Improvement of Biometric Authentication System Applying Fingerprint

Fatamatuz Ayasa Khan

Computer Science & Engineering, Islamic University, kushtia, Bangladesh

Abstract—*The biometric system plays an important role in everyone life. To identify one identity, the finger is one of many forms of the biometrics are generally used. The fingerprint is the verified function to identify a match between two person's fingerprints. Here a simple and effective system for biometric fingerprint based voter identity system has been proposed that is based on image enhancement and correct minutiae extraction. Automatic and reliable extraction of minutiae from fingerprint images is a critical step in fingerprint matching. In this research a fast fingerprint enhancement and minutiae extraction algorithm have been presented which improve the clarity of the ridge and valley structures of the input fingerprint images based on the frequency and orientation of the local ridges and thereby extracting correct minutiae*.

Keywords— Biometric System, Identify Fingerprint, Authentication System, Person Identification.

I. INTRODUCTION

A biometric system gives automatic recognition of an individual based on some sort of unique feature or characteristic possessed by the individual. Biometric systems have been created based on fingerprints, facial features, voice, hand geometry, handwriting, the retina [1], and the systems work by first capturing a sample of the feature, such as recording a digital sound of mathematical function into a biometric template. The biometric template will provide a normalized, efficient and highly discriminating representation of the feature, which can then be objectively compared with other templates in order to determine identity. Most biometric systems allow two modes of operation. An enrolment mode for adding templates to a database, and an identification mode, where a template is created for an individual and then a match is searched for in the database of pre-enrolled templates.

A fingerprint is the pattern of curved lines on the end of a finger or thumb that is distinctive in every person or a mark left by this pattern. However, shown by intensive research on fingerprint recognition, fingerprints are not distinguished by their ridges and furrows, but by Minutia, which are some abnormal points on the ridges.

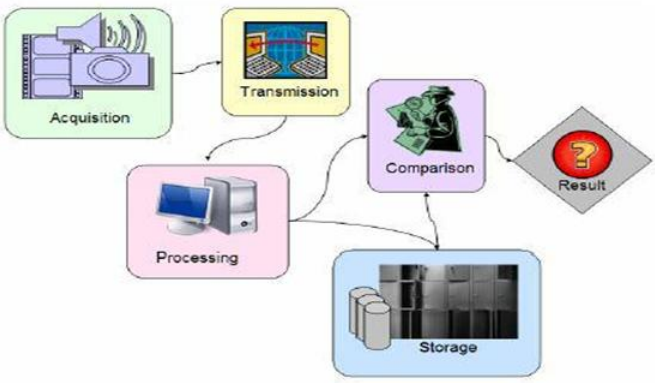

FIGURE 1: Characteristic of biometric system

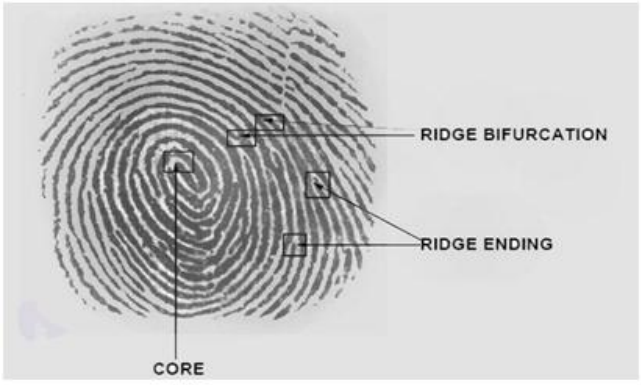

FIGURE 2: Minutia (Ending is also called Termination and Bifurcation is also called Branch)

Fingerprint-based person identity system can progress the user identification process by utilizing biometric recognition. Fingerprints are unique to each person and different finger impressions of the same user look different. Minutiae Based Matching is a system in which minutiae are extracted from a fingerprint and stored as sets of points in a two-dimensional plane and then minutiae of the fingerprint to be recognized are extracted and matched with the stored points. Minutiae matching essentially consist of finding the alignment between the template and the input minutiae sets that result in the maximum number of minutiae pairings. Generally, elements of this system are the sensor, minutia extractor, minutia matcher and a database.

