International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue II, February 2018- Available at www.ijraset.com

Fingerprint Recognition System: Issues and Challenges

Munish Kumar[1], Priyanka[2]
[1]*ECE Department, D.C.R. University of Sciences & Technology, Murthal*

Abstract: Fingerprint Recognition (FPR) Systems are an automatic system that confirms the identity of a person or verifies the person based on fingerprint patterns or features. The analysis of finger for matching purposes is done by comparing extracted features from fingerprints. This paper presents the basic steps used in FPR system, various matching techniques, identification keys and challenges in fingerprint recognition system. An overview is provided for research and development in the field of FPR system.

Keywords: Fingerprint System, Biometric, Physiological, Behavioral.

I. INTRODUCTION

This is an era of competition, speed, quality & fast growth of the business. The globalization has pushed the competition on the fast track and made it hard & tough. To convert the dreams of the organization into reality and face the competition of the Global market, the use of information & technology became compulsory. But the use of information & technology has attracted some threats in the shape of evils & frauds by way of the cyber-crimes. Thus, such systems are needed to be used, which can identify the person duly authorized by the organization for its access by some method. Many methods such as password & PIN (Personal Identification Number) protected etc. can be decoded by the hackers. The best method for authentication is the biometric system. The biometric information never matches with another person because the biometric information is unique by the gift of God/Nature and cannot be stolen. After adopting such system, all types of security issues like internet/cyber-crime may be almost eliminated. Biometric information may be physiological that are related to the shape of the body of a person i.e. face, fingerprint, hand, iris & DNA (Deoxyribonucleic acid) or may be behavioral characteristics of a person i.e. keystroke, signature & voice [1]. The fingerprint is a type of physiological information and mostly used biometric for authentication. The fingerprint is one of the unique characteristics that every individual is having and it is widely used for recognition & authentication in digitized systems. It plays a key role for identification in biometric systems. Fingerprint recognition systems have been used for security purposes for a long time i.e. criminal identification, authentication & verification. Fingerprint systems that have been used for one to one matching are known as verification systems and that have been used for one to many matching are known as identification systems. Verification is used to authenticate the person to use a system and identification is used to know the identity of the person [2] [3].

II. ANALYSIS OF DIFFERENT BIOMETRIC INFORMATION

In this section, comparison of different biometrics information is presented based on the different parameters. As there are many biometrics information that can be used for authentication. Parameters used for accuracy or to compare different biometric system are FAR (False Acceptance Rate), FRR (False Reject Rate) & EER (Equal Error Rate). If unauthorized users want to access the system and wrongly accepted by the system due to hacking or any other reasons, then this acceptance is called false acceptance. The FAR is defined as the ratio of the number of the false acceptances to the number of identification attempts [3]. If an authorized user wants to access the system and wrongly rejected by the system due to hacking or any other reasons, then this rejection is called false reject. The FRR is defined as the ratio of the number of the false rejections to the number of identification attempts. EER is defined as the value at the point of intersection between the FAR & FRR. At this point the value of FAR & FRR is same. The performance of the system increases with a decrease in the value of EER. Table 1 summarizes the analysis of different biometrics information according to different parameter [4].

Table 1 Analysis of different Biometric Information [3][4][5].

S. No.	Biometric Type / Facts	Signature	Voice Recognition	Face Recognition	Iris Scan	Hand Scan	Fingerprint Recognition
1	Uniqueness	L	L	L	H	M	H
2	Accuracy	L	M	M	H	M	H
3	Acceptance	VH	H	M	M	H	M
4	Performance	L	L	L	H	M	H
5	Stability	Average	Average	Average	H	Average	H
6	Identification & Authentication	Both	Authentication	Both	Both	Authentication	Both
7	Interference	Changeable or Easy Signature	Noise, Cold	Age, angle of view, Facial Expression	Glasses & Irritation	Arthritis, Rheumatism	Dirtiness, Injury & Roughness
8	Uses	Industrial	Remote access in bank or data base etc.	General	Nuclear Installations, Medical Services etc.	General	Police, Industrial etc.
9	Easiness of the use	Average	H	H	H	H	H
10	Reliability	H	H	H	VH	H	H
11	Market Share	2.7%	4.3%	15.4%	6.2%	10.4%	48.8%
12	Cost	M	M	M	H	L	M
13	FAR	2-5%	2000 to 5000 in 100,000 (2-5%)	100 to 1000 in 100,000 (.1-1%)	>=.001%	10 to 20 in 1000 (1-2%)	1 to 10 in 100,000 (.001-.01%)
14	FRR	10 to 20 in 100 (10-20%)	10 to 20 in 100 (10-20%)	10 to 20 in 100 (10-20%)	2 to 10 in 100 (2-10%)	1 to 2 in 100 (1-2%)	3 to 7 in 100 (3-7%)
H-High, M-Medium, L-Low, VH-Very High, FAR-False Acceptance Ratio, FRR-False Reject Ratio							

