Pattern Recognition 44 (2011) 2555–2564

Contents lists available at ScienceDirect

Pattern Recognition

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

Pair-polar coordinate-based cancelable fingerprint templates

Tohari Ahmad [a], Jiankun Hu [b,*], Song Wang [c]

[a] School of Computer Science and Information Technology, RMIT University, VIC 3001, Australia
[b] School of Engineering and Information Technology, UNSW@ADFA, ACT 2600, Australia
[c] School of Engineering and Mathematical Sciences, La Trobe University, VIC 3086, Australia

ARTICLE INFO

Article history:
Received 8 September 2010
Received in revised form
11 February 2011
Accepted 13 March 2011
Available online 24 March 2011

Keywords:
Privacy
Biometrics security
Fingerprint security
Cancelable template

ABSTRACT

Fingerprint-based authentication has been widely implemented, however, security and privacy of fingerprint templates still remain an issue. Some schemes have been proposed to protect fingerprint templates, such as the design of cancelable fingerprint templates. Yet, most of the existing schemes rely on accurate fingerprint image registration, which is very hard to achieve, especially considering the need to avoid storing any information related to the raw fingerprint features. In this paper, a pair-polar coordinate-based template design method is developed which does not need registration. The proposed scheme explores the relative relationship of minutiae in a rotation- and shift-free pair-polar framework. A many-to-one mapping is applied to ensure the non-invertible recovery of raw templates. A random translation parameter is introduced to further distort the minutia distribution. Under various scenarios, the proposed scheme is evaluated using the public databases, FVC2002DB1, FVC2002DB2 and FVC2002DB3. The experiment results show that the new method satisfies the template protection requirements and the performance degradation caused by the transformation is very low.

1. Introduction

Biometry has become a potential authentication tool which can address the inherent weakness of the traditional knowledge-based (e.g. password) and possession-based (e.g. key or token) recognition systems in terms of authenticating genuine users. This is because biometric features are relatively unique and permanent. Furthermore, by using biometric data, users do not have to worry about forgetting the password or losing the token.

There are two steps involved in biometric authentication, namely:

1. Enrollment: the biometric characteristic and/or its related information is extracted and stored in the database as a template.
2. Verification: the biometrics in query are compared with the existing template to measure the degree of similarity.

Unlike knowledge- or possession-based recognition systems, the biometric feature extracted tends to be unstable due to the associated environment and device. This instability can make it hard to distinguish between intrauser variation and interuser similarity.

Another security concern of biometrics is that once biometric data are compromised, the effect will be forever. Indeed, many research findings have proven that biometric information stored in a database may leak biometric features which can be used to reconstruct a biometric image. For example, Ross et al. [1] show that a minutiae template can provide three levels of fingerprint information: orientation field, class or type and friction ridge structure. Feng and Jain [2] present a method to reconstruct the gray scale image through the phase image. They are able to produce the whole fingerprint with few spurious minutiae. In addition, Cappeli et al. [3] reconstruct a fingerprint image based on a standard template. Note though, as shown in [4], it is hard to fool the image-based matching system given minutiae information only. Most recently, Wang and Hu [5] have proposed an effective scheme in reconstructing a full fingerprint from partial fingerprint.

Protecting biometric templates using conventional cryptography such as RSA and DES is problematic. This is because, if biometric authentication is conducted after decryption, then raw biometric features will be revealed. On the other hand, conducting authentication in a transformed domain (i.e. cipher text) is very hard because a small change in the biometric data may result in a totally different transformed template due to the inherent uncertainty of retrieved biometric features. It is infeasible to solve the conflict that exists between the uncertainty of biometrics and the demand for the exactness of cryptography if an encryption scheme is used.

* Corresponding author.
E-mail addresses: tohari.ahmad@rmit.edu.au (T. Ahmad), J.Hu@adfa.edu.au (J. Hu), song.wang@latrobe.edu.au (S. Wang).

0031-3203/$ - see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.patcog.2011.03.015

A cancelable template is a potential solution in addressing the above issues. It aims to project the raw feature template into another domain using a non-invertible parameterized transformation. In case the transformed template is compromised, it cannot be used to recover the raw template. Issuing a different set of parameters can produce another template. However, most cancelable template design schemes require accurate registration, which is difficult to achieve. In this paper, we propose a cancelable fingerprint template design scheme that is rotation- and shift-free, i.e. registration-free, and also non-invertible. The proposed scheme explores the relative relationship of minutiae points in a pair-polar framework. The experiment results show that the proposed scheme performs better than the existing methods and that the performance degradation caused by the transformation is very low.

The rest of this paper is organized as follows. Section 2 discusses the related works. The proposed pair-polar coordinate-based fingerprint template design is presented in Section 3. The experiment results are demonstrated and discussed in Section 4. The conclusion is given in Section 5.

2. Related works

Generally speaking, biometric template protection techniques can be roughly classified into two categories [6,54]: biometric cryptosystem-based techniques and feature transformation-based techniques. The first category deals with bio key binding and bio key generation while the second one deals with the cancelable template and its variation (e.g. salting).

2.1. Biometric cryptosystem

Juels and Wattenberg [7] propose the use of fuzzy commitment scheme which binds the codeword w of an error correcting code (ECC) to a biometric feature vector x. In the verification process, the codeword w' is produced by query feature vector x'. If the distance between w and w' is close, then it is concluded that $x=x'$, which means that the verification is successful. This concept is implemented in [8] in the fingerprint verification process by using spectral representation. Also, Hao et al. [9] implement the same concept in iris biometrics. Here, Hadamard and Reed–Solomon codes are used to differentiate a genuine user from an imposter. In addition, passwords and tokens are also included in the system design.

Linnartz and Tuyls [10] introduce a shielding function which is intended to prevent a verifier from learning the biometric information of the user during or after the authentication process. This is done by using delta-contracting and epsilon-revealing functions.

Juels and Sudan [11] develop a fuzzy vault scheme which hides the key in a polynomial. Biometric representation is projected on this polynomial and chaff points are added to it. In the verification process, a private key is reconstructed from the coefficients of the polynomial. This idea has been applied in many biometric modalities, such as face [12] and iris [13]. Uludag and Jain [14] combine the fuzzy fingerprint vault with helper data that are extracted from the fingerprint automatically. The helper data are generated based on the orientation field information. Nandakumar et al. [15] improve the fuzzy fingerprint vault by implementing a minutiae matcher through decoding and multiple impressions for both verification and enrollment. Xi and Hu [16] make further improvements by using composite feature-based fingerprint.

Dodis et al. [17,18] propose a secure sketch and a fuzzy extractor to derive a key from biometric information. The secure sketch is used for biometric reconstruction while the fuzzy extractor is for generating the key based on the reconstructed template. For the measurement, they use Hamming, set difference and edit distance metrics. Arakala et al. [19] apply this concept in a polar coordinate system by extracting both local and global features. It is argued that the performance of their method is affected by inaccurately detecting the core point in the global features. Some possible issues in secure sketch implementation are analyzed in [20].

2.2. Cancelable template

Ratha et al. [21,22] introduce the concept of cancelable biometric templates, which shows that it only needs to store a transformed template instead of the original one. The transformation can be carried out either in the signal domain or in the feature domain. The features are transformed using a non-invertible function such that it is hard to recover the original template given the transformation and transformed features. In case the stored (transformed) template is compromised, a new template can be generated using different functions (parameters/keys). Therefore, the original biometric data are still safe. Based on fingerprint modality, Ratha et al. [23,24] propose three types of transformation: Cartesian, polar and functional.

