ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.4, Pages : 61-65 (2014)
Special Issue of ICCEIT 2014 - Held on September 01, 2014 in The Solitaire Hotel, Bangalore, India

Enhancing Security With Fingerprint Combination Using RSA Algorithm

Safnitha P Y
Department Of Computer Science and Engineering
KMEA College Of Engineering
Aluva
safnithayusef@gmail.com

Sheena Kurian K
Department Of Computer Science and Engineering
KMEA College Of Engineering
Aluva
sheenakuriankcs@kmeacollege.ac.in

***Abstract*— Fingerprint recognition is an active research area nowadays. In many areas we are using fingerprint recognition to improve the security and privacy. In fingerprint recognition system the recognition can be done by fingerprint matching techniques. Fingerprint matching techniques are classified in two categories namely:- fingerprint verification and fingerprint identification. In this system we are using the fingerprint verification. For this we propose here a novel system for protecting fingerprint privacy by combining two different fingerprints into a new identity. In the enrollment, two fingerprints are captured from two different fingers. We extract the minutiae positions from one fingerprint, the orientation from the other fingerprint, and the reference points from both fingerprints. Based on this extracted information combined minutiae template is generated and stored. The combined minutiae template is used to generate key using RSA algorithm. In the authentication, the system requires two query fingerprints from the same two fingers which are used in the enrollment. A two-stage fingerprint matching process is proposed for matching the two query fingerprints against a combined minutiae template. A new virtual identity is created for the two different fingerprints, which can be matched using minutiae-based fingerprint matching algorithms. Authentication is granted the user can able to decrypt the message send by a external source. Thus the system provide a high level of security.**
Key Words — Fingerprint, Orientation, Minutiae, Reference Points, RSA, Enrollment, Authentication.

INTRODUCTION

Our modern era faces an inevitable problem in securing our most integrated data and messages. The main problem is to protect our data in a unique way that could only be worked upon by the sender and the recipient. As the Internet and other forms of electronic communication becomes more prevalent, electronic security is becoming increasingly important. Cryptography is mainly, to protect e-mail messages, credit card information, and corporate data.

Traditional techniques that are probably in-use today, emphasizes on keys that are generated by generic function, algorithms or in random key generators. But the query is whether this key is unique and authentic in nature. More than how can these keys be unique to one and one person only? The answer to this would be Biometric Cryptosystems.

The newest members of the field of security is biometric cryptosystems. The important basis of this biometric cryptosystem depends on the fact that special features of human body are significantly unique to each and every human in the world, such as fingerprint, DNA sequence, Iris, etc. Based on those biometric we are able to generate an exclusive key that will be unique for each and every individual. Now using these generated keys we can encrypt our message without any afraid of attacks. Chance of there will be a matching keys also less because these keys are uniquely generated for individual persons.

As we use RSA algorithm based encryption technique, the encryption lies on two basic sets of keys to decrypt the message. Hence, eavesdropper or third unwanted parties have to acquire two set of keys which adds up to security level of the encryption and hence protect the message from unwanted third parties from acquiring our secret message [2].

In this paper we discussing a secure approach for the privacy protection of the biometric feature fingerprint in authentication system. Fingerprint recognition is an active research area. In many areas we are using fingerprint recognition to improve the security and privacy. In fingerprint recognition system the recognition can be done by fingerprint matching techniques. Fingerprint matching techniques are classified in two categories namely:- fingerprint verification and fingerprint identification. In this system we use fingerprint verification.

Moreover fingerprint techniques have widespread applications in this era. In ancient days fingerprint matching was used extremely for forensic purposes and it performed manually by the human experts. Privacy Protection of fingerprint in authentication system is an important issue. Traditional encryption involves decryption and it required before the fingerprint matching so it is not sufficient for fingerprint privacy protection because which exposes the fingerprint to the attacker [1]. Therefore, in recent years, significant efforts have been put into developing specific protection techniques for fingerprint.

Most of the previous techniques make use of the key for the fingerprint privacy protection, which creates inconvenience. They may also be vulnerable when both the key and the protected fingerprint are stolen.

