Hindawi
Security and Communication Networks
Volume 2019, Article ID 4202671, 8 pages
https://doi.org/10.1155/2019/4202671

Research Article

A Cancelable Template for the Low-Quality Fingerprints from Wearable Devices

Sanghoon Lee and Ik Rae Jeong

School of Information Security, Korea University, Seoul 02841, Republic of Korea

Correspondence should be addressed to Ik Rae Jeong; irjeong@korea.ac.kr

Received 1 February 2019; Revised 29 April 2019; Accepted 14 May 2019; Published 2 June 2019

Guest Editor: Alvaro Araujo

Biometric authentication in wearable devices is different from the common biometric authentication systems. First of all, sensitive information such as fingerprint and iris of a user is stored in a wearable device owned by the user rather than being stored in a remote database. Wearable devices are portable, and there is a risk that the devices might be lost or stolen. In addition, the quality of the extracted image from the wearable devices is lower than that of the common biometric acquisition sensor. In the paper, we propose a novel cancelable fingerprint template which is irreversible to the original biometrics and has excellent accuracy even in low quality images.

1. Introduction

Biometrics is a physical or behavioral characteristic of an individual. Commonly, knowledge-based and token-based recognition can be easily forgotten, lost, stolen, or shared. Biometrics is more difficult to be forgotten, lost, or shared. And it has universality, distinctiveness, and permanence [1]. Therefore, biometrics is used as a tool for authentication in a variety of environments. With advances in sensor technology, user biometric recognition on wearable devices has become popular in recent years. Authentication with sensor-equipped wearable devices offers many advantages over existing authentication methods. Previous authentication has fixed sensors and biometric information is stored on connected databases managed by the third party. On the other hand, biometrics used in the wearable devices can perform continuous authentication of a user, and biometric information of the user is stored on a wearable device [2]. This means that the user does not need to share sensitive information with third parties. However, this approach causes other security problems. First, due to the property of wearable devices, sensors are limited in size. Then the quality of biometric information measured is necessarily low, resulting in a high error rate. Second, wearable devices can be worn and carried around by the user, which can cause the device to be lost or stolen. The adversary then has a chance to get the user biometrics. Cancelable template is suitable for this application. It makes it possible to revoke a compromised template and reissue by a new one. Cancelable template protection scheme is required to satisfy the following requirements [3]:

(i) Revocability: The transformed template should be possible to be revoked and replaced. The requirement is necessary, because if the transformed biometric template is compromised, it should be revoked and replaced with a new one based on the same user's biometric information.

(ii) Unlinkability: It should be impossible to link the transformed templates of the same user. The requirement is necessary, because if the user has made a new transformed template after the user's old transformed template is revoked, it might be desirable that the two transformed templates look independent.

(iii) Noninvertibility: It must be computationally difficult to obtain the original template from the transformed template. Consequently, the template matching must be done between the transformed templates

(iv) Performance: The performance of the biometric recognition using template transformation should be plausibly efficient compared to the performance of the biometric recognition without transformation.

Design of cancelable fingerprint template is divided into alignment methods and alignment-free methods. Alignment methods need the position and orientation of the singular points and align minutiae with them. So, accuracy of alignment based technique depends on how precise the singular points are extracted. However, it is hard to precisely determine the core and delta (singular) points [4]. Alignment-free methods rely on the local structures of minutiae which is invariant rotation and translation. Minutiae extraction is much simpler than singular extraction. Then alignment-free based technique has higher accuracy in low quality images.

We propose a novel alignment-free features of the Delaunay triangle which is robust against low quality fingerprint images [5, 6]. We organized rest of the paper as follows. In Section 2, we review cancelable fingerprint template approaches. In Section 3, we present the proposed method. We comparing existing cancelable fingerprint template with experimental results are analysed in Section 4. The last section includes conclusion.

2. Related Works

The simple approach to protect sensitive information like biometrics is to use encryption or hash function. It is hard to infer from the transformed information to original information. This is an important property in protecting information. However, these functions produce a dramatically different output even with small changes in the input. In practice, all biometric traits are easily affected by the environment. For example, changes in illumination can make a large variation in the appearance of faces. The biometric encryption schemes are promising in some environments, but they might not be directly used in the other environments. We note that the encrypted template should be decrypted in order to be matched with the query template, and thus we need to trust the server.

