Pattern Recognition 66 (2017) 295–301

Contents lists available at ScienceDirect

Pattern Recognition

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

Design of Alignment-Free Cancelable Fingerprint Templates with Zoned Minutia Pairs

Song Wang[a], Wencheng Yang[b], 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

Keywords:
Cancelable biometrics
Cancelable fingerprint templates
Alignment-free
Partial discrete Fourier transform
Security

ABSTRACT

Cancelable fingerprint templates effectively protect original fingerprint data by revoking a compromised template and reissuing a new one. Alignment-free cancelable templates require no image pre-alignment and therefore do not suffer from inaccurate singular point detection. In this paper we propose to construct local minutia structures through zoned minutia pairs in the design of alignment-free cancelable fingerprint templates. Because the structures formed by zoned minutia pairs are truly local, they are more discriminating, which benefits fingerprint matching, leading to good recognition performance. We also apply a simple yet effective measure to mitigating the risk of the attack via record multiplicity (ARM). The proposed method features a partial discrete Fourier transform-based non-invertible transformation, which is compact and computationally efficient. The new cancelable templates meet the requirements of diversity, revocability, non-invertibility and performance. Evaluated over four public databases, the proposed alignment-free cancelable fingerprint templates exhibit superior performance with the Equal Error Rate in the lost-token scenario being 0.19% for FVC2002 DB1, 1% for FVC2002 DB2, 4.29% for FVC2002 DB3 and 9.01% for FVC2004 DB2.

1. Introduction

Fingerprint authentication is witnessing rapid growth in identity management globally, from increasing deployment of fingerprint sensors within smartphones to the introduction of fingerprints in visa and border checking processes. Although fingerprint authentication verifies a person's identity with greater level of assurance since it is highly unlikely that two people share the same fingerprint pattern, fingerprint data, stored as a template, is not immune to attacks. Compromising fingerprint templates can have serious privacy and security consequences.

Cancelable fingerprint templates effectively protect original fingerprint data by allowing a compromised template to be revoked and replaced by a new one. This is implemented through a non-invertible transformation to distort fingerprint data intentionally and repeatedly; see e.g., the representative work of Ratha et al. [1], in which three non-invertible transformations (cartesian, polar and surface folding) are proposed.

A biometric template protection scheme, including cancelable biometrics, is required to meet the following requirements [2,3]:

1. Diversity: generation of different transformed templates from the same biometric data.
2. Revocability: cancellation of a compromised template and replacement with a new one based on the same biometric data.
3. Accuracy: preservation of recognition accuracy after transformation.
4. Non-reversibility: infeasibility of reconstructing the original biometric data from the transformed template.

Cancelable fingerprint template design can be classified into registration-based methods and alignment-free methods. Registration-based cancelable fingerprint templates require the estimation of the position and orientation of the singular points (core and delta) and align minutiae with respect to them. However, precise estimation of the core and delta remains a challenge [4]. With no a priori fingerprint image registration, alignment-free cancelable fingerprint templates do not suffer from inaccurate singular point estimation as they rely on local structures to handle the alignment issue. Given that structures formed locally tend to be more resistant to image rotation and translation, alignment-free cancelable fingerprint templates have been intensely studied, evidenced by the amount of literature over the past several years, a sample of which is included

* Corresponding author.
E-mail addresses: song.wang@latrobe.edu.au (S. Wang), W.Yang@adfa.edu.au (W. Yang), J.Hu@adfa.edu.au (J. Hu).

http://dx.doi.org/10.1016/j.patcog.2017.01.019
Received 25 November 2016; Received in revised form 7 January 2017; Accepted 11 January 2017
Available online 15 January 2017
0031-3203/

herein [5–20,25].

In this paper we develop a new method for the design of alignment-free cancelable fingerprint templates. Due to the importance of feature extraction and representation in the overall cancelable template design, we propose a novel idea of zoning minutia pairs in the construction of local minutia structures. Specifically, minutiae are paired up with a reference minutia central to each local zone, the size of which is controllable. Invariant features are then extracted for those zoned minutia pairs. The rationale behind the "zoning" idea is that non-linear distortion tends to have a larger impact on a pair of distant minutiae than close-by minutia pairs. So minutia pairs which are far apart are more likely to cause matching inaccuracy. Because the structures formed by zoned minutia pairs are truly local, they are more discriminating, which is beneficial to fingerprint matching, leading to good recognition performance.

Upon completion of local structure formation, we introduce a simple yet effective measure to alleviate the threat of the attack via record multiplicity (ARM) [26]. The measure is implemented by a modular operation so that despite being derived from the same user, the input vector to the subsequent transformation function is variable for different applications, thus mitigating the risk of the ARM. The non-invertible transformation in the proposed method features a partial discrete Fourier transform (DFT), controlled by a randomly generated index vector. Fingerprint matching is carried out in the transformed domain to avoid the exposure of original features. The proposed alignment-free cancelable fingerprint templates are evaluated over four public databases [29,30] – FVC2002 DB1, DB2 and DB3 and FVC2004 DB2. The experimental results show that the new method performs favorably compared to the existing alignment-free cancelable fingerprint templates.

In summary, the contributions of the proposed alignment-free cancelable fingerprint template design are as follows:

i. The proposed local minutia structure of zoned minutia pairs has strong discriminative power. This is justified by the superior matching performance of the designed alignment-free cancelable fingerprint templates; for example, the Equal Error Rate (EER) of the proposed method in the lost-token scenario is 0.19% for FVC2002 DB1 and 1% for FVC2002 DB2.
ii. The partial DFT is an effective and efficient non-invertible transformation. It is also more compact than some of our previously proposed transformation functions, e.g., [18,25]. The well-known fast Fourier transform (FFT) algorithms [31] can be applied to the computation of the partial DFT.
iii. The proposed method not only increases the difficulty of launching the ARM, but it also fulfills the non-invertibility requirement for cancelable biometrics. In this sense, the security strength of the new method is enhanced.

