Finger Print Parameter Based Cryptographic Key Generation

B.Raja Rao, Dr.E.V.V.Krishna Rao, S.V.Rama Rao,M.Rama mohan rao
(Associate Professor, Department of ECE, URCE, Telaprolu,vijayawada.
(Professor & H.O.D, Department of ECE, ALIET, vijayawada.
(Associate Professor, Department of ECE, NRIIT,vijayawada.
(Associate Professor & H.O.D, ECE, URCE, Telaprolu,vijayawada.

ABSTRACT

A method is proposed for generation of unique cryptographic key which is generated using figure prints of the user, which are stable throughout person's lifetime. The proposed approach reduces the cost associated with lost keys, addresses non-repudiation issues and provides increased security of digital content. This approach has reduced the complicated sequence of the operation to generate crypto keys as in the traditional cryptography system . The key is derived directly from the figure print data and is not stored in the database, since it creates more complexity to crack or guess the cryptographic keys. Biometrics, cryptography and data hiding will provide good perspectives for information security. We proposed an algorithm for deriving the key from biometric for ECC (Elliptic Curve Cryptography) based applications which will provide high security with good performance in terms of computational and bandwidth requirements.There are several biometric systems in existence that deal with cryptography, but the proposed figure print parameter based cryptographic key introduces a novel method to generate cryptographic key. This approach is implemented in MATLAB and can generate variable size cryptographic key, with minimum amount of time complexity, which is aptly suited for any real time cryptography.

***Keywords* -** Cryptography, Biometrics, Minutiae points, Morphological Operation, Histogram Equalization, Crossing Number.

I. INTRODUCTION

With the widespread use of information exchange across the Internet, and the storage of sensitive data on open networks, cryptography is becoming an increasingly important feature of data security. Many cryptographic algorithms are available for securing information E.g. RSA, DES, AES etc. Normally used cryptosystem [1] have a number of associated inconveniences and problems such as:-

1. Conventional Cryptography authenticates messages based on the key but not on the user. Hence unable to differentiate between the legitimate user & an attacker.
2. These keys can be guessed or cracked.
3. Large size of strong keys results in longer delay in encryption/decryption.
4. It is difficult to remember the keys, storing them in a data base may be insecure.
5. Moreover, maintaining and sharing lengthy, random keys is the critical problem in the cryptography system.

A number of biometric characteristics are being used in various applications as Universality, Uniqueness, Permanence, Measurability, Performance, Acceptability, and Circumvention [2].

1.1 Biometric Based Cryptography

Biometrics and cryptography are two potentially complementary security technologies. Biometrics gives a unique, measurable biological characteristic for automatically recognizing or verifying the identity of a human being. Cryptography is an important feature of computer and network security. Using biometrics by means of cryptography is a new hot research topic. In this approach unique cryptographic key is derived directly from the biometric data of the user (i.e. fingerprint in this approach).The encryption process begins with the acquisition of the required biometric samples. Features and parameters are extracted from these samples and used to derive a biometric key that can be used to encrypt a plaintext message. The minutiae points are extracted from the fingerprint and that point set is used for generating encryption key. Minutiae points are locations where a fingerprint ridge ends or bifurcates. There are several benefits of the proposed approach:

1. This Biometric based cryptosystems combine cryptography and biometrics to benefit from the strengths of both fields.
2. Provides increased security of digital content.
3. Biometrics brings in non repudiation. Allow only the legal user to utilize the content.
4. The simplicity of use and the very limited risk of losing, stealing or forging the user's biological identifier.

1.2 Fingerprint

A fingerprint is the feature pattern of one finger [3]. Each person has his own fingerprints with the permanent uniqueness. However, shown by intensive research on finger print recognition, fingerprints are not distinguished by their ridges and furrows, but by Minutia, which are some abnormal points on the ridges as shown in Fig. 1. Among the variety of minutia types reported in literature, two are mostly significant and in heavy usage: one is called termination, which is the immediate ending of a ridge; the other is called bifurcation, which is the point on the ridge from which two branches derive. Valley is also referred as Furrow, Termination is called as Ending, and Bifurcation is also called as Branch.

The general shape of the finger print is generally used to pre-process the images .The first scientific study of figure print was made by Galton who divided the figure print into 3 classes.ie Loop, whorl and arch.

