A Revocable Fingerprint Template for Security and Privacy Preserving

Zhe Jin[1], Andrew Beng Jin Teoh[2], Thian Song Ong[1] and Connie Tee[1]
[1] Faculty of Information Science & Technology, Multimedia University
Jalan Ayer Keroh Lama, Bukit Beruang, Melaka, 75450 - Malaysia
[e-mail: jin.zhe@mmu.edu.my]
[2] Electrical and Electronic Engineering Department, Yonsei University
Seoul, 120-749 – South Korea
[e-mail: bjteoh@yonsei.ac.kr]
*Corresponding author: Andrew Beng Jin Teoh

Received July 16, 2010; revised September 4, 2010; accepted September 20, 2010; published December 23, 2010

Abstract

With the wide deployment of biometric authentication systems, several issues pertaining security and privacy of the biometric template have gained great attention from the research community. To resolve these issues, a number of biometric template protection methods have been proposed. However, the design of a template protection method to satisfy four criteria, namely diversity, revocability and non-invertibility is still a challenging task, especially performance degradation when template protection method is employed. In this paper, we propose a novel method to generate a revocable minutiae-based fingerprint template. The proposed method consists of feature extraction from fingerprint minutiae pairs, quantization, histogram binning, binarization and eventually binary bit-string generation. The contributions of our method are two fold: alignment-free and good performance. Various experiments on FVC2004 DB1 demonstrated the effectiveness of the proposed methods.

Keywords: Template protection, minutiae pair representation, helper data, privacy

A preliminary version of this paper appeared in ICINT 2010, June 22-24, Shanghai, China. This version includes a detailed description of the proposed method and a concrete demonstration on security and privacy through experiments.

DOI: 10.3837/tiis.2010.12.020

1. Introduction

Biometric system is an attractive alternative to conventional knowledge and possession based identity authetication approaches that has been widely deployed recently [1]. However, the biometric system also suffers from many inherent risks. For example, biometrics is permanently associated with the user, subsequently, once a biometric compromised, it is compromised forever.

Recently, cancelable or revocable biometrics as a biometric template protection technique has been proposed to address the above mentioned problem [1][2]. Cancelable or revocable biometrics refers to an irreversible transform of the biometric template which preserves the security and privacy of the actual biometric information. Hence, instead of the original biometric data, only the transformed templates are stored in the user database. If a cancelable biometric feature is compromised, a new template can be re-generated from the same biometrics. Theoretically, a template protection method must fulfill the following requirements [3]:

1. **Diversity**: No same cancelable template can be used in two different applications.
2. **Reusability**: Straightforward revocation and reissuance in the event of compromise.
3. **One-way transformation**: Non-invertibility of template computation to prevent recovery of biometric data.
4. **Performance**: The formulation should not deteriorate the recognition rate.

In this paper, we propose a novel method to generate revocable fingerprint binary templates from minutiae pairs. The proposed method offers a reasonable recognition rate and it is alignment free. Besides, various experiments are conducted to evaluate the performance, revocability, diversity and non-invertibility of the proposed method.

The organization of this paper is as follow: in Section 2, we briefly describe recent works in the cancelable fingerprint template. Our proposed method is presented in Section 3. The experimental results and analysis are presented in Section 4. Discussion and conclusion are given in Section 5 and Section 6 respectively.

2. Related Work

Here, we provide a brief review of literatures on cancelable/revocable fingerprint methods which is based on minutiae representation. Among these methods, we broadly divide them into two categories, alignment-based and alignment-free categotries.

For the alignment-based category, a registration point (core or delta) is required to align the minutiae coordinates. For instance, Ratha et al. [4] described three transformation methods, Cartesian, polar and surface folding transformation. The Cartesian and polar transformation methods divided a fingerprint into sub-blocks and then scrambled them. In the surface folding transformation, which is the best among the three, a mixture of 2D Gaussians and 2D electric potential field random charge distributions are used to translate the minutiae points. A minimal effect on the error rate can be achieved as the transformation is locally smooth. However, all the three methods required accurate alignment before transformation.

Although the above transformation functions were claimed to be non-invertible due to many-to-one mapping property, the work reported by Feng et al. [5] successfully degenerated the Ratha's surface folding transforms when the transformed template and parameters are known to the attacker. Their experiments showed that approximately 90% of the original

minutiae can be inferred. Meanwhile, Shin, et al. [6] showed that the surface folding transform could be inverted if two transformed templates that are originated from the same fingerprint are compromised.

Ang et al. [7] proposed a key-dependent transformation method to generate cancelable fingerprint templates from fingerprint minutiae. In this method, a core point need to be determined at the beginning and a line through the core point is specified. The line orientation, which defined in the range of 0 and 180 is determined by the key transformation function. However, it is not always feasible to determine the accurate core point location. Moreover, the minutiae above the line are reflected symmetrically, the transformed template still retains some information of the original template.