Ang et al. [25] perform biometric transformation by dividing the fingerprint image into two spaces. The first space is reflected into the second, while the second is still in the original position. The angle of the reflection line, which is obtained through the core point, is used as the key. Matching is conducted by evaluating the minutiae points in the combined space. To determine the degree of similarity, a matching algorithm [26] is used.

Teoh et al. [27,28] propose BioHashing to protect biometric templates by employing random multispace quantization (RMQ). The RMQ consists of three steps: biometric projection using linear transformation (e.g. principle component analysis (PCA) [29], Fisher discrimination analysis (FDA) [30]), projection into multiple subspaces and quantization. In terms of performance, this approach renders a relatively low error rate. However, it is inapplicable to fingerprint biometrics [31] because fingerprint minutiae position may change in every capture. Kong et al. [32] and Cheung et al. [33] find that the low equal error rate (EER) of [27] is due to an impractical assumption that every user has a secure unique seed which is used to calculate tokenized random number (TRN). It means that the seed has never been compromised which is unrealistic. Nanni and Lumini [34] propose an improved BioHashing by employing random subspace (RS) in order to develop K feature spaces. It has been able to obtain a better result. Overall, the BioHashing concept is more appropriate to implement using image-based features and the singular point as in [27,35].

Yang et al. [36] develop a scheme by utilizing both local and global features of a fingerprint. In this scheme, a circle of a certain radius is drawn where the core point acts as the center of the circle. A pair of minutiae points in the circle are connected with a line, and both points are mapped to the circle in the perpendicular direction. For the local feature definition, they employ triangular properties which include the angle between two minutiae and the angle between two lines connecting two minutiae pairs.

All of the above cancelable template schemes require image registration based on the position of singular points (core or delta).

Chikkerur et al. [37] design registration-free cancelable templates by localizing the representation of texture. This method does not rely on the minutiae representation. Lee et al. [38] propose a scheme by generating invariant values, which are extracted from minutiae using orientation information. This has made their proposed method much dependent on the quality of images. If the image is of poor quality, then the matching

performance may decrease significantly. This type of feature extraction is similar to [39], in which the method of [40] is implemented for matching. The transformation is performed by randomizing the minutiae location controlled by two changing functions: L_{PIN} and Θ_{PIN}, while revocability is achieved by generating a new template using different changing functions. Jin et al. [41] generate a hash vector by employing random triangle hashing. Then, a bit string is produced based on this hash vector. By using the random triangle, the bit string function is computationally hard to reverse, making it a one-way function.

Lee and Kim [31] also use bit strings as cancelable templates, where a three-dimensional array is defined. A minutia point is selected as a reference of other minutiae transformation such that every point acts as a reference of others. The transformation is performed by mapping every minutia into this three-dimensional array. The result shows that this approach works well if every user has a different key. In case the key is compromised, the performance degrades. This is due to image distortion and quantization error. Still using a string-based template, Jin et al. [42] add helper data to enhance the recognition rate and use an external token to make it revocable in case the template is compromised. Furthermore, the token can randomize each user's template, which results in increasing dissimilarity between users. Maiorana et al. [43] propose BioConvolving, a cancelable transform which represents the template as a set of sequences. This approach has been applied to an on-line signature recognition system.

The cancelable fingerprint template schemes proposed in [37,38,41,31,42] are alignment-free, which do not need singular point information. Trade-offs in fingerprint recognition and comparisons between registration-based and registration-free cancelable templates are provided in [44,45], respectively.

Overall, some properties which should be met in designing a biometric template protection scheme can be summarized as follows [46,47]:

- No cross-matching between databases.
- Capable of revoking and reissuing a new secure template from same biometric information.
- Unable to find the original biometric information from a transformed template.
- Maintaining the original performance (e.g. EER). Performance of biometric template protection may not be as good as the original performance (without protection). However, the decrease in performance must be minimized.

3. Proposed scheme

To the best of our knowledge, most of the existing cancelable fingerprint template schemes, either fully or partially, rely on the global features (singular points), which are very hard to detect accurately [24]. As a result, a small change in the singular point coordinate may greatly affect the performance. Most recent investigations have shown that even the routine image rotation transformation process can cause significant singular points deviation and minutiae changes [55,56]. It is even more challenging considering that raw fingerprint features have not been prestored in the template [48].

To address this issue, we propose a scheme that only uses local features, that is, a relative position of a minutia point to other minutiae points in the polar coordinate space. Different from our previous composite feature [16] which is developed for fuzzy vault, in this cancelable template scheme, we design a pair-polar minutiae coordinate system. Here, each minutia point calculates their relative location between one another in a pair-polar coordinate system.

In the proposed scheme, the matching process is performed in the transformed domain so that the original template remains safe in case the transformed template is compromised. In addition, only a set of selected minutiae points are to be processed. The overall operation of the proposed scheme is illustrated in Fig. 1, which is made up of the following three processes:

1. Minutiae point selection.
2. Template generation.
3. Matching.

3.1. Minutiae point selection

The minutiae points generated through feature extraction process can be denoted as

$$\left.\begin{aligned} &B_u \in \psi \\ &B_u = \{(m_i)_u\}_{i=1}^{n} \\ &m_i = (x_i, y_i, \theta_i, t_i) \end{aligned}\right\} \quad (1)$$

where ψ denotes a fingerprint domain space, B_u is a set of minutiae points extracted from a fingerprint image belonging to the user u, m_i is a minutia point, (x,y) is the minutia point coordinate in the Cartesian space, θ is the minutia orientation, n is the total number of minutiae points in B_u and t_i is the minutia

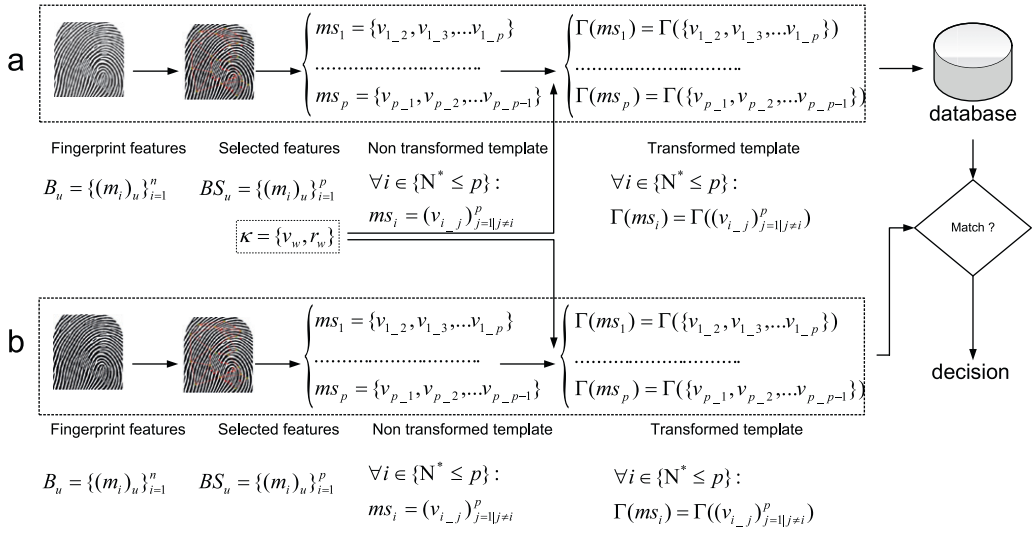

Fig. 1. Pair-polar matching scheme (a) template, (b) query.

type (e.g. ridge ending or bifurcation). Among n minutiae points available in B_u, we select at least k points whose distance is greater than the specified threshold, $thold\_dis_1$. Let BS_u and p be the set of selected minutiae points generated from B_u and the actual total number of points being selected, respectively, and $dis(m_i,m_j)$ be the distance between minutiae points m_i and m_j. Thus, the set of selected minutiae points is written as

$$BS_u = \{(m_i)_u\}_{i=1}^{p}, \quad k \le p \le n \tag{2}$$

In order for a point m_r to be included in BS, it must meet the requirement:

$$dis(\{m_i\}_{i=1}^{r-1}, m_r) > thold\_dis_1, \quad 1 \le r \le p \tag{3}$$

If a fingerprint image fails to generate at least k points, it will be ineligible to be either a template or a query.

