ISSN: 0974-5823 Vol. 7 No. 1 January, 2022

International Journal of Mechanical Engineering

Cryptographic Key Generation from Fingerprint Image Based on Minutiae Neighborhood Information

Mithak Ibrahim Hashem[1]
Department of Software
College of Information
University of Babylon, IRAQ

kadhim alibraheemi[2]
Department of Computer Science
Technology College of Education for Pure Sciences
University of Thi Qar, IRAQ

Abstract – Biometrics likes fingerprint plays a very important role nowadays in many applications such as user authentication. Biometrics technology offers a more practical and trustworthy 'who you are' method. In order to identify someone, they must be physically present. It is the arithmetical analysis of biological events such as physical and behavioral features. Physiological characteristics include fingerprint, hand geometry, iris, face, palm print, and ear. Handwriting, signatures, voiceprints, and keyboard patterns are examples of behavioral traits. We proposed an approach to generate cryptographic key based on biometric features which exists in individual fingerprint. Our research extract features based on two factors: one is the fingerprint traditional minutiae points' information and the other one is the topological information. Chain code representation based method was applied to derive the topological information of minutiae pixels. Adding topological information to the feature extraction methodology increase the accuracy and then the reliability of the cryptographic key generated.

Index Terms – Key Generation, Cryptosystems, Fingerprint Minutiae, Chain Code Representation, Topological Information.

INTRODUCTION

Most security apps use knowledge or tokens to protect data. Identity is verified via a PIN or password. Using a token-based app checks a key or a card. Both of these security methods have major weaknesses. Forgotten or guessed knowledge such as passwords and PINs may be obtained through social engineering [1] or dictionary assaults [2]. Keys and cards may also be lost or stolen.

Biometrics technology offers a more practical and trustworthy 'who you are' method. In order to identify someone, they must be physically present. It is the arithmetical analysis of biological events such as physical and behavioral features [3]. Physiological characteristics include fingerprint, hand geometry, iris, face, palm print, and ear. Handwriting, signatures, voiceprints, and keyboard patterns are examples of behavioral traits. These are the three major biometric traits:

- Universality: Everyone has biometric traits.
- Uniqueness: It is individual.
- Performance stability: Its characteristics are steady over time.

In addition, four variables should be considered while evaluating and comparing biometric features:

- Collectability: Ease of measurement acquisition
- Performance: Accuracy, speed, and robustness of verification.
- Acceptability: Acceptance of a technology.

Circumvention: Ease of substituting.

LITERATURE REVIEW

Key management is needed in conventional cryptography to keep keys secret. Unauthorized access to cryptographic keys may be controlled using user biometrics. The secret is concealed in a cryptographic construct using biometric features of the actual user. When the key is needed, another sample of the authentic user's biometric characteristics is provided, and the cryptographic construct is released. Crypto-biometric methods generate cryptographic keys directly from biometric characteristics. Several works in the literature use biometric or cancelable biometric to produce cryptographic keys. In order to protect the privacy of biometric characteristics, cancelable biometrics is extremely helpful. Numerous researchers suggest the following methods.

Gaddam and Lal [4] proposed generating cryptographic keys using fingerprint templates. The technique generates an intermediate key from the minutiae points and converts it to a matrix. The Secure Feature Matrix (SFM) is created using the AES key matrix. Finally, the SFM generates the key. The SFM is secure since it is produced using the AES algorithm, but the fuzziness characteristic of biometrics makes it impossible to regenerate the same intermediate key for decryption.

Jagadeesan et al. [5] suggested using multi-modal biometrics, including iris and fingerprint. They used feature equal fusion of minutiae themes and iris texture characteristics to create multi-modal biometric patterns. Similar biometrics (fingerprint and iris) but different methods were employed in the second article [6]. Exponentiation uses iris value of texture as base numbers and minutiae

synchronizes as exponents. For respective involution outcome, a multi-modal prototype is created by multiplying two resulting prime numbers. A cryptographic key (256 bits) is created using the method in [5]. S. Dutta et al. described fingerprint-based cryptography [7]. The sender and receiver's fingerprints are used to create a cryptographic key (128 bits). The technique uses the sender and receiver's fingerprints to create a 128-bit cryptographic key. Their technique generates key at sender and sends it to recipient with encrypted message. As a consequence, each communication party's fingerprint privacy is revealed. The issue with these methods is that they cannot create revocable keys. Key generation methods generate helper data directly from the biometric template. Keys are generated from the helper data, as in key binding schemes. Key generating methods include fuzzy extractor and secure sketch schemes like [8, 9, 10, 11, 12, and 13]

PROPOSED METHODOLOY

We propose a new method to generate cryptographic key based on fingerprint biometric features. This methodology is done by the following general steps:

1. Image Enhancement

The noise is influenced during the acquisition of fingerprint image. The poor quality images are captured and leads to inaccurate levels of gray level values.

