Generating Provably Secure Cancelable Fingerprint Templates Based on Correlation-invariant Random Filtering

Kenta Takahashi and Shinji Hirata
Hitachi, Ltd., Systems Development Laboratory, Tokyo, Japan

Abstract—Biometric authentication has attracted attention because of its high security and convenience. However, biometric feature such as fingerprint can not be revoked like passwords. Thus once the biometric data of a user stored in the system has been compromised, it can not be used for authentication securely for his/her whole life long. To address this issue, an authentication scheme called cancelable biometrics has been studied. However, there remains a major challenge to achieve both strong security and practical accuracy. In this paper, we propose new methods for generating cancelable fingerprint templates with provable security based on the well-known chip matching algorithm for fingerprint verification and correlation-invariant random filtering for transforming templates. Experimental evaluation shows that our methods can be applied to fingerprint authentication without much loss in accuracy compared with the conventional chip matching algorithm.

I. INTRODUCTION

Biometric verification technology, which automatically identifies a person based on his/her physical or behavioral features, has been used for user authentication for physical access control or computer login, and is expected to be applied to remote user authentication over networks. A typical remote biometric authentication system consists of an authentication server with database and client terminals with biometric sensors. The server keeps biometric feature data, which are called templates, in the database.

There are some problems here. The first is a security concern: because biometric features such as fingerprint patterns are unchangeable, they can not be revoked even if the templates or feature data are leaked. The second is a privacy concern: biometrics are strongly linked to a person’s identity, so some users have aversion to disclose their biometric data to the server over the network.

Conventional remote biometric authentication systems have been dealt with these problems by encrypting templates in the database and feature data sent to the sever. However, these encrypted data have to be decrypted on the server to perform pattern matching at the time of authentication. Thus a skilled attacker who aims at this timing, or a malicious administrator of the server can acquire the original biometric feature or templates.

To address these issues, some biometric authentication schemes such as “cancelable biometrics” [12] and “biometric cryptosystems” [14] have been studied for about a decade. However, there remains a major challenge, namely, to achieve both strong security and practical accuracy.

Biometric cryptosystems, such as ones using fuzzy vault (e.g. [9]), take an approach of extracting stable binary representation from “analogue” biometrics data (biometric key generation), and using it as a private key or a password. However, generating user-specific key from biometric data with practical accuracy (i.e. low error rates of generating wrong key from a genuine user, and of generating correct key from an impostor user) is a major challenge in this approach.

On the other hand, in cancelable biometrics, biometric data is transformed in the feature (or signal) domain, and matched in the transformed domain directly, without restoring the original feature. Some methods of cancelable biometrics such as [2], [13], [11], [4] have potential to take advantage of conventional matching algorithms with practical accuracy. However, the security analyses of most methods of cancelable biometrics do not seem so rigorous as those of the conventional encryption algorithms. It is a challenge to construct transformations for cancelable biometrics with provable security.

In this paper, we propose new methods of generating cancelable fingerprint templates for the chip matching algorithm [8] based on the correlation-invariant random filtering [5]. Our methods have provable security in the meaning that the cancelable templates does not leak any information about original fingerprint.

II. CANCELABLE BIOMETRICS AND RELATED WORKS

A typical model of server/client type biometric authentication system with cancelable biometrics is shown in Fig.1.

![System model of cancelable biometrics](image)

Fig. 1. System model of cancelable biometrics

Biometric feature data $a$ for enrollment and $b$ for authentication are transformed via a function $F_P$ determined by a parameter $P$, and sent to the server. The server stores $F_P(a)$ as a template, and matches it to $F_P(b)$ at the time of authentication. $P$ corresponds to an encryption key and kept in the client or some token of the user. Note that $P$
should not be stored with $F_P(a)$, because in that case, the both data could leak out at once. An attacker who obtained both $F_P(a)$ and $P$ is able to recover the original feature $a$, if $F_P(\cdot)$ is injective (one-to-one) function, as in many cases of cancelable biometrics. Even if $F_P(\cdot)$ is not an injective (many to one) function as proposed in [11], it is shown to be possible to recover $a$ from $F_P(a)$ and $P$ [10].

