Journal of Mechanical Engineering Research and Developments
ISSN: 1024-1752
Website: http://www.jmerd.org
Vol. 39, No. 2, 2016, pp. 441-449

The Application of Improved Fuzzy Vault Key Binding Algorithm in Fingerprint Feature Encryption System

F. Wang[*], B. Han, L. Niu, & Z. Y. Liu

School of Computer and Information Engineering College, Fu Yang Teachers College, Fu Yang, 236037, Anhui, China, *Email: wffync@fync.edu.cn

ABSTRACT: For traditional encryption algorithm existing key security management problem, an improved fingerprint minutiae key binding method is proposed based on Fuzzy Vault. The algorithm has the following improvements: Firstly, we effectively fuse the Lagrange polynomial interpolation formula and personal information. Secondly, we make use of helper data direction angle information to align center point, so that the algorithm has the translation rotation invariant property. Experimental result shows that: the algorithm not only can well protect the security key, but also there is a very low error rate.

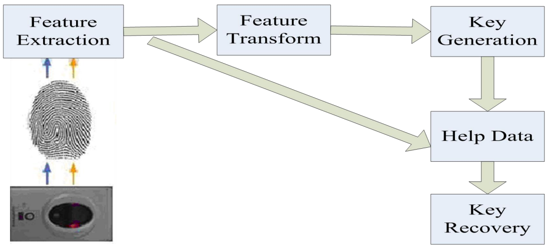
KEYWORDS: Fuzzy Vault; Key binding; Fingerprint minutiae; Helper data.

INTRODUCTION

Today society is a highly information-oriented, network-based society, the internet has become an indispensable part of people life, it brings great convenience to work and learn, but it also brings a lot of security risks, network security incidents frequently make people concern of personal privacy and information security .

Driven by the security demand, biometric encryption technology [1] has attracted widespread attention and become a hot research work, thus promoting the development of the technology in individual key management. Biometric features include physiological and behavioral characteristics, the physical characteristics include fingerprints, iris, palm prints, face, retina, etc., and they represent the inherent characteristics of human physiology. Behavioral characteristics include gait, signature, keystroke, sound, etc. These features are unique behavioral characteristics of people living gradually, it is difficult to guess, no memory and many other advantages. The use of individual biometric identification has a more secure network identity, and it is more reliable, more convenient advantages than the traditional private. On the other hand, binding biometrics and individual identity together, can represent physical identity of a person which can not be achieved based on key identification technology.

Existing encryption scheme can be divided into two categories based on biometrics: one is the key generation method, the main idea of this method is to extract the key from the user biometrics, and then using the extracted key to encrypt the data. When decrypting, from the captured user biometric extracting the same key again to decrypt the data, this method ensures the user physical identity legitimacy, but its drawback is that the attacker can attack on the traditional cryptographic algorithm to obtain the user encryption key, due to the stability of the user biometric information, so the user key in other biological applications will also be threatened, it may cause leakage of biometric permanent key. The other is the key binding method, it was proposed to bind the user key with its biometric in a fuzzy set, at the same time generating helper data which is used to align biological template information. When users need to encrypt or decrypt, extracting the biological characteristics of the user, with the help of helper data key is recovered for encryption and decryption operation. For legitimate user it can accurately recover protected key from the biometric and fuzzy sets, and it is difficult for unauthorized users to find out the real biometric information, thus it ensures the key security.



DOI: 10.7508/jmerd.2016.02.021

Figure 1. Biometric Encryption system diagram.

Biometric Encryption (as shown in Figure 1) concept was firstly proposed by Canadian George Tomko in 1994 [2]. Since 2000, many international research institutions and scholars in the emerging field of biometric encryption have carried out research. One of the most representative theoretical results is that Dodis et al [3] proposed fuzzy extractor and secure sketch theoretical framework in 2004. The framework provides a consistent theoretical framework and algorithm model that extracting random key must comply with cryptographic system. it unified the Fuzzy Vault [4], Fuzzy Commitment [5] algorithm which was proposed by Juels and others. Based on the theoretical framework, Kanukurthi et al [6] proposed a robust Fuzzy Extractor encryption scheme. Since then, many programs [7] have been proposed by some scholars. Keys can be extracted from the standard biometric, these standard features include bit vector, a real vector, etc. These forms of features expression can be measured in some simple measurement space, such as the Hamming distance, Euclidean distance, etc.