To overcome limitations of the existing biometric authentication system, many biometric template protection methods have been proposed. Ratha et al. analyzed the vulnerabilities of the existing system and first proposed the concept of a cancelable biometric as a way to resolve them [7]. Ahn et al. have proposed alignment-free fingerprint cancelable template using minutia triplets [8]. Ahmad et al. used rotation- and translation-free polar coordinate instead of Cartesian coordinate for information between minutia points [9]. Ferrara et al. have developed cancelable fingerprint template based on MCC (Minutia Cylinder-Code) [10–12]. Sandhya et al. have utilized Delaunay triangulation for creation fingerprint features [13]. Wang et al. have proposed a cancelable fingerprint template formed zoned minutia pair [14].

Yang et al. have proposed a cancelable fingerprint template on mobile devices [15]. To mitigate the effect of distortion, the authors combined two features, polar coordinate-based features, and Delaunay triangulation-based features. Therefore, their scheme requires more storages to store the combined features. For example, the fingerprint image 1_1.tif in FVC2002 DB2 is transformed as the protected template whose size is 148.2 KB [15]. On the other hand, our scheme requires just 2.27 KB for the same image 1_1.tif. Therefore, our proposed scheme is about 65 times more efficient than the Yang et al.'s scheme and thus more suitable for wearable devices with limited storage.

Even though all these researches have the EER less than 1% of medium and high quality fingerprint images in FVC databases, they have high EER almost 10% on low quality images in FVC2002 DB3 and FVC2004 DB2 fingerprint databases. Our proposed approach in this paper provides a solution to prior studies and satisfy requirements of cancelable fingerprint template.

3. Noise-Resistant Cancelable Fingerprint Template

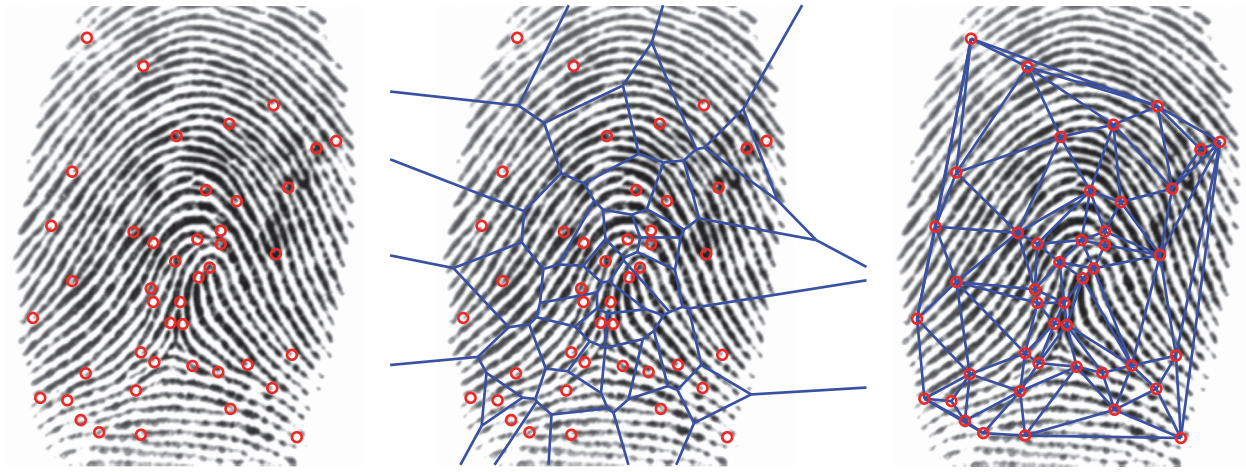
The main idea of the proposed method for cancelable fingerprint template is to generate 4-dimensional points using the extracted triangles that belong to the individual. These 4-dimensional points are used as a secured fingerprint template for user authentication.

