Comparative and Analysis of Biometric Systems

Manivannan [#1], Padma [*2]
[#1]Research Scholar CSA Dept, [*2]Assistant Professor CSE Dept.,
SCSVMV University, Kanchipuram Tamil Nadu, India
[#1]E-mail : mscmani01@gmail.com
[*2]E-mail : priya.reachu@gmail.com

Abstract – Biometric as the science of recognizing an individual based on his or her physical or behavioral traits, it is beginning to gain acceptance as a legitimate method for determining an individual identity. Biometric have now been deployed in various commercial, civilian, and national security applications. Biometric described overview of various biometric techniques and the need to be addressed form making biometric technology an effective tool for providing information security.

Index Terms- Biometrics, digital rights management, statistical measures, analysis of biometrics, receiver operating characteristics.

I.INTRODUCTION

Biometric recognition technology to use the problem of information security entails the protection of information elements (e.g., digital data) to access authorized users only. The content owners, such as authorized users, are losing billions of dollars annually due to the illegal copying and sharing of digital media. In order to address the growing problem, digital rights management (DRM) system are being deployed to regulate the duplicate data of digital content. The critical component of a DRM system is user authentication which determines whether a certain individual is indeed authorized to access the content available in a particular digital medium. To solve this problem lot of authentication technique is available. In a generic cryptographic system, the user authentication method is possession based. The possession of the decrypting key is sufficient to establish the authenticity of the user. Since cryptographic key are long and random (e.g., 128 bits for the advanced encryption standard (AES)[2][3][14], they are difficult to memorize. But these key are s tored somewhere and released based on some alternative authentication mechanism (e.g., password)[15].most of the passwords are so simple, that they can be easily find it. Some user tend to store complex password at easily accessible locations. Most people use the same password access different applications.

Many of these limitations associated with the use of password and the incorporation of better method for user authentication. Biometric authentication or, simply biometrics,[5][6][7] refers to establishing identity based on the physical and behavioral characteristics of an individual such as face, fingerprint, hand geometry, iris, keystroke, signature, voice, etc. Biometric systems offer several advantages over traditional authentication schemes. They are inherently more reliable than password-based authentication as biometric traits cannot be lost or forgotten; biometric treat are difficult to copy, share, and distribute; and they require the person being authenticated to be present at the time and point of authentication. It is difficult to forge biometrics(it require more time, money, experience, access privileges) and it is unlikely for a user to repudiate having accessed the digital content using biometrics. Thus, a biometrics-based authentication scheme is a powerful alternative to traditional authentication schemes. It can be used in conjunction with passwords to enhance the security offered by the authentication system.

II- TYPE OF BIOMETRICS

They involve two categories: physiological biometrics and behavioral biometrics.[5]

A. Physiological Biometrics

The **Fig 1** shows this category the recognition is based upon physical characteristics. (e.g., face, fingerprint, hand, iris, DNA).

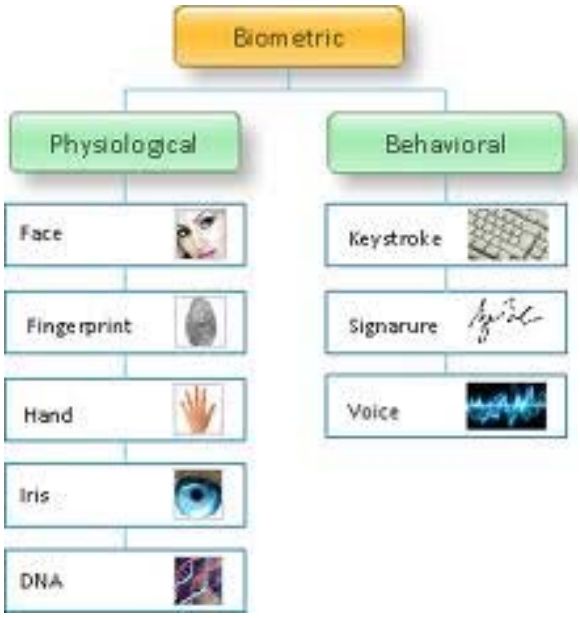

Fig.1. biometric characteristic

B. Behavioral Biometrics

The **Fig 1** shows behavioral biometrics is traits that is learned or acquired over time as differentiated from physical characteristics (e.g., keystroke, signature, voice).

