Dictionary Attack on Functional Transform-Based Cancelable Fingerprint Templates

Sang Wook Shin, Mun-Kyu Lee, Daesung Moon, and Kiyoung Moon

ABSTRACT—Recently, Ratha and others proposed a cancelable biometrics scheme which transforms an original fingerprint template into a new one using a noninvertible transformation. However, we show that the original template is recovered by a dictionary attack if two transformed templates originating from it are revealed. In our attack, we simulate the transformation and construct a set of possible pre-images for each transformed template. Then, we find the correct pre-image by computing the intersection of these sets. We present an algorithm implementing this idea as well as successful experimental results.

Keywords—Cancelable fingerprint templates, functional transform, surface folding transform.

I. Introduction

Biometric verification schemes raise security concerns because biometric data is permanently associated with its owner and therefore cannot be replaced even if it is compromised. One of the most promising solutions to this problem is cancelable biometrics [2], where a system does not store the original biometric data; rather, it stores only the version transformed by a noninvertible transform [3]. Then, verification is done on this transformed data without any need to recover the original data, keeping the original data safe even if the system is compromised.

Since Ratha and others pioneered the concept of cancelable biometrics [2], various schemes have been introduced. A more detailed review of cancelable biometrics may be found in [3] and [4]. The most well-known scheme is Ratha's surface folding scheme for cancelable fingerprint templates [3].

It is claimed in [3] that the original fingerprint template is secure even if a transform and a transformed template using this transform are compromised. In this letter, however, we show that this claim does not always hold. The original fingerprint template can be recovered by a dictionary attack if an attacker obtains two transformed templates originating from an identical fingerprint template and their transformation parameters.

II. Ratha's Surface Folding Transform

Ratha's one-way transformation moves minutia positions using two-dimensional Gaussian functions defined over the feature domain. In this scheme, each user is given a unique key which specifies the centers and shapes of Gaussian kernels. These Gaussian kernels overlap to form two surfaces, $F(x, y)$ and $G(x, y)$, as shown in Fig. 1. Then, they are used to decide the direction and amount of shift for each feature point at (x, y).

To be precise, a Gaussian mixture $F(z)$ for a position vector $z = [x, y]^{\mathrm{T}}$ is defined by

$$F(z)=\sum_i \frac{\pi_i}{|2\pi\Lambda_i|}\exp\left\{-\frac{1}{2}(z-\mu_i)^{\mathrm{T}}\Lambda_i^{-1}(z-\mu_i)\right\}, \quad (1)$$

where the weight π_i, covariance Λ_i, and center μ_i for each Gaussian kernel are parameters given by the key. We also define the phase of F for z as

$$\Phi_F(z)=\frac{1}{2}\arg\{\nabla F(z)\}+\Phi_{\text{rand}}, \quad (2)$$

Manuscript received Apr. 1, 2009; revised July 20, 2009; accepted Aug. 4, 2009.

The preliminary version of this paper was presented at CISC-W 2008 [1].

This work was supported by the IT R&D Program of MKE/IITA [2007-s-020 Development of Privacy Enhanced Biometric System], Rep. of Korea.

Sang Wook Shin (phone: +82 32 873 7456, email: nextion1981@inhaian.net) and Mun-Kyu Lee (email: mklee@inha.ac.kr) are with the School of Computer and Information Engineering, Inha University, Incheon, Rep. of Korea.

Daesung Moon (phone: +82 42 860 1083, email: daesung@etri.re.kr) and Kiyoung Moon (email: kymoon@etri.re.kr) are with the S/W & Content Research Laboratory, ETRI, Daejeon, Rep. of Korea.

doi:10.4218/etrij.09.0209.0137

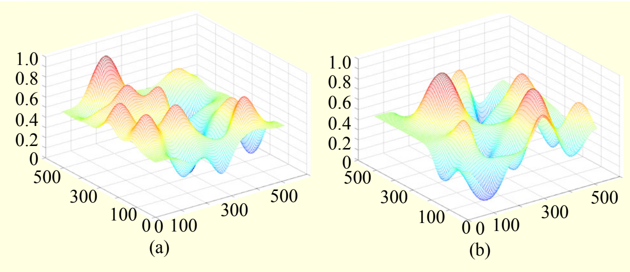

Fig. 1. Examples of Gaussian mixtures: (a) surface F and (b) surface G.

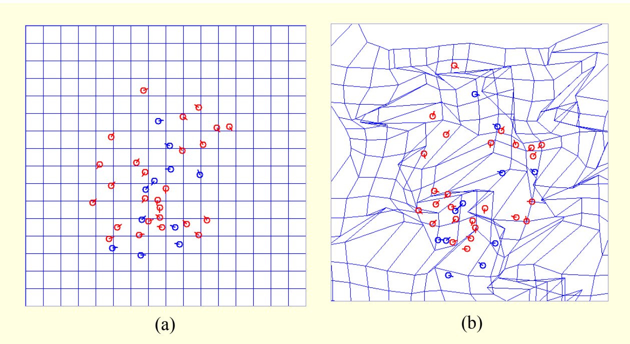

Fig. 2. Transformation of a fingerprint template: (a) original template and (b) transformed template.

where Φ_{rand} is a random phase offset, which is also given by the key. Another Gaussian mixture $G(z)$ and its phase $\Phi_G(z)$ are defined in a similar way.

