Multimodal Authentication For High End Security

K.Elumalai[#1], M.Kannan[*2]

[#1]Research Scholar CSA Dept, SCSVMV University, Enathur Kanchipuram -631 561

[*2]Assistant Professor CSA Dept., SCSVMV University, Enathur Kanchipuram -631561

***Abstract*—In earlier days Traditional authentication method in computer systems are based on knowledge and token based. Unfortunately lot of drawbacks are in these systems. Passwords often be forgotten, disclosed or changed. A reliable and accurate identification/verification technique may be designed by Biometrics technologies. In Biometrics field there are two types of technologies are present. Unimodel and Bi-model or Multimodel Technology we are going to work with multimodal authentication method for high end security purpose.**

When dealing with unimodal technologies almost drawbacks are present in all methods. So the multimodal technology gives most security when compared to unimodal technology. In this research paper we deals with multimodal authentication for high end security result. Aim is to reduce the false rate totally. we recommend this multimodal authentication for highly valuable area like defence information and banking sector .

***Keywords*—Multimodal,Biometric,Authentication,Security**

I. Introduction

Biometric authentication is modern technique with highly reliable, because physical human characteristics are much more difficult to attack then security codes, passwords, hardware keys sensors, fast processing equipment and substantial memory capacity, so the system are costly biometric authentication application include workstations, and network access, single sign-on, application logon, data protection, remote access to resources, transaction security, and web security secure electronic banking, investing and other transaction process, we want to develop a neat approach for defence area. biometric technologies are expected to play a key role in personal authentication for large scale enterprise network authentication environments.

It is weak approach when deals with the behavioural characters of human like voice, typing key stroke, signature

Authentication:

In technical world we need authentication in all fields to protect our informations, our secrecy, and also to deliver our information to the right person. Authencication is the process to avoid the third person who are acting as a intruder, hacker etc. For our data safe.

Early Methods :

In early days we used token system, passwords are the authentication key to decide a user is the right person or not. This token system is used for long time.

Drawbacks in Early Methods:

While considering the token system, the passwords are maximum guessable. So this system failed . the hacker can easily judge the password by guessing the users favourite word or his birthday. Some users wrote their passwords in their rooms or in their personal notes. So the hackers can easily notify theirs passwords and they can easily access their information as authenticated users.

"We routinely use body characteristics such as face, voice, gait, etc. to recognize each other. The discovery of the distinctive nature of fingerprints in the late 19th century by Faulds, Herschel and Galton (Faulds, 1880, Herschel, 1880, Galton 1888) has enabled almost all the law enforcement agencies in the world to rely on fingerprints for criminal and forensic identification.[1]

Biometric recognition forms a strong link between a person and his identity because biometric traits cannot be easily shared, lost or duplicated. Hence, biometric recognition is intrinsically superior and more resistant to social engineering attacks (eg., phishing) than the two conventional methods of recognition, namely, passwords and tokens.

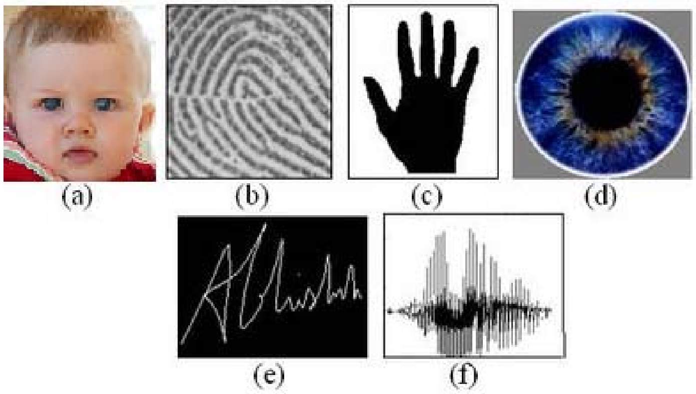


Figure 1: Examples of biometric characteristics that are commonly used: (a) face, (b) fingerprint, (c) hand geometry, (d) iris, (e) signature, and (f) voice.

