IJCSC 0973-7391 Volume 8 • Issue 2 March 2017 - Sept 2017 pp. 174-179 available online at www.csjournals.com

Overview of Fingerprint Based Biometric System

Pooja Chaudhary
Chaudharypooja348@gmail.com

Abstract: Biometric fingerprints are one of the most permanence biometric system, that is widely used in various identification and authentication applications. Fingerprint- based Biometric system is very well-known and oldest form of biometrics, the reason can be considered that it is highly reliable, unique and uses distinctive features of fingers. Human fingerprint image exhibits, some pattern of ridges and valleys (minutiae) found on the surface tips of a human finger to identify an individual. Furthermore, the system requires the user's finger surface to have a point of minutiae or pattern in order to have matching images. Most of fingerprint authentication have some problems associated with it ,that is to be solved. Problems can be captured images are easily affected by the condition of finger surface, fake fingers etc. This paper is mainly concerned with principles of fingerprint biometric system, the generalize algorithms to recognize fingerprints and also looked up into various methods to overcome the above disadvantages in fingerprint biometric system.

Keywords: Fingerprint biometric system, fingerprint patterns, identification and authentication, Minutiae Matching, Fingerprint deformations, Multimodal biometric system.

I. INTRODUCTION

A biometric system is a technological system that uses information about a person to verify identity or claimed identity of that person. Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals.

Biometric identifiers that are used to identify individual's identity are often categorized as physiological versus behavioral characteristics. A physiological biometric would identify by one's face, fingerprint, handprint, iris or DNA. Behavioral biometrics are related to the behavior of a person, including keystroke, signature or voice.[1]

Biometric systems rely on specific data about unique biological traits in order to work effectively and able to uniquely identify individual's on the basis of these traits.

II. IDENTIFICATION AND AUTHENTICATION

Biometric identification and verification system are defined as:

A. Identification (1: n):

In an identification system, an individual is recognized 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 individual to be identified does not have to claim an identity (*Who am I?)[2].*

*B.Verification (authentication)***:** In a verification system, the individual to be identified has to claim his/her identity (*Am I whom I claim to be?)* and this template is then compared to the individual's biometric characteristics. The system conducts one-to-one comparisons to establish the identity of the individual.[2] Before a system is able to verify/identify the specific biometrics of a person, the system requires something to compare it with. Therefore, a profile or template containing the biometric properties is stored in the system. Recording the characteristics of a person is called enrollment .[3]

The processes of enrollment, verification, and identification are depicted graphically in fig. 1

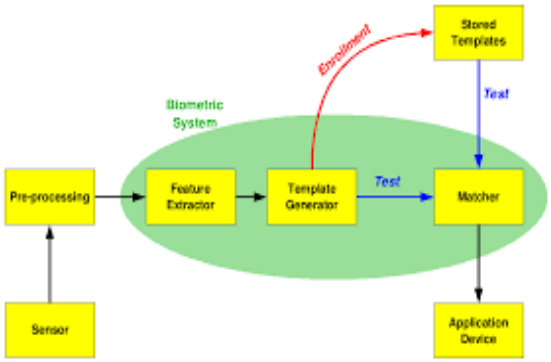


Fig. 1.Enrollment, verification and identification

III. FINGERPRINT BIOMETRIC SYSTEM

Fingerprint recognition is the technology that verifies the identity of a person based on the fact that everyone has unique fingerprints. It is one of the most heavily used and actively studied biometric technologies. known only by the user. For e.g. - authentication require pin and password.

A. Fingerint Patterns:

The following 5 patterns that appear on our fingerprints generally explain one's personality, each pattern on each different finger may be explained differently with different analysis. The most common fingerprint patterns are as given

below and also shown in figure 2:

(1) *Simple Arch Patterns***:**

Form**:** hill-shaped, curved top, no triangle was

Formed in with the shape.

Characteristics**:** hard working, introverted, cautious, works without complaint, do not like taking risks.

(2) Tented Arch Pattern:

Form**:** like a camping tent with a sharp tip top. Characteristics**:** with extreme personalities, can be outgoing and welcoming one day and shy the other; it all depends on how nurture and development during childhood. Not afraid of challenges and obstacles, but may sometimes be impulsive.

