A New Approach to Alignment-Free Fingerprint Cryptosystem Using Fuzzy Vaults

Ali Akbar Nasiri, Mahmood Fathy, and Mina Zolfy Lighvan

Abstract. It is very important to protect fingerprint templates in the fingerprint recognition systems. Fuzzy vault is a promising and applicable scheme for this purpose. It can protect biometric templates. Also, it can perform secure key management. Alignment of the query fingerprint sample in the encrypted domain and the template fingerprint sample is a challenging task. In this paper, we propose an alignment-free fingerprint cryptosystem based on multiple fuzzy vaults. In the proposed method, in registration phase, multiple vaults are constructed for one fingerprint and in verification phase, if at least two of the vaults are decoded successfully by the query fingerprint, the secret will be recovered. The experiments of the proposed fingerprint cryptosystem are conducted on FVC2002-DB1a and FVC2002-DB2a datasets to evaluate the performance of the proposed fingerprint cryptosystem.

Keywords: Fingerprint; minutia; reference point; fuzzy vault.

1. Introduction

Privacy violations may happen if biometric templates are compromised. Therefore, biometric template protection is an important issue in the current biometric recognition systems. An unknown original fingerprint image can be reconstructed from a fingerprint [1]. Authors in [1] have shown that three levels of information could be obtained from minutiae templates: the friction ridge structure, the orientation field and the type or class of information. The minutiae triplets were used to estimate local ridge orientation. The estimated local ridge orientation was then used to predict the type of the fingerprint. Finally, streamlines that were based on the estimated orientation field were used to generate the ridge structure of the original fingerprint.

Recently, authors in [2] showed that matcher which works based on minutiae could be faked using reconstructed minutiae but matcher which works on image could not be faked. Furthermore, usual methods for identifying persons which are based on identification numbers (PINs) or ID can be re-issued if the privacy issues are compromised. But when biometric systems are used for identification, re-issuing is not possible or practicable because biometric data do not change much over time. Therefore, when the same biometric templates are used in multiple identification applications, a biometric template can be shared between government agencies and commercial companies. This can lead to the possibility of tracking personal biometric data through cross matching.

In current biometric recognition systems, templates are stored in databases in unsecure manner. To protect these templates better, both cryptographic and biometric researchers have proposed many solutions. These solutions can be divided into two categories: cancelable biometrics and biometric cryptosystems.

1. 1. Cancelable Biometrics

For identification cancelable biometrics uses distorted or transformed biometric data instead of original biometric data [3]. In these methods, the original biometric data cannot be reconstructed from the transformed data because the transformation is noninvertible. A new set of biometric templates can be regenerated and it can be discarded if a set of biometric templates is found to be compromised.

Authors in [4] described three transformation methods. In the polar and Cartesian transformation methods, a fingerprint image were divided into sub-blocks and then those sub-blocks were scrambled. In the functional transformation method, a Gaussian function was used to make transformation. These three methods required alignment before transformation. Singular points were used to align the fingerprints.

Authors in [5] used a key-based transformation method for fingerprint biometric. At first, they detected a core point and then a line through the core point was determined. The angle of the line depends on the key. This line was used to generate transformed fingerprint templates. By changing the key which determines the angle a new transformed fingerprint template can be generated. Core point detection and the alignment of the fingerprint image are two disadvantages of this method. Another disadvantage of this method is that the minutia above the line can reveal some information from the original fingerprint data because these minutia were not transformed.

Authors in [6] used fingerprint minutia to generate a cancelable fingerprint template. At first the rotation and translation invariant values were extracted. Then, the extracted rotation and translation invariant values were used to transform each minutia. Finally, by moving each minutia based on the calculated movements, cancelable fingerprint templates were generated. The new templates could be regenerated if the cancelable templates were compromised.

Manuscript received May 25, 2014; revised August 22, 2014; accepted September 5, 2014.

A. A. Nasiri and M. Zolfy Lighvan are with the Department of Electrical and Computer Engineering, University of Tabriz, Iran. M. Fathy is with Computer Engineering Department, Iran University of Science and Technology, Tehran, Iran.
The corresponding author's e-mail is: aliakbar.nasiri@gmail.com.

1. 2. Biometric Cryptosystems

Biometric cryptosystems try to combine biometric templates with cryptographic keys. Successful biometric authentication can reveal the keys.

Biometric cryptosystems can act in one of the following three modes [7]: 1) key release, 2) key binding, and 3) key generation. In the key-release mode, biometric authentication is completely decoupled from the key release mechanism. The biometric template and the key are stored as separate entities and the key is released only if the biometric matching is successful. Implementing a biometric cryptosystem in the key release mode is easy, however such a system is not appropriate for high security applications because it has two major vulnerabilities. First, the biometric template is not secure. Template security is a critical issue in biometric systems because stolen templates cannot be revoked. Second, since authentication and key release are decoupled, it is possible to override the biometric matcher using a Trojan horse program.

In the key binding mode, the key and the template are monolithically bound within a cryptographic framework (see Fig. 1). It is computationally infeasible to decode the key or the template without any knowledge of the user's biometric data. A crypto-biometric matching algorithm is used to perform authentication and key release in a single step. In the key generation mode, the key is derived directly from the biometric data and is not stored in the database.

Biometric cryptosystems that work in the key binding/generation modes are more secure but difficult to implement due to large intra class variations in biometric data (i.e., samples of the same biometric trait of a user obtained over a period of time can differ substantially). For example, factors, such as translation, rotation, nonlinear distortion, skin conditions, and noise lead to intraclass variations in fingerprints (see Fig. 2).