Similar to [15] in selecting minutiae points for their fuzzy vault, in this cancelable template scheme we define the distance between points m_i and m_j as

$$dis(m_i,m_j) = t_1 \times \Delta r + t_2 \times \Delta a \tag{4}$$

where $\Delta r = \sqrt{(x_i-x_j)^2+(y_i-y_j)^2}$, $\Delta a = \min(|\theta_i-\theta_j|,(360-|\theta_i-\theta_j|))$, and the parameters are set to be $t_1 = 1$ and $t_2 = 0.2$.

Using this approach, the total number of selected points is between 16 and 49. This has significantly reduced the number of selected points, as most fingerprint images have a total of minutiae points between 70 and 150.

3.2. Template generation

Let m_i and m_j be the minutia point being compared and a neighboring point, respectively, as depicted in Fig. 2a. We define a pair-polar coordinate vector v_{i_j}, which contains the relative location information of m_i to m_j. Here, m_i serves as the center of the coordinate space whose orientation acts as the 0° axis (in a polar space) or the x-axis (in a Cartesian space).

The vector v_{i_j} contains three characteristics:

$$v_{i\_j} = (r_{i\_j}, \alpha_{i\_j}, \beta_{i\_j}) \tag{5}$$

Each of those characteristics can be described as follows:

- r_{i_j}: the radial distance between the center $m_i(0,0)$ and a neighbor point $m_j(x_j,y_j)$ such that

  $$r_{i\_j} = \sqrt{x_j^2+y_j^2}$$

- α_{i_j}: the angle between the center's orientation (x-axis) and the edge r_{i_j} in the counter-clockwise direction such that

  $$\alpha_{i\_j} = \arctan\left(\frac{y_j}{x_j}\right)$$

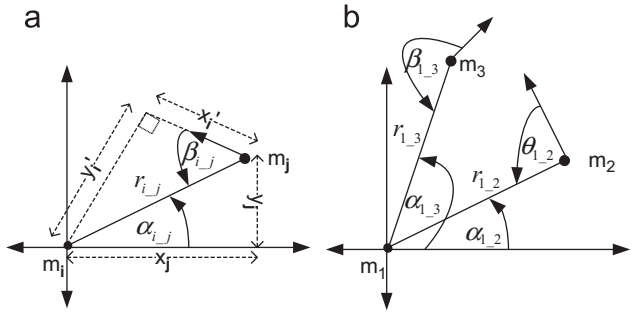

Fig. 2. Pair-polar coordinate (a) vector properties' definition, (b) an example of vector set of points, $ms_1 = \{v_{1\_2}, v_{1\_3}\}$.

- βi_j: the angle between the neighbor's orientation and the edge r_{i_j} in the counter-clockwise direction such that

  $$\beta_{i\_j} = \arctan\left(\frac{y_i'}{x_i'}\right)$$

It follows from this definition that $r_{i\_j} = r_{j\_i}$, $\alpha_{i\_j} = \beta_{j\_i}$ and $\beta_{i\_j} = \alpha_{j\_i}$.

Let ms_i be the set of all pair-polar vectors centered around m_i. The sets of these pre-transformed vectors (in the non-transformed template) in BS can be denoted as

$$\forall i \in \{\mathbb{N}^* \le p\} : ms_i = \{v_{i\_j}\}_{j=1|j\neq i}^{p} \tag{6}$$

Every minutia point selected from the first process (minutiae point selection) has $(p-1)$ vectors. It means that each point in BS has relative location information to other $(p-1)$ points. An example of forming ms_i, as depicted in Fig. 2b, can be described as follows. Let $BS = \{m_1, m_2, m_3\}$ where m_1 is the point being compared, and m_2 and m_3 are m_1's neighboring points. Thus, the point m_1 has a set of vectors defined by $ms_1 = \{v_{1\_2}, v_{1\_3}\}$, where $v_{1\_2} = (r_{1\_2}, \alpha_{1\_2}, \beta_{1\_2})$ and $v_{1\_3} = (r_{1\_3}, \alpha_{1\_3}, \beta_{1\_3})$. By the same token, $ms_2 = \{v_{2\_1}, v_{2\_3}\}$ and $ms_3 = \{v_{3\_1}, v_{3\_2}\}$. So, the pre-transformed template of BS is $\{ms_1, ms_2, ms_3\}$. As BS is actually generated from B, $BS = \{ms_1, ms_2, ms_3\}$ is also the pre-transformed template of B.

The transformation is performed such that the features in the transformed template are different from those in the original template. In order to perform the transformation, similar to [24], we divide the polar coordinate space into some sectors and map each sector to a different position. A random vector, υ_w, is generated to determine where a sector is mapped to. Here, sector mapping is many-to-one so that it is infeasible to find the features in the original sector. Specifically, the points in each sector are mapped based on the random vector υ_w, and a new sector is determined by

$$new\_sect = abs(old\_sect + \upsilon_w) \bmod (total\_sect) \tag{7}$$

where new_sect is the transformed sector number, old_sect is the original sector number and $total\_sect$ is total number of sectors.

Different from [24], we apply the transformation to each set of vectors, $\{ms_i\}_{i=1}^{p}$, because we do not employ the singular point. Moreover, we introduce a transformed-radial factor r_w to the vectors in the randomly chosen sector locations in the transformed domain, such that the new $r_{i\_j} = (r_{i\_j} * r_w) \bmod (\mu)/r_w$. The combination of the random vector υ_w, the transformed-radial factor r_w and modulo μ form the transformation key κ. Hence, for the transformation Γ, the transformed domain is determined by the key $\kappa = \{\upsilon_w, r_w, \mu\}$. To eliminate possible linkage among templates, each vector set $\{ms_i\}_{i=1}^{p}$ is transformed using a different κ.

3.3. Matching

Matching is conducted in the transformed domain, in which only selected points of both the template and the query are processed, as what has been explained in the previous section. It is possible that the template and the query have a different set of selected minutiae points, although they are extracted from exactly the same biometric data. To address this potential problem, we set some threshold values to filter out non-overlapping points.

In general, point matching is performed by comparing each vector in the vector set of each point in the query with the vectors in the vector sets associated with all points in the template. A pair of query and template points is defined as matched if they meet the following requirements:

1. Their difference is smaller than when they are paired to other points.
2. Their difference is smaller than the thresholds.

If the number of pair-matching points is greater than or equal to the specified threshold, then the query is judged as matched to the template.

