A Delaunay Quadrangle-Based Fingerprint Authentication System With Template Protection Using Topology Code for Local Registration and Security Enhancement

Wencheng Yang, Jiankun Hu, and Song Wang

***Abstract*— Although some nice properties of the Delaunay triangle-based structure have been exploited in many fingerprint authentication systems and satisfactory outcomes have been reported, most of these systems operate without template protection. In addition, the feature sets and similarity measures utilized in these systems are not suitable for existing template protection techniques. Moreover, local structural change caused by nonlinear distortion is often not considered adequately in these systems. In this paper, we propose a Delaunay quadrangle-based fingerprint authentication system to deal with nonlinear distortion-induced local structural change that the Delaunay triangle-based structure suffers. Fixed-length and alignment-free feature vectors extracted from Delaunay quadrangles are less sensitive to nonlinear distortion and more discriminative than those from Delaunay triangles and can be applied to existing template protection directly. Furthermore, we propose to construct a unique topology code from each Delaunay quadrangle. Not only can this unique topology code help to carry out accurate local registration under distortion, but it also enhances the security of template data. Experimental results on public databases and security analysis show that the Delaunay quadrangle-based system with topology code can achieve better performance and higher security level than the Delaunay triangle-based system, the Delaunay quadrangle-based system without topology code, and some other similar systems.**

***Index Terms*— Fingerprint, Delaunay triangle, Delaunay quadrangle, topology code, template protection.**

I. Introduction

FINGERPRINT-BASED authentication is one of the most reliable and mature biometric recognition techniques owning to the distinctiveness and stability that fingerprints can provide compared to other biometrics, e.g. iris, palm print or face [1]. The methods used in fingerprint authentication systems can be roughly divided into following two categories: texture-based methods and minutiae-based methods. Generally speaking, minutiae-based methods are more reliable and popular [2]. In minutiae-based algorithms [3]–[5], a fingerprint image is represented by a set of labeled minutiae, which refer to ridge ending and bifurcation. Fingerprint matching with minutiae-based algorithms can be considered as point pattern matching [6].

Although much attention has been given to minutiae-based matching in recent years, fingerprint matching is not an easy task due to the fingerprint uncertainty caused by rotation, translation and nonlinear deformation at each fingerprint image acquisition. In order to mitigate fingerprint uncertainty and improve the recognition rate, the Delaunay triangle-based structure is proposed and studied, leveraging its benefits that the relative position and orientation between each minutia and its neighbours can remain unchanged under rotation, translation and a certain extent of nonlinear distortion in fingerprint images.

A. Delaunay Triangle-Based Structure

The Delaunay triangle-based structure has demonstrated some excellent characteristics [7], [8]. Firstly, it has a good structural stability under random positional disruptions [9]. Each minutia is likely to maintain a similar structure with its neighbouring minutiae under translation, rotation and a small scale change caused by nonlinear distortion. Secondly, missing and spurious minutiae influence the Delaunay triangulation net only locally, which means that under random positional perturbations, some parts of the Delaunay triangulation net can still maintain structural stability [10]. Figure 1(a) shows a set of minutia points and Figure 1(b) gives the Voronoi diagram (thin line) and Delaunay triangulation net (bold line) formed by this minutia point set.

Due to the pleasant properties of the Delaunay triangulation net, a number of methods based on Delaunay triangles have been proposed for minutiae-based fingerprint matching [11]–[18]. In [11], Parziale and Niel proposed an approach that applies the minutia point set to forming a Delaunay triangulation net, and utilizes several rotation, translation unchanged features (e.g., the length of the sides, the

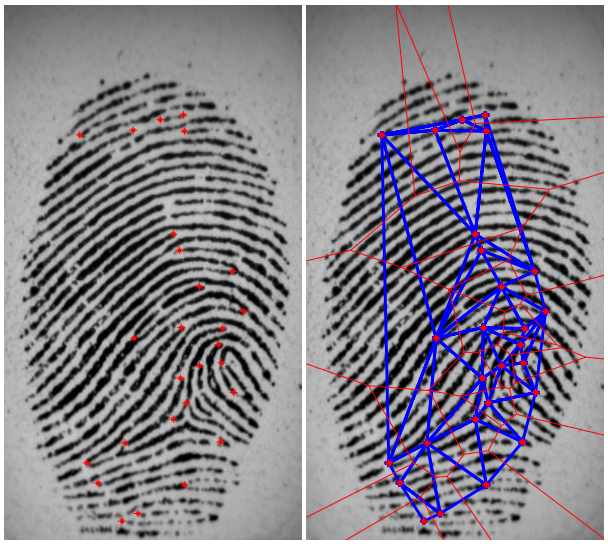
Manuscript received January 7, 2014; revised April 11, 2014; accepted May 20, 2014. Date of publication June 3, 2014; date of current version June 17, 2014. This work was supported by the Australian Research Council under Grant LP100200538 and Grant LP120100595. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Kar-Ann Toh.

W. Yang and J. Hu are with the School of Engineering and Information Technology, University of New South Wales, Canberra, ACT 2600, Australia (e-mail: wencheng.yang@student.adfa.edu.au; j.hu@adfa.edu.au).

S. Wang is with the Department of Electronic Engineering, La Trobe University, Melbourne, VIC 3083, Australia (e-mail: song.wang@latrobe.edu.au).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2014.2328095



(a) (b)

Fig. 1. Examples of (a) Minutiae points, (b) Voronoi diagram (thin line) and Delaunay triangulation net (bold line).

internal angles) of each Delaunay triangle to perform matching between the template and query images. In [12], some possible best-matching edge pairs, instead of best-matching minutiae pairs, are first found in local structure matching, and then a global matching score between two fingerprint images is computed by the triangle matching procedure guided by the aligned-edges. In both [13] and [14], the authors first select some similar minutiae pairs from both template and query images as reference points for alignment. Then fingerprint matching is performed on the aligned feature sets.

In [15], the identification of the Delaunay triangle-based features is carried out first, followed by applying a function named Radial Basis Function (RBF) to aligning the fingerprint image. After that, a global matching is conducted to calculate the matching score between the template and query images with additional information. In [16], triangle candidates which are formed by Delaunay triangulation are obtained and larger local structures (growing regions) are generated by joining several triangles based on the credibility of each triangle candidate. Then a much larger local structure (fusion region) is fused via several growing regions. This step is similar to the procedure proposed in [19] which merges minutiae triangles according to their compatibility in an extended searching step. The matching score [16] is calculated using both the growing region and the fusion region. In this way, fingerprint matching can be accomplished without image pre-alignment.

To account for the problem of missing and spurious minutiae, Uz *et al*. [17] proposed a hierarchical matching based template synthesis approach to combine several enrolment feature sets into a higher quality super-template set. Built upon Delaunay triangulation, the hierarchical matching based algorithm enables higher levels of the hierarchy to correspond to higher quality minutiae and lower levels of the hierarchy to correspond to low and medium quality minutiae. In [18], Soleymani *et al*. combined Delaunay triangulation and Voronoi diagram together to generate a hybrid matching algorithm. The comparison of global topological polygons generated from the boundaries of the Delaunay triangulation net is carried out firstly, and then the central Voronoi cells are compared to calculate the similarity between template and query fingerprint images.

B. Template Protection

Apart from the issue of large variability caused by nonlinear distortion during fingerprint acquisition, template protection is another important issue that needs more attention. In biometric authentication systems, templates are usually stored in a central database at the enrollment stage and compared with queries at the verification stage [20], [21]. However, serious security concerns may arise from the storage of raw template data as biometric traits cannot be replaced or reset. Once they are compromised, they cannot be changed like passwords or tokens. Furthermore, the same template is usually used in different applications, such as banking systems, mobile devices or building entry systems. Template loss in one application means its loss in all other applications [22].

Cancellable biometrics and biometric cryptosystems are two major techniques to provide secure protection to biometric templates. In cancellable biometrics [23]–[30], original template features are transformed into a new format by a non-invertible transformation function during the enrolment stage. The same non-invertible transformation function is applied to query features during the authentication stage, and fingerprint matching is performed between the transformed template and query features rather than between the original features. In such a way, original template features are concealed and protected. For example, in [24] the authors designed cancelable fingerprint templates in the form of binary strings. The proposed binary string representation for fingerprint minutiae avoids the requirement for registration and is computationally infeasible to invert and recover original minutiae data. Ferrara *et al*. [29] proposed a non-invertible minutiae-based template to protect the state-of-the-art minutia descriptor, Minutia Cylinder-Code (MCC), through a non-invertible transform based on dimensionality reduction and binarization. The MCC [31] is a fixed-length local minutia descriptor for fingerprint recognition in the unencrypted domain. The protected MCC (P-MCC) [29] greatly improves the security of the original MCC although the P-MCC cannot be revoked.

One drawback of cancellable biometrics is that it can only provide a matching/non-matching sign. As an alternative to cancellable biometrics, biometric cryptosystems [32]–[34] merge the advantages of both biometrics and cryptosystems. The security level of a biometric cryptosystem is adjustable and the trouble of remembering a long password or carrying a token is avoided. In a biometric cryptosystem, a secret key is either technically bound with the biometric features or directly extracted from the biometric features. Meanwhile, the original biometric template features are encrypted by a secure sketch, e.g. fuzzy commitment [32], fuzzy vault [33] or PinSketch [34], which outputs some helper data. The helper data are generated by an irreversible encryption process so that it is computationally difficult for the adversary to

obtain the original biometric template features from the helper data.

C. Motivation and Contribution

There exist some challenging issues in relation to the Delaunay triangle-based structure and, in general, fingerprint authentication with template protection, among which we list two such issues in the following. The motivation for this research work is to find an effective approach in addressing these issues.

1) The Issue of Feature Set Suitability and Fingerprint Matching With Template Protection Over the Encrypted Domain: In spite of significant improvement in recognition accuracy by using the Delaunay triangle-based structure in the unencrypted domain (without template protection) [11]–[18], (for example, the EERs of the method [18] are reported to be 2.04%, 3.44% and 2.27% for databases FVC2002 DB2, FVC2004 DB3 and FVC2006 DB1, respectively,) fingerprint matching over the encrypted domain (with template protection) remains an open issue for two reasons. Firstly, the feature sets used in the unencrypted domain [11]–[18] are not suitable for currently available template protection techniques, e.g. fuzzy commitment [32], fuzzy vault [33] and PinSketch [34], all of which deal with feature disparity in terms of metrics, such as hamming distance or set difference, and tend to require fixed-length and alignment-free feature descriptors [29]. Secondly, similarity measures are restricted in the encrypted domain. The methods [11]–[18] for measuring feature similarities that work well in the unencrypted domain are inapplicable to the encrypted domain. Some reference features, e.g., best-matching edge pairs [12], reference points [13] and [14], radial basis structure [15], growing regions [16], lower levels of the hierarchy [17] and global topological polygons [18], are acquired or generated in order to assist subsequent matching steps in these methods. However, with template protection, all the features in the original (unprotected) template are encrypted by secure sketches, and hence these reference features are unavailable for access. In other words, fingerprint matching in the encrypted domain cannot make use of the same similarity measures that have been used in the unencrypted domain.