(3) Ulnar Loop Patterns

Form**:** like a waterfall flowing towards the little finger with triangular points.

Characteristics**:** gentle, observant, passive, likes

To go with the flow, little self- motivation.

(4) *Concentric Whorl Patterns*

Form**:** Lines starting from the center of the small circle, the lines on finger tip appear to be a complete circle and spread out like concentric circles with two triangular points.

Characteristics**:** Self-centered, likes competition.

(5) Spiral Whorl Patterns

Form**:** A spiral pattern starting from the center and move outward, has two triangular points. Characteristics**:** Self motivated; Parents should encourage accordingly.

ARCH

LOOP

WHORL

B. Principles of fingerprint biometrics

There are three fundamental principles of fingerprints are as follows:

1.A fingerprint is an individual characterstic –out of which the millions of sets of prints that have been taken ,no two individuals have been found to have the same fingerprints ,not even identical twins.

2. A fingerprint will remain unchanged during an individual's lifetime-The ridges on the grasping surface of hands and on the soles of feet are present at birth and remain unchanged for life except for size as growth occurs.

3. fingerprints have general ridge patterns classified as:[4]

Arches;5%population

Loops;60-65%

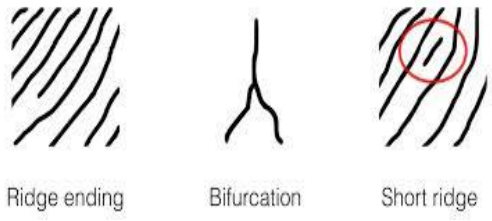
Whorls; 30 - 35 %

C. How does fingerprint biometrics work

There are various main technologies used to capture the image of finger by various sensors like optical, silicon, and ultrasound are used to capture fingerprint image . There are two main algorithm families to recognize fingerprints:

1) Patterns: The three basic patterns of fingerprint ridges are the arch, loop, and whorl.[5] An arch is a pattern where the ridges enter from one side of the finger, form a rising arc in the centre, and then exit from the other side of the finger. The loop is a pattern where the ridges enter from one side of a finger, form ing a curve line, and then it exit from the same side form where they entered. In the whorl pattern, ridges form circularly around a central point on the finger. Pattern matching comparisons are done on the basis of the overall characteristics of the fingerprints, not only by the points of individual points. Fingerprint characteristics can include sub-areas of certain interest including ridge thickness, curvature, or density. During enrollment, small sections of the fingerprint and their relative distances are extracted from the fingerprint.

2) Minutia features: The major Minutia feature of fingerprint ridges are: ridge ending, bifurcation, and short ridge (or dot). The ridge ending is the point at which a ridge terminates. Bifurcations are points at which a single ridge splits into two ridges. Short ridges (or dots) are ridges which are significantly shorter than the average ridge length on the fingerprint. Minutiae and patterns are very important in the analysis of fingerprints since no two fingers have been shown to be identical. Minutia matching comparisons specifies the specific details that are within the ridges of fingerprints. At the time of enrollment, the minutia points are located, together with their relative positions to each other and their directions. At the matching stage, the fingerprint image is processed to extract its minutia points, which are then compared with the registered template.[4]



D. advantages of fingerprint biometric systems

- Very high accuracy.
- Is the most economical biometric PC user authentication technique.
- it is one of the most developed biometrics
- Easy to use.
- It is standardized.

E. Disadvantages fingerprint biometric systems

- Some people have damaged and eliminated fingerprints.
- Vulnerable to noise and distortion due to dryness or dirt on the skin of finger.
- using fake fingers by attackers.