3.1. Delaunay Triangulation Net. Extract the minutiae points $\mathrm{m_i} = (x_i, y_i, \theta_i)_{i=1}^{n}$, where n is the number of minutiae, in the fingerprint image. (x_i, y_i) and θ_i represent the coordinates and orientation of minutiae, respectively. A Voronoi diagram which divides the entire region into some small partitions is generated from the minutiae points. In each small region, a minutia point $\mathrm{m_i}$ is only one. Other points in neighbor areas are closer to $\mathrm{m_i}$ than other minutiae points. Then, Delaunay triangulation net is created by connecting between the minutiae of every region and its neighbor regions [5] (see Figure 1). The reason for using the Delaunay triangulation net is that it is structurally more stable under distortion. If any variable distortion is occurring in fingerprint image, every minutia holds the same vicinity structure as long as the minutiae under tolerance region. And several spurious minutiae are added or missed affects only those regions that contain the minutiae [6].

3.2. Noise-Resistant Feature Extraction. We used interior angles of each triangle as a feature in the Delaunay triangulation net. The main steps of extraction features are the following:

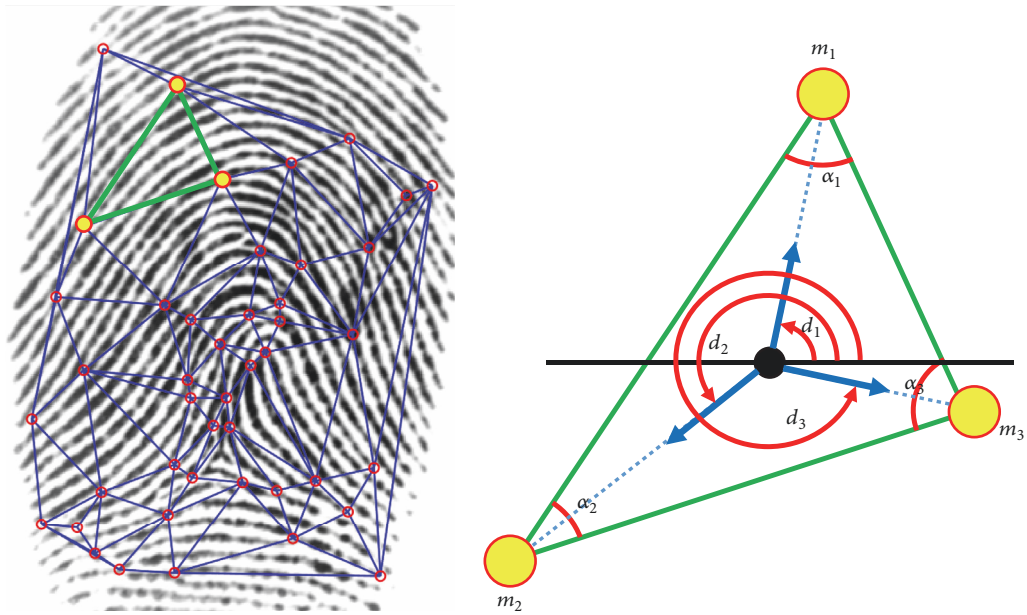
(i) Select a triangle $\triangle \mathrm{m_1 m_2 m_3}$ from Delaunay triangulation net as shown in Figure 2(a).

(ii) Compute the directions $\mathrm{d_i}$ $(i = 1, 2, 3)$ of the vectors from the centroid of the triangle to each vertex $\mathrm{m_i}$ $(i = 1, 2, 3)$.



(a) (b) (c)

Figure 1: Various features on an image: (a) Minutiae, (b) Voronoi diagram, and (c) Delaunay triangulation net.



(a) (b)

Figure 2: Feature generation for our method from (a) triangles on Delaunay triangulation net to (b) triangles with only interior angles without side lengths.

(iii) Calculate the included angle α_i ($i = 1, 2, 3$) (interior angle) between the normalized vectors from each minutia to the remaining minutiae.

(iv) Align the calculated interior angles $(\alpha_1, \alpha_2, \alpha_3)$ in ascending order of d_i.

(v) Repeat the above procedures for each triangle.

Figure 2(b) shows the diagram of proposed triangle features. If k triangles are present in the fingerprint, the proposed feature set is a $k \times 3$ matrix of interior angles.

3.3. Generation of 4D Feature Set. Using the user-specific key, features set of 3-dimensional point is projected to 4-dimensional space. It is set differently by applications, which enables 4D template to be diverse. The user-specific key is 3 by 4 matrix which elements are randomly chosen in the range $(0, 10]$. The projected 4-dimensional features set is calculated by multiply 3-dimensional features set and user-specific key. Figure 3 shows the process of creating the proposed feature.

