A Cancellable Ranking Based Hashing Method for Fingerprint Template Protection

Zhe Jin[1], Jung Yeon Hwang[2], Soohyung Kim[2], Sangrae Cho[2],
Yen-Lung Lai[1], and Andrew Beng Jin Teoh[3](✉)

[1] School of IT, Monash University Malaysia, Jalan Lagoon Selatan,
46150 Bandar Sunway, Selangor Darul Ehsan, Malaysia
{jin.zhe,lai.yenlung}@monash.edu

[2] Electronics and Telecommunications Research Institute (ETRI),
Seoul, South Korea
{videmot,lifewsky,sangrae}@etri.re.kr

[3] School of Electrical and Electronic Engineering, Yonsei University,
Seoul, South Korea
bjteoh@yonsei.ac.kr

Abstract. Despite a variety of theoretical-sound techniques have been proposed for biometric template protection, there is rarely practical solution that guarantees non-invertibility, cancellability, non-linkability and performance simultaneously. In this paper, a cancellable ranking based hashing is proposed for fingerprint template protection. The proposed method transforms a real-valued feature vector into an index code such that the pairwise-order measure in the hashed codes are closely correlated with rank similarity measure. Such a ranking based hashing offers two major merits: (1) Resilient to noises/perturbations in numeric values; and (2) Highly nonlinear embedding based on the rank correlation statistics. The former takes care of the accuracy performance mitigating numeric noises/perturbations while the latter offers strong non-invertible transformation via nonlinear feature embedding from Euclidean to Rank space that leads to toughness in inversion yet still preserve accuracy performance. The experimental results demonstrate reasonable accuracy performance on benchmark FVC2002 and FVC2004 fingerprint databases. The analyses justify its resilience to inversion, brute force and preimage attack as well as satisfy the revocability and unlink ability criteria of cancellable biometrics.

Keywords: Cancellable biometrics · Fingerprint recognition · Rank hashing

1 Introduction

Biometrics become commonplace for identity management systems nowadays. The proliferation of biometric systems yields massive number of templates. The security and privacy of biometric template is an escalating concern if compromised. Such a concern is attributed to the strong binding of individuals and privacy, and further complicated by the fact that biometric is irrevocable. Given the above threats, a number of proposals have been reported for protecting the biometric templates. However,

J. Hu et al. (Eds.): MONAMI 2017, LNICST 235, pp. 378–389, 2018.
https://doi.org/10.1007/978-3-319-90775-8_30

designing a decent biometric template protection (BTP) scheme with the following criteria [1, 2, 7] remain challenge:

- Non-invertibility or Irreversibility: It should be computationally infeasible to derive the original biometric template from a single or multiple protected template and/or the helper data of BTP.
- Revocability or Renewability: A new instance of protected template can be revoked when the existing template is compromised.
- Non-linkability or Unlinkability: It should be computationally difficult to differentiate two or more instances of the protected biometric templates derived from the same biometric trait.
- Performance preservation. The accuracy performance of the protected biometric template should be preserved.

Generally, the BTP schemes in literature can be broadly divided into two categories: cancellable biometrics and biometric cryptosystems. Biometric cryptosystem serves the purpose of either securing the cryptographic key using biometrics (key binding) or directly generating the cryptographic key from the biometrics (key generation) [2]. On the other hand, cancellable biometrics [3] is a more direct solution for BTP as biometric cryptosystem is primary meant to protect secret (such as crypto key) rather than biometric templates. Cancellable biometrics refers to the irreversible transform applied to the biometric template to generate the protected template ensuring the security and privacy of the original biometric template. If a cancellable biometric template is compromised, a new template can be re-generated from the same biometrics.

Several decent review papers exist for BTP such as [2, 4–6]. We focus a few latest and relevant fingerprint related BTP schemes. Ferrara et al. [8] propose a non-invertible scheme for minutia cylinder code (MCC), a state-of-the-art fingerprint descriptor [9], namely protected MCC (P-MCC) via binary principle component analysis. Despite the cancellability is not addressed in P-MCC, a two-factor P-MCC, namely 2P-MCC [10] is later proposed to make P-MCC becomes cancellable. MCC and its successors are dedicated for fingerprint minutiae and thus it is not directly transferred to other popular biometrics such as face and iris.