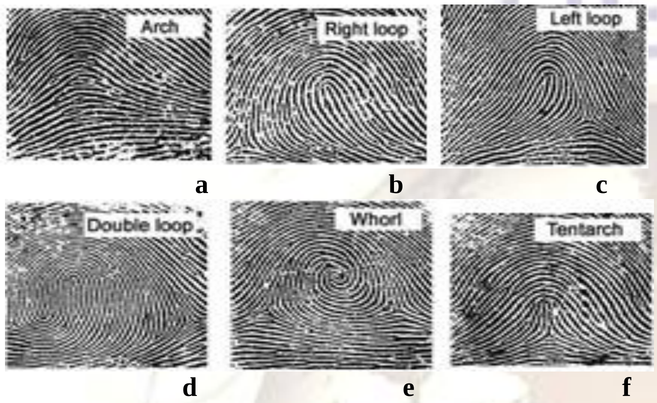
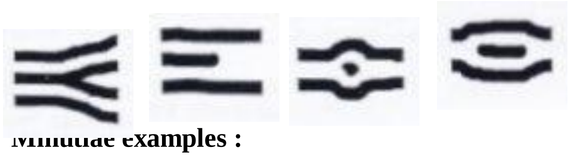


Fig.1.finger print types (a) arch (b) right loop (c) left loop (d) double loop (e) whorl (f) tent arch

The loop is by far the most common type of figure print .The human population has figure prints in the following percentages.

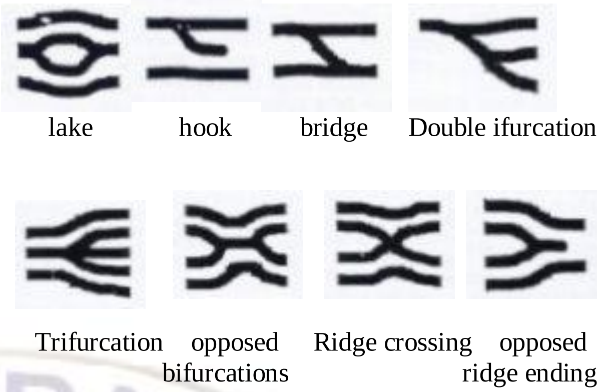
Loop – 65 % Whorl -30 % Arch - 05%.

In this approach fingerprint is used as a biometric parameter for generation of encryption key. Fingerprints have been used for over a century and are the most widely used form of biometric identification. The fingerprint of an individual is unique and remains unchanged over an individual's lifetime. A fingerprint is formed from an impression of the pattern of ridges on a finger. A ridge is valley is the region between two adjacent ridges. The set of minutiae types are restricted into only two types, ridge endings and bifurcations, Ridge endings are the points where the ridge curve terminates, and bifurcations are where a ridge splits from a single path to two paths at a Y-junction. Figure 1 illustrates an example of a ridge ending and a bifurcation. In this example, the black pixels correspond to the ridges, and the white pixels correspond to the valleys.



Minutiae examples :

Bifurcation Ridge ending dot island



lake hook bridge Double ifurcation

Trifurcation opposed bifurcations Ridge crossing opposed ridge ending

fig.2. Minutiae types with examples.

1.3 Unique Features Of Fingerprint :

1. Each fingerprint is unique to individuals i.e. no two fingers have identical ridge characteristics.
2. They are highly universal as majority of the population have legible fingerprints.
3. They are very reliable as no two people have same fingerprint. Even identical twins having similar DNA, are believed to have different fingerprints.
4. Fingerprints are formed in the fetal stage and remain structurally unchanged throughout an individual's lifetime.
5. It is one of the most accurate forms of biometrics available.
6. Fingerprint acquisition is non intrusive and hence is a good option.

II . CRYPTOGRAPHIC KEY GENERATION FROM FINGER PRINT BIOMETRIC

In our approach we have selected fingerprint as the biometrics feature for generating cryptographic key. We have extracted minutiae points from the fingerprint and that point set is used for generating cryptographic key.

