Alignment-free Cancellable Template Generation for Fingerprint based Authentication

Rumana Nazmul[1], Md. Rafiqul Islam[1] and Ahsan Raja Chowdhury[2]
[1]*Charles Sturt University, Albury, NSW-2640, Australia*
[2]*Federation University Australia, Mount Helen, VIC-3350, Australia*

Keywords: Biometric Authentication, Cancellable Template, Minutia.

Abstract: With the emergence and extensive deployment of biometric based user authentication system, ensuring the security of biometric template is becoming a growing concern in research community. One approach of securing biometric data is cancellable biometric which transforms the original biometric features into a non-invertible form for enrolment and matching. However, most of the schemes for generating cancellable template are alignment-based requiring an accurate alignment of query and enrolled images, which is very difficult to achieve. In this paper, we propose an alignment-free technique for generating revocable fingerprint template that exploits the local features i.e., minutiae details in a fingerprint image. A rotation and translation invariant values are extracted from the neighbouring region of each minutia. The invariant values are then used as inputs in a transformation function and combined with a stored and a user-specific key based random vectors using the type and orientation information of the minutiae. Hence, by varying the stored and user-specific keys in the transformation, multiple application-specific templates can be generated to preserve users' privacy. Besides, if the transformed template is compromised, a new template can be reissued by assigning different keys for transformation to achieve revocability. Furthermore, the proposed approach preserves the actual geometric relationships between the enrolled and query templates even after transformation and offers reasonable recognition rate. Experiments conducted on FVC2000 DB1 demonstrate that the proposed method exhibits promising performance in terms of recognition accuracy, computational complexity, security along with diversity, revocability and non-invertibility that are the key issues of cancellable template generation.

1 INTRODUCTION

Biometrics identifiers, due to the distinctiveness and permanence, have emerged as a convenient and reliable technology to verify the identities of the users. However, there are several vulnerabilities (Wang and Hu, 2012) and challenges in biometric authentication that can lead to numeral security breaches and privacy threats. Due to the strong association between biometric property and the user's identity, once a biometric data is compromised, it results in permanent loss of a subject's biometrics and consequently, the lost biometric trait may cause serious privacy threats (Nagar et al., 2010). Thereby, the revelation of user's privacy is one of the major concerns for biometric template security (Ratha et al., 2007) which drives the motivation of designing an effective and secure method for biometric template protection.

Cancellable biometrics is an approach for template protection that uses transformed biometric data instead of the original one for user identification and thereby ensures security and privacy in biometrics. Although a number of methods for biometric template protection have been introduced, devising a technique that provides both privacy protection and verification accuracy is still challenging and must have to satisfy the key issues (i) Diversity: The transformed templates must be dissimilar to ensure non-linkability and privacy of user's data stored in different databases across different applications (ii) Revocability: A number of different cancellable templates should be generated from the original biometric so that a new template can be revoked if the transformed one is compromised (iii) Non-invertibility: It must be impossible or computationally hard to retrieve the original biometric data back from the transformed template even if the transformation method and the transformed data are known, and (iv) Performance: The performance while using transformed templates should not degrade much than the performance of us-

Nazmul, R., Islam, M. and Chowdhury, A.
Alignment-free Cancellable Template Generation for Fingerprint based Authentication.
DOI: 10.5220/0006614303610366
In *Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP 2018)*, pages 361-366
ISBN: 978-989-758-282-0

ing the original biometric template.

By exploiting the geometric invariant value extracted from the neighbouring region around fingerprint minutiae and hinging on a stored as well as a user-specific key based transformation, we propose an effective method for cancellable fingerprint template generation. The merits of the proposed method lies in the aspects outlined as: it 1) conceals the biometric data in such a way that it remains irretrievable even though an impostor obtains the transformed template as well as the transformation; 2) satisfies the cancelability and diversity by changing the stored and user-specific keys in the transformation; 3) performs matching in the transformed domain without requiring alignment of the input fingerprint images prior transformation; 4) preserves the geometric relationships even after transformation and alleviates the trade-off between security and performance in recognition accuracy.