The size of the key matrix is determined experimentally. We conducted an experiment with various feature dimensions, from 1 to 5 dimensions (see Table 1). As the dimension

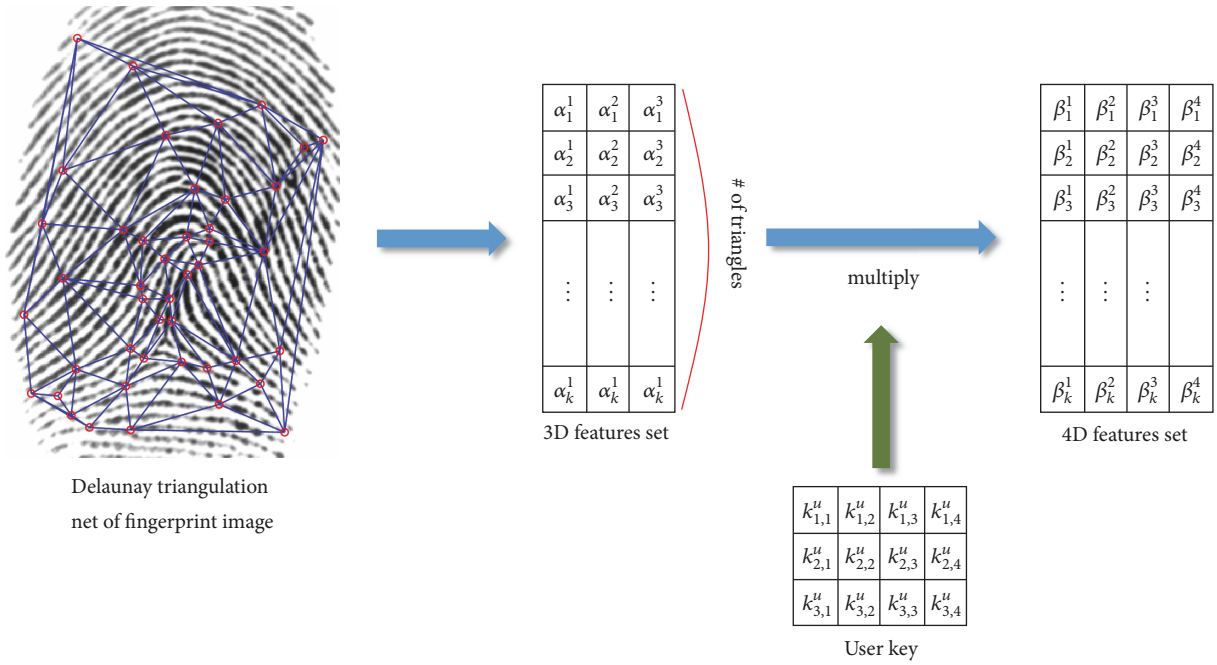


Figure 3: Overview of our method.

Table 1: EERs and template sizes depending on the dimensions of features in FVC2002 DB2.

	1	2	3	4	5
EER (%)	27.86	5.959	0.6087	0.0202	0.0143
Size (KB)	0.756	1.284	1.76	2.27	2.78

increases, the EER (Equal Error Rate, mentioned in Section Experimental Analysis) greatly decreases. On the other hand, the size of the template is linearly increased proportional to the dimension of features. We note that the EER with the four dimensions seems to be sufficient for many applications. And the template size with the four dimensions is still small and thus adequate for devices with the limited storage.

3.4. Matching. Matching between the enrolled template T^{enroll} and the query template T^{query} depends on how many triangles are matched each other. Assuming that the numbers of triangles matched between T^{enroll} and T^{query} are N^{match}, the numbers of triangles of T^{enroll} and T^{query} are n^{enroll} and n^{query}, respectively, the similarity score S is calculated by

$$S = \sqrt{\frac{N^{match} \times N^{match}}{n^{enroll} \times n^{query}}} \quad (1)$$

If S is larger than a threshold, then these two templates are regarded as a match.

4. Experimental Analysis

In this section, we evaluate the proposed technique on FVC2002 DB1, DB2, DB3, and FVC2004 DB2 fingerprint databases, using the Fingerprint Verification Competition protocol [16].