Fuzzy Vault algorithm was first proposed by Juels and Sudan et al. [8] as an independent biometric encryption algorithm, it binds key and biometric template by utilizing an encryption framework, thereby it can achieve to protect key and biometric template. This method effectively solves the contradiction between cryptography accuracy and biometric fuzziness, and provides an efficient algorithm model for the key binding algorithm.

Security and computational complexity of Fuzzy Vault method depend on the number of hash points. The decryption process for the vault must ensure that real user can quickly and accurately locate the minutiae set by contrasting the minutiae feature set to be queried with corresponding vault minutiae, and then reconstruct the polynomial in order to recover protective key. At the same time, an attacker can not filter out most of the hash points by comparing their own minutiae set with the vault set. Nandakumar et al. [9] proposed an improved fuzzy vault method in 2007 based on Fuzzy Vault frame, whose idea combines the fingerprint center point adjustment [10] with the minutiae matching based on map [11].

On the basis of fuzzy vault algorithm idea, we propose an improved fuzzy vault algorithm. The encryption process of this algorithm is as follows: we firstly extract minutiae correctly from the fingerprint image, and then filter some good quality minutiae as feature set, subsequently quantify and code these minutiae, and then by Lagrange formula constructing correlative polynomial, Meanwhile joining several hash points randomly to get a mixed set of points, at the last, a registered hash table is generated by quantifying the real minutiae and scrambling sequence, as well as the fuzzy vault is generated by merging mixing point and the hash table.

TRADITIONAL FUZZY VAULT KEY BINDING ALGORITHM

Extracting Minutiae

It is necessary to extract the fingerprint minutiae because our proposed Fuzzy Vault key protection method uses characteristic fingerprint minutiae, so minutiae feature accuracy directly impacts on the success rate of our approach when key is decrypted. It is necessary to preprocess fingerprint image before minutiae feature extraction, whose purpose is to improve the quality of fingerprint image, increasing ridges and valleys contrast, in order to extract minutiae features accurately.

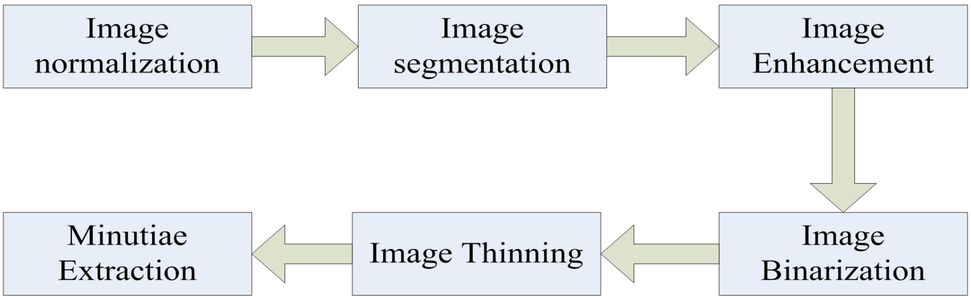


Figure 2. Fingerprint minutiae feature extraction process.

Fingerprint minutiae feature extraction (flow is shown in Figure 2) includes the following steps:

(1) Image normalization: The purpose of normalization is to adjust different original fingerprint image contrast and gray to a fixed level, which provides a more unified image specification for subsequent processing.

(2) Image segmentation: segmentation is to remove the background area from the image, reduce the processing time and computational complexity.

(3) Image enhancement: fingerprint image enhancement is a very important part of the fingerprint identification system, because its effect directly affects on fingerprint feature extraction, fingerprint matching and so on. The effect of fingerprint enhancement is to remove the image cross, breakpoints, and obscure part, to give a clearer fingerprint gray image.

(4) Image binarization: fingerprint image binarization is to convert fingerprint image into a gray binary image, which makes this image no longer involved pixel gray value and subsequent processing simple, and the amount of data has been greatly compressed.

(5) Image thinning: the purpose of thinning is to remove the fingerprint ridge edge pixel, making it only one pixel width. A good fingerprint thinning algorithm must meet the convergence, connectivity, topological, retention, thinning properties.

The effect of the fingerprint image preprocessing directly affects the extraction of minutiae. Generally minutiae extraction algorithm is divided into two categories: one is extracting minutiae feature directly from the fingerprint grayscale image. The other is extracting from the image after the thinning.

