5thSASTech 2011, Khavaran Higher-education Institute, Mashhad, Iran. May 12-14.

Alignment-Free Fingerprint Cryptosystem Based On Multiple Fuzzy Vault and Minutia Local Structures

Ali Akbar Nasiri
Computer Engineering Department
Iran University of science and technology
Tehran, Iran
ali_nasiri@iust.ac.ir

Mahmood Fathy
Computer Engineering Department
Iran University of science and technology
Tehran, Iran
mahfathi@iust.ac.ir

Abstract

The popularity of biometrics and its widespread use introduces privacy risks. To mitigate these risks, solutions such as the helper-data system, fuzzy vault, fuzzy extractors, and cancelable biometrics were introduced, also known as the field of template protection. Fuzzy vault is a practical and promising scheme, which can protect biometric templates and perform secure key management simultaneously. Alignment of the template biometric sample and the query one in the encrypted domain remains a challenging task. In this paper, we propose an alignment-free cryptosystem based on multiple fuzzy vaults and minutia local structures. In proposed method, in registration phase, multiple vaults construct for one fingerprint and in verification phase, if at least one of the vaults with respect to its minutiae local structures decoded successfully by the query fingerprint, the secret will be recovered. Experiments on FVC2002-DB2a and FVC2002-DB1a are conducted to show the promising performance of the proposed fingerprint cryptosystem.

Keywords: Fingerprint, minutia, local structures, fuzzy vault

1. Introduction

When biometric templates are compromised, privacy violations may occur. Therefore, biometric template protection has become a critical issue in the current biometric community. Several researchers have shown that an unknown original biometric image can be reconstructed from a fingerprint[1]. Authors in [1] showed that three levels of information about the original fingerprint could be obtained from minutiae templates: the orientation field, the class or type of information, and the friction ridge structure. The local ridge orientation was estimated using the minutiae triplets. This was then used to predict the class of the fingerprint. Finally, the ridge structure of the original fingerprint was generated using streamlines that were based on the estimated orientation field. Recently, authors in [2] experimentally showed that minutiae based matcher could be faked using reconstructed minutiae but image based matcher could not be faked. Furthermore, traditional methods for identifying persons, for example, ID and personal identification numbers (PINs), can be canceled and re-issued if the above privacy issues are compromised. But this is not possible with biometric data because biometric data do not vary much over time and are very rarely shared by two people. Therefore, when the same biometric data are used in multiple security applications, biometric data can be shared between commercial companies and law enforcement or government agencies. This may lead to the possibility of tracking personal biometric data stored in one security application by getting access to another security applications through crossmatching.

1-1. Previous ways of protecting biometric templates

In general biometric systems, templates are stored fairly insecurely in databases. To protect them better, many alternate solutions have been proposed by both biometric and cryptographic researchers. These solutions can be roughly divided into two categories: cancelable biometrics and biometric cryptosystems.

A. Cancelable biometrics

Cancelable biometrics uses transformed or intentionally-distorted biometric data instead of original biometric data for identification. Because the transformation is noninvertible, the original biometric templates cannot be recovered from the transformed templates. When a set of biometric templates is found to be compromised, it can be discarded and a new set of biometric templates can be regenerated.

Authors in [3] proposed a key-based transformation method for fingerprint minutiae. A core point of an input fingerprint image was detected and then a line through the core point was specified. The angle of the line depended on the key, where $0 \leq key \leq \pi$. The transformed fingerprint templates were generated by reflecting the minutiae under the line into those above the line. The new transformed fingerprint template was then generated by changing the key (angle). A disadvantage of this method is that it required core point detection as well as the alignment of the input fingerprint image into a canonical position. Also, since the minutiae above the line were not transformed, the transformed template still retained some information from the original fingerprint.

Authors in [4] described three transformation methods such as Cartesian, polar, and functional transformation. The Cartesian and polar transformation methods divided a fingerprint into sub-blocks and then scrambled those sub-blocks. In the functional transformation method, transformation was based on a Gaussian function. However, all three methods required alignment before transformation. To align the fingerprints, these methods used singular points. Authors in [5] proposed a cancelable fingerprint template using fingerprint minutiae. Translation and rotation invariant values were extracted using orientation information around each minutia. The obtained invariant value was input into two changing functions (which output translational and rotational movement) to transform each minutia. Final cancelable templates were generated by moving each minutia according to the calculated movements. When the cancelable templates were compromised, new templates were regenerated by replacing the changing functions.

