database may be distributedon smart cards, optically read cards or magnetic stripe cards carriedby each enrolled user. Depending upon system policy, no central databaseneed exist, although in this application a centralized database can be usedto detect counterfeit cards or to reissue lost cards without re-collecting thebiometric pattern.

The database will be centralized if the system performs one-to-*N*matching with *N* greater than one, as in the case of identification or "PIN-lessverification" systems. As *N* gets very large, system speed requirementsdictate that the database be partitioned into smaller subsets such that anyfeature sample need only be matched to the templates or models stored inone partition, or indexed by using an appropriate data structure

whichallows the templates to be visited in an advantageous order during theretrieval. These strategies have the effect of increasing system speedand decreasing false matches, at the expense of increasing the false non-matchrate owing to partitioning errors.Thismeans that system error ratesdo not remain constant with increasing database size and identification systems do not scale linearly. Consequently, database partitioning/indexing strategies represent a complex policy decision.

If it may be necessary to reconstruct the biometric patterns from storeddata, raw (although possibly compressed) data storage will be required.The biometric pattern is generally not reconstructable from the storedtemplates or models, although some methods do allow a coarse reconstructionof patterns from templates. Further, the templates themselves arecreated using the proprietary feature extraction algorithms of the systemvendor. The storage of raw data allows changes in the system or systemvendor to be made without the need to re-collect data from all enrolledusers.

1.4.5 Decision

The decision subsystem implements system policy by directing the databasesearch, determines “matches” or “non-matches” based on the distanceor similarity measures received from the pattern matcher, and ultimatelymakes an “accept/reject” decision based on the system policy. Such a decisionpolicy could be to reject the identity claim (either positive or negative)of any user whose pattern could not be acquired. For an acquired pattern,the policy might declare a match for any distance lower than a fixedthreshold and “accept” a user identity claim on the basis of this singlematch, or the policy could be to declare amatch for any distance lower thana user-dependent, time-variant, or environmentally linked threshold andrequire matches from multiple measures for an “accept” decision. Thepolicy could be to give all users,good guys and bad guys alike, three tries toreturn a low distance measure and be “accepted” as matching a claimedtemplate. Or, in the absence of a claimed template, the system policy couldbe to direct the search of all,or only a portion,of the database and return asingle match or multiple “candidate” matches. The decision policyemployed is a management decision that is specific to the operational andsecurity requirements of the system. In general, lowering the number offalse non-matches can be traded against raising the number of falsematches. The optimal system policy in this regard depends both upon thestatistical characteristics of the comparison distances coming from thepattern matcher,

the relative penalties for false match and false non-matchwithin the system,and the *a priori* (guessed in advance) probabilities that auser is, in fact, an impostor. In any case, in the testing of biometric devices,it is necessary to decouple the performance of the signal processingsubsystem from the policies implemented by the decision subsystem.

1.5 Biometrics and Privacy

1. Unlike more common forms of identification, biometric measures contain no personalinformation and are more difficult to forge or steal.
2. Biometric measures can be used in place of a name or Social Security number to secure anonymous transactions.
3. Some biometric measures (face images, voice signals and "latent" fingerprints left on surfaces) can be taken without a person's knowledge, but cannot be linked to an identity without a pre-existing invertible database.
4. A Social Security or credit card number, and sometimes even a legal name, can identify a person in a large population. This capability has not been demonstrated using any single biometric measure.
5. Like telephone and credit card information, biometric databases can be searched outside of their intended purpose by court order.
6. Unlike credit card, telephone or Social Security numbers, biometric characteristics change from one measurement to the next.
7. Searching for personal data based on biometric measures is not as reliable or efficient as using better identifiers, like legal name or Social Security number.
8. Biometric measures are not always secret, but are sometimes publicly observable and cannot be revoked if compromised.

1.6 Factors of Evaluation

1.6.1 False Accept Rate (FAR) and False Match Rate (MAR): The probability that thesystem incorrectly declares a successful match between the input pattern and a nonmatchingpattern in the database. It measures the percent of invalid matches. Thesesystems are critical since they are commonly used to forbid certain actions bydisallowed people.

1.6.2 False Reject Rate (FRR) or False Non-Match Rate (FNMR): The probability thatthe system incorrectly declares failure of match between the input pattern and the matchingtemplate in the database. It measures the percent of valid inputs being rejected.

1.6.3 Relative Operating Characteristic (ROC): In general, the matching algorithmperforms a decision using some parameters (e.g. a threshold). In biometric systems the FARand FRR can typically be traded off against each other by changing those parameters. The

ROC plot is obtained by graphing the values of FAR and FRR, changing the variables implicitly. A common variation is the Detection Error Tradeoff (DET), which is obtainedusing normal deviate scales on both axes. This more linear graph illuminates the differencesfor higher performances (rarer errors).

1.6.4 Equal Error Rate (EER): The rates at which both accept and reject errors are equal.

ROC or DET plotting is used because how FAR and FRR can be changed, is shown clearly.

When quick comparison of two systems is required, the ERR is commonly used. Obtainedfrom the ROC plot by taking the point where FAR and FRR have the same value. The lowerthe EER, the more accurate the system is considered to be.

1.6.5 Failure to Enroll Rate (FTE or FER): The percentage of data input is consideredinvalid and fails to input into the system. Failure to enroll happens when the data obtained bythe sensor are considered invalid or of poor quality.

