Biometric Authentication: A Review

S. R. Kodituwakku
Department of Statistics and Computer Science,
University of Peradeniya, Sri Lanka.

Abstract: Advances in the field of Information Technology make Information Security an inseparable part of life. In order to deal with security, Authentication, access control and auditing play important roles. Among them authentication has become an important first activity to be performed in ensuring security. This paper presents an analysis of the biometric authentication techniques have been proposed and widely used to be performed in ensuring security. This paper also outlined opinions about the usability of biometric authentication systems, comparison between different most widely used techniques and their advantages and disadvantages.

Keywords: biometric, pattern, IRIS, Retina, 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 in managing information security. Among all such systems biometric based systems have evolved to support some aspects of information security. Biometric authentication supports the identification, authentication and non-repudiation.

Biometric authentication has grown in popularity as a way of providing personal identification based on human characteristics. Person’s identification is crucially significant in many applications. For example, the hike in credit card fraud and identity theft in recent years indicates that this is an issue of major concern. Traditional individual passwords and pin identification like techniques have deficiencies that restrict their applicability in wide range of applications. Standard validation systems often use multiple inputs of samples for sufficient validation, such as particular characteristics of the sample. On the other hand biometric authentication can establish an unbreakable one-to-one correspondence between an individual and a piece of data.

In the past, in order to identify the crime and the criminal, fingerprints and portraits detecting procedures were used, but these days a mechanized system is established to do so. Biometric technology can be divided into two general categories as shown in Figure 1.

1. Physiological biometric techniques
2. Behavioral biometric techniques

Behavioral biometric technique has four main sections:

1. Sensor Block: responsible for receiving biometric information
2. Extracting Features Block: it takes the taken information to extract its vector features
3. Comparing Block: responsible for comparing the gained vector with templates
4. Decision Block: this section identifies identity, so either accept or reject identity

![Figure 1: General categories of biometric features](image)

Biometrics science is seeking a way to identify people based on unique features - related to the human body. It is expected that this method be better than previous traditional methods. In practical applications, the performance of system is determined according to the balance of giving the wrong diagnosis (FAR) and the percentage of not giving the wrong diagnosis (FRR). A good biometric identifier that should have the following characteristics:

1. Uniqueness: Each person is unique and has the distinctive features with others.
2. Extracting accountability: the feature could be gained quickly and without the need for high processing for each individual case.
3. High resolution capabilities: the difference between two persons is too different to be easily separable.
4. Sustainability: the extracted features remain unchanged over time and due to changes in a person’s life.

Figure 2 depicts some of the most widely used biometrics.
This paper presents 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 which is useful for the researchers.

Figure 2: Some of the most widely used biometrics

2. OVERVIEW

Biometrics refers to two very different fields of study and application. The first one is the older and is used in biological studies, including forestry, for 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 viewed as "biological statistics". The second one is the newer one used for authentication of humans. Authentication is the act of establishing or confirming something (or someone) as authentic. That is to make sure that claims made by or about the thing are true. Since there are several proposed Biometrics techniques for this purpose a short overview in this field is presented by describing the Past, Present and Future of this field.

A) Past

Joao de Barros recorded the first known example of fingerprinting, which is a form of biometrics, 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 in identifying criminals. The police used his method, the Bertillonage method, until it falsely identified some subjects. Once the Bertillonage method was abandoned fingerprinting idea was brought back into use by Richard Edward Henry. Karl Pearson studied biometric research early in the 20th century at University College of London. His studies in the field of biometrics were applied to animal evolution. This historical work included the method of moments, the Pearson system of curves, correlation and the chi-squared test.

In the 1960s and 1970s, 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.

B) Present

Biometrics authentication is a growing and controversial field in which some people express concern over privacy and identity issues. Today, biometric laws and regulations are in process. Additionally, biometric industry standards are being investigated. Face recognition biometrics has not reached the same level as fingerprinting. However, constant technological advancement and the threat of terrorism lead to stimulate this security technology for the twenty-first century. As a result, this becomes one of the modern approaches for human detection and hence several methods have been proposed and still researches are being carried out.

Biometric characteristics can be divided in two main classes:

1. 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.

2. 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.

A new trend has also been developed that merges human perception to computer database in a brain-machine interface and it is referred 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.