B. Biometric cryptosystems

Biometric cryptosystems combine cryptographic keys with biometric templates so that the keys cannot be revealed without successful biometric authentication.

One of the most popular approached is fuzzy vault scheme proposed by Juels and Sundan [6]. Based on the fuzzy vault scheme, in [7] the minutiae positions were used to encode and decode secret codes. However, this method inherently assumed that the fingerprints were aligned. Several works have been proposed to overcome this issue. [8] proposed more robust and effective implementation of fuzzy fingerprint vault (FFV). They also developed an automatic alignment method in the encrypted domain, using the high curvature points on ridges (i.e., so-called helper data). Authors in [9] developed another effective implementation which took the minutia descriptor into consideration and made the FAR decrease greatly in low polynomial degrees. However, their scheme also aligns the corresponding fingerprints using high curvature points on ridges. Authors in [10] developed a novel alignment algorithm for FFV, by tracing the ridges associated with the minutiae around the core point of the fingerprint and storing the location and orientation of the sampling points. By using this alignment method, authors in [11] proposed a security-enhanced version of FFV integrating local ridge information of minutiae, which excluded the possibility of cross-matching between different vaults constructed with the same finger.

1-2. Motivation and Scope

One problem of previous efforts to protect fingerprint templates such as fuzzy vault scheme is that they require the alignment of fingerprint images to make protected templates. The alignment issue here is different from the alignment problem in matching between registered and query fingerprint. The matching algorithm tries to align a query fingerprint with a registered fingerprint (relative alignment). However, when making protected fingerprint templates, a registered fingerprint is already transformed so that it cannot provide any cue to a query fingerprint for alignment (absolute alignment). Some previous methods [8,9,10] proposed some alignment methods to overcome this problem before using of fuzzy vault decoding. However, as described in [12], the security of fuzzy vault systems may be decreased by existing alignment methods. In this paper, we propose an alignment-free implementation of fuzzy vault for fingerprints, which can avoid the alignment procedure. To achieve this, at encoding phase, we bulid multiple fuzzy vault for a template fingerprint. At decoding phase, if at least one of the vaults is decoded successfully, the secret will be recovered. The propose method don't decrease security of fuzzy vault because we don't use alignment procedure. The organization of this paper is as follows. In section 2, the main idea of fuzzy vault for fingerprint is described. In section 3, the details of minutia local structure are elaborated. Section 4 is the main body of this paper and gives the specific description of implementing the alignment-free fingerprint cryptosystem. Experimental results are discussed in Sections 5, and we draw the conclusion in Section 6.

2. FUZZY FINGERPRINT VAULT

A fingerprint minutia represented by $m_i=(x_i,y_i, \theta_i, t_i)$ is composed of four elements: *x*-, *y-coordinates*, *angle*, and *type*. The fuzzy fingerprint vault system is composed of two steps, encoding and decoding. For the purpose of explanation of the proposed method in the following section, each step of the fuzzy fingerprint vault is explained in the following.

2-1. Encoding Processing

1. let $L= \{(x_i,y_i, \theta_i, t_i) \mid i= 1,...,n\}$(where *n* denote the number of minutiae) be a set of minutiae from a template fingerprint image of a user. These minutiae are called as real minutiae.
2. Generate a degree-*k* polynomial from a secret(*S*), and compute a hash value κ from a hash function *hash*(*S*)

$$p(x) = a_0 + a_1\, x + ... + a_k\, x_k \qquad \textbf{(1)}$$

$$S=(a_0||a_1||\ldots||a_k) \qquad \textbf{(2)}$$

$$a_i \in GF(p^2) \qquad \textbf{(3)}$$

$$\kappa= hash(S) \qquad \textbf{(4)}$$

3. Compute the polynomial projections, $p(x)$, after converting all elements of L to an element of GF[1](p^2), and define this result as Set *RL*. For example, if an element of GF(p^2) is represented as $AX+B$ ($A,B \in \mathrm{GF}(p^2)$), we can replace x and y coordinates of the minutia to A and B, respectively.

$$R_L=\{(r_i, v_i) \mid i=1,\dots,n\},\ r_i=(x_i,y_i,\theta_i,t_i) \tag{5}$$

$$v_i=p(X_i),\ X_i=x_iX+y_i \in GF(p^2),\ i=1,\dots,n \tag{6}$$

4. Randomly generate chaff minutiae that do not lie on $p(x)$ to protect real minutiae.

$$C=\{(c_i, v_i) \mid i=n+1,\dots,r\},\ c_i=(x_i,y_i,\theta_i,t_i) \tag{7}$$

$$v_i=p(X_i)+\alpha_i,\ X_i=x_iX+y_i \in GF(p^2),\ i=n+1,\dots,r \tag{8}$$

where α_i is a non-zero element over finite fields of the form GF(p^2).