1.6.6 Failure to Capture Rate (FTC): Within automatic systems, the probability that thesystem fails to detect a biometric characteristic when presented correctly is generallytreatedas FTC.

1.6.7 Template Capacity: It is defined as the maximum number of sets of data which canbeinput in to the system.

1.7 Biometric Applications

Biometric applications can be categorized in horizontal categories as well as verticalmarkets.Biometrics are most frequently used in the following horizontal categories:

a) **Citizen Identification:**

Identify/authentify citizens interacting with government agencies

b) **PC / Network Access:**

Secure access to PCs, networks and other computer resources

c) **Physical Access / Time and Attendance:**

Secure access to a given area at a given time

d) **Surveillance and Screening:**

Identify/authentify individuals present in a given location

e) **Retail / ATM / Point of Sale:**

Provide identification/authentication for in-person transactions for goods/services

f) **E-Commerce / Telephony:**

Provide identification/authentication for remote transactions for goods/services

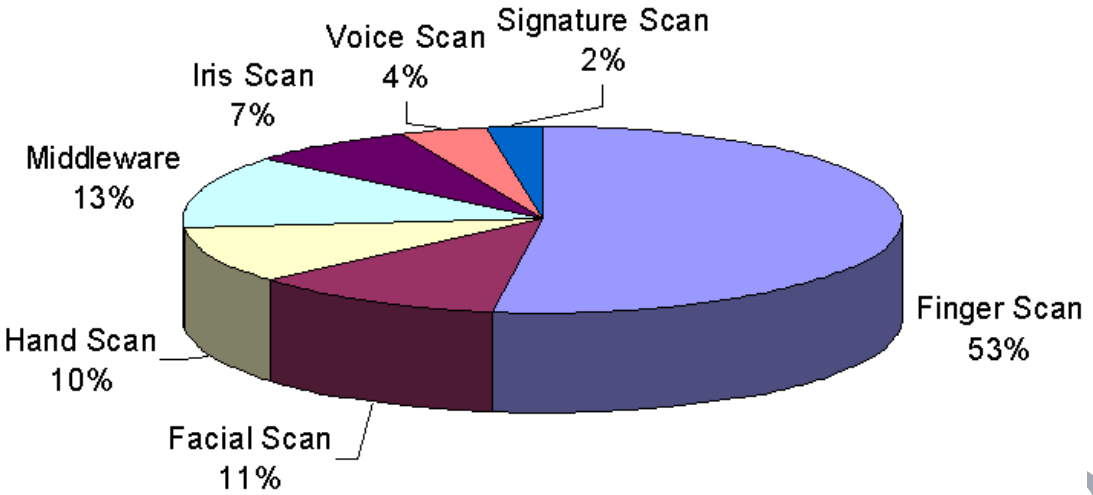
g) **Criminal Identification:**

Identify/verify individuals in law enforcement applications.

In each of those applications, biometric systems can be used to either replace or complementexisting authentication methods.

- ➔ **Government Sector**
- ➔ **Travel and Transportation**
- ➔ **Financial Sector**
- ➔ **Health Care**
- ➔ **Law Enforcement**

Among the technologies, finger scan is the undisputed leader with more than 50% market share. [4]



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 odour 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

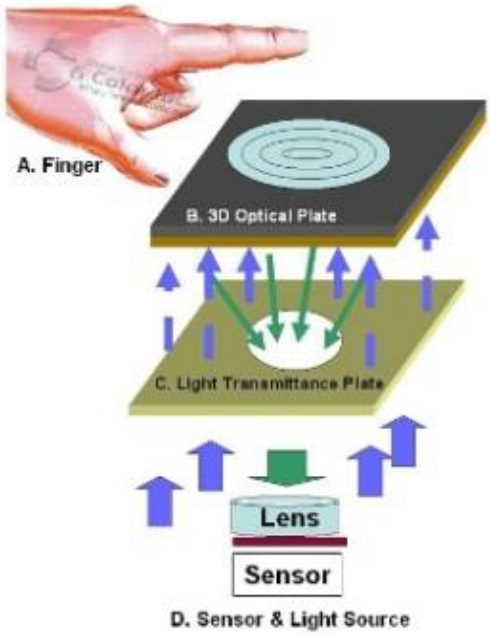
Fingerprint identification is perhaps the oldest of all the biometric techniques. Fingerprints were used already in the Old China as a means of positively identifying a person as an author of the document. Their use in law enforcement since the last century is well known and actually let to an association 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.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.

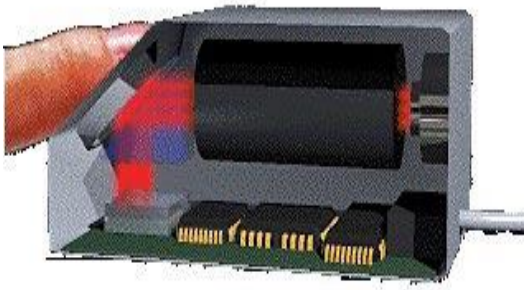
Fingerprint readers

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 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 reader's surface.[3]

All the optical fingerprintreaders comprise of thesource of light, the lightsensor and a special reflectionsurface that changes the reflection according tothe pressure.Some of the readers arefitted out with the processingand memory chips as well.





