International Journal of Computational Intelligence and Informatics, Vol. 2: No. 4, January - March 2013

Cryptographic key generation from multiple fingerprints

K Sasirekha
Department of Computer Science
Periyar University
Salem, Tamilnadu
Ksasirekha7@gmail.com

K Thangavel
Department of Computer Science
Periyar University
Salem, Tamilnadu
drktvelu@yahoo.com

K Saranya
Department of Computer Science
Periyar University
Salem, Tamilnadu
saranyasekar19@gmail.com

***Abstract*- This research deals with new innovative model for biometric Automated Teller Machines (ATMs) for joint account without the remembrance of a Personal Identification Number (PIN). Since the banks in India are not providing ATM card for "joint and other account" system. In this research cryptographic key is generated from the fused biometric fingerprint of the joint account holders which can be used as a PIN at the ATM terminal. Among all the biometrics, fingerprint based identification is highly scalable and proven technique. Proposed model provides high security in authentication for joint account holders. At the time of transaction fingerprint images are acquired from the account holders at the ATM terminal using high resolution fingerprint scanner and the extracted images are preprocessed for enhancing the image, then the minutiae points (ridge ending and bifurcation) are extracted from the preprocessed fingerprint image. The extracted features from the account holders are compared with the existing image in the database for authentication. If there is a match, then the extracted features are fused at the feature level to attain the fused fingerprint model. Finally a 256-bit cryptographic key is generated from the fused fingerprint image. The generated cryptographic key can be used as a PIN at the ATM terminal for transaction. This model reduces complexity with authentication as "authentication is always with you" with high security. It also saves time, cost and efforts compared with the traditional ATMs.**

Keywords-ATM, joint account, fingerprint, fusion, cryptographic key

I. INTRODUCTION

A. Biometric Fingerprint

Biometric authentication refers to verifying individuals based on their physiological and behavioral characteristics. Biometric technologies are widely used in many applications for various purposes for personal authentication. Biometric methods provide a higher level of security and are more convenient for the user than traditional methods of personal authentication based on the use of passwords (codes) [1]. Among all the biometrics, fingerprints is a great source for identification of individuals. Fingerprint authentication is essentially a pattern recognition system that distinguishes a person by determining the authenticity of specific physiological characteristics of the fingerprint. Minutiae-based method compares fingerprint using a small number of features extracted from the fingerprint such as ridge ending and bifurcation, called minutiae. It is the most widely used method to perform fingerprint authentication because of its high speed and accuracy. For these reasons, fingerprint method has been selected among all other biometrics and the minutia points are extracted from the fingerprint image for authentication and key generation [2]. The fingerprint image is shown in fig. 1.

Figure 1. Biometric Fingerprint

B. Biometric Cryptography

Biometric cryptosystems combine cryptography and biometrics to benefit from the strengths of both fields [3]. In such systems, cryptography provides high and adjustable security levels; biometrics brings in non-repudiation and eliminates the need to remember passwords or to carry tokens. In biometric cryptosystems, a cryptographic key is generated from the biometric template of a user stored in the database in such a way that the key cannot be revealed without a successful biometric authentication. In this work, the cryptographic key is generated from the fused fingerprint image of the joint account holders.

C. Biometric ATM for Joint Account

Banks in India have started introducing biometric ATMs as it seems to be an effective way of preventing card usage [4, 5 and 6]. So far no banks in India have been introduced ATM for the joint account holders. In this research, biometric based key generation has been used to operate ATM with the fusion of fingerprint images of the joint account holders.

The overall methodology is depicted in the following fig. 2.