One of the best and most common approaches that operates in the key binding mode is fuzzy vault scheme which was proposed by Juels and Sundan [8]. Based on the fuzzy vault scheme, in [9] the minutiae positions were used to encode and decode secret codes. However, alignment of fingerprints is crucial for this method to work properly. Many works have been conducted to overcome this problem. Authors in [7] proposed more effective implementation of fuzzy fingerprint vault. They also proposed an automatic

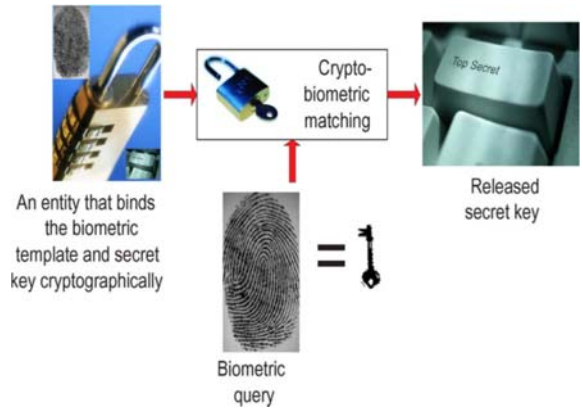


Fig. 1. Operation of a biometric cryptosystem in the key binding mode.

Fig 2. Illustration of intraclass variability in fingerprints. Two different impressions of the same finger obtained on different days are shown with minutia points marked on them. Due to translation, rotation, and distortion, the number and location of minutiae in the two images are different.

alignment method in the encrypted domain. They used the high curvature points on ridges to do alignment. Authors in [10] proposed another effective implementation of fuzzy vault scheme. They used minutia descriptor to propose their systems. This method made the false accept rate decrease greatly in low polynomial degrees. However, their scheme also needed the alignment. Authors in [11] proposed a new alignment algorithm for fingerprint fuzzy vault. They used ridges associated with the minutiae around the core point of the fingerprint for the alignment. By using this alignment method, authors in [12] developed a new version of fingerprint fuzzy vault. They integrated local ridge information of minutiae, which exclude the possibility of cross-matching among different vaults constructed from the same finger. So they improve the security of fuzzy vault. Authors in [13] developed an alignment-free fingerprint cryptosystem. Their method was based on modified Voronoi neighbor structures.

In this paper we propose a novel alignment free fingerprint cryptosystem which does not have any alignment procedure. We use minutiae near the reference point to constitute Cartesian systems. Based on these Cartesian systems, we calculate the new positions and orientations of minutiae to use them in encryption and decryption procedures.

The rest of this paper is organized as follows. Section 2 introduces the problems with previous methods. Section 3 introduces the basic fuzzy vault construction and Section 4 gives the details of the fuzzy vault implementation using fingerprint minutiae. The proposed alignment free fuzzy vault construction is described in Section 5. The experimental results are presented in Section 6. Section 7 summarizes our work.

2. Motivation and Scope

The major problem of previous efforts to protect fingerprint templates such as fuzzy vault scheme is that they need the alignment to protect templates. Here the alignment issue is different from the alignment problem in matching between query and registered fingerprint in usual fingerprint recognition systems. The matching algorithms in usual fingerprint recognition systems try to align a query

fingerprint template with a registered fingerprint template. However, when making protected fingerprint templates, a registered fingerprint is already transformed. So the registered fingerprint cannot be used for alignment. Some previous methods [7], [9] proposed some alignment methods to overcome this problem before using of fuzzy vault decoding. However, as described in [13], existing alignment methods may decrease the security of fuzzy vault schemes. In this paper, we propose a new alignment-free implementation of fuzzy vault for fingerprints, which does not have any alignment procedure. To achieve this, at encoding phase, we build multiple fuzzy vaults for a template fingerprint. At the decoding phase, if at least two of the vaults are decoded successfully, the secret will be recovered. The proposed method does not decrease security of fuzzy vault as we do not use alignment procedure.

3. Fuzzy Vault

Fuzzy vault [8] is a cryptographic construction that is designed to work with biometric features which are represented as an unordered set (*e.g.,* minutiae in fingerprints). The security of the fuzzy vault scheme is based on the infeasibility of the polynomial reconstruction problem. The ability to deal with intraclass variations in the biometric data along with the ability to work with unordered sets, which is commonly encountered in biometrics, makes the fuzzy vault scheme a promising solution for biometric cryptosystems.

Fig. 3 depicts the operation of a fuzzy vault scheme [7]. Suppose that a user wishes to hide a secret K (*e.g.,* a cryptographic key) using his or her biometric sample (template) which is represented as an unordered set X. The user selects a polynomial P that encodes the secret K and evaluates the polynomial on all elements in X. The user then chooses a large number of random chaff points which do not lie on the polynomial P. The entire collection of points consisting of both points lying on P and those that do not lie on P constitute the vault V. The chaff points conceal the genuine points lying on P from an attacker. Since the points lying on P encode the complete information about the template X and the secret K, concealing these points secures both the template and the secret simultaneously.

The user can retrieve the secret K from the vault V by providing another biometric sample (query). Let the query be represented as another unordered set X'. If X' overlaps substantially with X, then the user can identify many points in V that lie on P.

