Generating Public Key from Fingerprint using Fuzzy Extractor

Mohammed S. Khalil

Abstract—The biometric data is an excellent candidate for authentication and verification secure systems. Whoever, it is not uniformly distributed, nor it be reproduced precisely each time it is processed. This makes biometric data difficult to be used as a password or as a cryptography secret. In this paper, a method is presented to extract fingerprint features and generate a public key using the fuzzy extractor. The public key can be used as a key in a cryptographic application or as authentication or verification system. The experiment shows that %93.13 of success rate indicate the method is excellent to be used to generate the public key from the fingerprint.

Index Terms—Biometric, Fingerprint, Local feature, Security, Fuzzy extractor, and Cryptography.

1 Introduction

Biometric ensures the identification of human being automatically based on the principle of measureable physiological or behavioral characteristics such as fingerprint, an iris pattern, or a voice sample [1]. A significant feature associated with Biometric data is that: it is hard to forge, unique to each person, and excellent source of entropy which makes them an excellent candidate for security applications. However, they have some disadvantage, such as biometric data cannot be subjected to any change, biometric template easy to steal, biometric data are not uniformly distributed and exactly reproducible; they cannot be used directly as password or cryptography secret [2].

When biometric data are used in an application it has to be stored in a database. This data might be used across a network for matching against reference database. Due to this basic step, the biometric system gets exposed to a new security risk such as: constructing false biometrics from stolen biometric template, and stolen biometric data are stolen for life [3]. There have been several researches in the literature addressing this issue [4; 5; 6; 7].

Fingerprint is the oldest biometric-based identification system [8]. It has been used widely by a numerous application, for example forensic test, security, personal identification due to its uniqueness, accessibility, reliability. When a finger is pressed against a smooth surface the fingerprint is produced. The most visual characteristics of a fingerprint are a pattern of ridges and valleys, they run in parallel; sometimes they get terminated and sometimes they are bifurcated.

There are two type of feature for fingerprint recognition: global feature and local feature. Global feature form special pattern of ridge and furrows, which are called singularities or singular point, and the important points are the core and the delta. The core is defined as the most point on the inner most ridges; and a delta is defined as the point where three flows meet [9]. There have been several approaches for singular point detection in the literature [10; 11; 12; 13; 14; 15; 16; 17; 18; 19; 20] and most of them operate on the fingerprint orientation field [10; 11; 12; 13; 14; 15]. The Poincare index (PI) method [9; 19; 21; 22] is one of the commonly used methods to detect singular point. Minutiae are important at the local feature; it carries information about the individuality of the fingerprint. Minutiae, in fingerprint context, are the various ridge discontinuities of a fingerprint. The ANSI [22] classified minutiae to four classes: termination, bifurcations, trifurcations, and undetermined. Consistent extraction of these features is essential for fingerprint recognition. There are many approaches in the literature about locating the local feature [23; 24; 25; 26].

Juels and Wattenberg [27] presented the first fuzzy commitment sachems by combined well-known techniques from the areas of error-correcting codes and cryptography, in which a cryptographic key is de-committed using biometric data. Though this scheme worked well, but it has two major shortcomings; First, it does not allow modifications of the key. Second, the security proof holds if the key is uniformly distributed.

Juels and sudan overcome these drawbacks by proposing a fuzzy vault scheme [28]. The main drawback of this scheme is that if it's used for different application with different vault each times it could reveal the fingerprint minutiae. To overcome the drawback of the fuzzy commitment and the fuzzy vault Yevgeniy et al [29] defined a fuzzy extractor, which will be used in this paper to convert the fingerprint local feature into a public key which can be used by any security application as a cryptographic key. This paper proposes a novel method to extract the fingerprint local feature using the ridge after that converting it to a public key using the fuzzy extractor.

2 Proposed Method

The proposed method contains two components the first one is the fingerprint pre-processing, which include the fingerprint enhancement, reference point detection, extracting the reference point sub-image & orientation normalization, and feature extraction; the second component is the fuzzy extractor which comprises of the generated and the verified. The following describes in detail the modules of the proposed method

2.1 Fingerprint Pre-Processing

This stage is very important for generating the public key. Since the fingerprint is affected by the skin condition, sensor noise, and incorrect pressure produced a low-quality image all of this produce different feature each time. The following Fingerprint Enhancement, Reference Point Detection, Extracting the Reference Point Sub-Image & Orientation, and Feature

Extraction are used for extracting the fingerprint feature as vectors, which are used for the fuzzy extractor input.

