2018

Biometrics based privacy-preserving authentication and mobile template protection

Wencheng Yang
Edith Cowan University, w.yang@ecu.edu.au

Jianku Hu

Song Wang

Qianhong Wu

10.1155/2018/7107295 Yang, W., Hu, J., Wang, S., & Wu, Q. (2018). Biometrics Based Privacy-Preserving Authentication and Mobile Template Protection. *Wireless Communications and Mobile Computing*, *2018*, 17 pages. Available here

Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 7107295, 17 pages
https://doi.org/10.1155/2018/7107295

Research Article

Biometrics Based Privacy-Preserving Authentication and Mobile Template Protection

Wencheng Yang, [1] Jiankun Hu, [2] Song Wang, [3] and Qianhong Wu [4]

[1] *Security Research Institute, School of Science, Edith Cowan University, WA 6027, Australia*
[2] *School of Engineering and Information Technology, University of New South Wales at the Australian Defence Force Academy (UNSW@ADFA), Canberra, ACT 2600, Australia*
[3] *School of Engineering and Mathematical Sciences, La Trobe University, VIC 3086, Australia*
[4] *School of Electronic and Information Engineering, Beihang University, Beijing, China*

Correspondence should be addressed to Jiankun Hu; j.hu@adfa.edu.au

Received 27 December 2017; Revised 26 April 2018; Accepted 10 May 2018; Published 12 June 2018

Academic Editor: Kim-Kwang Raymond Choo

Smart mobile devices are playing a more and more important role in our daily life. Cancelable biometrics is a promising mechanism to provide authentication to mobile devices and protect biometric templates by applying a noninvertible transformation to raw biometric data. However, the negative effect of nonlinear distortion will usually degrade the matching performance significantly, which is a nontrivial factor when designing a cancelable template. Moreover, the attacks via record multiplicity (ARM) present a threat to the existing cancelable biometrics, which is still a challenging open issue. To address these problems, in this paper, we propose a new cancelable fingerprint template which can not only mitigate the negative effect of nonlinear distortion by combining multiple feature sets, but also defeat the ARM attack through a proposed feature decorrelation algorithm. Our work is a new contribution to the design of cancelable biometrics with a concrete method against the ARM attack. Experimental results on public databases and security analysis show the validity of the proposed cancelable template.

1. Introduction

Nowadays, mobile devices, e.g., smartphone, have become one of our daily necessities. They are used to store personal data and handle private communication. Unfortunately, there are some privacy and security issues along with the use of smartphones; for example, a user's private data, e.g., photo, contacts, and bank details, can be compromised, if his/her smartphone without any protection is stolen or lost. Secret knowledge-based approaches, e.g., password or PIN, are commonly used for authentication. However, these methods rely heavily on the user to ensure continued validity, and poor use of password or PIN may lead to great security breaches [1].

Fingerprint recognition has been extensively used in various applications, e.g., authentication on mobile devices. With good recognition accuracy and high convenience, fingerprint-based authentication systems hold more markets than other biometrics, e.g., face, iris, and voice. Fingerprint authentication is usually composed of two stages, the enrollment stage and the verification stage [2]. In the enrollment stage, feature data extracted from a captured fingerprint image are considered as a template, which is stored in a database. In the verification stage, the query feature data, extracted in the same way as template feature data, are compared with the stored template, and a match or nonmatch verdict will be made.

The use of fingerprint authentication systems eliminates the need of remembering long passwords or PIN, which is the disadvantages of traditional password- or PIN-based authentication schemes. However, fingerprint-based biometric systems have one main drawback; that is, once a fingerprint is compromised, it will be lost forever. To address this issue, cancelable fingerprint templates [3], among other biometric template protection schemes, have been proposed. Instead of storing raw fingerprint data as a template, it is distorted through a one-way transformation function in the enrollment stage. Such a transformation is intentional and repeatable. One important property of cancelable fingerprint templates is noninvertibility, which means that it should be computationally hard to recover the raw fingerprint data from the transformed fingerprint template [4]. In the verification stage, the same transformation is applied to the query data. Matching between the transformed template and query is conducted in the transformed domain. In this way, if the stored template is compromised, a new version of it can be generated by changing the transformation parameter(s) [5].

1.1. Related Work

1.1.1. Mobile Biometrics. A lot research effort has been devoted to the design of more precise, usable, and secure biometric authentication schemes on mobile devices. For instance, in [16], Clarke and Furnell introduced a method for authenticating users by getting them to input telephone numbers or write text messages. This method is called biometric keystroke analysis. In [17], Kim and Hong proposed to use teeth together with voice to authenticate users, which is the first research work using the teeth and voice combination. The matching scores of each individual trait are calculated and fused using a weighted-summation operation. The experiments are conducted by using a dataset that contains one thousand teeth images and voices collected by smartphones. Later they proposed an enhanced multimodal authentication system [18], which adds another biometric trait, face, on top of teeth and voice to achieve better results.

In [19], Lee et al. designed a mobile multimodal biometric system based on finger-vein and fingerprint. The proposed system can obtain fingerprint and finger-vein images simultaneously and also is able to overcome some limitations of unimodal biometric systems, e.g., lack of accuracy. In [20], Tao and Veldhuis developed a face-based biometric authentication system on mobile devices, which contained detailed information about the process, including face detection, registration, illumination normalization, verification, and information fusion.

In [21], Chen et al. proposed a fingerprint-based remote authentication method using mobile devices. In their method, both fingerprint and password are involved to improve the security level of the system. Moreover, hashing functions are used to implement mutual authentication. In [22], a palmprint-based recognition system is proposed for mobile devices. Specifically, a hand-shaped guide window is introduced for fast image acquisition and an enhanced competitive code is used to cope with image variation.

In [23], Rattani et al. investigated gender prediction from ocular images acquired by smartphones so as to enhance the accuracy of the integrated biometric authentication and mobile healthcare system. In [24], Marsico et al. compared the performance of several participant methods in the Mobile Iris Challenge Evaluation-1 contest. Furthermore, some analysis is given to image covariate and interoperability.

Several survey papers, e.g., [25, 26], discussed the biometric authentication methods on mobile devices, including current development, trends, and challenges. The significance of template protection on mobile devices is described in [26]. However, we notice that most of above-mentioned biometric authentication methods do not protect the biometric template on mobile devices, which potentially put important personal information at risk. With good recognition accuracy and high convenience offered by fingerprint, in this paper, we propose a fingerprint-based authentication system using the cancelable technique to provide template protection on mobile devices.

1.1.2. Cancelable Biometrics. The concept of cancelable biometrics was initiated by Ratha et al. in [27]. Later, they constructed a practical cancelable fingerprint authentication system [4] by using three different transformation functions, namely, Cartesian transformation, polar transformation, and functional transformation. The transformation functions are able to distort the fingerprint minutiae feature into a new data format. This method is registration-based and hence relies on precise detection of the reference points, e.g., singular, core, or delta points. However, fingerprint uncertainty caused by displacement, nonlinear distortion, and rotation during the process of fingerprint capturing is unavoidable, thus making accurate registration hard to achieve. A matching error can possibly be caused by a registration error [28].

To relinquish the process of global registration and also reduce the impact of nonlinear distortion [29, 30], registration-free local structure based methods have been proposed; see, e.g., [5–11, 13, 14, 31–40]. In [5], Yang et al. proposed a cancelable template design based on geometric transformation. Each local Delaunay triangle-based structure instead of each single minutia acts as a unit to be transformed under the guidance of two transformation matrices. In [31], Farooq et al. presented a cancelable fingerprint template based on a set of triangles derived from any three minutiae. The features extracted from the set of triangles are further converted into the binary format. Then this binary string was randomly permuted into a different feature representation under the conduct of a user specific key. The cancelability of the feature representation can be achieved by applying different keys. Lee et al. [32] proposed an approach to calculating a rotation- and translation-invariant value from the orientation information of neighboring local regions around each minutia. The invariant value is then utilized as the input of two transformation functions to generate transformed features. The cancelable template is governed by these two transformation functions. In [33], in order to avoid global alignment, the authors used localized matching, which consists of matching minutia triplets constructed by each minutia and its two nearest neighbors. Invariant features extracted from these triplets are varied and secured by the symmetric hash functions. A major drawback of this approach is the assumption that the genuine query sample minutiae, being described as locations in a complex plane, are linearly transformed from the template minutia set. However, the most challenging issue for fingerprint minutia-based matching is the nonlinear elastic distortion of minutia locations. Therefore, this assumption is not realistic. Ahn et al. [6] applied geometrical properties, e.g., local relation, from minutiae triplets to hiding the minutiae information. Generation of these geometrical features is conducted via a transformation function in an attempt to keep the discriminating capability.

In [7], Yang et al. introduced the geometrically aligned and protected minutia vicinity for template protection. The proposed method transforms the original minutia vicinity by adding some parameter guided offsets into each minutiae group so as to destroy the original local topological relationship among those minutiae. The original minutia vicinity is defined by a minutia together with its M closest neighboring minutiae. In [34], minutia pairs applying redundant combinations of two minutiae points are formed to counter some image noise. A bit-string cancelable template is derived from the minutia pairs. Similarly to [31], the same user specific tokens are used to guarantee that the bit-string features are permuted in the same manner during both enrollment and verification stages. A different local structure represented by a 3D array was proposed in [35]. In this structure, each minutia is chosen as the reference point and other minutiae are rotated and translated based on the orientation and position of the reference point so as to map the minutiae into the 3D array. Each minutia after transformation falls into a specific cell of the 3D array and each cell is marked as 1 if more than one minutia locates in it; otherwise it is marked as 0. A resultant bit-string is then permuted by using a user specific PIN. Yang et al. [8] proposed to use a dynamic random projection method to protect the biometric features extracted from local structures composed of a reference minutia and three closest minutiae around it. Although this method can dynamically choose a projection matrix from a set of candidate projection matrices, it is a primitive direct biometric key generation technique, which has poor error tolerance for low quality fingerprint images.

Ahmad et al. [9] built a pair-polar coordinate-based alignment-free structure. The pair-polar structure uses the relative position of each minutia to other minutiae in a polar coordinate space. Three local features are extracted from any two minutiae and then a functional transformation is applied to these local features to achieve the resultant cancelable template. In [36], a circular region is constructed around each minutia and the circular region can be divided into different levels according to different radiuses. Then the circular regions are encrypted by two transformation functions and stored as the cancelable template. In [37], Jin et al. generated a revocable fingerprint template via a polar grid-based method. For each reference minutia, the polar transform is performed first to align the remaining minutiae. After that, a 3-tuple quantization technique is utilized to generate the local feature in the form of a bit-string. The user specific token based permutation technique is also utilized for feature transformation. Das et al. [38] proposed to use the minimum distance graphs, which involve a set of interminutia minimum distance vectors starting from the core point, as rotation- and translation-invariant features to conduct hash transformation so as to protect the original template.

In contrast to the pair-polar based structure proposed in [9], Wang and Hu [10–12, 41] mainly considered the noninvertible transformation functions. In [10], a densely infinite-to-one mapping method is presented to accomplish the transformation; in [11], a curtailed circular convolution is used to achieve noninvertible transformation; in [41], the identifiability condition in blind channel estimation is deliberately violated to protect the source input—the binary string's frequency samples; and, in [12], the binary biometric representations are securely protected by the partial Hadamard transformation, which transforms them into complex vectors. In [39], Wong et al. designed a multiline code for generating the cancelable fingerprint template. The multiline code is a string-based minutia descriptor extracted from a set of minutiae surrounding a virtual line within a specified range. Then a user specific secret key guided permutation is performed to achieve feature transformation. In [13], Jin et al. developed a two-dimensional random projection technique to secure the minutiae-based fingerprint template generated from minutia vicinities. Each minutia vicinity is formed by a minutia and three nearest minutiae around it. The feature matrix generated from a set of minutia vicinities is transformed/mapped onto a random subspace determined by an external orthogonal random matrix, which is generated by a user specific token. In [14], Jin et al. adopted the same local structure as [13] but incorporated a different noninvertible transformation method named randomized graph-based hamming embedding (RGHE) to protect the original features. In [40], Zhang et al. presented two methods, which are a designed combo plate and a functional transformation, to produce cancelable templates based on the MCC code, which associates a local structure to each minutia [42]. Note that the method named P-MCC in [42] is not a cancelable template as it does not provide the property of revocability. Subsequently, a partial permutation based scheme named 2P-MCC [15] was proposed to add revocability to P-MCC. However, 2P-MCC suffers from the ARM. P-MCC is not revocable, which means that the feature vector $\widehat{V}$ that contains k binary values in P-MCC remains unchanged in different applications. The 2P-MCC scheme uses a user specific key s as the index and chooses c ($0 < c \leq k$) binary values from those k binary values of $\widehat{V}$ to create a new feature vector $\ddot{V}$. When unlinkability is required, at least one element of the c binary values from any two templates, e.g., $\ddot{V}$, should be different. By combining templates from at most (k-c+1) applications, the feature vector $\widehat{V}$can be restored. Once feature vector $\widehat{V}$ is obtained by the adversary and due to $\widehat{V}$ being the same in different applications, the adversary can verify the correctness of the inverted feature generated from template $\ddot{V}$ and the user specific key s by comparing it with $\widehat{V}$.