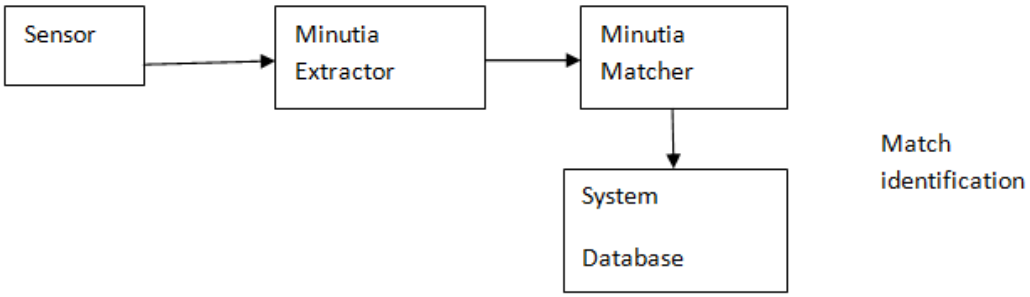

FIGURE 3: Block diagram of person identity system using fingerprint

Personal identification is to associate a specific individual with an identity. It plays a major role in our society, in which questions related to the identity of an individual such as "Is this the person who he or she claims to be?", "Has this applicant been here before?", "Should this individual be given access to our system?" "Does this employee have the authorization to perform this transaction?" etc are asked millions of times every day by hundreds of thousands of organizations in financial services, health care, electronic commerce, telecommunication, government, etc. With the rapid growth of information technology, people are becoming even more and more electronically connected. As a result, the capacity to achieve highly accurate automatic personal identification is becoming more critical. Traditionally, passwords (knowledge-based security) and ID cards (token-based security) have been used to restrict access to systems.

In the world of computer security, biometrics refers to authentication techniques that rely on measurable physiological and different characteristics that can be automatically verified. In other words, we all have unique personal attributes that can be utilized for distinctive identification purposes, including a fingerprint, the pattern of a retina, and voice characteristics. Strong or two-factor authentication—identifying oneself by two of the three methods of something you know (for example, a password), have (for example, a swipe card), or is (for example, a fingerprint)—is becoming more of a genuine standard in secure computing environments. Some personal computers today can include a fingerprint scanner where you place your index finger to provide verification. The computer analyzes your fingerprint to determine who you are and, based on your identity followed by a pass code or pass phrase, allows you different levels of access. Access levels can include the ability to open sensitive files, to use credit card information to make electronic purchases, and so on.

II. SYSTEM DESIGN

A fingerprint recognition system constitutes of fingerprint acquiring devices, minutia extractor, and minutia matcher. For fingerprint acquisition, optical or semi-conduct sensors are widely used. They have high efficiency and acceptable accuracy except for some cases that the user's finger is too dirty or dry.

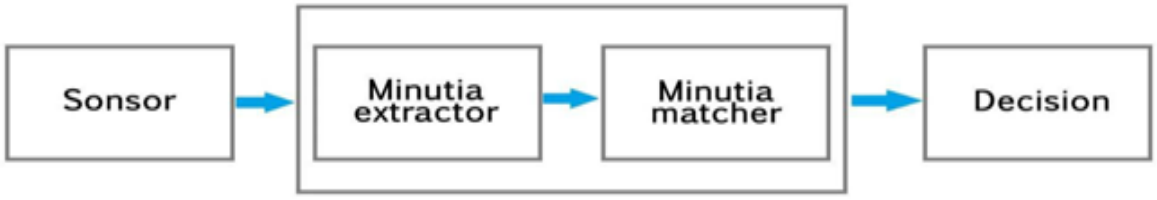

FIGURE 4: Block diagram of Simplified Fingerprint Recognition System

III. ALGORITHM

To implement a minutia extractor, a three-stage approach is widely used by researchers. They are preprocessing, minutia extraction and post-processing stage. For the fingerprint image preprocessing stage, Histogram Equalization and Fourier Transform are used to do image enhancement and then the fingerprint image is binarized using the locally adaptive threshold method. The image segmentation task is fulfilled by a three-step approach: block direction estimation, segmentation by direction intensity and Region of Interest extraction by Morphological operations.

