"A SURVEY OF BIOMETRIC AUTHENTICATION TECHNIQUES"

ANKUSH DESHMUKH[1], POONAM HAJARE[2], RAJESHRI KACHOLE[3],AMITKUMAR MANEKAR[4]
[1,2,3] Department of Computer Science And Engineering SSGMCE Shegaon, Maharashtra, India.
deshmukhank@gmail.com[1]
hajarepv123@gmail.com[2]
rajeshrikachole2012@gmail.com[3]
asmanekar24@gmail.com[4]

ABSTRACT: *Security is not a single layer issue. Now a day's only passwords, cards, or other keys are not sufficient to provide high level security. So we need to upgrade our security standards. We need something that cannot be stolen or copied. To resolve this problem another level of security comes into picture that is biometric security. Biometric security identifies an individual on the basis of distinctive biometric characteristics that may be a fingerprint, face, DNA, or any other unique character. Biometric identification becomes important part of today's security systems. Many countries are accepting the biometry based personal identification of their employees in various departments like armed forces, national security departments etc to prevent important national information secure. This increases the importance of biometrics in the field of security. Now a day IT companies are also moving towards the biometric security to avoid unauthorized access to their data and much commercial software***.**

Keywords: Security , Biometric, Authentication, Fingerprint
.

1. INTRODUCTION

The biometric identification and/or verification system works on the basis of template matching. At the time of registration any biometric system takes the biometric characteristics as input and generates a template from them and at the time of verification it takes the biometric characters as input and again generates the template and match with the template generated at the time of registration. Depending on the results of template matching the verification of an individual is done. The biometric characters may be physiological or behavioral. The shape of body such as pattern of fingerprint, face, palms, eyes and DNA etc are considered as physiological characters of humans and behavioral characteristics are nothing but the way of typing, signature, voice etc. Today's technology is using some behavioural and/or physiological biometric characters for identification and verification of users such as fingerprint, DNA, face detection method, identification on the basis of iris of user, signature identification (Digital signature), voice based identification method, ECG and body odder based identification system. These technologies are upgrading the standards of today's security system in all directions [1].The reasons behind fast adaptation of the biometric authentication system in large number is the features provided by biometric system like, universality, performance, uniqueness, measurability, acceptability. Universality identifies each user of it uniquely. It sufficiently distinguishes one person from emaining population. Performance is related to speed of operation and robustness in operation. Uniqueness is nothing but how uniquely the system identifies the each user. Measurability is nothing but ease of measuring the traits. Performance is related to speed of operation and robustness in operation. Acceptability means how eagerly users accept it [2].

2. WORKING OF BIOMETRIC AUTHENTICATION TECHNIQUE

The working of all the biometric authentication technique uses the same patterns shown in figure (1). The whole biometric system is divided into three sub modules i.e. registration, verification and result. At the very first stage of system i.e. registration, a new user needs to get registered into database. In process of registration system ask for biometric characters of a user. The system applies the certain algorithm on the input feature and converts them into template and stores them in database. In second sub module the verification is done. In this module the user who wants to get identified provide his biometric characters and then the system will apply the exactly same algorithm to generate the template from it which was previously applied at the time of, registration. Templates never contain all the information, it only contain the minimum required information to identify the user uniquely. In third and final sub module depending on the result of previously stored and new generated template matching the authentication is done [3].