In [43], Kaur and Khanna presented a cancelable biometric method, named random slop, which can reduce the feature dimensions by up to 75%. This method has been tested on many biometric databases, such as face, palmprint, palmvein, and fingervein, except fingerprint, although it can be implemented to fingerprint features. In order to further enhance recognition accuracy and security of cancelable unibiometric systems, in [44], Paul et al. developed a cancelable biometric template creation algorithm using random biometric feature fusion, random projection, and selection based on face and ear. In [45], Yang et al. proposed a fingerprint and fingervein based cancelable multibiometric system, in which a feature-level fusion strategy with three fusion options are designed. In the meantime, an enhanced partial discrete

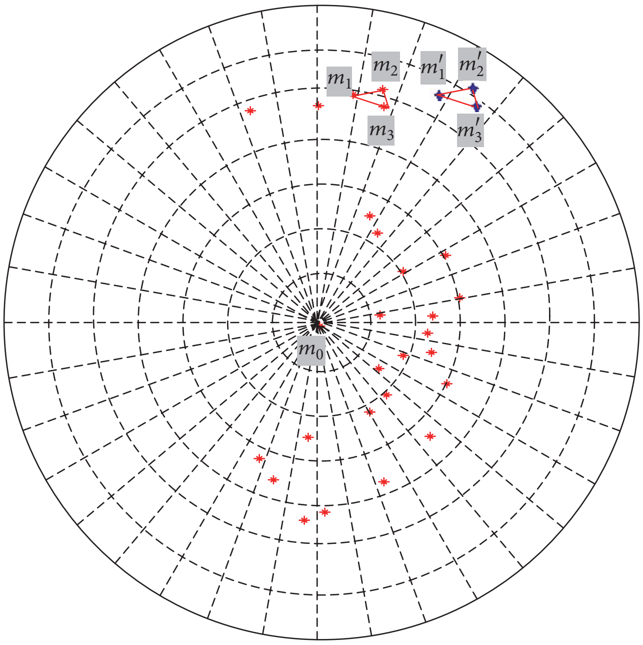


Figure 1: A polar space centering around minutia m_0.

Fourier transform based noninvertible transformation is applied.

1.2. Motivation and Contributions. From the above-mentioned cancelable fingerprint template systems, it is observed that the rotation- and transformation-invariant local region based structures are employed and the main difference between these local structures is the region size. For example, small-sized local structures are used in [6–8, 13, 14, 33]. In these systems, the local structures are only composed of one reference minutia and two or three of its neighboring minutiae. Small-sized structures can resist nonlinear distortion to some extent. However, since these local structures only contain a moderate number of minutiae, the feature data extracted from them are not discriminative enough. By contrast, relatively large local structures are employed in [9–11, 31, 34, 35, 37–40]. Large-sized structures consist of more minutiae and tend to include relatively more information that can be exploited for matching. However, the positional change of minutiae for large-sized structures is likely to occur under nonlinear distortion, especially when minutiae are located far away from the reference point. Because of nonlinear distortion, for example, minutiae m_1, m_2, and m_3 in the template image and their corresponding minutiae m_1', m_2', and m_3' in the query image are possibly located in different cells in a polar coordinate system, as shown in Figure 1. To strike a balance and achieve good matching performance, some authors [32, 36] proposed to use parameters to control the region size. However, testing different parameter settings in a practical authentication process would create additional computational load and resource burden or even be infeasible.

Another issue that troubles the existing cancelable template systems is the security concern. The methods in [5, 31, 34, 35, 37, 39] use permutation matrices for feature transformation. Since the permutation functions are invertible [10], original fingerprint features are not secured safely if the permutation matrices are compromised. Although the methods in [7, 9–15, 40, 41] that use the noninvertible many-to-one mapping strategy can avoid the above issue, they suffer from the attacks via record multiplicity (ARM) [46, 47], if multiple transformed templates and their corresponding transformation parameters are acquired by an adversary. Readers can refer to [46, 47] for more details about the ARM.

To address the above issues, in this paper, we propose a new cancelable fingerprint template system. Not only can the proposed system reduce the impact of nonlinear distortion on those minutiae that are located far away from the reference point, but it also can defend the system against the ARM attack. In particular, the new cancelable fingerprint template system processes both local and global structures and fuses two different schemes at the score level, so that the overall system achieves better recognition accuracy than a single scheme only. The overall processing flow of the proposed system is shown in Figure 2. Specifically, in the enrollment stage, two feature sets, the polar coordinate-based feature set (T1) and the Delaunay triangulation-based feature set (T2), are extracted from the polar coordinate-based local structure and Delaunay triangulation-based global structure, respectively. Next, feature set T1 is processed by the proposed feature decorrelation algorithm and then varied by a random projection transformation function. Feature set T2 is permutated under the guidance of the feature codes. Both transformed feature sets, T1 and T2, are stored in the database. In the verification stage, the same transformations used in the enrollment stage are applied to the query feature sets, Q1 and Q2. Matching between the transformed template and query feature sets is conducted in the transformed domain.

The main contributions of this paper are highlighted as follows.

(1) Two schemes, polar coordinate-based scheme and Delaunay triangulation-based scheme, are utilized and fused on the score level. Specifically, the polar coordinate-based scheme uses the feature set from the polar coordinate space and acts as our basic scheme, which can provide reasonable feature discrimination. The Delaunay triangulation-based scheme that uses the feature set from Delaunay triangulation serves as a complement to the basic scheme. It can effectively reduce the negative impact of nonlinear distortion on the minutiae that are located far away from the reference minutia. As a result, compared with the system that only uses the polar coordinate-based scheme, higher recognition accuracy is achieved.

(2) A main reason that cancelable biometrics suffer the ARM attack is due to feature correlation which exists among cancelable templates stored across multiple applications but actually derived from the same biometric features. To address the issue, we propose a feature decorrelation algorithm so that the feature vectors, which are generated from the same feature set, are uncorrelated in different applications. Without feature correlation, the adversary would not have adequate information to determine the original feature data.

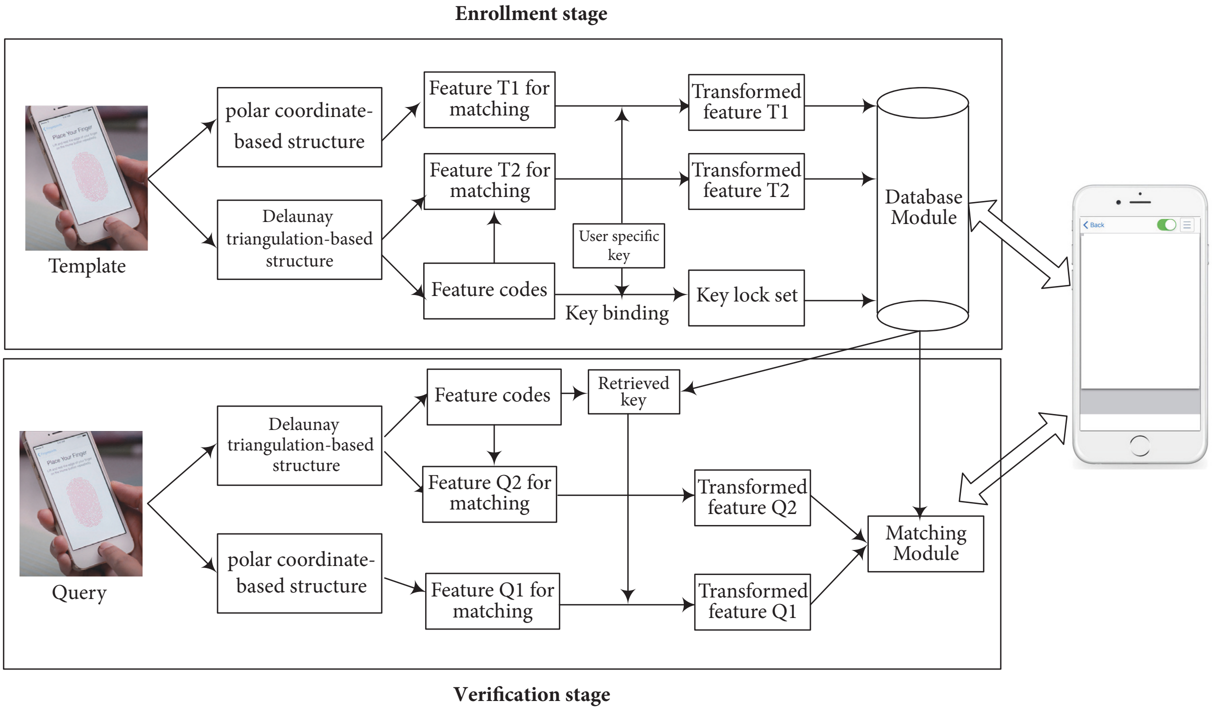


Figure 2: The overall processing flow of the proposed system (Features T1, T2, Q1, and Q2 represent the feature sets from the polar coordinate-based structure and Delaunay triangulation-based structure of the template image and query image, respectively).

The rest of the paper is organized as follows. In Section 2, two feature sets, polar coordinate-based feature set and Delaunay triangle-based feature set, are introduced. The proposed cancelable fingerprint authentication system, which can defeat the ARM attack, is presented in Section 3. In Section 4, experimental results and security analysis are demonstrated and discussed. The conclusion is given in Section 5.

2. Generation of Two Feature Sets

In this section, we introduce two feature sets that are extracted from the polar coordinate-based and Delaunay triangulation-based structures, respectively. These two structures are derived from the same minutiae set of a fingerprint image. Each polar coordinate-based structure is composed of a reference minutia and other minutiae in a predefined range. The use of the polar coordinate system allows the relationships between the reference minutia and other minutiae to be readily defined and measured. The Delaunay triangulation-based structure formed by a set of minutiae is a triangulation where no minutia in that set of minutiae is inside the circumcircle of any triangle in the triangulation. Specifically, given a set of minutiae $M = (m_0, m_1, m_2, \ldots, m_{N-1})$, where N is the number of minutiae, each minutia $m_{i\in[0,N-1]}$ can be represented by a vector $(x_i, y_i, \theta_i, t_i)$, where x_i and y_i are the x, y coordinates in the Cartesian coordinate system, θ_i is the orientation in the range of $[0, 2\pi)$, and t_i is the minutia type. For each fingerprint image, the following two feature sets are generated from the above two structures.