There are many technologies exist in the market to identify and authenticate the user in the field of automated security systems. According to the requirement or uses, one can easily select the biometric system/type. From above table, we can conclude that fingerprint recognition is widely used technology in the market and after that face recognition & hand scan is used for the biometric system. Fig. 1 shows the popularities/market share of different biometric systems in the market [6].

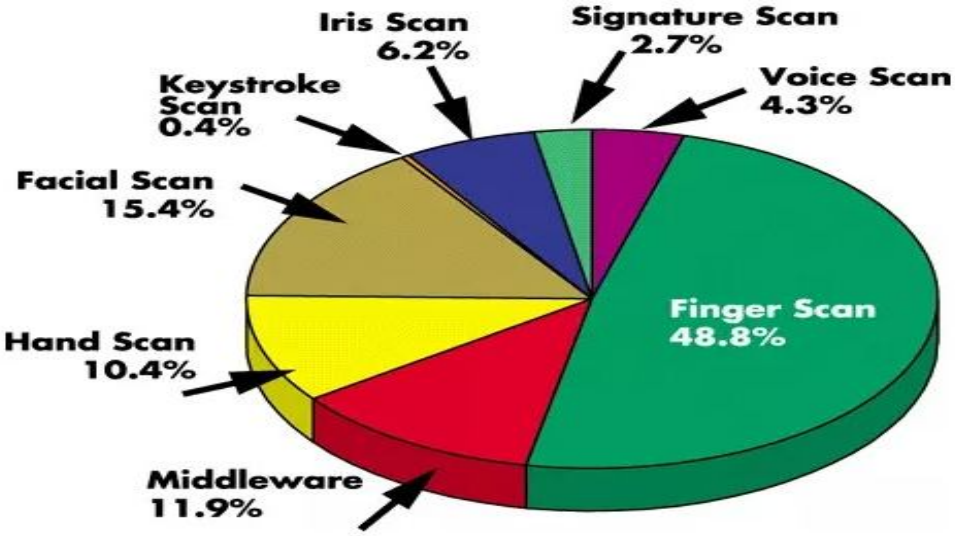

Fig. 1 Biometric Market Share [6]

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor : 6.887
Volume 6 Issue II, February 2018- Available at www.ijraset.com

III. BASIC STEPS IN FPR (FINGERPRINT RECOGNITION) SYSTEM

In this section, basic steps of FPR system are discussed. The basic block diagram of fingerprint recognition systems is shown in fig. 2. The sensor may be a type of audio sensor, a video sensor, and an image sensor. In FPR system the image of the fingerprint is acquired by the sensor. Then in pre-processing step, the fingerprint image is enhanced to a very good level, so that feature extractor clearly extracts the features from the image and from that features