In this system we use an idea of combining two fingerprints from two different fingers and generate a combination and stored in a database. This will be a virtual identity. Then apply conventional RSA method to the virtual identity to generate PKI keys. Using these keys store the information in a database. In authentication phase access is granted based on the matching

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.4, Pages : 61-65 (2014)
Special Issue of ICCEIT 2014 - Held on September 01, 2014 in The Solitaire Hotel, Bangalore, India

of information stored in databases i.e., a matching is performed against the features extracted from the fingerprints of the two same fingers at the time of requesting access with the features of combined fingerprint stored in database along with the key generated.

The paper is outlined as follows. Motivation, System Environment, System Evaluation.

MOTIVATION

In first stage, the system identifies the different minutiae points of the scanned fingerprint [2]. There are different kinds of minutiae for a fingerprint such as-Ridge ending, Ridge bifurcation, Crossover, Island, etc. We will be using ridge ending and bifurcation which are distinctive to each other. Automatically and reliably extract minutiae from the input fingerprint image is a critical step in fingerprint combination.

The extraction of orientation of a fingerprint image is performed [3]. The orientation of the image shows an intrinsic property of the fingerprint. It defines invariant coordinates for ridges and valleys in a local neighborhood. We present a fast orientation extraction algorithm, which can adaptively improve the clarity of ridge and valley structures of input fingerprint images based on the estimated local ridge orientation and frequency.

Certain landmark points are needed for the reference point extraction alignment of two fingerprints [4]. These should be extracted automatically with low misidentification rate. The prominent symmetry points (singular points, SPs) in the fingerprints are the landmarks. In this system the points are core and delta. These are the global features of a fingerprint. We identify an SP by its symmetric properties. SPs are extracted from the complex orientation field estimated from the global structure of the fingerprint, i.e. the overall pattern of the ridges and valleys. Complex filters, applied to the orientation field in multiple resolution scales, are used to detect the symmetry and the type of symmetry.

This explores the possibility of mixing two different fingerprints at the image level in order to generate a new fingerprint [5]. To mix two fingerprints, each fingerprint is decomposed into two different components the continuous and spiral components. After pre-aligning the components of each fingerprint, the continuous component of one fingerprint is combined with the spiral component of the other fingerprint image. Experiments on a subset of the fingerprint dataset show that the proposed approach can be used to generate virtual identities from images of two different fingers pertaining to a single individual or different individuals.

This system proposes a fingerprint minutiae matching technique, which matches the fingerprint minutiae by using both the local and global structures of minutiae [6]. The local structure of a minutiae describes a rotation and translation invariant feature of the minutiae in its neighborhood. It is used to find the correspondence of two minutiae sets and increase the reliability of the global matching. The global structure of minutiae reliably determines the uniqueness of fingerprint. Therefore, the local and global structures of minutiae together provide a solid basis for reliable and robust minutiae matching. The proposed minutiae matching scheme is suitable for an online processing due to its high processing speed.

The work deals with modern computing systems security issues, focusing on biometric based asymmetric keys generation process [7]. Conventional PKI systems are based on private/public keys generated through RSA or similar algorithms. The present solution embeds biometric information on the private/public keys generation process. In addition the corresponding private key depends on physical or behavioral biometric features and it can be generated when it is needed. Starting from fingerprint acquisition, the biometric identifier is extracted, ciphered, and stored in tamper-resistant smartcard to overcome the security problems of centralized databases. Biometric information is then used for user authentication and for public/private keys generation.

This system is an adaptive fingerprint enhancement method that is based on contextual filtering provides several improvement in fingerprint enhancement [8]. Based on locally estimated features such as fingerprint ridge frequency, orientation, and curvature, contextual filtering works. These estimated features are used to perform matched filtering locally. In this system the term adaptive indicates that the parameters required for the enhancement method are automatically adjusted based on the input fingerprint image. Five processing blocks comprise the adaptive fingerprint enhancement method, where four of these blocks are updated in our proposed system. The five processing blocks are: 1) equalization; 2) global analysis; 3) local analysis; 4) matched filtering; and 5) image segmentation . In the equalization block there is a histogram equalization performed and local analysis blocks a nonlinear dynamic range adjustment method is used. In the global analysis and matched filtering blocks, different forms of order statistical filters are applied.