Besides, a set of extensive experiments and comprehensive testing on fingerprint benchmark dataset are conducted to analyse the performance, diversity, revocability and non-invertibility of the proposed method.

2 RELATED WORK

A number of research works have been proposed to address template protection problem in biometric systems. Here we provide a brief review on several existing alignment-based and alignment-free approaches proposed for fingerprint template protection which are based on minutiae representation.

Among these approaches, Ratha et al. (Ratha et al., 2007) pioneered the concept of cancellable template generation using Cartesian, polar, and functional transformation. In Cartesian and polar transformation methods, a fingerprint was divided into several grid blocks which were scrambled subsequently. Although the methods were claimed to be non-invertible due to many-to-one mapping property, these were successfully degenerated by the work reported in (Quan et al., 2008) provided that the transformed template and parameters are known to the attacker. Further, as the minutiae were transformed according to their positions, alignment between the enrolled and query images was required to acquire the same transformed image from different impressions of the same finger.

A key-based transformation method was proposed by Ang et al. (Ang et al., 2005) for fingerprint template protection. At first a core point in the fingerprint image was determined and then a line through the core point was specified. The orientation of the line depends on the key, where $0 \leq \text{key} \leq \pi$. Then by reflecting the minutiae under the line to those above the line, transformed fingerprint templates were generated. However, this method required detecting the accurate location of the core point which was not always feasible. Furthermore, by retaining the minutiae above the line intact, the template even after transformation disclosed some information from the original fingerprint.

A hash-based transformation method has been presented by Tulyakov et al. (Tulyakov et al., 2007). In this method, fingerprint minutiae information was hashed and matching between enrolled and query fingerprint was performed in the hashed domain subsequently. Due to one-way transformation characteristic of hashing function, reforming the original features with hash values was computationally hard (Jin et al., 2012). The method does not need pre-alignment between the enrolled and query fingerprint templates.

Lee et al. (Lee et al., 2007) proposed a method for template protection in which translation and rotation invariant values were extracted from the orientation information of neighbouring local region around each minutia. The obtained invariant values were then used as inputs into two changing functions. These functions provided two values that were used as parameters for translational and rotational movement to transform the original minutia. Finally, the transformed template was generated by moving each minutia according to the movements calculated by the changing functions. However, the performance of this method degrades for fingerprints of poor quality.

A bit-string was generated from fingerprint minutiae based on minutiae triplets in a method proposed by Farooq et al. (Farooq et al., 1991). 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, followed by quantization and hashing into a binary-string (bits). To enhance the security of the template, binary-string was further permuted and encrypted. However, this method involves the calculation of all possible triple invariant features which incurs high computational costs. Jin et al. (Jin et al., 2010) proposed another bit-string based template generation method that extracted a set of invariant features from minutiae pairs, and then applied quantization, histogram binning and binarization operations to generate a bit-string. Finally, using a helper data and user's key based permutation procedure the bit-string was transformed into a non-invertible template.

Lee et al. (Lee and Kim, 2010) proposed a minutiae-based bit string for generating fingerprint

template. In this method, a minutia was mapped into a predefined array which consisted of small cells. Firstly, a minutia was chosen as reference minutiae and other minutiae were translated and rotated in order to map the minutiae into the cells based on the position and orientation of the reference minutia. Next, each cell containing more than one minutia was set to 1 (otherwise 0) and thus a bits-string was generated by sequentially visiting the cells in the 3D array. Finally, the resultant bit-string was permuted using user-specific key. The method performs well, however, the performance degrades when the key is compromised.

Another alignment-free fingerprint hashing algorithm (Das et al., 2012) was proposed which used a graph, called the Minimum Distance Graph (MDG), consisting of the inter-minutia minimum distance vectors originating from the core point as a feature set. However, the performance of this algorithm degrades for poor quality images due to inaccurate core point detection.

