IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-5, Issue-9 E-ISSN: 2347-2693

Biometric Recognition System: A Review

Manpreet Kaur[1*],Sawtantar Singh Khurmi[2]

[1*]Dept. of Computer Science and Applications, DBU, Mandi Gobindgarh, India
[2] Dept. of Computer Science and Engineering, DBU, Mandi Gobindgarh, India

[*]*Corresponding Author: preetbhullar82@gmail.com*

Available online at: www.ijcseonline.org

Received: 07/Aug/2017, Revised: 18/Aug/2017, Accepted: 14/Sep/2017, Published: 30/Sep/2017

***Abstract*—**Biometric system is used for identification of an individual on the basis of their physical and behavioral features. As the research in the information technology is increasing day by day, so, the security of information becomes a great issue. Therefore, to deal with security, authentication access control plays an important role and this is the first step to ensure security. This paper describes the study of widely used biometric technologies. The principle by the biometric system work is being defined with the stages by which biometric system works. In biometrics, according to some characteristics, we need to identify human physiological parameters. The comparison of biometric traits on the basis of feature description is given with their characteristics on the basis of uniqueness, university, measurability, acceptability, circumvention and premenance. Work done by number of authors in biometric system is given in the form of comparison with the techniques and outcomes. A biometric system requires a reliable personal identification scheme to confirm or determine the needs of their individual identity services. The aim of this technique is to ensure that only legitimate users can access these services, and are not accessible to others. The notable features of biometric can be confirmed or established a personal identity.

***Keywords*—**Biometric, fingerprint hand, iris, face, DNA, keystroke, signature, Voice

I. INTRODUCTION

Data security is concerned with the guarantee of privacy, integrity and accessibility of information in all forms. There are various tools and methods available to provide information security. Among all the security systems, biometric system usually provides better security. Biometric system deals with individuals on the basis of their behavioral and physical characters like fingerprint, iris, face, signature etc. that have advantages over the systems. In traditional authentication system, one has to remember password or secret code to identify an individual. But passwords can be hacked by attacker and thus, can leak the secret or we can say that it is not a secure technique. It is also very difficult to remember the entire password. Therefore, nowadays, an automatic system is based on physical or behavior of human which usually used widely for identification and providing security to the system [1]. This paper is organized in the way that a brief description of biometrics along with their types is given in section I. Related work along with different techniques is given in section II. Finally conclusion is being drawn in section III.

A. Working principle of Biometric system

A biometric system is a real time identification system that is used to recognize an individual by measuring their behavioral and physical characteristics by comparing it to the data stored in the data base [2]. A biometric system consists of a scanning device to read the data and convert that into digital forms and then stored into the data base. The various steps used in the biometric system are defined below:

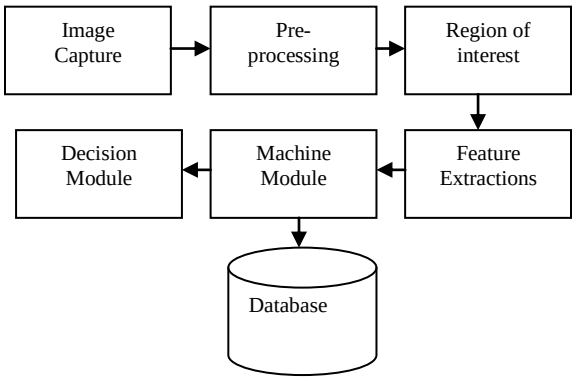

Figure 1. Biometric system [1]

A biometric system mainly consists of image captured unit, Pre-processing, feature extraction unit, image matching unit and decision stage as shown in figure 1 and are defined below:

1) Pre-processing Stage

This is the first step in Biometric system, in which the input data is processed to increase the quality of the captured image. This is mostly used to reduce the noise and thus, obtained an image ready for feature extraction.

2) Region of Interest Stage

In this process, the interesting features of the biometric image are divided into smaller regions that are used for matching the characteristics in a biometric system.

3) Feature Extraction Stage

Feature extraction is mainly used to take out some of the features used to sort input image and capture patterns present in the original data set [3].

