Biometric: Fingerprint Recognition for Authentication

Lovepreet Kaur

Assistant Professor in PG dept. of Computer Science & Applications

Swami Ganga Giri Janta Girls College,Raikot(Ludhiana) Punjab, India

Email-Id:lovepreetkaur12378@gmail.com

Abstract: Biometrics system verifies the personal identity by measuring and analyzing unique characteristics. There are various biometric techniques for recognition but from all of them recognition done by fingerprint technique is best. Fingerprint technique like easy to use, high stability, reliability, high acceptance in identification and authentication, fingerprint technique is used mostly. Fingerprint recognition for authentication is one of the oldest and most reliable biometric used to authenticate a person's identification. Human's fingerprints remain unchanged for lifetime and are unique for each person. In this Paper, study of fingerprint in biometric recognition is taken place. I would like to discuss the process of fingerprint recognition for authentication.

Keywords: - Biometrics, fingerprint recognition, identification, verification, Authentication

I. INTRODUCTION

Biometric systems conduct on behavioral (e.g. Signature, gait, speech) and physiological biometric data (e.g. fingerprint, iris, face, palm print) to identify a person. Biometrics technology can be used to prevent unauthorized access to cellular phones, smart cards, ATMs, desktop PCs, workstations, and computer networks. Biometrics system provides more security to user because in biometric system there is no need to remember passwords or PINs, so there is no chance of stolen or forgotten the passwords or PIN. Fingerprint is preferred to biometric system that is widely used in various authentication applications such as PC logon, and gate access control systems. Fingerprint can achieve the best balance among authentication performance, cost, size of device, and ease of use.

Fig.1.biometric traits

II. FINGERPRINT RECOGNITION

Human's fingerprint is comprised of ridges and valleys. The dark area of the fingerprint is known as ridges and the valleys are the white area that exists between the ridges. In Fingerprint recognition fingerprint is compared against another fingerprint to determine if the impressions are from the same finger or palm. It divided into two sub-domains: fingerprint verification and fingerprint identification.
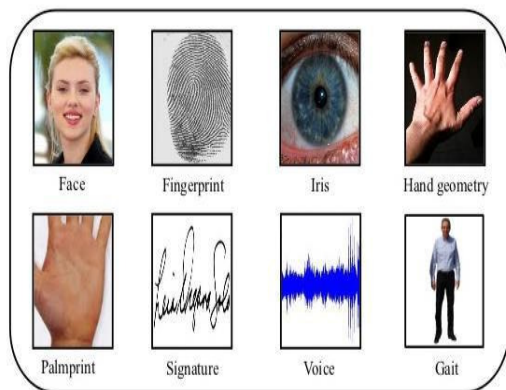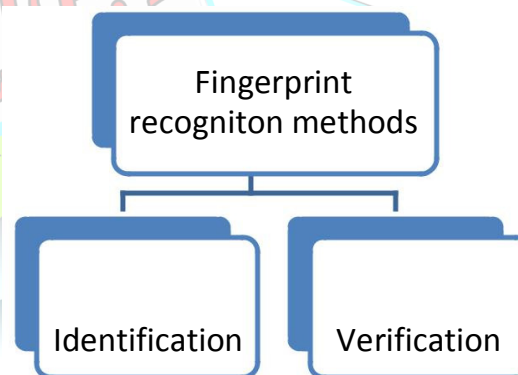

Fig.2. Sub-domains

i. **Fingerprint verification**: In this method, the system compares an input fingerprint to the "enrolled" fingerprint of a specific user to determine if they are from the same finger. Verification is mainly used to verify a person's authenticity. One-to-one comparison of a submitted biometric characteristic (sample) set against specified stored biometric references, and returns the comparison score and decision. Fingerprint verification process is also called, one-to-one matching.

Fingerprint identification: This method is used to specify any person's identity by his/her fingerprint. Identification is adopted for criminal fingerprint matching. One-to-many comparison is made to establish the identity of the individual. Fingerprint identification process is also called, one- to many matching.

III. FINGERPRINT RECOGNITION PROCESS

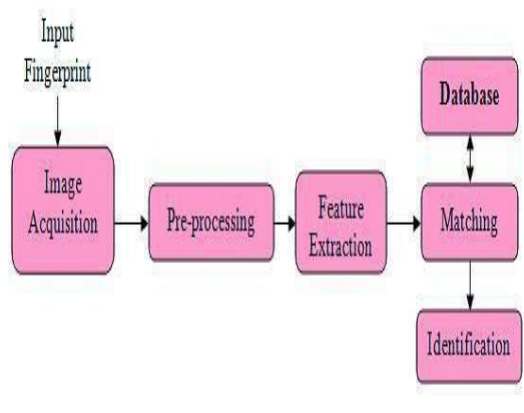The **process of fingerprint recognition** consists of four stages that are explained below.

