International Journal of u- and e- Service, Science and Technology
Vol. 2, No. 3, September, 2009

Biometric Authentication: A Review

Debnath Bhattacharyya[1], Rahul Ranjan[1], Farkhod Alisherov A.[2], and Minkyu Choi[3]

[1]Computer Science and Engineering Department
Heritage Institute of Technology, Kolkata-700107, India
[2]Hannam University, Daejeon-306791, Korea
{debnathb,rahul.sadbahar}@gmail.com[1], sntdvl@yahoo.com[2],
freeant07@naver.com[3]

Abstract

Advances in the field of Information Technology also make Information Security an inseparable part of it. In order to deal with security, Authentication plays an important role. This paper presents a review on the biometric authentication techniques and some future possibilities in this field. In biometrics, a human being needs to be identified based on some characteristic physiological parameters. A wide variety of systems require reliable personal recognition schemes to either confirm or determine the identity of an individual requesting their services. The purpose of such schemes is to ensure that the rendered services are accessed only by a legitimate user, and not anyone else. By using biometrics it is possible to confirm or establish an individual's identity. The position of biometrics in the current field of Security has been depicted in this work. We have also outlined opinions about the usability of biometric authentication systems, comparison between different techniques and their advantages and disadvantages in this paper.

Keywords: *biometric, pattern, IRIS, authentication.*

1. Introduction

Information security is concerned with the assurance of confidentiality, integrity and availability of information in all forms. There are many tools and techniques that can support the management of information security. But system based on biometric has evolved to support some aspects of information security. Biometric authentication supports the facet of identification, authentication and non-repudiation in information security.

Biometric authentication has grown in popularity as a way to provide personal identification. Person's identification is crucially significant in many application and the hike in credit card fraud and identity theft in recent years indicate that this is an issue of major concern in wider society. Individual passwords, pin identification or even token based arrangement all have deficiencies that restrict their applicability in a widely-networked society. Biometric is used to identify the identity of an 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 and 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. So, the advantage claimed by biometric authentication is that they can establish an unbreakable one-to-one correspondence between an individual and a piece of data.

In this paper, we present a detail survey on Biometric Authentication and we hope that this work will definitely provide a concrete overview on the past, present and future aspects in this field.

2. Overview

Biometrics (ancient Greek: bios ="life", metron ="measure") refers to two very different fields of study and application. The first, which is the older and is used in biological studies, including forestry, is the collection, synthesis, analysis and management of quantitative data on biological communities such as forests. Biometrics in reference to biological sciences has been studied and applied for several generations and is somewhat simply viewed as "biological statistics" [1].

Authentication is the act of establishing or confirming something (or someone) as authentic, that is, that claims made by or about the thing are true. A short overview in this field can be divided into three parts and they are Past, Present and Future.

2.1. Past

European explorer Joao de Barros recorded the first known example of fingerprinting, which is a form of biometrics, in China during the 14th century. Chinese merchants used ink to take children's fingerprints for identification purposes.

In 1890, Alphonse Bertillon studied body mechanics and measurements to help in identifying criminals. The police used his method, the Bertillonage method, until it falsely identified some subjects. The Bertillonage method was quickly abandoned in favor of fingerprinting, brought back into use by Richard Edward Henry of Scotland Yard.

Karl Pearson, an applied mathematician studied biometric research early in the 20th century at University College of London. He made important discoveries in the field of biometrics through studying statistical history and correlation, which he applied to animal evolution. His historical work included the method of moments, the Pearson system of curves, correlation and the chi-squared test.

In the 1960s and '70s, signature biometric authentication procedures were developed, but the biometric field remained fixed until the military and security agencies researched and developed biometric technology beyond fingerprinting.

2.2. Present

Biometrics authentication is a growing and controversial field in which civil liberties groups express concern over privacy and identity issues. Today, biometric laws and regulations are in process and biometric industry standards are being tested. Face recognition biometrics has not reached the prevalent level of fingerprinting, but with constant technological pushes and with the threat of terrorism, researchers and biometric developers will stimulate this security technology for the twenty-first century. In modern approach, Biometric characteristics can be divided in two main classes:

a. Physiological are related to the shape of the body and thus it varies from person to person Fingerprints, Face recognition, hand geometry and iris recognition are some examples of this type of Biometric.
b. Behavioral are related to the behavior of a person. Some examples in this case are signature, keystroke dynamics and of voice . Sometimes voice is also considered to be a physiological biometric as it varies from person to person.