Image Normalization determines the new intensity value for each pixel in an image. It is a pixel-wise operation, which does not change the clarity of ridges and valleys. The main purpose of this method is to reduce the variation of grayscale values along the ridge and valley.

$$N(i,j) = \begin{cases} M_0 + \sqrt{\frac{V_0 (I(i,j)-M)^2}{V}} & \text{if } I(i,j) > M \\ M_0 - \sqrt{\frac{V_0 (I(i,j)-M)^2}{V}} & \text{otherwise} \end{cases}$$

Where

$$M = \frac{1}{w \times h} \sum_{i=0}^{w-1} \sum_{i=0}^{h-1} I(i,j)$$

$$V = \frac{1}{w \times h} \sum_{i=0}^{w-1} \sum_{j=0}^{h-1} (I(i,j) - M)^2$$

M and V are the mean and variance of the fingerprint image I (i, j), M_o and V_o are the desired mean and variance values.

2. Image Binarization

is the process of converting a pixel image to a binary image. It reducing the information contained within the image from 256 level in case of gray image to two; black and white. The enhanced image can be converted into a binary image by dividing the image into (W×W) non overlap blocks and calculating the mean for each block using equation:

Block Mean = $\frac{1}{W*W} \sum_{i=0}^{W-1} \sum_{j=0}^{W-1} I(i,j)$

Then each pixel in binary image becomes:

Binary image (i, j) =255 if enhanced image pixel (i, j) ≥ block mean,

Binary image (i, j) =0 if enhanced image pixel (i, j) < block mean.

3. *Image Thinning*

Thinning plays a very important role in the preprocessing step of fingerprint recognition/identification systems. A good fingerprint thinning algorithm can depress image noise and promote the robustness of the minutiae extraction algorithm which helps improve the overall performance of the system. The ridges in binary image are thinned to one pixel wide by examining the eight neighborhoods of each pixel in the binary image and deciding if the pixel can be thinned or not until one pixel wide. Thinning is a process of extracting a skeleton from an object in a digital image. The ridges in binary image are thinned to one pixel wide by examining the eight neighborhoods of each pixel in the binary image and determining if the pixel can be thinned or not until one pixel wide.

Figure1: Fingerprint Image Thinning

4. *Proposed Feature Extraction Method*

We propose new method to extract the fingerprint

minutiae with high accuracy by three steps:

1. Feature extraction by four types of minutia (Ridge Ending, Spur, Bifurcation and Lake) instead of the common extraction methods based on only ridge ending and bifurcation minutiae.

2. Using another topological information (neighbor information) by splitting each fingerprint image into sub-images according to the topological information to enhance the feature extraction method.

3. Using Chain Code (FCC) and Run Length Encoding (RLE) to emulate the Feature Shapes among sub-image of step 2 to increase accuracy and reliability of feature extraction method.

Minutiae Detection

Minutiae are local discontinuities in the fingerprint pattern .It is represented by the intersection in the ridges. The most common two types are Ridge End and Bifurcation. We add Spur and Lake to our method of feature extraction..

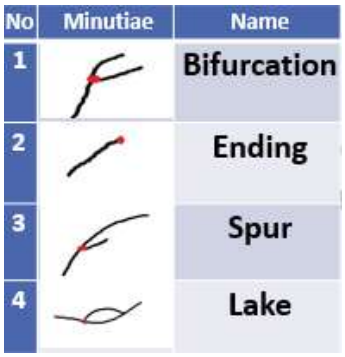

Figure 2: Fingerprint Minutiae Types

THE EXTRACTION OF TOPOLOGICAL INFORMATION ALGORITHM

THIS ALGORITHM IS PROPOSED BY [15]:

INPUT: BINARY ENHANCED THINNING FINGERPRINT SUB-IMAGES

OUTPUT: VECTORS OF THE TOPOLOGICAL NEIGHBORS

BEGIN

FOR EACH MINUTIAE IN SUB-IMAGE

WHILE THE VALUE OF THE RADIUS IS IN A DETERMINED VALUE

WHILE THE ANGLE VALUE IN THE INTERVAL [0,360]

x = x c + r * Cos (angle)

y = x c + r * Sin (angle)