Then, a transformation $(x, y, \Theta) \rightarrow (X', Y', \Theta')$ is given by

$$X' = x + KG(x,y) + K\cos\left(\Phi_F(x,y)\right), \quad (3)$$

$$Y' = y + KG(x,y) + K\sin\left(\Phi_F(x,y)\right), \quad (4)$$

$$\Theta' = \left(\Theta + \Phi_G(x,y) + \Phi_{\text{rand}}\right) \bmod 2\pi, \quad (5)$$

where K is a predefined constant.

Figure 1 shows examples of F and G produced by placing 24 Gaussian distributions in the 512×512 image space according to the key, where each distribution has a standard deviation of 50 pixels and a peak magnitude of either +1 or -1 as in [3]. The two mixtures are scaled so that the highest and lowest peaks have values of 1 and 0, respectively. Figure 2 shows an example of the transformation using these Gaussian mixtures.

Ratha and others [3] showed that the original fingerprint and its transformed version are difficult to correlate and claimed that inverting a transformed template into its original version is much harder than a naïve brute force attack.

III. Vulnerability of Surface Folding Transform

According to [3], the transform depends only on the key. That is, all the parameters for the surfaces F and G as well as the phase offset Φ_{rand} are specified by the key. If the transformation (the key) is revealed to an attacker, he or she can simulate the transform and build a *dictionary* that maps every possible point on the image space to its transformed one. The dictionary consists of pairs $((x, y), H(x, y))$ for all possible points (x, y), where H is the transform. For example, for a 512×512 image space, this dictionary contains 512^2=262,144 pairs. The elements in the dictionary are sorted according to values of $H(x, y)$.

Note that the attacker is also given a transformed template $T=\{m_1,\cdots, m_n\}$, where each m_i represents a minutia point. Thus, the attacker can construct n sets C_1 through C_n using the dictionary so that each C_i contains all possible pre-images of m_i. Then, the original template can be viewed either as an element in the Cartesian product $C_1\times\cdots\times C_n$ or as a subset of union $C_1\cup\cdots\cup C_n$. For efficiency, we adopt the latter interpretation. Note that we have too many candidates at this point in both of the interpretations. However, if the attacker obtains two or more pairs of (key, transformed template) originating from the same template by attacking a newly enrolled template of the same user one more time or by attacking multiple databases at the same time, the number of candidates can be substantially reduced by computing intersections of those sets.

Figures 3 and 4 present a typical example that we discovered in our experiment. Figure 3 shows two templates transformed from the same original template using two distinct keys, K and

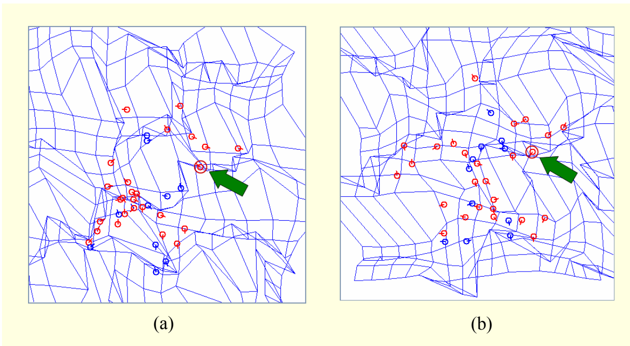

Fig. 3. Two transformed versions of the same template using two distinct keys.

Minutiae	x	y	θ
m_1	181	153	184
m_2	280	146	178
m_3	317	260	221
⋮			
m_{37}	235	455	252

(a)

Minutiae	x	y	θ
m'_1	251	95	232
m'_2	359	233	125
m'_3	324	180	5
⋮			
m'_{37}	235	401	346

(b)

Fig. 4. Transformed minutia points shown in Fig. 3(a) and (b).

K'. Figure 4 provides two lists of minutia points corresponding to the templates shown in Fig. 3(a) and (b), respectively. Note that minutia m_1 through m_{37} and m'_1 through m'_{37} are randomly enumerated; therefore, their order should not be interpreted as m_i and m'_i originating from the same point in the original template. We do not need any information for which m'_i corresponds to a specific m_j. For clarity, we explain the case in which m_3 and m'_2 come from the same original point. The highlighted minutia point in Fig. 3(a) represents $m_3=(317, 260)$. Using the dictionary built from K, we obtain C_3, the set of pre-images for m_3, which contains two distinct possible sources (324, 217) and (362, 261). All the other sets C_i are obtained in a similar way. Another key, K', helps us to construct another dictionary which tells us that the set C'_2 of pre-images for $m'_2=(359, 233)$ contains (324, 217) and (358, 279). Then, the point (324, 217) is one of the original minutia points with high probability.

