International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

# Fingerprint Reorganization Using Minutiae Based Matching for Identification and Verification

**Deepika Sahu[1], Rashmi Shrivas[2]**

[1]M.Tech, Mats University, School of Engineering and IT, Gullu Arang, Chhattisgarh, India

[2]Assistant Professor, Mats University, School of Engineering and IT, Gullu Arang, Chhattisgarh, India

**Abstract:** ***Fingerprints play distinguishing role in biometrics. Fingerprints are the most widely used parameter for personal identification amongst all biometric based personal authentication systems. They give unique identification to the individual. They are permanent and non changing character pattern. As most automatic fingerprint recognition systems are based on local features of ridge known as minutiae, marking minutiae accurately and rejecting false ones is critically important. This paper is a study and implementation of a fingerprint recognition system based on Minutiae based matching which is quite frequently used in various fingerprint algorithms and techniques. This approach mainly involves extraction of minutiae points from the sample fingerprint images and then performing fingerprint matching based on the score of minutiae pairings among two fingerprints. Our implementation mainly assimilates image enhancement, image segmentation, feature extraction and minutiae matching. It finally generates a result which tells whether two fingerprints match or not.***

**Keywords:** ***Fingerprint, FRR, Minutiae based algorithm, Enhancement, Feature Extraction***

## 1. Introduction

In today's advanced digital technology world, there is an increased requirement of security measures leading to the development of many biometrics based personal authentication systems. Biometrics is the science of uniquely recognizing humans based upon one or more intrinsic physical traits. Fingerprints are the most widely used parameter for personal identification amongst all biometrics. Fingerprint based authentication is one of the most reliable and mature biometric recognition techniques The reason behind the attractiveness of fingerprint-based recognition among the biometrics-based security systems is the unchanged ability of fingerprints during the human life span and their uniqueness [5].

However to meet the performance necessities of high security applications, multimodal biometrics [6] is also used as it helps to minimize system error rates. Fingerprint is a unique pattern of ridges and valleys on the surface of finger of an individual. A ridge is defined as a single curved segment and a valley is the region between two adjacent ridges. Most automatic fingerprint recognition systems are based on local ridge features known as minutiae. There are about 150 different types of minutiae [4] categorized according to their configuration. Among these minutia types "ridge ending" and "ridge bifurcation" are the most commonly used, since the other types of minutiae can be seen as combinations of "ridge endings" and "ridge bifurcations".

These are the minutiae points which are used for formative uniqueness of a fingerprint. Automated fingerprint recognition systems can be categorized as: verification or identification systems. The verification process either accepts or rejects the user's identity by matching against an existing fingerprint database. In identification, the identity of the user is recognized using fingerprints. Since accurate matching of Fingerprints depends largely on ridge structures, the quality of the fingerprint image is of critical importance. However, in practice, a fingerprint image may not always be well defined due to elements of noise that alter the clarity of the ridge structures. Many algorithms [4] have been proposed in the literature for minutia analysis and fingerprint classification for better fingerprint verification and identification. Some algorithms classify the fingerprint pattern into different groups at the time of enrollment [9]. Their results also depend largely on the quality of the input image . Thus, image enhancement techniques are often employed to reduce the noise and to enhance the definition of ridges against valleys so that no spurious minutiae are identified.

## 2. Literature Review

There are many techniques presented previously based on fingerprint matching techniques. Most of the techniques undertaken in previous researches are based on the biometric authentication like fingerprint. Fuzzy vault system [10] is one of the most important mechanisms for secure biometric authentication based on fingerprint minutiae in which a secret key is produce selecting chaff points from minutiae template. Fingerprint matching using a Gabor filter [11] is one more technique which uses fingerprint matching using a 16 Gabor filter from the template which results in designing a new method for comparing two ridge patterns map of image using adaptive filter method.

Several methods have been proposed for enhancement of fingerprint images which are based on image normalization and Gabor filtering (Hong' s algorithm) [12], Binarization method [17], Fingerprint image thinning using pcnns [16]. Minutiae based fingerprint matching algorithm [3] is helpful in certain application for privacy protection. Previously, some work has been carried out to reduce the FRR (False Rejection Rate) by using certain techniques. Some of the techniques use the minutiae position of fingerprint images like Gabor filter technique [11] in which core & ridge pattern

is used. Descriptor based Hough algorithm [2] is also proposed previously which uses a minutiae cylinder code to improve distinctiveness & Hough transform method to improve stoutness & distortion of fingerprint image. In this paper we propose a novel algorithm for extracting minutiae from a fingerprint image and calculating the Euclidean distance between input image and query image. Here we use alignment based match algorithm for determining whether the two minutia sets are from the same finger or not.

