I. J. Computer Network and Information Security, **2017, 5, 1-10**
Published Online May 2017 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2017.05.01

Toward Constructing Cancellable Templates using K-Nearest Neighbour Method

Qinghai Gao
Farmingdale State College/Department of Security Systems, Farmingdale, NY 11735, USA
E-mail: GaoQJ@farmingdale.edu

***Abstract*—**The privacy of biometric data needs to be protected. Cancellable biometrics is proposed as an effective mechanism of protecting biometric data. In this paper a novel scheme of constructing cancellable fingerprint minutiae template is proposed. Specifically, each real minutia point from an original template is mapped to a neighbouring fake minutia in a user-specific randomly generated synthetic template using the k-nearest neighbour method. The recognition template is constructed by collecting the neighbouring fake minutiae of the real minutiae. This scheme has two advantages: (1) An attacker needs to capture both the original template and the synthetic template in order to construct the recognition template; (2) A compromised recognition template can be cancelled easily by replacing the synthetic template. Single-neighboured experiments of self-matching, nonself-matching, and imposter matching are carried out on three databases: DB1B from FVC00, DB1B from FVC02, and DB1 from FVC04. Double-neighboured tests are also conducted for DB1B from FVC02. The results show that the constructed recognition templates can perform more accurately than the original templates and it is feasible to construct cancellable fingerprint templates with the proposed approach.

***Index Terms*—**Fingerprint, minutiae, pseudo random number generator, synthetic template, k-nearest neighbours, cancellable template.

I. INTRODUCTION

Biometric recognition systems aim to establish a genuine connection between a real person and the person’s digital identity through the measurements of human body features, such as fingerprint, iris, face, etc. In general, a biometric system operates in two stages: enrollment and recognition (verification or identification). During enrollment, a template is extracted from biometric images and then stored in a database. During recognition, the user is required to provide the same body features for new measurements, from which a new template will be generated. For verification, one score is produced by matching the new template against the stored template for the user. For identification, the user is unknown and multiple scores are produced by matching the new template against each template in the database in order to find the best match or to obtain a candidate list of possible matches. Whether a score indicates a match or a non-match depends on an arbitrarily selected threshold.

Biometric templates are not exactly reproducible due to the factors such as the dynamics of human body features, changes in environmental factors, and interaction variations between a user and biometric sensor. Error correction methods, such as averaging, discretization, majority voting, and other error correction algorithms, can reduce some fuzzy bits, but cannot completely solve the non-exact reproducibility problem. Therefore, biometric matching is never 100% accurate.

A person has limited number of biometrics and they cannot be changed easily. Therefore, a well-designed biometric system should be able to revoke a compromised template and reissue a new one based on original biometrics – the so-called cancellable biometrics.

According to [1], cancellable biometrics must meet four criteria:

- Diversity: dissimilar templates can be generated from the same biometrics.
- Revocability: a compromised template can be replaced with a new one using the same biometrics.
- Non-reversibility: it is impractical to recover the original biometrics given a recognition template.
- Accuracy: matching with the recognition template does not reduce the recognition accuracy.

The approach proposed in this paper can be utilized to construct cancellable fingerprint minutiae templates that satisfy the four requirements.

The rest of the paper is organized as follows. Section 2 reviews related works; Section 3 introduces the proposed approach; Section 4 gives the testing results obtained with three FVC databases; and Section 5 concludes the paper.

II. RELATED WORKS

Many researchers have attempted to solve the problem of generating cancellable biometrics. The main challenge to cancellable biometrics lies in transforming the original template in such a way that matching can be done accurately in the transformed domain.

Ratha et al. [2] proposed three techniques to transform fingerprint template, including image morphing, block scrambling, and domain mapping. Ratha et al. [3] [4] also proposed using Cartesian, polar, and surface-folding transformations to generate cancellable minutiae templates. Yang et al. [5] proposed using features obtained from minutiae pairs to generate cancellable template. References [6-10] also proposed methods of deriving new features from minutiae pairs.

Delaunay triangulation is proposed as an approach for fingerprint identification in [11-21]. Tulyakov et al. [22], Li [23], and Sandhya et al. [24] [25] proposed methods of deriving and transforming new features based on minutiae triplets for the purpose of generating cancellable templates. Similar schemes were proposed using Delaunay quadrangle [26] [27], pentangle [28] [29], and hexangle [30].

Li et al. [31] [32] proposed an approach of generating cancellable palmprint template by applying chaotic stream cipher on orientation features of palmprint. Du et al. [33] proposed a scheme of generating cancellable iris template by using a key and helper information generated during feature extraction to transform the original template. Rathgeb et al. [34] [35] [36] proposed a method of generating cancellable iris templates [34] and cancellable multi-biometric templates (iris-iris [35], face-iris [36]) using bloom filters. Hämmerle-Uhl et al. [37] proposed using block-wised mapping and key-based image warping to generate cancellable iris templates. Phillai et al. [38] proposed a method of generating cancellable iris template, in which the iris image is divided into small sectors and each sector is projected onto a random matrix. Osama et al. [39] proposed a seed-based method of generating cancellable iris templates. Kanade et al. [40] proposed a scheme of generating cancellable iris and face templates by using a user-specific key to shuffle the feature vectors. Savvides et al. [41] proposed a cancellable face template generation method by utilizing PIN-based random convolution kernels. Hirata and Takahshi [42] [43] developed a method of generating cancellable biometric template by using correlation-invariant pseudorandom filters to filter biometric images. Maiorana et al. [44] proposed a method of generating cancellable templates for sequence-based biometrics, such as voice and signature. Xu et al. [45] proposed a method of generating cancellable voiceprint. Connie et al. [46] proposed an approach of generating cancellable palmprint using pseudorandom keys. Zuo et al. [47] proposed a method of generating cancellable iris template with using key-based image transformation. Bajwa and Dantu [48] proposed a scheme of generating cancellable template based on the electroenciphalograms (EEG).

Currently, generating cancellable biometric template is still in research stage. As Jain et al. [49] recently indicated that one of the unsolved problems is to protect the privacy of biometric data. In this paper we make an effort to approach this problem.

