Review Paper on Fingerprint Biometric and Security

Kirti Sharma, Dr. Parul Agarwal
Jamia Hamdard University, Delhi, India.

Abstract—Fingerprint biometric is one of the most popular system used in various authentication applications. Uniqueness of biometric data makes it very effective. The primary aim of this paper is to discuss the details of fingerprint biometrics and its comparisons with other biometric techniques. It also discusses the issues and problems related t fingerprint biometrics. One of the them is that finger surface is easily effected by outer conditions like moisture, temperature, dust etc. The other is fake and spoofed fingers. And the last but not least is the loss of privacy and security. It is also aimed to discuss the solutions related to privacy and security.

Index Terms—Fingerprint biometric system, fake fingers, security issues, fingerprint pattern, privacy and security in biometric system, Minutiae.

IJSER

1. INTRODUCTION

A Fingerprint Authentication System [1] is one of the most commonly used Biometric system which uses human fingerprint patterns to verify the identity of a person. Fingerprints are the tiny ridges, whorls and valley patterns on the tip of each finger[2]. They are unique and remain unchangeable throughout a person's life under normal conditions. A biometric trait cannot be forgotten, lost, or stolen. So they are widely used in today's world where the security is main concern.

In traditional authentication system password or pin need to be remember and private. Privacy makes this system work. But biometric information is not private, people leave there fingerprint everywhere, you can find retinal match from high resolution photo, you can mimic someone's voice unchangeable throughout a person's life under normal conditions. A biometric trait cannot be forgotten, lost or stolen. So they are widely used in today's world where security is the main concern.

2. VERIFICATION AND IDENTIFICATION

In a fingerprint biometric first a fingerprint is read then some features are extracted from them and stored in database which is called as a **Enrolment** phase, which are used later for matching the identity of a person which is known as an identification or verification

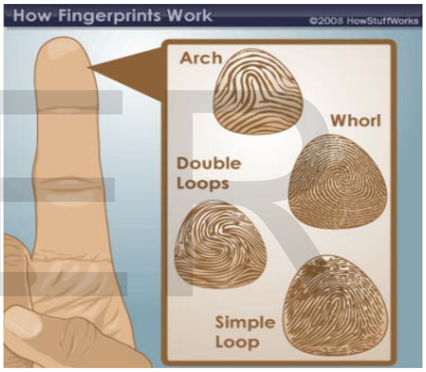


Fig.1 Fingerprint image[3]

Verification: In a Verification system[4], an individual presents himself or as a specific person. The system checks his biometric information against a biometric profile that already exists in the database linked to that person's file in order to find a match Verification is described as a one to one matching because security system tries to find the match between biometric traits presented by an individual against a specific biometric in a database

Because verification needs to compare the biometric to some referenced biometric already stored in database , it is more quick and accurate than identification.

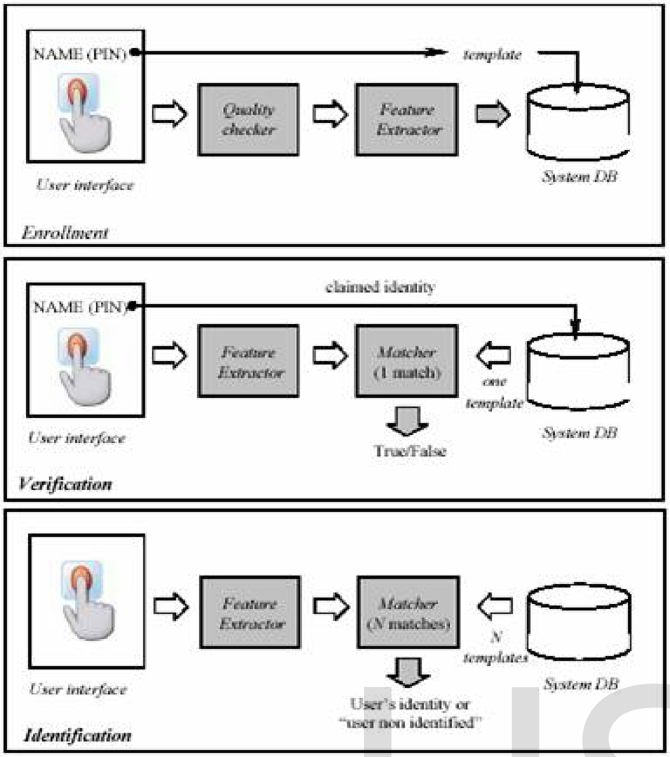


Fig.2 Enrolment, Verification and Identification in Fingerprint biometrics[14].

