International Journal of Cryptology Research 7(1): 27 - 41 (2017)

Cancellable Fingerprint Minutiae Template Protection Using Bit Toggling Technique for Privacy Preserving

Badiul Alam[1], **Zhe Jin**[2,*], **Wun-She Yap**[1], and **Bok-Min Goi**[1]

[1] *Lee Kong Chian Faculty of Engineering and Science, Universiti Tunku Abdul Rahman, Sungai Long, Malaysia*

[1] *School of Information Technology, Monash University Malaysia, Bandar Sunway, Malaysia*

E-mail: jin.zhe@monash.edu
[*]*Corresponding author*

ABSTRACT

Due to the strong linkage between an individual and a claimed identity, biometric authentication is widely used to authenticate an individuals identity by matching an individuals biometric with a database of records. Yet, if the biometric template stored inside the database is compromised, invasion of user privacy is inevitable. For instance, a fingerprint image can be reconstructed with high accuracy using existing technologies if the corresponding set of fingerprint minutia is revealed to an adversary. In this paper, we enhanced the polar grid-based 3-tuple quantization with random bits toggling technique to protect fingerprint minutiae template. The promising experimental results on FVC2002 DB1 and DB2 justify the feasibility of the proposed method.

Keywords: Fingerprint, template protection, security, privacy

1 INTRODUCTION

Biometrics has been integrated in large-scale personal identification systems and the rapid proliferation of biometric recognition applications is a foreseeable trend in future. The foreseen pervasiveness of biometric authentication systems speeds up the growing biometric databases. However, if biometric databases breach is occurred, severe influences of biological nature of human are concerns. Particularly, the damage to persons privacy and security is permanent due to the irrevocability and irreplaceability nature of human traits. As a result, various biometric template protection techniques have been proposed to secure biometric templates.

Fingerprint is probably the most widely used biometric trait for the biometric-based authentication systems (Maltoni et al., 2009). Minutia represents the fingerprint ridge characteristics at local level. There are two most prominent ridge characteristics, called ridge bifurcations and ridge termination. Generally, fingerprint minutiae are stable and robust to fingerprint impression conditions (Maltoni et al., 2009). Each minutia can be associated with a number of attributes, including location coordinates, orientation, type (e.g. ridge termination or ridge bifurcation), a weight based on the quality of the fingerprint image in the neighborhood of each minutia, and so on. However, from the common practices, only two attributes are used to represent a minutia: x- and y-coordinates pertaining to the location of minutia in the fingerprint; the orientation θ of the ridge line to which the minutia is attached (Krivokuća, 2015). In this paper, fingerprint minutia is solely focused.

However, compromisation of fingerprint templates may breach user privacy. More importantly, once biometrics are compromised, they are lost forever. Different attack models in recovering the user identity by compromising biometric templates had been presented by Ratha et al. (2001), Jain and Pankanti (2006) and Roberts (2007) independently. In addition, the attacks proposed by Ross et al. (2007) and Wang and Hu (2011) can reconstruct the original fingerprint information from the compromised fingerprint template.

To protect the fingerprint templates, many methods had been proposed. However, to design a biometric template protection scheme, it is still a chal-

lenging task to design a biometric template protection scheme that follows the following criteria (Jain et al., 2008):

- Performance: The recognition accuracy of the proposed scheme should be preserved or improved.
- Non-invertibility: It should be infeasible to reconstruct the original biometric template from the transformed template.
- Unlinkability: It should not be matched with multiple instances from the same biometric template which prevent the cross matching application.
- Revocability: It should be possible to replace the compromised template with new template generated from the original biometric data.

In this paper, we propose a cancellable fingerprint template protection scheme by enhancing the polar grid-based 3-tuple quantization with random bits toggling technique.

2 LITERATURE REVIEW

Generally, biometric template protection refers a set of techniques that mitigate the aftermaths due to the compromise of biometric templates databases for the purpose of malicious use. Technically, biometric template protection is to design a protect function and apply it into unprotected template to generate protected template. The template protection methods proposed in literature can be broadly divided into two categories, namely, feature transformation approach (or cancellable biometrics) and biometric cryptosystem (or helper data methods) (Jain et al., 2008).

