A Fingerprint and Finger-vein Based Cancelable Multi-biometric System

Article *in* Pattern Recognition · June 2018

DOI: 10.1016/j.patcog.2018.01.026

5 authors, including:

Wencheng Yang
Edith Cowan University
36 PUBLICATIONS **362** CITATIONS
SEE PROFILE

Song Wang
La Trobe University
62 PUBLICATIONS **776** CITATIONS
SEE PROFILE

Jiankun Hu
UNSW Sydney
280 PUBLICATIONS **4,207** CITATIONS
SEE PROFILE

Zheng Guanglou
Edith Cowan University
34 PUBLICATIONS **233** CITATIONS
SEE PROFILE

A Fingerprint and Finger-vein Based Cancelable Multi-biometric System

Wencheng Yang[a,*], Song Wang[b], Jiankun Hu[c], Guanglou Zheng[a], Craig Valli[a]

a. *Security Research Institute, School of Science, Edith Cowan University, WA 6027, Australia*.

b. *School of Engineering and Mathematical Sciences, La Trobe University, VIC 3086,Australia.*

c. *School of Engineering and Information Technology, University of New South Wales at the Australian Defence Force Academy (UNSW@ADFA), Canberra ACT 2600, Australia.*

Abstract: Compared to uni-biometric systems, multi-biometric systems, which fuse multiple biometric features, can improve recognition accuracy and security. However, due to the challenging issues such as feature fusion and biometric template security, there is little research on cancelable multi-biometric systems. In this paper, we propose a fingerprint and finger-vein based cancelable multi-biometric system, which provides template protection and revocability. The proposed multi-biometric system combines the minutia-based fingerprint feature set and image-based finger-vein feature set. We develop a feature-level fusion strategy with three fusion options. Matching performance and security strength using these different fusion options are thoroughly evaluated and analyzed. Moreover, compared with the original partial discrete Fourier transform (P-DFT), security of the proposed multi-biometric system is strengthened, thanks to the enhanced partial discrete Fourier transform (EP-DFT) based non-invertible transformation.

Keywords: cancelable; multi-biometrics; feature level fusion; data type incompatibility

* Corresponding author.
E-mail addresses: w.yang@ecu.edu.au (W. Yang), song.wang@latrobe.edu.au (S. Wang), j.hu@adfa.edu.au (J. Hu), g.zheng@ecu.edu.au (G. Zheng), c.valli@ecu.edu.au (C. Valli).

1. Introduction

Biometrics is the science of recognizing a person based on his/her physiological characteristics or behavioral traits and has shown significant advances in a range of applications, such as access control, authentication, security and surveillance. Compared to traditional authentication, e.g. passwords or tokens, biometric traits are not subject to oblivion or loss and are difficult to counterfeit. However, uni-biometric systems that use only one biometric trait for recognition often suffer from issues like biometric data variation, lack of distinctiveness, low recognition accuracy and spoof attacks [1]. To overcome these problems, a multi-biometric system that fuses multiple biometric features from two or more sources, e.g., fingerprint, finger-vein, iris and face, not only leads to higher recognition accuracy, but it is also more difficult to be fooled or attacked.

Fingerprint is one of the most widely used and well researched biometric traits and finger-vein biometrics is potentially robust against spoofing as finger-veins are embedded inside a finger and need to be captured by an infrared sensor. If an adversary attempts to spoof a biometric system, he/she typically has to obtain a biometric sample to use as the basis of a spoofing attempt. Unlike face or fingerprint, which can be seen or traced, finger-vein is not visible and incapable of leaving traces behind, so the finger-vein biometrics is highly resilient to spoofing. The fingerprint and finger-vein based multi-biometric system, which holds richer and more discriminative information than a fingerprint- or finger-vein-based uni-biometric system [2], is supposed to improve recognition performance as well as enhance system security and reliability. Despite the advantages demonstrated by fingerprint and finger-vein biometrics, there is inadequate research on multi-biometric systems with fused fingerprint and finger-vein features. To address this issue, we propose a fingerprint and finger-vein-based cancelable multi-biometric system. In the design of

such a multi-biometric system, we must resolve two challenges: multi-biometric feature fusion and template security.

Multi-biometric feature fusion is non-trivial for the reason that feature representation of multiple traits may be different and incompatible to one another, e.g. minutia-based fingerprint features and image-based finger-vein features [3]. The only reported work on the feature fusion of fingerprint and finger-vein data is found in [4] and [5]. In [4], the image-based fingerprint and finger-vein codes are first extracted using a unified Gabor filter, and then a supervised local-preserving canonical correlation analysis (SLPCCA) algorithm is proposed to implement feature fusion. In this method, feature representation for both fingerprint and finger-vein information is image-based. The performance of this image-based multi-biometric system can be seriously affected by non-linear distortion and noise present in the fingerprint image. Therefore, in general, for the fingerprint image which has a set of salient points, minutia-based techniques are preferred to image-based ones [6]. Different to [4], in [5], minutia-based features are first extracted from fingerprint and finger-vein images, and then the fused feature point-sets from template and query images are matched using a point pattern matching and weight matching algorithm. However, the number of minutiae for the vein pattern is relatively small compared to that for fingerprint [7], causing low recognition accuracy. Actually, neither [4] nor [5] renders technically sound feature fusion, because identical feature representations are used at the feature extraction stage with the same technique. Although the issue of feature level incompatibility does not exist, the advanced minutia-based techniques for fingerprint feature extraction and image-based techniques for finger-vein feature extraction are ignored in [4] and [5], respectively. To take advantage of these good techniques which are suitable for respective biometrics, we fully exploit minutia-based fingerprint

features and image-based finger-vein features in the proposed multi-biometric system, and further develop an effective feature-level fusion strategy.

Security of multi-biometric templates is also a challenge. The security of the multi-biometric templates is crucial because they include information regarding multiple traits of the same individual [8]. The leakage of template data to the adversary can cause serious privacy and security risks, e.g. unauthorized access to the system or reproduction of original biometric traits. What makes things worse is that a compromised biometric template cannot be reset or replaced. Therefore, a template protection scheme should be designed to protect the fused templates of fingerprint and finger-vein data. Cancelable biometrics is an important template protection technique, which implements a one-way transformation to secure original biometric data. This one-way transformation is mathematically non-invertible and a compromised template can be easily revoked and replaced with another transformed template just by changing transformation parameters.

In recent years there has been a considerable amount of research effort in cancelable uni-biometric systems, e.g., [9-18]. However, there has been limited study on cancelable multi-biometrics [19-22]. In [19], Canuto *et al*. conducted an investigation on different fusion methods for cancelable multi-biometric systems, but the proposed fusion methods are based on score level fusion instead of feature level fusion. Paul *et al*. in [20] proposed a cancelable biometric template creation algorithm which utilizes random projection and transformation-based feature extraction and selection. In the proposed template creation algorithm, both face and ear biometric templates are divided into two parts, and then parts of the face image are combined with the parts of the ear image to generate a new mixed image before carrying out the cancelable transformation. This method is a kind of image fusion, which avoids the issue of feature data type incompatibility. In

[21], Chin *et al*. proposed a 3-stage hybrid template protection scheme. First, it integrates the fingerprint and palmprint at the feature level to generate a unified template. Then unique and random features are extracted from the fused features using a key-guided algorithm so as to achieve revocability. Finally, an algorithm referred to as equal-probable 2^N discretization is proposed to generate the binary string template from the unified feature vector created in the first stage. In [22], Rathgeb *et al*. proposed a framework to generate a non-invertible multiple biometric template based on Bloom filters, which enable different biometrics, e.g., face and iris, to be fused at the feature level. Specifically, the Bloom filters are utilized to transform the binary face and iris features into another representation, which cannot be reversed back to the original feature.

Although the cancelable multi-biometric systems in [20], [21] and [22] use a uniform feature data type, it is common to have different feature data types, when features are extracted from different biometric traits. In this paper, we perform feature data type conversion on minutia-based fingerprint features and image-based finger-vein features. We develop a feature-level fusion strategy with three fusion options. Matching performance and security strength using these different fusion options are evaluated and analyzed. Furthermore, based on our previous work [18] on cancelable fingerprint template design using the partial discrete Fourier transform (P-DFT), we propose an enhanced partial discrete Fourier transform (EP-DFT) based non-invertible transformation. The contribution of our work is highlighted below:

i. Unlike the universal feature extraction technique used for both fingerprint and finger-vein biometrics in [4] and [5], we adopt different feature extraction methods so that quality features can be extracted from fingerprint and finger-vein data. Specifically, for fingerprint feature extraction, we employ alignment-free local structures, formed by pairs of minutiae. In contrast, we apply an image-based technique to finger-vein feature

extraction. To address the issue of feature incompatibility, we make use of data type conversion methods.

ii. The proposed feature-level fusion strategy includes three different fusion options. These different fusion options demonstrate the trade-off between recognition accuracy and security, evidenced by our experiments. The EP-DFT based non-invertible transformation protects the fused fingerprint and finger-vein features and offers revocability when transformed multi-biometric templates are compromised.

iii. The proposed EP-DFT based non-invertible transformation strengthens system security by increasing possible solutions from many to infinite, which is a substantial improvement over the original P-DFT [18].

