A Review Paper on Fingerprint Biometric and Security

Lokesh Sharma
M. tech Scholar
Dept. of Computer Science
MACERC, Jaipur
lokesh.maiet@gmail.com

Manish Mathuria
Associate professor
Dept. of Computer Science
MACERC, Jaipur
manishmathuria@outlook.com

Abstract: Fingerprint authentication is the most sophisticated method of all biometric techniques and has been thoroughly verified through various applications. Biometric fingerprints are the most widely used personal identification tool because of their individuality, uniqueness and reliability. Even features such as person's face or signature can change with changing in time and may be fabricated or imitated. But a fingerprint occurs uniquely to an individual and remains unchanged for lifetime.

The primary aim of this paper is to discuss the details of fingerprint biometrics and its comparisons with multifactor authentication techniques. 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.

Keywords: ***Fingerprint biometric system, Performance Measurements fake fingers, security issues, fingerprint pattern, privacy and security in biometric system***

I. INTRODUCTION

In traditional authentication system personal pin or passwordwas required to be remembering and make it private. 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 condition(s). Such biometric trait cannot be lost, stolen or forgotten. So Fingerprint biometric systemare mostly used in this era where security is more important[1].

Fingerprinting was the first example of biometrics that being used by China.Fingerprints are matchlessly thebest sure and unchangeable form of all other forms like signature and other method/ system.

II. WORKING PRINCIPLE OF BIOMETRIC SYSTEM

All the biometric system depends on the same principle as given below. It involves predefined steps as well as we must have known about some basic terms of biometric system like enrollment, biometric data, presentation, template, feature extraction, matching[5].

A. Enrollment or Registration

The process, by which a user's biometric data is primarily acquired, processed and stored in the form of a template and it will use further use as authentication in a fingerprint biometric system. It is called enrollment or registration process.

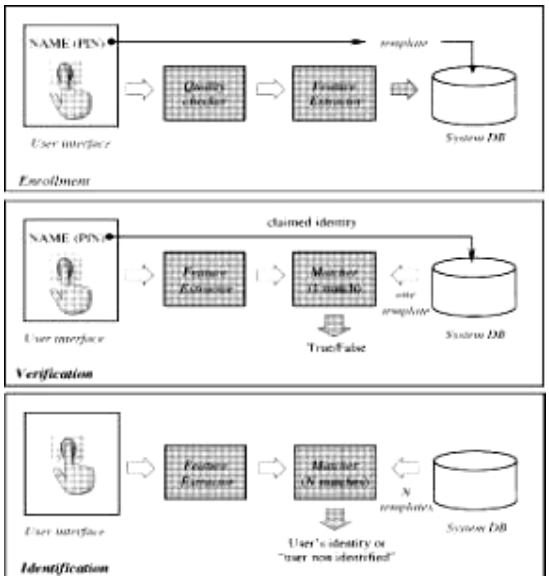

Fig.1 Enrolment, Verification and Identification in Fingerprint biometrics

B. Biometric Data

The information presented by the user(s) during the registration process is known as unprocessed image data, which is also called as raw biometric sample or biometric data. User's biometric data cannot be used to perform biometric comparison so it is used for create biometric template with the help of process and that process is called as feature extraction process.

C. Presentation

The processes by which user(s) presents his/her biometric sample to the capture devices, the hardware which is used to collect data. For example put a finger on a surface of finger reader.

D. Template

After applying a number of feature extraction algorithm(s), biometrics sample convert in to the form of mathematical called as template. A template size may be different in size as few bytes for hand geometry to several thousand bytes for facial recognition. At the time of registration, template is known as stored template and at the time of authentication, it is known as live template.

E. Feature Extraction

The process of locating and encoding distinctive features from biometric sample in order to create/generate a template is called feature extraction. During the enrollment and verification, feature extraction takeplace when template generated.

F. Matching

At the time of verification, stored template is compared with live template. This process is known as matching. It obtained a score on the basis of this biometrics sample score and identify that a person is authenticate human or not.

