A

Seminar report

On

BIOMETRIC SECURITY SYSTEMS

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

SUBMITTED TO:
www.studymafia.org

SUBMITTED BY:
www.studymafia.org

Acknowledgement

I would like to thank respected Mr…….. and Mr. ……..for giving me such a wonderful opportunity to expand my knowledge for my own branch and giving me guidelines to present a seminar report. It helped me a lot to realize of what we study for.

Secondly, I would like to thank my parents who patiently helped me as i went through my work and helped to modify and eliminate some of the irrelevant or un-necessary stuffs.

Thirdly, I would like to thank my friends who helped me to make my work more organized and well-stacked till the end.

Next, I would thank Microsoft for developing such a wonderful tool like MS Word. It helped my work a lot to remain error-free.

Last but clearly not the least, I would thank The Almighty for giving me strength to complete my report on time.

Preface

I have made this report file on the topic **BIOMETRIC SECURITY SYSTEMS**; 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.

Contents

1.Introduction

Biometrics, which is formed from the two ancient Greek words *bios* and *metron* which mean life and measure respectively, refers to two very different fields of study and application. The first, which is the older and is used in biological studies, is the collection, synthesis, analysis and management of biology. Biometrics in reference to biological sciences, or biostatistics, has been studied since the early twentieth century[1].

More recently and incongruously, the term's meaning has been broadened to include the study of methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits.

Some researchers have coined the term **behaviometrics** for behavioral biometrics such as typing rhythm or mouse gestures where the analysis can be done continuously without interrupting or interfering with user activities.

Biometrics uses unique features, like the iris of your eye, to identify you.

2.Overview

Biometrics are used to identify the input sample when compared to a template, used in cases to identify specific people by certain characteristics.

- possession-based

  using one specific "token" such as a security tag or a card

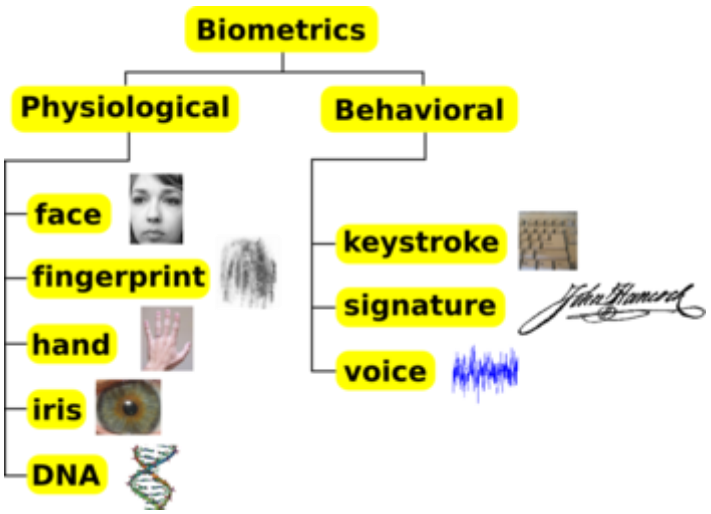
- knowledge-based

  the use of a code or password.

Standard validation systems often use multiple inputs of samples for sufficient validation, such as particular characteristics of the sample. This intends to enhance security as multiple different samples are required such as security tags and codes and sample dimensions.

For some security systems, one method of identification is not enough. **Layered** systems combine a biometric method with a keycard or PIN. **Multimodal** systems combine multiple biometric methods, like an iris scanner and a voiceprint system.

3.Biometricals



Classification of some biometric traits

Biometric characteristics can be divided in two main classes, as represented in figure on the right:

- **physiological** are related to the shape of the body. The oldest traits, that have been used for more than 100 years, are fingerprints. Other examples are face recognition, hand geometry and iris recognition.

Recently, a new trend has been developed that merges human perception to computer database in a brain-machine interface. This approach has been referred to as **cognitive biometrics**. Cognitive biometrics is based on specific responses of the brain to stimuli which could be used to trigger a computer database search. Currently, cognitive biometrics systems are being developed to use brain response to odor stimuli, facial perception and mental performance for search at ports and high security areas. These systems are based on use of functional transcranial Doppler(fTCD) and functional transcranial Doppler spectroscopy(fTCDS) to obtain brain responses, which are used to match a target odor, a target face or target performance profile stored in a computer database. Thus, the precision of human perception provides the data to match that stored in the computer with improve sensitivity of the system.

- **behavioral** are related to the behavior of a person. The first characteristic to be used, still widely used today, is the signature. More modern approaches are the study of keystroke dynamics and of voice.

Strictly speaking, *voice* is also a physiological trait because every person has a different pitch, but voice recognition is mainly based on the study of the way a person speaks, commonly classified as behavioral.

Other biometric strategies are being developed such as those based on gait(way of walking), retina, hand veins, finger veins, ear canal, facial thermograph, DNA, odor and scent and palm prints.

3.1 Odor and Scent Cognitive Biometric Systems

In forensics, odor evaluation can make important contributions in both prosecution and defense of criminal cases. The use of blood hounds and other scent following dogs to identify individual people or their scent trails in the environment on the basis of a previous offered reference scent article such as handkerchief, hat, and other items of clothing has been described Canine scent identification evidence is usually accepted in court to suggest the unique identification of an accused individual in the same way that finger prints are used. The latter is premised on the alleged factuality of the "individual odor theory," which hold that each person has a unique scent that can be identified by the dog and related back to a specific individual. High courts have accepted the performance of canine scent identification, even when it is claimed that they are detecting the scent of a specific individual at the scene of a crime nearly 2 years after the crime was committed. It is also imperative that further research studies of the abilities of such scenting dogs be undertaken. Especially, the ability to scent match odors from individuals to handled objects, under controlled laboratory conditions. However, in some studies dogs have proven capable of performing such scent matching tasks at levels greater than chance, their error rates are seldom more than 10 to 20% . Errors may also be introduced by the interpretation of the behavioral response of the dog. What is probably lacking is an objective physiologic correlate of scent matching odors in canine detectives.