2.1. Polar Coordinate-Based Feature Set. In the polar coordinate-based structure, if the minutia, e.g., m_0, is considered as the origin of the polar coordinate and the remaining minutiae in range of R (=300 pixels) are rotated and translated with respect to m_0 such that the orientation of m_0 equals 0 degree in the polar coordinate system, then any minutia $m_{i\in[1,N-1]}$ can be converted and expressed as a triplet $(\rho_i, \alpha_i, \beta_i)$, where $0 < \rho_i \le 300$ is the radial distance, $0 < \alpha_i \le 2\pi$ is the radial angle, and $0 < \beta_i \le 2\pi$ is the relative orientation of minutia m_i to m_0. An example of the polar space centered around minutia m_0 is shown in Figure 1. In order to tolerate small distortion, polar grid-based quantization [35] is performed on all the minutiae in the range of R. We assume that the step sizes of ρ_i, α_i, and β_i are s_ρ, s_α, and s_β, respectively ($5 \le s_\rho \le 20$ and $\pi/12 \le s_\alpha, s_\beta \le 2\pi/9$). Then the polar space centered around m_0 can be quantized into a 3D cube containing $l_C = L \times S \times H$ cells, where $L = \lfloor R/s_\rho \rfloor$, $S = \lfloor 2\pi/s_\alpha \rfloor$, and $H = \lfloor 2\pi/s_\beta \rfloor$. The cell where the minutia m_i is located in the 3D cube is $(\rho_i^q, \alpha_i^q, \beta_i^q)$, where $\rho_i^q = \lfloor \rho_i/s_\beta \rfloor$, $\alpha_i^q = \lfloor \alpha_i/s_\alpha \rfloor$, and $\beta_i^q = \lfloor \beta_i/s_\beta \rfloor$. By this means, we obtain a vector $P(m_0)$ of length l_C containing only ‘0’s and ‘1’s, in which ‘1’ means the appearance of one or more minutiae in the corresponding cell. l_C varies under different parameter settings of s_ρ, s_α, and s_β. It is obvious that when these parameter settings change, the value of l_C changes accordingly. In our application, different parameter settings are chosen for different databases in order to achieve best performance. Within the value range of these parameter settings, the largest value of l_C that can be obtained is 34560. Therefore, we use a fixed value of $l_C = 34560$ for all the chosen databases and pad ‘0’ to those feature vectors with elements

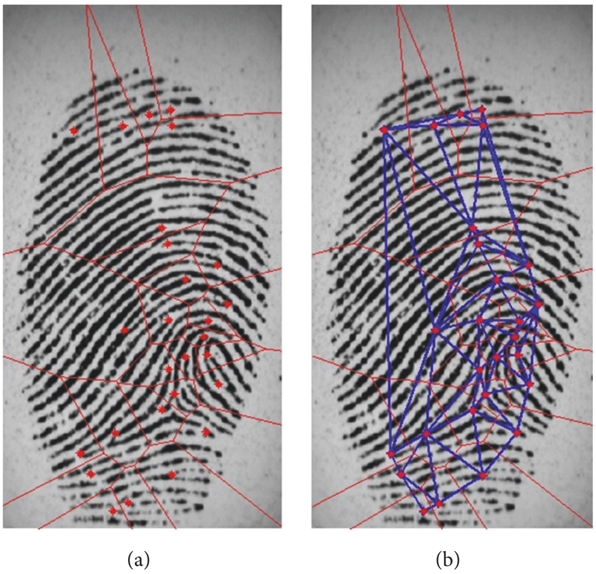

(a) (b)

Figure 3: An example of (a) Voronoi diagram, (b) Delaunay triangulation (bold line).

less than 34560. By applying the above approach to every minutia in the set of minutiae $M = (m_0, m_1, m_2, \ldots, m_{N-1})$, a polar coordinate-based feature set $C = \{P(m_i)\}_{i=0}^{N-1}$ is generated.

2.2. Delaunay Triangulation-Based Feature Set. As a complement to the polar coordinate-based feature set, we propose the second feature set, which is extracted from the Delaunay triangulation-based structure and takes advantage of the desirable features [48–50] of Delaunay triangulation. In the presence of nonlinear distortion, Delaunay triangulation has a stable local neighborhood structure. Minutiae will keep the same neighboring structure if the nonlinear distortion does not move minutiae out of the tolerance region. Also, noise in fingerprint images influences the Delaunay triangulation only locally. Spurious or missing minutiae affect only those local Delaunay structures which contain them. A brief description about the generation of a Delaunay triangulation is given below; readers can refer to [51] for more details.

For the set of minutiae $M = (m_0, m_1, m_2, \ldots, m_{N-1})$, a Voronoi tessellation, which divides the whole fingerprint image region into several smaller regions centering on each minutia, is created first as shown in Figure 3(a). All the points in the region around m_i are closer to m_i than to any other minutia. The Delaunay triangulation is generated by connecting the centers of every neighboring region as shown in Figure 3(b).

Assume that there are N_1 Delaunay triangles generated from N minutiae; several invariant features can be defined from each Delaunay triangle. Taking triangle $\Delta m_1 m_2 m_3$ as an example, four rotation- and translation-invariant features are defined as follows:

(i) $o_{m_1 m_2}$ is the orientation differences between m_1 and m_2.

(ii) $l_{m_2 m_3}$ is the length of edge $m_2 m_3$.

(iii) α_{m_3} is the angle between edge $m_1 m_3$ and $m_2 m_3$.

(iv) $t_{m_1 m_2 m_3}$ is the concatenation of minutia type of m_1, m_2, and m_3.

$0 < o_{m_1 m_2} \leq 2\pi$, $0 < l_{m_2 m_3} \leq 300$, and $0 < \alpha_{m_3} \leq 2\pi$. A feature data set, e.g., $f_{m_1 m_2 m_3} = (o_{m_1 m_2}, l_{m_2 m_3}, \alpha_{m_3}, t_{m_1 m_2 m_3})$, can be extracted from each Delaunay triangle. To tolerate the variation caused by nonlinear distortion that is inherent in fingerprint images, quantization is applied to each feature set. The quantization step sizes are set to be s_o, s_l, and s_α for $o_{m_1 m_2}$, $l_{m_2 m_3}$, and α_{m_3}, respectively ($15 \leq s_l \leq 25$, $\pi/12 \leq s_o, s_\alpha \leq \pi/9$). Each element of $f_{m_1 m_2 m_3}$, after quantization, can be expressed as $o^q_{m_1 m_2}$, $l^q_{m_2 m_3}$, $\alpha^q_{m_3}$, and $t_{m_1 m_2 m_3}$. If $o^q_{m_1 m_2}$, $l^q_{m_2 m_3}$, $\alpha^q_{m_3}$, and $t_{m_1 m_2 m_3}$ are represented by a_1, a_2, a_3, and a_4 bits, respectively, then the triangle $\Delta m_1 m_2 m_3$ can be represented by a bit-string $f^q_{m_1 m_2 m_3}$by putting them in sequence together. The integer value of this bit-string falls in the range of $[0, l_D - 1]$, where $l_D = 2^{a_1 + a_2 + a_3 + a_4}$. With N_1 Delaunay triangles constructed from a given fingerprint image, each of them should match a value in $[0, l_D - 1]$ and so the corresponding bin is indexed by 1, as shown in [34]. As a result, the Delaunay triangulation-based feature set can be represented by a binary vector D of length l_D.

We now explain why we add the second feature set. In the Delaunay triangulation-based feature set, each Delaunay triangle rather than each minutia is treated as a feature unit because a Delaunay triangle is more robust against nonlinear distortion than each individual minutia. For example, as mentioned in Section 1, minutiae m_1, m_2, and m_3 in the template image may not seem to match their corresponding minutiae m_1', m_2', and m_3' in the query image in a polar coordinate system since they fall in different cells due to nonlinear distortion, as shown in Figure 1. However, if we consider the triangle $\Delta m_1 m_2 m_3$ constituted by minutiae m_1, m_2, and m_3 as a unit, no matter where $\Delta m_1 m_2 m_3$ is moved, features such as the edge length and angle, extracted from it,

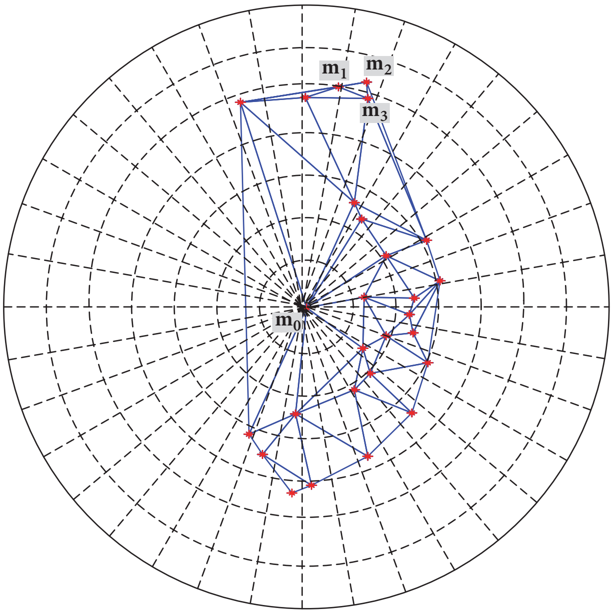


FIGURE 4: Delaunay triangulation-based structure centering around m_0.

still remain invariant. Thus, using these features, $\Delta m_1 m_2 m_3$ and $\Delta m'_1 m'_2 m'_3$ can match each other.

3. Design of the Cancelable Fingerprint Authentication System

In this section, we present the two general stages included in the proposed cancelable fingerprint authentication system.

3.1. Enrollment Stage. In the enrollment stage, the original feature sets are transformed. The detail of the enrollment stage is explained below.

Given a template image F^T (letter T means template), the untransformed feature sets C_T and D_T as introduced in Section 2 can be extracted from the polar coordinate-based and Delaunay triangulation-based structures as shown in Figure 4. However, feature sets C_T and D_T are vulnerable. Because if the adversary acquires the vector C_T, he/she would be able to know the minutiae's location in the 3D cube. Subsequently the feature triplet (ρ, α, β) of each minutia can be recovered. Similarly, it is not difficult to reveal the original minutiae information from D_T. Hence, it is crucial to protect the feature sets C_T and D_T. To achieve this, the polar coordinate-based scheme and the Delaunay triangulation-based scheme are utilized to protect each element of C_T and D_T, respectively.

3.1.1. The Polar Coordinate-Based Scheme. In the polar coordinate-based scheme, the feature set is processed by a feature decorrelation algorithm and then varied by a random projection matrix $\mathscr{M}$ generated under the participation of a user specific key k_{pm}. The loss of key k_{pm} means the loss of the projection matrix $\mathscr{M}$. The feature decorrelation algorithm can eliminate feature correlation in different applications, thus making it robust against the ARM attack.

INPUT: the original feature $P(m_i)$
Process:
Step 1: Each position V_p of value 1 that is located in the binary string $P(m_i)$, is input into a folding function $f_P = \text{mod}(V_p, L_C)$, where L_C is an application-specific parameter and set to be smaller than l_C. $\text{mod}(\cdot)$ is a modulo operation, for example, mod(7,5) = 2 and mod(12,5) = 2.
Step 2: With each value of 1 in $P(m_i)$ relocated to a new position depending on f_P, a new binary string $\mathscr{P}(m_i)$ of length L_C is generated.
Step 3: $\mathscr{P}(m_i)$ is converted into a real-value vector through the Discrete Fourier Transform (DFT) as $\mathbb{P}(m_i) = DFT(\mathscr{P}(m_i))$.
OUTPUT: decorrelated feature $\mathbb{P}(m_i)$

ALGORITHM 1: Feature decorrelation algorithm.

For an element, e.g., $P(m_0)$, of the feature set $C_T = \{P(m_i)\}_{i=0}^{N^T-1}$, where N^T is the number of minutiae in the template image F^T, before performing random projection, it is first processed by the feature decorrelation algorithm as shown in Algorithm 1. This feature decorrelation algorithm is useful because $P(m_i)$ only includes values of 1 and 0 and has a sparse distribution, which might restrict the search space if the random projection is directly implemented on it. Furthermore, if C_T is applied in multiple applications, its feature correlation can be utilized by the adversary to launch the ARM attack. For the above reasons, Algorithm 1 is proposed to eliminate feature correlation in different applications.

It follows from Steps 1 and 2 in Algorithm 1 that the new binary string $\mathscr{P}(m_i)$, generated from the original feature $P(m_i)$, can be varied by simply adjusting the application-specific parameter L_C in different applications. Note that even if one bit in $\mathscr{P}(m_i)$ is changed, the output vector $\mathbb{P}(m_i)$ will be totally different due to the nature of the Discrete Fourier Transform (DFT) in Step 3. Therefore, feature correlation does not exist in the real-value vector $\mathbb{P}(m_i)$ used in different applications.

The modulo operation in Step 1 is a many-to-one mapping and controlled by the parameter L_C. Different L_C values may lead to varying matching performance, which is discussed in Case 3 of Section 4.1. Under the assumption that the random projection based transformation is conquered, the modulo operation might not be strong enough to safeguard $P(m_i)$ from the compromised $\mathscr{P}(m_i)$ if L_C is set to be a large value. For example, when $l_C = 34560$ and L_C is set to be 20000, for values of '1' that appear in $\mathscr{P}(m_i)$ from positions 1 to 14560, e.g., 123, its original position in $P(m_i)$ only has three possible locations, either 123 or 20123 or both. To increase security, we further propose Algorithm 2 as an enhancement of Algorithm 1.