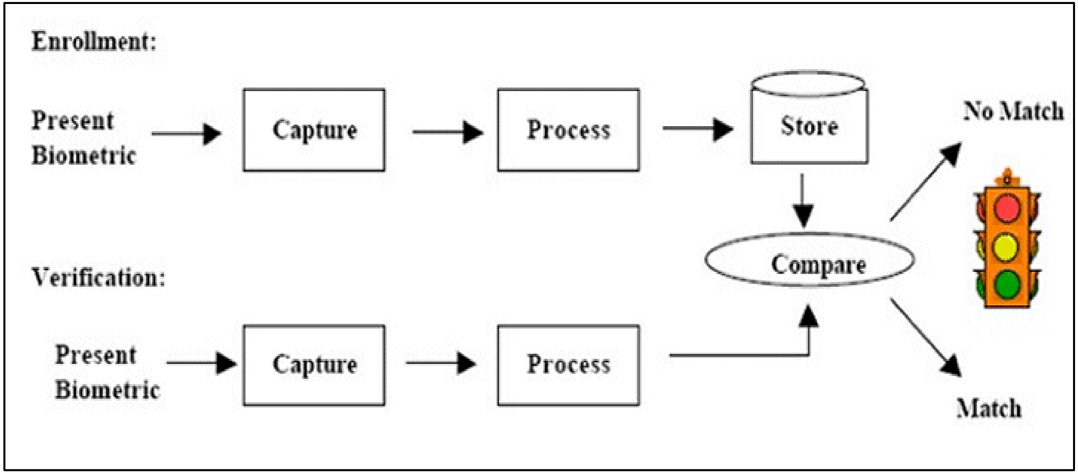

Figure 1: Biometric Authentication Process [7]

3. OVER VIEW OF TODAY'S AUTOMATED BIOMETRIC AUTHENTICATION TECHNIQUES

There are various biometric characteristics (physiological and behavioural) that can be separately used to develop biometric identification system like fingerprints, face detection, iris based identification, voice detection, DNA matching and many more. Each system has its own advantages and disadvantages. Each system is supposed to efficiently meet all the requirements of user. The selection of system is depends upon the need of application and the security level needed [4].

a. FINGERPRINT BASED AUTHENTICATION

Fingerprint based authentication technique is the most well known and widely used biometric identification and verification system. Due to uniqueness and persistence in fingerprints of an individual, the fingerprint based authentication technique is most reliable, secure and long lasting biometric authentication technology. This technique uses patterns of finger of an individual's (as shown in fig (2)) to identify them uniquely. Pattern mainly consists of ridges and minutiae positions in fingerprint image. The three crucial patterns of fingerprint ridges are arch, loop and whorl. In arch the ridges starts from the one side, rise in the middle forming an arch and then exit on the other side of finger. In loop pattern the ridges starts from one side of a finger, form a curve and then exit on the same side of finger. And in whorl type the ridges form circularly around a central point of finger.

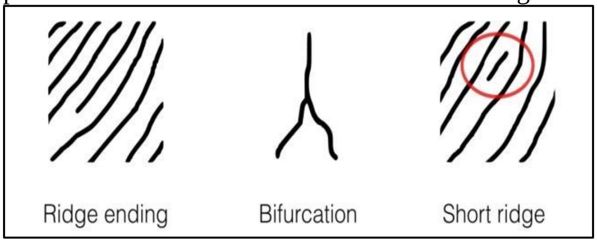

Figure 2: Fingerprint Patterns

To calculate minutiae points from fingerprint image the two most important characteristics of ridges are ridge ending and ridge bifurcation. Ridge ending is end or start of a ridge. And ridge bifurcation means a point where a ridge gets divided into branches. Those points i.e. a point where ridge finish or ridge split are precise as minutia point and on the basis of arrangement of minutiae points the verification is done between saved image and currently scanned image of fingerprint of an individual.

b) FACE DETECTION BASED AUTHENTICATION

Face detection is one of the biometric identification techniques which uses facial features such as position and shape of eyes, nose, mouth etc. Figure (3) shows the landmarks on the face of human beings. Facial identification is one of the simple and easy techniques for biometric identification. Generally face detection algorithm uses one of the two main face detection algorithm strategies for identification and verification of an individual. One is geometric strategy. Geometric strategy work on the geometry i.e. position and shape of chin, lips, eyes and other parts of the face and interrelationship between them. And second strategy for face detection algorithm is photometric algorithm. This algorithm converts the image into pixel values and then generates the template from those values. This algorithm is static in nature.

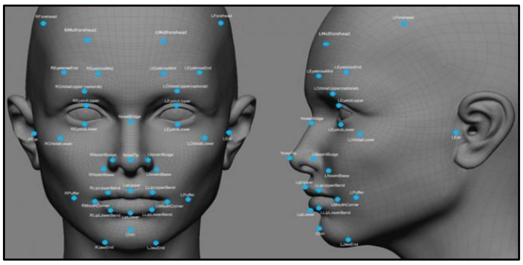

Fig (3): Landmarks Used In Face Detection Method

c) HAND GEOMETRY BASED IDENTIFICATION

Hand based identification is the another biometric identification method which identifies an individual on the basis of geometric features of hand like height and width of fingerprint, diameter of palm and he total perimeter of hand. The pictorial view of this system is as shown in the figure (4). This technique is simple and very easy to use. This technique does not provide very high level of security. The changing weather and skin problem can affect the accuracy of the hand geometric based identification technique. The accuracy of system can be affected by various problems such as change in shape of hand and some other physiological changes in body. This technology is mainly accepted in low level security applications. Since only the geometry of hand is unable to identify the mass of users uniquely this system has many drawbacks in it [6].