III. Proposed Scheme

Minutiae are points of ridge ending or ridge bifurcation. Each minutia is represented with one triplet (x, y, θ), where (x, y) is a minutia's Cartesian coordinates, and θ is the orientation of ridge flow at the point. A fingerprint minutiae template contains a number of minutiae, which can be generated with random number generators.

Random number generators play an important role in information security [50]. They can be classified into two categories: Truly Random Number Generator (TRNG) and Pseudo Random Number Generators (PRNG). TRNG utilizes nondeterministic physical sources, such as the position/velocity of an atomic electron, decay of a radioactive material, or quantum entanglement, to produce random numbers. As Ellison [51] pointed out, "*getting true randomness can be extremely difficult*." Most random numbers used in computer security, such as cryptographic keys, are generated with software-based PRNG. As shown in Fig. 1, the synthetic templates in this paper are generated with PRNG. Specifically, three numbers (x, y, and θ) associated with every minutia are independently generated with PRNG. The ranges of the two coordinates (x, y) are determined by the original dimensions of the fingerprint image. The orientation angle is set between 0 and 360. A synthesized fingerprint template consists of an arbitrary number of synthetic minutiae.

In the proposed approach, every real minutia point from an original template is positioned among the fake minutiae of a user-specific synthetic template. Then, the nearest neighbours of the real minutia are found and stored in a sequential array, which contains only fake minutiae. The recognition template is constructed simply by selecting a particular set of neighbours. Note that the recognition template is a subset of the synthetic template and there is no common minutia between the original template and the recognition template.

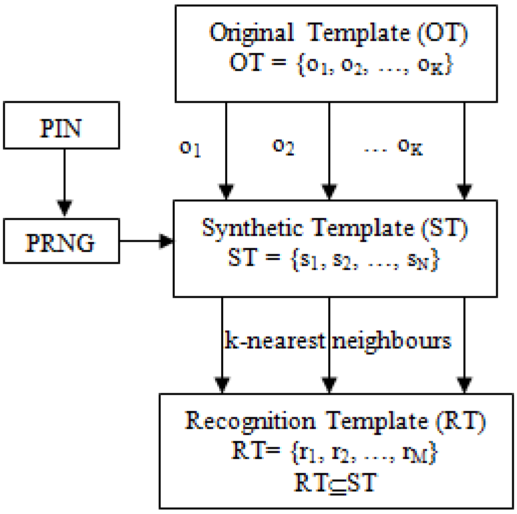

Fig.1. Schematic Diagram of Generating Cancellable Template (N ≥ M)

It is important for readers to realize that two PRNG-generated synthetic templates do not match, and the sub-templates of one synthetic template do not match the sub-templates of another synthetic template. Therefore, the false (imposter) match rate should be close to zero.

The recognition template constructed with this approach meets the four criteria of cancellable biometrics as follows:

- Diversity can be achieved by pairing different synthetic templates with one real template;
- Revocability can be achieved by changing the synthetic template;
- Non-reversibility: recognition template does not contain any real minutia. It only contains fake minutiae. With proper selection (For example, selecting the 20TH nearest neighbour), the synthetic neighbour does reveal much information about the real minutia it is associated with.
- The desired accuracy can be achieved by controlling the size of synthetic templates and the proper selection of the nearest neighbours.

The constructed recognition templates are matched with the *Bozorth* algorithm as described in [52].

In addition to using genuine matching score and imposter matching score to characterize the matching performance, we use the database-based average matching scores to compare the accuracy before and after template transformation. It is generally true that the higher the average score is, the higher the accuracy is. The results are given as follows.

IV. Experimental Results

To test the validity and feasibility of our proposed approach, we carried out experiments with three publicly available fingerprint databases as given in Table 1.

Table 1. Database Information

Source	FVC00	FVC02	FVC04
Database	DB1B	DB1B	DB1
Reference	[53]	[54]	[55]
Sensor type	Optical	Optical	Optical
Image size	300x300	388x374	640x480
Resolution	500dpi	500dpi	500dpi
No. Fingers	10	10	110
Images/per finger	8	8	8
Imaging sessions	1	1	3
Avg. & std. minutiae count	52 ± 12	44 ± 13	58 ± 18
Avg, & std. self-matching score of original templates*	420.0 ± 110.4	330.0 ± 130.0	461.9 ± 138.0
Avg, & std. nonself-matching score of original templates*	47.0 ± 32.0	62.3 ± 44.6	56.9 ± 44.6

*Self-matching score is obtained by matching a template with itself; nonself-matching score is obtained by matching two different templates from the same finger.

In the three databases, there are eight images originated from each finger. Using the minutiae extraction utility *mindtct* [56], one template is obtained from every image. In all, there are eight original templates per finger. One synthetic template is pseudo-randomly generated and paired with each of the eight original templates, which gives eight original-synthetic pairs. Given a pair, we apply our proposed approach to construct the recognition template. For each pair, a number of different recognition templates can be constructed by selecting different synthetic neighbours (1ST, 2ND, …, or 36TH) for each real minutia.

Matching is carried out between the constructed recognition templates. For self-matching, a recognition template is matched with itself; for nonself-matching, matching is carried out only between two different recognition templates constructed for the same finger (constructed with same synthetic template but different original templates); for imposter matching, matching is conducted between recognition templates constructed for different fingers (constructed with different synthetic templates and different original templates). Since biometric templates are non-exact reproducible, nonself-matching score represents the real-world scenario of genuine matching and imposter matching represents the real-world scenario of false matching in biometric recognition. Averages and standard deviations are calculated based on all the matching scores for the entire database.

Upon designing the experiments, we consider the following two factors:

- The size N of the synthetic templates. N is chosen in the range between 50 and 1600.
- The ordinal number L when selecting the nearest neighbours for each real minutia. In this paper we limit L in the range between the 1ST and the 36TH nearest neighbour, and either one or two neighbours of each real minutia are utilized to construct the recognition template. If only one neighbour is selected, we call it single-neighboured the transformation; if two neighbours are selected, we call it double-neighboured transformation. The results are given below.

A. Single-neighboured transformation

In this section, the recognition templates are constructed by selecting just one neighbour for every real minutia. If multiple real minutiae are mapped to one synthetic minutia, duplicates are removed and only one copy of the synthetic minutia is kept in the recognition template.