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.

2.3. Future

A biometric system can provide two functions. One of which is verification and the other one is Authentication. So, the techniques used for biometric authentication has to be stringent enough that they can employ both these functionalities simultaneously. 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. Other biometric strategies are being developed such as those based on gait (way of walking), retina, Hand veins, ear canal, facial thermogram, DNA, odor and scent and palm prints. In the near future, these biometric techniques can be the solution for the current threats in world of information security.

Of late after a thorough research it can be concluded that approaches made for simultaneous authentication and verification is most promising for iris, finger print and palm vain policies. But whatever the method we choose, main constraint will be its performance in real life situation. So, application of Artificial System can be a solution for these cases. We have given emphasis on the Iris recognition. According to us, after detection of an iris pattern, the distance between pupil and the iris boundary can be computed. This metric can be used for the recognition purposes because this feature remains unique for each and every individual. Again, an artificial system can be designed which will update the stored metric as the proposed feature may vary for a particular person after certain time period.

After doing the manual analysis of the above discussed method, we have got a satisfactory result. Due to the dynamic modification of the proposed metric, the rejection ration for a same person reduces by a lot. The work is being carried out to make the system viable.

3. Detail, Techniques and Technologies

We have already stated that there exist two kind of biometric characteristics. So, techniques for biometric authentication have been developed based on these characteristics. Details of different techniques are discussed below.

3.1. Finger Print Technology

A fingerprint is an impression of the friction ridges of all or any part of the finger. A friction ridge is a raised portion of the on the palmar (palm) or digits (fingers and toes) or plantar (sole) skin, consisting of one or more connected ridge units of friction ridge skin. These ridges are sometimes known as "dermal ridges" or "dermal ". The traditional method uses the ink to get the finger print onto a piece of paper. This piece of paper is then scanned using a traditional scanner. Now in modern approach, live finger print readers are used .These are based on optical, thermal, silicon or ultrasonic principles [22, 23, 27]. It is the oldest of all the biometric techniques. Optical finger print reader is the most common at present. They are based on reflection changes at the spots where finger papilar lines touch the reader surface. All the optical fingerprint readers comprise of the source of light, the light sensor and a special reflection surface that changes the reflection according to the pressure. Some of the readers are fitted out with the processing and memory chips as well.

The finger print obtained from an Optical Fingerprint Reader is shown in figure 1.

Figure 1. Fingerprint Bitmap.

The size of optical finger is around 10*10*15. It is difficult to minimize them much more as the reader has to comprise the source on light reflection surface and light sensor.

Optical Silicon Fingerprint Sensor is based on the capacitance of finger. Dc-capacitive finger print sensor consists of rectangular arrays of capacitors on a silicon chip. One plate of the capacitors is finger, other plate contains a tiny area of metallization on the chips surfaces on placing finger against the surfaces of a chip, the ridges of finger print are close to the nearby pixels and have high capacitance to them. The valleys are more distant from the pixels nearest them and therefore have lower capacitance.

Ultrasound finger print is newest and least common. They use ultrasound to monitor the figure surfaces, the user places the finger on a piece of glass and the ultrasonic sensor moves and reads whole finger print. This process takes 1 or 2 seconds.

Finger print matching techniques can be placed into two categories. One of them is Minutiae based and the other one is Correlation based. Minutiae based techniques find the minutiae points first and then map their relation placement on the finger. Correlation based techniques require the precise location of a registration point and are affected by image translation and rotation [2, 3, 19, 24].

3.2. Face Recognition Technology

A facial recognition technique is an application of computer for automatically identifying or verifying a person from a digital image or a video frame from a video source. It is the most natural means of biometric identification [6].

Facial recognition technologies have recently developed into two areas and they are Facial metric and Eigen faces.

Facial metric technology relies on the manufacture of the specific facial features (the system usually look for the positioning of eyes, nose and mouth and distances between these features), shown in figure 2 and 3.

Figure 2. Recognition of face from Body.

The face region is rescaled to a fixed pre-defined size (e.g. 150-100 points). This normalized face image is called the canonical image. Then the facial metrics are computed and stored in a face template. The typical size of such a template is between 3 and 5 KB, but

there exist systems with the size of the template as small as 96 bytes. The figure for the normalized face is given below.

Figure 3. Normalized Face.