4) Matching module stage

The extracted features are compared at this stage with the dataset. After the comparison, a matching score is being generated.

5) *Decision making*

This is the last stage of the biometric system, in which the user is recognized or unrecognized on the basis of the score generated by the matching module [4]

B. Types Of Biometric Identifiers

Biometric identifiers are mainly of two types as shown in figure 2:

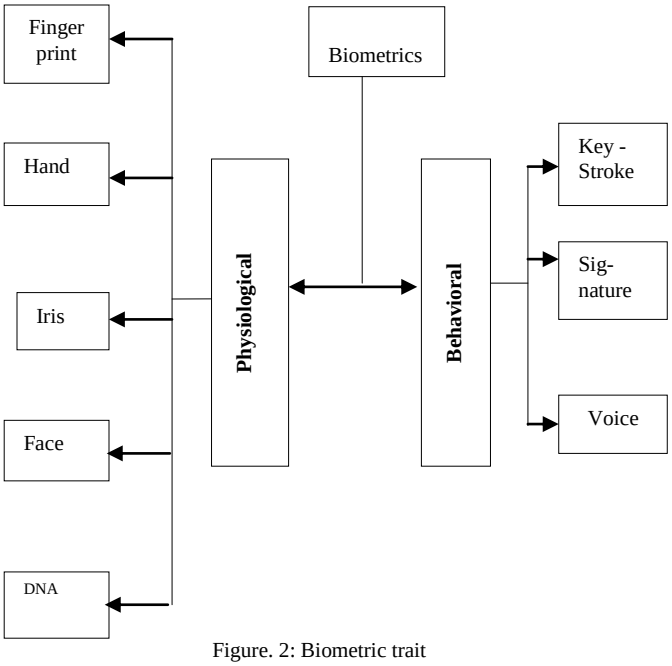

Figure. 2: Biometric trait

1) Physiological characteristics

This section defines the physiological traits came under biometric system.

a) Finger print technology

Fingerprint recognition is one of the oldest and best methods used for identifying an individual. The reason is that each person has a different fingerprint. A fingerprint is an impact of the ridges or any part of the finger. Finger ridges are the raised section of the palm consisted of one or more connected ridge of the skin. Few year back, the finger impression usually printed on the paper and that later scanned by the scanner. An image of fingerprint map is shown below:

Figure 3: Fingerprint Bitmap

- *Finger Print Sensors*

A finger print sensor is a device used for capturing the digital image of the finger when it is placed over it. The captured image is known as scanned or digital image. This scanned image is stored in data base in order to create a template that is used at the time of matching. A number of technologies have been used like optical, capacitive, RF, thermal, piezo-sensitive, ultrasonic, piezoelectric. Some of them are explained below:

- *Optical*

In this technique, laser beam is used to scan finger print. The sensor device consists of a group of lenses. The top surface of the lens is known as touch surface, where finger is placed. Below this layer, a light emitting diode is there that illuminate the surface of the finger. When light strikes on the surface of the finger, it reflects back. Thus, the reflected ray falls on the charged couple capacitor, which stores the image in the form of charge. The image quality gets affected in the case of dirty hand [7].

- *Ultrasonic*

The working of ultrasonic sensors is based the principle of medical ultra-sonography. As an optical sensor uses light to capture the image, in ultrasonic sensors, it captures the image by penetrating the high frequency sound waves under

the skin of the finger. These waves are generated by using piezoelectric transducers. These sensors do not need for clean hands and a clean sensing surface.

- *Capacitance*

These sensors are based on the principle of capacitance, in order to form fingerprint images. The sensed image is stored in the form of charge on the capacitor plate.

Fingerprint matching techniques are divided into two forms, namely, Minutiae based and correlation based. In minutia based technique, initially the minutiae areas are discover and later, maps the relation placement on the finger. Correlation based fingerprint recognition needs the precise location of a registration point.

It is defined as the pattern created and the uniqueness of the way in which ridges end, split and join, or appear as a simple dot.

