Efficient Cryptographic Key Generation Using Fingerprint

Ginu Thomas, K.Rahimunnisa, Sonima Parayil

Abstract— T Biometrics are used for the high secure applications in cryptography. Cryptography is intended to ensure the secret and authenticity of a message. Identity theft can be easily solved by the integration of biometrics and cryptography. To establishing identity biometrics system has been used in various commercial, civilian and for forensic applications. In this paper fingerprint is used as biometric system. Our main aim is to integrate the volatility of the user's biometric features into the generated key and it make unpredictable to the hacker. If a biometric key is missing or stolen ,it is lost completely and possibly for every application where the biometric is utilized ,because a biometric is permanently linked with a user and cannot be altered. In this paper 256-bit secure cryptographic key is generated from the fingerprint biometric feature. The experimental results have showed that the generated 256-bit cryptographic key is capable of providing better security.

Index Terms— Cryptography, Biometrics, fingerprint, Cryptographic key.

1 Introduction

Cryptography is considered as the one of the building block for the security. Data can be encoded and decoded with the help of cryptographic key. It ensures high security and a hacker can't be able to hack the data .DES, AES and public key architectures are widely utilizing cryptographic techniques.

Cryptographic security is conditioned by an authentication step that depends upon the pseudo random keys, which are impossible to keep in mind[1]. The inability of human users to remember powerful cryptography keys helps to ensure the security. Numerous historical instances show that a person is capable of remembering only tiny passwords or keys. Typically write down and store keys in an insecure place can make communal among users, and thus is not capable of non-repudiation. More over many people are intended towards using identical keys and passwords for a variety of applications .This makes the work of an attacker to be very simple and it lead to reduce the security.

Biometric provide a person with distinct characteristics that is always unique[3]. Diverse biometric techniques that are under research include fingerprints, facial, retinal, iris scans and hand geometry, signature capture and vocal features. Biometric technologies have established their importance in a variety of security, access control and monitoring applications.

Humans have used fingerprints for personal identification of many decades and matching accuracy is high for fingerprint.

Ginu Thomas is currently pursuing PG degree in VLSI Design in Karunya University, Coimbatore,Tamil Nadu ,India 641114 .E-mail: ginuvallattu@gmail.com.
K.Rahimunnisa is currently working as an Associate Professor in Karunya University, Coimbatore,Tamil Nadu ,India 641114 .E-mail: krahimunnisa@gmail.com.
Sonima Parayil is currently pursuing PG degree in VLSI Design in Karunya University, Coimbatore,Tamil Nadu ,India 641114 .E-mail: @gmail.com.

A fingerprint is the pattern of ridges and valleys on the surface of the fingertip and the formation of which is determined during the first seven months of fetal development. Fingerprints of identical twins are even different.Most automatic systems for fingerprint are based upon minutiae matching. Minutiae characteristics are local discontinuities in the fingerprint pattern which represent the ridge endings and bifurcations.

A ridge ending is defined as the point where a ridge ends abruptly. A ridge bifurcation is defined as the point where a ridge forks or diverges into branch edges. Reliable automatic extracting of minutiae is a critical step for the fingerprint classification. The ridge structures in fingerprint images are not always well defined, and therefore, an enhancement algorithm, which can improve the clarity of the ridge structures, is necessary for identification[3] . Most of the minutiae detection methods which have been proposed in the literature are based on image binarization, while some others extract the minutiae directly from gray scale images . The proposed method is carried out using local histogram equalization, Wiener filtering, and image binarization.

The organization of the paper is as follows. The proposed methodologies and the steps are related in Section .the experimental analysis and the results are given in Section and conclusions are summed up in Section.

II.PROPOSED METHOD FOR THE KEY GENERATION

Biometric cryptosystems combines both biometrics and cryptography to afford the advantages of both for security purposes . This technique provide the advantages like better security levels for data transmission and eliminating the must to memorize passwords or to carry tokens etc. In this section,

fingerprint and iris features integration for cryptographic key generation is discussed in detail. The steps involved in the proposed approach based on multimodal biometrics for 256 bit cryptographic key generation are[2],

1.Extraction of minutiae points from fingerprint.

2.Cryptographic key generation from fingerprint features.

The basic block diagram is diagrammed in Fig 1.