For cancelable fingerprint template design, feature extraction and non-invertible transformation function design are key factors which can greatly impact matching accuracy. In terms of feature extraction, how to construct good local minutia structures plays a vital role in the design of cancelable biometrics. In the existing study, e.g., [10,13,14,18], some local structures are of large size, which may not be resistant against non-linear distortion. However, in the proposed method the local structure, formed by zoning minutia pairs, constitutes a reasonable size and hence increases its robustness. When it comes to the design of non-invertible transformation functions, some of the existing methods (e.g., [13–16]) use a permutation process, which is invertible. This undoubtedly poses a security threat. By contrast, the partial DFT designed in the proposed scheme is a true non-invertible transformation function. In addition, we take the effective measure to strengthen the functionality of many-to-one mapping so that it is not easy to launch the ARM.

2. Related work

Image pre-alignment (or registration) is a non-trivial process which requires accurate detection of singular points. This is hard to achieve in noisy and rotated fingerprint images [4]. Without global registration, alignment-free cancelable biometrics has attracted substantial research interest from the biometric security community in recent years. Alignment-free cancelable fingerprint templates usually exploit local minutia structures such as pair minutiae and triangles, because these local structures are rotation- and shift-invariant. In the following we review the state-of-the-art alignment-free cancelable fingerprint templates.

One of the early alignment-free cancelable templates was proposed by Chikkerur et al. [5] with a two factor key. They built the cancelable fingerprint templates based on localized, self-aligned texture features. Although several modes of attack were presented in [5], the authors did not discuss how the proposed algorithm deals with the loss of the template and the two factor key. Another early alignment-free cancelable fingerprint template design appeared in [6]. The invariant values in [6] are calculated using the orientations of neighboring regions around each reference minutia. Two changing functions are provided to decide the amount of transformation around each minutia. Unfortunately, the performance of the method [6] deteriorates with poor quality images.

With no a priori image registration, Tulyakov et al. [7] derived a family of symmetric hash functions to secure fingerprint templates. The hash functions are designed based on minutia locations, taking into account accidental shifting of minutiae points in fingerprint scanning. The developed fingerprint hashes are cancelable and demonstrate reasonable performance. Security of the generated templates is strengthened in [8] by combining more hash functions. However, the computational complexity of the improved method increases as well.

Yang et al. [9] proposed a dynamic random projection approach to securing the extracted local minutia feature vectors, called minutiae vicinity. In this method, the random projection matrix is dynamically assembled and the selection of projection vectors is determined by the feature vector itself. Although the matching performance of the proposed algorithm over FVC2002 DB2 is quite good, the testing result is too limited to predict whether the approach would perform well on other public databases.

Motivated by the polar transformation in [1], Ahmad et al. [10] designed alignment-free cancelable fingerprint templates in a polar space. The presented approach makes use of the relative position between each reference minutia and other minutiae in a pair-polar coordinate system. The weakness of the proposed method is its inferior performance over a comparatively poor quality database, FVC2002 DB3.

Das et al. [11] proposed a minimum distance graphs (MDG) based alignment-free fingerprint hashing algorithm. The MDG consists of a set of connected nodes formed by computing the distance between the core and the next nearest minutia and then the distance between the next closest minutia and its predecessor and so on. The MDG hash is further extended to a cancelable template. While the presented method can defend the brute force attack, it relies on accurate detection of the core point.

Yang et al. [12] extracted local structures like Delaunay triangles in the design of alignment-free cancelable templates. For non-invertible transformation, the authors applied a polar transformation similar to that designed by Ratha et al. [1]. The proposed method shows somewhat poor performance over FVC2002 DB1, a database with relatively good quality images.

Binary string (or binary vector) type of alignment-free cancelable templates have become popular because they are simple to represent and save storage. One early work in this direction was accredited to Farooq et al. [13], where a triangle-based feature vector is established. A bit-string cancelable template is formed through quantization and

bin shuffling. The binary string cancelable template designed by Lee and Kim [14] is derived from a three-dimensional array, which is used to represent pair minutiae feature vectors. Jin et al. [15] developed cancelable bit-string templates using polar grid based 3-tuple quantization. Wong et al. [16] applied the multi-line code (MLC), a string-based minutia descriptor, to the design of cancelable templates in the form of binary codes. Based on minutia vicinity decomposition, Jin et al. [17] proposed the graph-based Hamming embedding technique to generate binary string cancelable templates.

To make bit-string templates more secure, a number of non-invertible transformation functions are studied. These include an infinite-to-one mapping approach [18], the curtailed circular convolution in [19], a blind system identification[1] approach [20] and more recently, a partial Hadamard transform [25]. Despite these methods showing continual improvement in recognition performance, some of them are vulnable to the ARM (attack via record multiplicity) [26].

3. Proposed scheme

In this section we present the design of alignment-free cancelable fingerprint templates using zoned minutia pairs. Cancelable fingerprint templates that are developed using global features usually depend on singular points for image pre-alignment or registration. The performance of these cancelable templates is likely to be affected by inaccurate singular point detection. To circumvent fingerprint registration, the proposed scheme only uses local minutia structures and is therefore alignment-free. Another advantage of local minutia structures is that they are robust to elastic distortion, which is unavoidable in the fingerprint acquisition process. The local minutia structure in the proposed scheme is featured by zoning minutia pairs with respect to each reference minutia. The proposed scheme is made up of the following three processes:

1. Extraction and representation of zoned minutia pairs
2. A partial DFT-based non-invertible transformation
3. Fingerprint matching in the transformed domain

3.1. Extraction and representation of zoned minutia pairs

Suppose minutiae 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 predefined threshold. We denote the set of the selected minutiae by

$$\boldsymbol{M} = \{m_i\}_{i=1}^{N} \text{ with } m_i = (x_i, y_i, \theta_i, t_i) \tag{1}$$

where N is the number of minutiae, x_i, y_i are the x, y coordinates of the ith minutia, θ_i is orientation of the ith minutia and t_i is the minutia type. As discussed in [32], local features such as relative distance and angle information between two local minutiae are invariant to global rotation and translation of fingerprints. Our objective is to construct robust features as locally as possible and represent them in a way suitable for subsequent non-invertible transformation. For this purpose, we zone the minutia set $\boldsymbol{M}$ in (1) into multiple local regions by drawing N circles, each with radius r and centered at every minutia in the set $\boldsymbol{M}$. Obviously, some minutiae are present in more than one zone. Within each zone, minutia pairs are formed locally between the central minutia and all other minutiae. These minutia pairs "zoned" locally should be rotation- and translation-invariant.