C) Future

A biometric system can provide two functions: verification and Authentication. Therefore, biometric authentication techniques have to be strong enough to perform 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 such as those based on gait (way of walking), retina, Hand veins, ear canal, facial thermogram, DNA, odor and scent and palm prints are also being considered. In the near future, these biometric techniques could be the solution for the increasing threats in world of information security. However, the success of these approaches depends on their performance in real life situations. Artificial systems can also be designed which will update the stored metric as the proposed feature may vary for a particular person after certain time period.

3. BIOMETRIC TECHNIQUES AND TECHNOLOGIES

We have already stated that there exist Two kinds of biometric characteristics have been researched and biometric authentication have been developed based on these characteristics. Details of such techniques are discussed below.

A) Finger Print Technology

Fingerprint identification is the oldest and best-known method of biometric identification for individuals. The important fact is that each person has a different fingerprint. However, the fingerprint identification has been subjected to major changes in recent years. A fingerprint is an impression of the friction ridges of a finger or any part of the finger. A friction ridge is a raised portion of 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 methods use ink to get the finger print onto a piece of paper. This piece of paper is then scanned using a traditional scanner. A sample fingerprint bitmap is shown in Figure 3.

![Figure 3 - Fingerprint Bitmap.](image)

Now live finger print readers based on optical, thermal, silicon or ultrasonic principles [1, 2, 3, 4] are used for this purpose. Optical finger print reader is the most common at present and which has the ability to assess and adapt the fingerprint with recorded samples. They are based on reflection changes at the spots where finger papilar lines touch the reader surface 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 with chips as well.

Fingerprint matching techniques can be categorized into two: Minutiae based and 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 [5, 6, 7, 8].

Fingerprint identification is one of the most common methods of identification. For example, most of the organizations maintain the staff attendance systems using this method. Furthermore, some new laptops have been used this method as a reliable and rapid method. On the other hand, there are some practical problems in fingerprint identification systems. Due to the elasticity of the skin, there may be distortions in the shape and location of the fingerprint. In addition, high reliability and real-time processing are important factors in automatic fingerprint identification. To solve this problem, plug extraction from fingerprint images and its application in fingerprint matching is examined [5, 9].

Fingerprint Classification

Classifications of fingerprint are used in identification systems. The goal is to minimize the search space by partitioning the fingerprint database into smaller parts as possible. In systems that work with low population, a class can be used which fingerprints belonging to a single individual characteristics to determine or verify identity. Setting a classification for fingerprint takes place according to the edges direction around the core as well as the number of the core and delta points. However, later it was found that a fingerprint cannot be attributed to a particular class. Therefore, in any classification system, a class is considered to be "unexpected classification" and such these fingerprints are fall into this category. Fingerprints are divided into five main classifications: Arc, Diagonal arc, Left ring, Right ring and Spiral.

Fingerprint analysis methods

Not all images are fully maintained to minimize the fingerprint data in a database. First, the entire image is analyzed, and then its key points are stored. This action is very important for faster searching of databases. Each fingerprint image has about 35 important features such as cross points, end points, forks and so on which so-called "minutiae". Figure 4 depicts such features.

![Figure 4 - features of the finger](image)
Use of 8 to 22 such features is sufficient to detect and notify any fingerprints with certainty. The fingerprint profile could be stored either directly on the workstation or on a server or on a smart card.

B) Identification using hand geometry

This is based on the fact that every person’s hand is shaped differently and 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 methods are used to measure the hands-Mechanical or optical principle [10, 11]. The identification systems then store these data in a database and it is compared with the input data to identify the person.

Two categories of optical scanners are used to obtain the hand geometry data. The first category creates a black and white bitmap image of the hand’s shape using a source of light and a black and white camera. The bitmap image is processed by the computer software and only the 2D characteristics of hand can be used in this case. The other category is more complicated as they use special guide marking to portion the hand better and have both vertical and horizontal sensors for the hand shape measurements. So, sensors from this category handle data of all 3D features [8, 12, 13]. Figure 5 and 6 shows the hand geometry system.

![Figure 5 - Hand Geometry Scanner](image)

Some of the hand geometry scanners produce only the video signal with the hand shape. Image digitalization and processing is then performed to process those signals in order to obtain required video or image of the hand [14, 15].