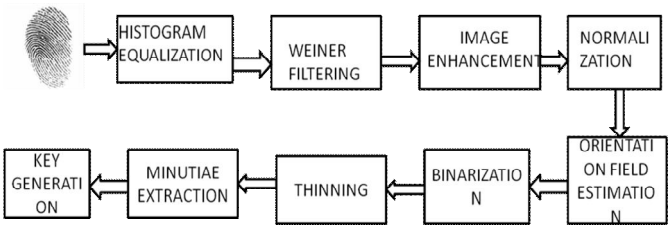


Fig 1.Basic Block Diagram

A.*Fingerprint Feature Extraction*

Fingerprints are the most widely used biometric features due to the easier accessibility,distinctiveness,persistence and and low cost properties[11].The interleaved ridges and valleys are the most evident structural characteristic of a fingerprint.The steps involved in the proposed approach for minutiae extraction are as follows,

1)*Preprocessing :* The fingerprint image is first preprocessed using following methods,

a)Histogram Equalization

b)Wiener Filtering

Histogram Equalization: Histogram equalization is a main technique for adjusting image intensities to enhance the contrasting. Consider an image which represented as a m_r by m_C matrix of integer pixel intensities ranging from 0 to L – 1. L is the number of possible intensity values i.e. 256[12]. Let p_n denote the normalized histogram of given image for each possible intensity. Then

$$p_n = \frac{\text{number of pixels with intensity n}}{\text{total number of pixels}} \qquad n = 0, 1\ldots\ldots L-1 \qquad (1)$$

Wiener Filtering: It increases the legibility of the fingerprint without changing in its ridge structures[2]. The filter is based only on local statistics estimated from a local neighborhood of size 3x3of each pixel, and is given in the following equation:

$$w(n1,n2)=\mu+\frac{\sigma^2-v^2}{\sigma^2}(I(n1,n2)-\mu) \qquad (2)$$

Where v^2 is the noise variance, μ and σ^2 are local mean and variance and I represents the gray level intensity in n1,n2 ϵ η.

2) *Image Enhancement***:** The fingerprint image enhancement is obtained by the Gaussian low pass filter method.

Gaussian Low-Pass Filter: The Gaussian low-pass filter is used as to blurring an image[13]. The Gaussian filter generates a `weighted average' of each pixel's in neighborhood, with, the average weighted more towards the value of the central pixels. The Gaussian filter using the following 2-D distribution as a point-spread function, and is achieved by the convolution .

$$G(x,y)=\left(\frac{1}{2\pi\sigma}\right)^2 \exp\left\{\frac{(x^2+y^2)}{2\sigma^2}\right\} \qquad (3)$$

Where σ is the standard deviation of the distribution.

3) Normalization: Normalization is used to standardize the intensity values in an image by adjusting the range of grey-level values so that it lies within a desired range of values[12]. Let I(i,j) represents the grey-level value at pixel (i, j), and N(i,j) represents the normalized grey-level value at pixel (i, j). The normalized image is defined as:

$$N(i,j)=\begin{cases} M0+\sqrt{\frac{V0(I(i,j)-M)^2}{V}} & \text{If } I(i,j)>M \\ M0-\sqrt{\frac{V0(I(i,j)-M)^2}{V}} & \text{Otherwise} \end{cases} \qquad (4)$$

Where M and V are the estimated mean and variance of I(i; j), respectively, and M0 and V0 are the desired mean and variance values, respectively.

4)Orientation Field Estimation: A fingerprint orientation field is defined as the local orientation of the ridge-valley structures. In the gradient-based methods, gradient vectors $[g_x, g_y]^T$ are first calculated by taking the partial derivatives of each pixel intensity in the Cartesian coordinates[12]. Traditional gradient-based methods divide the input fingerprint image into equal-sized blocks of N X N pixels, and average over each block independently . The direction of orientation field in a block is given by,

$$\theta_B = \frac{1}{2}\tan\left(\frac{\sum_{i=1}^{N}\sum_{j=1}^{N}2g_x(i,j)g_y(i,j)}{\sum_{i=1}^{N}\sum_{j=1}^{N}g_x^2(i,j)-g_y^2(i,j)}\right)+\frac{\pi}{2} \qquad (5)$$

The function a tan(.) gives an angle value in the ranges of $(-\pi,\pi)$ which corresponds to the squared gradients, while θ_B is the desired orientation angle within $[0,\pi]$.