A generic cancellable biometrics scheme, namely bloom filter has been introduced for iris [11], face [12] and fingerprint [13] recently. Despite the decent performance preservation, the security and privacy of bloom filter based schemes remains open. For instance, Hermans et al. [14] demonstrate a simple and effective attack scheme that matches two protected templates derived from the same IrisCode using different secret bit vectors, thus break the requirement of non-linkability. Bringer et al. [15] further analyzed the non-linkability of the protected templates generated from two different IrisCode of the same subject.

Sandhya and Prasad [16] propose a k-nearest neighbor structure from fingerprint minutia to construct a fixed-length binary vector. The binary vector is Fourier transformed yield a complex vector. Cancellable template can be generated by simply multiplying the complex vector with Gaussian random matrix. This technique yields reasonable recognition accuracy. However, the security of the proposed method is insufficiently analyzed.

Wang and Hu [17] propose a blind system identification approach to protect biometric template. This is motivated by the fact that source signal cannot be recovered if the identifiability is dissatisfied in blind system identification. This new approach exhibits well accuracy performance preservation and the irreversibility of transformed template is justified theoretically and experimentally.

In this paper, we report a new cancellable biometric scheme based on the ranking based hashing, which is inspired from the "Winner Takes All" (WTA) hashing [18] that used for solving the fast similarity search. The proposed scheme enjoys the merits of strong theoretical guarantee of accuracy preservation after hashing. With its pure discrete indices representation nature, a product of non-linearly transformed real-valued biometric features, the scheme can strongly protect the biometric data from being inverted. The analyses justify its resilience to inversion, brute force and pre-image attacks as well as satisfy the revocability and unlinkability criteria of cancellable biometrics. Besides, the implementation is also incredibly simple for practical applications. We demonstrate the feasibility of this method with fingerprint modality.

2 Preliminary

The basic idea of WTA hashing [18] is to compute the ordinal embedding of an input data based on the partial order statistics. More specifically, the WTA hashing is a non-linear transformation based on the *implicit order* rather than the absolute/numeric values of the input data, and therefore, offers certain degree of resilience to numerical perturbation while giving a good indication of inherent similarity between the compared items. The overall WTA hashing procedure can be summarized into five steps as follows:

1. Perform P random permutations on the input vector with dimension n, $\mathbf{x} \in \mathbb{R}^n$.
2. Select the first K items of the permuted $\mathbf{x}$. Choose the largest element within the K items.
3. Record the corresponding index values in bits.
4. Step 1–step 3 are repeated m times, yielding a hash code of length m, which can be compactly represented using $m\lceil log_2 K \rceil$ bits.

WTA is indeed a special instance of Locality Sensitive Hashing (LSH) [24], which is primarily used to reduce the dimensionality of high-dimensional data by hashing the input items so that similar items map to the same "buckets" with high probability where the number of buckets being much smaller than the input items.

Formally, the definition of LSH is given as follows:

Definition 1. *A LSH is a probability distribution on a family H of hash functions h such that $P[h(X) = h(Y)] = S(X, Y)$.With a similarity measure function, S define on the collection of object X and Y.*

The key ingredient of the LSH is the hashing of object collection X and Y by means of multiple (m to be exact) hash functions h_i, $i = 1, \ldots, m$. The use of h_i enables approximation of the pair-wise distance of X and Y in terms of collision probability. LSH ensures that X and Y with high similarity renders higher probability of collision in the hashed domain; on the contrary, the data points far apart each other result a lower probability of hash collision.

$$P_{h\in H}(h_i(X) = h_i(Y)) \leq p_1, \text{if } S(X,Y) < \epsilon_1$$

$$P_{h\in H}(h_i(X) = h_i(Y)) \geq p_2, \text{if } S(X,Y) > \epsilon_2$$

Given that, $p_2 > p_1$, while $X, Y \in \mathbb{R}^n$, and $H = \{h : \mathbb{R}^n \rightarrow M\}$, where M is the hashed metric space depends to similarity function defined by S, i refers to the number of hash functions h.