3.2 Facial Cognitive Biometric Systems

The analysis and recognition of facial features is a tool used in the detection of criminals and undesirables. Conventional biometric methods introduced to improve security are mainly based on cross matching the face of the person with that recorded the in their identification materials. At present, the data is static and would not, for example, identify suspects with cosmetic or plastic surgery modification of their faces to escape identification. However, it is possible to train persons that could be referred to as "face-minders", to memorized faces of suspects on a watch-list, by way of example. Trainees could acquire skills of cross-matching key features of faces of persons seen at the ports as compared to that in the forensic facial database. However to be effective, subjective judgment must be replaced with objective physiologic correlates of good matches. This will require objective online detection of

physiologic variables, suggestive of facial memory involvement and cross matching the online variables to expected variables, for the particular face involved. The brain-machine interface method is based on functional transcranial Doppler spectroscopy(fTCDS) and detects the presence of an equivalent to cortical long-term potentiation (CLTP), in the left middle cerebral artery in male face minders and triggers a search for a matching face, to be reviewed by other observers.

3.3 Cognitive Performance Biometric Systems

Task performance using general intelligence must elicit responses in neural anatomic structures for processing of the information. It has been shown that working memory is typically associated with activations in the prefrontal cortex (PFC), anterior cingulate, parietal and occipital regions. These brain areas received blood supply from the middle cerebral arteries. Two fundamental working-memory processes have been identified: the passive maintenance of information in short-term memory and the active manipulation of this information. A brain-machine interface system was designed. A pattern of blood flow velocity changes is obtained in response to a set intelligence task, which is used to form a 'mental signature' that could be repeatedly recognized, in an automated man-machine interface system. The system is designed to go beyond passive recognition, but rather to set a desired level of 'mental performance', before access is gained into the system. The device could be used as a 'lie detector' based on the fact that, it could distinguish Wrong ANSWER from Correct ANSWER.

3.4 Handwriting

At first glance, using handwriting to identify people might not seem like a good idea. After all, many people can learn to copy other people's handwriting with a little time and practice. It seems like it would be easy to get a copy of someone's signature or the required password and learn to forge it.

But biometric systems don't just look at how you shape each letter; they analyze the act of writing. They examine the pressure you use and the speed and rhythm with which you write. They also record the sequence in which you form letters, like whether you add dots and crosses as you go or after you finish the word.

This Tablet PC has a signature verification system.

Unlike the simple shapes of the letters, these traits are very difficult to forge. Even if someone else got a copy of your signature and traced it, the system probably wouldn't accept their forgery.

A handwriting recognition system's sensors can include a touch-sensitive writing surface or a pen that contains sensors that detect angle, pressure and direction. The software translates the handwriting into a graph and recognizes the small changes in a person's handwriting from day to day and over time[7].

3.5 Hand and Finger Geometry

People's hands and fingers are unique -- but not as unique as other traits, like fingerprints or irises. That's why businesses and schools, rather than high-security facilities, typically use hand and finger geometry readers to **authenticate** users, not to **identify** them. Disney theme parks, for example, use finger geometry readers to grant ticket holders admittance to different parts of the park. Some businesses use hand geometry readers in place of timecards.

A hand geometry scanner

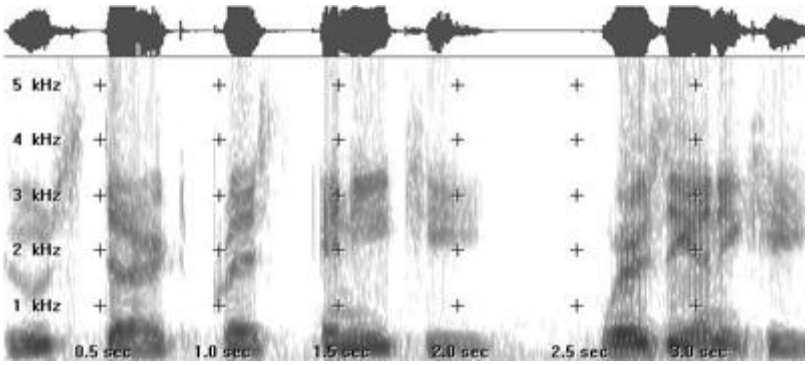
Systems that measure hand and finger geometry use a digital camera and light. To use one, you simply place your hand on a flat surface, aligning your fingers against several pegs to ensure an accurate reading. Then, a camera takes one or more pictures of your hand and the shadow it casts. It uses this information to determine the length, width, thickness and curvature of your hand or fingers. It translates that information into a numerical template.

Hand and finger geometry systems have a few strengths and weaknesses. Since hands and fingers are less distinctive than fingerprints or irises, some people are less likely to feel that the system invades their privacy. However, many people's hands change over time due to injury, changes in weight or arthritis. Some systems update the data to reflect minor changes from day to day. For higher-security applications, biometric systems use more unique characteristics, like voices[7].