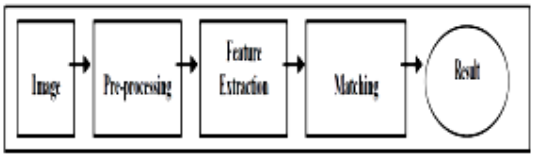

Fig 2: Matching Process

III. PERFORMANCE MEASUREMENTS

The performance of a fingerprint biometric system totally depends on the False Reject Rate (FRR) and False Accept Rate (FAR).

- **False Rejection Rate (FRR):**The rate at which biometric system falsely rejects the authorized person's due to incorrect matching of biometric information and does not allow him to access is called FRR. ` FRR is also known as Type-I error or False Non Match Rate (FNMR)

- **False Acceptance Rate (FAR):** The rate at which the biometricsystems incorrectly authorized a non-authorized person due to incorrect matching of biometric information and allow him to access is called FAR. FAR is also known as Type-II error or False Match Rate (FMR).

FAR and FRR both are inversely proportional to each other that mean when FAR will improved, then the FRR declines.

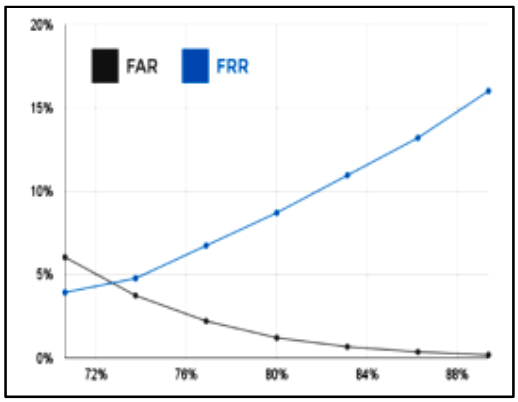

Fig3: Security Threshold

- **Success Rate:**The rate at which successful verifications or identifications are performed as compared to the total number of trials on a fingerprint device. Success rate is directly proportional to number of correct authentication.

IV. DIFFERENT BIOMETRICS TECHNIQUES

Different type of biometrics is given below and their Biometric data is unique to an individual[7].

1. **Finger Print:**A fingerprint is a combination of the friction ridges. A friction ridge is a raised portion of digits (fingers and toes) or plantar (sole) skin, including of one or more connected ridge units. In current time, live finger print readers are used because these reader are based on optical, thermal, silicon or ultrasonic principles. 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. **Retinal Scan:** A Biometric Retinal scan is used to map the unique pattern of a user's retina.Before the Retina scans, the person need to removes their glasses, place their eye close to the Retinal scanner, stare at a particular point, and remain not move, and focus on a particularlocation for 10- 15 seconds. An infrared light beam used during this scanning process.Retina pattern is recognized except Retinal blood vesselsand it is converted into binary code and stored into DB (Database).
3. ***Iris:***Each iris structure have an unique and complex pattern with the combination of corona, crypts, filaments, freckles, pits, furrows, striations and rings. Iris patterns are unique and they obtained through digital image or video based image acquisition system. The iris of the eye which is colored area that surrounds the pupil are used for recognition method.
4. ***DNA:***For DNA analysis we need a specific lab environment and a form of tissue, blood or other bodily sample part. In traditional DNA system, it taken more than 30 minutes but now days, DNA human analysis is possible within 10 minutes. DNA can be matched automatically in real time, it may become more significant and sophisticated.
5. **Palm/Hand Geometry:** Every person's hand shape is different to other one and after certain age, person's hand shape does not change. Person's hand length, width, thickness and surface are the main component of this technique. Mechanical or optical principal based method are used to measure the palm/hands shape.
6. **Facial Recognition:** A facial recognition is one of the applications of computer based automatically identifying/verifying technique that convert person face in to digital image or a video frame a video source. Person's eyes, nose, ear and mouth are the main component of facial recognition technique and distance between these features create a unique code for a particular person. It is totally natural mean of biometric.

V. FINGERPRINT PATTERNS

There are three types of finger patterns.

- Arches
- Loops
- Whorl

A. Arches

Arches are seen in about 5% of fingerprint patterns encountered. In arches, the ridges of the finger run continuous from one side of the finger to the other with no backward turn. Normally, no delta found in an arch pattern but where there a delta, no backward turn ridge must intervene between the delta and core points. There are two type of arch pattern[8]:

- **Plain Arch:** Such pattern starts on one side of the finger, and then the ridge cascades upward slightly, almost resembling a wave out on the ocean. These pattern have a consistency of flow to it. The plain arch is the simplest of the fingerprint patterns.