A non-invertible Randomized Graph-based Hamming Embedding (RGHE) technique (Jin et al., 2014; Jin et al., 2016) was proposed to generate a secure fingerprint template. This method initially constructed a set of minutiae vicinity where each minutia vicinity was decomposed into four minutiae triplets. Then a set of nine geometric invariant features was extracted from each triplet which were projected onto a random subspace determined by a pseudorandom sequence. Finally, using Graph-based Hamming Embedding, the randomized minutia vicinity decomposition features (RMVD) were embedded into the Hamming space. However, this method requires 36 feature components for a minutia vicinity, resulting in a $N \times 36$ features for the entire vicinity set, which is computationally extensive.

Hence, in the alignment-based methods alignment between the enrolled and query fingerprint images is required prior transformation to protect the template. However, while generating protected templates enrolled fingerprint image is transformed in such a way that it cannot provide any clue to a query fingerprint for alignment. To overcome this alignment issue, various alignment-free approaches have been proposed. From the above literature review, it is noteworthy that due to transformation applied to achieve irreversiblity, the performance in recognition accuracy deteriorates, hence demonstrating the inevitable trade-off between non-invertibility and performance.

3 PROPOSED METHOD

In this section, our proposed approach for alignment-free cancellable fingerprint template generation is described. Due to the large variation in different impressions of the same finger, most of the methods require aligning input images prior to the transformation in order to obtain the same transformed template from different impressions. The proposed method, as a typical indirect approach, derives a set of geometric invariant features from the neighbourhood of each minutia and hence relinquishes the process of pre-alignment prior to the transformation in response to rotational and translational variation. The feature set of a minutia is then used as an input to a transformation function that combines the feature values with random offsets to convert into the transformed form. The random offsets that conceal the local topological relationship among the neighbouring minutiae are selected from stored and user-specific key based random vectors using the type and orientation information of the corresponding minutiae. In the following three subsections, we describe the three stages of the proposed method, namely, Invariant features extraction, Protected template generation and Matching transformed templates.

3.1 Extraction of Invariant Features from Fingerprint Minutiae

As the first step of cancellable template generation process, a set of minutiae $M = \{m_i | i = 1,2,\ldots,N\}$ is extracted to derive the geometric invariant features where $N = N_E$ or N_Q denote the number of minutiae in the enrolled and query images, respectively. To extract the geometrical invariant features, for each minutia m_i in M, a neighbourhood set $\aleph_i = \{m_{ij} | j = 1,2,\ldots,L\}$ of L nearest neighbours (measured in terms of Euclidean distance) in its vicinity is constructed. Next, for each neighbour minutia m_j i.e., $m_j \in \aleph_i$, its distance with m_i and with adjacent minutia in $\aleph_i$, denoted by $dist_{i,j}$ and $d_{j,j_{next}}$ respectively, are calculated. Hence, a feature vector ϑ_i for m_i consists of L pairs of two distance values i.e., $\{(dist_{i,1}, d_{1,2}), (dist_{i,2}, d_{2,3}), \ldots, (dist_{i,L}, d_{L,1})\}$ as shown in eq.(1):

$$\vartheta_i = \bigcup_{j=1}^{L} D_{ij} \tag{1}$$

where $D_{ij} = (dist_{i,j}, d_{j,j_{next}})$. This process is continued for all the minutia in M and all the feature vectors are stacked into a matrix V of size $N \times L$ in which

each row corresponds to the feature vector of a minutia and can be defined as follows:

$$V = \bigcup_{i=1}^{N} \bigcup_{j=1}^{L} D_{i,j} \tag{2}$$

Here, V generated from enrolled or query images are represented by V_E and V_Q, respectively.