3.6 Voiceprints

Your voice is unique because of the shape of your vocal cavities and the way you move your mouth when you speak. To enroll in a voiceprint system, you either say the exact words or phrases that it requires, or you give an extended sample of your speech so that the computer can identify you no matter which words you say.

When people think of voiceprints, they often think of the wave pattern they would see on an oscilloscope. But the data used in a voiceprint is a sound **spectrogram**, not a wave form. A spectrogram is basically a graph that shows a sound's frequency on the vertical axis and time on the horizontal axis. Different speech sounds create different shapes within the graph. Spectrograms also use colors or shades of grey to represent the acoustical qualities of sound.



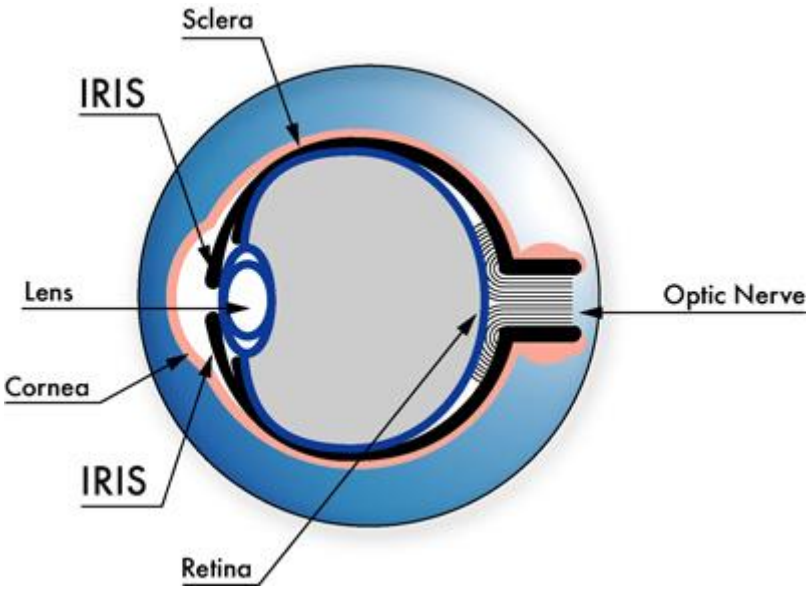
Speaker recognition systems use spectrograms

to represent human voices.

Some companies use voiceprint recognition so that people can gain access to information or give authorization without being physically present. Instead of stepping up to an iris scanner or hand geometry reader, someone can give authorization by making a phone call. Unfortunately, people can bypass some systems, particularly those that work by phone, with a simple recording of an authorized person's password. That's why some systems use several randomly-chosen voice passwords or use general voiceprints instead of prints for specific words. Others use technology that detects the artifacts created in recording and playback[7].

3.7 Iris Scanning

Iris scanning can seem very futuristic, but at the heart of the system is a simple CCD digital camera. It uses both visible and near-infrared light to take a clear, high-contrast picture of a person's iris. With near-infrared light, a person's pupil is very black, making it easy for the computer to isolate the pupil and iris.



Eye anatomy

When you look into an iris scanner, either the camera focuses automatically or you use a mirror or audible feedback from the system to make sure that you are positioned correctly. Usually, your eye is 3 to 10 inches from the camera. When the camera takes a picture, the computer locates:

- The center of the pupil
- The edge of the pupil
- The edge of the iris
- The eyelids and eyelashes

It then analyzes the patterns in the iris and translates them into a code.
Iris scanners are becoming more common in high-security applications because people's eyes are so unique.

An iris scanner

The iris is a visible but protected structure, and it does not usually change over time, making it ideal for biometric identification. Most of the time, people's eyes also remain unchanged after eye surgery, and blind people can use iris scanners as long as their eyes have irises. Eyeglasses and contact lenses typically do not interfere or cause inaccurate readings.