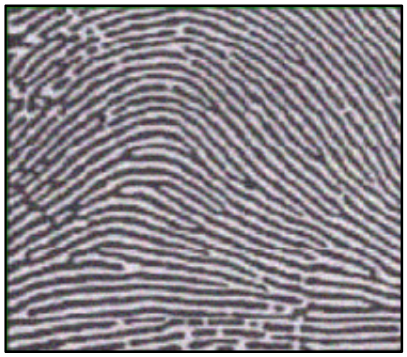

Figure4: Plain Arch

- **Tented Arch:**Tented arch is similar to plain arch in the way of it starts on one side of the finger and flows out in a similar pattern to the other side. The main difference between is the tented arch lies in the ridges in the center, which are not continuous as in the case of the plain arch.

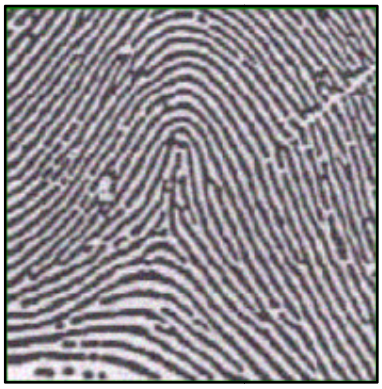

Fig 5:Tented arch

B. Loops

Loops found in about 60-70 % of fingerprint patterns encountered.In loops, the ridges make a backward turn but do not twist. This backward turn, or loop, is differentiated by how the loop flows on the hand and not how it flows on the card on which the imprint is taken. Each loop pattern contain one core and one delta and has a ridge count. There are two sub-groups of this category:

- **Radial Loop:** these are loops that flow toward the radius bone of the hand or, in other words, when the downward slope of the loop is from the direction of the little finger toward the thumb of the hand.

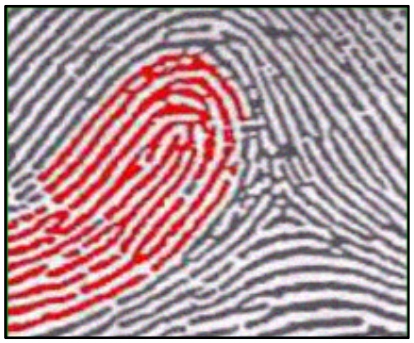

Fig 6. Radial Loop

- **Ulnar Loop**-These are loops that flow toward the ulna bone of the hand or, in other words, when the downward slope of the loop is from the direction of the thumb toward the little finger of the hand.

Fig7. Ulnar loop

C. Whorl

Whorls found in about 25-35 % of fingerprint patterns encountered. In whorls, there are patterns in which there are two or more deltas (first ridge nearest the divergence point of two type lines) and there exists a recurve preceding each delta. There are four types of whorls:

- Plain Whorl
- Central Pocket
- Double Loop
- Accidental Whorl

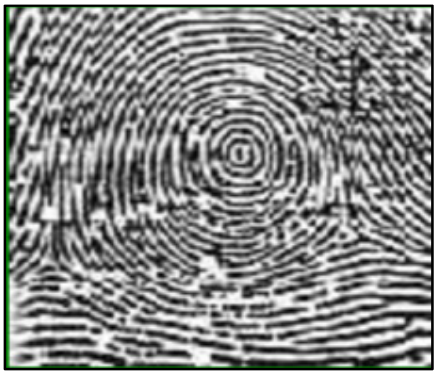

Fig 8. Plain Whorl

Minutiae are very special and most important feature in fingerprint pattern on which recognition of an individual is performed. Minutiae and patterns are very important in the analysis of fingerprints since no two fingers have been shown to be identical.A Minutiae is defined as the points of interest in a fingerprint, such as bifurcations (a ridge splitting into two) and ridge endings. 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.