Han et al. [8] generated Personal Identification Numbers (PINs) from five minutiae closet to the core point of fingerprint. The PIN consists of two parts: a six-digit binary number and a three-digit decimal integer. In their method, a fictitious triangle with three longest lines connecting two minutiae is constructed. The maximal side, the minimal and medial angles as well as the minutiae type are extracted as the feature set and convert to the PINs by using an error-tolerant transform.

Nagar et al. [9] described a scheme to extract binary features from fingerprint using minutia points and fingerprint ridges. They developed the method based on the cuboid-based feature extraction algorithm proposed by Sutcu et al. [10]. In this method, three minutiae-based features are extracted, namely aggregate wall distance, minutiae average and minutiae deviation from each randomly chosen cuboidal regions. Furthermore, the ridge orientation and ridge wavelength have been utilized to form a much richer fingerprint feature set. This feature set is finally binarized into a bit-string. A bits-selection method is used to select the most discriminant bits to form a final template. This method offers a high accuracy; however, it requires the use of the registration points.

In contrast to the alignment-based approach, no registration point is needed in the alignment-free approach. Tulyakov et al. [11] presented a method that hashes fingerprint minutiae information and performs fingerprint matching in the hashed domain. Given n minutia points $\{c_1, c_2, ..., c_n\}$, m symmetric hash functions are constructed. It is computationally hard to reconstruct the original features with resultant hash values due to one-way transformation characteristic of hashing function. User can re-enroll a new hash function to generate new hash values when the old hash values are compromised. Hence both non-invertibility and reusability requirements are satisfied. For the performance, the method achieved 3% of EER in the best case; however, this is slightly less accurate than the baseline system that is 1.7% of EER.

Farooq et al. [12] generated a bit-string from fingerprint minutiae representation based on minutiae triplets. The seven invariant features: the length of three sides, the three angles between the sides and minutiae orientations and the height of the triangles were extracted, quantized and hashed into bit-string (2^{24} bits). However, this method required calculating all the possible triple invariant features which results in higher computation costs.

Lee et al. [13] proposed a cancelable fingerprint template using fingerprint minutiae. The invariant was then used as the inputs for user-specific transformation function (changing functions) which output translational and rotational parameters to transform each minutia. The cancelable fingerprint templates were generated by changing each minutia according to the said parameters. In case the cancelable fingerprint template is compromised, the new template can be reissued by changing the transformation functions. However, the performance of this method degraded when the quality of the fingerprints is poor. It is because the invariant values for moving minutia were extracted from the orientation information around each minutia [15].

Jin et al. [14] proposed a minutiae-based fingerprint template protection method using random triangle hashing approach. The random triangle hashing is applied to the minutia to generate a hash vector. Then the bit-block mechanism is employed to convert the hash vector into a bit-string. The use of random triangle hash is to ensure that the generated template is computationally hard to be inverted. However, this method consumes undesirable computation time.

Recently, Lee et al. [15] proposed a cancelable fingerprint template in bit string using fingerprint minutiae. Firstly, a 3 dimensional array is pre-defined and a number of tessellations contain in the pre-defined 3D array is determined by the quantization level. Secondly, one of a minutia is selected as reference minutiae and other minutiae are translated and rotated based on this reference minutiae. The transformed minutiae are fallen into each specific tessellation according to the x-axis, y-axis and orientation. Then, each tessellation is marked to 1 if it contains more than one minutia and otherwise 0, a bits-string is generated sequentially by visiting the tessellation in the 3D array. The resultant bits-string is permuted using user-specific PIN to achieve revocability. The recognition rate is highly encouraging in different PINs situation. However, in the duplicated PINs scenario, the template is unsecure.

3. Proposed Method

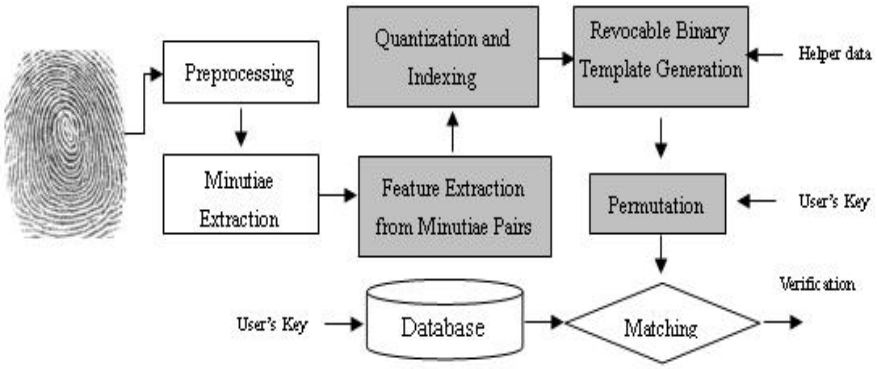


Fig. 1. The proposed revocable fingerprint template protection method

In this section, we present a novel alignment-free transformation method to generate a revocable minutiae-based fingerprint binary bit-string as a template. Given a set of minutiae points, $m_i = \{x_i, y_i, \theta_i\}$, where x_i , y_i and θ_i represent the coordinate and the orientation of the *i*-th minutiae. We first derive a set of the minutiae pairs from a set of minutiae points. Then invariant features are extracted from the derived minutiae pairs and are further processed through quantization, histogram binning and binarization and eventually a binary bit-string. After that, by incorporating the helper data that is generated from the resultant bit-strings, a key-specific permutation procedure is used to generate a revocable and non-invertible binary bit-string as template. In case when a template is compromised, a different key can be used to reissue a different binary bit-string as template. **Fig. 1** depicts the overall revocable fingerprint template protection method.