The construction of the local minutia structure is illustrated in Fig. 1. For the sake of clear presentation, we exhibit one local zone circled in red in Fig. 1. Suppose the central (reference) minutia in a zone is denoted by m_c, for $c = 1, 2\ldots,N$. We pair up all other minutiae in the zone with m_c. If the zone centered at m_c encloses P_c minutiae, for $\forall\ c \in [1, N]$, then there is a total of $P_c - 1$ minutia pairs in the zone and the value of P_c may vary from zone to zone. The invariant features extracted from the zoned minutia pair (m_c, m_i) are expressed by

$$V_{c,i} = (l_{c,i}, \phi_{c,i}, \delta_{c,i}), \quad i = 1, 2, \ldots, P_c - 1 \text{ and } c = 1, 2\ldots,N \tag{2}$$

where

- $l_{c,i}$ is the distance between m_c and m_i,
- $\phi_{c,i}$ is the angle from the orientation of m_c to the line segment connecting m_c and m_i in a counter-clockwise rotation and the range of $\phi_{c,i}$ is between 0 and 2π, and
- $$\delta_{c,i} = \begin{cases} \theta_c - \theta_i, & \theta_c \geq \theta_i \\ 2\pi + \theta_c - \theta_i, & \theta_c < \theta_i \end{cases}$$

To alleviate elastic distortion in the fingerprints, we quantize each term in $V_{c,i}$. Specifically, we choose σ_l, σ_ϕ and σ_δ to be the step sizes for $l_{c,i}$, $\phi_{c,i}$ and $\delta_{c,i}$, respectively. Let us define a cuboid which contains $\overline{S}$ cubicles, where $\overline{S} = L \times \Phi \times \Theta$ with $L = \lfloor r/\sigma_l \rfloor$, $\Phi = \lfloor 2\pi/\sigma_\phi \rfloor$ and $\Theta = \lfloor 2\pi/\sigma_\delta \rfloor$. Then for $1 \leq i \leq P_c - 1$, $V_{c,i}$ after quantization should match the cubicle whose location in the cuboid is $(\lfloor l_{c,i}/\sigma_l \rfloor, \lfloor \phi_{c,i}/\sigma_\phi \rfloor, \lfloor \delta_{c,i}/\sigma_\delta \rfloor)$. Accordingly, this cubicle is assigned the value of 1. For the cubicles with no $V_{c,i}$ corresponding to them, they are given the value of 0.

Concatenating the 1 s and 0 s assigned to all cubicles in the cuboid yields a binary string $\{\overline{b}_c(j)\}_{j=0}^{\overline{S}-1}$, where $\overline{S}$ is the total number of cubicles in the cuboid. To achieve many-to-one mapping, we apply the modulo operation to the index j of the binary string $\{\overline{b}_c(j)\}$, i.e., $j \bmod S$, with S being a positive integer and $S < \overline{S}$. We then map the elements of $\{\overline{b}_c(j)\}$ to a new (shortened) binary string $\{b_c(k)\}$ as follows:

$$b_c(k) = \overline{b}_c(j), \quad k = j \bmod S, \quad j = 0, 1, \ldots, \overline{S} - 1 \tag{3}$$

Hence, for each reference minutia m_c, $c = 1, 2, \cdots N$ with N being the total number of minutiae in the fingerprint image, we can produce the binary string $\{b_c(k)\}_{k=0}^{S-1}$ from the invariant features of $V_{c,i}$ in (2). Stacking up the elements of this binary string, we obtain the following binary vector:

$$\mathbf{b}_c = [b_c(0),\ b_c(1),\ \ldots,\ b_c(S-1)]^T \tag{4}$$

Remarks:

1. The parameter S in (3) is user- and application-specific, which means that it can be set to different values for different applications. By varying the value of S, the binary vector $\mathbf{b}_c$ in (4) can be made different for the same user in different applications even though these binary vectors are derived from the same features. This makes the ARM (attack via record multiplicity) [26] difficult; refer to more details in Security Analysis (Section 4.3).
2. Since the modular arithmetic has the effect of "wrapping around", for $b_c(p) = 1$, $0 \leq p \leq S - 1$, in the binary vector $\mathbf{b}_c$, the 1 s are likely to be attributed to either $\overline{b}_c(p) = 1$ or being wrapped around by the modulo operation or both. Such uncertainty that exists in $\mathbf{b}_c$ is a desirable consequence to have because it creates a many-to-one mapping from $\{\overline{b}_c(j)\}_{j=0}^{\overline{S}-1}$ to $\{b_c(k)\}_{k=0}^{S-1}$. Although the binary vector $\mathbf{b}_c$ is equipped with a certain degree of security, it contains information about minutia pairs and thus needs further protection, which is accomplished by the non-invertible transformation in the next section.

3.2. A partial DFT-based non-invertible transformation

Linear models have been used in the design of non-invertible transformation in biometric template protection and have found successful applications in other fields, e.g., [27,28]. In this section we

[1] Blind system identification is a digital signal processing-based technique, see e.g., [21–24].

