Cancelable Biometrics with Perfect Secrecy for Correlation-Based Matching

Shinji Hirata and Kenta Takahashi

Hitachi Ltd., Systems Development Laboratory,
292, Yoshida-cho, Totsuka-ku, Yokohama-shi, Kanagawa-ken, 244-0817, Japan
{shinji.hirata.sb,kenta.takahashi.bw}@hitachi.com

Abstract. In this paper, we propose a novel method of Cancelable Biometrics for correlation-based matching. The biometric image is transformed by Number Theoretic Transform (Fourier-like transform over a finite field), and then the transformed data is masked with a random filter. By applying a particular kind of masking technique, the correlation between the registered image and the input matching image can be computed in masked domain (i.e., encrypted domain) without knowing the original images. And we proved theoretically that in our proposed method the masked version does not leak any information of the original image, in other words, our proposed method has perfect secrecy. Additionally, we applied our proposed method to finger-vein pattern verification and experimentally obtained very high verification performance.

1 Introduction

Biometric authentication has the advantage of security and usability compared to traditional authentication methods like password or token. Biometrics cannot be stolen, forgotten, or shared. But recently, protecting biometric templates has become an issue. In a client/server-type biometric authentication system, biometric templates are stored in a database on the authentication server. In this case, it is difficult to prevent internal fraud by server's administrator, such as taking out biometric templates from the server. Furthermore, user's psychological resistance against centralized control of biometric is high. Besides, it is impossible to revoke biometric unlike password or token, and therefore if biometric is leaked out once and threat of forgery has occurred, the user cannot securely use his biometric anymore. The only remedy is to replace the template with another biometric feature. However, a person has only a limited number of biometric features.

Cancelable Biometrics [1] is a biometric verification scheme which was introduced to address this problem. This scheme enables the system to store and match templates while keeping them secret. The biometric is transformed using a parametrized distortion function. This preserves user's privacy and enhances security since it is impossible to recover the original biometric from the transformed version. A compromised template can be revoked using another transformation. Many authors have proposed methods for realizing Cancelable Biometrics. The

M. Tistarelli and M.S. Nixon (Eds.): ICB 2009, LNCS 5558, pp. 868–878, 2009.

followings are some of the works in this direction. Savvides et al. [2] proposed a method that encrypts the training images used to synthesize the correlation filter for face recognition. Connie et al. [3] proposed a method that hashes palmprint templates with a set of pseudo-random keys to obtain a unique code called palmhash. Ratha et al. [4] proposed several transformations for cancelable fingerprint, such as cartesian, radial and functional transformation. In order to realize Cancelable Biometrics, to design the transform function properly is important. First, it is important to preserve the accuracy. Secondly, it is required to prevent the attacker from recovering the original biometric feature from the transformed feature. Ideally, the transformed feature itself does not leak any information about the original one. But none of the existing methods meets both requirements at the same time.

In this paper, we propose a novel method of Cancelable Biometrics which meets both requirements at the same time. It is applicable to correlation-based matching and utilizes "Number Theoretic Transform" [5]. We show theoretically that the accuracy is preserved and the transformed version (i.e, our cancelable template) does not leak any information of the original image Additionally, we apply our proposed method to finger-vein pattern verification and show experimentally that the verification performance is high enough.

2 Preliminary

2.1 Motivation

Here, we explain our motivation to propose a new method of Cancelable Biometrics. Savvides et al. [2] developed a method of generating cancelable template for face recognition using the minimum average correlation energy (MACE) filter. They encrypt the training face images by multiplying the Fourier transform of the face images with the Fourier transform of a random convolution kernel (that is equivalent to convolving the images with random convolution kernel) and synthesize the encrypted MACE filter, which is their cancelable template. Their cancelable template $\boldsymbol{h'}$ is defined as follows: Let $\boldsymbol{h} = \{h_i\}$ be the unencrypted original MACE filter (i.e., original template). Let $\boldsymbol{l} = \{l_i\}$ be the random filter. Then the encrypted MACE filter, that is, their cancelable template $\boldsymbol{h'} = \{h'_i\}$ is defined as $h'_i = l_i h_i$ for i-th component.