3.1 Feature Extraction from Minutiae Pairs

The invariant features derived from the minutiae pairs were inspired by the work of Parziale and Niel [16]. A single minutiae point suffers from the elastic deformation from fingerprint to fingerprint. However, the change of a minutiae pair formed by two minutiae points is not

evident under rigid transformation. Besides that, minutiae pairing provides certain degree of immunity against noise due to the use of redundant combinations of two minutiae points. The four invariant features used are:

1. The distance L between the two minutia, where L is measured in pixel units;
2. The angle α between the orientation of the two minutiae (angular difference between O_1 and O_2), the range of the angle α is $(0,2\pi]$ and O_1 and O_2 represent the orientation of minutiae m_1 and m_2 respectively;
3. The angles β_1 and β_2 between the orientation of each minutia and the segment connecting them, the range of β_1 and β_2 is $(0,\pi]$.

Fig. 2 demonstrates the invariant features extracted from a minutia pair formed by minutia m_1 and m_2. Besides, the detailed generation of fingerprint's bit-string from minutiae pairs is given in the **Fig. 3**.

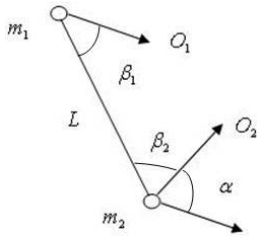


Fig. 2. Invariant features extraction from minutiae pair

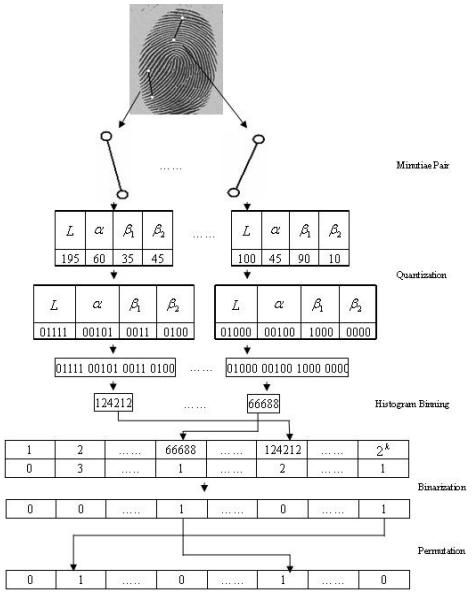


Fig. 3. Generating fingerprint binary representation from minutiae pair

3.2 Quantization

Due to the distortion occurred during the image capturing process, the invariant features are quantized to alleviate this problem. Assume that the maximum distance, *L*, between two

minutiae is l pixels, we quantize L into q segments with each segment containing l/q pixels for each quantization step. To represent these q segments in binary form, $\log_2(l/q)$ bits are required.

Similarly, assume that the maximum angle between the orientations of two minutiae is 2π, and we set the quantization step to be p, thus $\lfloor 2\pi / p \rfloor$ bits are required to represent the angle between the orientations of the two minutiae, α. The same procedure applies to the remaining features, i.e. β_1 and β_2.

After determining the number of bits required to represent each feature, we are in place to quantize the feature into binary form. The feature value is quantized based on the index of the segment it falls in. Each segment is labelled by a binary decimal code. If L is represented by l bits, angle α by a bits, angle β_1 by b_1 bits and β_2 by b_2 bits, then every minutiae pair can be represented by a bit string with length l_{mp} bits, where $l_{mp} = l + a + b_1 + b_2$. The bit string is then converted to its corresponding integer, such as 01111 00101 0011 0100 to 124212, as shown in Fig. 3.

The same procedure is repeated to all the minutiae pairs found in the fingerprint image. In general, there are $s = {}^{n}C_2 = \frac{1}{2}n(n-1)$ possible combinations of the minutiae pairs that can be generated from a fingerprint image, where n is the number of minutiae in an image.

3.3 Histogram Binning and Bit-string Generation

Since there are $2^{l_{mp}}$ possible combinations of bits for each minutiae pair, a histogram m_i is formed to count the number of minutiae pairs that fall in each of the disjoint bins in the histogram. Mathematically, the histogram binning function is given as follows:

$$s = \sum_{i=1}^{2^{l_{mp}}} m_i \tag{1}$$

where s is the total number of minutiae pair for all $2^{l_{mp}}$ of bins, $2^{l_{mp}}$ is the total number of bins. Next, we binarize the histogram m_i by retaining the count of value 1 while setting the rest of the count values to 0. This is to ensure that the fingerprint image can be represented by a set of unique minutiae pairs, i.e. occur only once in the fingerprint image. The binarization rule is given as follow:

$$\forall i \in [0, 2^{l_{mp}}), \quad b_i = \begin{cases} 0 & if\ m_i \neq 1, \\ 1 & otherwise \end{cases} \tag{2}$$

3.4 Transformation of Binary String: Permutation

Next, the resultant binary bit-string that represents the unique minutiae pairs will be used as the transformed fingerprint template. However, it is undesirable to store this template in the database due to privacy concern. Therefore, a transformed version of the binary bit-string is used as the user template. The said transformation is the permutation that is based on a user-specific token, which is uniquely assigned to each individual. The user-specific token guarantees that the fingerprint presented for verification is permuted in the same manner as the one enrolled for the same users and in different manner for different users.