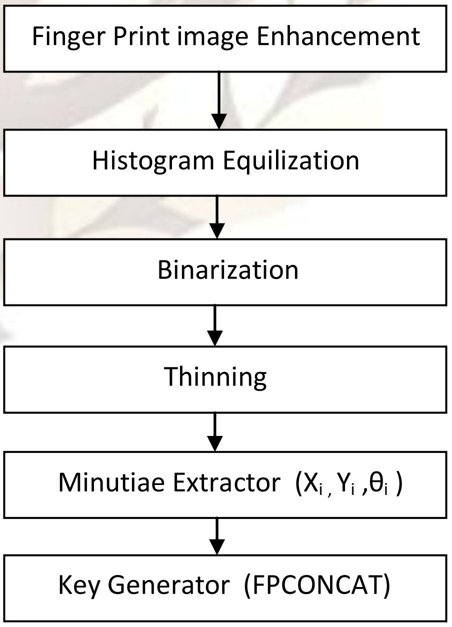

Finger Print image Enhancement
Histogram Equilization
Binarization
Thinning
Minutiae Extractor (X_i, Y_i, $θ_i$)
Key Generator (FPCONCAT)

fig.3.Block diagram of key generation system

The various steps required for generating cryptographic key from fingerprint biometric are

1. Fingerprint Image Enhancement
2. Histogram Equalization
3. Fingerprint Image Binarization
4. Thinning
5. Minutiae Extraction
6. Key generation

2. 1.Finger print Image Enhancement

Fingerprint Image Enhancement is to make the image clearer for easy further operations. Since the fingerprint images acquired from sensors or other media are not assured with perfect quality, 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 to keep a higher accuracy to fingerprint recognition[5]. The quality of the ridge structures in a fingerprint image is an important characteristic, as the ridges carry the information of characteristic features required for minutiae extraction. Ideally, in a well-defined fingerprint image, the ridges and valleys should alternate and flow in locally constant direction. This regularity facilitates the detection of ridges and consequently, allows minutiae to be precisely extracted from the thinned ridges. However, in practice, a fingerprint image may not always be well defined due to elements of noise that corrupt the clarity of the ridge structures. This corruption may occur due to variations in skin and impression conditions such as scars, humidity, dirt, and non-uniform contact with the fingerprint capture device. Thus, image enhancement techniques are often employed to reduce the noise and enhance the definition of ridges against valleys.

2.2. Histogram Equalization

Histogram equalization is to expand the pixel value distribution of an image so as to increase the perceptional information [6]. The original histogram of a fingerprint image has the bimodal type, the histogram after the histogram equalization occupies all the range from 0 to 255 and the visualization effect is enhanced.

2.3. Fingerprint Image Binarization

Most minutiae extraction algorithms operate on binary images where there are only two levels of interest: the black pixels that represent ridges, and the white pixels that represent valleys. Binarization is the process that converts a grey level image into a binary image. This improves the contrast between the ridges and valleys in a fingerprint image, and consequently facilitates the extraction of minutiae. The outcome is a binary image containing two levels of information, the foreground ridges and the background valleys. 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

2.4.Thinning

Thinning is the process of reducing the thickness of each line of patterns to just a single pixel width The requirements of a good thinning algorithm with respect to a finger print are

a) The thinned fingerprint image obtained should be of single pixel width with no discontinuities.

b) Each ridge should be thinned to its centre pixel.

c) Noise and singular pixels should be eliminated.

d) No further removal of pixels should be possible after completion of thinning process.

The final image enhancement step typically performed prior to minutiae extraction is thinning [9]. Thinning is a morphological operation that successively erodes away the foreground pixels until they are one pixel wide. A standard thinning algorithm is employed, which performs the thinning operation using two sub iterations. This algorithm is accessible in MATLAB via the `thin' operation under the bwmorph function. Each sub iteration begins by examining the neighborhoods of each pixel in the binary image, and based on a particular set of pixel-deletion criteria, it checks whether the pixel can be deleted or not. These sub iterations continue until no more pixels can be deleted. The application of the thinning algorithm to a fingerprint image preserves the connectivity of the ridge structures while forming a skeletonised version of the binary image. This skeleton image is then used in the subsequent extraction of minutiae.

2.5 Minutiae Extraction

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. Finger print verification is to verify the authenticity of one person by his fingerprint. There is one-to-one comparison in this case. 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 Techniques are used for Finger print Recognition

2.5.1.Minutiae Extraction Technique Most of the finger-scan technologies are based on Minutiae. Minutia-based techniques represent the finger print 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 work also concentrates on same approach.

