ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

Biometric Identification Techniques: A Review

Muhanad Faris Saleh [1], Akram Abdul_Maujood Dawood [2]

Assistant Lecturer, Department of Computer Engineering, College of Engineering, University of Mosul, Mosul, Iraq[1]

Lecturer, Department of Computer Engineering, College of Engineering, University of Mosul, Mosul, Iraq[2]

ABSTRACT: In this paper, we provide an overview of the fundamentals of biometric identification techniques and their applications. Biometrics is a realistic authentication and automatic recognition used as a form of identification of individuals based on their physiological and/or behavioral characteristics. The existing computer security systems are using username and passwords for person identification. The recent advances of information technology and the increasing requirement for security have led to a rapid development of intelligent personal identification systems based on biometrics. Biometric identification, such as identification systems using fingerprint, iris, facial recognition, Retina scans, palm print, hand geometry, and signature, etc; have many advantages over the traditional authentication techniques based on what you know or what you possess. A comparison on different of these technologies is also given.

KEYWORDS: Biometrics; Facial recognition; Fingerprints; Voice recognition; Retina scans; Palm print

I. INTRODUCTION

Biometrics is automated methods of recognizing a person based on a physiological or behavioural characteristic [1]. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. In the past years, an extensive research and development has been taken place in the areas of unique identification. A brief background of biometric and biometric security systems will provide a greater understanding of the concept of computer system security. Biometrics is defined as the unique (personal) physical/logical characteristics or traits of human body [2]. These characteristics and traits are used to identify each human. Any details of the human body which differs from one human to other will be used as unique biometric data to serve as that person's unique identification (ID), such as: retinal, iris, fingerprint, palm print and DNA. Biometric systems will collect and store this data in order to use it for verifying personal identity.

The combination of biometric data systems and biometrics recognition/ identification technologies creates the biometric security systems. The term "biometrics" is derived from the Greek words bio (life) and metric (to measure). The word refers to automated methods of authentication based on physical or behavioural characteristics of an individual. Identifying ourselves is indeed a very common procedure in modern society. Traditionally, identification strategies are based on something we know, e.g., a password or a personal identification number (PIN). As the transaction fraud raises and level of security infringes, the requirement for highly secure identification and personal verification technologies are becoming apparent. Biometric-based solutions are able to provide for confidential personal data privacy. In order to access the biometric security system, an individual will need to provide their unique characteristics or traits which will be matched to a database in the system. If there is a match, the locking system will provide access to the data for the user. The necessity for biometrics can be found in its extensive use in law enforcement to identify criminals. It is also being increasingly used today in to establish person recognition in a large number of civilian applications. Secure electronic banking, investing and other financial transactions, retail sales, law enforcement, and health and social services are already benefiting from these technologies. Moreover, biometric recognition systems can operate in two modes [3]. Identification mode, where the system identifies a person searching a large database of enrolled users for a counterpart. And authentication mode where the system verifies a person's claimed identity from his earlier enrolled pattern.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

II. RELATED WORK

Due to the uniqueness of human biometrics witch played a master role in degrading imposters' attacks. Such authentication models have overcome other traditional security methods like passwords and PIN. Biometric characteristics divided into two categories, the physiological and the behavioral features. Physiological characteristics related to human body traits such as retinal, iris, fingerprint, palm print and DNA. Behavioural approach of biometric related to behavioural traits a human such as signature, voice recognition, gait, and keystroke dynamics [1].

A wide variety of systems requires reliable personal recognition and authentication mechanisms techniques to either confirm or determine the identity of an individual. The purpose of such technique is to ensure that the rendered services are accessed only by a genuine user and no one else. Examples of such applications include secure access to buildings, computer systems, laptops, cellular phones, and ATMs. By using biometrics, it is possible to confirm or establish an individual's identity based on "who she is," rather than by "what she possesses" (e.g., an ID card) or "what she remembers" (e.g., a password) [2].

Authentication process means whether the person is genuine or intruder. The statistical calculations of various values like reference threshold, FAR (False Acceptance Rate), FRR (False Rejection Rate) are required for real-time automated biometric authentication system because the measurements of biometric features are statistical values. Reference threshold value plays an important role in authentication system and it is the main factor in authenticating a person as genuine or imposter. After analyzing all values in threshold range, the reference threshold is calculated for suitable values of FAR and FRR. Selection of FAR and FRR also plays important role in selecting suitable value of reference threshold. In simple words, reference threshold can be defined as a value that can decide whether a person is genuine or intruder by using biometric authentication. Wavelet transform, a multi-resolution analysis method is used for line features extraction. These line features are referred as feature vectors. The two feature vectors used in palm print matching are: first from enrollment stage or database and second from authentication stage. [4].

