A Hierarchical Fingerprint Alignment Method and Its Application to Fuzzy Vault

Peng Li[a†], Xin Yang[a†], Yali Zang[a], Kai Cao[a] and Jie Tian[a,b‡]

[a]Institute of Automation, Chinese Academy of Sciences, Beijing, China;
[b]School of Life Science and Technology, Xidian University, Xi'an, Shaanxi, China

ABSTRACT

Fuzzy vault is a practical and promising scheme, which can protect biometric templates and perform secure key management simultaneously. Aligning the query sample and the template sample in the encrypted domain remains a challenging task in the fingerprint-based fuzzy vault scheme. To some extent, all the existing fingerprint aligning methods in the encrypted domain have their own drawbacks, e.g., not enough alignment accuracy or information leakage because of publishing helper data. In this paper, a novel fingerprint aligning method is proposed, which integrates the fingerprint reference points and its neighboring region of interest(ROI) in a hierarchical manner. The concept of mutual information(MI) in the information theory is used to assess the coincidence extent of two fingerprints after being aligned. The novel alignment method is applied to fingerprint-based fuzzy vault implementation. Out of information leakage consideration, the orientation features of fingerprint minutiae are discarded and another distinguishing local feature, inter-minutiae ridge count, is used to replace the minutiae orientation in the implementation of fingerprint-based fuzzy vault. Experiment on FVC2002 DB2a is conducted to show the virtue of proposed alignment method and the promising performance of proposed fingerprint-based fuzzy vault implementation.

Keywords: Fingerprint alignment, OFROI, Mutual information, Ridge count, Fuzzy vault

1. INTRODUCTION

With large-scale application of biometric authentication systems, the security and privacy issues involved in the raw storage of biometric templates is brought to the forefront. People worry about that their biometric information is abused and hence their personal interest is threaten. And some biometric modalities may leak the user's privacy, for instance, retina or iris can tell some eye diseases, which the user may not want to let others know. Once this problem is well solved, the social acceptance for the biometric authentication systems will be gained more and it is beneficial to popularize biometric technology in the commercial and civilian environment. Therefore, many emerging technologies, called biometric cryptosystem or biometric encryption, tend to solve the template protection issue. Ref.[1] is a good survey paper for this topic.

Many previous works have been done in the biometric cryptosystem field. Fuzzy commitment scheme[2] is a pioneer theory contribution to combine cryptography and biometrics in the sense of Hamming measure. Hao et al.[3] applied fuzzy commitment to iris pattern and derived 140-bit length keys from iris images at FRR=0.47% and FAR=0%. Soutar et al.[4] proposed to bind a private key with a fingerprint by Fourier Transform and derive it while the fingerprint identification succeeds. Juels et al.[2] proposed a cryptographic primitive, called fuzzy vault, to deal with the unordered set of noisy data. Dodis et al.[5] generalized most of previous methods and gave a theoretical framework of generating robust key from biometric data and analyzed the security in the information theory sense. Many other researches[6–12] also concentrated on generating a key from biometric data. However, there are not encouraging experimental results reported in these literatures because of some implementation difficulties.

†These authors contribute equally to the work.
‡Further author information: (Send correspondence to Dr. Tian)
Dr. Tian: E-mail: tian@ieee.org, Telephone: 86-10-82618465, Fax: 86-10-62527995

Biometric Technology for Human Identification VII, edited by B. V. K. Vijaya Kumar, Salil Prabhakar, Arun A. Ross,
Proc. of SPIE Vol. 7667, 76670E · © 2010 SPIE · CCC code: 0277-786X/10/$18 · doi: 10.1117/12.849860

In this paper, we focus on a relatively practical and promising biometric cryptosystem, called fuzzy vault,[13] which can protect users' biometric data and cryptographic key simultaneously. Fuzzy vault consists of encoding and decoding phases. Suppose a user wants to hide a cryptographic key K into his/her biometric sample, which can be represented as an unordered set X. In the encoding phase, the user employs a polynomial's coefficients to encode K, and evaluates the polynomial P on all the elements in X to obtain $(X, P(X))$. Then a large number of chaff points, which do not lie on P, i.e., $(Y, Z), Z \neq P(Y)$, are added to constitute the vault V along with the points lying on P. In the decoding phase, if the user wants to retrieve K from V, he/she must presents another biometric sample X'. If X and X' overlaps substantially(i.e., the number of the elements both in X and X' exceeds P's degree n), P can be reconstructed using error correction scheme to decode K. If there are not enough elements to reconstruct the polynomial, the identification is claimed unsuccessful.

In the implementation of fuzzy vault, especially minutiae-based fuzzy fingerprint vault, the alignment phase is a necessary and important phase to lower the intra-class difference and hence decode the vault successfully. However, not like the alignment phase in the traditional biometric authentication system, the alignment in the fuzzy vault implementation must be performed in the encrypted domain. That is to say, the feature used for constructing the vault can not be used to align the biometric samples. For minutiae-based fuzzy fingerprint vault, the minutiae themselves can not be used for alignment and we must look for other features(e.g., singular points and high curvature points), called **auxiliary feature**, to align the query sample and the template sample. However, the alignment accuracy level using singular points or high curvature points is much lower than using minutiae themselves, thus the automatic alignment in the encrypted domain may cause more False Reject(FR) instances. In addition, the feature used for computing alignment parameters(e.g., high curvature points) may leak some information about the vault. In this paper, we extract the fingerprint's reference point and the orientation field ROI(OFROI) centering on it as the auxiliary feature, which is easy to be obtained. A novel hierarchical method is proposed to perform the alignment procedure based on mutual information search. While constructing the vault, the minutiae's orientation features are discarded considering that the auxiliary feature may leak the global orientation information and help recognizing the real minutiae from all the vault points. Alternatively, another local feature in fingerprint representation, inter-minutiae ridge count, is adopted to replace the minutiae's orientation features when implementing the minutiae-based fuzzy fingerprint vault. Thus the auxiliary feature has nothing with the feature used to construct the vault(i.e., the minutiae and the inter-minutiae ridge counts) and it will not leak any information about the concealed minutiae features.