Save (x, y, r, angle) in a vector

End While

End While

End For

End algorithm

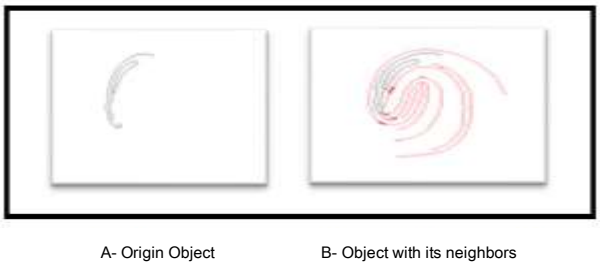

Figure 4: Minutiae Object with neighbors

CHAIN CODE REPRESENTATION

- The first technique to represent the shape of an image is the Freeman Chain Code (FCC). It was initiated by Freeman in 1961. Chain code uses straight-line segments with a particular length and direction that are sequentially linked to represent the boundary of the object in an image. There are two types of chain code representations which are 4 or 8 connectivity. A numbering model can be used to encode each segment's direction. Figure below demonstrates the 4-connected Freeman Chain Code and the 8-directional Freeman Chain Code.

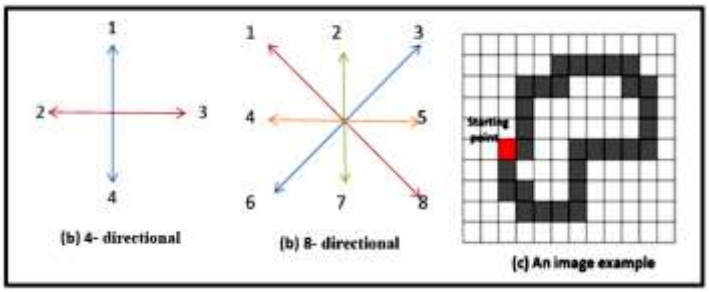

Figure 5: Chain Code Representation

There are 8 possible directions from one pixel to a neighbor pixel in the Freeman Chain Code 8-connected (FCCE). The angle between any two codes is 45^0. The chain code can be calculated either clockwise or counter-clockwise. The chain code representation of an object in figure can be extracted as follow:

1. 4-connectivety: (3,1,1,1,3,3,1,3,3,3,3,4,3,4,4,4,2,2,2,2,4,4,4,2,2,2,1,2,1)

2. 8-connectivety(clockwise): (5,2,2,2,5,5,2,5,5,5,5,7,5,7,7,7,4,4,4,4,7,7,7,4,4,4,2,4,2)

3. 8-connectivety (counter-clockwise): (7,7,5,7,555,2,2,2,5,5,5,5,2,2,2,2,4,2,4,4,4,4,7,4,4,7,7,7,)

In our proposed system, the 8- connectivity chain code will be used for representing the object shape of each feature that extracted from image.

IMAGES SPLITTING

According to the types of minutiae object that are extracted in the previous step, the binary enhanced fingerprint image is split into four images based on minutiae objects as shown in the figure below [15]:

Figure 4: Image splitting to sub-images based on minutiae objects

KEY GENERATION

We propose a method to generate the encryption key. After feature extraction by the previous proposed technique, the information of the extracted minutiae points from fingerprint binary image are recorded, then we can get the fingerprint minutiae set: M = {i = (xi,yi,ti) | i = 1, 2, . . . ,N},

where N is the total minutia number, xi is X-coordinate, yi is Y-coordinate and ti = 0, 1, 2, 3 is the minutia type representing Ending, Bifurcation, Spur or Lake point, respectively.

KEY GENERATION ALGORITHM

Notation:

- RE: is a feature array for Ridge Endings minutiae Points.
- RB: is a feature array for Ridge Bifurcations minutiae Points.
- SP: is a feature array for Spur minutiae Points.
- LK: is a feature array for Lake minutiae Points.
- MA = RE + RB + SP + LK.
- L: is the length of the MA array (the total features array).

Input: MA and L arrays.

Outputs: Cryptographic Key of 256-bit.

(1) A[X] = (X1,X2,…..,XL) ; X coordinates of MA array.

(2) A[Y] = (Y1,Y2,…..,YL) ; Y coordinates of MA array.

(3) A[T] = (T1,T2,……,TL) ; Minutiae Type array.

