Pattern Recognition 45 (2012) 4129–4137

Contents lists available at SciVerse ScienceDirect

Pattern Recognition

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

Alignment-free cancelable fingerprint template design: A densely infinite-to-one mapping (DITOM) approach

Song Wang [a,1], Jiankun Hu [b,*]

[a] School of Engineering and Mathematical Sciences, La Trobe University, VIC 3086, Australia
[b] School of Engineering and Information Technology, University of New South Wales at the Australian Defence Force Academy (UNSW@ADFA), Canberra ACT 2600, Australia

ARTICLE INFO

Article history:
Received 24 June 2011
Received in revised form
17 February 2012
Accepted 7 May 2012
Available online 18 May 2012

Keywords:
Cancelable templates
Alignment-free
Non-invertible
Infinite-to-one mapping
Security

ABSTRACT

Registration-based cancelable template schemes rely on accurate fingerprint image alignment, which is very difficult to achieve. In this paper, by exploiting pair-minutiae vectors, we develop a lightweight, alignment-free scheme for generating cancelable fingerprint templates. The proposed mathematical model is based on a densely infinite-to-one mapping (DITOM) aiming to achieve the non-invertible property. The transformation designed describes the intersection of a collection of hyperplanes and effectively realizes infinite-to-one mapping. The proposed scheme has the properties of non-invertibility, revocability and multiple template independence. Evaluation of the proposed scheme over FVC2002 DB1, DB2 and DB3 shows that the new method exhibits satisfactory performance compared to existing methods.

1. Introduction

Due to the distinctiveness and permanence of biometric identifiers, e.g., fingerprints, face, iris, biometric recognition provides good security, high efficiency and user convenience [1], thus overcoming weaknesses in traditional token- and knowledge-based recognition methods. In biometrics-based authentication systems, users need not worry about losing keys or forgetting different (or sometimes complex) passwords.

Among various types of biometric identifiers, fingerprints have a good balance of all desirable properties, such as high individuality, permanence and good recognition accuracy. Apart from a long history of use in forensic and criminal investigations, fingerprint-based biometric systems have been widely used in civilian, commercial and financial applications. There is no doubt that new, powerful fingerprint systems will continue to be developed.

Fingerprint recognition consists of two phases: (a) user enrollment, during which a user's fingerprint image is scanned, processed and stored as a template in a central database or on a smartcard, and (b) fingerprint verification, in which individuals are authenticated at the point of access by comparing a query finger with the template via a matching function.

Despite the advantages of fingerprint biometrics, vulnerabilities [2] and challenges do exist in fingerprint recognition, and therefore security and privacy concerns arise. Once a fingerprint image/template is stolen, it is lost forever. Unlike a compromised token or password, compromised fingerprint data cannot be replaced or reissued. A fingerprint template, if compromised, may leak fingerprint features that can be used to reconstruct a fingerprint image. For example, Cappeli et al. [3] reconstructed a fingerprint image based on a standard template. More recently, Feng and Jain [4] developed a method to reconstruct a whole grayscale fingerprint image through the phase image. Wang and Hu [5] proposed a scheme for reconstructing a full fingerprint from a partial fingerprint. In addition, due to various physical factors in fingerprint acquisition, fingerprint images involve uncertainty and large variability, leading to intra-class variations and inter-class similarity.

To protect original biometric data, Ratha, Bolle and Connell [6,7] initiated the idea of cancelable biometrics. As far as cancelable fingerprint templates are concerned, the idea is to transform original fingerprint features in either the signal domain or the feature domain with an irreversible transformation, so that a transformed fingerprint template is generated and stored in the database. If the transformed template is compromised, it does not reveal raw fingerprint data and can be revoked, thus making no security threat to a genuine user and the associated fingerprint authentication system. Contrary to the necessity of retrieving channel coefficients in blind channel identification [8], it is essential that for cancelable biometrics, original biometric data

* Corresponding author. Tel.: +61 2 6268 8186; fax: +61 2 6268 8581.
E-mail addresses: song.wang@latrobe.edu.au (S. Wang), J.Hu@adfa.edu.au (J. Hu).
[1] Tel.: +61 3 9479 3744; fax: +61 3 9471 0524.

0031-3203/$ - see front matter © 2012 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.patcog.2012.05.004

be irretrievable when an impostor obtains the transformed template (and the transformation). Another advantage of cancelable fingerprint templates is that multiple application-specific templates can be built by changing parameters in the chosen transformation, thus preserving users' privacy across different applications.

Generating cancelable fingerprint templates mainly involves registration-based and registration-free methods. A review of these methods is detailed in Section 2. Registration-based cancelable fingerprint templates are required to register (or pre-align) fingerprint images with respect to singular points (core and delta). However, reliable detection of singular points is difficult in noisy images and arch type fingerprints. To overcome difficulties in fingerprint alignment and to better cope with local distortions, registration-free (or alignment-free) cancelable fingerprint templates have been proposed and gained a lot of research momentum in recent years. Registration-free methods rely on local features such as minutiae details to produce cancelable templates.

The focal point in cancelable fingerprint templates is the design of a non-invertible parameterized transformation. Ratha et al. [9] proposed three registration-based transform methods for generating cancelable fingerprint templates: Cartesian, polar and functional transformations. The essence of all three transformations is many-to-one mapping. The first two transformations are built on cell or sector swapping. In light of the heuristic nature of these two transformations, an insight into them shows that "many" (as in many-to-one mapping) become limited choices and hence vulnerable to brute force attack. With tight constraints weakening the many-to-one property, the third transformation is cracked by Feng et al. [10] through solving nonlinear equations.

As for the design of an irreversible transform in registration-free cancelable fingerprint templates, a common drawback in some recently published alignment-free methods (e.g., [11–13]) is that the underpinning transformation is not mathematically non-invertible. Consequently, if a transformed template and the parameter of the transform function are hacked, original fingerprint information would be at risk.

In this paper we develop a transformation mechanism aiming to achieve densely infinite-to-one mapping (DITOM). The mapping can be a line, a plane or more generally, a hyperplane (i.e., a linear surface of higher dimension), being mapped to a point in a complex space. The linear surface as such contains infinitely many densely distributed points. Such an infinite-to-one mapping falls nicely in the framework of linear affine algebraic varieties in the well-established discipline of algebraic geometry [14]. Taking a more algebraic approach, we design the transformation which describes the intersection of a collection of hyperplanes and effectively realizes the infinite-to-one mapping. We then prove that the transformation designed is theoretically non-invertible in that it admits an infinite number of points in the solution space.

By exploiting pair-minutiae vectors and hinging upon the DITOM based non-invertible transformation, we propose a light-weight, registration-free cancelable fingerprint template scheme. The transformed template takes the form of a finite-length, complex-valued vector and can be revoked and replaced when compromised. Fingerprint matching is performed in the transformed domain to enhance security. We conducted comprehensive testing to evaluate the proposed scheme using three databases (DB1, DB2 and DB3) of FVC2002 [15]. The experiment results show that the new method exhibits better performance than the most recent method [16] and other methods listed in [16].

The contribution of the proposed scheme lies in three aspects. First, with no constraint imposed whatsoever, the DITOM based non-invertible transformation addresses the fundamental issue in the design of cancelable fingerprint templates. The DITOM guarantees the secrecy of original fingerprint data. Second, we make use of minutiae features in an efficient manner in that all minutiae data are processed in a batch. This is in contrast to a minutia-by-minutia treatment in the recent work of [16,17,13]. Clearly, batch operation speeds up processing time, which is beneficial to practical implementation. Third, the performance of the proposed method is superior to that of the most recent method [16] and other existing methods therein (same database comparison).