A.1. Self-matching

In theory it is possible to regenerate a biometric template with 100% accuracy. Self-matching represents this theoretically possibility. The averages and standard deviations of self-matching scores obtained from the constructed recognition templates for the DB1B of FVC00, the DB1B of FVC02, and the DB1 of FVC04 are given in Table 2, Table 3, and Table 4, respectively. Note that the averages and standard deviations of self-matching scores for the original templates are listed in the last row of each table for easy comparison.

From Table 2, Table 3, and Table 4 we can observe the follows:

- Average self-matching score increases as the size of synthetic templates increases.
- Average self-matching score increases as the ordinal number of the nearest neighbour selected to construct the recognition templates increases, except when N=50 and/or 100.
- For the DB1B of FVC02 and the DB1 of FVC04, the average self-matching scores obtained from the recognition templates are lower than those from the original templates. For the DB1B of FVC00, the average self-matching scores obtained from the recognition templates can be higher than those from the original templates.

Table 2. Averages and Standard Deviations of Self-matching Scores with DB1B FVC00

N	1ST	6TH	16TH	26TH	31ST	36TH
50	116.2±38.1	153.0±45.4	171.2±57.0	165.1±56.6	154.2±47.7	134.2±41.6
100	187.2±63.8	249.5±89.1	273.7±93.0	286.8±102.2	279.4±99.8	279.5±102.4
150	251.0±86.9	317.5±115.7	335.3±114.1	345.7±119.4	346.0±116.8	346.9±116.6
200	285.8±103.6	340.5±115.7	363.6±114.6	380.9±117.7	371.8±118.9	375.1±116.7
250	294.5±109.4	353.6±116.9	373.2±113.6	381.0±115.5	376.1±116.8	397.0±113.0
400	342.3±113.7	386.3±113.3	397.9±114.0	407.0±114.2	412.7±116.2	412.6±116.1
800	384.5±118.2	405.4±111.2	415.6±110.5	415.9±113.2	420.1±112.0	427.8±110.7
1600	396.5±113.6	414.3±115.9	420.8±109.2	423.4±111.7	420.5±110.3	426.9±109.9
DB1B	420.0±110.4					

Table 3. Averages and Standard Deviations of Self-matching Scores with DB1B FVC02

N	1ST	6TH	16TH	26TH	31ST	36TH
50	61.6±28.3	84.8±35.9	91.0±39.8	87.8±36.6	85.4±31.6	78.0±29.3
100	103.3±52.9	145.4±66.1	161.5±73.6	158.8±71.9	164.4±75.7	156.4±72.8
150	133.2±68.1	182.0±91.4	188.2±88.4	196.2±87.0	198.6±92.4	200.3±92.1
200	149.4±76.3	196.6±101.5	208.7±101.6	217.0±98.6	226.0±110.5	220.8±101.7
250	166.3±89.2	206.9±109.0	229.3±114.5	233.1±114.0	234.4±113.3	244.9±115.9
400	193.5±105.1	223.4±114.2	242.4±128.4	249.7±124.9	247.7±122.1	250.8±125.1
800	223.6±120.0	240.4±127.0	252.4±130.4	258.1±129.9	262.3±132.7	262.4±130.3
1600	241.1±125.1	247.7±130.4	256.3±133.0	260.2±133.4	261.8±133.3	264.9±135.0
DB1B	330.0±130.0					

Table 4. Averages and Standard Deviations of Self-matching Scores with DB1 FVC04

N	1ST	6TH	16TH	26TH	31ST	36TH
50	49.8±19.6	77.8±26.1	90.6±31.2	89.3±31.0	82.4±29.1	72.3±25.1
100	99.3±40.6	158.5±64.6	172.6±70.1	179.0±76.9	179.2±77.1	179.8±77.8
150	134.1±59.0	216.5±93.6	233.7±102.6	234.9±103.7	235.4±105.2	236.0±107.1
200	160.0±73.8	256.5±111.9	274.5±119.3	275.7±120.4	276.0±121.2	276.9±120.4
400	225.1±109.8	319.5±134.1	342.3±134.5	343.7±134.5	345.4±134.4	345.0±133.6
800	280.7±130.6	352.9±140.2	373.5±141.2	379.6±141.2	378.2±142.0	380.8±140.5
1600	319.2±138.8	369.7±146.1	385.9±149.4	393.1±149.7	394.4±150.8	396.0±148.1
DB1	461.9±138.0					

For self-matching, the matching score is closely related to the number of minutiae in a template. In general, the matching score increases as the number of minutiae in a template increases. For a database, a lower average matching score indicates that the average number of minutiae in the constructed recognition templates is less than that of the original templates. The reason is that multiple real minutiae are mapped to a single fake minutia during the neighbour-finding process of the proposed method.

Based on the results given in Table 2, Table 3, and Table 4, we can conclude that when the size of synthetic templates is greater than 100, selecting the neighbours further away to construct the recognition template can help reduce the chance of mapping multiple real minutiae to a single fake minutia.

For comparison, the self-matching results with the 16TH nearest neighbours are plotted in Fig. 2.

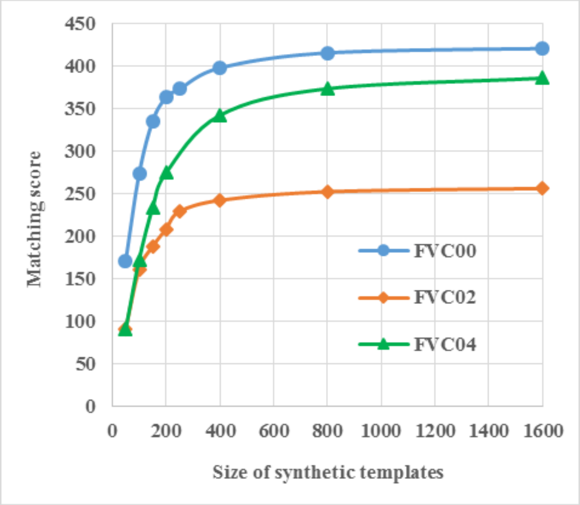

Fig.2. Self-matching results with the 16TH Nearest Neighbours

From Fig. 2 we can see that for a given size of the synthetic template the constructed recognition templates for the DB1B of FVC00 produce the highest average score, while those for the DB1B of FVC02 produce the lowest score.

