ISSN 0975-2366
https://doi.org/10.31838/ijpr/2018.10.04.050

Review Article

Survey on Biometric Identification System

SREEJA V S[1],DR M S JOSEPHINE[2]AND V. JEYABALA RAJA[3]
[1]Asst Professor, Department of BCA & IT, Vels University, Pallavaram, Chennai
Email id :sreeja.vs87@gmail.com
[2]Professor, Department of MCA, Dr MGR University Madhuravayal, Chennai
Email id : josejbr@yahoo.com
[3]Professor, Deprtment of Computer Science and Engineering, Velammal Engineering College, Chennai, India.
Email id: jeyabalaraja@gmail.com
Received: 24.07.18, Revised:24.08.18, Accepted:24.09.18

ABSTRACT
Biometric Identification is an evergreen system in the field of security. This system is used for ensuring security by providing personal identification. Biometric identification system provides an automated identification of the individual based upon their physiological or behavioral characteristics. In biometric identification Finger Print andIris Recognition plays a vital role. This system is used in government sectors to identify the person as well as to for information security. Though there are no of biometric authentication, intruders still try to break the security and acquire the information they want. Each biometric system poses its own limitations.This paper would brief you about the various biometric features available and about the limitations of the biometric features.

Keywords: Biometric identification, Physiological, behavior characteristic, iris identification, iris recognition.

INTRODUCTION

Personal identification and authentication are the important aspects of providing security. Initially authentication of a person was done using passwords, ID cards, swipe cards, etc.[1]. Later biometric identification techniques started to play a vital role in authenticating individuals. It became a trended topic in the field of research from the 19th century. Many researches are being conducted on biometric features and on its techniques to provide a better security.Biometric identification is classified on the basis of physiological and behavioral features [2]. It provides an automated authentication system to recognize the individual based on the physiological features such as fingerprints, DNA, palm, face, iris, vein and retina or behavioral features such as Handwriting, speech and signature [3]. It was introduced to identify the criminals, but nowadays it has been increasingly used in authenticating the employee in their office or by the government for authenticating the individual. Though biometric authentication techniques assures more accuracy over normal authentication techniques, still many researchers are conducting research to enable 100% accuracy in recognition with a maximum speed at low cost without causing harm to the individuals [4]. Among all the biometric authentication system iris recognition is said to be a better authentication. Iris is an internal part of the human eye which is developed even before the birth. The iris pattern of the left is different from the pattern of the right eye, hence a person will have two different iris pattern [5]. This paper would give an overview of various biometric techniques and the methods for iris recognition.

Survey on Existing Biometric Technologies

Biometric technologies are classified based on the individuals physiological, behavior characteristic. Physiological behavior deals with the parts possessed by the individual such as finger print, iris pattern, DNA etc. The behavioral characteristic deals with the behavior of the individual such as signature, password, keystroke etc.

Face Recognition Technology

It is a most casual biometric technique which is used to identify the person automatically from a digital video or image [8]. The person need not be present at the time of scanning, the face of the person can be got from a photograph or from a video frame. Various technology has been used for facial recognition, facial recognition uses metrics such as edge of face, position of eye, nose, mouth and distance between these features. The scanned face will be saved in a template, these images will have a greater file size which is then processed to be saved in a file [9]. This system is mainly used in crime cases and shopping mall to identify the intruders and criminals. The disadvantage of this system is that it can be easily spoofed [7].

Finger Print Technology

Finger print is a unique physiological characteristic of an individual where all the fingers have their own pattern. These patterns becomes prominent according to the age. Finger prints have solid structure which helps us in classifying them. Dr. Nehemiah Grew in 1684 proposed that hand and feet prints both have an own ridges, furrows and pores. Professor Johannesh proposed a system for classifying finger print. Sir Galton proposed finger

print can be used for identifying the individual [6]. It has become a common biometric technologyin various places such as banks, government and private offices, etc. for recognizing a person due to its uniqueness. This technology has its own disadvantage, it can be easily satirized, other problems are if there is a wound or allergy in the finger or if the finger is wet or filled with dust in such cases it would be difficult to scan the finger pattern and identify the person [7].