5. Randomly generate Set R that is integrated with R_L and C.

$$R=\{(r_i, v_i) \mid i=1,\dots,r\},\ r_i=(x_i,y_i,\theta_i,t_i) \tag{9}$$

6. Finally, the vault is constituted by the real and chaff minutiae, the degree k of the polynomial and the secret. The secret should be stored in a hashed form.

$$V=\{(r_i, v_i) \mid i=1,\dots,r,\ \kappa,k \mid i=1,\dots,r\} \tag{10}$$

2-2. Decoding Processing

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

1. Let $U=\{((x'_i,y'_i,\theta'_i,t'_i)) \mid i=1,\dots,m\}$ (where m denotes the number of minutiae) be a set of minutiae from input fingerprint image.
2. Execute fingerprint matching with Set U and r_i of Set V stored in the Encoding processing. The matching results are stored in Set M with t matched minutiae and corresponding *vi* in Set V.

$$M=\{(m_i, v_i) \mid i=1,\dots,r\},\ m_i=(x_i,y_i,\theta_i,t_i) \tag{11}$$

where $M \in R$, $t \leq r$.

3. If k and M are used as input values for the RS_{DECODE}, the degree-k polynomial($p'(x)$) will be returned. Then, κ' is computed by Eq. 14.

$$p'(x)=RS_{DECODE}(k,M) \tag{12}$$

$$p'(x)=a'_0+a'_1x+\dots+a'_k x_k \tag{13}$$

$$\kappa'=hash(a'_0||a'_1||\dots||a'_k) \tag{14}$$

4. If κ' and κ are exactly same, the user is accepted. Otherwise, he is rejected.

$$Decision=\begin{cases} Accept, & if\ \kappa'=\kappa \\ Reject, & Otherwise \end{cases} \tag{15}$$

If Set M contains k+1 real minutiae, the fuzzy fingerprint vault can reconstruct the same polynomial used in the encoding process.

[1] Galois Field

3. Minutia local structure

To construct the alignment-free cryptosystem, we need to select the feature invariant to rigid transformation (translation and rotation).

Authors in [12] proposed a local structure for minutiae, which described a rotation and translation invariant feature of the minutia in its neighborhood. They use relative distance, radial angle, and minutia orientation to construct a six-element feature vector of the minutia associated with its two nearest neighbors. As shown in Fig. 1, let $M_i(x_i, y_i, \theta_i)$ denote the primary minutia and $N_0(x_{n0},y_{n0},\theta_{n0})$, $N_1(x_{n1},y_{n1},\theta_{n1})$ its two nearest neighbors, where x and y are the location and θ is the orientation. Authors in [12] construct a six-element feature vector $LS_i(d_{i0}, d_{i1}, \theta_{i0}, \theta_{i1}, \emptyset_{i0}, \emptyset_{i1})$, where d_{i0} and d_{i1} are the Euclid distances between M_i and its neighbors, θ_{i0} and θ_{i1} are the orientation difference between M_i and line segment M_iN_0 and M_iN_1, respectively, $\emptyset_{i0}$ and $\emptyset_{i1}$ are the orientation between M_i and its neighbors. The value range of $\theta_{i0}, \theta_{i1}, \emptyset_{i0}$ and $\emptyset_{i1}$ is $[0, \pi)$. Note that the two nearest neighbors N_0 and N_1 are not ordered by their Euclid distance to M_i but by satisfying the equation:

$$|\overrightarrow{N_0M_i} \times \overrightarrow{N_1M_i}| \geq 0, \qquad \textbf{(16)}$$

where ‘‘ × ’’ denotes the cross product operation. While satisfying Eq. (1), N_0 is the first neighbor and N_1 is the second.