## 3. Fingerprint Features

This section summarizes the main features of real fingerprint images and introduces the basic terminology that will be used throughout the rest of the paper. A fingerprint is the representation of the epidermis of a finger. The macroscopic analysis, a fingerprint is composed of a set of ridge lines which often flow parallel and sometimes produce local macro-singularities called core and delta, respectively. In nature, the number of cores and deltas in a single fingerprint is regulated by some strict rules: in particular, cores and deltas are present in pairs. Fingerprints are usually partitioned into five main classes tented arch, arch, right loop, left loop and whorl according to the number and position of their macro-singularities as shown below in fig 1 . These micro singularities, called minutiae.


**Figure 1 :** Basic Rigid Patterns

## 4. Proposed Methodology

The salient features of our approach for feature extraction can be described as follows the overall process can be divided into three main operations (i) preprocessing (ii) thinning and feature extraction and (iii) Post-processing. The details of various stages in feature extraction are described in [figure 2].

We view a fingerprint image as a flow pattern with a definite texture. Orientation field for the flow texture is computed .To accurately determine the local orientation field, the input image is divided into equal sized blocks windows of 16x16 pixels. Each block is processed independently .The gray level projection along a scan line perpendicular to the local orientation field provides the maximum variance. We locate the ridges using the peaks and the variance in this projection. Ridges are thinned and the resulting skeleton image is enhanced using an adaptive morphological filter. Feature extraction stage applies a set of masks to the thinned and enhanced ridge Image. The post-processing stage deletes noisy feature points.

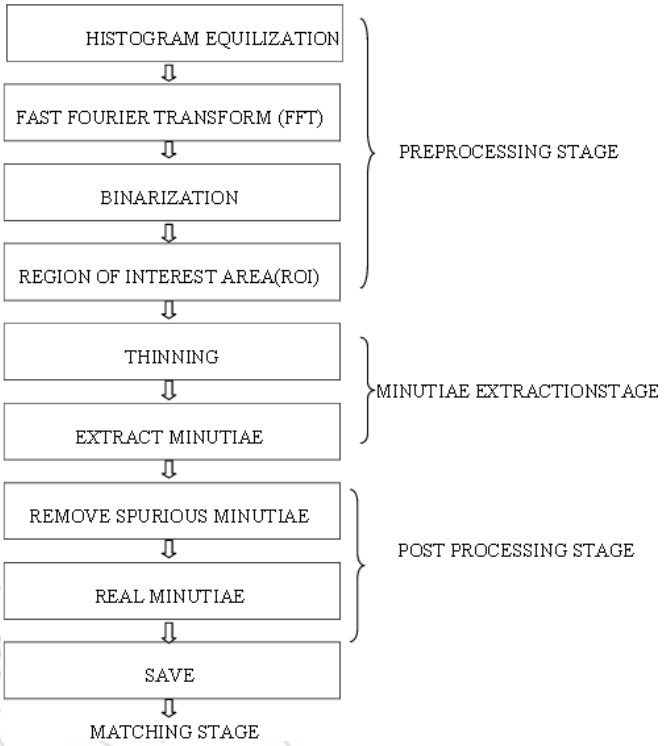


**Figure 2 :** Steps involved in Fingerprint Recorgnization

## 5. Fingerprint Image Preprocessing

### 5.1 Fingerprint Image Enhancement

Fingerprint Image enhancement is to make the image clearer for easy further operations. The fingerprint images acquired from sensors or other medians are not assured with better quality, those enhancement methods, for increasing the contrast between ridges and furrows and for connecting the false broken points of ridges due to insufficient amount of ink, are very useful for keep a better accuracy to fingerprint recognition.

**5.1.1 Histogram Equalization:** Histogram is a process that attempts to spread out the gray levels in an image so that they are evenly distributed across their range. It basically reassigns brightness value of each pixel based on the image histogram. Histogram equalization[15]is to expand the pixel value distribution of an image so as to increase the perceptional information.