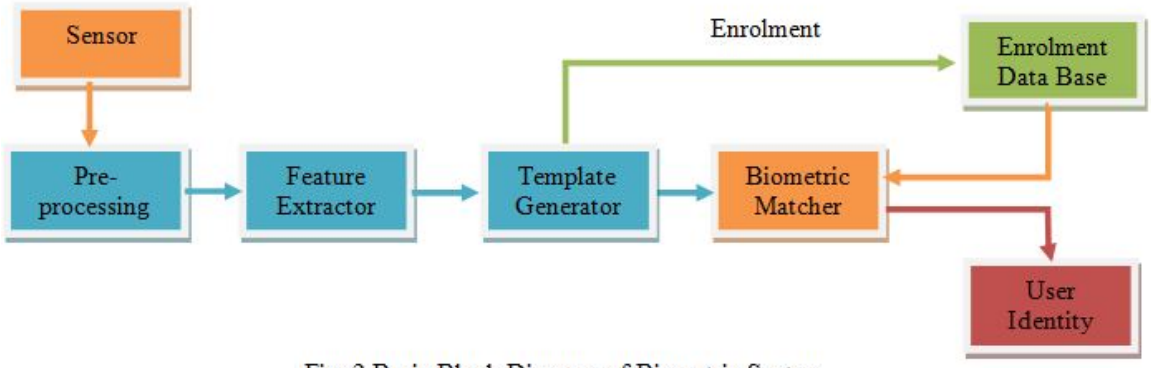

Fig. 2 Basic Block Diagram of Biometric System

template is generated by the template generator for enrolment purpose and for matching purpose. In enrollment process, the template is stored in the database for future purposes and in matching process identification & verification of a person is done by the biometric matcher. And finally, a matching is done at biometric matcher [7]. For finding the matching score between the stored template and live template a comparison between them is required. Based on that comparison a matching score is generated by the biometric matcher. Depending on this score the system will decide the authentication of users. Parameters used for the FPR system for accuracy or to compare different algorithms of FPR are FAR, FRR & EER. In FPR systems correct decision means that authorized individual user is accepted, and the unauthorized individual user is rejected and incorrect decision means that authorized individual user is rejected (False Reject) and the unauthorized individual user is accepted (False accept). A good FPR system should have a high probability of correct decision and low for incorrect decision. Strengths of FPR approach may be summarized as below [8]

A. High uniqueness, accuracy, performance & stability.
B. Easy to use and more reliable than other techniques.
C. Low cost and small size.
D. Have approx. 50% popularity in the market as compared to other techniques.

However, FRS has some weaknesses also and these are summarized as below [2][8]:

E. Small area fingerprint sensors may result in less information.
F. The problem of fake fingerprint i.e. clays or dummy printing.
G. Due to finger injuries or cuts users unable to use FRS.
H. Due to cleaning work, their fingerprints are vanishing or faded.

IV. FINGERPRINT CLASSES, MATCHING TECHNIQUES & IDENTIFICATION KEYS

Fingerprints are basically the impression or mark made on a surface or feature pattern of one finger. Fingerprints are widely used biometric characteristics because it offers several advantages. We can classify fingerprints based on pattern types, size, and position of the finger. The three fundamental principles of fingerprints are:

A. A Fingerprint is an individual characteristic.
B. Fingerprint will remain unchanged during an individual's lifetime
C. Fingerprints have general ridge patterns that can be systematically classified.

Based on their visual pattern fingerprints are classified in three classes that are whorls, arch, and loop as shown in fig. 3.

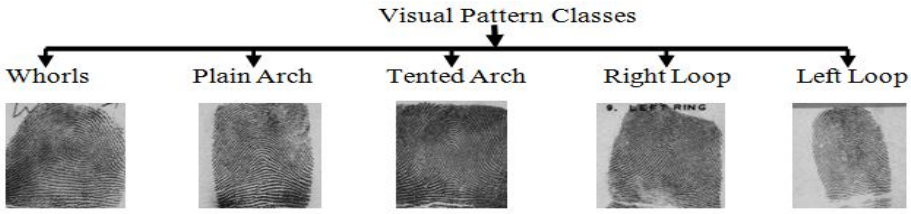

Fig. 3 Visual Pattern Classes [5]

A fact about fingerprint is that 60% of people have loops, 35% have whorls & 5% have arches. Large volumes of fingerprints data are collected in everyday applications. Classification of fingerprints means that collect the fingerprints of same nature/characteristics in pre-defined groups or classes. There are many techniques for classification of data. Classification of fingerprints plays a very important role in FRS. By classifying the fingerprint, the search time is reduced for the system and computational complexity is reduced. The purpose of fingerprint classification is to reduce the matching time during the matching process and to increase the efficiency of the system. In FRS, minutiae are matched, which are basically line patterns of furrows and ridges those give uniqueness to a fingerprint. Uniqueness means that no two people have same fingerprint pattern that is their patterns are unique to each other and not change over time. Even identical twins do not have identical fingerprints [5]. Line type classifications of fingerprints that is a bifurcation, arch, loop, ellipse, sweat gland, island, tented arch, rod & spiral are shown in fig. 4.