The rest of the paper is organized as follows. Section 2 presents some related work on registration-based and registration-free cancelable fingerprint templates. Section 3 describes the proposed scheme and qualitatively compares it with some existing methods. Section 4 demonstrates experiment results and discusses the security of the proposed method. The conclusion is given in Section 5.

2. Related work

Requirements of cancelable fingerprint templates are summarized in [1]. These include: (a) original fingerprints and their (stored) cancelable templates should not match, (b) two differently transformed templates should not match, and (c) if the transformed template is compromised, a new template can be issued and original fingerprint information should not be retrieved from the compromised template.

As noted in Section 1, design of cancelable fingerprint templates can be registration-based or registration-free. Registration-based methods entail accurate detection of singular points, which is hard to achieve. Any error or inaccuracy in singular point detection will have an adverse effect on fingerprint image registration, leading to a faulty cancelable template. Relinquishing the process of fingerprint alignment, registration/alignment-free methods take advantage of local minutiae features, such as the relative angles and distances between a pair of fingerprint minutiae, because they are robust to geometric transformation, e.g., rotation and translation.

Below is a brief review of some existing registration-based and alignment-free cancelable fingerprint template schemes. It is worth mentioning that the literature cited herein is far from complete and only meant to show the current state of the art.

Ratha et al. [9] introduced registration-based cancelable fingerprint template schemes using three non-invertible transformations. Feng et al. [10] and Shin et al. [18] argued that the cancelable template schemes in [9] are vulnerable, especially the surface-folding functional transformation. In [10], a solving-equation attack was launched while in [18], a brute force attack was carried out by trying all possible points in the original fingerprint image.

Takahashi and Hirata [19] developed a registration-based method to generate cancelable templates. They used correlation-invariant random filtering in template transformation and chip matching in fingerprint verification.

Yang et al. [20] proposed a registration-based cancelable fingerprint template design by employing both local and global features of a fingerprint image. In [20], a pair of minutiae points in the circle centered on the core are connected with a line, and both points are mapped onto the circle through perpendicular projection. Additionally, they made use of triangular properties, including the angle between two minutiae and the angle between two lines connecting two minutiae pairs.

A registration-free cancelable template algorithm was proposed in [21] based on localized, self-aligned texture features, in contrast to the global texture descriptor applied in the registration-based method [22]. Lee et al. [17] presented an alignment-free fingerprint

cancelable template approach by generating invariant values, which are calculated using orientation information around each minutia. This makes the method [17] dependent on the quality of fingerprint images. If the image quality is poor, the performance of the method decreases.

Farooq et al. [23] introduced a triangle-based alignment-free method to build cancelable fingerprint templates in the form of bit strings. In this method, a triangle is formed by any set of three minutiae. Three sides of the triangle, three angles of minutiae orientation and the height of the longest triangle side constitute seven invariants. Through quantization and bin shuffling, a bit string (cancelable template) is produced.

Bit-string type methods can also be found in [24,11–13]. In [11,12], invariant features are first extracted from minutiae pairs, then quantized and bin indexed to generate a bit string. In [13], a three-dimensional array is defined, and each minutia in turn is selected as the reference point, according to which other minutiae are transformed and rotated. Transformed minutiae are then mapped into the 3D array so that a bit string is generated. In [11–13], the resultant bit string is permuted with a user-specific PIN. However, since the permutation matrix is invertible, which would enable a hacker to figure out the topological structure of minutiae points via brute force attack, the security of original minutiae locations is seriously weakened.

Recently, Ahmad et al. [16] designed alignment-free cancelable fingerprint templates in a polar coordinate space. Motivated by polar transformation in [9], the authors explored relative locations of minutiae between one another in a pair-polar coordinate system. The proposed method [16] has acceptable performance over FVC2002 DB2 but poor performance over FVC2002 DB3, in which fingerprint images are of low quality.

Comparisons regarding registration-based and alignment-free cancelable templates are given in [25].

3. The DITOM based method for the design of alignment-free cancelable fingerprint templates

Minutiae points in fingerprint images contain rich information about fingerprint patterns [1]. More importantly, the relative relationship between fingerprint minutiae is rotation- and shift-invariant to any coordinate transform. We leverage this invariance property in forgoing the process of registering fingerprint images. Designing a non-invertible parameterized transformation plays a central role in our development of an alignment-free, pair-minutiae vector based scheme for generating cancelable fingerprint templates. Our main idea is captured in the following simple but representative examples; see the illustration in Fig. 1. In Fig. 1a, any point of the line is mapped to the same point. Fig. 1b and c refers to higher dimensional cases. The simplest DITOM is effected by a linear algebraic transformation.

Example 1. A line is defined by $ax+by=c$ in the two-dimensional space, where a, b and c are scalars (real- or complex-valued). This linear polynomial map allows an infinite number of choices of x and y to be mapped to c. Similarly, a plane defined by $ax+by+cz=d$ in the three-dimensional space allows an infinite number of x, y and z to be mapped to d.

Example 2. In the case of two planes expressed by $a_1x+b_1y+c_1z=d_1$ and $a_2x+b_2y+c_2z=d_2$, the intersection of them is possibly a line or a plane. Again infinitely many x, y and z can be mapped to d_1 and d_2.

The above examples can be generalized to higher-dimensional hyperplanes. The intersection of a collection of hyperplanes is representable by a linear transformation algebraically, and the transformation can be designed in a controllable manner to realize infinite-to-one mapping.

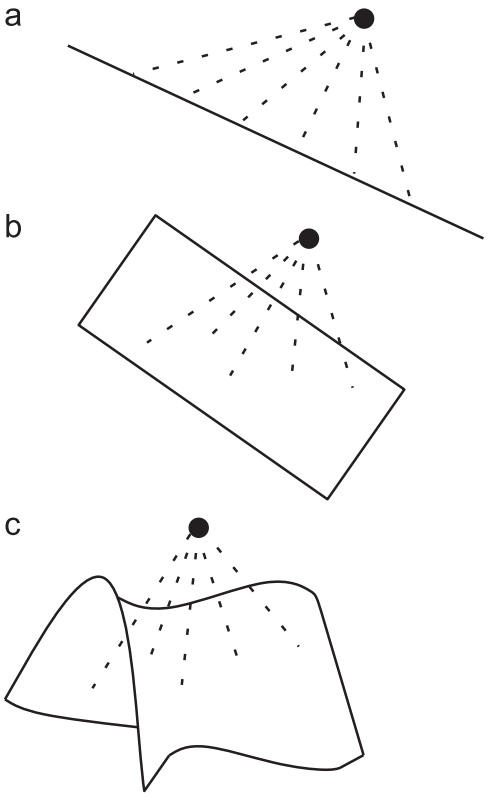

Fig. 1. Infinite-to-one mapping from a line, a plane and a hyperplane.

In the following section (Section 3.1), we first define pair-minutiae vectors and then process them with an intention to lay the foundation of constructing a DITOM based non-invertible transformation. Next, we concentrate on the transformation which leads to the cancelable templates.

