Pattern Recognition 47 (2014) 1309–1320

Contents lists available at ScienceDirect

Pattern Recognition

journal homepage: www.elsevier.com/locate/pr

An alignment-free fingerprint bio-cryptosystem based on modified Voronoi neighbor structures

Wencheng Yang [a], Jiankun Hu [a,*], Song Wang [b], Milos Stojmenovic [c]

[a] School of Engineering and Information Technology, University of New South Wales at the Australia Defence Force Academy, Canberra ACT 2600, Australia
[b] School of Engineering and Mathematical Sciences, La Trobe University, VIC 3086, Australia
[c] Department of Informatics and Computing, Singidunum University, Belgrade, Serbia

ARTICLE INFO

Article history:
Received 7 January 2013
Received in revised form
22 April 2013
Accepted 2 October 2013
Available online 8 October 2013

Keywords:
Fingerprint
Bio-cryptosystem
Modified Voronoi neighbor structure
Distortion robust
Alignment-free
Fuzzy extractor

ABSTRACT

Bio-cryptography is an emerging security technology which combines cryptography with biometrics. A good bio-cryptosystem is required to protect the privacy of the relevant biometric data as well as achieving high recognition accuracy. Fingerprints have been widely used in bio-cryptosystem design. However, fingerprint uncertainty caused by distortion and rotation during the image capturing process makes it difficult to achieve a high recognition rate in most bio-cryptographic systems. Moreover, most existing bio-cryptosystems rely on the accurate detection of singular points for fingerprint image pre-alignment, which is very hard to achieve, and the image rotation transformation during the alignment process can cause significant singular point deviation and minutiae changes. In this paper, by taking full advantage of local Voronoi neighbor structures (VNSs), e.g. local structural stability and distortion insensitivity, we propose an alignment-free bio-cryptosystem based on fixed-length bit-string representations extracted from modified VNSs, which are rotation- and translation-invariant and distortion robust. The proposed alignment-free bio-cryptosystem is able to provide strong security while achieving good recognition performance. Experimental results in comparison with most existing alignment-free bio-cryptosystems using the publicly-available databases show the validity of the proposed scheme.

1. Introduction

Cryptography is an important technology which is used for secure communications in the presence of opponents. In normal circumstances, cryptography focuses on the construction and analysis of protocols that can counter the negative impact of the opponents and is related to various aspects of information security, such as authentication, data confidentiality and data integrity [1]. In traditional cryptographic systems, user authentication is token-based and/or password-based. However, it is well-known that tokens may be lost or stolen and passwords can be forgotten or guessed. In addition, in practical applications, passwords do not have a strong relation with the password user. For example, the authentication system will give access to the owner of the correct password but is unable to tell who actually presents the password.

As a reliable and convenient technology, biometric recognition has emerged to potentially replace the traditional token- and/or password-based authentication. Biometrics, which are physical or behavioral traits of a person, such as fingerprint, face, iris, voice and so on, are not subject to oblivion or loss and are difficult to counterfeit. However, compared with tokens and/or passwords, there are two biggest drawbacks concerning biometrics. The first drawback is the diverse and noisy nature of biometrics in the process of biometric image capturing [2]. Fig. 1 shows a pair of fingerprint images from the same finger. Because of distortion, after registration, some of the corresponding minutiae (in the circular region) are partially overlapped, while the distances between some corresponding minutiae (in the rectangular region) are stretched and may be more than a set threshold value [2]. The second drawback in biometric authentication is that biometrics cannot be reset or replaced. If the template is stored in the database without any protection, it may lead to serious security breaches and privacy threats when the template is hacked [3]. Hence, protecting biometric templates is a critical issue.

Due to the security and privacy concerns associated with biometric templates, an emerging technology named bio-cryptography, which combines the prominent research in the fields of biometrics and cryptography, has received considerable attention. Bio-cryptosystems provide security either by securing the cryptographic key using biometric features or generating the cryptographic key directly from biometrics, which represents the physical identity of a person and is not stored explicitly but in the encrypted domain [4]. However, the matching of fingerprint minutiae is a non-trivial task. First of all,

* Corresponding author. Tel.: +61 2 6268 8186; fax: +61 2 6268 8581.
E-mail addresses: wencheng.yang@student.adfa.edu.au (W. Yang), J.Hu@adfa.edu.au (J. Hu), Song.Wang@latrobe.edu.au (S. Wang), mstojmenovic@singidunum.ac.rs (M. Stojmenovic).

0031-3203/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.patcog.2013.10.001

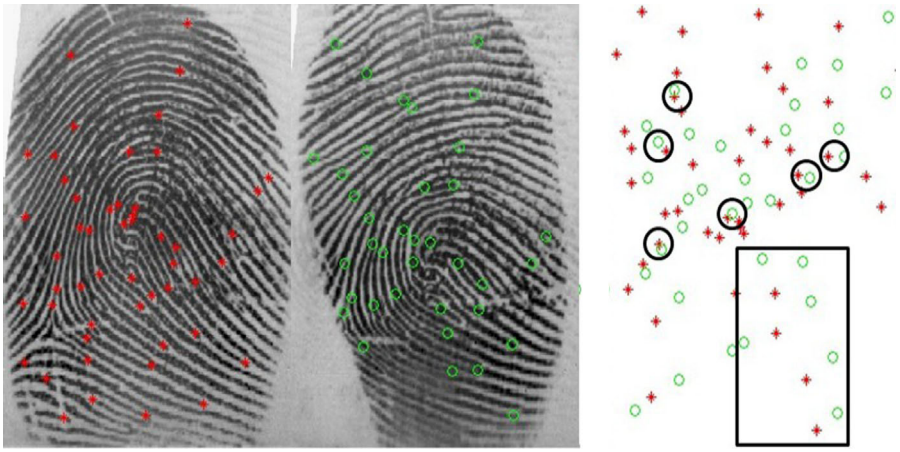

Fig. 1. An example of two fingerprints with distortion from the same finger.

fingerprint uncertainty is unavoidable due to large intra-class variations, such as displacement, rotation noise, and especially the non-linear distortion during the process of fingerprint capturing. Most existing bio-cryptosystem matching algorithms are dependent on error–correction codes to rectify biometric uncertainty. However, biometrics captured from the same individual at different times tends to be different, which may cause the biometric data to fail falling close to the correct codeword. Therefore, it is more important to reduce the biometric uncertainty which is intrinsic to bio-cryptosystems than relying on error–correction codes for rectification [5]. Moreover, the similarity measure for query and template minutia sets is limited [6]. For example, in an unencrypted fingerprint verification system, similarity can be computed by an equation that contains both local and global features of a fingerprint image, but it is difficult to measure similarity as such in a secure sketch. Thus the types and means of features used in the secure sketch are much restricted [4]. Last but not least, fingerprint registration or alignment, which is an important procedure to reduce intra-class variation in the unencrypted domain, cannot be used in the encrypted domain because the template in a bio-cryptosystem is unavailable to computing alignment parameters. All of these drawbacks degrade the performance of a fingerprint bio-cryptosystem.

In this paper, we propose an alignment-free fingerprint bio-cryptosystem based on modified Voronoi neighbor structures (VNSs) to mitigate the influence of fingerprint uncertainty while providing reliable biometric template protection. In the proposed scheme, we first present VNSs, which possess the characteristics of being reliable, distortion-tolerant, rotation- and translation-invariant. The new scheme is able to compensate the VNS change caused by large non-linear distortion which moves the minutiae out of the Voronoi tolerance region, thus making the local structure more robust to distortion. The modified VNSs are the outcome of this compensation process. Then all VNSs are mapped into a pre-defined three-dimensional (3D) array to generate fixed-length bit-strings. Finally, encrypted matching is performed and protected by the secure sketch, PinSketch. Experiments using public databases show that the proposed method based on modified VNSs performs better than most existing alignment-free local structure based schemes, such as the two local features fusing based scheme [7], the five nearest minutiae based scheme [8], the dual layer structure check based scheme [9], and the Delaunay triangle based scheme [10].

This paper makes the following main contributions compared with the existing work:

(i) The proposed scheme has relinquished the need of fingerprint image pre-alignment and the modified VNS based feature representations are minutiae based only, to which the existing template protection technique, e.g. PinSketch, can be applied.
(ii) The proposed scheme takes the novel step of mitigating biometric uncertainty by compensating the possible local structural change caused by non-linear distortion. This mitigation and compensation process is conducted at two levels. To be more specific, at the first level, small distortion, which shifts the minutiae position and orientation in a small local region (tolerance region) which is not large enough to change the VNS, can be addressed by the 3D array quantization technique. At the second level, large distortion, which makes the minutiae move over a certain tolerance margin and also change the VNS, is compensated by the modified VNSs.

The rest of the paper is organized as follows. Related works are reviewed in Section 2. In Section 3, we describe the basic security technique used in this paper, namely the fuzzy extractor. The proposed bio-cryptosystem based on modified VNSs is presented in Section 4. In Section 5, experimental results and security analysis are demonstrated and discussed. The conclusion and future work are given in Section 6.

