5-31-2021

A cancelable biometric authentication system based on feature-adaptive random projection

Wencheng Yang
Edith Cowan University

Song Wang

Muhammad Shahzad

Wei Zhou

10.1016/j.jisa.2020.102704
This is an author's accepted manuscript of: Yang, W., Wang, S., Shahzad, M., & Zhou, W. (2021). A cancelable biometric authentication system based on feature-adaptive random projection. *Journal of Information Security and Applications, 58*, article 102704. https://doi.org/10.1016/j.jisa.2020.102704

A Cancelable Biometric Authentication System Based on Feature-Adaptive Random Projection

Wencheng Yang[a,*], Song Wang[b], Muhammad Shahzad[b], Wei Zhou [c]

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 Computer and Information Security, Guilin University of Electronic Technology, China*

Abstract: Biometric template data protection is critical in preventing user privacy and identity from leakage. Random projection based cancelable biometrics is an efficient and effective technique to achieve biometric template protection. However, traditional random projection based cancelable template design suffers from the attack via record multiplicity (ARM), where an adversary obtains multiple transformed templates from different applications and the associated parameter keys so as to assemble them into a full-rank linear equation system, thereby retrieving the original feature vector. To address this issue, in this paper we propose a feature-adaptive random projection based method, in which the projection matrixes, the key to the ARM, are generated from one basic matrix in conjunction with local feature slots. The generated projection matrixes are discarded after use, thus making it difficult for the adversary to launch the ARM. Moreover, the random projection in the proposed method is performed on a local-feature basis. This feature-adaptive random projection can mitigate the negative impact of biometric uncertainty on recognition accuracy, as it limits the error to part of the transformed feature vector rather than the entire vector. The proposed method is evaluated on four public available databases FVC2002 DB1-DB3 and FVC2004 DB2. The experimental results and security analysis show the validity of the proposed method.

Keywords: Biometric authentication, template protection, random projection, cancelable biometrics.

1. Introduction

Nowadays biometric recognition systems are widely deployed for authentication purposes, such as biometric sensors mounted on smartphones or other devices. Compared with traditional password- or token-based authentication, biometrics uses physical traits, such as fingerprint, face and iris, to provide identification or verification, overcoming the drawbacks of traditional authentication methods [1]. Although biometric systems own many desirable benefits, e.g., convenience and good security, biometric data are vulnerable and may cause serious privacy and identity threats if compromised. When the biometric data are acquired by an adversary, they are

* Corresponding author.
Email addresses: w.yang@ecu.edu.au (Wencheng Yang); song.wang@latrobe.edu.au (Song Wang); m.shahzad@latrobe.edu.au (Muhammad Shahzad); weizhou09@gmail.com (Wei Zhou)

lost forever, because biometric information is intrinsically linked to a person's identity and cannot be changed or reissued like passwords or tokens.

Due to security and privacy concerns, it is critically important to protect biometric template data stored in biometric recognition systems. One straightforward method for biometric template protectionn is to use standard encryption, e.g., DES (Data Encryption Standard) and AES (Advanced Encryption Standard), which employ a secret key to encrypt the template data in the enrollment stage and decrypt them in the verification stage [2]. However, this allows the template data to be recovered in case the secret key is stolen. To resolve the issue, generally there are two techniques: biometric cryptosystems and cancelable biometrics [3]. In a biometric cryptosystem, biometric data are bound with a cryptographic key to generate a biometric template in a secure manner. Even if the stored template is compromised, the cryptographic key and original biometric data cannot be revealed. In contrast, cancelable biometrics, which relies on a non-invertible transformation, converts the (original) biometric template data into an irreversible version. If the transformed version is compromised, it can be revoked and replaced by simply changing the transformation parameters [4]. Compared with cancelable biometrics, biometric cryptosystems are not equipped with revocability and the recognition performance of these systems is limited, because the error correction code requires specific data formats, e.g., binary data for the hamming distance and discrete data for the set difference [5]. That is why cancelable biometric systems are currently a research topic of great interest.

Among various one-way transformation, random projection is a popular privacy-preserving tool to generate revocable biometric templates, e.g., [6-11]. In a random projection based method, template protection is achieved by projecting the original template feature vector into another feature vector of fewer dimensions, which is also known as many-to-one mapping. The projection is guided by a projection matrix, which is created with the help of a user-specific key. Unlike standard encryption methods, e.g., AES, which assume that these parameters, e.g., user-specific keys, are secret [12], in biometrics, the user-specific key and all other transformation parameters are assumed to be public. For the reason that usually transformation parameters are kept in a token, it is called a token-stolen scenario if the token is compromised. As storing these parameters has the same security concern as storing the original template data, it is desirable that the disclosure of these parameters does not threaten system security, especially the security of template data.

In this paper, we propose a new biometric authentication system to secure biometric template data with the feature-adaptive random projection, where projection matrices are generated according to local feature slots and discarded after use. The proposed method belongs to the category of cancelable biometrics and can prevent original template data from being retrieved, even if the user-specific key is lost. When template data are secure, user identity is safe, which ensures that personal data or sensitive information stored in mobile phones or other devices can only be accessed by legitimate users.

The rest of the paper is organized as follows. Section 2 reviews the related work of state-of-the-art random projection based cancelable biometric systems. The motivation and contributions of this work are presented in Section 3. The proposed system is detailed in Section 4. In Section 5, the experiment results and analysis are given. Finally, the conclusion can be found in Section 6.

2. Related Work

The notion of cancelable biometrics was first introduced by Ratha et al. [13] in 2001 and they subsequently developed cancelable fingerprint templates through cartesian, polar and functional transformations [14]. Since then, cancelable template design has flourished, among which random projection based methods are effective and high-performing. In the realm of random projection based cancelable biometrics, BioHashing is one of the well-known methods, initiated by Teoh et al. [15]. In this method, the authors devised a user-specific random projection algorithm and a discretization process to generate a binary vector, leading to a cancelable template. Specifically, given a feature vector Γ, which is extracted from a biometric image, e.g., fingerprint, a user-specific transformation matrix r is randomly generated, associated with a USB token or smartcard. The matrix r is further processed to be an orthonormal matrix r' by applying the Gram-Schmidt process. Then the inner product of the feature vector Γ and matrix r' is computed, i.e., $x = r'\Gamma$. The resultant vector x is quantized into binary values of b_i=1, if $x \geq t$, and b_i=0, if $x < t$, where t is a predefined threshold, usually specified to be 0. Teoh et al. [16] made more improvements to the original BioHashing scheme using random multispace quantization (RMQ), which extends the single random subspace formulation to multiple subspaces. The information content and robustness of the generated template are increased by RMQ.

Pillai et al. [17] proposed sector-based random projection to overcome the issue of varying quality in different parts of an iris. The low-quality region tends to corrupt the data of the good-quality region if random projection is applied to the whole iris image. By dividing the iris into many sectors and applying random projection to each sector separately, the negative effect of the low-quality region is restricted locally. Pillai et al. [18] introduced an iris recognition framework based on random projection and sparse representation. Random projection together with random permutation is employed to enable revocability, while sparse representation is used for iris image selection. Jin et al. [19] developed a cancelable fingerprint template based on two-dimensional random projection using a minutia local structure called minutia vicinity decomposition (MVD). The MVD feature vector is represented by a matrix of size $N \times 36$, where N is the number of minutia vicinity extracted from a fingerprint sample.