For minutia extraction stage, the iterative parallel thinning algorithm is used. The minutia marking is a relatively simple task. For the post-processing stage, a more rigorous algorithm is developed to remove false minutia. The minutia matcher chooses any two minutiae as a reference minutia pair and then matches their associated ridges first. If the ridges match well, the two fingerprint images are aligned and matching is conducted for all the remaining minutiae.

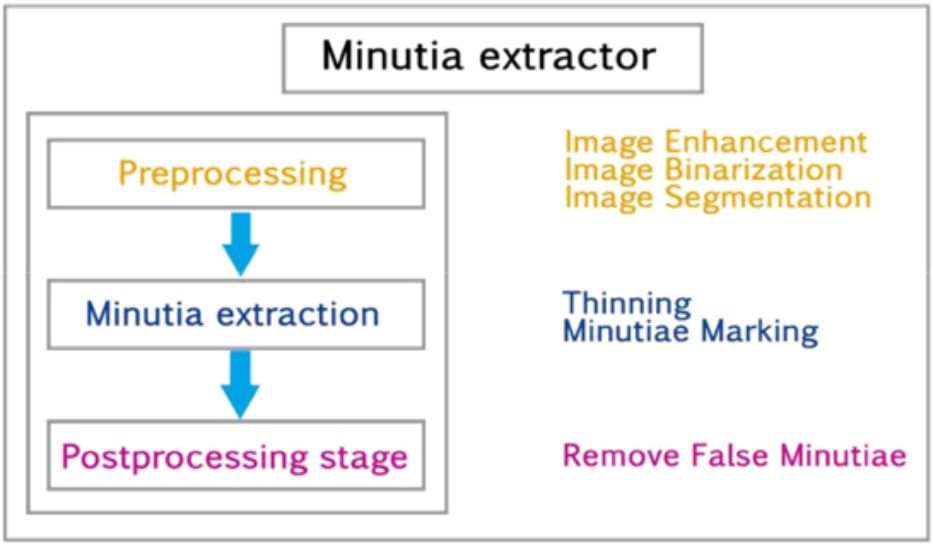

FIGURE 5: Block Diagram of minutia extractor of Fingerprint Recognition system

IV. FINGERPRINT IMAGE PRE-PROCESSING

Fingerprint Image Enhancement: Two Methods are adopted in my fingerprint recognition system; a. Histogram Equalization b. Fourier Transform.

a. The right side of the following figure [Figure 6] is the output after the histogram equalization.

FIGURE 6: Histogram Enhancement Original Image (Left). Enhanced image (Right)

b. Divided the image into small processing blocks (32 by 32 pixels) and perform the Fourier transform according to-

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

$$F(u,v) = \sum_{r-0}^{M-1}\sum_{y=0}^{N-1} f(x,y)x * exp\{j2r * (\frac{ux}{M} + \frac{vy}{N})\}$$

For u = 0, 1, 2, ..., 31 and v = 0, 1, 2, ..., 31.

In order to enhance a specific block by its dominant frequencies, 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

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

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

$$f(x,y) = \frac{1}{MN}\sum_{r-0}^{M-1}\sum_{y=0}^{N-1} f(x,y)x * exp\{j2r * (\frac{ux}{M} + \frac{vy}{N})\}$$

for $x = 0, 1, 2, ..., 31$ and $y = 0, 1, 2, ..., 31$.

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. Figure 7 presents the image after FFT enhancement.

FIGURE 7: Fingerprint Enhancement by FFT Enhanced image (right) Original image (left)

The enhanced image after FFT has the improvements to connect some falsely broken points on ridges and to remove some spurious connections between ridges. The shown image at the left side of figure 7 is also processed with histogram equalization after the FFT transform. The side effect of each block is obvious but it has no harm to the further operations because I find the image after consecutive binarization operation is pretty good as long as the side effect is not too severe.

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 color while furrows are white. A locally adaptive binarization method is performed to binarize the fingerprint image. Such a named method 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 in Figure 8.

