Comparative Study on Secure Biometrics for Human Identification

Shreya Prakash
Department of IT
Amity University
Uttar Pradesh

Nidhi Sharma
Department of IT
Amity University
Uttar Pradesh

Nitasha Hasteer
Acting Head, Department of IT
Amity University
Uttar Pradesh

ABSTRACT
In this paper, a comparative study of biometric security using various techniques is presented. This paper presents the authentication of information using fingerprint and face biometric technique. A detailed comparison between finger-print biometric and face biometric & their pros and cons while using for the devices is presented. Face biometric identification is more beneficial than fingerprint biometric identification. Face recognition provides more authentication and verification for identification in biometric.

General Terms
Information Security, Identity Management

Keywords
Biometric, Authentication, Identification, Design

1. INTRODUCTION
Information Security has been the primary concern for the user while using any devices. Many techniques provide information security to the devices but using biometrics in devices help to provide more security and privacy of the information & it also put a restriction to unauthorized user to access the information.

Personal identification is the method of associating a particular individual with an identity. Identification can be in the form of verification, which requires validating a claimed identity, which entails determining the uniqueness of a certain person from a database of persons known to the system. Knowledge & token-based automatic identification methodologies have been the two traditional techniques widely used [1]. Token-based approaches use something you have to make a particular ID, such as a passport, keys, ID card.

Knowledge-based approaches use something you know to make an individual ID, such as a key or a personal identification number (PIN). Since these traditional approaches are not based on any inherent attributes of an individual to make a personal identification, they suffer from the obvious disadvantages: tokens may be lost, stolen, forgotten,, and a PIN may be forgotten by a valid user or guessed by an impostor. (Surprisingly, nearly 25% of the people look to write their PIN on their ATM card, thus overcoming the safety offered by the PIN when ATM cards are stolen [2]. Because knowledge-based and token-based approaches are unable to differentiate between an authorized or knowledge of the authorized person [1], they are unsatisfactory means of achieving the security requirements of electronically interconnected information society.

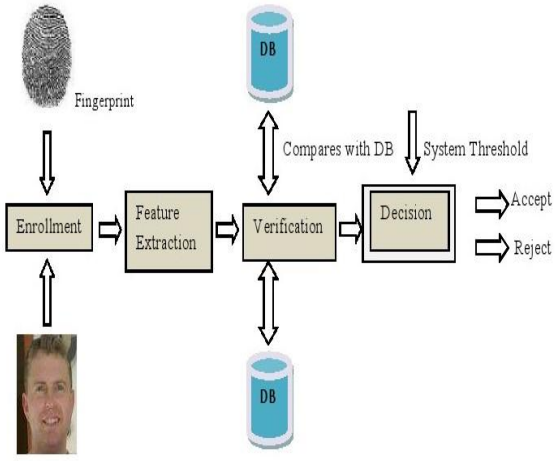

Figure 1. The working of Biometric [4]

In this paper, a detailed comparison of biometric authentication techniques is presented.

2. OVERVIEW
Biometric recognition, refers to the automatic recognition of a person based on his/her anatomical (e.g., fingerprint, iris) or behavioral (e.g., signature) characteristics or traits [10].

The first, which is the older and is used in biological studies, including forestry, is the collection, synthesis, analysis and management of quantitative data on biological communities Such as forests. Biometrics in reference to biological sciences has been studied and applied for several generations and is somewhat simply viewed as "biological statistics"[3] [14]. A study has been made about past, present and future aspect of biometrics.

2.1 Past
Joao de Barros was a Spanish explorer who first identified the use of fingerprint biometric in China during 14 century. Chinese merchant used fingerprint technique to differentiate between children.

In 1858, William Herschel for first time capture hand image of the employee, in order to identify the working employee to be paid on a daily basis. In 1892, classification system was developed for fingerprint. In 1894, Mark Twain describes the use of fingerprint for identification.

In 1960 Woodrow W. Bledsoe developed the first semi-automated face recognition system. Kirby and Sirovich in 1988 introduced Eigen face technique to be used in face recognition. During 1994 Recoware Ltd. developed first automated fingerprint identification system (AFIS). In 1996, Olympic Games use hand geometry. In 2002, ISO establishes

a subcommittee known as ISO/1EC to support standardization of biometric technologies. In 2004 department of defense implemented automated biometric identification system in order to increase the national security.

2.2 Present

In current scenario biometric technique has been more secure and advance to use .Recently University of Wolver Hampton has developed a technique of biometric based on heart and brain patterns. It states that for every person brain and heart patterns are different.

Current techniques have an edge compared to traditional biometric techniques is that it is more fraud resistance but it has a limitation of low accuracy & low reproducibility.