**5.1.2 Fingerprint Enhancement by Fourier Transform:** We divide the image into small processing blocks (32 by 32 pixels) and perform the Fourier transform according to:

$$F(u,v) = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y) \times \exp\left\{-j2\pi \times \left(\frac{ux}{M} + \frac{vy}{N}\right)\right\} \quad (1)$$

For u=0,1,2….31and y=0,1,2…..31
In order to enhance a specific block by its dominant frequencies, we multiply the FFT of the block by its magnitude a set of times. Where the magnitude of the original FFT = abs(F(u,v)) = |F(u,v)|.Get the enhanced block according to

$$g(x,y) = F^{-1}\left\{ F(u,v) \times |F(u,v)|^{k} \right\} \quad (2)$$

where $F^{-1}(F(u,v))$ is done by:

$$f(x,y) = \frac{1}{MN} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} F(u,v) \times \exp\left\{ j2\pi \times \left( \frac{ux}{M} + \frac{vy}{N} \right) \right\} \quad (3)$$

For x=0,1,2,…..31 and y= 0,1,2……31.

The k in formula (2) is an experimentally determined constant, which we choose k=0.45 to calculate. While having a higher "k" improves the appearance of the ridges, filling up small holes in ridges, having too high a "k" can result in false joining of ridges. Thus a termination might become a bifurcation.

### 5.2 Fingerprint Image Binarization

Fingerprint Image Binarization is to transform the 8-bit Gray fingerprint image to a 1-bit image with 0-value for ridges and 1-value for furrows. After the operation ridges in the fingerprint are highlighted with black colour while furrows are white. A locally adaptive binarization method is performed to binarize the fingerprint image. Locally adaptive binarization method [15]comes from the mechanism of transforming a pixel value to 1 if the value is larger than the mean intensity value of the current block (16x16) to which the pixel belongs.

Local adaptive thresholding is applied to the directionally filtered image, which produces the final enhanced binary image. This involves calculating the average of the grey level values within an image window at each pixel, and if the average is greater than the threshold, then the pixel value is set to a binary value of one; otherwise, it is set to zero. The grey-level image is converted to a binary image, as there are only two levels of interest, the foreground ridges and the background valleys.

### 5.3 Fingerprint Image Segmentation

To extract the ROI, a two-step method is used. The first step in this method is block direction estimation and direction variety check,while the second is intrigued from some Morphological methods.

#### 5.3.1 Block Direction Estimation:

Estimate the block direction for each block of the fingerprint image with WxW in size (W is 16 pixels by default)

- Calculate the gradient values along x-direction (gx)and y-direction (gy) for each pixel of the block. Two Sobel filter are used to fulfill the task.
- For each block, use the following formula to get the Least Square approximation of the block direction.

$$tg2\beta = 2 \sum \sum (g_x * g_y) / \sum \sum (g_x^2 - g_y^2)$$

for all the pixels in each block.

The formula is easy to understand by regarding gradient values along x-direction and y-direction as cosine value and sine value. The tangent value of the block direction is estimated nearly the same as the way illustrated by the following formula

$$tg2\theta = 2\sin\theta \cos\theta / (\cos^2\theta - \sin^2\theta) \quad (4)$$

After finished with the estimation of each block direction, those blocks without significant information on ridges and furrows are discarded based on the following formulas:

$$E = \{2 \sum \sum (g_x * g_y) + \sum \sum (g_x^2 - g_y^2)\} / W*W*\sum \sum (g_x^2 + g_y^2) \quad (5)$$

For each block, if its certainty level E is below a threshold, then the block is regarded as a background block

*5.3.2 ROI Extraction by Morphological Operations*:

Two Morphological operations called 'OPEN' and 'CLOSE' are adopted. The 'OPEN' operation can expand images and remove peaks introduced by background noise The 'CLOSE' operation can shrink images and eliminate small cavities.

## 6. Minutia Extraction

### 6.1 Fingerprint Ridge Thinning

Ridge Thinning is to eliminate the redundant pixels of ridges till the ridges are just one pixel wide[14] uses an iterative, parallel thinning algorithm. In each scan of the full fingerprint image the algorithm marks down redundant pixels in each small image window (3x3). And finally removes all those marked pixels after several scans

### 6.2 Minutia Marking

After the fingerprint ridge thinning marking minutia points is relatively easy. In general for each (3x3) window, if the central pixel is 1 and has exactly 3 one-value neighbors then the central pixel is a ridge branch. If the central pixel is 1 and has only 1 one-value neighbor, then the central pixel is known as ridge ending

## 7. Minutia Postprocessing

### 7.1 False Minutia Removal

The pre-processing stage does not totally heal the fingerprint image. The false ridge breaks due to insufficient amount of ink and ridge cross-connections due to over inking are not totally eliminated. All the earlier stages themselves occasionally introduce some artifacts which later lead to spurious minutia.