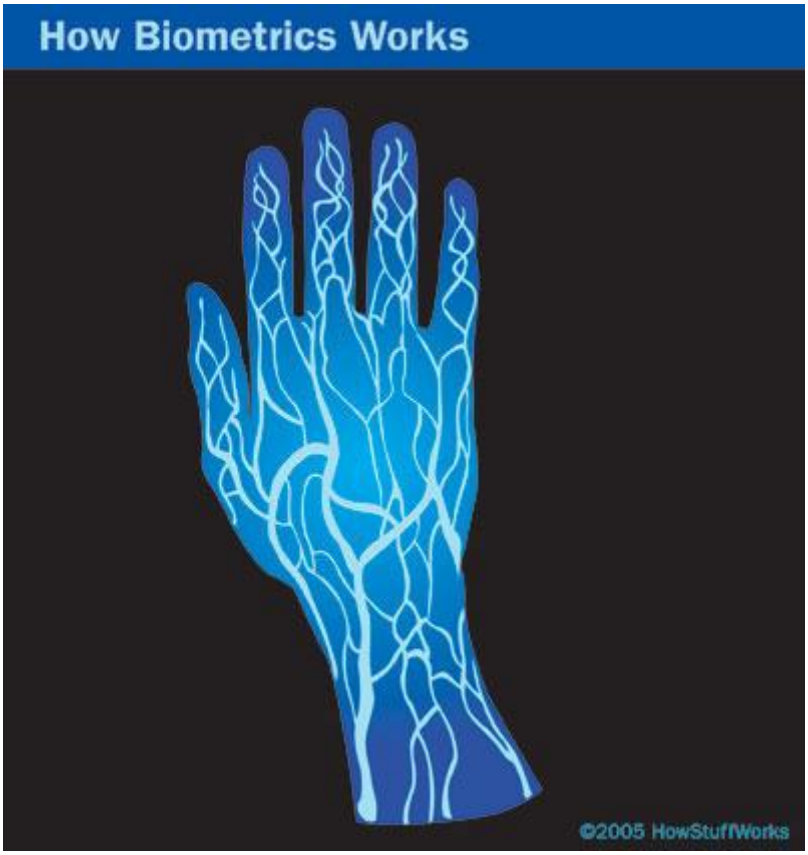
Retinal Scan

Some people confuse iris scans with **retinal scans**. Retinal scans, however, are an older technology that required a bright light to illuminate a person's retina. The sensor would then take a picture of the blood vessel structure in the back of the person's eye. Some people found retinal scans to be uncomfortable and invasive. People's retinas also change as they age, which could lead to inaccurate readings[7].

3.8 Vein Geometry

As with irises and fingerprints, a person's veins are completely unique. Twins don't have identical veins, and a person's veins differ between their left and right sides. Many veins are

not visible through the skin, making them extremely difficult to counterfeit or tamper with. Their shape also changes very little as a person ages.



Vein scanners use near-infrared light to reveal the patterns in a person's veins.

To use a vein recognition system, you simply place your finger, wrist, palm or the back of your hand on or near the scanner. A camera takes a digital picture using near-infrared light. The hemoglobin in your blood absorbs the light, so veins appear black in the picture. As with all the other biometric types, the software creates a reference template based on the shape and location of the vein structure.

Scanners that analyze vein geometry are completely different from vein scanning tests that happen in hospitals. Vein scans for medical purposes usually use radioactive particles. Biometric security scans, however, just use light that is similar to the light that comes from a remote control[7].

4. Comparison of various biometric technologies

It is possible to understand if a human characteristic can be used for biometrics in terms of the following parameters[2]:

- Universality

  each person should have the characteristic

- Uniqueness

  is how well the biometric separates individually from another.

- Permanence

  measures how well a biometric resists aging.

- Collectability

  ease of acquisition for measurement.

- Performance

  accuracy, speed, and robustness of technology used.

- Acceptability

  degree of approval of a technology.

- Circumvention

  ease of use of a substitute.

The following table shows a comparison of existing biometric systems in terms of those parameters:

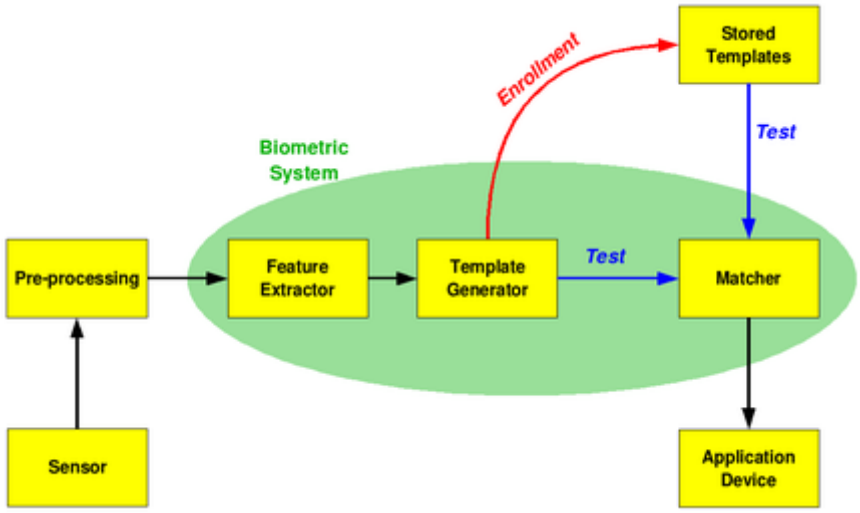
Comparison of various biometric technologies, modified from Jain et al., 2004 (**H**=High,

M=Medium, L=Low)

Biometrics:	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention*
Face	H	L	M	H	L	H	L
Fingerprint	M	H	H	M	H	M	H
Hand geometry	M	M	M	H	M	M	M
Keystrokes	L	L	L	M	L	M	M
Hand veins	M	M	M	M	M	M	H
Iris	H	H	H	M	H	L	H
Retinal scan	H	H	M	L	H	L	H
Signature	L	L	L	H	L	H	L
Voice	M	L	L	M	L	H	L
Facialthermograph	H	H	L	H	M	H	H
Odor	H	H	H	L	L	M	L
DNA	H	H	H	L	H	L	L
Gait	M	L	L	H	L	H	M
Ear Canal	M	M	H	M	M	H	M

A. K. Jain ranks each biometric based on the categories as being either low, medium, or high. A low ranking indicates poor performance in the evaluation criterion whereas a high ranking indicates a very good performance.

5.Biometric Systems



The basic block diagram of a biometric system

The diagram shows a simple block diagram of a biometric system. When such a system is networked together with telecommunications technology, biometric systems become telebiometric systems. The main operations a system can perform are *enrollment* and *test*. During the enrollment, biometric information from an individual is stored. During the test, biometric information is detected and compared with the stored information. Note that it is crucial that storage and retrieval of such systems themselves be secure if the biometric system is to be robust. The first block (sensor) is the interface between the real world and our system; it has to acquire all the necessary data. Most of the times it is an image acquisition system, but it can change according to the characteristics desired. The second block performs all the necessary pre-processing: it has to remove artifacts from the sensor, to enhance the input (e.g. removing background noise), to use some kind of normalization, etc. In the third block features needed are extracted. This step is an important step as the correct features need to be

extracted and the optimal way. A vector of numbers or an image with particular properties is used to create a *template*. A template is a synthesis of all the characteristics extracted from the source, in the optimal size to allow for adequate identifiability.

