IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 11, Issue 4, Ver. I (Jul.-Aug .2016), PP 25-30
www.iosrjournals.org

A Review on Different Biometric Techniques: Single and Combinational

[1] S.sravan Kumar, [2] N.Anand Ratnesh
[1] *Assistant professor, Dept of ECE, RVR&JCCE, A.P, India.*
[2] *Assistant professor, Dept of ECE, RVR&JCCE, A.P, India.*

Abstract: *In this paper comparison of different biometric techniques are shown. Here we propose a new method called combinational biometrics (combination of two or more biometric techniques) for providing better security and authentication.*
In present day scenario security systems are essential almost everywhere, especially in commercial areas and educational institutions to provide such security, biometric systems are essential. A brief introduction of every biometric technique is also written and the results are compared with one another to choose the best biometric technique or combination.
Keywords: *biometrics, authentication, security, combinational biometrics.*

I. Introduction

In the ever-changing world of global data communications, and fast-paced software development, security is becoming more and more of an issue. No system can ever be completely secure, all one can do is make it increasingly difficult for someone to compromise the system. The more secure the system is, the more intrusive the security becomes. One needs to decide where in this balancing act the system will still be usable and secure for the purposes.

Here we have discussed different Biometric tools and related security issues [1]. Biometrics are nothing but methods to identify a human uniquely based on their psychological or behavioural characteristics in which psychological traits include facial features, iris, retina, and behavioural traits include voice, gait, keystroke. This identification method is preferred over traditional methods like passwords or pins because it has several advantages like the person who has to be authenticated has to be physically present and no other person can authenticate for him .in the modern day as the usage of computers increased exponentially there are lot of pins and passwords we have to remember, so biometrics can take the place of the traditional methods to make the life easier for the human beings [2]. There are many ways to identify the identity of a person such as finger print, voice, retina signature, face recognition and we all know that there is no perfect security system yet. Every system has its pro's and con's we will see each of them in detail to seek the more advantageous one.

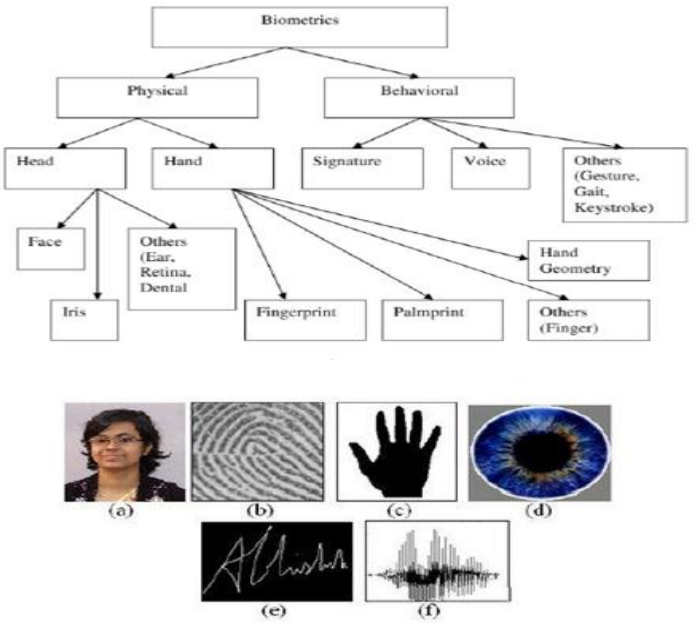

Figure1. a) Face b) Finger Print c) Hand Biometry d) Iris e) Signature f) Voice.

II. Different Methods Of Biometry

Finger print: These are minute ridges or patterns which are round in shape which are at your fingertips no two (even twins) will doesn't have same kind of patterns at their fingertips. These patterns are formed on our fingers at the time of eight month in the mother's womb and remain unchanged throughout the life. Until now this is the most used technique across the world which is simple and reliable.

- Cuts or scars or burnt accidents can have negative effect on the results.
- Can be cheated at the training itself by taking two finger impressions of a person and can be treated as two persons because they are not identical

Figure 2: A simple fingerprint

Voice recognition: Speech is more simpler way of proving your identity because you don't need to touch the machine also you can talk and verify yourself as if you are talking to your friend these speech features different for different people and these features can be extracted by several feature extraction methods such as MFCC, LPC etc .Though proper care is needed to be taken care during the training

- This way of identity can vary in the high noisy environment
- This system may not produce accurate results when the person is suffering from cold or throat problems

Figure 3: Voice transmission over a biometric machine.