The size of the optical fingerprint readers typically is around 10x10x5 cms. It is difficult to minimize them much more as the reader has to comprise the source of light, reflection surface and the light sensor.

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.

Optical readers are relatively cheap and are manufactured by a great number of manufacturers. The field of optical technologies attracts many newlyestablished firms (e.g., American BiometricCompany, Digital Persona) as well as a few big and well-known companies (such as HP, Philips or Sony). Optical fingerprintreaders are also often embedded in keyboards, mice or monitors.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 otherplate is a tiny area of metallization (a pixel) on the

chip's surface.One places his/her finger against the surface of the chip (actuallyagainst an insulated coating on the chip's surface). The ridges ofthe fingerprint are close to the nearby pixels and have high capacitanceto them. The valleys are more distant from the pixels nearestthem and therefore have lower capacitance.

Such an array of capacitors can be placed onto a chip as small as 15 x 15x 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.

Fig: Fingerprint Reader

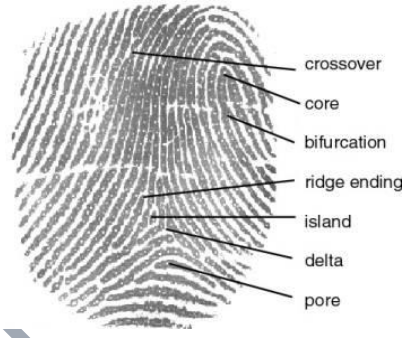


Fig: Typical features in a fingerprint

The fingerprintbitmap obtainedfrom the siliconreader is affected bythe finger moistureas the moisture significantlyinfluencesthe capacitance. Thisoften means that toowet or dry fingers donot produce bitmapswith a sufficient quality and so people with unusually wet or dryfingers have problems with these silicon fingerprint readers.Both optical and silicon fingerprint readers are fast enough tocapture and display the fingerprint in real time. The typical resolutionis around 500 DPI.

Ultrasonic fingerprintreaders are the newest andleast common. They use ultrasoundto monitor the fingersurface.The user places the fingeron a piece of glass and theultrasonic sensor moves andreads whole the fingerprint.This process takes one or twoseconds. Ultrasound is notdisturbed by the dirt on thefingers so the quality of the bitmap obtained is usually fair.

Fingerprint processing

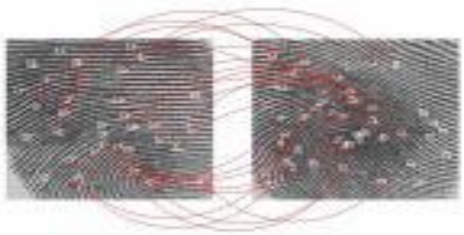
Fingerprints are not compared and usually also not stored as bitmaps. Fingerprint matching techniques can be placed into two categories: minutiae-based and correlation

based. Minutiae-based techniques find the minutiae points first and then map their relativeplacement 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 followingpage). In the recent years automated fingerprint comparisons havebeen most often based on minutiae.

The problem with minutiae is that it is difficult to extract theminutiae 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 overcomesome of the difficulties of the minutiae-based approach.However, it has some of its own shortcomings. Correlation-basedtechniques require the precise location of a registration point andare affected by image translation and rotation.

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%. There are about 30 minutiae within a typical fingerprint image obtained by a live fingerprint reader. 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.

The speed ofthe decision sometimesdepends onthe security leveland the negativeanswer very oftentakes longertime than the positive one (sometimes even 10 times more).There is no direct dependency between the speed and accuracy ofthe matching algorithm according to our experience. We have seenfast and accurate as well as slow and less accurate matching algorithms.



The minutiae matching is aprocess where two sets ofminutiae are compared todecidewhether theyrepresentthe same finger or not.

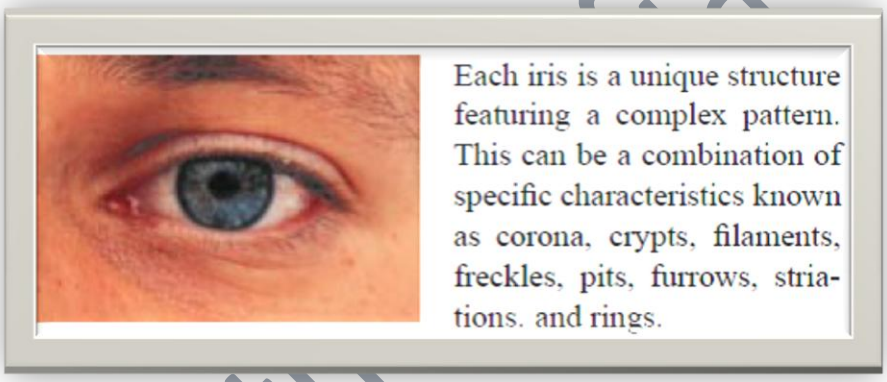
The minutiae found in the fingerprint image are also used to store the fingerprint for future comparisons. The minutiae are encoded and often also compressed. The size of such a master template usually is between 24 bytes and one kilobyte. Fingerprints contain a large amount of data. Because of the high level of data present in the image, it ispossible to eliminate falsematches and reduce the number of possiblematches to a smallfraction. This means that the fingerprint technology can be usedfor identification even within large databases. Fingerprint identificationtechnology has undergone an extensive research and developmentsince the seventies. The initial reason for the effort wasthe response to the FBI requirement for an identification searchsystem. Such systems are called Automated Fingerprint IdentificationSystems (AFIS) and are used to identify individuals in large databases (typically to find the offender of a crime according to afingerprint found at the crime scene or to identify a person whose identity is unknown). AFIS systems are operated by professionalswho manually intervene the minutiae extraction and matching processand thus their results are really excellent. In today's criminaljustice applications, the AFIS systems achieve over 98% identificationrate while the FAR is below 1%.The typical access control systems, on the other side, are completelyautomated. Their accuracy is slightly worse. The qualityof the fingerprint image obtained by an automated fingerprint readerfrom 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.[1][3]