![Figure 6 - Acquired Image of Hand](image)

The advantage of this method is that geometric method is not sensitive to dirty hands. So this is a good application for identifying workers. Since this method is independent of the police and criminal matters people are willing to use such systems and therefore it is suitable for access control applications. Main disadvantage of this method is that it is claimed that it is not possible to indentify the image of one person’s hand among many people. Therefore, it is limited just to confirm the identity of an individual, but it is not suitable for search applications [43].

C) Identification using Vein Pattern

A new method is presented in [16, 39] for identifying individuals based on the image of the vessels. This method is useful for access control systems under network coverage. Figure 5 demonstrates the sample vessels of a hand. This method consists of two stages: registration and data collection, and the approval or recognition. In the registration phase, N numbers of hand images are collected using near-infrared imaging for different individuals. The images are being processed in pre-processing, feature extraction, and modeling stages so that the adaptive samples are generated and then the neural network is used for the verification. The preprocessing consists of Image detection threshold, edge detection, edge removing, skeleton extraction vessel, resolution enhancement using morphological functions. In the feature extraction stage, the required vectors are needed to be prepared after applying the wavelet transform to image and statistical feature extraction for comparison in authentication phase. In fact, this technology has been brought a new experience in identification technology and only by using hand vein obtained by the CCD camera.

![Figure 7: The condition of the vessel](image)
D) 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 [9]. Facial recognition technologies have recently developed into two areas: Facial metric and Eigen faces.

Facial metric technology relies on the specific facial features such as the positioning of eyes, nose and mouth, and distances between these features. These properties are recorded on an image database. In this method, the face region is normalized (rescaled) to a fixed pre-defined size and the normalized image is called the canonical image. Secondly 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 smaller sizes as well.

The Eigen Face method 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 process is done using Face Recognition software [8, 17, 18, 19]. Figure 8 shows an image with marked interested points.

For this purpose, 3 set cameras which make a 90-degree angle or a moving camera that forms a semicircle whose center is the face of the concerned person has been used and then a three-dimensional image can be generated. Figure 9 shows a 3D image obtained for recognition. The position of the eyebrows, eyes, nose, mouth, chin and forehead and the distance between the eyes and the eyebrows are computed and stored in a face template. The method is implied significant cost due to the use of expensive hardware and software. However, the reliability of this method is high compared to the method based on 2D images.

E) Retina Geometry Technology

In this method, to obtain a focused image, eyes should be
placed close to the camera. Retinal scanners are using low-power infrared laser and cameras to identify information patterns on retinal blood vessel. 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. 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. Retina scans require that the person removes their glasses and to 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 [15, 20]. Figure 10 depicts an image of a retina.

Figure 10 - Image of Retina

However, recent medical research has shown that retinal characteristics are not sustained and changeable due to some certain diseases. On the other hand many people are afraid to put their eye close to the light source. Therefore, this method is replaced by iris scanning.

F) IRIS Technology

This method uses the fact that each person's iris is unique and different with other people in terms of color and texture. Therefore, the complex appearance and structure (pattern) of iris allows extracting comparable features which can be used for recognition purpose. In the method, the colored part of the eye is scanned and analyzed [21, 22].

Imaging of the surface of the iris is not much difficult, but it should be considered carefully. For example, if the ambient light is changed or the rotation angle of the eye is not appropriate as well as the contrast, resolution and image focus is altered; then the possibility of error is considerable. Hence, iris scanning is an appropriate method for individual identification.

Recognition methods use 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 [21]. An IRIS Image is shown in figure 11.

Figure 11 - Image of IRIS

The iris pattern is taken by a special gray scale camera. Once the gray scale image of the eye is obtained then the iris within the image is located using software. 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. There are two influences to be taken into account: overall darkness of image and the size of the iris. The first is influenced by the lighting condition so the darkness threshold is used to decide whether a given point is dark or bright. It must be dynamically computed according to the overall darkness of the picture. The second changes as the size of the pupil changes. Before computing the iris code, a proper transformation must be applied to solve this problem.

In recognition process, two iris codes are taken and the hamming distance is computed based on the number of different bits. The hamming distances score is then compared with the security threshold to make the final decision. Computing the hamming distance of two iris codes is very fast, because it is only the counting of the number of bits in the exclusive OR of two iris codes. The concept of template matching could also be used in this technique. In template matching, some statistical calculation is done between a stored iris template and a produced [3, 15, 23, 24].

