Hindawi
Security and Communication Networks
Volume 2020, Article ID 8256929, 8 pages
https://doi.org/10.1155/2020/8256929

Research Article

On the Unlinkability of Fingerprint Shell

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 5 September 2019; Revised 12 November 2019; Accepted 29 January 2020; Published 4 March 2020

Academic Editor: Jiankun Hu

To prevent the leakage of original biometric information of a user, it may be transformed into a cancelable form. A cancelable biometric transformation should satisfy four requirements: unlinkability, revocability, noninvertibility, and performance. In 2014, Moujahdi et al. proposed a new cancelable fingerprint transformation called fingerprint shell, which was also later discussed by Ali et al. In this paper, we show that all of the shell fingerprint schemes presented by Moujahdi et al. and Ali et al. do not satisfy the condition of unlinkability.

1. Introduction

The development of sensor technology has made it easier to use biometric recognition systems, and as a result, the demand for biometric authentication has increased sharply in devices such as smart phones and tablets. Biometric authentication is simpler and more convenient than other authentication methods using the secret user information.

However, biometric information cannot be replaced if it is compromised or exposed, meaning that it must be protected [1, 2]. In feature transformation schemes, biometric information is transformed into a protected biometric template using the transformation function stored on a server. During the verification process, queried biometric information is also transformed using the same function and a matching score is calculated between the stored transformed template on the server and the queried transformed template to determine the validity of the information.

According to the property of transformation functions, feature transformation can be classified two ways: noninvertible transformation [3, 4] and salting [5, 6]. The noninvertible transformation applies a one-way function such as a hash function to the original biometric information. It should be computationally difficult to reconstruct the original biometric information from the transformed template even if the parameters of the functions are revealed. Salting is an invertible transformation that uses a user-specific key. That is, if an adversary obtained both the user key and the transformed template, they could recover the original biometric information.

The noninvertible feature transformation methods must meet the following properties [7]:

(i) Revocability: it should be possible to revoke and replace the transformed template. This is necessary because if the transformed biometric template were to become compromised, it should be revoked and replaced with a new one based on the biometric information of the same user.

(ii) Unlinkability: it should be impossible to link transformed templates derived from the same user. This is necessary because if the user were to make a new transformed template after the user's old transformed template is revoked, it is desirable for the two transformed templates to look independent.

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

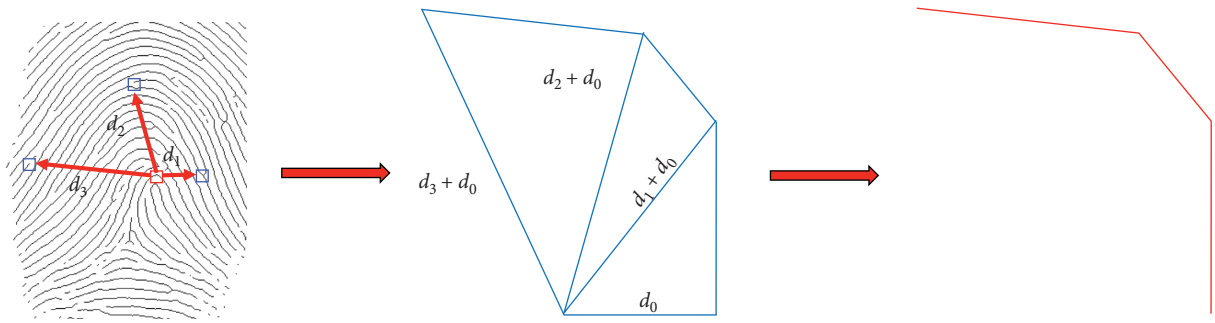

Figure 1: Simple example of fingerprint shell construction.

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

The unlinkability is often called diversity [8, 9]. Diversity means that it is necessary to be able to generate diverse templates in one fingerprint, and there should be no relation between them. In addition, cross-matching should not be possible between templates in different applications. In other words, it is called unlinkability. We use unlinkability, which is more intuitive than diversity.

Recently, as various biometric traits such as ECG (electrocardiogram) and speech are widely used, concern about security has increased. Chee et al. proposed the speech template protection technique using the cancelable transform, called Random Binary Orthogonal Matrices Projection (RBOMP) hashing [10]. Wu et al. generated cancelable ECG templates with a subspace-based approach, MUSIC algorithm [11]. Some attacks have also been studied for cancelable biometric templates such as zero effort attack, inversion attack, ARM (attacks via record multiplicity), and similarity-based attack [8, 12]. Dong et al. proposed a similarity-based attack framework that can be applied to any cancelable biometric templates [13].