3 Proposed Method

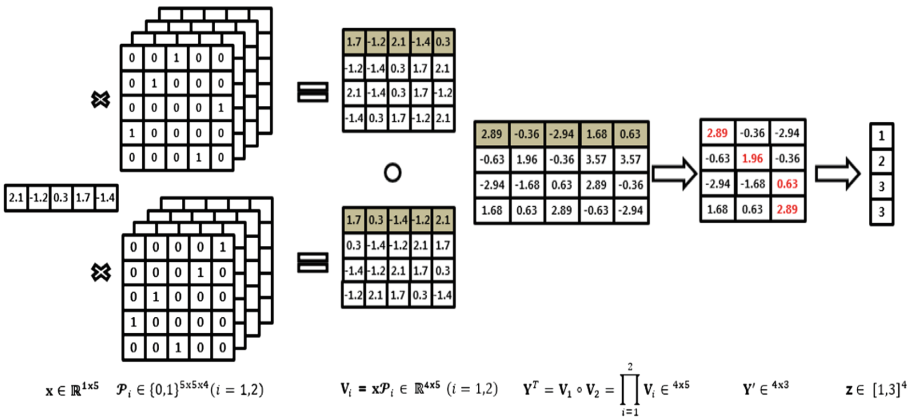
In this section, we present a ranking based hashing as a means of cancellable biometrics construct. Assume an input feature vector $\mathbf{x} \in \mathbb{R}^n$, the hashed code is generated according to the procedure as follows:

1. Generate p number of 3D permutation arrays that made by stacking up m n x n permutation matrices $\boldsymbol{\mathcal{P}}_i \in \{0,1\}^{n\times n\times m}$, $i = 1,\ldots,p$ where m is the desired length of resulting hashed code and $m > n$. Note a permutation matrix is a square binary matrix that has exactly one entry of 1 in each row and each column and 0 s elsewhere. $\boldsymbol{\mathcal{P}}_i$ is user-specific.
2. Multiplying $\mathbf{x}$ to $\boldsymbol{\mathcal{P}}_i$, yield a matrix, $\mathbf{V}_i = \mathbf{x}\boldsymbol{\mathcal{P}}_i \in \mathbb{R}^{n\times m}$, $i = 1,\ldots,p$.
3. Perform Hadamard product (element-wise product) yields $\mathbf{H} = \prod_{i=1}^{p} \mathbf{V}_i \in^{n\times m}$ where p is Hadamard product order.
4. Discard last $n - k$ column vectors from $\mathbf{H}$, yields $\mathbf{H}' \in \mathbb{R}^{k\times m}$, where we named k as window size.
5. For each row vectors of $\mathbf{H}'$ the *indices of the largest magnitude entry* are recorded and form a discrete hashed code, $\mathbf{h} \in [1\, k]^m$.

Note the proposed ranking based hashing is not exactly identical to WTA hashing described in Sect. 2 in the sense that our method is reformulated into a mathematically equivalent non-iterative matrix form instead of WTA iterative algorithmic form. Furthermore, Hadamard product is introduced to enhance the security and privacy protection strength. Figure 1 illustrates the proposed ranking based hashing.

Similar to WTA hashing that follows LSH theory that strives to ensure two similar biometric vectors renders higher probability of match (collision) in the rank domain, and vice versa for the vectors that are far apart to each other. Indeed, each entry $\boldsymbol{h}_i$ in the hashed code $\mathbf{h}$ (step 5) can be seen as a LSH projected instance of biometric vector $\mathbf{x} \in \mathbb{R}^n$ i.e. $\boldsymbol{h}_i = h(\mathbf{x}) \in [1, k]$ where $h(\mathbf{x}) \in \{j \mid \max_j(\text{trunc}_k(\prod_{i=1}^{p} \mathbf{x}\boldsymbol{\mathcal{P}}_i))\}$, $\boldsymbol{\mathcal{P}}_i \in \{0,1\}^{nxnx1}$, index j and $\text{trunc}_k()$ refers to a function that discards last m-k entries of a vector.