Some newer systems are based not only on minutiae extraction,they use the length and position of the papilar lines as well. Afew system take into account even pores (theirspatial distribution), but the problem with pores is that they are too dependent on thefingerprint image quality and finger pressure.Most of the biometric fingerprint systems use the fingerprintreader to provide for the fingerprint bitmap image only, whole theprocessing 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 fingerprintdevices that do all the processing by the hardware.Themanufacturers of the fingerprint readers used to deliverthe fingerprint processing software with the hardware. Today, themarket specializes. Even if it is still possible to buy a fingerprintreader with a software package (this is the popular way especially for the low-

end devices for home or office use) there are manymanufacturers that produce fingerprint hardware only (e.g. fingerprintsilicon chips by Thomson) or software companies that offerdevice-independent fingerprint processing software (e.g. Neuro-dynamics).Device-independent software is not bound to imagesobtained by one single input devices, but their accuracy is very lowif various input devices are mixed.[7]

2.2 Iris

The iris is the coloured 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.[7]



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).

The PC iris uses a hand-held personal iris imager that functions as a computer peripheral.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 hasstepped in front of the camera. It is also able to guide the person audily into the correctposition.

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. 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.

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. 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}).

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 rate 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 (nonprofessional) users. 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. 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.

2.3 Retina

Retina scan isbased on the bloodvessel pattern in theretina of the eye.Retina scan technologyis older than theiris scan technologythat also uses a partof the eye. The firstretinal scanning systemswere launchedby EyeDentify in1985. The main drawback of the retina scan is its intrusiveness. The method of obtaining a retina scan is personally invasive. A laserlight must be directed through the cornea of the eye. Also the operationof the retina scanner is not easy. A skilled operator is requiredand the person being scanned has to follow his/her directions.A retina scan produces at least the same volume of data as afingerprint 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 theeye signature template is 96 bytes.The retinal scanning systems are said to be very accurate. Forexample the EyeDentify's retinal scanning system has reputedlynever falsely verified an unauthorized user so far. The false rejectionrate, on the other side, is relatively high as it is not always easyto capture a perfect image of the retina.

Retina is not directly visibleand so a coherent infraredlight source is necessary toilluminate the retina. Theinfrared energy is absorbedfaster by blood vessels in theretina than by the surroundingtissue. The image of the retina blood vessel pattern is then analysedfor characteristic points within the pattern. The retinascan is more susceptible to some diseases than the iris scan,but such diseases are relatively rare. [6]

Retinal scanningis used only rarelytoday because it isnot user friendly andstill remains veryexpensive. Retinascan is suitable forapplications wherethe high security isrequired and the user'sacceptance is nota major aspect. Retinascan systems areused in many U.S.prisons to verify theprisoners before theyare released.The check of the eye liveness is usually not of a significant concern as themethod of obtaining the retina blood vessel pattern is rather complicated and requiresan operator.[2]

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.

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 aremost 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 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.

Fig: ***Hand Geometry Scanner***
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 diode on the front panel.

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 x 30 x 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. 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 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 about0.1%. These numbers are difficult to obtain in reality. FAR of 3% and FRR of 10% at the middle security threshold are more realistic.The verification 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 dynamicsof making the signature, rather than a direct comparison of the signatureitself afterwards. The dynamics is measured as a means ofthe pressure, direction, acceleration and the length of the strokes, number of strokes and their duration. The most obvious and importantadvantage of this is that a fraudster cannot glean any informationon how to write the signature by simply looking at one thathas been previously written.

Pioneers of the signature verification first developed a reliablestatistical method in 1970s. This involved the extraction of ten ormore writing characteristics such as the number of times the penwas lifted, the total writing time and the timing of turning points.The matching process was then performed using fairly standardstatistical correlation methods. Newer sequential techniques treatthe signature as a number of separate events, with each event consistingof the period between the pen striking the writing surfaceand lifting off again. This approach is much more flexible. If themajority of the signature is accurate and only one event is missingor added then this event can be easily ignored.

There are various kinds ofdevices used to capture the signaturedynamics. These are eithertraditional tablets or specialpurpose devices. Tablets capture 2D coordinates and the pressure.Special pens are able to capture movements in all 3 dimensions.

Tablets have two significant disadvantages. First, the resulting digitalisedsignature 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 inkcartridge inside and can be used to write with them on paper. [6]

Fig: (a) E-pad (b) SmartPen

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 obtainedfrom a signature from a person has to allowfor quite some variability. Most of the signature dynamics systemsverify the dynamics only, they do not pay any attention to the resultingsignature. A few systems claim to verify both (i.e. the signaturedynamics as well as the resulting signature look itself). Ourexperience shows that if the system does not verify the resulting signature, then the signature that is accepted as a true match maylook significantly different from the master template. The speedof writing is often the most important factor in the decision process,so it is possible to successfully forge a signature even if theresulting signature looks so different that any person would notice.We have tried simple attempts to sign as other users as wellas simulation of attacks where the attacker has seen a user signingonce or several times. Our results show that individuals' ability to fake signature dynamics substantially improves after they see theway the true signers sign.