G) Voice 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. Voice 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. It 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) [25, 26]. Such systems employ three styles of spoken input: Text dependent, Text prompted and 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) [27, 28].

In fact, sound spectrogram makes a graph visible and shows sound frequency on the vertical axis and shows the time on the horizontal axis. In this case, each sound/voice will have its own special graph. To increase accurately and acoustic sound quality, the device uses colors and shadows to show the graph. Since the act of speaking is dynamic and changeable, even the smallest factors – such as flu-like voices- may result in altering the sound and low-clarity. But some factors such as accent, emphasis on words or speech rate have almost no effect on this process. An overview of speaker authentication system is shown in Figure 12.

![Figure 12 - An overview of speaker recognition systems](image)

**H) 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. 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 detection of the signature method analyzes the writing mode of the user. In this method, the case of written directions in X and Y as well as the change mode of the pen pressure is assessed. To do this, motion and pressure sensors are either under the paper or within the pen. As mentioned, the sensor has achieved pressure, direction and speed. Then, data are being processed and a simultaneous vector is created and the data of the vectors are compared with the original one. The most obvious and important advantage of this method is that a fraudster cannot glean any information on how to write the signature by simply looking at someone is writing. 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 [29, 30]. Signature captured by a tablet is shown in figure 13.

![Figure 13 - A Signature taken using Tablet](image)

Tablets have two significant disadvantages: the resulting digitalized signature looks different from the usual user signature and in 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 [27, 28]. 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. Such special pens are able to capture movements in all three dimensions.

Signature recognition methods are divided into two main groups: static (off-line) and dynamic (on-line). Static methods are considered a signature as two-dimensional image which do not contain any information that is time-dependent. Accordingly, the static properties of the signatures is time-invariant, are used to verify the signature. As a result, the signature recognition action becomes a regular pattern recognition process. Given that the change in the signature pattern is inevitable, signature verification process in this method can be limited to identify and map area of major changes [31].

**I) Identification of people based on their gait**

Numerous methods have been presented to identify the identification of people based on their gait in video images which they can be classified into two general categories: statistical approaches and model-based approaches, the proposed approach consists of three phases: pre-processing, feature extraction, and recognition. Evaluation of this approach shows that usually a simple background removal algorithm is done in the preprocessing phase and no serious work has been done in this phase. In the proposed method to identify people from their gait, the pre-processing is used in order to accurately estimate of the background and for object detection of the new approach based on fuzzy sets, and in
certainty a new algorithm is used based on Warping Dynamic Time. DTW is a method based on dynamic programming technique for non-linear time normalization. In this method, the Euclidean distance of each sequence of feature vectors extracted from the test image is calculated with the each component of the reference sequence of feature vectors [32].

J) Identification by key typing mode

Identification on key typing mode is one of the newest biometric identification methods. To do this, the user is asked to type a password or a specified text. Systems analysis the intervals between each key and the generated data are stored as reference data. For the function of the system at least eight characters are necessary but 12 characters or more is recommended. These characteristics can vary from one to six string such password, user name or e-mail. To maximize accuracy, this method combines the spreading technologies. The more times the user logged into the system, the more accurately system identifies her/him. The average error rate is three percent [40, 41].

K) Identification by heartbeat

Researchers at the University of Wisconsin - Madison have found a new biometric technique for identifying persons. The researchers have based heart palpitations as a pattern. They have found that each heart has its unique beating pattern. They have been used this pattern to create a biometric method to identify people. Like all biometric methods, the system first generates a template of the heartbeat. To do so, a special feature is used which can be collected with conventional sensors such as ECG. Then, the cardiograph key data are stored in a database for future comparison. To maximize the reliability of this method, pre- processing and pre-screening operations are particular important. At this stage, the filtered heartbeats will be processed and stored in a database. The accuracy and reliability of this method is still not enough and is still in its infancy. But the researchers are confident that the identification by heart beating is completely possible.