If enrollment is being performed the template is simply stored somewhere (on a card or within a database or both). If a matching phase is being performed, the obtained template is passed to a matcher that compares it with other existing templates, estimating the distance between them using any algorithm (e.g. Hamming distance). The matching program will analyze the template with the input. This will then be output for any specified use or purpose (e.g. entrance in a restricted area) .

6.Functions

A biometric system can provide the following two functions[3]:

- Verification

  Authenticates its users in conjunction with a smart card, username or ID number. The biometric template captured is compared with that stored against the registered user either on a smart card or database for verification

  .

- Identification

  Authenticates its users from the biometric characteristic alone without the use of smart cards, usernames or ID numbers. The biometric template is compared to all records within the database and a closest match score is returned. The closest match within the allowed threshold is deemed the individual and authenticated.

7.Performance

Biometric systems are succeptable to the following kinds of errors:

- False Rejection Rate (FRR) or Type I Error
- False Acceptance Rate (FAR) or Type II Error

Performance measurement:

Measurement	Shorthand acronym	Description
false accept rate/false match rate	FAR/FMR	The probability that the system incorrectly declares a successful match between the input pattern and a non-matching pattern in the database. It measures the percent of invalid matches. These systems are critical since they are commonly used to forbid certain actions by disallowed people.
false reject rate/false non-match rate	FRR/FNMR	The probability that the system incorrectly declares failure of match between the input pattern and the matching template in the database. It measures the percent of valid inputs being rejected.
Receiver operating characteristic/relative operating characteristic	ROC	In general, the matching algorithm performs a decision using some parameters (e.g. a threshold). In biometric systems the FAR and 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 trade-off (DET),* which is obtained using normal deviate scales on both axes. This more linear graph illuminates the differences for higher performances (rarer errors).

equal error rate/crossover error rate	EER/CER	The rate 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. Obtained from the ROC plot by taking the point where FAR and FRR have the same value. The lower the EER, the more accurate the system is considered to be.
failure to enroll rate	FTE or FER	When the percentage of data input is considered invalid and fails to input into the system. Failure to enroll happens when the data obtained by the sensor are considered invalid or of poor quality.
failure to capture rate	FTC	Within automatic systems, the probability that the system fails to detect a biometric characteristic when presented correctly.
template capacity		The maximum number of sets of data which can be input into the system..

As the sensitivity of biometric devices increases, it decreases the FAR but increases the FRR.The following table shows the state of art of some biometric systems:

State of art of biometric recognition systems

Biometrics	**EER**	**FAR**	**FRR**	**Subjects**	**Comment**	**Reference**
Face	n.a.	1%	10%	37437	Varied lighting, indoor/outdoor	FRVT (2002)
Fingerprint	n.a.	1%	0.1%	25000	US Government operational data	FpVTE (2003)

Fingerprint	2%	2%	2%	100	Rotation and exaggerated skin distortion	FVC (2004)
Hand geometry	1%	2%	0.1%	129	With rings and improper placement	(2005)
Iris	< 1%	0.94%	0.99%	1224	Indoor environment	ITIRT (2005)
Iris	0.01%	0.0001%	0.2%	132	Best conditions	NIST (2005)
Keystrokes	1.8%	7%	0.1%	15	During 6 months period	(2005)
Voice	6%	2%	10%	310	Text independent, multilingual	NIST (2004)

One simple but artificial way to judge a system is by EER, but not all the authors provided it. Moreover, there are two particular values of FAR and FRR to show how one parameter can change depending on the other. For fingerprint there are two different results, the one from 2003 is older but it was performed on a huge set of people, while in 2004 far fewer people were involved but stricter conditions have been applied. For iris, both references belong to the same year, but one was performed on more people, the other one is the result of a competition between several universities so, even if the sample is much smaller, it could reflect better the state of art of the field.

8. Issues and concerns

As with many interesting and powerful developments of technology, there are concerns about biometrics. The biggest concern is the fact that once a fingerprint or other biometric source has been compromised it is compromised for life, because users can never change their fingerprints. A theoretical example is a debit card with a personal Identification Number (PIN) or a biometric. Some argue that if a person's biometric data is stolen it might allow someone else to access personal information or financial accounts, in which case the damage could be irreversible. However, this argument ignores a key operational factor intrinsic to all biometrics-based security solutions: biometric solutions are based on matching, at the point of transaction, the information obtained by the scan of a "live" biometric sample to a pre-stored, static "match template" created when the user originally enrolled in the security

system. Most of the commercially available biometric systems address the issues of ensuring that the static enrollment sample has not been tampered with (for example, by using hash codes and encryption), so the problem is effectively limited to cases where the scanned "live" biometric data is hacked. Even then, most competently designed solutions contain anti-hacking routines. For example, the scanned "live" image is virtually never the same from scan to scan owing to the inherent plasticity of biometrics; so, ironically, a "replay" attack using the stored biometric is easily detected because it is too perfect a match.

The television program *MythBusters* attempted to break into a commercial security door equipped with biometric authentication as well as a personal laptop so equipped. While the laptop's system proved more difficult to bypass, the advanced commercial security door with "live" sensing was fooled with a printed scan of a fingerprint after it had been licked. There is no basis to assume that the tested security door is representative of the current typical state of biometric authentication, however. With careful matching of tested biometric technologies to the particular use that is intended, biometrics provide a strong form of authentication that effectively serves a wide range of commercial and government applications.

