International Journal of Electronics Engineering (ISSN: 0973-7383 )
Volume 11 • Issue 1 pp. 1033-1037 Jan 2019-June 2019 www.csjournals.com

# Study on Biometric Authentication, Challenges and Future Research Aspects

[1]Rekha Rani , [2]Narinder singh
[1]Assistant Professor, Department of Computer Science, [2]Assistant Professor, Department of Computer Science
[1]Guru Nanak College, Budhlada, Mansa Punjab, India, [2]Guru Nanak College, Budhlada, Mansa Punjab, India
[1]rekha_ns_kalra@yahoo.co.in, [2] ns_kalra@yahoo.co.in

**Abstract:** Today we come across lot of cases related to cybercrime, data leak, and data manipulation by various unauthenticated persons, personal accounts hacking etc. by reason of conventional password security systems that could be easily hacked. So this has made an even protected framework necessity which could take out these security related issues, the substitute solution for which should have been visible in biometric confirmation technology which couldn't be hacked as this framework comprises of software which recognizes or approves the client by coordinating the information being taken care of with the computerized pictures of the special qualities of the user .This information can't be duplicated or hacked, so it makes the ID more dependable.
**Keywords:** Biometrics, Authentication, Hacking, Iris, Retina.

## 1. INTRODUCTION

In biometrics the words 'bio' meaning is Life and 'matron' meaning is Measurement. It is consequently the recognizable proof/validation by utilization of estimation of a few unique characteristics of the client. So the process of approval of client to sign in to the record or gaining access to individual information etc. by utilizing the remarkable attributes of client for example finger print filter, facial imaging, signature, voice acknowledgment, is the Biometric Identification. Confirmation of Identity happens when the client is enlisted or client's information is already uploading for the software. For this situation the client's feedback information being taken care of is compared and the recently fed input information, if the information for example the physiological or behavioral characteristic matches with currently enrolled characteristic, at that point, the client is checked and permitted to gain access or sign in. In case if the client isn't signed in, and is enrolling firstly, then at that point, the characteristic information is fed and saved in the software for any further access[1].

## 2. RELATED WORK

Earliest form of identification, people has use vision to identify others using their facial images. They scanned by their eyes, as well as recognized their voices by ears and remembered by brain. In last of 19th century, a French police officer named Bertillon, take first steps in technical policing. With the use of human body measurements he had taken of particular anatomical features to identify reoffending criminal, a technique that often proved successful. There are number of technology problem faces by [2], of an undesirable level of mistake recognize.
Some of these limits can be addressed using the exploitation of multimodal biometric systems that incorporate facts from different sources of data. Since this inherent issue, attempting to improve the performance of individual match in these conditions cannot establish successful [3].
Multi-biometric structure incorporates anti-spoofing steps by construction of spoofing several biometric personalities at the same time is difficult. An well-organized fusion scheme, though, is desired to merge the data in the view of different domain experts [4].
According to Mondal and Bours[5], biometrics is a way of deliver detection using identifiable physical assets. It uses body characteristics to instruct data as a tool. Physical characteristics like retinas, irises, fingerprints, palm prints, hand written signatures, voice recognition and facial structure are a only some biometric identification techniques that are currently used [6]. Since the mentioned characteristics are distinctive to each person, biometrics is a feasible solution in fight adjacent to theft and fraud, particularly relating to Internet. The reason behind this advanced application is idea to be improved than using recommendation or PINs as it is not easy to replicate, hack, misplace, biometric characteristics.
Human identification has usually been carried out in utilizing identity cards and passwords. These methods can be violated simply. Passwords may be guessed and identity cards can be robbed, representation them unreliable [7].

An individual's personality can be established out in two behavior verification and Identification. Working of biometric organization is divided in eight stages by Liu and Silverman Start from capturing biometrics than

processing, enroll and biometric template extraction after that data storage in tokens like smart card. Than lively scan elected biometric and processing of biometric, match of biometric with stored data. And last match score is being provide to business application and record of correct audit train in regard to system [8].