The rest of the paper is organized as follows. In Section 2, we present fingerprint and finger-vein feature extraction and data type conversion. In Section 3, we propose a feature-level fusion strategy with three different fusion options. In Section 4, experimental results and security analysis are demonstrated and discussed. We draw the conclusion in Section 5.

2. Feature extraction and data type conversion

In this section, we first introduce a minutia-based technique for fingerprint feature extraction and an image-based technique for finger-vein feature extraction. Then data type conversion methods are designed to convert both fingerprint and finger-vein feature vectors into binary strings, or equivalently binary vectors. These binary vectors or their variants are the inputs to the transformation function EP-DFT, which provides non-invertibility and revocability to the inputs.

2.1. Fingerprint feature extraction

With no demand on accurate detection of singular points, alignment-free structures are an appealing alternative to registration-based structures [16], since feature extraction from alignment-free structures does not rely on fingerprint image registration. Thus, in this paper we employ an alignment-free local structure based on pairs of minutiae. Extraction of this local structure was originally proposed in [14]. Compared with the feature extraction approach in [14], one more feature, the minutia type, is added to the local structure in [14]. The details are given as follows.

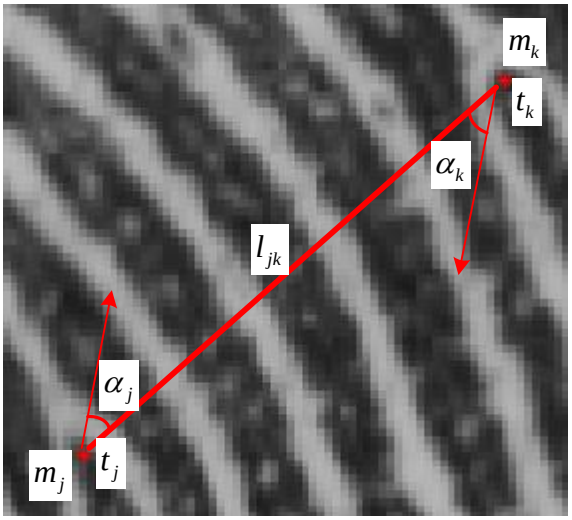

Figure 1: An example of local minutia structure - minutia pair p_{jk}.

Given a fingerprint image f_p, a set of minutiae can be extracted from it and each minutia is represented as (x, y, o, t), where (x, y) are the x and y coordinates in the Cartesian coordination system, o is orientation, and t is minutia type. The local structure is composed of pairs of minutiae, formed by pairing up each minutia with all other minutiae in the fingerprint image. For example,

a minutia pair, which is made up of minutia m_j and m_k, is shown in Figure 1. To avoid repetition, if m_j has been paired with m_k to generate the minutia pair p_{jk}, then the symmetric minutia pair p_{kj} will not be considered. Suppose that there are N_1 minutiae in the fingerprint image f_p, then there is a total of $C_{N_1}^2$ minutia pairs that can be constructed. For each minutia pair, e.g., p_{jk}, several translation- and rotation-invariant features (as shown in Figure 1) are defined as follows:

1. The length of the edge, e.g., l_{jk}.
2. The angles between the orientation of each minutia and the edge, e.g., α_j and α_k.
3. The type of each minutia, e.g., t_j and t_k.

In this way, a total of $C_{N_1}^2$ features, e.g., $\{l_{jk}, \alpha_j, \alpha_k, t_j, t_k\}$, can be extracted from $C_{N_1}^2$ minutia pairs formed by N_1 minutiae in fingerprint image f_p.

2.2. Fingerprint feature data type conversion

To mitigate the intra-user variation between the corresponding minutia pairs from the template and query, and at the meantime convert those real-valued features into binary strings, we apply the quantization technique [13] to the extracted features of each minutia pair and convert them into several short binary strings. Specifically, we set s_l and s_α as the quantization step sizes of the edge length and angle, respectively. For example, the feature vector $\{l_{jk}, \alpha_j, \alpha_k, t_j, t_k\}$ extracted from minutia pair p_{jk}, the values of $\{l_{jk}, \alpha_j, \alpha_k\}$, after quantization and conversion to binary representation, are represented by $\{\%_{jk}, \%_j, \%_k\}$, which are of length L_1, L_2 and L_3 bits, respectively. The minutia type can be represented by one bit. We then concatenate all these short

binary strings into a long binary string $V_{jk} = l_{jk} \| \alpha_j \| \alpha_k \| t_j \| t_k$, which contains L_f = L_1+ L_2+L_3+2 bits. The number of bits required to represent the quantized result is determined by the quantization step sizes, s_l and s_α . It is worth noting that these step sizes should be chosen judiciously, because too small a step size is sensitive to slight image distortion, while too large a step size could lose the discriminative power of feature data. Since L_f bits can represent 2^{L_f} binary values or integers ranging from 0 to $2^{L_f} - 1$, each of the $C_{N_1}^2$ binary strings, e.g., V_{jk} , can be converted to an integer that belongs to the set [0, $2^{L_f} - 1$]. For example, if the integer value of V_{jk} is V_{jk}^I =300, then the 300th position of the set [0, $2^{L_f} - 1$] is indexed by '1'. For those positions that are not indexed by '1', the value of '0' is assigned to them. By inspecting all position indexes of the set [0, $2^{L_f} - 1$], we can integrate all $C_{N_1}^2$ binary strings into one binary vector $\mathbf{b}_p$ of length 2^{L_f} , of which the value of 1 mean that the corresponding element position of the set [0, $2^{L_f} - 1$] matches the integer value of a certain binary string among $C_{N_1}^2$ candidates. This process is illustrated in Figure 2.

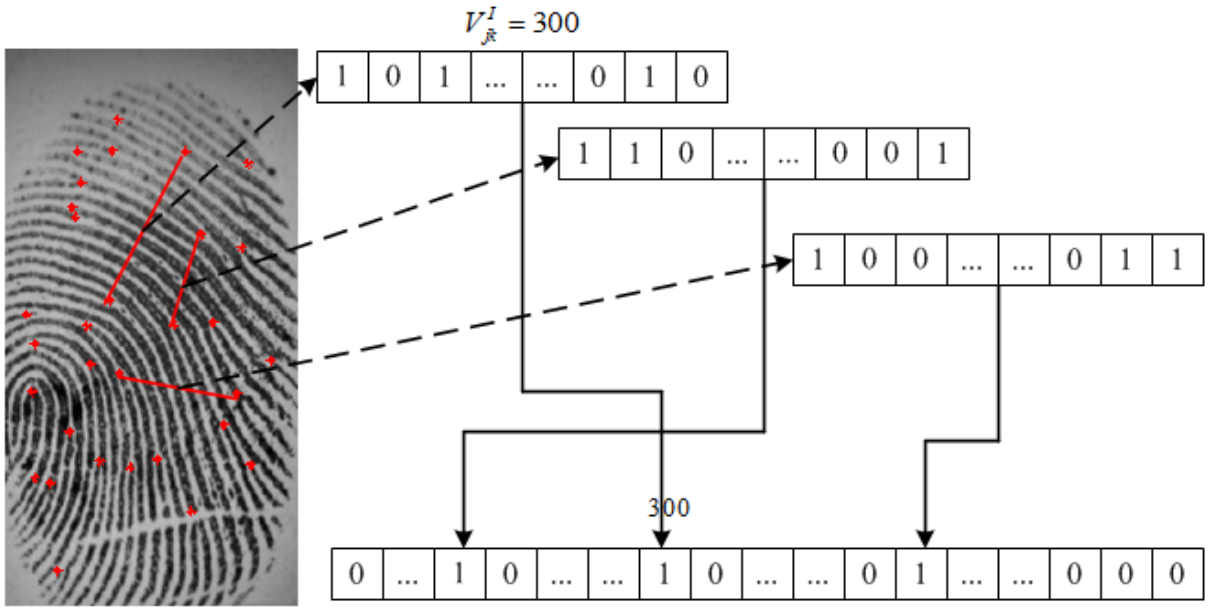

Figure 2: An example of local minutia structure, minutiae pair

By going through the above procedure, the extracted minutia pairs from the fingerprint image f_p are represented by the binary vector $\mathbf{b}_p$, which can be further fused with finger-vein features or directly treated as an input to the EP-DFT based transformation function.