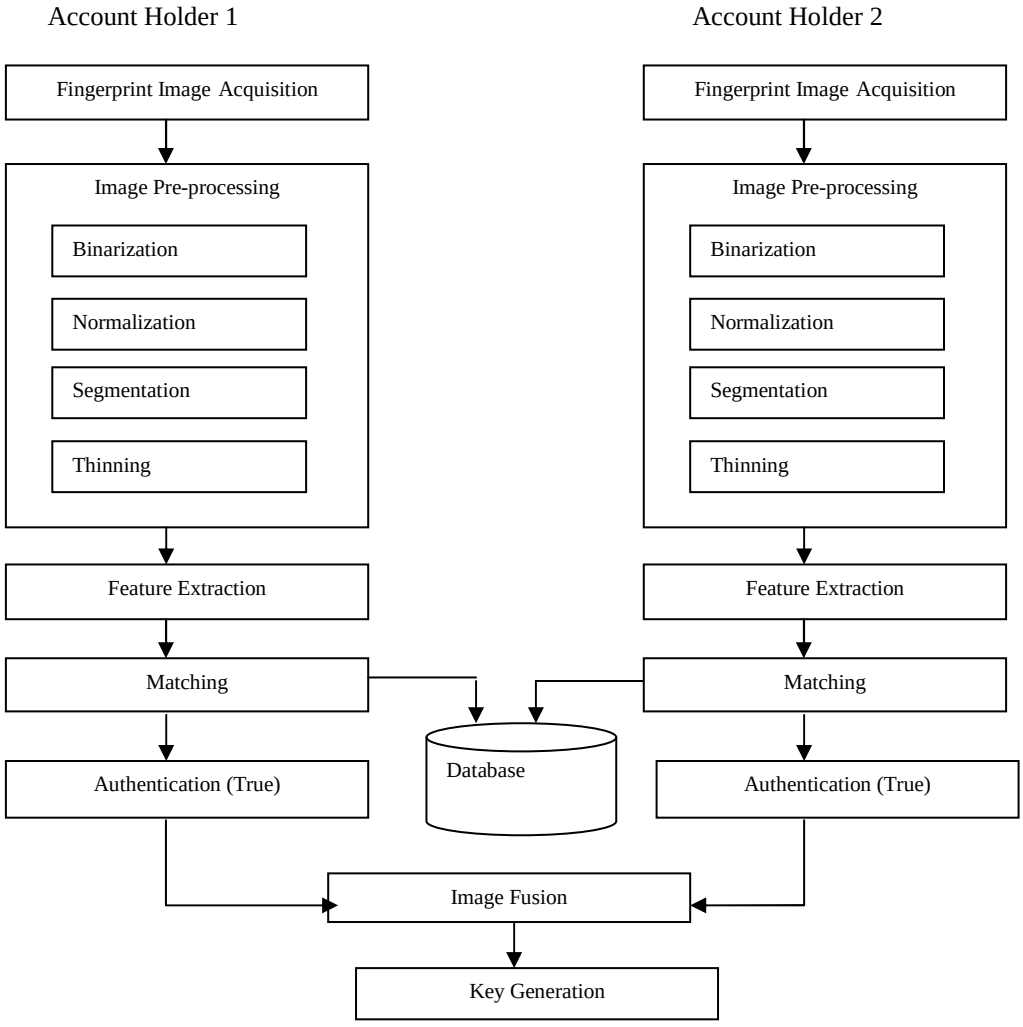


Figure 2. Overall Methodology

II. ORGANIZATION OF THE PAPER

Fingerprint images are acquired from the publicly available sources. The acquired images are preprocessed in section III. Preprocessing includes binarization using threshold, normalization using min-max method, segmentation to extract ROI and thinning to reduce the ridge thickness. After preprocessing, the minutiae points are extracted in section IV using Crossing Number (CN) method. Fingerprint matching and fusion is performed in section V. Finally a 256-bit cryptographic key is generated from the fused fingerprint in section VI.

III. PREPOCESSING OF THE FINGERPRINT IMAGE

Fingerprint images are difficult to interpret, and pre-processing phase of the images is necessary to improve the quality of the images and make the feature extraction phase more reliable [7].

A. Binarization

The acquired grayscale image is converted to binary image based on the threshold. The output image replaces all pixels in the input image with luminance greater than threshold with the value 1 (white) and replaces all other pixels with the value 0 (black). The threshold value is in the range (0, 1). We have used the function graythresh to compute the threshold.

$$Pval[i] = \begin{cases} 1 & if\ G[i] \geq Threshold \\ 0 & Otherwise \end{cases}$$

where G[i] is the intensity value of the grayscale image at the pixel i and Pval[i] is the grey value of the binarized image at the pixel i. Grey value 1 denotes the background of the image and the valley of the fingerprint. Grey value 0 denotes the ridge of the fingerprint in the image. The binarized image (fig. 3b) of original image (fig. 3a)

Figure 3a. Original Image **3b. Binarized Image**

B. Normalization

Normalization is a process that changes the range of pixel intensity values. Normalization is a necessary step and we normalize the fingerprint image by mapping the intensity levels into the range [gmin, gmax]. The formula for gray level normalization is given below.

$$g(i,j) = g_{\min} + \frac{(g_{\max} - g_{\min})\mathrm{X}(g_o(i,j) - g_{o\min})}{(g_{o\max} - g_{o\min})}$$

where gomin and gomax are the minimum and maximum intensity levels of the original image, gmin and gmax are the minimum and maximum intensity levels of the normalized image, and go(i, j) and g(i, j) are the gray levels at the coordinates (i, j) before and after normalization[8]. The normalized image is shown in fig. 4.

