Indian Journal of Science and Technology, Vol 8(35), DOI: 10.17485/ijst/2015/v8i35/80504, December 2015
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

A Comprehensive Survey on Fingerprint Recognition Systems

P. Pakutharivu[1*] and M. V. Srinath[2]

[1]Department of Computer Science, Bharathiar University, Coimbatore - 641 046, Tamil Nadu, India; pakutharivu.p@gmail.com
[2]Department of MCA, STET Women's College, Mannargudi - 614 016, Tamil Nadu, India; sri_induja@rediffmail.com

Abstract

Matching finger prints is the most popular biometric technique used for providing authentication. Fingerprint recognition systems scans for raw image, performs little preprocessing, features are extracted as vectors and stored in fingerprint databases. A review on various aspects of fingerprint recognition systems is presented in this paper. The paper briefs various types of fingerprint patterns, followed by minutiae based approach. Fingerprint ridges called minutiae are able to capture the invariant and discriminatory information present in the fingerprint images. Pattern recognition based approach is also studied followed by wavelet based approaches. The challenges and issues relating to fingerprint recognition system are critically reviewed in this paper. It is important for fingerprint recognition system to use good quality, noise free fingerprint image as input to achieve high accuracy. Various fingerprint image enhancement techniques were also analyzed and discussed in this paper.

Keywords: Authentication, Biometrics, Fingerprint, Minutiae, Recognition, Wavelet

1. Introduction

Fingerprint recognition is the automated process of identifying the identity of an individual based on comparison of stored fingerprint information with input fingerprint information. It is one of the most well known biometrics, used for authentication on computer systems. Fingerprints are the impressions/patterns available in human finger. With the age, these impressions get notable but the structures do not change over the time[2].

There exist a number of advantages which makes fingerprint recognition methods popular. One biggest advantage is that it is very well accepted in the legal community. It is the cost effective, quick, reliable and most convenient way to identify a person Fingerprint recognition is widely accepted as highly accurate method of authentication since the chance of two people identical finger prints are scarce[4].

Fingerprints cannot change unless there is a physical disturbance such as accidents or works in an industry with caustic or hot materials which may damage fingerprints[5,6]. This is extremely useful. For example, if parents acquire fingerprints of their children and put it in a file and if they are kidnapped, childhood fingerprints can be used to make a match when they are identified at later stage.

Automated fingerprint recognition systems are having certain pitfalls. It may sometimes require not only fingerprint but also a valid pin, which can be more difficult to use than traditional systems. Sometimes false rejection may happen when the finger print recognition system fails to register someone's fingerprint. This is called type I error[7]. Sometimes fingerprint recognition system may identify a wrong person during authentication process leading to unauthorized access grant. This is called type II error[7]. Hence a good finger print recognition system should overcome type I and type II errors and it should also be accurate.

2. Types of Fingerprint Patterns

The patterns on fingerprint are broadly classified into three categories:

*Author for correspondence

2.1 Arches

Fingerprint patterns where the ridges run from one side to the other side without any turn. Generally there is no delta in an arch pattern whenever there is a delta point, no re-curving ridge intervenes between core and delta points[8]. There exist four types of arches namely:

- Plain Arches.
- Radial Arches.
- Tented Arches.
- Ulnar Arches.

2.2 Loops

Patterns in which the ridges flows inwards and returns in the direction of the origin. Ridgesenter in either side of the impression, re-curves and terminates in the direction of the side where ridges entered. There are four types of loops.

- Plain Loop.
- Lateral Pocket Loop.
- Central Packet Loop.
- Twinned Loop.

2.3 Whorls

Patterns in which ridges form circularly around a central point. Any pattern that contains two or more delta points is whorl patterns. There are four types of whorl patterns.

- Plain Whorls.
- Central Pocket Loop Whorls.
- Double Pocket Loop Whorls.
- Accidental Whorls.

Figure 1. Arches.

Figure 2. Loops.

Figure 3. Whorls.

3. Existing Methods

3.1 Minutiae based Approach

In biometrics and forensic sciences, minutiae refer to specific points in a fingerprint. They are the major features which are used to compare one pattern with another[9]. It includes ridge bifurcation or ridge ending on a finger print. Detected minutia in a fingerprint pattern is identified by a set of attributes such as minutia position, minutia direction and type such as bifurcation or ending. Thus a finger print is represented by a set of minutia present in the fingerprint pattern[10]. Fingerprint can be verified by comparing minutiae points present in two images. Minutia is stored as the composition of attribute values such as minutia position in the fingerprint pattern[10].