IJSER

Identification : Identification system[4] seeks to identify an unknown person, or unknown biometric. In an identification system, an individual is recognised by comparing with an entire database of templates to find a match. The system conducts one-to-many comparisons to establish the identity of the individual. The system tries to answer the questions "Who is this person?" Processes of enrolment, verification, and identification are depicted graphically in Fig.2

3. PERFORMANCE OF FINGERPRINT BIOMETRICS

Performance of fingerprint biometrics is based on verification and identification. Some of the key terms used in its performance are as follows

Success Rate[13]: It is a rate at which successful verifications or identifications are performed as compared to the total number of trials on a fingerprint device.

False Acceptance Rate(FAR)[13] : It is the rate at which the system incorrectly authorised a non-authorised person to the total number of trials due to incorrect matching of biometric information with already stored template in database. It falsely matches one person's biometric identity with another person. It should be minimum.

False Rejection Rate(FRR) [13] : The rate at which biometric system falsely rejects the authorised person's biometric information and does not allow him to access is FRR. Like FER, FRR should also be minimum.

True Rejection Rate(TRR)[5] : It is the probability that the system truly rejects the biometric information of a person because that person is not in records of database of biometrics. Developer attempts to maximise this measure.

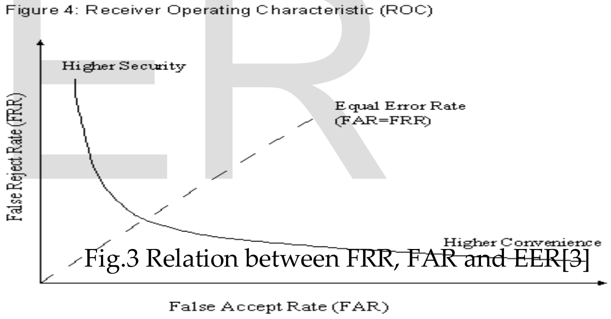


Fig.3 Relation between FRR, FAR and EER[3]

Equal error rate (EER)[13]: It is the common value of the FAR and FRR when the FAR equals the FRR. This is the value where both the FAR and FRR are kept as low as possible at the same time. A low EER value indicates a high accuracy of the system.[4] Fig.3 shows the general relationship between FRR,FAR and EER. High False Rejection rate tends to low False acceptance rate and vice-versa. Small value of EER of system indicates better security of biometric system.