Wang and Hu [20] designed alignment-free cancelable biometric templates, featured by the densely infinite-to-one mapping (DITOM), which is essentially random projection. The DITOM describes the intersection of a set of hyperplanes. Wang and Hu [4] developed a blind system identification approach to protecting binary fingerprint feature vectors. The security of original fingerprint features is theoretically guaranteed when the identifiability condition is not met in blind system identification. Wang et al. [21] applied the partial Hadamard transform to fingerprint template protection. The discrete Fourier transform (DFT) is first taken to spread the spectrum of the sparsely distributed binary biometric feature vectors. Then the partial Hadamard transform is performed on the post-DFT samples, guided by a user-specific matrix. This can be regarded as a variant of random projection, since it achieves the same effect of random projection. Jindal et al. [22] protected face templates using the deep convolutional neural network (CNN) with random projection. A feature vector is first extracted from each face image with a pre-trained Visual Geometry Group (VGG)-Face CNN. Then the extracted feature vector is transformed using random projection, which reduces its dimension from 4096 to 1599. In this way, the redundancy in the feature vector can be removed. Meanwhile, the proposed random projection acts as a cancelable transformation.

Kho et al. [23] presented a cancelable fingerprint template based on Permutated Randomized Non-Negative Least Square (PR-NNLS) and applied it to a local structure descriptor called Partial

Local Structure (PLS). The proposed PLS is alignment-free and the PR-NNLS is specially designed for binary-valued fingerprint template data, providing properties such as cancelability and non-invertibility. Sadhya et al. [24] designed the locality sampled code (LSC) to protect iris features. The proposed scheme is based on a locality sensitive hashing (LSH), which is able to hash intra-class features to the same location, while hashing inter-class features to different locations. Trivedi et al. [25] proposed a non-invertible cancellable fingerprint template, of which the features extracted from Delaunay triangulation of minutiae are protected through a user-specific key in the form of a random binary string. The proposed template is revocable and a new (different) template can be created by just changing the user-specific key.

A randomized cuckoo hashing and minHash based cancelable palmprint authentication system was proposed by Li et al. [26]. First, the palmprint feature is extracted by the use of an anisotropic filter and then the extracted binary-valued feature is secured by the randomized cuckoo hashing as the first layer protection. To further improve the unlinkability of the transformed templates, MinHash as the second layer is used to transfer the output of the first layer. A cancelable biometric template called PolyCodes was put forward by Kaur and Khanna in [27]. PolyCodes distorts the original biometric template data by using random polynomial functions. The random polynomial functions can reduce the dimensionality of template data to certain sizes. In this study, the proposed PolyCodes are applied to several different biometric traits, such as thermal face, finger-vein, palm-vein and palmprint. Asaker et al. [28] introduced a cancelable iris biometric recognition system based on salting. Specifically, a synthetic binary string is generated and XORed with the original binary-valued iris data. In this way, the original iris data are protected and the system's recognition performance is not degraded. The revocability of the proposed system is achieved by generating different synthetic binary strings.

In summary, cancelable biometric templates can be constructed by many different methods, such as random projection [19], [20], [21], hashing [26], and salting [28], but they all share the same core idea of converting the original biometric template into a transformed version, making it difficult for an adversary to restore the original template from the transformed one. Cancellable template designs have been applied to biometric features from various traits, e.g., face, iris, and palmprint, to generate different secure biometric systems. In this study, we focus on designing cancellable fingerprint templates based on random projection and address a key challenge, the attack via record multiplicity (ARM), faced by random projection based cancellable biometrics.

3. Motivation and Contributions

3.1. Motivation

In the above-mentioned random projection based cancelable methods, the irreversibility of the many-to-one mapping is guaranteed base on the theory that in a linear system, there are infinite solutions if the linear equation system is non-full-rank [29]. However, if the adversary obtains multiple protected templates generated from the same original feature vector, the projection matrix can be made to be full-rank by concatenating multiple non-full-rank ones. This attack is also known as the attack via record multiplicity (ARM) [30] [31]; readers can refer to [30] and [31] for details of the ARM. We illustrate the ARM attack strategy targeting cancelable templates through a simple example here. From the analysis of the ARM attack, we show that one key element in random projection based cancelable template systems could be used by the attacker to launch the

ARM. To protect this key element, we propose our solution against the ARM.

Here, an example is given to demonstrate how the ARM can threaten the cancelable systems that use many-to-one random project or mapping [32]. Assume that, in application *A*, the original template feature $\mathbf{X}=[x_1,x_2,x_3,x_4,x_5]=[1, 2, 3, 4, 5]$, and the corresponding transformation matrix of it is

$$\mathbf{M}=\begin{bmatrix}2 & 3 & 3\\ 4 & 2 & 5\\ 1 & 4 & 3\\ 3 & 2 & 4\\ 3 & 1 & 2\end{bmatrix}.$$

By the many-to-one projection equation, $\tilde{\mathbf{X}}=\mathbf{XM}$, a transformed template feature is obtained as $\tilde{\mathbf{X}}=[40,32,48]$. In this case, even if $\tilde{\mathbf{X}}$ and $\mathbf{M}$ are known to an adversary, it is hardly possible to find the original template feature $\mathbf{X}$ via Equation (1),

$$\begin{aligned}2x_1+4x_2+x_3+3x_4+3x_5&=40\\ 3x_1+2x_2+4x_3+2x_4+x_5&=32\\ 3x_1+5x_2+3x_3+4x_4+2x_5&=48\end{aligned}\tag{1}$$

The solutions to $\mathbf{X}$ are infinite because the number of variables in Equation (1) is larger than the number of equations, so $\mathbf{X}$ is safe in this case. But, if there is another projection matrix $\mathbf{M}'$ and its corresponding transformed feature $\tilde{\mathbf{X}}'$ are also acquired by the attacker in application *B*, where

$\mathbf{M}'=\begin{bmatrix}3 & 3 & 1\\ 6 & 5 & 1\\ 4 & 2 & 3\\ 2 & 5 & 4\\ 2 & 1 & 4\end{bmatrix}$ and $\tilde{\mathbf{X}}'=[45,44,48]$, then the attacker is able to obtain the Equation (2) below:

$$\begin{aligned}3x_1+6x_2+4x_3+2x_4+2x_5&=45\\ 3x_1+5x_2+2x_3+5x_4+x_5&=44\\ x_1+x_2+3x_3+4x_4+4x_5&=48\end{aligned}\tag{2}$$

By combining the linear equations from both Equations (1) and (2), the attacker will have enough information to uniquely determine the value of $\mathbf{X}$ that is [1, 2, 3, 4, 5].

In the above example, the key is that multiple random projection matrixes are obtained and utilized by the adversary to generate a full-rank linear equation system and launch the ARM. Our proposed solution is based on the observation that if neither $\mathbf{M}$ nor $\mathbf{M}'$ is available to the adversary, then the adversary cannot calculate the original feature vector $\mathbf{X}=[x_1,x_2,x_3,x_4,x_5]$. Therefore, to prevent the transformation matrix from being known by the adversary is a feasible solution to combating the ARM.

3.2. Contributions

In this paper, we propose a new cancelable biometric authentication system using a

feature-adaptive random projection method to provide user authentication while protecting biometric template data against the ARM. The main contributions of this paper are as follows:

1. In the proposed method, the generation of the projection matrix for performing random projection is feature-adaptive. In other words, the projection matrix is generated from one basic matrix together with a number of vectors extracted from local feature slots. With a different feature slot, the generated projection matrix is different. Moreover, the projection matrixes after usage will be discarded. In this way, the adversary is unable to obtain enough information to launch the ARM, which is a clear advantage over traditional random projection based schemes.