3.1. Cancelable template generation

Suppose minutiae points are extracted from a fingerprint image and a set of minutiae are selected such that the distance between a pair of minutiae is not less than a small threshold. Let us denote the set of the selected minutiae by

$$\boldsymbol{M}=\{M_k(x_k,y_k,\theta_k)\}_{k=1}^{m} \tag{1}$$

where m is the number of minutiae, x_k, y_k and θ_k are the x, y coordinates and orientation of the kth minutia, respectively. By pairing up any two minutiae $M_i(x_i,y_i,\theta_i)$ and $M_j(x_j,y_j,\theta_j)$ in the set $\boldsymbol{M}$, a pair-minutiae vector V_{ij} can be constructed. Given that the number of minutiae in the set $\boldsymbol{M}$ is m, there will be $(m(m-1)/2)$ pair-minutiae vectors, constituting the set $\mathbf{V}$. We express $\mathbf{V}$ as

$$\mathbf{V}=\{V_{ij}:\ 1\le i,j\le m \text{ and } i\ne j\} \tag{2}$$

Each V_{ij} in the set $\mathbf{V}$ is characterized by the distance and relative angles of the minutiae pair (M_i,M_j). To make the angle definition for V_{ij} unambiguous, we assume that the reference direction of the line segment connecting the minutiae pair is from $M_i(x_i,y_i,\theta_i)$ to $M_j(x_j,y_j,\theta_j)$. Hence, V_{ij} is defined by

$$V_{ij}=(L,\alpha_i,\beta_j) \tag{3}$$

where L denotes the distance between the two minutiae, α_i is the angle between the reference direction of the line segment and the orientation of $M_i(x_i,y_i,\theta_i)$ in the counter-clockwise direction, and

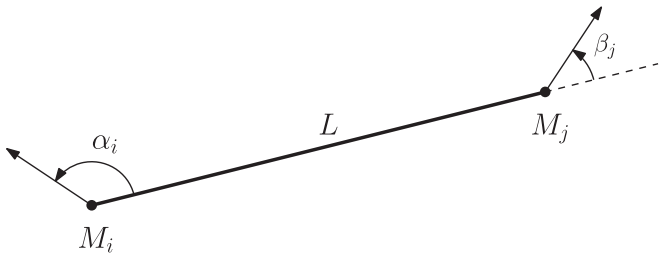

Fig. 2. The triplet (L,α_i,β_j) formed by minutiae pair (M_i,M_j).

β_j is defined analogously. The range of α_i and β_j is between 0 and 2π. The formation of the triplet (L,α_i,β_j) from the minutiae pair (M_i,M_j) is illustrated in Fig. 2.

To determine V_{ij}, we first calculate the following two quantities $\mathcal{X}$ and $\mathcal{Y}$:

$$\mathcal{X}=(x_j-x_i)\cos\theta_i+(y_j-y_i)\sin\theta_i$$

$$\mathcal{Y}=(x_j-x_i)\sin\theta_i-(y_j-y_i)\cos\theta_i$$

Based on $\mathcal{X}$ and $\mathcal{Y}$, $V_{ij}=(L,\alpha_i,\beta_j)$ is then obtained by

$$L=\sqrt{\mathcal{X}^2+\mathcal{Y}^2}$$

$$\alpha_i=\arctan\frac{\mathcal{Y}}{\mathcal{X}}$$

$$\beta_j=\alpha_i+\theta_j-\theta_i \tag{4}$$

Clearly, the pair-minutiae vector set $\mathbf{V}$ [see (2)] contains original fingerprint data. To protect this information, we quantize each V_{ij} in $\mathbf{V}$ using a similar procedure in [12]. For convenience, we briefly describe this procedure. After selecting a quantization stepsize for each term of the triplet (L,α_i,β_j) in (3), the number of bits required to represent the quantized results in binary notation can be determined. Suppose n_L, n_{α_i} and n_{β_j} are respectively the bit length for representing the binary outputs of the quantized L, α_i and β_j. Then the total number of bits required for quantizing the set $\mathbf{V}$ is

$$n=n_L+n_{\alpha_i}+n_{\beta_j} \tag{5}$$

Thus, for each pair-minutiae vector V_{ij} in $\mathbf{V}$, we can find a binary representation $V_{ij}^{(b)}$ of n bits. Denote the set formed by $V_{ij}^{(b)}$ as $\mathbf{V}^{(b)}$, i.e.,

$$\mathbf{V}^{(b)}=\{V_{ij}^{(b)}:\ 1\le i,j\le m \text{ and } i\ne j\} \tag{6}$$

Since n bits can represent 2^n binary values, binning from $00\ldots0$ (the first bin with n zeros) to $11\ldots1$ (the last bin with n ones), we go through each $V_{ij}^{(b)}$ in the set $\mathbf{V}^{(b)}$ and index a bin by one if $V_{ij}^{(b)}$ falls in it. It is possible that some bins are indexed multiple times. We follow the same rule in [12] to binarize the resultant index. That is, only the bins indexed once are assigned the value of 1 and all other bins the value of 0. At the end of this process, we obtain a binary string $\{h_k\}$ of length 2^n, in which 1 s correspond to the unique occurrence of those $V_{ij}^{(b)}$ in (6).

Although quantization and indexing provide some protection over original fingerprint biometrics featured in V_{ij}, an attacker is able to configure the locations of minutiae if he/she acquires the binary string $\{h_k\}$. This is because if $\{h_k\}$ is compromised, the binary representations $V_{ij}^{(b)}$ that appear once would be revealed, which would further disclose the corresponding V_{ij}. It is not a difficult task to recover the topology of original minutiae from the disclosed V_{ij}. Therefore, it is critical to secure the binary string $\{h_k\}$. That is, we need to transform it irreversibly. However, since $\{h_k\}$ only contains values of 0 and 1, it is likely to impose limitation on the result if transformation is directly performed on it. To address the issue, we convert $\{h_k\}$ into a complex vector in the frequency domain by taking the Discrete Fourier Transform (DFT). As the length of $\{h_k\}$ is 2^n, we perform the 2^n-point DFT on $\{h_k\}$ to obtain its frequency–domain complex samples H_i, given by

$$H_i=\sum_{k=0}^{2^n-1}h_k e^{-j2\pi ik/2^n},\quad i=0,1,\ldots,2^n-1 \tag{7}$$

We rewrite H_i into the $2^n\times1$ vector $\boldsymbol{H}=[H_0\ H_1\ \cdots\ H_{2^n-1}]^T$. Obviously, it is equally important to secure the complex vector $\boldsymbol{H}$. Now the task is to transform it non-invertibly. The problem is approached from a geometric point of view and solved with an algebraic approach as follows.

A hyperplane in the 2^n-dimensional complex space can be described by a linear polynomial in 2^n variables. The intersection of a collection of such hyperplanes, which is known as a linear variety [14], is itself a linear surface of dimension 2^n-r, where r is the number of linearly independent polynomials. Evidently, such a linear surface contains infinitely many points for an appropriate value of r. Naturally, it would be desirable if $\boldsymbol{H}$ happens to be a point of this linear surface, making the possibility of locating it almost nil.

The geometric realization of the intersection of hyperplanes is closely connected to the solution set of a system of linear equations. As a matter of fact, all this is essentially determined by a linear parametric transformation in the algebraic sense, and this transformation basically maps infinitely many points of the above-mentioned linear surface to a point in the complex space of dimension p. The transformation is compactly described in the matrix form by

$$\mathbf{A}\boldsymbol{H}=\boldsymbol{T} \tag{8}$$

where $\mathbf{A}$ is a $p\times q$ matrix with $q=2^n$ and $p<q$, $\text{rank}(\mathbf{A})=r$, and $\boldsymbol{T}$ is the $p\times1$ complex vector resulting from the transformation of $\boldsymbol{H}$. The vector $\boldsymbol{T}$ is the generated template to be stored in the database. The matrix $\mathbf{A}$ in (8) plays the role of parameter key, which can be randomly generated.

It is a well-known theorem in linear algebra that for a system of linear equations [26], if the coefficient and augmented matrices have the same rank, then solutions exist, and what is more, if this rank is less than the number of unknowns, then there is an infinite number of solutions. Next, we show that a system of linear equations $\mathbf{A}\boldsymbol{G}=\boldsymbol{T}$, with a general vector $\boldsymbol{G}$ representing q unknowns, has infinitely many solutions. Obviously, considering (8), $\boldsymbol{H}$ is one solution to $\mathbf{A}\boldsymbol{G}=\boldsymbol{T}$.