III-WORKING PRINCIPLE OF BIOMETRICS

A. Enrollment, template, Algorithm and Verification

Biometric devices consist of a reader or scanning device, software that converts the gathered information into digital form, and a database that stores the biometric data for comparison with previous records. When converting the biometric input, the software identifies specific points of data as match points. The match points are processed using an algorithm into a value that can be compared with biometric data in the database[13][16].

All Biometric authentications require comparing a registered or enrolled biometric sample (biometric template or identifier) against a newly captured biometric sample (for example, a fingerprint captured during a login)

The **Fig 2** explains the authentication Techniques[1].

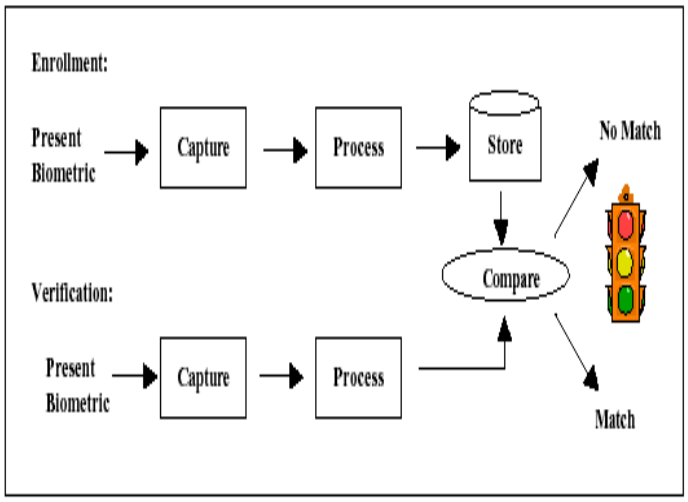

Fig.1. Enrollment and Verification Technique

During Enrollment, as shown in the picture above, a sample of the biometric trait is captured, processed by a computer[5], and stored for later comparison. Biometric recognition can be used in Identification mode, where the biometric system identifies a person from the entire enrolled population by searching a database for a match based solely on the biometric. For example, an entire database can be searched to verify a person has not applied for entitlement benefits under two different names. This is sometimes called "one-to-many" matching.

A system can also be used in Verification mode, where the biometric system authenticates a person's claimed identity from their previously enrolled pattern. This is also called "one-to-one" matching. In most computer access or network access environments, verification mode would be used. A user enters an account, user name, or inserts a token such as a smart card, but instead of entering a password, a simple glance at a camera is enough to authenticate the user.

IV. STATISTICAL MEASURES OF BIOMETRICS

The statistical measures to be used for biometrics technology are[4][5][8]:

FAR- False Acceptance Rate
FRR- False Rejection Rate
FTE- Failure to Enroll
EER- Equal Error Rate

In a biometric system, a physical trait to be recorded. The recording is referred to enrollment. This enrollment is based on the creation of a template. A template is the digital representation of a physical trait. The template is normally a long string of alphanumeric characters that describe, based on a biometric algorithm. The algorithm will also allow the matching of an enrolled template with a new template with just created for verifying an identity called a live template. When a stored and live template are compared, they either match or they do not match. What happens if it is not you who is trying to match to your template. If that person were to match as you, it would be classified as a false acceptance. The probability of this happening is referred to as the false acceptance rate(FAR). The FRR defined as the probability that a user making a true claim about his/her identity will be rejected as him/herself. The FTE is defined as the probability that a user attempting to biometrically enroll will be unable to. It's normally defined by a minimum of three attempts. Fig.3. The EER is defined as the crossover point on a graph that has both the FAR and FRR curves
plotted. The EER can also be calculated from a receiver operating characteristic (ROC)[5] curve, which plots FAR against FRR to determine a particular device's sensitivity and accuracy. The choice of using the crossover point of the FRR/FAR or using a ROC is a question of significance.