2. Related works

2.1. Minutia-based Voronoi neighbor structures (VNSs)

The Voronoi tessellation formed by fingerprint minutiae owns some desirable local and global features. First, its local neighborhood structure is stable. Even if an elastic distortion occurs in a fingerprint image, every minutia always keeps the same neighboring structure as long as this elastic distortion does not move minutiae out of the tolerance region. Second, insertion of a new minutia or removal of an existing minutia in a Voronoi tessellation affects only those local Voronoi structures which contain that minutia. In other words, noise affects the Voronoi tessellation only locally [11]. Because of these good characteristics of Voronoi tessellation, the local VNSs have been used in several fingerprint authentication systems and achieved satisfied performance. In [12], Ceguerra et al. proposed an automatic fingerprint verification system relying on VNSs. In their scheme, the VNSs act as local features and help to find a reference axis consisting of the center minutia of a VNS and one of its neighbor minutiae. Then the reference axis found from the local VNSs is used to generate the global features which are finally taken to calculate the similarity between a pair of template and query fingerprints. In [13], Yu et al. presented a radial structure (same as the VNS) based fingerprint

matching algorithm. The radial structures are used for local matching and followed by a global matching when the local matching between template and query fingerprints fails. In [14], Khazaei et al. designed a fingerprint matching algorithm based on Voronoi diagram. In the algorithm, the minutia set generates a Voronoi diagram with minutiae as verties and an unique central cell is found and used for local matching. With the help of local central cell matching, this algorithm can reject un-matched fingerprint pair instantly. In addition, a second algorithm is taken into account when the local central cell matching fails under distortion. In [15], Soleymani et al. combined Delaunay triangulation and Voronoi diagram together to generate a hybrid matching algorithm. Unlike algorithms in [12–14] which start with local structure comparison, in this algorithm [15], the comparison of global topological polygons generated from the boundaries of Delaunay triangulation is carried out firstly and then the central Voronoi cells of fingerprints are compared to calculate the similarity between template and query fingerprints.

All the above-mentioned algorithms take advantage of the desirable features of local VNSs, such as translation and rotation invariance, local structural stability and distortion insensitivity, however, none of them tries to compensate the local structural change caused by large distortion which is likely to shift the minutiae beyond the tolerance margin. Moverover, the similarity measure for template and query minutia sets in these unencrypted fingerprint verification systems cannot be applied directly to the encrypted domain, as explained in the previous section. Fingerprint matching in the secure sketch is like a one-step procedure, in which the query features can only be compared with the secured template features once and output a match or non-match report.

2.2. Bio-cryptosystems

Bio-cryptosystems can be broadly divided into two categories, i.e., alignment-based and alignment-free methods [16].

For alignment-based methods, one or more registration points (singular points or minutiae) are required to align the fingerprint image before performing the matching procedure. For instance, Juels et al. proposed a fuzzy commitment scheme [17], in which the user selects a secret message C in the encoding stage. Let t denote the vector difference between the user biometric key X and C. The secured message or fuzzy commitment then contains t and $Y=hash(C)$, where *hash* is a non-invertible one-way hash function. In the decoding stage, with biometric representation, $Y+t$ is used to decode the closest codeword C'. With the aid of error-correcting techniques, the error in C' is supposed to be corrected to generate the original message C. This scheme requires the biometric representation X and Y to be aligned and ordered so that their correspondence is distinct. However, in the real application of fingerprint minutiae matching, the extracted minutia set is unordered.

To overcome the above shortage, Juels et al. [18], developed a fuzzy vault scheme. In their fuzzy vault scheme, the secret key K is divided and embedded into a polynomial $P(x)$ as its coefficients, where x is the variable. For different x, the value set, $y=P(x)$, of the polynomial can be computed. Apart from a set of value pairs (x, y) lying on $P(x)$, a set of chaos points (x', y') which creates a number of random chaff points that do not lie on P are also introduced to hide the secret key K. In the decoding stage, a query biometric representation Q which substantially matches the template T can own many of the genuine points with a few chaos points. The restored set of points is then used to recover K'. With the help of error-correction techniques, K' would be the same as the secret key K, if the coefficients of polynomial $P(x)$ can be successfully recovered.

Two modified fingerprint fuzzy vault algorithms have been presented in [19,20]. Clancy et al. [19] focused on using a modified version of the original fuzzy vault to encrypt the private key on the smart card using fingerprint information. In the scheme they proposed a concrete description about the degree of the polynomial for the fingerprint domain. In the decoding stage, the fingerprint features are used to find the corresponding points within the encoded message using the bounded nearest-neighbor algorithm. The contribution of their work is that it specifically describes the fuzzy vault in a real application combining with a smart card. Nandakumar et al. [20] proposed an automatic implementation of the fuzzy vault scheme based on fingerprint minutiae and used the high curvature points derived from the orientation field of the template fingerprint to assist in alignment so as to make the alignment more accurate without revealing any minutia position or orientation information in the template.

All the methods mentioned above primarily attempt to address the issue of how biometric-based key schemes should handle the uncertainty and variability in the biometric representation caused by noisy data, distortion and rotation in the image capturing process. In these schemes, pre-alignment is required to rotate and translate the query images with respect to the template images. Therefore, registration algorithms are needed to deal with this problem. Registration algorithms usually use the singular point as the reference point to establish a rotation and translation

Fig. 2. Example of rotation-induced position and orientation change of the singular point.

relationship between query and template images. However, accurate registration is a non-trivial task [21,22]. Recently, an investigation [23] was conducted on analyzing the underlying schemes of fingerprint image rotation and the effects on the features of singular point and minutiae points of the rotated fingerprints. It has shown that the pre-alignment process can cause noticeable singular point alteration and produce a non-negligible number of fake minutiae. An example of the influence of rotation on the singular point is shown in Fig. 2.

In contrast to alignment-based methods, alignment-free methods require no image registration. Li et al. [7] fused both local features, namely the minutiae descriptor and minutia local structure, in their fuzzy vault scheme. Both local features, which are invariant to transformation in the fingerprint capturing process, are integrated by employing three fusion strategies. This scheme is alignment-free and incurs no sacrifice at the security level of the system.

Unlike a fuzzy vault which is a key binding system, a fuzzy extractor is a key generation system which was first introduced as a concept by Dodis et al. [24,25]. Arathi et al. [8] proposed a fuzzy extractor for minutiae-based fingerprint authentication, which can be considered as an implementation of the fuzzy extractor concept. All the minutiae are to be quantized and digitally represented as a set of binary strings so as to be applied to the existing secure sketch, PinSketch. In this scheme, both global and local feature vectors are used. More specifically, global feature representations are extracted from a polar coordinate system, in which a core serves as a reference, while the local feature representations are extracted from a centered minutia and its five nearest local structures. A fuzzy extractor based on dual layer local structures has been derived by Xi et al. [9]. In this scheme, the stable, discriminative, rotation- and shift-free dual layer structures are included to protect the biometric template and at the same time achieve relatively high verification accuracy. Two layers of each minutia are constructed and checked in the proposed method. Yang et al. [10] formed an alignment-free Delaunay triangle based fuzzy extractor. The structurally stable Delaunay triangles are used to mitigate biometric uncertainty and also eliminate the feature pre-alignment process in fingerprint authentication. This Delaunay triangulation based structure could tolerate elastic distortion to some extent.

3. Preliminary

In this section, we present some preliminaries about fuzzy extractors and explain a secure sketch construction, PinSketch, which we will use for fingerprint matching in the encrypted domain.

The fuzzy extractor was first proposed as a concept by Dodis et al. [24,25]. The following is a description of the fuzzy extractor [24,25]. Let $\mathcal{M}=(0,1)^n$ be a finite-dimensional metric space consisting of biometric data points. Let ℓ be the number of bits of the extracted output string R from biometric ω. Here, R is ε-close to uniform distribution rather than uniform distribution, but ε can be set to be extremely small so as to make R as good as a uniform distribution for all real applications. Assume m is the min-entropy or the "worst case" entropy of the distribution ω, and t is the error threshold value. An $(\mathcal{M}, m, \ell, t, \varepsilon)$-fuzzy extractor is a pair of corresponding randomized procedures, "generate" (*Gen*) and "reproduce" (*Rep*) or "secure sketch" (*SS*) and "recover" (*Rec*), with the following properties:

1 The *Gen* procedure on input $\omega \in \mathcal{M}$ outputs an extracted string $R=(0,1)^{\ell}$, and $P=(0,1)^*$, which is the helper data. The *Gen* procedure can be expressed by $(R, P)=Gen(\omega)$.
2 The reproduction procedure *Rep* takes two values $\omega' \in \mathcal{M}$ and $P=(0,1)^*$ as function inputs. Since the fuzzy extractor owns the property of correction, it can guarantee that $Rep(\omega' P)=R$, if $dis(\omega, \omega') \le t$. If $dis(\omega, \omega') > t$, then no guarantee is provided about the output of *Rep*.
3 The security property of the fuzzy extractor guarantees that for any distribution $\omega \in \mathcal{M}$, the string R is nearly uniformly distributed.

From the above description, we can see that fuzzy extractors allow one to extract some random R from ω and then successfully reproduce R from any string ω' that is close to ω. The reproduction uses the helper string P produced during the initial extraction. However, P need not remain secret, because R looks truly random even given P. The two functions, *Gen* and *Rep*, of the fuzzy extractor are shown in Fig. 3.

To be more specific, the secure sketch, *SS*, used in this paper is named PinSketch, which is one of the secure sketch constructions proposed in [24]. PinSketch is based on syndrome encoding and decoding in our application. Below is a brief of the PinSketch, more details about PinSketch can be found in [24].