5)Binarization: The fingerprint binarization is an algorithm which producing a 1-bit type image, with 0 as ridges which are tinted with black and 1 as valleys which are tinted with white. However, the binarization method is based on a threshold t, with grey-level pixels lower than t assigned to 0 and the others to 1[3]. It is known that dissimilar fingerprint images have special contrast and intensity, and therefore, a unique threshold t is not proper for a general fingerprint image analysis. The local threshold technique changes t locally, by adapting its value to the average local intensity. In

this paper this method is applied based on determining the mean value of each 32-by-32 input matrix and transferring the pixel value to 1 if it is larger than mean and to 0 if it is smaller. However, in very poor quality fingerprint images, the local threshold method cannot guarantee acceptable results and a special threshold, which has sufficient effect, is required.

6)Thinning: Thinning is the last step of the fingerprint image enhancement before feature extraction, and it is used in order to clarify the endpoints and the bifurcations in each specific pixel, subject to the numbers of pixels belonging to these features in the original fingerprints[3]. Different thinning algorithms and techniques have been developed but they are based on thinning the neighborhood of the pixels that have maximum values in a sequential process obtaining a characteristic pixel value for each feature at each step. In addition, because of false H breaks and lonely points which could appear when using such algorithms the fingerprint images have to be filtered in order to remove them. In this paper an algorithms has been developed, which eliminates the development of such false information in a fingerprint image by using initially a slide neighborhood processing and then thinning the result in only one step without any intermediate filtering and with a substantial reduction of the computational complexity.

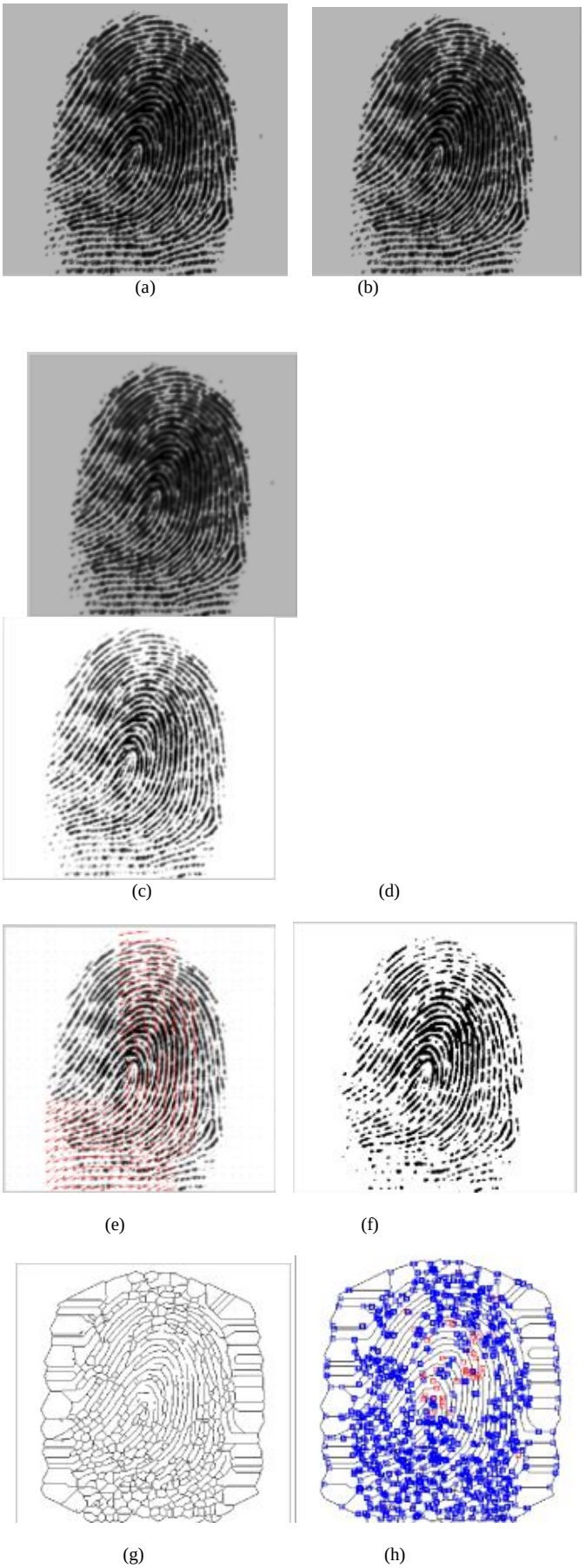
7) Minutiae Extraction: The Crossing Number (CN) method is used to perform minutiae extraction effectively. This method extracts the ridge endings and bifurcations from the skeleton image by examining the local neighborhood of each ridge pixel using a 3X 3 window[12].