Face recognition: A facial recognition system is a computer application for automatically identifying or verifying a person from a digital image or a video frame from a video source. One of the ways to do this is by comparing selected facial features from the image and a facial database. It is typically used in security systems. Face recognition can be considered to be same as photograph recognition, so it lacks in many areas [5]. Even the automated system for face recognition has lacking as photographs are highly affected by camera angle, brightness, etc. And also the face of the person changes over the time, unlike fingerprint which remains same throughout the life span of a person. Face recognition has been getting pretty good at full frontal faces and 20 degrees off, but as soon as you go towards profile, there've been problems Face is the most easiest feature that can be remembered in our mind to recognize others facial features can be many it is based on the region of interest (ROI) we can scan the particulars face there are several methods to recognize the features of a face principle component analysis (PCA) is one of the most used methods. This is also an easy way of identifying yourself.

- Identity may be difficult sometimes when you have spectacles, moustache , beard etc
- The identification can be difficult when a person changes over a period of time

Figure 4: Face biometric machine

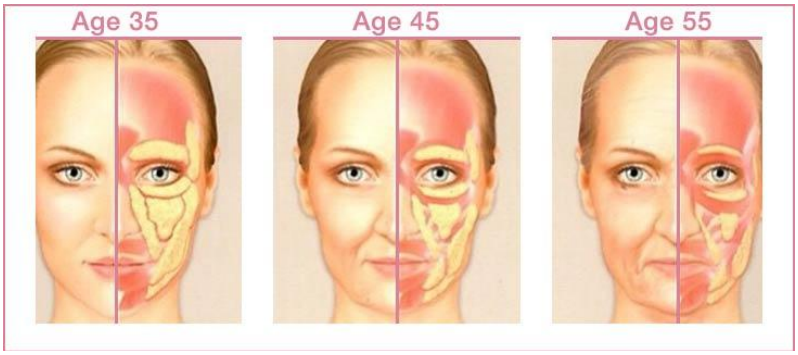

Figure 5: Face changes over a period of time

Iris recognition: Iris recognition is a method of biometric authentication that uses pattern-recognition techniques based on high resolution images of the irises of an individual's eyes. Iris recognition uses camera technology, with subtle infrared illumination reducing specular reflection from the convex cornea, to create images of the detail-rich, intricate structures of the iris. Converted into digital templates, these images provide mathematical representations of the iris that yield unambiguous positive identification of an individual [6].
Iris recognition efficacy is rarely impeded by glasses or contact lenses. Iris technology has the smallest outlier (those who cannot use/enroll) group of all biometric technologies. Because of its speed of comparison, iris recognition is the only biometric technology well-suited for one-to-many identification. A key advantage of iris recognition is its stability, or template longevity, a single enrollment can last a lifetime.

There are few advantages of using iris as biometric identification: It is an internal organ that is well protected against damage and wear by a highly transparent and sensitive membrane (the cornea). This distinguishes it from fingerprints, which can be difficult to recognize after years of certain types of manual labour. The iris is mostly flat, and its geometric configuration is only controlled by two complementary muscles (the sphincter pupillae and dilator pupillae) that control the diameter of the pupil. This makes the iris shape far more predictable than, for instance, that of the face. The iris has a fine texture that like fingerprints is determined randomly during embryonic gestation [7] . Iris is an indusial ring shaped coloured area around the pupil it is formed at the age of two it stabilizes at that point and remains same throughout no two will have same iris same as in the case of fingerprint and it is also more reliable as it could work even if you are wearing contact lenses distance is also not an criteria.

- This is high in cost
- Also users acceptance level has to be taken into consideration as we are taking photo of such sensitive part of eye

Figure 6: Iris sample

Signature recognition: we know that signature is the most known method it is observed as the trace of pen and paper but signatures may vary depends upon the pen paper and area where we are writing

- ❖ It can be easily copied.
- ❖ This is not accurate in all conditions.

Besides these there are palm print recognition, retinal recognition and other biometrics but they are tough to implement when the people are in large number.