Cancellable biometrics (Ratha et al., 2007) is truly meant designed for biometric template protection. It refers to the irreversible transform of the biometric template to ensure security and privacy of the actual biometric template. On the other hand, biometric cryptosystem serves the purpose of either securing the cryptographic key using biometric feature (i.e., key binding) or directly

generating the cryptographic key from biometric feature (i.e., key generation) (Jain et al., 2008). In this paper, cancellable biometric is focused.

Ratha et al. (2007) proposed three non-invertible transform functions, namely Cartesian, polar and surface-folding transformation. Although the three transformation functions were claimed to be non-invertible due to the many-to-one mapping property, a scheme by Feng et al. (2008) reveals that the surface-folding transform can be degenerated when the transformed template and parameters are revealed to the attacker.

Sutcu et al. (2008) proposed to transform the biometric data into binary feature vectors which are appropriate for low density parity check codes. To generate n bits from a minutiae map, it is sufficient to ask n questions where each question with a binary answer. Each question can be formed as counting the number of minutiae points that fall in a randomly chosen cuboid in three dimensions, i.e. X, Y and Θ. A threshold value is fixed based on the median of the number of minutiae points in the chosen cuboid measured across the training set. If the number of minutiae points in a randomly generated cuboid exceeds the threshold, a bit '1' is generated; otherwise, a bit '0' is generated. By repeating n questions, a n-bit feature vector will be generated.

Nagar et al. (2010) extended the method (Sutcu et al., 2008) by using more discriminative features instead of the number of minutiae. These discriminative features may include the distance from one minutiae to the nearest boundary, the average and standard deviation of minutiae coordinates. However, pre-alignment of fingerprint image is required for these two methods. On the other hand, Bringer and Despiegel (2010) proposed a scheme that generates binary feature vectors of fingerprint by local comparisons. By matching small minutiae vicinities with a set of representative vicinities, binary feature vectors of fingerprint can be generated. However, no security analysis had been performed on the proposed transformation.

Wang and Hu (2012) proposed a cancellable fingerprint template based on a dense infinite-to-one mapping (DITOM). A complex vector is generated from the proposed method by applying a discrete Fourier transform and the final template is obtained by blending the complex vector with a randomly generated parametric matrix. In addition to DITOM, Wang and Hu (2014)

proposed another cancellable fingerprint template based on curtailed circular convolution, which demonstrates an improvement on accuracy and security over DITOM.

Das et al. (2012) proposed an alignment-free fingerprint hashing algorithm based on minimum distance graph (MDG). The MDG formed by a set of connected nodes and the nodes are formed by computing the distance between the core and next nearest minutia. It also consists of distance between the next closest minutiae and so on. Subsequently, the MDG hash is extended to generate cancellable templates. However, the proposed method relies on accurate detection of the core point of fingerprint image.

Jin et al. (2014) proposed a fingerprint template with strong non-invertibility, namely randomized graph-based hamming embedding (RGHE). This technique is able to protect the minutiae vicinity decomposition features and preserve the recognition performance in the original feature space.

3 PROPOSED METHOD

Polar grid-based 3-tuple quantization (PGTQ) is an alignment-free minutiae descriptor that utilizes variable-sized tessellated quantization in polar coordinate (Jin et al., 2012). In this method, sectors near the reference minutia have smaller area and vice versa. This leads to a smaller (resp. larger) quantization step around (resp. further away from) the reference minutia to tolerate fingerprint elastic deformation. In the original PGTQ descriptor, polar coordinate covers the entire image and produces a lengthy bit string, which is undesirable for practical applications due to large storage of templates. As a solution, in this paper, we consider polar coordinate that only covers a part of the image limited by a circle with radius R. With this, the size of the resultant bit-string can be significantly reduced. The details of the modified PGTQ descriptor are described as follows:

1. Let $m_r = \{x_r, y_r, \theta_r\}$ be the reference minutiae. The neighboring minutiae within a circle with radius R in Euclidean distance is rotated and translated based on the reference minutiae using Eq. (1) and Eq. (2). The

transformed minutiae are represented as $m^t = \{x_i^t, y_i^t, \theta_i^t | i = 1, N_R - 1\}$, where N_R is the total number of minutiae within a pre-defined radius R.

$$\begin{bmatrix} x_i^t \\ y_i^t \end{bmatrix} = \begin{bmatrix} \cos\theta_r & -\sin\theta_r \\ \sin\theta_r & \cos\theta_r \end{bmatrix} \begin{bmatrix} x_i - x_r \\ -(y_i - y_r) \end{bmatrix} \tag{1}$$

$$\theta_i^t = \begin{Bmatrix} \theta_i - \theta_r; & \theta_i \geq \theta_r \\ 360^\circ + \theta_i - \theta_r; & \theta_i < \theta_r \end{Bmatrix} \tag{2}$$

2. The translated and rotated minutiae are then converted into polar coordinates using Eq. (3) and Eq. (4). ρ_i and α_i indicate the radial distance (in pixels) and the radial angle of the i-th minutia in Polar coordinates ($\alpha_i \in (0, 360^\circ]$), respectively.

$$\rho_i = \sqrt{(x_i^t)^2 + (y_i^t)^2} \tag{3}$$

$$\alpha_i = \arctan(\frac{y_i^t}{x_i^t}) \tag{4}$$

3. *3-Tuple-based Quantization*. The 3-tuple-based quantization is a sector-based quantization involving all minutiae in the neighborhood. Each quantized minutia can be represented as a vector $\omega = \{\rho^q, \alpha^q, \theta^q\}$, such that

$$\rho_i = \lfloor \rho_i / x \rfloor \tag{5}$$

$$\alpha_i = \lfloor \alpha_i / y \rfloor \tag{6}$$

$$\theta_i = \lfloor \theta_i / z \rfloor \tag{7}$$

where $/$ denotes quotient; x, y and z indicate the radius for each polar grid (in pixels), radial angle for tolerance ($y \in (0, 360^\circ]$) and orientation angle to be tolerated $z \in (0, 360^\circ]$, respectively. The quantization level is determined by x, y and z.

4. *Binarization*. The quantized minutiae ω are then binarized using the polar grids. We adopt a simple rule to map a polar grid to 1 if the polar grid contains more than one minutia, and otherwise, a polar grid is mapped to 0. By concatenating the individual output bits from the polar grids, we eventually obtain a binary vector with length equals to the number of polar grids $l = \lceil 360/x \rceil \lceil 360/y \rceil \lceil 360/z \rceil$, where $\lceil \cdot \rceil$ denotes the ceiling function. The above steps are repeated by changing the reference minutia with every remaining minutia to generate the full binary PGTQ descriptor. As the total minutiae number (N_m) extracted from each fingerprint image could be different, this template, denoted by $\Omega \in \{0,1\}^{(N_m \times l)}$ is variable in size.

5. *Matching*. To evaluate the similarity between two sets of modified PGTQ descriptor, we adopt a typical two-stage matching strategy that is composed of local and global matching. The local descriptor matching searches for the intersections between two binary strings in which the PGTQ descriptor is represented. On the other hand, the global matching is to find the ratio of the matched descriptor pairs over all potential pairs as the final matching score.

Let $\Omega^e = [b_1^e; b_2^e, \ldots, b_{n^e}^e]$ and $\Omega^q = [b_1^q; b_2^q, \ldots, b_{n^q}^q]$ be the enrolled and query descriptor sets that consist of n^e and n^q l-bit binary strings, respectively. From this point onwards, we slightly abuse the notation of b, where $b_{i,k}$ represents the k-th bit for i-th binary string with $1 \leq k \leq l$ and $1 \leq i \leq n^e$ or n^q. To take into account the difference of minutiae quantity in the enrolled and query image, we normalize the similarity scores between two local descriptors Ω^e and Ω^q as follows:

$$S_{ij}^b = \frac{(N_j^q + N_i^e) \sum_{k=1}^{l} (b_{j,k}^q \cdot b_{i,k}^e)}{(N_j^q)^2 + (N_i^e)^2} \tag{8}$$