3.5 Generating Helper Data

Since helper data is generated from the transformed templates, it contains highly discriminative feature for different users. Effectively, it expands the inter-class variation and assists in enhancing the recognition rate. In this context, 5 out of 8 images are selected as the training samples. To avoid statistical bias, we test all the possible combinations which are ${}^{8}C_{5}$ times and calculated the average equal error rate (EER). During the training process, we adopt majority voting to render a set of helper data for a user. The value in every position in the helper data is based on the majority count of the training data. **Fig. 4** shows the majority voting scheme to generate helper data with permutation. In order to ensure computational efficiency, an integer vector that contains the index position of the bit-string with the value '1' (instead of the entire bit-string) is stored as helper data in database. During verification, the permuted template will be updated by taking the integers of stored helper data to find the index of the permuted template and set the value of this position to 1.

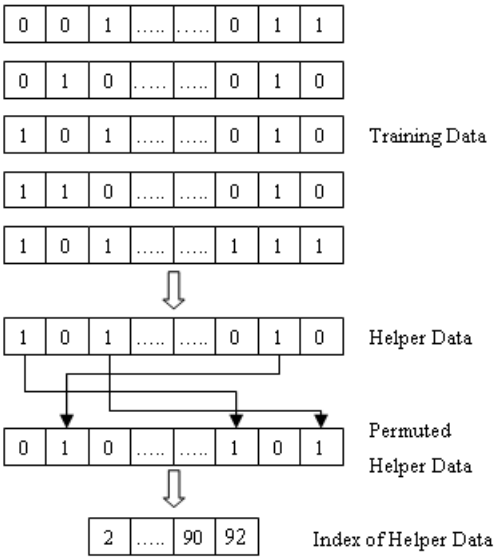


Fig. 4. Generation of helper data

3.6 Similarity Distance Metric

Assume that B^E represents an enrolled binary template and B^Q represents the query binary template, the similarity matching score can be calculated as follows:

$$33\, S(B^E, B^Q) = \frac{\sum_{i=1}^{n}\left(B_i^E \bullet B_i^Q\right)}{\sqrt{\sum_{i=1}^{n} B_i^E \sum_{i=1}^{n} B_i^Q}} \tag{3}$$

where $\bullet$ represents a bit-wis3e AND operator. $\sum_{i=1}^{n}\left(B_i^E \bullet B_i^Q\right)$ counts the positions in the binary strings that have a value 1 in both enrolled and query templates and sum them up.

$\sum_{i=1}^{n} B_i^E$ and $\sum_{i=1}^{n} B_i^Q$ denote the total number of 1's of the enrolled and query templates. The score ranges from 0 to 1 where a '1' indicates a perfect match and otherwise.

4. Experimental Results

A well-known public database, FVC2004 (DB1) [17], is used to evaluate the proposed method. This dataset contains 100 fingers and each finger has 8 fingerprint images. False accept rate (FAR), false reject rate (FRR) and equal error rate (EER) are used as the performance metrics in our experiments. We perform experiments in the plain verification (different token) as well as in other scenarios, i.e. lost token, lost helper data etc. The experiments on the tuning of parameters and comparison between existing methods and our method are also showed in the ROC figures.

4.1 Quantization

In general, proper quantization step is sensitive to slight distortions, while too large or too small quantization step results in the loss of discriminative power of the invariant features. We conduct experiments to evaluate the effect of different levels of quantization, p and q, as described in section 3.2 where L is set to 400 pixels. We select the different bit length, ie. l_{mp} = 10 bits, 14 bits, 18 bits and 22 bits, respectively to represent a minutiae pair and observe the results on accuracies. Fig. 5 shows the effect of different levels of quantization on the accuracies. We observed that the performance increases when large number of bits is used. However the performance level off at around 18 bits and degrades when 22 bit is used to represent a minutiae pair. Therefore, we conclude that the performance peaks when a length of 18 bits is used to represent a minutiae pair and the length of 18 bits is constructed by a length of 5 bits for distance L, a length of 5 bits for the difference of orienation angle α, a length of 4 bits for β_1 and β_2 as shown in Table 1.

