Biometric Parameter Based Cryptographic Key Generation

Rashi Bais, K.K.Mehta

Abstract— A method is proposed for generation of unique cryptographic key which is generated using biometrics 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 biometric data and is not stored in the database, since it creates more complexity to crack or guess the cryptographic keys. We evaluated our technique using 50 different fingerprint samples, and found that an error-free key can be reproduced reliably with a 99.5% success rate. 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.

Index Terms—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 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.

Solution: Biometric Based Cryptography:- Biometrics and cryptography are two potentially complementary security technologies.

Manuscript Received on June 2012

Rashi Bais, Pursuing M.Tech., Department of Computer Science & Engineering, SSCET-Bhilai (C.G.), India.

Dr. K.K. Mehta, Professor & Head, Department of Computer Science & Engineering, SSCET-Bhilai (C.G.), India.

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.

Fingerprint: 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.

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.

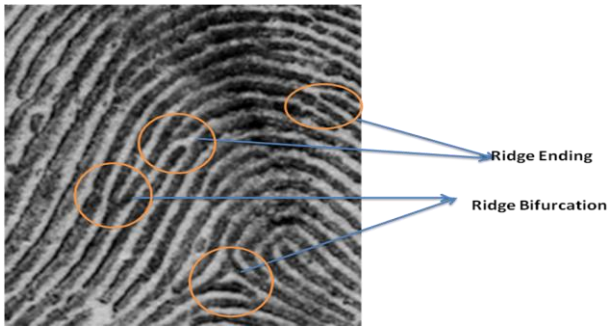


Figure 1: Example of a ridge ending and a bifurcation.

II. CRYPTOGRAPHIC KEY GENERATION FROM FINGERPRINT 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. The various steps required for generating cryptographic key from fingerprint biometric are:-

A. Fingerprint Image Enhancement

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.

Histogram Equalization

Histogram equalization is to expand the pixel value distribution of an image so as to increase the perceptional information. 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.

B. 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.

C. Thinning

The final image enhancement step typically performed prior to minutiae extraction is thinning. 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.

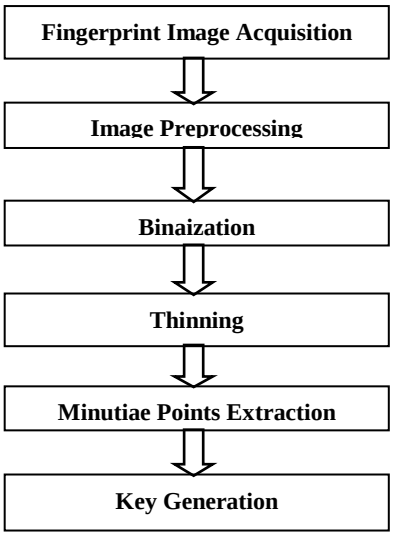


Figure 2: Steps for Key Generation

D. Minutiae Extraction

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.

Table I: Properties of the Crossing Number

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

.

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:

$$CN = 0.5 \sum_{i=1}^{8} |Pi - Pi + 1|, P_9 = P_1$$

where Pi 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:

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)

Figure 3: An Example 3×3 Matrix

- If the central is one-value and has only one one-value as neighbor, then it is an endpoint like in Figure b).
- If the central is one-value and has three one-value as neighbor, then it is an bifurcation like in Figure 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
397	327	1	45
503	537	3	225
698	112	1	90
856	381	3	270

E. Key Generation

The key generation algorithm is as follows:-
key = key vector
k = key vector size
cnAry = Array of crossing Number of extracted Minutiae Point.
minutiae()= minutiae point matrix

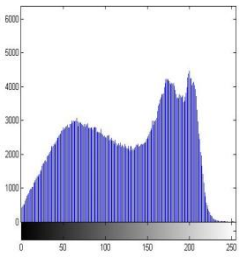
Step1: Read the minutiae points.
cnAry = minutiae(:, 3)
Step2: Set the key size according to the encryption algorithm.
Set k = 64;
Step3: if k > size(cnAry)
k = size(cnAry)
Step4: key = [k];
Step5: for x = 1 to k
if cnAry(x) = 3
then key(x) = 0
else key(x)= cnAry(x)
Step6: key= The final required key vector.