2) Delaunay Triangle-Based Structural Change Under Non-Linear Distortion: None of the aforementioned work [11]–[18] has considered the local Delaunay structural change under elastic distortion. If distortion moves a minutia out of the tolerance region, the local Delaunay structure which contains that minutia will be altered [7]. Figure 2 gives an example of the local Delaunay structural change under distortion that moves a minutia out of the tolerance region. The gray region in Figure 2(a) and 2(b) is the tolerance region of a Delaunay triangle. As long as minutia c moves within the tolerance region, triangles, T(acb) and T(acd), contained by convex quadrilateral Q($abcd$) would not be altered in this case, as shown in Figure 2(a). However, if the distortion moves c by a large amount out of the tolerance region, then triangles, T(acb) and T(acd), originally contained by convex quadrilateral Q($abcd$) will be changed to be triangles, T(abd) and T(cbd), as shown in Figure 2(b). We assume that the convex quadrilaterals in Figure 2(a) and Figure 2(b) are from the template image and query image, respectively. In this case, during the matching procedure, the triangles, T(acb) and T(acd), from the template image would surely not match with the triangles, T(abd) and T(cbd), from the query image in a Delaunay triangle-based fingerprint authentication system even if they are formed by corresponding minutiae.

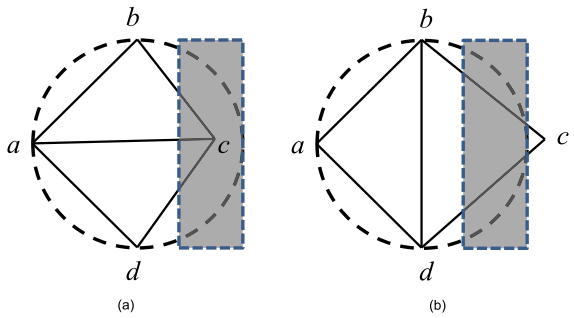


Fig. 2. Local Delaunay structural change under distortion (a) minutia c moves within the tolerance region, (b) minutia c moves out of the tolerance region.

In this paper we propose a Delaunay quadrangle-based fingerprint authentication system which exploits the stable Delaunay quadrangle-based structure to reduce biometric uncertainty and provide strong security protection to the template data. The main contributions of this work are:

1) We propose a new local Delaunay quadrangle-based structure. The feature vector obtained from each local structure is of fixed-length and alignment-free, so it can be readily applied to existing template protection techniques, e.g. PinSketch [34]. This solves the problem of incompatibility between unencrypted and encrypted domains.
2) The proposed local Delaunay quadrangle-based structure has better structural stability than the Delaunay triangle-based structure and is able to tolerate a certain extent of nonlinear distortion-induced structural change that the Delaunay triangle-based structure suffers.
3) Feature representation from the Delaunay quadrangle-based structure is potentially more discriminative than that from the Delaunay triangle-based structure.
4) A polar coordinate based auxiliary feature is proposed to increase the system matching reliability.
5) A unique topology code is derived from each Delaunay quadrangle. The topology code not only can assist in accomplishing accurate local registration in the presence of distortion, but also contributes to enhancing the security level of the proposed system.

The rest of the paper is organized as follows. In Section II, we introduce the local Delaunay quadrangle-based structure and its feature representations, including a derived topology code. A polar coordinate based auxiliary feature is also proposed. Encrypted matching using the feature representations extracted from the proposed Delaunay quadrangle-based structure is presented in Section III. In Section IV, experimental results and security analysis are demonstrated and discussed. The conclusion is given in Section V.

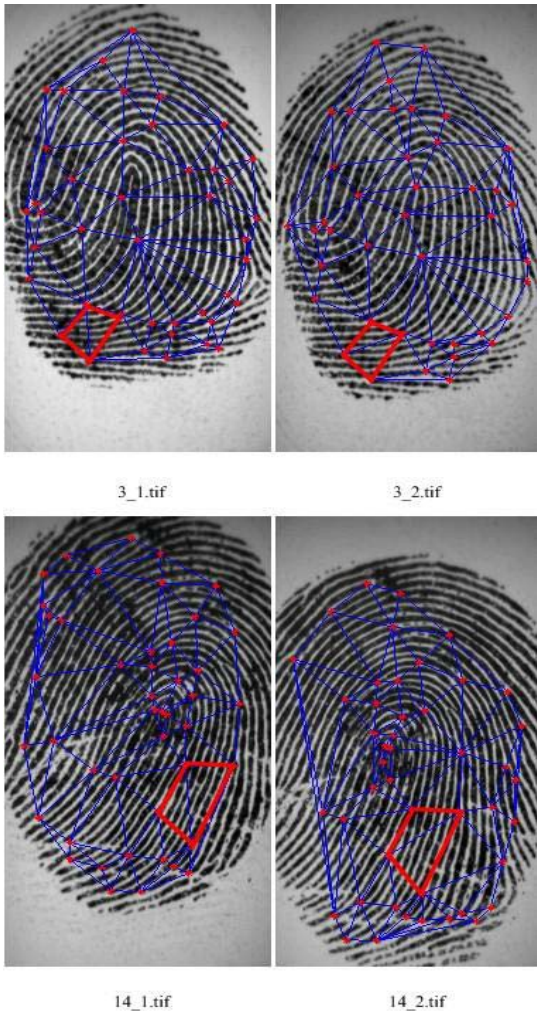


Fig. 3. Examples that the Delaunay quadrangles (bold line) are not changed but the Delaunay triangles which comprise them are altered under distortion.

II. The Delaunay Quadrangle-Based Structure and Feature Representations

In this section, we present the Delaunay quadrangle-based structure and its feature representations. A unique topology code is derived from each Delaunay quadrangle. Not only can this unique topology code help to carry out accurate local registration that absolute geometrical measurement usually fails when distortion is present, but it also enhances the security of template data, which will be discussed in the next section. A polar coordinate based auxiliary feature is also proposed.

A. Delaunay Quadrangle Generation

The construction of the Delaunay quadrangle-based structure is motivated by the observation that even if the triangles that constitute a Delaunay quadrangle are changed, the minutiae that form this Delaunay quadrangle do not change. In Figure 3, we show some real examples from the publicly available database FVC2002 DB2 that the Delaunay quadrangles (bold line) do not alter but the Delaunay triangles which comprise them are changed under distortion, even if the fingerprint images in the same row are from the same finger.

Delaunay quadrangles are built upon the construction of the Delaunay triangulation net. The algorithm for producing the Delaunay triangulation net is detailed in [35]. Here we give a brief description. Given a set of minutiae $M = \{m_i\}_{i=1}^{N}$, where N is the number of minutiae, as shown in Figure 1(a), a Voronoi diagram is generated first, which partitions the entire fingerprint region into small cells centering on each minutia. All the points in the cell around m_i are closer to m_i than to any other minutiae. Then the Delaunay triangulation net is produced by linking the centers of every pair of neighbor cells as shown in Figure 1(b). For a Delaunay triangulation net formed by the minutia set $M = \{m_i\}_{i=1}^{N}$, it is composed of $(2 \times N - 2 - K)$ Delaunay triangles, where K is the number of minutiae on the convex hull of the Delaunay triangulation net. Once the Delaunay triangulation net is generated, a Delaunay quadrangle can be formed by joining any two Delaunay triangles that share a common side.

The proposed Delaunay quadrangle-based structure can tolerate the local structural change suffered by the Delaunay triangle-based structure under nonlinear distortion, as discussed in Section I. Generally speaking, the features extracted from the proposed Delaunay quadrangle-based structure are more discriminative than those from the Delaunay triangle-based structure. This is because a quadrangle has more attributes (e.g., one more edge and angle) than a triangle.

B. Local Registration Using Topology Code

Fingerprint image registration or alignment is a critical process in fingerprint matching. But unfortunately, fingerprint registration usually takes place in the unencrypted domain rather than the encrypted domain. This is because for a fingerprint authentication system with template protection, the original template data are unavailable to compute the alignment parameters. For instance, reference points, e.g., singular point, are usually used as the reference to establish a rotation and translation relationship between query and template images; however, the exposure of the reference points during the alignment procedure would leak important information about the fingerprint data, thus weakening the security of the associated fingerprint authentication system.

The proposed Delaunay quadrangle-based structure can avoid this global image registration process because only local registration is needed by using local minutiae information. For example, as shown in Figure 4, there is a pair of corresponding Delaunay quadrangles, $Q(ABCD)$ and $Q(A'B'C'D')$ from the template and query images, respectively. The key to matching $Q(ABCD)$ with $Q(A'B'C'D')$ is that $Q(A'B'C'D')$ has to be correctly aligned with $Q(ABCD)$. Assume that the points A, B, C and D in $Q(ABCD)$ are corresponding to points A', B', C' and D' in $Q(A'B'C'D')$, respectively, and that the feature extraction procedure starts from point A, the vertex of the smallest angle, in $Q(ABCD)$ and then moves to point D in the clock-wise direction. In this case, the correct local registration is about precisely finding A's corresponding point A' in $Q(A'B'C'D')$. A straightforward method is to search the vertex of the smallest angle from $Q(A'B'C'D')$ and consider it as the starting point of the

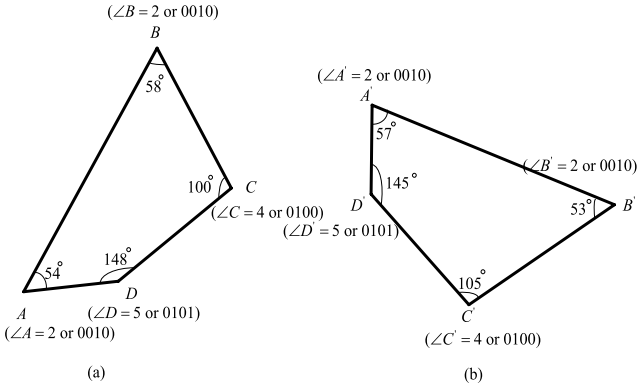


Fig. 4. Corresponding Delaunay quadrangles $Q(ABCD)$ and $Q(A'B'C'D')$ in (a) the template fingerprint image and (b) the query fingerprint image, respectively.

quadrangle $Q(A'B'C'D')$. This method, which uses an absolute geometrical measurement, is effective only when no structural change happens. Unfortunately, nonlinear distortion caused by elastic finger skin always exists in fingerprint images, thus structural change is inevitable. Distortion may cause the genuine corresponding angle $\angle A'$ of the smallest angle $\angle A$ in $Q(ABCD)$ to be the second smallest angle in $Q(A'B'C'D')$ as shown in Figure 4. As a result, point B' would be mistakenly chosen as the starting point of $Q(A'B'C'D')$. Then, the matching result between $Q(ABCD)$ and $Q(A'B'C'D')$ would definitely be negative because the corresponding attributes (e.g. edge length, orientation of minutiae) of these two Delaunay quadrangles are different.