Desirable properties of a transform function are as follows.

(i) **Accuracy Preservation:** In general, an error would occur in computing the score in the transformed domain, and the accuracy may degrade compared to the original version. It is important that the degree of degradation of accuracy due to applying transformation is small.

(ii) **Recovery Resistance:** It is required to be sufficiently hard to recover or estimate the original biometric feature $a$ (or $a'$ sufficiently similar to $a$) from $F_P(a)$ without knowing $P$, and from $P$ without knowing $F_P(a)$. Attacks using a set of multiple data of different version of transform ($\{F_{P_1(a)}, F_{P_2(a)}, \cdots \}$, or $\{P_1, P_2, \cdots \}$) should also be considered. Ideally, it is desired that no information about $a$ is leaked from $F_P(a)$ or $P$.

Some transformation methods have been proposed for several kinds of biometrics, such as iris [2], face [13], [4] and finger vein [5].

As for fingerprint, Ratha, et. al. [11] proposed three transforms: Cartesian, polar, and functional transformation. The first two methods have a drawback of the **boundary problem**, i.e. if a original minutiae point crosses a boundary of sectors dividing the feature space due to minor deviation of image alignment or distortion of a fingerprint, then the transformed version of the minutiae point is located far from the appropriate position. The third method deals with this issue by some locally smooth functions to distort the feature space. Lee, et. al. [6] also proposed a locally smooth function for cancelable fingerprint template which does not need alignment for matching process. However, the security analysis of above methods seems insufficient. For example, an attacker might be able to narrow down the candidates of original minutia patterns based on the constrains of continuity of minutiae orientation and local smoothness of the transform function.

Chikkerur, et. al. [3] proposed a provably secure method for cancelable fingerprint templates. Their method extracts a local image (called a patch) around each minutiae, and transforms it by a projection matrix which does not change the dot product measure of two patches. However, the experimental accuracy is poor (FAR:1%, FRR:20%). Considerable reasons are as follows. (i) The matching measure of patches does not allow extraction error of minutiae locations, i.e. if a detected minutiae location is apart from the true position by only several pixels, the extracted patch image would not be matched. (ii) The final score is calculated according to the minimum total distance among all combinations of patches, thus an impostor’s fingerprint whose patch set is similar to the genuine one, for a certain permutation, can easily cause a false acceptance, even if the minutia locations are totally different.

### III. Preliminary

#### A. Correlation Invariant Random Filtering

The correlation invariant random filtering or CIRF, which we proposed in [5], is an elemental algorithm of cancelable biometrics with provable security for correlation-based matching. The following is a brief description of the CIRF.

We assume that the biometric feature is represented as image data (i.e. two-dimensional array of brightness values), and the value of each pixel is an integer. Furthermore, we assume the similarity score of two images $a(x,y), b(x,y)$ can be calculated from the cross-correlation function $a*b$, which can be expressed in the following convolution formula,

$$(a*b)(u,v) = \sum_{x,y} a(x,y)b(u-x,v-y),$$

where $b$ denotes the flipped image of $b$, i.e. $b(x,y) = b(-x,-y)$, and $a*b$ denotes the convolution of $a$ and $b$.

To establish cancelable biometrics, it is required to calculate $a*b$ without knowing $a$ or $b$.

Here, we introduce the two-dimensional **number theoretic transform (NTT)**, a kind of discrete Fourier transform (DFT) defined over Galois field $\mathbb{Z}_p$ ($p$ is a prime number),

$$A(u,v) = \sum_{x=0}^{w-1} \sum_{y=0}^{h-1} \alpha^{ux} \beta^{vy} a(x,y) \mod p,$$

where $w, h$ are the width and the height of the image respectively, and $\alpha, \beta$ are the elements of $\mathbb{Z}_p$ whose orders are $w, h$ respectively. The NTT is known to have a cyclic convolution property or CCP [1]. We make use of this property to establish cancelable biometrics as follows.