Figure 4. Normalized Image

C. Segmentation

Segmentation is the process of separating the foreground regions in the image from the background regions. The foreground regions correspond to the clear fingerprint area containing the ridges and valleys, which is the area of interest. The background corresponds to the regions outside the borders of the fingerprint area, which do not contain any valid fingerprint information [9]. When minutiae extraction algorithms are applied to the background regions of an image, it results in the extraction of noisy and false minutiae. Thus, segmentation is employed to discard these background regions, which facilitates the reliable extraction of minutiae.

In a fingerprint image, the background regions generally exhibit a very low grey-scale variance value, whereas the foreground regions have a very high variance. Hence, a method based on variance threshold can be used to perform the segmentation. First, the image is divided into blocks and the grey-scale variance is calculated for each block in the image. If the variance is less than the global threshold, then the block is assigned to be a background region; otherwise, it is assigned to be part of the foreground. The grey-level variance for a block of size W×W is defined as:

$$V(k) = \frac{1}{W^2} \sum_{i=0}^{W-1} \sum_{j=0}^{W-1} \big(I(i,j) - M(k)\big)^2$$

where V(k) is the variance for block k, I (i, j) is the grey-level value at pixel (i, j) and M(k) is the mean grey-level value for the block k.

D. Thinning

After the fingerprint image is enhanced, it is then converted to thinned image as in fig. 5 which reduces the ridge thickness to one pixel wide. Thinning is a morphological operation that is used to remove selected foreground pixels from enhanced images. The result of thinning shows that the connectivity of the ridge structures is well preserved, and that the skeleton is eight-connected throughout the image [10].

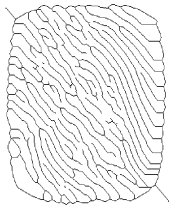


Figure 5. Thinned Image

IV. EXTRACTION OF MINUTIA POINTS FROM FINGERPRINTS

After the enhancement of the fingerprint image, minutiae points have been extracted in the next step [11, 12]. The ridge endings and bifurcations are from the skeleton image by examining the local neighbourhood of each ridge pixel using a 3×3 window.

The most commonly employed method of minutiae extraction in this category is the Crossing Number (CN) concept as shown in Table1 [13]. A large number of techniques for minutiae extraction available in the literature belong to this category. This method involves the use of the skeleton image where the ridge flow pattern is eight-connected. The minutiae are extracted by scanning the local neighborhood of each ridge pixel in the image using a 3×3 window. CN is defined as half the sum of the differences between the pairs of adjacent pixel.

The ridge pixel can be divided into bifurcation, ridge ending and non-minutiae point based on the neighbor. A ridge ending point has only one neighbor, a bifurcation point possesses more than two neighbors, and a normal ridge pixel has two neighbors. A CN value of zero refers to an isolated point, value of one to a ridge ending, two to a continuing ridge point, three to a bifurcation point and a CN of four means a crossing point. Minutiae detection in a fingerprint skeleton is implemented by scanning thinned fingerprint and counting the crossing number as given in table 3 and table4. The CN is given by,

$$CN = 0.5 \sum_{i=1}^{8} |p_i - p_{i+1}|, \qquad p_9 = p_1$$

where p_i is the pixel value in the neighbourhood of p. For a pixel p, its eight neighbouring pixels are scanned in an anti-clockwise direction. Table 2 shows the pixel representation of 3×3 window. Fig. 6 shows the extracted minutiae.