An EER[5][11] calculated using the FRR and FAR is susceptible to manipulation based on the granularity of threshold values. A ROC- based EER is not affected by such manipulation because the FRR and FAR are graphed together. Thus, the EER calculated using a ROC is less dependent on scaling.

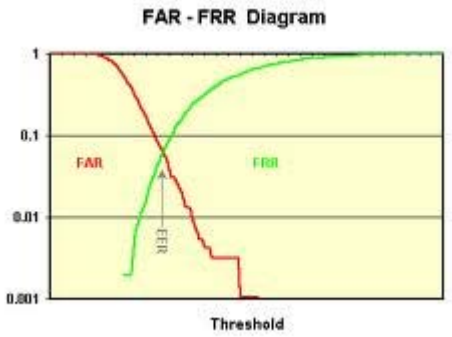

Fig.3.calculating EER from FAR-FRR intersection

V- BIOMETRIC COMPARISON

Comparison of various biometric technologies based on the perception of the authors[1]. High, Medium, and Low are denoted by H, M, L, respectively. Universality (do all people have it?), Distinctiveness (can people distinguished based on an identifier), permanence (how permanent are the identifiers?), and collectable (how well can the identifiers be captured and quantified?), performance (matching speed and accuracy), acceptability (willingness of people to accept), and circumvention (ease use of a substitute) are attributes of biometric systems[5][8][13] (**TABLE.I**.).

TABLE.I.
Comparison of Various Biometric Technologies

Factors → / Biometric identifier ↓	Universality	Distinctiveness	Permanence	Collectable	Performance	Acceptability	Circumvention
Face	H	H	M	H	L	H	H
Fingerprint	M	H	H	M	H	M	M
Hand geometry	M	M	M	H	M	M	M
Iris	H	H	H	M	H	L	L
Keystroke	L	L	L	M	L	M	M
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

H-High L-Low
M-Medium

VI-ANALYSIS OF BIOMETRICS

To analysis the good biometric technology for network security the following characteristics are used: [5][9][13]Acceptance (user willingly accept the biometric device), Ease (user find it ease to use), ROI (total technology costs and benefits provide a suitable), deployable (technology is deployable and supportable),

Noninvasive (technology is not invasive and requires the user to actively submit to its use), Mature (technology is mature and reliable), FAR, FRR, Size, Habituation (user become habituated quickly to the device). For the biometrics examined, a score of 0 to 10 was assigned for each characteristic[5]. An ideal biometric was defined as having a perfect score of 10 in each category.

A- FINGER BIOMETRICS

The finger biometric scored very well relative to the ideal biometric, as shown in[5][8] Fig.4. Its greatest strengths are its deployable and maturity. The greatest weakness comes from the cost and hence ROI.

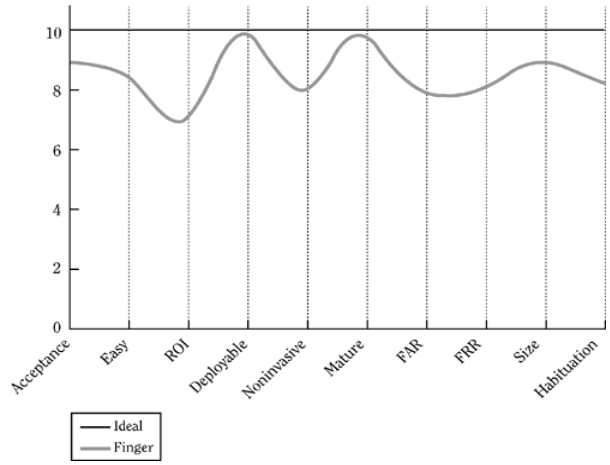

Fig.4. Score for finger biometrics.