Proposition. *A non-homogeneous system of p linear equations with q unknowns, written in the matrix form of* $\mathbf{A}\boldsymbol{G}=\boldsymbol{T}$, *has an infinite number of solutions.*

Proof. First we shall prove that $\mathbf{A}\boldsymbol{G}=\boldsymbol{T}$ has solutions. It follows from (8) that $\boldsymbol{T}$ is a linear combination of columns of $\mathbf{A}$, which means that $\boldsymbol{T}$ must lie in the column space of $\mathbf{A}$. Therefore, $\text{rank}(\mathbf{A})=\text{rank}([\mathbf{A}\ \boldsymbol{T}])$. Since the coefficient matrix and the augmented matrix have the same rank, solutions of $\mathbf{A}\boldsymbol{G}=\boldsymbol{T}$ exist [26]. Next, because $\text{rank}(\mathbf{A})=r<q$, there are infinitely many solutions to $\mathbf{A}\boldsymbol{G}=\boldsymbol{T}$. □

The above development shows that there is an infinite number of $\boldsymbol{G}$ mapped to $\boldsymbol{T}$ via $\mathbf{A}$, yielding infinite-to-one mapping. Moreover, $\boldsymbol{H}$ to be protected is hidden among the infinitely many solutions to $\mathbf{A}\boldsymbol{G}=\boldsymbol{T}$, making the search for $\boldsymbol{H}$ difficult even when an attacker acquires both $\boldsymbol{T}$ and $\mathbf{A}$. Lastly, the generated template $\boldsymbol{T}$ is revocable if it is compromised. A new template can be issued with a different key, which is easily done by generating a different matrix $\mathbf{A}$.

In the following we give a small yet representative example to demonstrate that performing pseudo-inversion does not help to

find the true $\boldsymbol{H}$ when $\mathbf{A}$ and $\boldsymbol{T}$ are both lost. For simplicity, $\boldsymbol{H}$ under protection is represented by a low dimensional real vector. Suppose that

$$\boldsymbol{H}=[0.5\ \ 1\ \ 1\ \ -1]^T,\quad \mathbf{A}=\begin{bmatrix} 2 & -1 & 3 & 1 \\ 1 & 2 & -1 & 1.5 \\ -1 & 0.5 & -1.5 & -0.5 \end{bmatrix}$$

Hence, $\mathrm{rank}(\mathbf{A})=2$, and $\boldsymbol{T}=\mathbf{A}\boldsymbol{H}=[2\ \ 0\ \ -1]^T$ is the transformed template. Let $\hat{\boldsymbol{H}}$ denote the pseudo-inverse estimate of $\boldsymbol{H}$. $\hat{\boldsymbol{H}}$ is obtained by

$$\hat{\boldsymbol{H}}=\mathbf{A}^{\dagger}\boldsymbol{T}=[0.2963\ \ -0.0864\ \ 0.3827\ \ 0.1728]^T$$

where $\mathbf{A}^{\dagger}$ is the pseudo-inverse of $\mathbf{A}$. Meanwhile, we manually calculate another solution $\tilde{\boldsymbol{H}}=[0.5\ \ -0.1\ \ 0.3\ \ 0]^T$. It can be readily shown that $\mathbf{A}\hat{\boldsymbol{H}}=\boldsymbol{T}$ and $\mathbf{A}\tilde{\boldsymbol{H}}=\boldsymbol{T}$. We now use the (normalized) inner product to determine how close $\hat{\boldsymbol{H}}$ and $\tilde{\boldsymbol{H}}$ are to the true $\boldsymbol{H}$, respectively. We get

$$1-\frac{\boldsymbol{H}^T\hat{\boldsymbol{H}}}{\|\boldsymbol{H}\|_2\|\hat{\boldsymbol{H}}\|_2}=0.7109$$

and

$$1-\frac{\boldsymbol{H}^T\tilde{\boldsymbol{H}}}{\|\boldsymbol{H}\|_2\|\tilde{\boldsymbol{H}}\|_2}=0.5781$$

where $\|\cdot\|_2$ denotes the 2-norm [27]. It follows that neither $\hat{\boldsymbol{H}}$ nor $\tilde{\boldsymbol{H}}$ is close to the true $\boldsymbol{H}$ with $\hat{\boldsymbol{H}}$ being even further.

We summarize the proposed DITOM based cancelable template design algorithm as follows:

1. Use (4) to compute pair-minutiae vectors V_{ij} defined in (3) and establish the set $\mathbf{V}$ in (2).
2. Determine the bit length n in (5) and quantize each pair-minutiae vector V_{ij} in $\mathbf{V}$ such that its binary representation $V_{ij}^{(b)}$ (6) is obtained.
3. Index and binarize all 2^n bins to produce the binary string $\{h_k\}$ of length 2^n. This process follows the same rule as in [12].
4. Perform the DFT on $\{h_k\}$ using (7) so as to convert it to the complex-valued vector $\boldsymbol{H}$.
5. Transform $\boldsymbol{H}$ using (8) to build the cancelable template $\boldsymbol{T}$.

To end the section, we make the following remarks about the proposed cancelable template design in comparison with some existing work:

1. With the angles α_i and β_j ranging from 0 to 2π, the triplet (L,α_i,β_j) in (3) adequately characterizes the pair-minutiae vector V_{ij}. As a result, the required bit length in the subsequent quantization process benefits from this triplet characterization of V_{ij} in our method, as opposed to the quadruplet defined in [12], which requires more bits.
2. The pair-minutiae vector set $\mathbf{V}$ [see (2)] is an efficient casting of the relationship between a pair of minutiae in the sense that V_{ji} is not included in the set $\mathbf{V}$, because it contains the same information as V_{ij}. In contrast, both V_{ij} and V_{ji} are repeatedly used in the algorithm [16], which makes the algorithm [16] implementation-wise more cumbersome than the proposed method.
3. The transformation (8) in our method is dependent on the parameter key $\mathbf{A}$. The key should be user-specific, that is, each individual in the database is assigned a unique key. This minimizes potential linkage among users, making the templates in the database independent of one another. Moreover, it is suggested in [19] that user-specific keys be stored separately from the cancelable templates to prevent them being leaked at the same time.
4. Compared to the existing bit-string type methods (e.g., [11–13]), the proposed algorithm undertakes a completely different treatment on the bit string generated. The vector $\boldsymbol{H}$ is the DFT outcome of the binary string $\{h_k\}$. Given that the length of $\{h_k\}$ is 2^n, as far as the DFT operation is concerned, powerful FFT (fast Fourier transform) techniques (e.g., radix-2 algorithms) can be applied to expedite the DFT computation [28].
5. The proposed DITOM method is fundamentally different to random projection based Biohashing [29,30]. Biohashing combines a user's biometric feature with a set of user-specific random numbers to produce a BioCode (binary string), which is the end product of Biohashing. By contrast, the binary string generated in the proposed scheme is an intermediate result, followed by the DFT and the transformation (8). In particular, the transformation (8) aims to hide the true $\boldsymbol{H}$, frequency–domain samples of the generated binary string, among infinite solutions by means of DITOM. Note that in the binary domain, the number of binary solutions would be finite and often very limited.
Despite seeming resemblance, in essence there are disparate requirements about the matrix $\mathbf{A}$ in the proposed transformation (8) and the random mapping matrix (say $\mathbf{R}$) used in Biohashing [29,30]. The matrix $\mathbf{A}$ in our method is merely a "fat" matrix with no other string attached. However, the projection matrix $\mathbf{R}$ in Biohashing is not only required to be a rectangular matrix but to have orthonormal row vectors such that $\mathbf{R}\mathbf{R}^{\dagger}=\mathbf{I}$, where $\mathbf{R}^{\dagger}$ is the pseudo-inverse of $\mathbf{R}$ and $\mathbf{I}$ is the identity matrix. It is this property of $\mathbf{R}$ that makes Biohashing vulnerable to preimage attack [31]. Moreover, the orthogonality of projection vectors keeps the relative distance between features in the projection space, but distance preservation narrows down the search for the genuine inverse of the protected template in the stolen token case [32,33].