The rest of the paper is structured as follows: Section 2 introduces the related works about the biometric cryptosystem and the alignment methods for fuzzy fingerprint vault in the last years; Mutual information based hierarchical fingerprint alignment method is proposed and elaborated in section 3; Section 4 describes our proposed fuzzy fingerprint vault implementation which adapts to the mutual information based alignment method; The experimental result on FVC2002 DB2a is given in section 5 and we draw the conclusion in section 6.

2. RELATED WORKS

Fuzzy vault, proposed by Juels and Sudan,[13] is a smart biometric cryptosystem operating in key binding mode, which is based on Shamir's Secret Sharing Scheme.[14] Fingerprint modality particularly suits fuzzy vault scheme, because it requires unordered feature set and fingerprints' minutiae exactly satisfy this demand. So most practical fuzzy vault schemes are implemented with fingerprints,[15–21] except some implementations with other modalities, for instance iris,[22] face[23] and handwritten signatures.[24] In all present fuzzy vault implementations with fingerprints, alignment is an important procedure to lower the intra-user variation. Clancy et al.[15] conducted external pre-alignment and Uludag et al.[18] expert manual alignment. But pre-alignment only can be used for experimental study, not for practical application. Yang et al.[16,17] performs automatic alignment by storing the reference minutia local structure. The stored reference minutia local structure may leak the information about the minutiae through exhaustive search. And the specific minutia local structure corresponding to the stored one may not be captured in the input fingerprint. They reported the result of $GAR = 83\%$ on a small database with 10×10 fingerprints. Chung et al.[25] proposed an alignment method based on geometric hashing table. In their method, the selection of the first minutia(i.e., the reference minutia) is important and the alignment result may be affected by the spurious minutia and the minutiae without being detected. The alignment time they reported is $1.3s$ implemented with C++. Moon et al.[26] employed the alignment method proposed by Chung

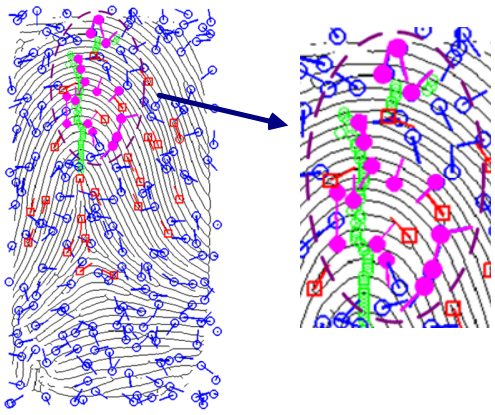

Figure 1. High curvature points can help recognize chaff points. Green hollow circles without segments represent high curvature points,[20] and all the other points, each one with a short line segment denoting its orientation, construct the whole vault. In the area near the high curvature points, i.e., the area enclosed by the purple elliptic curve, the solid pink circles can be easily recognized as chaff points because their orientations are apparently different from the orientations field estimated by the high curvature points. The red hollow squares in the elliptic curve denote the real minutiae.

et al.[25] to construct an fuzzy fingerprint vault system with automatic alignment. The experimental result they reported is $GAR = 88\%(FAR = 0)$ on an in-house optical fingerprint database with $400 \times 4 = 1600$ fingerprints. Jeffers et al.[27] proposed the alignment method based three kinds of minutia structure(five nearest neighbor structure, Voronoi neighbors and triangle based structures). Their method is not suitable to the fuzzy vault scheme with chaff points, because the minutiae structures may act as a filter to identify true points among the random-generated chaff points. However, the constructions of PinSketch and improved fuzzy vault[5] do not involve the chaff points and the alignment method proposed by Jeffers et al.[27] may suit to them. But the authors did not give the implementation with the proposed alignment method. In all existing literatures, the alignment method used by Uludag et al.,[19] Nandakumar et al.[20] and Nagar et al.,[21] which is based on high curvature points near the fingerprint's core points, is the most practical and effective one. However, the feature used for computing alignment parameters(i.e., high curvature points) may leak some information about the vault. The smart attackers can easily exclude some chaff points near the high curvature points from the vault by comparing their orientation, as shown in Figure 1. So the security level may decrease because there are less chaff points in the vault and it will cost the smart attacker less time to compute the correct polynomial coefficients. In addition, it is difficult to extract the high curvature points because it depends on the orientation flow curves. Li et al.[28] proposed an alignment method based on the fingerprint reference point's neighboring topological structure. They trace the thinned ridges from the minutiae in the circle centering on the fingerprint's reference point and stop after certain pixels. Then a perpendicular line is made to the stopping point's orientation and crosses with another thinned ridge. The cross points are recorded as the auxiliary features. The tracing procedure is assumed to be irreversible. The same problem exists in this method, because the orientation of the region near the auxiliary points can be estimated and used to filter out some chaff points.

3. MUTUAL INFORMATION BASED HIERARCHICAL FINGERPRINT ALIGNMENT METHOD

The idea of aligning two fingerprints by maximizing the mutual information of two orientation fields is first proposed by Liu et al.[29] Their algorithm employs the whole orientation field and searches the whole 3-D space of X, Y and Θ for the optimal alignment parameters. Apparently, it is a time-consuming task and not suitable for real time fingerprint matching. In this paper, we import the fingerprint's reference point to perform the coarse alignment. Then the orientation field ROI(OFROI) centering the reference point is extracted to perform the fine alignment by maximizing the mutual information of template OFROI and query OFROI.