The size of data obtained during the signing process is around20 KB. The size of the master template, which is computed from 3to 10 signatures, varies from around 90 bytes up to a few kilobytes. Even if the size of the master template is relatively high the signaturerecognition has problems with match discrimination and thusis suitable for verification only.The accuracy of the signature dynamics biometric systems is not high, the crossover rate published by manufacturers is around2%, but according to our own experience the accuracy is muchworse.The leading companies in the signature systems are Cyber-Sign, 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 facialrecognition has never been treated as a science.

Any camera (with a sufficient resolution) can be used to obtainthe image of the face. Any scanned picture can be used aswell. Generally speaking the better the image source (i.e. cameraor scanner) the more accurate results we get. The facial recognition systems usually use only the gray- scale information. Colours (if 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 featuresmay not be easily discernible. There exist even infrared camerasthat can be used with facial recognition systems.

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

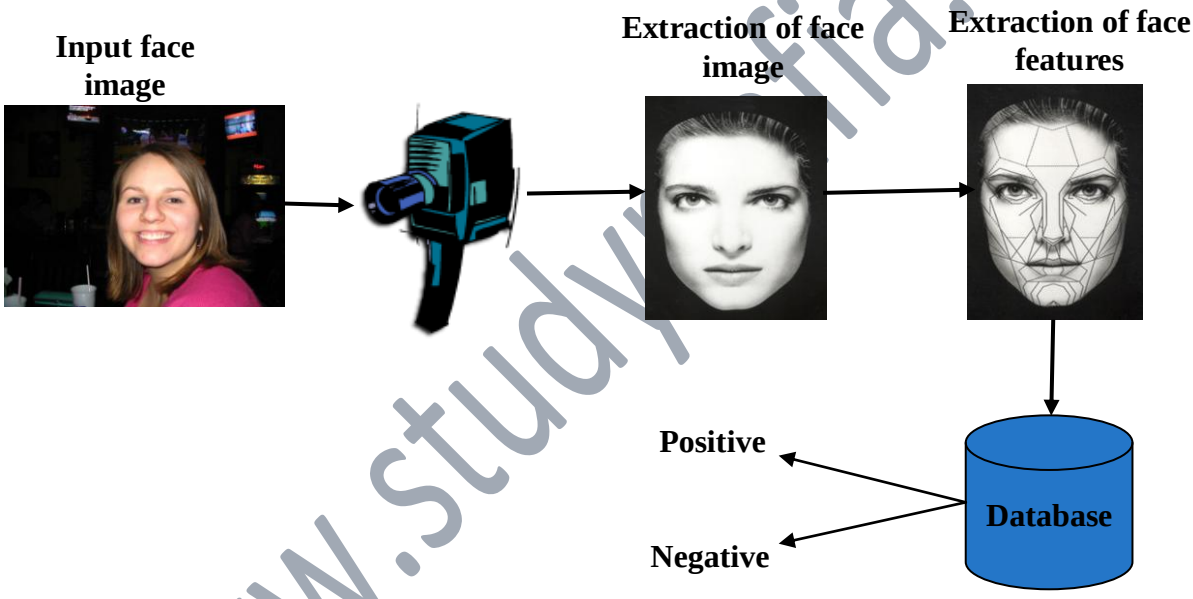
The first task ofthe processing softwareis to locate theface (or faces) withinthe image. Then thefacial characteristicsare extracted. Facialrecognition technology has recently developed into two areas: *facial metrics* and *eigenfaces*.Facial metrics technology relies on the measurement of the specificfacial features (the systems usually look for the positioning ofthe eyes, nose and mouth and the distances between these features).Another method for facial recognition has been developed inthe past three years. The method is based on categorizing facesaccording 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 basedon 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 processingand facialsimilarity decisionprocess is done bythe computer softwareat the moment,this processing requiresquite a lotof computing powerand so it is noteasy to assemble astand-alone devicefor face recognition. There are some efforts (by companies like Siemens) to create a special-purpose chip with embedded facerecognition instruction set.

The accuracy of the face recognition systems improves withtime, but it has not been very satisfying so far. According to ourexperience there is still a potential for improving the algorithms forface location. The current software often does not find the face atall or finds “a face” at an incorrect place. This significantly makesthe results worse. Better results can be achieved if the operatoris able to tell the system exactly where the eyes are positioned.The systems also have problems to distinguish very similar per- sons like twins and any significant change in hair or beard style requiresre-enrollment. Glasses can also cause additional difficulties.The quoted accuracy of facial recognition systems varies significantly,many systems quote the crossover accuracy of less than onepercent.