Algorithm 2 produces a binary code based segment permutation before carrying out the steps in Algorithm 1.

```
INPUT: the original feature $P(m_i)$
Process:
Step 1: $P(m_i)$ is divided into two parts, $P_1$ and $P_2$,
    where $P_1$ contains the first $L_C$ elements of $P(m_i)$,
    while $P_2$ contains the remaining elements.
Step 2: $P_1$ is evenly divided into $N_S$ segments, so
    $P_1 = \{S_j\}_{j\in 1}^{Ns}$ and each segment $S_j$ is of length $L_S = L_C/N_S$.
Step 3: For each segment $S_j$, calculate $\phi_j = sum(k * S_j(k))$,
    where $1 \le k \le L_S$. $\phi_j$ is a weighted sum of
    position $k$ and its binary value for segment $S_j$. Then
    all the elements in $S_j$ are circularly shifted left by $\phi_j$
    bits to generate a permutated segment $S'_j$.
Step 4: All the permutated segments $\{S'_j\}_{j\in 1}^{Ns}$ are
    concatenated into a new binary vector $P'_1$, which is
    further concatenated with $P_2$ to create a binary vector
    $P'(m_i) = P'_1 \parallel P_2$
Step 5: Perform Steps 1 to 3 in Algorithm 1 with
    input $P'(m_i)$.
OUTPUT: decorrelated feature $\mathbb{P}(m_i)$
```

Algorithm 2: Enhanced feature decorrelation algorithm.

The segment permutation is guided by an on-the-fly binary code $\phi_j = sum(k * S_j(k))$, which is calculated using the elements' positions and values instead of a user specific key, so its security does not suffer from the lost key attack. Moreover, the binary code ϕ_j is calculated based on just L_S binary elements in S_j, which is only a portion of the original feature $P(m_i)$. This means that the error in one ϕ_j does not affect the permutation of other segments of $P(m_i)$. The parameter L_S is the length of each segment, which impacts on the matching performance and security strength. A larger value of L_S means that it would require more computational effort to invert S'_j to S_j, but it would be more likely to cause errors in ϕ_j, thus having a negative effect on matching accuracy. The matching performance and security related to parameter L_S are discussed in Case 3 of Section 4.1 and Section 4.4, respectively. We remark that Algorithm 2 offers an alternative pathway for tighter security at the expense of performance, as shown in Section 4.1 and that when $L_S = 1$, Algorithm 2 reverts to Algorithm 1.

The output vector $\mathbb{P}(m_i)$ of Algorithm 1 or 2 is then transformed by projecting onto a random space with the help of the random projection matrix $\mathscr{M}$ of size $X \times Y$, where $X = L_C$. The transformation of $\mathbb{P}(m_i)$ using the random matrix $\mathscr{M}$ can be compactly expressed by

$$\widehat{P}(m_i) = \mathbb{P}(m_i) \times \mathscr{M}, \tag{1}$$

where $\widehat{P}(m_i)$ is the inner product of $\mathbb{P}(m_i)$ and $\mathscr{M}$. The above transformation makes the dimension of transformed feature $\mathbb{P}(m_i)$ reduced to Y so that the feature set $\mathbb{P}(m_i)$ is protected. Different values of Y affect the performance of the proposed system, which is discussed in Section 4. Moreover, revocability is achieved—a new template can be issued easily by just changing the user specific key k_{pm}, which is analyzed in Section 4. By applying Algorithm 1 or 2, and random projection to each element of C_T, C_T can be transformed to be $\widehat{C_T} = \{\widehat{P}(m_i)\}_{i=0}^{N^T-1}$.

3.1.2. The Delaunay Triangulation-Based Scheme. In the Delaunay triangulation-based scheme, the feature set D_T, which is a binary vector of length l_D, is transformed by permutation guided by feature codes. Specifically, for each triangle, e.g., $\Delta m_1 m_2 m_3$, a feature code is calculated first. Some stable local features can be used to obtain the feature code. These features are defined as follows:

(i) $o_{m_2 m_3}$ is the orientation differences between m_2 and m_3.

(ii) $l_{m_1 m_2}$ is the length of edge $m_1 m_2$.

(iii) $l_{m_1 m_3}$ is the length of edge $m_1 m_3$.

(iv) α_{m_1} is the angle between edges $m_1 m_2$ and $m_1 m_3$.

$0 < o_{m_2 m_3} \le 2\pi$, $0 < l_{m_1 m_2}, l_{m_1 m_3} \le 300$, and $0 < \alpha_{m_1} \le 2\pi$. Quantization is applied to each of these features to tolerate small variation. Accordingly, a quantized four-element array $f^q_{m_1 m_2 m_3} = [o^q_{m_1 m_2}, l^q_{m_1 m_2}, l^q_{m_1 m_3}, \alpha^q_{m_1}]$ can be extracted from triangle $\Delta m_1 m_2 m_3$ which is further input into (2), based on [52], to generate the feature code $f^c_{m_1 m_2 m_3}$, which corresponds to the triangle $\Delta m_1 m_2 m_3$, as follows:

$$\begin{aligned} f^c_{m_1 m_2 m_3} &= \Upsilon^3 f^q_{m_1 m_2 m_3}(4) + \Upsilon^2 f^q_{m_1 m_2 m_3}(3) \\ &\quad + \Upsilon^1 f^q_{m_1 m_2 m_3}(2) + \Upsilon^0 f^q_{m_1 m_2 m_3}(1), \end{aligned} \tag{2}$$

where $\Upsilon = f(f^q_{m_1 m_2 m_3}(1), \dots, f^q_{m_1 m_2 m_3}(4), \Phi)$. Υ is the output of function $f(\cdot)$ corresponding to inputs $f^q_{m_1 m_2 m_3}(1)$ to $f^q_{m_1 m_2 m_3}(4)$ and a random parameter Φ. Φ is set to be different in different applications, which enables Υ to be diverse. In this way, one set of feature codes $\{f^c_i\}_{i=1}^{N_1^T}$ are computed as such from F^T, where N_1^T is the number of Delaunay triangles in the template image F^T. After the feature code $f^c_{m_1m_2m_3} \in \{f_i^c\}_{i=1}^{N_1^T}$ is obtained, the original bin to which $\Delta m_1m_2m_3$ is matched in D_T, which is decided by its corresponding integer value $f^{it}_{m_1m_2m_3}$, can be permutated under the guidance of the feature code $f^c_{m_1m_2m_3}$. So the new bin becomes $f^{it}_{m_1m_2m_3}+f^c_{m_1m_2m_3}$. To increase the permutation randomness, an extra key guided permutation could be added on top of above permutation. By the same token, bins of other Delaunay triangles can be shuffled to new locations determined by their corresponding feature codes in $\{f_i^c\}_{i=1}^{N_1^T}$. The vector array D_T, after permutation, is transformed into a new version $\widehat{D}_T$. Since each feature code in $\{f_i^c\}_{i=1}^{N_1^T}$ is generated from its corresponding Delaunay triangle feature and not saved in the database or on the smart card, it is hard to figure out the original bin location, even if the new bin position is acquired by the adversary from $\widehat{D}_T$.

The reason why permutation is used to protect the feature set D_T rather than random projection, as in the case of the feature set C_T, is that permutation does not reduce feature dimension, which can help minimize the impact on the system's matching performance. Moreover, feature code set is not saved in the database or on the smart card, which greatly improves the security of the original feature set D_T. Most importantly, noise in fingerprint images influences the Delaunay triangulation only locally. Spurious or missing minutiae affect only those local Delaunay structures which contain them. Each Delaunay triangle is formed by only three minutiae, which means that if a feature code, e.g., $f^c_{m_1m_2m_3}$, is incorrect, it only influences the permutated position of that Delaunay triangle, from which the feature code is generated. On the contrary, each polar coordinate-based structure is composed of a reference minutia and a number of other minutiae (usually more than ten minutiae) in a certain range. Obviously, the chance of generating an incorrect feature code from the polar coordinate-based structure is much higher than that from the Delaunay triangle, which only includes three minutiae. If we choose fewer minutiae from the polar coordinate-based structure, say, only three minutiae are chosen, which is the same number as that in the Delaunay triangle, then how to correctly determine the three minutiae from a query image and their corresponding minutiae from a template image is a tricky issue, especially under the presence of biometric uncertainty, e.g., spurious or missing minutiae. Therefore, compared with permutation, random projection is a better option for the protection of the feature set C_T.

3.2. Verification Stage. In the verification stage, the same projection matrix used in the enrollment stage is used to transform the polar coordinate-based feature set extracted from the query image, and the Delaunay triangulation-based feature set can also be transformed under the guidance of the feature codes. Finally, matching between the template image F^T and query image F^Q is conducted using the transformed features in the transformed domain. The detailed steps of the verification stage are explained below.

Given a query image F^Q (letter Q means query), untransformed query feature sets C_Q and D_Q together with a set of feature codes $\{f_j^c\}_{j=1}^{N_1^Q}$ are extracted first, where $C_Q = \{P(m_i)\}_{i=0}^{N^Q-1}$, N^Q is number of minutiae, and N_1^Q is the number of Delaunay triangles in the query image F^Q.

In the polar coordinate-based scheme, suppose that $\widehat{P}^Q(m_j)$ denotes the j^{th} transformed local feature of the query and $\widehat{P}^T(m_i)$ denotes the i^{th} transformed local feature of the template. Then the similarity score between them is calculated by

$$S_C = 1 - \frac{\left\| \widehat{P}^T(m_i) - \widehat{P}^Q(m_j) \right\|_2}{\left\| \widehat{P}^T(m_i) \right\|_2 + \left\| \widehat{P}^Q(m_j) \right\|_2}, \tag{3}$$

where $\|\cdot\|_2$ denotes the 2-norm. Each polar coordinate-based local feature in the query is compared with each polar coordinate-based local feature in the template to output a similarity score. Upon the completion of the comparison, there will be a score matrix of size $N^T \times N^Q$. The maximum value $S_{C\max}$ in this score matrix is considered to be the matching score of the first feature set between the template and query images.

In the Delaunay triangulation-based scheme, the set D_Q of the query is permuted under the guidance of the feature codes to generate the transformed version $\widehat{D}_Q$. The permutation procedure is the same as that in the enrollment stage. The similarity score between $\widehat{D}_Q$ and $\widehat{D}_T$ can be calculated as

$$S_D = \frac{\sum_{k=1}^{2^{l_D}} \left(\widehat{D}_{Q,k} - \overline{\widehat{D}_Q} \right) \left(\widehat{D}_{T,k} - \overline{\widehat{D}_T} \right)}{\sqrt{\sum_{k=1}^{2^{l_D}} \left(\widehat{D}_{Q,k} - \overline{\widehat{D}_Q} \right)^2 \sum_{k=1}^{2^{l_D}} \left(\widehat{D}_{T,k} - \overline{\widehat{D}_T} \right)^2}}, \tag{4}$$

where $\overline{\widehat{D}}$ represents the mean value.

The final score between the template image F^T and query image F^Q is calculated using both $S_{C\max}$ and S_D from the polar coordinate-based scheme and the Delaunay triangulation-based scheme, respectively, that is,

$$\begin{aligned} \mathit{final\_score} = {} & \rho_C \times \mathit{norm}\left(S_{C\max}\right) + \left(1 - \rho_C\right) \\ & \times \mathit{norm}\left(S_D\right), \end{aligned} \tag{5}$$

where $\mathit{norm}(\cdot)$ is a score normalization function; ρ_C is the weight of score $S_{C\max}$, which is set to be 0.7 in our application so as to give more relevance to the use of our basic scheme, the polar coordinate-based scheme. If the final matching score $\mathit{final\_score}$ is larger than a predefined threshold S_t, then the template image F^T and query image F^Q are considered to be matching.

4. Experimental Results and Security Analysis

Three databases (DB1, DB2, and DB3) of FVC2002 and one database (DB2) of FVC2004 were used to evaluate the proposed fingerprint cancelable template design. Detailed

TABLE 1: Detailed information about the databases used in our experiments.

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

information about these four databases is listed in Table 1. To extract minutiae from fingerprint images, a software package called VeriFinger 4.0 from Neurotechnology [53] was utilized.