Traditional Fuzzy Vault Description

Fuzzy Vault algorithm was firstly proposed by Juels and Sudan as a independent biometric encryption algorithm, the method realized key protection and biometric feature encryption technology by binding key and biometric feature template which provides an efficient algorithm model for key binding algorithm, thereby to effectively solve the contradiction between accuracy of cryptosystem and ambiguity of biometric feature.

Fuzzy Vault key binding process is shown in Figure 3:

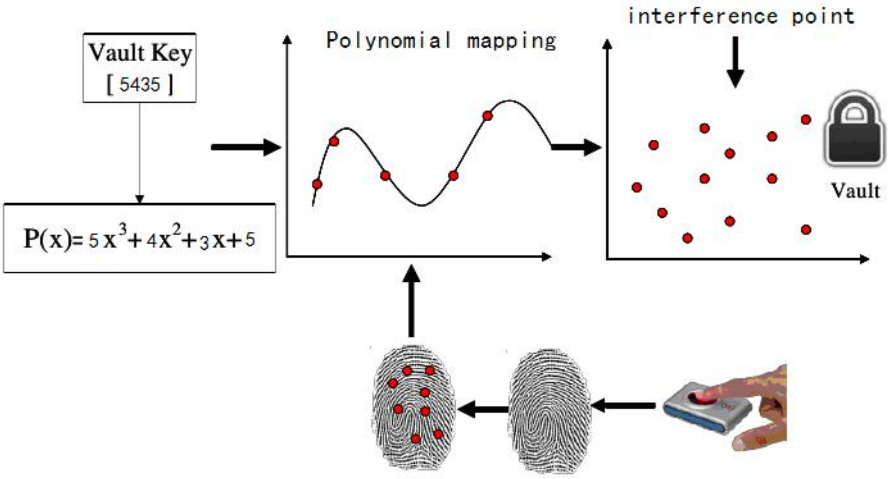


Figure 3. Fuzzy Vault Key binding algorithm flow.

In the key binding phase, firstly capturing user fingerprint image, extracting minutiae information of registered fingerprint image and helper data for aligning center point, selecting distinguish good minutiae as candidate minutiae used in the binding minutiae M. Secondly calculating binding cyclic redundancy check (CRC) value of key K, and K' is obtained after the value is connected to the key K, then K' is divided into (n+1) part as the polynomial coefficients and constants, thus obtaining a polynomial F. The values are obtained after these candidate minutiae are quantified and encoded as an independent variable into the polynomial, and denoted by P (M) {P (m), m ∈ M}, meanwhile randomly generating many hash point set CM, they must have good discriminative with the same minutiae requirement, while these hash points can not fall on the polynomial F, and then the vault is obtained after the real points and the hash points on the polynomial randomly shuffled together, lastly, the key binding process is completed when vault and helper data are stored on computer.

There are three main parameters in Fuzzy Vault key binding system:

(1) The number of points felling on polynomial, that is, the true minutiae number, which depends on the user fingerprint minutiae extraction number.

(2) The number of hash points, that is, not felling on polynomial points. those selection mainly depend on security level of the system, the more hash points, the higher the security level, generally the required hash point number is far greater than the real number points.

(3) The polynomial power n. the higher polynomial power is, the more difficult reconstructing polynomial is.

IMPROVED FUZZY VAULT ALGORITHM

Fuzzy Vault key binding method is proposed based on U. Uludag [12] and other improvements. The method filter n+1 minutiae from the candidate minutiae, and then using Lagrange interpolation method to reconstruct polynomial, connecting the polynomial coefficients so as to obtain key, calculating the key cyclic redundancy (CRC) code value, comparing it with CRC value of the original key, if they are equal, then outputting the key. Otherwise, repeating the above steps by reselecting the different n+ 1 minutia until traversing all possible minutias. If you still have not recovered the key, the key unbundling failed.

We choose minutiae location information and direction information in the application, in minutiae matching process, conditions require not only Euclidean distance to meet certain threshold, but also the direction of the deviation is less than a certain threshold, so it avoids false match in the case meeting Euclidean distance and not meeting direction deviation, improving the success rate of matching. In addition, the helper data method proposed in this paper has translation rotation invariant property, it is robust for image deformation and orientation change, improving the recognition rate of the system. For the extracting minutiae we used extraction method [13] proposed.