Firstly, we perform two-dimensional NTT to $a(x,y), b(x,y)$ and get $A(X,Y), B(X,Y)$, where $(X,Y)$ is the coordinates in the NTT domain. Secondly, transform $A, B$ to $T, U$ by using a random filter $R(X,Y)$ whose pixels are non-zero random value of $\mathbb{Z}_p$ as follows,

$$T(X,Y) = A(X,Y)R(X,Y)$$

$$U(X,Y) = B(X,Y)/R(X,Y).$$

$T$ plays a role as a cancelable template generated in enrollment stage, and $U$ as a transformed feature in authentication stage. The random filter $R$ corresponds to a parameter. We can calculate $a*b$ from $T$ and $U$ as follows,

$$NTT^{-1}(TU) = NTT^{-1}(AB) = a*b.$$  

Fig.2 describes the outline of the CIRF.

Note that all operations in the above calculations are carried out over the finite field $\mathbb{Z}_p$. In this case, for any non-zero $\alpha \in \mathbb{Z}_p$, the set $\{\alpha, 2\alpha, \cdots, (p-1)\alpha\}$ is equal to the set $\{1, 2, \cdots, p-1\}$ as a whole. Thus when $R(X,Y)$ is uniformly random over $\mathbb{Z}_p^*$, and $A(X,Y)R(X,Y)$ is also uniformly random over $\mathbb{Z}_p^*$ for any $A(X,Y) \in \mathbb{Z}_p^*$. This is the same for the case of $R(X,Y)/R(X,Y)$. Thus the transformed image is indistinguishable from a random sequence. This property is called **perfect secrecy**. Refer to [5] for details of the security proof of the CIRF.
Finally, the similarity score is calculated as the number of matched chips.

\[ a \hat{\otimes} b \xrightarrow{\text{Convolution}} a \ast \hat{b} \]

\[
\begin{array}{c|c|c}
NTT & NTT^{-1} & NTT^{-1} \\
\hline
A, B & AB & \text{Randomization} \\
\text{Multiplication} & TU & \text{non-invertible without } R
\end{array}
\]

Fig. 2. Outline of the CIRF

Actually, the CIRF can be implemented with normal DFT instead of NTT. However, the perfect secrecy is only derived from NTT. Besides, data size of the templates is reduced by NTT, because each element can be represented as an integer of \([\log_2(p)]\) bits (= 9 bits, in our implementation), whereas in the case of DFT, each element is a complex number represented as a pair of floating-point numbers.

B. Chip Matching Algorithm

The chip matching [8] is a well-known algorithm for fingerprint verification. Fig.3 shows the outline of the algorithm.

A captured fingerprint image is preprocessed to a binary (white and black) image of \(W \times W\) pixels, and the core is detected for fingerprint registration. We implemented the pre-process including image enhancement using the directional Gabor filter, threshold binarization and shrinking. The focal point method was used to detect the core as the point where pairs of lines normal to the ridges intersect. Refer to [7] for details of the above processes.

Then, in the enrollment stage, minutiae are extracted. The coordinate of each minutia is represented as \((x_i, y_i)\) \((i = 1, 2, \cdots, N)\) where \(N\) is the number of extracted minutiae and the origin \((0, 0)\) is the core point. Next, a chip image \(a_i\) of size \(w_C \times w_C\) centered at each minutiae point \((x_i, y_i)\) is extracted from the binary image. The set of minutiae coordinates and chip images \(T = \{((x_i, y_i), a_i) \mid i = 1, 2, \cdots, N\}\) is enrolled as a template of the fingerprint.