Let ω denote a template biometric feature vector. The syndrome encoding procedure $SS(\omega)=syn(\omega)$ can be expressed as:

$$SS(\omega) = syn(\omega) = (s_1, s_3, s_5, ..., s_{2t-1}) \tag{1}$$

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

Let ω' denote the query biometric feature vector, the syndrome decoding procedure $Rec(\omega', SS(\omega))$ can be expressed as

$$Rec(\omega', SS(\omega)) = supp(\omega') \Delta supp(v) \tag{2}$$

where Δ represents set difference. $supp(\omega')$ can be obtained based on the syndrome of ω' i.e., $syn(\omega') = (s_1', s_3', s_5', ..., s_{2t-1}')$, and $supp(v)$ can be computed based on the syndrome of v as follows:

$$supp(v) = (s_1' - s_1, s_3' - s_3, s_5' - s_5, ..., s_{2t-1}' - s_{2t-1}) \tag{3}$$

If the distance $dis(\omega, \omega') \le t$, then $Rec(\omega', SS(\omega)) = supp(\omega)$.

4. Proposed method

To relinquish the process of image pre-alignment and effectively compensate the possible local structural change caused by distortion, we propose to generate the modified VNSs (Voronoi neighbor structures). The modified VNSs have the properties of being reliable, distortion-insensitive, rotation- and translation-invariant.

Firstly, we construct the VNSs, which have good local and global structural stability under small distortion. Secondly, the VNSs are modified to compensate for the local structural change caused by large distortion during fingerprint acquisition. Thirdly, all the VNSs are quantized and mapped into a pre-defined 3D array to generate fixed-length bit-strings, which are convenient to be applied in the existing secure sketch construction. Finally, encrypted matching is performed. Specifically, at the encoding stage, a secret key which needs protection is skillfully bound with the modified VNS based template features by a polynomial which is evaluated at all the VNSs and each VNS is protected by the secure sketch, PinSketch. At the decoding stage, the secret key can be retrieved by sequentially concatenating the coefficients of the reconstructed polynomial if a sufficient number of secure sketches

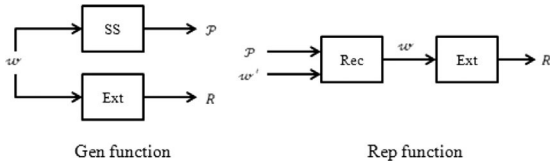

Fig. 3. Gen and Rep functions of fuzzy extractor.

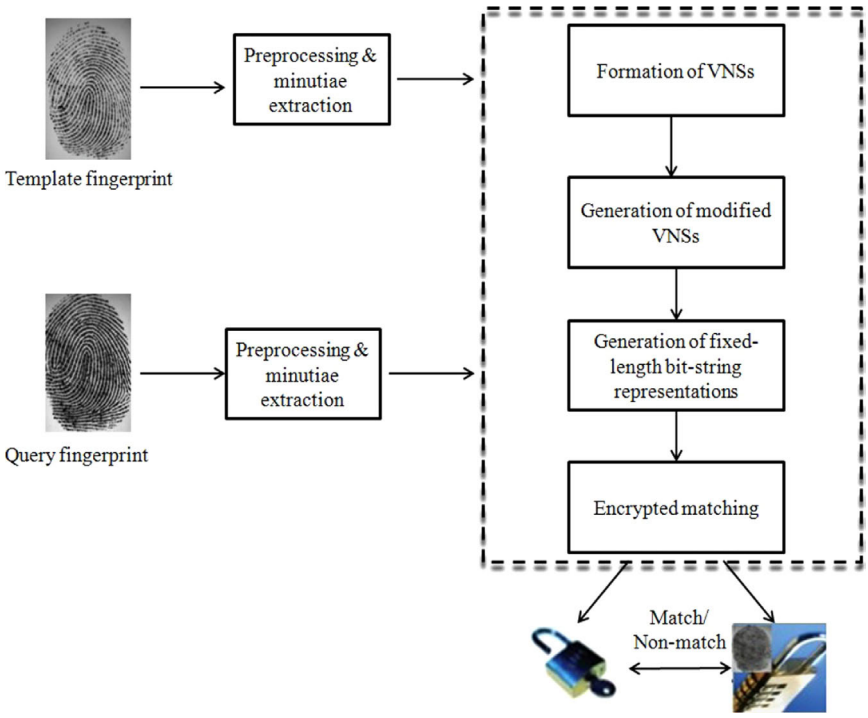

Fig. 4. Overall processing flow of the proposed method.

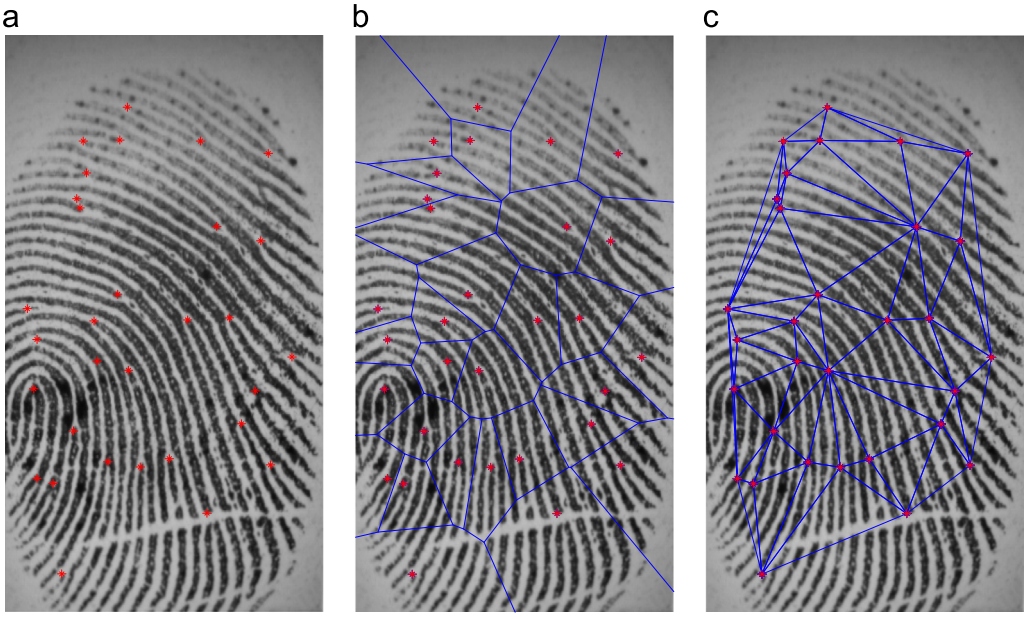

Fig. 5. Examples of (a) Minutiae points, (b) Voronoi tessellation and (c) Voronoi neighbor structures.

can be decoded. The entire process of the proposed scheme is illustrated in Fig.4, which consists of four steps – formation of VNSs, generation of modified VNSs, generation of fixed-length bit-string representations and encrypted matching.

4.1. Formation of VNSs

Given a set of minutiae $M = (m_1, m_2, m_3, ..., m_N)$, Voronoi tessellation partitions a whole fingerprint region that is composed of minutiae set M into many smaller regions, and presents the closest neighbor structures of minutiae in a precise manner. The steps to construct the Voronoi tessellation [11] and VNSs of the minutiae set M are described below.

First, we create the minutiae set M's Voronoi tessellation, which decomposes the space into regions around each minutia such that all the points in the region around m_i are closer to m_i than to other minutiae in M. With the Voronoi tessellation, we then form the VNSs by connecting the centers (minutiae) of every pair of neighboring Voronoi regions. Fig. 5a shows a set of minutia points. Fig. 5b gives the Voronoi tessellation and the VNSs are presented in Fig. 5c.

4.2. Generation of modified VNSs

The generation of modified VNSs is a process of compensating for local Voronoi neighbor structural change caused by large distortion. Although the VNS has very good local stability and

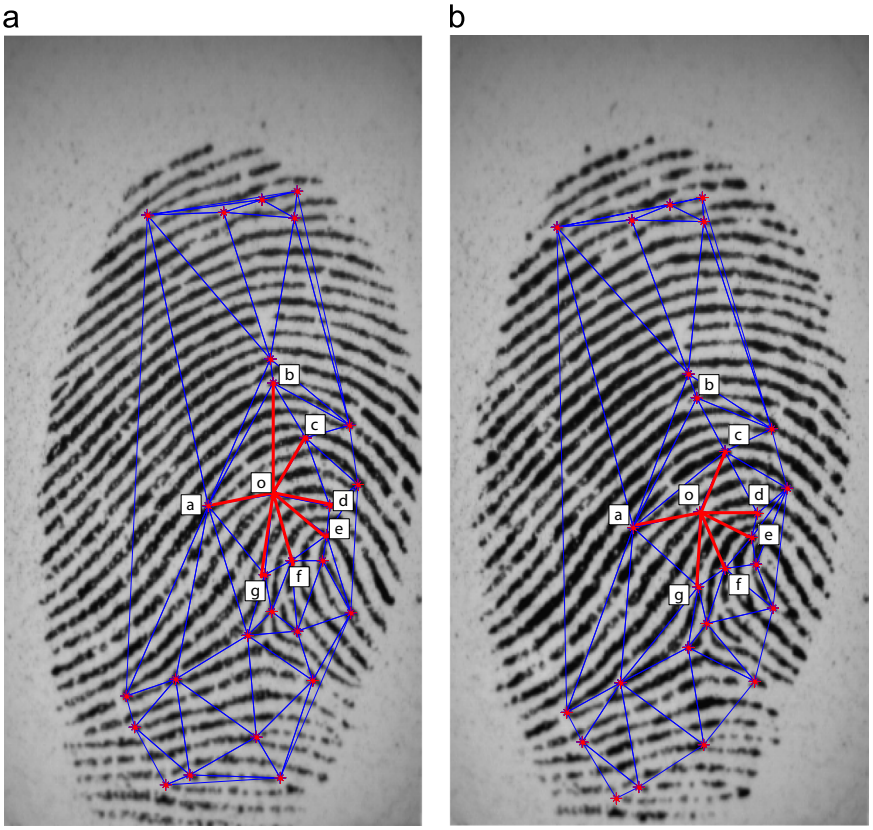

Fig. 6. Local Voronoi neighbor structures in (a) the template fingerprint image and (b) the query fingerprint image.