The numbers from real systems are not so pleasant, thecrossover accuracy is much higher and indicates that these systemsare not suitable for identification. If security is the main concernthen even the verification accuracy may not be sufficiently good.Facial recognition systems are offered by a great number ofsuppliers nowadays, to name a few of them: Miros, Neurodynamicsor Visionics.[7]

The face recognition system does not require any contact with the person and can be fooled with a picture if no countermeasuresare active. The liveness detection is based most commonly on facialmimics. The user is asked to blink or smile. If the image changes properly then the person is considered "live". A few systemscan simultaneously process images from two cameras, fromtwo different viewpoints. The use of two cameras can also avoidfooling the system with a simple picture. [5]



2.7 Speaker verification

The principle of speaker verification is to analyse the voice ofthe user in order to store a voiceprint that is later used for identification/verification. Speaker verification and speech recognition aretwo different tasks. The aim of speech recognition is to find *what* has been told while the aim of the speaker verification is *who* toldthat. Both these technologies are at the edge between research andindustrial development. Texas Instruments reported their work inspeech verification for access control already in the early 1970's.There are many commercial systems available today, but their accuracystill can be improved.

Speaker verification focuses on the vocal characteristics thatproduce speech and not on the sound or the pronunciation of thespeech itself. The vocal characteristics depend on the dimensionsof the vocal tract, mouth, nasal cavities and the other speech processingmechanisms of the human body.

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

The system typically asks the user to pronounce a phrase duringthe 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 replayattacks; if an attacker records the user's phrase and replays it laterthen he/she can easily gain the user's privilege. More sophisticatedsystems use a kind of challenge-response protocol. During the enrolment 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 casethe system not only compares the voiceprints, but also deploys thespeech recognition algorithms and checks whether the proper challengehas really been said. There exist (very few) systems that arereally text independent and can cope with the full vocabulary.

Speaker verification is quite secure from the professional mimics since the system make a comparison of the word stored in adifferent way than humans compare voices.Currently there are three major international projects in thefield 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 fewof the leading companies.Speaker verification is a biometric technique based on behavioural characteristic and as such can be negatively affected by the current physical condition and the emotional state. The accuracyof the speaker verification can also be affected by the background and network noise in the input signal. This increases the false rejectionrate. During the tests of a speaker verification system inthe Sandia Labs the false acceptance rate after a single attempt was 0.9% and the false

rejection rate after *three* attempts was 4.3%. Atrial at UBS's Ubilab achieved the equal error rate of 0.16% after aone attempt.

2.8 Other biometric techniques

2.8.1 Palmprint

Palmprint verification is a slightly different implementation ofthe fingerprint technology. Palmprint scanning uses optical readersthat are very similar to those used for fingerprint scanning, theirsize is, however, much bigger and this is a limiting factor for theuse in workstations or mobile devices.

2.8.2 Hand vein

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

2.8.3 DNA

DNA sampling is rather intrusive at present and requires a formof tissue, blood or other bodily sample. This method of capture stillhas to be refined. So far the DNA analysis has not been sufficientlyautomatic to rank the DNA analysis as a biometric technology.The analysis of human DNA is now possible within 10 minutes. Assoon as the technology advances so that DNA can be matched automaticallyin real time, it may become more significant. At present DNA is very entrenched in crimedetection and so will remain inthe law enforcement area for the time being.

2.8.4 Thermal imaging

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

2.8.5 Ear shape

Identifying individuals by the ear shape is used in law enforcementapplications where ear markings are found at crime scenes.Whether this technology will progress to access control applicationsis yet to be seen. An ear shape verifier (Optophone) is producedby a French company ART Techniques. It is a telephonetypehandset within which is a lighting unit and cameras whichcapture two images of the ear.

2.8.6 Body odour

The body odour biometrics is based on the fact that virtually eachhuman smell is unique. The smell is captured by sensors that arecapable to obtain the odour from non-intrusive parts of the body suchas the back of the hand. Methods of capturing a person's smell arebeing explored by Mastiff Electronic Systems. Each human smellis made up of chemicals known as volatiles. They are extracted bythe system and converted into a template.The use of body odour sensors brings up the privacy issue asthe body odour carries a significal amount of sensitive personalinformation. It is possible to diagnose some diseases or activitiesin the last hours (like sex, for example) by analysing the body odour.

2.8.7 Keystroke dynamics

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

2.8.8 Fingernail bed

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

Chapter – 3

PRACTICAL ISSUES

3.1 The Core Biometric Technology

There are at least ten biometric techniques commercially availableand new techniques are in the stage of research and development.Whatconditions must be fulfilled for a biological measurement to become a biometric? Any human physiological or behavioural characteristics can become a biometric provided the followingproperties are fulfilled.

*__Universality:__ This means that every person should have thecharacteristics. It is really difficult to get 100% coverage. There are mute people, people without fingers or with injuredeyes. All these cases must be handled.

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

*__Permanence:__ This means that the characteristics should beinvariant with time. While the iris usually remains stableover decades, a person's face changes significantly with time.The signature and its dynamics may change as well and thefinger is a frequent subject to injuries.

*__Collectability:__ This means that the characteristics must bemeasured quantitatively and obtaining the characteristicsshould be easy. Face recognition systems are not intrusiveand obtaining of a face image is easy. In the contrast theDNA analysis requires a blood or other bodily sample. Theretina scan is rather intrusive as well.

*__Performance:__ This refers to the achievable identification/verification accuracy and the resources and working orenvironmental conditions needed to achieve an acceptableaccuracy. The crossover accuracy of iris-based systems isunder 1% and the system is able to compare over 4 X 10^6iriscodes in one second. The crossover accuracy of somesignature dynamics systems is as high as 25% and theverification decision takes over one second.