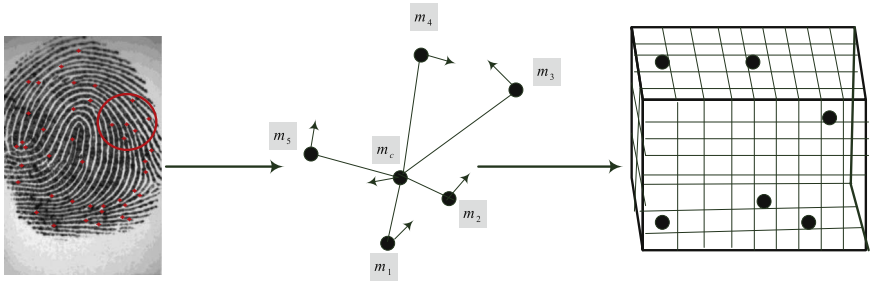

Fig. 1. Local minutia structure. Left: one local zone circled in red. Middle: minutia pairs constructed for the zone shown by the red circle. Right: quantized minutia pairs matched to corresponding bins in a cuboid. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

present a partial DFT-based non-invertible transformation to protect the binary vector $\mathbf{b}_c$ in (4). The proposed transformation builds upon a partial DFT matrix and makes use of the DFT matrix's characteristics (for example, orthogonality of two distinct rows) and computational advantage, thanks to the efficient FFT algorithms [31].

It is well known that the S-point DFT of $\mathbf{b}_c$ is given by

$$\mathbf{f}_c = \boldsymbol{W}\mathbf{b}_c \tag{5}$$

where

$$\mathbf{f}_c = [f_c(1),\ f_c(2),\ \ldots,\ f_c(S)]^T \tag{6}$$

and the DFT matrix $\boldsymbol{W}$ is expressed as

$$\boldsymbol{W} = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & W & W^2 & \cdots & W^{S-1} \\ 1 & W^2 & W^4 & \cdots & W^{2(S-1)} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & W^{S-1} & W^{2(S-1)} & \cdots & W^{(S-1)(S-1)} \end{bmatrix} \tag{7}$$

with $W = e^{-j2\pi/S}$. Since the DFT matrix $\boldsymbol{W}$ is unitary, the DFT operation in (5) is invertible and hence cannot be used to protect $\mathbf{b}_c$. However, the DFT matrix $\boldsymbol{W}$ has some nice properties. For example, any two distinct rows of it are linearly independent and orthogonal. Thus, if we choose R rows of $\boldsymbol{W}$ to form a submatrix, named $\boldsymbol{V}$, then such a partial DFT matrix $\boldsymbol{V}$ is a column rank-deficient matrix.

The formation of $\boldsymbol{V}$ is controlled by a randomly generated vector $\mathbf{P}$, defined below:

$$\boldsymbol{p} = [p_1,\ p_2,\ \ldots,\ p_R] \tag{8}$$

where $p_i \neq p_j$ for all $i \neq j$ and all elements of $\boldsymbol{p}$ are positive integers. As the vector $\boldsymbol{p}$ is generated at random, it serves as a parameter key in the proposed cancelable templates and is used to produce $\boldsymbol{V}$ from the DFT matrix $\boldsymbol{W}$. Specifically, the ith row of $\boldsymbol{V}$ is the p_ith row of $\boldsymbol{W}$, for $i = 1, 2, \ldots, R$ and $R < S$. The matrix $\boldsymbol{V}$ is of size $R \times S$. We then take the following partial DFT:

$$\mathbf{h}_c = \boldsymbol{V}\mathbf{b}_c \tag{9}$$

to obtain a complex vector $\mathbf{h}_c$ of length R.

Since the partial DFT in (9) is built upon the DFT (5), it is not hard to observe the relationship between $\mathbf{h}_c$ and $\mathbf{f}_c$ in (6), i.e.,

$$\mathbf{h}_c = [f_c(p_1),\ f_c(p_2),\ \ldots,\ f_c(p_R)]^T$$

It goes without saying that powerful FFT techniques [31] can be exploited to implement the DFT. The partial DFT in (9) gives rise to an underdermined system, which has non-unique solutions of many possibilities with the true solution $\mathbf{b}_c$ embedded in them. In other words, the partial DFT in (9) is a non-invertible transformation; see detailed analysis in Section 4.3 (Security Analysis)

In addition, the formation of the partial DFT matrix $\boldsymbol{V}$ is parameter-controlled. Changing the parameter key $\boldsymbol{p}$ in (8) yields a different $\boldsymbol{V}$, which further leads to a different $\mathbf{h}_c$. That is, the complex vector $\mathbf{h}_c$ is revocable. Therefore, $\mathbf{h}_c$ is taken as the resultant cancelable template of the zone centered at minutia m_c, for $c = 1, 2, \ldots, N$. As minutia pairs are constructed in a total of N zones and each zone produces one $\mathbf{h}_c$, the proposed method ends up with altogether N such complex vectors, each of which is of length R.

3.3. Fingerprint matching in the transformed domain

Fingerprint matching for cancelable biometrics is performed in the transformed domain to protect original features. So a query fingerprint goes through the same feature extraction and transformation procedures as the template fingerprint. That is, the zoned minutia pairs are first constructed through (2), followed by quantization and modulo operation (3). Then the partial DFT (9) is applied to the binary vector. For clarity, in the notation below we use letters 't' and 'q' as subscript to distinguish between 'template' and 'query'.

Suppose that there are N_q zones in the query as opposed to N_t zones in the template. It is possible that $N_t \neq N_q$ as the total number of minutiae in the query might not be equal to the total number of minutiae in the template. We apply the same feature extraction and representation process to the query fingerprint such that minutia pairs in each zone are formed and quantized, followed by the modulo operation to add uncertainty to the non-transformed binary string. After this feature extraction and representation process, we get the binary vector $\mathbf{b}_{c_q}$, for $c_q = 1, 2, \ldots, N_q$. Then the partial DFT (9) is performed to obtain the complex vector $\mathbf{h}_{c_q}$ for the query.