4.1. Experimental Procedure. The trial version of Neurotechnology VeriFinger SDK 11 which is commercial software is used to extract minutiae from the fingerprint images [17]. Each FVC databases contain 800 fingerprint sample images from 100 distinct subjects (i.e., each subject has 8 different images from same finger). These databases have different quality images because they were created using different types of fingerprint sensors. Details of each database are in Table 2.

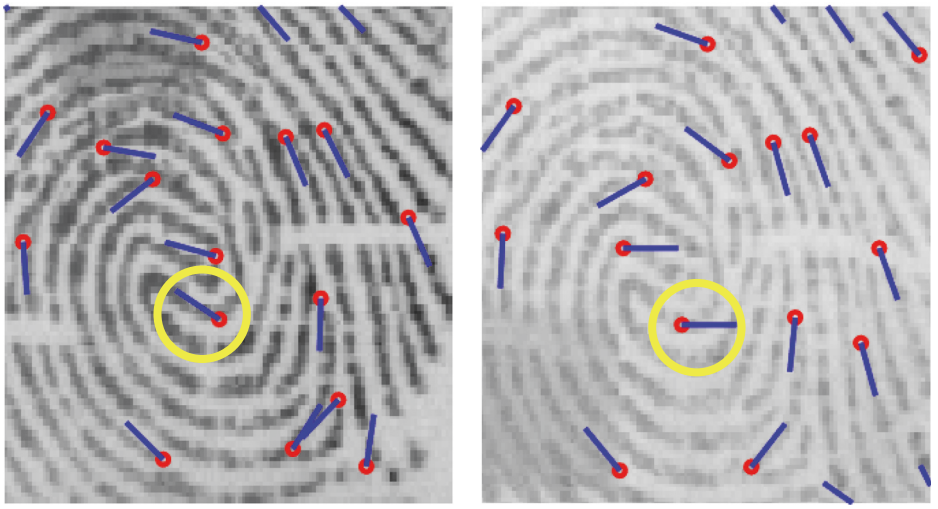
To assess whether the proposed method meets the requirements of the cancelable template, focus on the following:

(i) Performance of lost key scenario

(ii) Revocability and unlinkability

(iii) Security

Our experiments use Equal Error Rate (EER), False Accept Rate (FAR), and False Reject Rate (FRR) to measure performance. FAR is the probability that two fingerprint templates from different subjects successfully matched. FRR is the probability that two fingerprint templates from the same subject failed to match. EER means the probability that FAR and FRR are equal. The values indicating performance are calculated from the genuine test and the imposter test. According to the FVC protocol, the genuine test compares the subject's fingerprint template with the remaining fingerprint templates of the same subject and calculates the distribution of the similarity score (i.e., 2800 = 28 × 100 test results in this case). The imposter test compares the subject's first fingerprint template with the other subject's first fingerprint



(a) (b)

Figure 4: Different direction of same minutia (a) FVC2004 DB2 1_4.tif. (b) FVC2004 DB2 1_7.tif.

Table 2: Information databases used for our experiments.

Database	FVC2002 DB1	FVC2002 DB2	FVC2002 DB3	FVC2004 DB2
Total fingers	100	100	100	100
Sample per finger	8	8	8	8
Sensor type	Optical	Optical	Capacitive	Optical
Image size	388x374	296x560	300x300	328x364
Quality of images	Good - Medium	Medium	Medium - Low	Very Low

Table 3: Performance comparison under lost key scenario (EER in %).

Method	FVC2002			FVC2004
	DB1	DB2	DB3	DB2
Yang et al. [18]	5.93	4	-	-
Wang et al. [19]	2	2.3	6.12	-
Sandhya et al. [13]	3.69	2.98	6.89	12.95
Sandhya et al. [20]	2.19	1.6	6.14	12.71
Wang et al. [21]	1	2	5.2	13.3
Wang et al. [14]	0.19	1	4.29	9.01
Kumar et al. [22]	1.58	1.7	5.47	7.74
Kho et al. [23]	2.48	1.51	7.03	7.44
proposed	1.82	1.06	2.2	2.46

template and calculates the distribution of the similarity score (i.e., $4950 = 100 \times 99/2$ test results in this case).