A.2. Nonself-matching

Nonself-matching represents the practical scenario of biometric matching. The averages and standard deviations of nonself-matching scores obtained from the constructed recognition templates for the DB1B of FVC00, the DB1B of FVC02, and the DB1 of FVC04 are given in Table 5, Table 6, and Table 7, respectively. Note that the averages and standard deviations of nonself-matching scores for the original templates are listed in the last row of each table for comparison.

From Table 5 it can be seen that the average nonself-matching scores are maximized when the size N of the synthetic templates equals to 75. To achieve an overall higher accuracy with the transformed templates than with the original templates, any combination of row (N) and column (L) with an average score higher than 47.0 can be selected. For example, the average score equals to 61.1 when N=150 and L=21ST.

From Table 6 it can be seen that the average nonself-matching scores are maximized when the size N of the synthetic templates equals to 50 or 75. However, all the combinations of row (N) and column (L) produce lower average matching scores than the original templates. Therefore, the proposed scheme with the single-neighboured transformation cannot be applied to generate cancellable templates for this database due to performance degradation. The solution to the problem is given in section B.2.

From Table 7 it can be seen that the average nonself-matching score is maximized when the size N of the synthetic templates is around 100. To achieve an overall better accuracy with the transformed templates than with the original templates, any combination of row (N) and column (L) with an average score higher than 56.9 can be selected. For example, the average score equals to 60.5 when N=150 and L=6TH.

For comparison, the nonself-matching results with the 16TH nearest neighbours are plotted in Fig. 3, from which it can be seen that recognition templates for FVC00 produce the highest scores when the size N of the synthetic templates is less than 150, while those for FVC04 produce the highest scores when the size N of the synthetic templates is greater than 150.

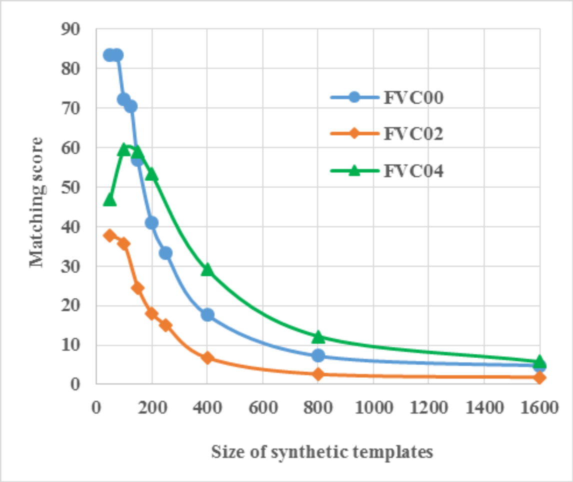

Fig.3. Nonself-matching results with the 16TH Nearest Neighbours

A.3. Imposter matching

Imposter matching is carried out between two recognition templates constructed for different fingers. The matching score distributions for DB1B of FVC00 with N=150 and L=11TH are plotted in Fig. 4.

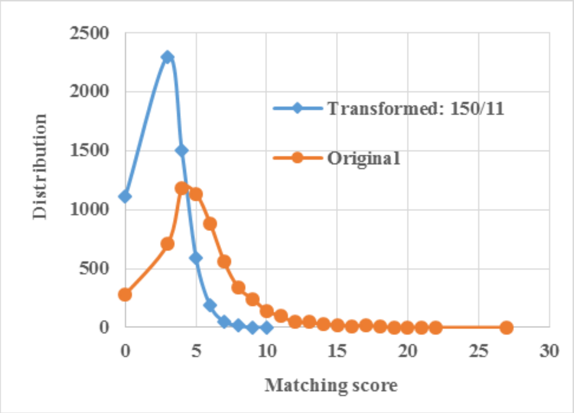

Fig.4. Distributions of Imposter Matching scores DB1B_FVC00

Table 5 Averages and Standard Deviations of Nonself-matching Scores with DB1B FVC00

N	1ST	6TH	16TH	21ST	26TH	31ST	36TH
50	56.6±23.9	75.0±30.5	83.4±38.1	76.8±37.2	75.4±37.6	71.0±31.6	62.5±27.6
75	63.9±33.2	79.9±41.4	83.4±40.4	81.5±42.8	83.2±41.7	74.3±42.5	70.8±39.5
100	65.0±31.6	69.1±35.4	72.2±40.3	71.6±39.0	70.6±39.6	65.4±37.0	61.0±34.3
125	62.1±28.1	64.6±36.3	70.5±36.6	66.6±38.3	66.1±38.9	67.6±40.8	61.6±36.4
150	57.4±29.8	55.2±33.9	56.8±33.8	61.1±37.7	56.2±32.3	57.2±34.6	55.6±35.5
200	52.9±31.5	42.8±26.7	40.8±24.6	44.2±27.2	44.2±26.1	40.8±24.5	40.5±24.7
250	43.9±27.3	39.8±26.3	33.3±22.4	33.8±22.6	31.9±21.0	32.4±23.1	35.5±23.0
400	30.8±20.1	20.9±14.5	17.6±12.3	17.6±13.3	17.0±13.5	16.0±12.2	16.9±12.2
800	15.0±12.3	9.7±6.9	7.2±5.5	7.1±4.9	7.3±5.7	6.6±5.5	6.9±4.9
1600	7.9±6.9	5.1±3.3	4.8±3.1	4.3±2.5	4.7±2.6	4.4±2.6	4.5±2.3
DB1B	47.0±32.0						

Table 6. Averages and Standard Deviations of Nonself-matching Scores with DB1B FVC02