The similarity score between $\mathbf{h}_{c_t}$ for the template and $\mathbf{h}_{c_q}$ for the query is expressed by

$$S(\mathbf{h}_{c_t}, \mathbf{h}_{c_q}) = 1 - \frac{\| \mathbf{h}_{c_t} - \mathbf{h}_{c_q} \|_2}{\| \mathbf{h}_{c_t} \|_2 + \| \mathbf{h}_{c_q} \|_2} \tag{10}$$

where $\|\cdot\|_2$ denotes the 2-norm [33]. The similarity score $S(\mathbf{h}_{c_t}, \mathbf{h}_{c_q})$ ranges from 0 to 1. The value of $S(\mathbf{h}_{c_t}, \mathbf{h}_{c_q})$ indicates the degree of similarity between the minutia pairs from one zone in the query and one zone in the template. The larger the value of $S(\mathbf{h}_{c_t}, \mathbf{h}_{c_q})$, the more similar the minutia pairs from the zone in the query and those from the zone in the template and vice versa.

As the proposed method is alignment-free, in order to match all zoned minutia pairs in the query and template images, each $\mathbf{h}_{c_q}$ from the query, for $1 \le c_q \le N_q$, has to be compared with each $\mathbf{h}_{c_t}$ from the template, for $1 \le c_t \le N_t$. This zone-to-zone matching using (10) ends up with a score matrix of size $N_t \times N_q$. We choose the maximum value $S_{\max}(\mathbf{h}_{c_t}, \mathbf{h}_{c_q})$ from the score matrix to be the matching score between the template and the query. The template and query images are considered a match if $S_{\max}(\mathbf{h}_{c_t}, \mathbf{h}_{c_q})$ is greater than a pre-defined threshold.

4. Experimental results and analysis

We carried out extensive testing to evaluate the proposed cancelable fingerprint template design over the public databases FVC2002 DB1-DB3 [29] and FVC2004 DB2 [30]. Each of the four databases chosen contains 100 fingers with eight impressions per finger. Quality of fingerprint images in these databases can be vastly different, varying from reasonably good quality to very low quality. Details of each

Table 1
Information about the databases used in our experiments.

Database	FVC2002 DB1	FVC2002 DB2	FVC2002 DB3	FVC2004 DB2
No. of fingers	100	100	100	100
No. of images per finger	8	8	8	8
Resolution	500 dpi	569 dpi	500 dpi	500 dpi
Sensor type	Optical	Optical	Capacitive	Optical
Image size	388×374	296×560	300×300	328×364
Image quality	Good – Medium	Medium	Medium – Low	Very low

database are given in Table 1.

To assess whether the proposed method fulfills the requirements of a biometric template protection scheme, we focus on the following area:

- Performance in the lost-key scenario
- Revocability and diversity
- Security analysis

In the experiments we employed the commercial fingerprint recognition software *VeriFinger SDK* [34] to extract minutia points from fingerprint images in the four databases. The performance measures adopted in our experiments were the Equal Error Rate (EER), False Acceptance Rate (FAR) and False Rejection Rate (FRR), which is related to the Genuine Acceptance Rate (GAR) by GAR + FRR = 1. 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. The values of these performance indexes were collected from both genuine testing and imposter testing. In genuine testing the first impression image of each finger was compared with the second impression image of the same finger, while in imposter testing the first impression image of each finger was matched against the second impression of all other different fingers. For each database, there were 100 genuine testing scores and 4950(=(100 × 99)/2) imposter testing scores. Table 2 lists some parameter settings we used in the experiments. In addition, the parameter key $\boldsymbol{p}$ in (8) was randomly generated.

4.1. Performance in the lost-key scenario

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 users in the dataset. Both genuine and impostor testing were conducted under this same key setting. The Receiver Operating Characteristic (ROC) under the lost-key scenario for each database is plotted in Fig. 2. The variations of the ROC indicate the matching performance of the

Table 2
Parameter settings in the experiments.

Parameters set for feature extraction and the partial DFT	Value range
l_{ci}	[10, 300] pixels
ϕ_{ci}, δ_{ci}	[0, 360°)
σ_l	[15, 25] pixels
σ_ϕ, σ_δ	[15°, 40°]
S	[2^{14}, 20000]
R	[300,2000]

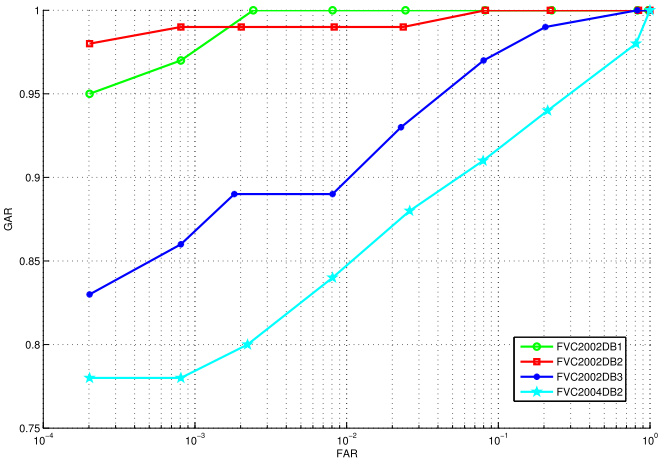

Fig. 2. ROC curves for FVC2002 DB1, DB2, DB3 and FVC2004 DB2 in the lost-key scenario.

proposed approach over different databases. It is shown in Fig. 2 that the performance of our method that goes from highest to lowest over the four databases is in this order: FVC2002 DB1, FVC2002 DB2, FVC2002 DB3 and FVC2004 DB2. This comes as no surprise since FVC2004 DB2 has the lowest quality images among the four databases, while the image quality of FVC2002 DB1 is high.