Fig.3. Diagram of fingerprint recognition process

1. **Image Acquisition**:-This is the first phase in which image of Fingerprint is first acquired with the help of sensors. Images may be blurred or may contain noises, which decreases the quality of an image and directly affect the performance rate of Fingerprint recognition system.

2. **Pre-processing:** it consists of Image filtering and enhancement. Input image is processed to remove the noise and blurring effect. Fingerprint image enhancement is used to make image clear for better use which is very easy to handle and can operate easily for further operation. Sometimes human fingers comes in contact with the most of the manual tasks we perform like fingertips become dirty, cut, worn, scarred, creased, dry, wet, etc. The image enhancement step is designed to remove noise with help of filters in this phase.

3. **Feature Extraction:** In this stage, the preprocessed image is used to extract the features .Fingerprint images are categorized into three levels.
   a. **Level 1**: The ridges are parallel. They are divided as delta, loop and Whorl.
   b. **Level 2**: In this level the ridges are not in order. Ridges are classified as ridge ending, ridge

bifurcation, lake, independent ridge, point or island, spur and crossover.
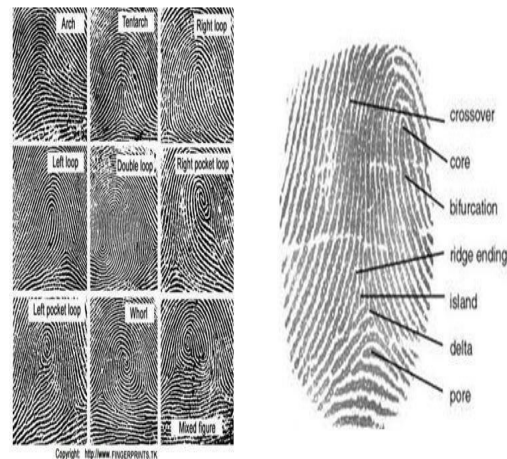   c. **Level 3**: in which Intra ridge details are detected.

Fig.4. Fingerprint patterns

4. Matching: After feature extraction next phase is matching process. This phase identifies Similarities between recognition templates and master template. Input images are matched with master templates that are already stored in database.

IV. FINGERPRINT MATCHING TECHNIQUES

There are various approaches of fingerprint matching which are classified basically into three categories:

Correlation-based fingerprint matching: The correlation-based fingerprint verification first selects characteristic templates in the primary fingerprint. In second step, template matching is used to find the positions in the secondary fingerprint at which the templates match best. Finally, the template positions in both fingerprints are compared in order to make the decision whether the prints match.

Minutiae-based fingerprint matching: It is widely used for fingerprint verification. In this method first, Fingerprint image is enhanced using Fast Fourier Transform and converted to binary image for further processing. In the next step, image is thinned and minutiae are extracted. In the final step, minutiae pairs of two fingerprints are matched to get matching score. This method finds the similarity between input minutiae sample and the stored minutiae sample without using the tiring investigation.

Pattern-based fingerprint matching: This algorithm compares the basic fingerprint patterns

(arch, whorl, and loop) with stored template and a candidate fingerprint. It requires that the images be aligned in the same orientation. The algorithm finds a central point in the fingerprint image and centers on that. The template contains the type, size, and orientation of patterns within the aligned fingerprint image. Pattern-based templates involve making a graphical comparison of the two templates and determining a measure of the difference. The greater the difference the less likely the prints match.

IV. HOW DOES FINGERPRINT SCANNER WORKS

There are various ways to get an image of somebody's finger. The most common Scanners for scanning are explained below.

1. Optical fingerprint scanners:

These are the oldest method of capturing and comparing fingerprints. As the name suggests, this technique relies on capturing an optical image, essentially a photograph. In this technique algorithms are used to detect unique patterns on the surface, such as ridges or unique marks, by analyzing the lightest and darkest areas of the image. It works by shining a bright light over fingerprint and taking what is effectively a digital photograph. The image feeds into

a computer scanner. The scanner uses a light-sensitive microchip (either a CCD or a CMOS image sensor) to produce a digital image. The image is automatically analyzed by computer and it selects the fingerprint, and then uses sophisticated pattern-matching software to turn it into a code.

