Irreversible Fingerprint Template using Minutiae Relation Code with Bloom Filter

Narishige Abe, Shigefumi Yamada and Takashi Shinzaki
FUJITSU LABORATORIES LTD.
1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki, 211-8588, Japan
abe.narishige@jp.fujitsu.com, yamada.shige@jp.fujitsu.com, shinzaki@jp.fujitsu.com

Abstract

Template protected fingerprint authentication techniques have been proposed, which enables to create an irreversible fingerprint template. In this paper, we propose a new irreversible template creation technique using Minutiae Relation Code(MRC) which can describe the minutiae information efficiently, and Bloom Filter which can realize the irreversibility feature. We evaluate the authentication accuracy and security factors such as Shannon Entropy and the number of attack possibilities using FVC2002 and FVC2004 DBs. As a result, our proposed method can achieve 1.8% EER in FVC2002 DB2 with 2^{49} attack possibilities.

1. Introduction

Recently, template protection techniques have become more important in order to protect a raw biometric information. It is necessary to convert from a fingerprint image to a vectorized feature to use most template protection schemes, such as Fuzzy Vault, Fuzzy Commitment, and Bloom Filter.

Actually, many algorithms describing fingerprint characters with simple vector data have been proposed. These algorithms can be classified into two categories, image-based or minutiae-based techniques.

In terms of a fingerprint-specific descriptor, Jain et al.[10] proposed a fingerprint image description method called *FingerCode*, which was based on Gabor filter responses around an upper core region. Texture-based fingerprint descriptors have been proposed, such as using local ridge orientation by Tico et al.[16], ridge orientation and frequency information by Qi et al.[14][17]. Feng et al.[6] proposed a combination method of a texture-based feature and minutiae, which can create 17 dimensional vector data including orientation and minutiae information as a descriptor.

In minutiae-based techniques, Xu et al. proposed spectral information extracted from a minutiae two dimensional distribution, and they developed description techniques using position information of minutiae and orientation information[21][22] and quality information[19], and minutiae subsets[20]. Nandakumar[13] proposed a description technique using not only global phase information, but also local phase information of a minutiae distribution. Minutiae Cylinder-Code (MCC)[5] is a well known representation of a fingerprint proposed by Capelli et al. Furthermore, minutiae-triplets[11][23] are based on local minutiae distribution information, whose templates have a set of features describing minutiae triangles.

In terms of enhancing security for stored templates, there are many fingerprint template protection schemes[9] using previous fingerprint descriptors, such as spectral minutiae information, minutiae phase spectrum(MPS) with a fuzzy commitment scheme[12], and MCC with an invertible convert scheme[8]. Wei et al.[18] proposed Multi-line code (MLC) for fingerprint template protection, which is an expansion concept of MCC. Furthermore, Ferrara et al. proposed the new revocable MCC-based fingerprint authentication technique(2P-MCC) by using the two-factor protection scheme in [7].

Although some vector-base descriptors, such as MPS, MCC, MLC can be described by some relation information among minutiae, it is difficult to represent any relation information among arbitrary minutiae such as isolated minutiae and the minutiae located at the edge area in the fingerprint, since they are designed only for using local/global minutiae distribution. Actually, minutiae-triplets can handle a sort of a relation information between minutiae, however, it is difficult to describe *neighbor information* of the relation.

In this paper, we propose an efficient irreversible fingerprint technique by combining MRC[4] and Bloom Filter. MRC consists of a set of vector-represented relation information between arbitrary minutiae, which enables to create a useful fingerprint template by handling boarder minutiae and isolated minutiae efficiently.