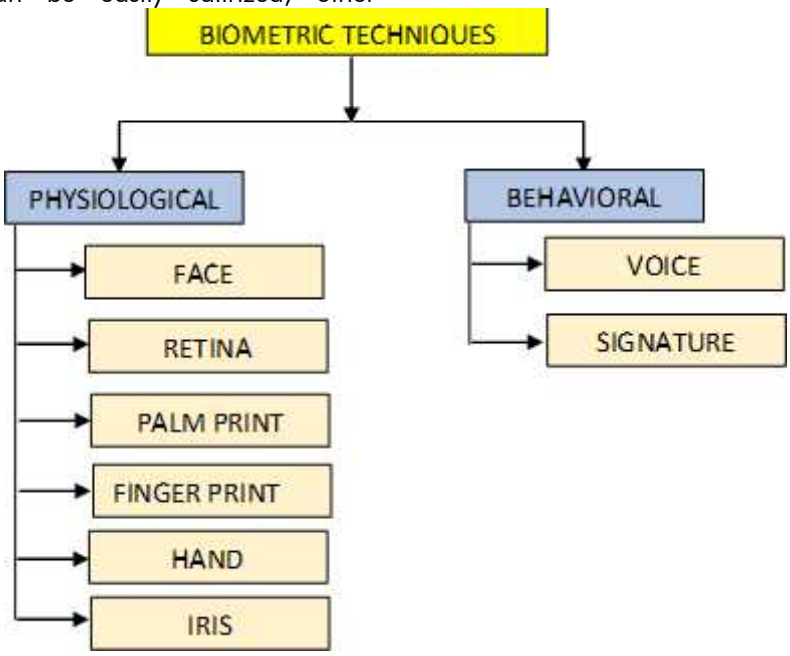

Figure 1: Types of Biometric Techniques

Hand Geometry Technology

It's a method of detecting an individual by their geometry such as shape, thickness, length, width, etc. Each individual will have a different geometric representation for their hand and finger [10].Hand geometric system requires less file size and aging doesn't affect this system like face recognition [11]. A special optical scanner is used to read the image of the hand, the shape of the hand is got by scanning it both vertically and horizontally using sensors. These sensors sends signals which might be in video format, it's then processed and digitalized [12].

Retina Geometry Technology

This system works by identifying the configuration of blood vessel pattern of the retina [13]. The infrared energy from the scanner system is absorbed by the blood vessel of the retina faster which enables it to give a clear pattern of the vessels. This system is used in place where high security is needed [14]. As the retina is the inner most part it would be difficult to spoof. The disadvantage of this system is that the person has to sit still for a long time which creates discomfort. A small moment would cause the processed to be repeated again, hence error rate would be more in this system [15].

Speaker Recognition Technique

This system uses the vocal characteristic which produce speech for the identification. This system doesn't focus much on the sound or the pronunciation. The vocal characteristic relies on the factors such as vocal tract, nasal cavities and various other speech producing mechanism of the person [16].The disadvantage of this system is that the background voice disturbance would reduce the accuracy of the system and error rate would also be high [9]. Another disadvantage is that voice changes according to the age [4].

Signature Verification Technique

Signature verification is the most common authentication technique used for past decades. Signatures verification is classified into two types online and offline. The metrics used for this technique are signature shape, the pressure put in the signature, number of strokes etc. [17]. The disadvantage in this technique is that the digital signature would have slight variation when compared with the original [4]. Another problem in this system is that the person doesn't put the signature in the same way always, so this the verification system works on the dynamic of the signature instead of comparing it with the user's true signature. Due to this there can be more number of errors and forgery [9].

IRIS Recognition Technique

Iris recognition is the most reliable technique as the iris pattern is formed even before the birth and it

doesn't change. The iris pattern of the left eye is different from the iris pattern of the right eye [18]. The iris is scanned and then it's segmented, then small portion of the segmented image is selected and converted into code and stored in the database. This enable the system to have a small file size. Later this code is used for matching. No two person can have the same iris colour or pattern even if they are twins [9]. This system gives a high level security and accuracy but still this system can be fooled by using lens. Chances of error is more if a person is wearing lens during the scanning process. This disadvantage can be overcome by using the metrics thickness near the edge.