2. In many existing random projection schemes, the random projection is carried out on the whole feature vector. Instead, in the proposed method, the random projection is performed locally on feature slots, each of which is part of the feature vector. By this means, any inaccuracy or errors are localised rather than affecting the entire transformed feature vector. Obviously, this is different to the traditional random projection based cancelable template design and an improvement over the existing methods.

3. The proposed method has good compatibility. No matter how feature data are extracted from whatever biometric traits, e.g., face, finger-vein, iris, as long as they are in the binary format, the proposed method is applicable. This allows the proposed method to be exploited by biometric authentication systems in general, e.g., face or fingerprint recognition systems, thus benefiting applications in different scenarios.

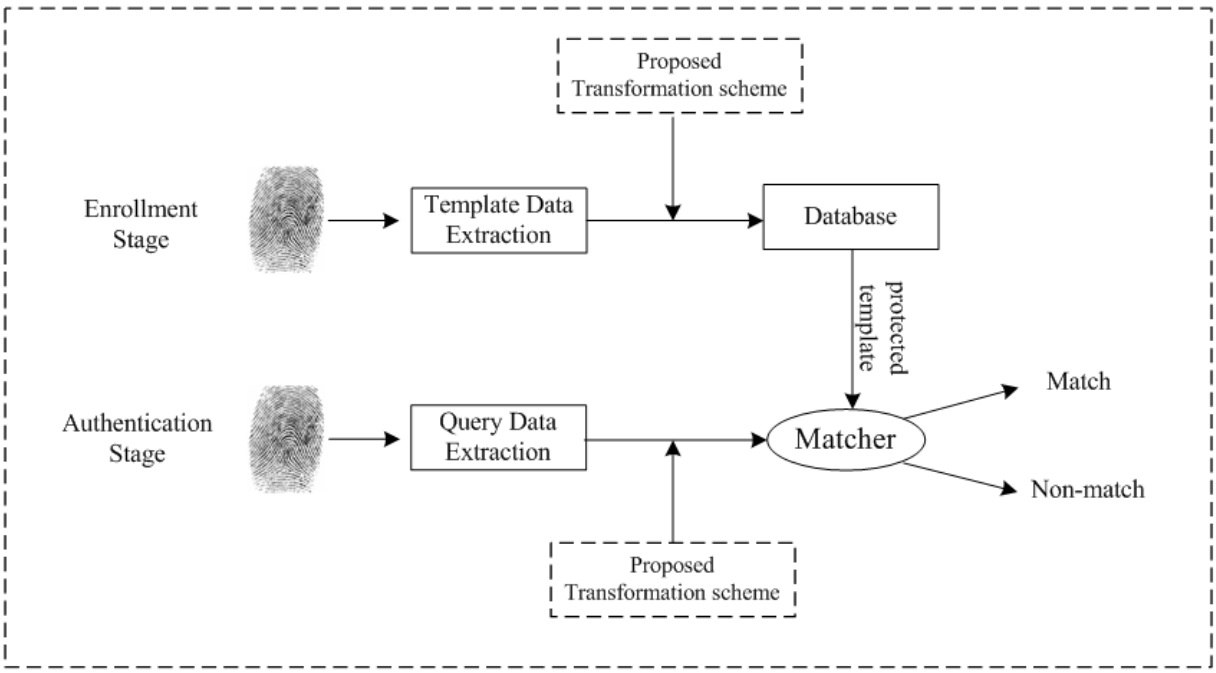

Fig. 1. An overview of the proposed cancelable biometric authentication system (adapted from [3]).

4. Proposed System

An overview of the proposed cancelable biometric authentication system is illustrated in Figure 1. The proposed system comprises three major steps, namely, stable biometric feature extraction, feature data protection with feature-adaptive random projection and matching in the encrypted domain, detailed as follows.

4.1. Stable Biometric Feature Extraction

The first step is to extract stable biometric features. The contribution of this work is not to design a new feature descriptor. Instead, we focus on proposing a feature-adaptive random projection based template protection scheme, which can be applied to a general binary-valued biometric feature descriptor. To this end, an existing fixed-length, minutia-based feature descriptor, named minutia pair (MP), is adopted in this work. The initial version and the variant of the MP descriptor used in this work can be found in our previous work [20] and [33], respectively. In this section, we briefly describe this minutia descriptor; interested readers can refer to [33] for more details.

Given any two minutiae $m_i = \{x_i, y_i, \theta_i, t_i\}$ and $m_j = \{x_j, y_j, \theta_j, t_j\}$ from a minutia set, a local structure can be constructed as shown in Figure 2. The feature vector to express this local structure is $V_{ij} = L_{ij} \| \alpha_i \| \alpha_j \| t_i \| t_j$, where L_{ij} represents the length of the line connecting minutiae m_i and m_j; α_i and α_j are the angles between the orientation of minutiae m_i, m_j and the line segment in the counter-clockwise direction, respectively; t_i and t_j are the minutia types of minutiae m_i and m_j, respectively. To accommodate biometric uncertainty such as elastic distortion, the feature vector V_{ij} is further quantized with suitable quantization step sizes set for L_{ij}, α_i and α_j, respectively. The values of t_i and t_j are binary, where '0' represents ridge ending and '1' ridge bifurcation, so no quantization is needed for t_i and t_j. A binary feature vector $\mathbf{b}$ can be obtained through a similar quantization and treating procedure in [33]. Then, we protect $\mathbf{b}$ using the proposed feature-adaptive random projection method (see details in Section 4.2) and perform matching in the encrypted domain (see details in Section 4.3).

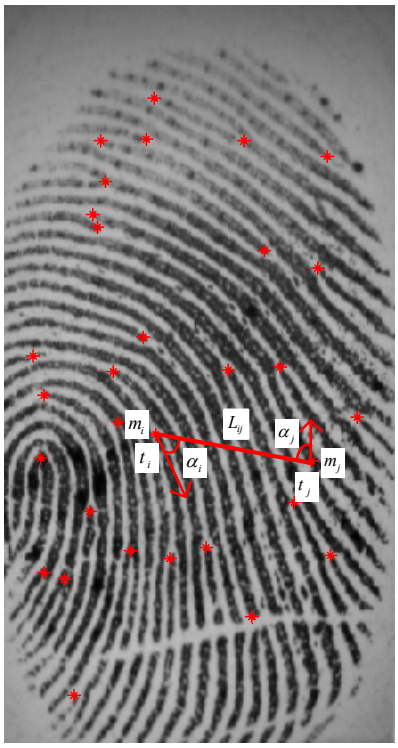

Fig. 2. An illustration of a local minutia structure - minutia pair (MP). (adapted from [33])

4.2. Feature Data Protection Using Feature-Adaptive Random Projection

To secure the extracted biometric feature data, as discussed in Section 4.1, in this section, a feature-adaptive random projection based transformation method is proposed. The entire transformation process of the proposed method is demonstrated in Figure 3. We enhance the random projection in such a way that the projection matrices must adapt to biometric local feature slots and be discarded after use. This makes it difficult for the adversary to figure out the actual projection matrices and to launch the ARM. The steps of the proposed method are detailed as follows.