III. WORKING PRINCIPLE OF BIOMETRIC SYSTEM

All the biometric system use the same basic working principle as explained below. It consists predefined steps as well as we must know some basic terms related to biometric system as enrollment, biometric data, presentation, template, feature extraction, matching [4]. The biometric process explained as shown in Figure 1.

A. *Enrollment or Registration*

The process, by which a user's biometric data is initially obtained, processed and stored in the form of a template for ongoing use in a biometric system. It is called enrollment or registration process. This template will be use for further process as authentication.

B. *Biometric Data*

The data presented by the user during registration is called unprocessed image data, which is also referred as raw biometric data or biometric sample. Raw biometric data cannot be used to perform biometric matches so it is used to generate biometric template with the help of feature extraction process.

C. *Presentation*

The process by which user presents his/her biometric data to the acquisition devices, the hardware which is used to collect data. For example placing a finger on a plate at finger reader device.

D. *Template*

A mathematical representation of raw biometric data which is obtained after applying a number of feature extraction algorithms. A template size can vary in size as few bytes for hand geometry to several thousand bytes for facial recognition. The template created at the time of registration is called stored template and at the time of authentication is called live template.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

E. *Feature Extraction*

The process of locating and encoding distinctive characteristics from biometric data in order to generate a template is called feature extraction. Feature extraction takes place during enrollment and verification, any time a template is created.

F. *Matching*

A process where stored template is matched with live template at the time of verification and we obtained a score, on the basis of this score we conclude that a user is authenticate human or not.

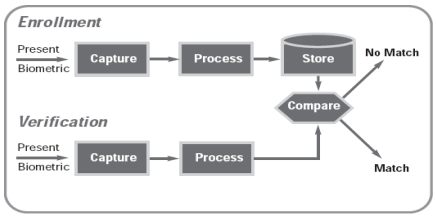


Figure 1. Biometric processing. In the enrolment stage, a collection of data of user biometric attributes is included. In the release process, a comparison is made between sample of data of a subject and the template that is already stored in the database from the first process.

IV. TYPES OF BIOMETRICS

Biometrics makes the use of biological terms that deals with data statistically. It verifies a person's uniqueness by analysing his physical features or behaviours. The systems record data from the user and compare it each time the user is claimed. Each biometric has its strengths and weaknesses, and the choice depends upon its application & biometric properties. No single biometric is sufficient to meet the requirements of all the applications. So, no biometric is “optimal”. Biometric devices are many types, but majorly there are five types of biometrics security which are commonly used. Biometrics is basically the recognition of human being personality that are unique to each human, which includes facial recognition, fingerprints, voice recognition, retina scans, palm prints, and more. An overview of commonly used biometrics is given below.

A. *DNA*

It is impossible to fake this characteristic because each person's DNA is unique. Each person's DNA contains some trait from his/her parents. Each cell in the human body contains a copy of this DNA. DNA biometrics technology is highly unique and the chance of two individuals having the exact same DNA profile is extremely impossible, but this technology is still new and is hardly applied in public. It is Used in forensic applications for person recognition, used for paternity testing, identification of missing or dead people.

B. *Retina Recognition*

A retinal scan is a biometric approach that makes use of the unique patterns on someone's retina to discover them. The human retina is a thin tissue composed of neural cells that is located within the posterior part of the eye. Due to the complex shape of the capillaries that deliver the retina with blood, all and sundry's retina is unique. The network of blood vessels within the retina is so complicated that even identical twins do not proportion a comparable sample [5]. Retinal scan captures the pattern of eye’s blood vessels. Retinal patterns are different for right and left eye, for identical twins, do not change with age. 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. [6].