Table 1. Properties of Crossing Number

CN	Property
0	Isolated point
1	Ridge ending point
2	Continuing ridge point
3	Bifurcation point
4	Crossing point

Table 2. 3 × 3 Neighbourhood pixel window

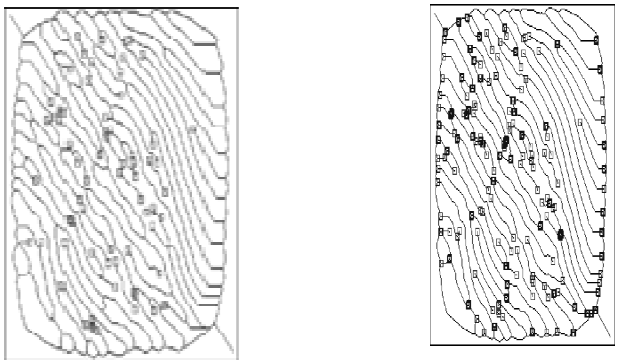
p4	p3	p2
p5	p	p1
p6	p7	p8

Table 3. Ridge Ending (CN=1)

p4	p3	p2
p5	p	p1
p6	p7	p8

Table 4. Bifurcation (CN=3)

p4	p3	p2
p5	p	p1
p6	p7	p8



Ridge Ending Bifurcation and Ridge Ending

Figure. 6 Minutiae Extraction (Ridge Ending and Bifurcation)

V. FINGERPRINT MATCHING AND FUSION

A. Minutiae Matching

Minutiae matching is the process which compares the minutiae extracted from the joint account holders with the minutiae already stored in the database and test whether they are from the same fingerprint or not.

In matching module, two fingerprint images are matched with the help of extracted local features. Depending upon the obtained matching score, two fingerprints are declared as matched or not-matched [14].

Minutiae based techniques represent the fingerprint by its local features, like terminations and bifurcations. Two fingerprints match if their minutiae points match. This approach has been intensively studied, also is the backbone of the current available fingerprint recognition products.

Hence, it is decided to implement a minutiae matching algorithm which was inspired by the techniques involving computation of local and global minutiae features. This algorithm grouped all the minutiae into triplets of minutiae. For each of these triplets of minutiae we stored the distance of one of the minutiae from both other minutiae and the angle formed in between these two distances. Fig. 7 shows the angle and distance between two minutiae points.

Here, the fingerprints of the joint account holders are compared with the existing through minutiae matching. If both the account holders fingerprints were matched, then he/she is authenticated.

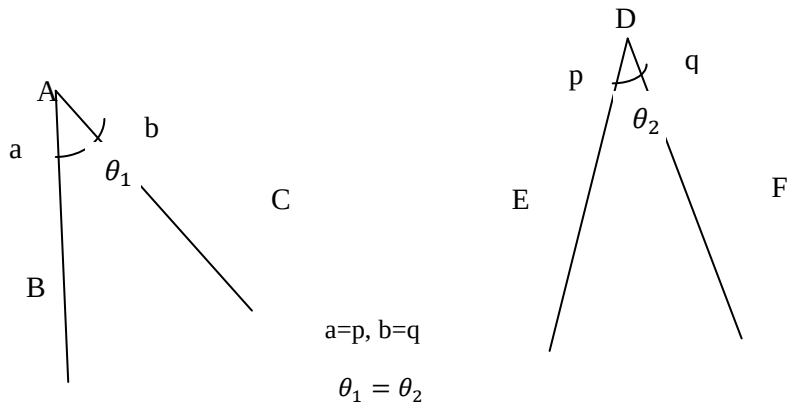


Figure 7. Angle and distance of minutiae points

B. Minutiae Fusion

After the matching process, the extracted features from the joint account holders are to be fused to get a fused matrix for generating the cryptographic key. The three possible levels of fusion are:

- Fusion at the feature extraction level
- Fusion at the matching score level
- Fusion at the decision level

In our research we have fused the minutiae at the feature extraction level. The extracted features are fused randomly.

$$C = A(D) + B(\sim D)$$

Where C is the fused matrix, A and D are feature matrices from the joint account holders respectively and D is a Boolean random matrix.

VI. CRYPTOGRAPHIC KEY GENERATION FROM FINGERPRINT

The fused minutiae points from joint account holders are maintained in a vector. The key generation algorithm [15] is as follows:

Algorithm 1: Cryptographic Key Generation

M_p- Fused Minutiae points set
S_p- Size of M_p
KeyLen- Initialize Key Length. Here KeyLen=256
Steps:
Step 1: Read the Fused Minutiae points
Step 2: Find the point H with highest x + y
Step 3: Draw a line from origin (0, 0) to the H and call it as L
Step 4: Sort the minutiae points and store in an array A
Step 5: value= KeyLen/S_p
vector= KeyLen%S_p
Step 6: For i=1 to value
For j=1 to S_p
Read point X from Array A and check the point whether it is above or below the line L
If it is above the line or on the line assign the value as "0" else value is "1"
Store them in array K
Final key=Append the key vector of length vector to value of K

VII. EXPERIMENTAL RESULTS

The proposed model is implemented in MATLAB and fixed size cryptographic key is generated with minimum amount of time complexity, which is aptly suited for any real time cryptography. Thus the generated 256-bit key can be used as a key at the ATM terminal for accessing the ATM without the need of a PIN number [16, 17]. Fig. 7 shows the overall implementation of the proposed model.