2.3. Finger-vein feature extraction

Finger-vein recognition is a relatively new biometric technology and research topic. The finger-vein pattern is unique to a specific individual, difficult to forge, contact-less, not affected by race and skin discolorations, and does not change as people age [23]. A considerable amount of work has been done to prove that the finger-vein can be used as a means for individual identification [4], [5], [24] and [25]. However, a finger-vein image could suffer from factors such as illumination and blood flow, which make the finger-vein image unstable and have low contrast, so reliable finger-vein recognition accuracy is hard to achieve. Before conducting feature

extraction from a finger-vein image, a pre-processing procedure, including reliable region of interest (ROI) determination and image enhancement, same as that conducted in [26], is employed in our application. An example of a finger-vein image before and after pre-processing is shown in Figure 3.

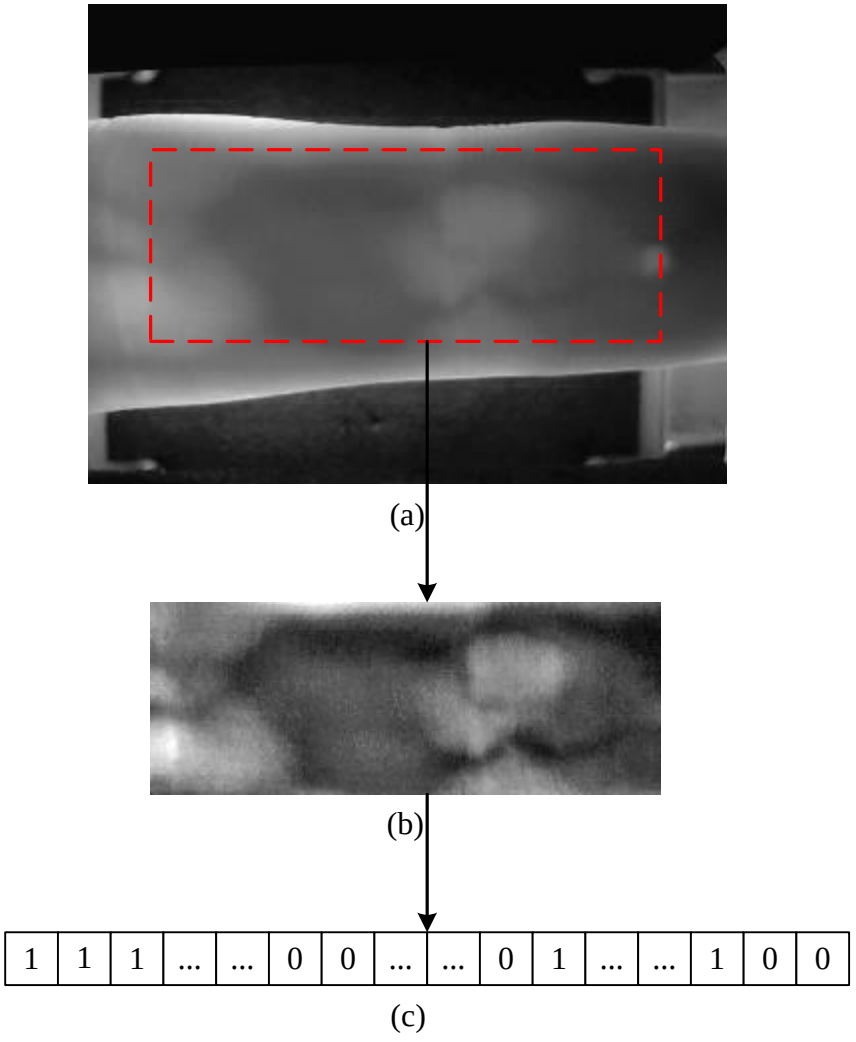

Figure 3. An example of a finger-vein image, (a) original finger-vein image, (b) finger-vein image after ROI extraction and image enhancement, (c) binary feature vector generated from finger-vein image

In the spatial domain, Gabor filter and linear discriminate analysis (LDA) have been shown to be powerful in image-based face recognition [27], so we employ the similar scheme in [27] to extract the finger-vein feature. Specifically, when deriving finger-vein feature representation from a given finger-vein image f_v, 40 Gabor filters are applied to filter f_v, which generates a real-valued vector with dimension 983040 (256×96×40). However, this real vector is too large for efficient processing and storage. To solve the issue, the dimensionality reduction technique, linear discriminant analysis (LDA) [27], is exploited to project the feature vector into a subspace, in which between-class variations of the projected patterns are maximized, while within-class variations are minimized [28]. Readers can refer to [27] for more details. By doing this, a feature vector $\mathbf{v}_v$, which contains N_2 real values, is generated from the given finger-vein image f_v.

2.4. Finger-vein feature data type conversion

Similar to the process applied to the fingerprint feature vector, the real-valued finger-vein feature vector $\mathbf{v}_v$ needs to be converted to a binary string, sharing the same data type as the fingerprint feature vector. One well-known method of converting real-valued data into a binary string is Bio-hashing [29], which is based on random projection and assigns a single bit to each projection according to a set threshold. Bio-hashing is utilized in our application to achieve the goal of data type conversion. Specifically, a user-specific orthonormal random matrix $\mathbf{R}_v$ of size $N_3 \times N_2$ is generated first. We then perform the inner-product of the extracted finger-vein feature vector $\mathbf{v}_v$ with $\mathbf{R}_v$, i.e., $X = \mathbf{R}_v \mathbf{v}_v$, where $X = \{x_i\}_{i=1}^{N_3}$. For each x_i, it is represented by a binary value b_i using the following equation:

$$b_i = \begin{cases} 0 & if\ x_i \le \tau \\ 1 & if\ x_i > \tau \end{cases} \quad (1)$$

where τ is a preset threshold and set to 0 in our application. In this way, the finger-vein image f_v can be represented by a single binary vector $\mathbf{b}_v = [b_1, b_2, ..., b_{N_3}]^T$.

3. Proposed feature-level fusion strategy

In this section, we propose a feature-level fusion strategy, which includes a non-invertible transformation based on the EP-DFT and three different fusion options. First, built upon our previous work, the partial discrete Fourier transformation (P-DFT) based non-invertible transformation [18], the enhanced P-DFT (EP-DFT) is introduced. Then we explore different feature fusion options, which is critical to the design of a multi-biometric system.

3.1. Enhanced partial discrete Fourier transform (EP-DFT)

Here, we first give a brief introduction to the P-DFT in [18]. The DFT matrix owns some favorable characteristics, e.g., orthogonality. Moreover, fast Fourier transform algorithms take advantage of the symmetries of the DFT matrix to reduce the time of multiplying it with a vector, thus making P-DFT based transformation compact and computationally efficient [18]. Assume that biometric feature $\mathbf{f} = [f_1, f_2, ..., f_K]^T$ is a binary vector with *K* elements and $\mathbf{W}$ is an *K*-by-*K* square DFT matrix,

$$\mathbf{W} = \frac{1}{\sqrt{K}} \begin{bmatrix} 1 & 1 & 1 & \mathsf{L} & 1 \\ 1 & w & w^2 & \mathsf{L} & w^{K-1} \\ 1 & w^2 & w^4 & \mathsf{L} & w^{2(K-1)} \\ \mathsf{M} & \mathsf{M} & \mathsf{M} & \mathsf{O} & \mathsf{M} \\ 1 & w^{(K-1)} & w^{2(K-1)} & \mathsf{L} & w^{(K-1)(K-1)} \end{bmatrix} \tag{2}$$

where $w = e^{-2\pi i/K}$ is the primitive *K*th root of unity, in which *i* is the imaginary unit, satisfying the equation $i^2 = -1$.Then the DFT based transformation is computed by $\mathbf{y} = \mathbf{Wf}$, which results a complex-valued vector $\mathbf{y} = [y_1, y_2, ...y_K]^T$. But the DFT matrix $\mathbf{W}$ is unitary, so the matrix multiplication operation $\mathbf{Wf}$ is invertible, which cannot be used to protect the biometric feature $\mathbf{f}$.