Biometric verification of an individual’s identity can help control the risks associated with misidentification. However, biometric verification can itself be compromised through vulnerabilities in the system. This can occur through deliberate attempts to breach security and the integrity of the biometric process as shown in the television program MythBusters. To address this risk the Biometrics Institute has established a Biometrics Vulnerability Assessment Methodology.

However, the clear concern is that the number of biometric samples of an individual are limited. If all samples are lost via compromise the legitimate owner will be unable to replace the old ones. Additionally, the limited number of samples means that there is a concern with secondary use of biometric data: a user who accesses two systems with the same fingerprint may allow one to masquerade is her to the other. Several solutions to this problem are actively being researched.

8.1 Privacy

A concern is how a person's biometric, once collected, can be protected. Australia has therefore introduced a Biometrics Institute Privacy Code in order to protect consumer personal data beyond the current protections offered by the Australian Privacy Act.

Another concern is that if the system is used at more than one location, a person's movements may be tracked as with any non-anonymous authentication system. An example of this would be posted security cameras linked to a facial recognition system, or a public transportation system requiring the use of biometry or registered identification card.

8.2 Biometrics sensors' obstacles

Different sensors (hardware producers), generating different biometrics outcomes, different outcomes cannot be encryptedly compared (they will never match). It is very difficult to create standard on identical encryption paths. Biometrics standard can be obtained only if the common information is unconcealed. Currently each biometric scanner's vendor is responsible for generating his own encryption method. In order to unify the biometrics collection method(s) the Standardization procedure must force Biometrics exposure, however, exposed biometrics information present a serious threat to privacy rights.

8.3 Marketing of biometric products

Despite confirmed cases of defeating commercially available biometric scanners, many companies marketing biometric products (especially consumer-level products such as readers built into keyboards) claim the products as replacements, rather than supplements, for passwords. Furthermore, regulations regarding advertising and manufacturing of biometric products are (as of 2006) largely non-existent. Consumers and other end users must rely on published test data and other research that demonstrate which products meet certain performance standards and which are likely to work best under operational conditions. Given the ease with which other security measures such passwords and access tokens may be compromised, and the relative resistance of biometrics to being defeated through alteration and reverse engineering, large scale adoption of biometrics may offer significant protection against the economic and social problems associated with identity theft.

- The use of fingerprints for identification in schools.

8.4 Sociological concerns

As technology advances, and time goes on, more private companies and public utilities may use biometrics for safe, accurate identification. These advances are likely to raise concerns such as:

- Physical

  Some believe this technology can cause physical harm to an individual using the methods, or that instruments used are unsanitary. For example, there are concerns that retina scanners might not always be clean.

- Personal Information

  There are concerns whether our personal information taken through biometric methods can be misused, e.g. by the government to determine unwanted traits in humans for global population control. Also, the data obtained using biometrics can be used in unauthorized ways without the individual's consent.

8.5 Danger to owners of secured items

When thieves cannot get access to secure properties, there is a chance that the thieves will stalk and assault the property owner to gain access. If the item is secured with a biometric device, the damage to the owner could be irreversible, and potentially cost more than the secured property. For example, in 2005, Malaysian car thieves cut off the finger of a Mercedes-Benz S-Class owner when attempting to steal the car.

8.6 Interoperability

In addition to the potential for invasions of privacy, critics raise several concerns about biometrics, such as:

- **Over reliance**: The perception that biometric systems are foolproof might lead people to forget about daily, common-sense security practices and to protect the system's data.
- **Accessibility**: Some systems can't be adapted for certain populations, like elderly people or people with disabilities.

Interoperability: In emergency situations, agencies using different systems may need to share data, and delays can result if the systems can't communicate with each other.

9. Cancelable Biometrics

Physical features, such as face, fingerprint, iris, retina, hand, or behavioral features, such as signature, voice, gait, must fulfill a certain criteria to qualify for use in recognition. They must be unique, universal, acceptable, collectible and convenient to the person, in addition, to reliability at recognition, performance and circumvention. Most importantly, however, permanence is a key feature for biometrics. They must retain all the above features in particular the uniqueness unchanged, or acceptably changed, over the lifetime of the individual. On the other hand, this fundamental feature has brought biometrics to challenge a new risk. If biometric data is obtained, for example compromised from a database, by unauthorized users, the genuine owner will lose control over them forever and lose his/her identity.

Previously, research was focusing on using biometrics to overcome the weakness in traditional authentication systems that use tokens, passwords or both. Weakness, such as sharing passwords, losing tokens, guessable passwords, forgetting passwords and a lot more, were successfully targeted by biometric systems, although accuracy still remains a great challenge for many different biometric data. But one ordinary advantage of password does not exist in biometrics. That is re-issue. If a token or a password is lost or stolen, they can be cancelled and replaced by a newer version i.e. reissued. On the other hand, this is not naturally available in biometrics. If someone’s face is compromised from a database, they cannot cancel it neither reissue it. All data, including biometrics is vulnerable whether in storage or in processing state. It is relatively recently research has been undertaken to consider protection of biometric data more seriously. Cancelable biometrics is a way in which

to inherit the protection and the replacement features into biometrics. It was first proposed by Ratha et al[4]. Besides reliable accuracy performance and the replacement policy cancellable biometric has to be non-revisable in order to fulfill the aim.