They show that the verification performance is preserved. However, their cancelable template leaks partial information of the original template, thus there is a possibility to recover the original template from the cancelable template. The reason is as follows: The range of l_i is given as a system parameter and naturally we can assume that the attacker knows this range. So, suppose $l_i \in (0, l_{max}]$. And we can also assume that the attacker knows the range of h_i. This is because she can estimate theoretically the range of h_i from the specification of their algorithm and the image used. Here, suppose $h_i \in (0, h_{i,max}]$. Note that the assumption of $h_i > 0$ does not cause loss of generality. Now assume that the attacker obtains the cancelable template $\boldsymbol{h'}$. Since $h_i = \frac{h'_i}{l_i}$, $l_i \in (0, l_{max}]$ and $h_i \in (0, h_{i,max}]$, then she gets to have the inequality of $\frac{h'_i}{l_{max}} \leq h_i \leq h_{i,max}$ For

the attacker, from the knowledge of h'_i, the range of h_i is confined to $[\frac{h'_i}{l_{max}}, h_{i,max}]$ compared to the original range of $(0, h_{i,max}]$. This means that h'_i leaks partial information about h_i.

We can address this problem if l_i, h_i and h'_i are elements of a finite field. The reason is as follows: Let $GF(p)$ be a finite field with order p, where p is prime. Assume $l_i, h_i, h'_i \in GF(p)(l_i \neq 0, h_i \neq 0, h'_i \neq 0)$ and l_i is uniformly random. By definition, we have $h_i = h'_i l_i^{-1}$. The mapping $\texttt{Inverse}; l_i \mapsto l_i^{-1}$ is bijective since $l_i \in GF(p)(l_i \neq 0)$. And for given h'_i, the mapping $\texttt{Multiply}_{h'_i}; l_i^{-1} \mapsto h'_i l_i^{-1}$ is bijective since $l_i^{-1}, h'_i \in GF(p)(l_i \neq 0, h'_i \neq 0)$. Thus, the composite mapping $\texttt{Multiply}_{h'_i} \circ \texttt{Inverse}$ for given h'_i is bijective. From this and the assumption that l_i is uniformly random, we conclude h_i is independent from h'_i, that is to say, h'_i cannot leak any information about h_i.

To make h_i be an element of $GF(p)$, the process of creating h_i must be performed over $GF(p)$. In their method, Fourier Transform (FT) is utilized to create h_i. In fact, there is a Fourier-like transform over $GF(p)$, which is called "Number Theoretic Transform (NTT)" [5]. If it is possible to create $\boldsymbol{h}$ by using NTT instead of FT, we can solve the problem. But unfortunately, we cannot create $\boldsymbol{h}$ by using NTT. Their method utilizes the MACE filter. To make the MACE filter, computing the spatial-frequency power spectrum of the images is required. The number theoretic transform of the image means nothing physical, while the fourier transform of the image means frequency component. Thus the power spectrum cannot be obtained through NTT. This is why we cannot create $\boldsymbol{h}$ by using NTT.

But it is possible to compute the simple correlation between two images by using NTT. Hence, not for the advanced correlation filter (like the MACE filter), but for a matching algorithm based on the simple correlation, we can construct a method of Cancelable Biometrics which multiplies the number theoretic transform of the image by a random filter. Thus, in the following , we propose a new method of Cancelable Biometrics for a simple correlation-based matching algorithm using NTT.

2.2 Correlation-Based Matching

Before presenting our proposed method, we describe the correlation-based matching algorithm. The following is a well-known algorithm of correlation-based matching [6], which is applicable to image-based biometric verification (e.g., fingerprint, iris, finger-vein and so on).