3.2 Protected Template Generation

To generate the cancellable template, the extracted features that are robust to geometric transformation are combined with stored and user specific key-based random vectors by using the type and orientation information of minutiae in the region. Let's consider ϑ_i^T be the transformed feature vector of m_i as shown in eq. (3).

$$\vartheta_i^T = \bigcup_{j=1}^{L} D_{ij}^T \tag{3}$$

where $D_{ij}^T = (dist_{i,j}^T, d_{j,j_{next}}^T)$ and $dist_{i,j}^T$, $d_{j,j_{next}}^T$ can be defined as follows:

$$\begin{aligned} dist_{i,j}^T &= dist_{i,j} + \triangle\, dist_{i,j} \\ d_{j,j_{next}}^T &= d_{j,j_{next}} + \triangle\, d_{j,j_{next}} \end{aligned} \tag{4}$$

Here, $\triangle\, dist_{i,j}$ and $\triangle\, d_{j,j_{next}}$ are random offsets selected by a transformation function *RndTrans*. The extracted feature vector ϑ_i along with the type and orientation information of m_i and its neighbouring minutiae are used as inputs in *RndTrans*. Next, the random offsets are selected by *RndTrans* from random vectors generated using two keys as seeds; a stored key (i.e., *PIN*)and a user-specific key (i.e., *UPIN*). The entire process is accomplished for N_E in the enrollled image before enrolment and the obtained matrix of transformed feature vectors V_E^T is considered as the protected template. In the authentication phase, the same process repeats for the query image to obtain V_Q^T. Thus, by storing the transformed feature vector the proposed technique offers high level of privacy and protection as the biometric data, i.e., location and orientation of the minutiae, are not directly revealed.

3.3 Matching Transformed Templates

In authentication phase,the matching algorithm first obtains the correspondence between V_E^T and V_Q^T. Since an exact one-to-one mapping between V_E^T and V_Q^T may not be obtained, finding the maximum possible κ matched pairs, where $\kappa \leq min(N_E, N_Q)$ is the objective of the matching algorithm. Firstly, each transformed feature vector ϑ_p^T in V_E^T for $p = 1, 2, \ldots, N_E$ is compared with each vector ϑ_q^T for $q = 1, 2, \ldots, N_Q$ in V_Q^T. Let ϑ_p^T and ϑ_q^T be the feature vectors in V_E^T and V_Q^T extracted from p-th and q-th minutia of the enrolled and query images, respectively. Next, if the number of matched elements ($\Phi_{p,q}$) between ϑ_p^T and ϑ_q^T is greater than a predefined threshold value, (p,q) is stored as a matched minutia pair. The whole process repeats for each of $N_E \times N_Q$ pairs. Subsequently, a set F is constructed by selecting the best distinct κ out of $N_E \times N_Q$ pairs having number of matched pairs greater than 1. Finally, if the ratio of the number of matched elements κ in F and the number of minutiae N_Q in the query image is more than a threshold value δ_{Th}, the authentication is accepted, otherwise rejected.

4 EXPERIMENTAL RESULT AND ANALYSIS

In our experiments, the proposed method is evaluated in terms of performance in verification accuracy and template security. While evaluating the first criteria, it has been tested how the recognition accuracy varies in the transformed templates used for matching. In addition, the proposed method has been examined against three criteria, namely revocability, diversity and non-invertibility to evaluate its performance in template security.

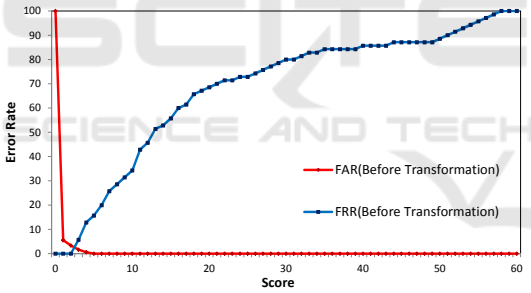
4.1 Experimental Setup

The proposed method has been evaluated using various sample fingerprint images available in public domain databases (Maltoni et al., 2003), namely, DB1 in FVC-2000. The database comprises of 10 users having 8 impressions per user and 80 (10×8) fingerprint images in total. The first impression from each finger is considered as the template and the seven other impressions are used as the query images. In the proposed method, minutiae points are extracted from each image in the databases using the method of (Thai, 2003) that involves image enhancement, binarization and thinning as preprocessing steps. In our experiment, the performance of the proposed method has been measured using False Acceptance Rate (FAR), Genuine Acceptance Rate (GAR), False Rejection Rate (FRR) and Equal Error Rate (ERR). To calculate FRR and GAR, experiments are conducted by comparing the image from the template set to the corresponding impressions in the query set. FAR is measured by comparing each image from the template set to all the images in