### 7.2 Minutia Match

**7.2.1 Alignment stage:** Given two fingerprint images to be matched, choose any one minutia from each image and calculate the similarity of the two ridges associated with the two referenced minutia points. If the similarity is more than a threshold transform each set of minutia to a new coordination system whose origin is at the referenced point and whose x-axis is coincident with the direction of the referenced point.

**7.2.2 Match stage:** After we get two set of transformed minutia points, we used the elastic match algorithm to count the matched minutia pairs by assuming two minutia having nearly the same position and direction are identical. My approach to elastically match minutia is achieved by placing a bounding box around each template minutia. If the minutia is to be matched is within the rectangle box and the direction

discrepancy between them is very small, then the two minutiae are regarded as matched minutia pair. Each minutia in template image either has no matched minutia or has only one corresponding minutia.

## 8. Working Steps of Project

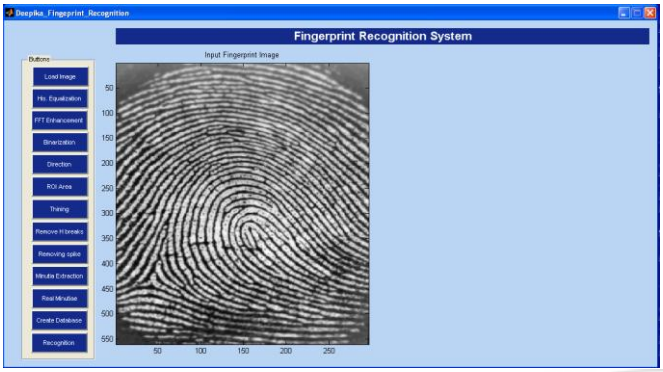


Fig : Input Fingerprint Image

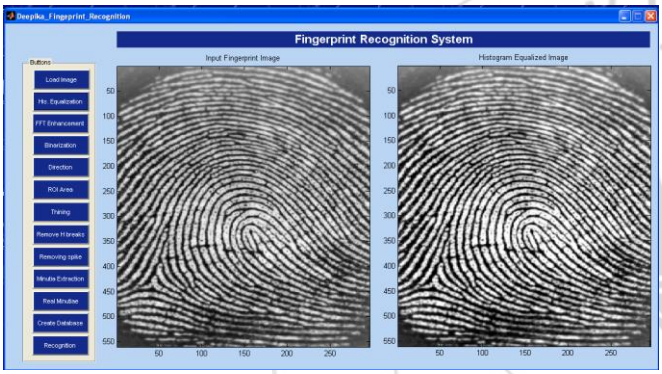


Fig : Histogram Equalization

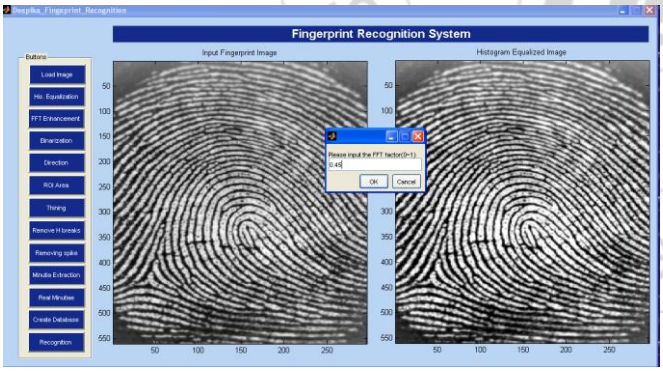


Fig : Input FFT factor

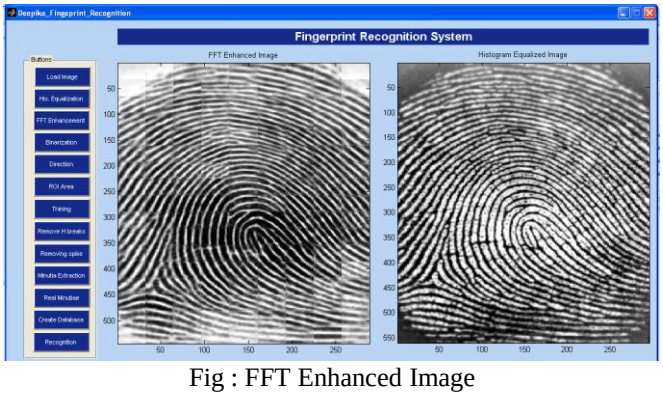


Fig : FFT Enhanced Image

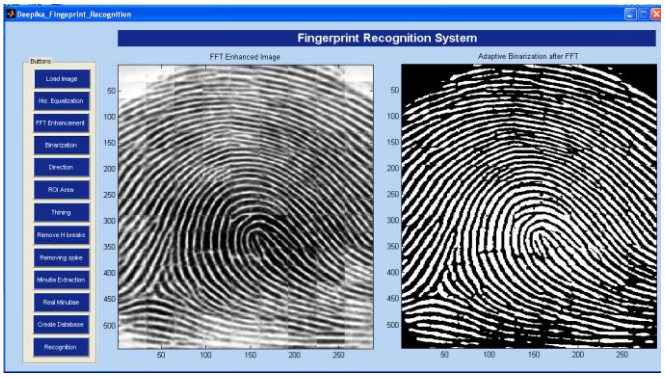


Fig : Adaptive Binarization

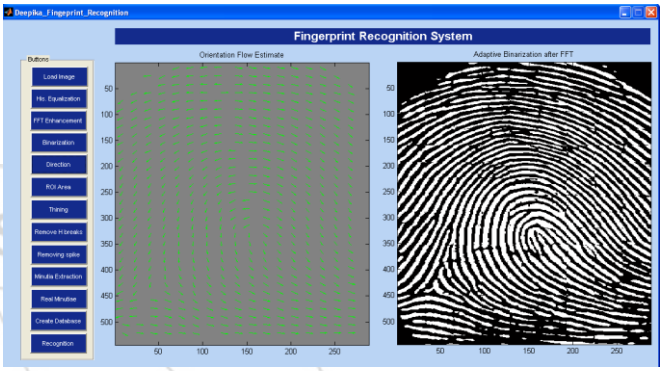


Fig : Orientation Flow

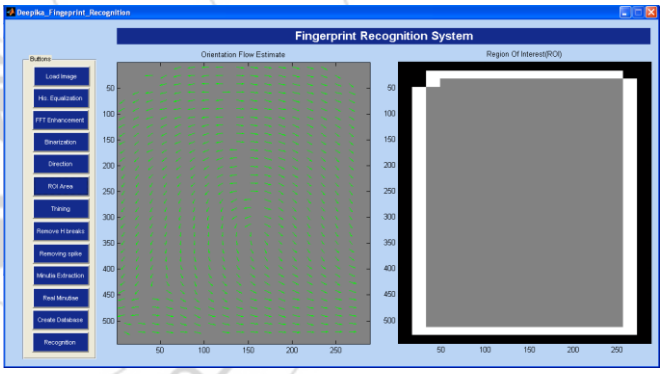


Fig : ROI Area Calculation

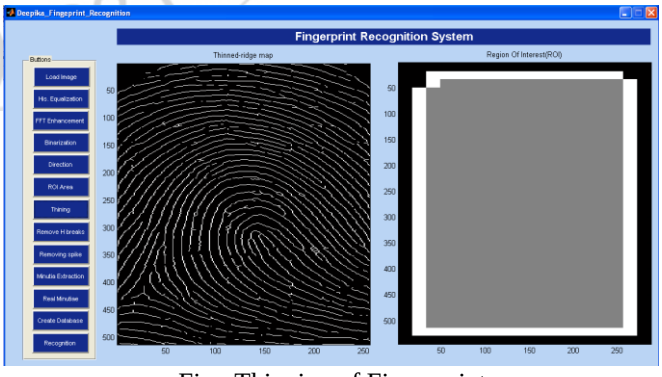