However, if we only use part of the DFT matrix $\mathbf{W}$, that is, *k* out of *K* rows are chosen to generate a P-DFT matrix $\mathbf{M}$, which is a *k*-by-*K* column rank-deficient matrix. The choice of *k* rows depends on a user-specific parameter, which contains the indexes of those *k* rows. Then the P-DFT based transformation is calculated by $\mathbf{y}' = \mathbf{Mf}$, which results in a complex vector $\mathbf{y}' = [y_1, y_2, ...y_k]^T$, where $k<K$. The application of the P-DFT here yields an underdetermined system, which has non-unique solutions of the biometric feature $\mathbf{f}$ when both the vector $\mathbf{y}'$ and matrix $\mathbf{M}$ are known by the adversary. So the P-DFT based transformation is non-invertible.

The biometric feature $\mathbf{f}$ only includes values of 1 and 0 and is sparsely distributed. This will narrow down the search space for the solutions of $\mathbf{f}$, when the vector $\mathbf{y}'$ and matrix $\mathbf{M}$ in transformation $\mathbf{y}' = \mathbf{Mf}$ are known by the adversary. To solve this issue, we first apply the wavelet transform to the binary feature $\mathbf{f}$, then the P-DFT. This enhanced version of the P-DFT based transformation converts the binary-valued feature into real-valued feature, and hence increases the

randomness and search space of solutions, making it harder to tackle the P-DFT to restore the binary feature $\mathbf{f}$. One may argue that the wavelet transform is an invertible process, but the purpose of adding it prior to the P-DFT is not to implement non-invertibility – non-invertibility is realized by the P-DFT itself rather than the wavelet transform. To summarize the proposed EP-DFT based non-invertible transformation, we perform the wavelet transform (WT) on biometric feature $\mathbf{f}$, expressed by $\mathbf{f}' = \mathbf{f}_L \| \mathbf{f}_H = WT(\mathbf{f}, \mathrm{L}_d, \mathrm{H}_d)$, where $\mathbf{f}_L$ and $\mathbf{f}_H$ are the approximation coefficients vector and detail coefficients vector obtained by the wavelet decomposition of feature $\mathbf{f}$, and $\mathbf{f}'$ is the concatenation of $\mathbf{f}_L$ and $\mathbf{f}_H$. L_d represents the decomposition low-pass filter and H_d represents the decomposition high-pass filter. These two parameters are determined by the use of a particular wavelet or any specified filters; for example, the Discrete FIR approximation of Myer wavelet 'dmey' is applied in our application. Following $\mathbf{f}' = \mathbf{f}_L \| \mathbf{f}_H = WT(\mathbf{f}, \mathrm{L}_d, \mathrm{H}_d)$, the P-DFT is performed on $\mathbf{f}'$ as

$$\mathbf{y}' = \mathbf{M}\mathbf{f}' \tag{3}$$

3.2. Three different feature fusion options

It follows from the latest research that biometric fusion on the feature level is most suitable for template protection schemes [30], since applying feature-level fusion to template protection is both straightforward and effective. The fused feature vectors have more components, which are likely to be more discriminative and robust. It is known that even minor differences in the design of a feature level fusion approach can greatly influence the overall system performance and security. In this paper, we propose a feature-level fusion strategy that contains three different

fusion options, meeting varying demands on system recognition accuracy and security. The detailed procedure of each fusion option is presented as follows and the corresponding workflow is shown in Figure 4.

Option one: The fingerprint and finger-vein feature vectors are concatenated into a new feature vector before being fed to the EP-DFT based non-invertible transformation. The detailed steps are listed below:

1. The fingerprint feature vector $\mathbf{b}_p$ and finger-vein feature vector $\mathbf{b}_v$ are concatenated into a new binary-valued feature vector $\mathbf{b} = [\mathbf{b}_p^T, \mathbf{b}_v^T]^T$.

2. The generated new binary-valued feature vector $\mathbf{b}$ is turned by *WT* as $\tilde{\mathbf{b}} = WT(\mathbf{b})$ and then transformed by the P-DFT based transformation as $\mathbf{Y} = \mathbf{M}\tilde{\mathbf{b}}$, where $\mathbf{M}$ is the P-DFT matrix whose dimension is $k \times K$.

Option two: The fingerprint feature vector $\mathbf{b}_p$ and finger-vein feature vector $\mathbf{b}_v$ are first turned by *WT* and transformed by the P-DFT, and then concatenated into a new feature vector. The detailed steps are listed below:

1. The fingerprint feature vector $\mathbf{b}_p$ is turned by *WT* as $\tilde{\mathbf{b}}_p = WT(\mathbf{b}_p)$ and then transformed by the P-DFT as $\mathbf{y}_p = \mathbf{M}_p\tilde{\mathbf{b}}_p$, where $\mathbf{M}_p$ is the $k \times K$ P-DFT matrix to transform the fingerprint feature. .

2. The finger-vein feature vector $\mathbf{b}_v$ is turned by *WT* as $\tilde{\mathbf{b}}_v = WT(\mathbf{b}_v)$ and then transformed by the P-DFT as $\mathbf{y}_v = \mathbf{M}_v\tilde{\mathbf{b}}_v$, where $\mathbf{M}_v$ is the $k \times K$ P-DFT matrix to transform the finger-vein feature.

3. The transformed fingerprint feature vector $\mathbf{y}_p$ and transformed finger-vein feature vector $\mathbf{y}_v$ are concatenated into a new feature vector $\mathbf{Y} = [\mathbf{y}_p, \mathbf{y}_v]$.

Option three: The fingerprint feature vector $\mathbf{b}_p$ and finger-vein feature vector $\mathbf{b}_v$ are mixed together by the XOR operation, which generates a feature vector $\mathbf{b}$ of the same length as $\mathbf{b}_p$ or $\mathbf{b}_v$. Then binary-valued feature $\mathbf{b}$ is turned by *WT* and fed to the P-DFT based non-invertible transformation. The detailed steps are listed below:

1. The fingerprint feature vector $\mathbf{b}_p$ is XORed with the finger-vein feature vector $\mathbf{b}_v$, i.e., $\mathbf{b} = \mathbf{b}_p \oplus \mathbf{b}_v$, where $\oplus$ denotes element-wise XOR.

2. Feature vector $\mathbf{b}$ is turned by *WT* as $\tilde{\mathbf{b}} = WT(\mathbf{b})$ and then transformed by the P-DFT as $\mathbf{Y} = \tilde{\mathbf{M}}\tilde{\mathbf{b}}$, where $\tilde{\mathbf{M}}$ is the $k \times K$ P-DFT matrix.

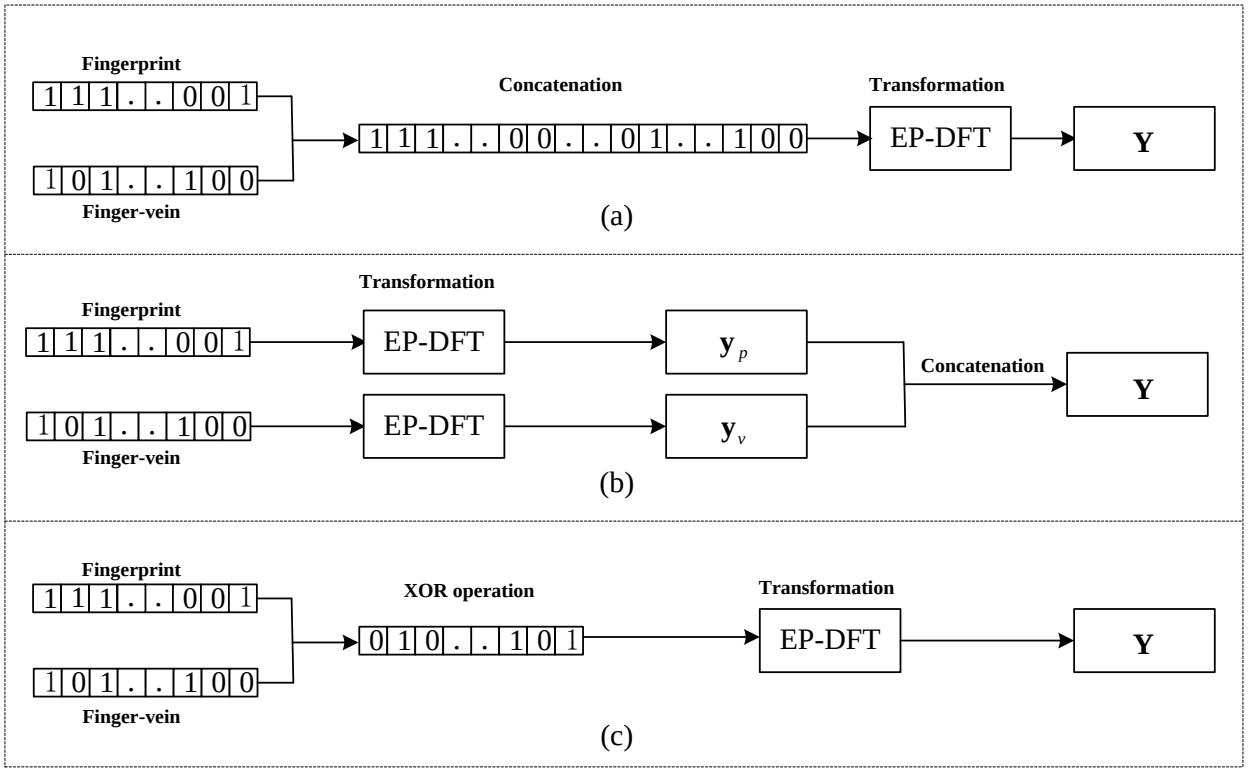

Figure 4: Three different fusion options (a), (b) and (c).