The above diagram shows the some characters which are used as a biometric authentication. The characters can be classified into two ways physical characters and behavioural characters the physical characters include face, finger etc., the behaviour character includes the behaviour of human like voice, signature, keystrokes etc.. we can differentiate a human by this behaviours

It is possible to understand if a human characteristic can be used for biometrics in terms of the following parameters:

- **Universality** – each person should have the characteristic.
- **Uniqueness** – is how well the biometric separates individuals from another.
- **Permanence** – measures how well a biometric resists aging and other variance over time.
- **Collectability** – ease of acquisition for measurement.
- **Performance** – accuracy, speed, and robustness of technology used.
- **Acceptability** – degree of approval of a technology.
- **Circumvention** – ease of use of a substitute.[2]

II TECHNIQUES:

In earlier days Biometrics authentication is purely based on Unimodal technique.Unimodal Biometric technology is based only on any single technique

A.Unimodal Technique:

While considering the unimodal technology almost some disadvantages is present. Our aim is to achieve a best authentication method which means accurate authentication and less false acceptance rate(FAR) and false rejection rate(FRR).

Drawbacks of Unimodal:

In unimodal technology it is very difficult to achieve FRR and FAR. Consider while using the finger print technique as unimodal technique .

Attacks on Finger Biometric System

- Attacking the physical finger
- Using Artifacts
- Attacking the communications
- Compromising the Template

So In critical situation the using of unimodal biometric finger print recognition leads to be failed cent percentage. Not only Finger print you can take risk with any technique like voice,signature,facial recognition any biometric technique using as Unimodal technique leads to fault at any situation

B.Multimodal Technique:

The combination of Two or more biometric modlities verification and identification. The important reason to combine different modalitiesis to improve the recognition rate and to decrease the attacks. [3]

The goal of Using Multimodal Biometric technique is to reduce:

- False accept rate (FAR)
- False reject rate (FRR)
- Failure to enroll rate(FTE)
- Equal Error rate(ERR)
- To reduce attack

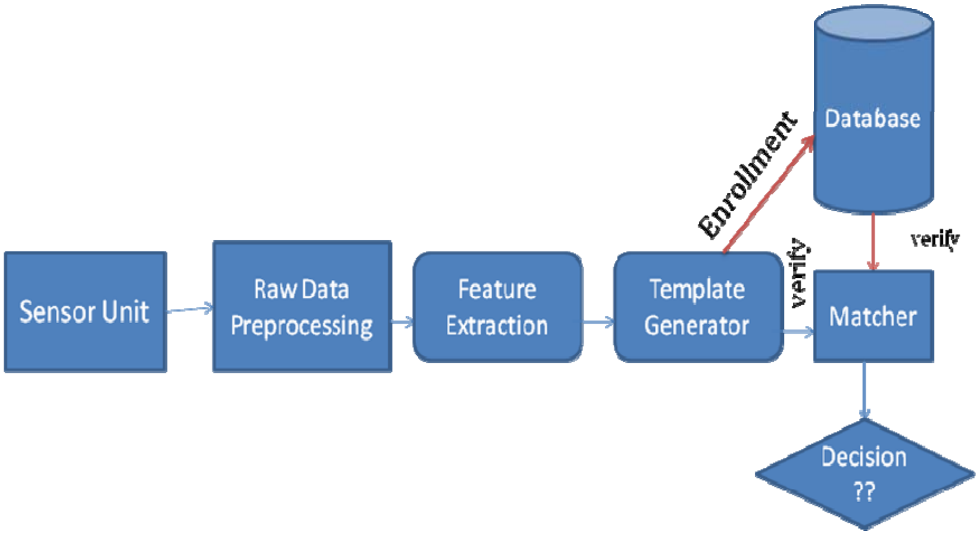
Multimodal biometric system works on two inputs system from single or multiple sensors. Consider the example if we combine the two techniques like iris and facial recognition this two techniques will be achieved by the combination of two sensors . I strongly recommend the multimodal technique is the right choice for the authentication method in biometric world. Our aim of using authentication technique is to secure our data need security. in Unimodal technique security is low and attack is high.

Steps involved in Biometric Authentication:
Sensor Unit: The sensor unit is the first step in biometric authentication. The sensor unit scans the physical character or behaviour character of the human. This will be done by using the preferred devices. Like speech recognition is done by microphone and the iris recognition is done by the iris scanner
Raw Data: The sensor unit captures the data of physical or behaviour character. It is the raw data.[4]

Extracting Features: From the raw data the needed features are then extracted.

Generating Template: The Extracted Features are used to create the template.