III. EXPERIMENTAL RESULTS

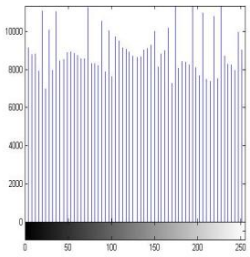
This scheme is programmed in Matlab (Matlab7.6). We have tested the proposed system with diverse fingerprint images. The minutiae points are extracted from the fingerprint images using the approach discussed. A Unique cryptographic key is generated from the biometric template of a user. The following are the experimental results obtained for the proposed approach:-

a)

b)



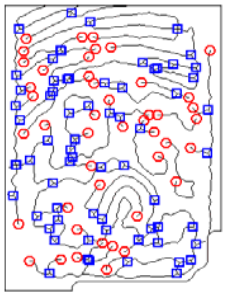
c)



d)

e)

f)



g)

h) Key generated from sample fingerprint
1100000000000011101000001100001000000000001101111101100000110010111001001011110000001110010000010110000011000001000000000101010 0

Figure 4 :a) Image before histogram equalization b)After histogram equalization c)Histogram for original image d)Histogram after histogram equalization e) Binarized image f)Thinned image g)Minutiae Points h)Key generated from sample fingerprint

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. 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.

REFERENCES

1. Umut Uludag, Sharath Pankanti, Salil Prabhakar, Anil K.Jain "Biometric Cryptosystems Issues and Challenges" Proceedings of the IEEE 2004.
2. P.Arul, Dr.A.Shanmugam "Generate a Key for AES Using Biometric For VOIP Network Security" Journal of Theoretical and Applied Information Technology 2009.107-112.
3. Je-Gyeong Jo, Jong-Won Seo, and Hyung-Woo Lee Div Biometric Digital Signature Key Generation and Cryptography Communication Based on Fingerprint. Computer Information of Software, Hanshin University
4. 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
5. Víctor López Lorenzo, Pablo Huerta Pellitero, José Ignacio Martínez Torre, Javier Castillo Villar, "Fingerprint Minutiae Extraction Based On FPGA and MatLab", http://www.escet.urjc.es/~phuerta/pdf/dcis_2005.pdf
6. Jain, A.K.; Prabhakar, S.; Hong, L.; Pankanti, S., "Filterbank-based fingerprint matching",IEEE Transactions on Image Processing, vol. 9, no. 5, pp: 846-859, May 2000, Doi:10.1109/83.841531.
7. Sang Keun Oh, Joon Jae Lee*, Chul Hyun Park, BumSoo Kim, Kil Houm Park School of Electrical Engineering, Kyungpook National University, SEOUL 702-701,Daegu , Korea,"New Fingerprint Image Enhancement Using DirectionalFilterBank" http://wscg.zcu.cz/wscg2003/Papers_2003/J37.pdf
8. A. Goh, D.C.L. Ngo, "Computation of cryptographic keys from face biometrics, "International Federation for Information Processing 2003, Springer-Verlag, LNCS 2828, pp. 1–13, 2003.
9. Y. Seto, "Development of personal authentication systems using fingerprint with smart cards and digital signature technologies," the Seventh International Conferenceon Control, Automation, Robotics and Vision, Dec 2002.

AUTHORS PROFILE

Rashi Bais, obtained her B.E. in Computer Science And Engineering from R.C.E.T. Bhilai, C.G. in 2008. She is an M.E.(C.T.A.) Scholar from S.S.C.E.T. Bhilai, India. Her research area includes Cryptography and Biometric based application development.

Dr. K. K. Mehta , obtained his B.E. (Computers) in 1994 from KITS Ramtek and M.Tech (Computers) from GEC Raipur in 2002. He is Ph.D. in Computers by Technical University of Chhattisgarh State. Presently he is working as Professor & Dept Head at Shri Shankaracharya College of Engineering & Technology Bhilai (C.G.) India. His research area includes Low Power Micro Electronics, Bus Encoding Scheme, Cryptography and Biometric based application development. He is a life member of IEI, ISTE, CSI and VSI INDIA.