Computing helper data

Helper data is mainly used to align between query fingerprint and template fingerprint minutiae in binding key, and obtaining translation rotation correction parameter so that there is minutiae overlap as much as possible. On the basis of matching, the user key is obtained after polynomial is recovered. Since the helper data is public, it should meet the following two conditions:

(1) it does not disclose any template minutiae information, if once compromised, the attacker is likely to use this information to get real minutiae, then using them to reconstruct the polynomial, thereby restoring the protected key.

(2) It should contain enough information to verify the alignment between the verification fingerprint and the template fingerprint, accordingly obtaining translation and rotation correction parameter.

Helper data extraction method proposed in this paper has a translation rotation invariant feature, a center point as reference, selecting the minutiae within a radius of τ concentric circle to construct helper data.

Figure 4 shows a schematic view of the helper data.

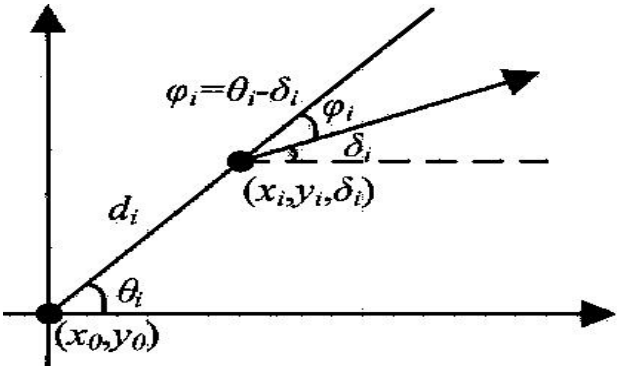


Figure 4. Helper data schematic diagram.

(x_0, y_0) is the coordinate of the fingerprint center point, $M^T = \{(x_i, y_i, \delta_i) \mid i = 1, 2, ..., N^T\}$ is minutiae set of extracted fingerprint minutiae, which (x_i, y_i) represents minutiae m_i abscissa and ordinate, δ_i expresses minutia m_i angle value relative to the horizontal axis, that is, the direction of minutiae. N^T represents the total number of minutiae extracted. For either minutia (x_i, y_i, δ_i), it is obtained in accordance with the following steps:

(1) Computing the Euclidean distance between current minutiae location and center points in accordance with the following formula.

$$d_i = \sqrt{(x_0 - x_i)^2 + (y_0 - y_i)^2} \tag{1}$$

In order to reduce the computational complexity, we use the square of the distance to represent. If d_i is greater than the radius of the center, then reselecting other minutiae

(2) Computing angle whose direction is current minutiae position relative to center point

$$\theta_i = \arctan \frac{(y_i - y_0)}{(x_i - x_0)} * 180 / \pi \tag{2}$$

(3) From the direction of current minutiae starting according to counterclockwise rotation calculating the relative position deflection angle:

$$\varphi_i = \min(| \theta_i - \delta_i |, 360- | \theta_i - \delta_i |) \tag{3}$$

Through the above three steps we can get a triple $(d_i, \theta_i, \delta_i)$, which has translational rotation invariant feature, using the distance between two minutiae, relative angle and the deflection angle information to construct the helper data instead of global information, its benefit is that it will not be impacted due to deformation, the position and collecting direction and other factors caused at the time of capturing the fingerprint image. After the triples as auxiliary data is saved, repeating the above three steps for all minutiae. Finally, the center position information and all the others are saved together as auxiliary data. Finally, the center point position information and all the triples to get together as auxiliary data to be saved. Thus, we get helper data. Whole algorithm flow is shown in Fig 5:

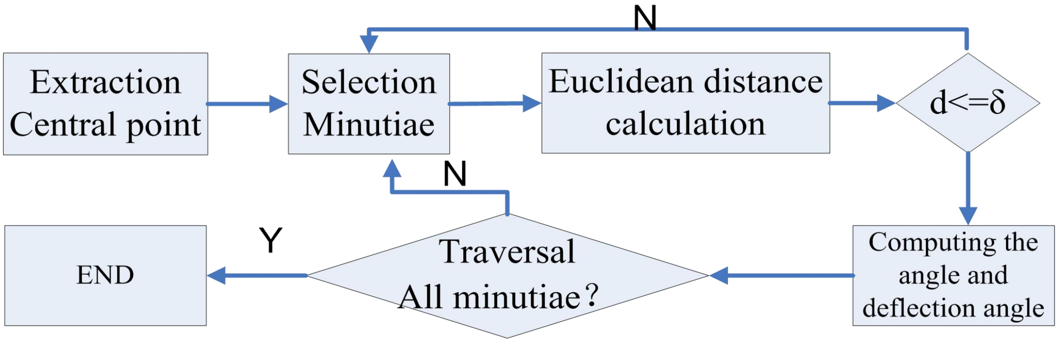


Figure 5. Helper data extraction process.