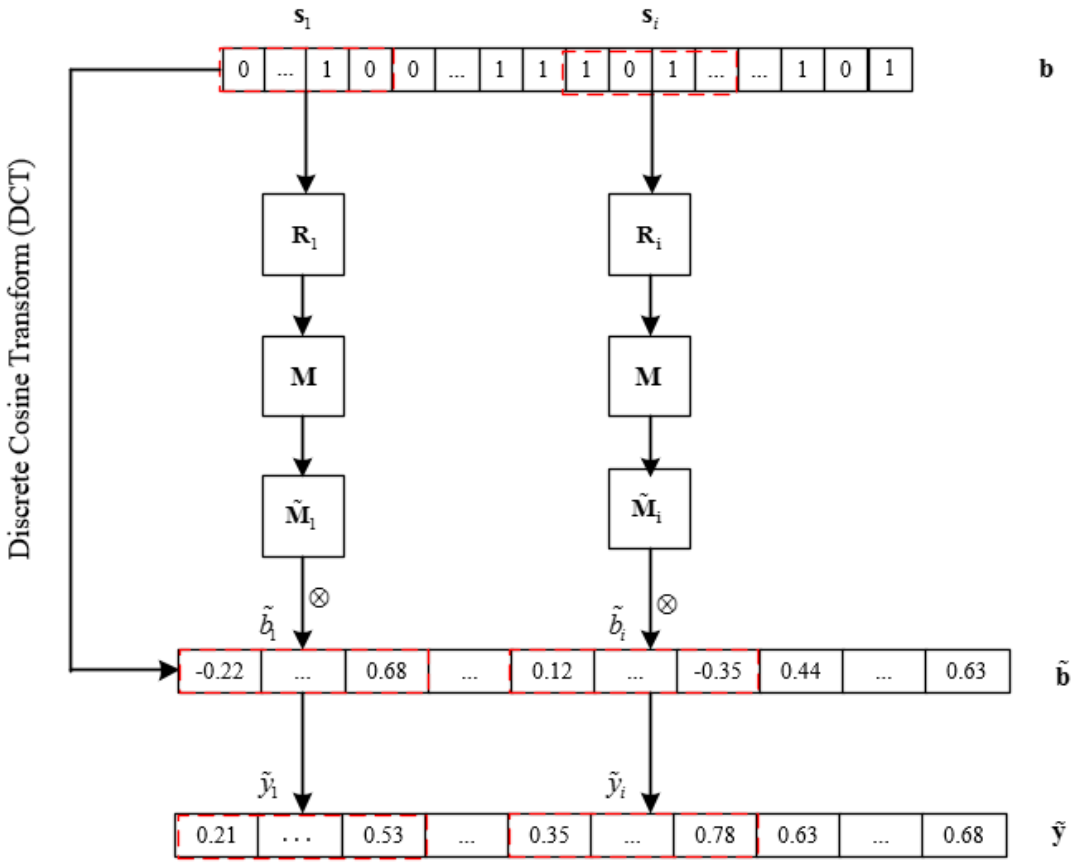

Fig. 3. The proposed feature-adaptive random projection based transformation

Suppose the extracted binary feature vector $\mathbf{b} = [0,1,...,0,0]$ of length l is derived from the feature extraction process conducted on an input biometric image. With a user-specific random projection matrix $\mathbf{M}$, which should have more rows than columns, the conventional random projection in the context of biometric template protection can be expressed by

$$\mathbf{y} = \mathbf{bM} \tag{3}$$

Our objective is to increase the security of the above transformation by altering both the binary feature vector $\mathbf{b}$ and the projection matrix $\mathbf{M}$.

Since the biometric feature vector $\mathbf{b}$ contains only values of 0 and 1, and is usually sparsely distributed, it might make the search space for the solution of $\mathbf{b}$ narrow, when $\mathbf{y}$ and $\mathbf{M}$ in Equation (3) are both acquired by the attacker. To address this problem, we first apply the Discrete Cosine Transform (DCT) to the binary-valued feature vector $\mathbf{b}$, i.e., $\tilde{\mathbf{b}} = DCT(\mathbf{b})$ before performing random projection. The DCT transfers $\mathbf{b}$ from a binary-valued feature vector into the real-valued feature vector $\tilde{\mathbf{b}}$, and therefore randomness and the search space are increased, making it harder for the attacker to deal with the random projection and restore $\mathbf{b}$. Note that the purpose of taking the DCT prior to the random projection is not to attain the property of non-invertibility in that the

DCT is invertible [33]. Non-invertibility is realized by the subsequent feature-adaptive random projection. The DCT simply transforms the binary vector $\mathbf{b}$ to the real vector $\tilde{\mathbf{b}}$.

To alter projection matrix $\mathbf{M}$, we adapt it to $\tilde{\mathbf{M}}_i$ under the help of a set of feature-specific matrices $\mathbf{R}_i$, generated from local feature slots $\mathbf{s}_i$, where i is the slot number. When random projection is performed, we use the feature-adapted projection matrix $\tilde{\mathbf{M}}_i$ in a slot-by-slot manner instead of the fixed matrix $\mathbf{M}$. We call this local feature projection. After local feature projection is done, the projection matrix $\tilde{\mathbf{M}}_i$ is discarded. Although $\mathbf{M}$ is a user-specific parameter key stored in the database, it is hard for the adversary to work out $\tilde{\mathbf{M}}_i$ from $\mathbf{M}$. So ARM can be defended; see security analysis in Section 5.4.

We now describe local feature projection in detail. Let matrix $\mathbf{M}$ of size $j \times q$ be user-specific with j>q. We divide the binary feature vector $\mathbf{b}$ into p slots and each slot contains j elements (here $p \times j = l$), denoted by $\mathbf{b} = \mathbf{s}_1 \| ... \| \mathbf{s}_i \| ... \| \mathbf{s}_p$. The i^{th} slot of $\mathbf{b}$ can be written as $\mathbf{s}_i = [s_{i\_1}, ..., s_{i\_j}]$, where $i \in [1, p]$. The vector $\mathbf{s}_i$ and its slot number i are used as the seed and input into a random number generator (RNG), $rand(\cdot)$, which outputs a real-valued, slot-feature related matrix $\mathbf{R}_i$ of size $j \times q$, i.e.,

$$\mathbf{R}_i = rand(\mathbf{s}_i, i) \tag{4}$$

The RNG function $rand(\cdot)$ can be any generic random number generator; for example, the well-known linear congruential generator, which is defined by the recurrence relation $X_{n+1} = aX_n \bmod m$, where m is the modulus, a is the multiplier and X_0 is the seed [34]. The size of matrix $\mathbf{R}_i$ is the same as that of $\mathbf{M}$, namely $j \times q$. Since $\mathbf{s}_i$ is used as part of the seed for $rand(\cdot)$, if any of the j elements in $\mathbf{s}_i$ are changed, then the generated $\mathbf{R}_i$ are totally different. Therefore, the slot length j of vector $\mathbf{s}_i$ is an important parameter, which impacts the system's recognition performance and thus needs careful tuning; see detailed discussion in Section 5.