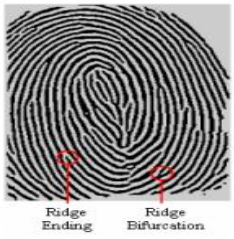

Figure 4. Minutiae

Fingerprint identification system finds the application in the organization for staff attendance like for, passport verification at border of the country, Population census, Driver's licenses and professional ID card verification [8].

b) Hand recognition

This technique is based on the concept of that the shape of hand of every person are different and it does not change with the time. This unique feature includes length, width, thickness and surface area of hand. By focusing light on the hand placed under the scanner, the hand gets scanned and thus, converted into digital image and stored in the data base [9]. The scanner is shown in figure below:

Figure 5. Hand geometry scanner

c) Face recognition

In this technique, face of an individual is identified by capturing the face with the help of camera. This biometric system mainly concentrates on the positioning of eyes, nose and mouth. It is one of the most secure mean of identification [10].

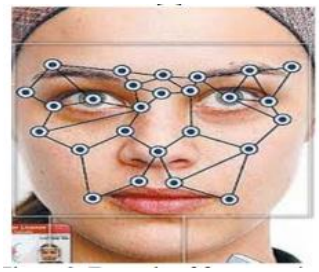

Figure 6. Face recognition

d) Iris recognition

This method is used to identify an individual on the basis of iris pattern within the round shaped region surrounding the pupil of eye. A high resolution image of an Iris is captured by using a digital camera and thus, comparing the captured image with the image stored in the data engine. To obtain the accurate results, the image is captured within a few meters of camera [11].

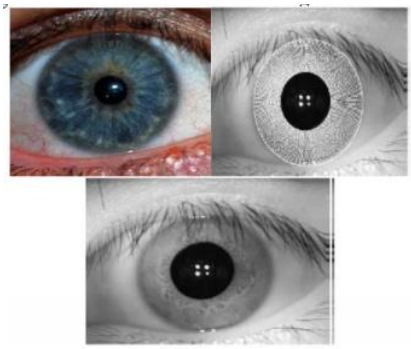

Fig.ure 7. Iris

e) DNA

DNA recognition needs lab environment to identify an individual on the basis of tissue, blood and other body samples. Presently, there is no technology that allows automatic recognition of DNA sample. DNA used sensors based on electrochemical detection [12].

Figure .8. DNA scanner example

2) Behavioural biometrics

In this technique, an individual is identified on the basis of their behaviour like on the present status of mind, voice. As we know that voice of human being gets changed due to various factors like sadness, happiness, disease, throat infection and so on. This technique comprises of voice recognition, signature and key stroke recognition.

a) Voice recognition

As every person has different voice that can be recognized on the basis of an individual speak. For recognition, it uses vocal characteristic that depends upon the dimension of mouth, nasal activities and the way of speech. It does not require any extra hardware [13].

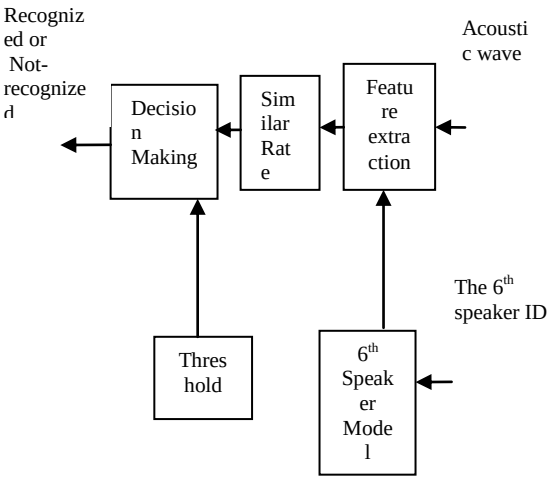

Figure 9. Voice recognition system

b) Signature recognition

In this recognition system, signature of an individual are used to identify an individual. As the style of signature varies from human to human due to different factors like stroke order, pressure applied on the pen velocity of the pen, holding style of pen and so on [14, 15].

Fig.ure 10. Signature reader

c) Keystroke recognition

In this, an individual typing style on keyboard is analyzed for recognizing the human. Keystroke is dependent upon the speed which is the time between the pressed keys, rhythm, precision, right shift key etc. [16-18].