Fig : Thinning of Fingerprint

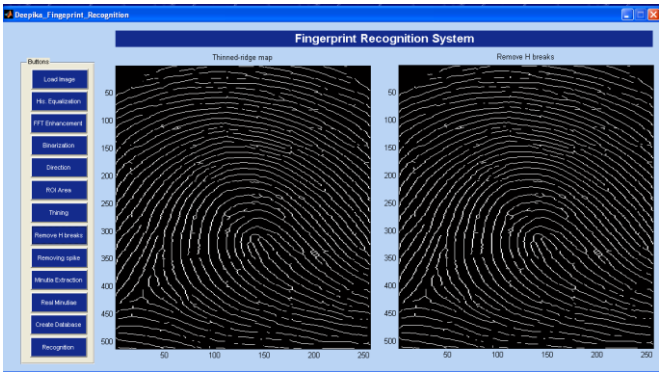

Fig : Remove H-Break

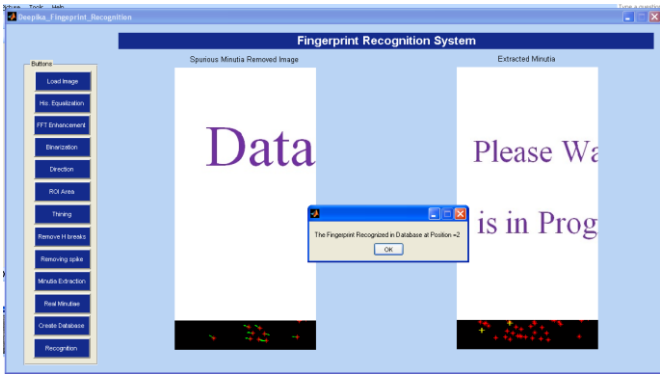

Fig : Matched Result

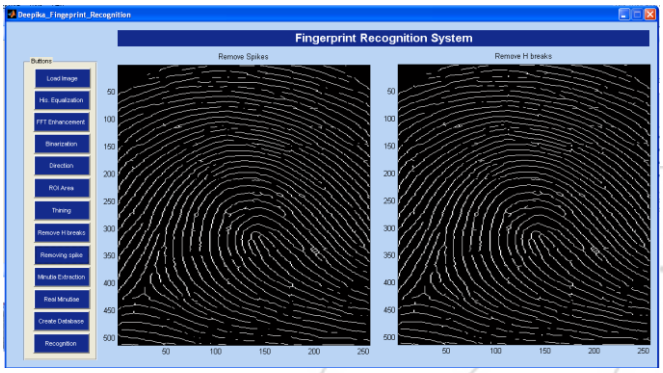

Fig : Remove Spike

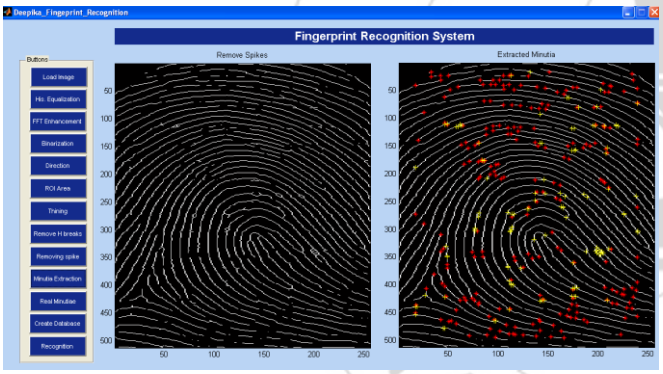

Fig : Minutia Extraction

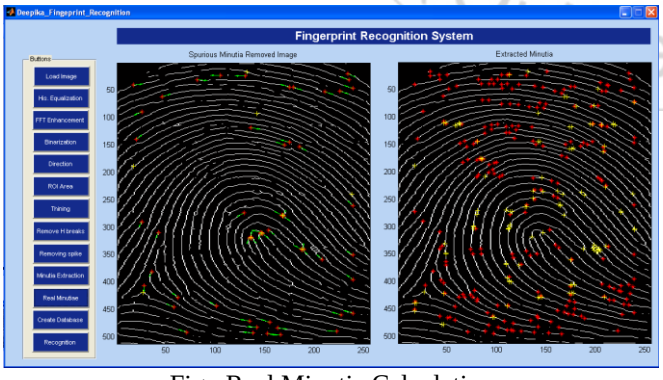

Fig : Real Minutia Calculation

## 9. Result and Conclusion

Two indexes are well accepted to determine the performance of a fingerprint recognition system: one is FRR (false rejection rate) and the other is FAR (false acceptance rate). For an image database each sample is matched against the remaining samples of the same finger to compute the False Rejection Rate (FRR). If the matching g against h is performed, the symmetric one (i.e., h against g) is not executed to avoid the correlation.