*__Acceptability:__ This indicates to what extend people are willing to accept the biometric system. Face recognition systemsare personally not intrusive, but there are countries wheretaking pictures of persons is not viable. The retina scannerrequires an infrared laser beam directed through the corneaof 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 controlsystem that can be easily fooled with a fingerprint modelor a picture of a user's face does not provide much security.[7]

3.2 The layer model

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

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. Thequality of the first biometric sample is crucial for further authenticationsof the user, so the quality of this biometric sample must beparticularly checked and if the quality is not sufficient, the acquisitionof the biometric sample must be repeated. It may happen thateven 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 injuredeyes. Both these categories create a "failed to enroll" group ofusers. Users very often do not have any previous experiences with the kind of the biometric system they are being registered with, sotheir behaviour at the time of the first contact with the technologyis not natural. This negatively influences the quality of the firstmeasurement and that is why the first measurement is guided by aprofessional 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 processingis 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 theraw format (say as a bitmap). The raw measurements contain a lotof noise or irrelevant information, which need not be stored. Sothe measurements are processed and only the important featuresare extracted and used. This significantly reduces the size of thedata. The process of feature extraction is not lossless and so the extracted features cannot be used to reconstruct the biometric samplecompletely.

Storage of master characteristics

After processing the first biometric sample and extracting thefeatures, we have to store (and maintain) the newly obtained mastertemplate. Choosing a proper discriminating characteristic forthe categorization of records in large databases can improve identification (search) tasks later on. There are basically 4 possibilitieswhere to

store the template: in a card, in the central database ona 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 storageon a card has an advantage, because in this case no biometricdata must be stored (and potentially misused) in a central database.The storage on a card requires a kind of a digital signature of themaster template and of the association of the user with the mastertemplate. Biometric samples as well as the extracted features are very sensitive data and so the master template should be storedalways encrypted no matter what storage is used.As soon as the user is enrolled, he/she can use the system forsuccessful authentications or identifications. This process is typicallyfully automated and takes the following steps:

Acquisition(s)

The current biometric measurements must be obtained for thesystem to be able to make the comparison with the master template.These subsequent acquisitions of the user's biometric measurementsare done at various places where the authentication ofthe user is required. This might be user's computer in the office, anATM machine or a sensor in front of a door. For the best performancethe kind of the input device used at the enrollment and forthe subsequent acquisitions should be the same. Other conditionsof use should also be as similar as possible with the conditions atthe 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 fullyautomatic 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 devicedoes not show any preview of the sample obtained, so for examplein the case of a fingerprint reader, the user does not know whetherthe positioning of the finger on the reader and the pressure is correct.Secondly, as the reader is left unattended, it is up to the readerto check that the measurements obtained really belong to a livepersons (the liveness property). For example, a fingerprint readershould tell if the fingerprint it gets is from a live finger, not from amask that is put on top of a finger. Similarly, an iris scanner shouldmake sure that the iris image it is getting is from a real eye not apicture of an eye. In many biometric

techniques (e.g. fingerprinting)the further processing trusts the biometric hardware to checkthe liveness of the person and provide genuine biometric measurementsonly. Some other systems (like the face recognition) checkthe user's liveness in software (the proper change of a characteristicwith time). No matter whether hardware or software is used, ensuring that the biometric measurements are genuine is crucialfor the system to be secure. Without the assumption of the genuinedata obtained at the input we cannot get a secure system. It isnot possible to formally prove that a reader provides only genuinemeasurements and this affects also the possibility of a formal proof of the security of whole the biometric system. The liveness test ofa person is not an easy task. New countermeasures are always to befollowed by newer attacks. We do not even know how efficient thecurrent countermeasures are against the attacks to come. Biometricreaders are not yet the main target ofsophisticated criminals.But then we can expect a wave of professional attacks. We haveseen a few biometric readers where the estimated cost of an attackis as low as a few hundred dollars. The security of such a system isreally poor.[3]

Creation of new characteristics

The biometric measurements obtained in the previous step areprocessed and new characteristics are created. The process of featureextraction is basically the same as in the case of the enrollment.Only a single biometric sample is usually available. Thismight mean that the number or quality of the features extracted islower than at the time of enrollment.

Comparison

The currently computed characteristics are then compared withthe characteristics obtained during enrollment. This process is verydependent on the nature of the biometric technology used. Sometimesthe desired security threshold is a parameter of the matchingprocess, 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 mastertemplates for a few different fingers). For an identification request the new characteristics are matched against a large number of mastertemplates (either against all the records in the database or if thedatabase is clustered then against the relevant part of the database)

Decision

The final step in the verification process is the yes/no decisionbased on the threshold. This security threshold is either a parameterof the matching process or the resulting score is compared withthe threshold value to make the final decision. In the case of identification the user whose master template exceeds the thresholdis returned as the result. If multiple master templates exceed thethreshold then either all these users are returned as the result or thetemplate 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 usersis much lower. Especially the false rejection rate is in reality veryhigh (very often over 10%). This prevents the legitimate users togain their access rights and stands for a significant problem of thebiometric systems.

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 inquestion or to find an offender of a crime according to trailsleft on the crime scene. The operators of these systems donot have any reason to cheat the system, so the only task forthe cryptography is to secure the sensitive biometric data.