3.2. Fingerprint matching in the transformed domain

Fingerprint matching refers to the process of comparing a template fingerprint and a query fingerprint and returning either a matching score (between 0 and 1) or a binary verdict (mated or not). Due to a variety of factors [1], such as displacement, rotation, nonlinear distortion, pressure and skin condition, and noise, different impressions of the same finger may look quite different while fingerprints from different fingers may appear very similar. The former accounts for intra-class variations and the latter is known as inter-class similarity. Because of the large variability in fingerprint acquisitions, fingerprint matching has always been a complex problem. In the proposed cancelable template scheme, we perform fingerprint matching in the transformed domain in order to enhance the security of original fingerprint biometrics.

Let $\mathcal{M}$ be the set of minutiae for a query fingerprint. We define $\mathcal{M}=\{\mathcal{M}_k(x_k,y_k,\theta_k)\}_{k=1}^{l}$, where all quantities involved are defined analogously to (1). Note that the query fingerprint has l minutiae, which might not equal the number of minutiae for the template fingerprint, even if they come from the same finger. We apply the algorithm presented in the previous section to the query minutiae set $\mathcal{M}$ such that $\mathcal{M}$ undergoes the same operation as the template minutiae set $\boldsymbol{M}$ in (1). As a result, the transformed vector $\mathcal{M}$ for the query is obtained. By the same token, $\mathcal{T}$ is complex-valued with length p. Then, the distance between the transformed template $\boldsymbol{T}$ and the transformed query $\mathcal{T}$ is defined by

$$d(\boldsymbol{T},\mathcal{T})=\frac{\|\boldsymbol{T}-\mathcal{T}\|_2}{\|\boldsymbol{T}\|_2+\|\mathcal{T}\|_2} \tag{9}$$

We remark that the Euclidean metric is chosen since it is inherently adapted to measurement variations in biometric signals [34].

With (9), the matching score between the template and the query in the transformed domain is given by

$$S(\boldsymbol{T},\mathcal{T}) = 1 - d(\boldsymbol{T},\mathcal{T}) = 1 - \frac{\|\boldsymbol{T}-\mathcal{T}\|_2}{\|\boldsymbol{T}\|_2 + \|\mathcal{T}\|_2} \tag{10}$$

With respect to (10), the range of S is between 0 and 1, and the value of S indicates the degree of similarity between the template and query fingerprints. That is, the larger the value of S, the more similar the template and the query. The template and query fingerprints are declared as a "matching pair" if the calculated S is greater than a threshold, which is usually determined through experiments.

4. Experiment results and analysis

The proposed method was evaluated using the FVC2002 databases [15] (DB1, DB2 and DB3). Fingerprint images in these databases cover a wide spectrum in terms of quality. Among three databases, fingerprint images in DB3 are of the lowest quality. Each database contains 100 fingers, for which we used two impression images per finger. Minutiae points were extracted from each image in the databases using the commercial fingerprint recognition software *VeriFinger SDK* [35]. Some widely used minutiae detection methods involve the following processes: image enhancement, binarization and thinning [1]. The VeriFinger software has a host of functionalities—image pre-processing, normalization, feature filtering and extraction.

We found that compared to DB1 and DB2, relatively few minutiae could be extracted from fingerprints in DB3 due to the low image quality with spurious and missing minutiae. Moreover, there are 2% of the mated-pair images in DB3 whose minutiae could not be extracted at all. An example of such an image is shown in Fig. 3, which is the second impression of Finger No. 95 in FVC2002 DB3. The proposed method cannot deal with such fingerprints due to the fact that our method operates on minutiae.

Another related issue is that for some poor quality images, although minutiae could be extracted, the number of minutiae extracted was small; e.g., see Fig. 4 (the image of the second impression of Finger No. 76 in DB3). Again, because the proposed method is minutiae based, a lack of reliable minutiae causes a decrease in recognition accuracy, which is shown by the ROC curve for DB3 in Fig. 5.

Fig. 3. The low quality image of the second impression of Finger No. 95 in FVC2002 DB3.

Fig. 4. The image of the second impression of Finger No. 76 in FVC2002 DB3.

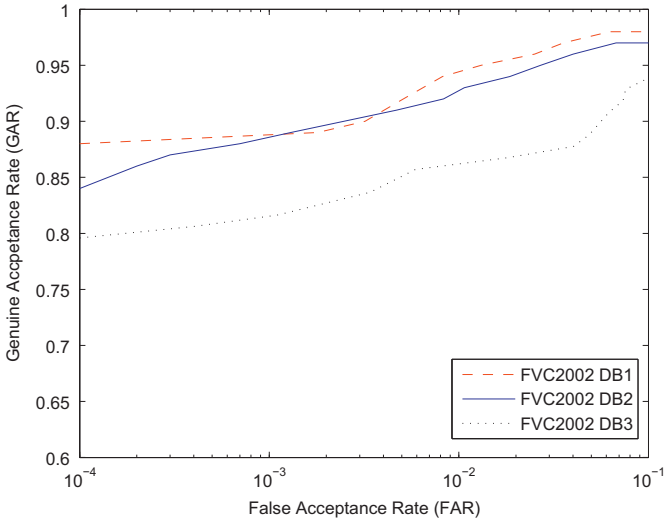

Fig. 5. ROC curves for FVC2002 DB1, DB2 and DB3. For each database, all subjects are assigned the same key.

The Equal Error Rate (EER), False Acceptance Rate (FAR) and False Rejection Rate (FRR) were used as performance measures in our experiments. FAR is the probability of mistaking biometric measurements from two different fingers to be from the same finger. FRR is the probability of mistaking two biometric measurements from the same finger to be from two different fingers. EER denotes the error rate when the FAR and the FRR are equal.

For the sake of clarity, the two impression images we used for each finger in a database were grouped into two sets—template and query. Thus, for each database, there were 100 images in the template set and 100 mated images in the query set. For all testing scenarios, genuine testing was conducted by comparing each image from the template set to its corresponding image in the query set, while impostor testing was performed by comparing each image from the template set to all images in the query set except its corresponding mated-pair image. In addition, the parameter key **A** was randomly generated.

As quantization is one of the steps in the proposed algorithm, it was observed in our testing that performance of the proposed method varies with the bit length chosen for quantizing V_{ij} (3). A small bit length n [see (5)] cannot sufficiently distinguish

pair-minutiae vectors whereas choosing too many bits increases sensitivity to slight distortions in different acquisitions of the same finger. This phenomenon was also noted in [23,12]. Moreover, the size of **A** grows exponentially with the bit length n, which further impacts on computational efficiency of (8) and the storage of **A**. We found from our testing that $n=15$ is a suitable choice, resulting from $n_L = n_{\alpha_i} = n_{\beta_j} = 5$; refer to (5). The experiment results with associated figures shown below are all based on $n=15$.

The evaluation of the proposed method focuses on the following aspects:

- Lost key attack (worst-case scenario)
- Revocability
- Security analysis

4.1. Lost key attack

Losing a user-specific key represents the worst-case scenario in practice where a user's key is stolen and known by an adversary. We simulated this scenario by assigning the same key to all subjects in a database. We conducted both genuine and impostor testing under this same key situation. The ROC curves for all three databases are illustrated in Fig. 5, where it is shown that the performance of the proposed method is worst for FVC2002 DB3 due to the poor image quality of this database.