$f(x, y)$ and $g(x, y)$ are the values at position (x, y) of the registered image and the input matching image, respectively. The size of the registered image $f(x, y)$ is $W_f \times H_f$ and the size of the input matching image is $W_g \times H_g$, where $W_f < W_g$ and $H_f < H_g$. And $f(x, y)$ and $g(x, y)$ are taken from integers. $w_{f,g}(p, q)$ is the correlation between $f(x, y)$ and $g(x, y)$ at the relative displacement (p, q). $w_{f,g}(p, q)$ is defined as follows:

$$w_{f,g}(p, q) = \sum_{(x,y) \in S(p,q)} f(x - p, y - q) g(x, y), \tag{1}$$

where $S(p,q)$ is the region that the registered image $f(x,y)$ overlaps the input matching image $g(x,y)$ at the displacement (p,q).

$w_{f,g}(p,q)$ is not directly used as a measure of match, instead we use *Peak-to-Mean*. First, let *peak* be the maximum value of $w_{f,g}(p,q)$. Second, on the correlation plane, let us consider the sidelobe region (excluding a central rectangular mask) centered at the peak. Let *mean* be the mean of $w_{f,g}(p,q)$ in this sidelobe region. Then, *Peak-to-Mean* is defined as follows: $Peak\text{-}to\text{-}Mean = peak - mean$. *Peak-to-Mean* means the peak's height to the sidelobe and this indicates the similarity of two images. Now note that *Peak-to-Mean* is computed based on only the correlation $w_{f,g}(p,q)$.

3 Proposed Method

In this section, we propose a new method of Cancelable Biometrics for the typical correlation-based matching which is described in Section 2.2. If the correlation can be computed while keeping the two images secret, we can construct Cancelable Biometrics for correlation-based matching. In order to realize this, we utilize "Number Theoretic Transform (NTT)"[5].

NTT Ψ is a Fourier-like transform over $GF(p)$ and is denoted as follows: $\Psi;(a_1,\cdots,a_n) \mapsto (A_1,\cdots,A_n)$, where $a_i, A_i \in GF(p)$. For details of NTT, please see [5]. Although here for convenience described for 1-D data arrays, it is easily applicable to 2-D image [7]. NTT Ψ has following property: $\Psi(\boldsymbol{a} * \boldsymbol{b}) = \Psi(\boldsymbol{a})\Psi(\boldsymbol{b})$, where $\boldsymbol{a} = \{a_i\}, \boldsymbol{b} = \{b_i\}$ and $*$ is convolution. This property means that the convolution of data arrays corresponds to the component-wise multiplication in the NTT domain, and this property is called "Cyclic Convolution Property (CCP)". In fact, Fourier Transform has the same property. And CCP implies that a convolution can be computed by:

$$\boldsymbol{a} * \boldsymbol{b} = \Psi^{-1}\{\Psi(\boldsymbol{a})\Psi(\boldsymbol{b})\}. \tag{2}$$

Note that in order to compute the correlation between $\boldsymbol{a}$ and $\boldsymbol{b}$, the order of the one data array has to be inverted.

By using CCP of NTT, we can compute the correlation while keeping the two images secret, thus we can construct Cancelable Biometrics for correlation-based matching. In order to apply NTT, the size of the registered image must be equal to the size of the input matching image. Thus, we pad the value to the pixels outside the registered image $f(x,y)$. The value of padding in the extended region is 0. By doing this, the registered image $f(x,y)$ is extended to the same size as the input matching image $g(x,y)$. Let $\widetilde{f}(x,y)$ be the extended version of $f(x,y)$. Note that the correlation is invariant under this extension since the padding value is 0, that is, $w_{\widetilde{f},g}(p,q) = w_{f,g}(p,q)$.