FIGURE 8: Fingerprint image after adaptive binarization, Binarized image (right), original image (left)

Fingerprint Image Segmentation: Generally, only a Region of Interest (ROI) is useful to be recognized for each fingerprint image. The image area without effective ridges and furrows is first discarded since it only holds background information. Then the bound of the remaining effective area is sketched out since the minutia in the bound region is confusing with that spurious minutia that is generated when the ridges are out of the sensor.

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

a) Block direction estimation**:** Estimate the block direction for each block of the fingerprint image with WxW_y in size (W is 16 pixels by default). The algorithm is:

1. Calculate the gradient values along x-direction (g_x) and y-direction (g_y) for each pixel of the block. Two Sobel filters are used to fulfill the task.

2. For each block, use following formula to get the Least Square approximation of the block direction.

$$tg2ß = 2(g_x*g_y) / (g_x^2-g_y^2)$$ 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. So the tangent value of the block direction is estimated nearly the same as the way illustrated by the following formula.

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

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

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

For each block, if its certainty level E is below a threshold, then the block is regarded as a background block. The direction map is shown in the following diagram. We assume there is only one fingerprint in each image.

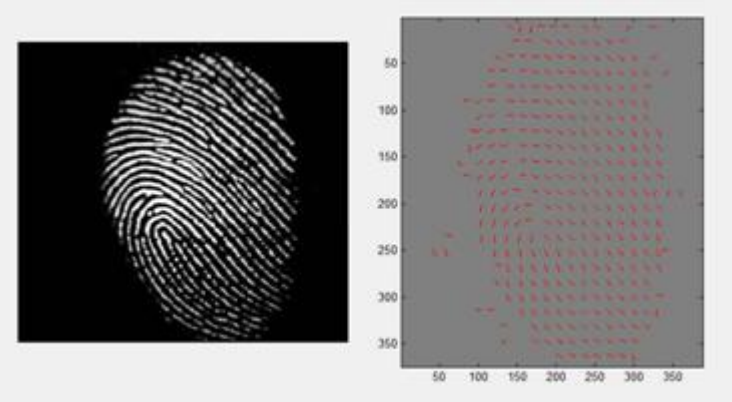

FIGURE 9: Direction map Binarized fingerprint (left), Direction map (right)

b) ROI extraction by Morphological operation: 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.

FIGURE 10: Region of Interest

Figure 10 shows the interest fingerprint image area and it's bound. The bound is the subtraction of the closed area from the opened area. Then the algorithm throws away those leftmost, rightmost, upper most and bottom blocks out of the bound so as to get the tightly bounded region just containing the bound and inner area.

V. MINUTIA POST-PROCESSING

The procedure of removing false minutia:

1. If the distance between one bifurcation and one termination is less than D and the two minutia are in the same ridge (m1 case) . Remove both of them. Where D is the average inter-ridge width representing the average distance between two parallel neighboring ridges.
2. If the distance between two bifurcations is less than D and they are in the same ridge, remove the two bifurcations. (m2, m3 cases).
3. If two terminations are within a distance D and their directions are coincident with a small angle variation. And they suffice the condition that no 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. (case m4, m5, m6).
4. If two terminations are located in a short ridge with length less than D, remove the two terminations (m7).

My proposed procedures in removing false minutia have two advantages. One is that the ridge ID is used to distinguish minutia and the seven types of false minutia are strictly defined comparing with those loosely defined by other methods. The second advantage is that the order of removal procedures is well considered to reduce the computation complexity. It surpasses the way adopted by [12] that does not utilize the relations among the false minutia types. For example, the procedure3 solves the m4, m5 and m6 cases in a single check routine and after procedure 3, the number of false minutia satisfying the m7 case is significantly reduced.