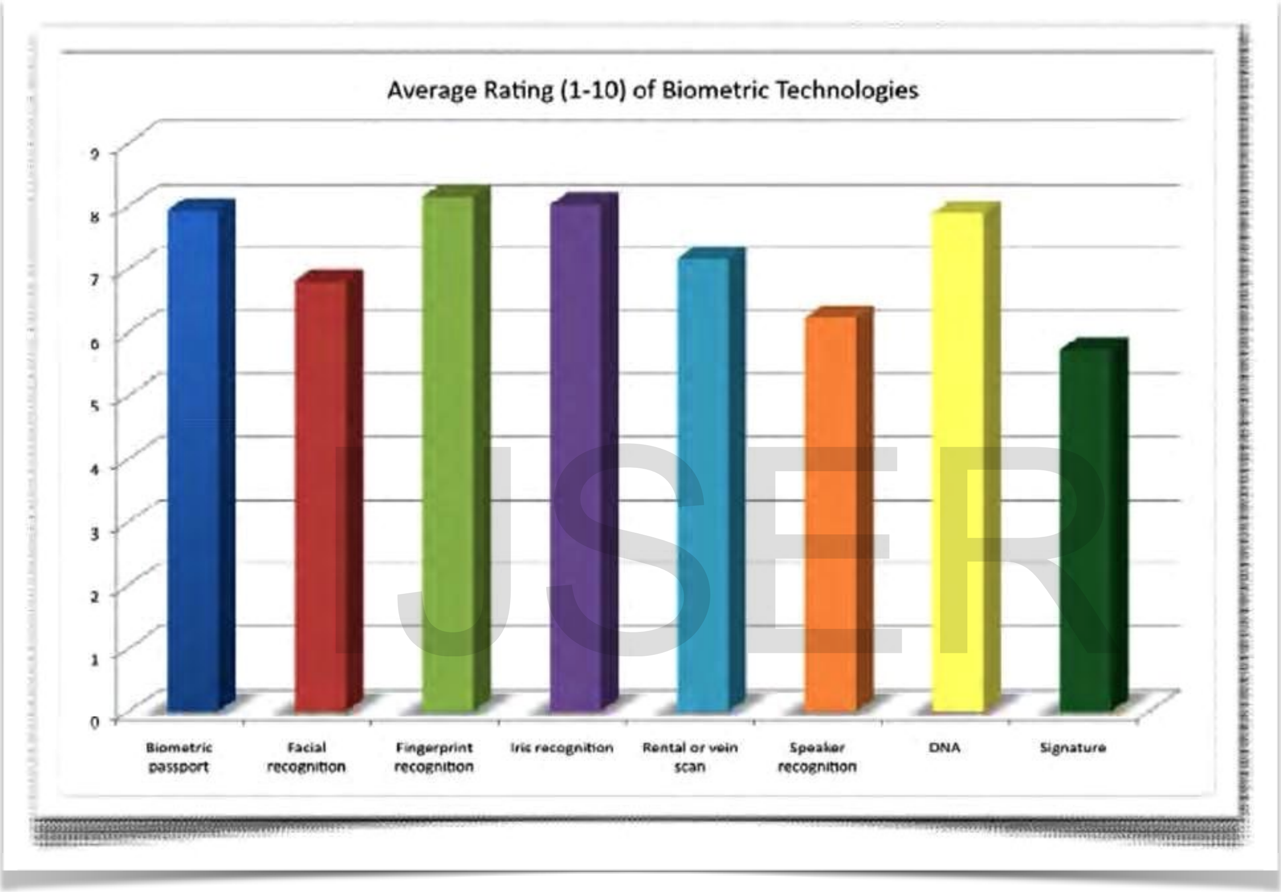
4. DIFFERENT BIOMETRICS TECHNOLOGIES

Biometric data is almost unique to an individual and it has many forms of identifiers. These include:

1. **Fingerprints**: A Fingerprint is made of of ridges and valleys on the surface of fingertips. Upper skin layer segments are called ridges and lower skin layer segments are called Valleys.

2. **DNA**: biometric identification is obtained by examining a rest of the part so the pattern is recognized and than it converted into computer code and get stored into database

3. **Voice Recognition:** It is the identification of a person from characterstics of voice such as tone, pitch cadenc and frequency. It can be affected by bad throat and in that condition system will not be able to recognize the person



IJSER

Fig.4 Preferences of common people in choosing the methods of biometrics.[16]

person's unique sequence of DNA base pairs; often used for evidence in criminal law cases.

3. Retinal Scan: A Biometric Retinal scan is used to map the unique pattern of a person's retina. It performed by casting an unperceived beam of infrared light into a person's eye. Retinal blood vessels are more absorbent of this light than rest of the part the pattern is recognized and than it is converted into computer code and get stored into database.

4. **Palm/Hand Geometry:** Biometric hand geometry.measures and analyze overall structure, shape, and proportion of a hand, e.g width and thicknessof hand, fingers and oints; characteristics of hand geometry biometrics systems measure up to 90 parameters. It is mainly used for verification and not suitable for identification due to low accuracy.

5. **Facial Recognition:** Facial recognition biometrics analyse individual's facial characteristics and identify a specific individual in a digital image.