This arrange method decreases the chance of flipping the order of the neighboring minutiae.

Suppose LS_Q^i is the local structure feature vector of minutia I from query fingerprint and LS_T^j of minutia j from template fingerprint, respectively. The similarity measure can be calculated as:

$$sl(i,j) = \begin{cases} \dfrac{bl - W|LS_i^Q - LS_j^T|}{bl} & \text{if } W|LS_i^Q - LS_j^T| < bl, \\ 0 & \text{others,} \end{cases} \qquad \textbf{(17)}$$

Where

$$W = (w_d, w_d, w_\theta, w_\theta, w_\emptyset, w_\emptyset). \qquad \textbf{(18)}$$

Empirically bl equals 6m and m is the dimension of LS_Q^i and LS_T^j.

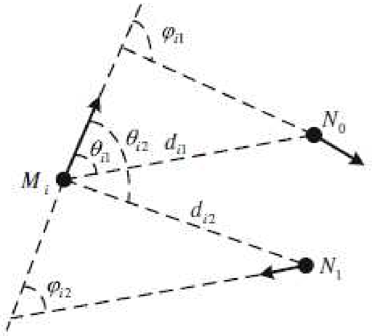

Fig. 1. Local structure of M_i [12]. Where d_{i0} and d_{i1} are the Euclid distances between M_i and its neighbors, θ_{i0} and θ_{i1} are the orientation difference between M_i and line segment M_iN_0 and M_iN_1, respectively, $\emptyset_{i0}$ and $\emptyset_{i1}$ are the orientation between M_i and its neighbors.

4. 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. Fig2 shows the overall method to construct alignment-free cryptosystem.

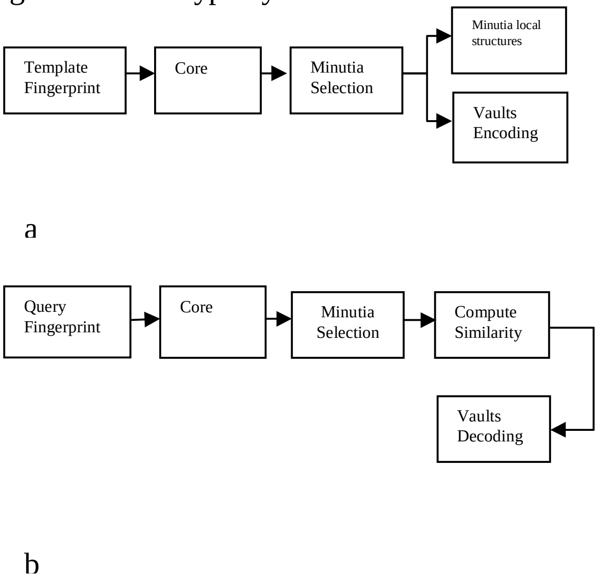

Fig2. Flowchart of proposed alignment-free fingerprint cryptosystem, a) Vaults encoding, b) Vaults decoding

4-1. Alignment-free cryptosystem encoding

Given the template fingerprint image T, the encoding procedure is as follows (see Fig.2a):

(1) Extracting core. At this stage, similar to [13], fingerprint image T is preprocessed and the orientation field is estimated. Afterwards, we calculate all of the possible singular points using Poincare and select the most reliable singular point as the core according to the changing of the orientation field and the ridges around the core.

(2) Selecting minutia. We draw a ring around the reference point by radius R1 and R2, and mark all minutiae M_i^T in the ring. Each M_i^T will define a coordinate system C_i. For each minutiae M_i^T, the minutia local structures MD_i^T are extracted using the method described in section 3.

(3) Constructing fuzzy vaults. Let $L=\{(x_i, y_i, \theta_i, t_i) \mid i= 1,...,n\}$ be a set of real minutia. Minutiae $M_i^T = (x_i^T, y_i^T, \theta_i^T, t_i^T)$ in the ring is selected as the reference minutiae, other minutiae in the set L are rotated and translated. Figure 3 shows the transformation of minutiae. A transformed minutia $M_i^{TT} = (x_i^{TT}, y_i^{TT}, \theta_i^{TT}, t_i^{TT})$ is obtained as follows:

$$\begin{bmatrix} x_i^{TT} \\ y_i^{TT} \\ \theta_i^{TT} \end{bmatrix} = \begin{bmatrix} cos\theta_i^T & -sin\theta_i^T & 0 \\ sin\theta_i^T & cos\theta_i^T & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_i^{TT} - x_i^T \\ -(y_i^{TT} - y_i^T) \\ \theta_i^{TT} - \theta_i^T \end{bmatrix} \quad and\ t_i^{TT} = t_i^T \qquad \textbf{(19)}$$