3.3. Matching in the transformed domain

Matching of the proposed multi-biometric authentication system is conducted in the transformed domain so as to protect the original biometric feature data. Two stages, namely, enrollment stage and verification stage, are included in the proposed authentication system. In the enrollment stage, the fingerprint and finger-vein feature data are extracted and converted into binary-valued feature vectors, which are further transformed by the EP-DFT based non-invertible transformation using one of the three fusion options provided by the proposed feature level fusion strategy. The output of the non-invertible transformation is stored in the database as a template, which is used for comparison in the verification stage. In the verification stage, a query goes through the same procedure of generating the transformed feature vector as in the enrollment stage. Then similarity between the template and query is calculated to decide whether or not the query matches the template.

We assume that $\mathbf{Y}^T$ is the resultant feature vector of the template and $\mathbf{Y}^Q$ is the resultant feature vector of the query (the superscripts T and Q stand for 'template' and 'query'). Both $\mathbf{Y}^T$ and $\mathbf{Y}^Q$ are complex vectors, and the following similarity calculation is to determine the similarity score between them:

$$S(\mathbf{Y}^T, \mathbf{Y}^Q) = 1 - \frac{\| \mathbf{Y}^T - \mathbf{Y}^Q \|_2}{\| \mathbf{Y}^T \|_2 + \| \mathbf{Y}^Q \|_2} \tag{4}$$

where $\|\cdot\|_2$ means the 2-norm. The similarity score $S(\mathbf{Y}^T, \mathbf{Y}^Q)$ calculated by Equation (4) falls in the range of 0 to 1. The larger the similarity score, the more similar the feature vectors of the template and query.

4. Experimental results and security analysis

In this section, experiments are conducted on several databases to evaluate the proposed cancelable multi-biometric system. Comparison regarding system recognition performance and security using different feature level fusion options is carried out.

4.1. Database selection

Fingerprint database: We chose the publicly available fingerprint databases, FVC2002 DB2 [31] and FVC2004 DB2 [32], in our testing. Each fingerprint database contains a total of 800 gray-level fingerprint images, which are collected from 100 fingers with eight samples per finger. We chose the first and second images of each finger from these fingerprint databases in our experiments. The software VeriFinger 4.0 of Neurotechnology [33] was utilized for minutiae extraction.

Finger-vein database: We chose the public finger-vein database from the Homologous Multi-modal Traits Database (FV-HMTD) [34] set up by the Group of Machine Learning and Applications, Shandong University, China. This finger-vein database contains images from 106 individuals. Each individual was asked to provide images of his/her index finger, middle finger and ring finger of both hands and the collection for each of the six fingers was repeated six times to obtain 36 finger-vein images. Therefore, there are 636 (=106×6) different fingers with six

finger-vein images per finger. Each finger-vein image is 320×240 pixels in size. We chose the first 100 fingers and the first four finger-vein images of each finger were used for training and the remaining two finger-vein images were used for testing.

Multi-biometric database: We set up two multi-biometric databases, MD-A and MD-B. In multi-biometric database MD-A, we combined the first and second images of each finger in the fingerprint database FVC2002 DB2 with the fifth and sixth images from each finger of the first 100 fingers in the finger-vein database FV-HMTD, respectively, thus forming two image pairs, each of which contains a fingerprint image and a finger-vein image. So there are 200 (=2×100) mated image pairs in the multimodal database MD-A. By the same token, 200 mated pairs of fingerprint and finger-vein images are generated and assigned to database MD-B by using the images from the fingerprint database FVC2004 DB2 and the finger-vein database FV-HMTD.

4.2. Matching performance evaluation

The performance of the proposed cancelable multi-biometric system is evaluated by three performance indices, the genuine accept rate (GAR), false accept rate (FAR) and equal error rate (EER). They are defined as follows:

GAR: the ratio of successful genuine attempts to the total genuine attempts.

FAR: the ratio of successful imposter attempts to the total imposter attempts.

EER: the error rate when the FAR is equal to 1-GAR.

As for the tests on each of the above databases in our experiments, the first image pair (fingerprint image + finger-vein image) is used as the template and the second image pair from the same finger is considered as the query to calculate the GAR. To compute the FAR, the first image pair from each finger is set as the template and first image pair from the remaining fingers (i.e., other fingers)

is set as the query. Therefore, for each database, according to the above rule, it yields 100 genuine matching tests and 4950 (= (100×99)/2) imposter matching tests.

Matching performance without transformation: The performance of fingerprint and finger-vein based uni-biometric systems is evaluated first, followed by performance evaluation of the multi-biometric system. All features tested in these three systems are untransformed, and the test results of all three systems on different databases are reported in Table 1, from which we can see that the multi-biometric system and the finger-vein based uni-biometric system perform better than the fingerprint based uni-biometric system. The multi-biometric system performs slightly worse than the finger-vein based uni-biometric system on database MD-A but they exhibit the same performance on database MD-B. Note that although multi-biometric systems do not perform absolutely better than uni-biometric systems, e.g., the finger-vein based uni-biometric system in our experiment, the performance of multi-biometric systems is competitive enough; what is more, multi-biometric systems provide higher security than uni-biometric systems, as discussed in Section 4.4. Also Table 1 shows that the fingerprint based uni-biometric system performs significantly better on FVC2002 DB2 (EER=1.00%) than FVC2004 DB2 (EER=10.00%). This is due to the poor image quality of FVC2004 DB2, in which the first two images are heavily distorted since individuals were requested to exaggerate finger skin distortion at the acquisition time [35].

Table 1. EER(%) of uni- and multi-biometric systems on different databases

Databases / **Systems**	2002DB2	2004DB2	FV-HMTD	MD-A (2002DB2+FV-HMTD)	MD-B (2004DB2+FV-HMTD)
Fingerprint system (untransformed)	1.00	10.00	-	-	-
Finger-vein system	-	-	0.18	-	-

(untransformed)							
Multi-biometric system (untransformed)	-	-	-	0.26		0.18	
				P-DFT	EP-DFT	P-DFT	EP-DFT
Multi-biometric system (fusion option 1)	-	-	-	0.36	0.12	0.12	0.12
Multi-biometric system (fusion option 2)	-	-	-	0.12	0.12	0.04	0.12
Multi-biometric system (fusion option 3)	-	-	-	0.32	0.55	0.28	0.69

Matching performance with three different fusion options: Choosing different fusion options affects not only the system security level but also matching performance. The matching performance with three different feature fusion options on the multi-biometric databases, MD-A and MD-B, is evaluated. We first evaluate the system matching performance using the original partial-DFT based transformation. As listed in Table 1, the cancelable multi-biometric system using the fusion option 2 performs best among all three fusion options on both MD-A and MD-B. Specifically, for database MD-A, EER is 0.12% when the cancelable multi-biometric system uses fusion option 2, which is about three times better than that using fusion option 1 (EER=0.36%) and using fusion option 3 (EER=0.32%). Similar observations can be made on database MD-B. In addition, the cancelable multi-biometric system with fusion option 2 demonstrates superior performance to the untransformed multi-biometric system on databases MD-A and MD-B, and the cancelable multi-biometric system with fusion option 1 performs better than the untransformed multi-biometric system on database MD-B.

Furthermore, we evaluate the system matching performance using the proposed EP-DFT based transformation. From Figure 5 and Figure 6, we can see that the cancelable multi-biometric

system using fusion options 1 and 2 achieves the same matching performance of EER=0.12% on both databases of MD-A and MD-B. The cancelable multi-biometric system using fusion 3 performs worse than other two fusion options and achieves the EER of 0.55% and 0.69% on databases MD-A and MD-B, respectively.