Minutia based fingerprint recognition systems are one among the popular methods which achieves very high accuracy. It consists of four steps and they are

- Orientation field estimation.
- Ridge extraction.
- Minutia extraction.
- Post processing.

Accurate representation of a fingerprint pattern depends on accurate extraction and storing of minutia information present in the fingerprint image. And also good representation of finger print pattern is essential because many commercial large-scale systems are dependent on fingerprint recognition systems. A minutia point is recognized as follows:

If the brightness value of a pixel is transposed, ridge endings become bifurcational and vice-versa. The position of the minutia is the tip of the ridge or valley.

Minutia extraction techniques can be broadly classified as binarized fingerprint images and gray scale fingerprint images[11]. Under the binarized fingerprint images, unthinned binarized images, thinned binarized images, chain code based, run representation based, ridge flow and local pixel based, crossing number based and morphology based methods are available.

Under gray scale fingerprint images, we have ridge line flow based and fuzzy based methods[11]. As stated earlier, minutiae based finger print recognition systems achieves high accuracy. However it has the following drawbacks

- Corrupted or noisy images (images with artifacts) cannot be used with finger print recognition systems. High quality fingerprint images are used.
- Minutiae based approaches are slow for real time applications.
- Many times, system fails to recognize actual people.

3.2 Pattern Recognition Approach

Fingerprint contains composition of ridges and valleys called patterns. Pattern recognition methods use patterns for authentication. Pattern recognition is imposing identities of input data by recognizing patterns it contains and relationships it maintains[12]. Pattern recognition approaches are broadly classified as decision theoretic and structural. Quantitative descriptors such as area, length and textures are used to describe a pattern under decision theoretic approach. Relationships of several descriptors are used to describe a pattern under structural approach. The important requirement in this type of fingerprint recognition system is to find the best descriptors that can represent a pattern in a best way[12].

Pattern based fingerprint recognition system works by generating the data, where input is generated. Preprocessing is done so that image becomes clean and free from noise. Next, features are extracted and stored as feature vector. Whenever input parameters are supplied, they are matched with Feature Vector database and based on the outcome, authentication is granted or rejected[13].

3.3 Wavelet based Approaches

Wavelet transforms can be used on fingerprint patterns to provide authentication. Wavelets cut data into different frequency components and each component is studied with a resolution matched to its scale[14]. In this type of approach, fingerprint images are decomposed using Discrete Wavelet transform. Three levels of decomposition of fingerprint images are performed for training. The mathematical tools like mean and standard deviation are also used during decomposition process[14].

For fingerprint classification, patterns are rotated from 0 to 360 degrees and 10 degrees are increased in each step. Set of wavelet statistical values and co-occurrence matrix features are extracted. It is obvious that directional resolving power of wavelets extracts texture information in LL, LH, HL and HH diagonal directions. Moreover, wavelet based fingerprint recognition systems does not require fingerprint image preprocessing or post processing[15]. Hence they are fast when compared to minutiae based approaches. Another advantage of wavelets is that it performs minimum three level of texture decomposition which makes automated fingerprint recognition system accurate. This is the weakness of most of the texture analysis schemes as the image is analyzed at single scale.

4. Challenges in Fingerprint Recognition

Performance of any fingerprint recognition system heavily relies on quality of finger print image. Quality of a fingerprint image is governed by factors such as skin conditions, sensor conditions, poor user cooperation, etc. Few factors can be avoided whereas few vary over a time. Hence lack of robustness is an important issue in fingerprint recognition systems[16]. It is better to reject degraded images during training so that performance of fingerprint recognition system can be maintained.

Another issue in fingerprint recognition system is the use of multiple sensors. Different sensors interpret and

represent fingerprint image in a different way[17]. Changing the sensors may affect the performance of the fingerprint recognition systems. It will be a good idea to represent fingerprint images under a common exchange format. Another way by which this problem can be avoided is to normalize the raw data and extracted features.

Apart from advantages of fingerprint recognition systems, they are also targets of attacks. Unfortunately, fake input to biometric recognition systems proved to be successful. Matching score (threshold value) is a pivotal element in fingerprint recognition systems. Additional challenges include matching fingerprints that are affected with plastic distortions. Classification method for efficient search of fingerprints in a fingerprint database is also a biggest challenge[17].