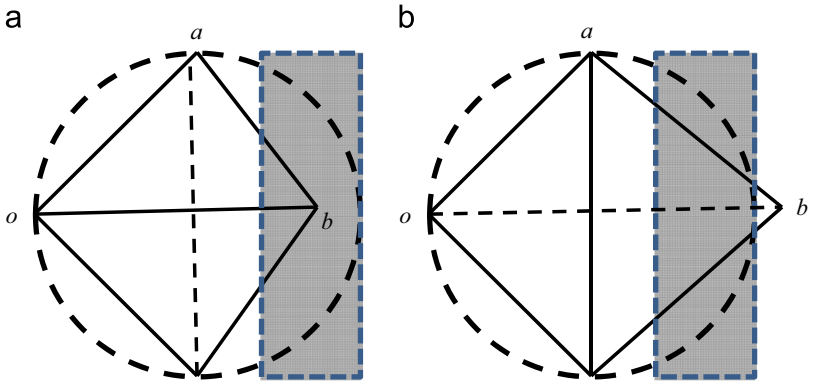

Fig. 7. Delaunay triangulations of the same point at different positions.

keeps the same neighborhood structure in the face of an elastic small distortion in a fingerprint image, the movement of minutiae caused by distortion should be within a certain tolerance region. If large distortion moves minutiae out of the tolerance region, the VNS will be altered [26]. For example, Fig. 6a shows the Voronoi tessellation and a VNS (bold lines), $VNS_o^T = (o, a, b, c, d, e, f, g)$, formed by a central minutia o and its Voronoi neighbors a, b, c, d, e, f, g in the template image T. VNS_o^T's corresponding VNS, $VNS_o^Q = (o, a, c, d, e, f, g)$, in the query image Q is shown in Fig. 6b. Because of large distortion, we can see that minutia b has been excluded in the VNS_o^Q. An obvious reason for this change is that the convex quadrilateral $Q(oabc)$ composed by two triangles, $T(oba)$ and $T(obc)$ in VNS_o^T, has been changed to the one that is composed by different triangles, $T(aco)$ and $T(acb)$, in VNS_o^Q. The variation occurred in the query image Q causes minutia b to be no longer the Voronoi neighbor of central minutia o, as compared to the template image T.

We now give a detailed explanation as to how the distortion acts on the component change of the convex quadrilateral *Q(oabc)* and how to deal with this local structural change under distortion. In Fig. 7a and b, assuming that the gray region is the tolerance region, if distortion makes minutia b move within the tolerance region, triangles, *T(oba)* and *T(obc)*, contained by convex quadrilateral *Q(oabc)* rarely alter in this case, as shown in Fig. 7a [26]. And the amount of distortion at this level can be addressed by the quantization technique, which will be introduced in Section 4.3. A different scenario is that the distortion moves b by a large amount out of the tolerance region, then triangles, *T(oba)* and *T(obc)*, contained by convex quadrilateral *Q(oabc)* will be changed to be triangles, *T(aco)* and *T(acb)*, as shown in Fig. 7b. If this happens, we attempt to find a way to compensate this structural change caused by large distortion.

For each convex quadrilateral *Q(oabc)* in a Voronoi tessellation formed by minutiae, it seems that the missing Voronoi neighbor minutia b (in VNS_o^T but not in VNS_o^Q) could be retrieved by simply flipping the shared edge of two triangles. For example, in *Q(oabc)*, flip the edge $\overline{ac}$ to $\overline{ob}$ in Fig. 7b. Unfortunately, if we just simply do edge flipping to all the convex quadrilaterals in a Voronoi tessellation, it could produce lots of fake Voronoi neighbors (not just minutia b) to the central minutia o. To reduce the probability of the addition of fake Voronoi neighbors to the local structure, we apply the order 1 triangle algorithm in [27–29]. For each convex quadrilateral in a Voronoi neighbor structure, e.g., *Q(oabc)*, with the edge $\overline{ac}$ flipped to $\overline{ob}$, if the circle *C(oba)* crossing *T(oba)* and the circle *C(obc)* crossing *T(obc)* both contain and only contain b and o inside the respective circle, then this flip action is considered to be valid, and vice versa. If edge flipping is valid, the newly added minutia b can be considered as one of the Voronoi neighbors of central minutia o, and the VNS which contains the newly added minutia b is called the modified VNS.

4.3. Generation of fixed-length bit-string representations

In the following we show how to generate fixed-length bit strings for each VNS, including the modified VNSs, using a predefined 3D array.

Each of the minutiae extracted from an input fingerprint image can be represented by a feature set:

$$m=(x,y,\theta,t) \tag{4}$$

where $(x,\ y)$ represents the coordinate of the minutia point, $\theta\in[0,2\pi]$ is the minutia orientation and t represents the type of the minutia. The ith VNS can be expressed as $VNS_i=(m_{i1},m_{i2},m_{i3},\ldots,m_{ik})$, where $1\le i\le N, 1\le k\le K$, with N being the number of VNSs in the fingerprint image and K the largest number of minutiae in the VNSs.

In order to allow the VNSs to be conveniently applied to the existing secure sketch construction, PinSketch, we transform each VNS into fixed-length feature vectors. We adopt a general method named 3D array mapping [30–32], which is to map all the Voronoi neighbor minutiae into a 3D array. The 3D array is defined by W_x, W_y, W_z, which are the length, width and height of the array, respectively. The length, width and height of each cell in the 3D array are represented by C_L, C_W, C_H, respectively. Specifically, the central minutia $m_o=\{x_o,y_o,\theta_o\}$ of each VNS is selected as the reference and located in the center of the first layer of the 3D array. Other $(k-1)$ Voronoi neighbor minutiae $m_i=\{x_i,y_i,\theta_i\}$, $i\in[1,k-1]$ are rotated and transformed based on the central minutia to the new coordinate $m_i'=\{x_i',y_i',\theta_i'\}$ in the 3D array as follows:

$$\begin{bmatrix}x_i'\\ y_i'\end{bmatrix}=\begin{bmatrix}cos\theta_o & -sin\theta_o\\ sin\theta_o & cos\theta_o\end{bmatrix}\begin{bmatrix}x_i-x_o\\ -(y_i-y_o)\end{bmatrix}+\begin{bmatrix}W_x/2\\ W_y/2\end{bmatrix} \tag{5}$$

$$\theta_i'=\begin{cases}\theta_i-\theta_o & \text{if } \theta_i\ge\theta_o\\ 2\pi+\theta_i-\theta_o & \text{if } \theta_i<\theta_o\end{cases} \tag{6}$$

Now the central minutia m_o is located in $(W_x/2,W_y/2,0)$, which is the center of the first layer of the 3D array. A bit-string can be obtained for the 3D array, according to the rule that if a cell in the 3D array contains the minutiae then it will be assigned 1, otherwise 0. By this means, the distortion which shifts the minutia within the tolerance region of a cell can be tackled. The length of the bit-string is $\ell=L\times W\times H$, which is the number of cells in the 3D array, where $L=W_x/C_L,\ W=W_y/C_W,\ H=W_z/C_H$.

In [31], the authors use the hashed address to represent the 3D array so as to protect the address information. In our scheme we only use the binary representation of the addresses of minutiae whose corresponding bit is 1 since the security of the address information could be protected by PinSketch. Assuming that there are k minutiae on average in each VNS, then each VNS will be represented by k bit-strings and each bit-string is $\ell_m=\log_2\ell$ bits in length. The generation process of bit-string based representations of each VNS is shown in Fig. 8.

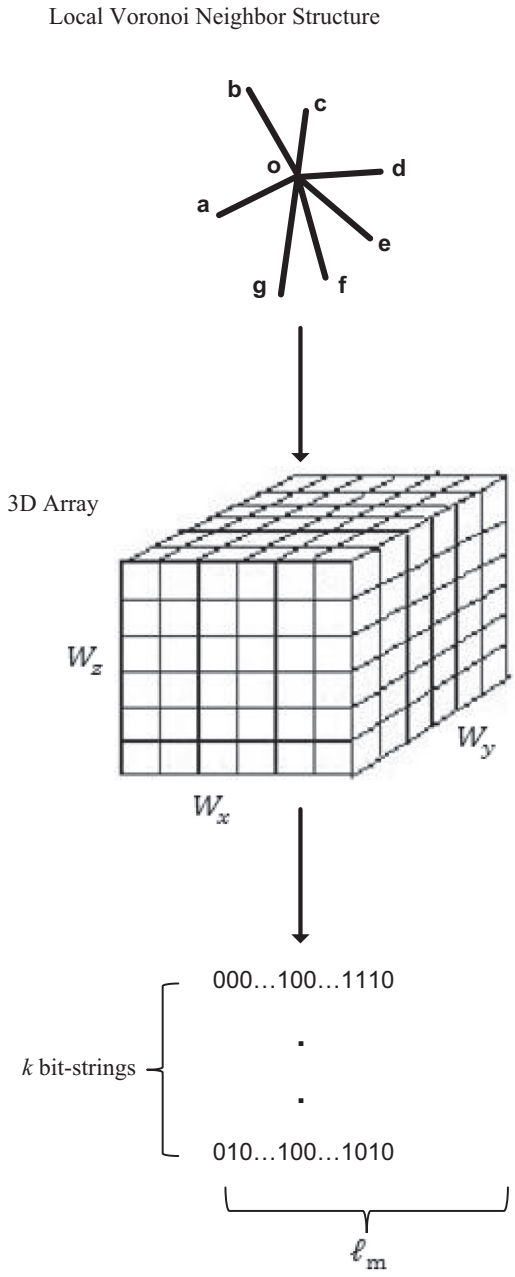

Fig. 8. Generation of fixed-length bit-string representation from VNS.