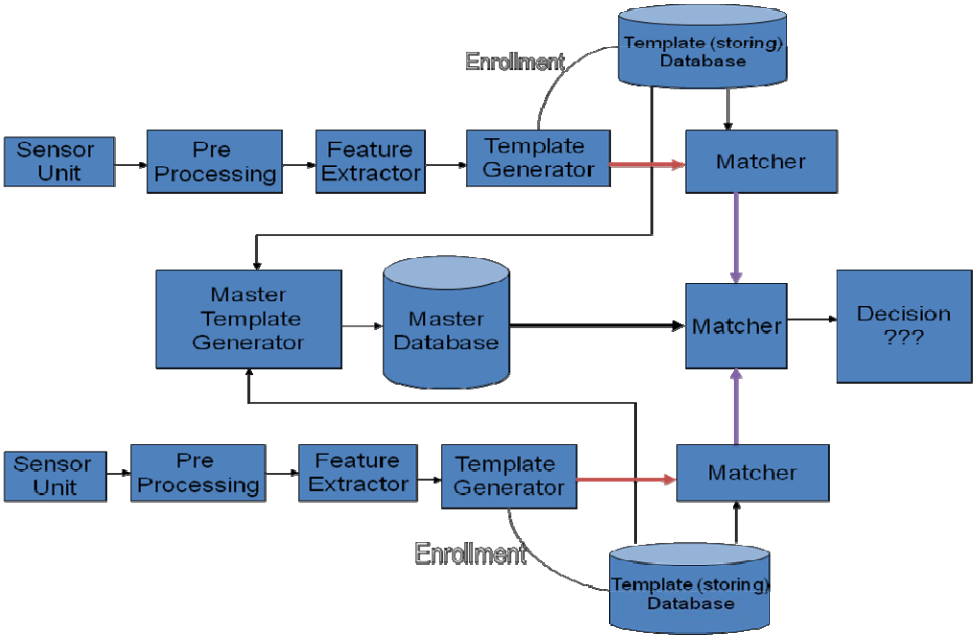
Database: The generated template is stored into the databases. It is used to future verification and to authenticate the user.



Steps involved in Biometric Authentication

The above process show about how a unimodal or biometric authentication steps takes place.

Multimodal Biometric Process:
Multimodal biometric process involes combining of two technology so we need two sensors the two sensors scan the humans two different characters and they produce the raw data from the created raw data features have been extracted then the extracted features are used to create the template then the two separated templates are stored in different databases.
Iris recognition is the most useful method in biometric authentication because spoofing is very difficult and false rate is very low and false acceptance is also very low. In Iris method the peoples acceptance rate and interaction to the device is the problem because they are in myth if the device scans his iris it leads to eye problem it is the only problem in iris technology.



The above working process shows how the multimodal biometric authentication is working it show clearly the security of authentication is increased.

Increasing Security in Multimodal Biometrics:

If we are using voice or facial recognition as a unimodal biometric authentication. If someone misuses users character. We cant save our data at the time because we are using single modal technology if some one attacks we lose our data

In unimodal technology analysing the statistical measures of the biometrics is not satisfaction in unimodal technology the

- FRR(False Rejection Rate)
- FAR(False Acceptance Rate)
- FTE(Failure To Enroll)
- ERR(Equal Error Rate)

Will be increased in rate. So it is not a best security technology.[5]

A Good Biometric Atuthentication is:

FRR: The authentication technology rejects the authorised user as non authorised user. This is false rejections rate. This must be low to achieve the good biometrics.