2.1.1Fingerprint Enhancment

High superiority clearance of the fingerprint image is very important for fingerprint verification system to function properly. In real life, the quality of the fingerprint image is affected by noise like smudgy area created by over-inked area, breaks in ridges created by under-inked area, changing the positional characteristics of fingerprint features due to skin resilient in nature. Furthermore, dry skin lead to fragmented and low contrast ridges. In addition, wounds may cause ridge discontinuities, and sweat on fingerprints leads to smudge marks and connects parallel ridges. The short time Fourier Transform analysis (STFT) proposed by [30, 31] is applied here for fingerprint image enhancement. Figure 1 shows the original image and the enhanced image.

Figure 1. Shows the original image and enhanced image.

2.1.2 Reference Point Detection

The fingerprint image is made up of shape of ridges and valleys; they are the replica of the human fingertips. The fingerprint image symbolizes a system of oriented texture and has very rich structural information within the image. This flow-like pattern forms the direction field extracted from the style of valleys and ridges. In the large part of fingerprint topologies, the orientation field is quite smooth, while in some areas, it appears in a discontinuous manner. These regions are called singular points, including core and delta, are defined as the centers of those areas. In addition, here the reference point is defined as the point with maximum curvature on the convex ridge. The reliability of the orientation filed describes the consistency of the local orientations in a neighborhood along the dominant orientation is used to locate the unique reference point constantly for all types of fingerprints. The reliability can be also computed using the coherence as proposed by [32]. Figure 2 shows the reference point on the fingerprint image. The implementation is explained on in the following:

1- The orientation image is hardly ever computed at full-resolution. Instead each non-overlapping block of size W × W of the image is assigned a single orientation that corresponds to the most apparent or dominant orientation of the block. In this proposed method, W is set equal to sixteen.
2- The horizontal and vertical gradients Gx(x, y) and Gy(x, y) at each pixel (x,y) respectively are computed using simple gradient operators such as a Sobel mask. The mask is set to 3×3.
3- Compute the ridge orientation of each pixel (x,y) by averaging the squared gradients within a W × W window centered at [xi,yj] as follows:

$$G_{xx} = \sum_{(x,y)\in w} G_x^2(x,y) \quad (1)$$

$$G_{yy} = \sum_{(x,y)\in w} G_y^2(x,y) \quad (2)$$

$$G_{xy} = \sum_{(x,y)\in w} G_x(x,y).G_y(x,y) \quad (3)$$

$$\theta(x,y) = \frac{1}{2}\tan^{-1}\left(\frac{2G_{xy}}{G_{xx}-G_{yy}}\right) \quad (4)$$

4- Because of noise, corrupted ridge, valley structures, and low gray value contrast, a low-pass filter can be used to adjust the erroneous local ridge orientation. However, to perform the low-pass filtering, the orientation image needs to be converted into a continuous vector field as follows:

$$\Phi_x = \cos(2\theta(x,y)), \quad (5)$$

and

$$\Phi_y = \sin(2\theta(x,y)) \quad (6)$$

where Φx and Φy are the x and y components of the vector field, respectively. With the resulting vector field, the Gaussian low-pass filter can be applied as follows:

$$\Phi_x^{'}(x,y) = \sum_{u=-1}^{1}\sum_{v=-1}^{1} w(u,v)\Phi_x(x-uw, y-vw), \quad (7)$$

$$\Phi_y^{'}(x,y) = \sum_{u=-1}^{1}\sum_{v=-1}^{1} w(u,v)\Phi_y(x-uw, y-vw), \quad (8)$$

where W is a two-dimensional low-pass filter with unit integral.