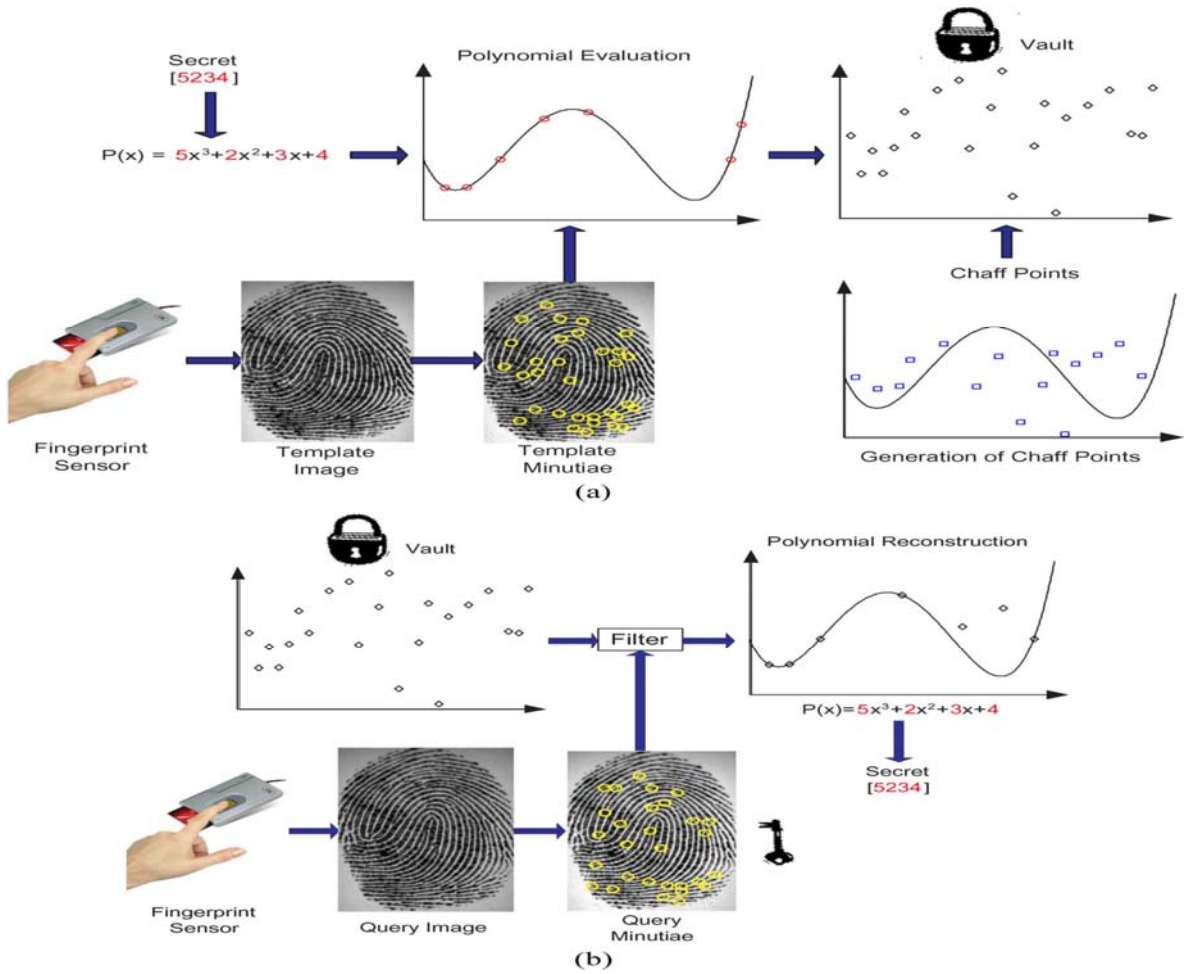


Fig. 3. Operation of the fuzzy vault scheme in [6] based on fingerprint minutiae. (a) Vault encoding. (b) Vault decoding.

If a sufficient number of points on P can be identified, an error correction scheme can be applied to exactly reconstruct P and thereby decode the secret K. If X' does not overlap substantially with X, it is infeasible to reconstruct P and the authentication is unsuccessful. Since the secret can be retrieved from the vault even when X and X' are not exactly the same, this scheme is referred to as a fuzzy vault.

The three main parameters in the fuzzy vault scheme are r, s, and n. The parameter r denotes the number of points in the vault that lie on the polynomial P and it depends on the number of features that can be extracted from the template (*e.g.,* number of minutia points in the user's fingerprint). The parameter s represents the number of chaff points that are added and this parameter influences the security of the vault. If no chaff points are added, the vault reveals the information about the template and the secret. As more chaff points are added, the security increases.

Typically, the number of chaff points is an order of magnitude larger than the number of genuine points (s>>r). Parameter n denotes the degree of the encoding polynomial and it controls the tolerance of the system to errors in the biometric data.

In order to retrieve the secret from the vault V, the user selects a subset of r points from V, which is known as the unlocking set. The unlocking set is selected based on the query X'. A (r, n) Reed–Solomon decoding algorithm is then applied to search for a polynomial P of degree n such that there are more than $(n+r)/2$ points in the unlocking set lie on P. If the number of discrepancies in the biometric data $|X-X'|$ are less than $(r–n)/2$, a valid polynomial P can be found and the secret K can be successfully retrieved.