3.1 Entropy and Mutual Information

Entropy is a statistical concept, often used in information theory, which reflects the variable's randomness. Given discrete random variable $X = \{x_i, i = 1, 2, \cdots, n\}$ and let $P(x_i)$ represent the probability of the element x_i. The entropy of discrete random variable X is defined as:

$$H(X) = -\sum_{i=1}^{n} P(x_i) \log P(x_i). \tag{1}$$

For two correlative random variables $X = \{x_i, i = 1, 2, \cdots, n\}$ and $Y = \{y_i, i = 1, 2, \cdots, m\}$, the conditional entropy and joint entropy are defined as:

$$H(X|Y) = -\sum_{i=1}^{n}\sum_{j=1}^{m} P(x_i, y_j) \log P(x_i|y_j), \tag{2}$$

and

$$H(X, Y) = -\sum_{i=1}^{n}\sum_{j=1}^{m} P(x_i, y_j) \log P(x_i, y_j), \tag{3}$$

where $P(x_i, y_j)$ and $P(x_i|y_j)$ represent the joint probability and the conditional probability respectively.

Mutual information $I(X;Y)$ between X and Y is defined as:

$$\begin{aligned} I(X;Y) &= H(X) - H(X|Y) = H(Y) - H(Y|X) \\ &= H(X) + H(Y) - H(X, Y). \end{aligned} \tag{4}$$

The measure of mutual information $I(X;Y)$ reflects that the appearance of Y decreases the entropy of X, or the appearance of X decreases the entropy of Y, equivalently. As done in Ref.,[29] we use normalized mutual information I_N to evaluate the fingerprint alignment accuracy. I_N is defined as:

$$I_N(X;Y) = \frac{H(X) + H(Y)}{H(X, Y)}. \tag{5}$$

3.2 Reference Point Location and OFROI Extraction

In Liu et al.,[29] the orientation fields of two fingerprints from the same finger are used to compute the maximum mutual information. The usage of the whole orientation and the search of the whole parameter space are both time-consuming tasks. Our alignment idea is inspired by Liu et al.[29]'s method, but we will first employ the fingerprint reference point to conduct coarse alignment to restrict the search space of parameters and then use the OFROI to perform fine alignment to obtain the final alignment parameters.

The complex filter technology[30] is used to locate the fingerprint singular points. It uses complex filters of first order symmetry, i.e., $h_1(x, y) = (x + jy)g_\sigma(x, y)$ and $h_1(x, y) = (x - jy)g_\sigma(x, y)$ to detect core and delta points, respectively, where g_σ denotes a 2-D Gaussian with standard deviation σ in the x and y direction. The complex filter technology can provide not only the position but also orientation of a singular point. The post-processing operations, proposed in Cao et al.,[31] are used to remove the false singular points. Only one singular point(usually the core point) is left as the reference point of fingerprint images. For the fingerprints of arch type, the point of maximum curvature in concave or convex ridges (MC point) is used as the reference point. The MC point detection method in Cao et al.[31] is also employed here. The direction of MC points are defined as the perpendicular direction to the value of ridge orientation field at the MC points' location. Some examples of core points and MC points are illustrated in Figure 2.

After the fingerprint reference point is determined, the orientation field ROI(OFROI) is extracted from the fingerprint block(8×8) orientation field image. As shown in the Figure 3, the region, defined by two concentric

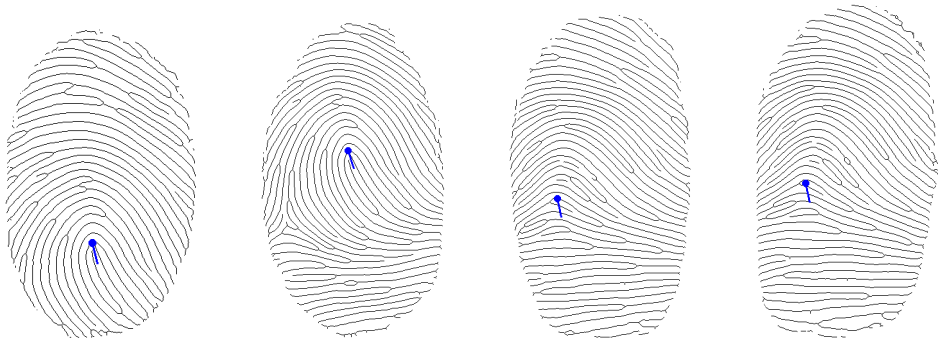

Figure 2. Some examples of reference point detection in thinned fingerprint images. (a)&(b) Core points; (c)&(d) MC points. The line segments denote the directions.

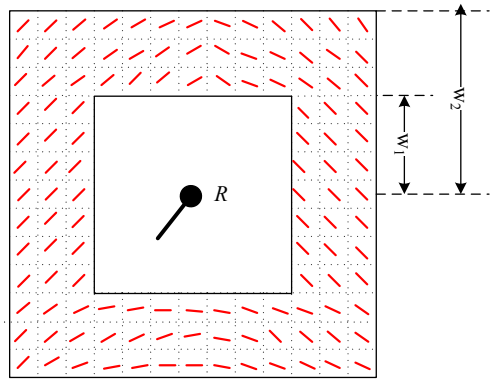

Figure 3. OFROI extraction illustration. R denotes the fingerprint reference point. w_1 and w_2 denote the inner square radius and outside square radius, respectively. The red line segment denotes the 8×8 block orientation value.

squares of radius w_1 and w_2(two empirical values) and with the reference point as the center, i.e., the blocks within a red line segment, are the ROI. The reason of excavating the inner square region of radius w_1 is that the orientation field near the fingerprint reference point is confused usually and not suitable to compute the mutual information. We compute the average orientation values on the 8×8 blocks of the ROI, called OFROI. Then the fingerprint reference point's location and direction, coupled with all the OFROI orientation values, are stored. In the verification phase, the reference point and OFROI of query fingerprint image are extracted and used to obtain the alignment parameter by maximizing the mutual information of stored template OFROI and query OFROI.