III. Training & Testing Of Samples

Enrolment: The enrolment is nothing but taking the samples whether it is for the speech or image or fingers or anything it has to go through a process of training and classification can be done in different ways for different input signals. For an instance we will see how the fingerprint training can be done and the rest of all likewise

The training phase is later followed by the testing phase in which the enrolment inputs that means the inputs at the training phase is taken as a reference suppose in a fingerprint biometry. when a user places his fingertip the value id is compared with the original id which is stored in the database it accepts and sends an acknowledgement like thank you for the verified and voice doesn't come up for the users who are not verified likewise, when training an speech samples in external conditions is as well as important, As internal no noise has to be found better to take it in a closed room more number of samples had to be taken for the correct identification for iris recognition it is easy somewhat when compared to others because it is not effected by external conditions. Face recognition also depends upon the angle of the face in which at we have trained it has to be verified at same angle.

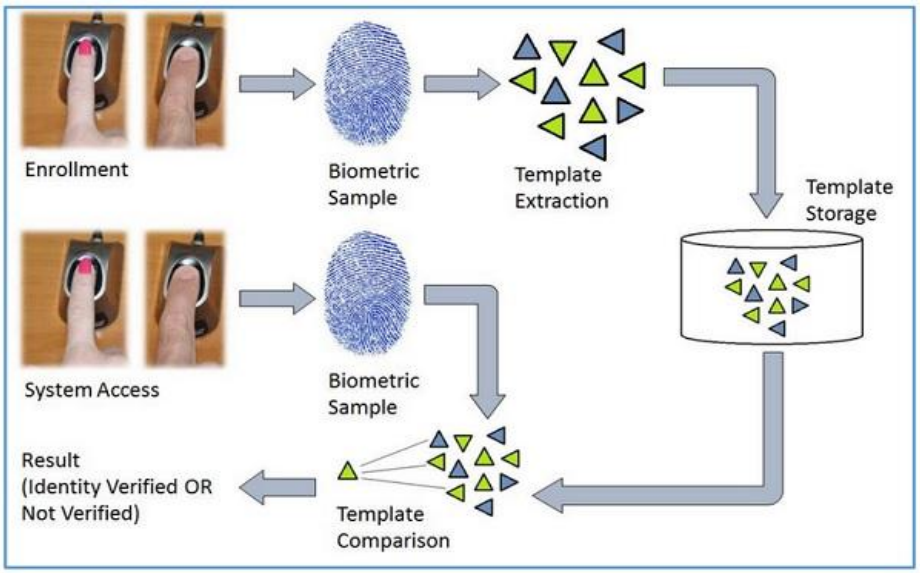

Figure 7: Training& Testing fingerprint

IV. Combinational Biometrcs

Combinational biometrics means mixing two or more biometric models to get a new one these are famously called as multimodal biometrics we propose various kinds of combinational biometrics for increasing the system accuracy

Voice-Iris biometry: it has to be happened in the feature extraction the voice features and the iris recognition is done separately by each node and the majority decision is taken by the classifier on the basis of majority principle

Fingerprint –Iris biometry: the finger prints are recognized for some users and then they are tested with iris if both of them show the same result then the user is identified

These methods are called as fusion methods we can any of two or even three recognizing methods if at all it is acceptability

There are many advantages by using this combinational biometrics

- ❖ Simple and robust.
- ❖ Reliability increases.
- ❖ Ease of use doesn't need to even touch it also by some methods.

By ignoring the cost-effectiveness, we have to say that these are methods which can give the luxury when they come into existence.

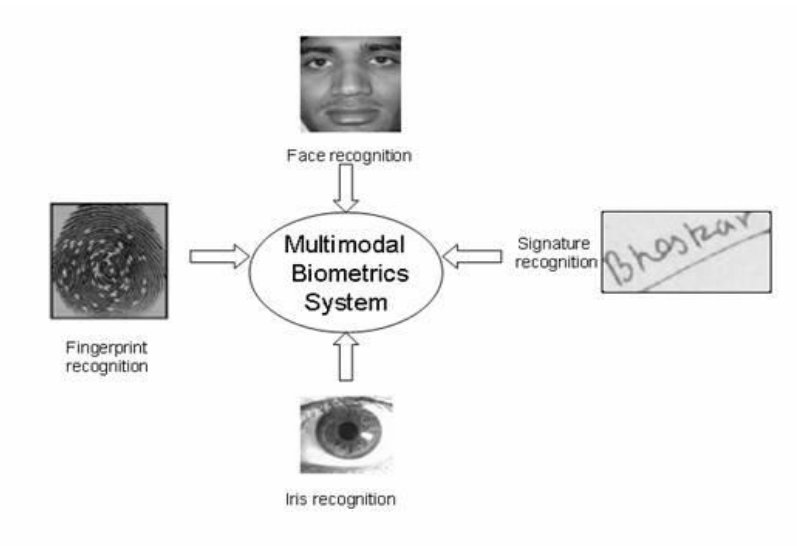

Figure 8: Sample multimodal biometric

Applications:

- Future phone banking.
- When making transactions through internet we can give your voice as a password.
- In smart phones thumb impression has already in existence.
- Military for preventing unauthorised entry.
- Public services, financial, healthcare, transportation etc.