4. Fuzzy Fingerprint Vault

A fingerprint minutia $m_i = (x_i, y_i, \theta_i, t_i)$ composes of four elements: x-coordinate, y-coordinate, angle, and type. Encoding and decoding phase are two steps of the fuzzy fingerprint vault systems. In order to explain the proposed method in the following section, encoding and decoding steps of the fuzzy fingerprint vault is explained in the following. We implement the fuzzy vault which is described in [8].

4.1. Encoding Processing

1. Let $\mathrm{SM^T} = \{m_j^T\}_{j=1}^r$ (where r denotes the number of minutiae) be a set of selected minutiae from a template fingerprint of a user. These minutiae are named real minutiae.
2. The chaff point set CM = $\{m_k^C\}_{k=1}^s$ is generated iteratively as follows. A chaff point $m_i = (x_i, y_i, \theta_i, t_i)$ is randomly chosen such that $x \in \{1, 2, \dots, U\}$, $y \in \{1, 2, \dots, V\}$, $\theta \in \{1, 2, \dots, 360\}$ and $t \in \{0, 1\}$. If the minimum distance, as defined in (1), between all points in the set CM $\cup$ $\mathrm{SM^T}$and m_i is greater than a value δ_1, the point m_i is added to CM.

$$D_M(m_i, m_j) = \sqrt{(u_i - u_j)^2 + (v_i - v_j)^2} + \beta_M \Delta(\theta_i - \theta_j), \quad (1)$$

where $\Delta(\theta_i - \theta_j) = \min(|\theta_i - \theta_j|, 360 - |\theta_i - \theta_j|)$ and β_M is the weight.

3. The minutia attributes u, v, θ, are quantized in order to get a set of bit strings of length B_u, B_v and B_θ, respectively. If B_u, B_v and B_θ are selected such that they add up to 15, by appending the bit strings corresponding to u, v, θ and t, we can get a 16-bit number. By this way, minutia points are encoded as elements in the field F = GF (2^{16}). Let $Y = \{y_k\}_{k=1}^s$ and $X = \{x_j\}_{j=1}^r$ be the encoded values of selected chaff points and template minutiae in the field F.
4. We choose a secret K of length $16n$, where n shows the degree of the polynomial. By appending a 16-b CRC code to secret K, a new secret S is obtained. The generator polynomial $G(w) = w^{16} + w^{15} + w^2 + 1$ is used for generating the CRC bits.
5. We encode the secret S into a polynomial P of degree n by partitioning it into 16-bit values $c_0, c_1, \dots, c_n$. The coefficients of P (i.e., $P(x) = c_n x^n + \dots + c_0$) shows the secret S.
6. We evaluate the polynomial P at all of the points in the selected minutiae set X to obtain the set $P(X) = \{P(x_j)\}_{j=1}^r$. The pair elements of the sets X and $P(X)$ form the locking set $L = \{(x_j, P(x_j))\}_{j=1}^r$. Also, we obtain a set $C = \{y_k, z_k)\}_{k=1}^s$ by randomly selecting values $y_k \in F$ and $z_k \in F$ such that the points (y_k, z_k) do not lie on the polynomial P. This set is called chaff set. We combine the chaff set with locking set to obtain V'.
7. We shuffle the elements of V' to form the vault V. The vault V is represented as $V = \{(a_i, b_i)\}_{i=1}^t$, where $t = r + s$. Only the vault V is stored in the system.

4. 2. Decoding Processing

Decoding processing is the step that reconstructs the polynomial from minutiae of input fingerprint image.

1. Let SMQ = $\{m_i^Q\}_{i=1}^{N^Q}$ be a set of minutiae from a query fingerprint image of a user.
2. We use the query minutiae to filter the chaff points in the vault. At first, we represent the abscissa values of the points in the vault as 16-bit strings. The 16-bit strings are partitioned into four strings of lengths B_u, B_v, B_θ, and B_t. Then we convert these four values into quantized minutia attribute values u, v, θ and t. Thus, we obtain the set MV = $\{m_i^v = (u_i, \alpha_i, \theta_i, t_i)\}_{i=1}^s$.
3. If the minimum distance between all of the selected minutiae in the query and the point $m_i^v \in$ MV is greater than a predefined value $\delta 2$, we consider the i–th element of the set MV as a chaff point. Let SMV = $\{m_k^v\}_{k=1}^{NV}$ be a subset of elements that are not considered as chaff points. This process is called coarse filter.
4. Only the elements of V that are included in SMV are added to the unlocking set L'.
5. We consider all possible subsets L'' of size $(n + 1)$ of the unlocking set L' and, for each subset, we construct a polynomial P^* by Lagrange interpolation. If $L'' = \{(a'_i, b'_i)\}_{i=1}^{n+1}$ is a specific candidate set, P^* is obtained as

$$P^*(x) = \frac{(x-a_2')(x-a_3')\dots(x-a_{n+1}')}{(a_1'-a_2')(a_1'-a_3')\dots(a_1'-a_{n+1}')}b_1' + \dots + \frac{(x-a_1')(x-a_2')\dots(x-a_n')}{(a_{n+1}'-a_1')(a_{n+1}'-a_2')\dots(a_{n+1}'-a_n')}b_{n+1}' \quad (2)$$

The aforementioned operations result in a polynomial

$P^*(x) = c_n^* x^n + c_{n-1}^* x^{n-1} + \dots + c_0^*$. The coefficients c_0^*, c_1^*, … , and c_n^* of the polynomial P^* are 16-bit values which are concatenated to obtain a $16(n + 1)$-bit string K^*. In this stage we apply CRC error detection to K^*. If an error is detected, it indicates that an incorrect secret has been decoded and we repeat this procedure again for the next candidate set L''. If no error is detected, it indicates $K' = K^*$.