(3) Calculate:

a. AVGX = $\frac{1}{L}\sum_{i=1}^{L} Xi$; $Average\ of\ X\ coordinates.$

b. AVGY = $\frac{1}{L}\sum_{i=1}^{L} Yi$; $Average\ of\ Y\ coordinates.$

(4) For i=1 to L

$$Z[Xi] = \begin{cases} 1 & if\ A[Xi] \geq AVGX \\ 0 & otherwise \end{cases}$$

$$Z[Yi] = \begin{cases} 1 & if\ A[Yi] \geq AVGY \\ 0 & otherwise \end{cases}$$

End For

(5) Merge the Array Z[X] , Z[Y] and A[T] then store the values in new Array Z such that:

For i=1 to L

Z[i] = Concatenate (Z[Xi] And Z[Yi] And A[Ti])

End for

(6) Generate the 256-bits Cryptographic Key according to Z array in binary code as the example key below:

Key =
(10101100111001101100010010101000100111100010101001010101000101111001001000101010100010101000101010010100100100100100100101010101010101010101010101000010001111110010101001000100010011001000011001101010101010100010101111100000111000101010011111000010100011 0)

1. Applications

APPLICATION

We proposed a technique to generate random cryptographic key of 256-bit size. This type of secret keys can be used in many applications such as Biometric based smart cards applications, digital wallets, digital identity, and data encryption such as symmetric cryptography systems, access control to digital rights and many other applications.

CONCLUSION

The experiments on the fingerprint images using Visual Studio 2012 on Windows 10 (64 bit) system shows that the using of addition information (the neighborhood information) in the feature extraction process make the generated key reliable and more accurate. The neighborhood information based on chain code representation which added to minutiae pixels will facilitate the matching process of each minutiae object based on shape similarity of that minutiae object within the fingerprint image.

REFERENCES

[1] K. D. Mitnick andW. L. Simon. "The Art of Deception: Controlling the Human Element of Security". John Wiley & Sons, Inc., New York, NY, USA, 2003. ISBN 076454280X.

[2] D. V. Klein. "foiling the cracker": A survey of, and improvements to, password security, 1990.

[3] A. K. Jain and D. Maltoni. "Handbook of Fingerprint Recognition". Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2003. ISBN 0387954317.

[4] Sunil V. K. Gaddam and M. Lal, "Efficient Cancellable Biometric Key Generation Scheme for Cryptography", International Journal of Network Security'vol.11, no.2, pp.57-65, sep.2010.

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

[6] A. Jagadeesan, T. Thillaikkarasi, K. Duraiswamy, "Cryptographic Key Generation from Multiple Biometrics Modalities: Fusing Minutiae with Iris Feature", International Journal of Computer Applications vol.2, no.6, June 2010.

[7] S. Dutta, A. Kar, B. N. Chatterji and N.C.Mahanti, "Network Security Using Biometric And Cryptography", Lecture Notes in Computer, Springer, 2008. ISBN: 978-3-540-88457-6: 38-44.

[8] X. Boyen, "Reusable cryptographic fuzzy extractors", in Proceedings of the 11th ACM Conference on Computer and Communications Security, ser. CCS '04. New York, NY, USA: ACM, 2004, pp. 82-91.

[9] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data", SIAM J. Comput., vol. 38, no. 1, pp. 97-139, Mar. 2008.

[10] Q. Li, Y. Sutcu, and N. Memon, "Secure sketch for biometric templates", in Proceedings of the 12th International Conference on Theory and Application of Cryptology and Information Security, ser. ASIACRYPT'06. Berlin, Heidelberg: Springer-Verlag, 2006, pp. 99-113.

[11] Saleem, Huda & Albermany, Salah & Hadi, Husien.. "Proposed Method to Generated Strong Keys by Fuzzy Extractor and Biometric". 7. 129-131. 10.14419/ijet.v7i3.27.17672. (2018).

[12] Wang, Y.; Li, B.; Zhang, Y.; Wu, J.; Ma, Q. "A Secure Biometric Key Generation Mechanism via Deep Learning and Its Application". Appl. Sci. 2021, 11, 8497. https://doi.org/ 10.3390/app11188497.

[13] Kaur, T., & Kaur, M. "Cryptographic key generation from multimodal template using fuzzy extractor". 2017 Tenth International Conference on Contemporary Computing.

[14] Dr. Azzam Talal Sleit, Rahmeh Omar Jabay, "A Chain Code Approach for Recognizing Basic Shapes", Conference: CSIT – Proceedings of the 4th International Multiconference on Computer Science and Information Technology - CSIT, Volume: 2, pp. 298-302, 2006.

[15] Tawfiq A. Al-Asadi, Diyar M. Witefee, "Object Matching Based Topological Neighbors in Fingerprint Image", International Journal of Advance Science and Technology, Vol. 29, No. 10S, (2020), pp. 8367-8377.