Figure 1 depicts the block diagram of our proposed method. $F(u,v)$ and $G(u,v)$ are the number theoretic transform of $\widetilde{f}(x,y)$ and $g(x,y)$, respectively, where (u,v) is the position in the NTT domain. $F(u,v) \in GF(p)$ and $G(u,v) \in GF(p)$. $R(u,v)$ is a random filter. Let $R(u,v)$ be uniformly random over $GF(p)$, but $R(u,v) \neq 0$. $R^{-1}(u,v)$ is a random filter which is the inverse element of

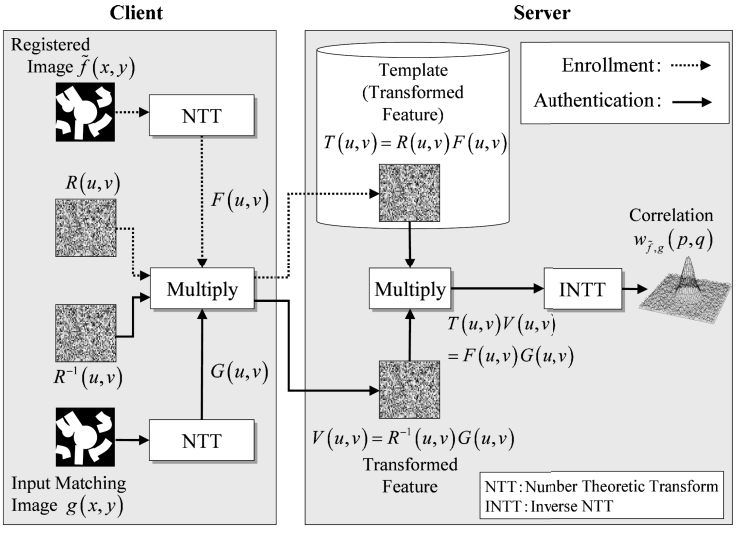

Fig. 1. Block diagram of the proposed method

$R(u,v)$. Thus $R^{-1}(u,v) \in GF(p)$, $R^{-1}(u,v) \neq 0$ and $R(u,v)R^{-1}(u,v) = 1$. In what follows, the transformed biometric feature is referred to as the transformed feature and the data to be used for transforming the feature is referred to as the parameter.

In enrollment stage, we first perform NTT to $\widetilde{f}(x,y)$ and get $F(u,v)$, and then multiply $F(u,v)$ by $R(u,v)$ (i.e., mask $F(u,v)$ with a random filter $R(u,v)$). Our cancelable template $T(u,v)$ is defined as $T(u,v) = R(u,v)F(u,v)$ and $R^{-1}(u,v)$ is the parameter. These processes are performed in the client. Then $T(u,v)$ is sent to the server and stored into the database and $R^{-1}(u,v)$ is stored in the client.

In authentication stage, we first perform NTT to $g(x,y)$ and get $G(u,v)$, and then multiply $G(u,v)$ by $R^{-1}(u,v)$ (i.e., mask $G(u,v)$ with a random filter $R^{-1}(u,v)$). Our transformed feature $V(u,v)$ is defined as $V(u,v) = R^{-1}(u,v)G(u,v)$. These processes are performed in the client and then $V(u,v)$ is sent to the server. The matching process is performed in the masked domain (i.e., encrypted domain) on the server. This process is as follows: we first multiply $T(u,v)$ by $V(u,v)$. Then we compute the correlation $w_{\tilde{f},g}(p,q)$ from $T(u,v)V(u,v)$ by using Inverse-NTT. This is because $T(u,v)V(u,v) = F(u,v)G(u,v)$ must hold since $R(u,v)R^{-1}(u,v) = 1$ and we can obtain the correlation according to Eq.(2). This means that we can compute the correlation between $f(x,y)$ and $g(x,y)$ in the masked domain (i.e., encrypted domain), while keeping $F(u,v)$ and $G(u,v)$ secret, that is, keeping $f(x,y)$ and $g(x,y)$ secret. Finally we compute *Peak-to-Mean* from the correlation $w_{\tilde{f},g}(p,q)$ and authenticate the user.

In addition, $T(u,v)$ can be changed by varying $R(u,v)$, thus revocation of the template is enabled.

4 Analysis

4.1 Accuracy Preservation

In general, an error in computing the score would occur due to applying the transformation and the matching accuracy may degrade compared to the version without transformation [4]. It is important to reduce the accuracy degradation and to preserve the accuracy.