5. Proposed Alignment-free Fingerprint Cryptosystem

The main idea in the proposed algorithm is defining a coordinate system with respect to minutia. A minutia point *p* in fingerprint has a position and local ridge orientation *v*, so each minutia defines coordinate system unambiguously. In this section, we describe how to construct fuzzy vault from minutia. Fig. 4 shows the overall method to construct alignment-free cryptosystem.

5. 1. Alignment-free Cryptosystem Encoding

Given the template fingerprint image *T*, the encoding procedure is as follows (see Fig. 4 (a)):

(1) Extracting core. At this stage, fingerprint image *T* is preprocessed and the orientation field is estimated. Next, we calculate all possible singular points using Poincare index. Then we choose the most reliable singular point as the core.

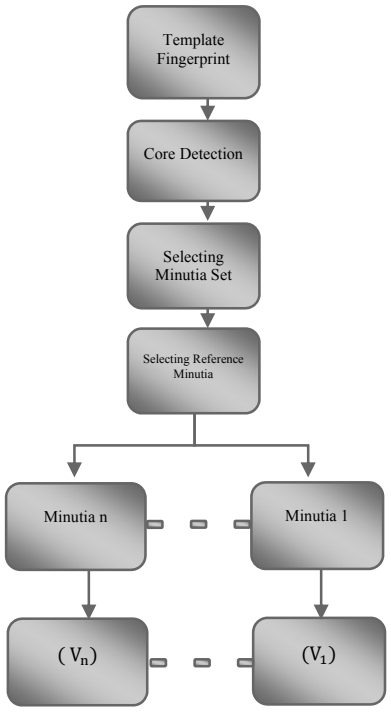
(2) Selecting minutia. We draw a ring around the core point by radius *R1* and *R2*, and mark all minutiae M_i^T in the ring. Each will define a coordinate system C_i.

(3) Minutia transformation. All minutia in template fingerprint are transformed based on minutiae M_i^T. Let $M_i^T = (x_i^T, y_i^T, \theta_i^T, t_i^T)$, a transformed minutia $M_i^{TT} = (x_i^{TT}, y_i^{TT}, \theta_i^{TT}, t_i^{TT})$ is obtained as follows:

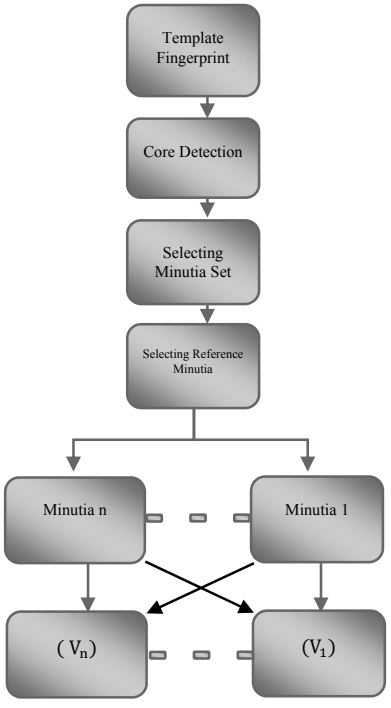
$$\begin{bmatrix} x_i^{TT} \\ y_i^{TT} \\ \theta_i^{TT} \end{bmatrix} = \begin{bmatrix} \cos\theta_i^T & -\sin\theta_i^T & 0 \\ \sin\theta_i^T & \cos\theta_i^T & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_i^{TT} - x_i^T \\ -(y_i^{TT} - y_i^T) \\ \theta_i^{TT} - \theta_i^T \end{bmatrix} \quad (3.1)$$

and

$$t_i^{TT} = t_i^T \quad (3.2)$$



(a)



(b)

Fig. 4. Flowchart of proposed alignment-free fingerprint cryptosystem, a) Vaults encoding, b) Vaults decoding.

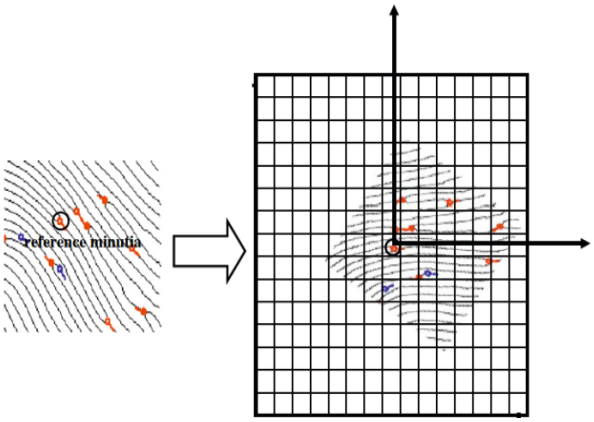


Fig. 5. Transformation of minutiae using a reference point.

Fig. 5 shows transformation of minutiae using a reference point. If r minutia is located in the ring, r minutia set are obtained.

(4) Constructing fuzzy vaults. A fuzzy vault V_i is constructed as described in fuzzy vault fingerprint section with every set of transformed minutia. Because we have r minutia in ring, we have r fuzzy vaults. The set of $V^T = \{V_i\}_{i=1}^{r}$ becomes the public information for the overall alignment-free crypto system.