SYSTEM ENVIRONMENT

The fundamental observation for this method is to prevent an attacker to compromise privacy of users or biometric data and not necessarily to the art by passing of the biometric authentication itself. The main problem statement of our existing system is security. The security level is relatively very low. So that the hackers easily hack the secured information. To avoid this problem, we proposes a fusion technique.

In this paper we proposes a novel system for providing security for RSA with the help of combination of fingerprint. This system involves generation of a combined fingerprint of two fingers, a key generation and authentication of them. There are three phases in the proposed method enrollment phase, authentication phase and key generation.

In enrollment phase fingerprints of two different fingers named as A and B are used. Then extract the minutiae positions from one fingerprint, the orientation from the other fingerprint, and the reference points from both fingerprints. Based on this extracted information and our proposed coding strategies, a combined minutiae template is generated and stored [1]. In key

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.4, Pages : 61-65 (2014)
Special Issue of ICCEIT 2014 - Held on September 01, 2014 in The Solitaire Hotel, Bangalore, India

generation, keys are generated from the combined minutiae stored in smart card using RSA. In authentication phase, the system requires two query fingerprints from the same two fingers which are used in the enrollment. A two-stage fingerprint matching process is proposed for matching the two query fingerprints against a combined minutiae template. If the access is permitted then using smart card the user able to decrypt the message send by an external source with the help of RSA algorithm key generation process.

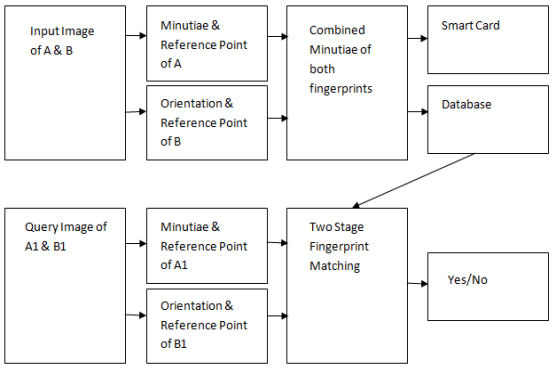

Fig:- 1. Enrollment & Authentication Phase

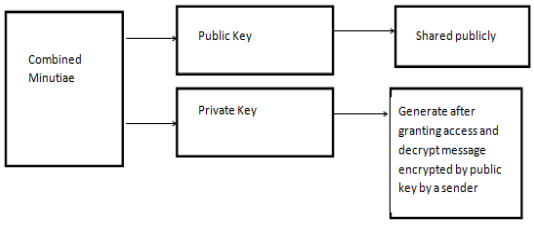

Fig:- 2. Key generation process

The system is implemented using Matlab version 7. 12. The five phases involved in the system are Minutiae Extraction, Orientation and Reference Point Detection, Combined Minutiae Template Generation, Two-Stage Fingerprint Matching and Key Generation Phase. Fig: 1 refers the enrollment, authentication and smart card generation phase and Fig: 2 refers key generation process.

A. MINUTIAE EXTRACTION

The minutiae point is the local feature of the fingerprint. The major minutia features of fingerprint ridges are ridge ending and bifurcation. The ridge ending is the point at which a ridge terminates. Bifurcations are points at which a single ridge splits into two ridges. Minutiae and patterns are very important in the analysis of fingerprints since no two fingers have been shown to be identical.

Due to the thicker structure of ridge first thinned the image. The objective of thinning is to make the ridges in to unit-width. We perform extraction phase using local analysis by moving a window. On moving a window presence of a zero in middle indicates either ridge ending or bifurcation. To identify whether it is a ridge ending or bifurcation we calculate the sum of window in this method. If sum is 2, then it is a ridge ending and when it is 4, then it is a bifurcation.

B. ORIENTATION AND REFERENCE POINT DETECTION

An input fingerprint image is normalized so that it has a pre specified mean and variance. Local orientation of the image is estimated from the normalized input fingerprint image. Orientation involves the calculation of image gradient that is change of ridges in x and y direction. So calculate the image gradient in x and y direction using [1].

Reference point is the global feature of the fingerprint. It involves core and delta point. Core is the U turn in ridge pattern and Delta is a Y shaped ridge meeting. These are the singular points [SP]. We identify an SP by its symmetry properties. SPs are extracted from the complex orientation field estimated from the global structure of the fingerprint. Complex filters applied to the orientation field in multiple resolution scales, are used to detect the symmetry and the type of symmetry [1] [4].