Regarding the rest of this paper, we describe what the

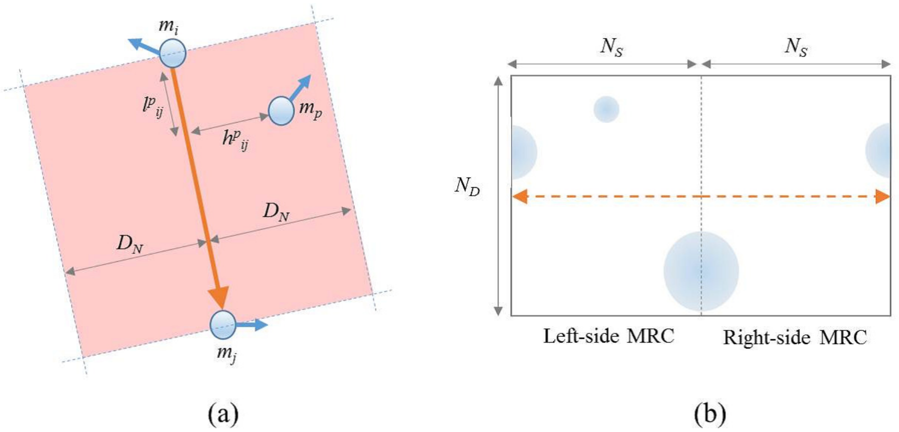

Figure 1. Example of minutiae distribution. (a) An example minutiae distribution. (b) The created MRC information from (a).

MRC is, and how to extract/match it in section 2 briefly, and we discuss the security factors and the authentication accuracy regarding our proposing method using two public fingerprint databases,FVC2002 and FVC2004, in section 4. Finally, we summarize our contribution in this paper and describe the future works in section 5.

2. Minutiae Relation Code

As Fig. 1 shows, MRC information can be represented as a two dimensional image, which includes not only two minutiae information but also neighbor minutiae information. We explain about the way to construct MRC in section 2.1, and how to compare MRCs in section 2.2.

2.1. How to construct MRC

Let $M = \{m_i\}_{i=1}^{N_M}$ be a minutiae set extracted from a fingerprint image I, and N_M be the number of the minutiae. The minutiae information is defined by the following equation,

$$m_i = (x_i, y_i, \theta_i). \tag{1}$$

Where x_i, y_i represents the position of the *i-th* minutiae and θ_i represents its angle. Let's think about an MRC between m_i and m_j, and let m_p be a neighbor minutiae which is located within the length D_N against the relation(Pink region in Fig. 1). In order to calculate the MRC, we calculate h^p_{ij} and l^p_{ij} in advance. First, h^p_{ij} can be calculated by the following equation,

$$h^p_{ij} = |\boldsymbol{v}_{ip}| \cdot sin\theta. \tag{2}$$

Here, $\sin\theta$ can be also calculated from the definition of the cross product between $\boldsymbol{v}_{ij}$ and $\boldsymbol{v}_{ip}$.

$$sin\theta = \frac{\boldsymbol{v}_{ip} \times \boldsymbol{v}_{ij}}{|\boldsymbol{v}_{ip}||\boldsymbol{v}_{ij}|} \tag{3}$$

$$\because \boldsymbol{v}_{ip} \times \boldsymbol{v}_{ij} = |\boldsymbol{v}_{ip}||\boldsymbol{v}_{ij}|sin\theta \tag{4}$$

Therefore, h^p_{ij} can be calculated by the following equation,

$$h^p_{ij} = \frac{|\boldsymbol{v}_{ip} \times \boldsymbol{v}_{ij}|}{L_{ij}}. \tag{5}$$

And, l^p_{ij} can be calculated easily using h^p_{ij}.

$$l^p_{ij} = \sqrt{L^2_{ij} - {h^p_{ij}}^2} \tag{6}$$

Where, L_{ij} represents a Euclidean distance between m_i and m_j, $\boldsymbol{v}_{ij}$ is a vector from m_i to m_j. Let N_S be the number of divided space information, and N_D the number of divided direction information, a MRC represents $N_S \times N_D$ matrix, and let S^l_{nm} be a set of neighbor minutiae on the left, S^r_{nm} a set of neighbor minutiae on the right, then the MRC can be calculated by the following equation,