4.2. Performance of The Lost Key Scenario. Lost key scenario is the worst scenario, assuming that the user has lost the secret key or that the attacker knows the secret key. We simulated this scenario by applying the same key to all of the subjects being tested. The differences between the proposed technique and the previous alignment-free cancelable fingerprint techniques are summarized in Table 3. In previous methods, the EER was very high in low quality images (FVC2002 DB3, FVC2004 DB2), but the proposed technique did not change EER significantly in low quality images. The existing methods used fingerprint features were the relative angles and distances between minutiae. To calculate orientation of minutia, the orientation map or direction of ridge must be exactly calculated. In low quality fingerprint images, and it is difficult to maintain the accuracy of calculations due to noise. Figure 4 shows the different directions of the same minutia. Our method shows powerful performance on FVC2002 DB3 and FVC2004 DB2, and this performance is similar to the accuracy of other methods on FVC2002 DB1 and DB2.

4.3. Revocability and Unlinkability. To satisfy the revocability, even if the template is compromised by the adversary, the new template from the same biometric data to be replaced

Table 4: Percentage of success attacks on revoked template attack.

Database	Medium-security (%)		High-security (%)	
	Type-I	Type-II	Type-I	Type-II
FVC2002 DB1	0.38	0.47	0	0
FVC2002 DB2	0.52	0.14	0	0
FVC2002 DB3	1.33	0.11	0.07	0
FVC2004 DB2	1.38	0.22	0	0