N	1ST	6TH	11TH	16TH	21ST	26TH	31ST	36TH
50	26.3±17.8	36.6±25.1	35.2±21.5	37.7±26.9	40.9±27.5	34.1±23.7	34.0±20.2	31.9±20.1
75	29.3±22.9	33.3±24.9	38.0±24.7	37.4±26.3	38.3±22.4	35.3±23.8	36.0±24.3	31.6±23.8
100	26.7±21.0	31.6±27.1	31.6±22.8	35.5±27.4	32.7±26.8	32.4±24.4	36.5±31.4	29.7±25.2
125	24.2±21.1	26.7±21.4	30.2±27.5	27.7±24.2	31.5±28.0	28.1±23.4	29.5±25.0	28.3±28.0
150	23.5±22.2	26.9±28.1	22.8±21.9	24.6±24.5	24.7±20.2	24.5±21.5	26.3±25.3	25.6±22.9
200	21.1±21.2	19.3±20.5	17.9±18.7	18.0±18.0	19.6±19.3	18.8±17.3	20.6±18.4	20.6±17.9
250	18.1±18.6	14.2±15.5	14.8±16.8	15.1±17.1	15.7±17.4	14.3±15.7	14.4±14.7	15.4±15.8
400	11.5±14.1	8.1±9.5	7.6±11.2	6.8±8.7	6.9±8.6	7.3±8.7	7.6±9.1	8.3±10.4
800	6.0±8.3	3.1±4.3	3.2±4.5	2.6±3.7	2.9±3.9	3.1±4.1	2.6±3.3	2.8±3.3
1600	2.8±4.3	1.8±2.5	1.9±2.3	1.9±2.5	1.8±2.2	2.0±2.3	2.0±2.3	1.8±2.1
DB1B	62.3±44.6							

Table 7. Averages and Standard Deviations of Nonself-matching Scores with DB1 FVC04

N	1ST	6TH	11TH	16TH	21ST	26TH	31ST	36TH
50	26.2±13.4	43.7±19.5	47.6±22.7	46.8±22.4	46.2±22.5	44.0±21.8	41.4±20.5	39.2±18.8
75	32.6±19.2	56.0±29.4	57.1±32.3	57.4±31.5	55.5±32.0	52.3±31.1	51.5±31.1	49.6±29.1
100	37.0±22.1	61.3±35.9	61.9±37.6	59.6±35.9	57.6±36.1	55.4±36.5	52.5±35.4	50.6±33.8
125	37.8±24.6	59.8±39.0	61.7±39.5	59.5±40.2	57.1±38.9	53.3±36.2	51.0±36.1	49.1±35.5
150	39.2±26.5	60.5±41.2	60.4±40.2	59.0±40.9	55.6±37.7	53.1±37.4	49.5±35.5	47.6±34.6
200	38.7±28.0	55.3±40.6	56.0±41.1	53.2±38.3	51.4±37.3	48.1±35.5	46.1±33.7	44.1±32.0
400	33.3±27.4	32.8±26.8	31.0±25.1	29.0±23.8	27.5±22.3	26.2±21.6	26.1±21.1	25.6±21.0
800	24.9±21.7	16.1±15.2	13.5±12.6	12.2±11.6	11.7±11.4	11.4±11.5	10.8±10.8	10.4±10.1
1600	17.4±16.3	8.8±9.1	6.6±7.3	5.8±6.1	5.4±5.5	5.1±5.2	5.0±5.3	4.8±4.7
DB1	56.9±44.6							

From Fig. 4, we can see that matching with the transformed templates produce lower imposter scores than that with the original templates. Therefore, the proposed approach can improve performance.

Fig. 5 gives matching score distributions for the DB1B of FVC02 with N=100 and L=11TH. From Fig. 5 we can see that the transformed templates produce lower imposter scores than with the original templates.

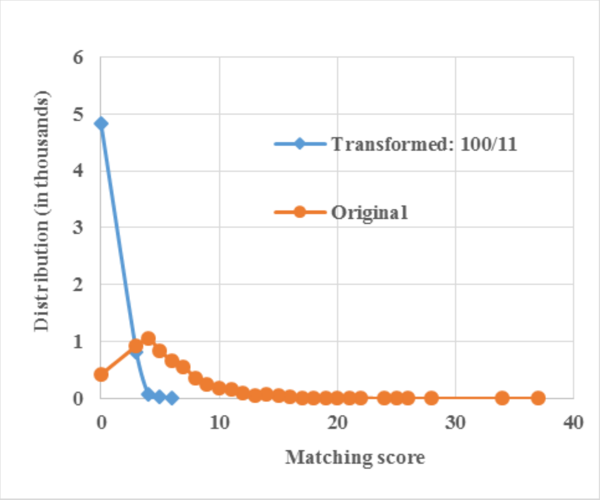

Fig.5. Distributions of Imposter Matching scores DB1B_FVC02

As given in Table 1, each of the two databases DB1B from FVC00 and DB1B from FVC02 only contain 80 images captured from 10 fingers. Due to the size limitation, they may not generate representative results. Therefore, we carry out experiments with the DB1 from FVC04, which contains 880 fingerprints obtained from 110 fingers. The imposter matching results are plotted in Fig. 6, from which we can draw the same conclusion: the transformed templates produce significantly lower imposter matching scores than the original templates.

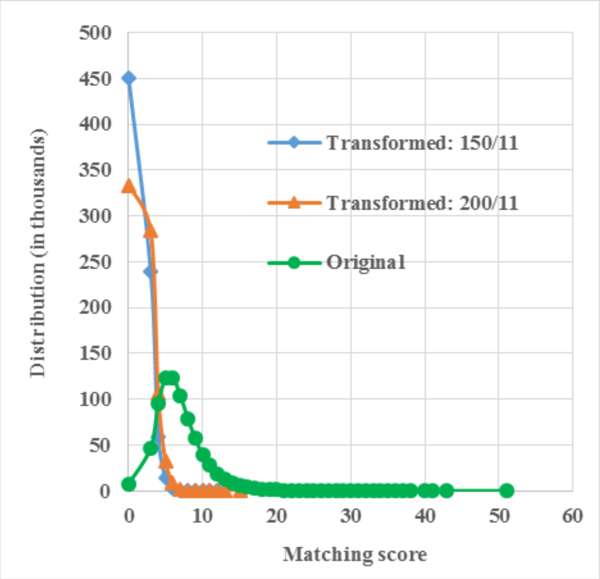

Fig.6. Distributions of Imposter Matching scores DB1_FVC04

In sum, we conclude that the recognition templates constructed with the proposed approach for all three databases can produce significantly lower imposter scores than the original (non-transformed) templates.