When all users in the database have the same key, the EER results for FVC2002 DB1, DB2 and DB3 are 3.5%, 4% and 7.5%, respectively, as shown in Fig. 6. These EER results are better than those of the recent method [16]. The EER comparison between our method and some existing methods is reported in Table 1, where it can be seen that the EER of the proposed algorithm over FVC2002 DB3 is 7.5%, whereas for the same database, the EER in [16] is as high as 27%.

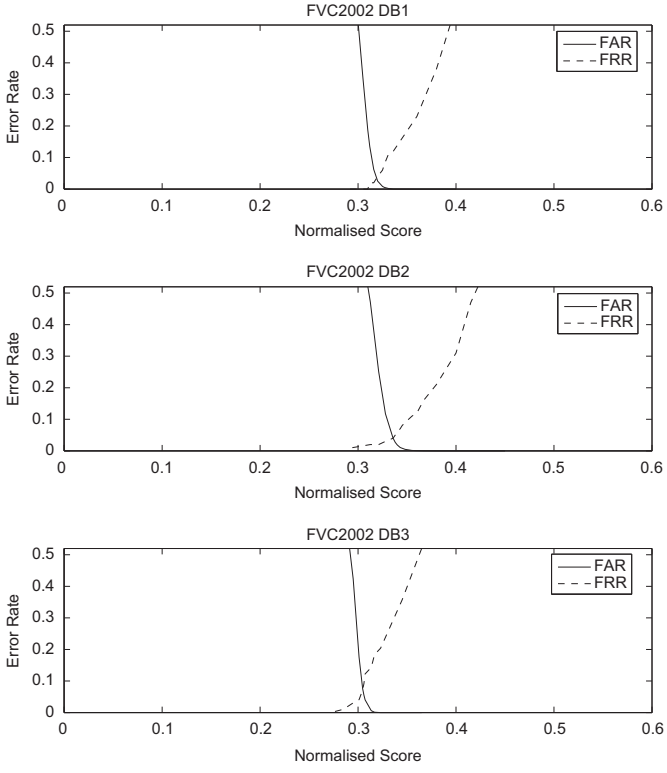

Fig. 6. EER for FVC2002 DB1, DB2 and DB3. For each database, all subjects are assigned the same key.

Table 1
Equal Error Rate (EER) comparison.

Research work on cancelable templates	FVC2002	FVC2002 DB2		FVC2002	FVC2004
	DB1 (%)	Partial data (%)	Full data (%)	DB3 (%)	DB1 (%)
Yang et al. [20]	–	13%	–	–	–
Lee and Kim [13]	–	–	–	–	10.3%
Jin et al. [12]	–	–	–	–	3%
Ahmad et al. [16]	9%	6%	–	27%	–
Proposed method	3.5%	4%	5%	7.5%	–

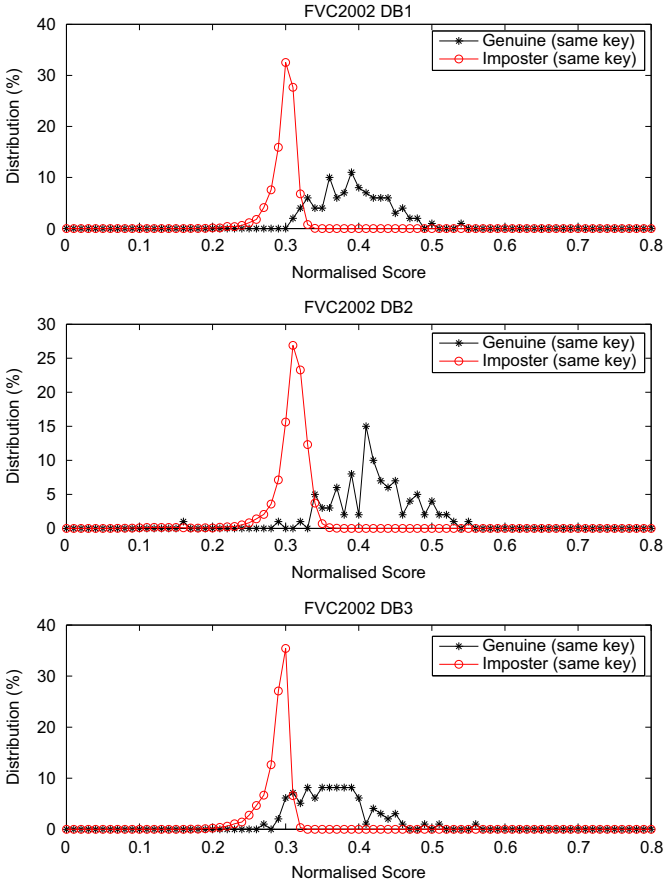

Fig. 7. Genuine and impostor distributions for FVC2002 DB1, DB2 and DB3. For each database, all subjects are assigned the same key.

Using FVC2002 DB2, we found in our testing that the EER before and after the transformation is 3% and 4%, respectively, which shows that the designed transformation only causes a minor degradation in matching performance.

We also plotted in Fig. 7 both genuine and impostor distributions for all three databases in the same key scenario. For the purpose of comparison, we depicted in Fig. 9 the genuine and impostor distributions for FVC2002 DB2 under a normal situation, where each user in the database has a different key. Comparing Figs. 7 and 9, it is evident that individual users are more distinct from one another when they have different keys.

To evaluate the proposed method more comprehensively, we also conducted testing over the full dataset of FVC2002 DB2, which contains 100 fingers with eight impression images per

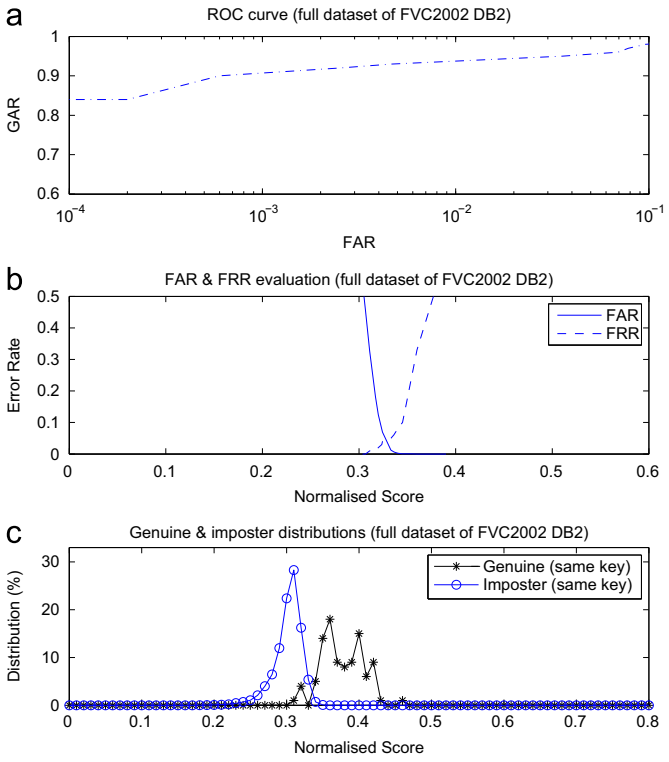

Fig. 8. Evaluation of the proposed method over the full set of FVC2002 DB2 under the lost key scenario: (a) ROC curve; (b) FAR and FRR curves, where the intersecting point corresponds to the EER; (c) genuine and impostor distributions.

finger. The ROC, FAR and FRR curves and genuine and impostor distributions, when all users have the same key, are provided in Fig. 8. The EER in this case is 5% (see Table 1), which is slightly higher than the EER of 4% when using two better quality images of each finger.