In the authentication stage, for each minutiae representation \(((x_i, y_i), a_i)\) \(\in T\), find the local area of size \(w_C \times w_C\) centered at \((x_i + u, y_i + v)\) \((u, v = 0, \pm 1, \pm 2, \cdots)\) most similar to the chip image \(a_i\), from the search area of size \(w_S \times w_S\) \((w_S > w_C)\) centered at \((x_i, y_i)\) in the binary image. Here, the origin \((0, 0)\) is defined as the core point in the binary image for authentication. Note that there is no need for minutiae extraction or minutiae alignment.

The similarity measure between the chip image \(a_i\) and the local area centered at \((x_i + u, y_i + v)\) is defined as the Hamming distance \(D_i(u, v)\), i.e. the number of pixels of different color (i.e. white-black or black-white). If the following inequality holds for a predetermined threshold \(\tau\), then the chip image \(a_i\) is counted as a matched chip.

\[
\min_{0 \leq u, v \leq \Delta} D_i(u, v) \leq \tau, \quad (\Delta = (w_S - w_C)/2).
\]  

(6)

Finally, the similarity score is calculated as \(n/N\) where \(n\) is the number of matched chips.

It will be shown in the next section that the minimum Hamming distance defined as the left side of the Eq.(6) can be calculated from the correlation function. This make it possible to apply the CIRF to the chip matching algorithm.

![Fig. 3. Chip matching algorithm](image)

IV. PROVABLY SECURECancelable Fingerprint Templates

In this section, we propose a method of generating provably secure cancelable fingerprint templates based on the CIRF and the chip matching algorithm.

A. Generating Cancelable Templates for Chip Matching (basic version)

We describe how to generate cancelable fingerprint templates for the chip matching, and then show the whole system of cancelable biometrics.

In what follows, all calculations are performed in the Galois field \(\mathbb{Z}_p\), where \(p\) is a prime number such that \(p - 1\) can be divided by \(w_S\) and \(p > 2w_S^2\). We represent the elements of \(\mathbb{Z}_p\) as \(\{-p^{-1}, \cdots, -1, 0, 1, \cdots, p^{-1}\}\). To calculate the Hamming distance from the cross-correlation function, we encode each pixel of a binary image to 1 (white) or \(-1\) (black).

Our cancelable template consists of cancelable chip images individually transformed using the CIRF. Fig.4 describes the outline of generating one cancelable chip image using the CIRF. In the enrollment stage, each chip image \(a_i\) is transformed as follows.

(i) \(a_i\) is extended to the same size as the search area \((w_S \times w_S)\) by padding the extra area with 0. This process is necessary to calculate linear cross-correlation from cyclic cross-correlation.

(ii) The extended chip image \(\hat{a}_i\) is transformed to \(A_i(X, Y)\) by two-dimensional NTT.

(iii) \(A_i\) is randomized by multiplying with the random filter \(R_t\) to make the cancelable chip image \(T_t\),

\[
T_t(X, Y) = A_i(X, Y)R_t(X, Y)
\]  

(7)

Here, the random filter \(R_t\) is prepared for each chip image \(a_i\) independently.

The transformation process for each chip image \(b_i\) in the authentication stage is as follows.

(i) The search area (of size \(w_S \times w_S\)) for \(a_i\) is clipped from the binary image. Let \(b_i(x, y)\) be the clipped image.

(ii) The flipped image \(\tilde{b}_i\) of \(b_i\) is transformed to \(B_i(X, Y)\) by two-dimensional NTT.
(iii) $B_i$ is randomized by dividing by the random filter $R_i$ to make the transformed image $U_i$.

$$U_i(X, Y) = B_i(X, Y) / R_i(X, Y)$$  \hfill (8)

The matching process for each chip image is as follows.

(i) Calculate $C_i(X, Y) = T_i(X, Y) / U_i(X, Y)$.