B. FACE BIOMETRICS

This biometric technique is greatest strengths are its noninvasiveness and user acceptance, as shown in [5]Fig.5. The greatest weakness comes from the ROI characteristic.

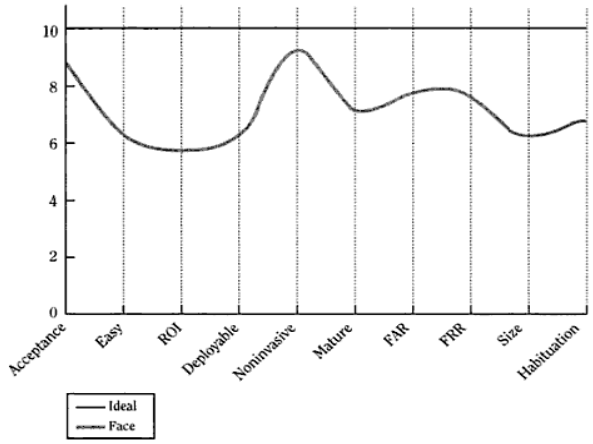

Fig.5. Score for face biometrics

C. VOICE BIOMETRICS

The voice biometrics is natural to use. When we can not see someone but can hear him/her, that can be sufficient for us to recognize who it is. This biometrics greatest strengths are its size and noninvasiveness. As shown in [5]Fig.6. The greatest weaknesses come from the FAR, and FRR.

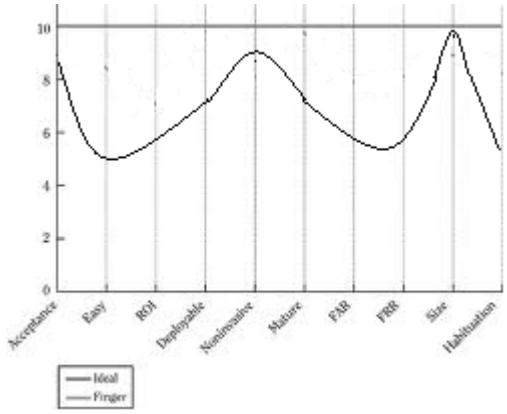

Fig.6. Score for voice biometrics

D. IRIS BIOMETRICS

The iris biometric is the biggest "cool" factor of all the biometrics. It's most often seen in spy movies, and the associated with securing only the most important data. Its greatest strengths lay in the FAR and FRR, as shown [5][8]Fig.7. The greatest weakness come from highly invasive.

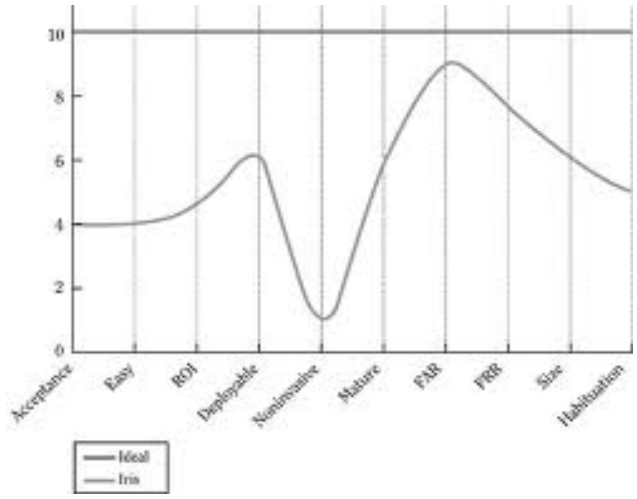

Fig.7. Score for iris biometrics

For each biometrics was evaluated for its suitability for network security and scores were given for each characteristic[5][9][12]. Fig.8. contains a graph showing all the individual graphs together.

