Finger Print Recognition: Survey of Minutiae and Gabor Filtering Approach

Megha Kulshrestha
ACET
Amritsar Punjab

V. K. Banga
Phd,ACET
Amritsar Punjab

Sanjeev Kumar
ACET
Amritsar Punjab

ABSTRACT
Fingerprints are the most popular and studied biometrics features. Their stability and uniqueness make the fingerprint identification system extremely reliable and useful for security applications. Fingerprints are the oldest and most widely used form of biometric identification. Everyone is known to have unique, immutable fingerprints. This paper deals with the issue of selection o fan optimal algorithm for fingerprint matching in order to design a system that matches required specifications in performance and accuracy. Two approaches have been discussed in this paper based on minutiae located in a fingerprint and based on gabor filter which is used to matching the fingerprint.

General Terms
Fingerprint recognition, minutiae technique, gabor filter technique.

Keywords
Minutiae, Gabor, Arch, Ridge.

1. INTRODUCTION
Fingerprint-based identification is one of the most important biometric technologies which have drawn a substantial amount of attention recently. Fingerprints are believed to be unique across individuals and across fingers of same individual. Even identical twins having similar DNA, are believed to have different fingerprints. Conventional security systems used either knowledge based methods (passwords or PIN), and token-based methods (passport, driver license, ID card) and were prone to fraud because PIN numbers could be forgotten or hacked and the tokens could be lost, duplicated or stolen. To address the need for robust, reliable, and foolproof personal identification, authentication systems will necessarily require a biometric component. The word "biometrics" comes from the Greek language and is derived from the words bio (life) and metric (to measure). Biometric systems use a person's physical characteristics (like fingerprints, irises or veins),or behavioral characteristics (like voice, handwriting or typing rhythm) to determine their identity or to confirm that they are who they claim to be. The most widely used biometric technology is the fingerprint system. In fact, fingerprint can be used to replace the PIN or passwords in most security aspect. Fingerprints can be used instead of PIN in the smart card applications, passwords on workstations, etc. Many researches about fingerprint technology are undergoing all around the world. There are two types of fingerprint systems [9]: fingerprint verification and identification. The verification system is a one-to-one matching and is based on the comparison of two groups of minutiae, respectively corresponding to two fingers to be compared. It is basically identity verification since you have to first input some information about yourself then the information is verified using your fingerprint. A fingerprint the pattern of ridges and valleys on the surface of fingertip.Fingerprint recognition can be categorized into identification and verification. Fingerprint identification is the process of determining which registered individual provides a given fingerprint. Fingerprint verification, on the other hand, is the process of accepting and rejecting the identity claim of a person using his fingerprint. Fingerprint recognition can also be categorized into minutiae extraction based and spectral features of the image based. All technologies of fingerprint recognition, identification and verification, minutiae extraction based and spectral features based, each has its own advantages and disadvantages and it may requires different treatments and techniques. The choice of which technologies to use is application specific.

2. FINGERPRINT RECOGNITION
The fingerprint recognition problem can be grouped into three sub-domains: fingerprint enrollment, verification and fingerprint identification. In addition, different from the manual approach for fingerprint recognition by experts, the fingerprint recognition here is referred as AFRS (Automatic Fingerprint Recognition System), which is program-based. Verification is typically used for positive recognition, where the aim is to prevent multiple people from using the same identity. This section provides a basic introduction to fingerprint recognition systems and their main parts, including a brief description of the most widely used techniques and algorithm [1].

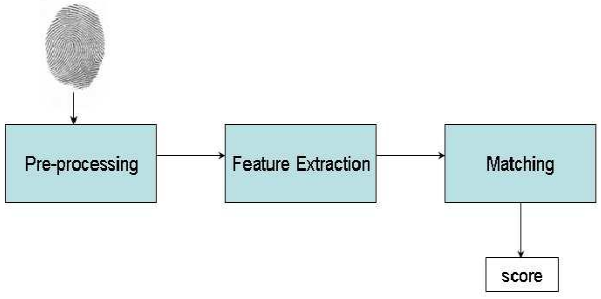

Figure 1 Main modules of a fingerprint verification system

The main modules of a fingerprint verification system (Fig.1) are:

a) fingerprint sensing, in which the fingerprint of an individual is acquired by a fingerprint scanner to produce a raw digital representation;
b) Preprocessing, in which the input fingerprint is enhanced and adapted to simplify the task of feature extraction;
c) feature extraction, in which the fingerprint is further processed to generate discriminative properties, also called feature vectors; and

d) Matching, in which the feature vector of the input fingerprint is compared against one or more existing templates. The templates of approved users of the biometric system, also called clients, are usually stored in a database. Clients can claim an identity and their fingerprints can be checked against stored fingerprints.