Palmprint Recognition Technology

This is just like the extended version of finger print recognition technology, where the whole palm is scanned instead of the finger. The disadvantage of this system is its file size. To store a normalized image of Palmprint the database would need double the size of the file used for finger print recognition technology [9].

DNA Recognition Technology

This is another common authentication technique which is widely used in the field of medicines and hospitals. This system works by extracting the DNA strands from the blood. It is mostly used for identifying the criminals enrolled in criminal cases [19]. It cannot be used for personal authentication system, as the same DNA pattern can be shared by more than one person of the same family or from same gene.

Open Challenges

Biometric has become an important part in authentication system. A failure or error in this system will post a big threat to the society and to individual. As biometric authentication is now necessary part in all the process such as ID card, Govt. proof, Banking etc., individuals can't compromise on the accuracy of the system. At present various levels of threats are posted on each biometric system.

The acquired data that is the scanned image might be noisy, filled with unwanted data. The scanned finger might have scar or a poor illumination of retina blood vessel, face, etc., might cause error and miss match with the data in the database [4].

The data attained from the person might vary from the data stored in the database (which is got during the development of the system). For example the stroke of the normal signature might vary from the stroke of the digital signature [4].

The biometric data is supposed to be distinct and unique to identify the individual but still it can be shared two person. DNA is used to identify an individual but it can be same for a twin or for people in the same family [4].

The system might fail to store the biometricinformation of an individual, due to excess light the blood vessels of retina won't be captured properly, failure to identify the edges of face, failure to identify the ridges of the finger, wearing contact-lens while scanning [4].

The data are spoofed. The skit of the data which is already stored in the database are used to forge the system. For data such as iris, finger print, and palm print this type attack is being done [4].

Spoofing of biometric data is getting familiar, as iris and finger print are used more for individual authentication in private sectors and government sectors spoofing is gaining more attention.Moreover contact lens have become a normal part of the life, which has become difficult to recognize the iris pattern. The system should be able to recognize the fake data (differentiate the normal iris and fake iris) and reject it.

Discussion

Biometric authentication system has been in use for several decades and many new techniques keep on emerging. This paper discusses about certain commonly used and familiar biometric recognition systems and its limitations, to overcome these limitations we can use a multimodal biometric system such as finger print and iris or retina and iris etc., but still these system can be spoofed. To overcome spoofing the anti-spoofing technique can be used. Anti-spoofing technique can be done in two levels a) hardware- based or sensor level b) software-based or feature level. Hardware-based technique is used to detect the fake data while scanning using special sensor. Software-based technique is used to detect the fake data after the data attained [20].

Conclusion

This paper presents an overview of various biometric authentication systems available. It helps in gaining knowledge on the advantages and disadvantages of each system. It also gives an overview on the limitation of biometric system. Spoofing of biometric traits is growing and gaining more attention.We would like to concentrate more on iris recognition system where no of challenges are put forward such contact-lens and skit of the iris pattern. Therefore we have planned to carry out the research on Iris anti-spoofing.

References

1. Muthana H. Hamd , Samah K. Ahmed , "Biometric System Design for Iris Recognition Using Intelligent Algorithms" , I.J. Modern Education and Computer Science, 2018, 3, 9-16.
2. Mohammad AakifKausar, GautamPurwar, RajulRaghuwanshi, Prof. SachinDeshmukh, "User Identification Using Iris Scan", International Journal of Science, Engineering and Technology Research

(IJSETR) ***ISSN: 2278 – 7798*** Volume 5, Issue 4, April 2016.