The Eigen Face method (figure 4) is based on categorizing faces according to the degree of it with a fixed set of 100 to 150 eigen faces. The eigen faces that are created will appear as light and dark areas that are arranged in a specific pattern. This pattern shows how different features of a face are singled out. It has to be evaluated and scored. There will be a pattern to evaluate symmetry, if there is any style of facial hair, where the hairline is, or evaluate the size of the nose or mouth. Other eigen faces have patterns that are less simple to identify, and the image of the eigen face may look very little like a face. This technique is in fact similar to the police method of creating a portrait, but the image processing is automated and based on a real picture. Every face is assigned a degree of fit to each of 150 eigen faces, only the 40 template eigen faces with the highest degree of fit are necessary to reconstruct the face with the accuracy of 99 percent. The whole thing is done using Face Recognition softwares [24, 25, 32, 39].

Figure 4. Eigen Face.

3.3. IRIS Technology

This recognition method uses the iris of the eye which is colored area that surrounds the pupil. Iris patterns are unique and are obtained through video based image acquisition system. Each iris structure is featuring a complex pattern. This can be a combination of specific characteristics known as corona, crypts, filaments, freckles, pits, furrows, striations and rings [7]. An IRIS Image shown in figure 5.

Figure 5. Image of IRIS.

The iris pattern is taken by a special gray scale camera in the distance of 10- 40 cm of camera. 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 iris code. Here, two influences have to take into account. First, the overall darkness of image is influenced by the lighting condition 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. Secondly, the size of the iris changes as the size of the pupil changes. Before computing the iris code, a proper transformation must be done.

In decision process, the matching software takes two iris codes and compute the hamming distance based on the number of different bits. The hamming distances score (within the range 0 means the same iris codes), which is then compared with the security threshold to make the final decision. Computing the hamming distance of two iris codes is very fast (it is the fact only counting the number of bits in the exclusive OR of two iris codes). We can also implement the concept of template matching in this technique. In template matching, some statistical calculation is done between a stored iris template and a produced. Depending on the result decision is taken [27, 30, 34].

3.4. Hand Geometry Technology

It 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. These techniques include the estimation of length, width, thickness and surface area of the hand. Various method are used to measure the hands- Mechanical or optical principle [8, 20].

Figure 6. Hand Geometry Scanner.

There are two sub-categories of optical scanners. Devices from 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 processed by the computer software. Only 2D-

chararcteristics of hand can be used in this case. Hand geometry systems from other category are more complicated. They use special guide marking to portion the hand better and have two (both vertical and horizontal) sensors for the hand shape measurements. So, sensors from this category handle data of all 3D features [5, 24, 33]. Figure 6 and 7 shows the hand geometry system.

Some of hand geometry scanners produce only the video signal with the hand shape. Image digitalization and processing is then done in the computer to process those signals in order to obtain required video or image of the hand [14, 30].

Figure 7. Acquired Image of Hand.

3.5. Retina Geometry Technology

It is based on the blood vessel pattern in the retina of the eye as the blood vessels at the back of the eye have a unique pattern, from eye to eye and person to person (figure 8).

Retina is not directly visible and so a coherent infrared light source is necessary to illuminate the retina. The infrared energy is absorbed faster by blood vessels in the retina than by the surrounding tissue. The image of the retina blood vessel pattern is then analyzed.

Figure 8. Image of Retina.

Retina scans require that the person removes their glasses, place their eye close to the scanner, stare at a specific point, and remain still, and focus on a specified location for approximately 10 to 15 seconds while the scan is completed. A retinal scan involves the use of a low-intensity coherent light source, which is projected onto the retina to illuminate the blood vessels which are then photographed and analyzed. A coupler is used to read the blood vessel patterns. A retina scan cannot be faked as it is currently impossible to forge a human retina. Furthermore, the retina of a deceased person decays too rapidly to be used to deceive a retinal scan. A retinal scan has an error rate of 1 in 10,000,000, compared to fingerprint identification error being sometimes as high as 1 in 500 [9, 30].

3.6. Speaker Recognition Technique

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

Speaker verification focuses on the vocal characteristics that produce speech and not on the sound or the pronunciation of speech itself. The vocal characteristics depend on the dimensions of the vocal tract, mouth, nasal cavities and the other speech processing mechanism of the human body. It doesn't require any special and expensive hardware.