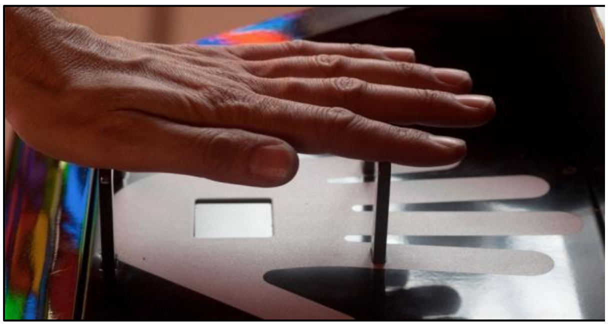

Figure 4: Hand geometry identification system

d) RETINA

Retina is nothing but the posterior part of human eye. The complex structure of eye retina is able to identify each and every individual from each other. The retina consists of vast and complex network of capillaries that makes retina different from the retina of other individual. Figure (5) shows the complex structure of retina. Capillaries are like pipes that provides blood to eye. Each individual has a unique structure of capillaries. Retina based identification technique uses this network to identify an individual separately. The retina based identification technique is very complex and used where very high security is required. The structure of eye retina is remains unchanged from birth to death. Only exception to this is diseases like diabetes, glaucoma, and other retinal degenerative disorder can make some changes in the structure of retina. The neural network of retina is so unique that twin's child also has the different structure.

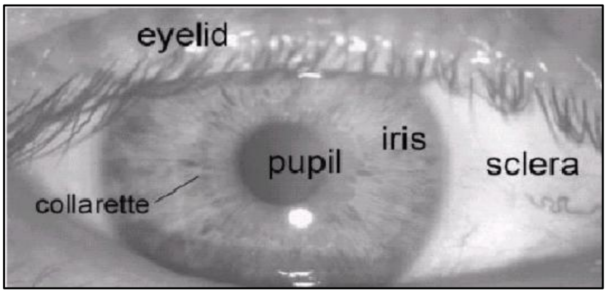

Figure 6: Structure of Human Eye [7]

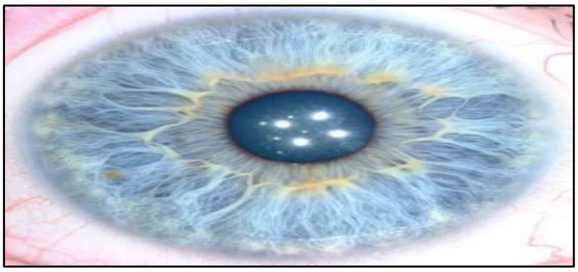

Figure 5: Structure of Eye Retina [7]

To capture the capillary network as shown in fig (5) of eye, the user needs to peep into an eye-pipe and concentrate on a particular point for specific period of time. The image captured in this process cannot be directly used for template generation. The image requires going through various image enhancement algorithms. Due to this kind of complex mechanism this technology is not accepted on much large amount in today's biometric security system.

e) IRIS BASED IDENTIFICATION

During the pre development of human child, at being a thin circular shaped structure stars to develop around pupil of eye. The purpose of that thin circular network is to control the thickness and dimension the structure of central part of eye i.e. pupil which indirectly control the amount of light reaching t to the retina. The development of iris starts during pre development of child and ends at the age of 2 years old. The structure of iris never changes during the whole life of an individual. It is near to impossible to change the iris by surgery and it is very easy to identify the duplicate iris. Due to these reasons the iris identification is one of the best biometric identification systems.

The human eye contains the parts as shown in the above figure fig (). The iris scanning algorithm needs to eliminate the reflections from various parts as eyelids, eyelashes; many other fake reflections and only identify the pixels of iris. After identifying the iris pixels, the algorithm creates the bit pattern for template generation. And this template is them get stored into database and used at the time of verification.

f) VOICE BASED IDENTIFICATION

Voice is also a one of the biometric character or feature of human beings. A voice based identification system uses various characteristics that are called as the voice biometrics of voice. Two voices are differentiated on the basis of auditory characters of two vices. These auditory characters consists of two parts first is anatomy and second one is learned behavioural pattern. The anatomy characters deals with shape and size of throat and mouth, and learned behavioural patterns deals with voice pitch and speaking style.