The performance of the proposed fingerprint cancelable template is evaluated by four performance indices, namely, genuine acceptance rate (GAR), false acceptance rate (FAR), false rejection rate (FRR), and equal error rate (EER). GAR is defined as the ratio of successful genuine tests to the total number of genuine tests. FAR is defined as the ratio of successful imposter tests to the total number of imposter tests, FRR (=1-GAR) is defined as the ratio of failed genuine tests to the total number of genuine tests, and EER is defined as the error rate when FRR and FAR are the same. For all the databases, the 1VS1 matching protocol and standard FVC matching protocol [42] were utilized in the experiments. In the 1VS1 matching protocol, the first two images of each finger were chosen for testing, while, in the FVC matching protocol, all eight images of each finger were used.

4.1. Performance of the Proposed System under the Lost Key Attack. The lost key attack was tested in the experiments by allocating the same key k_{pm} to all the genuine and imposter tests. Three different cases were evaluated as follows.

Case 1 (performance of the system under two different instances). The performance of the system under three different instances is compared:

(i) Instance 1: using only the basic polar coordinate-based scheme

(ii) Instance 2: using only the Delaunay triangulation-based scheme

(iii) Instance 3: combining the polar coordinate-based scheme and Delaunay triangulation-based scheme

The polar coordinate-based scheme in both instances 1 and 3 uses Algorithm 1 and the same parameter settings $L_C = 20000$. The comparison between Instances 1, 2, and 3 is conducted over the database FVC2002 DB2 using the 1VS1 matching protocol. ROC curves are drawn in Figure 5. It can be observed from Figure 5 that Instance 3 (EER = 0.64%) performs better than Instance 1 (EER = 1.00%) and Instance 2 (EER = 2.00%), which only uses the single structure under the same parameter setting ($Y = 300$).

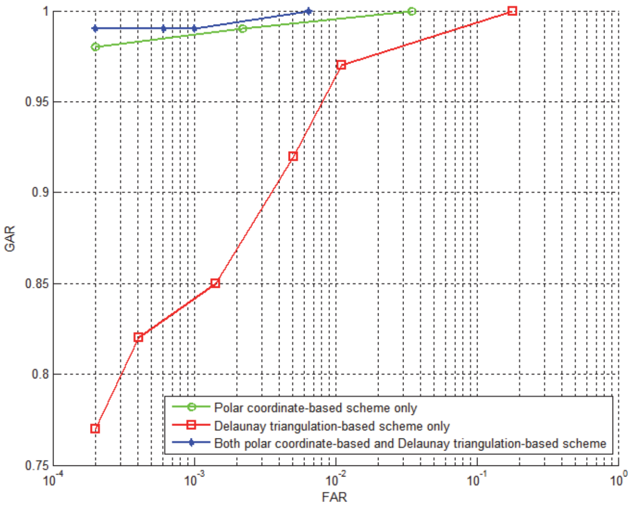


FIGURE 5: Performance of Instance 1 (the polar coordinate-based scheme only), Instance 2 (the Delaunay triangulation-based scheme only), and Instance 3 (both the polar coordinate-based scheme and Delaunay triangulation-based scheme).

Case 2 (performance of the proposed system using the untransformed feature sets and the transformed feature sets). Performance of the proposed system that uses the untransformed feature sets and the transformed feature sets was tested to evaluate the effect of feature transformation using Algorithm 1 and parameter settings $L_C = 20000$. This test was conducted on two databases, FVC2002 DB2 and DB3 with the 1VS1 matching protocol. For database DB2, we obtained EER = 0.62% using the untransformed feature sets and EER = 0.64% using the transformed feature sets. For database DB3, EER = 4% was obtained using the untransformed feature sets, while EER = 4.57% was obtained with the transformed feature sets. In this case, matching performance becomes worse than that before feature transformation.

Case 3 (effect of different parameter settings on the performance of the proposed system). The different parameter settings of L_C and L_S in Algorithms 1 and 2 result in a trade-off between security and matching performance [54]. Here, we investigate the effect of different parameter settings of L_C and L_S on the system's matching performance over databases FVC2002 DB2 and DB3 using the 1VS1 matching protocol. As shown in Table 2, choosing a smaller value of L_C in Algorithm 1 makes matching performance worse. This is because the modulo operation in Algorithm 1 is a many-to-one mapping and smaller L_C increases the possibility of

Table 2: EER (%) of the proposed system using different parameter settings in Algorithms 1 and 2.

		Using Algorithm 1	
L_C	20000	500	
FVC2002 DB2	0.64	1.00	
FVC2002 DB3	4.57	6.00	
		Using Algorithm 2 and L_C = 20000	
L_S	50	5	1
FVC2002 DB2	3.37	1.00	0.64
FVC2002 DB3	14.00	8.07	4.57

multiple '1's folded to the same position, leading to a decrease in feature discriminative ability. Algorithm 2 is proposed to increase the difficulty of obtaining the original feature vector. Under the same setting of $L_C = 20000$, we can see from Table 2 that a larger value of L_S reduces matching accuracy, for example, on database FVC2002DB2, EER is 3.37% when $L_S = 50$, as opposed to EER is 1.00% when $L_S = 5$. Both EERs are worse than EER = 0.64% when $L_S = 1$ (which is equivalent to just using Algorithm 1) because the feature-dependent segment permutation is controlled by the binary code ϕ_j and larger L_S, which represents a longer portion of the original feature vector, is more likely to make ϕ_j incorrect.

From the above analysis, we can see that smaller L_C or larger L_S can decrease matching performance. However, such a parameter setting makes the retrieval of the original feature vector harder under the assumption that random projection based transformation is conquered. Detailed security analysis is discussed in Section 4.4.

We also evaluated the performance of the proposed system using different values of Y over databases FVC2002 DB2 and DB3 with the 1VS1 matching protocol under the parameter setting $L_C = 20000$ in Algorithm 1. Security of the first feature set is provided by the random projection matrix $\mathscr{M}$ which is of size $X \times Y$, $(Y \leq X)$. The feature vector $P(m_i)$, extracted from the polar coordinate-base d structure, is transformed using Algorithm 1 and (1). The smaller the value of Y is set, the more the dimensions are reduced. A lower-dimensional transformed feature vector is more secure as less information of the original feature vector is kept. In the tests, we set the value of Y to be 300 and 50, respectively. The EER performance is listed in Table 3. It can be observed that the smaller the value of Y, the higher the EER. This is because less information about the original features is preserved with more dimension cut (smaller Y), leading to performance degradation. Moreover, under the same parameter setting ($Y = 300$), the proposed system demonstrates better performance on database FVC2002 DB2 with EER = 0.64% than the performance on FVC2002 DB3 with EER = 4.57%. The main reason for this is the vast difference of image quality between these two databases. The first two images from database FVC2002 DB2 have much better quality than the first two images of FVC2002 DB3 [10, 11].

4.2. Performance Comparison with the Similar Work. In this section, we compare the performance of the proposed system with other similar systems. The EER comparison under the lost key scenario is reported in Table 4. It can be observed that the proposed method outperforms all the existing similar methods under the 1VS1 matching protocol. Under the FVC matching protocol, the performance of proposed method is worse than that of original 2P-MCC$_{64,64}$; however, 2P-MCC suffers from the ARM, as analyzed in Section 1.1. By contrast, the proposed scheme is resilient to this attack. In [8] transformation parameters are derived directly from biometrics via quantization, causing them rarely to be identical for the same user when large minutia variance exists in fingerprint images, which leads to poor performance. The structures in [9–11] are constructed by each minutia with all other minutiae in the image, resulting in more computational complexity. By contrast, in the proposed method structures are only formed by each minutia and its local neighbors in the range of R. More importantly, the methods [7, 9–14] are vulnerable to the ARM attack [47].

Table 3: EER (%) of proposed system using different values of Y.

Y	300	50
FVC2002 DB2	0.64	1.00
FVC2002 DB3	4.57	8.00

4.3. Revocability and Unlinkability. Revocability is an essential property that a qualified cancelable template design should possess. Once a template is compromised, another transformed template should be generated and the newly generated template should be totally different from the compromised template and suffer no performance degradation. To measure revocability of the proposed system, we generated 50 different templates from the 1st image of each finger by 50 different user specific keys. Then the transformed templates were matched against the original ones. The imposter distribution (with different keys) and pseudo-imposter distribution on database FVC2002 DB2 are shown in Figure 6. It can be seen that the imposter distribution and pseudo-imposter distribution are similar, which means that even if multiple templates are generated from the same image, they are distinct from the original template and there is no performance degradation. The mean and standard derivations of the imposter distribution are 0.2457 and 0.0408, respectively, while the values of these two indicators of the pseudo-imposter distribution are 0.2419 and 0.0042, respectively.

Table 4: EER (%) comparison between the proposed system and similar systems under the lost-key scenario.

Methods	2002 DB1		2002 DB2		2002 DB3		2004 DB2	
	1VS1	FVC	1VS1	FVC	1VS1	FVC	1VS1	FVC
Yang et al. [5]	5.93	-	4	-	-	-	-	-
Ahn et al. [6]	-	7.18	-	3.61	-	11.80	-	-
Yang and Busch [7]	-	-	13	-	-	-	-	-
Yang et al. [8]	-	-	0.85	-	-	-	-	-
Ahmad et al.[9]	9	-	6	-	27	-	-	-
Wang and Hu [10]	3.50	-	4	5	7.5	-	-	-
Wang and Hu [11]	2	-	2.30	3	6.12	-	-	-
Wang and Hu [12]	1	-	2	-	5.20	-	13.30	-
Jin et al. [13]	3.07	-	1.02	-	-	-	-	-
Jin et al.[14]	4.36	-	1.77	-	-	-	21.82	-
Ferrara et al. [15] 2P-MCC$_{64,64}$	-	3.30	-	1.80	-	7.80	-	-
Instance 3 (proposed system)	0.32	5.75	0.64	4.71	4.57	10.22	9.90	12.00

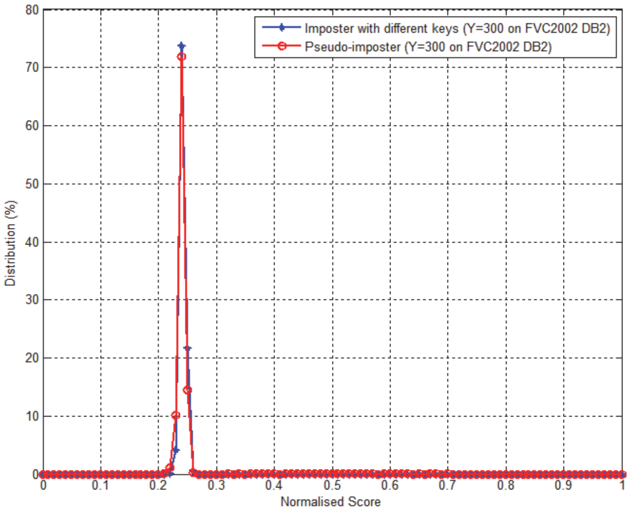


Figure 6: Imposter (with different keys) and pseudo-imposter distributions on FVC2002 DB2 when $Y = 300$.

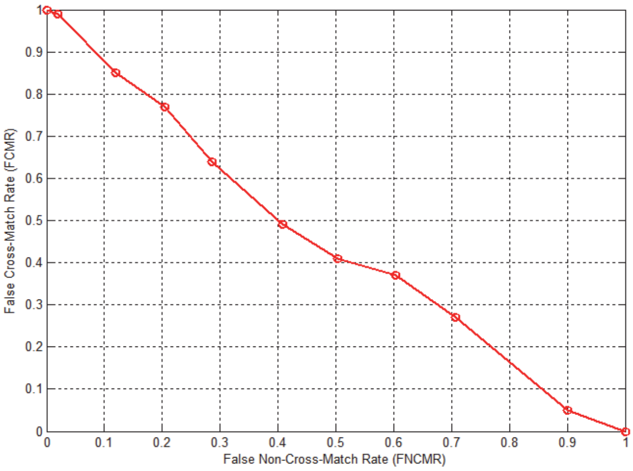


Figure 7: FCMR versus FNCMR tested on FVC2002 DB2 when $Y = 300$.