Speaker recognition uses the acoustic features of speech that have been found to differ between individuals. These acoustic patterns reflect both anatomy (e.g. size and shape of the throat and mouth) and learned behavioral patterns.(e.g. voice pitch, speaking style) [10, 31].

Speaker recognition system employs three styles of spoken input and they are listed below.

(a) Text dependent (b) Text prompted (c) Text independent

Text dependent involves selection and enrollment of one or more voice passwords.

Text prompted is used whenever there is concern of imposters. Various technologies used to process and store voice prints include hidden Markov models, pattern matching algorithms, neural networks, metric representation and decision tree.

Some technology also uses "anti maker" techniques, such as cohort models, and world models.

Voice changes due to aging also need to be addressed by recognition Systems. Capture of the biometric is seen as non-invasive. The technology needs additional hardware by using existing microphones and voice transmission technology allowing recognition over long distances via ordinary telephones (wire line or wishes) [4, 37].

3.7. Signature Verification Technique

The signature dynamics recognition is based on the dynamics of making the signature, rather than a direct comparison of the signature itself afterwards. The dynamics is measured as a means of the pressure, direction, acceleration and the length of the strokes, dynamics number of strokes and their duration. The most obvious and important advantage of this is that a fraudster cannot glean any information on how to write the signature by simply looking at one that has been previously written. There are various kinds of devices used to capture the signature dynamics. These are either traditional tablets or special purpose devices. Tablets capture 2D coordinates and the pressure [11, 21], figure 9.

Figure 9. A Signature taken using Tablet.

Special pens are able to capture movements in all three dimensions. Tablets have two significant disadvantages. First, the resulting digitalized signature looks different from the usual user signature. Secondly, while signing the user does not see what he or she has already written. He/she has to look at the computer monitor to see the signature [4, 37].

This is a considerable drawback for many (inexperienced) users. Some special pens work like normal pens, they have ink cartridge inside and can be used to write with them on paper.

3.8. Other Techniques

Some other available techniques for biometric authentication are described below.

3.8.1. Palmprint: Palmprint verification is a slightly different implementation of the fingerprint technology. Palmprint scanning uses optical readers that are very similar to those used for fingerprint scanning, their size is, however, much bigger and this is a limiting factor for the use in workstations or mobile devices [40, 15].

3.8.2. Hand Vein: Hand vein geometry is based on the fact that the vein pattern is distinctive for various individuals. The veins under the skin absorb infrared light and thus have a darker pattern on the image of the hand taken by an infrared camera. The hand vein geometry is still in the stage of research and development. One such system is manufactured by British Technology Group. The device is called Veincheck and uses a template with the size of 50 bytes [4, 13, 20].

3.8.3. DNA: DNA sampling is rather intrusive at present and requires a form of tissue, blood or other bodily sample. This method of capture still has to be refined. So far the DNA analysis has not been sufficiently automatic to rank the DNA analysis as a biometric technology. The analysis of human DNA is now possible within 10 minutes. As soon as the technology advances so that DNA can be matched automatically in real time, it may become more significant. At present Biometric Systems DNA is very entrenched in crime detection and so will remain in the law enforcement area for the time being [2, 4, 16].

3.8.4. Thermal Imaging: This technology is similar to the hand vein geometry. It also uses an infrared source of light and camera to produce an image of the vein pattern in the face or in the wrist [17].

3.8.5. Ear Shape: Identifying individuals by the ear shape is used in law enforcement applications where ear markings are found at crime scenes. Whether this technology will progress to access control applications is yet to be seen. An ear shape verifier (Optophone) is produced by a French company ART Techniques. It is a telephone type handset within which is a lighting unit and cameras which capture two images of the ear [4, 18].

3.8.6. Body Odor: The body odor biometrics is based on the fact that virtually each human smell is unique. The smell is captured by sensors that are capable to obtain the odor from non-intrusive parts of the body such as the back of the hand. Methods of capturing a person's smell are being explored by Mastiff Electronic Systems. Each human smell is made up of chemicals known as volatiles. They are extracted by the system and converted into a template. The use of body odor sensors brings up the privacy issue as the body odor carries a significant amount of sensitive personal information. It is possible to diagnose some diseases or activities in the last hours (like sex, for example) by analyzing the body odor [4, 38].

3.8.7. Keystroke Dynamics: Keystroke dynamics is a method of verifying the identity of an individual by their typing rhythm which can cope with trained typists as well as the amateur two-finger typist. Systems can verify the user at the log-on stage or they can continually monitor the Biometric Systems 32 typist. These systems should be cheap to install as all that is needed is a software package [12, 35].