Physiological part of human voice are remains constant but he behavioural patterns of speech get changed with the environmental conditions, emotional condition of speaker, age of speaker and many other medical conditions. Due to this reasons the voice based identification system is not that much reliable as compared to other biometric identification systems present today. Only the voice of person is not able to identify him uniquely in the mass of people. One of the main is disadvantage of voice based identification is background noise [4].

g) DNA BASED IDENTIFICATION

Deoxyribonucleic acid i.e. (DNA) identification and/or verification system provides the highest level of biometric security. The possibility of DNA replication is 1 person in a 6 billion. That makes the DNA identification at highest level. DNA encodes the basic instructions used in the growth of all living organism as well as viruses. It is all most distinct biometric identification for human beings except for monozygotic twins. Monozygotic twins are born when a particular egg is fertilized create one zygote which then divides into two separate embryos [9]. The anther advantage of DNA is that it never changes through life of a human being. The figure (7) shows the structure of DNA.

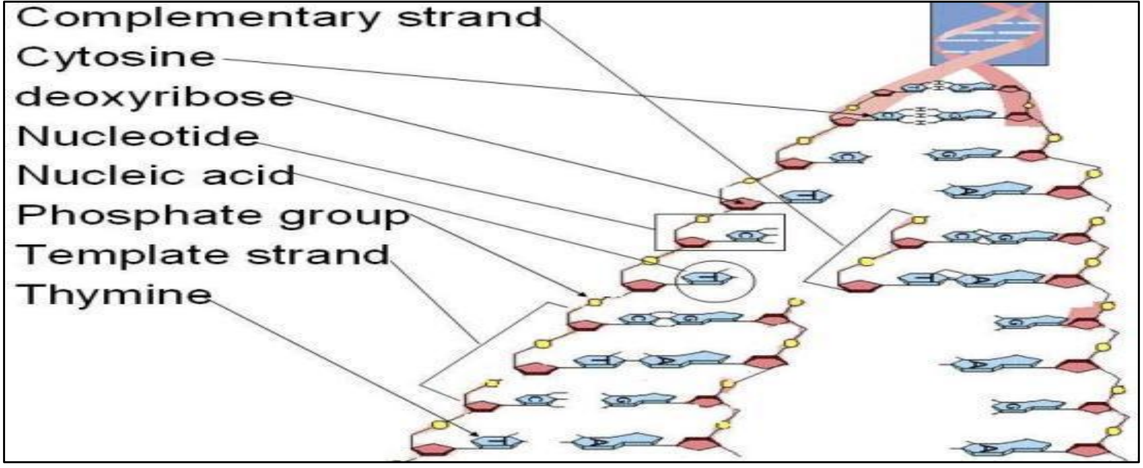

Figure 7: Structure of DNA [10]

The current DNA obtaining method need blood tissue or tissue from other part of body like DNA in blood, semen, skin, saliva or hair. In DNA profiling, the lengths of changeable sections of cyclic DNA, such as short tandem repeats and minisatellites, are compared between people. The acceptability of DNA based identification system is not adopted on large scale due to various reasons like, DNA matching can no performed at run time, DNA sample stored in lab needs more security and it is too costly also.

H) SIGNATURE BASED IDENTIFICATION SYSTEM

Signature based identification is mostly used identification system used today. This technique is accepted in various departments like government departments, commercial transaction such as banking and many others. This system uses the way in which person sign his/her name for identification. Today's signature recognition systems are also able to measure pressure and velocity of the point of the stylus. Signature reorganisation system can work in two ways one is static and second is dynamic. In static way the user needs to give his/her signature on paper and digitalized it using camera or scanner and them biometric system analyze for shape and size, and in dynamic mode user needs to put his/her signature directly on the digital writing pad and result is given at run time.

i) KEY STROKE BASED IDENTIFICATION

Identification system which uses the way of typing i.e. speed of typing alphabets, pressure on keys, and rhythm of typing is known as keystroke based identification. Only that much information is not sufficient to identify an individual in mass public, but this technique offer enough inequitable information to permit verification. This technology also uses pressure on the keys and timing information of keys up/hold/down events.