where S^b denotes the matching score between two binary strings, $\cdot$ represents a bitwise AND operator, $N_i^e = \sum_{k=1}^{l} (b_{i,k}^e)$ and $N_j^q = \sum_{k=1}^{l} (b_{j,k}^q)$ denote the total number of 1s of the enrolled and query bit-strings, respectively. The term $\sum_{k=1}^{l} (b_{j,k}^q \cdot b_{i,k}^e)$ in Eq. (8) counts the bit positions that have value '1' in both query and enrolled bit-strings. The scores in matrix $S^b \in \mathbb{R}^{n^q \times n^e}$ range from 0 to 1 where '1' indicates a perfect match.

Once the similarity score matrix S^b is calculated from the local descriptor matching; a global matching process is carried out. Given the score matrix $S^b = \{s^b_{ij}\}$, the final score can be calculated as:

$$S_{\text{PGTQ}} = \max\{\frac{1}{m}\sum_j s_j(\text{mbox}), \frac{1}{n}\sum_i s_i(\text{max})\} \tag{9}$$

where $s_{j(\text{max})} = \max_i\{s^b_{ij}\}$ and $s_{i(\text{max})} = \max_j\{s^b_{ij}\}$ represent the maximum score component of the i-th column and j-th row, respectively. The detailed matching process is illustrated in Algorithm 1.

Algorithm 1: Matching Two PGTQ-based Minutia Descriptors

Input: $\Omega^\theta, \Omega^q, n^\theta, n^q$
Function Prototype: *sim*$(\Omega^\theta, \Omega^q)$
$n^\theta \leftarrow \text{size}(\Omega^\theta)$
$n^q \leftarrow \text{size}(\Omega^q)$
for $i = 1 : n^\theta$ **do**
  $B^\theta_i = \Omega^\theta(i)$
  for $j = 1 : n^q$ **do**
    $B^1_j = \Omega^q(j)$ Calculate similarity score s^b_{ij} between b^θ_i and b^q_j using Eq. (8)
  end
end
$S^b = \{s^b_{ij}\}$
$s_{j(\text{max})} = \max_i\{s^b_{ij}\}$
$s_{i(\text{max})} = \max_j\{s^b_{ij}\}$
$S_{\text{PGTQ}} = \max\{\frac{1}{m}\sum_j s_j(\text{mbox}), \frac{1}{n}\sum_i s_i(\text{max})\}$
Output: The matching score, S_{PGTQ} between Ω^θ and Ω^q

The PGTQ descriptor as templates is required to be stored for verification. However, if the templates stored in database are compromised, the security and privacy of the system are vulnerable to template replay, spoof construction and targeted false accepts. To alleviate this problem, our treatment is to adopt a random bits-toggling process presented in Farooq et al. (2007). This process is to randomly select a fraction of bits and invert them. This process is a noise

addition process that distorts the template data. Since PGTQ descriptor is a feature matrix; the bit-toggling process is applied in a row-wise basis.

Figure 1 shows the overall process of the proposed cancellable fingerprint template protection scheme. The overall authentication protocol consists of two stages: enrollment and verification. In the enrollment stage, PGTQ descriptor is extracted by presenting users genuine fingerprint. Thereafter, a random bits-toggling process is performed to distort the PGTQ descriptor and generate the protected template stored in database. While for the verification stage, the query PGTQ descriptor is extracted and matched against the protected template. Such protocol gives several observations:

1. PGTQ essentially is a many-to-one transformation that provides first layer of protection against feature (e.g. minutiae) inversion;
2. Random bits-toggling process additionally offers second layer protection by introducing a significant portion of noise.

It thus can be expected that template replay, spoof construction and targeted false accepts can be prevented effectively.