In 2014, Moujahdi et al. proposed a new noninvertible feature transformation scheme for minutiae-based fingerprint recognition called fingerprint shell [9]. Ali and Prakash proposed new fingerprint shell schemes [14, 15]. We propose a method to extract the original distance that should be protected from the fingerprint shell and use the framework to quantify how unsafe the shells are in this method. As a result, we show that the shells do not satisfy the condition of unlinkability.

2. Review of Fingerprint Shell

The basic idea of the fingerprint shell is to make a spiral curve using the information extracted from minutiae and singular points of a user. The process of making a fingerprint shell is as follows:

(1) Minutiae and singular points are extracted from the fingerprint of a user.

(2) For each singular point, the distance between each minutiae and singular point is calculated. We note that the distances are not changed by shifting or rotating a fingerprint image. We also note that the number of curves will be equal to the number of singular points.

(3) Suppose there are n minutiae points. Then, $d_1, d_2, \ldots, d_n$ are n distances from a singular point to the minutiae. The distances are sorted in an ascending order.

(4) The sorted distances and user key d_0 are used to construct the hypotenuse of a number of adjacent right triangles (Figures 1 and 2). It should be noted that user key d_0 is added to all extracted distances d_i before triangle construction. h_i represents the length of the height of the triangle, which is calculated with the *Pythagorean* theorem. The hypotenuse of the previous triangle becomes the base of the proceeding triangle. As a result, except the initial triangle, all subsequent triangles rotate by the accumulated angle.

(5) Finally, the fingerprint shell template consists of the top vertices of the triangles, which are stored as transformed templates.

For example, suppose that a fingerprint has two minutiae with $(3, 2)$ and $(5, 7)$ and singular point with $(5, 5)$ coordinates. The sorted distances, d_1 and d_2, between the minutiae and the singular point are 2 and $\sqrt{13}$. Suppose also that a fingerprint shell is made using user key $d_0 = 1.5$. Then, $(\mathrm{DIS}_1, \mathrm{DIS}_2, \mathrm{DIS}_3)$, (h_1, h_2), and (θ_1, θ_2) are $(1.5, 3.5, 1.5 + \sqrt{13})$, $(\sqrt{10}, \sqrt{3 + 3\sqrt{13}})$, and $(0, 1.1279)$, respectively. Therefore, each point of the fingerprint shell to be stored is $(1.5, \sqrt{10})$ and $(-1.8585, 4.7533)$.

In the verification, the fingerprint shell template is created from a query fingerprint and it is compared with the enrolled fingerprint shell using the *Hausdorff* distance. The *Hausdorff* distance between two sets A and B is defined as $HD(A, B) = \max(h(A, B), h(B, A))$, where $h(A, B) = \max_{a \in A} \min_{b \in B} \|a - b\|$ and $\|\cdot\|$ is an Euclidean distance.

3. Analysis of Unlinkability of Fingerprint Shell

In this section, we show that the fingerprint shell does not satisfy unlinkability. We first show that we can extract a user's secret key from the fingerprint shell of the user, if the fingerprint shell is revealed. And we show that the fingerprint shell does not satisfy the condition of unlinkability either.

Fingerprint Shell Construction

Input : sorted distances $d_1, d_2, \ldots, d_n$ and user's key d_0

Output : a fingerprint shell $FS = \{(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)\}$

Let $(DIS_1, \ldots, DIS_{n+1}) = (d_0, d_1 + d_0, d_2 + d_0, \ldots, d_n + d_0)$ and $\theta_1 = 0$
for $i = 1$ to n **do**

$h_i = \sqrt{DIS_{i+1}^2 - DIS_i^2}$ /∗ h_i is the length of the height of the ith right triangle

if $i > 1$ **then**

$\theta_i = \theta_{i-1} + \arctan\left(h_{i-1}/DIS_{i-1}\right)$ /∗ Rotation angle for ith right triangle

end

$\begin{bmatrix} x_i \\ y_i \end{bmatrix} = \begin{bmatrix} \cos\theta_i & -\sin\theta_i \\ \sin\theta_i & \cos\theta_i \end{bmatrix} \times \begin{bmatrix} DIS_i \\ h_i \end{bmatrix}$ /∗ Rotation of the triangle

end

Figure 2: Fingerprint shell construction algorithm.