5. 2. Alignment-free Cryptosystem Decoding

Given the query fingerprint image Q, the decoding procedure is as follows (see Fig. 4 (b)):

(1) Extracting core: Similar to the first step at encoding procedure, the same core detection algorithm is applied to detect the core of fingerprint image Q.

(2) Selecting minutia. We draw a ring around the core point by radiuses $R1$ and $R2$ and mark all minutia M_i^Q in the ring (radiuses $R1$ and $R2$ are the same as the ring radiuses at the encoding procedure).

(3) Minutia transformation. All minutia in query fingerprint are transformed based on minutiae M_i^Q. If r' minutia is located in ring, r' minutia set is obtained.

(4) Decoding fuzzy vaults. For each minutia set that is obtained, a decoding procedure as describes in vault fingerprint section is done for every fuzzy vault in database. If at least two of the vaults decoded successfully, the secret will be recovered.

6. Experimental Result

In the experiments, we use two databases to validate the proposed algorithm: The FVC2002 databases, DB1 and DB2. The optical sensor is used to extract the images of FVC2002 DB1 database, with resolution of 500 dpi. Also, optical sensor FX2000 is used to extract the images of FVC2002 DB2 database, with resolution of 569 dpi. Both of them include 800 (100 × 8) fingerprint images. We choose the impressions 1 and 2 of each finger from each database, which both consist of 100*2 impressions in order to compare our results with previous work. An example of successful vault operation for a user from FVC2002-DB2 when $n = 8$ is shown in Fig. 6. The coarse filter eliminates many chaff points from the vault. The unlocking set mostly consists of genuine points from the vault.

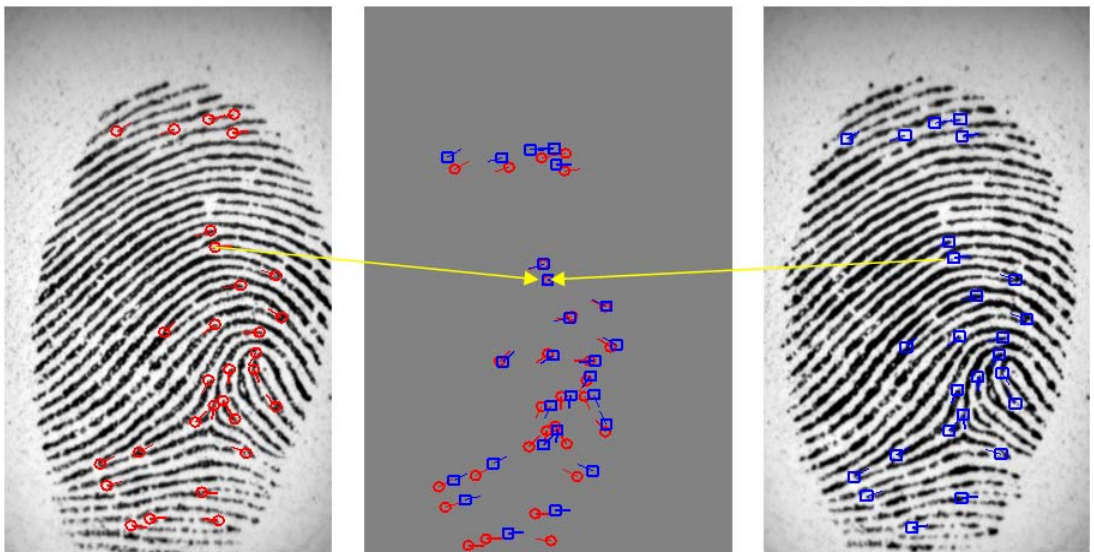


Fig. 6. Example of successful operation of the fuzzy vault.

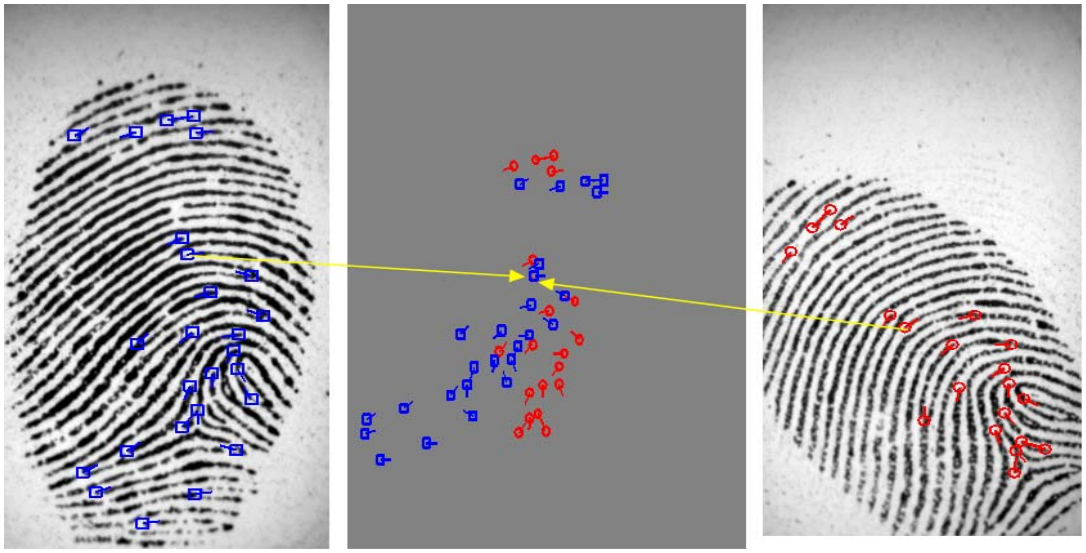


Fig. 7. Failure due to intraclass variations.