C. COMBINED MINUTIAE TEMPLATE GENERATION

Given a set of minutiae positions P_A, of fingerprint A, the orientation O_B of fingerprint B and the reference points of fingerprints A and B, a combined minutiae template MC is generated by minutiae position alignment and minutiae direction assignment, as shown in Fig: 3.

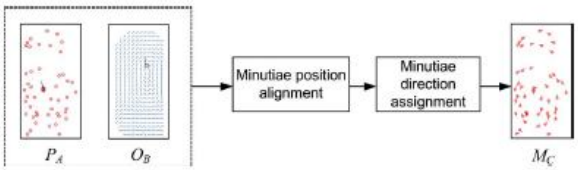

Fig:- 3. Combined minutiae template generation

a) Minutiae Position Alignment

Among all the reference points of a fingerprint for enrollment, we define a reference point with the maximum certainty value as the primary reference point. Therefore, we have two primary reference points R_a and R_b for fingerprints A and B , respectively. Let's assume R_a is located at $r_a = (r_{xa}, r_{yb})$ with the angle β_a , and R_b is located at $r_b = (r_{xb}, r_{yb})$ with the angle β_b . The alignment is performed by translating and rotating each minutiae point p_{ia} to $p_{ic} = (x_{ic}, y_{ic})$ by

$$(\mathbf{p}_{ic})^T = \mathbf{H} \cdot (\mathbf{p}_{ia} - \mathbf{r}_a)^T + (\mathbf{r}_b)^T$$

Where $()^T$ is the transpose operator and H is the rotation matrix where

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.4, Pages : 61-65 (2014)
Special Issue of ICCEIT 2014 - Held on September 01, 2014 in The Solitaire Hotel, Bangalore, India

$$\mathbf{H} = \begin{bmatrix} \cos(\beta_b - \beta_a), \sin(\beta_b - \beta_a) \\ -\sin(\beta_b - \beta_a), \cos(\beta_b - \beta_a) \end{bmatrix}.$$

As such, R_a and R_b are overlapped both in the position and the angle after the minutiae position alignment.

b) Minutiae Direction Assignment

Each aligned minutiae position p_{ic} is assigned with a direction θ_{ic} as follows:

$$\theta_{ic} = O_B(x_{ic}, y_{ic}) + \rho_i \pi$$

where ρi is an integer that is either 0 or 1. The range of $O_B(x_{ic}, y_{ic})$ is from 0 to 3.14. Therefore, the range of θ_{ic} will be from 0 to2*3.14 , which is the same as that of the minutiae directions from an original fingerprint.

$$\rho_i = \begin{cases} 1 & \text{if } \mathrm{mod}(\theta_{ia} + \beta_b - \beta_a, \pi) - O_B(x_{ic}, y_{ic}) > 0 \\ 0 & \text{otherwise} \end{cases}$$

D. TWO-STAGE FINGERPRINT MATCHING

Given the minutiae positions P_A of fingerprint A, the orientation O_B of fingerprint B and the reference points of the two query fingerprints. In order to match the stored in the database, we propose a two-stage fingerprint matching process including query minutiae determination and matching score calculation.

a) Query Minutiae Determination: The query minutiae determination is a very important step during the fingerprint matching. In order to simplify the description of our algorithm, we first introduce the local features extracted for a minutiae point in Mc. The local feature extraction is similar to the work proposed in [6].

b) Matching Score Calculation: For the combined minutiae templates that are generated using Coding Strategy 1, we do a modulo for all the minutiae directions in Mq and Mc , so as to remove the randomness. After the modulo operation, we use an existing minutiae matching algorithm [6] to calculate a matching score between Mq and Mc for the authentication decision. For other combined minutiae templates, we directly calculate a matching score between Mq and Mc using an existing minutiae matching algorithm [6]

E. KEY GENERATION PROCESS

This stage involves use of RSA algorithm for the generation of public/private key. Keys are generated from the combined minutiae template stored in smart card. Public key generated are shared publically and the external user who wants to send a secret message can use the public key for encryption. The keys generated are unique because it is created using biometrics so the message is free from attacks. The user can decrypt the message by generating private key with the help of RSA algorithm after the access is granted in authentication phase otherwise not. Keys are generated using algorithm described in [17]

EXPERIMENTAL RESULT

Formal definitions of FMR (False Match Rate), FNMR (False Non-Match Rate), and Equal Error Rate (EER)are given in [21]. Note that in single attempt, positive recognition applications, FMR and FNMR are often referred to as as FAR (False Acceptance Rate) and FRR (False Rejection Rate), respectively. Zero FMR is given as the lowest FNMR at which no False Matches occur and Zero FNMR is the lowest FMR at which no False Non- Matches occur.