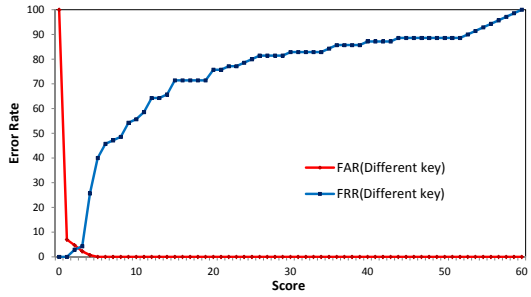
the query set except with the impressions from the same finger. Apart from these, two more performance measures namely, Receiver Operating Characteristic (ROC) curve and genuine-impostor distributions are used to demonstrate the performance of the proposed method. The genuine distribution is the score calculated by comparing the template of each user with the other impressions of the fingerprint from the same individual. On the contrary, the imposter distribution is generated by comparing the template of each user with the impressions of all other users' in the query set (Jin et al., 2012). A clear separability between the genuine and impostor distributions implies good performance while strong overlapping between the two indicates poor performance.

4.2 Performance Evaluation in Recognition Accuracy

As mentioned above, we have investigated the recognition performance before and after the transformation of the fingerprint images. The FAR vs FRR graph for the images in FVC2002 DB1-B before and after transformation are shown in Figure. 1 (a) and 1 (b), respectively.



(a) Before Transformation



(b) After Transformation

Figure 1: (a) The FAR and FRR curve before and (b) after transformation in FVC2002 DB1-B where EER is denoted by the intersecting point.

From the experiments we found that the EER before and after the transformation is 1% and 2%, respectively, which shows that the performance degradation in matching caused by transformation is rather insignificant for DB1 in FVC-2002. To illustrate the recognition performance of the proposed method, the ROC curve in the actual scenario, where each user in the databases is assigned a different key, is shown in Figure. 2. Finally, the genuine and the impostor distributions using different keys are plotted in Figure. 3, which depict that individual users are clearly distinct from one another. Hence, the experimental result presented in this section signifies the preservation of the actual geometric relationship between the original fingerprint and the transformed templates even after transformation.

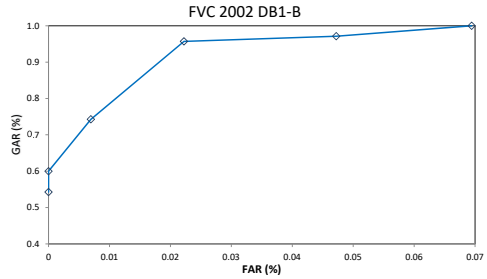
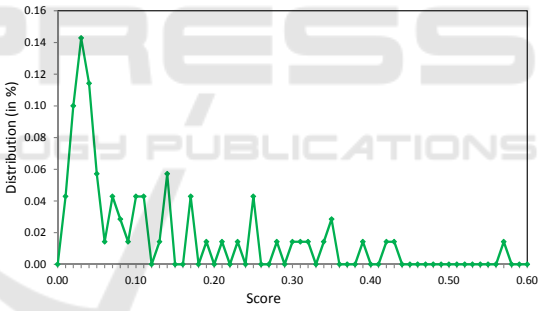
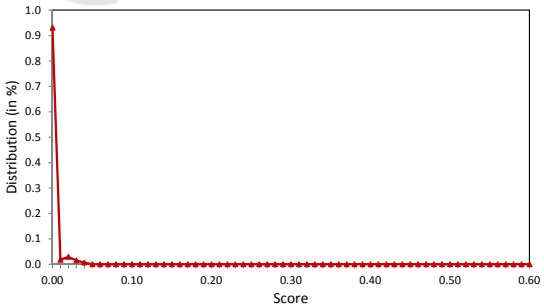


Figure 2: ROC Curve for different keys in FVC2002 DB1-B.