Once $\mathbf{R}_i$ is generated, it is treated as a kernel and used to alter the user-specific key, matrix $\mathbf{M}$ as follows:

$$\tilde{\mathbf{M}}_\mathbf{i} = f(\mathbf{R}_i, \mathbf{M}) \tag{5}$$

where function $f(\cdot)$ calculates the average of two corresponding elements from $\mathbf{R}_i$ and $\mathbf{M}$. By this means, matrix $\mathbf{M}$ is adapted to becoming $\tilde{\mathbf{M}}_\mathbf{i}$, which is of the same size as $\mathbf{M}$ but with different elements. We use $\tilde{\mathbf{M}}_\mathbf{i}$ as the projection matrix to transform $\tilde{b}_i$, which is the i^{th} slot of the post-DCT feature vector $\tilde{\mathbf{b}} = \tilde{b}_1 \| ... \| \tilde{b}_i ... \| \tilde{b}_p$. Through this feature-adaptive random projection process, the feature slot $\tilde{b}_i$ is transformed to $\tilde{y}_i$, i.e.,

$$\tilde{y}_i = \tilde{b}_i \tilde{\mathbf{M}}_i \tag{6}$$

In regards to $\tilde{b}_i$ of length j, the above feature-slot based random projection produces a size-reduced vector $\tilde{y}_i$ of length q. Moreover, for security reasons, the feature-adapted projection matrix $\tilde{\mathbf{M}}_i$ is

discarded after use. After applying Equation (6) to each of the p slots in $\tilde{\mathbf{b}} = \tilde{b}_1 \| ... \| \tilde{b}_i ... \| \tilde{b}_p$, we concatenate the p outputs to form the vector $\tilde{\mathbf{y}} = \tilde{y}_1 | ... \| \tilde{y}_i \| ... \| \tilde{y}_p$, which is the transformed and protected feature vector.

4.3. Matching under Encrypted Domain

In accordance with the proposed feature data protection in Section 4.2, once the transformed feature vectors $\tilde{\mathbf{y}}^T$ and $\tilde{\mathbf{y}}^Q$ are obtained from the template and query images, respectively, matching is conducted in the encrypted domain. Here, superscript T represents 'template', while Q represents 'query'. The similarity score between $\tilde{\mathbf{y}}^T$ and $\tilde{\mathbf{y}}^Q$ is given by the following equation [35],

$$S(\tilde{\mathbf{y}}^T, \tilde{\mathbf{y}}^Q) = 1 - \frac{\| \tilde{\mathbf{y}}^T - \tilde{\mathbf{y}}^Q \|_2 \text{ ^2}}{\| \tilde{\mathbf{y}}^T \|_2 \text{ ^2} + \| \tilde{\mathbf{y}}^Q \|_2 \text{ ^2}} \tag{7}$$

where $\|.\|_2$ denotes the 2-norm. The similarity score $S(\tilde{\mathbf{y}}^T, \tilde{\mathbf{y}}^Q)$ after processing is in the range of [0, 1], where 0 means two feature vectors are completely different, while 1 means they are the same.

Remarks: (i) A binarization procedure is applied to the MP descriptor. Binarization is a quantization technique, which can lessen feature differences caused by biometric uncertainty. The binary feature slot $\mathbf{s}_i$ is part of the seed to generate $\mathbf{R}_i$; see Equation (4). As analyzed in Section 4.2, any change in the elements of $\mathbf{s}_i$ would cause $\mathbf{R}_i$ to be different. Therefore, the binarization procedure is important and indispensable. That is why we choose the MP descriptor, which is a binary feature representation. (ii) To generate $\mathbf{R}_i$, we need the feature slots $\mathbf{s}_i$, but they come from the original binary feature vector $\mathbf{b}$, so it is likely to result in the same $\mathbf{R}_i$ in different applications. This presents a risk of the cross matching attack [36]. To address this, a key-guided permutation function $perm(\cdot)$ can be applied to the original binary feature vector $\mathbf{b}$, e.g., $perm(\mathbf{b}, k_{indx})$, where k_{indx} is a permutation index key and is application-dependent, set differently in different applications.

5. Experimental results and analysis

5.1. Experimental Results

In this section, the proposed system is evaluated over four public fingerprint databases FVC2002 DB1-DB3 [37] and FVC2004 DB2 [38] and compared with the state-of-the-art methods,. The details of these four databases are given in Table 1. Fingerprint minutiae are extracted by using the commercial software package, VeriFinger [39]. We applied the proposed feature-adaptive random projection method to secure the MP-based feature representation, which we call S_MP to ease notation. The binary feature representation is produced by the MP descriptor, as explained in Section 4.1. For the RNG, we adopted the built-in function $rand(\cdot)$ in MATLAB.

Table 1. Detailed information of fingerprint databases [40]

Databases	FVC2002 DB1	FVC2002 DB2	FVC2002 DB3	FVC2004 DB2
Resolution (dpi)	500	569	500	500
Number of fingers	100	100	100	100
Number of images per finger	8	8	8	8
Sensor type	Optical	Optical	Capacitive	Optical
Image size	388×374	560×296	300×300	328×364
Image quality	Medium	Medium	Medium to low	Low

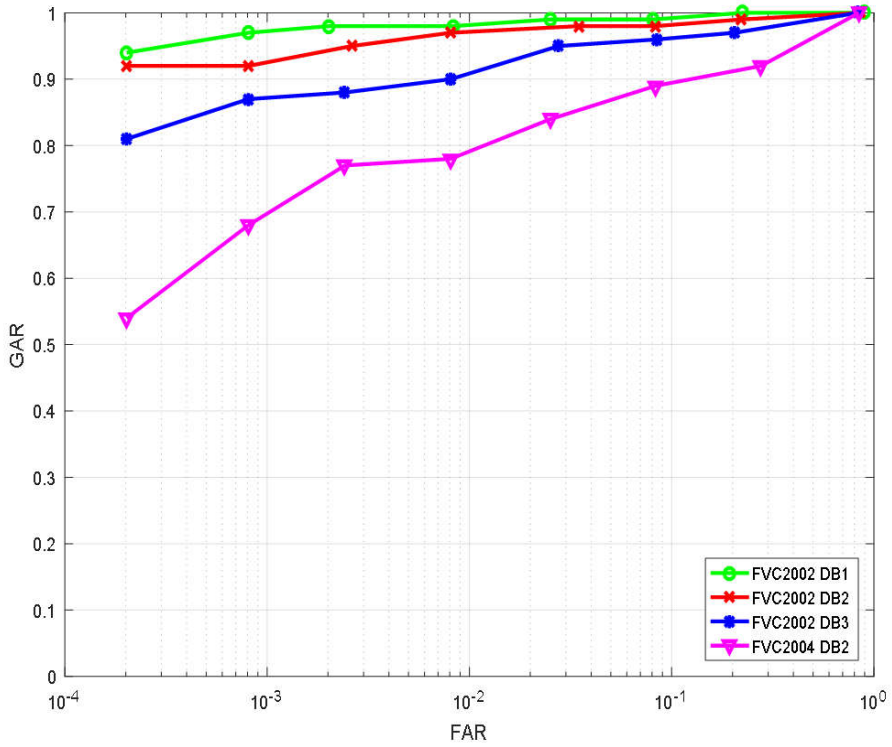

Fig. 4. The ROC curves of the protected system S_MP.

To evaluate the recognition performance of the proposed system, we employ several commonly used performance indices. They are the false rejection rate (FRR), false acceptance rate (FAR), genuine acceptance rate (GAR) and equal error rate (EER). Clearly, FRR+GAR=1. The EER is the error rate when FAR=FRR. The standard 1vs1 matching protocol [41] in the literature is used in our experiments. Specifically, the first fingerprint image of each finger is compared with the second fingerprint image of the same finger to obtain the FRR or GAR. The first fingerprint image of each finger is compared with the first fingerprint image of the remaining (other) fingers in the database to calculate the FAR.