Here, we discuss the accuracy preservation of our proposed method when applied to the algorithm described in Section 2.2. NTT is a transform over $GF(p)$, thus pixels of image must be elements of $GF(p)$. For this, if a pixel f is negative, then we convert f to $p - |f|$. Besides, any pixel of the correlation plane obtained through Inverse-NTT is not negative, that is, negative pixels are not computed correctly. To compensate this, the following is performed: let p be larger than about twice as large as the maximum of the correlation. If a pixel w of the correlation plane is larger than the maximum of the correlation, then we convert w to $w - p$. By this, we can compute the correlation plane correctly. Hence, the matching score is invariant when applying our proposed method, thus the accuracy is preserved.

4.2 Recovery Resistance

From the point of view of template protection, it is required to prevent the attacker from recovering the original biometric feature from the transformed feature without knowledge of the parameter. Ideally, the transformed feature itself does not leak any information about the original biometric. Furthermore, it is also required to prevent the attacker from recovering the original biometric feature from the parameter without knowledge of the transformed feature. Also ideally, the parameter itself does not leak any information about the original biometric.

(1) Resistance against Recovery from Template

We here discuss the resistance against recovery of the original images $f(x, y)$ or $g(x, y)$ from the cancelable template $T(u, v)$ or the transformed feature $V(u, v)$. In what follows, we will prove that it is impossible to recover $F(u, v)$ from $T(u, v)$ without knowledge of $R(u, v)$ (we will treat the case of $G(u, v)$ later).

Since the transform of masking $F(u, v)$ with $R(u, v)$ is component-wise in the NTT domain, it is sufficient to prove it for only one single component. Let us consider just one component at the position of (u, v). Let $r \in GF(p)$ $(r \neq 0)$ be the (u, v)-th component of $R(u, v)$, $s \in GF(p)$ be the (u, v)-th component of $F(u, v)$ and $t \in GF(p)$ be (u, v)-th component of $T(u, v)$. Then we have $t = rs$. We will prove that it is impossible to recover s from t without knowledge of r.

We now define the transform function $\phi_r(s) = rs$. And let $\mathbf{\Phi}$ be the family of the transform functions ϕ_r. We can here consider $\mathbf{\Phi}$ as an encryption algorithm, where r is a encryption key, s is a plaintext and t is a ciphertext. And we define the transform function $\phi_r^{-1}(t) = r^{-1}t$. Decryption algorithm $\mathbf{\Phi}^{-1}$ is defined as the family of the transform functions ϕ_r^{-1}.

There is a formal definition about secrecy in cryptography, that is, Perfect Secrecy [8]. Before presenting the definition of Perfect Secrecy, let us introduce the definition of Cryptosystem according to [8].

Definition 1. *Cryptosystem is a tuple* $(\mathbf{M}, \mathbf{C}, \mathbf{K}, \mathbf{E}, \mathbf{D})$ *with the following properties:*

1. $\mathbf{M}$ *is a set and called the plaintext space.*
2. $\mathbf{C}$ *is a set and called the ciphertext space.*
3. $\mathbf{K}$ *is a set and called the key space.*
4. $\mathbf{E} = \{E_k; k \in \mathbf{K}\}$ *is a family of functions* $E_k; \mathbf{M} \to \mathbf{C}$.
5. $\mathbf{D} = \{D_k; k \in \mathbf{K}\}$ *is a family of functions* $D_k; \mathbf{C} \to \mathbf{M}$.
6. *For each* $e \in \mathbf{K}$*, there is* $d \in \mathbf{K}$ *such that* $D_d(E_e(m)) = m$ *for all* $m \in \mathbf{M}$

In our case, the cryptosystem is $(S, T, R, \mathbf{\Phi}, \mathbf{\Phi}^{-1})$, where $S = \{0, 1, \cdots, p-1\}$ is the set of plaintexts s, $R = \{1, 2, \cdots, p-1\}$ is the set of encryption keys r (Note that R does not include 0) and $T = \{0, 1, \cdots, p-1\}$ is the set of ciphertexts t.