3. Nirali M. Bhagwagar, Yagnik A. Rathod, "A SURVEY ON IRIS RECOGNITION FOR AUTHENTICATION", International Journal of Technical Research and Applications e-ISSN: 2320-8163, www.ijtra.com Volume 3, Issue 2 (Mar-Apr 2015), PP. 148-151.
4. Anil K. Jain, Fellow, IEEE, Arun Ross, Member, IEEE, and SalilPrabhakar, Member, IEEE,"An Introduction to Biometric Recognition",IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 14, NO. 1, JANUARY 2004.
5. Nirali M. Bhagwagar, Yagnik A. Rathod, "A SURVEY ON IRIS RECOGNITION FOR AUTHENTICATION", International Journal of Technical Research and Applications e-ISSN: 2320-8163, www.ijtra.com Volume 3, Issue 2 (Mar-Apr 2015), PP. 148-151.
6. Rahul Sharma, Nidhi Mishra, Sanjeev Kumar Yadav,"Fingerprint Recognition System and Tehniques: A Survey",International Journal of Scientific & Engineering Research, Volume 4, Issue 6, June-2013 ISSN 2229-5518.
7. S.Vinitha, R. Karthiyani," IRIS Biometric Recognition for Person Identification and Security", International Journal of Scientific Research in Computer Science, Engineering and Information Technology © 2017 IJSRCSEIT | Volume 2 | Issue 3 | ISSN: 2456-3307.
8. M. A. Dabbah, W. L. Woo and S. S. Dlay,"Secure Authentication for Face Recognition," Proceedings of the 2007 IEEE Symposium on Computational Intelligence in Image and Signal Processing (CIISP 2007)
9. Debnath Bhattacharyya1, Rahul Ranjan1, FarkhodAlisherov A.2, and Minkyu Choi3," Biometric Authentication: A Review", International Journal of u- and e- Service, Science and TechnologyVol. 2, No. 3, September, 2009.
10. Ayeni,J.K, Sadiq,K.A, And AdedoyinAdeyinka ," Analysis of a Hand Geometry Based Verification System", International Journal of Scientific Research Engineering & Technology (IJSRET),Volume 2 Issue 6 pp 352-357September 2013 www.ijsret.org ISSN 2278-0882.
11. Pranoti Das, SachinMeshram," An Efficient Hand Geometry System for Biometric Identifications", IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) ISSN: 2278-2834, ISBN: 2278-8735.Volume 4, Issue 4 (Jan.-Feb. 2013), PP 17-19 www.iosrjournals.org
12. Ajay Kumar, David C. M. Wong, Helen C. Shen and Anil K. Jain,"Personal Verification Using Palmprint and Hand Geometry Biometric", J. Kittler and M.S. Nixon (Eds.): AVBPA 2003, LNCS 2688,pp. 668-678, 2003.Springer-Verlag Berlin Heidelberg 2003.
13. K. Saraswathi,B. Jayaram, Dr. R. Balasubramanian,"Retinal Biometrics based Authentication and Key Exchange System",nternational Journal of Computer Applications (0975–8887)Volume 19–No.1,April 201.
14. Samir Nanvati. (2002), Biometrics: Identity Verification in a Networked World, New York: Wiley and Sons, Inc, page 106-112.
15. Edmund Spinella SANS GSEC Original Submission San Francisco, CA Dec 2002 28 May 2003,"Biometric Scanning Technologies: Finger, Facial and Retinal Scanning", © SANS Institute 2003.
16. Lalitha S, Ashwini V, Madhusudhan.K.N, Sachin B S "Person Authentication Using Face And Voice Modalities", International Journal of Advances in Science Engineering and Technology, ISSN: 2321-9009 Volume-1, Issue-2, Oct-2013.
17. Muhammad Nazakat, Dr.Shehzad Khalid, Dr. Imran Siddiqi, "A Review of Offline Signature Verification Techniques ", J. Appl. Environ. Biol. Sci.,4 (9S)342-347, 2014© 2014, TextRoad Publication ISSN: 2090-4274 Journal of Applied Environmental and Biological Sciences www.textroad.com
18. Kalyani R. Rawate, Prof. P. A. Tijare,"Human Identification Using IRIS Recognition", © 2017 IJSRSET | Volume 3 | Issue 2 | Print ISSN: 2395-1990 | Online ISSN: 2394-4099 Themed Section: Engineering and Technology.
19. Alfred C. Weaver, "Biometric Authentication", IEEE Computer Society, Feb. 2006, Volume 39, No. 2, pp.96-97.
20. Javier Galbally, Marta Gomez-Barrero,"A REVIEW OF IRIS ANTI-SPOOFING",Conference Paper · March 2016DOI: 10.1109/IWBF.2016.7449676 https://www.researchgate.net/publication/301258103