From the above analysis, we can see that using absolute geometrical measurement in deciding a starting point under distortion is inaccurate. Naturally, the quantization operation is expected to solve this issue because it can make angle values insensitive to small-scale differences and assign same symbols to those angles that are located in the same range. The value of an angle in a Delaunay quadrangle is in the range of 0 to 2π. Assume the quantization step size is $ss_{tc} = \pi/6$ and the quantized angle value is expressed as a binary string of m_{tc} bits or an integer ranging from 0 to $2^{m_{tc}}$, then the smallest and second smallest angles, $\angle A$ and $\angle B$, in $Q(ABCD)$ are both quantized into the same value '2' or '0010' in a binary form. Similarly, $\angle A'$ and $\angle B'$ in $Q(A'B'C'D')$ are also quantized into the same value '2' or '0010' in a binary form. We use the integer value in the remaining part of the paper unless stated otherwise. In this way, point B' will not be mistaken for the starting point of the Delaunay quadrangle $Q(A'B'C'D')$. However, another issue arises from this treatment. Since the values of the smallest and second smallest angles, $\angle A$ and $\angle B$, after quantization, are both denoted by the same integer value '2', which point should be considered as the starting point?

The angles, $\angle A$, $\angle B$, $\angle C$ and $\angle D$, of $Q(ABCD)$ are quantized into '2', '2', '4' and '5', respectively. We observe that, by changing the starting point from *A to D* and counting the quantized angle values sequentially in clock-wise direction, four different code strings, 2-2-4-5, 2-4-5-2, 4-5-2-2 and 5-2-2-4, can be generated. Similarly, four code strings, 2-2-4-5, 2-4-5-2, 4-5-2-2 and 5-2-2-4, can also be produced for $Q(A'B'C'D')$.

We shall now seek a descriptor from each Delaunay quadrangle that owns two properties: (1) it should uniquely describe the different shape of each Delaunay quadrangle; (2) it should reflect the impact of different starting point selections. The second property of such a descriptor is highly critical in helping us to decide the starting point of a Delaunay quadrangle in local registration. In order to make each quadrangle correspond to a unique descriptor, we use an equation from [36] as follows:

$$TC = p_1 \times \Gamma^3 + p_2 \times \Gamma^2 + p_3 \times \Gamma^1 + p_4 \times \Gamma^0 \qquad (1)$$

where $\{p_i\}_{i=1}^4$ are the quantized angle values of the Delaunay quadrangle and $\Gamma = \max(p_1, p_2, p_3, p_4) + 1$. Using equation (1), we calculate a value for each of the four code strings and choose the smallest value to be the descriptor of the Delaunay quadrangle under consideration. The descriptor obtained by equation (1) is unique and the proof of the uniqueness of this descriptor can be found in [36]. Since the descriptor *TC* describes the shape feature of the Delaunay quadrangle, we call it topology code in this paper.

According to the topology code *TC* generation rule, each Delaunay quadrangle can be indexed by a unique value. For example, it follows from equation (1) that the resulting values of the four code strings, 2-2-4-5, 2-4-5-2, 4-5-2-2 and 5-2-2-4, from $Q(ABCD)$ are 533, 608, 1058 and 1168, respectively. Hence, the smallest value 533, which corresponds to the starting point of A, is chosen as the topology code of $Q(ABCD)$. Similarly, the topology code of $Q(A'B'C'D')$ is also calculated to be 533, which is corresponding to the starting point A'. The starting points A of $Q(ABCD)$ and A' of $Q(A'B'C'D')$ are just the correct corresponding points that we want to find. By this means, accurate local registration is achieved and the mistake that point B' is considered as the starting point of $Q(A'B'C'D')$ by using the absolute geometrical measurement can be avoided.

C. Invariant Features Extracted From the Delaunay Quadrangle

Several invariant features extracted from the Delaunay quadrangle can be used for matching. Below we define some rotation- and translation-invariant local features of a Delaunay quadrangle:

- the length of edges, l_{edge};
- the angles between the each minutia orientation and its neighbor edge in the clock-wise direction, a_m;
- angles between two edges, a_q;
- the type of each minutia, t_m;

All the above invariant features can be easily computed by the given minutia information $\{(x_i, y_i, o_i, t_i)\}_{i=1}^N$, where (x_i, y_i) are the x, y coordinates, $o_i \in [0, 2\pi]$ is the orientation of the i$^{\text{th}}$ minutia, t_i is the type of the i$^{\text{th}}$ minutia and N is the total number of minutiae in a fingerprint image. Figure 5 gives an example of the four invariant features for point A in a Delaunay quadrangle. Since there are

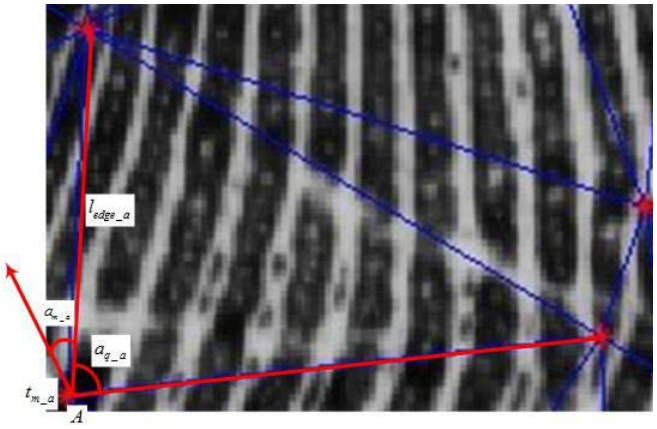


Fig. 5. An example of the invariant features (l_{edge_a}, a_{m_a}, a_{q_a}, t_{m_a}) from the point A in a Delaunay quadrangle.

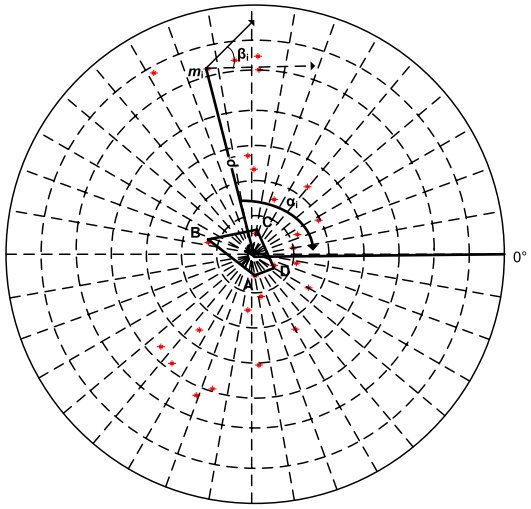


Fig. 6. A Delaunay quadrangle-centered polar coordinate space.

four points in each Delaunay quadrangle, a total of 16(= 4×4) invariant features are extracted from each Delaunay quadrangle.

Due to the elasticity of finger skin, a certain extent of deformation could be admitted to the invariant features extracted from each Delaunay quadrangle. To accommodate this, we quantize these features into short binary strings so as to tolerate the variability between template and query images. We assume that the quantization step size of l_{edge} is ss_{edge} and each l_{edge} after quantization is represented by ql_{edge} in L_1 bits; the quantization step size of a_q is ss_q and each a_q after quantization is represented by qa_q in L_2 bits; the quantization step size of a_m is ss_m and each a_m after quantization is represented by qa_m in L_3 bits; the type of each minutia t_m is represented by L_4 bit. After quantization, all these short binary strings are concatenated into a long binary string Q_i ordered from the starting point of the Delaunay quadrangle, which we can obtain using the topology code, to the end point in the clock-wise direction. For example, in Figure 5, the features at point A after quantization is represented by $Q_A = ql_{edge\_a} \parallel qa_{q\_a} \parallel qa_{m\_a} \parallel t_{m\_a}$, and a Delaunay quadrangle can be represented as $DQ = Q_A \parallel Q_B \parallel Q_C \parallel Q_D$. So the i^{th} Delaunay quadrangle can be represented by $\mathrm{D}Q_i$ which contains $L_{q\_\mathrm{i}} = 4 \times (L_1 + L_2 + L_3 + L_4)$ bits and a fingerprint image can be represented by a set of binary strings $\{DQ_i\}_{i=1}^{N_{DQ}}$, where N_{DQ} is the number of Delaunay quadrangles in the fingerprint image. It is noted [24] that a small quantization step size might be overly sensitive to slight distortions, while a large quantization step size would result in losing the discriminative power of these invariant features. The optimal setting of the step sizes based on our experiments will be given in Section IV.

D. Auxiliary Features Extracted From the Delaunay Quadrangle-Centered Polar Coordinate Space

To increase the discriminative ability of each Delaunay quadrangle, we further explore an auxiliary feature from the local region around each Delaunay quadrangle. To be specific, firstly, the center of each Delaunay quadrangle is found and considered as the reference point of a polar coordinate space. For example, the (x, y) coordinate of center C_{ABCD} of Delaunay quadrangle $Q(ABCD)$ is obtained by calculating the average of the x, y coordinates of minutiae A, B, C and D, i.e., $C_{ABCD}(x, y) = ((A(x)+B(x)+C(x)+D(x))/4, (A(y)+B(y)+C(y)+D(y))/4)$ and the orientation of C_{ABCD} is set to be the same as the orientation of the start point A, i.e., $C_{ABCD}(o) = A(o)$. Secondly, all minutiae covered by the circle of radius R centered at C_{ABCD} are translated and rotated into polar coordinates as shown in Figure 6. In this way, each minutia m_i in this circle range can be represented by a feature set $(\rho_i, \alpha_i, \beta_i)$, where ρ_i, α_i and β_i are respectively the radial distance, radial angle and orientation relative to C_{ABCD} in the polar coordinate. To reduce the influence of nonlinear distortion, a polar grid quantization on all the minutiae in the circle of radius R is carried out [24], [30]. The quantization steps of ρ_i, α_i and β_i are set to be ss_ρ, ss_α and ss_β, respectively. As a result, the feature set $(\rho_i, \alpha_i, \beta_i)$ is quantized to be $(\rho_{q\_i}, \alpha_{q\_i}, \beta_{q\_i})$ with

$$\begin{cases} \rho_{q\_i} = \rho_i / ss_\rho \\ \alpha_{q\_i} = \alpha_i / ss_\alpha \\ \beta_{q\_i} = \beta_i / ss_\beta \end{cases} \tag{2}$$

where $\rho_{q\_i} \in (0, \mathrm{R}/ss_\rho]$, $\alpha_{q\_i} \in (0, 2\pi/ss_\alpha]$ and $\beta_{q\_i} \in (0, 2\pi/ss_\beta]$. However, $(\rho_{q\_i}, \alpha_{q\_i}, \beta_{q\_i})$ is an unprotected feature set which would expose information about minutia m_i. To solve this, we transform the feature set $(\rho_{q\_i}, \alpha_{q\_i}, \beta_{q\_i})$ into an integer value tm_{i} by a non-invertible one-way function, implemented by $tm_{\mathrm{i}} = (\rho_{q\_i} \times \alpha_{q\_i}) + P_{\text{user}} \times \beta_{q\_i}$, where P_{user} is a user specific parameter. By using this function, it is hard to restore three variables ρ_{q_i}, α_{q_i} and β_{q_i}, because the number of equation is less than that of variables [37]. To produce an ordered feature set, we apply a similar idea to bin-indexing [30]. Specifically, a one-dimensional zero vector af_i of length L_{af} is constructed, and then we inspect the value of tm_{i} and replace 0 in the corresponding (bin) position indexed by tm_{i} with 1. If $tm_{\mathrm{i}} > L_{af}$, tm_{i} is set to be $\mathrm{mod}(tm_i, L_{af})$. After bin-indexing, we obtain the ordered auxiliary feature set af_i.