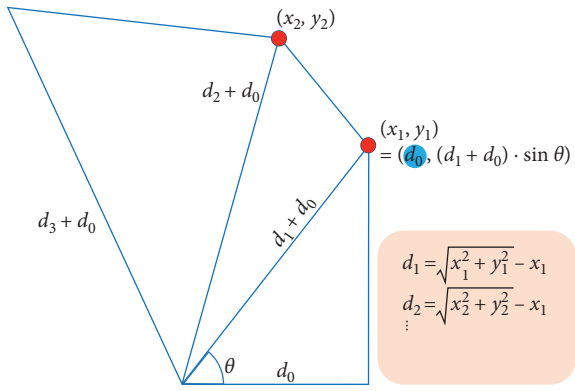

Figure 3: Example of fingerprint shell.

Extract d_i and d_0 from Fingerprint Shell

Input : Fingerprint Shell points $S = \{(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)\}$

Output : The secret key of the user and distances between minutiae and a singular point $(d_1, \ldots, d_n)$

Let $P = \begin{bmatrix} x_1 & x_2 & \cdots x_n \\ y_1 & y_2 & \cdots y_n \end{bmatrix}$ /∗ The Fingerprint Shell Points

$d_0 = P(1, 1) = x_1$ /∗ The secret key of the user

for $i = 1$ to n **do**

$h_i = \sqrt{P(1, i)^2 - P(2, i)^2}$ /∗ The length of the hypotenuse of the ith triangle

$d_i = h_i - d_0$ /∗ Original Distance d_i

End

Figure 4: Distance extraction algorithm.