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

C. *Iris Recognition*

The human iris is a thin circular structure in the eyes which is responsible for controlling the diameter and size of the pupils. It also controls the amount of light which is allowed through to retinal in order to protect the eye's retina. Iris color is also a variable different to each person depending upon their genes. The iris also has its own patterns from eye to eye and person to person, this will make up to uniqueness for each individual. Iris recognition is an automated method of biometric identification that uses mathematical pattern recognition techniques on video images of the irises of an individual's eyes, whose complex random patterns are unique and can be seen from some distance. iris recognition uses camera technology with subtle infrared illumination to acquire images of the detail-rich, intricate structures of the iris. A key advantage of iris recognition, besides its speed of matching and its extreme resistance to false matches is the stability of the iris as an internal protected [7]. An iris scan will analyze over 200 points of the iris, such as rings, furrows, freckles, and the corona [6]. Converted into digital templates, those snap shots offer mathematical representations of the iris that yield unambiguous wonderful identity of an individual [5]. The biometric person identification technique based on the pattern of the human iris is well suited to be applied to access control and provides strong e-security.

D. *Fingerprint Recognition*

Fingerprint identification is probably the best-known biometric technique, because of its widespread application in forensic sciences and law enforcement scenarios [8]. Finger print comprises of ridges and valleys. The ridges are the dark area of the fingerprint. The ridges form so-called minutia points: ridge endings (where a ridge end) and ridge bifurcations (where a ridge splits in two). A typical fingerprint image used for identification as shown in figure 6. the overall characteristics of the fingerprints (minutia points, ridge thickness, curvature, or density) are compared with the registered template. The fingerprints of individuals are unique, even for twins. There are several benefits of using fingerprint recognition systems. This system is easy to use and install. It requires cheap equipment which generally has low power consumption. Electronic fingerprint scanners capture digital "pictures" of fingerprints, either based on light reflections of the finger's ridges and valleys, ultrasonic's, or the electrical properties of the finger's ridges and valleys. These pictures are then processed into digital templates that contain the unique extracted features of a finger. These digital fingerprint templates can be stored in databases and used in place of traditional passwords for secure access [9].

E. *Face recognition*

The human face is one of the easiest characteristic which can be used in biometric security system to identify a user. Face recognition technology, is very popular and is used more widely because it does not require any kind of physical contact between the users and device. Cameras scan the user face and match it to a database for verification. The dimensions, proportions and physical attributes of a person's face are unique. The use of face recognition includes many applications such as access to secure areas, video surveillance, law enforcement applications, etc [8].

F. *Voice recognition*

Each person in the world has a unique voice pattern. Even though the changes are slight and hardly noticeable to the human ear [5]. Voice recognition systems can discriminate between two very similar voices, including twins. Voice recognition utilizes various audio capture devices (microphones, telephones and PC microphones). Its performance depends on the quality of the audio signal. Unauthorized access via tape recording can be prevented by asking the user to repeat random phrases [6].

G. *Hand Geometry /Palm print*

This biometric technique is based on the fact that virtually every person's hand is uniquely shaped, and this shape does not significantly change after a certain age. Hand geometry biometric techniques usually represent the hand geometry in terms of features comprising the lengths of the fingers, their widths and widths of the palm at various locations [8]. Hand prints can be used for criminal, forensic or commercial applications.

H. *Signature verification*

Another behavioural biometric is a signature at which the data can be extracted by the signature of that particular person. The responsibility of a signature is exclusively not only to provide evidence of the identity of the constricting

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

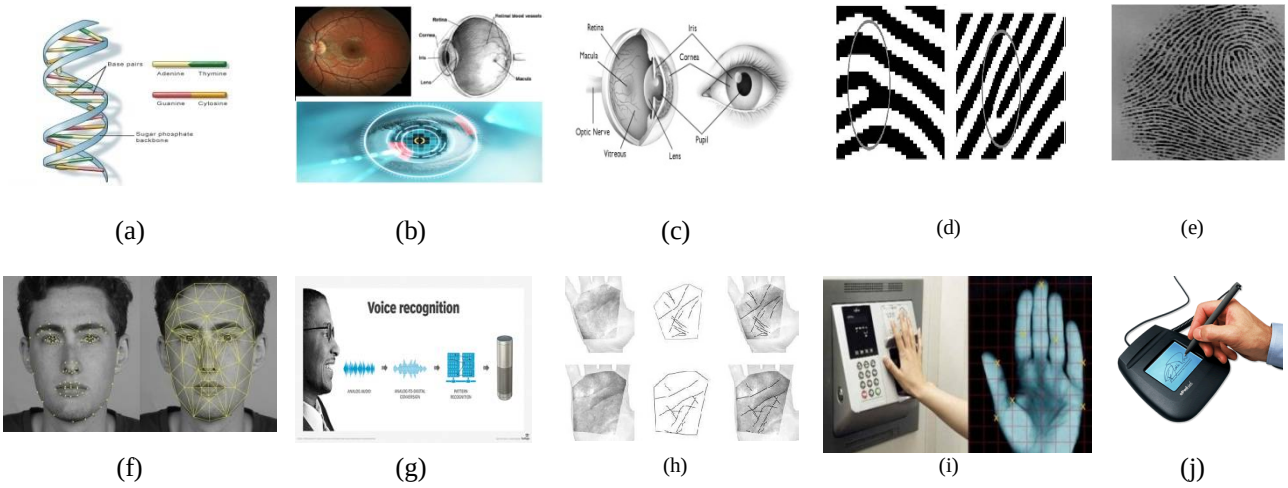
International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