2.3 Future

The challenges like spoof attack, noisy data, and privacy issues remain in the biometric recognition task. Hence, the research groups should give more attention toward the emerging physiological biometrics like EEG, ECG, and EMG, in biometric-based authentication task. In practice, these are more robust toward spoof attack and too do not concern with the privacy issues, those related to the more sensitive biometrics like fingerprint and speech. In contrast, there will be much requirement in quality signal processing approach on those physiological biometrics to improve their recognition accuracy or to bring together with the existing biometrics in multimodal applications. Again, the newly developed biometric, which requires less subject cooperation in the acquisition, by Unsang *et al.* [5] may attract the research community in near future.

3. TECHNIQUES

The identification and authentication in the device using fingerprint and face biometric technique are discussed below:

3.1 Fingerprint Technique

The fingerprint is used for the authentication and identification device to access the information. The FBI has stated that no two people can have the same pattern for their fingers & a specific person finger design cannot be changed during their lifespan.

A fingerprint is the pattern of points and ruts on the surface of a fingertip, the development of which is determined throughout the fetal period [6]. In earlier times merchant used to identify the children using fingerprint with the help of ink. Recently an optical reader is being used .The principle optical reader is based on is ultrasonic principle. The optical reader takes the help of total internal reflection for verification of the fingerprints. It helps to enhance quality of image.

Fingerprint matching is difficult due to large intra class variation caused by sensor noise; partial overlap .Small inter-class variation is another problem [11].

There are two matching algorithms for fingerprint:

3.1.1 Pattern based (or Image based) Algorithm:

It associates the basic fingerprint patterns between a previously stored pattern and an individual fingerprint. This involves that the pictures be aligned with the similar orientation [7].

3.1.2 Minutia Feature extraction based algorithm:

The major Minutia features as publicized during Fig.2 of fingerprint ridges are: ridge ending, bifurcation, and short ridge. The ridge ending is the point at which a ridge dismisses. Bifurcations are points at which a distinct ridge splits into two ridges. Short ridges are ridges which are significantly shorter than the average ridge length on the fingerprint. Minutiae extractions are very significant in the analysis of fingerprints since no two fingers have been shown to be identical [7].

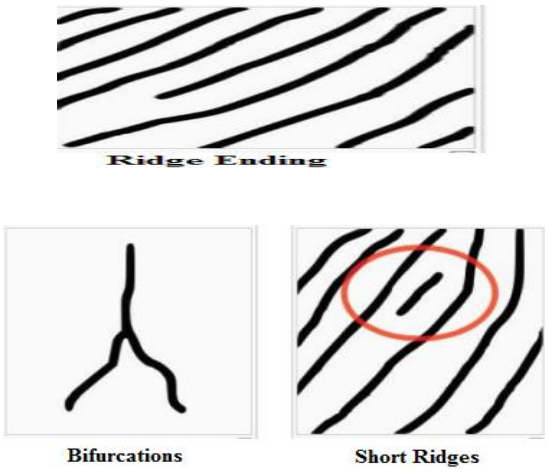

Figure 2 . Features of Minutia Techniques [7]

3.2 Face Recognition Technique

Using face in biometric is most generic characteristic that can be used for verifying a person. Identification based on the face is one of the most dynamic areas of research, with applications ranging from the stationary, controlled mugshot authentication to dynamic, uncontrolled face identification in a cluttered background [6]. In face recognition technique identification can be done with the help of location of eye, lip, nose. It is an appropriate biometric since it is one of the rare that is both “machine readable” and “human readable” so it is generally used for identification cards as well as badges, even though it must normally be used in combination with other biometrics, i.e. Multi- modal [8].

Figure 3. Face Biometric (Show the face recognition technique)

It is difficult to recognize a face from images captured from two drastically diverse views. Further, existing face detection systems enforce a number of limitations on how the facial picture is obtained, at times requiring a simple background or special illumination. In order for the face identification systems to be extensively adopted, they be supposed to automatically identify whether a face is present in the acquired image. Facial recognition is achieved by means of comparing the rigid features of the face which do not change over a period of time [12].

4. TERMINOLOGY USED TO EVALUATE THE FINGERPRINT AND FACE BIOMETRIC

4.1 False Accept Rate (FAR)

It is the probability of defining unsuccessful match. It is critical that unauthorized individuals are not misidentified as authorized. The FAR depends on several factors, such as the distinctiveness of the chosen biometric between individuals (essentially, its uniqueness), the ability to Capture the biometric information accurately, and the ability to match it correctly [13].

4.2 False Reject Rate (FRR)

It is the possibility of defining how many percent of successful input has discarded.

4.3 Equal Error Rate (EER)

It is the rate at which successful and unsuccessful error rate are equal.