To protect users' privacy, unlinkability is another essential property of cancelable fingerprint templates. It requires that the transformed templates generated from the same finger using different keys should be different to one another, as if they were transformed from different fingers. In this way, templates from the same individual used in different applications cannot be cross-matched. To verify the unlinkability property of the proposed method, two indicators [55], the false cross-match rate (FCMR) and the false non-cross-match rate (FNCMR), are used in two cases over database FVC2002 DB2. Case 1: FNCMR is the ratio of unsuccessful matching attempts between the transformed templates of the first and second images of each finger. Feature transformation is based on different keys. Case 2: FCMR is the ratio of successful matching attempts between the transformed templates of the first image from each finger and the first image of different fingers. The FCMR and FNCMR curves are shown in Figure 7, from which it is clear that $FCMR + FNCMR \approx 1$, which conforms to the expected behavior of a cross-comparator [55].

4.4. Security Analysis. Given a template image F^T, we obtain feature sets C_T and D_T from the polar coordinate-based and Delaunay triangulation-based structures. The polar coordinate-based feature set $C_T = \{P(m_i)\}_{i=0}^{N^T-1}$ is protected by algorithms included in the polar coordinate-based scheme. Specifically, each element $P(m_i)$ in C_T first goes through the proposed feature decorrection algorithm, Algorithm 1 or 2, which transforms it into another format $\mathbb{P}(m_i)$, making the transformed feature sets uncorrelated in different applications, governed by application-specific parameters, L_C and L_S. Since the DFT is invertible, $\mathbb{P}(m_i)$ is further protected by random projection through the projection matrix $\mathscr{M}$, as shown in (1), which is essentially a many-to-one mapping. $\mathscr{M}$ is of size $X \times Y$ and Y is set to be smaller than X. Hence, the transformed feature vector $\widehat{P}(m_i)$ has a reduced dimension compared with $\mathbb{P}(m_i)$. The adversary can only

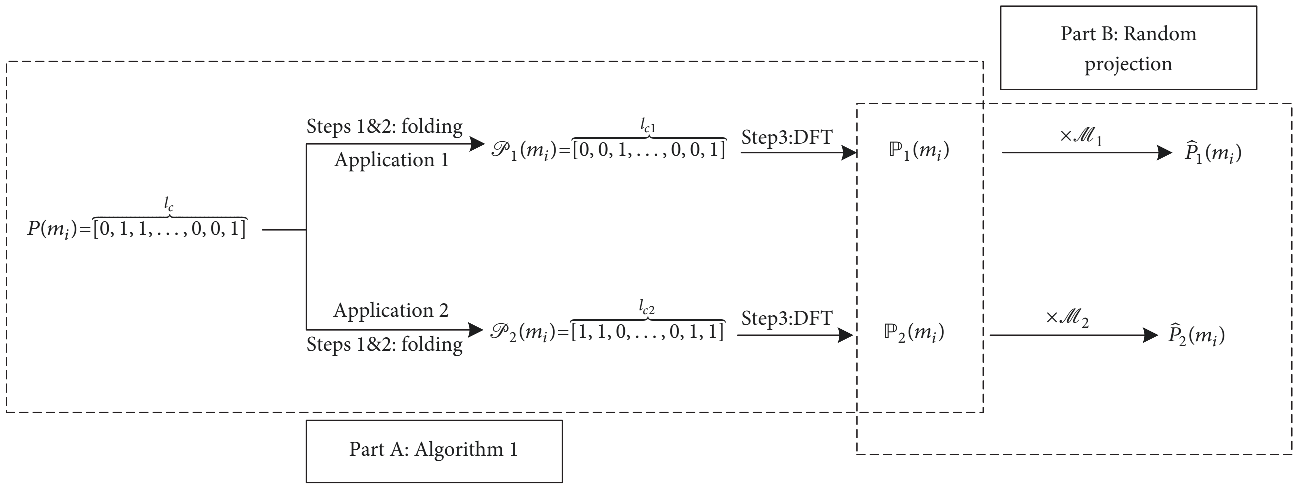


Figure 8: An example of the proposed feature transformation method for the first feature set under the scenario of ARM.

launch the ARM attack by obtaining multiple transformation matrices and transformed feature sets from the same original feature set. Thanks to the feature decorrelation algorithm, Algorithm 1 or 2, the ARM attack can be defended by the proposed method, because the transformed feature set $\mathbb{P}(m_i)$ is uncorrelated in different applications, which is achieved by varying the application-specific parameters, L_C and L_S.

Here we give an example to demonstrate how the proposed method defends the ARM. The whole transformation process is divided into two parts: A and B, as shown in Figure 8. Part A represents the procedure of Algorithm 1 and Part B represents the random projection based transformation. In Part A, with the original feature vector $P(m_i)$ of length l_C, which only contains values of 0 and 1, under the ARM scenario, we assume that the same $P(m_i)$ is used in two applications. Without loss of generality, L_{C1} is chosen for Application 1 and L_{C2} for Application 2, where $L_{C1} \neq L_{C2}$. The folding function in Algorithm 1 is expected to change the input bit stream, yielding two different binary strings for Applications 1 and 2, respectively. The purpose of the DFT (Step 3 in Algorithm 1) is to convert the two new (folded) binary strings into different real-value vectors, i.e., $\mathbb{P}_1(m_i)$ for Application 1 and $\mathbb{P}_2(m_i)$ for Application 2. In Part B, the feature vectors $\mathbb{P}_1(m_i)$ and $\mathbb{P}_2(m_i)$ are, respectively, transformed into $\widehat{P}_1(m_i)$ and $\widehat{P}_2(m_i)$ by random projection. Due to the absence of correlation between $\mathbb{P}_1(m_i)$ and $\mathbb{P}_2(m_i)$, even if the adversary acquires the transformed feature vectors $\widehat{P}_1(m_i)$ and $\widehat{P}_2(m_i)$ as well as the projection matrices $\mathscr{M}_1$ and $\mathscr{M}_2$, he/she cannot launch the ARM to obtain either $\mathbb{P}_1(m_i)$ or $\mathbb{P}_2(m_i)$, because it would be impossible for the ARM to find sufficient number of relevant systems equations matching the number of independent unknown variables.

It is worth noting that the outputs, $\mathbb{P}_1(m_i)$ and $\mathbb{P}_2(m_i)$, of Part A are the inputs to Part B as shown in the overlapped area of Part A and Part B in Figure 8. $\mathbb{P}_1(m_i)$ and $\mathbb{P}_2(m_i)$ are intermediate products, which are not stored in the database or on the smart card, because only the resultant feature vectors $\widehat{P}_1(m_i)$ and $\widehat{P}_2(m_i)$ are needed for similarity score calculation. Therefore, the adversary does not know $\mathbb{P}_1(m_i)$ and $\mathbb{P}_2(m_i)$ unless he/she can recover them. One may argue that if the random projection based transformation (or Part B) is conquered, then $\mathbb{P}(m_i)$ can be retrieved. We now show why this is computationally infeasible. The random projection based transformation in (1) effectively constitutes an underdetermined system of linear equations. Since the projection matrix $\mathscr{M}$ is of size $X \times Y$ with Y being smaller than X, rank($\mathscr{M}$) is no greater than Y, which is less than the number of unknowns, namely, elements of $\mathbb{P}(m_i)$. It is a well-known result in linear algebra [56] that when the coefficient and augmented matrices of (1) have the same rank, (1) has an infinite number of solutions. Clearly, $\mathbb{P}(m_i)$ is just one solution among so many solutions, making the search for $\mathbb{P}(m_i)$ tremendously hard, especially with $\mathbb{P}(m_i)$ having a relatively flat spectrum due to the DFT.

Let us analyze the security provided by Algorithms 1 and 2, under the assumption that $\mathbb{P}(m_i)$ is obtained by adversary. The DFT in Algorithm 1 is invertible and not meant to protect $\mathscr{P}(m_i)$. The DFT is applied for the purpose of rendering a dense data representation of the frequency samples of $\mathscr{P}(m_i)$ so that the search space for $\mathscr{P}(m_i)$ cannot be narrowed down [57]. The modulo operation in Algorithm 1 can provide certain protection to the original feature vector $P(m_i)$ depending on parameter settings. With an element of value '1' found at position f_P in $\mathscr{P}(m_i)$, where $f_P < L_C$, the number of positions in $P(m_i)$ that could yield the value of '1' at position f_P in $\mathscr{P}(m_i)$ is $N_p = \lceil l_C/L_C \rceil$. The number of possibilities that could result in the value of '1' at position f_P in $\mathscr{P}(m_i)$ is $\sum_{k=1}^{N_p} C^k_{N_p}$ in theory, where $C^k_{N_p}$ means choosing k from N_p positions, but, in reality, it is unlikely that a majority of these N_p positions in $P(m_i)$ contain '1'. Without loss of generality, we assume that at most two of these N_p positions are '1' for the rest of our discussions unless stated otherwise; then the computational complexity is $S_e = \log_2(C^1_{N_p} + C^2_{N_p})$

bits in order to search all the possible combinations by brute force attack. Suppose that there are N_e ‘1’s in $\mathscr{P}(m_i)$; then the computational complexity for brute force search will be $N_e \times S_e$. When $N_e = 30$, under the parameter settings $l_C = 34560$ and $L_C = 500$, $N_p = \lceil 34560/500 \rceil = 70$, the computational complexity is $30 \times \log_2(C_{70}^1 + C_{70}^2) \approx 330$ bits. However, if L_C is set to be a large value, e.g., $L_C = 20000$, for elements of value ‘1’ found in $\mathscr{P}(m_i)$ from positions 1 to 14560, say for value ‘1’ found at position 123, its original position in $P(m_i)$ only has three possibilities, either position 123 or position 20123 or both. In this case, the number of possibilities provided by the modulo operation is considerably reduced. To strengthen the security of Algorithm 1 for the case that L_C is set to be a large value, e.g., 20000, we propose Algorithm 2 on top of Algorithm 1.

In Algorithm 2, the first part P_1 of original feature vector $P(m_i)$ is first divided into N_S segments and each segment, e.g., S_j, is permutated by a segment-based binary code, e.g., ϕ_j. Take the segment S_j of length L_S as an example. For convenience, trivial segments containing full ‘0’s or full ‘1’s are excluded in the following discussion as permutation does not change the segment bit distribution. For a permuted segment S_j', there exists $L_S - 1$ number of different segments originating from S_j through the circular shift permutation. One-bit difference in one segment implies a different entire feature vector P_1 which contains N_S segments. The computational effort to determine all possible P_1 due to the circular shift permutation will be $(L_S - 1)^{N_S}$ under the brute force attack. Assume there are $N_c < N_S$ nontrivial segments that contain both zero and nonzero elements, then the actual computational complexity reduces to be $(L_S - 1)^{N_c}$ under the brute force attack. Take, for example, $L_S = 5$ and $N_c = 60$, which has been observed in many of our experiments. In this case, the number of security bits imposed by Algorithm 2 is $\log_2((5 - 1)^{60}) = 120$ bits, which is a substantial amount. Clearly, the added security from Algorithm 2 is at the expense of matching performance, as shown in Section 4.1, which reflects the fact that there is always a compromise between security and recognition accuracy. Note that, for a given permuted segment, it is hard to tell whether it is produced by an actual permutation or it has not been permuted at all. Therefore L_S instead of $L_S - 1$ can be used to account for all possible shift combinations which can help increase the security strength.

Regarding the security of the second feature set D_T, since the feature $\widehat{D}_T$ is obtained from D_T under the guidance of feature codes $\{f_i^c\}_{i=1}^{N_1^T}$, which are generated from their corresponding triangle feature and not saved in the database or on the smart card, the adversary has no idea about the original location of a triangle feature, even if $\widehat{D}_T$ is hacked. Under this situation, the adversary may try to guess the feature code through the brute force attack. The number of security bits for calculating one feature code, e.g., $f_{m_1 m_2 m_3}^c$, which is given by $f_{m_1 m_2 m_3}^q = [o_{m_1 m_2}^q, l_{m_1 m_2}^q, l_{m_1 m_3}^q, \alpha_{m_1}^q]$ through (2), can be expressed by $H(\Delta) = \log_2((2\pi/s_o) \times (300/s_l)^2 \times (\pi/s_\alpha))$ because the minutiae orientation range is $[0, 2\pi)$, the edge length is $(0, 300]$, and the range of an angle is $(0, \pi)$. In the experiments, the quantization steps for calculating the feature code were set to be $s_o = 5\pi/36$, $s_l = 25$ pixels and $s_\alpha = 5\pi/36$ on database FVC2002 DB2. With these quantization settings, the number of security bits $H(\Delta)$ is about 14 bits for one feature code. However, this feature code can only be used to find the original location of one triangle in D_T and the adversary cannot verify the correction of the original position. To exactly restore D_T, the original locations of N_1^T triangles have to be determined at the same time, which means that the security of D_T is $N_1^T \times 14$ bits. The average value of N_1^T is 32 on database FVC2002 DB2. Since a certain degree of error tolerance is allowed in the matching process, the real security is lower than $N_1^T \times 14$ bits, depending on the matching score threshold S_t. Note that, even if D_T is revealed, the original location of minutiae in the fingerprint image remains unavailable, because D_T only contains the relative information of the three minutiae forming the Delaunay triangle rather than the absolute coordinates on the image. This means that compromising D_T would not threaten the security of C_T.