j) PALM PRINT BASED IDENTIFICATION

Similar to pattern on the fingerprint, the palm of human also contain the unique pattern which can be used for identification and verification purpose. The area of a palm as compare to area of fingerprint is more so the capacity of palm for identification is also mare. Since area is more a palm cannot be scanned using fingerprint scanner it needs a special palm scanner device. The human palm also contains the features which are unique to the individuals. The palm contains principle lines and wrinkles which are helpful in identifying person [11]. Using high resolution scanner the geometric features of human palm like height, width, length of palm can be calculated. Palm also contains ridges and valley from those minutiae points can be calculated. Using all this information together a system with high level security can be develop [4].

COMPARISON OF VARIOUS BIOMETRIC AUTHENTICATION SYSTEM
H: HIGH, M: MEDIUM, L: LOW [4]

Biometric Characteristics	Universality	Uniqueness	Permanence	Measurability	Performance	Acceptability	Circumvention
Finger print	**M**	**H**	**H**	**M**	**H**	**M**	**M**
Palm print	**M**	**H**	**H**	**M**	**H**	**M**	**M**
Hand Geometry	**M**	**M**	**M**	**M**	**M**	**M**	**M**
Iris	**H**	**H**	**H**	**M**	**H**	**L**	**L**
Retina	**H**	**H**	**M**	**L**	**H**	**L**	**L**
Face	**H**	**L**	**M**	**H**	**L**	**H**	**H**
Voice	**M**	**L**	**L**	**M**	**L**	**H**	**H**
Signature	**L**	**L**	**L**	**H**	**L**	**H**	**H**
Keystroke	**L**	**L**	**L**	**M**	**L**	**M**	**M**
DNA	**H**	**H**	**H**	**L**	**H**	**L**	**L**

4. CONCLUSION

In today's digital world the acceptability of the biometric identification system is increasing more and more. All the features provided by biometric system such as uniqueness, persistence, universality etc makes it more powerful. The biometric security provides the higher level of security than the system with password, cards, or other keyword. The main objective of this paper is to provide abstract overview of currently used biometric identification and/or verification systems present in today's society. This paper also concludes that, security level required by todays Society can be fulfilled by various biometric security systems.

5. REFERENCES

[1] James Wayman, Anil Jain, Davide Maltoni and Dario Maio, "An Introduction to Biometric Authentication Systems". In Biometrics: Technology, Design and performance evaluation. Springer Publications. ISBN 978-0-7923-8345-1.

[2] Jain, A.K.; Bolle, R.; Pankanti, S., eds. (1999). Biometrics: Personal Identification in Networked Society. Kluwer Academic Publications. ISBN 978-0-7923-8345-1.

[3] QinghanXiao Biometrics—Technology, Application, Challenge And Computational Intelligence Solutions, May2007|Ieee Computational Intelligence Magazine.

[4] A. K. Jain, A. Ross, S. Prabhakar, "An Introduction to Biometric Recognition", IEEE Trans. on Circuits and Systems for Video Technology, Vol. 14, No. 1, pp 4-19, January 2004

[5] www.extremetech.com

[6] Kresimir Delac, Mislav Grgic, "a survey of biometric recognitionmethods", 46th International Symposium Electronics in Marine,ELMAR-2004, 16-18 June 2004, Zadar, Croatia.

[7] THE HUMAN EYE ADAPTIVE OPTICS, HTTP://WWW.INTECHOPEN.COM

[8] Mehrchilakalapudi.woedpress.com

[9] http//en.wikipedia.org

[10] www.teacherweb.com

[11] D. Zhang and W. Shu, "Two novel characteristic in palm print verification: Datum point invariance and line feature matching," Pattern Recognise, vol. 32, no. 4, pp. 691–702, 1999.

[12] Hand geometry – Eter – Biometric Technology, http://www.eter.it

6. AUTHOR PROFILE

	Ankush S. Deshmukh Pursuing 3rd Year BE at SSGMCE Shegaon
	Poonam V. Hajare Pursuing 3rd Year BE at SSGMCE Shegaon
	Rajeshri V. Kachole Pursuing 3rd Year BE at SSGMCE Shegaon
	Amitkumar S Manekar working as assistant Professor in IT Department SSGMCE, Shegaon. His research area is Big Data analysis and High performance Computing. He has guided many Under Graduate and Post Graduate Students