gathering but moderately to provide evidence of deliberation and educated consent signatures can be easily inaccurate With advanced signature capturing devices. Signature recognition correctly became easier and more efficient.



(a) (b) (c) (d) (e)

(f) (g) (h) (i) (j)

Figure 2. Some examples of Biometric characteristics that are commonly used. The images illustrate some of the human biometric entities: (a) Structure of DNA, (b) Retina scanning, (c) iris sample, (d) Ridge ending and ridge bifurcation, (e) A typical fingerprint image used for identification, (f) Example of face recognition scans, (g) Example of voice recognition, (h) Palm-print, (k) Hand Geometry, (j) Signature scanning.

V. PERFORMANCE EVALUATION METRICS

Performance testing comprises a critical aspect of biometric modality assessments. Investigators are able to draw from a wide range of performance evaluation metrics that assess functional system accuracy and usability. Traditional performance metrics describe system accuracy. To evaluate how accurate a biometric system is, i.e. to measure its biometric performance, many genuine and impostor attempts are made with the system and all similarity scores are saved. By applying a varying score threshold to the similarity scores, pairs of FRR and FAR can be calculated.

A. *False Acceptance Rate (FAR)*

This is defined as a percentage of impostors accepted by the biometric system. Hence it is necessary that this percentage is as small as possible so that the person not enrolled in the system must not be accepted by the system.

$$FAR = \frac{\text{number of successful authentications by impostors}}{\text{number of attempts at authentication by impostors}} \quad (1)$$

B. *False Rejection Rate (FRR)*

This is defined as a percentage of genuine users rejected by the biometric system. hence the system must not reject an enrolled user and number of False Rejections must be kept as small as possible.

$$FRR = \frac{\text{number of failed attempts at authentication by authorized users}}{\text{number of attempts at authentication by authorized users}} \quad (2)$$

C. *Genuine Acceptance Rate (GAR)*

This is defined as a percentage of genuine users accepted by the system. It is given by the following:

$$GAR = 100 - FRR \quad (3)$$

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

Equal Error Rate (EER)

This is defined as the point of intersection on the graph on which both FAR and FRR curves are plotted. The lower the EER is better for the system's performance and must be kept as small as possible.

D. ***Threshold***

Accuracy plays an important role in authentication system and it depends on the value of reference threshold chosen. Threshold can be defined as a value which decides whether the person is genuine or imposter [4].

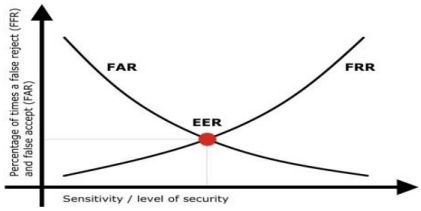


Figure 3. FAR, EER, FRR. The more accurate one would show lower FRR at the same level of FAR which defind as EER.

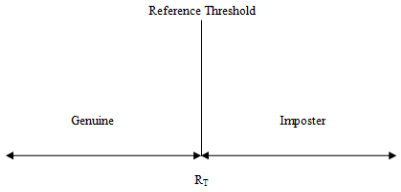


Figure 4. Criteria of authentication. It is basically the value of reference threshold that authenticates the person as genuine or imposter.