Several methods for generating cancellable biometrics have been proposed. Essentially, cancelable biometrics perform a distortion of the biometric image or features before matching. The variability in the distortion parameters provides the cancelable nature of the scheme.

In general, cancelable biometrics may be seen to represent a promising approach to address biometric security and privacy vulnerabilities. However, there are several concerns about the security of such schemes. First, there is very little work analysing their security, except for an analysis of biohashing[5]. Secondly, while distortion schemes should be *preferably non-invertible*[6], no detailed proposed scheme has this property. In fact, it would appear to be trivial to *undistort* the template given knowledge of the distortion key in most cases. Third, cancelable biometrics would appear to be difficult to implement in the untrusted scenarios for which they are proposed: if the user does not trust the owner of the biometric sensor to keep the biometric private, how can they enforce privacy on the distortion parameters used? This last concern is perhaps the most serious: the security of cancelable biometrics depends on secure management of the distortion parameters, which must be used for enrollment and made available at matching. Furthermore, such keys may not be much better protected than current passwords and PINs. In summary, cancelable biometrics offer a possible solution to certain serious security and privacy concerns of biometric technology; however, current schemes leave a number of important issues unaddressed. Research is very active in this subject, and may succeed in addressing these concerns.

10. Uses and initiatives

10.1 Australia

Visitors intending to visit Australia may soon have to submit to biometric authentication as part of the Smartgate system, linking individuals to their visas and passports. Biometric data are already collected from some visa applicants by Immigration. Australia is the first country

to introduce a Biometrics Privacy Code, which is established and administered by the Biometrics Institute. The Biometrics Institute Privacy Code Biometrics Institute forms part of Australian privacy legislation. The Code includes privacy standards that are at least equivalent to the Australian National Privacy Principles (NPPs) in the Privacy Act and also incorporates higher standards of privacy protection in relation to certain acts and practices. Only members of the Biometrics Institute are eligible to subscribe to this Code. Biometrics Institute membership, and thus subscription to this Code, is voluntary.

10.2 Brazil

Since the beginning of the 20th century, Brazilian citizens have had user ID cards. The decision by the Brazilian government to adopt fingerprint-based biometrics was spearheaded by Dr. Felix Pacheco at Rio de Janeiro, at that time capital of the Federative Republic. Dr. Pacheco was a friend of Dr. Juan Vucetich, who invented one of the most complete tenprint classification systems in existence. The Vucetich system was adopted not only in Brazil, but also by most of the other South American countries. The oldest and most traditional ID Institute in Brazil (Instituto de Identificação Félix Pacheco) was integrated at DETRAN (Brazilian equivalent to DMV) into the civil and criminal AFIS system in 1999.

Each state in Brazil is allowed to print its own ID card, but the layout and data are the same for all of them. The ID cards printed in Rio de Janeiro are fully digitized using a 2D bar code with information which can be matched against its owner off-line. The 2D bar code encodes a color photo, a signature, two fingerprints, and other citizen data. This technology was developed in 2000 in order to enhance the safety of the Brazilian ID cards.

By the end of 2005, the Brazilian government started the development of its new passport. The new documents are released by the beginning of 2007, at Brasilia-DC. The new passport included several security features, like Laser perforation, UV hidden symbols, security layer over variable data and etc.. Brazilian citizens will have their signature, photo, and 10 rolled fingerprints collected during passport requests. All of the data is planned to be stored in ICAO E-passport standard. This allows for contactless electronic reading of the passport content and Citizens ID verification since fingerprint templates and token facial images will be available for automatic recognition.

10.3 Germany

The biometrics market in Germany will experience enormous growth until 2009. “The market size will increase from approximately 12 million € (2004) to 377 million €” (2009). “The federal government will be a major contributor to this development”. In particular, the biometric procedures of fingerprint and facial recognition can profit from the government project. In May 2005 the German Upper House of Parliament approved the implementation of the ePass, a passport issued to all German citizens which contain biometric technology. The ePass has been in circulation since November 2005, and contains a chip that holds a digital photograph and one fingerprint from each hand, usually of the index fingers, though others may be used if these fingers are missing or have extremely distorted prints. “A third biometric identifier – iris scans – could be added at a later stage”. An increase in the prevalence of biometric technology in Germany is an effort to not only keep citizens safe within German borders but also to comply with the current US deadline for visa-waiver countries to introduce biometric passports. In addition to producing biometric passports for German citizens, the German government has put in place new requirements for visitors to apply for visas within the country. “Only applicants for long-term visas, which allow more than three months' residence, will be affected by the planned biometric registration program. The new work visas will also include fingerprinting, iris scanning, and digital photos”.

Germany is also one of the first countries to implement biometric technology at the Olympic Games to protect German athletes. “The Olympic Games is always a diplomatically tense affair and previous events have been rocked by terrorist attacks - most notably when Germany last held the Games in Munich in 1972 and 11 Israeli athletes were killed”.

Biometric technology was first used at the Olympic Summer Games in Athens, Greece in 2004. “On registering with the scheme, accredited visitors will receive an ID card containing their fingerprint biometrics data that will enable them to access the 'German House'. Accredited visitors will include athletes, coaching staff, team management and members of the media”.

As a protest against the increasing use of biometric data, the influential hacker group Chaos Computer Club published a fingerprint of German Minister of Interior Wolfgang Schauble in

the March 2008 edition of its magazine *Datenschleuder*. The magazine also included the fingerprint on a film that readers could use to fool fingerprint readers.