3. CLASSES OF FINGERPRINTS

Galton-Henry classification system accounts for more than 120 fingerprint classes. Fingerprint classification techniques have been a research topic for more than 30 years [3]. Many classification methods have been designed. However, most they use the same set of features: ridge line flow, orientation image, singular points, and Gabor filter responses. Orientation image contain all necessary information to classify fingerprints in five broad classes.

The five most common classes are:

- Arch: ridges enter from one side, rise to form a small bump, and then go down and to the opposite side. No loops or delta points are present.
- Tented Arch: similar to the arch except that at least one ridge has high curvature, thus one core and one delta points.
- Left loop: one or more ridges enter from one side, curve back, and go out the same side they entered. Core and delta are present.
- Right loop: same as the left loop, but different direction.
- Whorl: contains at least one ridge that makes a complete 360 degree path around the center of the fingerprint. Two loops (same as one whole) and two deltas can be found.
- Fingerprints in databases are non-uniformly distributed in these classes.

Figure 2 Fingerprint classes

Verification is to verify the authenticity of one person by his fingerprint. In the identification mode, the system recognizes an individual by searching the templates of all the users in the database for a match. Therefore, the system conducts a one to-many comparison to establish an individual's identity. The following are Fingerprint Recognition Techniques:

3.1 Minutiae Extraction Technique

Most of the finger-scan technologies are based on Minutiae. Minutia-based techniques represent the fingerprint by its local features, like terminations and bifurcations. This approach has been intensively studied, also is the backbone of the current available fingerprint recognition products [4]. This is the most popular and widely used technique, being the basis of the fingerprint comparison made by fingerprint examiners. Minutiae are extracted from the two fingerprints and stored as sets of points in the two- dimensional plane. Minutiae-based matching essentially consists of finding the alignment between the template and the input minutiae sets those results in the maximum number of minutiae pairings.

3.2 Pattern Matching or Ridge Feature

Feature extraction and template generation are based on series of ridges as opposed to discrete points which forms the basis of Pattern Matching Techniques [2]. The advantage of Pattern Matching techniques over Minutiae Extraction is that minutiae points may be affected by wear and tear and the disadvantages are that these are sensitive to proper placement of finger and need large storage for templates. Pattern based algorithms compare the basic fingerprint patterns (arch, whorl, and loop) between a previously stored template and a candidate fingerprint. This requires that the images be aligned in the same orientation. To do this, the algorithm finds a central point in the fingerprint image and centers on that. In a pattern-based algorithm, the template contains the type, size, and orientation of patterns within the aligned fingerprint image [5]. The candidate fingerprint image is graphically compared with the template to determine the degree to which they match.

3.3 Correlation Based Technique

Two fingerprint images are superimposed and the correlation between corresponding pixels is computed for different alignments (e.g. various displacements and rotations).The cross-correlation is a well-known measure of image similarity and the maximization in (1); it allows us to find the optimal registration. The direct application of (1) rarely leads to acceptable results, mainly due to the following problems:

i) Non-linear distortion makes impressions of the same finger significantly different in terms of global structure; the use of local or block-wise correlation techniques can help to deal with this problem.

ii) Skin condition and finger pressure cause image brightness, contrast, and ridge thickness to vary significantly across different impressions. The use of more sophisticated correlation measures may compensate for these problems.

iii) A direct application of (5) is computationally very expensive. Local correlation and correlation in the Fourier domain can improve efficiency.

3.4 Image Based Techniques

Image based techniques try to do matching based on the global features of a whole fingerprint image. It is an advanced and newly emerging method for fingerprint recognition. It is useful to solve some intractable problems of the first approach.

4. MINUTIAE EXTRACTION

The basic method of minutiae extraction is divided in to three part Preprocessing, Minutiae Extraction, Post processing. Our method divides three basic steps in to 7 modules which are given below [5].

Step 1: Input-

In this step we take five fingerprints of personas input and process them.

Step 2: Binarization:

This transform the 8-bit Gray fingerprint image to a 1-bit image with 0- value for ridges and 1-value for furrows.

Step 3: Thinning:

Ridge thinning is to eliminate the redundant pixels of ridges till the ridges are just one pixel wide. [7] Uses an iterative, parallel thinning algorithm.

1) To get a thinned image we find the location of middle black pixel at each stage of continuation of the curve.
2) In each scan of the full fingerprint image, the algorithm marks down redundant pixels in each small image window (3x3).
3) And finally removes all those marked pixels after several scans.