4 EXPERIMENT ANALYSIS

To measure the feasibility of the proposed method, the experiments were conducted on six public fingerprint datasets, FVC2002DB1 and FVC2002DB2. Each dataset consists of 100 users with 8 samples per user. In total, there are 800 (1008) fingerprint images in each dataset. VeriFinger 6 SDK was used for minutia extraction. The performance of the proposed framework is evaluated using equal error rate (EER). For matching protocol, the first sample (gallery) of every identity is matched against the second samples (probe) of every identity for false rejection rate (FRR) calculation. On the other hand, the first sample of each identity is matched against the first sample of the remaining identities for false acceptance rate (FAR) calculation. This matching protocol yields 100 genuine scores and 4950 imposter scores for each dataset. Note the

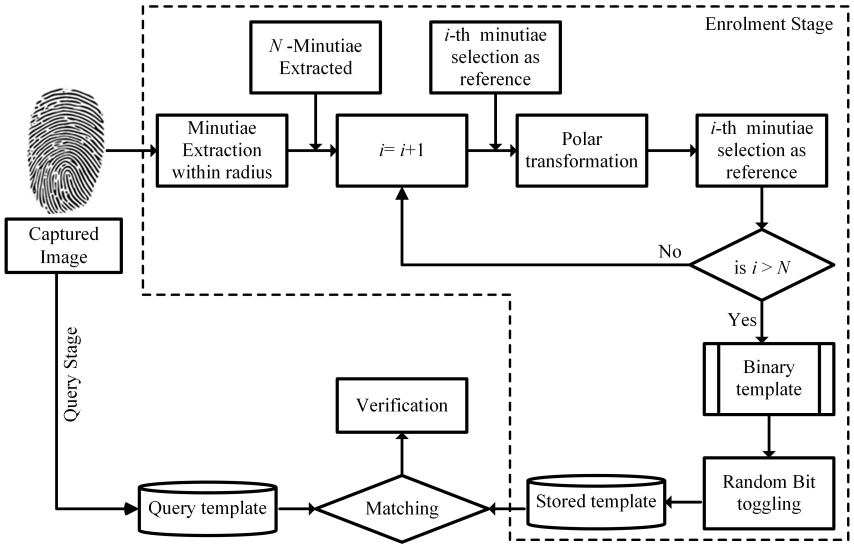

Figure 1: The higher view of our proposed cancellable fingerprint template protection scheme

same setup has been employed by the existing methods for a fair comparison. Table 1 tabulates the parameters used in our experiments.

Symbols	Description	Value
R	Radius for polar coordinates (in pixel)	70
x	Radius for polar grid segment (in pixel)	10
y	Radius angle for polar grid segment (in degree)	20
z	Minutiae orientation angle (in degree)	30

Table 1: The parameters used in experiment.

As aforementioned discussion, the bit-toggling process is applied to distort the templates. However, Farooq et al. (2007) reveals that a large number of randomly toggled bits would deteriorate accuracy performance. This deterioration can be alleviated by carefully selecting a portion of bits for flipping. We show in Table 2 that, even though a significant portion of noise (50%) has been added, the accuracy would not degrade significantly. Then, a comparative study of performance is conducted between the proposed technique and the ex-

isting methods, and the corresponding EER performances are listed in Table 2. It is noticed that the proposed method achieves performance that is better than the existing methods (Wang and Hu, 2012, 2014). Further, the original PGTQ is discouraged because of the lengthy template and worse performance due to the maximum noise (e.g. spurious minutia) as the entire image is included.

Methods	**DB1**	**DB2**
Jin et al. (2012)	1.19	6.94
Das et al. (2012)	2.27	3.79
Bringer and Despiegel (2010)	N.A.	5.3
Wang and Hu (2012)	3.5	4.0
Wang and Hu (2014)	2.0	2.3
Modified PGTQ	1.08	2.03
Modified PGTQ with random bit toggling	1.04	2.02

Table 2: The EER performances for different methods using FVC2002

5 SECURITY ANALYSIS

5.1 Non-invertibility

In our experiment, a 5-bit toggling is considered; to correctly guess the 5-bits among 1512 bits-length template requires approximately 245 attempts. Averagely, 40 minutiae point are extracted, subsequently, the size of binary feature is of 40×1512. Since 245 attempts are required for single feature vector, the effort to recover the entire feature matrix requires 21800 attempts. This is indeed computational hard in real time scenario to invert the transformed template into original feature matrix. To make it harder, PGTQ descriptor generation essentially is a many-to-one transformation, i.e. multiple minutiae may map into an identical element in transformed domain. Information lost in this process is evitable. Therefore, privacy preserving is gained even the template is compromised.