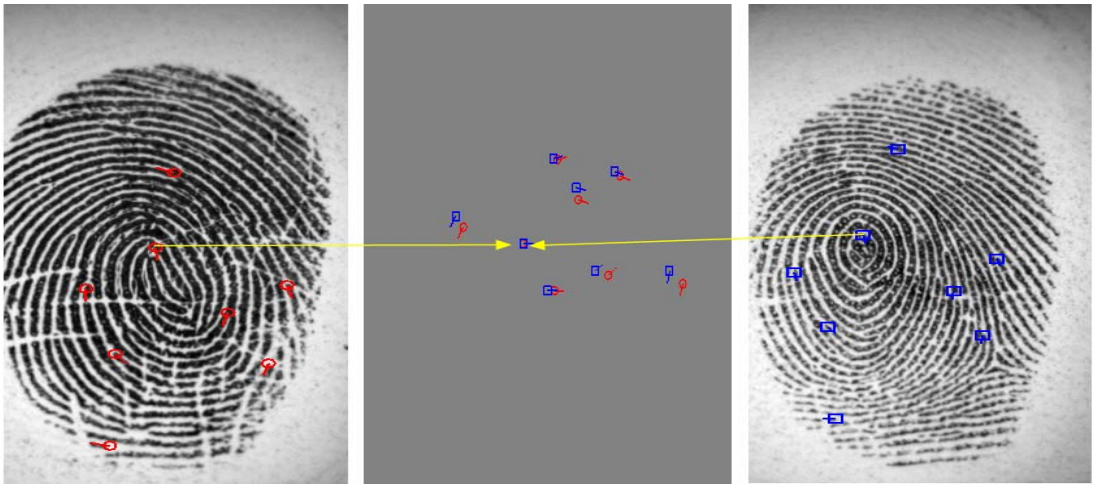


Fig. 8. Example of false accept when $n = 8$.

Fig. 7 shows an example where the false reject is due to intraclass variations. Because there are 6 number of paired minutia between the template and the query sample the vault decoding fails. We need at least 8 number of paired minutia between the template and the query sample in order to vault decode successfully.

Fig. 8 shows a case in which a false accept occurs. This is because there are 8 number of paired minutia between the template sample and query sample.

Table 1 shows results on DB2. As shown in this table, the two columns are the degree of the polynomial which is used in the encoding. More degree means more security in reconstruction of the polynomial. We evaluate the performance of the algorithm by GAR[1] and FAR[2]. The GAR shows genuine accept rate, and FAR shows false accept rate.

The same experiments are conducted on the FVC2002 DB1 in order to further test the performance of our algorithm. Experimental results on DB1 are shown in Table 2.

Table 1. Experimental results on FVC2002 DB2.

	N=8		*N=9*		*N=10*	
	GAR%	*FAR%*	*GAR%*	*FAR%*	*GAR%*	*FAR%*
Proposed algorithm	95	0.07	93	0.05	92	0.00
Product rule [12]	94	0.1	94	0,06	92	0.04
separated rule [12]	93	0	88	0	84	0
Algorithm in [15]	88	0.16	85	0.06	80	0
Algorithm in [10]	-	-	-	-	91	0.02

[1]Genuine accept rate
[2]False accept rate

Table 2. Experimental results on FVC2002 DB1.

	N=8		*N=9*		*N=10*	
	GAR%	*FAR%*	*GAR%*	*FAR%*	*GAR%*	*FAR%*
Proposed algorithm	91	0.02	90	0.02	88	0.01
Product rule [12]	91	0.44	91	0.26	87	0.1
Separated rule [12]	89	0.04	85	0.0	82	0
Algorithm in [10]	-	-	-	-	86	0.01

7. Conclusion

The security of biometric features is an important factor in the application of biometric identification. Fuzzy vault is a promise solution in encryption of both the secret key and fingerprint data. However, the alignment in fuzzy vault decoding is a complicated and difficult step because the registered fingerprint is already transformed so that it cannot provide any cue to a query fingerprint for alignment.

The goal of our technique was alignment-free fuzzy vault for fingerprint to overcome alignment difficulty in previous fuzzy vault fingerprint. Our technique used minutiae near the reference point to form new Cartesian system. To construct fuzzy vaults, we selected all minutia inside the ring surrounding the core. Then, with respect to coordinate system which every minutia inside the ring defined it, fuzzy vaults are constructed. The fuzzy vaults are stored in database. In decoding phase, also we selected all minutia inside the ring surrounding the core in query fingerprint. For each minutia inside the ring, other minutia are transformed based on the coordinate system corresponding to the selected minutia. After transforming minutia based on new coordinate system, we checked that this set of minutia can decode vaults or not. If at least two of the vaults are decoded successfully, the secret will be recovered.

The experiments of the proposed fingerprint cryptosystem are conducted on FVC2002-DB1a and FVC2002-DB2a datasets to evaluate the performance of the proposed fingerprint cryptosystem. Experimental results show the effectiveness of the proposed algorithm. As you can see from experiments, when we increase the degree of polynomial P, the GAR and FAR decreases. Therefore more minutiae is needed to be matched in decoding phase.

