Comparitive Study on Biometrics: a Review

Aditi Verma *	**Meha Khera**
M.Tech. Student, CSE Dept.	*Assistant Professor in CSE Dept.*
PDM College of Engineering for Women, India	*PDM College of Engineering for Women, India*

Abstract— This paper gives a review about various biometric technologies such as finger printing, face recognition, iris scan, retina scan and many more. Biometrics provide higher level of security rather than just using passwords or PINs which can easily be misused. Advantages and limitations of using various biometric technology has been covered and some future advancements in this field.

Keywords— Biometrics, Authentication, Finger print, Iris, Retina etc.

I. INTRODUCTION

Information Security plays an important role in computer system. In order to protect our data we use username and passwords or PINs which are even not secure enough. Authentication is the method of establishing any person's identity, that is, he is what he claims to be. Biometric authentication is to use personal characteristics in order to authenticate themselves. There are various types of biometric authentication schemes like fingerprint, face, hand geometry, voice, iris etc.

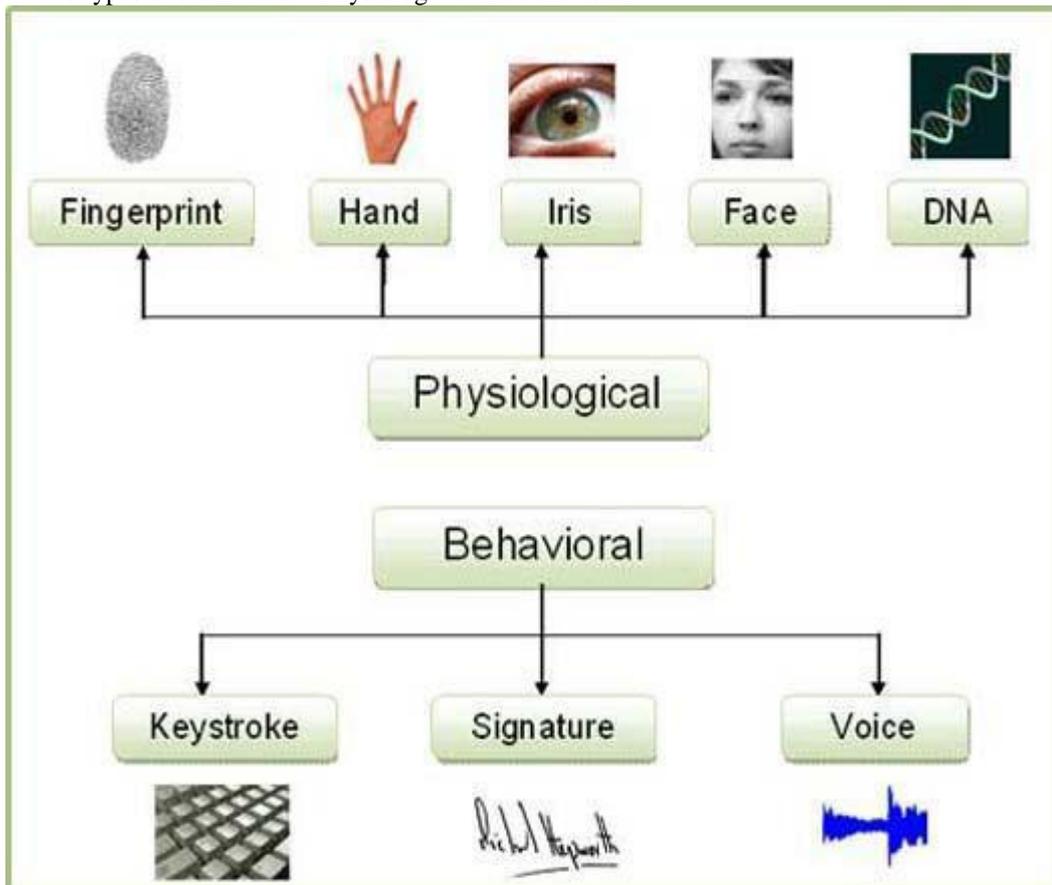There are two types of biometrics: - Physiological and behavioral.

Fig 1 Types of Biometrics

The biometrics are connected to an individual and cannot be forgotten, stolen or shared. If we use PINs or passwords people tend to use easy passwords which can easily be hacked by some intruder and if some person use difficult password and they may tend to write it somewhere which can also be stolen by any illegitimate user. So, biometrics has this advantage that they cannot be stolen or misused. Biometric is considered to be very secure.

II. FINGER PRINT SCAN

It is a kind of biometric that is very much secure as every person's finger print scan is unique and cannot be forged easily. Even the identical twins have different finger prints. It is the oldest biometric used. It is said that fingerprints of a child starts to develop when the child is inside the mother's womb. That's why they are unique. Finger prints have unique patterns and characteristics. They are made up of lines and spaces. Lines are called ridges and spaces between ridges are called valleys. Finger prints also have three types of patterns- arches, loops, whorls. Arch is a pattern where ridges enter on one side of a finger and exit on the other side. Loop is a pattern that enters and exit on same side of finger. Whorl swirls around the central point called core. Finger print ridges have three types of features: - ridge endings, short ridges and bifurcations.