The EER results of the proposed method in the lost-key scenario are 0.19% for FVC2002 DB1, 1.0% for FVC2002 DB2, 4.29% for FVC2002 DB3 and 9.01% for FVC2004 DB2, respectively. The length of the parameter key $\boldsymbol{p}$ in (8) was set to 300. These EER results agree with the image quality of respective databases with FVC2004 DB2 fetching the worst EER performance. This is due to the poorest image quality of FVC2004 DB2 among the four databases as for FVC2004 DB2, during fingerprint acquisition, the individuals were requested to deliberately distort their fingerprints [30]. To identify whether the high EER for FVC2004 DB2 is caused by the partial DFT-based non-invertible transformation, we tested the EER of this dataset without applying the partial DFT, and it turned out that the EER of the non-transformed feature vector is also 9.01%, which is the same as the EER after transformation. This means that matching performance is not worsened by the proposed non-invertible transformation function. The EER comparison of the proposed method with the existing alignment-free cancelable fingerprint template design is reported in Table 3. It is clearly seen from Table 3 that the proposed method shows competitive performance compared to the state of the art.

The partial DFT in (9) is governed by the randomly generated parameter key $\boldsymbol{p}$ in (8). In theory, the key length R affects the matching performance. When R is larger, the partial DFT matrix $\boldsymbol{V}$ is formed with more rows. This should result in better matching performance but

Table 3
Equal Error Rate (in percentage) comparison under the lost-token scenario.

Alignment-free cancelable template design methods	FVC2002 DB1	FVC2002 DB2	FVC2002 DB3	FVC2004 DB2
Tulyakov et al. [7]	3	–	–	–
Kumar et al. [8]	–	4.98	–	–
Ahmad et al. [10]	9	6	27	–
Jin et al. [15]	5.19	5.65	–	11.64
Das et al. [11]	2.27	3.79	–	–
Wang and Hu [18]	3.5	4	7.5	–
Wong et al. [16]	1.97	2.54	–	9.2
Yang et al. [12]	5.93	4	–	–
Jin et al. [17]	4.36	1.77	–	21.82
Wang and Hu [19]	2	2.3	6.12	–
Wang and Hu [20]	3	2	7	–
Wang et al. [25]	1	2	5.2	13.3
Proposed method	0.19	1	4.29	9.01

Table 4
EER comparison with different key lengths in the lost-token scenario.

Database	Key length R	EER (%)
FVC2002 DB1	300	0.19
	1000	0.12
FVC2002 DB2	300	1
	1000	1
FVC2002 DB3	300	4.29
	1000	3.99
FVC2004 DB2	300	9.01
	2000	9.01

poorer security since more information of $\mathbf{b}_c$ is kept; see (9). In contrast, with R smaller, while recognition accuracy is lower, the resultant cancelable template is more secure. Table 4 illustrates the effect of different key lengths on the EER. It is observed from Table 4 that the EER of the designed cancelable templates does not increase much with a decrease in the value of R; the EER for FVC2002 DB2 and FVC2004 DB2 does not deteriorate when R decreases. This shows that the matching performance of the proposed method is quite robust.

4.2. Revocability and diversity

Revocability is an essential property for cancelable biometrics. It requires that if a stored template is compromised, a new template can be issued to replace the compromised template, and that there should be no correlation between the new template and the compromised one although they are generated from the same biometric data. Diversity is related to revocability. Diversity requires that multiple differently transformed templates that are generated from the same user should not match as if they come from different users.

Revocability and diversity tests measure how different the re-issued templates are compared to the old one and whether transformed templates that originate from the same fingerprint are correlated. We generated 50 transformed templates from the first impression of each finger in FVC2002 DB2 using different parameter keys. These pseudo-imposter templates were compared against the original ones. We plot in Fig. 3 the pseudo-imposter distribution in comparison with the imposter distribution when each user in the database has a different key. It can be seen that the pseudo-imposter distribution is very similar to the imposter distribution. The mean and standard derivation of the pseudo-imposter distribution are 0.1539 and 0.0163, respectively, compared with 0.1498 (mean) and 0.0161 (standard derivation) of the imposter distribution. The results evince that new transformed templates are unrelated to the compromised template and are also different to one another, although they are generated from the same fingerprint.

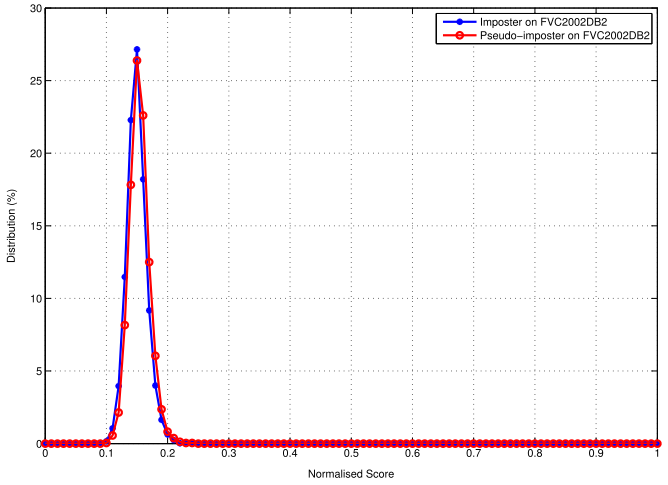

Fig. 3. Pseudo-imposter and imposter distributions for FVC2002 DB2.

4.3. Security analysis

From the development of our cancelable templates, it is clear that the zoned minutia pairs $V_{c,i}$ in (2) must be protected as they contain original fingerprint data. To secure $V_{c,i}$, we need to ensure the safety of the binary string $\{\bar{b}_c(j)\}_{j=0}^{\bar{S}-1}$, in which the 1 s correspond to quantized $V_{c,i}$. To achieve this, the proposed method offers a two-layered protection.