$$lMRC_{ij}(s,t) = \sum_{p \in S^l_{nm}} f(s, l^p_{ij}, \sigma_S) \cdot f(t, h^p_{ij}, \sigma_D), \tag{7}$$

$$rMRC_{ij}(s,t) = \sum_{p \in S^r_{nm}} f(s, l^p_{ij}, \sigma_S) \cdot f(t, h^p_{ij}, \sigma_D), \tag{8}$$

$$f(x,c,\sigma) = exp\left(-\frac{(x-c)^2}{2\sigma^2}\right), \tag{9}$$

$$0 \le s < N_S, 0 \le t < N_D. \tag{10}$$

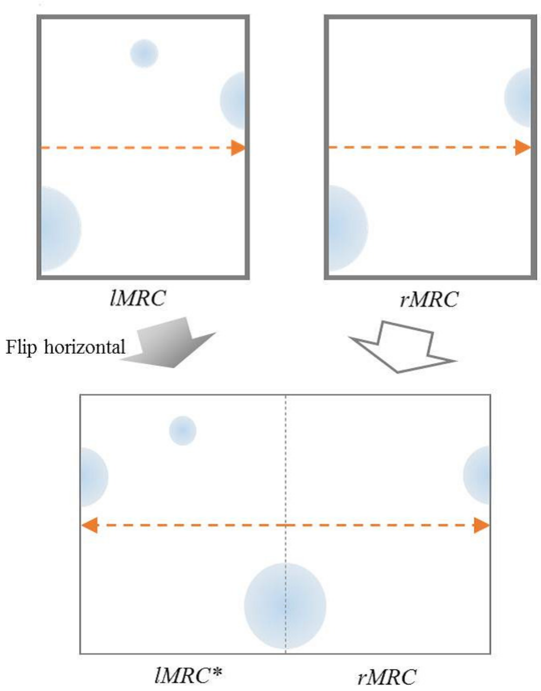

Figure 2. The construction of MRC.

Here, a MRC information should be separated to a left MRC($lMRC$) and a right MRC($rMRC$) in order to distinguish on which side minutiae are located. m_p can be assigned to the sets S^l_{nm} or S^r_{nm} by the following equation,

$$\begin{cases} m_p \in S^l_{nm} & |\boldsymbol{v}_{ip} \times \boldsymbol{v}_{ij}| > \epsilon \\ m_p \in S^r_{nm} & |\boldsymbol{v}_{ip} \times \boldsymbol{v}_{ij}| < \epsilon \\ m_p \in S^l_{nm}, S^r_{nm} & -\epsilon \leq |\boldsymbol{v}_{ip} \times \boldsymbol{v}_{ij}| \leq \epsilon \end{cases} \tag{11}$$

Then, MRC_{ij} between m_i and m_j can be calculated by concatenating $lMRC_{ij}$ and $rMRC_{ij}$,

$$MRC_{ij} = [lMRC^*_{ij} | rMRC_{ij}]. \tag{12}$$

Where $*$ represents a permutation of a matrix in order to adjust $lMRC_{ij}$ to the institute visual image(see Fig.2). Then, MRC_{ij} can be represented as $2 \cdot N_S \times N_D$ matrix.

Additionally, in order to convert to a bit-order representation, we normalize and quantize MRC_{ij}. Let c_{energy} be the summation value of MRC_{ij}, N_{norm} be the normalization factor, th be the bit-quantization threshold. The bit-ordered $bMRC_{ij}$ can be calculated by the following equation,

$$bMRC_{ij} = \begin{cases} 1 & MRC_{ij} \cdot N_{norm}/c_{energy} > th \\ 0 & MRC_{ij} \cdot N_{norm}/c_{energy} \leq th \end{cases} \tag{13}$$