VI. PROS OF FINGERPRINT BIOMETRIC SYSTEM

1. Obtaining a fingerprint via a scanner is non-invasive. It is very hard to forge a fingerprint[2].
2. it is the most economical biometric PC user authentication technique with very high accuracy
3. It is not possible to re-construct the original fingerprint from the template i.e. identify theft is not possible through this way.
4. Small storage space required for the biometric template, reducing the size of the database memory required
5. Replay attacks are hard to implement as the scanner and host computer use various methodologies to combat it. Encrypted messages are sent between the scanner and host using public/private keys. The host computer issues uses time stamps / challenge response to ensure messages are not being diverted or replayed [4].

VII. CONSOF FINGERPRINT BIOMETRIC SYSTEM

1. Cannot be used in Chemical industry and hospitals because use chemicals on hands can change the fingerprint pattern.
2. It can make mistakes with the dryness or dirty of the finger's skin, as well as with the age.
3. For some people it is very intrusive, because is still related to criminal identification.
4. The problem of artificial gummy, spoofed or fake fingers [6].
5. Criminals could get hold of people body parts to use on bio-metric scanners.
6. Fingerprints can be recreated from things people have touched. This could then be used to access a biometric scanner.

VIII. SECURITY ENHANCEMENT BY USING FINGERPRINT BIOMETRIC

Fingerprint devices have some problem like captured images on devices can be easily affected by the some condition like oil, moisture, dust and many more and such conditions impact on fingerprint biometric performance. The main another security concern is fake or gummy finger. Now in following given below section we will give some solution regarding the loss of privacy and policy of fingerprint biometrics[4].

- **CHAOS ENCRYPTION**Chaos encryption is advanced encryption technique used to transmit important information via unsecured path/channel efficiently with losing information.Chaos encryption process input image pixel values are encrypted with chaotic encryption key with threshold value using bit-xor operation. Through this method we can increase the security.

- **Fuzzy Vault**: The "vault" seems to be a securestorage for biometric data because it contains the usefulbiometric template data mixed up with the meaningless chaffpoints.Therefore, the information of biometric template wouldnot be leaked out unless the identification completed correctly[3].

- **Integrating of another biometric technologies with Fingerprint biometrics:**In this method, we will use to integrate any one or more biometric technology (such as voice recognition, face recognition, iris recognition or retinal recognition) with fingerprint biometric to enhance security of fingerprint biometrics. This method is also known as Two or N-factor authentication technique. The main drawback of this method, we required another biometric capture device.

- **Protecting Biometric Templates with Cryptography/Data hiding** Cryptography focuses on methods to make encrypted information meaningless to unauthorized parties,whereas data hiding is based on concealing the privacy information itself. This is also very good technique to enhance the security of fingerprint biometrics.

IX. CONCLUSIONS

This paper provides a review of existing fingerprint biometrics technology Fingerprint biometrics is the cheapest, fastest, most convenient and most reliable way to identify someone. Fingerprint authentication has many usability advantages over traditional systems such as passwords. We discussed some solutions regarding privacy and security of fingerprint biometrics and how can be improve privacy and security of it. Future research work can be carried out toimprove the quality of the images by improving the imageenhancement techniques and to develop a better matchingtechnique for partial and rotated fingerprint images.

REFRENCES

[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] Ahonen, Timo, Abdenour Hadid, and Matti Pietikainen. "Face description with local binary patterns: Application to face recognition." IEEE transactions on pattern analysis and machine intelligence 28.12 (2006): 2037-2041.

[3] Khalil-Hani, Mohamed, Muhammad N. Marsono, and Rabia Bakhteri. "Biometric encryption based on a fuzzy vault scheme with a fast chaff generation algorithm." Future Generation Computer Systems 29.3 (2013): 800-810.

[4] Sharma, Kirti, and Parul Agarwal. "Review Paper on Fingerprint Biometric and Security".

[5] Bhattacharyya, Debnath, et al. "Biometric authentication: A review." International Journal of u- and e-Service, Science and Technology 2.3 (2009): 13-28.

[6] Anthony Delehanty"Security Issues in Biometric Identification" (2011) Bahria University Journal of Information & Technology Vol. 4, Issue 1August 2011.

[7] Aleksandra Babich "Biometric Authentication. Types of biometric identifiers "(2012) Haaga-Hella, university of applied science

[8] 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