The first layer of protection is provided by cutting down the length of $\{\bar{b}_c(j)\}_{j=0}^{\bar{S}-1}$ through the modular arithmetic (3), thus adding uncertainty to the length-shortened binary string $\{b_c(k)\}_{j=0}^{S-1}$. This is because the entries of 1 in $\{b_c(k)\}_{j=0}^{S-1}$ might be due to their original values being 1 or caused by the modular operation or both, as analyzed in Section 3.1. Moreover, this first layer of protection helps to mitigate the risk of the ARM. By changing values of the parameter S, we can vary $\{b_c(k)\}_{j=0}^{S-1}$, or equivalently $\mathbf{b}_c$ in (4), from application to application. With $\mathbf{b}_c$ being the input to the subsequent partial DFT, when $\mathbf{b}_c$ is different in different applications, it will be useless for an adversary to collect multiple copies of the cancelable template $\mathbf{h}_c$ in order to launch the ARM, because the ARM would only work if the same $\mathbf{b}_c$ is applied to all targeted applications.

The second layer of protection that the proposed method puts in place is the partial DFT (9), which brings about an underdetermined system of linear equations. Since the partial DFT matrix $\boldsymbol{V}$ in (9) is of full row rank but column rank-deficient,

$$\text{nullity}(\boldsymbol{V}) = S - \text{rank}(\boldsymbol{V}) = S - R > 0 \tag{11}$$

Any vector of the form $\mathbf{b}_c + \mathbf{g}$ is also a solution to (9) as long as $\mathbf{g}$ belongs to the null space of $\boldsymbol{V}$, and in theory, there are infinitely many choices for $\mathbf{g}$. However, in our case, choices are not infinite but still many. To see this, we analyze the solution to the underdetermined system (9) in terms of the number of basic (or fixed) variables and the number of free variables. As $\text{rank}(\boldsymbol{V}) = R$, there are R fixed variables and $(S - R)$ free variables for (9) and the solution of the system can be expressed as the fixed variables in terms of the free variables. Since only a binary vector, say $\hat{\mathbf{b}}_c$, rather than real- or complex-valued vectors, can qualify for the solution to (9), the $(S - R)$ free variables can take on values of either 0 or 1, resulting in 2^{S-R} possibilities for $\hat{\mathbf{b}}_c$, among which is the true solution $\mathbf{b}_c$. Take for example some of the values we tried in our experiments, e.g., $S = 2^{14}$ and R=800. This gives $2^{S-R} = 2^{15584}$, which shows that it is highly unlikely to successfully find the true solution $\mathbf{b}_c$ among 2^{15584} possible binary-valued solutions, even when both $\mathbf{h}_c$ and $\boldsymbol{V}$ in (9) are known.

5. Conclusion

In this paper we have proposed a new method for the design of alignment-free cancelable fingerprint templates using local minutia structures formed by zoned minutia pairs. Such local structures provide good discriminative strength, as demonstrated by the matching performance with low EER values. The proposed method features a partial DFT-based non-invertible transformation, which is compact and computationally efficient, making the proposed cancelable template design suitable for resource-limited applications, e.g., smartcards and mobile phones. The new method is also able to reduce the risk of the ARM, which is a clear improvement over some existing cancelable fingerprint templates that are vulnerable to the ARM [26]. Evaluation of the proposed scheme over FVC2002 DB1, DB2 and DB3 and FVC2004 DB2 demonstrates that the new method performs better than the state-of-the-art alignment-free cancelable fingerprint tem-

plates.

It is an easy-to-implement idea to zone minutia pairs for constructing local structures in the design of cancelable fingerprint templates. There is a lot of room for refinement. As for future work, we will investigate how to make zoning in a dynamic and adaptive fashion as opposed to only fixed zones in the current design. If minutia pairs are zoned according to minutia distribution and topology, we should be able to dynamically adjust the number of zones and reduce unnecessary presence of minutia pairs in multiple zones, thus further improving recognition efficiency and accuracy. To develop robust cancelable fingerprint templates also requires more work in terms of addressing the issue of the ARM, especially when the design involves dimension reduction. More powerful methods are needed to enable cancelable biometrics to fully combat the ARM.