Key binding algorithm

In using Fuzzy Vault for key binding process, we use the finite field GF (2^{16}) to construct the vault, it is reason to chose GF (2^{16}) because it can provide a large dimension (the number of finite field element) to ensure the vault safety, and make Fuzzy Vault computing easily. Specific key binding process is shown in Figure 6 which includes the following nine steps:

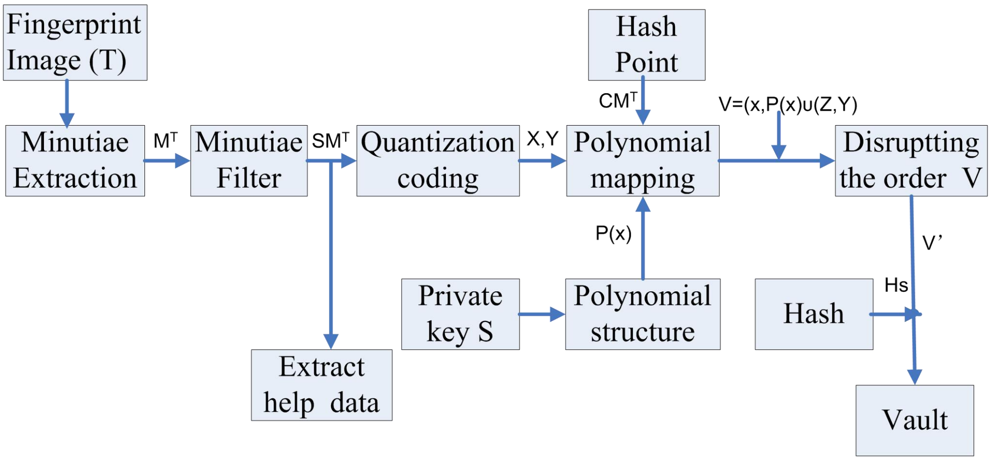


Figure 6. key binding process.

(1) Capturing registered user fingerprint image T, we obtain minutiae feature set M^T by minutiae extraction algorithm, where $M^T = \{m^T\}_{i=1}^{N^T}, m_i = (x_i, y_i, \delta_i)$

(2) Selecting distinguish good minutiae from the set of minutiae M^T, processing them from the two aspects:

① removing the false minutiae: high-quality minutiae is retained by extracting minutia algorithm, that is, any two candidate minimum distance to be selected between the points should be greater than a certain threshold. On the contrary, removing the minutiae from the minutiae set, such reserved minutiae are distinguishing good minutiae set (as shown in Figure 7). Selecting distinguish good minutiae can ensure to get a unique value when they are encrypted to the finite field F.

② In addition, it is necessary to construct polynomial to protect the key by the number of r minutiae polynomial interpolation, if the number of M^T set minutiae is less than r , or SM^T set can not successfully find the number of r distinguish good minutiae, the key is bound to fail.

(3) Helper data extraction method described in 3.1 processes SM^T minutiae set, to give the helper data H^T.

(4) Generating hash points set $CM^T = \{m_k\}_{k=1}^{s}$ randomly. Hash point is generated as follows: generating a hash point randomly $m = (x, y, \delta)$, when the minimum distance between the all points of $SM^T \cup CM^T$ set and m point is greater than the threshold, the hash point m is added to the CM^T set (as shown in Figure 9, where the red is true minutiae, green is hash points).

(5) Quantization and coding $SM^T \cup CM^T$ set. The minutiae component (x, y, δ) is quantized B_x, B_y and B_δ bits string respectively$(B_x + B_y + B_\delta = 16)$. After connecting three bits string together, the elements of a finite field F is obtained, and realized to code from minutia to finite domain. $X = \{x_i\}_{i=1}^{r}$ and $Y = \{y_i\}_{i=1}^{s}$ denotes respectively the real minutiae set and the set from the hash points coding to a finite field value

(6) calculating private S hash value H_s, and divided key S into n+1 sections, $S = s_0 || \ldots || s_n$, where "||" is the concatenation operator. Each segment as a polynomial of degree n polynomial coefficients is used to construct polynomial $P(x) = s_n x^n + s_{n-1} x^{n-1} + \ldots + s_0$.