We now present the Shanon's definition of Perfect Secrecy:

Definition 2. *Cryptosystem* $(\mathbf{M}, \mathbf{C}, \mathbf{K}, \mathbf{E}, \mathbf{D})$ *has Perfect Secrecy if the events that a particular ciphertext occurs and that a particular plaintext has been encrypted are independent (i.e.,* $\Pr(m|c) = \Pr(m)$ *for all plaintexts* m *and all ciphertexts* c*).*

Definition 2 implies that it is impossible even to estimate m from c without knowledge of k. Thus, in order to prove that it is impossible to recover s from t without knowledge of r, it is sufficient to prove that $(S, T, R, \mathbf{\Phi}, \mathbf{\Phi}^{-1})$ has Perfect Secrecy.

But it is easy to see that one can recover s without knowledge of r if $t = 0$ in $(S, T, R, \mathbf{\Phi}, \mathbf{\Phi}^{-1})$. This is because according to definition of ϕ_r if $t = 0$, then $s = 0$ must hold since $r \neq 0$. In order to avoid this, let us eliminate the case of $s = t = 0$ and define another set of plaintexts and ciphertexts; $\widetilde{S} = \{1, \cdots, p-1\}$ is the set of plaintexts $\widetilde{s}$, and $\widetilde{T} = \{1, \cdots, p-1\}$ is the set of ciphertexts $\widetilde{t}$. As we describe later, we can prove that the cryptosystem $(\widetilde{S}, \widetilde{T}, R, \mathbf{\Phi}, \mathbf{\Phi}^{-1})$ has Perfect Secrecy.

Now only the case of $s = 0$, that is, the case of $F(u, v) = 0$ is a problem. But if the case of $F(u, v) = 0$ rarely happens, this would not be a problem in practice. In order to examine how often the case of $F(u, v) = 0$ happens, as an example, we applied NTT to finger-vein pattern images and experimentally obtained the rate of the case of $F(u, v) = 0$ in all $F(u, v)$s among the whole dataset. The rate is 0.016%. The rate is low enough, thus the amount of leaked information is so small that in practice one cannot recover the entire $F(u, v)$ from it. We will see the details of this experiment in Section 5.

In order to prove that the cryptosystem $(\widetilde{S}, \widetilde{T}, R, \mathbf{\Phi}, \mathbf{\Phi}^{-1})$ has Perfect Secrecy, we use the following Shanon's theorem [8]:

Theorem 1. *Let* $|\mathbf{M}| = |\mathbf{K}| = |\mathbf{C}| < \infty$ *and* $\Pr(m) > 0$ *for any plaintext* m*. Cryptosystem* $(\mathbf{M}, \mathbf{C}, \mathbf{K}, \mathbf{E}, \mathbf{D})$ *has perfect secrecy if and only if the probability distribution on the key space is the uniform distribution and if for any platintext* m *and any ciphertext* c *there is exactly one key* k *with* $E_k(m) = c$*.*

Now we can prove the following theorem using Theorem 1:

Theorem 2. *Cryptosystem* $(\widetilde{S}, \widetilde{T}, R, \mathbf{\Phi}, \mathbf{\Phi}^{-1})$ *has Perfect Secrecy.*

Proof. By definition, $|\widetilde{S}| = |\widetilde{T}| = |R| < \infty$, $\Pr(\widetilde{s}) > 0$ for any $\widetilde{s}$ and the probability distribution of r is uniform.