The number of all possible relations is ${}_{N_M}P_2$, however, it can be decreased in order to avoid ambiguous relations. To be more specific, we introduce the limitation on the distance between a minutiae pair. MRCs should be calculated to meet the following inequality,

$$A = \{(i,j) | L_{min} < L_{ij} < L_{max}\}. \tag{14}$$

Finally, a template T of the image I can be described by the following,

$$T = \{i, j, L_{ij}, MRC_{ij}\}_{i,j \in A}. \tag{15}$$

2.2. How to calculate similarity between MRCs

2.2.1 Calculation of a raw score

Let's think about two templates, T_1 and T_2, and let MRC^1_{ij} be an MRC between i-th and j-th minutiae in T_1. At first, a distance function F_{fd} between two MRCs, MRC_{ij}, and MRC_{uv} is defined as,

$$F_{fd}(MRC_{ij}, MRC_{uv})$$

$$= \sum_{s=1}^{N_S} \sum_{t=1}^{N_D} |MRC_{ij}(s,t) - MRC_{uv}(s,t)|. \tag{16}$$

If MRCs are described as bit-order representations, $F_{fd}(\cdot,\cdot)$ could be hamming distance. At first, we prepare two tables, a *vote_score_table*(vst) to tabulate voting counts and a *feature_score_table*(fst) for storing the minimum MRC distance, which are $N_S \times N_D$ matrices. Then, vst and fst are updated by the algorithm 1.

Algorithm 1 uses greedy search to find the best minutiae pairs between T_1 and T_2, which generally requires high computational power depending on the number of minutiae pairs. For the sake of skipping inappropriate calculation, we use the length information L_{ij} since it is not necessary to vote on a pair whose length of the MRCs is longer than D_R.

Algorithm 1 Calculate a *vote_score_table* and a *feature_score_table*

```
$vst \Leftarrow 0$
$fst \Leftarrow max\_value$
for all $i, j, u, v$ such $abs(L^1_{ij} - L^2_{uv}) < D_R$ do
    $[i, j, u, v] \Leftarrow [i, j, u, v | min(F_{fd}(MRC^1_{ij}, MRC^2_{uv})]$
    $min\_score \Leftarrow F_{fd}(MRC^1_{ij}, MRC^2_{uv})$
    $vst(i, u) \Leftarrow vst(i, u) + 1$
    $vst(j, v) \Leftarrow vst(j, v) + 1$
    $fst(i, u) \Leftarrow min(fst(i, u), min\_score)$
    $fst(j, v) \Leftarrow min(fst(j, v), min\_score)$
end for
```

Then, we create a set vst_k which is created by sorting vst with respect to vote scores, and a set fst_k which consists of feature scores related to minutiae pairs with the smallest distance. Now, we calculate two scoring measures, voting scorevs and feature scorefs using the top K scores by the following equations,

$$vs = \frac{\sum_{k=1}^{K} vst_k}{n_v K}, \tag{17}$$

$$fs = \frac{\sum_{k=1}^{K} fst_k}{n_f K}. \tag{18}$$

Where n_v and n_f represent normalization factors. Here, The value K is related to a kind of *security factor*, which means that as K becomes greater, the number of minutiae pairs between a template and an input data must be large for an appropriate authentication. However, if an input fingerprint image is captured partially, it may be falsely rejected even though the image is taken from a genuine finger. On the other hand, if the value K is too small, the number of minutiae pairs is not enough for an authentication which may cause a false acceptance.

In this paper, we use vst in order to estimate appropriate K, which is defined by the following equation,

$$K = \#\{(vst(i,j) > \mu + 3\sigma\}, \tag{19}$$

$$\nu_{min} \leq K \leq \nu_{max}. \tag{20}$$

Where μ and σ represent the average and the standard deviation of vst respectively, and ν_{min} and ν_{max} represent the minimum number of the matched pairs and the maximum number of the matched pairs respectively, and $\#\{\cdot\}$ is a count function. This equation is designed for utilizing *reliable* minutiae pairs for score calculation which allows us to be able to compare the similarity score even though the number of overlapping minutiae is small.