Table 1. Quantization for the invariant features

Features	Bits	Segments	Quantum
L	5	$2^5 = 32$	$\frac{400}{2^5} = 12.5$ pixels
α	5	$2^5 = 32$	$\frac{360}{2^5} = 11.25$ degree
β_1	4	$2^4 = 16$	$\frac{180}{2^4} = 11.25$ degree
β_2	4	$2^4 = 16$	$\frac{180}{2^4} = 11.25$ degree

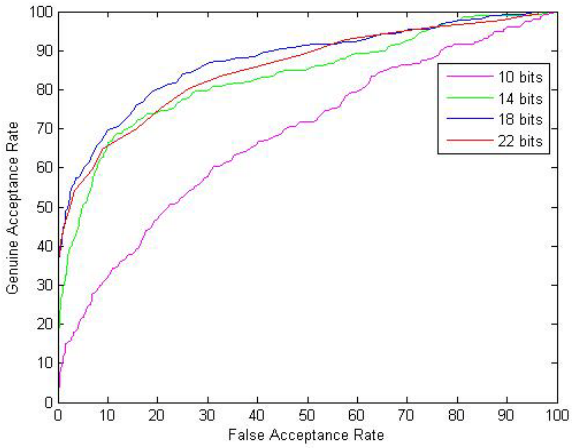


Fig. 5. Receiver Operating Curve (ROC) for effecting of different quantization levels on the accuracy (length in pixels and angles in degrees)

4.2 Performance

In the two-factor authentication system [3], the performance is not only evaluated in different token case where either token or helper is not lost, but also in lost token cases as lost-token attack is a security threat. Similarly, in our proposed method, we consider the following scenarios: 1) plain verification; 2) lost of external token only; 3) lost of helper data only.

4.2.1 Plain Verification

In this experiment, we assume that the helper data and external token are not lost. An external token is assigned to each individual in the database and it is different from individual to individual. The purposes of having this external token are to: 1) enable revocability; 2) permute the user's template. The performance in this experiment is ideal (the EER is close to 0). This is due to the fact that the bit-string that we generated has an order property. Therefore after permutation, the dissimilarity between different users increased tremendously. **Fig. 6** and **Fig. 7** show the genuine and imposter distributions, which represent the dissimilarity between same users and different users, respectively, and also the FAR/FRR curves.

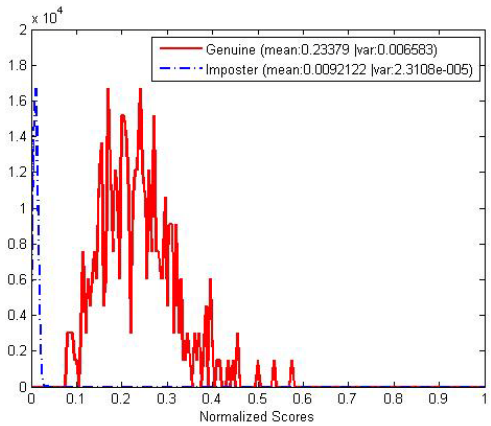


Fig. 6. Genuine & imposter distributions with different tokens

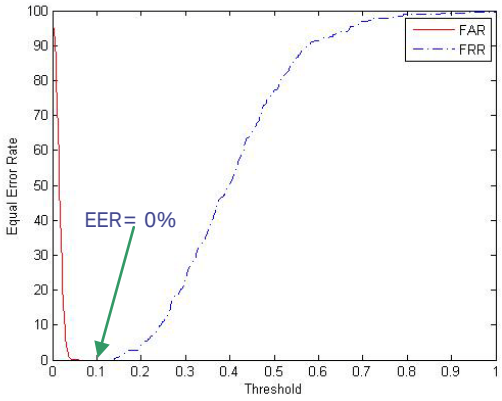


Fig. 7. Equal error rate with different tokens

4.2.2 Lost-token Attack

Lost-token attack occurs when a genuine user lost his/her token and an imposter has gained this token to perform verification. The lost of token implies all the potential adversaries gain this token so that we simulate this situation by using the same external token for all the users. By comparing the templates from all the 100 users with the same external token, we achieved approximately 3% equal error rate as shown in the **Fig. 8** and **Fig. 9**. This experiment implies that we can obtain an acceptable security guarantee if some impostor has the stolen key to access the system.

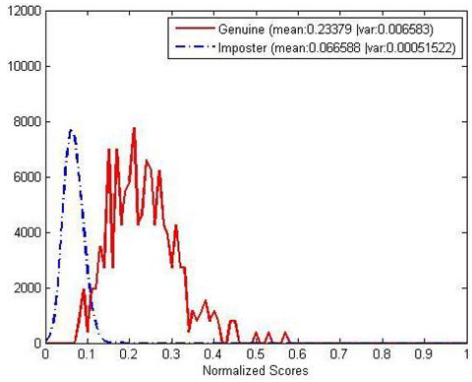


Fig. 8. Genuine and imposter distributions with same token scenario

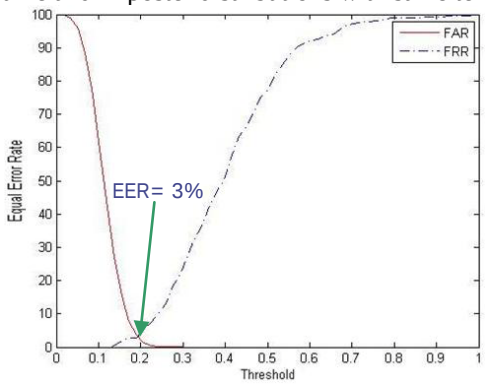


Fig. 9. Equal error rate with same token scenario

4.2.3 Lost Helper Data Attack

Similarly, we performed an experiment for the lost helper data scenario by using the same helper data for all the users. The experiment shows that although the helper data has been revealed, the combined strength provided by the fingerprint and token still can distinguish the genuine and impostor. In this case, the EER that we obtained from the experiments is around 1%, as depicted in **Fig. 10** and **Fig. 11**.