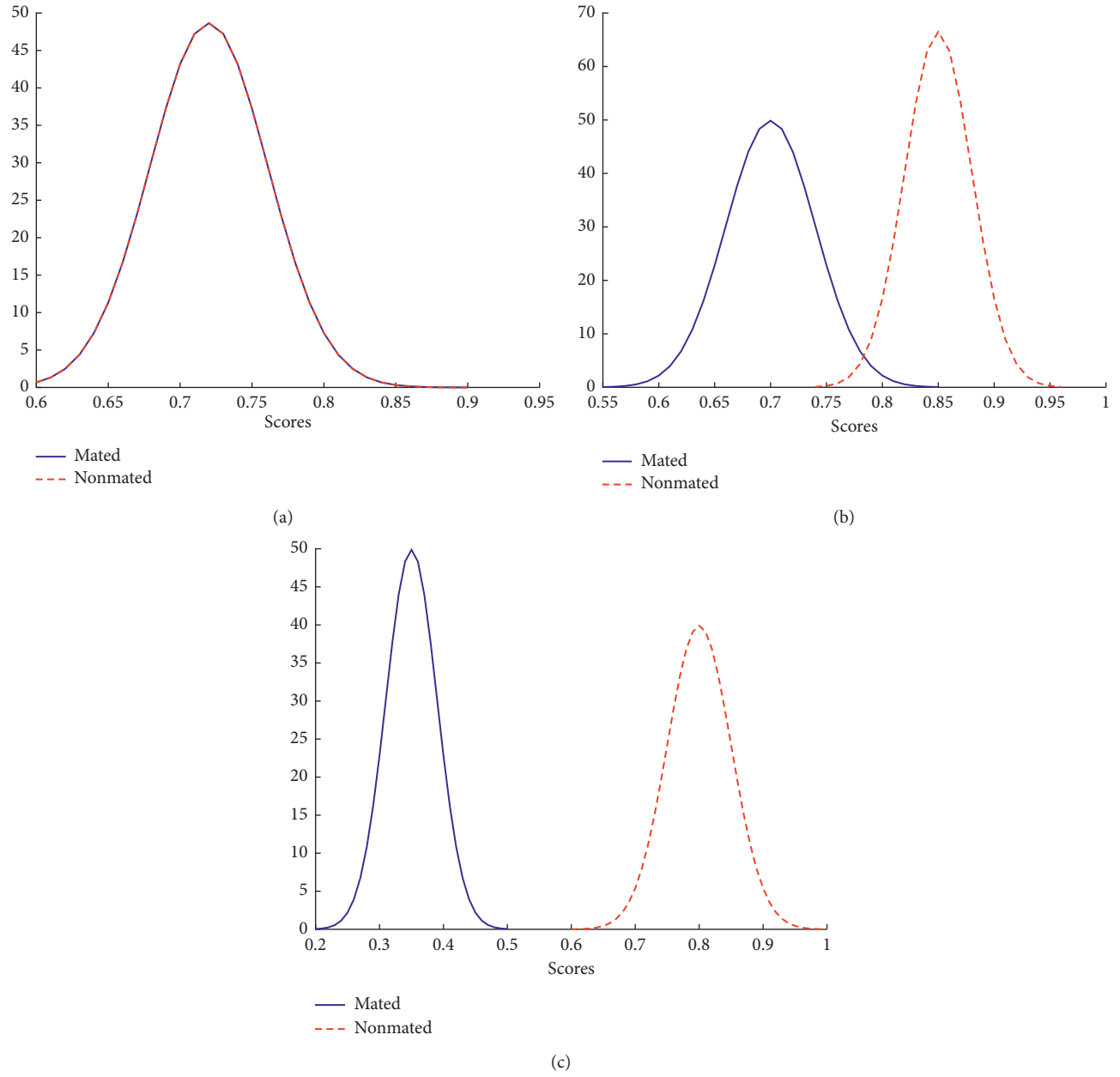

Figure 5: Sample distributions for different levels of linkability. (a) Fully unlinkable. (b) Semilinkable. (c) Fully linkable.

3.1. Extraction of User Key. In [9], the authors proposed a new template representation for fingerprint feature protection. Due to design problems, however, the user private key used to create the fingerprint shell is easily exposed. The fingerprint shell used $(d_i + d_0)$ to protect d_i, the features of user fingerprint. It is not difficult to reconstruct d_i using an exposed user private key d_0 because it uses simple addition operations. It can be done without any additional information besides the fingerprint shell. The fingerprint shell is stored on the server without any additional cryptographic operations because of the cancelable template property. Thus, if an attacker gets a fingerprint shell from the server, it causes key exposure and template linkable.

The first point (x_1, y_1) in Figure 3) in the fingerprint shell is the top vertex of the first triangle. In the first triangle, the length of the base is d_0 (as same as x_1 in Figure 3), the length of the hypotenuse is $d_1 + d_0$, and the length of the height is $\sqrt{(d_1 + d_0)^2 - d_0^2}$ (as same as y_1 in Figure 3). Therefore, the coordinates of the first point are $(x_1, y_1) = (d_0, \sqrt{(d_1 + d_0)^2 + d_0^2})$ (Figure 3). As a result, we can easily obtain the user key $d_0 = x_1$ from the first point of the fingerprint shell. Furthermore, since the distances between each point in the fingerprint shell and origin point are in the form of $d_0 + d_i$, we can reconstruct d_i from the given fingerprint shell by extracting d_0 as described above (Figure 4).

3.2. Linkability of the Fingerprint Shell. Unlinkability is defined by ISO/IEC 24745 : 2011 as "a property of two or more biometric references that cannot be linked to each other or to the subject(s) from which they were derived" [16].

In [17], the authors proposed a framework to evaluate linkability. This framework defines mated and nonmated samples as two types of score distributions. The mated sample distribution is a set of scores computed between two templates from the same user. The nonmated sample distribution is made using scores computed between two templates from two different users. As shown in Figure 5, the sample distributions can be used to distinguish three different levels of linkability: fully unlinkable, fully linkable, and semilinkable. Figure 5(a) shows that the mated sample distribution with different keys (cross-matching) is identical to the nonmated sample distribution. It means that similarity scores between templates from the same finger using different keys are indistinguishable from similarity scores between different fingers. This is referred to as fully unlinkable. Under a fully linkable scenario, the mated sample and nonmated sample distributions are completely separable (Figure 5(c)). Thus, given the two templates, we can distinguish templates whether they originated from the same finger or different fingers. Semilinkable means that they were linked only for a subset of the templates. In the overlapping part of the mate sample and nonmated sample distributions (Figure 5(b)), it is impossible to differentiate which templates are from the same or different fingers.

We measured the unlinkability of the fingerprint shell using the framework in [17]. The experiments were executed on four FVC2002 databases (DB1, DB2, DB3, and DB4) [18]. Each database contains 100 fingers with 8 impressions each. A linkage score calculated for two fingerprint shells, FS_1 and FS_2, is $HD(D_1', D_2')$, where $HD(\cdot)$ is the *Hausdorff* distance and D_1' and D_2' are the extracted distance sets from FS_1 and FS_2 using Figure 4, respectively. If the given fingerprint shell FS_1 and FS_2 are the mated samples, the *Hausdorff* distance is small. Otherwise, the *Hausdorff* distance is large.

For the linkability test, we generated 51 fingerprint shells from the first impression of each finger using different user keys. Then, one of them is selected as a reference and compared against the remaining fingerprint shells of the same finger (i.e., 5000 attempts). Figure 6 represents the sample distributions for each FVC2002 database. It can be seen that the mated and nonmated distributions are clearly separated in all of the databases. In other words, the fingerprint shell is fully linkable on these four FVC2002 databases.