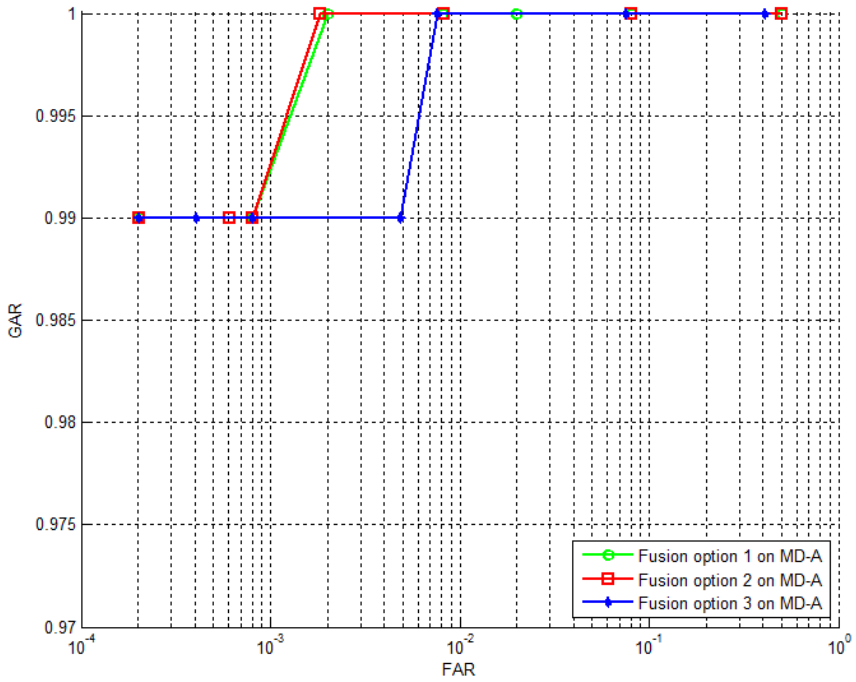

Figure 5: ROC curves for database MD-A using the EP-DFT based transformation.

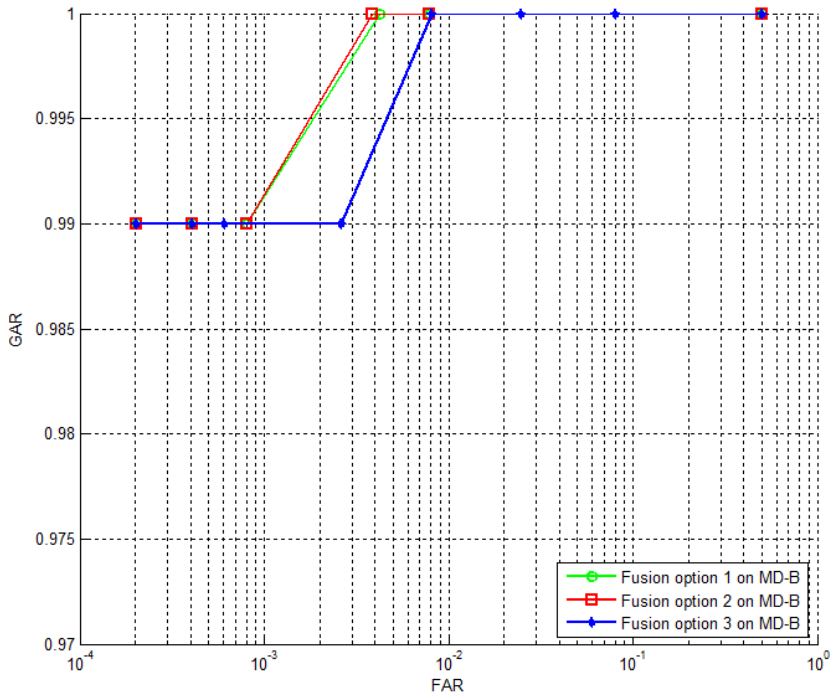

Figure 6: ROC curves for database MD-B using the EP-DFT based transformation.

In terms of matching performance, we see from Table 1 that there is no remarkable difference between the original P-DFT and the proposed EP-DFT. However, the EP-DFT makes the security of the cancelable multi-biometric system stronger, as analyzed in Section 4.4.

Matching performance by using different keys: In a cancelable biometric system, once a transformed template is compromised, it can be simply revoked and re-generated by applying another different key. In order to test the effect of revocation on the system performance and evaluate the discriminative power of biometric features, we carry out the feature transformation for one hundred times by utilizing one hundred different keys. After each transformation, we evaluate the matching performance of the cancelable multi-biometric system using the fusion option 1 on both databases MD-A and MD-B. All the results obtained are listed in Table 2, from which we can see that the best matching performance is Min_EER=0, the worst matching

performance is Max_EER=1.00%, and the average matching performance of these one hundred tests is Ave_EER=0.45% on database MD-A, while the best matching performance is Min_EER=0.02%, the worst matching performance is Max_EER=1.00%, and the average matching performance of the one hundred tests is Ave_EER=0.38% on database MD-B. The EERs on both databases are in the range of 0 to 1.00% with the average EER below 0.5%. Therefore, the EERs are consistently low, which shows that the discriminative power of the biometric features does not vary significantly when the transformed features are revoked and re-generated.

Table 2. EER(%) of the multi-biometric system using 100 different keys

Test no.	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
MD-A	.16	.30	1	1	.63	.77	.26	.40	.69	1	1	.02	.38	.36	.16	1	.02	.22	.06	1
MD-B	.04	.38	1	.91	.57	.59	.08	.30	1	.53	1	.02	.44	.14	.22	.34	.14	.18	.08	1
Test no.	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**	**32**	**33**	**34**	**35**	**36**	**37**	**38**	**39**	**40**
MD-A	.46	.44	.89	.08	1	.20	.06	.18	.06	.51	.12	.44	.18	.55	.40	1	.16	.36	1	0
MD-B	.55	.38	.79	.08	1	.20	.08	.34	.08	.61	.22	.40	.18	.48	.40	.34	.28	.48	.79	.02
Test no.	**41**	**42**	**43**	**44**	**45**	**46**	**47**	**48**	**49**	**50**	**51**	**52**	**53**	**54**	**55**	**56**	**57**	**58**	**59**	**60**
MD-A	.08	.65	.65	1	.16	.06	.22	.56	.28	1	.14	.12	.06	.42	.53	1	.54	.30	.20	1
MD-B	.04	.53	.08	1	.24	.08	.04	.16	.24	1	.06	.14	.04	.18	.81	.86	1	.38	.38	.22
Test no.	**61**	**62**	**63**	**64**	**65**	**66**	**67**	**68**	**69**	**70**	**71**	**72**	**73**	**74**	**75**	**76**	**77**	**78**	**79**	**80**
MD-A	.28	.04	.06	.81	.22	.20	1	.86	.67	1	.12	.51	.20	.08	.06	.28	.10	.06	.10	.48
MD-B	.30	.12	.08	.24	.24	.28	.46	.72	.67	1	.10	.24	.12	.04	.08	.40	.32	.22	.18	.59
Test no.	**81**	**82**	**83**	**84**	**85**	**86**	**87**	**88**	**89**	**90**	**91**	**92**	**93**	**94**	**95**	**96**	**97**	**98**	**99**	**100**
MD-A	.20	.22	.24	.81	.36	.99	.97	.55	.16	.10	.75	.16	.97	1	.69	.10	1	.02	.24	1
MD-B	.12	.34	.04	1	.38	.30	.71	.24	.36	.16	.61	.12	.63	.38	.71	.06	1	.02	.16	.32

Compare with other fingerprint and finger-vein based multi-biometric systems: Regarding the performance comparison with other fingerprint and finger-vein based multi-biometric systems such as [4] and [5], the best matching performance reported in [4] is FAR= 1.35% when FRR=0, while FAR=0.97% when FRR=1.85 is reported in [5]. We notice that the finger-vein databases used in both systems were collected by the author themselves and are not publicly available, so it is hard for us to compare them with the proposed method on the same basis. Since our approach employs the cancelable template technique to protect the fingerprint and finger-vein template data, it renders a clear advantage over the approaches without template protection in [4] and [5].