4.2. Revocability

Any cancelable fingerprint template scheme requires that when a template is compromised, it is discarded and a new template can be issued by changing the underlying transform. In addition, the new template should be uncorrelated to the compromised template although it is actually derived from the same fingerprint. The revocability test measures how different the reissued template is compared to the old one.

Testing was performed over FVC2002 DB2 by transforming fingerprints in the template set using different keys and then matching the transformed templates against existing ones. We generated 100 transformed templates per fingerprint in the template set. The pseudo-impostor distribution is shown in Fig. 9 and is very similar to the impostor distribution with users having different keys. The mean and standard derivation of the pseudo-impostor distribution are 0.2897 and 0.0057, respectively, compared with 0.2817 (mean) and 0.0208 (standard derivation) of the impostor distribution. This indicates that although transformed templates are generated from the same fingerprint, they are treated as disparate prints. Therefore, we conclude that using the proposed method, a compromised template can be replaced with a new one and that there is no correlation between them.

4.3. Security analysis

If there are m minutiae in a fingerprint image and $n=15$ bits are used to quantize pair-minutiae vectors V_{ij}, in theory, to construct $\mathbf{V}^{(b)}$ in (6) from $\mathbf{V}$ in (2), assuming that each V_{ij} is unique, there are $\binom{2^{15}}{m(m-1)/2}$ different combinations, which yield ones (1 s) in the corresponding positions in the binary string $\{h_k\}$. It can be easily seen that there are far fewer combinations in reality. Hence, once $\mathbf{V}^{(b)}$ or the associated binary string $\{h_k\}$ is tackled, it is possible to reconstruct $\mathbf{V}$ through brute force attack. Therefore, to protect $\{h_k\}$, or equivalently its DFT output $\boldsymbol{H}$, is vital.

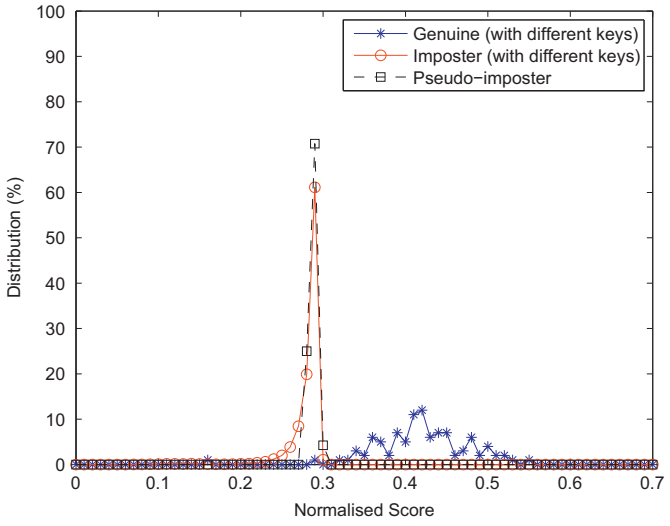

Fig. 9. Genuine, impostor and pseudo-impostor distributions for FVC2002 DB2.

The security of the proposed method is strong and guaranteed by virtue of the DITOM based non-invertible transformation in (8). If a template is compromised, it reveals no clue about $\boldsymbol{H}$. Even in the worst-case scenario where both the stored template $\boldsymbol{T}$ and the parameter key $\mathbf{A}$ are stolen, it would be hard to retrieve the true $\boldsymbol{H}$ among infinite solutions. We indicate that according to [36] (Problem 9, Chapter 2), there exists a matrix $\mathbf{B}$ such that $\overline{\boldsymbol{H}} = \arg\ \min_{\boldsymbol{H}} \|\mathbf{B}\boldsymbol{H}-\boldsymbol{T}\|_2^2$ subject to $\|\mathbf{A}\boldsymbol{H}-\boldsymbol{T}\|_2^2 = 0$. To find $\overline{\boldsymbol{H}}$ however, $(\lambda\mathbf{A}^T\mathbf{A}+\mathbf{B}^T\mathbf{B})^{-1}$ has to exist for all $\lambda > 0$. This is non-trivial. $\overline{\boldsymbol{H}}$ obtained as such may be similar to $\boldsymbol{H}$ but not identical.

When $\boldsymbol{H}$ is secure, the attacker has no way to find out quantized pair-minutiae vectors $V_{ij}^{(b)}$ in (6), so that the essential information about raw minutiae is invulnerable. This contrasts with the security weakness in [11–13], as in these methods, the quantized minutiae locations are revealed if the permutation function is compromised, which results in narrowing down the candidates of original minutiae pattern.

5. Conclusion

Fingerprint registration can become a very challenging issue in the presence of noise and rotation distortion [37–39]. Because of obviation of fingerprint alignment, registration-free cancelable fingerprint templates have increasingly gained popularity in the field of biometric protection. Using pair-minutiae vectors, we have developed an effective alignment-free scheme for generating cancelable fingerprint templates. One prominent feature of the proposed scheme is the design of a DITOM based non-invertible transformation. We analyze geometrically the infinite-to-one mapping in our design and how it is brought about by a system of linear equations algebraically. The proposed scheme has strong security in that given both the transformation and the (stored) transformed template, raw fingerprint data cannot be recovered. Evaluation of the proposed scheme over FVC2002 DB1, DB2 and DB3 shows that our method demonstrates better performance than the most recent work of [16] and other methods therein.

The solution space of a system of linear equations is a simple and straightforward form of realizing infinite-to-one mapping. It is foreseen that the proposed scheme can be extended to more complex topological spaces (e.g., manifolds) to implement infinite-to-one mapping. Further work along this direction is underway. It is also interesting to investigate cancelable templates for a multimodal biometric system based on the proposed infinite-to-one mapping.

Acknowledgments

The authors wish to thank Dr Hua Ye of La Trobe University for his assistance with the testing in this research work.

The research is sponsored by ARC projects LP110100602, LP100200538, LP100100404 and DP0985838.