5- Since the singular point has the maximum curvature. It can be located by measuring the strength of the peak using the following:

$$mi = ((G_{yy}+G_{xx}) - (\Phi_x^{'}G_{xx} - G_{yy}) - (\Phi_y^{'}G_{xy})/2, \quad (9)$$

$$mx = G_{yy} + G_{xx} - mi, \quad (10)$$

$$reliability = 1 - \frac{mi}{mx} \quad (11)$$

6- After locating the singular points, the pixel position of the singular points is needed. So the following morphological operations are applied to locate the exact value of x and y:
   a. A region of interest based on the color is selected to threshold the image.
   b. Skeletonization is applied to reduce all ob-

jects on the image without affecting the important structure of the image.

c. Objects with holes shrink to a connected ring.
d. Objects without holes shrink to a point.
e. Isolated pixels are removed.
f. The pixels value of the singular points is indicated by red point.

Figure 2. Reference point

2.1.3 Extracting theRefrence Point Sub-Image & Orientation Normalization

Different acquisition for fingerprint may result in different size or location of fingerprint image. Since the area near the reference point covers correct and efficient information about the fingerprint. Khalil et. al. [32] extracted a sub image of 129 X 129 from the original image making the reference point as the center after that rotating the sub image to zero orientation at the reference point. Figure 3 shows the sub image after the rotation.

Figure 3. Sub image

2.1.4 Feature Extraction

The importance of texture for human visual system provides information for recognition and interpretationused in identifying objects or regions of interest in an image. Texture is a region descriptor that provides a quantifying measure of the property such as smoothness, coarseness and regularity. The three main approaches to describe texture are statistical, structural and spectral. Statistical techniques describe texture by the statistical properties of the grey levels of the points comprising a surface such as smooth coarse grains. In general, these properties are computed from the statistical moments of the intensity histogram or gray level co-occurrence matrix of an image or region. To incorporate this type of information into the texture-analysis process is to consider not only the distribution of intensities, but also the relative positions of pixels in an image. The use of co-occurrence matrix produces this type of information. Structural techniques characterize texture as being composed of simple "texture primitive", that are regularly arranged on a surface according to some rules. These rules limit the number of possible arrangement of the primitives. Spectral techniques are based on properties of the Fourier spectrum and describe the directionality period of the grey levels of a surface by identifying high-energy peaks in the spectrum.

Haralick et al. [33] introduced the Gray-level co-occurrence matrix (GLCM); it is a statistical approach that can describe second-order statistics of a texture image. A GLCM is basically a two-dimensional histogram in which the *(i, j)th* element is the frequency that event i co-occurs with event j. A co-occurrence matrix is specified by the relative frequencies $P(i, j, d, \theta)$ in which two pixels, separated by distance d, occur in a direction specified by angle θ, one with gray level i and the other with gray level j. A co-occurrence matrix is therefore a function of distance r, angle θ and grayscales i and j.

Haralick et al [33]. showed that a fingerprint image can be decomposed into regions with regular textures. Thus, these regular texture regions can represent by using co-occurrence matrices. The co-occurrence matrices utilize angles of 0°, 45°, 90°, and 135° as follows [33]:

$$p(i,j,d,0^\circ) = \#\{((k,l),(m,n)) \in (L_y \times L_x) \times (L_y \times L_x) \mid |k-m=0, |l-n| = d, I(k,l) = i, I(m,n) = j\} \quad (12)$$

$$p(i,j,d,45^\circ) = \#\{((k,l),(m,n)) \in (L_y \times L_x) \times (L_y \times L_x) \mid |k-m=d, l-n=-d \text{ or } (k-m=-d, l-n=d), I(k,l) = i, I(m,n) = j\} \quad (13)$$

$$p(i,j,d,90^\circ) = \#\{((k,l),(m,n)) \in (L_y \times L_x) \times (L_y \times L_x) \mid |k-m=d, l-n=-d \text{ or } (k-m=d, l-n=0), I(k,l) = i, I(m,n) = j\} \quad (14)$$

$$p(i,j,d,135^\circ) = \#\{((k,l),(m,n)) \in (L_y \times L_x) \times (L_y \times L_x) \mid |k-m=d, l-n=d \text{ or } (k-m=-d, l-n=-d), I(k,l) = i, I(m,n) = j\} \quad (15)$$

where # denotes the number of elements in the set, L_x is the horizontal spatial domain, and L_y is the vertical spatial domain.