3.8.8. Fingernail Bed: The US Company AIMS is developing a system which scans the dermal structure under the fingernail. This tongue and groove structure is made up of nearly

parallel rows of vascular rich skin. Between these parallel dermal structures are narrow channels and it is the distance between these which is measured by the AIMS system [30].

4. Applications

Biometric authentication is highly reliable, because physical human characteristics are much more difficult to forge then security codes ,passwords ,hardware keys sensors ,fast processing equipment and substantial memory capacity , so the system are costly. Biometric-based authentication applications include workstation and network access, single sign-on, application logon, data protection, remote access to resources, transaction security, and Web security. The promises of e-commerce and e-government can be achieved through the utilization of strong personal authentication procedures.

Secure electronic banking, investing and other financial transactions, retail sales, law enforcement, and health and social services are already benefiting from these technologies. Biometric technologies are expected to play a key role in personal authentication for large-scale enterprise network authentication environments, Point-of-Sale and for the protection of all types of digital content such as in Digital Rights Management and Health Care applications. Utilized alone or integrated with other technologies such as smart cards, encryption keys and digital signatures, biometrics is anticipated to pervade nearly all aspects of the economy and our daily lives. For example, biometrics is used in various schools such as in lunch programs in Pennsylvania, and a school library in Minnesota. Examples of other current applications include verification of annual pass holders in an amusement park, speaker verification for television home shopping, Internet banking, and users' authentication in a variety of social services [4].

5. Evaluation

When it is time to use the biometric authentication, the degree of security is concerned. In this paper, we have discussed the various types of biometric authentication techniques. In this section, we will evaluate different techniques and find degree of security.

There are various parameters with the help of which we can measure the performance of any biometric authentication techniques. These factors are described below [28, 29, 30]. Table 1 shows the evaluated vales of various evaluation techniques.

5.1. Factors of Evaluation

5.1.1. False Accept Rate (FAR) and False Match Rate (MAR): 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.

5.1.2. False Reject Rate (FRR) or False Non-Match Rate (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.

5.1.3. 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 Tradeoff (DET), which is obtained using normal deviate scales on both axes. This more linear graph illuminates the differences for higher performances (rarer errors) .

5.1.4. 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. 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.

5.1.5. Failure to Enroll Rate (FTE or FER): 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.

5.1.6. Failure to Capture Rate (FTC): Within automatic systems, the probability that the system fails to detect a biometric characteristic when presented correctly is generally treated as FTC.

5.1.7. Template Capacity: It is defined as the maximum number of sets of data which can be input in to the system.

5.2 Results of Evaluation

The evaluations of various techniques using the above parameters are presented in a tabular format.

5.2.1. Finger Print Technology: The finger print bit map obtained from the reader is affected by the finger moisture as the moisture significantly influences the capacitance .This means that too wet or dry fingers do no produce bitmaps with sufficient quality and so people with unusually wet or dry figures have problems with these silicon figure print readers.

5.2.2. Face Recognition Technology: The accuracy of face recognition systems improves with time, but it has not been very satisfying so far. There is need to improve the algorithm for face location.. The current software often doesn't find the face at all or finds "a face" at an incorrect place .This makes result worse. The systems also have problems to distinguish very similar person like twins and any significant change in hair or beard style requires re – enrollment .glasses also causes additional difficulties .It doesn't require any contact with person and cab be fooled with a picture if no countermeasures are active The liveness detection is based most commonly on facial mimics. The user is asked to blink or smile .If the image changes properly then the person is considered "live".

5.2.3. Iris Technology: The artificial duplication of the iris is virtually impossible because of 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 the death. It should be therefore very difficult to create an artificial iris to fraudulently bypass the biometric systems if the detection of the iris liveness is working properly.

Table 1. Evaluation of Biometric Techniques

Biometric	EER	FAR	FRR	Subjects	Comments
face	NA	1%	10%	37437	varied light, indoor /outdoor
finger print	2%	2%	2%	25000	rotation and exaggerated skin distortion
hand geometry	1%	2%	2%	129	with rings and improper placement
iris	.01%	.94%	.99%	1224	indoor environment
keystrokes	1.8%	7%	.1%	15	during 6 months period
voice	6%	2%	10%	30	text dependent and multilingual

5.2.4. Hand Geometry Technique: Its condition to be used is hand must be placed accurately, guide marking have been incorporated and 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. Hand geometry doesn't produce a large data set. Therefore, give a large no. of records, hand geometry may not be able to distinguish sufficiently one individual from another. The size of hand template is often as small as 9 bytes. Such systems are not suitable for identification at all. It shows lower level security application.