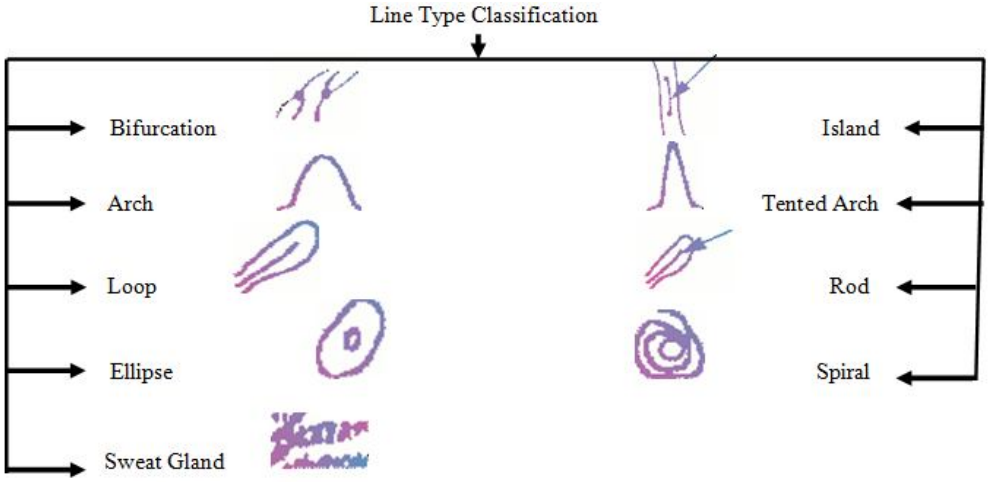

Fig. 4 Line type Classifications

There are various types of fingerprint matching techniques. Matching techniques are responsible for recognition of the fingerprint patterns [11] [4]. A good matching technique provides a better result during matching. Various types of fingerprint matching techniques & identification keys are shown in fig. 5 (a) & (b).

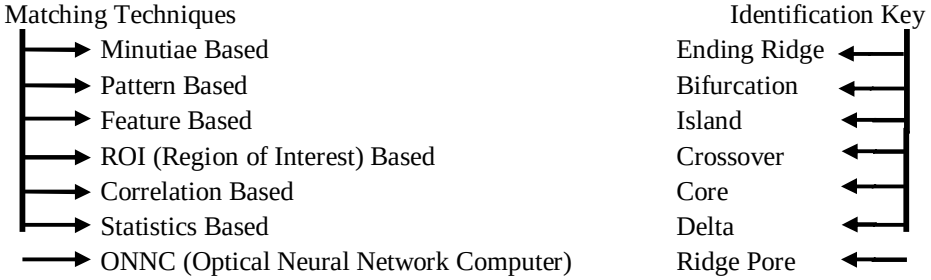

Fig. 5 (a) Matching Techniques (b) Identification Keys

There are two types of matching criteria for fingerprint recognition [7]
reliable and widely used.
Pattern matching: In this process, two images are compared for matching to find how similar they are, often used to find duplicates finger in the database.

D. Challenges In Frs & Applications Of Frs

Biometric systems are extensively used for security purposes & provide wide scope to identify/authenticate the users, thereby removing a lot of burden from the user's end. Fingerprints Recognition Systems are widely used biometric systems for authentication to access the system because of their uniqueness. The uniqueness of fingerprint means that no two people have same/identical fingerprint pattern i.e their patterns do not change over time and unique to everyone. Even identical twins do not have identical fingerprints [5]. There are few areas like sensors, feature extraction techniques & matching techniques etc. which are creating lots of challenges/ problems in implement the Fingerprint Recognition System. The main challenges/problems in FRS are given below:

1) Mismatching due to physical distortion i.e. finger injuries and cuts in fingers.
2) Mismatching due to displacement/rotation while scanning the finger over the sensor.
3) Unauthorized access due to finger plasticity or clay printing.
4) Variability between impressions of the same finger that may be due to skin conditions, noise in the sensor.For researchers, there is a lot of scope in this filed to improve the performance of FRS. For example, one can work to:
5) Use the image processing techniques to improve or enhance the input image to a very good level so that features are extracted more accurately without losing any information.
6) Provide a better algorithm for reducing the mismatching due to physical distortion & displacement etc.
7) By combining different fingerprint recognition algorithms, a new approach with better recognition rate and matching technique may be developed for FRS. Fingerprint recognition system (FRS) has applications in different areas. Some of the main applications are given below [7] [8]:
8) Physical Access control such as Border, Airports etc.
9) Physical Access control in Ministry of Defence & other National Security Organization
10) All type of card security such as ATM, Credit Cards & purchasing cards etc
11) In banking security such as account transaction etc
12) Criminal identification
13) Cardless money
14) Network security & protection
15) National ID system and other personal uses.
16) Electronic commerce & Attendance management.
17) It may be used in voting to avoid bogus poll and generate a fair democracy etc.