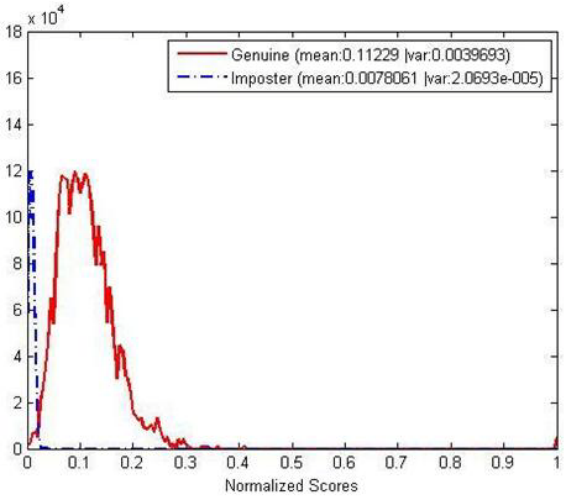


Fig. 10. Genuine & imposter distributions in lost helper data case

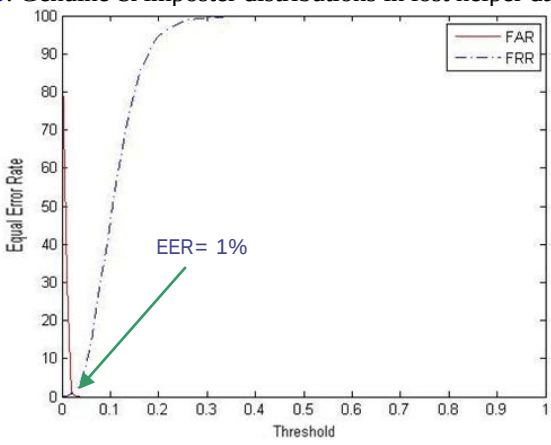


Fig. 11. Equal error rate in lost helper data case

4.3 Performance Comparison

In this section, our proposed technique is compared with Farooq's scheme [12] and Lee's scheme [15] based on FVC2004 DB1. As illustrated in **Fig. 12**, our method outperforms both Lee's and Farooq's scheme. Moreover, our template requires a length of 2^{18} bits which is much lesser than the length of Farooq's template at 2^{24}. Lee's scheme has lower complexity and high accuracy. However, the template may not be secure when the PINs are lost. To address the problem that occurred in Lee's scheme, we propose the use of helper data to resolve the performance in the stolen token case.

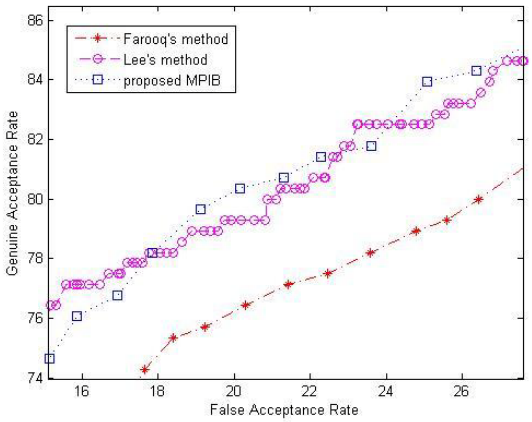


Fig. 12. ROC curve for comparison between proposed MPIB with Farooq's scheme and Lee's scheme

4.4 Revocability

In revocable biometric systems, once the templates are compromised, a new transformed template can be generated. Ideally, the new transformed templates should be completely different from the compromised templates. Meanwhile, the performance of using the new template should not degrade much as compared to the compromised templates. In this experiment, we generated 2880 binary templates that permuted by 2880 different permutation factors/external tokens. The templates were matched to each other for generating the scores so called pseudo-imposter. In **Fig. 13**, a significant overlap between imposter (see section 4.2.1 for imposter distribution generation) and pseudo-imposter distribution can be observed which implied the pseudo-imposter templates are essentially similar to imposter templates. As such when a template is compromised, the new template generated is never matched with other templates stored in database.