(1) *System performance using different parameter settings*: In the proposed method, the binary feature vector $\mathbf{b}$ is divided into a number of slots $\mathbf{s}_i$ of equal length. The length j of each slot affects the system's recognition performance. The proposed system is tested using different slot lengths and the corresponding recognition performance in terms of the EER is given in Table 2. From Table 2, it can be seen that when the slot length j increases, the EER of S_MP deteriorates on databases FVC2002 DB1 and FVC2004 DB2, while no obvious trend is found on the other two databases (FVC2002 DB2 and DB3). Moreover, we observe that under the optimal parameter setting, S_MP performs best on database FVC2002 DB1 with EER=1.00% and performs worst on database FVC2004 DB2 with EER=11.00%. This is because the fingerprint image quality of FVC2004 DB2 is much worse than that of FVC2002 DB1. The Receiver Operating Characteristic (ROC) of S_MP under the best parameter setting is also plotted in the lost-key scenario, as demonstrated in Figure 4, where it shows that the FAR increases with the GAR.

Table 2. The system's recognition performance in terms of the EER(%) with different slot lengths

Slot length, j	**2002DB1**	**2002DB2**	**2002DB3**	**2004DB2**
10	1.00	2.46	4.00	11.00
15	1.00	2.00	7.00	11.00
20	1.05	4.20	6.00	12.11
25	4.00	2.82	7.08	15.00
30	4.00	3.00	7.00	15.43

The parameter q is fixed to be 5 in the experiment.

(2) *Performance comparison with similar existing methods*: Similar to most existing cancelable biometric methods, the proposed method is evaluated in the lost-key scenario, which is the worst case in practice. The recognition performance comparison of the proposed system with the existing random projection based methods in terms of the EER is reported in Table 3. It can be seen from Table 3 that our system S_MP levels with the method in [21] to achieve equal best performance on FVC2002 DB1 and DB2, whereas S_MP performs best on FVC2002 DB3 and FVC2004 DB2. It is worth pointing out that apart from the satisfactory performance of S_MP, the proposed method is invulnerable to the ARM, which many existing random projection based cancelable biometric systems cannot compete with.

Table 3. Comparison of recognition performance in terms of the EER (%) under the lost-key scenario

Methods	**FVC2002 DB1**	**FVC2002 DB2**	**FVC2002 DB3**	**FVC2004 DB2**
Jin et al. [19]	3.07	1.02	-	-
Jin et al. [42]	4.36	1.77	-	21.82
Das et al. [43]	2.27	3.79	-	-
Wang and Hu [20]	3.50	4.00	7.50	-
Wang and Hu [4]	3.00	2.00	7.00	-
Wang et al. [21]	1.00	2.00	5.20	13.30
S_MP (proposed method)	1.00	2.00	4.00	11.00

5.2. Revocability

Revocability ensures that a compromised template can be canceled and replaced with a new one generated from the same biometric data [44]. It is one of the basic requirements for cancelable biometrics. In the revocability test, 50 transformed templates were created from the first image of each finger in FVC2002 DB2 by assigning different keys, e.g., different $\mathbf{M}$ and different permutation index key k_{indx}. This leads to 5000 (=50×100) new templates totally. The first template was matched against the rest 49 templates generated from the same finger, so there was a total of 4900 comparisons in this pseudo-imposter test. The score distribution of the test is plotted in Figure 5, from which it can be seen that the score distribution almost overlaps with that of the imposter test with different keys for each different finger. It demonstrates that the transformed templates of the same fingerprint are uncorrelated.

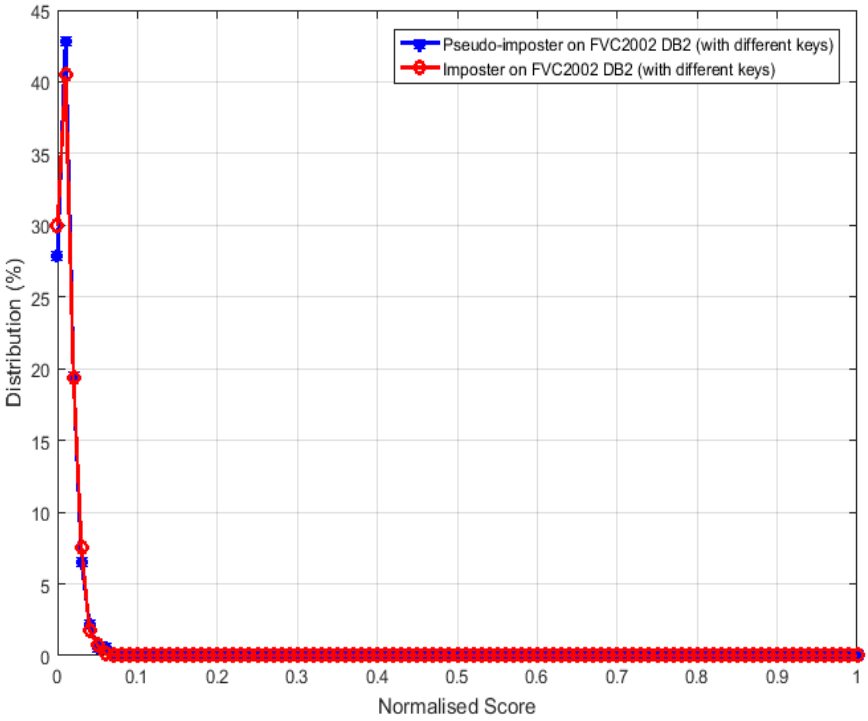

Fig. 5. The imposter and pseudo-imposter distributions for the revocability test using S_MP.

5.3. Unlinkability

Unlinkability ensures that cancelable templates produced from a same finger to be used in different applications do not cross-match. Recently, a general framework was proposed by Gomez-Barrero et al. [45] to evaluate the unlinkability of a system at local and global levels. This framework uses two types of score distributions, namely mated and non-mated sample score distributions. In the mated score distribution, each score is computed by comparing two templates generated from a same impression using different keys. Non-mated scores are acquired by

matching templates which are obtained from different fingers using different keys. Using these score distributions, we can compute local linkability or score-wise linkability, $D_{\leftrightarrow}(s)$ and system's overall linkability or global linkability, $D_{\leftrightarrow}^{sys}$. Score-wise linkability $D_{\leftrightarrow}(s)$ determines the linkability of the system for each score s in both mated and non-mated score distributions, while $D_{\leftrightarrow}^{sys}$ provides a system's overall linkability. With local linkability, if $D_{\leftrightarrow}(s)$=0, then two templates are considered fully unlinkable; otherwise, if $D_{\leftrightarrow}(s)$=1, the two templates are considered fully linkable. Similarly, the global indicator $D_{\leftrightarrow}^{sys} \in [0,1]$, with 0 meaning a fully unlinkable system and 1 a fully linkable system. Practically, both $D_{\leftrightarrow}(s)$ or $D_{\leftrightarrow}^{sys}$ have values between 0 and 1, which demonstrate a certain degree of local or global linkability. The unlinkability analysis of the proposed system was conducted on FVC2002 DB2. To compute the mated scores, we transformed the first impression of each finger using 50 different user keys. By doing so, we obtained 5000 (=50×100) templates. The first transformed template is compared with the other transformed templates from the same finger, yielding 4900 (=49×100) mated scores. By comparing the transformed template of the first impression of each finger with the first impression of a different finger transformed using different keys, we produced a total of 4950 (=100×99/2) non-mated scores. According to [45], the mated and non-mated score distributions are plotted in Figure 6, where both curves overlap to a great extent with $D_{\leftrightarrow}^{sys}$=0.04. Hence, we can infer that proposed system is almost unlinkable.