Some biometrics identifiers such as sibling/ twins facial scans and identical twins's DNA are not unique. Some forms of biometric data does not work well in large groups such as facial scans, palm shape scan and person's gait. They work well in small groups. According to survey [7] in 2012 Fig.4 shows the preferences of choosing the biometric methods in voice. Speaker Recognition can be affected by bad throat as well in that condition device will not be able to recognise the

which Fingerprint Biometric is at top leading behind Iris and DNA Recognition. The least preference is given to the Speaker Recognition. One of the reason of its least preference is that it can be easily affected by age and people can easily mimic the person.

Table1 shows the various biometric technologies with their pros and cons.

Fingerprint are makeup of numerous ridges and valleys the surface of fingers which are unique to everyone.It is one of the most used and most researched biometric technology.

IJSER

Biometric Technology	Affecting Factors	Demonstrated vulnerability	Database	How it works	Cost	Variability with age
Fingerprint	Dirty, dry, oily, worn fingertips	Artificial fingers	Suitable for large DB	Capture and compare fingertips pattern	Low	Stable
Palm	Hand injuries, arthritis, sweeling	none	Not suitable for large DB	Measures and compares hand and fingers	Moderate	stable
Iris	Poor eyesight, Reflection	Low Resolution picture of iris	Suitable for large DB	Capture and compare iris pattern	High	stable
Face	Age,weight gain orientation of face	lighting, eyeglasses, hats, hairstyle,weight gain	Not suitble for large DB	capture and compares facial patterns	Moderate	Affected by age
DNA	identical twins have same DNA pattern	extremely intrusive	Not suitable for large DB	DNA pattern is captured and compared	Very high	stable
Retinal	Glaucoma, Diadiabetes, retinal degenerative disorders	none	Suitable for large DB	Capture and compare retinal pattern.	Very high	Stable but harmful for eyes

Table1. Comparisons among various Biometric technologies

5. FINGERPRINT BIOMETRICS SYSTEM

There are basic three fingerprint patterns: Loops, whorls and arches. **Loops:** Loop is pattern in which ridge enters from one end of a finger, form a curve and exit from the same end. Loops cover about 60-70 % of fingerprint patterns. Each loop pattern has is one delta and one core and has a ridge count[8]. There are two types of loops 1. **Radial Loop**: The flow of the pattern in radial loops runs in the direction of the radius (toward the thumb). Radial loops are not very common and most of the time radial loops will be found on the index fingers.[8]

2. **Ulnar Loops**: The ulna is on the same side as the little finger and the flow of the pattern in a ulnar loop runs in the direction of the ulna (toward the little finger).[8]

Whorl: When ridges form around a central point in a finger surface then it makes Whorl.It contains two or more deltas.There is four types of whorl pattern. Whorl contribute 25-35% of fingerprint pattern.

1. **Plain Whorl:** It simplest form of whorl and most common formed by ridges that make a turn of one complete circuit so they are circular or spiral in shape. **2**. **Central Pocket**: In Central pocket , one or more simple recurves of plain whorl recurves again . **3**. **Double loop:** There is two loop formations in which each formation is entirely separate and distinct sets of shoulders[9] and delta[10]. **4. Accidental Whorl:** The accidental whorl pattern is derived from two distinct types of pattern. They have minimum two deltas.

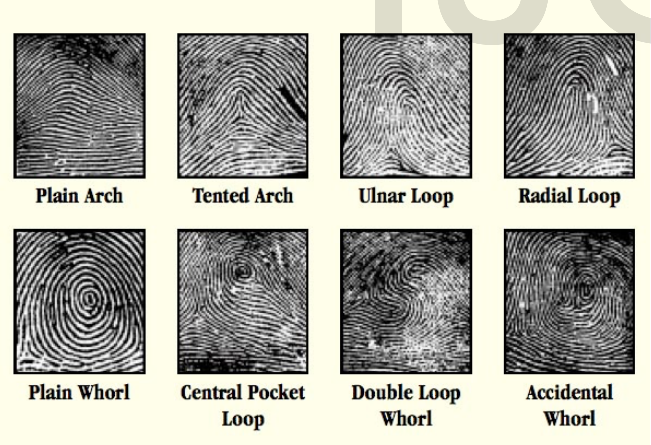


Fig.5 Different patterns of fingerprint[17]

Arches: The ridge move from one side to the other side of finger pattern with no backward turn forms arches. The contribute about 5%of fingerprint pattern. Usually they don't have delta on their pattern. There are four types of arches: **1**. **Plain Arches**: They have even flow of ridge from one side to other of the pattern. **2**. **Ulnar Arches:** In these arches the ridges enter slope down towards the little finger. **3 Radial Arches**: The ridges slope down towards the thumb. 4. **Tented Arches**: Tented arches have an angle and an upthrust. Different fingerprint patterns are shown in Fig. 5.