3.3. Linkability of Enhanced Fingerprint Shell. Ali and Prakash proposed the enhanced fingerprint shell scheme in [14]. Their method is a two-step process of fingerprint shell construction and shell translation that uses two keys. The first step uses one of the key pairs to create a fingerprint shell that essentially replicates the original fingerprint shell construction. The next step is to add $(k_0 \times \sin k_0, k_0 \times \cos k_0)$, which is generated by the second key k_0 of the key pair, to all points in the created fingerprint shell.

For example, suppose that a fingerprint shell which is created in Section 2 is used to construct an enhanced fingerprint shell and a second user key k_0 used to shift the fingerprint shell is 1.2. For translation $(k_0 \times \sin k_0, k_0 \times \cos k_0) = (1.1184, 0.4348)$ is added to all points of the fingerprint shell. Then, each point of the enhanced fingerprint shell to be stored is $(1.5 + 1.1184, \sqrt{10} + 0.4348) = (2.6184, 3.5971)$ and $(-1.8585 + 1.1184, 3.7533 + 0.4348) = (-0.7401, 4.1881)$.

They wanted to enhance the security of the original fingerprint shell scheme with the additional key. However, it is not difficult to reconstruct the original fingerprint shell from a shell of the Ali and Prakash scheme [14]. The shell of Ali and Prakash's scheme consists of right angle triangles [14]. Therefore, we can calculate the origin of the shell by finding intersection of perpendicular lines to connecting lines of neighboring shell points (Figure 7). The lines can be expressed as follows:

$$l_i = a_i x + b_i, \tag{1}$$

$$l_i^{\perp} = -\frac{1}{a_i} x + k_i. \tag{2}$$

The l_i in (1) is an equation connecting P_i and P_{i+1}, and the $l_i^{\perp}$ in (2) is an equation perpendicular to l_i passing through P_i (Figure 7). The shifted origin is an intersection of the perpendicular lines $l_i^{\perp}$.

Even if we do not know the second key of the key pair, we can recover the original fingerprint shell with only one key if the origin of the shell from Ali and Prakash's scheme is moved to the coordinate origin [14]. The translated shell is exactly the same as the original fingerprint shell [9]. Therefore, Ali and Prakash's scheme in [14] also shows that it does not provide unlinkability in the same method as the previous section.

3.4. Linkability of 3D Secured Fingerprint Shell. Ali and Prakash also proposed a new 3D fingerprint shell scheme based on the fingerprint shell [15]. They used an angle in addition to the distance between singular and minutia. It is used to generate a new secured distance, l_i. The set of l_i and user key l_0 are used to generate a new one. The generated shell is rotated in the xy plane and xz plane using the user key s_0 and l_0, respectively, and translated using the user key k_0 (see Figure 8). However, this algorithm is also vulnerable.

Translate the transformed 3D curve so that the first point of the curve is the origin and project each point on the curve to the xy plane such that the distance to the origin is maintained. Then, using the origin calculation of the previous chapter, we can get the shell before the translation, as shown in Figure 9(b). As mentioned earlier, we can easily recover the l_i from the shell. The l_i is as follows:

$$l_i = \sqrt{d_i^2 + s_0^2 + 2\left(d_i \times s_0 \times \cos\left(\theta_i\right)\right)}. \tag{3}$$

Suppose that the attacker has three different databases, DB_A, DB_B, and DB_C. Let l_i extracted from the template of each database be $l_{i,A}$, $l_{i,B}$, and $l_{i,C}$. If $l_{i,A}$, $l_{i,B}$, and $l_{i,C}$ are made