## 3. OBJECTIVE OF THE STUDY

Biometrics are more suitable and give better security than other traditional schemes for human recognition. In some applications, biometrics can addition current techniques. This paper provides a study of the existing biometric technologies, challenges and future scope their cons and pros that are used in real life to solve various types of problems. The rest of paper is organized as: Section 4 is the classification of biometric and their challenges, Section 5 are the advantages and Section 6 disadvantages of biometric systems. Section 7 future work and conclusion the paper.

## 4. BIOMATRICS TECHNOLOGIES AND CHALLENGES

This system gives better quality then the conventional Password or some other Identity or based systems as:

1. The person has no need to carry any ID card or remembering any pin code.
2. The person in regard needs to be present at the point of time and place, the system is one to one interface, so more secure.
3. Biometric verification can be characterized into two classes of distinguishing proof plans:

A. Social attributes

B. Physiological trademark

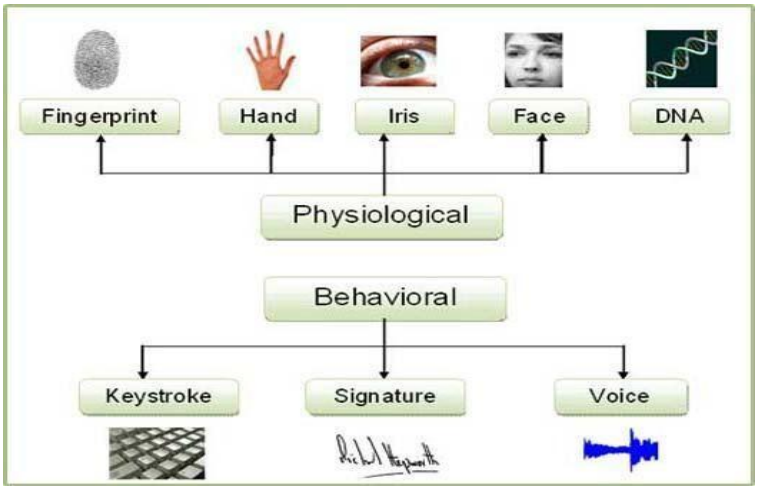


Fig-1: biometrics Technologies

**Eye Scanning**

In the eye scanning two methods are recognition:

Iris Scanning: In the retinal scanning there is no need for a person to be close to the scanning device this technique use a camera for image generation. The iris designs are gotten through a video based imaging system. The image so gains is analyzed by the device. Every image have 266 distinct spots, these spots depend on the attributes of iris. The iris is steady all through the life [9].

Retina checking: same as the iris scanning a client needs to search in a device that performs laser-examining of his retina. The device examines configuration of blood vessels of client. The configuration of blood vessels an individual is unique. It represents a trouble as client needs to fix a point till the laser is examining his eye [10].

**Challenges**: It has to be creating to differentiate or identify individual wearing lens or glasses.

**Fingerprints Identification**

Biometric is an oldest method of security. One of the main purposes for fingerprints is to assist investigators with connecting one crime scene to other affecting a similar person. In this technology the digital image of finger prints is carried out. Finger print scanning machine have sensors which senses the unique bifurcations, curves of

the skin of fingers [11].

**Challenges**: The rate of recognition of finger print is based on biometric recognition system degrade significantly at the time when finger is wrinkled and wet. The collision of wrinkled and wet finger on biometric machine fact has not been fine addressed yet.

**Facial recognition**

Facial recognition is an approach to recognizing or affirming a person's character using their face. Facial recognition system is utilized to recognize individuals in photographs, recordings, or regular activities.
Facial acknowledgment is a class of biometric security. Different types of biometric software incorporate voice acknowledgment, finger impression etc. Eye retina scanning or iris scanning is also included in facial recognition. The method is usually used for security purpose.

**Challenges**: Facial recognition suffers from number of challenges including facial rotation, distinction in lighting circumstances, person wearisome collusions likes eye glasses, scrap, hat, etc., and also various face expressions degrade performance of system. Research requirements are more focused to address every issue in order to extend a reliable and robust recognition system.