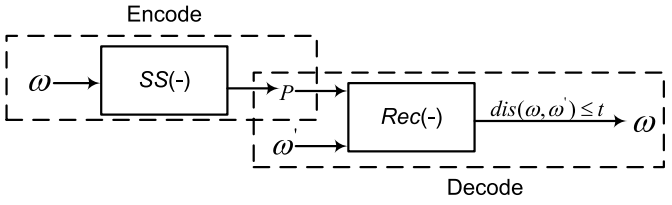


Fig. 7. An example of PinSketch construct.

The similarity between two auxiliary features af_i and af_j can be calculated as follows:

$$score(af_i, af_j) = \frac{\sum_{k=1}^{L_{af}} (af_{i,k} - \overline{af_i})(af_{j,k} - \overline{af_j})}{\sqrt{\sum_{k=1}^{L_{af}} (af_{i,k} - \overline{af_i})^2 \sum_{k=1}^{L_{af}} (af_{j,k} - \overline{af_j})^2}} \quad (3)$$

where $\overline{af_i} = \text{mean}(af_i)$ and $\overline{af_j} = \text{mean}(af_j)$. If the value of $score(af_i, af_j)$ is larger than threshold value t_{score}, af_i and af_j can be considered as corresponding auxiliary feature sets.

Note that the auxiliary feature af_i is only utilized to assist in enhancing the discriminatory power of Delaunay quadrangles rather than used for key binding.

III. Feature Matching With Template Protection

In the proposed fingerprint authentication system, fingerprint matching between template and query images is performed in the encrypted domain. Each local feature vector extracted from the Delaunay quadrangles is encrypted by the secure sketch, PinSketch. In other words, multiple secure sketches are applied in the proposed system.

A. The Template Protection Technique: PinSketch

PinSketch, which was first proposed by Dodis *et al.* [34], is a construct that is based on Bose Chaudhuri Hocquenghem (BCH) code to recover biometric template data, and at the meantime, to provide the secure protection of the template data. Below we give a brief overview of PinSketch which contains two modals, namely the encode modal and decode modal, as shown in Figure 7. More details about PinSketch can be found in [34].

1) Encode: Let ω be a template feature vector that is error-prone and needs protection. A sketching procedure $SS(\cdot)$ is applied to ω to compute the helper data, syndrome of ω, expressed as:

$$SS(\omega) = syn(\omega) = (s_1, s_3, s_5, \ldots, s_{2t-1}) \quad (4)$$

where $s_i = \sum_{\alpha \in \text{supp}(\omega)} \alpha^i$ and $supp(\omega)$ is represented by a list of non-zero positions of ω and is called the support set; t is the error tolerance which PinSketch can deal with.

2) Decode: Let ω' be a query feature vector. ω' together with $SS(\omega)$ is given as the input to the recover module $Rec(\cdot)$ of PinSketch, where the syndrome of ω' is first computed by

$$SS(\omega') = syn(\omega') = (s'_1, s'_3, s'_5, \ldots, s'_{2t-1}) \quad (5)$$

Then the difference between syndromes $SS(\omega)$ and $SS(\omega')$ is calculated as

$$\begin{aligned} syn(\lambda) &= SS(\omega) - SS(\omega') \\ &= (s_1 - s'_1, s_3 - s'_3, s_5 - s'_5, \ldots, s_{2t-1} - s'_{2t-1}) \end{aligned} \quad (6)$$

where $\lambda = \omega - \omega'$ according to the fact that $SS(\omega - \omega') = SS(\omega) - SS(\omega')$. If the difference between ω and ω', $dis(\omega, \omega')$, is no more than t, applying BCH decoding to $syn(\lambda)$ can successfully recover λ. Then ω can be recovered by adding λ to ω', i.e.

$$\omega = Rec(\lambda, \omega') = syn(\lambda) + syn(\omega'). \quad (7)$$

B. Enrollment Stage

In the enrollment stage, a security key k that needs protection is skillfully bound with template features which are protected by PinSketch. The procedure of the enrollment stage is shown in Figure 8 and the detailed steps are explained below:

1) Template Protection by PinSketch:

1) Given the template fingerprint image fp^T, the template quadrangle feature set $V^T = \{DQ_i^T\}_{i=1}^{NT}$, topology code set $\{TC_i^T\}_{i=1}^{N_{tc}}$ and auxiliary feature set $\{af_i^T\}_{i=1}^{NT}$ are extracted from fp^T using the approach described in Section II, where NT is the number of Delaunay quadrangles and N_{tc} is the number of unique topology codes in fp^T.
2) The user-specific secret key k that needs protection is technically bound with the template feature set V^T. To be specific, it is encoded into a polynomial P of degree n by dividing it into $(n+1)$ segments and using them as the coefficients of P, e.g., $P(x) = k_n x^n + \cdots + k_1 x + k_0$ [38], [39]. P is evaluated at all the elements in the feature set $V^T = \{DQ_i^T\}_{i=1}^{NT}$ to obtain a value set, $P(V^T) = \{P(DQ_i^T)\}_{i=1}^{NT}$. Security protection should be provided to the data set $\{V^T, P(V^T)\}$ because the polynomial P can be reconstructed using Lagrange interpolation [38], if more than n pairs of elements from $\{V^T, P(V^T)\}$ are obtained by an adversary.
3) To protect $\{V^T, P(V^T)\}$, the sketching procedure $SS(\cdot)$ of PinSketch is applied to each element DQ_i^T in V^T and this process will output the sketch data $SS(DQ_i^T)$ which will act as the helper data in the verification stage, where $SS(\cdot)$ is defined in Section III-A and the error-correction capability is set to be t_{ps}. After $SS(V^T) = \{SS(DQ_i^T)\}_{i=1}^{NT}$ is generated, V^T is destroyed.

2) Security Enhancement Using Topology Code: Since the template data V^T is destroyed, an adversary can only obtain V^T from sketch data $SS(V^T)$ through brute force attack. The security of each element $SS(DQ_i^T)$ from $SS(V^T)$ can be evaluated from entropy analysis, which will be discussed in Section IV-C, and the entropy depends on several factors, such as the length of the sketch data $SS(DQ_i^T)$ and the error tolerance t_{ps}. In order to further enhance the security level of the system, a security enhancement method using topology code set $\{TC_i^T\}_{i=1}^{N_{tc}}$ is applied to each sketch data $SS(DQ_i^T)$.

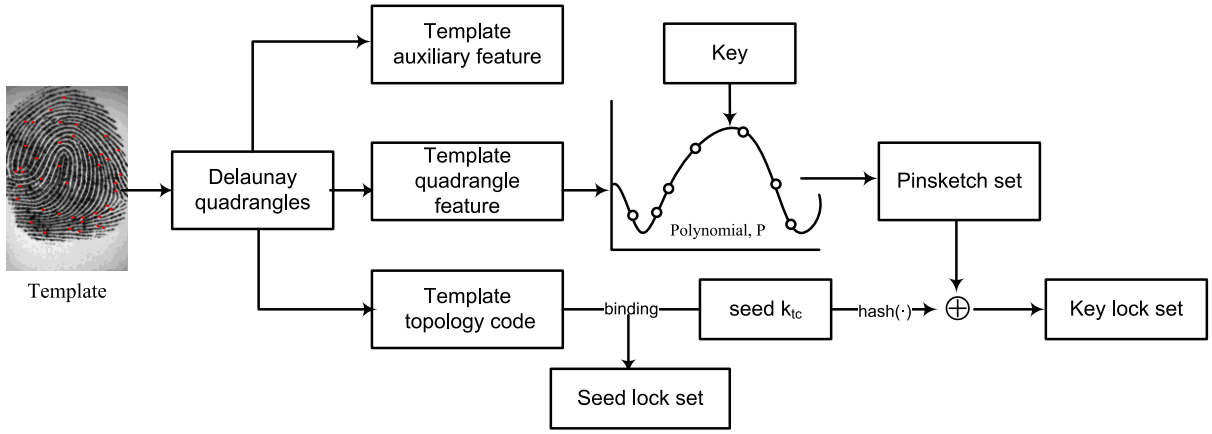


Fig. 8. Enrollment stage.

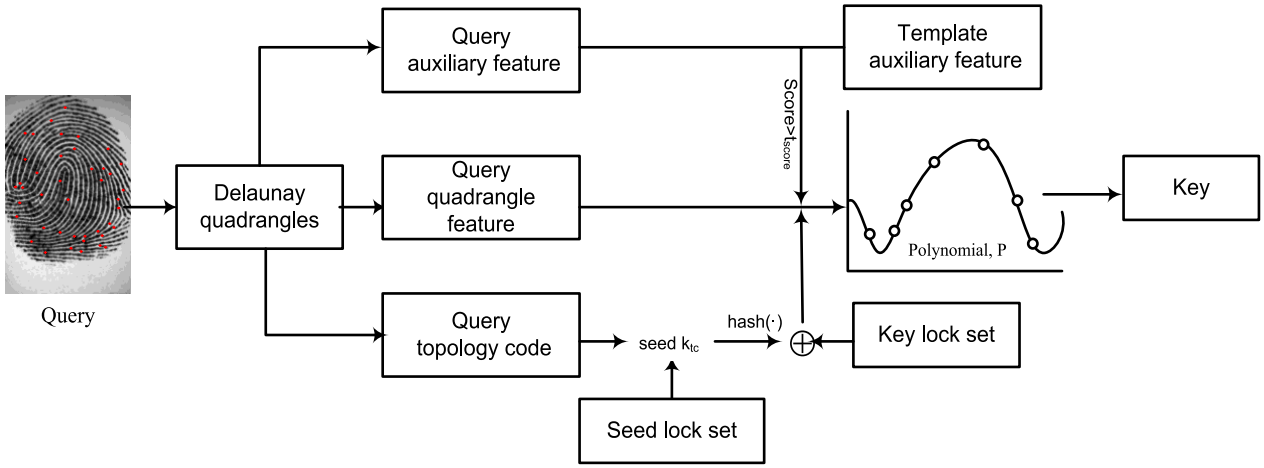


Fig. 9. Verification stage.