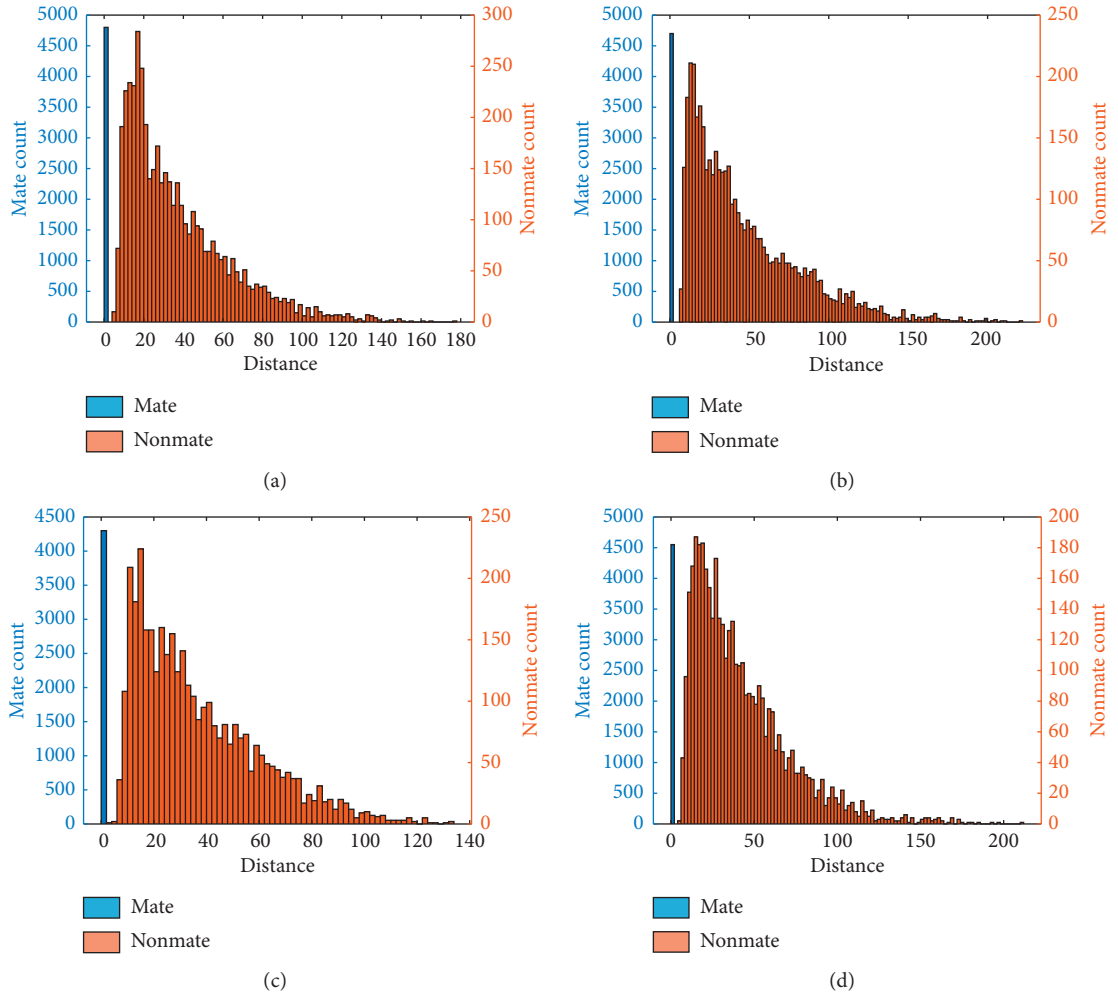

Figure 6: Sample distributions of the fingerprint shell on (a) FVC2002 DB1. (b) FVC2002 DB2. (c) FVC2002 DB3. (d) FVC2002 DB4.

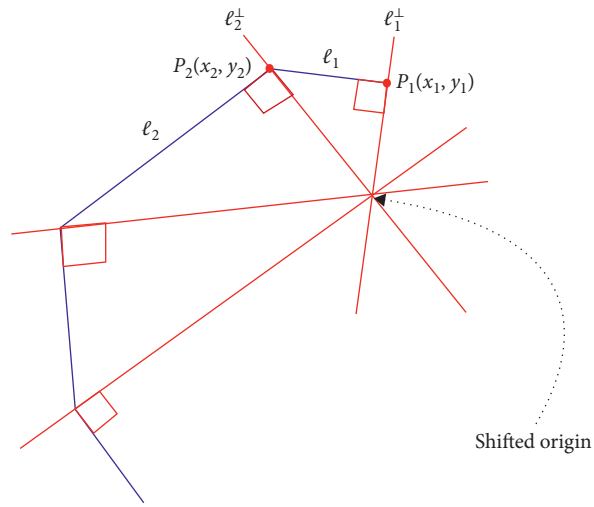

Figure 7: Shell origin calculation.

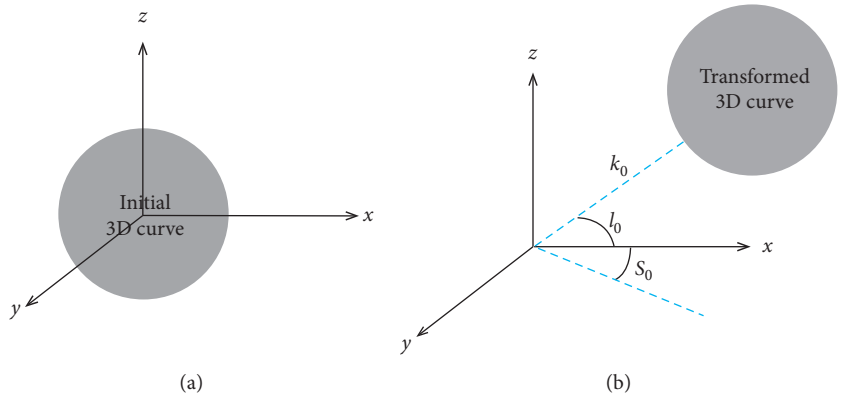

Figure 8: The 3D transformation of [11]. (a) Initial spiral curve. (b) Spiral curve translation using user key s_0, l_0, and k_0.