References

[1] D. Maltoni, D. Maio, A.K. Jain, S. Prabhakar, Handbook of Fingerprint Recognition, second ed., Springer, 2009.
[2] N.K. Ratha, J.H. Connell, R.M. Bolle, Biometrics break-ins and band-aids, Pattern Recognition Letters 24 (2003) 2105–2113.
[3] R. Cappelli, D. Lumini, D. Maio, D. Maltoni, Fingerprint image reconstruction from standard templates, IEEE Transactions on Pattern Analysis and Machine Intelligence 29 (9) (2007) 1489–1503.
[4] J. Feng, A. Jain, Fingerprint reconstruction: from minutiae to phase, IEEE Transactions on Pattern Analysis and Machine Intelligence 33 (2) (2011) 209–223.
[5] Y. Wang, J. Hu, Global ridge orientation modeling for partial fingerprint identification, IEEE Transactions on Pattern Analysis and Machine Intelligence 33 (1) (2011) 72–87.
[6] N.K. Ratha, J.H. Connell, R.M. Bolle, Enhancing security and privacy in biometrics-based authentication systems, IBM Systems Journal 40 (3) (2001) 614–634.
[7] R.M. Bolle, J.H. Connell, N.K. Ratha, Biometrics perils and patches, Pattern Recognition 35 (12) (2002) 2727–2738.
[8] 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 (1) (2011) 116–120.
[9] N.K. Ratha, S. Chikkerur, J.H. Connell, R.M. Bolle, Generating cancelable fingerprint templates, IEEE Transactions on Pattern Analysis and Machine Intelligence 29 (4) (2007) 561–572.
[10] Q. Feng, F. Su, A. Cai, Cracking Cancelable Fingerprint Template of Ratha, in: The International Symposium on Computer Science and Computational Technology (ISCSCT'08), 2008, pp. 572–575.
[11] Z. Jin, A. Teoh, T.S. Ong, C. Tee, Generating revocable fingerprint template using minutiae pair representation, in: The Second International Conference on Education Technology and Computer (ICETC), 2010, pp. V5/251–255.
[12] Z. Jin, A. Teoh, T.S. Ong, C. Tee, A revocable fingerprint template for security and privacy preserving, KSII Transactions on Internet and Information Systems 4 (6) (2010) 1327–1341.
[13] C. Lee, J. Kim, Cancelable fingerprint templates using minutiae-based bit-strings, Journal of Network and Computer Applications 33 (3) (2010) 236–246.
[14] K.E. Smith, L. Kahanpaa, P. Kekalainen, W. Traves, An Invitation to Algebraic Geometry, Springer-Verlag Inc., 2000.
[15] Fingerprint Verification Competition 〈http://bias.csr.unibo.it/fvc2002/〉, 2002.
[16] T. Ahmad, J. Hu, S. Wang, Pair-polar coordinate-based cancelable fingerprint templates, Pattern Recognition 44 (10–11) (2011) 2555–2564.
[17] C. Lee, J.-Y. Choi, K.-A. Toh, S. Lee, Alignment-free cancelable fingerprint templates based on local minutiae information, IEEE Transactions on Systems, Man, and Cybernetics, Part B 37 (4) (2007) 980–992.
[18] S.W. Shin, M.-K. Lee, D. Moon, K. Moon, Dictionary attack on functional transform-based cancelable fingerprint templates, ETRI Journal 31 (5) (2009) 628–630.
[19] K. Takahashi, S. Hirata, Generating provably secure cancelable fingerprint templates based on correlation-invariant random filtering, in: IEEE Third International Conference on Biometrics: Theory, Applications, and Systems (BTAS), 2009, pp. 1–6.
[20] H. Yang, X. Jiang, A.C. Kot, Generating secure cancelable fingerprint templates using local and global features, in: Second IEEE International Conference on Computer Science and Information Technology, 2009, pp. 645–649.
[21] S. Chikkerur, N. Ratha, J. Connell, R. Bolle, Generating registration-free cancelable fingerprint templates, in: Second IEEE International Conference on Biometrics: Theory, Applications and Systems, 2008, pp. 1–6.
[22] A.B.J. Teoh, D.C.L. Ngo, A. Goh, Biohashing: two factor authentication featuring fingerprint data and tokenised random number, Pattern Recognition 37 (11) (2004) 2245–2255.
[23] F. Farooq, R. Bolle, J. Tsai-Yang, N. Ratha, Anonymous and revocable fingerprint recognition, in: IEEE Conference on Computer Vision and Pattern Recognition, 2007, pp. 1–7.
[24] Z. Jin, A. Teoh, T.S. Ong, C. Tee, Secure minutiae-based fingerprint templates using random triangle hashing, in: First International Visual Informatics Conference, 2009, pp. 521–531.
[25] A.O. Thomas, N. Ratha, J. Connell, R. Bolle, Comparative analysis of registration based and registration free methods for cancelable fingerprint biometrics, in: 19th International Conference on Pattern Recognition, 2008, pp. 1–4.
[26] E. Kreyszig, Advanced Engineering Mathematics, ninth ed., John Wiley & Sons, 2006.
[27] G.H. Golub, C.F. Van Loan, Matrix Computations, third ed., Johns Hopkins University Press, 1996.
[28] J.G. Proakis, D.G. Manolakis, Digital Signal Processing: Principles, Algorithms, and Applications, third ed., Prentice-Hall Inc, 1996.
[29] A.B.J. Teoh, A. Goh, D.C.L. Ngo, Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs, IEEE Transactions on Pattern Analysis and Machine Intelligence 28 (12) (2006) 1892–1901.
[30] A.B.J. Teoh, C.T. Yuang, Cancelable biometrics realization with multispace random projections, IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics 37 (5) (2007) 1096–1106.
[31] Y. Lee, Y. Chung, K. Moon, Inverse operation and preimage attack on BioHashing, in: IEEE Workshop on Computational Intelligence in Biometrics: Theory, Algorithms, and Applications, 2009, pp. 92–97.
[32] X. Zhou, T. Kalker, On the security of biohashing, in: Proceedings of SPIE-IS&T Electronic Imaging, Media Forensics and Security II, vol. 7541, 2010, 75410Q, 8 pages.
[33] B. Yang, D. Hartung, K. Simoens, C. Busch, Dynamic random projection for biometric template protection, in: IEEE International Conference on Biometrics: Theory Applications and Systems (BTAS), 2010, pp. 1–7.
[34] J.D. Golic, M. Baltatu, Entropy analysis and new constructions of biometric key generation systems, IEEE Transactions on Information Theory 54 (5) (2008) 2026–2040.
[35] Neurotechnology, VeriFinger SDK 〈http://www.neurotechnology.com/megamatcher.html〉.
[36] W.-H. Steeb, Problems and Solutions in Introductory and Advanced Matrix Calculus, World Scientific Publishing Co. Pte. Ltd., 2006.
[37] Y. Wang, J. Hu, D. Philip, A fingerprint orientation model based on 2D Fourier Expansion (FOMFE) and its application to singular-point detection and fingerprint Indexing, Special Issue on Biometrics: Progress and Directions, IEEE Transactions on Pattern Analysis and Machine Intelligence 29 (4) (2007) 573–585.
[38] P. Zhang, J. Hu, C. Li, M. Bennamoun, V. Bhagavatula, A pitfall in fingerprint bio-cryptographic key generation, Computers & Security 30 (5) (2011) 311–319.
[39] Y. Wang, J. Hu, F. Han, Enhanced gradient-based algorithm for the estimation of fingerprint orientation field, Applied Mathematics and Computation 185 (2) (2007) 823–833.

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, University of Melbourne, Australia. Her research areas are biometric security, blind system identification and wireless communications.

Jiankun Hu is a full professor of Cyber Security at the School of Engineering and Information Technology, the University of New South Wales at the Australian Defence Force Academy (UNSW@ADFA), Australia. His major research interest is in computer networking and computer security, especially biometric security. He has been awarded seven Australia Research Council Grants. He served as Security Symposium Co-Chair for IEEE GLOBECOM'08 and IEEE ICC'09. He was Program Co-Chair of the 2008 International Symposium on Computer Science and its Applications. He served and is serving as an Associate Editor of the following journals: Journal of Network and Computer Applications, Elsevier; Journal of Security and Communication Networks, Wiley; and Journal of Wireless Communication and Mobile Computing, Wiley. He is the leading Guest Editor of a 2009 special issue on biometric security for mobile computing, Journal of Security and Communication Networks, Wiley. He received a Bachelor's degree in industrial automation in 1983 from Hunan University, PR China, a PhD degree in engineering in 1993 from the Harbin Institute of Technology, PR China, and a Master's degree for research in computer science and software engineering from Monash University, Australia, in 2000. In 1995 he completed his postdoctoral fellow work in the Department of Electrical and Electronic Engineering, Harbin Shipbuilding College, PR China. He was a research fellow of the Alexander von Humboldt Foundation in the Department of Electrical and Electronic Engineering, Ruhr University, Germany, during 1995–1997. He worked as a research fellow in the Department of Electrical and Electronic Engineering, Delft University of Technology, the Netherlands, in 1997. Before he moved to RMIT University Australia, he was a research fellow in the Department of Electrical and Electronic Engineering, University of Melbourne, Australia.