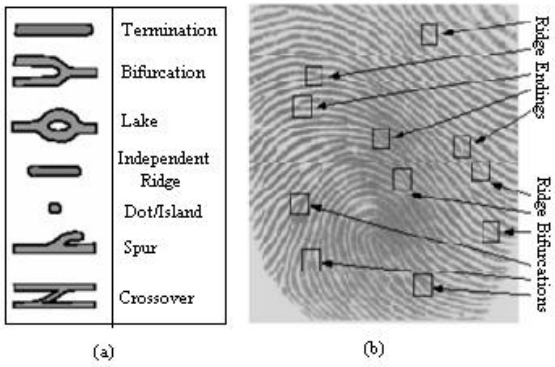

Figure 3 Different minutiae types, (b) Ridge ending & Bifurcation

Step 4: Minutiae Connect:

This operation takes thinned image as input and produces refined skeleton image by converting small straight lines to curve to maximum possible extant.

Step 5: Minutiae Margin:

This increases the margin of endpoints by one pixel of curves of length at least three pixels.

Step 6: Minutiae point Extraction:

For extracting minutiae point we compute the number of one-value of every 3x3 window:

- If the centroid is 1 and has only 1 one valued neighbor, then the central pixel is a termination.
- If the central is 1 and has 3 one-value neighbors, then the central pixel is a bifurcation.
- If the central is 1 and has 2 one-value neighbors, then the central pixel is a usual pixel.

Step 7: False Minutiae Removal

Procedure for removing false minutiae is given below [2]:

- If the distance between one bifurcation and one termination is less than D and the two minutiae are in the same ridge. Remove both of them. Where D is the average inter-ridge width representing the average distance between two parallel neighboring ridges.

- If the distance between two bifurcations is less than D and they are in the same ridge, remove the two bifurcations.

- If two terminations are within a distance D and their directions are coincident with a small angle variation. And they suffice the condition that now any other termination is located between the two terminations. Then the two terminations are regarded as false minutia derived from a broken ridge and are removed.

- If two terminations are located in a short ridge with length less than D, remove the two terminations.

- If a branch point has at least two neighboring branch points, which are each no further away than maximum distance threshold value and these branch points are closely connected on common line segment than remove the branch points.

And last we do the minutiae matching. Two fingerprint images to be matched, any one minutia is chosen from each image, and then the similarity of the two ridges associated with the two referenced minutia points is calculated. If the similarity is larger than a threshold, each set of minutiae to a new coordination system is transformed, whose origin is at the referenced point and whose x-axis is coincident with the direction of the referenced point. After we get two sets of transformed minutia points, we use the elastic match algorithm to count the matched minutia pairs by assuming two minutiae having nearly the same position and direction are identical.

5. GABOR FILTERS

The different processing steps from pre-processing to matching as the final step of the fingerprint authentication are

- Quantized co-sinusoidal triplets
- Discrete Fourier transform
- Gabor filters

The first step is the normalization, which results in a better contrast of the fingerprint image. After that, the fingerprint is segmented, which crops areas of the recorded image, which do not contain any relevant information. This is the end of the pre-processing. The last pre-processing step usually consists of a fingerprint enhancement as described in [7]. However, tests have shown that the subsequent reference point detection works on non-enhanced fingerprint images as well as on enhanced. Therefore, any further enhancement is not required for the subsequent processing steps. After that, the fingerprint image is

filtered using a Gabor filter. Now, it is possible to create the feature map, which is used as the template. This template is matched in the subsequent matching step with templates of other fingerprints. The result of the matching is the matching score, which represents how good two fingerprints resemble each other.

Most methods for fingerprint identification use minutiae as the fingerprint features. For small scale fingerprint recognition system, it would not be efficient to undergo all the preprocessing steps (edge detection, smoothing, thinning ...etc), instead Gabor filters will be used to extract features directly from the gray level fingerprint. No preprocessing stage is needed before extracting the features [7].