Unlike [16] in formulating the distance of points, in our matching process, we use neither the primary matching rate nor the conditional matched state. Instead, we apply an additional threshold value. Furthermore, in the transformed domain, we define the neighboring points as all points except the point being compared (the center). So, all points have the same contribution to the matching result regardless of their distance from the center.

The detailed matching process, as illustrated through an example in Fig. 3, can be described by the following steps:

*Step*1: *Construct vector sets for the template and the query*. Let p and p' be the total number of points in the template (BS) and the query (BS'), respectively. Denote m_i a minutia point in the template and $m_{i'}$ a minutia point being compared in the query. The example in Fig. 3 shows that $p=6$, $p'=5$ and $i=i'=1$. The vector sets of m_i and $m_{i'}$ are $ms_1=\{v_{1\_2},v_{1\_3},v_{1\_4},v_{1\_5},v_{1\_6}\}$ and $ms_1'=\{v'_{1\_2},v'_{1\_3},v'_{1\_4},v'_{1\_5}\}$, respectively. In this case, m_1 has five neighboring points while m'_1 has four neighbors.

Step 2: *Vector comparison.* If m_1 and m'_1 are of the same type (i.e. $t_1=t'_1$), then proceed with the vector comparison; otherwise, move to the next minutia point. Each vector in ms'_1 is to be compared with all vectors in ms_1. That is, each v'_{1_k}, where $2\le k\le 5$ is compared with all v_{1_j}, where $2\le j\le 6$, so there are $(p'-1)*(p-1)$ comparisons. The vectors are compared by calculating the differences, as shown below.

Let $\Delta r_{i,k\_i,j},\Delta\alpha_{i,k\_i,j},\Delta\beta_{i,k\_i,j}$ be the differences between two vectors in ms'_i and ms_i, defined as follows:

$$\Delta r_{i,k\_i,j}=\frac{|r'_{i\_k}-r_{i\_j}|}{r_{i\_j}}\times 100\%$$

$$\Delta\alpha_{i,k\_i,j}=\frac{\min(|\alpha'_{i\_k}-\alpha_{i\_j}|,360-|\alpha'_{i\_k}-\alpha_{i\_j}|)}{360}\times 100\%$$

$$\Delta\beta_{i,k\_i,j}=\frac{\min(|\beta'_{i\_k}-\beta_{i\_j}|,360-|\beta'_{i\_k}-\beta_{i\_j}|)}{360}\times 100\%$$

*Step*3: *Find pair-matched vectors, leading to pair-matched minutiae points.* The vector comparison result from the previous step is evaluated for finding pair-matching vectors based on their difference level. The smaller the difference level of two vectors, the more similar they are. Consequently, the possibility for them to be pair-matching vectors is higher.

Specifically, for the vector v'_{i_k} to be matched to v_{i_j}, the difference vector $\Delta v_{i,k\_i,j}=(\Delta r_{i,k\_i,j},\Delta\alpha_{i,k\_i,j},\Delta\beta_{i,k\_i,j})$ has to meet all the following conditions [16]:

$$\left.\begin{aligned}\Delta r_{i,k\_i,j}&<thold\_r_1\\ \Delta\alpha_{i,k\_i,j}&<thold\_\alpha_1\\ \Delta\beta_{i,k\_i,j}&<thold\_\beta_1\end{aligned}\right\}\quad(8)$$

In addition to passing the requirements in (8), the difference vector has to meet the total distance threshold $thold\_dis_2$, such that $\Delta f\le thold\_dis_2$, where

$$\Delta f=(\Delta r\times wgh_r+\Delta\alpha\times wgh_\alpha+\Delta\beta\times wgh_\beta)_{i,k\_i,j}\quad(9)$$

If all the above requirements are met, then the vector v'_{i_k} is judged as "matched" to v_{i_j}. Each vector in ms'_1 can have at most one pair-matched vector in ms_1 and vice versa; therefore, the matching is one-to-one. If there is more than one difference vector satisfying those thresholds, only the one with the least Δf will be chosen. So, in every ms'_i and ms_i comparison, there are at most $\min((p'-1),(p-1))$ pair-matched vectors generated, as illustrated in Fig. 4. In other words, the relation between ms'_i and ms_i is injective but does not have to be bijective.

If the number of pair-matched vectors between ms'_i and ms_i is greater than or equal to the threshold λ, the point m'_i will be judged as "matched" to the point m_i.

The steps 2 and 3 are repeated until all $\{ms'_i\}_{i=1}^{p'}$ and $\{ms_i\}_{i=1}^{p}$ are processed.

Step 4: *Determine if the query is matched to the template.* The previous step gives rise to q pair-matched points between BS' and BS, which may contain duplicate points, as a result of possible many-to-many, one-to-many or many-to-one point matching.

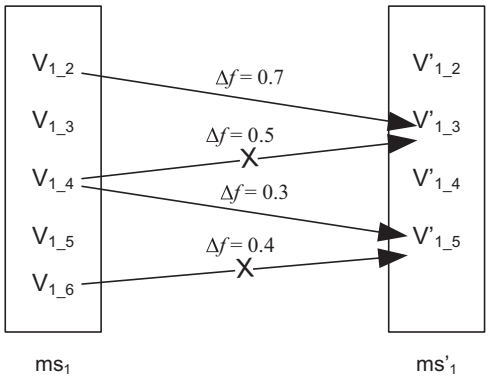

Fig. 4. The pair-matched vectors of ms_1 and ms'_1 are (v_{1_2},v'_{1_3}) and (v_{1_4},v'_{1_5}).

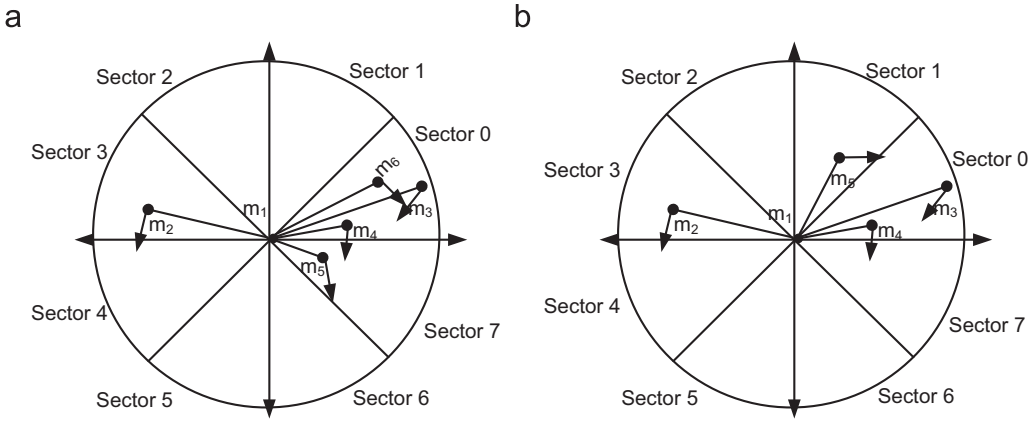

Fig. 3. An example of matching process of two transformed biometric data (a) template, (b) query.