IV.FINGERPRINT DEFORMATIONS

Acquiring high-quality images of distinctive fingerprint ridges and minutiae is a complicated task. People with no or few minutiae points (surgeons as they often wash their hands with strong detergents, people with special skin conditions) cannot enroll or use the system. The number

of minutiae points can be limiting factor for security of the algorithm. Results can also be confused by false minutiae points (areas of obfuscation that appear due to low-quality enrollment or fingerprint ridge detail).So fingerprint deformation are those factors that can affect/reduce system performance. Various fingerprint deformations are given below.[6]

- Cold finger
- Dry/oily finger
- High or low humidity
- Angle of placement
- Pressure of placement
- Cuts to fingerprint

V. MULTIMODAL BIOMETRIC SYSTEM

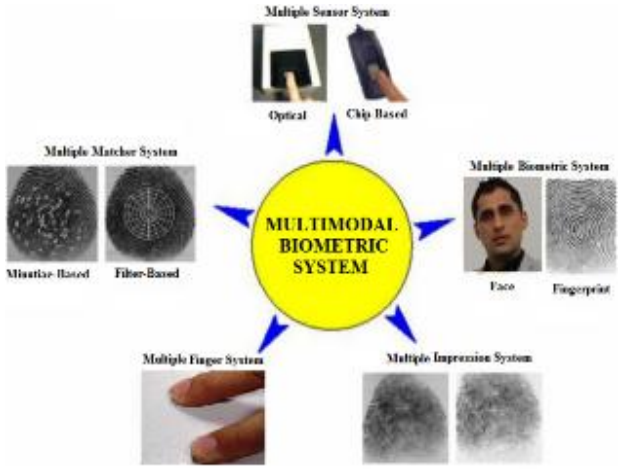
Multimodal biometrics System refers to the use of a combination of two or more biometric modalities in a verification/identification system. Identification based on multiple biometrics represents an emerging trend. The main disadvantages are overcome by this system. we have two approaches to follow up:-

A. Using more than one finger

As we have ten fingers we can use more than one finger for higher accuracy and security. The number of fingers we choose is directly propotional to the realiability of system.[4]

B. Using other biometric factors

In this we use different modalities to improve recognition rate. for example if we integrate face recognition, fingerprint making personal identification. we can get advantage over the problem of single biometrics.



VI. FAKE FINGERPRINT DETECTION

It is ongoing research problem to detect whether the fingerprint image is taken from the real or fake fingertip. It can be resolved by liveness detection[7], this system detect whether the fingerprint is alive or not.

Fingerprint scanners can be spoofed by artificial fingers using moudable, plastic, clay etc.

Fake fingerprint detection approach:

There are different methods to check to check liveness of scanned finger

- Temperature sensing
- Pulse oximetry
- Electrical conductivity[8]

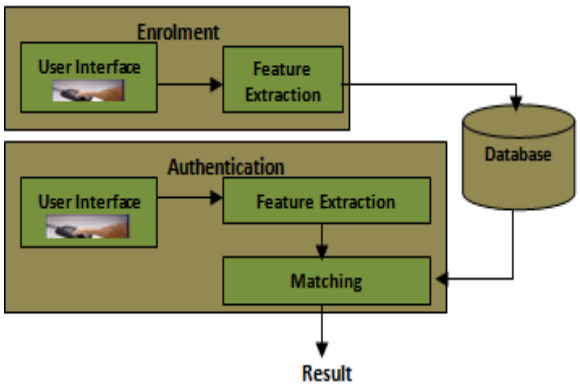
By considering these properties we can use sensors to sense real or fake fingers.

Table 1: comparison of various biometric traits

Biometric Technology	Accuracy	Co	Social acceptability
Fingerprint	High	Medium	Medium
Voice	Medium	Medium	High
Face	Medium- L	Medium	High
Hand	Medium	Medium	High
Iris	High	High	Medium-Low

VII. FINGERPRINT BASED AUTHENTICATION

Fingerprint authentication or recognition is one of automated method of verifying a match between two human fingerprints. Fingerprints are one of many forms of biometrics used to identify individuals and verify their identification. System as shown below in the fig.3.