2.5.2. Pattern Matching or Ridge Feature Based Techniques

Feature extraction and template generation are based on series of ridges as opposed to discrete points which forms the basis of Pattern Matching Techniques. The advantage of Pattern Matching techniques over Minutiae Extraction is that minutiae points may be affected by wear and tear and the dis advantages are that these are sensitive to proper placement of finger and need large storage for templates.

2.5.3. Correlation Based Technique

Two figure prints are superimposed and correlation between corresponding pixels is computed for different alignments.

The most commonly employed method of minutiae extraction is the Crossing Number (CN) concept. 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 neighborhoods of each ridge pixel in the image using a 3×3 window. The CN value is then computed, which is defined as half the sum of the differences between pairs of adjacent pixels in the eight-neighborhoods. Using the properties of the CN as shown in Table I below, the ridge pixel can then be classified as a ridge ending, bifurcation or non-minutiae point. For example, a ridge pixel with a CN of one corresponds to a ridge ending, and a CN of three corresponds to a bifurcation..

A method of securing communication is proposed which overcomes several problems associated with traditional cryptography. It provides a practical and secure way to integrate the fingerprint biometric into cryptographic applications. The crypto keys have been generated reliably from genuine fingerprint samples, which is stable throughout person's lifetime[7]. This approach has reduced the complicated sequence of the operation to generate crypto keys as in the traditional cryptography system and hence requires minimum amount of time complexity, which is aptly suited for any real time cryptography. Provides increased security of digital content. Biometrics brings in non repudiation and allow only the legal user to utilize the content. There is very limited risk of losing, stealing or forging the user's biological identifier.

Table I: Crossing Number Properties

S.no	Property	Crossing Number
1	Isolated point	0
2	Ridge ending point	1
3	Continuing ridge point	2
4	Bifurcation point	3
5	Crossing point	4

The Crossing Number (CN) method is used to perform minutiae extraction. This method extracts the ridge endings and bifurcations from the skeleton image by examining the local neighborhood of each ridge pixel using a 3×3 window. The CN for a ridge pixel *P* is given by

$$CN = 0.5\sum_{i=1}^{9}|P_i - (P_{i+1})| \text{ , } P_9 = P_1$$

P_4	P_3	P_2
P_5	P	P_1
P_6	P_7	P_8

a

0	0	1
0	1	0
0	0	0

b

1	1	0
1	1	0
0	0	0

c

where P_i is the pixel value in the neighborhood of P. For a pixel P, its eight neighboring pixels are scanned in an anti-
clockwise direction as follows

- If the central is one-value and has only one one-value as neighbor, then it is an end point like in Figure b).
- If the central is one-value and has three one-value as neighbor, then it is an bifurcation like in Fig c).

After the CN for a ridge pixel has been computed, the pixel can then be classified according to the property of its CN value. As shown in Table I, a ridge pixel with a CN of one corresponds to a ridge ending, and a CN of three corresponds to a bifurcation. For each extracted minutiae point, the following information is recorded

a) X and Y coordinates,
b) Orientation of the associated ridge segment, and
c) Type of minutiae (ridge ending or bifurcation).

Table II : Minutiae Points

Minutiae Position		Minutiae type	Minutiae Direction
X-Coordinate	**Y–Coordinate**	**Crossing Number**	**Theta**
33	238	3	270
174	335	1	135
394	327	1	45
503	537	3	225
698	112	1	90
856	381	3	270

2.6. Cryptographic Key Generation

Elliptic curves are mathematical constructs that have been studied by mathematicians since the seventeenth century. The following section will provide the general architecture of implementation and details about the algorithms for embedding minutiae on elliptic curve and the biometric based key generation method. To encode plaintexts as points on some elliptic curve E defined over a finite field Fp. Here plaintext is nothing but the minutiae co-ordinate which is extracted from the fingerprint. Minutiae is represented in three co-ordinate system as (x,y,θ). To map the minutiae on to the elliptic curve, this three co-ordinate minutiae are converted into one co-ordinate system and then this single co-ordinate value is mapped on to elliptic curve.Therefore in the proposed algorithm, by using these co-ordinates, the private key is generated. To generate the key, all the minutiae co-ordinates of the given image are to be extracted.