**Handprint Imaging**

Among various body scanning techniques, hand-print has attracted to the researchers somewhat recently and many papers have been introduced in view of it. There are a few reasons which have caused the popularity of hand printing methods. High user acceptance, High accuracy, Stable line elements, and Low-resolution imaging are the most important factors of hand print [12].

**Challenges**: identification rate degrades at time when a person use artificial body odors like gloves.

**Palm print Recognition**

Features like principle orientation, lines, vein geometry ridges, minutiae and creases, are extract for detection. For different persons, p*alm print recognition* is distinct. For verification, hand is positioned on the device screen, infrared lights are used for scan the palm. It captures image of hand, a pattern of palm is extracted, which is the bright or dark pattern. The darker pattern is formed due to absorbing of infrared light by palm of hand. A stencil of this biological pattern is saved in device. This image is transformed into digital image by transducer for comparison purpose.

**Challenges**: Research have to be advanced to address the impact of wet and wrinkle palm on recognition rate.

**Deoxyribonucleic acid (DNA) Analysis**

This technique of authentication is generally used in criminal cases. Deoxyribonucleic acid of the user in form of tissue, blood, nails, hair, is gathering to confirm. Deoxyribonucleic acid analyzing take time. Deoxyribonucleic acid as well is exclusive quality but a nail or hair can be stolen.

**Challenges**: This technique is not acquisition and automatic method must be developed.

**Voice Verification**

In this method, user is asked to tell a slogan or a secret pin. His voiced character are considered both physiological and behavioral characteristics. The authentication process is different from voice recognition process. In authentication taster of speaking mode pattern is saved and evaluated with the similar person's speech although recognition is rather numerous to one or one too many process [13].

**Challenges**: Research have to be advanced to minimize the memory requirement to store unique code. The identification rate degrades in case person’s tone of voice changes like when he emotional or sick.

**Signature scanning**

Signature scanning is the dynamic comparison of time taken for signing, signature size, shape, pressure applied, writing speed etc. although signature may be copied however the traits as signing may not be.

International Journal of Electronics Engineering (ISSN: 0973-7383 )
Volume 11 • Issue 1 pp. 1033-1037 Jan 2019-June 2019 www.csjournals.com

**Challenges**: with long period reliability, lack of accuracy and cost are main issues to be generated in this technique.

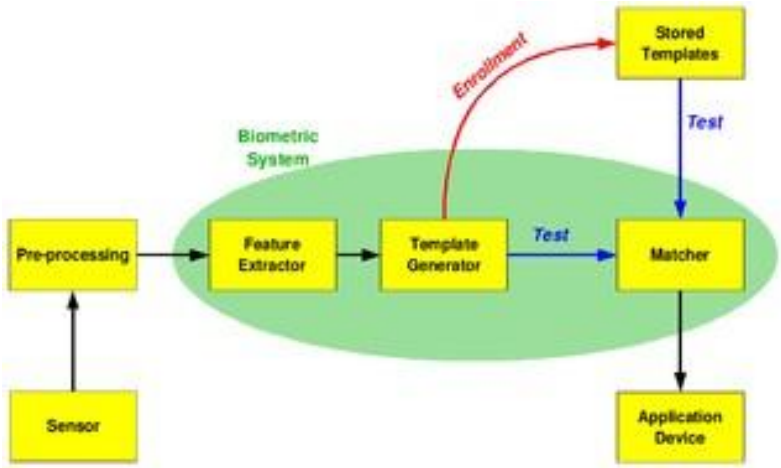


Fig-2: Mechanism of biometric operation

## 5. PROS OF BIOMETRIC AUTHENTICATION

1. No remembering of passwords or login ID's is required.
2. Better alternate of saving time and resources.
3. Only Legitimate user can get access to the personal data or accounts.
4. Elimination of need of carrying authorized documents

## 6. CONS OF BIOMETRIC VERIFICATION

1. Some of these methods are limitation for physically challenged people.
2. Changing of amount of light entering into eye due to pupil contraction may lead to system showing error.
3. DNA analysis takes time, retina scanning requires expensive device.
4. Some characteristics of face or palm may change with time and age.