Fig.ure 11. Typing Rhythm

Table1. Biometric comparison based on features extracted

Biometric traits	**Feature description**
Finger print	A friction Ridge curves-a raised portion, pore structure, indents and marks
Hand	Estimation of length, width, thickness, shape and surface area of the hand.
Iris	Texture of the iris such as freckles, coronas, strips, furrow, and crypts
Face	Distance of specific facial features (eyes, nose, mouth)
DNA	DNA code can be extracted from blood, hair, skin cells and other bodily substances
Keystroke	Time gap between each key stroke
Signature	It measures pressure, direction, timing, acceleration and the length of the strokes
Voice	Tone, words

Table 2. Comparison of characteristics of biometric entities

	Uniqueness	Premenance	University	Measurability	Collectability	Performnace	Acceptability	Circumvention
Finger print	High	High	Medium	High	Medium	Medium	High	Medium
Hand	Medium	Low	High	High	High	Medium	Medium	Medium
Iris	High	High	High	Medium	Medium	High	Medium	Low
Face	Medium	Medium	High	Medium	Low	High	High	High
DNA	High	High	High	Low	Low	High	High	Low
Keystroke	Low	Low	Low	Low	Medium	Low	Low	Medium
Signature	High	Low	Low	Medium	High	Medium	High	High
Voice	Low	Low	Medium	Medium	Medium	Low	High	High

II. RELATED WORK

This section defines a glance of existing work in biometric system in tabular form. The elements taken for defining the work are proposed work, techniques undertaken and outcome.

Author	Proposed work	Techniques	Outcomes
S. B. Dabhade et al. [2, 2016]	Biometric recognition based on Hyper spectral	Principle component analysis (PCA) and Kernel principle component analysis (KPCA)	Authors determined recognition rate which is 69.20 %.
A. Mansour et al.[4,2017]	Multimdal Biometric authentication system	Discrete time markov chain	Simulations are performed on MATLAB software to measure probability w.r.t discrete time interval
S. Bhilare et al. [5, 2017]	Attack is prevented by using hand vein recognition system	SVM support vector machine, Local binary pattern (LBP)	The average rate of 0.16% for same device and 0.8% for the cross device has been obtained
R. Priya, V. Tamilselvi and G. P. Rameshkumar, [7, 2014]	Finger print recognition system used for internet banking	Minutia feature extration	Accuracy upto 100 % is obtained
B. Saropourian [8, 2009]	Neural network has been used in finger print recognition	Neural network	Neural network has been used for removing the noise image, deficient image and pieced image thus accuracy of the system get increased.
S. Samoil and S. N. Yanushkevich [9, 2016]	Hand recognition system has been used for multispectral data	Principle component analysis (PCA), k-nearest neighbor (KNN) and Support vector machine (SVM)	The parameters like recognition rate has been measured which is about 76 5 to 89 %.
Lihong Wanet al. [10, 2017]	Recognize keystroke for virtual keyboard	k-nearest neighbor (KNN)	Recognition accuracy lies between 69 % to 96 %.

III. CONCLUSION

This paper has dealt with the summary of biometric recognition system. It is being analyzed from the review that the main aim of biometric system is the security that can be determine on the basis of physical and behavioral traits and for that biometric system is used. Biometric system is consisted of different stages like image captured unit, pre-processing, interest region, decision module, and machine module and feature extraction. The paper has discussed biometric traits in terms of features, like for fingerprint; it is a friction ridge curve, pore structure. A comparison has been given for different biometric entities on the basis of different parameters. Number of authors has discussed their work in this area, so, a highlight has been provided in this paper in tabular form on the basis of their techniques and the concluded remarks by means of the outcome.

REFERENCES

[1] M. O. Oloyede and G. P. Hancke, "*Unimodal and Multimodal Biometric Sensing Systems: A Review*," *IEEE Access*, Vol. 4, No. , pp. 7532-7555, 2016.

[2] S. B. Dabhade, N. S. Bansod, Y. S. Rode, M. M. Kazi and K. V. Kale, "*Hyper spectral face image based biometric recognition*," International Conference on Global Trends in Signal Processing, Information Computing and Communication *(ICGTSPICC)*, Jalgaon, pp. 559-561,2016.