2.6.1. Algorithm

First, add all x co-ordinates, y co-ordinates and θ co-ordinates separately and then take average value each co-ordinates separately. This resultant average values of X and Y co-ordinates are in decimal representation and the co-ordinate θ will be in radians. Now this average values are converted into binary string separately subject to the condition that the input image should be resized into 256x256 array during preprocessing of the image for minutiae extraction. So maximum value for each co-ordinate require 9 bits for each X and Y co-ordinates to represent 256 and θ require maximum of 3 bits. Finally, these three binary strings are converted into one co-ordinate value by concatenation these three binary strings, which will give the private key for the given finger printimage. The algorithm **FPCONCAT** for the above processes follows as below:

Step 1: Get the binary values XBi, YBi and θBi of Xi, Yi and θi for given i th minutiae.

Step 2: Concatenate all the binary values in the following order.

MB_i = X Location (9bits) + X Location (9bits) +angle(3 bits)

Step 3: Convert the above concatenated binary string MBi to decimal to get the single co-ordinate value M1i.

Let K be a large enough integer so that the failure probability of 1 out of 2k will be satisfied when the plaintext m is attempted to imbed; in practice k=30. Suppose message units are integers 0 <= m <= M, then finite filed should be selected to satisfy q>Mk. Therefore the integers are from 1 to Mk in the form mk+j, where 1<=j<=k [10]. Thus the given m, for each j = 1,2,…,k obtain an element x of Fp corresponding to mk+j by using the following equation.

$$Y^2 = x^3 + a x + b \quad …….. \quad (1)$$

Step 1: Let k = 30

Step 2: $X_i = MB_i + j$ where 1 <=j<=k

Step 3. For each Xi, compute Yi using the following equation.

$$F(Xi) = Yi^2 = Xi^2 + aX_i + b \bmod p \;……(2)$$

Step 4: If f(X_i) is non square, then increment j by 1 and try

again with new X_i.

Step 5: If j reaches K, then increment k

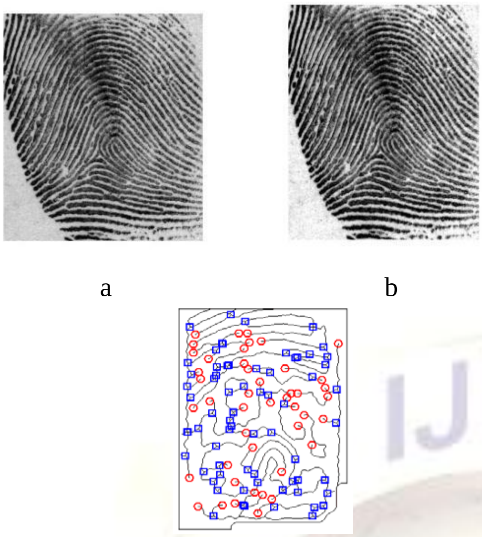
Step 6: Repeat the above steps for all minutiae

Step 7: Mapped points Pmi € E(F q)

Thus the single co-ordinate value is mapped on to the elliptic curve.

III. Experimental Results

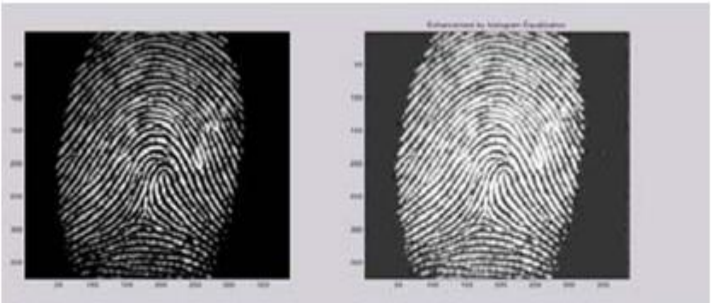
In real time application, it is applied in such a way that the enhanced finger print is given as input to the Minutiae Extractor. Output of Minutiae Extractor is the list of Minutiae Co-coordinators, which is given as input to the Key Generator, which will generates the biometric based key.. More than 100 finger print images were tested using different ECC parameter sets. The average computation time taken for the key generation process is 0.032 ms. This scheme is programmed in Matlab (Matlab7.6). We have tested the proposed system with diverse fingerprint images. The minutiae points are extracted from the fingerprint images using the approach discussed. A Unique cryptographic key is generated from the biometric template of a user. The following are the experimental results obtained for the proposed approach



a b

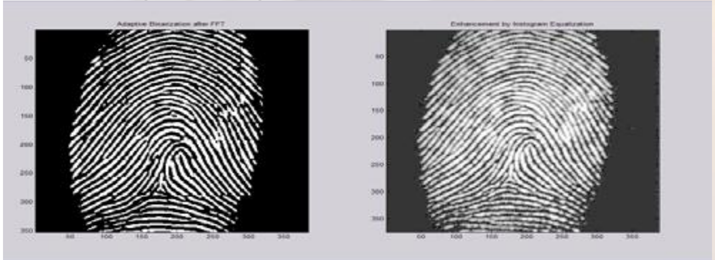
c

fig 4 a) Image of sample fingerprint b) Image after histogram equalization c) Minutiae Points