III EXPERIMENTAL RESULTS

This section describes our experiments during the evaluation of the proposed method. The proposed approach is implemented in Matlab 7.10.0a.Several samples are used and results are analyzed, the fingerprint images that are used from National Institute of Standards Fingerprint database .The minutiae points are extracted from the fingerprint images using the approach discussed in the paper.

A. *Results and Discussion*

The input fingerprint image, the extracted minutiae points and the intermediate results of the proposed method are shown in figure 2.Several images used to find out the variation of the fingerprint. Finally the generated 256 bit cryptographic key obtained from the proposed approach is depicted in figure 5. The resulted 256 bit key is high randomness key.



(a) (b) (c) (d) (e) (f) (g) (h)

Fig 2. (a)Input Fingerprint image (b) Histogram equalized image (c) Weiner filtered image (d) Normalized image (e) Orientation field estimation image (f)Binary image (g) Thinned image (h) Fingerprint image with minutiae point

IV CONCLUSION

The growing problem for the information security is owing to the gradually rising information on security intrusions. In this paper, presented an approach that generates cryptographic key from fingerprint images in an efficient manner. This paper illustrates a method of securing a cryptographic key of arbitrary length using a given biometric The method is also flexible, the bio-keys used to protect the cryptographic key can be changed and revoked and is a significant feature not possessed by other methods. This method has shown that the improvement in the minutiae detection process in terms of efficiency. For reducing noise, Weiner filtering is applied and finally binarization and thinning is applied over the fingerprint image to get the good resultant image.

ACKNOWLEDGMENT

The authors would like to thank the reviewers for their insightful comments.

REFERENCES

[1] Arun Ross and Anil K. Jain(2004) "Multimodal Biometrics: An Overview", *in proceedings of the 12th European Signal Processing Conference*, pp. 1221-1224.

[2] A. Jagadeesan, K.Duraiswamy (2010) "Secured Cryptographic Key Generation from Multimodal Biometrics: Feature Level Fusion of Fingerprint and Iris", *International Journal of Computer Science and Information Security*, IJCSIS, vol. 7, no. 2, pp. 28-37.

[3] M. Sepasian, W. Balachandran and C. Mares, "Image Enhancement for Fingerprint Minutiae- Based Algorithms Using CLAHE, Standard Deviation Analysis and Sliding Neighborhood", *inProceedings of the World Congress on Engineering and Computer Science 2008*, SanFrancisco, USA, October 2008.

[4] L. Hong, A.K. Jain and S. Pankanti, "Can multibiometrics improve performance?", *in Proceedings of IEEE Workshop on Automatic Identification Advanced Technologies*, pp. 59–64, NJ, USA, 1999 .

[5] Anil Jain, Karthik Nandakumar and Arun Ross, "Score normalization in multimodal biometric systems", *Pattern Recognition*, vol. 38, pp. 2270 –2285, 2005.

[6] Muhammad Khurram Khan and Jiashu Zhang, "Multimodal face and fingerprint biometrics authentication on space-limited tokens", *Neurocomputing*, vol. 71, pp. 3026-3031, August 2008

[7] A.M. Bazen and S.H. Gerez(2002) "Systematic methods for the computation of the directional fields and singular points of fingerprints", *IEEE Transaction on Pattern Analysis and Machine Intelligence*, vol. 24, no.7, pp.905–919.

[8] Feng Hao, Ross Anderson and John Daugman(2006) "Combining Crypto with Biometrics Effectively", *IEEE Transactions on Computers*, vol. 55, no. 9, pp. 1081 – 1088.

[9] Andrew Rukhin, Juan Soto, James Nechvatal,Miles Smid, Elaine Barker, Stefan Leigh, Mark Levenson, Mark Vangel, David Banks, Alan Heckert, James Dray, San Vo"A Statisticel Test Suite For Random And Pseudorandom Number Generators For Cryptographic Applications"*NIST Special Publication* 800-22,May 2001.

[10] Anant P. Godbole and Stavros G. Papastavridis, (ed),(1994) "Runs and patterns in probability": Selected papers. Dordrecht: Kluwer Academic.

[11] Yi Wang , Jiankun Hu and Fengling Han, "Enhanced gradient-based algorithm for the estimation of fingerprint orientation fields", *Applied Mathematics and Computation*, vol. 185, pp.823–833, 2007

[12] Raymond Thai,"Fingerprint Image Enhancement and Minutiae Extraction",*Thesis of fingerprint extraction,University of Western Australia*