Given two OFROIs OF^T and OF^Q, the mutual information $I_N(T;Q)$ between them can be calculated based on the theory described in Subsection 3.1. The detailed calculation method can be found in Liu et al.[29] The value range of $I_N(T;Q)$ is $[0, 2]$.

3.3 Hierarchical Alignment Procedure

In this paper, the alignment is the process to search the optimal rigid transformation paramete $P = (\Delta x, \Delta y, \Delta\theta)$, which can be used to overlap the most entries of the template OFROI and query OFROI. Let T denote the template fingerprint image and Q the query one. The procedures of proposed hierarchical alignment method are described as follows:

- Read the reference point information $R^T(x_R^T, y_R^T, \theta_R^T)$ and OFROI $OF^T = \{O_{ij}^T, i, j \in ROI^T\}$ of the template fingerprint from the stored vault data.
- Extract the reference point of query fingerprint, including the location and the direction, denoted as $R^Q(x_R^Q, y_R^Q, \theta_R^Q)$.

- Initialize the alignment parameter as $P' = (x_R^Q - x_R^T, y_R^Q - y_R^T, \theta_R^Q - \theta_R^T)$. Transform the query fingerprint image Q into Q' according to P'. Extract the OFROI $OF^{Q'} = \{O_{ij}^{Q'}, i,j \in ROI^{Q'}\}$ using the method described in Subsection 3.2.
- Set a mutual information threshold M_{th}. Calculate the mutual information $I_N(T;Q')$ between OF^T and $OF^{Q'}$. If $I_N(T,Q') > M_{th}$, the alignment accuracy is enough and the final alignment parameter $P = P'$. Else go to the next step.
- This is the coarse search step. If the reference point is a core point, set $[-l_c, l_c]$ as the coarse search range of the location and $[-d_c, d_c]$ of the direction. If the reference point is a MC point, set $[-l_m, l_m]$ as the coarse search range of the location and $[-d_m, d_m]$ of the direction. The coarse search steps of the location and the direction are set s_{lc} and s_{dc}, respectively. It is worth noting that $l_c < l_m$ and $d_c < d_m$, because the location and direction of core points are usually more accurate than MC points. Assume the maximum mutual information is obtained on the search point $(\Delta x_c, \Delta y_c, \Delta\theta_c)$, where $\{\Delta x_c \in [-l_c, l_c], \Delta y_c \in [-l_c, l_c], \Delta\theta_c \in [-d_c, d_c]\}$ or $\{\Delta x_c \in [-l_m, l_m], \Delta y_c \in [-l_m, l_m], \Delta\theta_c \in [-d_m, d_m]\}$. Now the alignment parameter becomes $P'' = (x_R^Q - x_R^T + \Delta x_c, y_R^Q - y_R^T + \Delta y_c, \theta_R^Q - \theta_R^T + \Delta\theta_c)$. Then go to the fine search step.
- This is the fine search step. Here it is not necessary to differentiate between core points and MC points. Set $[-l_f, l_f]$ as the fine search range of the location and $[-d_f, d_f]$ of the direction. The fine search steps of the location and the direction are set s_{lf} and s_{df}, respectively. Assume the maximum mutual information is obtained on the search point $(\Delta x_f, \Delta y_f, \Delta\theta_f)$, where $\Delta x_f \in [-l_f, l_f], \Delta y_f \in [-l_f, l_f], \Delta\theta_f \in [-d_f, d_f]$. Now the alignment parameter becomes $P''' = (x_R^Q - x_R^T + \Delta x_c + \Delta x_f, y_R^Q - y_R^T + \Delta y_c + \Delta y_f, \theta_R^Q - \theta_R^T + \Delta\theta_c + \Delta\theta_f)$.
- The final alignment parameter $P(\Delta x, \Delta y, \Delta\theta) = P'''$.

Let $(x_m^Q, y_m^Q, \theta_m^Q)$ denote an original query minutia. The aligned minutia can be calculated by:

$$\begin{bmatrix} x_m^{Q'} \\ y_m^{Q'} \end{bmatrix} = \begin{bmatrix} cos(\Delta\theta) & sin(\Delta\theta) \\ -sin(\Delta\theta) & cos(\Delta\theta) \end{bmatrix} \begin{bmatrix} x_m^Q + \Delta x \\ y_m^Q + \Delta y \end{bmatrix} \quad \theta_m^{Q'} = \theta_m^Q + \Delta\theta \tag{6}$$

where, $(x_m^{Q'}, y_m^{Q'}, \theta_m^{Q'})$ denotes the transformed minutia according to the alignment parameter. Some examples of hierarchical alignment results are illustrated in Figure 4.

4. PROPOSED FINGERPRINT-BASED FUZZY VAULT IMPLEMENTATION

A practical implementation of fingerprint-based fuzzy vault scheme is developed based on the proposed hierarchical alignment method. The specific implementation details are described as follows.

4.1 Inter-minutiae Ridge Count

As a local feature, inter-minutiae ridge count has been typically used in forensic matching because of the difficulty of human experts to work in the Euclidean space.[32] As we use much orientation information of the fingerprint image to perform alignment, the orientation of the fingerprint minutiae is discarded in the implementation in order to protect the chaff points from being filtered according to the orientation information. Alternatively, we employ the inter-minutiae ridge counts of the nearest three minutiae to replace the minutiae orientation. On one hand, it can improve the distinguishing ability of minutiae feature; on the other hand, the space of selecting chaff points is augmented and the system security is also enhanced. The binarized fingerprint image is utilized to count the number of ridges between two minutiae. An example is illustrated in Figure 5. Note that the ridge count between two minutiae has nothing with the Euclidean distance between them. For example, in Figure 5, $r_2 > r_3$, but the corresponding Euclidean distances d_2 and d_1 hold the relation of $d_2 < d_1$. Therefore, in the construction of fuzzy vault, the ridge count feature can hide the information better than inter-minutiae Euclidean distance feature. The latter may be vulnerable to filtering real minutiae by exhaustively searching around a specific minutia if used for constructing fuzzy vault.