III. CONCLUSION

A review on Fingerprint Recognition System is presented for further improvement in the system. Basic steps of FRS are discussed with various matching techniques & identification keys for a better understanding of the system. Analysis of different biometric systems and strengths of FRS are discussed to specify why fingerprint is chosen among other techniques. Challenges are defined in this field to know the task clearly and applications in this area are defined to clear the task practically. A scope for the researcher is presented in this field.

REFERENCES

[1] www.cedarbuffalo.edu/govind/presentations/FingerprintsOverview.
[2] Anil K. Jain, Jijanjiang Feng, Karthik Nanda Kumar "Fingerprint Matching", 0018-9162/10/$26.00 © 2010 IEEE pp 36-44.
[3] http://www.bayometric.com/blog/false-acceptance-rate-far-false-recognition-rate-frr/
[4] Harpreet Saini, Kanwal Garg "Comparative Analysis of Various Biometric Techniques for Database Security" International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064Volume 2 Issue 4, April 2013
[5] https://en.wikipedia.org/wiki/Fingerprint
[6] www.google.com/images
[7] Biometric – Theory « Bio-Metrica, LLC. http://bio-metrica.com/biometric-theory
[8] Priyanka "Fingerprint Recognition Techniques and its Applications" IEEE International Conference on Advances in Engineering & Technology Research (ICAETR - 2014), August 01-02, 2014.
[9] http://www.biometric-solutions.com/solutions/index.php?story=fingerprint_recognition
[10] Jyotika Chopra, Dr. P.C. Upadhyay "Various Fingerprint Enhancements and Matching Technique" International Journal of Electronics and Communication Engineering. ISSN 0974-2166 Volume 5, Number 3 (2012), pp. 279-289.
[11] Kribashnee Dorasamy, Leandra Webb, Prof. Jules Tapamo, Nontokozo P. Khanyile "Fingerprint Classification Using a Simplified Rule-Set Based on Directional Patterns and Singularity Features" 978-1-4799-7824-3/15/$31.00 ©2015 IEEE.
[12] Rosario Arjona and Iluminada Baturone "A Fingerprint Biometric Cryptosystem in FPGA" 978-1-4799-7800-7/15/$31.00 ©2015 IEEE

[13] Diego Gragnaniello, Giovanni Poggi, Carlo Sansone, Luisa Verdoliva "An Investigation of Local Descriptors for Biometric Spoofing Detection", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 4, APRIL 2015.
[14] Omid Zanganeh, Bala Srinivasan, Nandita Bhattacharjee "Partial Fingerprint Matching through Region-Based Similarity" 978-1-4799-5409-4/14/$31.00 ©2014 IEEE.
[15] Pallav Gupta, Srivaths Ravi, Anand Raghunathan, Niraj K. Jha "Efficient Fingerprint-based User Authentication for Embedded Systems" pp- 244-47.
[16] Preethy Prabhakar, Tony Thomas "Finger Vein Identification Based On Minutiae Feature Extraction With Spurious Minutiae Removal" 2013 Third International Conference on Advances in Computing and Communications, 978-0-7695-5033-6/13 $26.00 © 2013 IEEE.
[17] Jithin P. Thomas, K.R.S.N. Kumar, Vamsidhar Addanki, Anu Gupta, Nitin Chaturvedi "Hardware Implementation Of A Biometric Fingerprint Identification System With Embedded Matlab" 2010 International Conference on Advances in Recent Technologies in Communication and Computing, 978-0-7695-4201-0/10 $26.00 © 2010 IEEE.
[18] Fons M, Fons F, Canyellas N, Cantó E, López M "Hardware-Software Co-design of an Automatic Fingerprint Acquisition System" IEEE ISIE 2005, June 20-23, 2005, Dubrovnik, Croatia, 0-7803-8738-4/05/$20.00 ©2005 IEEE.
[19] Yee-Yin Choong, Mary F. Theofanos, and Haiying Guan, "Fingerprint Self-Captures Usability of a fingerprint system with real-time feedback" 978-1-4673-1228-8/12/$31.00 ©2012 IEEE.