Simply wherever we need high security we can replace the existing PIN/ PASSWORD systems by biometrics and with the combinational biometrics it is easier and reliable.

V. Results

These results obtained considering various factors are shown in the table given below.

Table 1: Comparison of performance of various biometric methods

Biometric Methods	Accuracy	Uniqueness	Ease of use	Reliability & stability	Error causing factors
Finger print	High	High	medium	Medium	Scars, dryness, age
Voice	medium	High	High	Medium	Noise,environmental
Iris	high	High	High	High	Lightning
Facial	Medium	High	High	Medium	Age, head angle
Signature	Low	Medium	High	Low	Surface

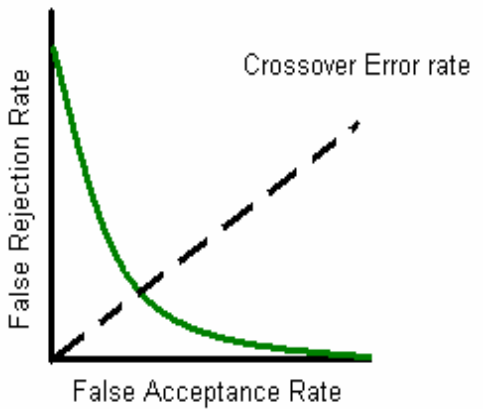

Figure 9: FAR (VS) FFR

The table below indicates cross over rates different biometric methods.

Table 2: Indicates the cross over rate for various biometric methods

Biometric methods	Cross over rate
Finger print	0.8%
Iris	0.000793%
Facial	0.5%
Voice	3%
Signature	3.5%

References

[1]. K.P Tripathi "A Comparative Study of Biometric Technologies with reference to Human interface International Journal of Advances in Science and Technology (IJAST) Vol. 2 Issue I (March 2014).
[2]. Kalyani Mali, Samayita Bhattacharya "Comparative Study of Different Biometric Features" IJARCE Vol. 2, Issue 7, July 2013.
[3]. Alina Klokova "Comparison of various biometric methods" Southampton, UK, SO17 1BJ.
[4]. Rula Abu Samaa'n,"Biometrics Authentication Systems", April 2003, PP 1-2.
[5]. Rupinder Saini, NarinderRana "Comparison of various biometric methods" International Journal of Advances in Science and Technology (IJAST) Vol. 2 Issue I (March 2014).
[6]. Arpita Gopal, Chandrani Singh, e-world Emerging Trends in Information Technology, Excel Publication, New Delhi (2009).
[7]. Bonsor, K. "How Facial Recognition Systems Work". Http://computer.howstuffworks.com/facial-recognition.htm.

AUTHOR'S BIBLOGRAPHY

MR. SIKHAKOLLI SRAVAN KUMAR Completed his M. Tech in the field of Communication Engineering and Signal Processing (CESP) under Acharya Nagarjuna University in 2015; he completed his B.Tech (ECE) under JNTUK in 2013. He is Currently Working as an Assistant Professor from past 1 year in department of ECE RVR & JC College of Engineering (Autonomous). His research areas include Speech signal processing and wireless communications.

Mr. N. ANAND RATNESH was born in 1988 in Guntur district, Andhra Pradesh, India. He completed his M.Tech in Communication and Radar Systems in the ECE department from K L University. He completed his B.Tech at NIET College Affiliated to JNTUK and received his Bachelor's degree in ECE, from JNTU Kakinada in 2010. He is Currently Working as an Assistant Professor in department of ECE RVR & JC College of Engineering (Autonomous). He published nearly 7 papers in the International Journals like IJEMS, IJAST, IJERA, IJCSIT, IJAET and IJEAT. His interested research areas are Antennas, Radars and Wireless & Satellite Communications.