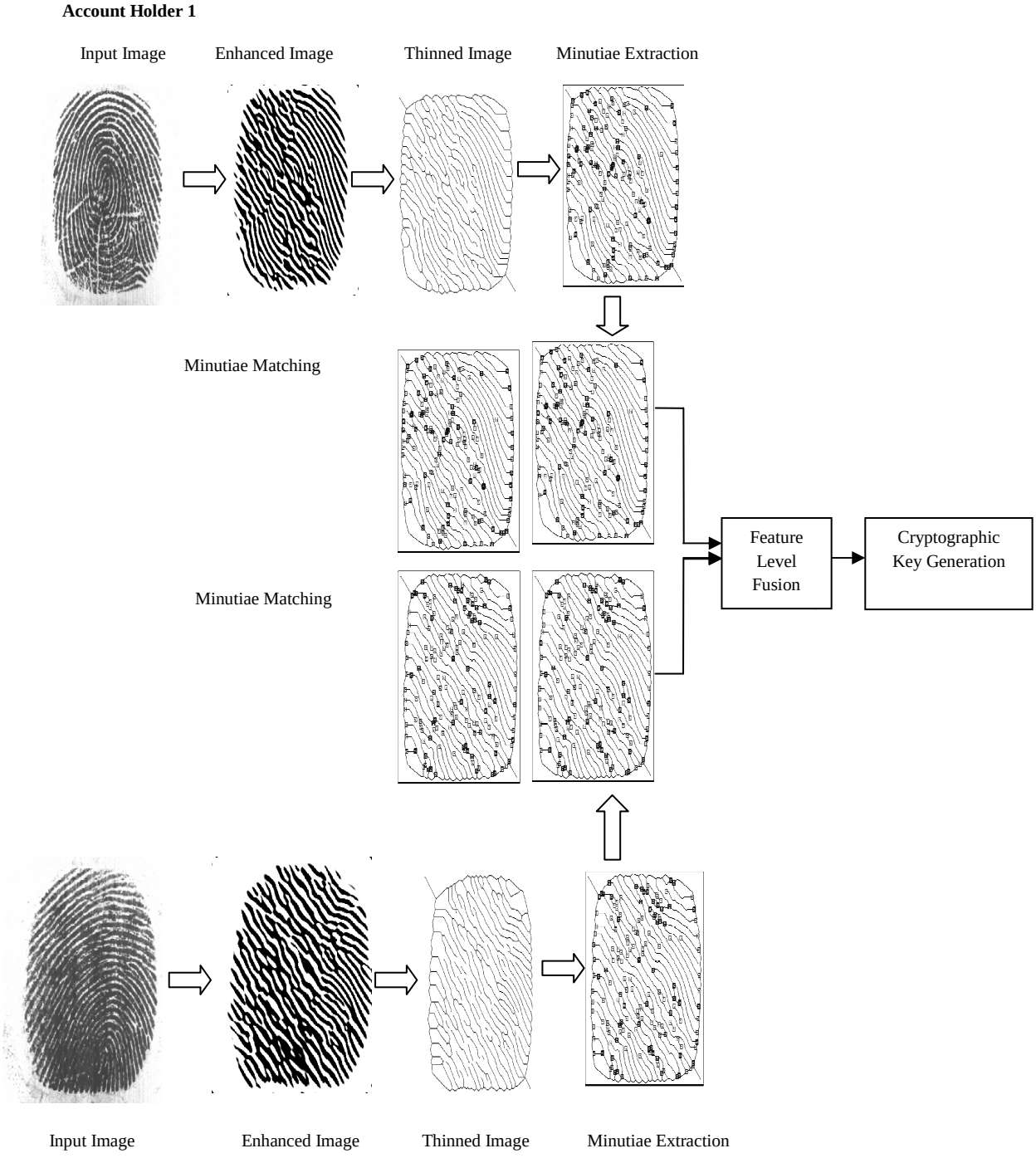


Figure 7. Overall Implementation

The generated 256- bit cryptographic key is

1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1 1 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0

VIII. CONCLUSION

Securing the information system becomes most challenging task because of the increased number of theft. The conventional ATM system for single account holder uses card and PIN for authentication; but those card and PIN can be easily stolen by the theft. To overcome these issues, fingerprint biometrics was used for accessing the ATM. Thus the biometric ATMs for joint account holders were introduced with the generation of 256-bit cryptographic key from the fused fingerprint image of the joint account holders. The main advantage of this system is that there is no need to remember PIN for accessing the ATM since the authentication is always with you.