With a set of transformed minutiae, a fuzzy vault v_i is encoded with the method which described in section 2-1. Another minutiae M_j^T in the ring is selected as the reference minutia, and a new fuzzy vault Vj is encoded. Encoding of fuzzy vaults is repeating for whole minutia inside the ring. The set of pairs $\mathrm{MV}^{\mathrm{T}} = \{(\mathrm{MD}_{\mathrm{i}}^{\mathrm{T}}, \mathrm{V}_{\mathrm{i}})\}_{i=1}^{r}$become the public information for the overall alignment-free cryptosystem.

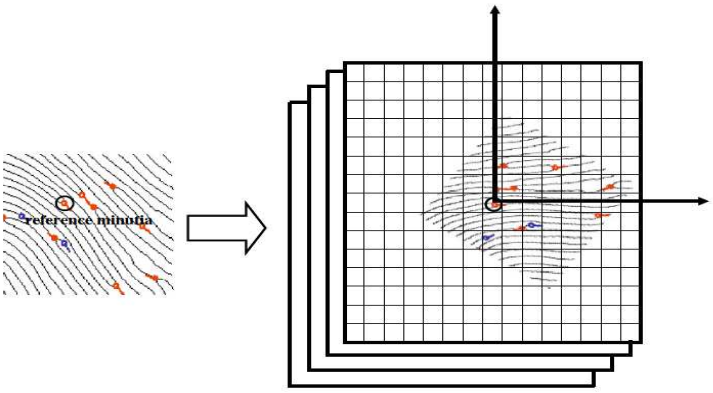

Fig. 3. The transformation of minutiae using a reference point.

4-2. Alignment-free cryptosystem decoding

Given the query fingerprint image Q, the decoding procedure is as follows (see Fig. 2b):

(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 reference point by radiuses R1 and R2 and mark all minutiae M_i^Q in the ring (radiuses R1 and R2 are the same as the ring radiuses at the encoding procedure). For each minutia M_i^Q, the minutia local structures $\mathrm{MD}_{\mathrm{i}}^{\mathrm{Q}}$ are extracted based on the method described in section 3 to obtain the set of pairs $\mathrm{MV}^{\mathrm{Q}} = \{(M_i^Q, \mathrm{MD}_{\mathrm{i}}^{\mathrm{Q}})\}_{i=1}^{r'}$.

(3) Decoding fuzzy vaults. For the ith minutia M_i^Q inside the set MV^{Q}, its corresponding minutia local structures are $\mathrm{MD}_{\mathrm{i}}^{\mathrm{Q}}$. The similarity measure $\{S_{ij}\}_{j=1}^{r+r'}$ between $\mathrm{MD}_{\mathrm{i}}^{\mathrm{Q}}$ and the first elements in MV^{T} (i.e. $\mathrm{MD}_{\mathrm{j}}^{\mathrm{T}}, 1 \leq \mathrm{j} \leq \mathrm{r}$) is computed by equation 20. If S_{ij} satisfy the following condition:

$$S_{ij} \geq T_m, \qquad \textbf{(20)}$$

Where T_m is threshold, thus we can say M_i^Q has a reliable counterpart M_j^T in the template fingerprint. So with minutiae M_i^Q as the reference minutia, other minutiae are rotated and translated with equation 19. Decoding of vault V_{j} in MV^{T} (corresponding to MD_j^Q) is checked by using method which described in 2-2. If V_{j} is not decoded, another minutia inside the set MV^{Q} is selected as the reference minutiae and this step repeats until whole minutia inside the set MV^{Q} are selected. If at least one of the vaults decoded successfully, the secret will be recovered.

5- Experimental result

In the experiments, we use two databases to validate the proposed algorithm: The FVC2002 databases, DB1 and DB2. The images of FVC2002 DB1 database have been extracted by the optical sensor Touch View II, with resolution of 500 dpi. Also, the images of FVC2002 DB2 database have been extracted by the optical sensor FX2000, with resolution of 569 dpi. Both of them include 800(100 × 8) fingerprint images.