Let us confirm that for any $\widetilde{s}$ and any $\widetilde{t}$ there is exactly one key r with $\phi_r(\widetilde{s}) = \widetilde{t}$. If we assume that for arbitrary $\widetilde{s}$ and $\widetilde{t}$, $\widetilde{t} = \phi_{r_1}(\widetilde{s}) = \phi_{r_2}(\widetilde{s})$ where $r_1 \neq r_2$, then $r_1\widetilde{s} = r_2\widetilde{s}$ must hold. There exists $\widetilde{s}^{-1}$ and we can multiply both parts of this equation by $\widetilde{s}^{-1}$. Then we have $r_1 = r_2$. But this contradicts the assumption that $r_1 \neq r_2$. Hence, for any $\widetilde{s}$ and $\widetilde{t}$ there is exactly one key r with $\phi_r(\widetilde{s}) = \widetilde{t}$. This proves the theorem. □

Therefore, $T(u, v)$ does not leak any information of $F(u, v)$, hence it is impossible to recover $F(u, v)$ from $T(u, v)$ without knowledge of $R(u, v)$ (note that there is the exceptional case of $F(u, v) = 0$, but in practice this case is rare and not a problem).

In the same way, we can prove that $V(u, v)$ does not leak any information of $G(u, v)$, hence it is impossible to recover $G(u, v)$ from $V(u, v)$ without knowledge of $R^{-1}(u, v)$ (also note that there is the exceptional case of $G(u, v) = 0$, but this case is not a problem in practice).

(2) Resistance against Recovery from Parameter

We here discuss the resistance against recovery of the original image $f(x, y)$ from the parameter $R^{-1}(u, v)$ which is stored in the client. $R^{-1}(u, v)$ is uniformly random and independent from $f(x, y)$. Hence, it is impossible to recover $f(x, y)$ from $R^{-1}(u, v)$ without knowledge of $T(u, v)$. In addition, even if the attacker collects two or more different $R^{-1}(u, v)$s which are used to match against the same original image $f(x, y)$, he cannot recover $f(x, y)$ because $R^{-1}(u, v)$ does not include any information of $f(x, y)$.

(3) Resistance against Recovery from Correlation

We here discuss another possible approach to recover the original images $f(x, y)$ and $g(x, y)$. The server knows the correlation between $f(x, y)$ and $g(x, y)$ in matching phase. If the server administrator is malicious, she would try to take advantage of this correlation to recover $f(x, y)$ and $g(x, y)$.

In order to recover $f(x, y)$ and $g(x, y)$, the attacker regards Eq.(1) as a simultaneous equation and try to solve it. This simultaneous equation has $H_f W_f + H_g W_g$ variables and $H_g W_g$ equations. The solution of the equation is underspecified because the number of variables is larger than the number of equations. If the authentication is repeated n times, the number of variables is $H_f W_f + nH_g W_g$ and the number of equations is $nH_g W_g$. The solution of the equation is also underspecified because the number of variables is larger than the number of equations. Thus, we conclude that to recover the original images from the correlation is impossible.

5 Experiments

In our experiment, we applied the proposed method to finger-vein pattern matching and examine the verification performance. We used the infrared finger images obtained from 17 volunteers in our company. For each person, three fingers of each hand are used. The dataset contains infrared images of 102 different fingers, with a pair of images per finger. The images are captured by the infrared sensing device which was developed as a prototype in our company (for details of the device, see [9]). Figure 2 shows an example of infrared finger image. By using the algorithm described in [9], the finger-vein pattern images are extracted from the infrared finger images.

Fig. 2. Example of infrared finger image

We applied our proposed method to finger-vein pattern images and measured matching score (*Peak-to-Mean*) for assessing the verification performance. We generated 102 genuine scores and 10302 ($= 102 \times 101$) impostor scores by performing all-against-all matches. Figure 3 shows the normalized frequency distribution of score for genuine and impostor matching. There is a clear margin of separation between the scores of the genuine class and the impostor class, that is, the verification performance is high enough.