5. Fingerprint Enhancement

To make image clear for better usage by fingerprint recognition systems, it is necessary to enhance fingerprint image. Generally fingerprint image is full of noise as human fingers are often comes in contact with most of the manual tasks and becomes creased, dirty, wet, dry, cut, worn, etc. Purpose of image enhancement is to remove noise from fingerprint images so that ridges against valleys are clearly visible. Image enhancement techniques are broadly classified as spatial domain techniques and frequency domain techniques[18].

Spatial domain methods directly deal with image pixels. In frequency domain methods, Fourier transform of an image is obtained. All the necessary image enhancement procedures are applied on Fourier transform of the image. Finally, inverse Fourier transform is applied to get the resultant image[18]. Few fingerprint enhancement techniques under spatial domain and frequency domain are discussed below:

5.1 Histogram Equalization

Histogram equalization is mainly used to adjust image intensities to enhance contrast of the whole image. Histogram is the graphical representation of relative frequency of various gray levels available in an image[19]. By equalizing the histogram, we can improve the contrast of an image. It's a type of spatial domain technique and it is widely accepted technique in image enhancement[19].

5.2 Fourier Transform

Fourier transform is an important mathematical tool used to decompose an image into sine and cosine components.

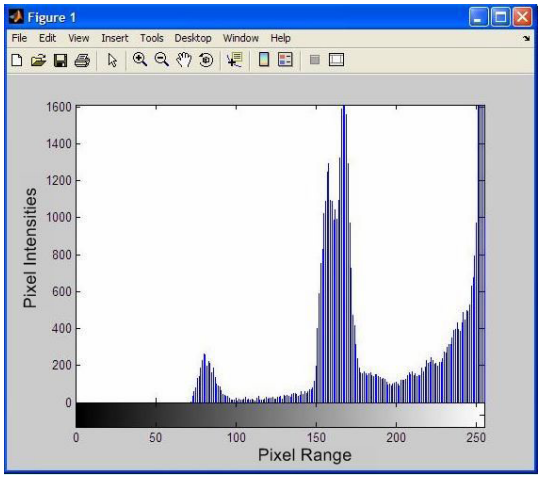

Figure 4. Histogram Figure.

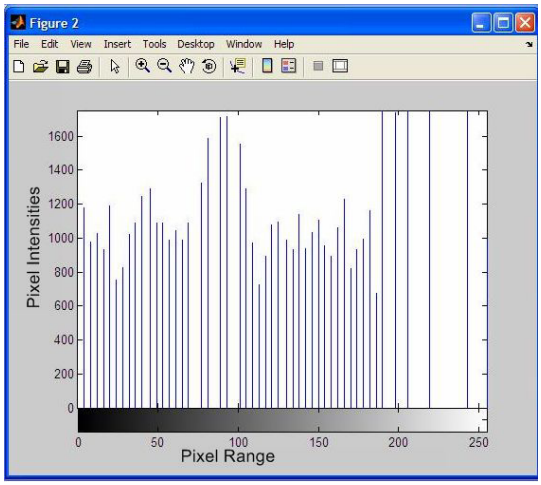

Figure 5. Equalized Histogram.

The basic idea here is to divide the fingerprint image into small processing blocks and enhance each block independently[20]. To decompose an image into blocks, the following formula is used:

$$F(u,v)=\sum_{i=0}^{m-1}\sum_{j=1}^{n-1} f(\mathrm{i},\mathrm{j}) \times exp\left\{-k2\pi\times\frac{u_i}{m}+\frac{v_j}{n}\right\}$$

for u = 0,1,2,…31 and v=0,1,2,3…31

Now each block is enhanced according to some formula. For example,

$g(x,y) = F^{-1}\{F(u,v)+|F(u,v)|k\}$

where is $F^{-1}\{F(u,v)\}$ represented by

$$f(x,y)=\frac{1}{mn}\sum_{x-0}^{n-1}\sum_{y-0}^{n-1} F(u,v) \times exp\left\{j2\pi\times\frac{u_x}{m}+\frac{v_y}{n}\right\}$$

5.3 Filtering Methods

Filters are mainly used to suppress either high frequencies or low frequencies in an image. Filtering high frequencies in the image makes output image smooth and restricting low frequencies enhances or detects edges in an image. Filtering concept work in both frequency domain and spatial domain[21]. Different types of filters are available which are well suited for fingerprint image enhancements.

Median filtering is used to remove salt and pepper type noise. Median value of all the pixels in a window is calculated and this value is replaced with pixels around the window[21]. Median filtering arranges pixel values of the window in an order and then choosing the median value among these pixels.