(7) Polynomial mapping. Substituting set $X = \{x_i\}_{i=1}^{r}$ into polynomial P (x), then we can get corresponding function value P_x. $P_x = \{x_i, P(x_i)\}_{i=1}^{r}$, $x_i \in X$.

(8) Generating hash point function value randomly in order that they can not fell on polynomial p(x), $P_y = \{(y_i, z_i) \mid z_i \neq P(y_i)\}_{i=1}^{s}$, $y_i \in Y$.

(9) All set are shuffled randomly, the hash value H_s of key S and V' together are saved to generate vault $V = V' \cup H_s$. The key binding process is completed based on Fuzzy Vault.

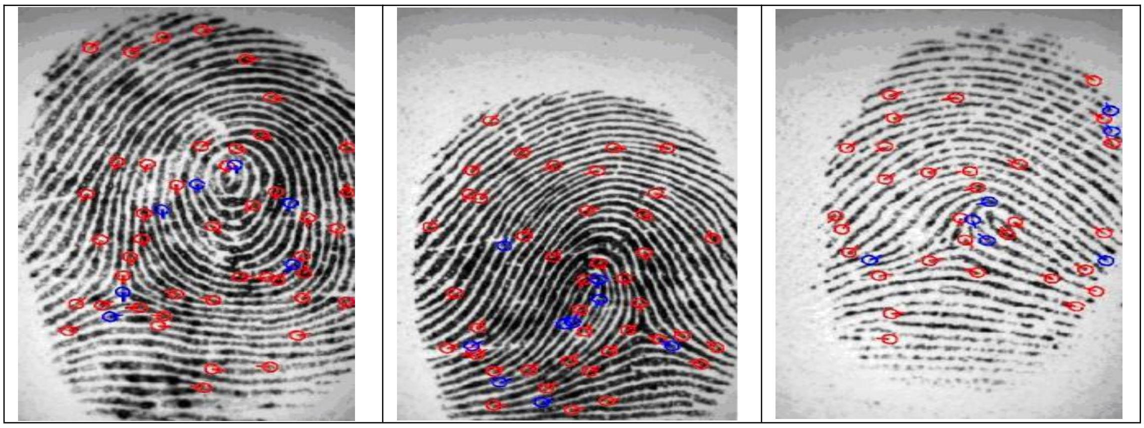


Figure 7. Encryption minutiae extraction.

EXPERIMENTAL TESTING AND ANALYSIS

Security analysis

Attacker must find the n+1 real minutiae of the Vault to reconstruct polynomial by way of violent attack in order to restore the key S. Suppose the length of the protected key is 128 bits, polynomial degree n is 8. In the process of implementation, vault contains 25 real minutiae and 100 hash points, in order to recover the protected key by way of violent attack, a total calculations number reaching C_8^{125} , where there is a real and effective reaching C_8^{25} , the probability of success from the vault to recover key is very low, so it is not feasible to recover key directly from the vault. Therefore, the safety performance is good.

Performance Analysis

In order to verify the performance of the method, we conduct the test on FVC2004 fingerprint database (DB2), the image size is 296×560, resolution is 500dpi.There are several main performance to be measured in fingerprint identification system:

(1) FAR: false acceptance rate, it refers to the probability from a different fingerprint determined to be the same finger, the lower the FAR is, the safety performance of the system is higher.

(2) FRR: false rejection rate. it refers to the same fingerprint is determined to come from different. The lower the FRR is, the safety performance of the system is higher.

(3) GAR: general acceptance rate. the higher GAR is, the system performance represents more better and stable, $GAR = 1 - FRR \cdot$

Experimental parameters are as follows: minutia neighborhood radius $\tau = 60$, the number of real minutiae in Vault r =25, when the user is registering, the minimum distance of two minutiae is set as 25, the maximum distance between two minutiae is 20 when minutiae are filtered, and the maximum distance is 30 when minutiae matching. Minutiae (x, y, δ) is mapped to the finite field GF (2^{16}) after it is quantized and coded, the quantization length of each component is: $B_x = 6$, $B_y = 5$, $B_\delta = 5$, polynomial degree n =9.