Original Image Enhanced image

fig. 5 Histogram Enhancement



Binarized image Enhanced gray image

fig. 6. Finger print image after Binarization

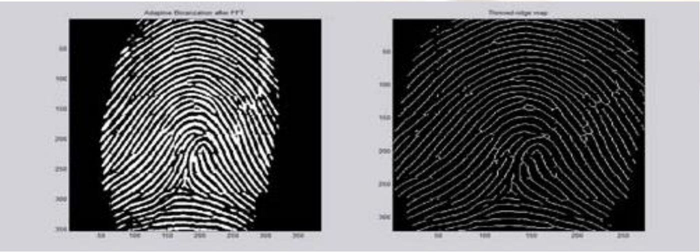


fig. 7. Finger print image after Thinning

The key generated from the sample finger print is

11000000000000011101000000110000010000000000001
10111110110000001100101110010010111110000000011
100100000010110000011000001000000000001010100
fig. 8. Generated key.

IV.CONCLUSION

A method of securing communication is proposed which overcomes several problems associated with traditional cryptography. It provides a practical and secure way to integrate the fingerprint biometric into cryptographic applications. The crypto keys have been generated reliably from genuine fingerprint samples, which is stable throughout person's lifetime. This approach has reduced the complicated sequence of the operation to generate crypto keys as in the traditional cryptography system and hence requires minimum amount of time complexity, which is aptly suited for any real time cryptography[11]. Since ECC is adopted, this architecture may be suitable for mobile based biometric applications.

References

[1] Umut Uludag, Sharath Pankanti, Salil Prabhakar, Anil K.Jain "Biometric Cryptosystems Issues and Challenges" Proceedings of the IEEE 2004.

[2] A. Jain, R. Bolle, and S. Pankanti, "Biometrics Personal Identification in Networked Society", Kluwer Academic Publishers New York, Boston, Dordrecht, London, Moscow, pp. 1-64, 2002.

[3] P. Komarinski, P. T. Higgins, and K. M. Higgins, K. Fox Lisa,"Automated Fingerprint Identification Systems (AFIS)", Elsevier cademic Press, pp. 1-118, 2005.

[4] D. Maltoni, D. Maio, and A. Jain, S. Prabhakar, "4.3: Minutiae-based Methods' (extract) from Handbook of Fingerprint Recognition",Springer, New York, pp. 141-144, 2003.

[5] N.Lalithamani, K.P.Soman "Irrevocable Cryptographic Key Generation from Cancelable Fingerprint Templates: An Enhanced and Effective Scheme". European Journal of Scientific Research ISSN 1450-216X Vol.31 No.3 (2009), pp.372-387

[6] K. Nallaperumall, A. L. Fred, and S. Padmapriya, "A Novel Technique for Fingerprint Feature Extraction Using Fixed Size Templates", IEEE2005 Conference, pp. 371-374, 2005.

[7] P. Komarinski, P. T. Higgins, and K. M. Higgins, K. Fox Lisa, "Automated Fingerprint Identification Systems (AFIS)", ElsevierAcademic Press, pp. 1-118, 2005.

[8] Y. Seto, "Development of personal authentication systems using fingerprint with smart cards and digital signature technologies," the Seventh International

Conferenceon Control, Automation, Robotics nd Vision, Dec 2002

[9] L.C. Jain, U. Halici, I. Hayashi, S.B. Lee, and S. Tsutsui, “Intelligent biometric techniques in fingerprint and face recognition”, The CRC Press, 1999.

[10] Koblitz.N A course in Number Theory and Cryptography, New York, Springer Verlog, Second Edition, 1994.

[11] L.Lam, S.W.Lee and C.Y.Suen, “Thinning Methodologies – A comprehensive study”, IEEE Transaction on Pattern Analysis and Machine Intelligence, vol. 14,no 9,1992

.