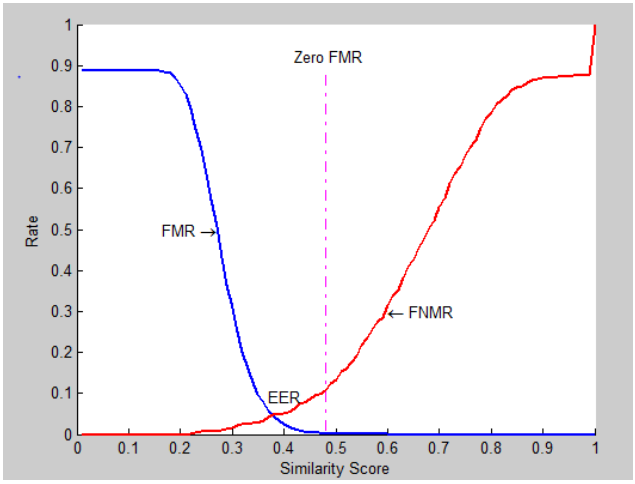

Fig :- 4 Shows FMR and FNMR calculations.

The calculation shows rate of false match rate decreases as the similarity score increases and the false non match rate increases with similarity score. EER is the value where FMR and FNMR are equal, i.e., where FMR = FNMR. Fig: 4 shows an EER value of 0.01 for both FMR and FNMR related to score value 0.3. Note that EER is the value that guarantees the same FMR and FNMR error rates for the algorithm. The EER is the best single description of the Error Rate of an algorithm and as lower be the EER the lower error rate of the algorithm[16].

CONCLUSION

In this method, we introduce a novel system for fingerprint privacy protection by combining two fingerprints into a new identity. In the enrollment, the system captures two fingerprints from two different fingers. A combined minutiae template containing only a partial minutiae feature of each of the two fingerprints can generate. To make the combined minutiae template look real as an original minutiae template, a coding strategies can introduce. In the authentication process, two query fingerprints from the same two fingers are required.

A two-stage fingerprint matching process is proposed for matching the two query fingerprints against the enrolled template. Grant the access for authenticated images. Finally a cryptographic key generation using RSA algorithm form combined fingerprint. Thereby we will able to increase the level of security. It is also difficult for an attacker to break other traditional systems by using the combined minutiae templates.

REFERENCES

[1] Sheng L and Alex C. Kot, "Fingerprint Combination For privacy Protection," *in Proc. IEEE transactions on information forensics and security, vol. 8, no. 2, February 2013.*

[2] Sayani Chandra, Sayan Paul, Bidyutmala Saha and Sourish Mitra, "Generate an Encryption Key by Using Biometric Cryptosystems to Secure Transferring of Data over a network" *IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 12, Issue 1 (May. - Jun. 2013), PP 16-22*

[3] L. Hong, Y. F. Wan, and A. Jain, "Fingerprint image enhancement: Algorithm and performance evaluation," IEEE Trans. Pattern Anal. Mach. Intell., vol. 20, no. 8, pp. 777–789, Aug. 1998.

[4] K. Nilsson and J. Bigun, "Localization of corresponding points in fingerprints by complex filtering," Pattern Recognit. Lett., vol. 24, no. 13,pp. 2135–2144, 2003.

[5] A. Othman and A. Ross, "Mixing fingerprints for generating virtual identities," in Proc. IEEE Int. Workshop on Inform. Forensics and Security (WIFS), Foz do Iguacu, Brazil, Nov. 29–Dec. 2, 2011.

[6] X. Jiang and W.Yau, "Fingerprint minutiae matching based on the local and global structures," in Proc. 15th Int. Conf. Pattern Recognition. 2000, vol. 2, pp. 1038–1041.