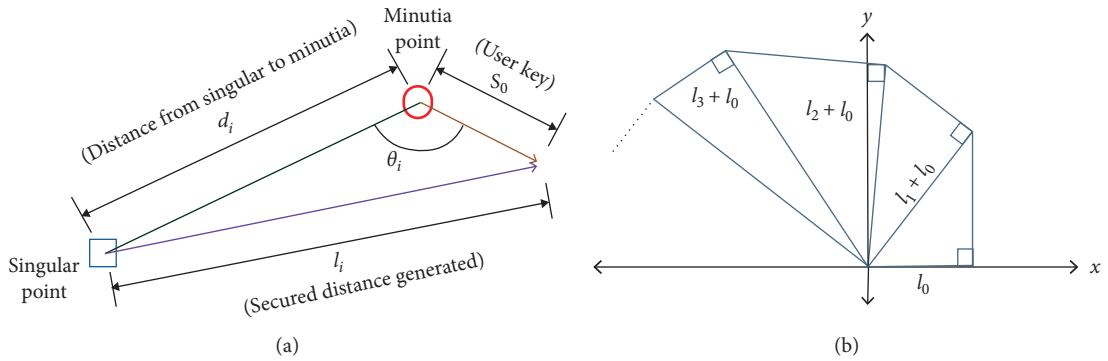

Figure 9: Basic components of [11]. (a) Computation of secured distance. (b) Computation of spiral curve.

Table 1: The number of images used for experiments.

	FVC2002 DB1	FVC2002 DB2	FVC2002 DB3	FVC2004 DB2
[11]	799	797	757	750

from the same d_i and θ_i, then two equations can be obtained as follows:

$$\begin{aligned} l_{i,A}^2 - l_{i,B}^2 &= d_i^2 + s_{0,A}^2 + 2\left(d_i \times s_{0,A} \times \cos\left(\theta_i\right)\right) \\ &\quad - d_i^2 - s_{0,B}^2 - 2\left(d_i \times s_{0,B} \times \cos\left(\theta_i\right)\right), \\ l_{i,A}^2 - l_{i,C}^2 &= d_i^2 + s_{0,A}^2 + 2\left(d_i \times s_{0,A} \times \cos\left(\theta_i\right)\right) \\ &\quad - d_i^2 - s_{0,C}^2 - 2\left(d_i \times s_{0,C} \times \cos\left(\theta_i\right)\right). \end{aligned} \tag{4}$$

We know the $s_{0,A}$, $s_{0,B}$, and $s_{0,C}$ through the inverse operation of the rotation in calculating l_i from the new 3D shell. Equation (4) can be transformed as follows:

$$\begin{aligned} \frac{\left(l_{i,A}^2 - l_{i,B}^2\right) - \left(s_{0,A}^2 - s_{0,B}^2\right)}{2\left(s_{0,A} - s_{0,B}\right)} &= d_i \times \cos\left(\theta_i\right), \\ \frac{\left(l_{i,A}^2 - l_{i,C}^2\right) - \left(s_{0,A}^2 - s_{0,C}^2\right)}{2\left(s_{0,A} - s_{0,C}\right)} &= d_i \times \cos\left(\theta_i\right). \end{aligned} \tag{5}$$

The left side of equation (5) consists of the known values. So, the values obtained from the template of each database are calculated by using the left side of equation (5) and compared to determine whether the user is the same user.

4. Conclusions

Moujahdi et al. proposed a new noninvertible fingerprint transformation method called the fingerprint shell in [9] and Ali and Prakash proposed an enhanced fingerprint shell scheme in [14] and a new 3D fingerprint shell scheme in [15]. All the schemes present low computational cost and high levels of accuracy and are less sensitive to rotating fingerprint images.