At last, the raw score between T_1 and T_2 can be calculated by the following equation,

$$raw\_score = \alpha \cdot vs + (1 - \alpha) \cdot fs. \tag{21}$$

Where α is a weight to adjust the combination of vs and fs. As the equation says, raw_score is lower if the two templates are similar with each other.

3. Bloom Filter

Bloom Filter has a dimension reduction scheme to project an item to a probabilistic data structure, and the bloom filter is also used as a detector of the existence of the item in the data structure. This is why the bloom filter has some possibilities of false acceptance, however, there are no false rejection.

In this paper, we use the bloom filter with MRC. Fig. 3 represents the flow of our method. First, a random matrix whose size is $N_D \times 2N_S$ is created as a *helper data* which enables to re-generate different templates, then the masked MRC can be generated by calculating XOR between the helper data and the original MRC. The masked MRC is divided into the local blocks whose size is $b \times w$. Each column bits(b bits) are converted to a decimal number(0 to 2^b), and set 1 to the corresponding bit in the projection structure. In this scheme, an original bit is corresponding to the position in the projection structure directly. This conversion is conducted w times in each block, then converted code can be calculated. $\frac{N_D}{b} \times \frac{2N_S}{w}$ converted codes can be generated from an MRC. Finally, the converted codes for all MRCs are stored as a protected template.

Params	Value	Note
N_S	8	Space resolution in MRC
N_D	24	Direction resolution in MRC
D_N	32	Search distance for neighbor minutiae
L_{min}	16	The min distance to construct MRC
L_{max}	160	The max distance to construct MRC
σ_S	0.4	The sigma value for space
σ_D	1.1	The sigma value for direction
N_{norm}	300	The normalization factor for MRC
th	0	The threshold for bit-order conversion
D_R	8	The distance for matching MRC
ν_{min}	5	The min number of matching minutiae
ν_{max}	12	The max number of matching minutiae
α	0.89	The weight for vs and fs

Table 1. Used parameters.

4. Evaluations

4.1. Evaluation condition

In order to evaluate the authentication and security performance of MRC with Bloom Filter, we use a public fingerprint databases, FVC2002[1] and FVC2004[2]. We calculated matching scores with the same protocol in FVC, which involves 2,800 genuine matches and 4,950 impostor matches.

We implement extract and matching algorithms of MRC in C/C++. Evaluations are conducted on a PC (Windows 7 Professional x64, Intel Xeon CPU X3480 3.07GHz, 8GB RAM). The parameters for extraction/matching MRCs are shown in Table 1.

The precision of minutiae extraction is very important in obtaining better authentication accuracy, so a state-of-the-art minutiae extractor should be adopted. However, we used Verifinger SDK 6.0[3] as a minutiae extractor which allows interested third parties to conduct the same experiment.

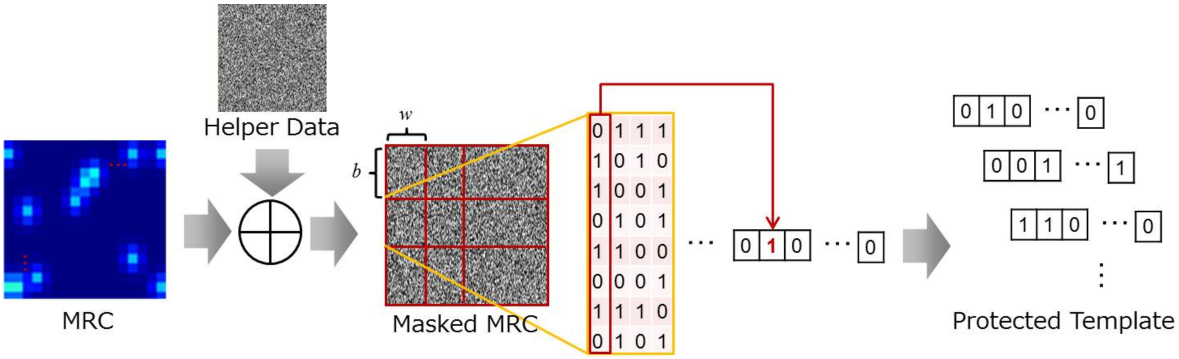

Figure 3. The flow of MRC with Bloom Filter.