All the scores for such matches are composed into a series of Correct Scores. Also the first sample of each finger in the database is matched against the first sample of the remaining fingers to compute the False Acceptance Rate(FAR). If the matching h against h is performed, the symmetric one (i.e., h against g) is not executed to avoid correlation. All the scores from such matches are composed into a series of Incorrect Score.FAR and FRR measures can be calculated as:

FAR=(FA/N)*100
FA= number of incidents of false acceptance
N=total number of samples

FRR= (FR/N)*100
FR=number of incidents of false rejection
N=total number of samples

A fingerprint database is used to test the experiment performance. To get better performance of the matching algorithms and fingerprint analysis, an efficient algorithm has been proposed. The step by step procedure for the extraction of minutiae is accepted with necessary illustration is provided. The minutiae extraction performed for the input image and the processed image are compared to test the proposed algorithm.

The performance evaluation shows that the minutiae extracted from the processed image are closely matching with its original input image. The quality, classification, various pressure and placement of the fingerprint on the scanner has impacted the accuracy of minutiae. Further studies on good designs of training and testing are expected to improve the result and requires further enhancement, Research is also in progress to eliminate the limitation of the algorithm to reduce computation time, cost and to provide good accuracy.

## References

[1] Sreenath.M, Sukumar.P, Naganarasaiah Goud.K, P.Sivakalyani & V.Phani Kumar, "GSM based electronic voting machine using touch screen," 10SR Journal of Electronics and Communication Engineering, June 2014
[2] Paulino & Jianjang Feng, "Latent Fingerprint Matching Using Descriptor-Based Hough Transform," IEEE Transactions on Information Forensics and Security, March 2013
[3] Sheng Li and Alex C. Kot "Fingerprint Combination for Privacy Protection," IEEE Transactions on Information Forensics and Security, February 2013.
[4] A. Jain, L. Hong, "Online Fingerprint Verification",IEEE Transactions on Pattern Analysis and MachineIntelligence 19, 4 (1997), 302–314.
[5] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition. Springer, 2003
[6] A. George, Multi-Modal Biometrics Human Verification Using LDA and DFB, International Journal of Biometrics and Bioinformatics, vol. 2, issue 4, 2008
[7] Sreenath.M, Sukumar.P, Naganarasaiah Goud.K, P.Sivakalyani & V.Phani Kumar, "GSM based electronic voting machine using touch screen," 10SR Journal of Electronics and Communication Engineering, June 2014
[8] Sheng Li and Alex C. Kot, "A Novel System for Fingerprint Privacy Protection," 7th International Conference on Information Assurance and Security, 2011
[9] Chander Kant, R. Nath, Reducing Process Time for Fingerprint Identification System, International Journal of Biometrics and Bioinformatics,vol. 3, issue 1, 2009.
[10] Karthik Nandakumar, Anil K. Jain & Sharath Pankanti, "Fingerprint Based Fuzzy Vault: Implementation and Performance, "IEEE Transactions on Information Forensics and Security, December 2007
[11] Muhammad Umer Munir and Dr. Muhammad Younas Javed, "Fingerprint Matching using Gabor Filters," National Conference on Emerging Technologies, 2004.
[12] L.Hong, Y. Wan, A. K. Jain Fingerprint Image Enhancement: Algorithm and Performance Evaluation IEEE Transaction on pattern analysis and machine intelligence, Vol 20 No. 8, p.p. 777-789, 1998
[13] L. Rosario Gil, Mohamed Tawfik, Alberto Pesquera Martin & Sergio Martin, "Fingerprint Verification System in Tests in Moodie," IEEE Journal of Latin-american Learning Technologies, February 2013
[14] L.C. Jain, U.Halici, I. Hayashi, S.B. Lee and S.Tsutsui. Intelligent biometric techniques in fingerprint and face recognition. 1999, the CRC Press
[15] R.C. Gonzalez, R. E. Wood, Digital Image Processing, Second Edition, Prentice Hall,2006
[16] J. Luping, Y. Zhang , S. Lifeng, P. Xiaorong, Binary Fingerprint Image Thinning using PCNNs, IEEE Trans. On Systems, Man and cybernetics, Part B, vol. 7, No. 5, October 2007
[17] S. Greenberg, M. Aladjem, D. Kogan and I. Dimitrov Fingerprint Image Enhancement using Filtering Techniques,Electrical and Computer Engineering Department, Ben-Gurion University of the Negev, Beer-Sheva, Israel, 2000.