Acknowledgment

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

References

[1] N.K. Ratha, S. Chikkerur, J.H. Connell, R.M. Bolle, Generating cancelable fingerprint templates, IEEE Trans. Pattern Anal. Mach. Intell. 29 (4) (2007) 561–572.
[2] A.K. Jain, K. Nandakumar, A. Nagar, Biometric template security, EURASIP Journal on Advances in Signal Processing, Special Issue on Advanced Signal Processing and Pattern Recognition Methods for Biometrics. (2008) ArticleID 579416.
[3] D. Maltoni, D. Maio, A.K. Jain, S. Prabhakar, Handbook of Fingerprint Recognition, Springer, 2nd ed., 2009.
[4] 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, Spec. Issue Biom.: Prog. Dir. IEEE Trans. Pattern Anal. Mach. Intell. 29 (4) (2007) 573–585.
[5] S. Chikkerur, N. Ratha, J. Connell, R. Bolle, Generating registration-free cancelable fingerprint templates, in: Proceedings of the 2nd IEEE International Conference on Biometrics: Theory, Applications and Systems, 2008, pp. 1–6.
[6] C. Lee, J.-Y. Choi, K.-A. Toh, S. Lee, Alignment-free cancelable fingerprint templates based on local minutiae information, IEEE Trans. Syst., Man, Cybern., Part B 37 (4) (2007) 980–992.
[7] S. Tulyakov, F. Farooq, P. Mansukhani, V. Govindaraju, Symmetric hash functions for secure fingerprint biometric systems, Pattern Recognit. Lett. 28 (2007) 2427–2436.
[8] G. Kumar, S. Tulyakov, V. Gavindaraju, Combination of symmetric hash functions for secure fingerprint matching, in: Proceedings of the 20th International Conference on Pattern Recognition, 2010, pp. 890–893.
[9] B. Yang, D. Hartung, K. Simoens, C. Busch, Dynamic Random Projection for Biometric Template Protection, in: Proceedings of the 4th IEEE International Conference on Biometrics: Theory Applications and Systems (BTAS), 2010, pp. 1–7.
[10] T. Ahmad, J. Hu, S. Wang, Pair-polar coordinate-based cancelable fingerprint templates, Pattern Recognit. 44 (10–11) (2011) 2555–2564.
[11] P. Das, K. Karthik, B.C. Garai, A robust alignment-free fingerprint hashing algorithm based on minimum distance graphs, Pattern Recognit. 45 (9) (2012) 3373–3388.
[12] W. Yang, J. Hu, S. Wang, J. Yang, Cancelable Fingerprint Templates with Delaunay Triangle-based Local Structures, Cyberspace Safety and Security, Lecture Notes in Computer Science, 8300, 2013 pp. 81–91.
[13] 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.
[14] C. Lee, J. Kim, Cancelable fingerprint templates using minutiae-based bit-strings, J. Netw. Comput. Appl. 33 (3) (2010) 236–246.
[15] Z. Jin, A.B.J. Teoh, T.S. Ong, C. Tee, Fingerprint template protection with minutiae-based bit-string for security and privacy preserving, Expert Syst. Appl. 39 (2012) 6157–6167.
[16] W.J. Wong, A.B.J. Teoh, M.L.D. Wong, Y.H. Kho, Enhanced multi-line code for minutiae-based fingerprint template protection, Pattern Recognit. Lett. 34 (2013) 1221–1229.
[17] Z. Jin, M.H. Lim, A.B.J. Teoh, B.M. Goi, A non-invertible randomized graph-based Hamming embedding for generating cancelable fingerprint template, Pattern Recognit. Lett. 42 (2014) 137–147.
[18] S. Wang, J. Hu, Alignment-free cancelable fingerprint template design: a densely infinite-to-one mapping (DITOM) approach, Pattern Recognit. 45 (12) (2012) 4129–4137.
[19] S. Wang, J. Hu, Design of alignment-free cancelable fingerprint templates via curtailed circular convolution, Pattern Recognit. 47 (3) (2014) 1321–1329.
[20] S. Wang, J. Hu, A blind system identification approach to cancelable fingerprint templates, Pattern Recognit. 54 (1) (2016) 14–22.
[21] S. Wang, J. Manton, D.B.H. Tay, C. Zhang, J.C. Devlin, An FFT based method for blind identification of FIR SIMO channels, IEEE Signal Process. Lett. 14 (2007) 437–440.
[22] S. Wang, J.H. Manton, Blind SIMO channel identification using FFT/IFFT, Signal Process. 88 (12) (2008) 3007–3010.
[23] S. Wang, J. Cao, J. Hu, A frequency domain subspace blind channel estimation method for trailing zero OFDM systems, J. Netw. Comput. Appl. 34 (1) (2011) 116–120.
[24] S. Wang, J. Hu, Blind channel estimation for single-input multiple-output OFDM systems: zero padding based or cyclic prefix based?, Wirel. Commun. Mob. Comput. 13 (2013) 204–210.
[25] S. Wang, G. Deng, J. Hu, A partial hadamard transform approach to the design of cancelable fingerprint templates containing binary biometric representations, Pattern Recognit. 61 (2017) 447–458.
[26] C. Li, J. Hu, Attacks via record multiplicity on cancelable biometrics templates, Concurr. Comput.: Pract. Exp. 26 (8) (2013) 1593–1605.
[27] M. Rezaei, M. Valipour, M. Valipour, Modelling evapotranspiration to increase the accuracy of the estimations based on the climatic parameters, Water Conserv. Sci. Eng. 1 (3) (2016) 197–207.
[28] M. Valipour, M.A.G. Sefidkouhi, M. Raeini, Selecting the best model to estimate potential evapotranspiration with respect to climate change and magnitudes of extreme events, Agric. Water Manag. 180 (Part A) (2017) 50–60.
[29] Fingerprint Verification Competition. http://bias.csr.unibo.it/fvc2002/,2002.
[30] Fingerprint Verification Competition. ⟨http://bias.csr.unibo.it/fvc2004/⟩, 2004.
[31] J.G. Proakis, D.G. Manolakis, Digital Signal Processing: Principles, Algorithms, and Applications, 3rd ed., Prentice-Hall Inc, 1996.
[32] A.K. Jain, K. Nandakumar, A. Nagar, Fingerprint Template Protection: From Theory to Practice, Chapter 8, Security and Privacy in Biometrics, Chapter 8, 2013, pp. 187–214.
[33] G.H. Golub, C.F. Van Loan, Matrix Computations, 3rd ed., Johns Hopkins Univ. Press, 1996.
[34] Neurotechnology, VeriFinger SDK (⟨http://www.neurotechnology.com/megamatcher.html⟩)

Song Wang is a Senior lecturer in the Department of Electronic Engineering, La Trobe University, Australia. She obtained her Ph.D. 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.

Wencheng Yang is a research fellow at UNSW Canberra, Australia. He has obtained his Ph.D. degree in the field of biometrics security from UNSW under the supervision of Prof. Jiankun Hu.

Jiankun Hu is full Professor, School of Engineering and IT, University of New South Wales, Canberra, Australia. He has obtained his B.E. from Hunan University, China in1983; Ph.D. in Control Engineering from the Harbin Institute of Technology, China in1993 and Masters by Research in Computer Science and Software Engineering from Monash University, Australia in 2000. He has worked in the Ruhr University Germany on the prestigious German Alexander von Humboldt Fellowship1995–1996; research fellow in Delft University of the Netherlands 1997–1998, and research fellow in Melbourne University, Australia 19981999. Jiankun's main research interest is in the field of cyber security including Image Processing/Forensics and machine learning 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 including the top venue IEEE Transactions on Information Forensics and Security and served as Security Symposium Chair of IEEE flagship conferences of IEEE ICC and IEEE Globecom. He has obtained 7ARC(Australian Research Council) Grants and has served at the prestigious Panel of Mathematics, Information and Computing Sciences (MIC), ARC ERA(The Excellence in Research for Australia) Evaluation Committee.