Suppose two ranking based hashed codes, enrolled $\mathbf{h}^e$ and query $\mathbf{h}^q$ generated from fingerprint vector $\mathbf{x}^e$ and $\mathbf{x}^q$ respectively, the probability of match can be calculated by counting the number of agreed position (i.e. indices of $\mathbf{h}$) between $\mathbf{h}^e$and $\mathbf{h}^q$ over m as



2.1 -1.2 0.3 1.7 -1.4
$\mathbf{x} \in \mathbb{R}^{1\times5}$
$\mathcal{P}_i \in \{0,1\}^{5\times5\times4} (i = 1,2)$
$\mathbf{V}_i = \mathbf{x}\mathcal{P}_i \in \mathbb{R}^{4\times5} \; (i = 1,2)$
$\mathbf{Y}^T = \mathbf{V}_1 \circ \mathbf{V}_2 = \prod_{i=1}^{2} \mathbf{V}_i \in {}^{4\times5}$
$\mathbf{Y}' \in {}^{4\times3}$
$\mathbf{z} \in [1,3]^4$

Fig. 1. Illustration of ranking based hashing with $n = 5$, $p = 2$, $k = 3$ and $m = 4$. Note $m > n$ in our experiment, yet the parameters ($n = 5$, $m = 4$) in figure 1 is only for illustration.

$\mathrm{P}\left[\mathrm{h}_{\mathrm{i}}^{\mathrm{e}} - \mathrm{h}_{\mathrm{j}}^{\mathrm{q}}\right] = \mathrm{S}(\mathrm{x}, \mathrm{y})$ for $i = 1, \ldots, m$. As a WTA hashing instance, $S(\mathbf{x}, \mathbf{y})$ represents the similarity measure between two hashed codes that corresponds to the rank correlation measurement (a type of ordinal measure [18, 20]) of $\mathbf{x}^e$ and $\mathbf{x}^q$. This suggested the similarity would preserve as the hashed codes collision.

In the event of template compromised, a new hashed code can be re-issued by repeating the above 5-step procedure. The effectiveness of cancellability is experimentally verified in Sect. 5.3.

In real world scenario, the permutation seed is user-specific for cancellability. However, lost token/seed case should be primary attended, as it is closely associated to accuracy performance, security and privacy attacks [1, 19]. To evaluate the lost token scenario, our experiment is performed with same permutation seed for all subjects (presented in Sect. 4.2).

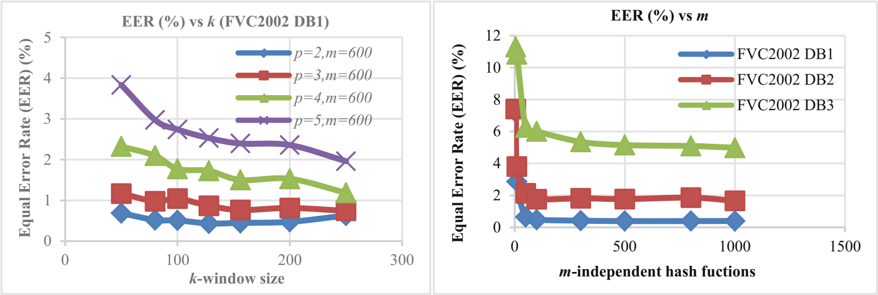
4 Experiments and Discussions

In this paper, a real-valued fixed-length fingerprint vector with size 299 that generated from MCC and Kernel Principal Component Analysis [21] is used as input to evaluate the proposed method. We refer the readers for the details about the fingerprint vector construction in [22]. The evaluations are conducted on six public fingerprint datasets, FVC2002 (DB1, DB2, DB3) [23] and FVC2004 (DB1, DB2, DB3) [23]. Each dataset consists of 100 users with 8 samples per user. In total, there are 800 (100 × 8) fingerprint images in each dataset. The performance accuracy of the proposed method is assessed using Equal Error Rate (EER) and the genuine-imposter distribution. Noted that since the random permutation is applied, to avoid the bias of single random permutation, the EERs is calculated by taking the average of EER repeated for 5 times. The fixed-length feature vector generated from fingerprint is described in [22].

For matching protocol, as described in [22], 1st to 3rd samples of each identity are used as training samples to generate the fingerprint vector; the rest samples (i.e. 4th–8th) of each identity are used in this experiment. There are totally 500 (100 × 5) samples used for experiment. Within this subset of data, The Fingerprint Verification Competition (FVC) [23] protocol is applied across the six data sets, which yields 1000 genuine matching scores and 4950 imposter matching scores for each data set.