B. Double-neighboured transformation

As given in section A.2, the nonself-matching performance with the transformed templates for DB1B of FVC02 is worse than that with the original. The solution to problem is to select multiple nearest neighbours when construct the recognition templates. In this paper, we utilize two synthetic neighbours for each real minutia. Multiple real minutiae may be mapped to a single synthetic minutia. When this happens, only one copy of the synthetic minutia is kept (the duplicate is removed). With the double-neighboured transformation, the results for self-matching, nonself-matching, and imposter matching are given below.

B.1. Self-matching

The average self-matching scores with double-neighboured transformation are given in Table 8, from which we can see:

- The average matching score with the transformed templates increases as N increases.
- When N=50 or 75, the average matching scores with the transformed templates are lower than that with the original.
- When N≥100, the average matching scores with the transformed templates are higher than that with the original, with the exception when N=100 and L=1ST+2ND.
- For any given N, the transformed templates with L=1ST+2ND produce the lowest average matching score than those with other combinations of L.

Table 8. Self-matching with Two Neighbours (DB1B_FVC02)

N	1+2	7+8	13+14	19+20	25+26	31+32
50	131.7	169.2	182.7	183.1	193.4	172.7
75	196.8	266.4	270.6	282.2	288.8	294.8
100	275.5	366.8	375.5	380.9	378.5	387.6
150	349.2	414.3	429.1	428.5	427.2	427.6
200	392.8	432.3	438.7	443.5	441.8	443.1
300	422.0	453.7	456.4	464.2	466.7	471.8
400	451.8	470.9	478.8	482.8	480.9	486.6
600	473.5	504.1	511.9	517.4	513.3	512.7
1200	525.7	548.5	550.8	540.1	543.5	543.0
DB1B	330.0					

Comparing Table 2 with Table 8, we can see that the average self-matching score can be increased significantly by using two nearest neighbours.

B.2. Nonself-matching

The average nonself-matching scores with two neighbours are given in Table 9.

Table 9. Nonself-matching with Two Neighbours (DB1B_FVC02)

N	1+2	7+8	13+14	19+20	25+26	31+32
50	82.2	111.3	123.9	120.5	131.1	116.8
75	101.5	140.1	143.1	147.8	152.6	153.5
100	123.2	156.1	160.1	161.5	155.7	157.3
150	113.1	116.2	121.8	112.5	114.4	118.8
200	98.6	90.4	90.4	89.1	88.3	88.0
300	74.3	59.3	54.7	55.0	55.6	60.2
400	57.8	43.5	39.5	37.0	35.4	35.1
600	44.0	30.0	27.2	22.4	21.9	22.0
1200	22.0	14.6	11.4	9.3	9.0	8.3
DB1B	62.3					

From Table 9, we can see that:

- When N≤200, the average matching scores with the transformed templates are higher than that with the original.
- When N≥300, the average matching scores with the transformed templates are lower than that with the original, with the exception when N=300 and L=1ST+2ND.
- When N=50, 75, or 100, the average matching score tends to increase as L increases; When N=200, 300, 400, 600, or 1200, the average matching score tends to decrease as L increases.

Comparing Table 6 with Table 9, we can see that the average nonself-matching score can also be increased significantly by using two nearest neighbours.

B.3. *Imposter matching*

With double-neighboured transformation, the imposter matching results are given in Fig. 7, from which we can see that the transformed templates produce significantly lower imposter matching scores than the original templates do.

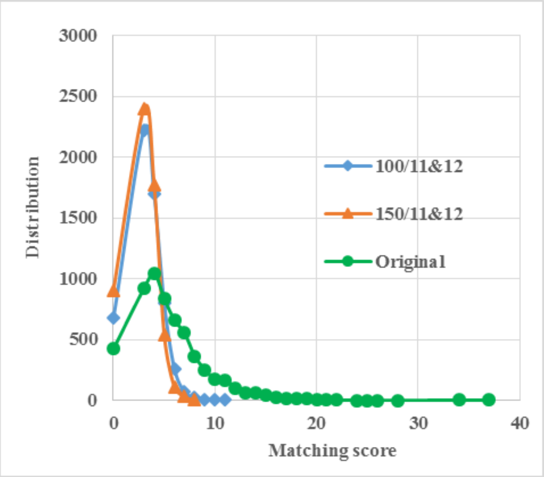

Fig.7. Distributions of imposter matching scores of DB1B_FVC02

The usage of two nearest neighbours may cause the concern about reversibility. However, we believe that the concern can be alleviated for the reason that the two neighbours are randomly generated and can be chosen arbitrarily from a large set of available neighbours.

In this paper, we store 36 nearest synthetic neighbours into an array for each real minutia. Instead of using two contiguous neighbours, we may choose any pair (For example, L=9TH+23RD, i.e., 9TH and 23RD nearest neighbours). Therefore, it is challenging for an attacker to find the two neighbours belonging to a real minutia in the recognition template. Even if the two neighbours are found, it is still mathematically difficult in finding the exact position of the real minutia.

V. CONCLUSION

A new method of constructing cancellable template is proposed. Recognition template is constructed by mapping real minutiae to the fake minutiae in a PRNG generated synthetic template using the K-nearest neighbour method. In this paper one or two synthetic neighbours of each real minutia are utilized to construct the final recognition templates. The cancellability of a recognition template is achieved by replacing the user-specific synthetic template.

Our testing results for genuine matching indicate that the recognition templates constructed with the proposed approach can achieve better accuracy than the original templates by properly selecting the size of synthetic templates and the ordinal number of nearest neighbours.

It should be noted that two randomly generated synthetic templates do not match with each other, and the sub-templates of one synthetic template do not match the sub-templates of another synthetic template. Our testing results show that the imposter matching scores obtained from the transformed templates are extremely low and significantly lower than those obtained from the original templates.

The usage of two nearest neighbours should not raise the concern about reversibility for the reason that the two neighbours are randomly generated and can be chosen arbitrarily from a large set of available neighbours.

REFERENCES

[1] D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*, 2nd ed., Springer, London, 2009.

[2] N. Ratha, J. Connell, and R. Bolle, “Enhancing security and privacy in biometrics-based authentication systems,” *IBM Systems Journal*, vol. 40, no. 2, pp. 614-634, 2001.