These duplicate points are removed based on the following criteria:

1. The total number of the corresponding pair-matched vectors (in step 3). Only the point with the highest number of pair-matched vectors is selected.
2. The level which the values of Δf fall into. In this case, Δf values for each pair of the q pair-matched points are mapped into an array vector f_v of length L according to a predefined level L for Δf. For example, let a set of Δf be {0.5, 0.7, 1.6, 2.3, 1.2, 3,2}. If the predefined level L is set to 5 (this means f_v should have five elements), then {0.5, 0.7} falls in the first level of L, i.e. [0,1), so we set 2 as the first element in f_v. Similarly, {1.6, 1.2} falls in the second level of L, i.e. [1,2), so we set 2 as the second element in f_v. The third, fourth and fifth elements of f_v are respectively 1,1,0, because {2.3} falls in [2,3), {3.2} falls in [3,4) and no value in the Δf set falls in [4,5). Thus, for the given set of Δf, $f_v = (2,2,1,1,0)$ if we set $L = 5$. The array vector f_v with the highest first element is selected. If there are some array vectors whose first element is same, then the array vector whose second element is the highest is selected, and so on.
3. Average of Δf, where only the point with the least Δf is selected.

The second criterion is applied only if there are more than one point satisfying the first criterion, and the third criterion is applied only if there are more than one point meeting the second criterion. Hence, by this means, we ensure that only those pairs of minutiae points with the highest number of corresponding pair-matched vectors are included. This is analogous to the previous vector matching process in Fig. 4.

If the number of pair-matched points is greater than or equal to the threshold η, the fingerprint query (BS' or B') is judged as matched to the template (BS or B).

Table 1
Parameters used in the experiment.

Threshold	Value
$thold\_r_1$	15
$thold\_\alpha_1$	7.5
$thold\_\beta_1$	7.5
whg_r	1
whg_α	0.2
whg_β	0.2
$thold\_dis_2$	4
λ	6
η	5

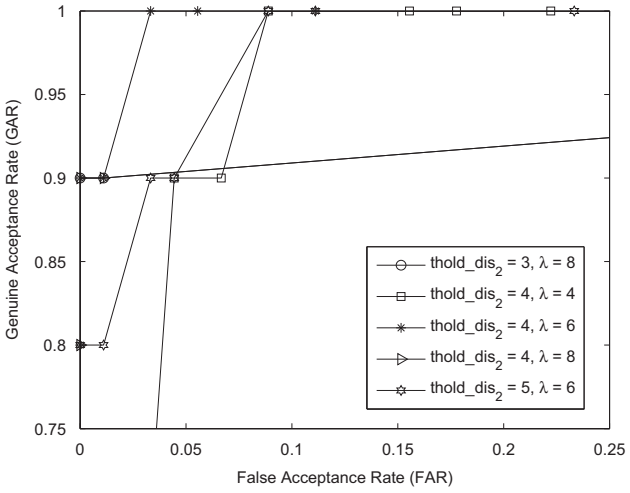

Fig. 5. ROC in the transformed domain of various $thold\_dis_2$,λ combination using small database.

4. Experiment and analysis

The proposed scheme is evaluated in terms of performance, diversity and revocability by measuring the difference (or similarity) level between the template and the query. The security of the proposed method is also analyzed. As in Nandakumar et al. [15], Jain et al. [6], and Xi and Hu [16], it is assumed that users have willingness to provide their biometric data. Under this circumstance, the quality of the biometric data should be relatively good. To test the proposed scheme, we use the public database FVC2002DB2 [49], which contains 100 fingers with each finger having two impression images. The fingerprint images of this database are of various quality. With a similar strategy to [15,6,16], the first and second impression images of the database are used as the template and query, respectively. This leads to 10,000 testing in total, which comprises 100 genuine testing and 9900 imposter testing.

Suppose we group the two impression images in two sets (template and query). For all testing scenarios, the genuine testing is conducted by comparing each image from the second set to its corresponding image in the first set, while the imposter testing is performed by comparing each image from the second set to all images in the first set except its corresponding pair image. In addition, the key κ is randomly generated.

For the purpose of comparison, we also conduct experiments using the databases FVC2002DB1 and FVC2002DB3, both of which have lower quality images with spurious and missing minutiae. This may represent the practical situation where the users do not want to be authenticated or an adversary tries to fool the system by using the incomplete fingerprint of a legitimate user.

The minutiae points are extracted from the databases by using Verifinger 5.0 software [50]. For evaluation, the parameters are empirically set as shown in Table 1. These parameter values are derived from [15,16] and also tuned by running the trial experiment on a smaller database (100 genuine and 90 imposter testing, respectively) for various values of $thold\_dis_2$ and λ in order to find the best combination. Using FVC2002DB2, this genuine testing is conducted by matching the 100 image-pairs while the small imposter testing is performed by randomly selecting 10 out of 100 image-pairs which leads to 90 comparisons. Once the optimal parameter values have been found, the formal testing is performed. The EER of the small database testing is synchronized to that of the bigger database. In addition, the ROC curve of this small database is provided in Fig. 5. We find that ($thold\_dis_2 = 4$, $\lambda = 6$) gives the best performance among all. When the false acceptance rate (FAR) is between 0 and 0.01, the genuine acceptance rate (GAR)=0.90, which is same as the one for ($thold\_dis_2 = 3, \lambda = 8$). The GAR goes up 1, however, the FAR also increases to about 0.03. At this FAR level, all other parameter combination values have a lower GAR level. Hence, we use ($thold\_dis_2 = 4, \lambda = 6$) in the formal testing on FVC2002DB1, FVC2002DB2 and FVC2002DB3.

4.1. Performance

The performance difference between before and after the transformation is compared to measure the amount of degradation. The evaluation is performed such that it represents the worst case in the real world situation (e.g. the key is lost/stolen and the template generated using a new key). Let $\delta(a,a')$ be the difference

level of template a and query a', and Φ be the highest difference level allowed for a and a' to be recognized as "matched".

4.1.1. Lost key attack

In this evaluation, both the genuine user and imposter are tested using the same key, so it is equivalent to the worst case situation where the key is compromised and known by the public. The testing scenarios are constructed for evaluating these conditions:

$$\left.\begin{array}{l}\delta(BS,BS') \le \Phi \\ \delta(\Gamma_1(BS),\Gamma_1(BS')) \le \Phi\end{array}\right\} \quad (10)$$

Using FVC2002DB2, we find that the EER in the transformed and non-transformed domains is 0.06 and 0.05, respectively, as shown in Fig. 6. Hence, the amount of EER difference between before and after the transformation is 0.01. This is better than the result in [25], where the EER difference is about 0.13 (the EER before and after the transformation being 0.04 and 0.168, respectively). The EER of 0.06 is lower than the ones with other parameter settings, as shown in Table 2 whose ROC curve is provided in Fig. 7. The EER of the proposed scheme is lower than that of other fingerprint template protection schemes, as summarized in Table 3. Note that the databases used for evaluation may be different.

For further comparison, the EER of the non-transformed and transformed fingerprint templates of FVC2002DB1 is 0.03 and 0.09, respectively, while the EER of the non-transformed and transformed templates of FVC2002DB3 is 0.16 and 0.27, respectively, which is higher than that of FVC2002DB2. We also find that only a few of minutiae points can be extracted from the images in FVC2002DB1, and even fewer from FVC2002DB3, and that there are 2% of the mated-pair images in FVC2002DB3 whose minutiae points cannot be extracted at all by using Verifinger 5.0 software

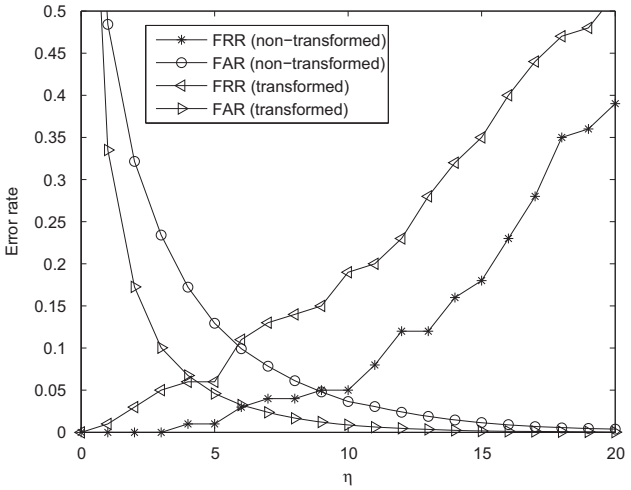

Fig. 6. Equal error rate (EER) in both the transformed and non-transformed domains of FVC2002DB2.