(ii) Perform the inverse NTT to the $C_i$ to yield the cyclic cross-correlation $c_i$, where

$$c_i(u, v) = \left(\hat{a}_i \ast b_i\right)(x, y) = \sum_{0 \leq x', y' < w_S} \hat{a}(x, y) b(x', y')$$

$$= \sum_{0 \leq x, y < w_S} \hat{a}(x, y) b(x', y').$$ \hfill (9)

c_i(u, v) is the summation of products of corresponding pixels of $b$ and cyclically shifted version of $\hat{a}$. As the extended region of $\hat{a}$ padded with zeros does not contribute to the summation, the cyclic-correlation is equal to the linear correlation within the following region.

$$-\Delta \leq u, v \leq \Delta \quad (\Delta = (w_S - w_C)/2)$$ \hfill (10)

Additionally, each product is equal to $1$ when the corresponding pixels are the same color (white-or black-black), and $-1$ when different color (white-black or black-white). Thus, within the region of Eq.(10), $c_i(u, v)$ can be expressed using the Hamming distance $D_i(u, v)$ as follows,

$$c_i(u, v) = \#\{\text{pixels of the same color}\}$$

$$-\#\{\text{pixels of different colors}\} = (w_C^2 - D_i(-u, -v)) - D_i(u, v)$$

$$= w_C^2 - 2 \cdot D_i(-u, -v).$$

Therefore, Eq.(6) is equivalent to the following inequality.

$$\min_{-\Delta \leq u, v \leq \Delta} w_C^2 - c_i(-u, -v) \leq \tau$$ \hfill (11)

This enables us to decide whether the chip image $a_i$ is matched or not according to completely the same criteria as the original chip matching algorithm.

By applying the above process to all chip images, the cancelable biometrics for fingerprint authentication can be established. However, the minutia coordinates are necessary to determine the search areas in the authentication stage. For that purpose we store the coordinates $\{x_i, y_i\}$ together with the random filters $R_i$ as a part of the parameter. Fig.5 shows the whole system of our cancelable biometrics. The outline of enrollment process is as follows.

(E1) The client preprocess the captured fingerprint image, and extract the core and the minutia location.

(E2) For each minutiae coordinates $(x_1, y_1), \cdots, (x_N, y_N)$ where the origin $(0, 0)$ is the core position, clip a chip image $a_i$ from the processed binary image.

(E3) Generate a random filter $R_i$ for each chip image $a_i$.

(E4) Translate each chip image $a_i$ to a cancelable chip image $T_i$ by using the random filter $R_i$.

(E5) Send the ordered list $T$ of cancelable chips to the server.

$$T = \{T_1, T_2, \cdots, T_N\}$$

(E6) The server enrolls $T$ as a cancelable template.

(E7) The client stores the ordered list $P$ of pairs of the minutiae coordinates and the random filter as a parameter.

$$P = \{(x_1, y_1), (x_2, y_2), \cdots, (x_N, y_N), R_N\}$$

The outline of authentication process is as follows.

(A1) The client preprocess the captured fingerprint image, and extract the core position as the origin $(0, 0)$.

(A2) For each minutiae coordinates $(x_1, y_1), \cdots, (x_N, y_N)$ recorded in the parameter $P$, clip a local image $b_i$ of the search area from the processed binary image.

(A3) Translate each local image $b_i$ to $U_i$ by using the random filter $R_i$ recorded in $P$.

(A4) Send the ordered list of transformed local images $\{U_1, U_2, \cdots, U_N\}$ to the server.

(A5) The server calculate the cross-correlation $c_i = NTT^{-1}(T_i U_i)$ for each cancelable chip image, and decide whether it is matched or not according to Eq.(11).

(A6) Let $n$ be the number of matched chip images. If the similarity score $s = n/N$ exceeds an authentication threshold $t$, the user is accepted.

The server can calculate completely the same similarity score as the conventional chip matching algorithm. Thus, the fingerprint authentication system using cancelable templates can be established without degrading the accuracy.

If the template $T$ leaks out from the server, or if the parameter $P$ leaks out from the client, the system can revoke them according to following steps.