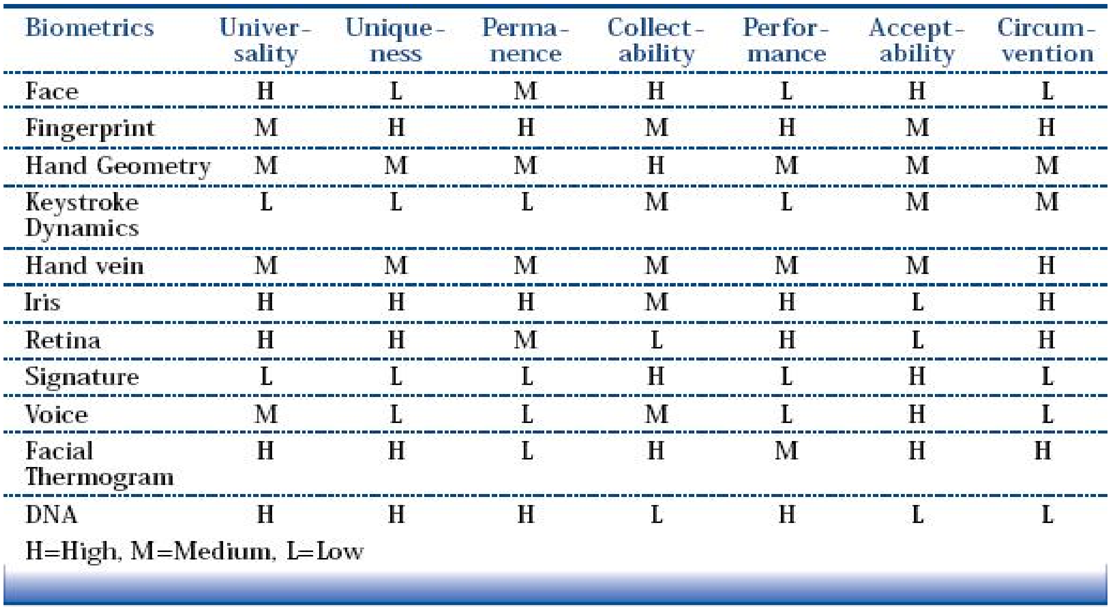
FAR: If Non authorised user is accepted as authorised user for authentication it will be the False acceptance rate.This also must be low to achieve good biometrics.

FTE: If the new user wants to create his identity. The technique failed to enroll the user it is said to failure to enrol rate. This must be reduced to achieve the good biometrics.

ERR: To calculate Equal Error Rate **FRR/FAR** a good biometric must poseses a reduced rate of all statistical measures

In above work process of multimodal biometric system there are three databases are used. The two normal databases are used to scan different characters of human and store the template in different database a master template database is generated using the two separate template the master template is stored in master database when the user needs to authenticate the device scan and create the template then match with the master template from the master database if the features are matched then only the user will be authenticated.

The technique used in single is compared to the same technique used in multi authentication will increase the security. Also the multi modal biometrics decrease the error rates maximum hence we can get high security with less error rate.[6]



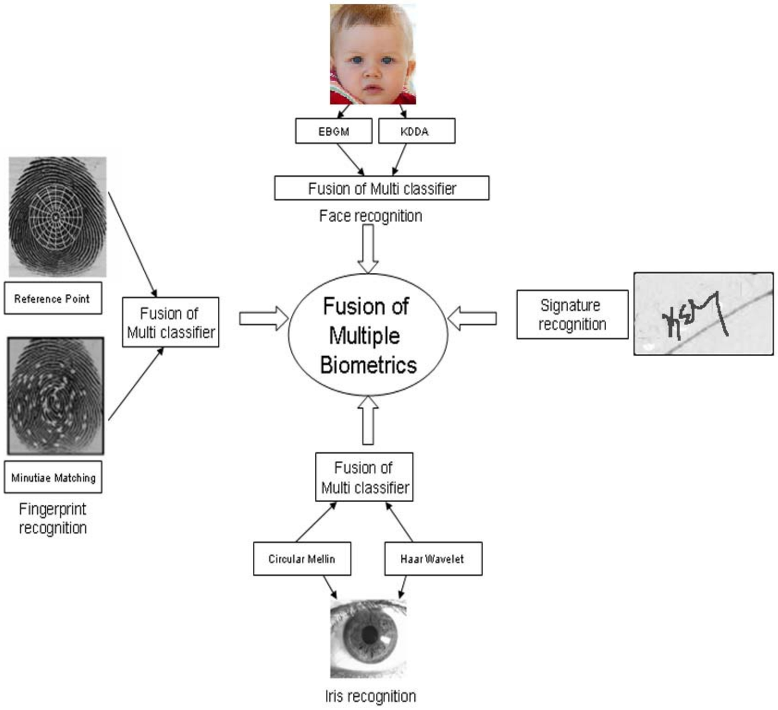
Biometrics	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	H	L	M	H	L	H	L
Fingerprint	M	H	H	M	H	M	H
Hand Geometry	M	M	M	H	M	M	M
Keystroke Dynamics	L	L	L	M	L	M	M
Hand vein	M	M	M	M	M	M	H
Iris	H	H	H	M	H	L	H
Retina	H	H	M	L	H	L	H
Signature	L	L	L	H	L	H	L
Voice	M	L	L	M	L	H	L
Facial Thermogram	H	H	L	H	M	H	H
DNA	H	H	H	L	H	L	L