## 7. FUTURE TRENDS

As biometric techniques expand and grow, number of methods is also being developed in order to recognize a person correctly. Trends have begin to appear in following main areas [14].

• Palm print and Fingerprint recognition techniques together will be major biometric in predictable future to law enforcement depend on.

• Facial identification shall be improved investigative and intelligence use. Though, law enforcement shall not be use face identification for confirmation in coming period [15].

• Palm printing may be use with better investigation in near future.

• Multimodal biometrics, cataloged is merged two or more biometrics achieve highest accurateness of recognition or verification

• Cooperation is a most important present trend. As cooperation is strength of character enforcement agencies, biometric information requires to be shared between them.

• Obtaining passive biometric information will be future trend of biometric. Collecting and comparing biometrics passively without any interaction by human is very exciting.

## 8. CONCLUSION

The biometric system may find applications in attendance system, security systems, and identification purposes and may find even more applications in the time to come. The prevalent systems would be worked upon and modified for error free secure system. The accuracy levels need to be increased for efficient security system. Proper selection of technique has to be considered according to the requirement. Scientific work is being carried out for future applications and progress in the biometrics.

**REFERENCE**

[1]. Debnath Bhattachary,et.al. "Biometric Authentication: A Review", International Journal of u- and e- Service Science and Technology, September 2009 [1]

[2] Abozaid, A., Haggag, A., Kasban, H., & Eltokhy, M. "Multimodal biometric scheme for human authentication technique based on voice and face recognition fusion", Multimedia Tools and Applications, 78(12), 2019.

[3] Ahmad, S. M. S., Ali, B. M., & Adnan, W. A. W. "Technical issues and challenges of biometric applications as access control tools of information security", international journal of innovative computing, information and control, 8(11), 2012.

[4] S. Latifi, Nimalan Solayappan, "A Survey of Unimodal Biometric Methods", Published in Security and Management 2006.

[5] Mondal, S., & Bours, P. "A study on continuous authentication using a combination of keystroke and mouse biometrics" Neuro computing, 230, 2017.

[6] Anil K. Jain, Salil Prabhakar, "An Introduction to Biometric Recognition", IEEE transactions on circuits and systems for video technology, 14(1), 2004

[7] Jain, A., Bolle, R., & Pankanti, S. (Eds.) "Biometrics: personal identification in networked society", Springer Science & Business Media (Vol. 479) 2006.

[8] Liu, Simon, and Mark Silverman. "A practical guide to biometric security technology." *IT Professional* 3.1, 2001.

[9]. Sanjay R. Ganorkar, Ashok A. Ghatol, "Iris Recognition: An Emerging Biometric Technology", In Proc. of the 6th WSEAS International Conference on Signal Processing, Robotics and Automation, Greece, 2007.

[10]. Pramodini Punde, et.al., "A study of eye tracking technology and its applications", 1st International Conference on Intelligent Systems and Information Management (ICISIM), 2017.

[11] L Karthik Narayan , Sonu. G , Soukhya S. M, "Fingerprint Recognition and its Advanced Features", IJERT, 2020.

[12 Khamael Abbas, Aiman Al-Sabaawi "Handprint Recognition Technique based on image segmentation for recognize", International Journal of Computer Information Systems, 2(6), 2011

[13] Kar, B. Kartik, B. Dutta, P.K. "Speech and Face Biometric for Person Authentication", In Proc. of IEEE International Conference on Industrial Technology, India, 2006.

[14] Massimo Tistarelli and Marks Nixon, "Advances In Biometrics", Springer-Verlag Berlin Heidelberg 2009.

[15] L. Hong, A. K. Jain, "Integrating faces and fingerprints for personal identification," IEEE Trans. Pattern Analysis Machine Intell., Vol. 20, 1998.