High pass filtering is used to extract edges of the image. High pass filtering sharpens the edge of the image. To achieve this, a fraction of high pass filtered image is added to the original image. This is the basic concept for most of the image sharpening models. High pass filters tend to keep high frequency information while reducing low frequency information[21]. The strength of high pass filters is that it increases the brightness of the centre pixel relative to neighbouring pixel.

Directional filtering is also used for edge detection. Edge of an image is made visible if there is a huge change with a pixel to its adjacent pixel. This change is measured by first derivatives and directional filters compute first derivatives of an image[22]. Directional filters can be designed to compute first derivatives in any direction.

Another method used to detect edges of an image is using Laplacian filters. Laplacian filters are used to compute second derivatives where as directional filters compute first derivatives. Second derivatives represent the rate of change of first derivative. This helps to determine whether the adjacent pixel values are edges or continuous progression[22].

5.4 Comparison of Various Fingerprint Image Enhancement Techniques

Fingerprint matching algorithms does not have any difficulty in matching good quality finger print images. But if the image quality is low, it is an issue for fingerprint matching algorithm and in this situation, fingerprint image enhancement is obligatory. There are various fingerprint image enhancement techniques available with few working under spatial domain and few in frequency domain. The below table provides comparison of various fingerprint image enhancement techniques.

Fingerprint recognition systems works by acquiring individual's fingerprints from scanner. This is the raw data (image). Next some amount of preprocessing is done on the raw image so that the output image is well suited for feature extraction. Preprocessing includes fingerprint enhancement and filtering. Features are extracted from fingerprint images and stored as feature vectors in fingerprint database. Finally matching is done with input fingerprint with stored ones[23].

The accuracy of a fingerprint recognition system is measured by the following parameters.

Table 1. Comparison of various fingerprint image enhancement techniques

Method	Advantages	Disadvantages
Histogram Equalization	This method directly works on fingerprint image pixels	This method is discriminate and it can increase the background noise also
Band Pass Filtering	Removes noise and maintains true structures and ridges of fingerprint	This method fails if the input image contains heavy noise
Gabor Filtering	It combines the features of anisotropic filter and low pass filter to give high efficiency	This method fails to perform if the regions of the input image are tainted with heavy noises.
Binarization and Thinning	This method preserves the connectivity of the ridges and features of the fingerprints that do not get distorted	Sometimes this method may yield non-connected or even empty medial lines in fingerprint images
2D Fourier Transform	This method is fast and classifies the orientation to 16 directions	Since this method assumes that frequency is constant throughout the image, the enhanced image can be with less accuracy
Wavelet based Transformation	This method is computationally fast and effective in denoising fingerprint images	Lack of shift variance and poor directional selection of diagonal features because wavelets are separable and real

- False Acceptance Rate (FAR) is the measure that fingerprint recognition system wrongly allows access to the unauthorized users. It is defined as the ratio of number of false acceptances divided by the number of identification attempts.
- False Rejection Rate (FRR) is the measure that fingerprint recognition system wrongly rejects access to the authorized users. It is defined as the ratio of number of authentic images not considered divided by the total number of authentic images.
- False Matching Rate (FMR) is the number of imposter comparisons with threshold value 'T' divided by the total number of imposter comparisons.
- False Non Matching Rate (FNMR) is the number of genuine comparisons with threshold value 'T' divided by the total number of genuine comparisons.
- Equal Error Rate (ERR) is the best single descriptor of error rate of a biometric algorithm. ERR is the value where FMR and FNMR values are equal.

6. Conclusion

In this paper, an elaborate literature on fingerprint recognition systems has been studied. Fingerprint recognition system is a widely used biometric approach having applications like criminal investigations, terrorist identifications and other security issues. Fingerprint is a physiological biometric feature used to identify a person. Fingerprint does not change unless there is some physical disturbance such as accidents or works in an industry. These impressions become notable over the age and the chance of two people having identical fingerprints is rare. A good quality, noise free fingerprint image is the real need for fingerprint recognition systems to achieve robustness and accuracy. It is important to concentrate more on fingerprint image enhancement techniques.