The figure shows the relationship between FAR, EER & FRR. It shows the increase of security and increase user rejection rate [9].

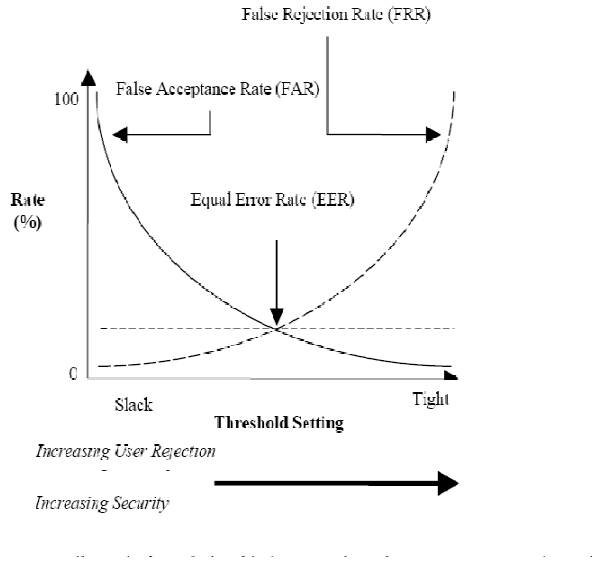

Figure 4. Relationship between False Acceptance and False Rejection Rate [9]

Relationship between FAR and FRR leads in the direction of a trade off situation involving high security with low user acceptance & low security along with high user acceptance, to which resolution has to be made regarding what threshold setting to set that meets together the security requirement of device & user [14].

5. COMPARISON BETWEEN FACE AND FINGERPRINT BIOMETRIC

Biometric	FAR	FRR	EER	Bodily Injury	Tolerance
Fingerprint Recognition	Low	High	NA	High	No
Face Recognition	High	Low	High	Low	High

Face recognition has 1% of the FAR and EER is not valid in it. In it FRR is very high i.e. 10% as match up to fingerprint recognition which 2% is. In fingerprint recognition, the equal error rate is 2% & FAR is 2%.

6. APPLICATIONS:

It has the following applications on Mobile devices, Time monitoring, Attendance monitoring, criminal identification, Online banking, ATM, National identification cards, voter ID cards, telephony transactions, E-commerce, Border Crossing, Passports, parenthood determination, missing child identification, Educational institutes, hospitals, companies etc.

7. CONCLUSION

Biometric provide more security and privacy of information, as compare to traditional identification method. Face Recognition and fingerprint recognition biometrics has their own benefits and limitations. But when both the techniques are compared, face recognition biometric is more beneficial in respect of fingerprint recognition biometric. Face recognition biometric provide more secure, authentication and protection of information to the user.

In recent time, biometric use heart and brain pattern for recognition. It states that for every individual brain and heart patterns are different.

8. REFERENCES

[1] Miller.B ”Vital signs of identity” ,IEEE Spectrum 31, 2 (1994)

[2] Jain, A.K. Bolle, R. and Pankanti S. (Eds.):”Biometrics: Personal Identification in Networked Society”, Kluwer, New York, 1999

[3] “Smart Cart Alliance Identity Council”: Identity and Smart Card Technology and Application Glossary, http://www.smartcardalliance.org, 2007.

[4] Johnson I Agbinya et al.,”Design and Implementation of Multimodal Digital Identify Management System Using Fingerprint Matching and Face Recognition” in Int. Conf. on broadband communication and biomedical applications, Melbourne, Australia, pp. 273, 2011.

[5] Unsang et al. ,“Multimodal Biometric Person Authentication” pp. 54-75,2012

[6] Anil Jain et al .,”Biometric identification” in communication of Acm, pp 91-98,2000

[7] Mazumdar, Subhra, Dhulipala, Venkata :"Biometric Security Using Finger Print Recognition" ,University of California, San Diego,2008

[8] Report on "Defense Biometric" in Defense Science Board Task Force, Washington, D.C ,,March 2007

[9] N.L.Clarke et al. "Biometric Authentication for Mobile Devices" in Australian Information Warfare & Security Conference,2002

[10] "An Overview of Biometric Recognition": http://biometric.cse.msu.edu/info.html, Dec.18, 2006.

[11] Anil K. Jain, "Biometric Authentication: How do I know who are you" in The Wall Street Journal, 2004

[12] Atul Gupta et al. "Facial recognition" in White Paper of Infosys, 2011

[13] Ashbourn J, "Biometric Advanced Identify Verification" In The Complete Guide Springer, 2000.

[14] "Biometrics":http://mistral.univavignon.fr/mediawiki/index.php/Biometrics, Feb.14, 2013.