5.2 Revocability

The revocability is evaluated by matching a particular fingerprint template with the other fingerprint templates generated from distinct random token (i.e. random bit toggling). We use 100 distinct random token to generate 100 different templates using a fingerprint image. The entire process is repeated using the same random token for different users to produce a total of $100 \times 8 \times 100 = 80000$ scores. The experiment was conducted on FVC2002DB1. Figure 2 shows the distributions of the impostor scores and pseudo-impostor scores. Since the distribution of pseudo-impostor scores resembles the distribution of impostor scores, this vindicates that the newly generated fingerprint templates are indistinguishable to each another. This justifies that the proposed scheme can achieve the property of revocability.

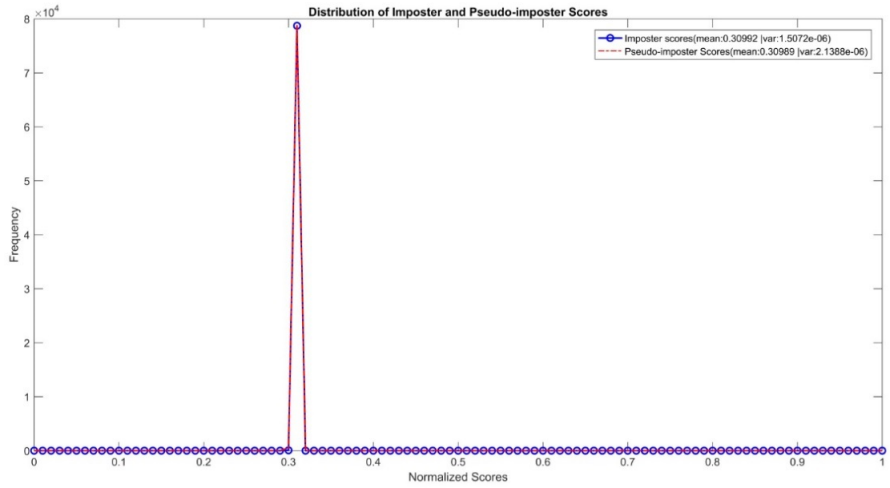

Figure 2: The distributions of impostor scores and pseudo-impostor scores

5.3 Non-linkability

To evaluate non-linkabilty criteria, pseudo-genuine score is introduced where the pseudo-genuine score is computed by matching the fingerprint templates

generated from different fingerprint images (or samples) of the same user using 100 different random token (i.e. random bit toggling). This experiment thus yields $7! \times 100 = 2800$ pseudo-genuine scores given that there are 8 samples per user. The experiment was conducted on FVC2002DB1. Figure 3 shows the distribution of the pseudo-genuine scores and the pseudo-impostor scores. Since the distribution of pseudo-impostor scores overlaps the distributions of pseudo-genuine scores, the attacker cannot distinguish whether the templates are generated from the same user. This justifies that the proposed scheme can achieve the property of non-linkability.