4.4. Encrypted matching

Assume N modified $VNS_{i=1\ldots N}$ are extracted from the input fingerprint image, and each VNS is represented by a set of bit-strings. To perform fingerprint matching in the encrypted domain, at the encoding stage, a security key that needs protection is skillfully bound with the modified VNS based template features by

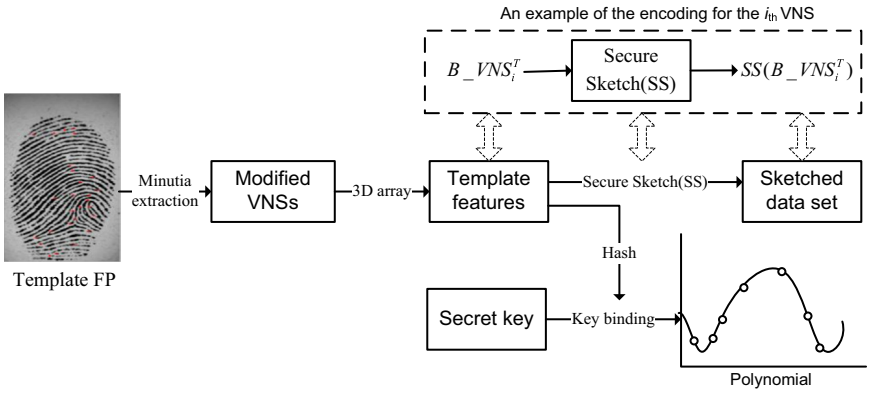

Fig. 9. The encoding stage.

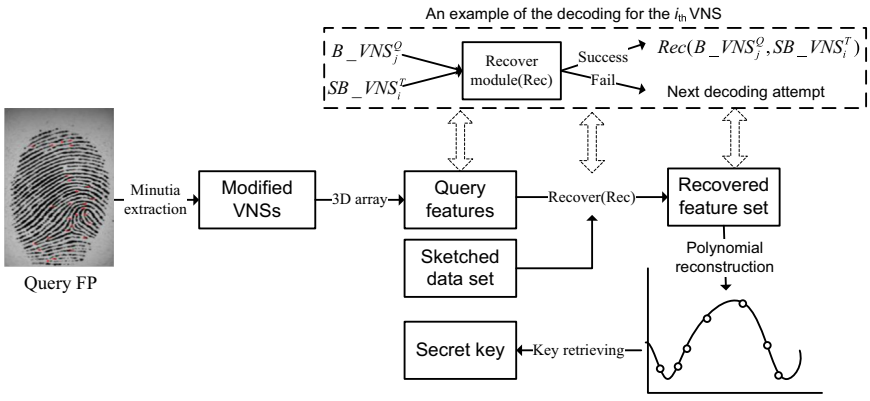

Fig. 10. The decoding stage.

a polynomial which is evaluated at all VNSs and each VNS is protected by the secure sketch, PinSketch. The detailed technique of PinSketch has been introduced in Section 3. At the decoding stage, the secret key can be retrieved by sequentially concatenating the coefficients of the reconstructed polynomial if an enough number of secure sketches can be decoded.

4.4.1. Encoding stage

The procedure of the encoding stage is shown in Fig. 9 and the detailed steps are explained as follows:

1. Given the template fingerprint image T, NT local structures, $\{VNS_i^T\}_{i=1}^{NT}$ based on modified VNSs are generated and represented by their bit-string based representations, $\{B\_VNS_i^T\}_{i=1}^{NT}$. An irreversible universal hash function, $H(\cdot)$ is applied to each $B\_VNS_i^T$ and a hashed value set $\{H(B\_VNS_i^T)\}_{i=1}^{NT}$ is outputted. Here, $H(B\_VNS_i^T)$ is a uniformly distributed random string.
2. Given a key provided by the user, if we expect that $(num+1)$ terms of $B\_VNS_i^T$ are able to recover it, then it is encoded into a polynomial $P(x)$ of degree num by dividing it into $(num+1)$ segments and using them as the coefficients of $P(x)$, e.g., $P(x)=k_{num}x^{num}+\ldots+k_0$ [33,34]. $P(x)$ is evaluated at all the elements of $\{H(B\_VNS_i^T)\}_{i=1}^{NT}$ to obtain the value set $\{P(H(B\_VNS_i^T))\}_{i=1}^{NT}$.
3. To protect the template data, each $B\_VNS_i^T$ is secured by PinSketch and the sketch data can be obtained by $SB\_VNS_i^T = SS(B\_VNS_i^T)$. Here secure sketch $SS(\cdot)$ is defined in (1).
4. The union of polynomial value set $\{P(H(B\_VNS_i^T))\}_{i=1}^{NT}$ and the sketch data set $\{SB\_VNS_i^T\}_{i=1}^{NT}$ form the lock set for the secret key and are stored for decoding.

4.4.2. Decoding stage

The procedure of the decoding stage is shown in Fig. 10 and the detailed steps are explained as follows:

1. Given a query fingerprint image Q, NQ local structures, $\{VNS_j^Q\}_{j=1}^{NQ}$ based on modified VNSs are generated and represented by their bit-string based representations, $\{B\_VNS_j^Q\}_{j=1}^{NQ}$.
2. In order to retrieve the encoded secret key, an unlock set which is composed of the decoded value from sketch data set $\{SB\_VNS_i^T\}_{i=1}^{NT}$ by $\{B\_VNS_j^Q\}_{j=1}^{NQ}$ should be generated first. To see if the ith sketched data set $SB\_VNS_i^T$ from template T could be decoded by the jth local Voronoi neighbor structure VNS_j^Q from query Q, a decoding attempt between the feature representation, $B\_VNS_j^Q$ of VNS_j^Q from query Q and the sketch data, $SB\_VNS_i^T$ from template T is performed. Specifically, the central minutiae's types of local structures, VNS_j^Q and VNS_i^T are compared firstly. If they are different, a fail is reported and the next decoding attempt is carried on. If they are same, both $B\_VNS_j^Q$ and $SB\_VNS_i^T$ are inputted into the recover module, Rec of PinSketch which outputs a recovered value $Rec(B\_VNS_j^Q, SB\_VNS_i^T)$ or an error report. PinSketch has the capability of correcting t errors between two VNSs. In the proposed method, we define that two VNSs are matched if $N_{\text{threshold}} = \lceil k \times \varphi \rceil$ minutiae are matched between VNS_i^T and VNS_j^Q. Here, $\varphi \in (0,1]$ is a similarity threshold between the two local structures, so $t = 2(k - N_{\text{threshold}})$ symmetric set differences can be tolerated in our scheme. For instance, assume φ is set to be 0.65 and there are $k=8$ minutiae in both VNS_i^T and VNS_j^Q, then the symmetric set difference can be tolerated is $t=6$. If $dis(B\_VNS_i^T, B\_VNS_j^Q) \le t$, it can guarantee that the recovered value, $Rec(B\_VNS_j^Q, SB\_VNS_i^T)$ is equal to $B\_VNS_i^T$. However, a fail

Table 1
Summary of databases used in our experiments.

Parameter	FVC2000DB1	FVC2002DB1	FVC2002DB2	FVC2002DB3	FVC2002DB4	FVC2004DB2
Resolution	500 dpi	500 dpi	569 dpi	500 dpi	500 dpi	500 dpi
Number of fingers	100	100	100	100	100	100
Number of images per finger	8	8	8	8	8	8
Sensor type	Low-cost optical sensor	Optical sensor	Optical sensor	Capacitive sensor	SFinGe v2.51	Optical sensor
Image size	300×300	388×374	560×296	300×300	288×384	328×364
Image quality	Medium	Medium	Medium	Medium to low	Medium to low	Low

will be reported if $dis(B\_VNS_i^T, B\_VNS_j^Q) > t$ and the next decoding will continue.