REFERENCES

[1] F. Ahmad and D. Mohamad, "A Review on Fingerprint Classification Technique ", IEEE International Conference on Computer Technology and Development, pp. 411 – 415, 2009.

[2] Manvjeet Kaur, Mukhwinder Singh and Akshay Girdhar, "Fingerprint Verification System using Minutiae Extraction Technique", World Academy of Science, Engineering and Technology, pp. 497-502, 2008.

[3] U. Uludag, S. Pankanti, S. Prabhakar and A.K. Jain, "Biometric cryptosystems: issues and challenges", Proceedings of the IEEE, vol. 92, no. 6, pp. 948-960, 2004.

[4] Prof. Selina Oko and Jane Oruh, "Enhanced ATM Security System using Biometrics " International Journal of Computer Science(IJCSI) , vol. 9(5), no. 3, 2012.

[5] S.T. Bhosale and Dr. B.S.Sawant, "Security in E-Banking via Card Less Biometric ATMs", International Journal of Advanced Technology & Engineering Research (IJATER), vol. 2(4), 2012.

[6] Gang Zheng, Wanqing Li and Ce Zhan, "Cryptographic Key Generation from Biometric Data Using Lattice Mapping", Proceedings of the 18th International Conference on Pattern Recognition, vol.4, pp. 513 - 516, 2006.

[7] Om Preeti Chaurasia, "An Approach to Fingerprint Image Preprocessing", I.J. Image, Graphics and Signal Processing, pp.29-35, 2012.

[8] R. Subash Chandra Boss, K. Thangavel and D. Arul Pon Daniel, "Automatic Mammogram image Breast Region Extraction and Removal of Pectoral Muscle", International Journal of Scientific & Engineering Research, vol. 4, issue 2, February-2013.

[9] C. X. Ren, Y. L. Yin, J. Ma and G. P. Yang, "Feature selection for sensor interoperability: a case study in Fingerprint segmentation", Proceedings of the IEEE International Conference on Systems, Man and Cybernetics, pp. 5057–5062, 2009.

[10] A. Saleh, A. Eldin and A. Wahdan, "A modified thinning algorithm for fingerprint identification systems," International Conference on Computer Engineering & Systems, pp. 371–376, Dec 2009.

[11] J. C. Amengual, A. Juan, J. C. Prez and F. Prat, "Real-time minutiae extraction in fingerprint images", Proceedings of the 6th Int. Conference on Image Processing and its Applications, pp. 871–875, 1997.

[12] Roli Bansal, Priti Sehgal and Punal Bedi, "Minutiae Extraction from Fingerprint Images-a Review", IJCSI International Journal of Computer Science Issues, vol. 8, pp. 74-85, 2011.

[13] Ravi.J, Venugopal. K. R, " Fingerprint Recognition using Minutiae Score Matching", International Journal of Engineering Science and Technology, vol. 1(2), pp. 35-42, 2009.

[14] Jianjiang Feng "Combining minutiae descriptors for fingerprint matching", Pattern Recognition (elsevier), pp. 342-352, 2008.

[15] R. Seshadri and T. Raghu Trivedi, "Efficient Cryptographic Key Generation using Biometrics", International Journal of Computer Technology and Applications, vol. 2 (1), pp. 183-187, 2011.

[16] Moses Okechukwu Onyesolu and Ignatius Majesty Ezeani, "ATM Security Using Fingerprint Biometric Identifier: An Investigative Study", International Journal of Advanced Computer Science and Applications, vol. 3, no.4, pp. 68-72, 2012.

[17] Shimal Das and Jhunu Debbarma, "Designing a Biometric Strategy (Fingerprint) Measure for Enhancing ATM Security in Indian E-Banking System", International Journal of Information and Communication Technology Research(IJICT), vol.1,no.5,2011.