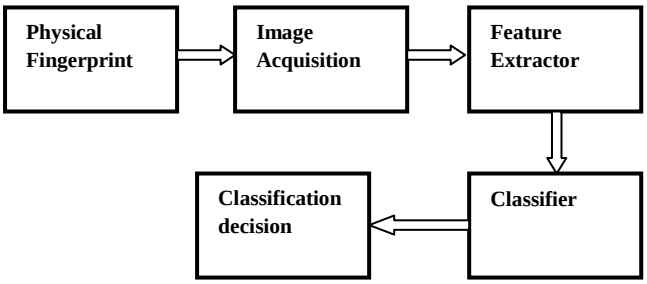

Figure 4. Building blocks for the Gabor approach

5.1) Image Acquisition

A number of methods are used to acquire fingerprints. Among them, the inked impression method remains the most popular one. Inkless fingerprint scanners are also present eliminating the intermediate digitization process [6]. Fingerprint quality is very important since it affects directly the minutiae extraction algorithm. Two types of degradation usually affect fingerprint images: 1) the ridge lines are not strictly continuous since they sometimes include small breaks (gaps); 2) parallel ridgelines are not always well separated due to the presence of cluttering noise. The resolution of the scanned fingerprints must be 500 dpi while the size is 300 x 300.

5.2) Feature Extractor

Gabor filter based features have been successfully and widely applied to face recognition, pattern recognition and fingerprint enhancement. The family of 2-D Gabor filters was originally presented by Daugman (1980) as a framework for understanding the orientation and spatial frequency selectivity properties of the filter. The fingerprint print image will be scanned by a 8x8 window; for each block the magnitude of the Gabor filter is extracted with different values of m (m = 4 and m = 8). The features extracted (new reduced size image) will be used as the input to the classifier.

5.3) Classifier

The classifier is based on the k-nearest neighborhood algorithm KNN. "Training" of the KNN consists simply of collecting k images per individual as the training set. The remaining images consists the testing set. The classifier finds the k points in the training set that are the closest to x (relative to the Euclidean distance) and assigns x the label shared by the majority of these k nearest neighbors. Note that k is a parameter of the classifier; it is typically set to an odd value in order to prevent ties. The last phase is the verification phase where the testing fingerprint image [5]:

1) Is inputted to the system
2) Magnitude features are extracted
3) Perform the KNN algorithm
4) Identify the person

6. CONCLUSION

Image quality is related directly to the ultimate performance of automatic fingerprint authentication systems. Good quality fingerprint images need only minor preprocessing and enhancement for accurate feature detection algorithm. This paper reviewed a large number of techniques described in the literature to extract minutiae from fingerprint images. The approaches are distinguished on the basis of several factors like: the kind of input images they handle i.e. whether binary or gray scale, techniques of binarization and segmentation involved, whether thinning is required or not and the amount of effort required in the post processing stage. In order to achieve desired accuracy and system performance, two methods have been widely used, first is minutiae and second one is Gabor filter based. Minutiae are local discontinuities in the fingerprint pattern. For small scale fingerprint recognition system, it would not be efficient to undergo all the preprocessing steps (edge detection, smoothing, thinning etc. as like of minutiae based technique), instead Gabor filters will be used to extract features directly from the gray level fingerprint. The Gabor filter method is widely accepted approach for the fingerprint matching.

7. ACKNOWLEDGMENTS

I like to extend my thanks to Dr. V. K. Banga HoD ECE ACET who guided me throughout the preparation of the paper and gave me relevant concept to materialize the paper. I would also like give my humble regards to Mr. Sanjeev kumar Professor ACET for helping me to shape out the important findings and necessary reseach for the paper. I wish both them all the success for future.

8. REFERENCES

[1] Anil Jain and Lin Hong, (1996) 'On-line Fingerprint Verification', Proc. 13th ICPR, Vienna, pp. 596-600.

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

[3] An Efficient Multi Fingerprint Verification System Using Minutiae Extraction Technique Chandra Bhan Pal, Amit Kumar Singh, Nitin, Amrit Kumar Agrawal.

[4] Jain LC, Intelligent Biometric Techniques in Fingerprint and Face Recognition, CRC Press, 1999.

[5] Minutiae Extraction from Fingerprint Images - a Review Roli Bansal, Priti Sehgal and Punam Bedi IJCSI

International Journal of Computer Science Issues, Vol. 8, Issue 5, No 3, September 2011.

[6] Lin Hong, Yifei Wang, and Anil Jain, "Fingerprint Image Enhancement: Algorithm and Performance Evaluation"' IEEE Transactions on Pattern Analysis and Machine Intelligence, 20(8), August 1998.

[7] Munir, M. U., Javed, M. Y., "Fingerprint Matching using Gabor Filters," 2005. http://www.isc365.com/Biometrics_Security_Vs_Convenience.aspx

[8] Maltoni D., Maio D., Jain A.K. and prabhakar S., "Handbook of Fingerprint Recognition," Second Edition, Springer , 2009.

[9] NTSC Subcommittee on Biometrics, "Fingerprint Recognition", 2000.