(R1) The client generate a new random filter $R'_i$ for each $i = 1, 2, \cdots, N$.

(R2) Calculate the differential filter $\Delta R_i$ as follows, and send $\{\Delta R_1, \cdots, \Delta R_N\}$ to the server.

$$\Delta R_i(X, Y) = R'_i(X, Y) / R_i(X, Y)$$ \hfill (12)

(R3) The server re-transform each cancelable chip $T_i$ to yield a new cancelable chip $T'_i$ as follows,

$$T'_i(X, Y) = T_i(X, Y) \Delta R_i(X, Y)$$

$$= A_i(X, Y) R'_i(X, Y)$$ \hfill (13)
(R4) The server replace the template $T$ with $T'$.

$$T' = \{T'_1, \ldots, T'_N\}$$

(R5) The client replace the parameter $P$ with $P'$.

$$P' = \{((x_1, y_1), R'_1), \ldots, ((x_N, y_N), R'_N)\}$$

Note that the template revocation process can be performed without re-enrolling the user’s fingerprint or recovering the original chip images.

B. Hiding the Minutiae Locations in the Parameter

In our basic version of the cancelable biometric system described in the previous section, the parameter $P$ stored in the client includes the minutiae coordinates $(x_1, y_1), \ldots, (x_N, y_N)$. Note that even an attacker who obtained the parameter $P$ of a genuine user can not easily impersonate the user because the decision of acceptance is not made based on the correspondence of minutiae location, but on the similarity of local images. In fact, we will see in the next section that the FAR evaluated in the scenario where an attacker abuse the parameter $P$ of a genuine user is same as the FAR of the conventional chip matching algorithm.

However, the information of minutiae location itself may be considered as a privacy information, as it can be used for personal identification to some extent. Thus it is preferable to hide the minutiae location in the parameter $P$.

For this end, we add some chaff points to the parameter as shown in Fig.6. Specifically, in the enrollment stage, we locate $N_c$ chaff points randomly other than $N_m$ minutiae, and shuffle the order of $N = N_c + N_m$ points randomly. This shuffling is necessary to keep the attacker from knowing the minutiae coordinates from the order of coordinates recorded in the parameter $P$. The subsequent process is the same as the basic version described in Sec.IV-A.

The authentication and revocation processes are also the same as the basic version. Note that in the revocation process, the coordinates $(x_1, y_1), \ldots, (x_N, y_N)$ in the parameter $P$ are kept unchanged. This is necessary because if only chaff points change randomly, an attacker who obtained both the old parameter $P$ and the new $P'$ can distinguish the true minutiae from the chaff points. In this manner, we can keep

the fingerprint information secret as long as the template $T$ and the parameter $P$ do not leak out at the same time.

The chip images are expected to be matched to the genuine fingerprint image with high probability, whether they are clipped from the minutiae points or the chaff points. However, the chip images of chaff points might also be matched to an impostor fingerprint image with relatively high probability, because they have less distinguishing structure, as shown in Fig.6. Therefore, if the $N_c$ is too large, the accuracy may be degraded. We will show the relationship between the $N_c$ and the accuracy in Sec.V.

V. ACCURACY EVALUATION AND SECURITY ANALYSIS

In this section, we experimentally evaluate the proposed system, and discuss the security.

A. Accuracy Evaluation

We evaluated the accuracy of fingerprint verification using the proposed cancelable templates, and compared with the accuracy of the conventional chip matching. We used 181 pairs of fingerprint images captured through a capacitive sensor (Veridicom 5th Sense\footnote{5th Sense is a trademark of Veridicom International Inc.}) to evaluate the FAR and FRR and generate the DET curve. Experimental parameters are set as follows: $W = 176, wc = 12, ws = 28, \tau = 44, p = 337$.