Some other issues are discussed here: (1) In our application, polar coordinate-based local structures are employed. Assume that m_i and m_j are two neighbor minutiae and are considered as the origin of the polar coordinate of two polar coordinate-based local structures S_{m_i} and S_{m_j}. Since m_i and m_j are neighbor minutiae, some of the minutiae points included in local structure S_{m_i} are also included in S_{m_j}. The feature vectors, e.g., $P(m_i)$ and $P(m_j)$, extracted from local structures, S_{m_i} and S_{m_j}, respectively, may have some correlation; however, they are different. Here ‘correlation’ indicates the existence of some common minutiae in different polar coordinate-based structures, but it does not mean that the features extracted from different polar coordinate-based structures are the same, because the features extracted from different polar coordinate-based structures are based on different reference minutiae and the information of the reference minutiae is nonpublic. For instance, according to Section 2.1, the positions of ‘1’ in $P(m_i)$ and $P(m_j)$ are decided by the triplet values $(\rho_{ij}, \alpha_{ij}, \beta_{ij})$ and $(\rho_{ji}, \alpha_{ji}, \beta_{ji})$. The radial distance ρ_{ij} is equal to ρ_{ji}, but α_{ij} and β_{ij} are different from α_{ji} and β_{ji}, respectively. A moderate variation on the orientation or/and its related line angle can change the values of $(\rho_{ij}, \alpha_{ij}, \beta_{ij})$ or $(\rho_{ji}, \alpha_{ji}, \beta_{ji})$. So even if minutiae m_i and m_j are neighbor minutiae, the triplet values $(\rho_{ij}, \alpha_{ij}, \beta_{ij})$ are different from $(\rho_{ji}, \alpha_{ji}, \beta_{ji})$, which leads to different feature vectors $P(m_i)$ and $P(m_j)$. As the radial distance ρ_{ij} is equal to ρ_{ji}, so $P(m_i)$ and $P(m_j)$ may have some correlation that can be utilized by the adversary. However, any correlation based attack needs at least a compromised feature vector, e.g., $P(m_i)$ or $P(m_j)$, as a base, which unfortunately is infeasible because $P(m_i)$ or $P(m_j)$ has been decorrelated and protected by the folding, permutation, and random projection. (2) Assume the number of ‘1’s, in feature vector $P(m_i)$, is N_{1s}. According to our statistics on the databases, N_{1s} is 34, which is much smaller than the length l_C (e.g., $l_C = 34560$) of the feature vector $P(m_i)$. If these N_{1s}‘1’s are uniformly distributed on $P(m_i)$, the computation complexity is about $\log_2(C_{34560}^{34}) =$

384 bits in order to correctly recover all the 34 ‘1’s in $P(m_i)$ by brute force attack. One may claim that these binary ‘1’s are not uniformly distributed. We give an example here. Assume that all the 34 ‘1’s are only located in the first 1000 bins out of a total of 34560 bins of the feature vector $P(m_i)$. Although this is a highly unlikely case, computational complexity for this example is about $\log_2(C_{1000}^{34}) = 210$ bits under the brute force attack, which demonstrates that the proposed method is still secure enough. Actually, it is nearly impossible if one can generate a binary string that is absolutely uniform. Our statistics of the probability distribution of bit ‘1’ over unfolded raw features, e.g., $P(m_i)$, shows that the features are with a good degree of uniform distribution. For example, the maximum probability of being ‘1’ of a bin is 10^{-4}, which shows that dominant probability does not exist. Moreover, even after removing bins with probability being ‘1’ that are equal to or less than 20% of the maximum probability, the remaining bins are still more than a thousand. The estimated figures, e.g., 330, 120, and 384 bits, in our security analysis, may be not tight. However, these could be the best analytical results one can get unless an accurate distribution model can be developed, which is far beyond the scope of this paper as such distribution model can be a research topic by its own. (3) There is a type of statistical attack, named Moore-Penrose inverse [58], to find possible solutions of the linear system (random projection is a linear system). If the linear system $b = Ax$ has any solutions, they are given by $x' = A^{+}b$, where A^{+} is the Moore-Penrose inverse of A. It is well known that a Moore-Penrose inverse based solution x' has the minimum Euclidean norm $\|x'\|_2$. There is no theoretic basis for any deterministic relationship between the Moore-Penrose inverse based solution x' and the ground truth x, if A is random. Some probabilistic relationship might exist for some cases, for example, based on the values of the Moore-Penrose inverse based solution x', one may estimate the position of ‘1’s in binary vector in x by general statistical relation that large values in x' corresponding to ‘1’s in x. However, for a specific application, the defender can select suitable random projection matrix, e.g., A, so that this statistical relation can be lessened. We have experimentally verified that a solution x' that is based on the Moore-Penrose inverse incorporating the statistical relation can find only one correct position of ‘1’ in x.

4.5. Suitability/Feasibility on Mobile Devices. In this section, the template size and computational complexity of the proposed system are discussed. In our application, the template consists of two parts. One is the transformed polar coordinate-based feature set $\widehat{C}_T = \{\widehat{P}(m_i)\}_{i=0}^{N^T-1}$ and the other one is the transformed Delaunay triangulation-based feature set $\widehat{D}_T$. The size of each element $\widehat{P}(m_i)$ in $\widehat{C}_T$ depends on the parameter setting Y of the transformation matrix. If Y is set to be 300, the size of $\widehat{P}(m_i)$ is 4.7 KB, and then the size of $\widehat{C}_T$ is $4.7 \times N^T$ KB. The feature set $\widehat{D}_T$ is of size $l_D = 20000$ bits ≈ 2.5KB. In terms of matching time, it takes about 0.000171 seconds to match an element $\widehat{P}^T(m_i)$ from $\widehat{C}_T$ against an element $\widehat{P}^Q(m_j)$ from $\widehat{C}_Q$. Assume that there are N^T elements in template feature set $\widehat{C}_T$ and N^Q elements in query feature set $\widehat{C}_Q$, then the matching time between $\widehat{C}_T$ and $\widehat{C}_Q$ is $N^Q \times N^T \times 0.000171$ seconds. The matching time between $\widehat{D}_T$ and $\widehat{D}_Q$ is about 0.00872 seconds.

Take the fingerprint image 1_1.tif and image 1_2.tif in FVC2002 DB2 for example. Assume that image 1_1.tif is template image and 1_2.tif is the query image. The value of N^T is 31 in the template, so the template size is 148.2 (=4.7 × 31 + 2.5) KB. The value of N^Q is 33 in the query, so the matching time between the template and query is 0.18263 (=31×33×0.00017+0.00872) seconds. The above experiment is conducted using MATLAB on a laptop with Intel processor: i5-2450M dual-core CPU of 2.50 GHz, 2.50 GHz, RAM of 8GB, and Operation System of 64-bit Win 7. With the powerful storage and computing capability of today’s mobile devices, e.g., smartphones, the imposed storage size and computational load are never an issue.

5. Conclusion

In this paper, a new fingerprint cancelable template system has been proposed for mobile device authentication. The new cancelable template can mitigate the negative impact of nonlinear distortion by combining multiple feature sets. Since the proposed system with two feature sets contains more feature information than most existing cancelable templates with just a single feature set, the discriminative power of the proposed system gets increased and thus recognition performance is enhanced. Furthermore, the proposed method can defeat the ARM attack through eliminating the feature correlation in different applications, which is a clear advantage over those existing cancelable templates that are vulnerable to the ARM attack. In the future work, the proposed scheme will be applied to other biometrics such as cancelable palmprint [59].

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This paper is supported by the Natural Science Foundation of China through Projects 61672083, 61370190, 61532021, 61472429, and 61402029 and by Defence Science and Technology Group (DST) of Australia through Project CERA 221.

References

[1] R. Spolaor, Q. Li, M. Monaro, M. Conti, L. Gamberini, and G. Sartori, “Biometric authentication methods on smartphones: A survey,” *PsychNology Journal*, vol. 14, no. 2-3, pp. 87–98, 2016.

[2] A. K. Jain, L. Hong, S. Pankanti, and R. Bolle, “An identity-authentication system using fingerprints,” *Proceedings of the IEEE*, vol. 85, no. 9, pp. 1365–1388, 1997.

[3] V. M. Patel, N. K. Ratha, and R. Chellappa, “Cancelable biometrics: A review,” *IEEE Signal Processing Magazine*, vol. 32, no. 5, pp. 54–65, 2015.

[4] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, no. 4, pp. 561–572, 2007.

[5] W. Yang, J. Hu, S. Wang, and J. Yang, "Cancelable Fingerprint Templates with Delaunay Triangle-Based Local Structures," in *Cyberspace Safety and Security*, vol. 8300 of *Lecture Notes in Computer Science*, pp. 81–91, Springer International Publishing, Cham, 2013.

[6] D. Ahn, S. G. Kong, Y. Chung, and K. Y. Moon, "Matching with Secure Fingerprint Templates Using Non-invertible Transform," in *Proceedings of the 2008 Congress on Image and Signal Processing*, pp. 29–33, Sanya, China, May 2008.

[7] B. Yang and C. Busch, "Parameterized geometric alignment for minutiae-based fingerprint template protection," in *Proceedings of the IEEE 3rd International Conference on Biometrics: Theory, Applications and Systems, BTAS 2009*, usa, September 2009.

[8] B. Yang, D. Hartung, K. Simoens, and C. Busch, "Dynamic random projection for biometric template protection," in *Proceedings of the 4th IEEE International Conference on Biometrics: Theory, Applications and Systems, BTAS 2010*, usa, September 2010.

[9] T. Ahmad, J. Hu, and S. Wang, "Pair-polar coordinate-based cancelable fingerprint templates," *Pattern Recognition*, vol. 44, no. 10-11, pp. 2555–2564, 2011.

[10] S. Wang and J. Hu, "Alignment-free cancelable fingerprint template design: A densely infinite-to-one mapping (DITOM) approach," *Pattern Recognition*, vol. 45, no. 12, pp. 4129–4137, 2012.

[11] S. Wang and J. Hu, "Design of alignment-free cancelable fingerprint templates via curtailed circular convolution," *Pattern Recognition*, vol. 47, no. 3, pp. 1321–1329, 2014.

[12] S. Wang, G. Deng, and J. Hu, "A partial Hadamard transform approach to the design of cancelable fingerprint templates containing binary biometric representations," *Pattern Recognition*, vol. 61, pp. 447–458, 2017.

[13] Z. Jin, B.-M. Goi, A. Teoh, and Y. H. Tay, "A two-dimensional random projected minutiae vicinity decomposition-based cancellable fingerprint template," *Security and Communication Networks*, vol. 7, no. 11, pp. 1691–1701, 2014.

[14] Z. Jin, M.-H. Lim, A. B. J. Teoh, and B.-M. Goi, "A non-invertible Randomized Graph-based Hamming Embedding for generating cancelable fingerprint template," *Pattern Recognition Letters*, vol. 42, no. 1, pp. 137–147, 2014.

[15] M. Ferrara, D. Maltoni, and R. Cappelli, "A two-factor protection scheme for MCC fingerprint templates," in *Proceedings of the International Conference of the Biometrics Special Interest Group (BIOSIG)*, pp. 1–8, 2014.

[16] N. L. Clarke and S. M. Furnell, "Advanced user authentication for mobile devices," *Computers & Security*, vol. 26, no. 2, pp. 109–119, 2007.