Fig 2 Finger print scan

The traditional and oldest method of capturing finger prints is by using ink. But now optical finger print readers are commonly used. Ultrasound finger print is quite rare. Ultrasound is used to monitor the figure surfaces, user places the finger on a piece of glass and the ultra sonic sensor moves and reads whole finger print. This process would take about 1or 2 seconds. There are five stages in finger scanning:-

A.   *Finger print image acquisition*
   At this stage, finger print of the person is taken by any of the above methods.
B.   *Image processing*
   Finger image is converted into a usable format. It consists of black ridges and white valleys.
C.   *Location of distinctive characteristics*
   At this stage, dirt, sweat, scars are removed from the image in order to enhance it.
D.   *Template creation*
   Template is created and stored. Template has enormous features that will later on match to check if a person's finger print matches or not.
E.   *Template matching*
   Matching is performed in this stage.

There are two matching techniques: - Minutiae based and Correlation based.
There is a weakness of finger scanning that is if the weather is cold, it becomes difficult to capture finger prints.

III. FACE RECOGNITION

Face recognition consists of various facial attributes such as eyes, eyebrows, nose, lips, chin and their relationship. It basically focuses on positioning of these attributes. There are two types of face recognition protocols: - face verification and face identification. Face verification is used to authorize the person and Face identification is used for matching input with registered input. This technique is quite widely used now-a-days in various smartphones.

Fig 3 Face scan

This technique has got some drawback also. Firstly, intruder can easily copy registered user's photo from any social networking site and can easily get access into the system. Secondly, identical twin's photo can also be used to login into the system.

IV.   RETINA SCAN

Retina is a surface at the back of the eye that processes the light entering into the pupil. It is based on the blood vessel pattern in the retina of the eye. It is a very unique biometric. This technology is still in its research stage.
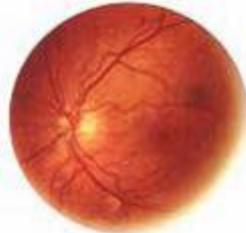

Fig 4 Retina of eye

V.   HAND GEOMETRY

It is based on the length, width, thickness of hand and surface area of the hand. Methods used are mechanical and optical principle. It includes the measurement of size and shape of palm and length of fingers. This technique is not commonly used so far.

Fig 5 Hand scan

VI.   VOICE

Voice of a person is recorded using a VOCODER or by using microphones. Voice of a person can be recorded in just 3 seconds because pitch of voice varies from person to person. This authentication system is also not that secure that's why it is not been used extensively.

VII.   IRIS

This feature is very unique and will remain stable over a person's lifetime. Iris of the eye is the colored area that surrounds pupil. Iris is a combination of corona, crypts, filaments, freckles, pits, furrows, striations and rings. Even left and right irises can be treated as individual unique identifier. Identical twins have different pair of irises. This feature is very much unique and it is considered to be quite secure. Image of iris is taken by a special gray scale camera.

Fig 6 Iris scan

VIII.   SIGNATURE VERIFICATION

In signature verification, signature dynamics are noted. Dynamics means the pressure, direction, acceleration and length of strokes, number of strokes and their duration. All the above characteristics are noted.
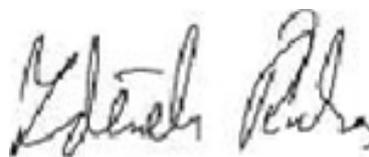

Fig 7 Signature scan

IX. OTHER TECHNIQUES

There are few techniques that are very rarely used.

A.   Palm print

It uses optical readers similar to finger print scanning. It is not as popular as finger scanning. It cannot be used in mobile devices because of its size.

B. Hand vein

Veins under the skin absorb infrared light and thus have a darker pattern of the image of hand.

C. Thermal imaging

This technique is similar to the hand vein. It also uses infrared source of light and camera to produce an image of the vein pattern in face or wrist.

D. Ear shape

Ear shape verifier also called optophone is a telephone type handset within which is a lighting unit and canvas which captures two images of camera.

E.   Body odor

Every human's smell is unique. Each human smell is made up of chemicals called as volatiles. Smell of a person is captured by sensors that are capable of obtaining odor of any body part.

X.   CONCLUSION

Biometric authentication should be implemented in various firms in order to promote security and to prevent valuable stuff from being attacked. There is scope for research that can also be done in this field and the limitations that come across while using these biometrics can also be reduced.

REFERENCES

[1] Debnath Bhattacharyya, Rahul Ranjan, Farkhod Alisherov A. and Minkyu Choi, Biometric Authentication: A Review International Journal of u- and e- Service, Science and Technology Vol. 2, No. 3, pp 13-28, September 2009

[2]   Markus Jakobsson and Sebastien Taveau, The Case for Replacing Passwords with Biometrics

[3] Sulochna Sonkamble, Dr. Ravindra Thool and Balwant Sonkamble, Survey of Biometric Recognition Systems and their Applications Journal of Theoretical and Applied Information Technology, pp 45-51

[4] Edmund Spinella, Biometric Scanning Technologies: Finger, Facial and Retinal Scanning, SANS Institute, San Francisco, CA Dec 2002, pp 1-13, 28 May 2003

[5] Donny Jacob Ohana, Liza Phillips and Lei Chen, Preventing Cell Phone Intrusion and Theft using Biometrics IEEE Security and Privacy Workshops, pp 173-180, 2013

[6] Yesha Pruthi, Harsha Singh and Aditi Verma, A Comparative Study on Biometric Technology, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 1, pp 993-996, January 2014