Table 2
EER obtained by varying the parameters.

($thold\_dis_2$,λ)	EER (%)
(2,7)	16
(4,4)	15
(4,6)	6
(4,8)	7.8
(6,7)	8
(6,8)	8

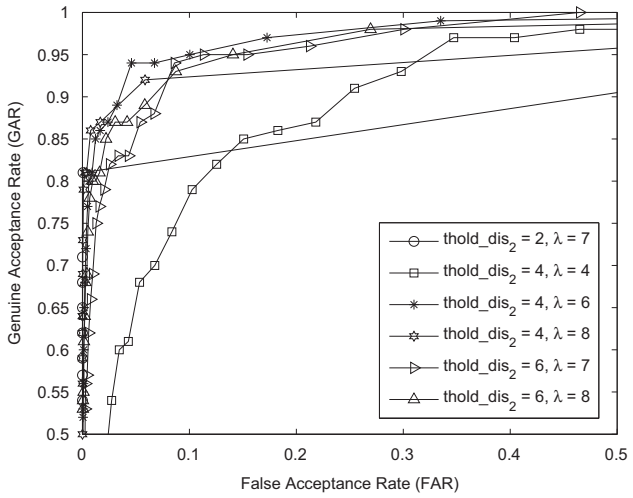

Fig. 7. ROC curve of various parameters.

Table 3
EER comparison of the proposed scheme with some existing fingerprint template protection schemes.

Author	EER (%) per database			
	FVC2002DB1	FVC2002DB2	FVC2002DB3	Other public/ private DB
Yang et al. [36]	–	13	–	–
Sutcu et al. cited in [36]	–	35	–	–
Arakala et al. [19]	–	–	–	15
Ang et al. [25]	–	–	–	16.8
Lee and Kim [31]	–	–	–	6.8; 9.5; 10.3
Jin et al. [41]	–	–	–	>10
Proposed scheme	9	6	27	–

[50]. Given that in the real application, users are likely to be cooperative in providing their fingerprints for authentication [15], the experiment results of FVC2002DB2 are more representative.

4.1.2. Revocability

In case a key is compromised, the template can be revoked and a new key can be issued to generate a new template. This new template must be different enough from the old one even though it is actually derived from the same finger. To evaluate this revocation capability, we perform testing to see if the following requirement is met:

$$\delta(\Gamma_1(BS),\Gamma_2(BS')) > \Phi, \Gamma_1 \neq \Gamma_2\} \quad (11)$$

Testing is performed over FVC2002DB2 by assuming the pseudo-imposter from the query set, that is, the same fingerprint is transformed using various keys and matched to the corresponding transformed template. The results show that all queries are rejected, which means that FAR=0. It also shows that the transformation has made the features to be sufficiently different between each other even though they are derived from the same finger. In other words, they do not replace one another. According to [51,41] this property not only solves the revocability issue but also prevents cross-matching among databases. This means that the same fingerprint can be enrolled in various applications using different keys.

4.1.3. Diversity

In a practical application, each user has a unique key which is different from other users. This is equivalent to the situation where the key is not compromised. To evaluate this situation, we test the following testing scenarios using FVC2002DB2 to check if they hold:

$$\left.\begin{array}{l}\delta(\Gamma_1(BS),\Gamma_2(BS')) > \Phi, \Gamma_1 \neq \Gamma_2 \\ \delta(\Gamma_1(BS),BS') > \Phi\end{array}\right\} \quad (12)$$

Different from the testing in (11), the first testing in (12) is conducted by comparing each fingerprint in the second set (query) with all fingerprints in the first set (template) except its corresponding fingerprint pair.

The second scenario in (12) is to evaluate the effect of the transformation on the original fingerprint. Testing is performed by comparing the transformed template with the non-transformed query derived from both the same and different fingers. The result shows that all queries in (12) are rejected (FAR=0), which means that they are relatively different and cannot replace one another either. This is best suited for a real world situation where each user has a unique key [24,31].

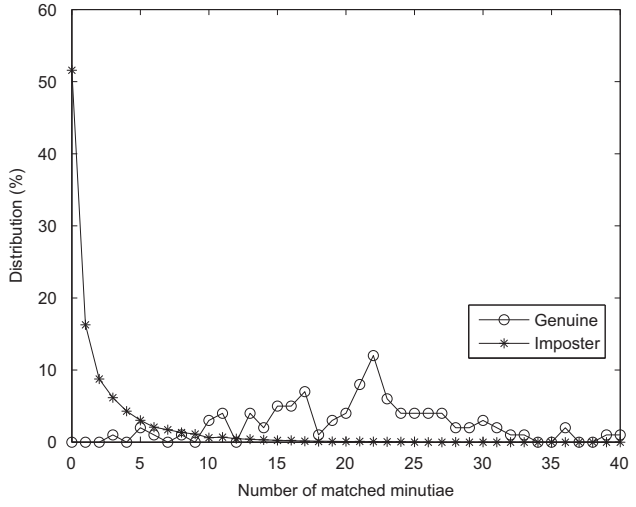

Fig. 8. Distribution of matched non-transformed genuine and imposter.

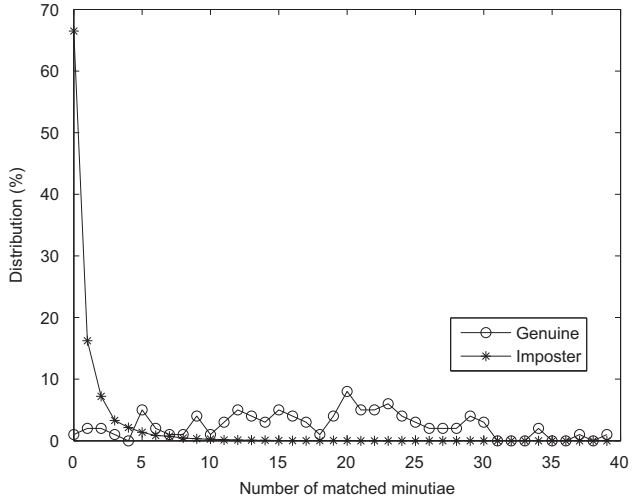

Fig. 9. Distribution of matched transformed genuine and imposter.

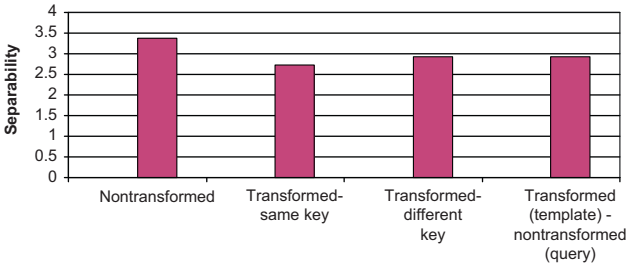

Fig. 10. Separability under various transformations.