All fingerprint based authentication are based on one the following 3 matching technique for fingerprint matching

A. Minutiae based Extraction Technique:

Most of the fingerprint technologies are used minutiae extraction techniques. Minutia based techniques characterize the fingerprint by its feature types, ridge terminations and ridge bifurcations. Minutia based technique first find minutiae points and then map their relative placement on the finger .This technique of fingerprint recognition is the most commonly used. [9]

B. Correlation Based Technique

In correlation based matching techniques initially two fingerprint images are superimposed and then the correlation between consequent pixels is calculated for different alignments.[10] The correlation based method is used over minutiae based methods so that it will be able to overcome difficulties of minutiae method

C. . Hybrid Based Technique

A hybrid fingerprint matching scheme that uses both minutiae and ridge, flow information to represent and match fingerprints.

VIII. RELATED WORK

Many studies have been done on impact of biometric in our life. Biometric provide better security concerns with respect to traditional approaches like token, pin, password etc.

Fingerprint authentication provide more realibility, uniqueness and security . Keuning, T. van der Putte j [3]performed "Fingerprint recognition". The authors proposed the concept of obtaining minutiae pattern using matching techniques that is better for the finger print.

Manvjeet kaur and akshay girdhar have discussed fingerprint authentication using minutae extraction based algorithm.[8] Biometric system has wide scale use in both public and private sectors due to security and authorized identity. It also used in various applications. The author also defines many different biometric technology like hand geometry, fingerprints, retina scanning, face recognition etc. with their impacts in different application. But most realiable and durable is fingerprint. At the end author discussed biometric technology used for border control and fight against terrorism. Biometric in real life, it is not 100% perfect but it provides better results in different fields to enhance privacy and security.

IX. CONCLUSION

Biometrics is a means of verifying personal identification of human by measuring and evaluating unique characterstics like fingerprints. This paper presents an overview of fingerprint biometric system and focued on the various matching techniques used in fingerprint authentication.this paper mainly reveals about methods to overcome disadvantages of fingerprint biometric system.

Fingerprint Biometric systems are almost used in all fields except in chemical industries because of chemicals fingers get affected, therefore these firms are not using fingerprint authentication. They rely on multimodal concept that is dicussed in this paper. Still, Fingerprint

authentication systems can be very useful if used in the right applications under the right situations.

We like to conclude that fingerprint biometrics is one of the efficient, reliable, easy to use, secure, cost effective technology for user authentication and according to our survey all drawbacks are also recoverd in this fingerprint biometric system.

REFERENCES

[1].Anil K Michigan State University, E. Lansing, Michigan, Ruud Bolle and Sharnath Pankanti IBM, T.J Watson research,"Biometric Personal Identification In Networked Society," Kulwer Academic Publishers New York, Boston,London, Moscow, 2002

[2]. D. Maltoni, D. Maio, A. K. Jain and S. Prabhakar," Handbook of FingerprintRecognition," Springer Verlag, New York, NY, USA, June 2003.

[3]. T. Van Der Putte And J. Keuning,"Biometrical Fingerprint Recognition: Don't Get Your Fingers Burned," In Proceedings Of IFIP TC8/WG8.8 Fourth Working Conference On Smart Card Research And Advanced Applications, Kluwer Academic Publishers, September 2000, pp. 289-303.

[4]. 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, pp. 307-311

[5]. Dileep Kumar, Yeonseung Ryua, "Brief Introduction Of Biometrics And Fingerprint Payment Technology" http://www.sersc.org/journals/IJAST/vol4/4.pdf

[6]. Arun Kumar Yadav, Sanjiv Kumar Grewal, IJCSC, Volume 5, NO. 1, March-September2014, pp-37-42.

[7]. Fingerprint liveness detection based on quality measures, IEEE, 08 July 2009

[8]. Utilizing Characteristic Electrical Properties of the Epidermal Skin Layers to Detect Fake Fingers in Biometric Fingerprint Systems—A Pilot Study, 16 April 2007.

[9].Manvjeet Kaur, Mukhwinder Singh, Akshay Girdhar, and Parvinder Sandhu, "Fingerprint Verification System using Minutiae Extraction Technique", World Academy of Science, Engineering and Technology 46 2008

[10]. Monika Sharma, "Fingerprint Biometric System: A Survey," International Journal Of Computer Science And Engineering Technology, IJCSET, Volume 5, No. 7 July 2014