Minutiae Features:

Minutiae[3] are very special and most important feature in fingerprint pattern on which recognition of an individual is performed. In fingerprint biometrics, minutiae are major features using which comparisons of two fingerprints can be performed. Minutiae are of two types: **Ridge Ending:** This is the abrupt ending of a ridge. **Ridge Bifurcation:** When a ridge get divided into two. The points at which scars begins also known as minutiae. Fig. 8 shows the minutiae points on a fingerprint.

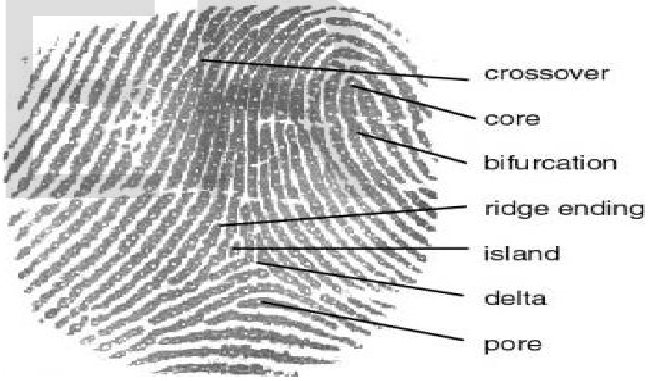


Fig.8 Minutiae Points on Fingerprint[18]

The number and locations of minutiae points on fingers are different for different people. When a finger is scanned in a device then its number of minutiae points and their location are recorded and stored in DB. A computer compare these minutiae points with anyone else who claimed the identity.

ADVANTAGES OF FINGERPRINT BIOMETRIC SYSTEM:

- It is matured and well proved core
- This technology have high accuracy.
- The most researched and standardised biometric

IJSER

technology

- It requires small storage space for biometric template.
- It is highly stable, does not change with age unlike Facial and Voice Recognition.
- Inexpensive equipments having low power intake.
- It has high accountability means it is able to keep track of user's activities like who? what? and when?
- It provides convenient and additional security to the system.

Disadvantages of Fingerprint biometric System:

- Performance can be deteriorate by dust, oil, water on the finger surface.
- Cannot be used in Chemical industry and hospitals because use chemicals on hands can change the fingerprint pattern.
- It is more associated with forensic.
- Loss of Privacy and security.
- The problem of artificial gummy, spoofed or fake fingers.

6. SECURITY ENHANCEMENT BY USING FINGERPRINT BIOMETRIC

Most of fingerprint devices have some problem like Captured images on devices are easily affected by the condition of surface of fingers means oil, dust, water and many more and impact its performance. The other problem is artificial gummy or fake fingers. Last but not least is loss of privacy and security in all biometric systems. Now in this paper we are trying to find the solution of loss of privacy and security.

A. **Switching Fingers:** One of the solution is that If someone stole the copy of our fingerprint scan than we can change the identifier nine more time only by switching fingers. [11] One of the benefit of this solution is that no more hardware is required in it. One of the issue with this solution is that It requires large database.

B. **Integrating other biometric technologies with Fingerprint biometrics:** In this technology, we try to integrate any one or more biometric technology (such as voice recognition, face recognition, iris recognition or retinal recognition) with fingerprint biometric to enhance its security. If any one of the technology is unable to identify the person, still system can work with the help of the other. Or we can enhance the security more by combining two or more technologies such that no access is possible until all of them authenticate the person.One of the drawback of this technology is that it required more than one device for identification that increases its cost.