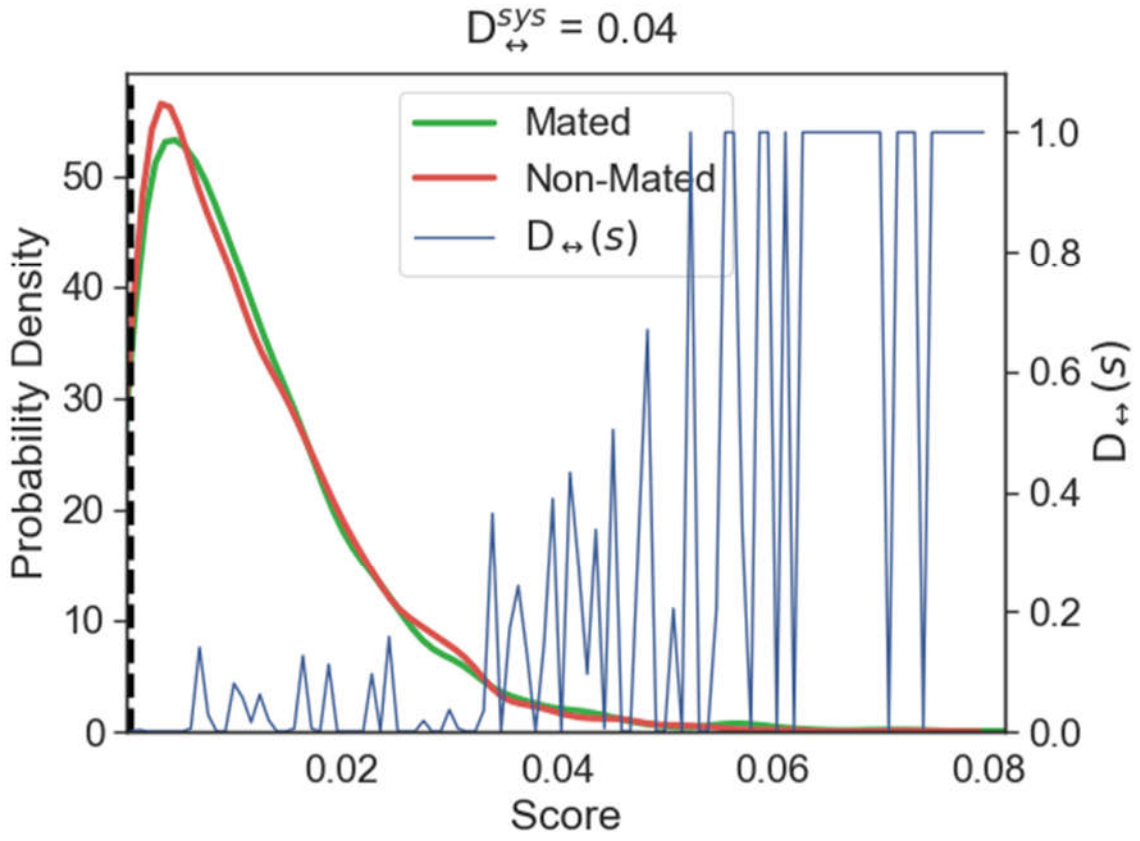

Fig. 6. Unlinkability analysis with mated and non-mated score distributions using S_MP.

5.4. Security Analysis

In this section, we analyze why the proposed method can defend the brute force attack and the ARM. In particular, we show that the proposed method can prevent the adversary reconstructing the original MP features from the resultant cancelable template in the lost-key scenario, where we assume that the adversary acquires the transformed feature vector $\tilde{\mathbf{y}}$, matrix $\mathbf{M}$, the RNG function $rand(\cdot)$ and the permutation index key k_{indx}.

The brute force attack: There is no easy way for the adversary to figure out the original feature vector $\mathbf{b}$ except through exhaustive guessing attempts, namely the brute force attack. In S_MP, the length of the binary feature vector $\mathbf{b}$ is l = 30000 in this work. Assume that there are $m=40$ minutiae in a fingerprint image and the local structure formed by any two minutiae from these 40 minutiae is unique, the number of possible locations of 1s in the binary feature vector $\mathbf{b}$ can be calculated by $\binom{l}{m(m-1)/2}$, which yields an incredibly huge number. Therefore, it is tremendously challenging for the adversary to determine the original feature vector $\mathbf{b}$ from brute force guesses.

The ARM: In this attack, if without using the proposed method, the adversary can utilize multiple compromised templates, e.g., $\mathbf{y}$, together with multiple copies of $\mathbf{M}$, to build a full-rank linear equation system and thus find a unique solution to Equation (3). However, the proposed feature-adaptive random projection method adapts the projection matrix $\mathbf{M}$ in Equation (3) to $\tilde{\mathbf{M}}_i$ in Equation (6) based on local feature slots. The adapted projection matrix $\tilde{\mathbf{M}}_i$ is discarded after each random projection, so it is unavailable and not publicly known. Moreover, the generation of matrix $\mathbf{R}_i$ is dependent on the feature vector $\mathbf{b}$ rather than any other parameters which are assumed to be public in the lost-key scenario. Therefore, the adversary is unable to work out $\tilde{\mathbf{M}}_i$ from $\mathbf{M}$ without the knowledge of the original binary feature vector $\mathbf{b}$. Without knowing $\tilde{\mathbf{M}}_i$, the adversary has no way to recover the original feature vector $\mathbf{b}$ via the ARM.

6. Conclusion

In this paper, a feature-adaptive random projection based cancelable biometric authentication system is proposed to provide user authentication and protect biometric template data simultaneously. The proposed method is applied to the fingerprint minutia feature descriptor MP, where the recognition performance of the protected system S_MP is evaluated on four public fingerprint databases. In the proposed method, projection matrices are generated from local feature slots, thereby adapting the user-specific key $\mathbf{M}$. The adapted projection matrices are discarded after each random projection. Because the attacker has no knowledge about actual projection matrices, he/she is not able to start the ARM even if the user-specific key $\mathbf{M}$ and the transformed feature vectors are both revealed. The proposed method is an enhancement of the existing random projection based cancelable biometric systems, many of which suffer from the ARM. The extensive experiments show that the proposed method achieves competitive recognition performance while protecting biometric template data.

It should be indicated that the performance of the proposed system is affected by the discriminative power of the feature descriptor. In this work, the feature descriptor used is MP. In

addition to MP, some other feature descriptors, such as the Minutia Cylinder-Code (MCC), have been shown to have good stability and discriminatory power [35]. In order to further improve recognition accuracy, applying the proposed scheme to the MCC feature descriptor is worthy of consideration. Furthermore, since the proposed scheme is compatible with any feature descriptor in a binary format, it is a potential research direction to investigate how to apply the proposed method to other biometric systems, e.g., face and/or iris recognition systems.

Acknowledgment

The work of Wei Zhou in this paper was supported in part by the National Natural Science Foundation of China under Grant 61802084.