Algorithm 1 presents the procedure which generalizes this idea. We assume that we have two pairs, (K, T) and (K', T'), where T and T' are templates transformed from an identical original template using K and K', respectively. Note that we do not need any other additional information for our attack.

Algorithm 1: Attack to the surface folding transform.

Input: (K, T) and (K', T'), where T = $\{m_1,\cdots,m_{N1}\}$, T' = $\{m'_1,\cdots,m'_{N2}\}$
Output: R = $\{r_1, r_2,\cdots,r_{N3}\}$
1. Construct dictionary D using K.
2. Construct dictionary D' using K'.
3. Compute $C_1,\cdots,C_{N1}$ and $U = C_1 \cup\cdots\cup C_{N1}$ using D and T.
4. Compute $C'_1,\cdots,C'_{N2}$ and $U' = C'_1 \cup\cdots\cup C'_{N2}$ using D' and T'.
5. Return $R = U \cap U'$.

IV. Experimental Results

To verify the feasibility of our attack, we performed an experiment using 16 real fingerprints in FVC2002 DB1 [5]. They have 20 to 37 minutia points over a 388×374 image space. Let $O_1,\cdots, O_{16}$ be these fingerprints. We generated 100 random keys, $K_1,\cdots, K_{100}$, and produced 1,600 transformed templates $T_{i,j}=H_{Kj}(O_i)$ for $i = 1,\cdots, 16$ and $j = 1,\cdots, 100$, where H_{Kj} is the transformation using key K_j which maps a 512×512-pixel image into another 512×512-pixel image.

We first tried the dictionary attack using a single transformed template. Given a single pair (K_j, $T_{i,j}$), we produced a result $U_{i,j}$ by performing only steps 1 and 3 of algorithm 1. Our experiment shows that, in all of the 1,600 tests, all the minutia points in the original template O_i are also included in $U_{i,j}$. However, $U_{i,j}$ also contains additional points. Table 1 shows the numbers of these additional points. In most cases, $U_{i,j}$ contains too many additional points compared to O_i. In a few extreme cases, however, the difference is very small, and the attack with only a single transformed template may be successful.

Table 1. Distribution of the differences between O_i and $U_{i,j}$.

$\lvert U_{i,j} - O_i\rvert$	<10	[10, 20)	[20, 40)	[40,60)	[60,80)	≥80	Total
Counts (Portion)	7 (0.4%)	94 (5.9%)	670 (41.9%)	571 (35.7%)	195 (12.2%)	63 (3.9%)	1,600 (100%)

Table 2. Distribution of the differences between O_i and $R_{i,j,k}$.

$\lvert R_{i,j,k} - O_i\rvert$	0	1	≥2	Total
Counts (Portion)	67,489 (85.2%)	9,908 (12.5%)	1,803 (2.3%)	79,200 (100%)

The next experiment is for the case in which the attacker obtains two transformed templates. For each $i = 1,\cdots, 16$, we tested all the 4,950 combinations of $T_{i,j}$ and $T_{i,k}$ ($j, k = 1,\cdots, 100$, $j\neq k$, $j<k$), producing 4,950×16=79,200 test results. The data shown in Table 2 implies that our attack is very successful. The second column indicates that, with a probability of 85.2%, there is no difference between O_i and $R_{i,j,k}$ (output of algorithm 1). According to our timing estimation, dictionary construction (lines 1 and 2) and template recovery (lines 3 to 5) require averages of 464.16 s and 54.31 ms, respectively, over a PC with a Pentium IV 3.0 GHz CPU and 2 GB of RAM.

V. Conclusion

We demonstrated that the surface folding transform in [3] may not be secure if two transformed templates originating from the same fingerprint are compromised. This implies that the transform in [3] is not perfectly noninvertible. Therefore, a new scheme is needed which can effectively hide the original biometric data even when multiple transformed templates are revealed.

References

[1] S.W. Shin et al., "Analysis on Functional Transform-Based Cancelable Fingerprints," *Proc. Conf. Information Security and Cryptology*, Dec. 2008, pp. 219-222 (in Korean).
[2] N.K. Ratha, J.H. Connell, and R.M. Bolle, "Enhancing Security and Privacy in Biometrics-Based Authentication System," *IBM Syst. J.*, vol. 40, no. 3, 2001, pp. 614-634.
[3] N.K. Ratha et al., "Generating Cancelable Fingerprint Templates," *IEEE Trans. Pattern Anal. Mach. Intell.* vol. 29, no. 4, Apr. 2007, pp. 561-572.
[4] C. Lee et al., "Alignment-Free Cancelable Fingerprint Templates Based on Local Minutiae Information," *IEEE Trans. Syst., Man, Cybern. B, Cybern.*, vol. 37, no. 4, Aug. 2007, pp. 980-992.
[5] FVC 2002 Databases, http://bias.csr.unibo.it/fvc2002/download.asp.