From the experimental results we can conclude that when the number of hash points increases to a certain extent, which influences on FRR (when polynomial number is 15, Hash point r = 80, FRR = 10%, r = 100, FRR = 10.4%), when the hash point filtering parameters are not set incorrectly, added hash points can mix the false with the genuine, which affects the performance of the system. On the other hand, hash points simulate real minutiae well to ensure the safety of the real minutiae. When the number of hash points is 100, there is a high recognition rate, but the reception error rate (FAR) is also very high, reaching 7%, and it is not feasible in the actual application.

Minutiae matching threshold is also a very important parameter in Fuzzy Vault key binding method, if the threshold is too low, it will lead to a decline recognition rate, affecting the performance of the system. If the threshold is too high, the error rate received will increase. Therefore, a reasonable choice to match the performance of the system threshold is also very important.

SUMMARY

This paper introduces the basic processes of minutiae classification, minutiae extraction and Fuzzy Vault key binding method idea. Then we propose helper data method which has the translation rotation invariant feature, and it is robust for fingerprint image distortion, direction, and noise, then we introduce implementation process for key binding based on Fuzzy Vault. Finally, we conduct experimental test and analysis proposed by us based on improved Fuzzy Vault key binding, the result shows that, by choosing reasonable system parameters, it can well protect the security key, and there is a very low error rate.

ACKNOWLEDGMENTS

This work is supported by Natural Science Foundation Key project of Anhui Provincial Education Department (No. KJ2015A295) and 2015KJ014, 2014KJ021, National Natural Science Foundation of China under Grant No. 61401101, and Natural Science Foundation of Anhui Province under Grant No. 1408085QF122. In addition, the authors would particularly like to thank the anonymous reviewers for helpful suggestions.

REFERENCE

[1] A.K.Jain, P.J.F1ynn, andA.A.Ross. Handbookofbiometrics.Springer, 2007.

[2] G.J. Tomko, C.Soutar, and G.J.Schmidt. Fingerprint controlled public key cryptographic system, July 30 1996. US Patent 5, 541, 994.

[3] Y Dodis, L. Reyzin, and A. Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In Advances in cryptology Euro-crypt 2004, pages 523-540. Springer, 2004.

[4] A.Juels and M. Sudan. A fuzzy vault scheme. In Proceedings of 2002 IEEE International Symposium on Information Theory., page 408. Lausanne Switzerland, 2002.

[5] A. Juels and M. Wattenberg. A fuzzy commitment scheme. In Proceedings of the 6th ACM conference on Computer and communications security, pages 28-36.ACM New York, N 丫 USA, 1999.

[6] B. Kanukurthi and L.Reyzin. An Improved Robust Fuzzy Extractor. In Proceedings of the 6th international conference on Security and Cryptography for Networks, pages 156-171. Springer Verlag Berfin, Heidelberg, 2008.

[7] Yevgeniy Dodis, Leonid Reyzin, and Adam Smith. Fuzzy extractors: A brief survey of results from 2004 to 2006. http://www.cs.bu.edu/reyzin/papers/fuzzy survey.pdf, 2007.

[8] A. Duels and M. Sudan. A Fuzzy Vault Scheme. Proceedings of IEEE International Symposium on Information Theory，Lausanne，Switzerland，2002. Designs,Codes and Cryptography,2006, 38(2):pp. 237-257.

[9] K. Nandakumar, A. K. Jain, and S. Pankanti. Fingerprint-Based Fuzzy Uault: Implementation and Performance. IEEE Transactions on Information Forensics and Security, 2007, Dec., 2(4), pp: 744-757.

[10] E. Liu, J. Liang, L. Pang, M. Xie, and J. Tian. Minutiae and modified Bio-code fusion for fingerprint-based key generation. Journal of Network and Computer.

[11] X. J Chen, J. Tian, and X. Yang. A New Algorithm for Distorted Fingerprints Matching Based on Normalized Fuzzy Similarity Measure. IEEE Transactions on Image Processing, 2006, Mar. 15(3), pp: 767-776.

[12] U.Uludag, S.Pankanti and A.K.Jain, Fuzzy Vault for Fingerprints. in Proceedings of Audio and Video-based Biometric Person Authentication, Rye Town, USA, July 2005, pp. 310-319.

[13] A. K. Jain, L. Hong, and R. Bolle, Online Fingerprint Verification. IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 19, no. 4, pp. 302-314,Apri1 1997.