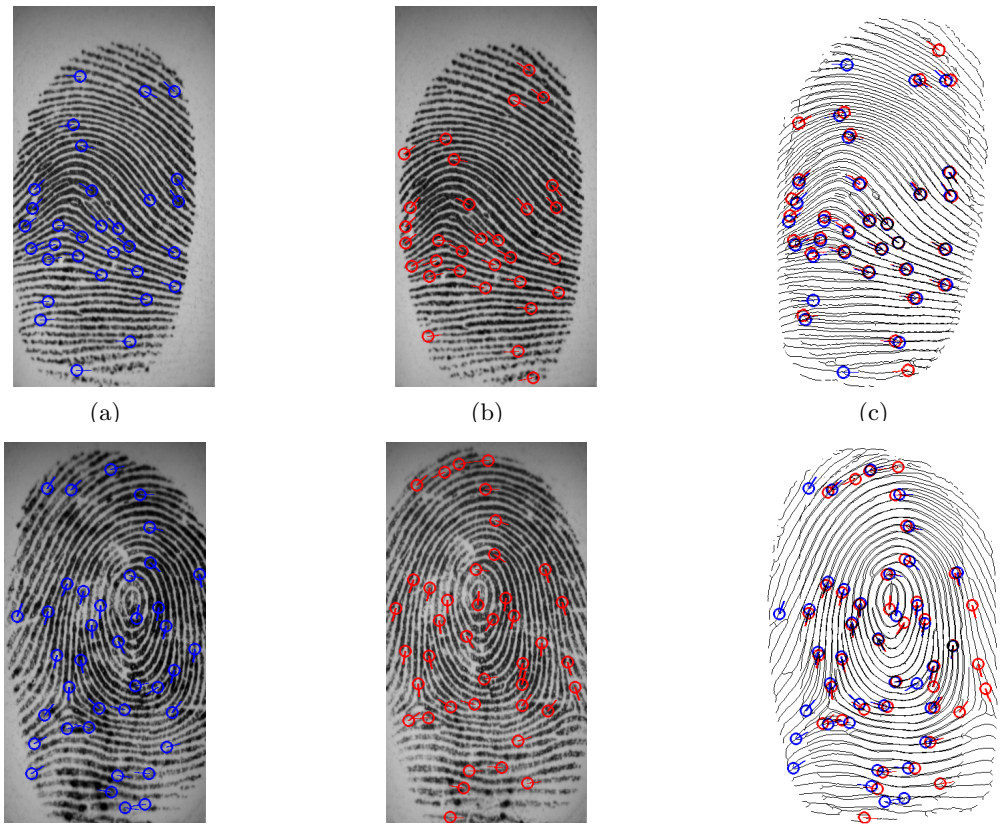

Figure 4. (a)&(b) Two fingerprint samples of arch type(MC point) from the same finger. (c) The alignment result of (a) and (b). Two fingerprint samples of whorl type(core point). (f) The alignment result of (d) and (e).

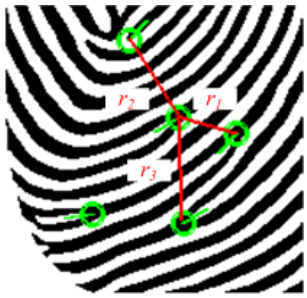

Figure 5. The inter-minutiae ridge counts of the nearest minutia, $r_1 = 1$, $r_2 = 4$, $r_3 = 3$. They are ordered by the Euclidean distance.

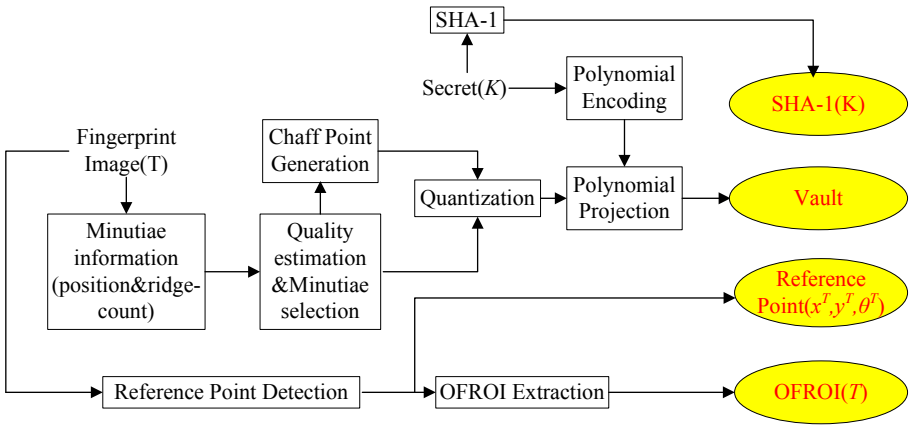

Figure 6. The encoding flowchart of proposed fingerprint-based fuzzy vault implementation. The items with yellow ellipse background need to be stored as the helper data.