1) A user specific seed value k_{tc} is bound with the topology code set $\{TC_i^T\}_{i=1}^{N_{tc}}$ by using a polynomial P_{tc} of degree of n, which is the same as the degree of polynomial P. P_{tc} is evaluated at all the elements in the set $\{TC_i^T\}_{i=1}^{N_{tc}}$ to obtain a value set $\{P_{tc}(TC_i^T)\}_{i=1}^{N_{tc}}$, where topology code TC_i^T is obtained from each Delaunay quadrangle using the scheme described in Section II-B. $\{TC_i^T, P_{tc}(TC_i^T)\}_{i=1}^{N_{tc}}$ is generated as a genuine set for seed k_{tc}. To protect $\{TC_i^T, P_{tc}(TC_i^T)\}_{i=1}^{N_{tc}}$, a chaff point set $\{c_i, d_i\}_{i=1}^{N_{cf}}$ is added to form the final secure vault $\{TC_i^T, P_{tc}(TC_i^T)\}_{i=1}^{N_{tc}} \cup \{c_i, d_i\}_{i=1}^{N_{cf}}$ for k_{tc}, which is similar to the encoding procedure of the fuzzy vault technique [40].
2) k_{tc} acts as a seed to a hash function $hash(\cdot)$ that generates two random binary strings CS_1^T and CS_2^T of the same length as $SS(DQ_i^T)$ and $P(V^T)$, respectively.
3) The random binary string CS_1^T is XORed with sketch data $SS(DQ_i^T)$ to generate the security enhanced sketch data $ES(DQ_i^T) = CS_1^T \oplus SS(DQ_i^T)$, where the helper data has been hidden. The set of all the enhanced sketch data can be denoted by $ES(V^T) = \{ES(DQ_i^T)\}_{i=1}^{NT}$. By the same token, CS_2^T is XORed with each element of $P(V^T)$ to generate a secure data set $EP(V^T) = CS_2^T \oplus P(V^T)$.
4) Instead of storing the original template feature set $\{V^T, P(V^T)\}$, a double secured key lock set $\{ES(V^T), EP(V^T)\}$ is stored in the database and the original template data V^T is destroyed. By this means, template protection is achieved.

C. Verification Stage

In the verification stage, if enough sketch data from the key lock set $\{ES(V^T), EP(V^T)\}$ can be decoded, the secret key k can be retrieved by reconstructing the polynomial P. The procedure of the verification stage is shown in Figure 9 and the detailed steps are explained below:

1) Given a query fingerprint image fp^Q, the query feature set $V^Q = \{DQ_j^Q\}_{j=1}^{NQ}$, topology code set $\{TC_j^Q\}_{j=1}^{N_{qc}}$ and auxiliary feature set $\{af_j^Q\}_{j=1}^{NQ}$ are extracted from fp^Q by using the approach described in Section II, where NQ is the number of Delaunay quadrangles and N_{qc} is the number of unique topology codes in fp^Q.
2) To retrieve the secret key k, a sufficient number of elements should be decoded from the secured key lock set $\{ES(V^T), EP(V^T)\}$. Since both $ES(V^T)$ and $EP(V^T)$ are encrypted by random binary strings CS_1^T and CS_2^T generated from seed k_{tc}, it should be retrieved first. The retrieval process of k_{tc} is similar to the

TABLE I
DETAILED INFORMATION ABOUT THE DATABASES USED IN OUR EXPERIMENTS

Parameter	2002DB1	2002DB2	2002DB3	2004DB2	2006DB2	2006DB3
Resolution	500 dpi	569 dpi	500 dpi	500 dpi	569 dpi	500 dpi
Number of fingers	100	100	100	100	140	140
Number of images per finger	8	8	8	8	12	12
Sensor Type	Optical Sensor	Optical Sensor	Capacitive Sensor	Optical Sensor	Optical Sensor	Thermal sweeping Sensor
Image size	388×374	560×296	300×300	328×364	400×560	400×500
Image quality	Medium	Medium	Medium to low	Low	Medium to low	Medium to low

fuzzy vault decoding procedure [40]. For example, if an element TC_j^Q from fp^Q is equal to TC_i^T, then $(TC_i^T, P_{tc}(TC_i^T))$ can be considered as a genuine point. If $(n+1)$ genuine points from $\{TC_i^T, P_{tc}(TC_i^T)\}_{i=1}^{N_{tc}} \cup \{c_i, d_i\}_{i=1}^{N_{cf}}$ can be found, the polynomial P_{tc} can be successfully reconstructed and a seed k'_{tc} can be restored.

3) The restored seed k'_{tc} is applied to the same hash function $hash(\cdot)$ used in the enrolment stage, outputting binary strings CS_1^Q and CS_2^Q which are further XORed with the security enhanced sketch data $ES(V^T)$ and $EP(V^T)$ respectively, to generate the recovered helper data set $SS'(V^T) = CS_1^Q \oplus ES(V^T) = \{CS_1^Q \oplus ES(DQ_i^T)\}_{i=1}^{NT}$ and polynomial value set $P'(V^T) = CS_2^Q \oplus EP(V^T) == \{CS_2^Q \oplus EP(DQ_i^T)\}_{i=1}^{NT}$.
4) For each element $SS'(DQ_i^T)$ from $SS'(V^T)$, we check whether the element DQ_j^Q from the query feature set V^Q can decode it or not. First, the similarity between af_i and af_j is checked. If the similarity score $score(af_i, af_j)$ is less than the threshold t_{score}, then next matching attempt will be carried on; otherwise, DQ_j^Q and its recovered helper data $SS'(DQ_i^T)$ are further inputted into the recover module $Rec(\cdot)$ of PinSketch, which would output a recovered value, $Rec(SS'(DQ_i^T))$. $dis(DQ_j^Q, DQ_i^T)$ is the hamming distance between DQ_j^Q and DQ_i^T. If $k'_{tc} = k_{tc}$ (equivalent to $CS_1^Q = CS_1^T$) and $dis(DQ_j^Q, DQ_i^T) \le t_{ps}$, it can guarantee that $Rec(SS'(DQ_i^T)) = DQ_i^T$; otherwise a failed decryption is reported.
5) Steps 3 and 4 are repeated until matching between all the elements in template and query feature sets is carried out. All the recovered feature data and their corresponding polynomial values in $P'(V^T)$ form the key unlock set $\{Rec(SS'(DQ_i^T)), P'(DQ_i^T)\}_{i=1}^{NU}$, where NU is the number of elements in the unlock set.
6) If NU is smaller than (n+1), a non-match report is generated. If NU is equal to or greater than (n+1), then the polynomial P can be reconstructed by Lagrange interpolation and the secret key k can be retrieved by sequentially concatenating the (n+1) coefficients as $k_0||k_1||\ldots||k_n$.

IV. EXPERIMENTAL RESULTS AND SECURITY ANALYSIS

A. Database Selection and Parameter Setting

We evaluated the proposed fingerprint authentication system on six publicly available databases, namely, three databases (DB1, DB2 and DB3) of FVC2002, FVC2004 DB2 and two databases (DB2 and DB3) of FVC2006 [41]. Detailed information about these six databases is shown in Table I.

TABLE II
PARAMETERS AND VALUE RANGE

Parameter	Explanation	Value Range
ss_{tc}	quantization step size for TC	$[\pi/9, 7\pi/36]$
ss_{edge}	quantization step size of l_{edge}	[15, 20] pixels
ss_m	quantization step size of a_m	$[\pi/12, \pi/9]$
ss_q	quantization step size of a_q	$[\pi/12, \pi/9]$
$L_{\text{q\_i}}$	bit length of DQ_i(binary)	63 bits
L_{af}	Length of auxiliary feature af_i(vector)	25920
t_{ps}	error correction capability of PinSketch	[7,10] bits

The software VeriFinger 4.0 from Neurotechnology [42] was used to extract minutiae from fingerprint images. As mentioned previously, choosing a small quantization step size increases sensitivity to slight distortions, whereas a large quantization step size is not discriminative enough [24]. Here, we list all the parameters and their value range used in our experiments in Table II. For example, the bit length L_{q_i} of each feature representation DQ_i is set to be 63 bits. Because different quantization step sizes are used for different databases, the lengths of the generated binary strings would be different. If the length of DQ_i is smaller than 63 bits, zeros will be padded to it; if the length of DQ_i is larger than 63, only the first 63 bits are kept.

B. Performance Evaluation

To evaluate the performance of the proposed fingerprint authentication system, three performance indices are utilized in this paper: (1) false reject rate (FRR), which is defined as the ratio of unsuccessful genuine attempts to the total genuine attempts, (2) false accept rate (FAR), which is defined as the ratio of successful impostor attempts to the total impostor attempts, and (3) equal error rate (EER), which is defined as the error rate when the FRR and FAR are equal.

On all the six databases, two matching protocols, the 1VS1 protocol and standard FVC protocol [29], [43], are employed. For the 1VS1 protocol, according to the rule, we set the 1st image from each finger in the data set as the template image and the 2nd image from the same finger as the query image to compute the FRR. And we set the 1st image from each finger in the data set as the template image and the 1st image from the remaining fingers in the data set as query images to calculate the FAR. For the standard FVC protocol, we set each image in the database as the template and compare it with the remaining

seven images from the same finger to calculate the FRR. And we set the 1st image from each finger in the database as the template to compare with the 1st image from the remaining fingers in the database to calculate the FAR. In order to avoid correlation, if image x has been compared with y, then the symmetric comparison (i.e. y against x) is not executed. Therefore, using the 1vs1 protocol results in 100 genuine matching attempts and $((100 \times 99)/2) = 4,950$ impostor matching attempts for each of the databases of FVC2002 DB1, FVC2002 DB2, FVC2002 DB3 and FVC2004 DB2, while 140 genuine matching attempts and $((140 \times 139)/2) = 9730$ impostor matching attempts are made for each of the databases of FVC2006 DB2 and FVC2006 DB3. Also, according to the standard FVC protocol, $((8 \times 7)/2) \times 100 = 2,800$ genuine matching attempts and $((100 \times 99)/2) = 4,950$ impostor matching attempts are made for each of the databases of FVC2002 DB1, FVC2002 DB2, FVC2002 DB3 and FVC2004 DB2, while $((12 \times 11)/2) \times 140 = 9,240$ genuine matching tests and $((140 \times 139)/2) = 9,730$ impostor matching tests are tried on each of the databases of FVC2006 DB2 and FVC2006 DB3.