5.2.5. Retina Geometry: The main drawbacks of the retina scan are its intrusiveness. The method of obtaining a retina scan is personally invasive. A laser light must be directed through the cornea of edge. Also the operation of retina scanner is not easy. A skilled operator is required and the person being scanned has to follow his or her direction. However, retina scanning systems are said to be accurate, It is used where high security is concerned.

5.2.6. Speaker Recognition Technique (voice): The greatest advantage of speaker verification systems is that they do not require any special and expensive hardware .It can also be used remotely via phone line. A high sampling rate is not required, but the background noise causes a significant problem that decreases the accuracy. It is based on behavioral characteristics and as such can be negatively affected by the current physical condition and the emotion state.

5.2.7. Signature Verification Technique: Person does not make a signature consistently the same way. So, the data obtained from a signature of a person has to allow for quite some variability. Most of the signature dynamics systems verify the dynamics only. They do not pay any attention to the resulting signature. A few systems claim to verify both (i.e. the signature dynamics as well as the resulting signature look itself). Our experience shows that if the system does not verify the resulting dynamics vs. signature, then the signature that is accepted as a true match may look significantly different from the master template. The speed of writing is often the most important factor in the decision process, so it is possible to successfully forge a signature even if the resulting signature looks so different that any person would notice. The size of data obtained during the signing process is around 20 KB. The size of the master template, which is computed from 3 to 10 signatures, varies from around 90 bytes up to a few kilobytes. If the size of the master template is relatively high the signature recognition has problems with match discrimination and thus is suitable for verification only. The accuracy of the signature dynamics biometric systems is not high, the crossover rate

published by manufacturers is around 2%, but according to our own experience the accuracy is much worse.

6. Discussion

Biometric authentication is highly reliable, because physical human characteristics are much more difficult to forge then security codes, passwords and hardware keys.

Tokens such as smart card, magnetic stripe cards, ID cards, physical keys, can be lost, stolen, duplicated or left at home. Password can be forgotten, shared or observed. Moreover, today's fast-paced electronic world means people are asked to remember a multitude of passwords and Personal Identification Number (PINs) for computer accounts, banks, ATMs, E-Mail, wireless, phones ,websites and so forth. Biometrics holds the promise of fast, easy, accurate, reliable and less expensive authentication for a variety of application.

When Biometric system is networked together with telecommunication technology, biometric systems become Tele-biometric systems. The main operations are enrollment and test.

7. Conclusion

While biometric authentication can offer a high degree of security, they are far from perfect solution. Sound principles of system engineering are still required to ensure a high level of security rather than the assurance of security coming simply from the inclusion of biometrics in some form.

The risks of compromise of distributed database of biometrics used in security application are high- particularly where the privacy of individuals and hence non-repudiation and irrevocability are concerned. It is possible to remove the need for such distributed databases through the careful application of biometric infrastructure without compromising security.

The influences of biometric technology on society and the risks to privacy and threat to identify will require mediation through legislation. For much of the short history of biometrics the technology developments have been in advance of ethical or legal ones. Careful consideration of the importance of biometrics data and how it should be legally protected is now required on a wider scale.

Acknowledgement

This work was supported by the Security Engineering Research Center, granted by the Korea Ministry of Knowledge Economy.

References

[1] Smart Cart Alliance Identity Council (2007): Identity and Smart Card Technology and Application Glossary, http://www.smartcardalliance.org, as visited on 25/10/2008.

[2] Jain, A. K.; Ross, A. & Pankanti, S., "Biometrics: A Tool for Information Security", IEEE Transactions on Information Forensics And Security, Volume 1, issue 2, Jun. 2006, pp 125 – 144.

[3] R. Cappelli, D. Maio, D. Maltoni, J. L. Wayman, and A. K. Jain, "Performance evaluation of fingerprint verification systems", IEEE Trans. Pattern Anal. Mach. Intell., Volume 28, issue 1, Jan. 2006, pp. 3–18.

[4] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," IEEE Trans. Circuits Syst. Video Technology, Special Issue Image- and Video-Based Biomet., Volume 14, Issue 1, Jan. 2004, pp. 4–20.