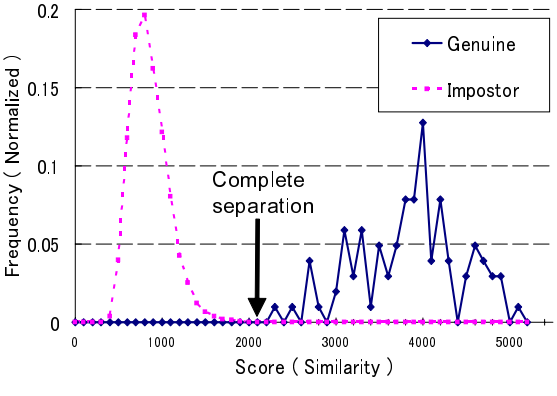

Fig. 3. Normalized frequency distribution of score for genuine and impostor matching

In Section 4.2, we analyzed the resistance against recovery of the original image from our cancelable template and noticed that only the case of NTT component being 0 is a problem. But if this case rarely happens, this would not

be a problem in practice. In order to see how often this case happens, we applied NTT to finger-vein pattern images and examined the rate of the case of NTT component being 0. We investigated all the NTT components among the whole dataset of finger-vein pattern images ($102 \times 2 = 204$ images) and then obtained a rate of 0.016% of NTT components being 0. Table 1 shows the number of images that include NTT component being 0. 70%(= 144/204) of the images include no NTT component being 0 and the number of NTT component being 0 is at most 3 per image. Thus, the rate is low enough and there is no particular image that include many NTT components being 0. Hence, the amount of leaked information is so small that in practice one cannot recover the entire $F(u, v)$ or $G(u, v)$ from it.

Table 1. Number of images that include NTT components being 0

Num of NTT component being 0 per image	0	1	2	3
Num of image (Total 204)	144	52	6	2

6 Conclusion

In this paper, we proposed a novel method of Cancelable Biometrics for correlation-based matching. The main idea is to transform the image by Number Theoretic Transform and mask the transformed data with a random filter. By applying a particular kind of masking technique, the correlation between the registered image and the input matching image can be computed in masked domain (i.e., encrypted domain) without knowing the original images. Thus, the matching accuracy is invariant when applying our proposed method. And we proved theoretically that in our proposed method the masked version does not leak any information of the original image, in other words, our proposed method has perfect secrecy. Additionally, we applied our proposed method to finger-vein pattern verification and experimentally obtained very high verification performance.

Acknowledgement

This paper partially contains research achievements of a national project funded by Ministry of Internal Affairs and Communications in Japan, "R&D for advancement of functionality and usability in information history management".

References

1. Ratha, N.K., Connell, J.H., Bolle, R.M.: Enhancing security and privacy in biometric-based authentication systems. IBM System Journal 40(3) (2001)
2. Savvides, M., Vijayakumar, B.V.K., Khosla, P.K.: Cancelable Biometric Filters for Face Recognition. In: 17th International Conference on Pattern Recognition (ICPR 2004), vol. 3, pp. 922–925 (2004)

3. Connie, T., Teoh, A., Goh, M., Ngo, D.: PalmHashing: a novel approach for cancelable biometrics. Information Processing Letters 93(1), 1–5 (2005)
4. Ratha, N.K., Connell, J.H., Bolle, R.M., Chikkerur, S.: Cancelable Biometrics: A Case Study in Fingerprints. In: 18th International Conference on Pattern Recognition (ICPR 2006), vol. 4, pp. 370–373 (2006)
5. Agarwal, R.C., Burrus, C.S.: Number theoretic transforms to implement fast digital convolution. Proc. IEEE 63(4), 550–560 (1975)
6. Rosenfeld, A., Kak, A.C.: Digital Picture Processing, 2nd edn., vol. 2. Academic Press, London (1982)
7. Reed, I.S., Truong, T.K., Kwoh, Y.S., Hall, E.L.: Image Processing by Transforms Over a Finte Field. IEEE Transactions on Computers C-26(9), 874–881 (1977)
8. Buchmann, J.A.: Introduction to Cryptography, 2nd edn. Springer, Heidelberg (2004)
9. Miura, N., Nagasaka, A., Miyatake, T.: Feature extraction of finger-vein patterns based on repeated line tracking and its application to personal identification. Machine Vision and Applications 15(4), 194–203 (2004)