The accuracy of the authentication system is given by the following:

$$\text{Accuracy (\%)} = (100 — (\text{FAR(\%)} + \text{FRR(\%)}) / 2) \quad (4)$$

E. ***MEASUREMENT REQUIREMENTS***

Any human physical and/or behavioural characteristic can be used as a biometric characteristic if it satisfies the following seven basic criteria requirements for biometric security system:

F. ***criteria requirements***

- Universality: each potential user possesses the modality.
- Uniqueness: the modality adequately differentiates between any two users.
- Permanence: the modality profile remains relatively constant over time.
- Collectability: the modality samples are easy to detect and acquire.
- Performance: the modality is robust and functional within a range of operational and Environmental factors.
- Acceptability: the extent to which users are willing to accept and use the modality.
- Circumvention: how susceptible the modality is to spoof attacks and identity fraud.

G. ***Comparing biometric systems***

The following table compares some of the biometric systems used. We show the more common biometric technologies and their performance.

TABLE I. COMPARISON OF VARIOUS BIOMETRIC [10]. A COMPARISON STUDY OF BIOMETRIC MODALITIES IN TERMS OF UNIVERSALITY, UNIQUENESS, PERMANENCE, COLLECTABILITY, PERFORMANCE, ACCEPTABILITY, CIRCUMVENTION.

Biometric	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
DNA	high	high	High	low	high	low	low
retina	high	high	Medium	low	high	low	low
iris	high	high	High	medium	high	low	low
fingerprint	medium	high	High	medium	high	medium	Medium
voice	medium	low	Low	medium	low	high	High
Hand Geometry	high	medium	Low	high	medium	Medium	medium
signature	low	high	Low	high	medium	high	high

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

VI. CONCLUSION

Biometrics refers to automatic recognition of an individual based on her behavioral and/or physiological characteristics. This paper presents biometric recognition system and methods for personal identification. This technique of identification offers several compensations over traditional methods involving ID cards or PIN numbers for various reasons. Hence these systems are proved highly confidential computer-based security systems. Each and every biometric system is useful and selection of particular biometric device depends upon the application area. As comparison demonstrate view of various perspectives so one can easily pick the biometric technology for deployment in real time. it is important to take more attention to these evaluation aspects (data quality and security). Finally, we believe that the evaluation aspects should be taking into account simultaneously when evaluating and comparing biometric systems.

REFERENCES

1. Alsaadi, I, M. "Physiological biometric authentication systems, advantages disadvantages and future development: A review". IJSTR, vol.4 , no.12, pp. 285-289, 2015.
2. Jain, A.K. and Ross, A Prabhakar, S. "An introduction to biometric recognition". IEEE Transactions On Circuits And Systems For Video Technology, vol.14 , no.1, pp. 4-20, 2004
3. Ahmed, A. and Traore, I. "Anomaly intrusion detection based on biometrics". In 6th IEEE Information Assurance Workshop, 2005.
4. Malik, J. and Girdhar, D. "Reference Threshold Calculation For Biometric Authentication". I.J. Image, Graphics and Signal Processing, no.2, pp. 46-53,2014. DOI: 10.5815/ijigsp.2014.02.06.
5. Biom, K, J. "Various Biometric Authentication Techniques". Journal of Biometrics & Biostatistics, vol.8 , no.5, pp.1-5, 2017. doi: 10.4172/2155-6180.1000371.
6. Singhal, z.; Gupta, p. and Garg, k. "Biometric Recognition: Personal Identification Technique". IJCEM, vol.15 , no. 2, pp. 6-10, 2012
7. Mallikarjuna, A. and Madhuri, S. "Biometric Security Techniques For IRIS Recognition System", International Journal of Research in Computer and Communication Technology, vol.12 , no.8, pp.589-593, 2013.
8. Garcia, R.; Lopez, C. and Aghzoutb, O. "Biometric identi cation systems". Signal Processing, vol.8 , no.1, pp. 2539-2557, 2003, doi:10.1016/j.sigpro.2003.08.001.
9. Mudholkar, S.; Shende, P.; and Sarode, M. "Biometrics Authentication Technique For Intrusion Detection Systems Using Fingerprint Recognition". IJCSEIT, vol.2 , no.1 pp. 57-65, 2012.
10. Srivastava, H. "A Comparison Based Study on Biometrics for Human Recognition". IOSR Journal of Computer Engineering, vol.15 , no.1, pp. 22-29, 2013.