2. Capacitive fingerprint Scanner:

The most commonly found type of fingerprint scanner used today is the capacitive scanner. Instead of creating a traditional image of a fingerprint, capacitive fingerprint scanners use arrays tiny capacitor circuits to collect data about a fingerprint. As capacitors can store electrical charge, connecting them up to conductive plates on the surface of the scanner allows them to be used to track the details of a fingerprint. In this type of scanning, it measures finger electrically. When finger rests on a surface, the ridges in fingerprints touch the surface while the hollows between the ridges stand slightly clear of it. There are varying distances between each part of human's finger and the surface below. The picture of fingerprint is builds up by measuring these distances**.**

3. Ultrasonic fingerprint Scanner:

To actually capture the details of a fingerprint, the hardware consists of both an ultrasonic transmitter and a receiver. An ultrasonic pulse is transmitted against the finger that is placed over the scanner. Some of this pulse is absorbed and some of it is bounced back to the sensor, depending upon the ridges,

pores and other details that are unique to each fingerprint. It is obvious that the reflected ultrasonic wave would have different intensity level than the one transmitted, mostly reduced as some amount of the pulse gets absorbed into the skin. The intensity levels are different for the waves reflected pulses from different points on the finger and create an image of human's fingerprint.

V. CHARACTERISTICS FINGERPRINT RECOGNITION

i. The fingerprint based biometric system is quite low in cost as compared to others like iris and face readers.
ii. Fingerprint biometric systems are quite strong and can be establish across any kind of environment.
iii. This system is less intrusive than iris or retina scans. Most people find it unacceptable to have their pictures taken by video cameras or to speak into a microphone.
iv. Finger based systems are more user friendly. Besides, the ability to enroll multiple fingers makes this a very flexible option.
v. It is a proven technology and has been in use for a long time as compared to other nascent technologies.
vi. Fingerprint sensors are best for devices such as cell phones, USB flash drives, notebook computers and other applications where price, size, cost and low power are key requirements.
vii. Fingerprint biometric systems are also used for law enforcement,dermatoglyphics,Forensics,background searches to screen job applicants, healthcare and welfare.

VI. CONCLUSION

I like to conclude that Finger print biometrics is one of the efficient, secure, cost effective, ease to use technologies for user authentication .Fingerprint Recognition is used in many applications like biometric measurements, solving crime investigation, terrorist identification and also in security systems. The above discussion was an effort to understand how fingerprint recognition is used as a form of biometric to recognize identities of human beings.

REFERENCES

1. Sravya. V, Radha Krishna Murthy,Ravindra Babu Kallam, Srujana B , "A Survey on Fingerprint Biometric System" ,*International Journal of Advanced Research in Computer Science and Software Engineering ,* Volume 2, Issue 4, April 2012 ISSN: 2277 128X

2. Manisha Sharma, Deepa Verma*, "A Comparative Analysis on Various Techniques of Fingerprint Recognition"*, International Journal of Engineering Research & Technology (IJERT) ,Vol. 2 Issue 11, November – 2013 ISSN: 2278-0181

3. Vishakha Bhadane, Manojkumar Deshpande, Prashant Mishra, *"REVIEW ON FINGERPRINT RECOGNITION METHODS",* International Journal

of Advanced Computational Engineering and Networking, ISSN: 2320-2106, Volume-2, Issue-2, Feb.-2014

4.   Cynthia D'Souza N, Leeda Jovita Rodrigues , Nausheeda B.S*,"A SURVEY ON FINGERPRINT RECOGNITIONTECHNIQUES",* International Journal of Latest Trends in Engineering and Technology Special Issue SACAIM 2016, pp. 441-447 e-ISSN:2278-621X

5.   Praveen Shukla, Rahul Abhishek, Chankit Jain*, "Fingerprint Recognition System",* International Journal of Engineering Development and Research (www.ijedr.org) 3140 , © 2014 IJEDR | Volume 2, Issue 3 | ISSN: 2321-9939 IJEDR1403054

6.   Jyotika Chopra and ,Dr. P.C. Upadhyay *,"Various FingerprintEnhancementsandMatching Technique",* International Journal of Electronics and Communication Engineering. ISSN 0974-2166 Volume 5, Number 3 (2012), pp. 279-289 © International Research Publication House http://www.irphouse.com

7.   Rahul Sharma, Nidhi Mishra, Sanjeev Kumar Yadav, "Fingerprint Recognition System and Tehniques: A Survey", International Journal of Scientific & Engineering Research, Volume 4, Issue 6, June-2013 1670 ISSN 2229-5518 IJSER © 2013 http://www.ijser.org

8.   Mohammed Nasir Uddin, Selina Sharmin, Abu Hasnat Shohel Ahmed , Emrul Hasan, Shahadot Hossain, Muniruzzaman*, "A Survey of Biometrics Security System",* IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.10, October 2011

9.   Sulochana Sonkamble, Dr. Ravindra Thool, Balwant Sonkamble*,"SURVEYOFBIOMETRIC RECOGNITIONSYSTEMSANDTHEIR APPLICATIONS"* Journal of Theoretical and Applied Information Technology © 2005 - 2010 JATIT

10. http://ieeexplore.ieee.org

BIOGRAPHY

Author Name: Ms. Lovepreet Kaur
Designation: Assistant Professor
Department: Post Graduate Department of
                Computer Science and Applications
Qualification: B.C.A., M.C.A.