4.2 Encoding

The encoding phase of proposed fingerprint-based fuzzy vault implementation is shown in Figure 6. In the encoding phase, the input fingerprint image is preprocessed and all the minutiae are detected. The reference point and OFROI are extracted by using the method described in subsection 3.2 and stored as parts of the helper data. At the same time, the minutiae's corresponding local image quality indexes are estimated using method proposed by Chen et al.[33] The top-ranking and well-separated 20-40 minutiae are selected according to the local image quality. As explained in subsection 4.1, the orientation features of the minutiae are discarded and the ridge counts of the nearest three minutiae to the specific minutia are utilized to construct the fuzzy vault. Let $M = \{m_i^T(x_i^T, y_i^T, r_i^{T1}, r_i^{T2}, r_i^{T3}), i = 1, 2, \cdots, r\}$ denote the feature corresponding to the i-th minutia, where $r_i^n (n = 1, 2, 3)$ usually is within the range of $[0, 8]$. The distance between two minutiae is defined as follow:

$$D(m_i, m_j) = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2 + \lambda \sum_{n=1,2,3} (r_i^n - r_j^n)^2} \tag{7}$$

where, $m_i(x_i, y_i, r_i^1, r_i^2, r_i^3)$ and $m_j(x_j, y_j, r_j^1, r_j^2, r_j^3)$ represent two minutiae features, and λ is an empirical parameter within $[5, 10]$. The minutiae attributes x, y and $r_i^n (n = 1, 2, 3)$ are quantized and represented as bit strings of length 10, 10 and 4, respectively. So a 32-b number by concatenating the bit strings of all the attributes can be obtained and we use the Galois field $\mathcal{F} = GF(2^{32})$. Let $X = \{x_i, i = 1, 2, \cdots, r\}$ denote the quantized minutiae feature set. The secret K is encoded into a polynomial $\mathcal{P}$ of degree n in $\mathcal{F}$ by partitioning it into $(n + 1)$ 32-b values and considering them as coefficients of $\mathcal{P}$ (i.e., $\mathcal{P} = c_n x^n + \cdots + c_0$). The polynomial $\mathcal{P}$ is evaluated on all of the quantized minutiae bit strings and to obtain the set $\mathcal{P}(X) = \{\mathcal{P}(x_i), i = 1, 2, \cdots, r\}$. The corresponding elements of X and $\mathcal{P}(X)$ form the locking set $R = \{(x_i, \mathcal{P}(x_i))\}_{i=1}^r$. Then a set C of chaff points $\{(y_j, z_j)\}_{j=r+1}^s$ is generated randomly to conceal the real minutiae, where the distance between the bit strings x_i and y_j in the term of Equ.7 is greater than a certain threshold δ, with randomly-selected chaff point locations and r^1, r^2, r^3. Thus the union of R and C, $R \cup C$, constructs the final vault.

4.3 Decoding

The decoding flowchart of proposed fingerprint-based fuzzy vault implementation is shown in Figure 7. In the decoding phase, a query fingerprint image is presented and the same preprocessing procedures as in the encoding phase are performed to obtain the query minutiae set $Y = \{m_i^Q(x_i^Q, y_i^Q, r_i^{Q1}, r_i^{Q2}, r_i^{Q3}), i = 1, 2, \cdots, p\}$, the reference point (x^Q, y^Q, θ^Q) and OFROI(Q). The hierarchical alignment method, described in subsection 3.3, is used to compute the alignment parameter $P(\Delta x, \Delta y, \Delta\theta)$. Then the query minutiae set Y is transformed into the aligned set $Y' = \{m_i^{Q'}(x_i^{Q'}, y_i^{Q'}, r_i^{Q'1}, r_i^{Q'2}, r_i^{Q'3}), i = 1, 2, \cdots, p\}$ by using Equ. 6. Note that the orientations of minutiae are not utilized and the ridge-count attributes remain unchanged, i.e., $r_i^{Qn} = r_i^{Q'n} (n =$

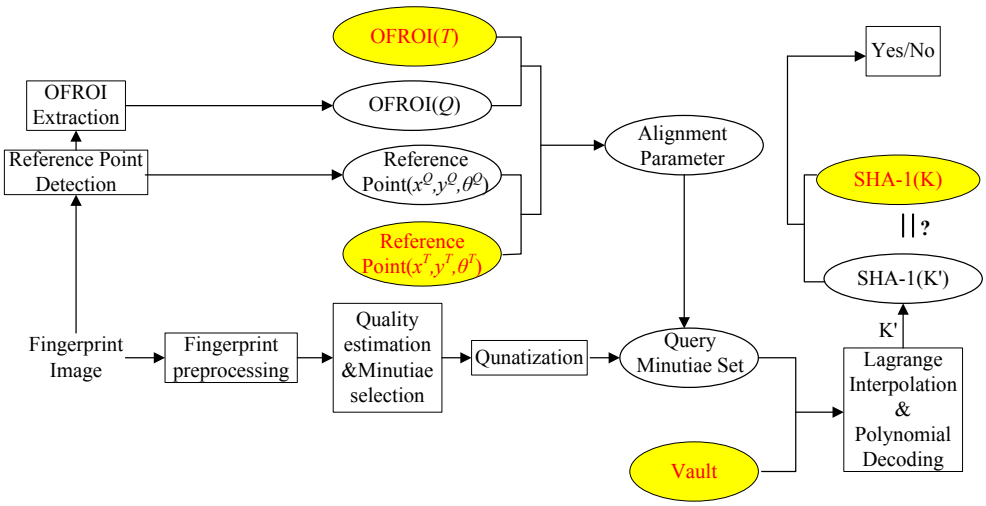

Figure 7. The decoding flowchart of proposed fingerprint-based fuzzy vault implementation. The items with yellow ellipse background are from the stored helper data.

$1, 2, 3$). Afterwards a bounding-box minutiae matcher, as used in Nandakumar et al.,[20] is adopted to search the corresponding minutiae in the vault and obtain an unlock set. Then exhaustive search is performed to get all the combination of $(n+1)$-point in the unlock set. For each combination, Lagrange polynomial interpolation is conducted to obtain the candidate polynomial coefficients and hence the candidate secret K', which is afterwards hashed by SHA-1 algorithm and compared with the stored SHA-1(K) to verify whether $K = K'$. If yes, an accept signal is reported. Or else if none of all the candidate combinations makes SHA-1(K) =SHA-1(K'), a reject signal is given.