A single GLCM might not be enough to describe the textural features of an input fingerprint. For example, a single horizontal spatial relationship might not be sensitive to texture with a vertical orientation. For this reason, multiple GLCMs are computed for values of θ at 0°, 45°, 90°, and 135°. And the relative distance is one pixel. Based on each computed GLCM, four features that can successfully characterize the statistical behavior of a co-occurrence matrix are extracted. They are as follows [32]:

$$i) \textit{Correlation} \sum_{i=1}^{k}\sum_{j=1}^{k} \frac{(i-m_r)(j-m_c)P_{ij}}{\sigma_r \sigma_c} \quad (16)$$

$$ii) \textit{Contrast} \sum_{i=1}^{k}\sum_{j=1}^{k} (i-j)^2 P_{ij} \quad (17)$$

$$iii) \textit{Energy} \sum_{i=1}^{k}\sum_{j=1}^{k} P_{ij}^2 \quad (18)$$

$$iv)\ Homogeneity \sum_{i=1}^{k}\sum_{j=1}^{k}\frac{P_{ij}}{1+|i-j|} \quad (19)$$

Where m_r, $m_c$are means and σ_r, $\sigma_c$are the standard deviations computed along the rows and columns respectively, and $P_{ij}$is the number of times that pixel occurred

2.2 Fuzzy Extractor

All tables and figures will be processed as images. You need to embed the images in the paper itself. Please don't send the images as separate files.

Yevgeniy et al [29] defined a Fuzzy Extractor, which extracts uniform string R from its input W′ the string R can be reproduced as long as the input remains reasonably close to the original. The fuzzy extractor output a non secret string p to assist in reproducing R from W'.

Yevgeniy et al [29] introduced two primitives called a Secure Sketch which allows recovery of a shared secret given a close approximation thereof, and a fuzzy Extractor which extracts a uniformly distributed string R from this shared secret in an error-tolerant manner.

During the enrolment of an error prone, none uniformly distributed input; the Secure Sketch generates some public information related to the input called a 'Sketch' which by itself cannot be used to recover the input. The Fuzzy Extractor is used to map the non-uniform input to a uniformly distributed string. The seed for the Fuzzy Extractor along with the Sketch will be stored publicly. When a query needs to be matched to the input, the Fuzzy Extractor uses the public Sketch of the input along with the query to reconstruct the input exactly. The Fuzzy Extractor's reconstruction procedure will be designed such that if the query is within a specified distance from the input, the reconstruction succeeds. The reconstructed input will then be mapped to the same string using the same seed stored along with the Sketch.

The public storage of the Sketch and the seed do not substantially compromise the security of the input as they cannot be used to recover the input without a query which is 'close' to the input.

3 Experimental Result

The experiment pre-processing method was prepared in MATLAB R2012b version 8.0 and run in Toshiba Intel core i5 CPU 2.50. For syndrome computation and syndrome decoding of BCH codes, the public domain written by Kevin Harmon and Leonid Reyzin [34] is used. For performing finite field computation Victor Shoup's [35] NTL library is used. The FVC2002 1a public fingerprint database is used in this experiment. It comprised of 800 fingerprints from 100 different fingers with eight images from each finger captured using low-cost capacitive sensor, which made it contains many poor-quality images. Each image is processed, and the public key is generated. Each impression is compared with the other seven fingerprint futures. The result of the comparison is outstanding only 6.87% false match due to poor-quality images in the database

4 Conclusion

In conclusion, this paper proposed an excellent method to extractthe fingerprint features using the reference point, after that a sub image selected, which has the fingerprint future. The texture of the sub image is used to extract the fingerprint futureand converts it to a public key which can be used as a key in a cryptographic application. Since the fingerprint images used in the experiment, an enhancement for the images is required. The experiment result shows that the success rate is %93.13, and the false match is only %6.87 false match, and this is due to low quality images. However, in the future a live fingerprint scanner will be used to test the method.

```
1 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1
 0 1 1 1 0 1 0 0 1 0 1 0 1 0 0 0 1 0 0 1
 1 1 1 0 1 1 0 1 0 1 1 1 1 1 0 0 0 0 1 1
   1 1 0 1 0 0 0 0 1 0 1 0 1 0 0 0 0 0 1
   0 1 1 1 1 0 0 0 1 0 0 1 0 0 0 0 0 0 1
  1 1 1 1 1 1 0 0 0 1 0 0 0 1 1 1 0 0 1
  1 0 1 1 1 1 1 0 0 1 1 0 1 1 1 1 0 1 1
 1 1 0 0 0 0 0 1 0 0 1 1 1 0 1 0 0 0 0 1
     0 0 1 0 0 1 0 1 1 1 0 1 0 0 0 1
```

Figure 4. Public key

Acknowledgment

The authors wish to thank Mr. FajriKurniawan for helping formatting this paper.