[3] M. Abdelazez, M. Hozayn, G. S. K. Hanna and A. D. C. Chan, "*Gating of false identifications in electrocardiogram based biometric system*," IEEE International Symposium on Medical Measurements and Applications (MeMeA), Rochester, MN, USA, pp. 338-343,2017.

[4] A. Mansour, M. Sadik, E. Sabir and M. Jebbar, "*AMBAS: An Autonomous Multimodal Biometric Authentication System*," 13th International Wireless Communications and Mobile Computing Conference (IWCMC), Valencia, Spain, pp. 2098-2104,2017.

[5] S. Bhilare, V. Kanhangad and N. Chaudhari, "*Histogram of oriented gradients based presentation attack detection in dorsal hand-vein biometric system*," Fifteenth IAPR International Conference on Machine Vision Applications (MVA), Nagoya, Japan, pp. 39-42,2017.

[6] Subban, Ravi, and Dattatreya P. Mankame, "*A study of biometric approach using fingerprint recognition*," Lecture Notes on Software Engineering Vol.1, pp.209-215,2013.

[7] R. Priya, V. Tamilselvi and G. P. Rameshkumar, "*A novel algorithm for secure Internet Banking with finger print recognition*," International Conference on Embedded Systems (ICES), Coimbatore, pp. 104-109,2014.

[8] B. Saropourian, "*A new approach of finger-print recognition based on neural network*," 2nd IEEE International Conference on Computer Science and Information Technology, Beijing, pp. 158-161,2009.

[9] S. Samoil and S. N. Yanushkevich, "*Multispectral hand recognition using the Kinect v2 sensor*," IEEE Congress on Evolutionary Computation (CEC), Vancouver, BC, pp. 4258-4264,2016.

[10] Lihong Wan, Na Liu, Hong Huo and Tao Fang, "*Face Recognition with Convolutional Neural Networks and subspace learning*," 2nd International Conference on Image, Vision and Computing (ICIVC), Chengdu, China, pp. 228-233,2017.

[11] N. Liu, J. Liu, Z. Sun and T. Tan, "*A Code-Level Approach to Heterogeneous Iris Recognition*," IEEE Transactions on Information Forensics and Security, Vol. 12, No. 10, pp. 2373-2386, Oct. 2017.

[12] P. Michaels, S. Ciampi, C. Y. Yean and J. J. Gooding, "*Target DNA recognition using electrochemical impedance spectroscopy*," International Conference on Nanoscience and Nanotechnology, Sydney, NSW, pp. 282-284,2010.

[13] G. K. Berdibaeva, O. N. Bodin, V. V. Kozlov, D. I. Nefed'ev, K. A. Ozhikenov and Y. A. Pizhonkov, "*Pre-processing voice signals for voice recognition systems*," 18th International Conference of Young Specialists on Micro/Nanotechnologies and Electron Devices (EDM), Erlagol (Altai Republic), Russia, pp. 242-245,2017.

[14] P. Chauhan, S. Chandra and S. Maheshkar, "*Static digital signature recognition and verification using neural networks*," 1st India International Conference on Information Processing (IICIP), Delhi, India, pp. 1-6,2016.

[15] N. Çalik, O. C. Kurban, A. R. Yilmaz, L. D. Ata and T. Yildirim, "*Signature recognition application based on deep learning*," 25th Signal Processing and Communications Applications Conference (SIU), Antalya, pp. 1-4,2017.

[16] A. Morales, M. Falanga, J. Fierrez, C. Sansone and J. Ortega-Garcia, "*Keystroke dynamics recognition based on personal data: A comparative experimental evaluation implementing reproducible research*," *IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, Arlington, VA, pp. 1-6,2015.

[17] J. Mantyjarvi, J. Koivumaki and P. Vuori, "*Keystroke recognition for virtual keyboard*," IEEE International Conference on Multimedia and Expo, Vol.2, pp. 429-432 2002.

[18] S. Ravindran, C. Gautam and A. Tiwari, "Keystroke user recognition through extreme learning machine and evolving cluster method," *IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*, Madurai, pp. 1-5,2015.