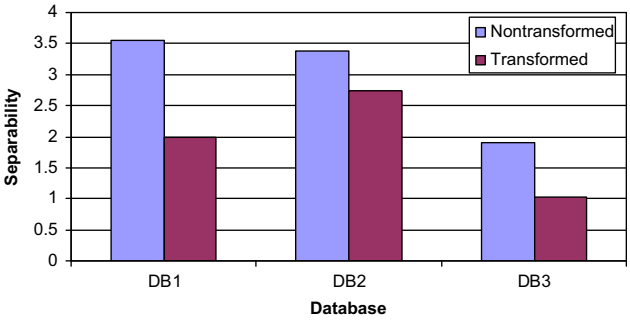

Fig. 11. Separability of both non-transformed and transformed fingerprints from different databases.

To measure the relation between the genuine and imposter distributions, we calculate the separability [38] defined as

$$Separability = \frac{|\mu_G - \mu_i|}{\sqrt{(\sigma_G^2 + \sigma_i^2)/2}} \quad (13)$$

where μ_G, μ_i, σ_G^2 and σ_i^2 are the mean and variance of genuine and imposter distributions, respectively. The distribution of matched minutiae of the non-transformed genuine and imposter is shown in Fig. 8, where separability ≈ 3.37 and EER ≈ 0.05. This separability is higher than that for the distribution of matched minutiae of the transformed genuine and imposter (see Fig. 9), for which separability ≈ 2.73 and EER ≈ 0.06. Separability under various transformation is illustrated in Fig. 10. The experiments on separability are conducted as follows:

1. The genuine and imposter fingerprints are not transformed.
2. The genuine and imposter fingerprints are transformed by using the same key.
3. The genuine and imposter fingerprints are transformed by using the same and different keys, respectively.
4. The genuine fingerprints are transformed by using the same key while the imposter fingerprints are not transformed.

It can be inferred that separability of the transformed fingerprints using the same key is the lowest while separability of the non-transformed fingerprints is the highest. It is also shown that item no. 3 and item no. 4 have an approximately equal separability level, which means that transforming template and query fingerprints using different keys is equivalent to the situation where the template is transformed while the query is not. In addition, their separability is higher than that of the transformed distribution using the same key, but lower than that of the non-transformed (original) distribution.

The separability of both non-transformed and transformed fingerprints from different databases is presented in Fig. 11. It shows that, overall, non-transformed fingerprints have higher separability than that of transformed fingerprints, and that

separability of non-transformed FVC2002DB1 is the highest while FVC2002DB3 has the lowest separability. This is inversely proportional to the EER. For transformed fingerprints, FVC2002DB2's separability is the highest while FVC2002DB3's is the lowest. This is also inversely proportional to the EER.

4.2. Security of the proposed method

In case a template is compromised, the attacker only finds the transformed minutiae version. On the other hand, the templates are transformed using different keys to minimize the possible linkage between them (refer to Section 4.1.3). Therefore, the transformed templates are independent of each other.

Shin et al. [52] and Quan et al. [53] argue that the feature transformation proposed by Ratha et al. [24] is vulnerable, especially the surface folding (functional) transformation. Note that our propose scheme is motivated by the polar transformation instead of surface folding. In Shin et al. [52], a brute force attack is carried out by trying all possible points in the original fingerprint image while Quan et al. [53] present the solving-equation attack. It is worth pointing out that our scheme is fundamentally different to what is proposed in Ratha et al. [24]. The many-to-one mapping used in our method gives rise to so many possibilities/combinations that prevent hackers from finding original minutiae locations. This guarantees the security of the proposed scheme, as analyzed in detail below.

Let S, r_w, μ, m be the total number of sectors, transformed-radial factor, the modulo for randomizing minutia distance (Section 3.2) and the total number of minutiae points, respectively. It follows that each raw minutia has $(S\mu)$ possible locations in the transformed domain. So, there are $(S\mu)^m$ possibilities for m minutiae, or a brute force attack should try at least $(m*\log_2(S\mu))$ attempts. Finally, finding an original minutia location from given transformed templates needs to get r_{i_j} from $r'_{i\_j} = (r_{i\_j} * r_w) \bmod(\mu)/r_w$. This is hard because (i) there are many possible combinations of $(r_{i\_j} * r_w)$, and (ii) the modulo operation being used. However, for the authentication process, as parameters are given, it is straightforward to do sector mapping and scaling, etc.

5. Conclusion

As an appealing alternative to knowledge- and possession-based recognition systems, fingerprint authentication is developing at a fast rate for many applications. Without adequate protection of fingerprint templates, however, it may cause privacy and security issues. As one of the biometric protection methods, cancelable fingerprint template design faces the challenging issue of fingerprint registration. In this paper, a registration-free cancelable template design scheme has been proposed. The new scheme addresses the issues of revocability, non-invertability and multiple template independence. Statistical experiments demonstrate that the proposed scheme performs better when compared with several recently presented methods.