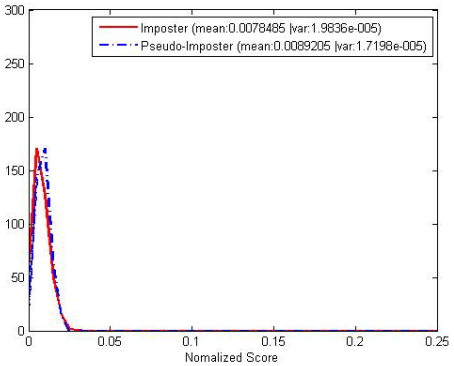


Fig. 13. Scores distribution for imposter & pseudo-imposter

4.5 Security Analysis

The binary template stored in database is a permuted version of the original template so that an adversary require on average $\sim 2^{18}!$ attempts to reconstruct the original template, which is computational infeasible in practice. Even in the worst case that an adversary gains both the transformed template and token and further successfully reconstruct the original binary template. However, the original binary template is merely a set of unique minutiae pairs which

does not provide any means of minutia information.

5. Discussions

In the proposed method, apart from a plain verification scenario, we also performed experiments in two scenarios: 1) lost of external token; 2) lost of helper data. In the lost external token case, the experiment shows that an EER of approximately 3% could be achieved. This satisfactory result was attained due to the binding of template with the helper data which provides strong discriminative power. Therefore, the system could nullify the external token even if the impostor has gained access to it. In the second scenario, we assume the impostor has gained the helper data and try to access the system. The experiment proved that only error rate of about 1% occurred in this case. This result is evident as the external token was used to permute/randomize the template. This treatment led to the change of order in the template and finally results expected performance. **Table 1** summarizes the results obtained in the experiments described in Section 4.2.1, 4.2.2, 4.2.3 and 4.4.

One security threat may occur when both the helper data and external token are lost. It is possible for the imposter to recover the updated bit-string acquired from the majority voting training by using the lost helper data and external token. This updated bit-string contains the user-specific information since it is acquired from the user templates. The impostor may gain access to the system by using the recovered bit-string. To prevent this problem, helper data and token can be stored separately by adapting certain secure cryptographic protocols such as the extension of the Diffie–Hellman protocol, Schnorr signature, and Zheng signcryption protocols, as reported in [18].

Anyway, user privacy is still preserved as the loss helper data and external token will not reveal the original minutiae data. In this context, the transformation of fingerprint into bit-string could be defined as $f \circ g$, where f is a transformation from real into integer space such that $f: R^k \to Q^k$ (using quantization and histogram binning) and $g: Q^k \to (0,1)^k$ (using permutation transformation). Since the range(g)≠domain(f), hence $g \circ f$ is not possible. Note that the transformation of the function g: $\boldsymbol{Q}^k \to (0,1)^2$ will could be regarded as lossy compression in which information will be lost due to the conversion. According to Joy-Thomas, the continuous to discrete entropy list is $\log(2^n)$ based on its segment size n [19]. Hence, the process is irreversible.

Table 2. Equal Error Rate (EER) of the various experiments

Experiment	Section No.	EER (%)
Plain verification	4.2.1	0%
Lost external token	4.2.2	3%
Lost helper data	4.2.3	1%
Revocability	4.4	0%

6. Conclusions

In this paper, we describe a novel method to generate revocable fingerprint binary template. The merits of our method are two folds: alignment-free and good performance. The proposed method is evaluated based on the four requirements of template protection mentioned in Section 1. The experiment shows that performance is ideal in plain verification, lost token and lost helper data scenarios. Besides that, revocability is also achieved as showed in the

experiment (Section 4.4). To address non-invertible property, we proposed a general way to prove that the proposed method gains the non-invertibility due to the lossy compression. We also discussed the security of the proposed method. However, a security threat may happen when both helper data and token are lost that we discussed in Section 5. Moreover, since the helper data generated from user templates, how to protect the helper data that does not leak to adversary is another critical issue in this method.

Acknowledgement

This work was supported by the Korea Science and Engineering Foundation (KOSEF) through the Biometrics Engineering Research Center (BERC) at Yonsei University. (Grant Number: R112002105080020 (2010)).