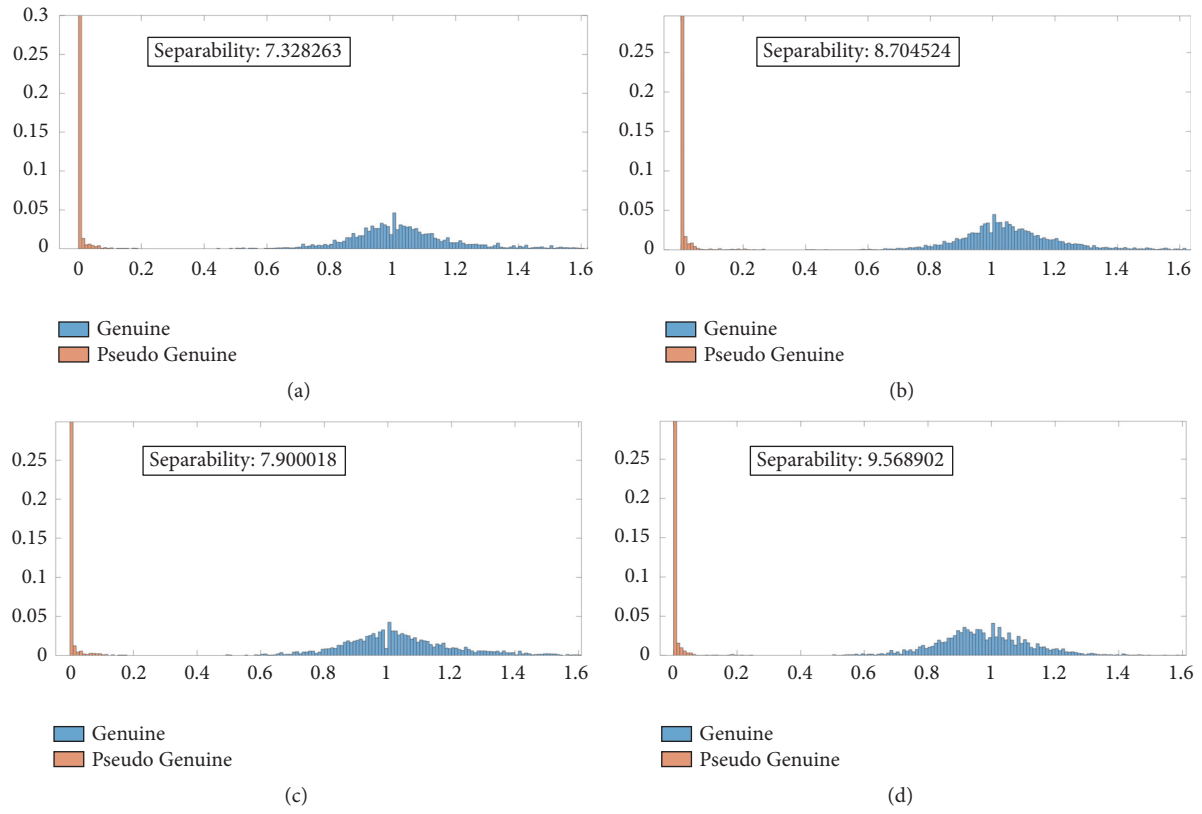


Figure 5: Histogram of Genuine/Pseudogenuine score distributions for the proposed approach (a) For FVC2002 DB1. (b) For FVC2002 DB2. (c) For FVC2002 DB3. (d) For FVC2004 DB2.

should not be related to the previous template. We assess the robustness of the proposed method against revoked template attack [11]. In the revoked template attack, there are following two scenarios:

Type-I: a revoked template is used to match a new template from same fingerprint image using different key

Type-II: a revoked template is used to match a new template from different fingerprint image of same fingerprint using different key

These scenarios have been measured under medium security level (used matching threshold is 0.1% FAR) and high security level (used matching threshold is 0% FAR) on four databases. Table 4 shows the success rate of simulated attacks.

Unlinkability is important property of cancelable template aspect to privacy. If two templates created by same fingerprint in different applications are not associated, it is said to satisfy unlinkability. To simulate unlinkability, our experiment sets two systems. For System 1, we randomly chose the secret key in the range $(0, 10]$ and chose randomly the secret key in the range $(10, 20]$ for System 2. Each fingerprint template in System 1 is compared with fingerprint template of same subject in System 2 to evaluate the Pseudogenuine score. Figure 5 shows that Genuine/Pseudo-Genuine score distributions. We used the separability measure proposed by Lee et al. [24].

$$separability = \frac{|\mu_G - \mu_P|}{\sqrt{(\sigma_G^2 + \sigma_P^2)/2}} \quad (2)$$

(i) μ_G and μ_P: the means of genuine and pseudo-genuine score distributions

(ii) σ_G^2 and σ_P^2: the variances of genuine and pseudo-genuine score distributions

The histograms are well separated. The separability of FVC2002 DB1, DB2, DB3, and FVC2004 DB2 is 7.33, 8.7, 7.9, and 9.57, respectively. It means that the template generated by proposed method has robustness against cross-matching.

4.4. Security. Noninvertibility of cancelable template ensures that it is computationally impossible to reconstruct the original biometrics from the transformed template. For the security analysis, [13] assume that the adversary attacks the feature set scenario. In [13], they have used three sides of Delaunay triangle to make a feature set. The triangles in the Delaunay triangulation net are adjacent to each other. Therefore, the adjacent triangles have the same length with respect to one of side lines. Finally, the Delaunay triangulation net made of the minutia points can be reconstructed from the feature set. This helps to know the approximate fingerprint minutia positions. Our feature set does not include the length of the triangle sides, and thus it is impossible to reconstruct the Delaunay triangles from our feature set. Note that our feature set includes only the information about the interior angles, and thus it is difficult to find the adjacent triangles for a given triangle.

5. Conclusion

This paper presented a new method to create accurate cancelable fingerprint templates even in low quality databases. Our method is based on the novel feature set from Delaunay triangles for fingerprint minutiae. Our proposed scheme meets revocability, unlinkability, security, and performance, which are required for template protection. The proposed approach is suitable for environments with limited sensor performance, such as wearable devices. This method will further improve the accuracy of user authentication using wearable devices.

Data Availability

Data used to support the findings of this study are included with in the article

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This research was supported by the MIST (Ministry of Science and ICT), Korea, under the National Program for Excellence in SW supervised by the IITP (Institute for Information & communications Technology Promotion) (2015-0-00936).

References

[1] A. K. Jain, A. A. Ross, and K. Nandakumar, *Introduction to Biometrics*, Springer Science & Business Media, New York, NY, USA, 2011.

[2] S. Seneviratne, Y. Hu, T. Nguyen et al., "A survey of wearable devices and challenges," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2573–2620, 2017.

[3] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP Journal on Advances in Signal Processing*, vol. 113, article no. 113, 2008.