4.3. Revocability

Revocability is one of the essential requirements of a qualified cancelable biometric system. The revocability property requires that when a biometric template is compromised, it can be revoked and a new template is able to replace the compromised one. The new template should be totally different to the compromised template. To evaluate the revocability of the proposed cancelable multi-biometric system, 50 different templates are created by applying 50 different user specific keys to the first image pair on database MD-A. Different user specific keys will generate different P-DFT matrixes. The fusion option 1 is chosen for this revocability test. The verification of revocability with other two fusion options can be performed in a similar fashion, since all three fusion options use the same idea of the EP-DFT based non-invertible transformation. The imposter distribution versus the pseudo-imposter distribution is plotted in Figure 7 under the situation where each user in database MD-A uses a different user specific key that is involved in the generation of the P-DFT matrix $\mathbf{M}$. In Figure 7, it is shown that the imposter distribution almost overlaps the pseudo-imposter distribution, which means any newly generated transformed template from the

same original template is unrelated to the old/compromised transformed template and is also different from other new transformed templates.

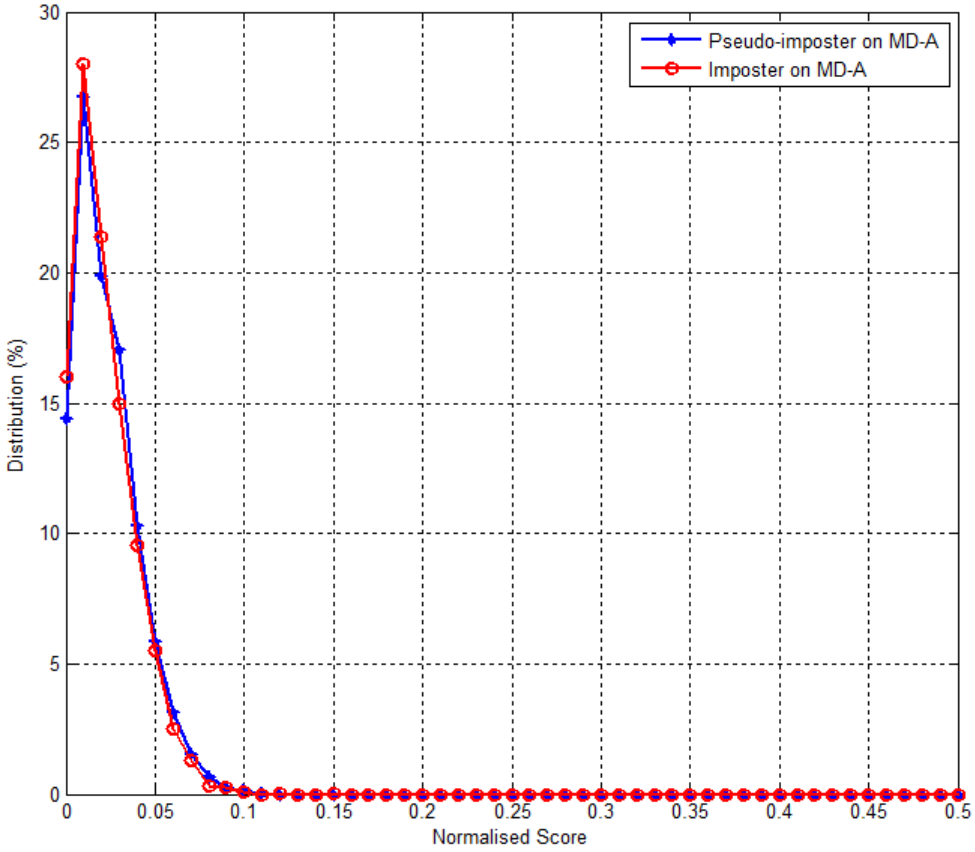

Figure 7: Pseudo-imposter and imposter distributions on database MD-A.

4.4. Security Analysis

In our experiments, to ensure that matching performance is measured for all three fusion options under the same parameter settings, the length of feature vectors $\mathbf{b}_p$ and $\mathbf{b}_v$ are empirically set to 30000, and the resultant transformed feature vector $\mathbf{Y}$ is of length 600. According to these parameter settings, if we assume that the P-DFT matrix $\mathbf{M}$ and the transformed feature vector $\mathbf{Y}$

are both obtained by the adversary, the security of the proposed system is provided by the EP-DFT, which constitutes a system of linear equations, rendering an underdetermined system. From the matching performance evaluation, we can see that the proposed cancelable multi-biometric system using the EP-DFT performs better with fusion options 1 and 2 than that with fusion option 3. However, there is a trade-off between recognition accuracy and security.

The P-DFT matrix $\mathbf{M}$ used in the EP-DFT based transformation (Equation (3)) is a *k*-by-*K* column rank-deficient matrix with $rank(\mathbf{M}) = k$, where $k < K$. In theory, Equation (3) has an infinite number of solutions, because any vector in the form of $\mathbf{f}' + h$ is also a solution to Equation (3), provided that *h* is in the null space of $\mathbf{M}$. However, if the original P-DFT [18] is used, the solutions to Equation $\mathbf{y}' = \mathbf{M}\mathbf{f}$ are many but not infinite, since the feature vector $\mathbf{f}$ only contains binary values, 0 and 1, which greatly narrows down the search space of the solutions to Equation $\mathbf{y}' = \mathbf{M}\mathbf{f}$. Instead, if we perform the proposed EP-DFT, the wavelet transform $\mathbf{f}' = WT(\mathbf{f})$ included as part of the EP-DFT converts the binary-valued vector $\mathbf{f}$ into real-valued vector $\mathbf{f}'$, which enables $\mathbf{f}'$ to have a relatively flat spectrum and thus significantly increases the number of possible solutions to $\mathbf{y}' = \mathbf{M}\mathbf{f}'$. It is a noted result in linear algebra that Equation (3) owns infinite solutions and $\mathbf{f}'$ is just one of them, when the coefficient and augmented matrixes of Equation (3) have the same rank [36].

Another benefit brought about by the proposed EP-DFT is that it can prevent the system from the attacks via record multiplicity (ARM), which is a threat to existing cancelable biometric systems. According to the analysis in [37] and [38], the main reason that cancelable biometric systems suffer from the ARM is due to the fact that the same feature vector, e.g., $\mathbf{f}$, is applied across multiple applications. The proposed EP-DFT can address this issue by adjusting values of

parameters L_d and H_d in the wavelet transform $\mathbf{f}' = WT(\mathbf{f}, L_d, H_d)$ to generate different outcomes, for example, $\mathbf{f}_1'$ and $\mathbf{f}_2'$ ($\mathbf{f}_1' \neq \mathbf{f}_2'$) can be generated for applications 1 and 2, respectively. In this way, the adversary cannot launch the ARM to obtain either $\mathbf{f}_1'$ or $\mathbf{f}_2'$ by reversing DFT, because it would be highly unlikely for the attacker to be able to gather a sufficient number of relevant system equations from different applications to match the number of independent unknown variables so as to solve them.

With the proposed EP-DFT, we can see from Table 1 that with fusion option 3, the system demonstrates the lowest matching performance; however, the use of fusion option 3 provides a higher security level than fusion options 1 and 2. In fusion option 3, the feature vector $\mathbf{b}$ is first produced by the XOR operation using the fingerprint feature vector $\mathbf{b}_p$ and finger-vein feature vector $\mathbf{b}_v$. The XOR operation can provide extra protection when the adversary tries to split either $\mathbf{b}_p$ or $\mathbf{b}_v$ from $\mathbf{b}$ under the assumption that $\mathbf{b}$ is obtained by the adversary. The primary merit of the XOR operation is that it is simple to implement and its computational cost is low [39]. In a tradition application of the XOR operation, e.g., $\text{plaintext} \oplus \text{key} = \text{ciphertext}$, the key is supposed to be a secret, because the XOR operator is vulnerable to a known-key attack, since $\text{ciphertext} \oplus \text{key} = \text{plaintext}$. For our system, both $\mathbf{b}_p$ and $\mathbf{b}_v$ are not stored in the database which eliminates the above risk caused by key loss. If $\mathbf{b}_p$ or $\mathbf{b}_v$ is truly randomly distributed, the result $\mathbf{b}$ is a one-time pad, which is provably unbreakable in theory [40]. In practical biometric applications, although $\mathbf{b}_p$ or $\mathbf{b}_v$ is sparsely distributed, the security strength offered by the XOR operation is still high.

In summary, from the above analysis, it is clear that the proposed cancelable multi-biometric system with the EP-DFT based non-invertible transformation provides higher security as opposed to the original P-DFT. Moreover, compared with fusion options 1 and 2, the fusion option 3 in our feature-level fusion strategy gives additional protection to the system by applying a simple and cost-effective XOR operation.