4.1 Effect of Window Size *k*, Hadamard Product Order *p*, and Number of Hashing Functions *m*

We first investigate the effect of window size *k* with respect to the performance in terms of EER. In this experiment, *k* is varied from 50, 80, 100, 128, 156, 200 to 250 with $m = 600$. The identical setting is repeated for $p = [2, 3, 4, 5]$. Figure 2(a) shows the curves of "EER (%)-vs-*k*" for FVC2002 DB1. Note we repeat the same experiments for DB2 and DB3, but only DB 1 is shown as all experiments exhibit the same performance trend.



(a) (b)

Fig. 2. (*a*) The curves of "EER (%) vs *k*"; (*b*) The curves of "EER (%) vs *m*"

We can observe that:

(1) The EER drops gradually when larger *k* is applied and levels off when *k* becomes large. This is not a surprise as small *k* implies less feature components are taken into account, which leads to insufficient discriminability; while larger *k* indicates more salient features are included;

(2) The smaller *p*, the lower EER. Step 3 described in Sect. 3 tells us that the Hadamard product is carried out by element-wise multiplying *p* permuted fingerprint vector in $\mathbf{x}$ i.e. $\bar{\mathbf{x}}(j) = \prod_{l=1}^{p}(\hat{\mathbf{x}}_l(j))$. Such an operation heightens the hardness against inversion at the expense of introducing distortion in the product code. Thus, it is expected that the performance drops with large *p*. This also demonstrates the common trade-off exists in cancellable biometric scheme, namely performance-security trade-off.

We also examine the relation of the number of hashing functions m and EER. Evaluation has been carried out by increasing the m from 5, 10, 50, 100, 300, 500, 800 and 1000 while fixing $k = 250$, and $p = 2$. As expected, a better EER can be gained with respect to the increment of m and level off at large m as illustrated in Fig. 2(b). This performance pattern is expected as the large m increases the collision probability of two highly similar hashed codes and vice versa, which is theoretically assured by the WTA hashing.

4.2 Accuracy Performance Evaluation

In this section, the accuracy performance experiments on FVC2002 and FVC2004 using the best parameters found in the previous section is carried out. Table 1 presents the accuracy performance as well as comparisons with the baseline systems and BTP schemes. The accuracy performance of ranking based hashing gradually decreases in FVC2002 (DB1 and DB2) and FVC2004 DB1 while remains approximately 3%-5% of deterioration in the rest of data sets. Such deterioration is expected, as the discriminate features are likely to be permuted out of the k-window. However, the use of user-specific seed compensates the loss of discriminate features; thus, the accuracy in genuine-token case is comparable to its original vector counterpart [18] and MCC [9]. This suggests that the ranking based hashing demands higher discriminative features in order to preserve accuracy. Nevertheless, the proposed method mostly outperforms state-of-the-arts [10, 17, 24] in which same datasets and protocol are adopted.

Table 1. Performance accuracy and comparison.

FVC2002			FVC2004		
DB1	DB2	DB3	DB1	DB2	DB3
Without template protection					
MCC [9]					
0.60%	0.59%	3.91%	3.97%	5.22%	3.82%
Fixed-length representation [23]					
0.20%	0.19%	2.30%	4.70%	3.13%	2.80%
With template protection					
Proposed (lost token case)					
0.43%	**2.**10%	**6.60%**	**4.51%**	**8.**02%	**8.**46%
Proposed (genuine token)					
0.20%	**0.**88%	**1.94%**	**0.44%**	**3.08%**	**2.**91%
2P-MCC64,64 [10]					
3.3%	1.8%	7.8%	6.3%	–	–
Bloom filter [25]					
2.3%	1.8%	6.6%	13.4%	8.1%	9.7%
Wang and Hu [17]					
4%	3%	8.5%	–	–	–

5 Privacy and Security Analysis

In this section, we provide the privacy and security analysis that consists of (1) non-invertibility/irreversibility analysis; (2) brute force attack and false accept attack; (3) revocability; (4) non-linkability analysis.

5.1 Noninvertibility/Irreversibility Analysis

Non-invertibility/Irreversibility analysis, a privacy analysis, refers to the computational hardness in restoring the fingerprint vector from the hashed code with and without information associated to hashing algorithm.