However, the accuracy of these three schemes depends on a technique of singular point extraction. The singular point extraction is challenged with low quality images [19]. Table 1 shows the number of images used for experiments in [15]. For FVC2002 DB3 and FVC2004 DB2, only about 750 of 800 were used. The authors in [15] observed that the singular point extraction had filed for about 50 images due to the low image quality and excluded those low-quality images in the experiments. Therefore, the fingerprint shell schemes might not be adequate for the low-quality images. Besides, we showed that all the fingerprint shell schemes of [9, 14, 15] do not provide unlinkability. That is, we have shown that we can construct a distinguisher which can tell whether the two

fingerprint shells are from the same user or different users with a high degree of success.

These problems come from using invertible operations such as translation, addition, and linear geometric transformation in making cancelable templates. To make secure and unlinkable templates, the cancelable template generation algorithms must use the nonlinear and noninvertible operations such as the many-to-one mapping and functional transformation in [20].

As a future work, it would be interesting to construct a new fingerprint shell scheme providing unlinkability.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

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

Acknowledgments

This work was partly 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) and the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2019R1F1A1060637).

References

[1] N. K. Ratha, "Privacy protection in high security biometrics applications," *Ethics and Policy of Biometrics*, Springer, Berlin, Germany, pp. 62–69, 2010.

[2] A. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP Journal on Advances in Signal Processing*, vol. 2008, no. 1, Article ID 579416, 2008.

[3] J. Zuo, N. K. Ratha, and J. H. Connell, "Cancelable iris biometric," in *Proceedings of the IEEE 19th International Conference on Pattern Recognition*, pp. 1–4, Tampa, FL, USA, December 2008.

[4] V. M. Patel, R. Chellappa, and M. Tistarelli, "Sparse representations and random projections for robust and cancelable biometrics," in *Proceedings of the 2010 11th International Conference on Control Automation Robotics & Vision*, pp. 1–6, Singapore, December 2010.

[5] 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.

[6] 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.

[7] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*, Springer, Berlin, Germany, 2003.

[8] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP Journal on Information Security*, vol. 2011, no. 1, 2011.

[9] C. Moujahdi, G. Bebis, S. Ghouzali, and M. Rziza, "Fingerprint shell: secure representation of fingerprint template," *Pattern Recognition Letters*, vol. 45, pp. 189–196, 2014.

[10] K.-Y. Chee, Z. Jin, D. Cai et al., "Cancellable speech template via random binary orthogonal matrices projection hashing," *Pattern Recognition*, vol. 76, pp. 273–287, 2018.

[11] S.-C. Wu, P.-T. Chen, A. L. Swindlehurst, and P.-L. Hung, "Cancelable biometric recognition with ECGs: subspace-based approaches," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 5, pp. 1323–1336, 2019.

[12] V. M. Patel, N. K. Ratha, and R. Chellappa, "Cancelable Biometrics: A review," *IEEE Signal Processing Magazine*, vol. 32, no. 5, pp. 54–65, 2015.

[13] X. Dong, Z. Jin, and A. T. B. Jin, "A genetic algorithm enabled similarity-based attack on cancellable biometrics," in *Proceedings of the IEEE 9th International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, pp. 1–9, Los Angeles, CA, USA, October 2019.

[14] S. S. Ali and S. Prakash, "Enhaced fingerprint shell," in *Proceedings of the IEEE International Conference on Signal Processing and Integrated Networks (SPIN)*, pp. 801–805, Noida, India, February 2015.

[15] S. S. Ali and S. Prakash, "3-Dimensional secured fingerprint shell," *Pattern Recognition Letters*, vol. 126, pp. 68–77, 2019.

[16] Information technology-Security techniques-Biometric information protection, ISO/IEC 24745:2011, ISO/IEC JTC1 SC27 Security techniques, 2011.

[17] M. Gomez-Barrero, J. Galbally, C. Rathgeb, and C. Busch, "General framework to evaluate unlinkability in biometric template protection systems," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 6, pp. 1406–1420, 2018.

[18] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, "FVC2002: Second fingerprint verification competition," in *Proceedings of the Object Recognition Supported by user Interaction for Service Robots*, vol. 3, pp. 811–814, Quebec City, Quebec, Canada, August 2002.

[19] Y. Wang, J. Hu, and D. Phillips, "A fingerprint orientation model based on 2D Fourier expansion (FOMFE) and its application to singular-point detection and fingerprint indexing," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, no. 4, pp. 573–585, 2007.

[20] N. Ratha, J. Connell, R. M. Bolle, and S. Chikkerur, "Cancelable biometrics: a case study in fingerprints," in *Proceedings of the 18th International Conference on Pattern Recognition*, vol. 4, pp. 370–373, Hong Kong, China, August 2006.