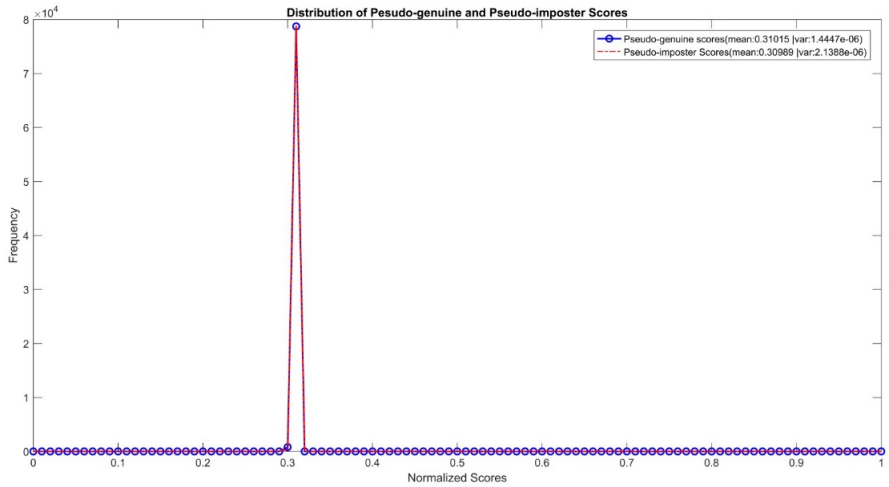

Figure 3: The distributions of pseudo-genuine scores and pseudo-impostor scores

6 CONCLUSION

In this paper, we proposed random bits togging based polar grid-based 3-tuple quantization to protect fingerprint minutia. The proposed method improves the security of PGTQ by preventing it from template replay, spoof construction and targeted false accepts. The experimental results vindicate that the proposed method could achieve satisfiable recognition performance and security properties (i.e. non-invertibility, revocability and non-linkability) in comparison with

several existing methods. In addition, with random bits togging procedure, a significant noise is salted to provide another layer of protection for fingerprint minutia without compromising recognition performance.

ACKNOWLEDGMENTS

Wun-She Yap and Bok-Min Goi would like to acknowledge MOSTI for financially funding their research through the MOSTI Science Fund numbers 01-02-11-SF0189 and 01-02-11-SF0201.

REFERENCES

Bringer, J. and Despiegel, V. (2010). Binary feature vector fingerprint representation from minutiae vicinities. In *Proc. IEEE International Conference on Biometrics: Theory Applications and Systems (BTAS2010)*, pages 1–6, Washington, DC, United State.

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

Farooq, F., Bolle, R., Jea, T., and Ratha, N. (2007). Anonymous and revocable fingerprint recognition. In *Proc. IEEE Conference on Computer Vision and Pattern Recognition (CVPR2007)*, pages 1–7, Minneapolis, MN, United State.

Jain, A. K., Nandakumar, K., and Nagar, A. (2008). Biometric template security. *EURASIP J. Adv. Signal Process.*, 579416:113.

Jain, A. K. and Pankanti, S. (2006). Biometrics: A tool for information security. *IEEE Trans. Inf. Forensics Security*, 1(2):125–143.

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 Recog. Lett.*, 42(3):137–147.

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 Syst. with Appl.*, 39(6):6157–6167.

Krivokuća, V. (2015). *Fingerprint Template Protection using Compact Minutiae Patterns*. PhD thesis, The University of Auckland, Auckland, NZ.

Maltoni, D., Maio, D., Jain, A., and Prabhakar, S. (2009). *Handbook of Fingerprint Recognition*. Springer-Verlag, London, UK, 2nd edition.

Ratha, N. K., Chikkerur, S., Connell, J. H., and Bolle, R. M. (2007). Generating cancelable fingerprint templates. *IEEE Trans. Pattern Anal. Mach. Intell.*, 29(4):561–572.

Ratha, N. K., Connell, J. H., and Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, 40(3):614–634.

Roberts, C. (2007). Biometric attack vectors and defences. *Computers & Security*, 26(1):14–25.

Ross, A., Shah, J., and Jain, A. K. (2007). From template to image: Reconstructing fingerprints from minutiae points. *IEEE Trans. Pattern Anal. Mach. Intell.*, 29(4):544–560.

Sutcu, Y., Rane, S., Yedidia, J. S., Draper, S. C., and Vetro, A. (2008). Feature extraction for a slepian-wolf biometric system using ldpc codes. In *Proc. IEEE International Symposiumm on Information Theory (ISIT2008)*, pages 2297–2301, Toronto, ON, Canada.

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

Wang, S. and Hu, J. (2014). Design of alignment-free cancelable fingerprint templates via curtailed circular convolution. *Pattern Recogn.*, 47(3):1321–1329.

Wang, Y. and Hu, J. (2011). Global ridge orientation modeling for partial fingerprint identification. *IEEE Trans. Pattern Anal. Mach. Intell.*, 33(1):72–87.