3. If the ith sketched data set $SB\_VNS_i^T$ from template T is decoded successfully by the jth local Voronoi neighbor structure VNS_j^Q from query Q, the recovered value $Rec(B\_VNS_j^Q, SB\_VNS_i^T)$ is hashed using the same hash function $H(\cdot)$ as in the encoding stage and a hashed value $H(Rec(B\_VNS_j^Q, SB\_VNS_i^T))$ is generated. The hashed value $H(Rec(B\_VNS_j^Q, SB\_VNS_i^T))$ together with and the stored corresponding polynomial equation value $P(H(B\_VNS_i^T))$ are added into the unlock set as an element to reconstruct the polynomial $P(x)$.
4. Finally, if the number of genuine elements in the unlock set is less than a certain threshold value, $(num+1)$, then a non-match is reported. If the number of genuine elements in the unlock set is more than or equal to $(num+1)$, then the polynomial, $P(x)$ can be correctly reconstructed by using Lagrange interpolating polynomials [33,34] and the secret key can be obtained by sequentially concatenating the $(num+1)$ coefficients $k_0 \| k_1 \| \ldots \| k_{\text{num}}$.

5. Experimental results and analysis

5.1. Database selection

We evaluated the proposed method over 6 public fingerprint databases, FVC2000 DB1, all of the 4 databases (DB1, DB2, DB3 and DB4) of FVC2002, and FVC2004 DB2, where each database contains 800 Gy-level fingerprint images collected from 100 fingers with 8 samples for each finger. An overview of each database is given in Table 1.

5.2. Minutia extraction and feature generation from modified VNSs

The software VeriFinger 6.0 from Neurotechnology [35] is used to extract the minutiae from every fingerprint image. The feature representations based on modified local VNSs are in the form of a set of decimal-valued arrays (transformed from the bit-strings in the proposed algorithm) that can be applied to the publicly available PinSketch code [36], which is an implementation of syndrome encoding and decoding for fuzzy extractor. The code for feature representations can be supplied on request and will be publicly available via UNSW Canberra Cyber Security Group link [37].

5.3. Performance evaluation

Three performance indices are used for performance evaluation: (1) false reject rate (FRR), which is defined as the ratio of unsuccessful genuine attempts to the total genuine attempts, (2) false accept rate (FAR), which is defined as the ratio of successful imposter attempts to the total imposter attempts, and (3) equal error rate (EER), which is defined as the error rate when the FRR and FAR are equal. In order to compare our results with the existing work, each database is further divided into two data sets with one data set containing only the 1st and 2nd (1 & 2) images of each finger and the other data set containing all the 8 images (1–8) of each finger. Two different protocols used in [38,39], the 1vs1 protocol and the standard FVC protocol, are utilized on these two data sets, respectively, to evaluate the recognition performance of the proposed method.

Table 2
3D array quantization parameters and corresponding EER(%) on data sets that contain images 1 and 2.

Data Set	Cell length C_L	Cell width C_W	Cell height C_H	EER (%)
2000DB1 images 1 and 2	15	15	$\pi/9$	17.98
	15	15	$\pi/6$	14.18
	20	20	$\pi/9$	15.22
	20	20	$\pi/6$	14.43
	25	25	$\pi/9$	13.50
	25	**25**	**$\pi/6$**	**13.11**
2002DB1 images 1 and 2	15	15	$\pi/9$	7.61
	15	**15**	**$\pi/6$**	**3.38**
	20	20	$\pi/9$	5.22
	20	20	$\pi/6$	4.81
	25	25	$\pi/9$	5.01
	25	25	$\pi/6$	4.81
2002DB2 images 1 and 2	**15**	**15**	**$\pi/9$**	**0.59**
	15	15	$\pi/6$	0.95
	20	20	$\pi/9$	2.04
	20	20	$\pi/6$	1.97
	25	25	$\pi/9$	2.56
	25	25	$\pi/6$	3.39
2002DB3 images 1 and 2	15	15	$\pi/9$	12.13
	15	**15**	**$\pi/6$**	**9.80**
	20	20	$\pi/9$	12.43
	20	20	$\pi/6$	13.89
	25	25	$\pi/9$	13.01
	25	25	$\pi/6$	10.67
2002DB4 images 1 and 2	15	15	$\pi/9$	18.27
	15	15	$\pi/6$	20.03
	20	**20**	**$\pi/9$**	**16.52**
	20	20	$\pi/6$	18.57
	25	25	$\pi/9$	22.66
	25	25	$\pi/6$	22.08
2004DB2 images 1 and 2	15	15	$\pi/9$	20.72
	15	**15**	**$\pi/6$**	**14.88**
	20	20	$\pi/9$	17.40
	20	20	$\pi/6$	18.27
	25	25	$\pi/9$	16.25
	25	25	$\pi/6$	18.00

For data sets that contain images 1 and 2, the 1vs1 protocol is used. Specifically, the 1st image from each finger in the data set is compared with the 2nd image from the same finger to compute the FRR. The 1st image from each finger in the data set is compared with the 1st image from the remaining fingers in the data set to calculate the FAR. In order to avoid correlation, if image g has been compared with h, then the symmetric comparison (i.e. h against g) is not executed. So it results in 100 genuine matching attempts and $((100 \times 99)/2) = 4950$ imposter matching attempts.

For data sets that contain images 1–8, the standard FVC protocol is used. Specifically, each image in the data set is compared with the remaining 7 images from the same finger to calculate the FRR. The 1st image from each finger in the data set is compared with the 1st image from the remaining fingers in the data set to calculate the FAR. In order to avoid correlation, if image g has been compared with h, then the symmetric comparison (i.e. h against g) is not executed. So it

results in $((8\times 7)/2)\times 100=2800$ genuine matching attempts and $((100\times 99)/2)=4950$ imposter matching attempts.

For all the 6 databases (12 data sets), we set $W_x=600$, $W_y=600, W_z=2\pi$ which means the maximum edge length allowed in each VNS is set to be 300 pixels. If the edge length between a minutiae, a and its center minutia, o is larger than 300, this minutia, a would be excluded from the VNS centered at minutia, o. We examined different configurations of the array cell, length C_L, width C_W and height C_H, and obtained the matching performance of the proposed method in terms of the EER on these 12 data sets as shown in Tables 2 and 3. From Table 2, we can see that for the data sets that contain images 1 and 2, the proposed method performs best over the database 2002DB2, for which the best EER is 0.59% under the parameter setting ($C_L=15, C_W=15$, $C_H=\pi/9$) and performs worst over the database 2002DB4, for which the best EER is only 16.52% under the parameter setting ($C_L=20, C_W=20, C_H=\pi/9$). This is because compared with database 2002DB2, the image quality of database 2002DB4 is considerably low with more spurious and missing minutiae, and some poor quality images are even incomplete. The ROC curves of the proposed method under the parameter setting that achieves the best EER performance on each data set in Table 2 are shown in Fig. 11. As shown in Table 3, for the data sets that contain images 1–8, the proposed method also performs best over the database 2002DB2, for which the best EER is 10.38%. It is much worse than the recognition performance (EER=0.59%) on the data set that only contains images 1 and 2 of database 2002DB2 under the same parameter setting ($C_L=15, C_W=15, C_H=\pi/9$). This is because that the first 2 images of each finger in the database 2002DB2 were acquired in the same session and hence have less variation than other images of the same finger [4]. Actually, in the real application, we assume that system users would be cooperative in providing their fingerprints so as to pass the authentication [20]. The ROC curves of the proposed method under the parameter setting that achieves the best EER performance over each data set in Table 3 are shown in Fig. 12.

Table 3
3D array quantization parameters and corresponding EER(%) on data sets that contain images 1–8.

Data Set	Cell length C_L	Cell width C_W	Cell height C_H	EER (%)
2000DB1 images	15	15	$\pi/9$	16.40
1–8	15	15	$\pi/6$	14.69
	20	20	$\pi/9$	15.06
	20	20	$\pi/6$	15.35
	25	**25**	$\boldsymbol{\pi/9}$	**14.30**
	25	25	$\pi/6$	15.48
2002DB1 images	**15**	**15**	$\boldsymbol{\pi/9}$	**11.84**
1–8	15	15	$\pi/6$	13.61
	20	20	$\pi/9$	13.01
	20	20	$\pi/6$	13.03
	25	25	$\pi/9$	13.55
	25	25	$\pi/6$	15.32
2002DB2 images	**15**	**15**	$\boldsymbol{\pi/9}$	**10.38**
1–8	15	15	$\pi/6$	10.92
	20	20	$\pi/9$	10.39
	20	**20**	$\pi/6$	11.35
	25	25	$\pi/9$	11.58
	25	25	$\pi/6$	13.92
2002DB3 images	15	15	$\pi/9$	20.91
1–8	15	15	$\pi/6$	17.98
	20	**20**	$\pi/9$	16.81
	20	20	$\boldsymbol{\pi/6}$	**16.52**
	25	25	$\pi/9$	17.40
	25	25	$\pi/6$	17.11
2002DB4 images	15	15	$\pi/9$	16.81
1–8	15	15	$\pi/6$	17.40
	20	**20**	$\boldsymbol{\pi/9}$	**15.63**
	20	20	$\pi/6$	16.83
	25	25	$\pi/9$	18.27
	25	25	$\pi/6$	20.61
2004DB2 images	15	15	$\pi/9$	23.64
1–8	15	15	$\pi/6$	20.91
	20	20	$\boldsymbol{\pi/9}$	**20.61**
	20	20	$\pi/6$	21.49
	25	25	$\pi/9$	22.37
	25	25	$\pi/6$	22.66

5.4. Comparison with other alignment-free bio-cryptosystems

We also compared the proposed method with several other existing similar methods, such as the two local features fusing based method [7], the five nearest minutiae based method [8], the dual layer structure check based method [9], and the Delaunay triangle based method [10] in term of FRR, FAR and EER over public databases in Table 4. We can see from Table 4 that the proposed method has better performance than other existing alignment-free methods over the same data set.