1) Performance Comparison of Different Structures: In order to evaluate the effects of the proposed Delaunay quadrangle-based structure and topology code, we tested and compared three different structures: (1) Delaunay triangle-based structure, (2) Delaunay quadrangle-based structure, and (3) Delaunay quadrangle-based structure with topology code for local registration, over the database FVC2002 DB2 by using the 1VS1 matching protocol. Note that the auxiliary feature set and topology code set for security enhancement are not used in this case. The quantization parameters set for these three structures are ($ss_{tc} = \pi/6$; $ss_{edge} = 20$ pixels; $ss_m = \pi/12$; $ss_q = \pi/12$). When testing these three structures, we used the absolute geometrical measurement to carry out local registration (i.e. selecting the point with the smallest angle as the starting point) for the Delaunay triangle-based structure and Delaunay quadrangle-based structure, while for the Delaunay quadrangle-based structure with topology code for local registration, we exploited the topology code for local registration. The performance comparison of these three different structures is illustrated in Figure 10. It can be observed from Figure 10 that the Delaunay quadrangle-based structure with topology code (EER = 1.07%) exhibits the best performance among the three structures. Both the Delaunay quadrangle-based structure with topology code (EER = 1.07%) and the Delaunay quadrangle-based structure without topology code (EER = 1.65%) perform better than the Delaunay triangle-based structure (EER = 4.02%). This proves that the Delaunay quadrangle is more stable than the Delaunay triangle under nonlinear distortion, and the feature vector obtained from the Delaunay quadrangle is more discriminative than that from the Delaunay triangle because the quadrangle has richer characteristics than the triangle. Under the same Delaunay quadrangle-based structure, the use of topology code for local registration also improves the performance of the system, which is justified by the EER = 1.07% with topology code, compared to the EER = 1.65% without topology code.

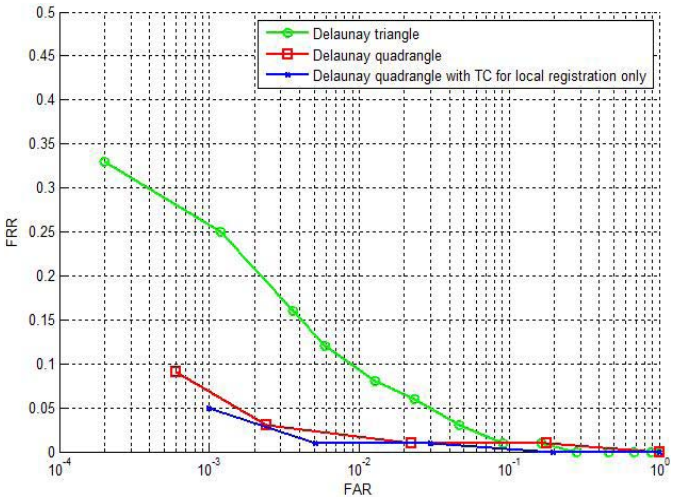


Fig. 10. Performance comparison of three different structures on the database FVC2002 DB2.

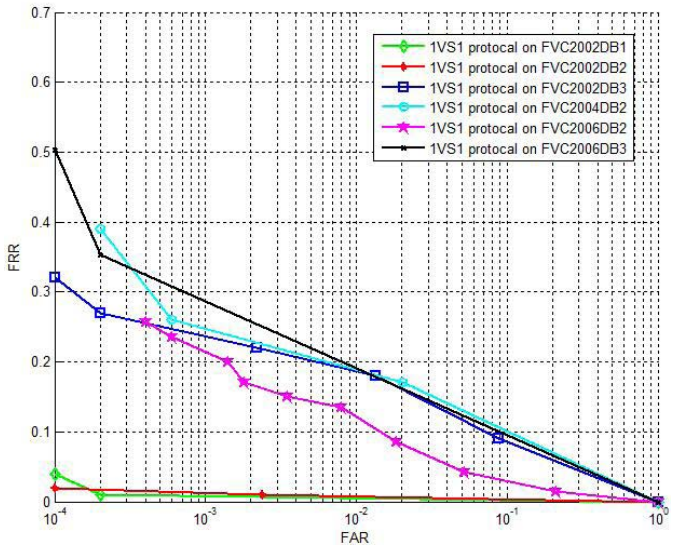


Fig. 11. Performance of the proposed method using the 1VS1 protocol.

2) Performance Evaluation With Different Public Databases: We evaluated the proposed system using the 1VS1 protocol and standard FVC protocol over six public databases, as discussed in Section IV-A. Feature representations used for these six databases are all based on the Delaunay quadrangle with topology code for local registration and security enhancement incorporating the topology code. Performance of the proposed method over these six databases varies because the image quality of different databases is different.

With the 1VS1 protocol, the proposed system performs best on database FVC2002 DB2 (FAR = 0, FRR = 2%); however, the performance drops substantially on databases FVC2006 DB3 (FAR = 0.1%, FRR = 28.67%) and FVC2004 DB2 (FAR = 0.1%, FRR = 24.72%) as shown in Figure 11. Performance degradation is mainly due to the poor image quality of these databases. Fingerprint images in FVC2006 DB3 have missing or spurious minutiae, which would adversely affect recognition accuracy. As indicated in [17], missing or spurious minutiae may eliminate important triangles or

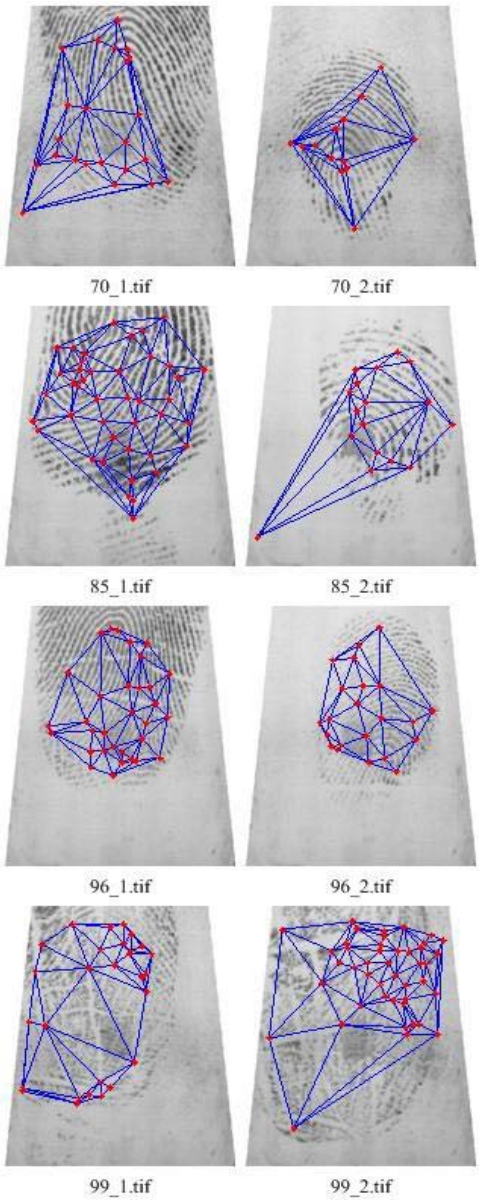


Fig. 12. Some images in FVC2004 DB2 that failed genuine matching attempts.

introduce spurious triangles. As for FVC2004 DB2, the first two images are heavily distorted because individuals were requested to exaggerate finger skin distortion at the acquisition time [44]. The proposed method can tackle nonlinear distortion to some extent, as shown in Section IV-B-1). Apart from large non-linear distortion, small overlap area between template and query images may be another reason for low performance on FVC2004 DB2. Figure 12 shows some mated-pair images in FVC2004 DB2, "x_1.tif" and "x_2.tif" with $x \in [70, 85, 96, 99]$, whose genuine matching attempts failed in our testing. Take the image pair, "96_1.tif" and "96_2.tif", as example. "96_1.tif" acts as the template image and "96_2.tif" acts as the query image. In "96_1.tif", the effective fingerprint region is mainly the lower part under the core point, whereas in "96_2.tif", only the upper part above the core point is available. In this case, template and query images almost have no overlapping area, which means that

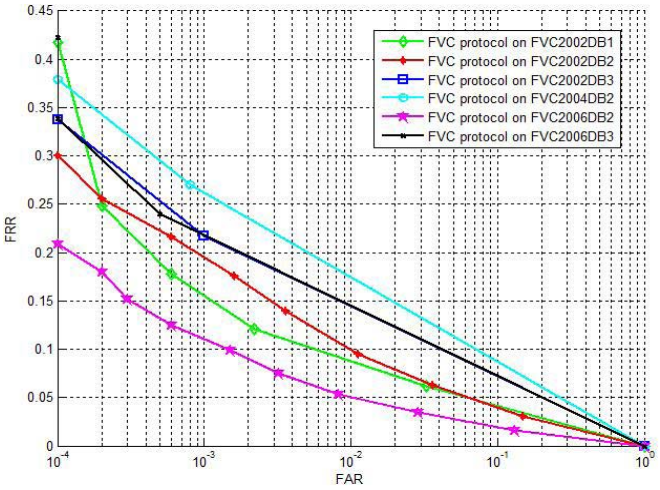


Fig. 13. Performance of the proposed method using the standard FVC protocol.

few or no corresponding minutiae from the template and query images can be extracted. Since the proposed system is minutiae local structure based, the lack of corresponding minutiae from template and query images [45] would cause matching to fail. Poor matching performance on FVC2004 DB2 is indicated by the ROC curve in Figure 11.

With the standard FVC protocol, we can see from Figure 13 that the proposed system performs best on database FVC2006 DB2 (EER = 3.07%). It is noted that the performance on FVC2002 DB2 with the standard FVC protocol is EER = 5.99%, which is worse than that (EER = 1.02%) with the 1VS1 protocol on the same database. This is because for the 1VS1 matching protocol, only the 1st and 2nd images are used, while for the standard FVC protocol, all the eight images from each finger are involved in the matching procedure, and the 1st and 2nd images in database FVC2002 DB2 are acquired in the same session and have less variation and distortion than the other six images.

We also compared the proposed system with some other similar works, such as the Delaunay triangle-based biometric cryptosystem [10], the dual layer structure check-based biometric cryptosystem [46], and three key release biometric cryptosystems based on fuzzy vault [40], [47], [48] in terms of the FAR, FRR and EER in Tables III and IV. It is shown that the performance of the proposed method is better than that of the existing similar biometric cryptosystems. Note that different feature extractors may be used for minutiae extraction in different systems and that accuracy of minutiae information may impact on system performance.