Here, we assume the adversary manages retrieve the hashed codes and he knows well the hashing algorithm as well as the corresponding parameters (e.g. *m, k, p* and permutation seeds). We noted that the proposed ranking based hashing converts the real-valued fingerprint feature into the index value. Hence, it is reasonable to assume there is no clue for an adversary to guess the fingerprint vector information directly from the stolen hashed code alone or even with the parameters.

The only way for the adversary to attack is to guess the real-value features directly. In the worst case, the adversary learns the minimum and maximum values of the feature components. Let's take FVC2002 DB1 as an example, the minimum and maximum values of the feature components are −0.2504 and 0.2132 respectively. The adversary has to examine from −0.2504, −0.2503, −0.2502 and so on, until 0.2132. Thus, there are 4636 possibilities. In our implementation, the precision is fixed at four decimal digits, the possibility of guessing a single feature component of fingerprint vector requires 4636 attempts $(\approx 2^{12})$ Thus, the 299 feature components of a fingerprint vector require around $2^{12\times 299} = 2^{3588}$ attempts in total. The possibilities to correctly guess a single and entire feature components are given in Table 2. Obviously, such combinations are computationally infeasible.

Table 2. Complexity to invert single and entire feature components

Databases	Min value	Max value	Possibilities for single feature component	Total possibilities for entire feature
FVC2002 DB1	−0.2504	0.2132	$4636 \approx 2^{12}$	$2^{12\times 299} = 2^{3588}$
FVC2002 DB2	−0.2409	0.2484	$4893 \approx 2^{12}$	$2^{12\times 299} = 2^{3588}$
FVC2002 DB3	−0.1919	0.2372	$4291 \approx 2^{12}$	$2^{12\times 299} = 2^{3588}$

Table 3. False accept attack complexity

Databases	τ	m	$\tau \times m$	k	Minimum attack complexity
FVC2002 DB1	0.11	600	66	$128 = 2^7$	$(2^7)^{66} = 2^{462}$
FVC2002 DB2	0.08	600	48	$250 \approx 2^8$	$(2^8)^{48} = 2^{384}$
FVC2002 DB3	0.05	600	30	$250 \approx 2^8$	$(2^8)^{30} = 2^{240}$

5.2 Brute Force Attack and False Accept Attack

Brute-force attack is an instance of security attacks, which meant to gain the illegitimate access, with feasible attack complexity to the biometric system by means of the randomly generated hashed code. We quantitatively analyze the required complexity to break the proposed method. For the realization, assume that the optimal parameters for the best performance are set to m = 600 and k = 128. Since the indices of hashed code taking a value between 1 and 128, the guess complexity for each entry is $k = 128 = 2^7$ and thus 600 entries require 2^{4200} attempts that are far beyond to reach by the present computing facility.

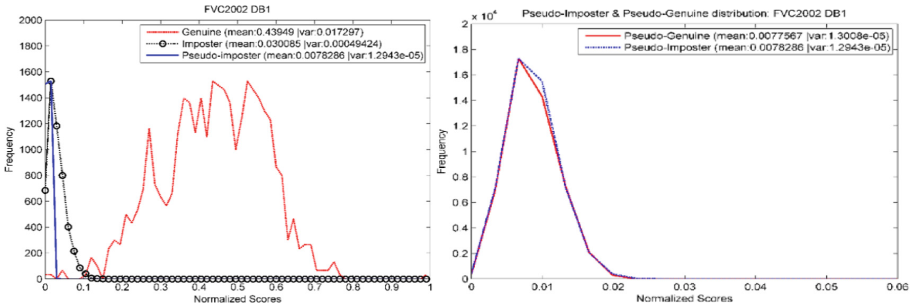
On the other hand, unlike the brute force attack, false accept attack (dictionary attack) may requires far less number of attempts to gain illegitimate access. In fact, biometric systems make decision based on the system threshold value, the access would be granted as long as the matching score succeeds the pre-defined threshold τ, which can significantly reduce the attack effort.