[17] D.-J. Kim and K.-S. Hong, "Multimodal biometric authentication using teeth image and voice in mobile environment," *IEEE Transactions on Consumer Electronics*, vol. 54, no. 4, pp. 1790–1797, 2008.

[18] D.-J. Kim, K.-W. Chung, and K.-S. Hong, "Person authentication using face, teeth and voice modalities for mobile device security," *IEEE Transactions on Consumer Electronics*, vol. 56, no. 4, pp. 2678–2685, 2010.

[19] H. C. Lee, K. R. Park, B. J. Kang, and S. J. Park, "A new mobile multimodal biometric device integrating finger vein and fingerprint recognition," in *Proceedings of the 4th International Conference on Ubiquitous Information Technologies and Applications, ICUT 2009*, jpn, December 2009.

[20] Q. Tao and R. Veldhuis, "Biometric authentication system on mobile personal devices," *IEEE Transactions on Instrumentation and Measurement*, vol. 59, no. 4, pp. 763–773, 2010.

[21] C.-L. Chen, C.-C. Lee, and C.-Y. Hsu, "Mobile device integration of a fingerprint biometric remote authentication scheme," *International Journal of Communication Systems*, vol. 25, no. 5, pp. 585–597, 2012.

[22] J. S. Kim, G. Li, B. Son, and J. Kim, "An empirical study of palmprint recognition for mobile phones," *IEEE Transactions on Consumer Electronics*, vol. 61, no. 3, pp. 311–319, 2015.

[23] A. Rattani, N. Reddy, and R. Derakhshani, "Convolutional neural networks for gender prediction from smartphone-based ocular images," *IET Biometrics*.

[24] M. De Marsico, M. Nappi, F. Narducci, and H. Proença, "Insights into the results of MICHE I - Mobile Iris CHallenge Evaluation," *Pattern Recognition*, vol. 74, pp. 286–304, 2018.

[25] T. Neal and D. Woodard, "Surveying Biometric Authentication for Mobile Device Security," *Journal of Pattern Recognition Research*, vol. 11, no. 1, pp. 74–110, 2016.

[26] A. Wojciechowska, M. Choraś, and R. Kozik, "The overview of trends and challenges in mobile biometrics," *Journal of Applied Mathematics and Computational Mechanics*, vol. 16, no. 2, pp. 173–185, 2017.

[27] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Systems Journal*, vol. 40, no. 3, pp. 614–634, 2001.

[28] Y. Wang, J. Hu, and D. Phillips, "A fingerprint orientation model based on 2D fourier expansion (FOMFE) and its application to singular-point detection and fingerprint indexing," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, no. 4, pp. 573–585, 2007.

[29] X. Chen, J. Tian, X. Yang, and Y. Zhang, "An algorithm for distorted fingerprint matching based on local triangle feature set," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, pp. 169–177, 2006.

[30] A. Gago-Alonso, J. Hernández-Palancar, E. Rodríguez-Reina, and A. Muñoz-Briseño, "Indexing and retrieving in fingerprint databases under structural distortions," *Expert Systems with Applications*, vol. 40, no. 8, pp. 2858–2871, 2013.

[31] F. Farooq, R. M. Bolle, T.-Y. Jea, and N. Ratha, "Anonymous and revocable fingerprint recognition," in *Proceedings of the 2007 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, CVPR'07*, usa, June 2007.

[32] C. Lee, J.-Y. Choi, K.-A. Toh, S. Lee, and J. Kim, "Alignment-free cancelable fingerprint templates based on local minutiae information," *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, vol. 37, no. 4, pp. 980–992, 2007.

[33] S. Tulyakov, F. Farooq, P. Mansukhani, and V. Govindaraju, "Symmetric hash functions for secure fingerprint biometric systems," *Pattern Recognition Letters*, vol. 28, no. 16, pp. 2427–2436, 2007.

[34] Z. Jin, A. B. J. Teoh, T. S. Ong, and C. Tee, "A Revocable Fingerprint Template for Security and Privacy Preserving," *KSII Transactions on Internet and Information Systems*, vol. 4, no. 6, pp. 1327–1342, 2010.

[35] C. Lee and J. Kim, "Cancelable fingerprint templates using minutiae-based bit-strings," *Journal of Network and Computer Applications*, vol. 33, no. 3, pp. 236–246, 2010.

[36] H. Chen and H. Chen, “A novel algorithm of fingerprint encryption using minutiae-based transformation,” *Pattern Recognition Letters*, vol. 32, no. 2, pp. 305–309, 2011.

[37] Z. Jin, A. B. Jin Teoh, T. S. Ong, and C. Tee, “Fingerprint template protection with minutiae-based bit-string for security and privacy preserving,” *Expert Systems with Applications*, vol. 39, no. 6, pp. 6157–6167, 2012.

[38] P. Das, K. Karthik, and B. Chandra Garai, “A robust alignment-free fingerprint hashing algorithm based on minimum distance graphs,” *Pattern Recognition*, vol. 45, no. 9, pp. 3373–3388, 2012.

[39] W. J. Wong, A. B. J. Teoh, M. L. D. Wong, and Y. H. Kho, “Enhanced multi-line code for minutiae-based fingerprint template protection,” *Pattern Recognition Letters*, vol. 34, no. 11, pp. 1221–1229, 2013.

[40] N. Zhang, X. Yang, Y. Zang, X. Jia, and J. Tian, “Generating registration-free cancelable fingerprint templates based on Minutia Cylinder-Code representation,” in *Proceedings of the 6th IEEE International Conference on Biometrics: Theory, Applications and Systems, BTAS 2013*, usa, October 2013.

[41] S. Wang and J. Hu, “A blind system identification approach to cancelable fingerprint templates,” *Pattern Recognition*, vol. 54, pp. 14–22, 2016.

[42] M. Ferrara, D. Maltoni, and R. Cappelli, “Noninvertible minutia cylinder-code representation,” *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 6, pp. 1727–1737, 2012.

[43] H. Kaur and P. Khanna, “Random Slope method for generation of cancelable biometric features,” *Pattern Recognition Letters*, 2018.

[44] P. P. Paul, M. Gavrilova, and S. Klimenko, “Situation awareness of cancelable biometric system,” *The Visual Computer*, vol. 30, no. 9, pp. 1059–1067, 2014.

[45] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, “A fingerprint and finger-vein based cancelable multi-biometric system,” *Pattern Recognition*, vol. 78, pp. 242–251, 2018.

[46] F. Quan, S. Fei, C. Anni, and Z. Feifei, “Cracking cancelable fingerprint template of Ratha,” in *Proceedings of the International Symposium on Computer Science and Computational Technology, ISCSCT 2008*, pp. 572–575, chn, December 2008.

[47] C. Li and J. Hu, “Attacks via record multiplicity on cancelable biometrics templates,” *Concurrency and Computation: Practice and Experience*, vol. 26, no. 8, pp. 1593–1605, 2014.

[48] C. Wang and M. L. Gavrilova, “Delaunay triangulation algorithm for fingerprint matching,” in *Proceedings of the 3rd International Symposium on Voronoi Diagrams in Science and Engineering 2006, ISVD 2006*, pp. 208–216, can, July 2006.

[49] R. Soleymani and M. Chehel Amirani, “A hybrid fingerprint matching algorithm using Delaunay triangulation and Voronoi diagram,” in *Proceedings of the 20th Iranian Conference on Electrical Engineering, ICEE 2012*, pp. 752–757, irn, May 2012.

[50] A. Muñoz-Briseño, A. Gago-Alonso, and J. Hernández-Palancar, “Fingerprint indexing with bad quality areas,” *Expert Systems with Applications*, vol. 40, no. 5, pp. 1839–1846, 2013.

[51] D.-T. Lee and B. J. Schachter, “Two algorithms for constructing a Delaunay triangulation,” *International Journal of Computer &amp; Information Sciences*, vol. 9, pp. 219–242, 1980.

[52] W. K. Gu, “Matching Perspective Views of a Polyhedron Using Circuits,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 9, no. 3, pp. 390–400, 1987.

[53] S. D. K. VeriFinger, *Neuro Technology*, 2010, http://www.neurotechnology.com/verifinger.html.

[54] K. Nandakumar and A. K. Jain, “Biometric template protection: Bridging the performance gap between theory and practice,” *IEEE Signal Processing Magazine*, vol. 32, no. 5, pp. 88–100, 2015.

[55] K. Simoens, B. Yang, X. Zhou et al., “Criteria towards metrics for benchmarking template protection algorithms,” in *Proceedings of the 5th IAPR International Conference on Biometrics, ICB ’12*, pp. 498–505, India, April 2012.

[56] E. Kreyszig, *Advanced engineering mathematics*, John Wiley and sons, Inc., New York, NY, USA, 2nd edition, 2010.

[57] M. Unser, “On the approximation of the discrete Karhunen-Loeve transform for stationary processes,” *Signal Processing*, vol. 7, no. 3, pp. 231–249, 1984.

[58] “Moore–Penrose inverse,” https://en.wikipedia.org/wiki/Moore%E2%80%93Penrose_inverse.

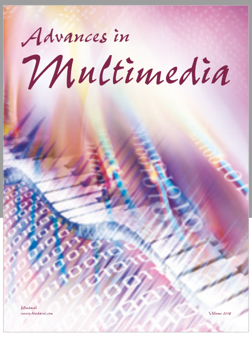
[59] L. Leng and A. B. J. Teoh, “Alignment-free row-co-occurrence cancelable palmprint Fuzzy Vault,” *Pattern Recognition*, vol. 48, no. 7, pp. 2290–2303, 2015.

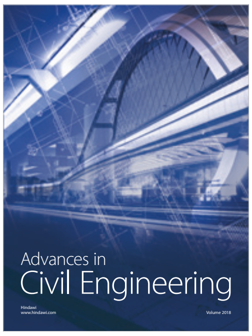
Journal of
Engineering

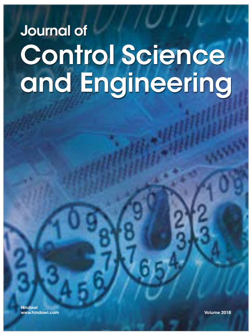
The Scientific
World Journal

International Journal of
Rotating
Machinery

Journal of
Sensors

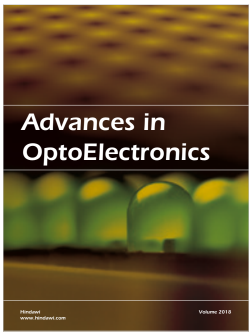

Advances in
Multimedia


Advances in
Civil Engineering


Journal of
Control Science
and Engineering

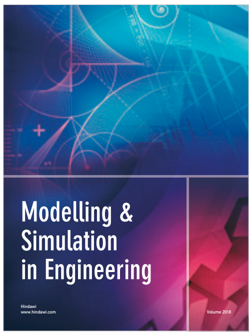
Journal of
Robotics

Journal of
Electrical and Computer
Engineering

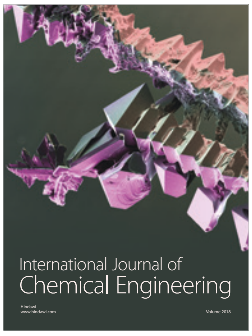

Advances in
OptoElectronics

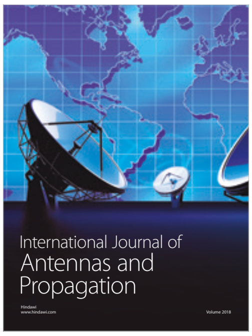
VLSI Design

International Journal of
Navigation and
Observation

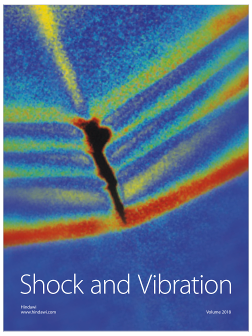

Modelling &
Simulation
in Engineering

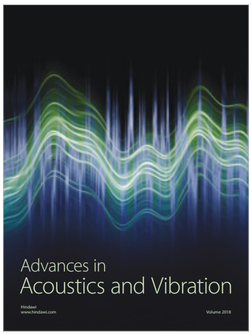
International Journal of
Aerospace
Engineering


International Journal of
Chemical Engineering


International Journal of
Antennas and
Propagation

Active and Passive
Electronic Components


Shock and Vibration


Advances in
Acoustics and Vibration