International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 1328-1335 www.ijaem.net ISSN: 2395-5252

Biometric Authentication

Dixit Pundir, Arjun Baghel, Krishan Gaur

school of computing science and engineering.galgotias university,gautam buddha nagar,uttar pradesh.
School of computing science and engineering.galgotias university,gautam buddha nagar,uttar pradesh.
School of computing science and engineering.galgotias university,gautam buddha nagar,uttar pradesh

Submitted: 25-06-2021 Revised: 06-07-2021 Accepted: 09-07-2021

ABSTRACT—Advancein 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 biometric, 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 biometric it is possible to confirm or establish an individual's identity. The position of biometric in the current field of security has been depicted in this work. We have outlined opinions about the usability of biometric authentication systems, comparison between different techniques and their advantages and disadvantages in this paper.

Keyword-
biometricauthentication,physiologicalparameters,authentication system

I. INTRODUCTION

Biometric authentication has grown in popularity as a way to provide personal identification. Person's identification is crucially significant in many applications and the hike in credit card fraud and identity theft in recent years indicates 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 case 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 advantages claimed by biometric authentication is that they can establish an unbreakable one-to-one correspondence between an individuals and a piece of data.

II. TECHNOLOGIES

2.1 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. 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.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 1328-1335 www.ijaem.net ISSN: 2395-5252

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.

2.2. 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. 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.

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 software [24, 25, 32 ,39].

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 1328-1335 www.ijaem.net ISSN: 2395-5252

Figure 4 Eigen Face

2.3. IRIS Technology

This recognition method uses the iris of the eye which is coloured 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. 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.

2.4. 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.

Figure 6 Hand Geometry Scan

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

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 1328-1335 www.ijaem.net ISSN: 2395-5252

features. 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.

2.5. 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 isthen analyzed.

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.

2.6. 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).

2.7. 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, figure 9.

Figure 9A 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. This is a considerable drawback for

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 1328-1335 www.ijaem.net ISSN: 2395-5252

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. Other Techniques Some other available techniques for biometric authentication are described below.

2.8.1. Palm print:

Palm print verification is a slightly different implementation of the fingerprint technology. Palm print 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.

2.8.2. 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 Vein check and uses a template with the size of 50 bytes.

2.8.3. 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.

2.8.4. 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.

2.8.5. 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 (Opto phone) 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.

2.8.6. Body Order:

The body order 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 order from nonintrusive 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 order sensors brings up the privacy issue as the body order 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 order.

2.8.7. 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.

2.8.8. 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 International Journal of u- and e-Service, Science and Technology Vol. 2, No. 3, September, 2009 22 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.

III. 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. Table 1 shows the evaluated vales of various evaluation techniques.

3.1. Factors of Evaluation

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 1328-1335 www.ijaem.net ISSN: 2395-5252

3.1.1. 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.

3.1.2. 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.

3.1.3. 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 International Journal of u- and e- Service, Science and Technology Vol. 2, No. 3, September, 2009 23 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) .

3.1.4. 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.

3.1.5. Failure to En roll Rate (FTE or FER):

The percentage of data input is considered invalid and fails to input into the system. Failure to en roll happens when the data obtained by the sensor are considered invalid or of poor quality.

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

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

3.2 Results of Evaluation

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

3.2.1. 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.

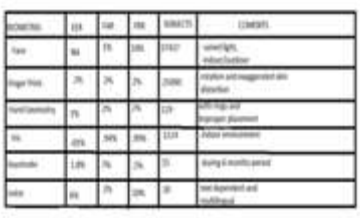
3.2.2. Face Recognition Technology:

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 live 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".

3.2.3.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 live is working properly.

Table 1 Evaluation of Biometric Techniques



3.2.4. 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.

3.2.5. 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.

3.2.6. 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.

3.2.7. 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 International Journal of u- and e- Service, Science and Technology Vol. 2, No. 3, September, 2009 25 published by manufacturers is around 2%, but according to our own experience the accuracy is much worse.

IV. 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..

ACKNOWLEDGEMENT

We would like to thanks our project guide Mr.Sanjay Gupta sir.Also our department professors who helped us throughout the project and research paper journey.Without their guidance this would have not been possible.

REFERENCES

[1]. R. Kannavara, N. Bourbakis, N. V. Boulgouris, K. N. Plataniotis and E. Micheli-Tzanakou, "A comparative survey on biometric identity authentication techniques based on neural networks" in Biometrics: Theory Methods and Applications, pp. 47-79, 2009.

[2]. S. R. Borra, G. J. Reddy and E. S. Reddy, "A broad survey on fingerprint recognition systems", Proc. Int. Conf. Wireless Commun. Signal Process. Netw. (WiSPNET), pp. 1428-1434, Mar. 2016.

[3]. C. S. Sreeja, M. Misbahuddin and N. P. H. Mohammed, "DNA for information security: A survey on DNA computing and a pseudo DNA method based on central dogma of molecular biology", Proc. Int. Conf. Comput. Commun. Technol., pp. 1-6, Dec. 2014.

[4]. S. Shunmugam and R. Selvakumar, "Electronic transaction authentication—A survey on multimodal biometrics", Proc. IEEE Int. Conf. Comput. Intell. Comput. Res., pp. 1-4, Dec. 2014.