Since the two local features fusing based scheme [7] is based on fuzzy vault sketch, the main problem is cross-matching attack. For instance, if same biometric data sets are reused for constructing different vaults in different applications, it is possible to figure out the genuine points by simply checking the correlation among the data stored in different databases [34]. This is similar to single-input multiple-output blind system identification, where source

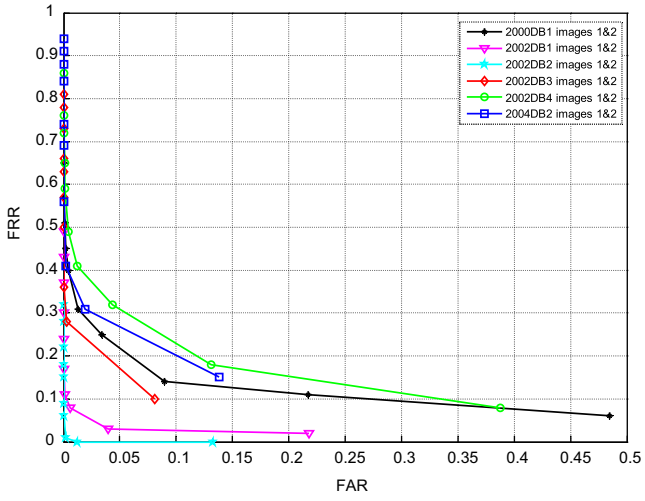

Fig. 11. ROC curves on data sets that contain images 1 and 2.

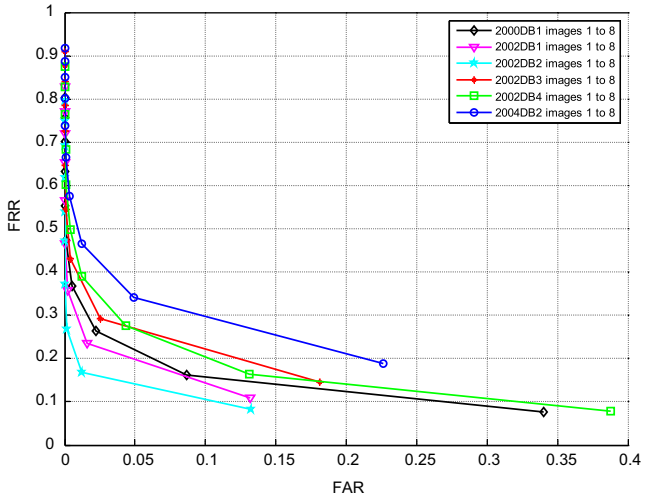

Fig. 12. ROC curves on data sets that contain images 1–8.

Table 4
Performance comparison with existing alignment-free bio-cryptosystems.

Method	2000DB1 images 1 and 2		2002DB1 images 1 and 2		2002DB2 images 1 and 2		2002DB3 images 1 and 2		2002DB4 images 1 and 2		2004DB2 images 1 and 2	
	FRR/FAR	EER	FRR/FAR	EER	FRR/FAR	EER	FRR/FAR	EER	FRR/FAR	EER	FRR/FAR	EER
Li et al. [7]	–	–	–	–	7/0	–	–	–	–	–	–	–
Kai et al. [9]	–	–	–	–	–	4.5	–	–	–	–	–	–
Proposed	40/0.44	13.11	8/0.59	3.38	6/0.02	0.59	28/0.3	9.80	49/0.42	16.52	41/0.22	14.88
Method	2000DB1 images 1–8		2002DB1 images 1–8		2002DB2 images 1–8		2002DB3 images 1–8		2002DB4 images 1–8		2004DB2 images 1–8	
	FRR/FAR	EER	FRR/FAR	EER	FRR/FAR	EER	FRR/FAR	EER	FRR/FAR	EER	FRR/FAR	EER
Arakala et al. [8]	–	15	–	–	–	–	–	–	–	–	–	–
Yang et al. [10]	–	–	–	–	–	13	–	–	–	–	–	–
Proposed	36.79/0.55	14.30	35.79/0.2	11.84	26.79/0.16	10.38	43/0.38	16.52	49.71/0.42	15.63	57.57/0.34	20.61

symbols can be recovered when multiple output blocks are collected [40]. However, cross-matching attack is not an issue for the proposed method. In the five nearest minutiae based scheme [8], the binary strings of both global and local representations are short and hence subject to brute force attack. For example, the entropy of the five nearest minutiae based bio-cryptosystem for database 2000DB1 is only 34 bits. By contrast, the security of our method is strong; see the security analysis on the proposed scheme in Section 5.5. In the dual layer structure check based scheme [9], two layers of each minutia have to be constructed with all the minutiae in the image and checked, it greatly increases the computational complexity of the overall system. Contrarily, in the proposed method, structures are only formed by each minutia and its Voronoi neighbors and only one layer comparison is conducted. In the Delaunay triangle based scheme [10], although the Delaunay triangulation based structure could tolerate elastic distortion to some extent, it could not handle large non-linear distortion which may alter the local triangulation structures. In contrast, the proposed method can effectively compensate the local structural change by using modified VNSs, thus mitigating the influence of large non-linear distortion on the local structures.

5.5. Security analysis

Suppose that an adversary tries to access the key of a genuine user, he or she has to decode $(num+1)$ sketched template data set so as to reconstruct the polynomial $P(x)$ and gain the secret key. The sketched template data set and the hash function are either stored on a smart card or in a central database. Assume the smart card and database are safe and the sketched data set $\{SB\_VNS_i^T\}_{i=1}^{NT}$ and hash function are unreachable for the adversary. The security level of each sketch in this case should be high and it is computationally infeasible for the adversary to conquer the system through brute force attacks. To analyze the security of the output of PinSketch of each VNS under the situation where the adversary has acquired the sketched data set $\{SB\_VNS_i^T\}_{i=1}^{NT}$ generated from template data set, we follow the notions of min-entropy and average min-entropy in [24]. In particular, the min-entropy $H_\infty(A)$ of a randomly and uniformly distributed variable A is defined as $H_\infty(A) = -\log(max_a \Pr(A=a))$. For two random variables A and B, the average min-entropy of A given B is defined as $\tilde{H}_\infty(A|B) = -\log(E_{b\leftarrow B}[2^{-H_\infty(A|B=b)}])$. This definition is useful in the analysis of residual entropy of A when the variable B is known. Because for any ℓ_B-bit string B, the mutual information of A and B is at most ℓ_B bits, which means $\tilde{H}_\infty(A|B) \geq H_\infty(A) - \ell_B$ [22].

For the data sets used in the proposed method, the min-entropy of $H_\infty(A)$ is $\ell_A = \ell_m \times k$ bits, and the string length of B is $\ell_B = \ell_m \times t$ bits [6], where $A = B\_VNS_i^T$, $B = SB\_VNS_i^T$. So even the adversary obtains the sketched data $SB\_VNS_i^T$, the residual entropy of $B\_VNS_i^T$ is $\tilde{H}_\infty(A|B) \geq \ell_m \times k - \ell_m \times t$. Taking the data set that contains images 1 and 2 of database 2002DB2 as an example, according to the quantization parameter setting ($C_L = 15, C_W = 15, C_H = \pi/9$), ℓ_m is 14 on this data set. Assume the average k is 8, then t is 6. The residual entropy of each sketched data set produced by the encoding procedure of PinSketch is 28 bits for this data set. At the EER point, 4 sketched VNSs from template have to be decoded simultaneously to retrieve the secret key. So the overall entropy of the proposed bio-cryptosystem is $(28 \times 4) = 112$ bits on this data set.

6. Conclusion and future work

Fingerprint image pre-alignment and uncertainty are two challenging issues in the design of bio-cryptosystems. In this paper, we have proposed an alignment-free bio-cryptosystem based on modified VNSs to address these issues. The proposed method obviates fingerprint pre-alignment by utilizing the rotation- and translation-invariant feature representations extracted from modified VNSs. Fingerprint uncertainty is mitigated by the construction of VNSs and modification of the originally formed VNSs. Specifically, small distortion within the tolerance region is dealt with by the 3D array quantization, while large non-linear distortion is compensated by the modified VNSs. Another contribution of the new scheme is that fingerprint matching is performed in the encrypted domain using PinSketch. This enhances the security of the proposed bio-cryptosystem. Experimental results over the public databases show that the new scheme outperforms several existing alignment-free bio-cryptosystems.

For future work, it is noted that although the local structural compensation in the proposed method can retrieve the missing Voronoi neighbors of the central minutia caused by image distortion, it is also likely to introduce some fake Voronoi neighbor minutiae. The use of order 1 triangle algorithm can reduce the possibility of adding fake minutiae, but it is not 100% effective. Therefore, to further improve system performance, we will investigate how to filter fake neighbor minutiae.

Conflict of interest statement

None declared.

Acknowledgements

This work was supported in part by the ARC grants LP110100602, LP100200538, LP100100404, and LP120100595.