References

[1] Colin Soutar, Danny Roberge, Alex Stoianov, Rene Gilroy, and B.V.K. Vijaya Kumar. Biometric Encryption. [book auth.] Randall K. Nichols. *ICSA Guide to Cryptography*. s.l. : McGraw-Hill, 1999, 22.W.-K. Chen, *Linear Networks and Systems.* Belmont, Calif.: Wadsworth, pp. 123-135, 1993. (Book style)

[2] Feng Hao, Ross Anderson, & John Daugman. *Combining Cryptography with Biometrics Effectively*. University of Cambridge, UK. 2005. Technical Report No. 640.K. Elissa, "An Overview of Decision Theory,"unpublished. (Unplublished manuscript)

[3] Valérie Viet Triem Tong, HervéSibert, JérémyLecoeur, and Marc Girault. Biometric Fuzzy Extractors Made Practical: A Proposal Based on FingerCodes. *Springer-Verlag Berlin Heidelberg*. Advances in Biometrics, 2007, Vol. LNCS 4642, pp. 604-613.

[4] PimTuyls& Jasper Goseling. Capacity and Examples of Template-Protecting Biometric Authentication Systems. Biometric Authentication Workshop, Prague, May 15 2004.

[5] . BWG. Biometric Security Concerns. November, 2003, Vol. 1.0.

[6] Vaclav Matyas, and ZdenekRiha. Biometric Authentication Security And Usability. *IFIP Conference Proceedings;Advanced Communications and Multimedia Security.* 2002, pp. 227-239.

[7] Ann Cavoukian, and Alex Stoianov. Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy. *Information and Privacy Commissioner/Ontario.* 2007.

[8] D. Maltoni, D. Maio, A.K. Jain, And S. Prabhakar. Hand-

book of Fingerprint Recognition. *Springer, New York.* 2003.

[9] QinzhiZhanga and HongYan. Fingerprint classification based on extraction and analysis of singularities and pseudo ridges. *Pattern Recognition.* 2004, Vol. 37, pp. 2233 – 2243.

[10] Wai Mun Koo and Alex Kot . Curvature-Based Singular Points Detection. *Audio- and Video-Based Biometric Person Authentication.* Lecture Notes In Computer Science; Vol. 2091, 2001, pp. 229 - 234.

[11] Arun, Vinodh C. Extracting and Enhancing the Core Area in Fingerprint Images. *IJCSNS International Journal of Computer Science and Network Security.* November 2007, Vol. 7, 11.

[12] Lin Hong and Anil Jain. Classification of Fingerprint Images. *11th Scandinavian Conference on Image Analysis.* Kangerlussuaq, Greenland, 1999.

[13] Kenneth Nilsson and Josef Bigun. Complex Filters Applied to Fingerprint Images Detecting Prominent Symmetry Points Used for Alignment. *Biometric Authentication, LNCS 2359.* Springer-Verlag Berlin Heidelberg 2002, pp. 39-47.

[14] Anil K. Jain, SalilPrabhakar, Lin Hong, and SharathPankanti. Filterbank-Based Fingerprint Matching. *IEEE TRANSACTIONS ON IMAGE PROCESSING.* MAY 2000, Vol. 9, No. 5.

[15] Sen Wang, Wei Wei Zhang, and Yang Sheng Wang. Fingerprint Classification by Directional Fields. *Proceedings of the Fourth IEEE International Conference on Multimodal Interfaces (ICMI'02).* 2002.

[16] Manhua Liu, Xudong Jiang, and Alex ChichungKot. Fingerprint Reference-Point Detection. *EURASIP Journal on Applied Signal Processing.* 2005, 4, pp. 498-509.