5. Conclusion

In this paper, we have proposed a cancelable multi-biometric system, which combines the minutia-based fingerprint feature set and image-based finger-vein feature set using a feature-level fusion strategy. After we apply data type conversion, different feature data types become compatible, paving the way for subsequent feature fusion. Moreover, the proposed feature-level fusion strategy has three different fusion options. Thanks to the EP-DFT based non-invertible transformation, the proposed cancelable multi-biometric system demonstrates satisfactory matching performance. Moreover, the proposed EP-DFT greatly enhances system security compared with the original P-DFT.

Cancelable multi-biometrics is an emerging area. We will investigate new approaches to feature extraction for multiple traits, and more importantly, effective fusion methods to increase the matching performance and security of the overall system. Furthermore, it is imperative to design good, efficient non-invertible transformation functions for cancelable multi-biometric systems.

Acknowledgement

This paper is supported by Defence Science and Technology Group (DST) of Australia through project CERA 221.

References

[1] A.Jagadeesan, K.Duraiswamy, Secured cryptographic key generation from multimodal biometrics: feature level fusion of fingerprint and iris, international Journal of Computer Science and information Security, 7 (2010) 028-037.

[2] C. Rathgeb, C. Busch, Multi-Biometric Template Protection: Issues and Challenges, New Trends and Developments in Biometrics, (2012) 173-190.

[3] A. Ross, R. Govindarajan, Feature level fusion in biometric systems, Proceedings of Biometric Consortium Conference2004, pp. 2.

[4] J.F. Yang, X. Zhang, Feature-level fusion of fingerprint and finger-vein for personal identification, Pattern Recognition Letters, 33 (2012) 623-628.

[5] K. Lin, F. Han, Y. Yang, Z. Zhang, Feature level fusion of fingerprint and finger vein biometrics, Advances in Swarm Intelligence, (2011) 348-355.

[6] A. Lumini, L. Nanni, Advanced methods for two-class pattern recognition problem formulation for minutiae-based fingerprint verification, Pattern Recognition Letters, 29 (2008) 142-148.

[7] C.B. Yu, H.F. Qin, Y.Z. Cui, X.Q. Hu, Finger-vein image recognition combining modified hausdorff distance with minutiae feature matching, Interdisciplinary Sciences: Computational Life Sciences, 1 (2009) 280-289.

[8] K. Nandakumar, A.K. Jain, Multibiometric template security using fuzzy vault, 2nd IEEE International Conference on Biometrics: Theory, Applications and Systems2008, pp. 1-6.

[9] N.K. Ratha, S. Chikkerur, J.H. Connell, R.M. Bolle, Generating cancelable fingerprint templates, IEEE Transactions on Pattern Analysis and Machine Intelligence, 29 (2007) 561-572.

[10] S. Chikkerur, N.K. Ratha, J.H. Connell, R.M. Bolle, Generating Registration-free Cancelable Fingerprint Templates, Biometrics: Theory, Applications and Systems, 2008. BTAS 2008. 2nd IEEE International Conference on2008, pp. 1-6.

[11] A.B.J. Teoh, Y.W. Kuan, S. Lee, Cancellable biometrics and annotations on BioHash, Pattern Recognition, 41 (2008) 2034-2044.

[12] Z. Jin, A. Teoh, T. Ong, C. Tee, A revocable fingerprint template for security and privacy preserving, KSII Transaction on Internet and Information System, 4 (2010) 1327-1342.

[13] C. Lee, J. Kim, Cancelable fingerprint templates using minutiae-based bit-strings, Journal of Network and Computer Applications, 33 (2010) 236-246.

[14] S. Wang, J. Hu, Alignment-free cancellable fingerprint template design: a densely infinite-to-one mapping (DITOM) approach, Pattern Recognition, 45 (2012) 4129-4137.

[15] W. Yang, J. Hu, S. Wang, J. Yang, Cancelable Fingerprint Templates with Delaunay Triangle-Based Local Structures, Cyberspace Safety and Security, Springer2013, pp. 81-91.

[16] S. Wang, J. Hu, Design of alignment-free cancelable fingerprint templates via curtailed circular convolution, Pattern Recognition, 47 (2014) 1321-1329.

[17] S. Wang, J. Hu, A blind system identification approach to cancelable fingerprint templates, Pattern Recognition, 54 (2016) 14-22.

[18] S. Wang, W. Yang, J. Hu, Design of Alignment-Free Cancelable Fingerprint Templates with Zoned Minutia Pairs, Pattern Recognition, 66 (2017) 295-301.

[19] A.M. Canuto, F. Pintro, J.C. Xavier-Junior, Investigating fusion approaches in multi-biometric cancellable recognition, Expert Systems with Applications, (2012).

[20] P.P. Paul, M. Gavrilova, Multimodal Cancelable Biometrics, Cognitive Informatics & Cognitive Computing (ICCI* CC), 2012 IEEE 11th International Conference on, IEEE2012, pp. 43-49.

[21] Y. Chin, T. Ong, A. Teoh, K. Goh, Integrated biometrics template protection technique based on fingerprint and palmprint feature-level fusion, Information Fusion, 18 (2014) 161-174.

[22] C. Rathgeb, M. Gomez-Barrero, C. Busch, J. Galbally, J. Fierrez, Towards cancelable multi-biometrics based on bloom filters: a case study on feature level fusion of face and iris, Biometrics and Forensics (IWBF), 2015 International Workshop on, IEEE2015, pp. 1-6.

[23] D. Mulyono, H.S. Jinn, A study of finger vein biometric for personal identification, International Symposium on Biometrics and Security Technologies2008, pp. 1-8.

[24] W. Yang, J. Hu, S. Wang, A Finger-Vein Based Cancellable Bio-cryptosystem, Network and System Security, Springer2013, pp. 784-790.

[25] N. Miura, A. Nagasaka, T. Miyatake, Feature extraction of finger-vein patterns based on repeated line tracking and its application to personal identification, Machine Vision and Applications, 15 (2004) 194-203.

[26] S.J. Xie, S. Yoon, J. Yang, Y. Lu, D.S. Park, B. Zhou, Feature component-based extreme learning machines for finger vein recognition, Cognitive Computation, 6 (2014) 446-461.

[27] Š.V.N. Pave˘si´c, The complete gabor-fisher classifier for robust face recognition, EURASIP Journal on Advances in Signal Processing, 2010 (2010) 26.

[28] T. Savič, N. Pavešić, Personal recognition based on an image of the palmar surface of the hand, Pattern Recognition, 40 (2007) 3152-3163.

[29] A.T.B. Jin, D.N.C. Ling, A. Goh, Biohashing: two factor authentication featuring fingerprint data and tokenised random number, Pattern Recognition, 37 (2004) 2245-2255.

[30] M. Gomez-Barrero, E. Maiorana, J. Galbally, P. Campisi, J. Fierrez, Multi-biometric template protection based on Homomorphic Encryption, Pattern Recognition, 67 (2017) 149-163.

[31] Fingerprint Verification Competition 2002, http://bias.csr.unibo.it/fvc2002.

[32] Fingerprint Verification Competition 2004, http://bias.csr.unibo.it/fvc2004.

[33] VeriFinger, S. D. K. Neuro Technology (2010), VeriFinger, S. D. K. Neuro Technology.

[34] Y. Yin, L. Liu, X. Sun, SDUMLA-HMT: a multimodal biometric database, Biometric Recognition, (2011) 260-268.

[35] D. Maio, D. Maltoni, R. Cappelli, J.L. Wayman, A.K. Jain, FVC2004: Third fingerprint verification competition, Biometric Authentication, Springer2004, pp. 1-7.

[36] E. Kreyszig, Advanced engineering mathematics, John Wiley & Sons2010.

[37] F. Quan, S. Fei, C. Anni, Z. Feifei, Cracking cancelable fingerprint template of Ratha, Computer Science and Computational Technology, 2008. ISCSCT'08. International Symposium on, IEEE2008, pp. 572-575.

[38] C. Li, J. Hu, Attacks via record multiplicity on cancelable biometrics templates, Concurrency and Computation: Practice and Experience, (2013).

[39] J. Wang, J. Sun, X. Zhang, D. Huang, M. Fejer, Ultrafast all-optical three-input Boolean XOR operation for differential phase-shift keying signals using periodically poled lithium niobate, Optics letters, 33 (2008) 1419-1421.

[40] I. Vajda, L. Buttyán, Lightweight authentication protocols for low-cost RFID tags, Second Workshop on Security in Ubiquitous Computing–Ubicomp2003.