4.2. Security evaluation

Each of the block size(b, w) is strongly related to the irreversible feature. In this section, we evaluate the security analysis of our proposing method using FVC2002 DB1. In order to estimate the irreversibility, Rathgeb et al.[15] proposed the following equation for the calculation of the number of possible codes,

$$g(N_b, N_w)$$

$$= \begin{cases} 1 & if N_b = 1 \\ N_b^l - \sum_{i=1}^{N_b-1} \binom{N_b}{i} \cdot g(i, N_w) & otherwise \end{cases} \quad (22)$$

Where N_b represents the number of 1 in a converted code. The number of correspondences between N_w original codes and bits set to 1 can be calculated. If using general hash function like SHA-1 and SHA-2, we have to determine the original codes by searching in the original code space. However, in this paper, an original code is correspondence with a specific bit in a converted code directly, which is why we do not have to consider it.

In [15], N_b is determined from the actual data. Since the position of the bit set to 1 means the existence of the original codeword, N_b can be seen as the number of useful bits in the data. In order to estimate the number of useful bits, we use the *Shannon Entropy*, which can be calculated by the following equation,

$$H = \lceil \sum_{i=1}^{n} \{-p_i(0) log_2 p_i(0) - p_i(1) log_2 p_i(1)\} \rceil. \quad (23)$$

Where $p_i(0)$, $p_i(1)$ represents the existence probability of 0, 1 respectively. N_b and N_w influence on not only the irreversibility but also the data size(see Table2). In this paper, the original data size of an MRC is 384bit, however, the size becomes large depending on the parameters. In order to save the data size, we chose 2,3,4,6 as the variations of N_b, and 2,4,8,16 as the variations of N_w.

		Word			
		2	4	8	16
bit	2	384bit	192bit	96bit	48bit
	3	512bit	256bit	128bit	64bit
	4	768bit	384bit	192bit	96bit
	6	2048bit	1024bit	512bit	256bit

Table 2. Data size.

The calculated Shannon entropy using each N_b, N_w are shown in Table 3. In addition, the number of possibilities is shown in Table 4. In the best case ($b = 6, w = 16$), the number of attack possibilities is 2^{49}. This results represent the value of a block in an MRC, which means that the actual value in a MRC is times by the number of blocks in the MRC. Furthermore, the number of attack possibilities increases depending on the number of MRCs in a fingerprint image.

In the viewpoint of authentication accuracy, we show the EERs in Table 5. In this experiment, the helper data is common to all fingerprint images. As the word size increases, the corresponding EER increases. However, the bit size does not influence on the accuracy. This is because the original code space is associated with the converted code space directly.

Although it is possible to create more secure templates by increasing the number of bit/word, the computational time increases too, which is why these parameters should be determined by depending on the system capacity and the necessary accuracy.

4.3. Authentication accuracy evaluation

In this section, we show the authentication accuracy using FVC2002 and FVC2004 with the FVC protocol. In addition to our results, in order to compare our method with the other fingerprint template protection techniques which

	FVC2002				FVC2004			
	DB1	DB2	DB3	DB4	DB1	DB2	DB3	DB4
Original	1.1%	1.1%	3.7%	2.7%	7.3%	6.2%	6.7%	3.5%
Bit4, Word8	2.3%	1.8%	6.6%	5.1%	13.4%	8.1%	9.7%	6.3%
Bit4, Word16	3.5%	1.8%	9.6%	7.4%	16.2%	10.4%	11.6%	9.1%
2P-MCC$_{64,64}$	3.3%	1.8%	7.8%	6.6%	6.3%	n/a	n/a	n/a
2P-MCC$_{64,48}$	4.6%	2.5%	9.9%	7.8%	8.4%	n/a	n/a	n/a
P-MCC$_{128}$	1.88%	0.99%	5.24%	4.84%	n/a	n/a	n/a	n/a
P-MCC$_{64}$	3.33%	1.76%	7.78%	6.62%	n/a	n/a	n/a	n/a
P-MCC$_{32}$	6.59%	4.29%	12.20%	11.19%	n/a	n/a	n/a	n/a
P-MCC$_{16}$	12.39%	10.16%	19.33%	17.70%	n/a	n/a	n/a	n/a
MPS	3.4%	3.8%	n/a	n/a	n/a	n/a	n/a	n/a