Table 1 shows experimental results on DB2. As shown in this table, the two columns are the degree of the polynomial used in the encoding. More degree means more security in reconstruction of the polynomial. We evaluate the performance of the algorithm by GAR[2] and FAR[3], where GAR is genuine accept rate, and FAR is false accept rate.

Table 1. Experimental results on FVC2002 DB2. N shows the degree of polynomial

	N=8		*N=9*	
	GAR%	*FAR%*	*GAR%*	*FAR%*
Proposed algorithm	91	0.02	90	0.0
Product rule[12]	83	0.1	79.8	0,05
sum rule[12]	87.2	0.19	84.3	0.1

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

Table 2. Experimental results on FVC2002 DB1. N shows the degree of polynomial.

	N=8		*N=9*	
	GAR%	*FAR%*	*GAR%*	*FAR%*
Proposed algorithm	85	0.01	84	0.0
Product rule[12]	77.3	0.2	73.5	0.12
sum rule[12]	79.2	0.2	76.3	0.12

6- Conclusion

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

In this paper, we propose an alignment-free fuzzy vault for fingerprint to overcome alignment difficulty in previous fuzzy vault fingerprint.

To construct fuzzy vaults, we extract a rotation and translation invariant feature (i.e. minutia local structures) for each minutia inside the ring surrounds the core. Then, with respect to coordinate system which every minutia inside the ring defined it, fuzzy vaults are constructed. The minutia local structures and its corresponding fuzzy vault stored in database. In decoding, we extract minutia local structures for each minutia inside the ring surrounds the core. Each extracted minutia local structures are compared with each minutia local structures stored in database. If similarity between two minutia local structures is greater than a threshold, then coordinate system corresponding to minutia that defined in query fingerprint is checked by corresponding vaults stored in the database which is decoded or not. If at least one of the vaults is decoded successfully, the secret will be recovered. Experimental results show the effectiveness of the proposed algorithm.

References

[1] Ross A, Shah J, Jain AK. "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] Nanni L, Lumini A. "Descriptors for image-based fingerprint matchers". Expert Systems with Applications, pp.12414–22, 2009.

[2] Genuine accept rate

[3] False accept rate

[3] Ang R, Safavi-Naini R, McAven L. "Cancelable key-based fingerprint templates". In Information security and privacy: 10th Australasian conference (ACISP2005), pp. 242–52, 2005.

[4] Ratha NK, Chikkerur S, Connell JH, Bolle RM. "Generating cancelable fingerprint templates". IEEE Transactions on Pattern Analysis and Machine Intelligence, Special Issue on Biometrics, pp.561–72, 2007.

[5] Lee C, Choi J, Toh K, Lee S, Kim J. "Alignment-free cancelable fingerprint templates based on local minutiae information". IEEE Transactions on Systems, Man and Cybernetics, pp. 980–92, 2007.

[6] Juels A, Sundan M. "A fuzzy vault scheme". In Proceedings of the IEEE international symposium on information theory, Lausanne, switzerland, 2002.

[7] Uludag U, Pankanti S, Jain A. "Fuzzy vault for fingerprints". In Proceedings of 5th international conference on audio and video based biometric person authentication, pp. 310–9, 2005.

[8] Nandakumar K, Jain A, Pankanti S. "Fingerprint-based fuzzy vault: implementation and performance". IEEE Transactions on Information Forensics and Security, pp.744–57, 2007.

[9] Nagar A, Nandakumar K, Jain A. "Securing fingerprint template: fuzzy vault with minutiae descriptors". In Proceedings of 19th international conference on pattern recognition, ICPR 2008, pp. 1–4, 2008.

[10] Li J, Yang X, Tian J, Shi P, Li P. "Topological structure-based alignment for fingerprint fuzzy vault". In Proceedings of 19th international conference on pattern recognition, ICPR2008, pp. 1–4. 2008.

[11] Li P, Yang X, Cao K, Shi P, Tian J. "Security-enhanced fuzzy fingerprint vault based on minutiae's local ridge information". In Proceedings of the 3rd international conference of biometrics, ICB'09, pp. 930–9. 2009.

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

[13] X. Luo, J. Tian, and Y. Wu. "A minutia matching algorithm in fingerprint verification". ICPR2000, pp. 833–836, 2000.