To measure the effect that the proposed cancelable transform has on the accuracy of fingerprint verification, a chip image for enrollment and the corresponding clipped image for authentication are transformed using the same parameter, as described in Sec.IV-A. Note that this means the FAR is evaluated in the scenario that an attacker who try to impersonate a genuine user finds the parameter of the target user and use it to transform his own fingerprint for authentication. Fig.7 shows the DET curves evaluated using (i) conventional templates and (ii) cancelable templates of the basic version (with no chaff), (iii-1) minutiae hiding version with 10 chaffs, and (iii-2) minutiae hiding version with 20 chaffs. (In comparison, the number of true minutiae varied among fingers, and the average was 18.)

As shown in the figure, the DET curves (i) and (ii) are completely overlapped. This result shows that the basic version of cancelable transform has no effect on the accuracy of fingerprint verification using the chip matching algorithm. In addition, it also implies that finding the parameter of a genuine user would do no practical good for an attacker.
aiming to impersonate the user, although the parameter includes information of the minutiae locations.

On the other hand, by adding chaffs, the DET curves (iii-1) and (iii-2) were moved to the upper right a little. For example, if the authentication threshold \( t \) is controlled so that the FAR is less than 0.2\% and the FRR with 0, 10 and 20 chaff points are 5.0\%, 5.0\% and 5.5\% respectively. This result shows that the chaff points slightly degrades the accuracy, but the impact is not so significant.

The proposed methods to generate cancelable fingerprint templates is based on the CIRF. As mentioned in Sec.III-A, it is proved that the CIRF has perfect secrecy [5], namely it is impossible to extract any information about the original image from the transformed one. Because our cancelable template consists only of cancelable chips transformed using the CIRF with different random filters, it is also provable that extracting any information from the original fingerprint from the proposed cancelable fingerprint template is impossible. Therefore, even if the cancelable templates have leaked from the server or communication channel, the original fingerprint feature can be kept secret, maintaining security and privacy.

Next, let us consider the security compromise when the parameter leaked out from the client. A parameter of the basic version consists of random filters and minutiae coordinates. The random filters do not include any information about the original fingerprint. Additionally, as shown in Sec.V-A, leakage of the parameter do not directly cause impersonation. However, the information of minutiae location itself may be considered as a privacy information, as it can be used for personal identification to some extent.

The minutiae hiding version was proposed to address this privacy issue. A parameter of this version includes coordinates of \( N_m \) true minutiae and \( N_c \) chaff points. Even if the attacker obtaining the parameter knows \( N_m \), the number of candidate sets of minutiae is still large:

\[
N_m + N_c \binom{N_c}{N_m} = \frac{(N_m + N_c)!}{N_m!N_c!}. \tag{14}
\]

By substituting \( N_m = 18 \) (experimental average number of minutiae) and \( N_c = 10, 20 \) in the above formula, the number of candidate sets are estimated as \( 1.3 \times 10^7 \) and \( 3.4 \times 10^{10} \) respectively, making it fully difficult to specify the true set of minutiae. Nevertheless, further discussion about how many chaffs are necessary and sufficient to hide minutiae information is a future work.

VI. CONCLUSIONS

In this paper we proposed new methods of generating cancelable fingerprint templates with provable security, using the chip matching algorithm and the correlation-invariant random filtering. We proposed the basic version and the minutiae hiding version. Both versions have provable security in the meaning of impossibility of extracting any information about original fingerprint from the templates. However, a parameter of the basic version contains minutiae coordinates, which may cause the privacy compromise when it leaked out. The minutiae hiding version address this privacy issue by adding chaff points to conceal true minutiae. The accuracy of the proposed methods were evaluated experimentally. The basic version achieved the same accuracy as conventional matching algorithm. The minutiae hiding version slightly degraded the accuracy, but the loss was not significant. By applying our method, we can realize a secure and privacy-enhanced system of remote biometric authentication.

ACKNOWLEDGMENT

This work was partially supported by the national project promoted by the Ministry of Internal Affairs and Communications of Japan.

REFERENCES