(a) Genuine Distribution



(b) Imposter Distribution

Figure 3: (a) Genuine and (b) Imposter distributions in FVC2002 DB1-B where all the users are assigned different keys.

5 CONCLUSION

In this paper, we have proposed a method for generating cancellable fingerprint templates to provide protection to minutiae-based fingerprint data. The notable contributions of our method are two folds: alignment-free and excellent recognition performance. The proposed construct preserves the geometric relationships among the original fingerprint image in the transformed templates and hence does not cause performance degradation. Further, the proposed scheme ensures strong security in that given both the user key and the transformed template, revealing raw fingerprint data is not be feasible. The stored and user-specific keys are employed to transform the invariant feature vector and thus diversity and revocability can be vindicated. Experiments conducted on the public domain database FVC2002-DB1 demonstrate the excellent performance of the proposed method in recognition accuracy, computational complexity and security.

REFERENCES

Ang, R., Safavi-Naini, R., and McAven, L. (2005). Cancelable key-based fingerprint templates. In *Australasian conference on information security and privacy*, pages 242–252. Springer.

Das, P., Karthik, K., and Garai, B. C. (2012). A robust alignment-free fingerprint hashing algorithm based on minimum distance graphs. *Pattern Recognition*, 45(9):3373–3388.

Farooq, S. T. F., Mansukhani, P., and Govindaraju, V. (1991). Symmetric hash functions for secure fingerprint biometric systems. In *Pattern Recognition Letters*.

Jin, Z., Lim, M.-H., Teoh, A. B. J., and Goi, B.-M. (2014). A non-invertible randomized graph-based hamming embedding for generating cancelable fingerprint template. *Pattern Recognition Letters*, 42:137–147.

Jin, Z., Teoh, A. B. J., Goi, B.-M., and Tay, Y.-H. (2016). Biometric cryptosystems: A new biometric key binding and its implementation for fingerprint minutiae-based representation. *Pattern Recognition*, 56:50–62.

Jin, Z., Teoh, A. B. J., Ong, T. S., and Tee, C. (2010). A revocable fingerprint template for security and privacy preserving. *TIIS*, 4(6):1327–1342.

Jin, Z., Teoh, A. B. J., Ong, T. S., and Tee, C. (2012). Fingerprint template protection with minutiae-based bit-string for security and privacy preserving. *Expert systems with applications*, 39(6):6157–6167.

Lee, C., Choi, J.-Y., Toh, K.-A., Lee, S., and Kim, J. (2007). Alignment-free cancelable fingerprint templates based on local minutiae information. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, 37(4):980–992.

Lee, C. and Kim, J. (2010). Cancelable fingerprint templates using minutiae-based bit-strings. *Journal of Network and Computer Applications*, 33(3):236–246.

Maltoni, D., Maio, D., Jain, A., and Prabhakar, S. (2003). Handbook of fingerprint recognition springer. *New York*.

Nagar, A., Nandakumar, K., and Jain, A. K. (2010). A hybrid biometric cryptosystem for securing fingerprint minutiae templates. *Pattern Recognition Letters*, 31(8):733–741.

Quan, F., Fei, S., Anni, C., and Feifei, Z. (2008). Cracking cancelable fingerprint template of ratha. In *Computer Science and Computational Technology, 2008. ISCSCT'08. International Symposium on*, volume 2, pages 572–575. IEEE.

Ratha, N. K., Chikkerur, S., Connell, J. H., and Bolle, R. M. (2007). Generating cancelable fingerprint templates. *IEEE Transactions on pattern analysis and machine intelligence*, 29(4):561–572.

Thai, R. (2003). *Fingerprint image enhancement and minutiae extraction*. The University of Western Australia.

Tulyakov, S., Farooq, F., Mansukhani, P., and Govindaraju, V. (2007). Symmetric hash functions for secure fingerprint biometric systems. *Pattern Recognition Letters*, 28(16):2427–2436.

Wang, S. and Hu, J. (2012). Alignment-free cancelable fingerprint template design: A densely infinite-to-one mapping (ditom) approach. *Pattern Recognition*, 45(12):4129–4137.