[5] R. Sanchez-Reillo, C. Sanchez-Avila, and A. Gonzales-Marcos, "Biometric identification through hand geometry measurements,", IEEE Trans. Pattern Anal. Mach. Intell., Volume 22, Issue. 10, Oct. 2000, pp. 1168–1171.

[6] M. A. Dabbah, W. L. Woo, and S. S. Dlay, "Secure Authentication for Face Recognition," In Proc. of IEEE Symposium on Computational Intelligence in Image and Signal Processing, Apr. 2007. USA, pp. 121 - 126.

[7] Sanjay R. Ganorkar, Ashok A. Ghatol, “Iris Recognition: An Emerging Biometric Technology”, In Proc. of the 6th WSEAS International Conference on Signal Processing, Robotics and Automation, Greece, Feb. 2007, pp. 91 – 96.

[8] E. Kukula, S. Elliott, “Implementation of Hand Geometry at Purdue University's Recreational Center: An Analysis of User Perspectives and System Performance”, In Proc. of 35th Annual International Carnahan Conference on Security Technology, UK, Oct. 2001, pp. 83 – 88.

[9] C. Marin˜ o Æ M. G. Penedo Æ M. Penas Æ M. J. Carreira F. Gonzalez, “Personal authentication using digital retinal images”, Journal of Pattern Analysis and Application, Springer, Volume 9, Issue 1, May. 2006, pp. 21–33.

[10] Kar, B. Kartik, B. Dutta, P.K. “Speech and Face Biometric for Person Authentication”, In Proc. of IEEE International Conference on Industrial Technology, India, Dec.2006, pp. 391 - 396.

[11] Samir K. Bandopadhaya, Debnath Bhattacharyya, Swarnendu Mukherjee, Debashis Ganguly, Poulumi Das, “Statistical Approach for Offline Handwritten Signature Verification”, Journal of Computer Science, Science Publication, Volume 4, Issues 3, May. 2008, pp. 181 – 185.

[12] S. Hocquet, J. Ramel, H. Cardot, “Fusion of Methods for Keystroke Dynamic Authentication”, In Proc. of 4th IEEE Workshop on Automatic Identification Advanced Technologies, USA, Oct. 2005, pp. 224 – 229.

[13] S. Im, H. Park, Y. Kim, S. Han, S. Kim, C. Kang, and C. Chung, “A Biometric Identification System by Extracting Hand Vein Patterns”, Journal of the Korean Physical Society, Korean Publication, Volume 38, Issue 3, Mar. 2001, pp. 268-272.

[14] R. Sanchez-Reillo, C. Sanchez-Avilla, and A. Gonzalez-Macros, “Biometrics Identification Through Hand Geometry Measurements”, IEEE Transactions on Pattern Anakysis and Machine Intelligence, Volume 22, Issue 18, Oct. 2000, pp. 1168-1171.

[15] Zhang, D.; Wai-Kin Kong; You, J.; Wong, M, “Online palmprint identification”, IEEE Transactions on Pattern Analysis and Machine Intelligence, Volume 25, Issue 9, Sep. 2003, pp. 1041 – 1050.

[16] Alfred C. Weaver, “Biometric Authentication”, IEEE Computer Society, Feb. 2006, Volume 39, No. 2, pp. 96-97.

[17] C. Lin and K. Fan, “Biometric Verification Using Thermal Images of Palm-Dorsa Vein Patterns”, IEEE Transactions on Circuits and systems for Video Technology Volume 14, No. 2, Feb. 2004, pp. 191- 213 .

[18] Hui Chen, Bhanu, B, “Shape Model-Based 3D Ear Detection from Side Face Range Images”, In Proc. of IEEE Computer Society Conference on Computer Vision and Pattern Recognition, USA, Jun. 2005, pp. 122 – 122.

[19] A. K. Jain, L. Hong, and R. Bolle, “On-line fingerprint verification”, IEEE Transactions on Pattern Recognition and Machine Intelligence, Volume 19, No. 4, Aug. 1996, pp. 302–314.

[20] A. Kumar, D. C. Wong, H. C. Shen, and A. K. Jain, “Personal Verification using Palmprint and Hand Geometry Biometric”, In Proc. of 4th International Conference on Audio- and Video-based Biometric Person Authentication, Guildford, UK, Jun. 2003, pp. 668 - 678.