Table 6. The accuracy results(EERs). The results are cited from [8][12][7] respectively.

.

		Word			
		2	4	8	16
bit	2	2bit	2bit	3bit	3bit
	3	2bit	3bit	4bit	4bit
	4	2bit	3bit	5bit	6bit
	6	2bit	4bit	6bit	9bit

Table 3. Shannon entropy.

		Word			
		2	4	8	16
bit	2	2^1	2^4	2^{13}	2^{26}
	3	2^1	2^6	2^{16}	2^{32}
	4	2^1	2^6	2^{16}	2^{41}
	6	2^1	2^5	2^{18}	2^{49}

Table 4. The number of possibilities.

		Word			
		2	4	8	16
bit	2	1.2%	1.6%	2.0%	3.4%
	3	1.4%	1.6%	2.2%	3.5%
	4	1.4%	1.7%	2.3%	3.5%
	6	1.3%	1.7%	2.8%	3.6%

Table 5. The EERs in FVC2002 DB1.

have the irreversibility, the results of 2P-MCC(key stolen scenario), P-MCC and MPS are listed in Table 6.

In our proposed method, as we have already seen, EER changes depending on the word size in all DBs. In terms of the comparison of the other algorithms, our method can achieve the same or better results compared to 2P-MCC and MPS, however, P-MCC$_{128}$ obtains better EERs than our method. In P-MCC, the irreversibility changes drastically depending on the reduction bit size(from 16 to 128), and the percentage of the number of reconstructed minutiae is up to 23.5%, 22.4% using P-MCC$_{128}$ and P-MCC$_{64}$ respectively in [8]. On the other hand, our method can achieve 2^{49} attack possibilities, which is why it is hard to compare the accuracy with the other template protection schemes using only the accuracy.

In this evaluation, we do not apply the regularization method in [4]. This is because the original minutiae information such as the position and the direction is necessary to apply the regularization method, so that this method is not applicable to the template protection scheme.

5. Conclusion

In this paper, we proposed a new irreversible fingerprint authentication scheme using MRC which consists of a simple binary-represented vectors and the Bloom Filter which enables to create an irreversible fingerprint template. In order to confirm the validity of the proposed method regarding the irreversibility, we showed the number of attack possibilities using the Shannon entropy, and we confirmed that the number is 2^{49}. In addition to the security factors, we showed the reasonable EERs compared to the other techniques in FVC2002 and FVC2004 DBs.

For our future work, we will keep looking into improvements regarding the authentication accuracy of MRC, and evaluate the other aspects like the unlinkability as a template protection scheme.

References

[1] Fvc2002 http://bias.csr.unibo.it/fvc2002/.

[2] Fvc2004 http://bias.csr.unibo.it/fvc2004/.

[3] Verifinger sdk 6.0 http://www.neurotechnology.com/verifinger.html.

[4] N. Abe and T. Shinzaki. Vectorized fingerprint representation using minutiae relation code. In *Proceedings of IEEE International Conference on Biometrics Compendium (ICB2015)*, pages 1–8, 2015.

[5] R. Cappelli, M. Ferrara, and D. Maltoni. Minutiae cylinder-code: A new representation and matching technique for fingerprint recognition. *IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE*, 32(12):2128–2141, 2010.

[6] J. Feng. Combining minutiae descriptors for fingerprint matching. *ELSEVIER Pattern Recognition Letters*, 41(1):342–352, 2008.