C. **Combining Fingerprints, Smart Cards and Cryptography[12]**:In today's world Debit cards/ Credit cards(smart cards) are used in many activities like, online transactions, ATM, marketing etc but if once they get stolen and got password to be cracked, it is unusual loss of money and all. Hence some research has done in this field in which combinational techniques are used in Smart Cards with using Biometric algorithm. Indian Government recently bring its idea of Aadhaar Card[13] in which fingerprint and cryptography are used to make it more secure and unique to each individual.

Hence, it provides a very high degree of security in authentication and secured transaction in smart cards.

• CONCLUSIONS

This paper presents the details information about fingerprint biometrics and at last we discussed some of the solutions of issues related to the privacy and security of fingerprint biometric so we concluded that fingerprint biometric has many advantages such as cost, robustness, reliability, accountability and efficiency. This is one of the cheapest biometric solution and easy to operate as well.The possibility of defeating this technology is fake fingerprints and lost of privacy and security. From this study it is concluded that more work need to be done in fake fingerprints and and the

IJSER

issue related to the privacy and security in database. So it is very necessary to make Fingerprint biometric more sophisticated by developing new fingerprint sensors with increased security having improvements in False Acceptance Rate(FAR) and False Rejection Rate(FRR). It is also necessary to work in fields of secured database technologies so that it can be prevented from hackers to attack.

- **REFERENCES**

[1] Jain, A.K.; Ross, A.; Prabhakar, S., "An introduction to biometric recognition," IEEE Transactions on, Vol. 14, no. 1, pp. 4,20, Jan. 2004 doi: 10.1109/TCSVT.2003.818349
[2] science.howstuffworks.com/fingerprinting1.htm,
[3] http://s.hswstatic.com/gif/fingerprint-2.gif
[4] F.A. Afsar, M. Arif and M. Hussain"Fingerprint Identification and Verification System using Minutiae Matching" National Conference on Emerging Technologies 2004
[5] Andrew S. Patrick "Fingerprint Concerns: Performance, Usability, and Acceptance of Fingerprint Biometric Systems" (June, 2008) National council of Canada.
[6] Ms. S. Bharathi and Dr. R. Sudhakar"Hand Biometrics: An Overview" International Journal of Automated Identification Technology, 3(2), July-December 2011, pp. 101-108
[7] Aleksandra Babich "Biometric Authentication. Types of biometric identifiers "(2012) Haaga-Hella, university of applied science
[8] Ching-Tang Hsieh, Shys-Rong Shyu and Kuo-Ming Hung "An Effective Method for Fingerprint Classification" amkang Journal of Science and Engineering, Vol. 12, No. 2, pp. 169E182 (2009) 169
[9] A Simplified Guide to Fingerprint Analysis "www.forensicsciencesimplified.org/prints/glossary.htm"
[10] handlines.blogspot.com/2005/09/do-you-have-unusual-fingerprints.html
[11]Anthony Delehanty"Security Issues in Biometric Identification" (2011) Bahria University Journal of Information & Technology Vol. 4, Issue 1August 2011
[12]Claude BARRAL"Biometrics & Security: Combining Fingerprints, Smart Cards and Cryptography" (2010) A LA FACULTÉ INFORMATIQUE ET COMMUNICATIONS LABORATOIRE DE SÉCURITÉ ET DE CRYPTOGRAPHIE
[13] Murthy,Ravindra Babu Kallam, Srujana B"A Survey on Fingerprint Biometric System" India(2012), 307-313, International Journal of Advanced Research in Computer and Software Engineering.
[14] http://www.geocities.ws/hnabhijith/image004.jpg http://www.geocities.ws/hnabhijith/image004.jpg
[15] Murthy,Ravindra Babu Kallam, Srujana B"A Survey on Fingerprint Biometric System" India(2012), Pg. No. 308 image, International Journal of Advanced Research in Computer and Software Engineering.
[16] Preferences of common people in choosing the methods of biometrics(2012): https://www.theseus.fi/bitstream/handle/10024/.../Babich_Aleksandra.pdf.
[17]http://www.viewzone.com/fingerprint1.jpg
[18] http://biometrics.derawi.com/wp-content/uploads/2011/01/fingerprint_definition.jpg

IJSER

IJSER