5. EXPERIMENTAL RESULTS AND SECURITY ANALYSIS

The first and second samples of each finger in FVC2002 DB2 Set A are selected for experiments because they have less nonlinear transformation than other samples. The first one is used for encoding and the second for decoding. The fingerprint images are captured by Biometrika FX2000 Optical Sensor, and the resultant image size is 296×560 at 569 dpi resolution. In the encoding phase, 660-680 of chaff points can be randomly added into the vault and make the vault size achieves 700 because the 5-dimension minutiae feature $m_i(x_i, y_i, r_i^1, r_i^2, r_i^3)$ augments the space of adding chaff points. In our experiment, we conduct two categories of verification trials, genuine matching and imposter matching. In the genuine matching category, the first sample of each finger is enrolled as template fingerprint and the second one is used as the query fingerprint to decode the vault, thus it leads to 100 trials in all. In the imposter matching category, the first sample of each finger is enrolled as template fingerprint, and the first samples of all the other fingers are used as input fingerprint. Thus the number of resultant imposter trials is $100 \times 99/2 = 4950$. We use two indexes Genuine Accept Rate(GAR) and False Accept Rate(FAR) to measure the performance of proposed fingerprint-based fuzzy vault implementation. The experimental results the their comparison with Nandakumar et al.[20] are reported in Table 1. In Nandakumar et al.,[20] the Failure to Capture Error(FTCR) is counted but not in our implementation.

From Table 1, we can see that proposed implementation outperforms Nandakumar et al.[20] And it is worth noting that, in proposed implementation, the minutiae orientation features are discarded and the risk of filtering the chaff points by estimated orientation field from the auxiliary feature(e.g., high curvature points in Nandakumar et al.[20] and OFROI in proposed implementation) is eliminated. However this kind of risk exists in Nandakumar et al.[20] according to the analysis in Section 2.

We employ the min-entropy method, as adopted in Nagar,[21] to analyze the security of our proposed scheme. Assuming both minutiae location and orientation are uniformly distributed, the min-entropy of minutiae template M^T given the vault V can be computed as

Table 1. Experimental results on FVC2002 DB2 Set A. d denotes the polynomial degree.

		$d=7$	$d=8$	$d=9$	$d=10$
Nandakumar et al.[20]	GAR(%)	91	91	-	86
	FAR(%)	0.13	0.01	-	0
Proposed Implementation	GAR(%)	93	91	89	87
	FAR(%)	1.19	0.42	0.08	0

$$H_\infty(M^T|V) = -log_2\left(\frac{\binom{r}{d+1}}{\binom{r+s}{d+1}}\right), \tag{8}$$

where, r, s and d denote number of minutiae, number of chaff points and polynomial's degree respectively and they are typically 30, 670 and 10, respectively. So the typical security measurement of our proposed scheme is approximately 48 bits.

6. CONCLUSION AND FUTURE WORK

In this paper, an orientation field based hierarchical fingerprint alignment technology is proposed and applied to fingerprint-based fuzzy vault implementation. To adapt to proposed alignment algorithm and improve the security and performance, we employ the inter-minutiae ridge count feature in the construction of fuzzy vault. Experiments conducted on FVC2002 DB2 Set A shows the promising performance of $GAR = 87\%(FAR = 0)$. Meanwhile, the proposed scheme can achieve the security level of 48 bits. In the future work, we will investigate the usage of orientation field model to smooth the OFROI. And more accurate reference point orientation detection method is necessary to narrow the search range in the alignment algorithm and hence to improve the alignment efficiency and accuracy.

7. ACKNOWLEDGEMENT

This paper is supported by the Project of National Natural Science Foundation of China under Grant No. 60875018 and 60621001, National High Technology Research and Development Program of China under Grant No. 2008AA01Z411, Chinese Academy of Sciences Hundred Talents Program, Beijing Natural Science Foundation under Grant No. 4091004, Scientific Databases Program of the Chinese Academy of Sciences during the 11th Five-Year Plan Period under Grant No. INFO-115-C01-SDB4-30.

The authors also thanks the anonymous reviewers for their valuable suggestions.

REFERENCES

[1] Jain, A., Nandakumar, K., and Nagar, A., "Biometric template security," *EURASIP Journal on Advances in Signal Processing* **2008**, 17 Pages (Article ID 579416 2008).

[2] Juels, A. and Wattenberg, M., "A fuzzy commitment scheme," in [*Proc. 6th ACM Conf. Comput. Commun. Secur.*], 28–36, ACM Press (1999).

[3] Hao, F., Anderson, R., and Daugman, J., "Combining crypto with biometrics effectively," *IEEE Transactions on Computers* **55**, 1081–1088 (Sept. 2006).

[4] Soutar, C., Roverge, D., Stojanov, S. A., Gilroy, R., and Kumar, B. V. K. V., "Biometric encryption using image processing," in [*Proc. SPIE-Optical Secur. and Count. Deter. Tech.*], **3314**, 178–188 (1998).

[5] Dodis, Y., Reyzin, L., and Smith, A., "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in [*Advances in Crypology-Eurocrypt*], **3027**, 523–540, Springer-Verlag (2004).

[6] Boyen, X., Dodis, Y., Katz, J., Ostrovsky, R., and Smith, A., "Secure remote authentication using biometric data," in [*In EUROCRYPT*], 147–163, Springer (2005).

[7] Boyen, X., "Reusable cryptographic fuzzy extractors," in [*ACM CCS 2004, ACM*], 82–91, ACM Press (2004).