References

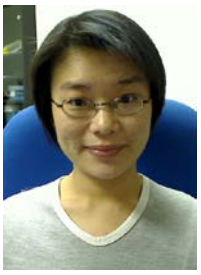
[1] N. K. Ratha, J. H. Connell, R. M. Bolle, “Enhancing security and privacy in biometrics-based authentication systems,” IBM Syst. J., vol. 40, no. 3, pp. 614–634, 2001. Article (CrossRef Link)
[2] http://www.scholarpedia.org/article/Cancelable_biometrics (accessed on 2010.05.31).
[3] Andrew B.J. Teoh, A. Goh, and D.C.L. Ngo, “Random Multispace Quantisation as an Analytic Mechanism for BioHashing of Biometric and Random Identity Inputs,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 28, no. 12, pp. 1892-1901, 2006. Article (CrossRef Link)
[4] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, “Generating Cancelable Fingerprint Templates,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Special Issue on Biometrics, vol. 29, no. 4, pp. 561-572, 2007. Article (CrossRef Link)
[5] Q. Feng, F. Su, A. Cai, F.F. Zhao, “Cracking Cancelable Fingerprint Template of Ratha,” in *Proc. of International Symposium on Computer Science and Computational Technology*, vol. 2, pp. 572-575, 2008. Article (CrossRef Link)
[6] S.W. Shin, M.-K. Lee, D.S. Moon, K.Y. Moon, “Dictionary Attack on Functional Transform-Based Cancelable Fingerprint Templates,” ETRI Journal, vol. 31, no. 5, pp. 628-630, 2009. Article (CrossRef Link)
[7] R. Ang, S.N. Rei, L. McAven, “Cancelable Key-Based Fingerprint Templates,” in *Proc. of 10th Australasian Conf. on Information Security and Privacy*, pp. 242-252, 2005. Article (CrossRef Link)
[8] F.L. Han, J.k. Hu, L.L. He, Y. Wang, “Generation of Reliable PINs from Fingerprints,” in *Proc. of IEEE International Conf. on communication*, pp. 1191–1196, 2007. Article (CrossRef Link)
[9] A. Nagar, S. Rane, A. Vetro, “Alignment and Bit Extraction for Secure Fingerprint Biometrics,” *SPIE Conference on Electronic Imaging*, vol. 7541, pp. 75410N-75410N-14, 2010. Article (CrossRef Link)
[10] Y. Sutcu, S. Rane, J. Yedidia, S. Draper, A, Vetro, “Feature extraction for a slepian-wolf biometric system using ldpc codes,” in *Proc. of International Symposium on Information Theory*, pp. 2297-2301, 2008. Article (CrossRef Link)
[11] S. Tulyakov, F. Farooq, V. Govindaraju, “Symmetric Hash Functions for Fingerprint Minutiae,” in *Proc. of International Workshop on Pattern Recognition for Crime Prevention, Security and Surveillance*, vol. 3687, pp. 30-38, 2005. Article (CrossRef Link)
[12] F. Farooq, R. Bolle, M. Ruud, T. Jea, and N. Ratha, “Anonymous and Revocable Fingerprint Recognition,” in *Proc. of Computer Vision and Pattern Recognition*, pp. 1-7, 2007. Article (CrossRef Link)
[13] C. Lee, J. Choi, K. Toh, S. Lee, and Jaihie Kim, “Alignment-Free Cancelable Fingerprint Templates Based on Local Minutiae Information,” *IEEE Transaction on Systems, Man and Cybernetics, Part B*, vol. 37, no. 4, pp. 980-992, 2007. Article (CrossRef Link)

[14] Z. Jin, A.B.J. Teoh, T. S. Ong, C. Tee, "Secure Minutiae-based Fingerprint Templates Using Random Triangle Hashing," in *Proc. of 1st International Visual Informatics Conf.*, pp. 521-531, 2009. Article (CrossRef Link)
[15] C.H. Lee, J. Kim, "Cancelable fingerprint templates using minutiae-based bit-strings," *J Network Comput Appl*, vol. 33, no. 3, pp. 236-246, 2010. Article (CrossRef Link)
[16] G. Parziale and A. Niel, "A fingerprint matching using minutiae triangulation," In *Proc. of ICBA*, pp. 241-248, 2004. Article (CrossRef Link)
[17] Third International Fingerprint Verification Competition. http://bias.csr.unibo.it/fvc2004/, 2004.
[18] A.B.J. Teoh, and C.T. Yuang, "Cancellable Biometrics Realization with Multispace Random Projections". *IEEE Transaction SMC Part B - Special Issue on Recent Advances in Biometrics Systems*, vol. 37, no. 5, pp. 1096-1106, 2007. Article (CrossRef Link)
[19] T. M.Cover and J. A.Thomas, "*Elements of Information Theory*," John Wiley & Sons, Inc., 1991. Article (CrossRef Link)

Jin Zhe received his Bachelor of Information Technology (Hons) degree in 2007 from Multimedia University of Malaysia. Currently, he is a postgraduate student in Multimedia University. He also works as an assistant lecturer in Faculty of Information Science and Technology at Multimedia University. His research interests cover the areas of biometrics, digital image processing, and pattern recognition.

Andrew Teoh Beng Jin obtained his BEng (Electronic) in 1999 and Ph.D degree in 2003 from National University of Malaysia. He is currently an assistant professor in EE department, college engineering of Yonsei University. He was an associate dean and senior lecturer of Faculty of Information Science and Technology in Multimedia University, Malaysia. His research interest is in biometrics security, watermarking and pattern recognition. He had published around 170 refereed international journal and conference papers in his area.

Ong Thian Song works in Faculty of Information Sciences and Technology (FIST), Multimedia University as a Senior Lecturer. He received his Master of Sciences in 2001 and Ph.D degree in 2008. His research interests include biometrics security, fingerprint recognition and human computer interaction. He also serves as advisory board on Technical Committee for Biometrics Standardization in Malaysia.



Tee Connie received her Bachelor of Information Technology (Hons) degree in 2003 and obtained Master of Science (IT) degree in 2005 from Multimedia University of Malaysia. Currently, she works as a senior lecturer in Faculty of Information Science and Technology at Multimedia University. Her research interests cover the areas of biometrics, computer vision, and pattern recognition.