C. Security Analysis

In the case that no information in the database is available to an adversary, the security of the biometric template is guaranteed because the adversary has to randomly guess the feature representations of the template image. This is computationally infeasible. In the case that the adversary has obtained all the sketch information stored in the database, the security of the proposed system is guaranteed by two layers of protection, PinSketch and topology code.

TABLE III
RECOGNITION ACCURACY USING THE FVC PROTOCOL (VALUES IN PERCENTAGE)

Method	2002DB1	2002DB2	2002DB3	2004DB2	2006DB2	2006DB3
	EER (FRR/FAR)	EER (FRR/FAR)	EER (FRR/FAR)	EER (FRR/FAR)	EER (FRR/FAR)	EER (FRR/FAR)
Yang et al.[10]	-	13	-	-	-	-
Proposed method incorporating TC for local registration and security enhancement	4.5	5.99	(21.84/0.1)	(26.13/0. 1)	3.07	(21.76/0.1)

TABLE IV
RECOGNITION ACCURACY USING THE 1VS1 PROTOCOL (VALUES IN PERCENTAGE)

Method	2002DB1	2002DB2	2002DB3	2004DB2	2006DB2	2006DB3
	EER (FRR/FAR)	EER (FRR/FAR)	EER (FRR/FAR)	EER (FRR/FAR)	EER (FRR/FAR)	EER (FRR/FAR)
Kai et al.[46]	-	4.5	-	-	-	-
Nandakumar et al.[40]	-	(14/0)	-	-	-	-
Nagar et al.[47]	-	(7/0)	-	-	-	-
Li et al.[48]	-	(7/0)	-	-	-	-
Proposed method incorporating TC for local registration and security enhancement	(4/0)	1.02 (2/0)	8.63	(24.72/0.1)	4.83	(28.67/0.1)

1) Non-Reusability of a User's Biometric: Under the assumption that a user's biometric is used in only one template, the security of the first layer, PinSketch, can be evaluated by the min-entropy of the feature vector when the helper data are acquired by the adversary. According to [34], PinSketch is equal to a code-offset construction in a small universe. According to the sphere-packing bound [49], the min-entropy of each PinSketch data can be expressed as

$$E_{ps} = \log\left(\frac{\left(2^{L_{q\_i}}\right)}{\binom{L_{q\_i}}{t_{ps}}}\right) \tag{8}$$

Regarding the security of the second layer, since the topology code set is used to bind seed k_{tc} using the fuzzy vault technique, according to [40], the security of k_{tc} can be computed as

$$E_{tc} = -\log\left(\frac{\binom{N_{tc}}{n+1}}{\binom{N_{tc}+N_{cf}}{n+1}}\right) \tag{9}$$

Since the feature vector is secured by the above two layers, the security of the proposed system can be calculated as $E = E_{tc} + E_{ps}$. We assume the average number of topology codes, N_{tc}, is 40 and the number of chaff point, N_{cf}, is set to be 400 in our experiments. Based on equations (8) and (9), we plot in Figure 14 and Figure 15 the genuine accept rate (GAR) versus the number of security bits [50] using the 1VS1 protocol and the standard FVC protocol, respectively.

2) Reusability of a User's Biometric: Assume that a user's biometric is used across different applications. Even if each measurement of a biometric is slightly different and a secure sketch also involves probabilistic selection, when biometric data from different applications are analyzed together, information leakage may still happen. Two types of attacks, namely, distinguishability and reversibility attacks, which aim at multiple secure sketches generated from the same noisy biometric, are defined in [51] and [52]. The distinguishability attack refers to an adversary trying to utilize the template sketch data as a unique identifier to link information from different applications. The reversibility attack is about an adversary obtaining several versions of sketch data from the same biometric used in different applications in an attempt to recover the original biometric data.

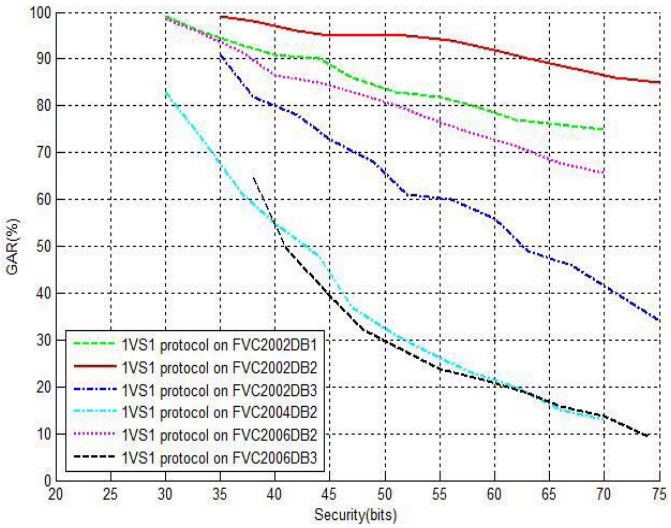


Fig. 14. GAR vs the number of security bits using the 1VS1 matching protocol.

Similar to other secure sketches, PinSketch used in our method also suffers from the aforementioned attacks if no countermeasure is taken. Blanton and Aliasgari [52] utilized

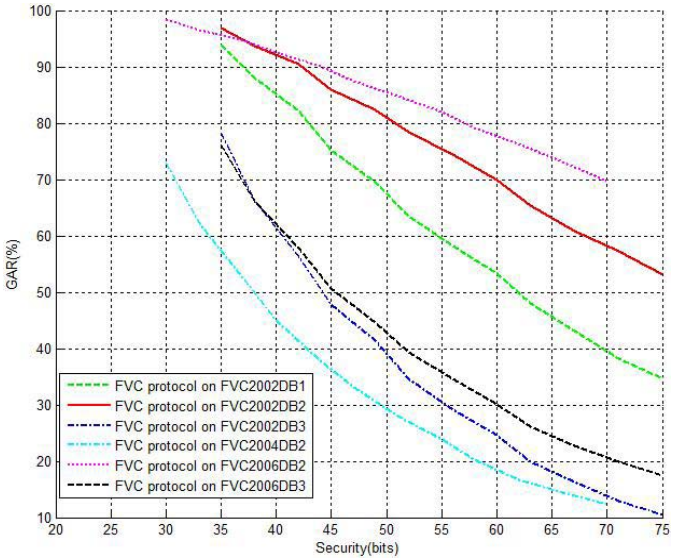


Fig. 15. GAR vs the number of security bits using the FVC matching protocol.

a random string generated from a user specific key together with a pseudo-random function to perform an XOR operation with the sketch data so as to protect the sketch data against information leakage. In the proposed method, the security of the sketch data is strengthened by the topology code in a similar fashion to [52]. Specifically, to protect the template sketch data $SS(DQ_i^T)$, a random binary string CS_1^T is first output from a hash function $hash(\cdot)$ by a seed k_{tc}. Then an XOR operation is performed between $SS(DQ_i^T)$ and CS_1^T, as $ES(DQ_i^T) = CS_1^T \oplus SS(DQ_i^T)$ (details in Section III-B). To make CS_1^T different in different applications, we can simply change the seed value k_{tc} in different applications. In this way, the adversary is unable to gain any information about the sketch data because all the sketch data are safeguarded.

What is proposed in our method and [52] aims to protect the resultant sketch data. There is an alternative approach to achieving this objective in a similar way to cancellable templates, by distorting original template data before they are further protected by secure sketches. If a non-invertible parametric function can be designed to transform the original template data into different distorted versions and further protected by secure sketches, then the correlation between sketch data generated from the different versions of the same original template data will disappear even when they are put together.

V. Conclusion

Although the Delaunay triangle-based structure has good local stability, nonlinear distortion, which generally exists in fingerprint images, may still change the local structure. This structural alteration might generate some Delaunay triangles that are different to those constructed from their corresponding minutiae in the template image. To address this, we propose to adopt the Delaunay quadrangle-based structure because Delaunay quadrangles are more stable and robust. They also contain more attributes than Delaunay triangles, and hence benefit feature representation.The fixed-length, alignment-free feature vector extracted from each Delaunay quadrangle is less sensitive to nonlinear distortion and more discriminative than that from a Delaunay triangle and is also compatible with the existing template protection techniques, e.g., PinSketch. Furthermore, the unique topology code originated from each Delaunay quadrangle can assist in accomplishing good local registration in the presence of nonlinear distortion. Experimental results have shown that the use of topology code helps the proposed system to achieve better recognition performance than the authentication system that uses the absolute geometrical measurement in local registration. Another benefit of the topology code is that it can further enhance the security of the overall system on top of what is provided by the secure sketch. The comparison with other similar biometric authentication systems with template protection shows that the proposed system performs favorably and has strong security.

References

[1] W. Zhong, X. Ning, and C. Wei, "A fingerprint matching algorithm based on relative topological relationship among minutiae," in *Proc. Int. Conf. Neural Netw. Signal Process.*, Jun. 2008, pp. 225–228.

[2] E. Liu *et al.*, "A key binding system based on n-nearest minutiae structure of fingerprint," *Pattern Recognit. Lett.*, vol. 32, no. 5, pp. 666–675, Apr. 2011.

[3] R. Cappelli, M. Ferrara, and D. Maltoni, "Fingerprint indexing based on minutia cylinder-code," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 33, no. 5, pp. 1051–1057, Mar. 2011.

[4] F. Benhammadi, H. Hentous, K. Bey-Beghdad, and M. Aissani, "Fingerprint matching using minutiae coordinate systems," in *Proc. Pattern Recognit. Image Anal.*, 2005, pp. 9–19.

[5] X. Jiang and W. Y. Yau, "Fingerprint minutiae matching based on the local and global structures," in *Proc. 15th ICPR*, 2000, pp. 1038–1041.

[6] H. Ogawa, "Labeled point pattern matching by Delaunay triangulation and maximal cliques," *Pattern Recognit.*, vol. 19, no. 1, pp. 35–40, 1986.

[7] M. Abellanas, F. Hurtado, and P. A. Ramos, "Structural tolerance and Delaunay triangulation," *Inform. Process. Lett.*, vol. 71, nos. 5–6, pp. 221–227, Sep. 1999.

[8] A. A. Khanban and A. Edalat, "Computing Delaunay triangulation with imprecise input data," in *Proc. 15th Can. Conf. Comput. Geometry*, 2003, pp. 94–97.

[9] G. Bebis, T. Deaconu, and M. Georgiopoulos, "Fingerprint identification using Delaunay triangulation," in *Proc. Int. Conf. Inform. Intell. Syst.*, 1999, pp. 452–459.