VI. MINUTIA MATCH

Given two sets of minutia of two fingerprint images, the minutia match algorithm determines whether the two minutia sets are from the same finger or not an alignment-based match algorithm partially derived from the [14] is used in my replace. It includes two consecutive stages:

Stage 1: Alignment Stage

The ridge associated with each minutia is represented as a series of *x*-coordinates $(x_1, x_2 \ldots x_n)$ of the points on the ridge. A point is sampled per ridge length L starting from the minutia point, where the L is the average inter-ridge length. And *n* is set to 10 unless the total ridge length is less than $10*L$. So the similarity of correlating the two ridges is derived from:

$S = m_{i=0}\, x_i X_i / [m_{i=0} x_i^2 X_i^2]^{0.5}$ Where, $(x_i \sim x_n)$ and $(X_i \sim X_N)$ are the set of minutia for each fingerprint image respectively and *m* is minimal one of the *n* and *N* value.

Stage 2: Match Stage

The matching algorithm for the aligned minutia patterns needs to be elastic since the strict match requiring that all parameters (x, y) are the same for two identical minutia is impossible due to the slight deformations and inexact quantization of minutia. My approach to elastically match minutia is achieved by placing a bounding box around each template minutia. If the minutia to be matched is within the rectangle box and the direction discrepancy between them is very small, then the two minutia are regarded as a matched minutia pair. Each minutia in the template image either has no matched minutia or has only one corresponding minutia. The final match ratio for two fingerprints is the number of total matched pair over the number of minutia of the template fingerprint. The score is 100*ratio and ranges from 0 to 100. If the score is larger than a pre-specified threshold, the two fingerprints are from the same finger. However, the elastic match algorithm has large computation complexity and is vulnerable to spurious minutia.

VII. EXPERIMENTATION RESULTS

A fingerprint database from the FVC2000 (Fingerprint Verification Competition 2000) is used to test the experiment performance. My program tests all the images without any fine-tuning for the database. The experiments show my program can differentiate imposturous minutia pairs from genuine minutia pairs in a certain confidence level. Furthermore, good experiment designs can surely improve the accuracy as declared by [10] further studies on good designs of training and testing are expected to improve the result.

Here is the diagram for Correct Score and Incorrect Score distribution:

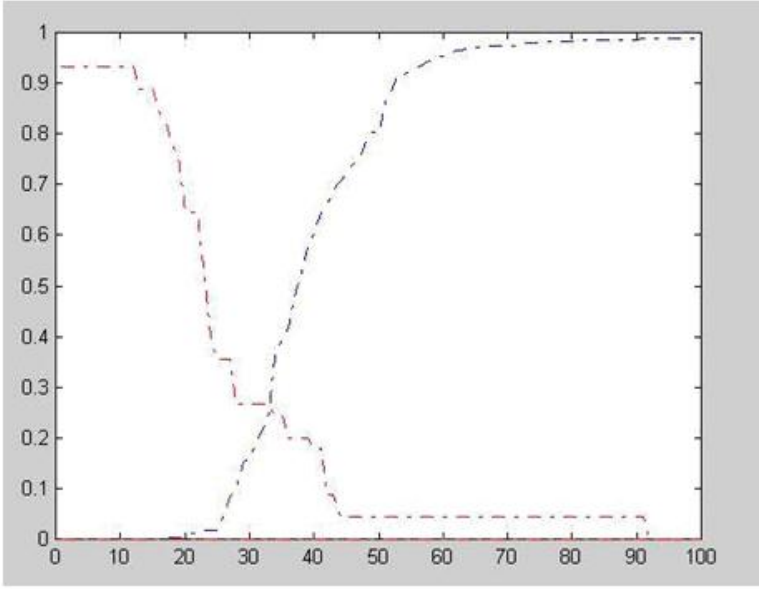

FIGURE 11: Distribution of Correct Scores and Incorrect Scores, Red line: Incorrect Score Green line: Correct Scores

It can be seen from the above figure that there exist two partially overlapped distributions. The Red curve whose peaks are mainly located at the left part means the average incorrect match score is 25. The green curve whose peaks are mainly located on the right side of red curve means the average correct match score is 35. This indicates the algorithm is capable of differentiate fingerprints at a good correct rate by setting an appropriate threshold value.