[3] N. Ratha, J. Connell, R. Bolle, and S. Chikkerur, “Cancellable biometrics: a case study in fingerprints,” *18th International Conference on Pattern Recognition*, 2006, pp. 370-373.

[4] N. Ratha, S. Chikkerur, J. Connell, and R. Bolle, “Generating cancellable fingerprint templates,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, no.4, pp. 561-572, 2007.

[5] H. Yang, X. Jiang, and A. Kot, “Generating secure cancellable fingerprint templates using local and global

features," *IEEE 2nd International Conference on Computer Science and Information Technology*, 2009, pp. 645-649.

[6] C. Lee and J. Kim, "Cancellable fingerprint templates using minutiae-based bit-strings," *Journal of Network and Computer Applications*, vol. 33, no. 3, pp. 236-246, 2010.

[7] T. Ahmad, J. Hu, and S. Wang, "Pair-polar coordinate-based cancellable fingerprint templates," *Pattern Recognition*, vol. 44, no. 10, pp. 2555-2564, 2011.

[8] S. Wang and J. Hu, "Alignment-free cancellable fingerprint template design: a densely infinite-to-one mapping (DITOM) approach," *Pattern Recognition*, vol. 45, no. 12, pp. 4129-4137, 2012

[9] S. Wang and J. Hu, "Design of alignment-free cancellable fingerprint templates via curtailed circular convolution," *Pattern Recognition*, vol. 47, no. 3, pp. 1321-1329, 2014.

[10] S. Wang and J. Hu, "A blind system identification approach to cancellable fingerprint templates," *Pattern Recognition*, vol. 54, pp. 14-22, 2016.

[11] G. Bebis, T. Deaconu, and M. Georgiopoulos, "Fingerprint identification using Delaunay triangulation," *International Conference on Information Intelligence and Systems*, 1999, pp. 452-459.

[12] G. Parziale and A. Niel, "A fingerprint matching using minutiae triangulation," *Biometric Authentication*, 2004, pp. 241-248.

[13] N. Liu, Y. Yin, and H. Zhang, "A fingerprint matching algorithm based on Delaunay triangulation net," *5th International Conference on Computer and Information Technology*, 2005, pp. 591-595.

[14] H. Deng and Q. Huo, "Minutiae matching based fingerprint verification using Delaunay triangulation and aligned-edge-guided triangle matching," *International Conference on Audio-and Video-Based Biometric Person Authentication*, 2005, pp. 270-278.

[15] Y. Yin, H. Zhang, and N. Liu, "Fingerprint matching based on Delaunay triangulation," *Journal of Computer Research and Development*, vol. 42, no. 9, pp. 1622-1627, 2005.

[16] C. Wang and M. Gavrilova, "Delaunay triangulation algorithm for fingerprint matching," *3rd International Symposium on Voronoi Diagrams in Science and Engineering*, 2006, pp. 208-216.

[17] X. Liang, A. Bishnu, and T. Asano, "A robust fingerprint indexing scheme using minutia neighbourhood structure and low-order Delaunay triangles," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 4, pp. 721-733, 2007.

[18] T. Uz, G. Bebis, A. Erol, and S. Prabhakar, "Minutiae-based template synthesis and matching using hierarchical Delaunay triangulations," *IEEE 1st International Conference on Biometrics: Theory, Applications, and Systems*, 2007, pp. 1-8.

[19] M. Vatsa, R. Singh, A. Noore, and S. Singh, "Quality induced fingerprint identification using extended feature set," *IEEE 2nd International Conference on Biometrics: Theory, Applications and Systems*, 2008, pp. 1-6.

[20] P. Júnior, A. de Nazare-Junior, and D. Menotti, "A complete system for fingerprint authentication using Delaunay triangulation," *Pattern Recognition*, Department of Computing, Federal University of Ouro Preto, 2010, pp. 1-7.

[21] A. C. Chau and C. Soto, "Hybrid algorithm for fingerprint matching using Delaunay triangulation and local binary patterns," *16th Iberoamerican Congress Conference on Progress in Pattern Recognition, Image Analysis, Computer Vision, and Applications*, 2011, pp. 692-700.

[22] S. Tulyakov, F. Farooq, P. Mansukhani, and V. Govindaraju, "Symmetric hash functions for secure fingerprint biometric systems," *Pattern Recognition Letters*, vol. 28, no. 16, pp. 2427-2436, 2007

[23] X. Li, "Interoperable protected fingerprint minutiae templates," Master Thesis (2012), Norwegian University of Science and Technology.

[24] M. Sandhya and M. Prasad, "A bio-cryptosystem for fingerprints using Delaunay neighbour structures (DNS) and fuzzy commitment scheme," *Advances in Signal Processing and Intelligent Recognition Systems*, 2016, pp. 159-171.

[25] M. Sandhya, M. Prasad, and R. Chillarige, "Generating cancellable fingerprint templates based on Delaunay triangle feature set construction," *IET Biometrics*, vol. 5, no. 2, pp. 131-139, 2016.

[26] C. Abirami and M. Begum, "Biometric cryptosystem based on Delaunay quadrangle structure for fingerprint template protection and person identification," *Middle-East Journal of Scientific Research*, vol. 24, no.S2, pp. 53-57, 2016.

[27] W. Yang, J. Hu, and S. Wang, "A Delaunay quadrangle-based fingerprint authentication system with template protection using topology code for local registration and security enhancement," *IEEE transactions on Information Forensics and Security*, vol. 9, no. 7, pp. 1179-1192, 2014.

[28] M. Sagayee, "A Delaunay pentangle-based fingerprint authentication system for preserving privacy using topology code," *Advanced Technology for Leaning*, vol. 2, no. 6, pp. 142-149, 2015.

[29] V. Krivokuca, W. Abdulla, and A. Swain, "A non-invertible cancellable fingerprint construct based on compact minutiae patterns," *International Journal of Biometrics*, vol. 6, no. 2, pp. 125-142, 2014.

[30] S. Kumari and A. Moghe, "Delaunay hexangle based fingerprint matching scheme for authentication," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 6, no. 5, pp. 489-494, 2016.