[10] W. Yang, J. Hu, and S. Wang, "A Delaunay triangle-based fuzzy extractor for fingerprint authentication," in *Proc. 11th Int. Conf. Trust, Security Privacy Comput. Commun.*, 2012, pp. 66–70.

[11] G. Parziale and A. Niel, "A fingerprint matching using minutiae triangulation," in *Proc. Biom. Authenticat.*, 2004, pp. 241–248.

[12] H. Deng and Q. Huo, "Minutiae matching based fingerprint verification using delaunay triangulation and aligned-edge-guided triangle matching," in *Proc. 5th Int. AVBPA Conf.*, 2005, pp. 270–278.

[13] N. Liu, Y. Yin, and H. Zhang, "A fingerprint matching algorithm based on Delaunay triangulation net," in *Proc. 5th Int. Conf. Comput. Inform. Technol.*, Sep. 2005, pp. 591–595.

[14] Y. Yin, H. Zhang, and X. K. Yang, "A method based on delaunay triangulation for fingerprint matching," in *Proc. Defense Security*, Mar. 2005, pp. 274–281.

[15] C. Wang and M. L. Gavrilova, "Delaunay triangulation algorithm for fingerprint matching," in *Proc. 3rd ISVD Sci. Eng.*, 2006, pp. 208–216.

[16] W. Xu, X. Chen, and J. Feng, "A robust fingerprint matching approach: Growing and fusing of local structures," in *Advances in Biometrics*. New York, NY, USA: Springer-Verlag, 2007, pp. 134–143.

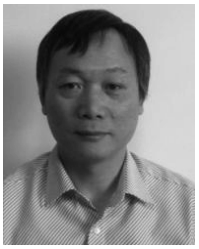
[17] T. Uz, G. Bebis, A. Erol, and S. Prabhakar, "Minutiae-based template synthesis and matching for fingerprint authentication," *Comput. Vis. Image Understand.*, vol. 113, no. 9, pp. 979–992, Sep. 2009.

[18] R. Soleymani and M. C. Amirani, "A hybrid fingerprint matching algorithm using Delaunay triangulation and Voronoi diagram," in *Proc. 20th ICEE*, 2012, pp. 752–757.

[19] Y. Feng, J. Feng, X. Chen, and Z. Song, "A novel fingerprint matching scheme based on local structure compatibility," in *Proc. 18th ICPR*, 2006, pp. 374–377.

[20] W. Yang, J. Hu, and S. Wang, "A finger-vein based cancellable bio-cryptosystem," in *Proc. Netw. Syst. Security*, 2013, pp. 784–790.
[21] W. Yang, J. Hu, S. Wang, and J. Yang, "Cancelable fingerprint templates with Delaunay triangle-based local structures," in *Cyberspace Safety and Security*. New York, NY, USA: Springer-Verlag, 2013, pp. 81–91.
[22] P. Li, X. Yang, H. Qiao, K. Cao, E. Liu, and J. Tian, "An effective biometric cryptosystem combining fingerprints with error correction codes," *Expert Syst. Appl.*, vol. 39, no. 7, pp. 6562–6574, Jun. 2011.
[23] A. T. B. Jin, D. N. C. Ling, and A. Goh, "Biohashing: Two factor authentication featuring fingerprint data and tokenised random number," *Pattern Recognit.*, vol. 37, no. 11, pp. 2245–2255, 2004.
[24] F. Farooq, R. M. Bolle, T. Y. Jea, and N. Ratha, "Anonymous and revocable fingerprint recognition," in *Proc. IEEE CVPR Conf.*, Jun. 2007, pp. 1–7.
[25] A. B. J. Teoh, Y. W. Kuan, and S. Lee, "Cancellable biometrics and annotations on BioHash," *Pattern Recognit.*, vol. 41, no. 6, pp. 2034–2044, 2008.
[26] T. Ahmad, J. Hu, and S. Wang, "Pair-polar coordinate-based cancelable fingerprint templates," *Pattern Recognit.*, vol. 44, nos. 10–11, pp. 2555–2564, 2011.
[27] M. H. Lim and A. B. J. Teoh, "An analytic performance estimation framework for multibit biometric discretization based on equal-probable quantization and linearly separable subcode encoding," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 4, pp. 1242–1254, Jul. 2012.
[28] S. Wang and J. Hu, "Alignment-free cancellable fingerprint template design: A densely infinite-to-one mapping (DITOM) approach," *Pattern Recognit.*, vol. 45, pp. 4129–4137, Dec. 2012.
[29] M. Ferrara, D. Maltoni, and R. Cappelli, "Non-invertible minutia cylinder-code representation," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 6, pp. 1727–1737, Dec. 2012.
[30] S. Wang and J. Hu, "Design of alignment-free cancelable fingerprint templates via curtailed circular convolution," *Pattern Recognit.*, vol. 47, no. 3, pp. 1321–1329, Mar. 2013.
[31] R. Cappelli, M. Ferrara, and D. Maltoni, "Minutia cylinder-code: A new representation and matching technique for fingerprint recognition," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 32, no. 12, pp. 2128–2141, Dec. 2010.
[32] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *Proc. 6th ACM Conf. Comput. Commun. Security*, 1999, pp. 28–36.
[33] A. Juels and M. Sudan, "A fuzzy vault scheme," *Des., Codes Cryptogr.*, vol. 38, no. 2, pp. 237–257, 2006.
[34] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *SIAM J. Comput.*, vol. 38, no. 1, pp. 97–139, Sep. 2008.
[35] D.-T. Lee and B. J. Schachter, "Two algorithms for constructing a Delaunay triangulation," *Int. J. Comput. Inform. Sci.*, vol. 9, no. 3, pp. 219–242, 1980.
[36] W. Gu, J. Yang, and T. S. Huang, "Matching perspective views of a polyhedron using circuits," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. PAMI-9, no. 3, pp. 390–400, May 1987.
[37] H. Chen, "A novel algorithm of fingerprint encryption using minutiae-based transformation," *Pattern Recognit. Lett.*, vol. 32, no. 2, pp. 305–309, Jun. 2011.
[38] J. P. Berrut and L. N. Trefethen, "Barycentric lagrange interpolation," *SIAM Rev.*, vol. 46, no. 3, pp. 501–517, 2004.
[39] K. Nandakumar, A. Nagar, and A. Jain, "Hardening fingerprint fuzzy vault using password," in *Proc. Int. Adv. Biometrics Conf.*, 2007, pp. 927–937.
[40] K. Nandakumar, A. K. Jain, and S. Pankanti, "Fingerprint-based fuzzy vault: Implementation and performance," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 4, pp. 744–757, Dec. 2007.
[41] J. Fierrez, J. Ortega-Garcia, D. Torre-Toledano, and J. Gonzalez-Rodriguez, "Biosec baseline corpus: A multimodal biometric database," *Pattern Recognit.*, vol. 40, no. 4, pp. 1389–1392, Apr. 2007.
[42] S. D. K. Verifinger. (2010). *Neuro Technology* [Online]. Available: http://www.neurotechnology.com/verifinger.html
[43] L. Nanni, S. Brahnam, and A. Lumini, "Biohashing applied to orientation-based minutia descriptor for secure fingerprint authentication system," *Electron. Lett.*, vol. 47, no. 15, pp. 851–853, Jul. 2011.
[44] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, "FVC2004: Third fingerprint verification competition," in *Biometric Authentication*, New York, NY, USA: Springer-Verlag, 2004, pp. 1–7.
[45] A. A. Paulino, J. Feng, and A. K. Jain, "Latent Fingerprint Matching Using Descriptor-based Hough Transform," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 1, pp. 31–45, Jan. 2013.
[46] K. Xi, J. Hu, and F. Han, "An alignment free fingerprint fuzzy extractor using near-equivalent dual layer structure check (NeDLSC) algorithm," in *Proc. 6th ICIEA*, Jun. 2011, pp. 1040–1045.
[47] A. Nagar, K. Nandakumar, and A. K. Jain, "Securing fingerprint template: Fuzzy vault with minutiae descriptors," in *Proc. 19th ICPR*, Dec. 2008, pp. 1–4.
[48] P. Li, X. Yang, K. Cao, X. Tao, R. Wang, and J. Tian, "An alignment-free fingerprint cryptosystem based on fuzzy vault scheme," *J. Netw. Comput. Appl.*, vol. 33, no. 3, pp. 207–220, May 2010.
[49] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, Amsterdam, The Netherlands: North Holland, 2006.
[50] A. Nagar, K. Nandakumar, and A. K. Jain, "Multibiometric cryptosystems based on feature-level fusion," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 255–268, Feb. 2012.
[51] K. Simoens, P. Tuyls, and B. Preneel, "Privacy weaknesses in biometric sketches," in *Proc. IEEE Symp. Security Privacy*, 2009, pp. 188–203.
[52] M. Blanton and M. Aliasgari, "On the (non-) reusability of fuzzy sketches and extractors and security improvements in the computational setting," in *IACR Cryptol. ePrint Archive*, 2012, pp. 608–636.

Wencheng Yang received the B.E. degree from the Wuhan University of Technology, Wuhan, China, in 2006, and the master's degree in computer science from Korea University, Seoul, Korea, in 2008. He is currently pursuing the Ph.D. degree with the School of Engineering and Information Technology, University of New South Wales, Kensington, NSW, Australia. His research fields include biometric pattern recognition and biometric security.



Jiankun Hu is a Professor and the Research Director of the Cyber Security Laboratory, School of Engineering and IT, University of New South Wales, Australian Defence Force Academy, Canberra, Australia. He received the B.E. degree from Hunan University, Changsha, China, in 1983, the Ph.D. degree in control engineering from the Harbin Institute of Technology, Harbin, China, in 1993, and the master's degree in computer science and software engineering from Monash University, Clayton, VIC, Australia, in 2000. He was with Ruhr University, Bochum, Germany, where he was a prestigious German Alexander von Humboldt Fellow from 1995 to 1996, a Research Fellow with the Delft University of the Netherlands, Delft, The Netherlands, from 1997 to 1998, and a Research Fellow with the University of Melbourne, Parkville, VIC, Australia, from 1998 to 1999.

His main research interest is in the field of cyber security, including biometrics security, where he has authored many papers in high-quality conferences and journals, including the IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE. He has served in the editorial board of up to seven international journals, and served as the Security Symposium Chair of the IEEE flagship conferences of the IEEE ICC and the IEEE Globecom. He has received seven Australian Research Council (ARC) Grants, and is currently serving at the prestigious Panel of Mathematics, Information and Computing Sciences, ARC Excellence in Research for Australia Evaluation Committee.

Song Wang is a Senior Lecturer with the Department of Electronic Engineering, La Trobe University, Melbourne, VIC, Australia. She received the Ph.D. degree from the Department of Electrical and Electronic Engineering, University of Melbourne, Parkville, VIC. Her research areas are biometric security, blind system identification, and wireless communication.