[7] M. Ferrara, D. Maltoni, and R. Cappeli. A two-factor protection scheme for mcc fingerprint templates. In *Proceedings of International Conference of the Biometrics Special Interest Group (BIOSIG 2014)*, 2014.

[8] M. Ferrara, D. Maltoni, and R. Cappelli. Noninvertible minutiae cylinder-code representation. *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY*, 7(6):1727–1737, 2012.

[9] A. K. Jain, K. Nandakumar, and A. Nagar. Fingerprint template protection: From theory to practice. In *Security and Privacy in Biometrics*, chapter 8. Springer, 2013.

[10] A. K. Jain, S. Prabhakar, L. Hong, and S. Pankanti. Filterbank-based fingerprint matching. *IEEE TRANSACTIONS ON IMAGE PROCESSING*, 9(5):846–859, 2000.

[11] X. Liang, A. Bishnu, and T. Asano. A robust fingerprint indexing scheme using minutia neighborhood structure and low-order delaunay triangles. *IEEE TRANSACTION ON INFORMATION FORENSICS AND SECURITY*, 2(4):721–733, 2007.

[12] K. Nandakumar. A fingerprint cryptosystem based on minutiae phase spectrum. In *Proceedings of IEEE International Workshop on Information Forensics and Security(WIFS)*, pages 1–6, 2010.

[13] K. Nandakumar. Fingerprint matching based on minutiae phase spectrum. In *Proceedings of IEEE 5th IAPR International Conference on Biometrics Compendium(ICB)*, pages 216–221, 2012.

[14] J. Qi, Z. Shi, X. Zhao, and Y. Wang. A robust fingerprint matching method. In *Proceedings of IEEE Seventh Workshops on Application of Computer Vision(WACV/MOTIONS)*, volume 1, pages 105–110, 2005.

[15] C. Rathgeb, F. Breitinger, and C. Busch. Alignment-free cancelable iris biometric templates based on adaptive bloom filters. In *Proceedings of IEEE International Conference on Biometrics Compendium (ICB2013)*, pages 1–8, 2013.

[16] M. Tico and P. Kuosmanen. Fingerprint matching using an orientation-based minutia descriptor. *IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE*, 25(8):1009–1014, 2003.

[17] X. Wang, J. Li, and Y. Niu. Fingerprint matching using orientationcodes and polylines. *ELSEVIER Pattern Recognition*, 40(11):3164–3177, 2007.

[18] W. J. Wong, A. G. J. Teoh, M. L. D. Wong, and Y. H. Kho. Enhanced multi-line code for minutiae-based fingerprint template protection. *ELSEVIER Pattern Recognition Letters*, 34(11):1221–1229, 2013.

[19] H. Xu and R. N. J. Veldhuis. Spectral minutiae representations of fingerprints enhanced by quality data. In *Proceedings of IEEE 3rd International Conference on Biometrics: Theory, Applications, and Systems(BTAS)*, pages 1–5, 2009.

[20] H. Xu and R. N. J. Veldhuis. Spectral representations of fingerprint minutiae subsets. In *Proceedings of IEEE 2nd International Congress on Image and Signal Processing(CISP)*, pages 1–5, 2009.

[21] H. Xu, R. N. J. Veldhuis, A. M. Bazen, T. A. M. Kevenaar, T. A. H. M. Akkermans, and B. Gokberk. Fingerprint verification using spectral minutiae representations. *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY*, 4(3):397–409, 2009.

[22] H. Xu, R. N. J. Veldhuis, T. A. M. Kevenaar, and T. A. H. M. Akkermans. A fast minutiae-based fingerprint recognition system. *IEEE SYSTEMS JOURNAL*, 3(4):418–427, 2009.

[23] B. Yuan, F. Su, and A. Cai. Fingerprint retrieval approach based on novel minutiae triplet features. In *Proceedings of IEEE Fifth International Conference on Biometrics: Theory, Applications and Systems(BTAS)*, pages 170–175, 2012.