4. APPLICATIONS OF BIOMETRIC TECHNIQUES

Biometric authentication is highly reliable, because physical human characteristics are much more difficult to forge than security codes, passwords, hardware keys and so forth. Biometric- based authentication applications require workstation and network access, single sign-on, application logon, data protection, remote access to resources, transaction security, and Web security. Strong personal authentication procedures could help strong e-commerce and e-government applications. More importantly applications such as secure electronic banking, investing and other financial transactions, retail sales, law enforcement, and health and social services are already benefiting from these technologies. Another promising area is the personal authentication for large- scale enterprises where Biometric technologies are expected to play a key role. Point-of-Sale and protection of all types of digital content such as in Digital Rights Management and Health Care applications are the other possible applications. Integration of Biometric technologies with other technologies such as smart cards, encryption keys and digital signatures, biometrics helps nearly all aspects of the economy and our daily lives. Examples of other current applications include speaker verification for television home shopping. Internet banking, and users’ authentication in a variety of social services [27].

5. EVALUATION OF DEGREE OF SECURITY

The degree of security is the main concern in using biometric authentication. Therefore, it is important to evaluate different techniques and find degree of security. There are various metrics which we can used to measure the performance of any biometric authentication techniques [15, 37, 38]. These factors are described in Table 1.

Table 1 – Metrics used to measure the performance of any biometric authentication techniques

<table>
<thead>
<tr>
<th>Factor</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>False Accept Rate (FAR) and False Match Rate (MAR)</td>
<td>The probability that the system incorrectly declares a successful match between the input pattern and a non-matching pattern in the database.</td>
</tr>
<tr>
<td>False Reject Rate (FRR) or False Non-Match Rate (FNMR)</td>
<td>The probability that the system incorrectly declares failure of match between the input pattern and the matching template in the database.</td>
</tr>
<tr>
<td>Relative Operating Characteristic (ROC)</td>
<td>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.</td>
</tr>
<tr>
<td>Equal Error Rate (EER)</td>
<td>The rates at which both accept and reject errors are equal. EER is commonly used when quick comparison of FAR and FRR is needed.</td>
</tr>
<tr>
<td>Failure to Enroll Rate (FTE or FER)</td>
<td>The percentage of data input is considered invalid and fails to input into the system. Failure to enroll.</td>
</tr>
<tr>
<td>Failure to Capture Rate (FTC)</td>
<td>The probability that the system fails to detect a biometric characteristic when presented correctly is generally treated as FTC.</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Template Capacity</td>
<td>The maximum number of sets of data which can be input into the system.</td>
</tr>
</tbody>
</table>

A) Factors to be considered

The widely used techniques have their advantages as well as limitations due to various reasons. This section discusses the factors to be considered in using such techniques.

**Finger Print Technology**: Too wet or dry fingers do not produce bitmaps with sufficient quality, because the finger print bit map is affected by the finger moisture as the moisture significantly influences the capacitance.

**Face Recognition Technology**: The current software often doesn’t find the face at all or finds “a face” at an incorrect place leading to worse results. The other problem is that very similar persons like twins could not be correctly identified. Any significant change in hair or beard style causes additional difficulties.

**Iris Technology**: The iris image covered with eye-lids etc. could introduced difficulties in correct identification. So additional processing overhead is required to resolve such problems.

**Hand Geometry Technique**: Hand geometry doesn’t produce a large data set. Therefore, give a large number of records, hand geometry may not be able to distinguish sufficiently one individual from another.

**Retina Geometry**: The main drawback of the retina scan is its intrusiveness. The method of obtaining a retina scan is personally invasive. A laser light must be directed through the cornea of edge. The operation of retina scanner is also not easy. A skilled operator is required and the person being scanned has to follow his or her direction.

**Speaker Recognition Technique (voice)**: 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.

**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. 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 accuracy of the signature dynamics biometric systems is not high.

6. CONCLUSION

Biometric authentication is highly reliable, because physical human characteristics are much more difficult to forge than security codes, passwords and hardware keys. Only other hand, smart card, magnetic stripe cards, ID cards, physical keys like things can be lost, stolen, duplicated or left at home. Moreover, today’s fast-paced electronic world means people have to remember a number 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 and users have nothing to remember. Biometric systems networked together with telecommunication technology, biometric systems become Tele-biometric systems. Enrollment and test are the main operations of such systems.

Though biometric authentication can offer a high degree of security, they are still not the perfect solution. Sound principles of system engineering are still required to ensure a high level of security rather than purely depend on invariant biometrics features. Non-repudiation and irrevocability are concerns over Biometrics systems based on distributed database. However, 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. Careful consideration of the importance of biometrics data and how it should be legally protected will popularize this technology further.

REFERENCES