H=High, M=Medium, L=Low

The above chart explains how the techniques are accepted and its security level if we combine the Iris and Face technique into Multimodal Biometric authentication it will gives the high end security because iris has high performance and facial recognition has low performance we can rectify the facial recognition techniques error rate and increase the security level of facial by adding iris technology.[7]

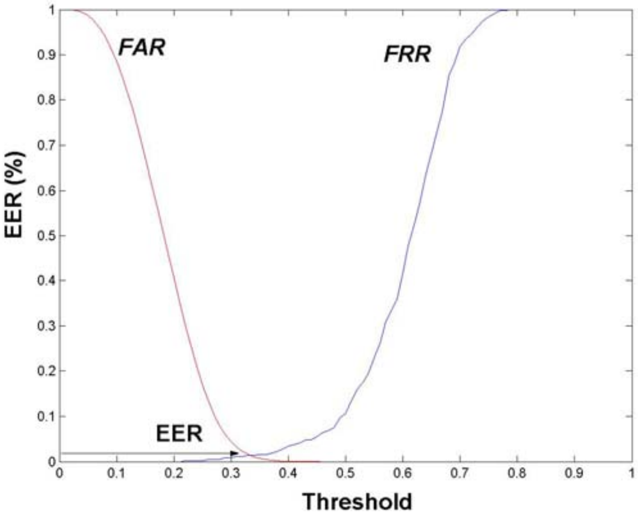
Another fact of using multimodal biometric authentication is we can strengthen the weak techniques like facial recognition, hand geometry like weak techniques can be strengthen by combining with high technique as multimodal authentication.

DNA technique is very high security we can use it as unimodal but the acceptance is low. The time to authenticate is also high. Hence we can combine the two or more technique and achieve the high security is possible one.[8]



When combining the multiple technologies we are able to easily reduce the ERR rate. High security of authentication is easily achieved by fusioning the multiple techniques.[9]

The below graph shows the various features and score of different techniques we can easily judge the acceptance and other characteristics then go with the multiple technologies for higher security



The ERR(Equal Error Rate) is calculated by subtracting FRR from FAR (FAR-FRR). If the ERR is low that technique is most secured and also most efficient technique for authentication if we combine two or more technique into single it gives less ERR rate.[10]

III.Conclusions

Biometric authentication is the best way of authenticating in modern technical world. In biometrics there are two types of techniques used unimodal and multimodal. From the thorough analysis it is clear we need the strong security and less attacks and less error. So we combine two or more unimodal technology as multimodal technology to achieve the high end security. In multimodal we also achieve very less attacks and errors. If we need better security we follow the multimodal technology. In future idea is to reduce the cost of multimodal and also we can use the low level security characters like voice, hand geometry, and other biometric characters into efficient security system by combination of two or more character recognition into single authentication as multimodal technology we can make the low security characters into high end security.

References

[1] http://en.wikipedia.org/wiki/Biometrics

[2] Biometrics for network security Paul Reid, 2004 by pearson education

[3] http://www.omicsonline.org/jbmshome.php

[4] Ching-Han CHEN and Chia Te Chu , "Fusion of Face and Iris Features for Multimodal Biometrics" Journal of Shou University

[5] http://www.security.iitk.ac.in/contents/publications/papers/multimodal_biometrics.doc

[6] http://www.cs.bham.ac.uk/~mdr/teaching/modules/security/lecturers/biometric/html

[7] K.Ramalinga reddy, G.R Babu, Lal Kishore, Larun Agarwal, and M.Maanasa *"Face Recognition Based on Multi Scale Low Resolution Feature Extraction and Single Neural Network"* IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.6, June 2008

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

[9] W.Stallings, cryptography and network security: principles, 3rd ed.

[10] Hand book Fingerprint recognition, D.Maltoni, A.K.Jain. Springer 2009. http://bias.csr.unibo.it/maltoni/handbook/

[11] George Chelin Chandran.J, Rajesh R.S "Performance Analysis of Multimodal Biometric System Authentication" IJCSNS 290 International Journal of Computer Science and Network Security, VOL.9 No.3, March 2009