10.4 Iraq

Biometrics are being used extensively in Iraq to catalogue as many Iraqis as possible providing Iraqis with a verifiable identification card, immune to forgery. During account creation, the collected biometrics information is logged into a central database which then allows a user profile to be created. Even if an Iraqi has lost their ID card, their identification can be found and verified by using their unique biometric information. Additional information can also be added to each account record, such as individual personal history. This can help American forces determine whether someone has been causing trouble in the past. One major system in use in Iraq is called BISA. This system uses a smartcard and a user's biometrics (fingerpint, iris, and face photos) to ensure they are authorized access to a base or facility. Another is called BAT for Biometric Automated Tool.

10.5 Israel

Biometrics have been used extensively in Israel for several years.

The border crossing points from Israel to the Gaza Strip and West Bank are controlled by gates through which authorized Palestinians may pass. Thousands of Palestinians (upwards of 90,000) pass through the turnstiles every day to work in Israel, and each of them has an ID card which has been issued by the Israeli Military at the registration centers. At peak periods more than 15,000 people an hour pass through the gates. The ID card is a smartcard with stored biometrics of fingerprints, facial geometry and hand geometry. In addition there is a photograph printed on the card and a digital version stored on the smartcard chip.

Tel Aviv Ben Gurion Airport has a frequent flyer's fast check-in system which is based on the use of a smartcard which holds information relating to the holders hand geometry and fingerprints. For a traveller to pass through the fast path using the smartcard system takes less than 10 seconds.

The Immigration Police at Tel Aviv Airport use a system of registration for foreign workers that utilizes fingerprint, photograph and facial geometry which is stored against the Passport details of the individual. There is a mobile version of this which allows the police to check on an individual's credentials at any time.

10.6 Japan

Several banks in Japan have adopted either palm vein authentication or finger vein authentication technology on their ATMs. Palm vein authentication technology which was developed by Fujitsu, among other companies, proved to have a false acceptance rate of 0.01177% and a false rejection rate of 4.23%. Finger vein authentication technology, developed by Hitachi, has a false acceptance rate of 0.0100% and a false rejection rate of 1.26%. Finger vein authentication technology has so far been adopted by banks such asSumitomo Mitsui Financial Group, MizuhoFinancial Group and Japan Post Bank. Palm vein authentication technology has been adopted by banks such as theBank of Toky0-MitsubishiUFJ.

10.7 United States

The United States government has become a strong advocate of biometrics with the increase in security concerns in recent years, since September 11, 2001. Starting in 2005, US passports with facial (image-based) biometric data were scheduled to be produced. Privacy activists in many countries have criticized the technology's use for the potential harm to civil liberties, privacy, and the risk of identity theft. Currently, there is some apprehension in the United States (and the European Union) that the information can be "skimmed" and identify people's citizenship remotely for criminal intent, such as kidnapping. There also are technical difficulties currently delaying biometric integration into passports in the United States, the United Kingdom, and the rest of the EU. These difficulties include compatibility of reading devices, information formatting, and nature of content (e.g. the US currently expect to use only image data, whereas the EU intends to use fingerprint and image data in their passport RFID biometric chip(s)).

The speech made by President Bush on May 15, 2006, live from the Oval Office, was very clear: from now on, anyone willing to go legally in the United States in order to work there

will be card-indexed and will have to communicate his fingerprints while entering the country.

"A key part of that system [for verifying documents and work eligibility of aliens] should be a new identification card for every legal foreign worker. This card should use biometric technology, such as digital fingerprints, to make it tamper-proof." President George W Bush (Addresses on Immigration Reform, May 15, 2006). Bush issued a presidential directive (NSPD 59, HSPD 24) in 2008 which requires increased capability for sharing and interoperability in "collection, storage, use, analysis, and sharing of biometric and associated biographic and contextual information of individuals" among the departments and agencies of the executive branch of the U.S.federal government. The US Department of Defense (DoD) Common Access Card, is an ID card issued to all US Service personnel and contractors on US Military sites. This card contains biometric data and digitized photographs. It also has laser-etched photographs and holograms to add security and reduce the risk of falsification. There have been over 10 million of these cards issued.

According to Jim Wayman, director of the National Biometric Test Center at San Jose State, Walt Disney World is the nation's largest single commercial application of biometrics. However, the US Visit program will very soon surpass Walt Disney World for biometrics deployment.

On February 6, 2008, West Virginia University, in Morgantown, West Virginia, became the national academic leader for the FBI's biometric research. The university was the first in the world to establish a Bachelor of Science Degree in Biometric Systems, and also established the initial chapter of the Student Society for the Advancement of Biometrics (SSAB) in 2003.WVU also offers a graduate level certificate and Master’s degree emphasis in Biometrics.

11. The Future of Biometrics

Biometrics can do a lot more than just determine whether someone has access to walk through a particular door. Some hospitals use biometric systems to make sure mothers take home the right newborns. Experts have also advised people to scan their vital documents, like birth certificates and social security cards, and store them in biometrically-secured flash

memory in the event of a national emergency. Here are some biometric technologies you might see in the future:

- New methods that use DNA, nail bed structure, teeth, ear shapes, body odor, skin patterns and blood pulses
- More accurate home-use systems
- Opt-in club memberships, frequent buyer programs and rapid checkout systems with biometric security

More prevalent biometric systems in place of passports at border crossings and airports.

REFERENCES :

www.google.com

www.wikipedia.org

www.studymafia.org