7. References

1. Jain AK, Feng J, Nandakumar K. Fingerprint Matching. Published by the IEEE Computer Society. 2010 Feb.
2. Ramaswamy G, Sreenivasarao V, Ramesh P, Kiran DR. A Novel Approach for Human Identification through Fingerprints. International Journal of Computer Applications (0975 –8887). 2010 Jul; 4(3):169–73.
3. Al-Ani MS. A Novel Thinning Algorithm for Fingerprint Recognition. International Journal of Engineering Sciences. 2013 Feb; 2(2):43–8.
4. Davis D, Higgins P, Kormarinski P, Marques J, Orlans N, Wayman J. MITRE TECHNICAL REPORT - State of the Art Biometrics Excellence Roadmap. Technology Assessment: Fingerprint, Palm print, Vascular, Standards. 2008 Oct; 1(3):357–60
5. Mikhail K, Dremin A, Leshko A. Fingerprint identification algorithm based on Delaunay triangulation and cylinder codes. 11th International Conference Pattern Recognition and Image Analysis (PRIA-11-2013); Adeliade. 2013.
6. Kimmins JP, Rempel RS, Welhamm CVJ, Seely B, Rees KCJ. Biophysical sustainability, process-based monitoring and forest ecosystem management decision support systems. Canadian Institute of Forestry. 2007 Aug; 83(4):502–14.
7. Kute A, Kumar V. Fingerprint Recognition System: A Review. International Journal of Electrical, Electronics and Computer Engineering . 2014; 3(2):61–6.
8. Prabhu RR, Ravikumar CN. A Novel Extended Biometric Approach for Human Character Recognition using Fingerprints. International Journal of Computer Applications (0975–8887). 2013 Sep; 77(1):37–44.
9. Su C, Srihari S. Evaluation of Rarity of Fingerprints in Forensics. Proceedings of Neural Information Processing Systems, Canada. 2010 Dec 6-9:1–9.
10. Loris N, Lumini A. Local binary patterns for a hybrid fingerprint matcher. Pattern Recognition. 2008 Nov; 41(11):3461–66.
11. Yongwha C, et al. Automatic alignment of fingerprint features for fuzzy fingerprint vault. Information Security and Cryptology. 2005; 3822(12):358–69.
12. Rajbhoj SM, Mane PB. An Improved Binarization based algorithm using minutiae approach for Fingerprint Identification. IJEAT. 2012 Aug; 1(6):219–22.
13. Strasburger H, Rentschler I, Jüttner M. Peripheral vision and pattern recognition: A review. Journal of Vision. 2011 May; 11(5):13.
14. Badwer IKSB, Kaur S. Image Denoising using different Wavelet Transforms with Hard and Soft Thresholding. International Journal of Advanced Research in Computer Science and Software Engineering. 2014 Aug; 4(8):153246.
15. Basha MSB, Ramakrishnan M. Color Image Enhancement based on Daubechie–s Wavelet and HIS Analysis. International Journal of Computer Applications. 2012 Jun; 47(13):8–11.
16. Singh J, Yashika. A Study of Optimistic Approaches and Applications of Biometric Systems. National Conference on Synergetic Trends in Engineering and Technology (STET-2014) International Journal of Engineering and Technical Research. 2014 Apr; 31–4.
17. Fernandez FA, Fierrez J, Garcia JO, Rodriguez JG, Fronthaler H, Kollreider K, Bigun J. A comparative study of fingerprint image-quality estimation methods. IEEE

Transactions on Information Forensics and Security. 2007 Dec; 2(4):734–43.
18. Basha MS, Ramakrishnan M. Color Image Contrast Enhancement using Daubechies D4 Wavelet and Luminance Analysis. International Journal of Computer Applications. 2014 Jan; 86(6):6–10.
19. Min BS, Lim DK, Kim SJ, Lee JH. A Novel Method of Determining Parameters of CLAHE Based on Image Entropy. International Journal of Software Engineering (CCECE'2007); Canada. 2007 Apr 22-26. p. 24–7.
20. Selvi PT, Radha N. Multimodal biometrics based authentication against dictionary attacks. International Journal on Computer Science and Engineering. 2010 Dec; 2(8):2652–58.
21. Ahmed RJ. Image enhancement and noise removal by using new spatial filters. U.P.B. Sci. Bull., Series C. 2011; 73(1):65–74.
22. Doutre C, Nasiopoulos P. An efficient compression scheme for colour filter array images using estimated colour differences. Electrical and Computer Engineering (CCECE'2007); Canada. 2007 Apr 22–26. p. 24–7.
23. Panchal V. A low cost fingerprint recognition system based on wavelet transform. IJETCAS. 2013 Apr; 481–6.