* Access control systems. These systems are used by ordinaryusers to gain a privilege or an access right. Securing such asystem 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 measurementsare secret and grant access when matching biometric measurementsare presented. Such systems cannot cope with the situationswhen the biometric measurements are disclosed, because thebiometrics cannot be changed (unless the user is willing to havean organ transplant). Moreover, the user will not learn that his/herbiometric is disclosed. People leave fingerprints on everythingthey touch, and the iris can be observed anywhere they look.Biometrics definitely are sensitive data and therefore should beproperly protected, but they cannot be considered secret. So the security of the system cannot be based on knowledge of thebiometric characteristics. When using secret keys or passwords for authentication, a common method to defeat replay attacksis to use a challenge-response protocol, in which the passwordis never transmitted. Instead, the server sends a challenge thatcan only be answered correctly if the client knows the correctpassword. Unfortunately, this method does not apply to biometricdata. The difference between a password and a fingerprint is that the password is supposed to be secret, while the fingerprint is not.[1]

Hence, replaying attacks are inherent with biometric authenticationschemes.The only way how to make a system secure is to make sure that the characteristics presented came from a real person and wereobtained at the time of verification.

The liveness problem

So-called liveness problem is a closely related issue. One has tomake sure that the authentication device is verifying a live person.The liveness test is dependent on the kind of biometric technologyused 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 protocolsused in cryptography. The user is then asked to pronounce a randomly chosen phrase or make a certain movement. The biometricsystem has to trust the input device it provides only genuine measurements.We cannot make a secure system if we do not trust the biometric input device. If a malicious party can easily tamper witha fingerprint scanner, the whole system is not secure no matter howsecure the other parts of the system are. In terms of the hardwareof the device, until now, only smartcard-based devices can providecertain level of tamper-resistance. (Note: Smartcards are hardlyever tamper-proof, rather tamper-resistant.) The trustworthiness ofa device is also a relative concept that depends on how the deviceis used. For example, a removable optical finger scanner put in apublic place may be treated

asuntrustworthy, while the same removableoptical finger scanner may be treated as trustworthy in aplace where there is a constant human supervision.[1]

Authentication software

The biometric system must be convinced that the presented biometricmeasurements 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 doneoff-device, then the operating environment of the software and thecommunication link between the software and the device, have tobe secure. For example, in a client-server application, if the clientworkstation is not trusted, then there is no point authenticating a user using that workstation. If one chooses to run the authenticationsoftware at the server side, then the communication link betweenthe server and the device itself (not just the clientworkstation) hasto be secured. Otherwise, a malicious party or even the workstationitself may intercept the communication and replay recordedbiometric data. One way to defeat replaying attacks is to put a separate secret key in the device and use challenge/response protocolwith this key. Obviously, the device has to be trustworthy.The best solution probably is to use a TLS-like protocol withmandatory authentication of both parties. In any case it is necessaryto transmit the whole biometric measurements over the connection.

Either the reader sends the biometric measurements to theworkstation (or server or whatever grants the access right) to make the match or the workstation provides the master template to thereader that makes the matching. Hashing in the usual sense andsending only the hash over the link does not help here, because thebiometric measurements never are the same. To make it work we either would have to ensure that the biometric measurements arealways the same (but see the warning below) or change the hashfunction not to depend on all the input.One has to consider that 100% similarity of two samples fromdifferent biometric measurements implies a good forgery. This istrue with almost 100% probability.

Improving security with biometrics

Can biometrics help cryptography to increase the security?Here the answer is not so clear.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 mustbe kept secret, and here the biometric technologies might help.Indeed, one of the most promising applications of biometricsis the secret key protection. If a user's local workstation is trusted,then the problem of the authentication software is minor, but the inputdevice must be trustworthy. The security concerns are the sameno matter whether the secret (or private) keys are stored on a smart-card 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 secureplace, usually a smartcard. Smartcard based solutions where the secret key is unlocked only after a successful biometric verificationincrease the overall security, as the biometric data does not need to leave the card. For smartcards the fingerprint techniqueswith a silicon fingerprint reader are most commonly used today.It is necessary to distinguish securing a key with biometrics andgenerating a key from biometrics. The latter does not work. It mustbe pointed out that biometric data cannot be used as capability tokensin 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 canmean that the user has the right to use certain application. However,this does not apply to biometric data. As we already know biometricsare not secrets. One viable way is to use digital certificates. Digital certificates can be used as capabilities or digital identitiesthat allow users to access remote applications, while biometrics isused to secure the access/usage of the private keys associated withthe digital certificates.[4]

Chapter – 4

CONCLUSION

Even if the accuracy of the biometric techniques is not perfectyet, there are many maturebiometric systems available now. Properdesign and implementation of the biometric system can indeedincrease the overall security, especially the smartcard based solutionsseem to be very promising. Making a secure biometric systemsis, however, not as easy as it might appear. The word biometricsis very often used as a synonym for the

perfect security. This isa misleading view. There are numerous conditions that must be takenin account when designing a secure biometric system. First, itis necessary to realize that biometrics are not secrets. This implies that biometric measurements cannot be used as capability tokensand it is not secure to generate any cryptographic keys from them.Second, it is necessary to trust the input device and make the communicationlink secure. Third, the input device needs to check theliveness of the person being measured and the device itself should be verified for example by a challenge-response protocol.

REFERENCES

- **Google.com**
- **Wikipedia.org**
- **Studymafia.org**
- **Pptplanet.com**