[4] P. Gupta and P. Gupta, "A robust singular point detection algorithm," *Applied Soft Computing*, vol. 29, pp. 411–423, 2015.

[5] S. Fortune, "Voronoi diagrams and delaunay triangulations," in *Handbook of Discrete and Computational Geometry*, J. E. Goodman and J. O'Rourke, Eds., pp. 377–388, CRC Press, Inc., Boca Raton, FL, USA, 1997.

[6] M. Abellanas, F. Hurtado, and P. A. Ramos, "Structural tolerance and delaunay triangulation," *Information Processing Letters*, vol. 71, no. 5-6, pp. 221–227, 1999.

[7] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Systems Journal*, vol. 40, no. 3, pp. 614–634, 2001.

[8] D. Ahn, S. G. Kong, Y. Chung, and K. Y. Moon, "Matching with secure fingerprint templates using non-invertible transform," in *Proceedings of the 2008 Congress on Image and Signal Processing*, vol. 2, pp. 29–33, IEEE, Sanya, China, May 2008.

[9] T. Ahmad, J. Hu, and S. Wang, "Pair-polar coordinate-based cancelable fingerprint templates," *Pattern Recognition*, vol. 44, no. 10-11, pp. 2555–2564, 2011.

[10] M. Ferrara, D. Maltoni, and R. Cappelli, "Noninvertible minutia cylinder-code representation," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 6, pp. 1727–1737, 2012.

[11] M. Ferrara, D. Maltoni, and R. Cappelli, "A two-factor protection scheme for MCC fingerprint templates," in *Proceedings of the International Conference of the Biometrics Special Interest Group (BIOSIG)*, pp. 1–8, IEEE, Darmstadt, Germany, 2014.

[12] R. Cappelli, M. Ferrara, and D. Maltoni, "Minutia cylinder-code: a new representation and matching technique for fingerprint recognition," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 32, no. 12, pp. 2128–2141, 2010.

[13] M. Sandhya, M. V. N. K. Prasad, and R. R. Chillarige, "Generating cancellable fingerprint templates based on delaunay triangle feature set construction," *IET Biometrics*, vol. 5, no. 2, pp. 131–139, 2016.

[14] S. Wang, W. Yang, and J. Hu, "Design of alignment-free cancelable fingerprint templates with zoned minutia pairs," *Pattern Recognition*, vol. 66, pp. 295–301, 2017.

[15] W. Yang, J. Hu, S. Wang, and Q. Wu, "Biometrics based privacy-preserving authentication and mobile template protection," *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 7107295, 17 pages, 2018.

[16] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, "FVC2000: fingerprint verification competition," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 24, no. 3, pp. 402–412, 2002.

[17] Neurotechnology, Verifinger SDK, http://www.neurotechnology.com.

[18] W. Yang, J. Hu, S. Wang, and J. Yang, "Cancelable fingerprint templates with delaunay triangle-based local structures," in *Cyberspace Safety and Security*, vol. 8300 of *Lecture Notes in Computer Science*, pp. 81–91, Springer International Publishing, Cham, Switzerland, 2013.

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

[20] M. Sandhya and M. V. N. K. Prasad, "Securing fingerprint templates using fused Structures," *IET Biometrics*, vol. 6, no. 3, pp. 173–182, 2017.

[21] S. Wang, G. Deng, and J. Hu, "A partial Hadamard transform approach to the design of cancelable fingerprint templates containing binary biometric representations," *Pattern Recognition*, vol. 61, pp. 447–458, 2017.

[22] M. M. Kumar, M. V. Prasad, and U. S. Raju, "Cancellable fingerprint template generation using rectangle-based adjoining minutiae Pairs," in *Proceedings of the 2nd International Conference on Biometric Engineering and Applications*, pp. 30–37, ACM, Amsterdam, Netherlands, May 2018.

[23] J. B. Kho, J. Kim, I. Kim, and A. B. Teoh, "Cancelable fingerprint template design with randomized non-negative least squares," *Pattern Recognition*, vol. 91, pp. 245–260, 2019.

[24] C. Lee, J.-Y. Choi, K.-A. Toh, S. Lee, and J. Kim, "Alignment-free cancelable fingerprint templates based on local minutiae information," *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, vol. 37, no. 4, pp. 980–992, 2007.