References

[1] A. Ross, J. Shah, and A. K. Jain, “From template to image: reconstructing fingerprints from minutiae points,” *IEEE Transactions on Pattern Analysis and Machine Intelligence, Special Issue on Biometrics*, pp. 544–60, 2007.

[2] L. Nanni and A. Lumini, “Descriptors for image-based fingerprint matchers,” *Expert Systems with Applications*, vol. 36, no. 10, pp. 12414–12422, 2009.

[3] S. Wang and J. Hu, “Design of alignment-free cancelable fingerprint templates via curtailed circular convolution,” *Pattern Recognition*, vol. 47, no. 3, pp. 1321–1329, Mar. 2013

[4] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, “Generating cancelable fingerprint templates,” *IEEE Transactions on Pattern Analysis and Machine Intelligence, Special Issue on Biometrics*, pp. 561–572, 2007.

[5] R. Ang, R. Safavi-Naini, and L. McAven, “Cancelable key-based fingerprint templates,” in *Information Security and Privacy: 10th Australasian Conference (ACISP2005),* pp. 242–252, 2005.

[6] C. Lee, J. Choi, K. Toh, S. Lee, and J. Kim, “Alignment-free cancelable fingerprint templates based on local minutiae information,” *IEEE Transactions on Systems, Man and Cybernetics,* vol. 37, pp. 980–992, 2007.

[7] K. Nandakumar, A. Jain, and S. Pankanti, “Fingerprint-based fuzzy vault: implementation and performance,” *IEEE Transactions on Information Forensics and Security*, vol. 2, pp. 744–757, 2007.

[8] A. Juels and M. Sundan, “A fuzzy vault scheme,” in *Proceedings of the IEEE International Symposium on Information Theory*, Lausanne, Switzerland, 2002, p. 408.

[9] U. Uludag, S. Pankanti, and A. Jain, “Fuzzy vault for fingerprints,” in *Proceedings of 5th International Conference on Audio and Video Based Biometric Person Authentication*, pp. 310–319, 2005.

[10] A. Nagar, K. Nandakumar and A. K. Jain, "Securing fingerprint template: Fuzzy vault with minutiae descriptors," *Pattern Recognition, 2008. ICPR 2008. 19th International Conference on*, Tampa, FL, 2008, pp. 1-4.

[11] J. Li, X. Yang, J. Tian, P. Shi, and P. Li, "Topological structure-based alignment for fingerprint fuzzy vault," *Pattern Recognition, 2008. ICPR 2008. 19th International Conference on*, Tampa, FL, 2008, pp. 1-4.

[12] P. Li, X. Yang, K. Cao, P. Shi, and J. Tian, “Security-enhanced fuzzy fingerprint vault based on minutiae’s local ridge information,” in *Proceedings of the 3rd International Conference of Biometrics*, ICB’ 2009, pp. 930–939.

[13] W. Yang, J. Hu, and S. Wang, “An alignment-free fingerprint bio-cryptosystem based on modified Voronoi neighbour structures,” *Pattern Recognition*, vol. 47, no. 3, pp.1309-1320, 2014.

[14] P. Lia, X. Yanga, K. Caoa, X. Taoa, R. Wanga, and J. Tian, “An alignment-free fingerprint cryptosystem based on fuzzy vault scheme,” *Journal of Network and Computer Applications*, vol. 33, pp. 207-220, May 2010.

[15] B. Tams, “Absolute fingerprint pre-alignment in minutiae-based cryptosystems,” in *Proc. of BIOSIG*, 2013, pp. 75–86

Ali Akbar Nasiri received his B.S. degree in computer engineering (hardware) from Shiraz University, Shiraz, Iran, in 2008, the M.S. degree in computer engineering (artificial intelligence) from Iran University of Science and Technology (IUST), Tehran, Iran, in 2011. Currently, he is pursuing his Ph.D. degree in computer engineering (artificial intelligence) in Faculty of Electrical and Computer Engineering, University of Tabriz, Tabriz, Iran. His major research interests include object oriented programming, Verilog, citation based plagiarism detection (CBPD), image processing, biometric security, and network security.

Mahmood Fathy received the B.S. degree in electronics from Iran University of Science and Technology, Tehran, Iran, in 1985, the M.S. degree in computer architecture from Bradford University, West Yorkshire, U.K., in 1987, and the Ph.D. degree in image processing computer architecture from the University of Manchester Institute of Science and Technology, Manchester, U.K., in 1991. Since 1991, he has been a Professor with the Department of Computer Engineering, Iran University of Science and Technology. His research interests include the quality of service in computer networks, including video and image transmission over internet, the applications of vehicular ad hoc networks in intelligent transportation systems, and real-time image processing with particular interest in traffic engineering.

Mina Zolfy Lighvan received her B.Sc. degree in computer engineering (hardware) and M.Sc. degree in computer engineering (computer architecture) from ECE Faculty, University of Tehran, Tehran, Iran in 1999, 2002, respectively. She received Ph.D. degree in electronic engineering (digital electronic) from Electrical and Computer Engineering Faculty, University of Tabriz, Tabriz, Iran. She currently is an Assistant Professor and works as a Lecturer in Tabriz University. She has more than 20 papers that are published in different national and international conferences and journals. Her major research interests include text retrieval, object oriented programming and design, algorithms analysis, HDL simulation, HDL verification, HDL fault simulation, HDL test tool VHDL, Verilog, hardware test, CAD tool, synthesis, digital circuit design and simulation.