[21] J. L. Wayman, “Fundamentals of Biometric Authentication Technologies”, International Journal of Image and Graphics, World Scientific Publication, Volume 1, No. 1, Jan. 2001, pp. 93-113.

[22] A. Ross, S. Dass, and A. K. Jain, “A deformable model for fingerprint matching”, Journal of Pattern Recognition, Elsevier, Volume 38, No. 1, Jan. 2005, pp. 95–103.

[23] T. Matsumoto, H. Hoshino, K. Yamada, and S. Hasino, “Impact of artificial gummy fingers on fingerprint systems”, In Proc. of SPIE, Volume 4677, Feb. 2002, pp. 275–289.

[24] L. Hong and A. K. Jain, “Integrating faces and fingerprints for personal identification”, IEEE Trans. Pattern Anal. Mach. Intell., Volume 20, No. 12, Dec. 1998, pp. 1295–1307.

[25] A. Ross and R. Govindarajan, “Feature level fusion using hand and face biometrics”, In Proc. of SPIE Conf. Biometric Technology for Human Identification II, Mar. 2005, pp. 196–204.

[26] Abiyev, R.H. Altunkaya, K., “Neural Network Based Biometric Personal Identification”, Frontiers in the Convergence of Bioscience and Information Technologies, Jeju, Oct. 2007, pp. 682 – 687.

[27] A. K. Jain, A. Ross, and S. Pankanti, “Biometric: A Tool for Information Security”, IEEE Trans. Information Forensics and Security, Volume 1, No. 2, Jun. 2006, pp. 125–144.

[28] A. K. Jain, S. Pankanti, S. Prabhakar, L. Hong, A. Ross, and J. L. Wayman, “Biometrics: a grand challenge”, In Proc. of International Conference on Pattern Recognition, Cambridge, U.K., Aug. 2004, pp. 935 - 942.

[29] J. Phillips, A. Martin, C. Wilson, and M. Przybocki, “An introduction to evaluating biometric systems”, IEEE Computer Society., Volume 33, No. 2, Feb. 2000, pp. 56–63.

[30] J. L. Wayman, A. K. Jain, D. Maltoni, and D. Maio, Eds., “Biometric Systems: Technology, Design and Performance Evaluation”, New York: Springer Verlag, 2005.

[31] A. Eriksson and P. Wretling, “How flexible is the human voice? A case study of mimicry,” In Proc. of European Conference on Speech Technology, Rhodes, Greece, Sep. 1997, pp. 1043–1046.

[32] S. Z. Li and A. K. Jain, Eds., Handbook of Face Recognition. New York: Springer Verlag, 2004.

[33] R. Sanchez-Reillo, C. Sanchez-Avila, and A. Gonzales-Marcos, “Biometric identification through hand geometry measurements”, IEEE Transaction on Pattern Analysis Machine Intelligence, Volume 22, No. 10, Oct. 2000, pp. 1168–1171,.

[34] J. Daugman, “The importance of being random: statistical principles of iris recognition”, Journal of Pattern Recognition, Elsevier, Volume 36, No. 2, Feb. 2003, pp. 279–291.

[35] F. Monrose and A. Rubin, “Authentication via keystroke dynamics”, In Proc. of 4th ACM Conference on Computer and Communications Security, Switzerland, Apr. 1997, pp. 48–56.

[36] V. S. Nalwa, “Automatic on-line signature verification”, In Proc. of IEEE, Volume 85, No. 2, Feb.1997, pp. 213–239.

[37] S. Furui, "Recent Advances in Speaker Recognition", In Proc. of First International Conference on Audio and Video based Biometric Person Authentication, UK, Mar. 1997, pp. 859-872.

[38] Z. Korotkaya, “Biometric Person Authentication: Odor”, Pages: 1 – 6,

http://www.it.lut.fi/kurssit/03-04/010970000/seminars/Korotkaya.pdf as visited on 10/08/2008

[39] F. Cardinaux, C. Sanderson, and S. Bengio, “User Authentication via Adapted Statistical Models of Face Images”, IEEE Transaction on Signal Processing, Volume 54, Issue 1, Jan. 2006, pp. 361 - 373.

[40] D. Zhang and W. Shu, “Two Novel Characteristic in Palmprint Verification: Datum Point Invariance and Line Feature Matching”, Pattern Recognition, Vol. 32, No. 4, Apr. 1999, pp. 691-702.