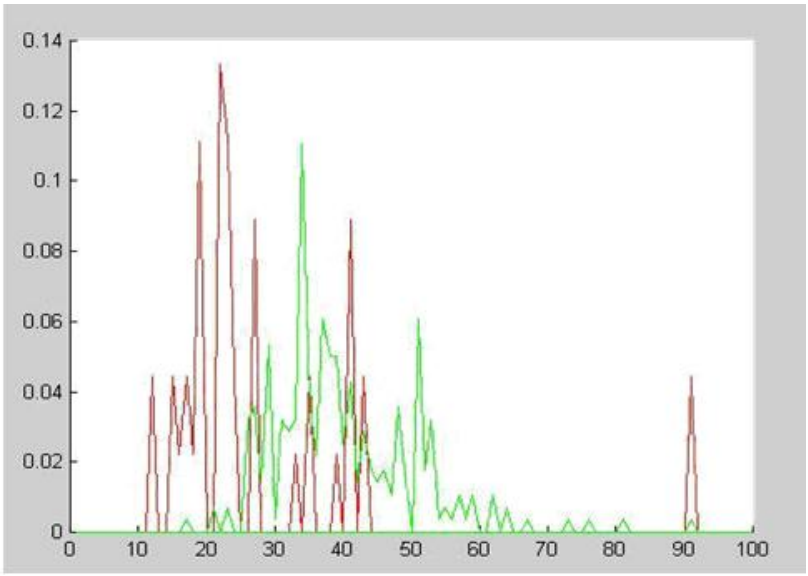

FIGURE 12: FAR and FRR curve, Blue dot line: FRR curve, Red dot line: FAR curve

The above diagram shows the FRR and FAR curves. At the equal error rate of 25%, the separating score 33 will falsely reject 25% genuine minutia pairs and falsely accept 25% imposturous minutia pairs and has 75% verification rate. The high incorrect acceptance and false rejection are due to some fingerprint images with bad quality and the vulnerable minutia match algorithm.

VIII. CONCLUSION

This research has combined many methods to build a minutia extractor and a minutia matcher. The combination of multiple methods comes from a wide investigation into the research paper. Also, some novel changes like segmentation using Morphological operations, minutia marking with special considering the triple branch counting, minutia unification by decomposing a branch into three terminations, and matching in the unified x-y coordinate system after a two-step transformation are used in my replace, which are not reported in other literature I referred to. Also, a program coding with

MATLAB going through all the stages of the fingerprint recognition is built. It is helpful to understand the procedures of fingerprint recognition and demonstrate the key issues of fingerprint recognition.

REFERENCES

[1] S. Sanderson, J. Erbetta. Authentication for secure environments based on iris scanning technology. IEE Colloquium on Visual Biometrics, 2000.

[2] D.Maio and D. Maltoni. Direct gray-scale minutiae detection in fingerprints.IEEE Trans. Pattern Anal. And Machine Intell., 19(1):27-40, 1997.

[3] Jain, A.K., Hong, L., and Bolle, R.(1997), "On-Line Fingerprint Verification," IEEE Trans. On Pattern Anal and Machine Intell, 19(4), pp. 302-314.

[4] N. Ratha, S. Chen and A.K. Jain, "Adaptive Flow Orientation Based Feature Extraction in Fingerprint Images", Pattern Recognition, Vol. 28, pp. 1657-1672, November 1995.

[5] Alessandro Farina, ZsoltM.Kovacs-Vajna, Alberto leone, Fingerprint minutiae extraction from skeletonized binary images, Pattern Recognition, Vol.32, No.4, pp877-889, 1999.

[6] Lee, C.J., and Wang, S.D.: Fingerprint feature extration using Gabor filters, Electron. Lett., 1999, 35, (4), pp.288-290.

[7] M. Tico, P.Kuosmanen and J.Saarinen. Wavelet domain features for fingerprint recognition, Electroni. Lett., 2001, 37, (1), pp.21-22.

[8] L. Hong, Y. Wan and A.K. Jain, "Fingerprint Image Enhancement: Algorithms and Performance Evaluation", IEEE Transactions on PAMI ,Vol. 20, No. 8, pp.777-789, August 1998.

[9] 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.

[10] M. J. Donahue and S. I. Rokhlin, "On the Use of Level Curves in Image Analysis," Image Understanding, VOL. 57, pp 652 - 655, 1992.