Let we take the best performing parameters from the FVC2002DB1 experiments in Sect. 4.1, i.e. m = 600 and k = 128, the decision threshold τ observed at this setting is 0.11. Hence, the minimum number of agreed (collided) entries in the hashed codes pair for successful access is mere $\tau \times m = 0.11 \times 600 = 66$. The window size k indicates 128 possible indices values that is equivalent to 2^7 $\left(= 2^{\log_2 k}\right)$ guessing effort is required for an entry. Therefore, the false accept attack complexity can be estimated from $\left(2^{\log_2 k}\right)^{\tau \times m}$. The complexity calculated is shown in Table 3, we observe that the attack complexity reduced to 2^{462} compare to 2^{4200} in brute force attack for FVC2002DB1 and the complexity reduction appears identical for the rest of testing data sets. However, we note that the reduced attack complexity is still favorably high to resist the false accept attack.

5.3 Revocability

Revocability is evaluated by conducting the experiment where 100 hashed codes of each fingerprint vector are generated with 100 sets distinct random permutation seeds, and then the first hashed code is matched with the other 100 hashed codes. The entire process is repeated and produces 100 × (5 × 100) = 50000 pseudo-imposter scores. The genuine, imposter, and pseudo-imposter distribution are computed with $p = 2, k = 128, m = 600$ as depicted in Fig. 3(a).

Note that the numbers of scores are different for the imposter and pseudo-imposter matching. This is because in pseudo- imposter matching, we only focus on the matching scores between the first hashed code and the newly generated hashed code for each fingerprint vector (same user). From Fig. 3, a large degree of overlapping occurs between the imposter and pseudo-imposter distributions. This implies the newly generated hashed codes with the given 100 random permutation seeds are distinctive despite it is generated from the identical fingerprint vector. In terms of verification performance, we obtain EER = 0.16% in which intersection of genuine and pseudo-imposter distribution is taken. This verifies that the proposed method satisfies the revocability property requirement.



(a) (b)

Fig. 3. (*a*) The genuine, imposter, and pseudo-imposter distribution: $p = 2$, $k = 128$, $m = 600$ on FVC2002 DB1; (*b*) Pseudo-imposter & pseudo-genuine distribution on FVC2002 DB1.

5.4 Non-linkability

To examine the non-linkability or our scheme, we introduce the *pseudo-genuine scores*, which refer to the matching scores between two hashed codes under different fingerprint's vector of the same individual (using different permutation seeds). This resembles the genuine matching that yields 1000 scores. Recall the pseudo-imposter score used under Sect. 5.2, when the pseudo-imposter and pseudo-genuine distributions are overlapped, it implies that the hashed codes generated from the same user or from the others are not differentiable. On the contrary, if both distributions are separated far apart, this offers the advantages to an adversary to differentiate the hashed code from the identical individual. The difficult in differentiating the hashed codes contributed to the non-linkability. Figure 3(b) illustrates the pseudo-imposter and pseudo-genuine distribution plot where the pseudo-imposter and pseudo-genuine distribution are largely overlapped hence, supports the non-linkability property.

6 Conclusion

In this paper, we presented a cancellable ranking based hashing for fingerprint template protection. The hashed codes can largely preserve accuracy performance with respect to its original counterparts thanks to the nice property that inherited from WTA hashing. The scheme is also shown satisfy both non-linkability and revocability criteria. The hashed code is strongly resilient against the non-invertibility analysis due to its indices representation that carry no information about original biometric data. We also demonstrate its resilience to brute force and dictionary attacks. Our future work consists of two directions. The first direction is to extend the work to unordered variable-sized representation such as fingerprint minutiae. The second direction is to integrate with biometric cryptosystem primitives such as Fuzzy Vault, Fuzzy Commitment etc., which would be a strong complement for cryptographic keys generation and protection purposes.

Acknowledgement. This work was supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIT) (No. 2016-0-00097, Development of Biometrics-based Key Infrastructure Technology for On-line Identification).