[17] SharatChikkerur and NaliniRatha. Impact of singular point detection on fingerprint matching performance. *Fourth IEEE Workshop on Automatic Identification Advanced Technologies.* 2005, pp. 207-212.

[18] Mohammad Reza Rahimi, Ehsan Pakbaznia, and ShohrehKasaei. An Adaptive Approach to Singular Point Detection in Fingerprint Images. *International Journal of Electronics and Communications.* 2004, 58, pp. 367-370.

[19] Mohammed S. Khalil "*Reference Point Detection for Camera-based Fingerprint Image based on Wavelet Transformation*",BioMedical Engineering Online, 2015, Online

[20] Lin Wang, and Mo Dai. An effective method for extracting singular points in fingerprint images. *AEU - International Journal of Electronics and Communications.* 2006, Vol. 60, 9, pp. 671-676.

[21] Anil Jain and SharathPankanti. Fingerprint Classification and Matching. *Handbook for Image and Video Processing. Academic Press.* April 2000, 59.

[22] ANSI. Fingerprint Identification-Data Format for Information Interchange. *International Standards Institute.* New York, 1986.

[23] Tsai-Yang Jea, and VenuGovindaraju. A minutia-based partial fingerprint recognition system. *Pattern Recognition.* October 2005, Vol. 38, 10, pp. 1672-1684.

[24] Prabhakar, Salil. Fingerprint Classification and Matching Using a Filterbank. *PhD thesis.* 2001.

[25] Xifeng Tong, Songbo Liu, Jianhua Huang and Xianglong Tang. Local relative location error descriptor-based fingerprint minutiae matching. *Pattern Recognition Letters.* February 2008, Vols. Pattern Recognition Letters, Volume 29, Issue 3, 1 February 2008, Pages 286-294, Pattern Recognition Letters, Volume 29, Issue 3, 1 February 2008, Pages 286-294, pp. 286-294.

[26] Duoqian Miao, Qingshi Tang and Wenjie Fu. Fingerprint minutiae extraction based on principal curves. *Pattern Recognition Letters.* December 2007, Vol. 28, 16, pp. 2184-2189.

[27] Ari Juels and Martin Wattenberg. A fuzzy commitment scheme. *Proceedings of the 6th ACM conference on Computer and communications security*. 1999, pp. 28-36.

[28] Ari Juels and Madhu Sudan. A Fuzzy Vault Scheme. *Proceedings of the IEEE International Symposium on Information Theory.* 2002.

[29] YevgeniyDodis, RafailOsrovsky, Leonid Reyzin, & Adam Smith. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. IACR ePrint report 2003/235., 2006, pp. 523-540. Preliminary version in proceedings of "Advances in Cryptology -- Eurocrypt 2004".

[30] Chikkerur, S.S., Online Fingerprint Verification System, in Department of Electrical Engineering. 2005, State University of New York: Buffalo.

[31] Chikkerur, S., A.N. Cartwright, and V. Govindaraju, Fingerprint Enhancement using STFT Analysis, in Pattern Recognition. 2007. p. 198–211.

[32] . Mohammed S. Khalil, Dzulkifli Muhammad, Muhammad Khurram Khan, Qais AL-Nuzaili, "Fingerprint Verification using Statistical Descriptors". *Digital Signal Processing*, Vol. 20, No. 2010, pp. 1264-1273.

[33] Haralick, R.M., K. Shanmugam, and I.h. Dinstein, *Textural Features for Image Classification*, in *IEEE Transactions on Systems, Man and Cybernetics*. 1973. p. 610-621.

[34] Kevin Harmon, Soren Johnson, and Leonid Reyzin. An implementation of syndrome encoding and decoding for binary BCH codes, secure sketches and fuzzy extractor. *Available at.* http://www.cs.bu.edu/~reyzin/code/fuzzy.html.

[35] Shoup, Victor. NTL: A Library for doing Number Theory (version 5.4.2). *Available from http://shoup.net/ntl/*

- *Mohammed S. Khalil is currently working as assistant professor at the Center of Excellence in Information Assurance, King Saud Univetsity, Saudi Arabia. E-mail: sayimkhalil@gmail.com*