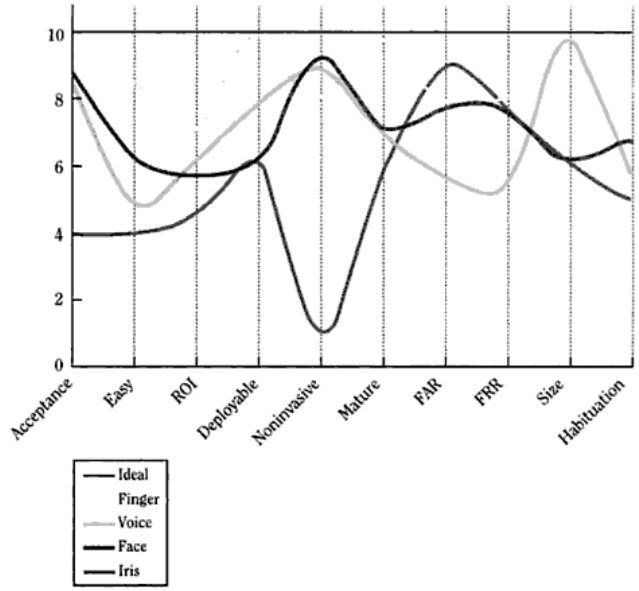

Fig.8. Score for all biometrics

It is clearly shows[5] Fig.8. The closet overall tom being ideal is the fingerprint biometrics. This is also what is being seen in the marketplace[12][13]. Fingerprint biometrics are clearly deployed more then any other type of biometric solution. The reasons for this are their overall general suitability for use and their robustness.

VII- CONCLUSION

This paper describes efficiency of biometric technologies for information security. This choice was based on the score that each biometric received based on the characteristics of an ideal biometric. While the iris biometric provides to be the most secure, and voice and face biometric had the highest level of user acceptance, it was the fingerprint biometric that offered the best overall solution.

REFERENCES

[1] Anil k. Jain, fellow, IEEE, Arun Ross, member, IEEE," Biometrics : A Tool for information security" IEEE Transactions on information forensics and security. VOL.1.No.2.June 2006.
[2] AES Encryption Information. http://www.bitzipper.com/aes-encryption.html.
[3] Advanced encryption standard. http://en.wikipedia.org/wiki/Advanced_encription_standerd
[4] Biometrics and Biostatistics. http://www.omicsonline.org/jbmbshome.php
[5] Biometrics for network security Paul Reid, 2004 by pearson education.
[6] Alfredo c.lopez,,Ricado R. lobez "fingerprint rscognition".
[7] Jammi Ashok, vaka shivashankar,"An overview of biometrics".(IJCSE)International journal an computer science and Engineering.VOL.02.no.07 ,2010.
[8] Ramen V.Ramen, V.yampoolskiy, biometrics: a survey and classification. Int. J. Biometrics,vol.1.1,no.1,2008.
[9] Chitresh Saraswat, An efficient automatic Attendence System using Fingerprint Verification Technique, IJCSE, Vol.02.No.02, 2010, 264-269.
[10] Anil k.Jain, Arun Ross, "An introduction to biometrics recognition", IEEE transactions Vol.14, Issue 1, Jan 2004.
[11] L.O'Gorman, "Overview of fingerprint verification technologies," Elsevier Information security technical Report,Vol.3, No.1.,1998.
[12] "Guide to fingerprint recognition" http://www.digitalpersona.com
[13] Hand book fingerprint recognition, D.Maltoni, A.K.Jain, Springer 2009. http://bias.csr.unibo.it/maltoni/handbook/
[14] W. Stallings, cryptography and network security: principles, 3rd ed.
[15] D.V. Klein, "Foiling the cracker: a survey of, and improvements to password security," in 2nd USENIX Workshop security, 1990.
[16] Fingerprint Database (FVC2002). http://bias.csr.unibo.it.