References

1. Teoh, A.B.J., Goh, A., Ngo, D.C.L.: Random multispace quantization as an analytic mechanism for BioHashing of biometric and random identity inputs. IEEE Trans. Pattern Anal. Mach. Intell. **28**(12), 1892–1901 (2006)
2. Jain, A.K., Nandakumar, K., Nagar, A.: Biometric template security. EURASIP J. Adv. Sig. Process. **2008**, 579416 (2008)
3. Ratha, N.K., Chikkerur, S., Connell, J.H., Bolle, R.M.: Generating cancelable fingerprint templates. IEEE Trans. Pattern Anal. Mach. Intell. **29**(4), 561–572 (2007)
4. Rathgeb, C., Uhl, A.: A survey on biometric cryptosystems and cancelable biometrics. EURASIP J. Inf. Secur. **2011**(1), 3 (2011)
5. Patel, V.M., Ratha, N.K., Chellappa, R.: Cancelable biometrics: a review. IEEE Sig. Process. Mag. **32**(5), 54–65 (2015)
6. Natgunanathan, I., Mehmood, A., Xiang, Y., Beliakov, G., Yearwood, J.: Protection of privacy in biometric data. IEEE Access **4**, 880–892 (2016)
7. Nandakumar, K., Jain, A.K.: Biometric template protection schemes: bridging the performance gap between theory and practice. IEEE Sig. Process. Mag. **32**(5), 88–100 (2015)
8. Ferrara, M., Maltoni, D., Cappelli, R.: Noninvertible minutia cylinder-code representation. IEEE Trans. Pattern Anal. Mach. Intell. **7**(6), 1727–1737 (2012)
9. Cappelli, R., Ferrara, M., Maltoni, D.: Minutia cylinder-code: a new representation and matching technique for fingerprint recognition. IEEE Trans. Pattern Anal. Mach. Intell. **32** (12), 2128–2141 (2010)
10. Ferrara, M., Maltoni, D., Cappelli, R.: A two-factor protection scheme for MCC fingerprint templates. In: 2014 International Conference of the Biometrics Special Interest Group, pp. 1–8 (2014)
11. Rathgeb, C., Breitinger, F., Busch, C., Baier, H.: On application of bloom filters to iris biometrics. IET Biom. **3**(4), 207–218 (2014)
12. Gomez-Barrero, M., Rathgeb, C., Galbally, J., Fierrez, J., Busch, C.: Protected facial biometric templates based on local gabor patterns and adaptive bloom filters. In: ICPR, pp. 4483–4488, August 2014
13. Li, G., Yang, B., Rathgeb, C., Busch, C.: Towards generating protected fingerprint templates based on bloom filters. In: 2015 International Workshop on Biometrics and Forensics, pp. 1–6 (2015)
14. Hermans, J., Mennink, B., Peeters, R.: When a bloom filter becomes a doom filter: security assessment of a novel iris biometric template protection system. In: Proceedings of the Special Interest Group on Biometrics, Darmstadt, pp. 1–6, September 2014
15. Bringer, J., Morel, C., Rathgeb, C.: Security analysis of bloom filter-based iris biometric template protection. In: Proceedings of International Conference on Biometrics (ICB), pp. 527–534 (2015)
16. Sandhya, M., Prasad, M.V.K.: k-Nearest Neighborhood Structure (k-NNS) based alignment-free method for fingerprint template protection. In: ICB 2015, pp. 386–393 (2015)
17. Wang, S., Hu, J.: A blind system identification approach to cancelable fingerprint templates. Pattern Recognit. **54**, 14–22 (2016)

18. Yagnik, J., Strelow, D., Ross, D.A., Lin, R.-S.: The power of comparative reasoning. In: IEEE ICCV, pp. 2431–2438 (2011)
19. Nagar, A.: Biometric template security. Ph.D. dissertation, Department of Computer Science and Engineering, Michigan State University (2012)
20. Bhat, D., Nayar, S.: Ordinal measures for visual correspondence. In: Proceedings of CVPR, pp. 351–357 (1996)
21. Schölkopf, B., Smola, A., Müller, K.R.: Nonlinear component analysis as a kernel eigenvalue problem. Neural Comput. **10**, 1299–1319 (1998)
22. Jin, Z., Lim, M.H., Teoh, A.B.J., Goi, B.M., Tay, Y.H.: Generating fixed-length representation from minutiae using kernel methods for fingerprint authentication. IEEE Trans. Syst. Man Cybern. Syst. **40**(10), 1415–1428 (2016)
23. BioLab: FVC2002, FVC2004. http://bias.csr.unibo.it
24. Indyk, P., Motwani, R.: Approximate nearest neighbors: towards removing the curse of dimensionality. In: Proceedings of 30th Symposium on Theory of Computing (1998)
25. Abe, N., Yamada, S., Shinzaki, T.: Irreversible fingerprint template using Minutiae Relation Code with Bloom Filter. In: IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS), Arlington, pp. 1–7 (2015)