References

[1] C. Kaufman, R. Perlman, M. Speciner, Network Security: Private Communication in a Public World, Prentice Hall, Upper Saddle River, NJ, 2002.
[2] K. Cao, X. Yang, X. Chen, Y. Zang, J. Liang, J. Tian, A novel ant colony optimization algorithm for large-distorted fingerprint matching, Pattern Recognition 45 (2012) 151–161.
[3] A. Nagar, Biometric Template Security, Dissertation, Michigan State University, 2012.
[4] E. Liu, J. Liang, L. Pang, M. Xie, J. Tian, Minutiae and modified biocode fusion for fingerprint-based key generation, Journal of Network and Computer Applications 33 (2010) 221–235.
[5] J. Hu, Mobile fingerprint template protection: progress and open issues, in: Proceedings of the 3rd IEEE Conference on Industrial Electronics and Applications (ICIEA'08), 2008, pp. 2133–2138.
[6] E. Liu, H. Zhao, J. Liang, L. Pang, M. Xie, H. Chen, Y. Li, P. Li, J. Tian, A key binding system based on n-nearest minutiae structure of fingerprint, Pattern Recognition Letters 32 (2011) 666–675.
[7] P. Li, X. Yang, K. Cao, X. Tao, R. Wang, J. Tian, An alignment-free fingerprint cryptosystem based on fuzzy vault scheme, Journal of Network and Computer Applications 33 (2010) 207–220.
[8] A. Arakala, J. Jeffers, K. Horadam, Fuzzy extractors for minutiae-based fingerprint authentication, Advances in Biometrics (2007) 760–769.
[9] K. Xi, J. Hu, F. Han, An alignment free fingerprint fuzzy extractor using near-equivalent dual layer structure check (NeDLSC) algorithm, in: Proceedings of the th IEEE Conference on Industrial Electronics and Applications (ICIEA), 2011, pp. 1040–1045.
[10] W. Yang, J. Hu, S. Wang, A delaunay triangle-based fuzzy extractor for fingerprint authentication, in: Proceedings of the IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2012, pp. 66–70.
[11] A. Okabe, B. Boots, K. Sugihara, S.N. Chiu, Spatial Tessellations: Concepts and Applications of Voronoi Diagrams, Wiley, 2009.
[12] A.V. Ceguerra, I. Koprinska, Integrating local and global features in automatic fingerprint verification, in: Proceedings of the 16th International Conference on Pattern Recognition, 2002, pp. 347–350.
[13] K.D. Yu, S. Na, T.Y. Choi, A fingerprint matching algorithm based on radial structure and a structure-rewarding scoring strategy, in: Proceedings of the 5th International Conference on Audio- and Video-based Biometric Person Authentication (AVBPA 2005), Springer, 2005, pp. 656–664.
[14] H. Khazaei, A. Mohades, Fingerprint matching algorithm based on voronoi diagram, in: Proceedings of the International Conference on Computational Sciences and Its Applications (ICCSA'08), IEEE, 2008, pp. 433–440.
[15] R. Soleymani, M.C. Amirani, A hybrid fingerprint matching algorithm using Delaunay triangulation and Voronoi diagram, in: Proceedings of the 20th Iranian Conference on Electrical Engineering (ICEE'12), 2012, pp. 752–757.
[16] Z. Jin, A.B. Jin Teoh, T.S. Ong, C. Tee, Fingerprint template protection with minutiae-based bit-string for security and privacy preserving, Expert Systems with Applications (2011).
[17] A. Juels, M. Wattenberg, A fuzzy commitment scheme, in: Proceedings of the 6th ACM conference on Computer and Communications Security, ACM, 1999, pp. 28–36.
[18] A. Juels, M. Sudan, A fuzzy vault scheme, Designs, Codes and Cryptography 38 (2006) 237–257.
[19] T.C. Clancy, N. Kiyavash, D.J. Lin, Secure smartcardbased fingerprint authentication, in: Proceedings of the 2003 ACM SIGMM Workshop on Biometrics Methods and Applications, ACM, 2003, pp. 45–52.
[20] K. Nandakumar, A.K. Jain, S. Pankanti, Fingerprint-based fuzzy vault: implementation and performance, IEEE Transactions on Information Forensics and Security 2 (2007) 744–757.
[21] Y. Wang, J. Hu, 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 29 (2007) 573–585.
[22] S. Wang, J. Hu, Alignment-free cancellable fingerprint template design: a densely infinite-to-one mapping (DITOM) approach, Pattern Recognition 45 (2012) 4129–4137.
[23] P. Zhang, J. Hu, C. Li, M. Bennamoun, V. Bhagavatula, A pitfall in fingerprint bio-cryptographic key generation, Computers & Security 30 (2011) 311–319.
[24] Y. Dodis, R. Ostrovsky, L. Reyzin, A. Smith, Fuzzy extractors: how to generate strong keys from biometrics and other noisy data, SIAM Journal on Computing 38 (2008) 97–139.
[25] Y. Dodis, L. Reyzin, A. Smith, Fuzzy extractors: How to generate strong keys from biometrics and other noisy data, Advances in cryptology-Eurocrypt, Springer (2004) 523–540.
[26] M. Abellanas, F. Hurtado, P.A. Ramos, Structural tolerance and Delaunay triangulation, Information Processing Letters 71 (1999) 221–227.
[27] J. Gudmundsson, M. Hammar, M. Van Kreveld, Higher order delaunay triangulations, Computational Geometry 23 (2002) 85–98.
[28] J. Gudmundsson, H.J. Haverkort, M. Van Kreveld, Constrained higher order delaunay triangulations, Computational Geometry 30 (2005) 271–277.
[29] X. Liang, A. Bishnu, T. Asano, A robust fingerprint indexing scheme using minutia neighborhood structure and low-order Delaunay triangles, IEEE Transactions on Information Forensics and Security 2 (2007) 721–733.
[30] F. Benhammadi, H. Hentous, K. Bey-Beghdad, M. Aissani, Fingerprint matching using minutiae coordinate systems, Pattern Recognition and Image Analysis (2005) 9–19.
[31] C. Lee, J. Kim, Cancelable fingerprint templates using minutiae-based bit-strings, Journal of Network and Computer Applications 33 (2010) 236–246.
[32] W. Wang, J. Li, W. Chen, Fingerprint minutiae matching based on coordinate system bank and global optimum alignment, in: Proceedings of the 18th International Conference on Pattern Recognition (ICPR'06) IEEE, 2006, pp. 401–404.
[33] J.P. Berrut, L.N. Trefethen, Barycentric lagrange interpolation, Siam Review 46 (2004) 501–517.
[34] K. Nandakumar, A. Nagar, A. Jain, Hardening fingerprint fuzzy vault using password, Advances in Biometrics (2007) 927–937.
[35] Software VeriFinger, Neuro Technology, 2010, 〈http://www.neurotechnology.com〉.
[36] K. Harmon, S. Johnson, L. Reyzin, An implementation of syndrome encoding and decoding for binary BCH codes, Secure Sketches and Fuzzy Extractors, in , 2006.
[37] Software code for modified VNS based feature representations, 〈http://seit.unsw.adfa.edu.au/staff/sites/hu/〉.
[38] M. Ferrara, D. Maltoni, R. Cappelli, Noninvertible minutia cylinder-code representation, IEEE Transactions on Information Forensics and Security 7 (2012) 1727–1737.
[39] L. Nanni, S. Brahnam, A. Lumini, Biohashing applied to orientation-based minutia descriptor for secure fingerprint authentication system, Electronics Letters 47 (2011) 851–853.
[40] S. Wang, J. Cao, J. Hu, A frequency domain subspace blind channel estimation method for trailing zero OFDM systems, Journal of Network and Computer Applications 34 (2011) 116–120.

Wencheng Yang received his B.E. degree in Management College of Wuhan University of Technology in China 2006 and master degree in Computer Science from Korea University in 2008. Now he is currently working toward the PhD degree in the School of Engineering and Information Technology, University of New South Wales (UNSW), Australia. His research fields include biometric pattern recognition and biometric security.

Jiankun Hu is Professor and Research Director of Cyber Security Lab, School of Engineering and IT, University of New South Wales at the Australian Defense Force Academy (UNSW@ADFA), Canberra, Australia. He has obtained his B.E. from Hunan University, China in 1983; PhD in Control Engineering from Harbin Institute of Technology, China in 1993 and Masters by Research in Computer Science and Software Engineering from Monash University, Australia in 2000. He has worked in Ruhr University Germany on the prestigious German Alexander von Humboldt Fellowship 1995–1996; research fellow in Delft University of the Netherlands 1997–1998, and research fellow in Melbourne University, Australia 1998–1999.

Jiankun's main research interest is in the field of cyber security including biometrics security where he has published many papers in high-quality conferences and journals including IEEE Transactions on Pattern Analysis and Machine Intelligence (PAMI). He has served in the editorial board of up to 7 international journals and served as Security Symposium Chair of IEEE flagship conferences of IEEE ICC and IEEE Globecom. He has obtained 7 ARC (Australian Research Council) Grants and is now serving at the prestigious Panel of Mathematics, Information and Computing Sciences (MIC), ARC ERA (The Excellence in Research for Australia) Evaluation Committee.

Song Wang is a senior lecturer in the Department of Electronic Engineering, La Trobe University, Australia. She obtained her PhD degree from the Department of Electrical and Electronic Engineering, the University of Melbourne, Australia. Her research areas are biometric security, blind system identification, and wireless communication.

Milos Stojmenovic is an assistant professor at the department of Informatics and Computation at Singidunum University, in Belgrade, Serbia. He received his PhD in Computer Science degree at the School of Information Technology and Engineering, University of Ottawa, in 2008. He has published roughly thirty articles in the fields of computer vision, image processing, and wireless networks. More details can be found at www.site.uottawa.ca/~mstoj075.