[31] H. Li, J. Zhang, and Z. Zhang, "Generating cancellable palmprint templates via coupled nonlinear dynamic filters and multiple orientation palmcodes," *Information Sciences*, vol. 180, pp. 3876–3893, 2010.

[32] H. Li and L. Wang, "Chaos-based cancellable palmprint authentication system," *Procedia Engineering*, vol. 29, pp. 1239-1245, 2012.

[33] E. Du, K. Yang, and Z. Zhou, "Key incorporation scheme for cancellable biometrics," *Journal of Information Security*, vol. 2, pp. 185-194, 2011.

[34] C. Rathgeb, F. Breitinger, and C. Busch, "Alignment-free cancellable iris biometric templates based on adaptive bloom filters," *IAPR International Conference on Biometrics*, 2013, pp. 1-8.

[35] C. Rathgeb and C. Busch, "Cancellable multi-biometrics: mixing iris-codes based on adaptive bloom filters," *Computers & Security*, vol. 42, pp. 1-12, 2014.

[36] C. Rathgeb, M. Gomez-Barrero, C. Busch, J. Galbally, and J. Fierrez, "Towards cancellable multi-biometrics based on bloom filters: a case study on feature level fusion of face and iris," *International Workshop on Biometrics and Forensics*, 2015, pp. 1-6.

[37] J. Hämmerle-Uhl, E. Pschernig, and A. Uhl, "Cancellable iris biometrics using block re-mapping and image warping," *International Conference on Information Security*, 2009, pp. 135-142.

[38] J. Pillai, V. Patel, R. Chellappa, and N. Ratha, "Sectored random projections for cancellable iris biometrics,"

International Conference on Acoustics, Speech and Signal Processing, 2010, pp. 1838-1841.

[39] O. Osama, N. Tsumura, and T. Nakaguchi, "Bioencoding: a reliable tokenless cancellable biometrics scheme for protecting iriscodes," *IEICE Transactions on Information and Systems*, vol. 93, no. 7, pp. 1878-1888, 2010.

[40] S. Kanade, D. Petrovska-Delacretaz, and B. Dorizzi, "Cancellable biometrics for better security and privacy in biometric systems," *1st International Conference on Advances in Computing and Communications*, 2011, pp. 20-34.

[41] M. Savvides, B. Kumar, and P. Khosla, "Cancellable biometric filters for face recognition," *International Conference on Pattern Recognition*, vol. 3, pp. 922-925, 2004.

[42] S. Hirata and K. Takahashi, "Cancellable biometrics with perfect secrecy for correlation-based matching," *Advances in Biometrics, Lecture Notes in Computer Science*, M. Tistarelli and M. Nixon, Eds., vol. 5558, pp. 868–878, 2009.

[43] K. Takahashi and S. Hirata, "Cancellable biometrics with provable security and its application to fingerprint verification," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 94-A, no. 1, pp. 233-244, 2011.

[44] E. Maiorana, P. Campisi, J. Fierrez, J. Ortega-Garcia, and A. Neri, "Cancellable templates for sequence-based biometrics with application to on-line signature recognition," *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans*, vol. 40, no. 3, pp. 525-538, 2010.

[45] W. Xu, Q. He, Y. Li, and T. Li, "Cancellable voiceprint templates based on knowledge signatures," *International Symposium on Electronic Commerce and Security*, 2008, pp. 412-415.

[46] T. Connie, A. Teoh, M. Goh, and D. Ngo, "Palmhashing: a novel approach for cancellable biometrics," *Information Processing Letters*, vol. 93, no. 1, pp. 1-5, 2005.

[47] J. Zuo, N. Ratha, and J. Connell, "Cancellable iris biometric," *International Conference on Pattern Recognition*, 2008, pp. 1-4.

[48] G. Bajwa and R. Dantu, "Neurokey: towards a new paradigm of cancellable biometrics-based key generation using electroencephalograms," *Computers & Security*, vol. 62, pp. 95-113, 2016.

[49] A. Jain, K. Nandakumar, and A. Ross, "50 years of biometric research: accomplishments, challenges, and opportunities," *Pattern Recognition Letters*, vol. 79, pp. 80-105, 2016.

[50] A. Rukhin et al., "A statistical test suite for the validation of random number generators and pseudo random number generators for cryptographic applications," NIST special publication: 800-22.

[51] C. Ellison, "Cryptographic random numbers," Accessed online on 07/29/2016: http://world.std.com/~cme/

[52] Q. Gao, "A preliminary study of fake fingerprints," International Journal of Computer Network and Information Security, vol. 6, no. 12, pp. 1-8, 2014.

[53] FVC2000, available at: http://bias.csr.unibo.it/fvc2000/

[54] FVC2002, available at: http://bias.csr.unibo.it/fvc2002/

[55] FVC2004, available at: http://bias.csr.unibo.it/fvc2004/

[56] NIST fingerprint software, Accessed online on 06/27/2016: http://www.nist.gov/itl/iad/ig/nbis.cfm

Authors' Profiles

Qinghai Gao, born in Shandong China in 1969, received a Ph.D. in computer science from the City University of New York in 2007.

Currently, he is an Associate Professor in the Department of Security Systems & Law Enforcement Technology at Farmingdale State College. Before joining Farmingdale, he taught full-time in the China University of Petroleum for a few years. From 1998 to 2007 he taught as Adjuncts in Brooklyn College, Lehman College, NYC College of Technology, College of Staten Island, and York College. Since 2001 he held various positions in IT industry as Software Developer, Database Administrator, Network Engineer, Researcher, Consultant, and Information Security Specialist. He has extensive experience with fingerprint identification, computer security, and cryptography. He has published one book and numerous articles. His present research interests include Fingerprint Identification, Digital Forensics, Computer Security, Biometrics, Cryptography, and Bioinformatics.

Dr. Gao is a current member of following professional organizations: International Association of Identification (IAI), Association of Computing Machinery (ACM), International Association of Computer Investigative Specialists (IACIS), and High Technology Crime Investigation Association (HTCIA).

How to cite this paper: Qinghai Gao,"Toward Constructing Cancellable Templates using K-Nearest Neighbour Method", International Journal of Computer Network and Information Security(IJCNIS), Vol.9, No.5, pp.1-10, 2017.DOI: 10.5815/ijcnis.2017.05.01