[8] Buhan, I., Doumen, J., Hartel, P., and Veldhuis, R., "Fuzzy extractors for continuous distributions," in [*Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security (ASIACCS), Singapore*], 353–355, ACM (2007).

[9] Li, Q., Sutcu, Y., and Memon, N., "Secure sketch for biometric templates," in [*In Asiacrypt*], 99–113, Springer-Verlag (2006).

[10] Sutcu, Y., Li, Q., and Memon, N., "Protecting biometric templates with sketch: Theory and practice," *IEEE Transactions on Information Forensics and Security* **2**, 503–512 (Sept. 2007).

[11] Bringer, J., Chabanne, H., Cohen, G., Kindarji, B., and Zemor, G., "Theoretical and practical boundaries of binary secure sketches," *IEEE Transactions on Information Forensics and Security* **3**, 673–683 (Dec. 2008).

[12] Sheng, W., Howells, G., Fairhurst, M., and Deravi, F., "Template-free biometric-key generation by means of fuzzy genetic clustering," *IEEE Transactions on Information Forensics and Security* **3**, 183–191 (June 2008).

[13] Juels, A. and Sudan, M., "A fuzzy vault scheme," in [*IEEE International Symposium on Proceedings of Information Theory*], 408 (2002).

[14] Shamir, A., "How to share a secret," *Commun. ACM.* **22**(11), 612–613 (1979).

[15] Clancy, T. C., Kiyavash, N., and Lin, D. J., "ecure smartcard-based fingerprint authentication," in [*Proceeding of ACMSIGMM 2003 Multimedia, Biometrics Methods and Applications Workshop*], 45–32 (2003).

[16] Yang, S. and Verbauwhede, I., "Secure fuzzy vault based fingerprint verification system," in [*Signals, Systems and Computers, 2004. Conference Record of the Thirty-Eighth Asilomar Conference on*], **1**, 577–581 Vol.1 (Nov. 2004).

[17] Yang, S. and Verbauwhede, I., "Automatic secure fingerprint verification system based on fuzzy vault scheme," in [*Proceedings of 2005 IEEE International Conference on Acoustics, Speech, and Signal. (ICASSP '05).*], **5**, 609–612 (March 2005).

[18] Uludag, U., Pankanti, S., and Jain, A. K., "Fuzzy vault for fingerprints," in [*Proceedings of Fifth International Conference on Audio- and Video-Based Biometric Person Authentication, 2005.*], 310–319 (2005).

[19] Uludag, U. and Jain, A., "Securing fingerprint template: Fuzzy vault with helper data," in [*Proceedings of Internatioanl Conference on Computer Vision and Pattern Recognition Workshop, 2006. CVPRW '06.*], 163–163 (June 2006).

[20] Nandakumar, K., Jain, A., and Pankanti, S., "Fingerprint-based fuzzy vault: Implementation and performance," *IEEE Transactions on Information Forensics and Security* **2**, 744–757 (Dec. 2007).

[21] Nagar, A., Nandakumar, K., and Jain, A., "Securing fingerprint template: Fuzzy vault with minutiae descriptors," in [*Proceedings of 19th International Conferenceon Pattern Recognition, 2008. ICPR 2008.*], 1–4 (Dec. 2008).

[22] Lee, Y. J., Park, K. R., Lee, S. J., Bae, K., and Kim, J., "A new method for generating an invariant iris private key based on the fuzzy vault system," *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics* **38**, 1302–1313 (Oct. 2008).

[23] Wang, Y. and Plataniotis, K., "Fuzzy vault for face based cryptographic key generation," in [*Biometrics Symposium, 2007*], 1–6 (Sept. 2007).

[24] Ortega-Garcia, F.-S. F.-A., aguilar A, J. F., and garcia A, J. O., "Cryptographic key generation using handwritten signature," in [*Proc. Def. Secur. Symp. Biom. Technol. Human Identification*], **6202**, 225–231 (2006).

[25] Chung, Y., Moon, D., Lee, S., Jung, S., Kim, T., and Ahn, D., "Automatic alignment of fingerprint features for fuzzy fingerprint vault," in [*Proceedings of 2005 SKLOIS Conference on Information Security and Cryptology*], 358–369 (2005).

[26] Moon, D., Lee, S., Jung, S., Chung, Y., Park, M., and Yi, O., "Fingerprint template protection using fuzzy vault," in [*Proceedings of ICCSA 2007*], 1141–1151 (2007).

[27] Jeffers, J. and Arakala, A., "Fingerprint alignment for a minutiae-based fuzzy vault," in [*Proceedings of Biometrics Symposium, 2007*], 1–6 (Sept. 2007).

[28] Li, J., Yang, X., Tian, J., Shi, P., and Li, P., "Topological structure-based alignment for fingerprint fuzzy vault," in [*Proceedings of 19th International Conference on Pattern Recognition, 2008. ICPR 2008.*], 1–4 (Dec. 2008).
[29] Liu, L., Jiang, T., Yang, J., and Zhu, C., "Fingerprint registration by maximization of mutual information," *Image Processing, IEEE Transactions on* **15**, 1100–1110 (May 2006).
[30] Nilsson, K. and Bigun, J., "Localization of corresponding points in fingerprints by complex filtering," *Pattern Recognition Letters* **24**(13), 2135 – 2144 (2003).
[31] Cao, K., Yang, X., Tao, X., Zhang, Y., Li, P., and Tian, J., "Minutiae-based fingerprint matching by incorporating global knowledge," *submitted to IEEE Trans. Image Processing* .
[32] Maltoni, D., Maio, D., Jain, A., and Prabhakar, S., [*Handbook of Fingerprint Recognition (Second Edition)*], Springer, London (2009).
[33] Chen, Y., Dass, S., and Jain, A., "Fingerprint quality indices for predicting authentication performance," in [*In: Proc. AVBPA, Springer LNCS-3546*], 160–170 (2005).