[7] Vincenzo Contiand, Salvatore Vitabile and Filippo Sorbell, *Fingerprint Traits and RSA Algorithm Fusion Technique,* 2012 Sixth International Conference on Complex, Intelligent, and Software Intensive Systems

[8] Safnitha P Y and Sheena Kurian K, "Fingerprint image enhancement with emphasis on histogram equalization adaptively", UGC sponsored national conference on information and communication technologies at BPC college piravom.

[9] Fingerprint Verification competition, For accessing fingerprint database, http://bias.csr.unibo.it/fvc2004/download.asp, accessed on 20.05.2014.

[10]Pan Dafu, Wang Bo. *An Improved Canny Algorithm. Proceedings* of the 27th Chinese Control Conference2008, 456-459.

[11] Devineni Venkata Ramana and Dr.Himasekhar, "PKI Key Generation Using Multimodal Biometrics Fusion Of Fingerprint And Iris" [IJESAT] *international journal of engineering science & advanced technology ISSN: 2250–3676 Volume-2, Issue-2 (March- April 2012), 285 – 290*

[12] M. K. Koo and A. Kot. Curvature-based singular points detection. Springer LNCS 2091. Springer Bigun Smeraldi Eds, 2001. Third International Conference AVBPA 2001, Halmstad, Sweden.

[13] M. Nilsson, M. Dahl, and I. Claesson, "Gray-scale image enhancement using the SMQT," in *Proc. IEEE Int. Conf. Image Process.*, vol. 1. Sep. 2005, pp. 933–936

[14] M. Nilsson, M. Dahl, and I. Claesson, "The successive mean quantization transform," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process.*, vol. 4. Mar. 2005, pp. 429–432.

[15] Josef Strom Bartunek, Mikael Nilsson, Benny Sallberg, and Ingvar Claesson, "*Adaptive Fingerprint Image Enhancement With Emphasis on Preprocessing of Data*," in Proc IEEE transactions on image processing, vol. 22, no. 2, february 2013.

[16] Equal Error Rate, For biometric evaluation, "http://www.griaulebiometrics.com/enus/book/understanding-biometrics/evaluation/accuracy/matching/interest/equal", accessed on 4.10.2014.

[17] S. Li and A. C. Kot, "A novel system for fingerprint privacy protection," in Proc. 7th Int. Conf. Inform. Assurance and Security (IAS), Dec. 5–8, 2011, pp. 262–266.

[18]https://www.math.washington.edu/~morrow/336_09/papers/Yevgeny.pdf, "RSA ALGORITHM", june 2.10.2014.

[19] B. J. A. Teoh, C. L. D. Ngo, and A. Goh, "Biohashing: Two factor authentication featuring fingerprint data and tokenized random number "Pattern Recognit., vol. 37, no. 11, pp. 2245–2255, 2004.

[20] A. Kong, K.-H. Cheung, D. Zhang, M. Kamel, and J. You, "An analysis of biohashing and its variants," Pattern Recognit., vol. 39, no. 7, pp. 1359–1368, 2006.

[21] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," IEEE Trans. Pattern Anal. Mach. Intell., vol. 29, no. 4, pp. 561–72, Apr. 2007.

[22] D. Maio, D. Maltoni, R. Cappelli, J.L. Wayman, and A.k.Jain, "FVC2000: Fingerprint Verification Competition," IEEE Trans. Pattern Analysis Machine Intelligence, vol. 24, no. 3, pp. 402-412, Mar. 2002

[23] S. Chikkerur and N. Ratha, "Impact of singular point detection on fingerprint matching performance," in Proc. Fourth IEEE Workshop on Automat. Identification Advanced Technologies, Oct. 2005, pp. 207–212.

[24] Y. Wang and J. Hu, "Global ridge orientation modeling for partial fingerprint identification," IEEE Trans. Pattern Anal. Mach. Intell., vol. 33, no. 1, pp. 72–87, Jan. 2011.

[25] X. Jiang and W. Yau, "Fingerprint minutiae matching based on the local and global structures," in Proc. 15th Int. Conf. Pattern Recognition, 2000, vol. 2, pp. 1038–1041.