References

[1] W. Yang, J. Hu, S. Wang, A Delaunay triangle group based fuzzy vault with cancellability, 2013 6th International Congress on Image and Signal Processing (CISP)2013, pp. 1676-1681.
[2] J. Daemen, V. Rijmen, The design of Rijndael: AES-the advanced encryption standard, Springer Science & Business Media2013.
[3] W. Yang, S. Wang, J. Hu, G. Zheng, C. Valli, Security and Accuracy of Fingerprint-based Biometrics: A Review, Symmetry, 11 (2019) 141.
[4] S. Wang, J. Hu, A blind system identification approach to cancelable fingerprint templates, Pattern Recognition, 54 (2016) 14-22.
[5] M. Tarek, O. Ouda, T. Hamza, Robust cancellable biometrics scheme based on neural networks, IET Biometrics, 5 (2016) 220-228.
[6] A.T.B. Jin, Cancellable biometrics and multispace random projections, 2006 Conference on Computer Vision and Pattern Recognition Workshop (CVPRW'06), IEEE2006, pp. 164-164.
[7] S. Chikkerur, N.K. Ratha, J.H. Connell, R.M. Bolle, Generating Registration-free Cancelable Fingerprint Templates, 2008 IEEE Second International Conference on Biometrics: Theory, Applications and Systems2008, pp. 1-6.
[8] A.B.J. Teoh, Y.W. Kuan, S. Lee, Cancellable biometrics and annotations on BioHash, Pattern Recognition, 41 (2008) 2034-2044.
[9] 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.
[10] T. Ahmad, J. Hu, S. Wang, Pair-polar coordinate-based cancelable fingerprint templates, Pattern Recognition, 44 (2011) 2555-2564.
[11] V.M. Patel, N.K. Ratha, R. Chellappa, Cancelable biometrics: A review, IEEE Signal Processing Magazine, 32 (2015) 54-65.
[12] B. Yang, D. Hartung, K. Simoens, C. Busch, Dynamic random projection for biometric template protection, 2010 Fourth IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS), IEEE2010, pp. 1-7.
[13] N.K. Ratha, J.H. Connell, R.M. Bolle, Enhancing security and privacy in biometrics-based authentication systems, IBM Systems Journal, 40 (2001) 614-634.
[14] 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.
[15] 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.
[16] 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 (2006) 1892-1901.
[17] J.K. Pillai, V.M. Patel, R. Chellappa, N.K. Ratha, Sectored random projections for cancelable iris biometrics, IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP), IEEE, Dallas, TX, 2010, pp. 1838-1841.
[18] J.K. Pillai, V.M. Patel, R. Chellappa, N.K. Ratha, Secure and robust iris recognition using random projections and sparse representations, IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, 33 (2011) 1877-1893.
[19] Z. Jin, B.M. Goi, A. Teoh, Y.H. Tay, A two-dimensional random projected minutiae vicinity decomposition-based cancellable fingerprint template, Security and Communication Networks, (2013) 11.
[20] S. Wang, J. Hu, Alignment-free cancellable fingerprint template design: a densely infinite-to-one mapping (DITOM) approach, Pattern Recognition, 45 (2012) 4129-4137.
[21] S. Wang, G. Deng, J. Hu, A partial Hadamard transform approach to the design of cancelable fingerprint templates containing binary biometric representations, Pattern Recognition, 61 (2017) 447-458.
[22] A.K. Jindal, S.R. Chalamala, S.K. Jami, Securing Face Templates using Deep Convolutional Neural Network and Random Projection, 2019 IEEE International Conference on Consumer Electronics (ICCE), IEEE2019, pp. 1-6.
[23] J.B. Kho, J. Kim, I.-J. Kim, A.B. Teoh, Cancelable Fingerprint Template Design with Randomized Non-Negative Least Squares, Pattern Recognition, 91 (2019) 245-260.
[24] D. Sadhya, B. Raman, Generation of Cancelable Iris Templates via Randomized Bit Sampling, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, 14 (2019) 2972 - 2986.
[25] A.K. Trivedi, D.M. Thounaojam, S. Pal, Non-Invertible cancellable fingerprint template for fingerprint biometric, Computers & Security, 90 (2020) 101690.
[26] H. Li, J. Qiu, A.B.J. Teoh, Palmprint template protection scheme based on randomized cuckoo hashing and MinHash, Multimedia Tools and Applications, (2020) 1-25.

[27] H. Kaur, P. Khanna, PolyCodes: generating cancelable biometric features using polynomial transformation, Multimedia Tools and Applications, (2020) 1-24.
[28] A.A. Asaker, Z.F. Elsharkawy, S. Nassar, N. Ayad, O. Zahran, F.E. Abd El-Samie, A novel cancellable Iris template generation based on salting approach, Multimedia Tools and Applications, (2020) 1-25.
[29] W.-H. Steeb, Y. Hardy, Problems and solutions in introductory and advanced matrix calculus, World Scientific Publishing Company2016.
[30] F. Quan, S. Fei, C. Anni, Z. Feifei, Cracking cancelable fingerprint template of Ratha, 2008 International Symposium on Computer Science and Computational Technology, IEEE2008, pp. 572-575.
[31] C. Li, J. Hu, Attacks via record multiplicity on cancelable biometrics templates, Concurrency and Computation: Practice and Experience, 26 (2014) 1593-1605.
[32] W. Yang, Local Structure Based Fingerprint Authentication Systems with Template Protection, University of New South Wales, Canberra, Australia2015.
[33] W. Yang, S. Wang, J. Hu, G. Zheng, C. Valli, A Fingerprint and Finger-vein Based Cancelable Multi-biometric System, Pattern Recognition, 78 (2018) 242-251.
[34] P. L'ecuyer, Tables of linear congruential generators of different sizes and good lattice structure, Mathematics of Computation, 68 (1999) 249-260.
[35] R. Cappelli, M. Ferrara, D. Maltoni, Minutia Cylinder-Code: A New Representation and Matching Technique for Fingerprint Recognition, IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, 32 (2010) 2128-2141.
[36] E.J.C. Kelkboom, J. Breebaart, T.A.M. Kevenaar, I. Buhan, R.N.J. Veldhuis, Preventing the decodability attack based cross-matching in a fuzzy commitment scheme, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, 6 (2011) 107-121.
[37] *Fingerprint Verification Competition 2002*. Available: http://bias.csr.unibo.it/fvc2002
[38] *Fingerprint Verification Competition 2004*. Available: http://bias.csr.unibo.it/fvc2004
[39] *VeriFinger, S. D. K. Neuro Technology*. Available: http://www.neurotechnology.com/verifinger.html
[40] W. Yang, J. Hu, S. Wang, A Delaunay Quadrangle-Based Fingerprint Authentication System With Template Protection Using Topology Code for Local Registration and Security Enhancement, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, 9 (2014) 1179-1192.
[41] M. Ferrara, D. Maltoni, R. Cappelli, Non-invertible Minutia Cylinder-Code Representation, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, 7 (2012) 1727-1737.
[42] Z. Jin, M.-H. Lim, A.B.J. Teoh, B.-M. Goi, A non-invertible Randomized Graph-based Hamming Embedding for generating cancelable fingerprint template, Pattern Recognition Letters, 42 (2014) 137-147.
[43] P. Das, K. Karthik, B. Chandra Garai, A robust alignment-free fingerprint hashing algorithm based on minimum distance graphs, Pattern Recognition, 45 (2012) 3373-3388.
[44] Z. Jin, Y.-L. Lai, J.Y. Hwang, S. Kim, A.B.J. Teoh, Ranking Based Locality Sensitive Hashing Enabled Cancelable Biometrics: Index-of-Max Hashing, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, 13 (2017) 393-407.
[45] M. Gomez-Barrero, J. Galbally, C. Rathgeb, C. Busch, General framework to evaluate unlinkability in biometric template protection systems, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, 13 (2017) 1406-1420.