Acknowledgments

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

References

[1] A. Ross, J. Shah, A. Jain, From template to image: reconstructing fingerprints from minutiae points, IEEE Transactions on Pattern Analysis and Machine Intelligence 29 (4) (2007) 544–560.
[2] J. Feng, A. Jain, Fingerprint reconstruction: from minutiae to phase, IEEE Transactions on Pattern Analysis and Machine Intelligence 33 (2) (2011) 209–223.
[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] L. Nanni, A. Lumini, Descriptors for image-based fingerprint matchers, Expert Systems with Applications 39 (10) (2009) 12414–12422.
[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] A. Jain, K. Nandakumar, A. Nagar, Biometric template security, EURASIP Journal on Advances in Signal Processing 2008 (2008) 1–17.
[7] A. Juels, M. Wattenberg, A fuzzy commitment scheme, in: 6th ACM Conference on Computer and Communications Security, 1999, pp. 28–36.
[8] H. Xu, R. Veldhuis, A. Bazen, T. Kevenaar, T. Akkermans, B. Gokberk, Fingerprint verification using spectral minutiae representations, IEEE Transactions on Information Forensics and Security 4 (3) (2009) 397–409.
[9] F. Hao, R. Anderson, J. Daugman, Combining crypto with biometrics effectively, IEEE Transaction on Computers 55 (9) (2006) 1081–1088.
[10] J.-P. Linnartz, P. Tuyls, New shielding functions to enhance privacy and prevent misuse of biometric template, Lecture Notes in Computer Science, vol. 2688, 2003, pp. 393–402.
[11] A. Juels, M. Sudan, A fuzzy vault scheme, Designs, Codes and Cryptography 38 (2) (2006) 237–257.
[12] Y. Feng, P. Yuen, Protecting face biometric data on smartcard with Reed–Solomon code, in: IEEE Conference on Computer Vision and Pattern Recognition Workshop, 2006, p. 29.
[13] Y. Lee, K. Bae, S. Lee, K. Park, J. Kim, Biometric key binding: fuzzy vault based on iris images, 2nd International Conference on Biometrics, Lecture Notes in Computer Science, vol. 4642, 2007, pp. 800–808.
[14] U. Uludag, A. Jain, Securing fingerprint template: fuzzy vault with helper data, in: IEEE Conference on Computer Vision and Pattern Recognition Workshop, 2006, p. 163.
[15] K. Nandakumar, A.K. Jain, S. Pankanti, Fingerprint-based fuzzy vault: implementation and performance, IEEE Transactions on Information Forensics and Security 2 (4) (2007) 744–757.
[16] K. Xi, J. Hu, Biometric mobile template protection: a composite feature based fingerprint fuzzy vault, in: IEEE International Conference on Communications (ICC), 2009, pp. 1–5.
[17] Y. Dodis, L. Reyzin, A. Smith, Fuzzy extractors: how to generate strong keys from biometrics and other noisy data, International Conference on the Theory and Applications of Cryptographic Techniques, Advances in Cryptology (EUROCRYPT'04), Lecture Notes in Computer Science, vol. 3027, 2004, pp. 523–540.
[18] Y. Dodis, R. Ostrovsky, L. Reyzin, A. Smith, Fuzzy extractors: how to generate strong keys from biometrics and other noisy data, Technical Report 235, Cryptology ePrint Archive, 2006.
[19] A. Arakala, J. Jeffers, K.J. Horadam, Fuzzy extractors for minutiae-based fingerprint authentication, ICB 2007, Lecture Notes in Computer Science, vol. 4642, 2007, pp. 760–769.
[20] Y. Sutcu, Q. Li, N. Memon, Protecting biometric templates with sketch: theory and practice, IEEE Transactions on Information Forensics and Security 2 (3 part 2) (2007) 503–512.
[21] 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.
[22] R.M. Bolle, J.H. Connell, N.K. Ratha, Biometric perils and patches, Pattern Recognition 35 (12) (2002) 2727–2738.
[23] N. Ratha, J. Connell, R.M. Bolle, S. Chikkerur, Cancelable biometrics: a case study in fingerprints, 18th International Conference on Pattern Recognition, vol. 4, 2006, pp. 370–373.
[24] 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.
[25] R. Ang, R. Safavi-Naini, L. McAven, Cancelable key-based fingerprint templates, ACISP 2005, Lecture Notes in Computer Science, vol. 3574, 2005, pp. 242–252.
[26] X. Jiang, W. Yau, Fingerprint minutiae matching based on the local and global structures, the 15th International Conference on Pattern Recognition, vol. 2, 2000, pp. 1038–1041.
[27] 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.
[28] 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.
[29] M. Turk, A. Pentland, Eigenfaces for recognition, Journal of Cognitive Neuroscience 3 (1) (1991) 71–86.
[30] P. Belhumeur, J. Hespanha, D. Kriegman, Eigenfaces versus Fisherfaces: recognition using class specific linear projection, IEEE Transactions on Pattern Analysis and Machine Intelligence 19 (7) (1997) 711–720.
[31] C. Lee, J. Kim, Cancelable fingerprint templates using minutiae-based bit-strings, Journal of Network and Computer Applications 33 (3) (2010) 236–246.

[32] A. Kong, K.-H. Cheung, D. Zhang, M. Kamel, J. You, An analyzing of biohashing and its variants, Pattern Recognition 39 (7) (2006) 1359–1368.
[33] K.-H. Cheung, A. Kong, D. Zhang, M. Kamel, J. You, Revealing the secret of facehashing, Advances in Biometrics, Lecture Notes in Computer Science, vol. 3822, 2005, pp. 106–112.
[34] L. Nanni, A. Lumini, Random subspace for an improved biohashing for face authentication, Pattern Recognition Letters 29 (3) (2008) 295–300.
[35] L. Nanni, A. Lumini, A deformation-invariant image-based fingerprint verification system, Neurocomputing 69 (16–18) (2006) 2336–2339.
[36] H. Yang, X. Jiang, A.C. Kot, Generating secure cancelable fingerprint templates using local and global features, in: 2nd IEEE International Conference on Computer Science and Information Technology, 2009, pp. 645–649.
[37] S. Chikkerur, N. Ratha, J. Connell, R. Bolle, Generating registration-free cancelable fingerprint templates, in: 2nd IEEE International Conference on Biometrics: Theory, Applications and Systems, 2008, pp. 1–6.
[38] 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.
[39] S. Yang, I. Verbauwhede, Automatic secure fingerprint verification system based on fuzzy vault scheme, in: IEEE International Conference on Acoustics, Speech, and Signal Processing, 2005, pp. v/609–v/612.
[40] D. Lee, K. Choi, J. Kim, A robust fingerprint matching algorithm using local alignment, in: International Conference on Pattern Recognition, 2002, pp. 803–806.
[41] Z. Jin, A.B.J. Teoh, T.S. Ong, C. Tee, Secure minutiae-based fingerprint templates using random triangle hashing, Lecture Notes in Computer Science, vol. 5857, 2009, pp. 521–531.
[42] Z. Jin, A. Teoh, T.S. Ong, C. Tee, Generating revocable fingerprint template using minutiae pair representation, in: The 2nd International Conference on Education Technology and Computer (ICETC), 2010, pp. V/5251–V/5254.
[43] E. Maiorana, P. Campisi, J. Fierrez, J. Ortega-Garcia, A. Neri, Cancelable templates for sequence-based biometrics with application to on-line signature recognition, IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans 40 (3) (2010) 525–538.
[44] F. Farooq, N. Ratha, J. Tsai-Yang, R. Bolle, Security and accuracy trade-off in anonymous fingerprint recognition, in: Ist IEEE International Conference on Biometrics: Theory, Applications and Systems, 2007, pp. 1–6.
[45] 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. 1–8.
[46] D. Maltoni, D. Maio, A.K. Jain, S. Prabhakar, Handbook of Fingerprint Recognition, Springer, 2003.
[47] T. Kevenaar, Protection of biometric information, in: Security with Noisy Data: Private Biometrics, Secure Key Storage and Anti-Counterfeiting, 2007, pp. 169–193.
[48] 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, IEEE Transactions on Pattern Analysis and Machine Intelligence 29 (4) (2007) 573–585.
[49] FVC2002, Fingerprint verification competition, 2002.
[50] Neurotechnology, Verifinger, version 5.0.
[51] 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.
[52] 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.
[53] F. Quan, S. Fei, C. Anni, Z. Feifei, Cracking cancelable fingerprint template of Ratha, in: International Symposium on Computer Science and Computational Technology, 2008, pp. 572–575.
[54] J. Hu, Mobile fingerprint template protection: progress and open issues, in: Proceedings of the Third IEEE Conference on Industrial Electronics and Applications, 2008, pp. 2133–2138.
[55] P. Zhang, J. Hu, C. Li, M. Bennamoun, V. Bhagavatula, A pitfall in fingerprint bio-cryptographic key generation, Computers & Security, Elsevier, 2011, doi:10.1016/j.cose.2011.02.003.
[56] P. Zhang, C. Li, J. Hu, A pitfall in fingerprint features extraction, in: Proceedings of the 11th International Conference on Control Automation Robotics & Vision (ICARCV), 2010, pp. 13–18.

Tohari Ahmad is a PhD student at the School of Computer Science and Information Technology, RMIT University, Australia. He had been an IT consultant in Accenture (Andersen Consulting) for several years before obtaining Master degree from Monash University, Australia. His research interest is in computer network, computer security and biometric security.

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 six 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.

Song Wang is a senior lecturer at the Department of Electronic Engineering, La Trobe University, Melbourne, Australia. She has obtained her PhD degree from the Electrical and Electronic Department, the University of Melbourne, Australia. Her research interest is in the area of digital signal processing and its application to image processing, wireless communication and biometric security. She has numerous publications in top journals of this field and also serves International Journal Editorial Board.