UNITARY TRANSFORM-BASED TEMPLATE PROTECTION AND ITS PROPERTIES

Ibuki NAKAMURA¹, Yoshihide TONOMURA², and Hitoshi KIYA¹

¹Tokyo Metropolitan University, Hino, Tokyo 191-0065, Japan
²NTT Network Innovation Laboratories, Nippon Telegraph and Telephone Corp.

ABSTRACT

We focus on the feature transform approach as one methodology for biometric template protection, where the template consists of the features extracted from the biometric trait. This paper considers some properties of the unitary transform-based template protection in particular. It is known that the Euclidean distance between the templates protected by a unitary transform is the same as that between original (non-protected) ones as a property. In this paper, moreover, it is shown that it provides the same results in $L^2$-norm minimization problems as those of original templates. This means that there is no degradation of recognition performance in authentication systems using $L^2$-norm minimization. Therefore, the protected templates can be reissued multiple times without original templates. In addition, a DFT-based template protection scheme is proposed as an unitary transform-based one. The proposed scheme enables to efficiently generate protected templates by the FFT, in addition to the useful properties. It is also applied to face recognition experiments to evaluate the effectiveness.

Index Terms—Biometrics, Template protection, Unitary transform, $L^2$-norm minimization

1. INTRODUCTION

Establishing the identity of a person is a critical task in any management system. A surrogate representation such as passwords and IC cards is not sufficient for reliable management systems, because it is easily shared, misplaced, or stolen. On the other hand, biometric recognition offers a reliable solution to the problem of user identification in identity management systems, due to a number of desirable properties of biometric traits. However, there are still some issues concerning the security of biometric recognition systems. One of the most critical issues is template security, on which we focus in this paper. Therefore, a lot of researchers have studies various kinds of biometric recognition schemes not only to improve recognition performance but also to protect biometric templates.


The unitary transform-based template protection in this paper corresponds to salting in the feature transformation approach. In generally, non-invertible transforms are preferable in terms of security, but it is difficult to guarantee no degradation of recognition performance in a deterministic way. In addition, it has been pointed out that there is some risk for estimating an original template from the protected one, by using some state-of-the-art techniques such as compressed sensing or non-linear filtering [8] [16]. On the other hand, the unitary transform-based protection provides a few good properties, although parameters have to be securely managed as a secret key. For example, the Euclidean distance between the protected templates is equal to that between original ones [5].

This paper considers additional properties of the unitary transform-based template protection. We show that the result of solving problem of $L^2$-norm minimization is exactly the same as that of original templates. As a result, the protected template can be reissued multiple times by simply repeating the protection. Besides, a DFT-based protection scheme is proposed as one of unitary transformation ones. In this scheme, random orthogonal matrices are easily produced and the FFT can be used to efficiently generate protected templates. Finally, the proposed scheme is also applied to face recognition experiments to verify the effectiveness of the proposed one.

2. PREPARATION

2.1. Biometric Authentication System

In this paper, we consider the biometric authentication system in Fig.1, which is using a parameter $p$, as a user specific password or key. In the enrollment, a feature set $f_i$, called a template is extracted from each biometric training sample, and then a transform function $T(\cdot)$ is applied to the template to generate a protected template $f = T(f_i, p_i)$. Next, only the protected template is stored into a database. The user $i$ receives the parameter $p_i$ from the enrollment system. On the other hand, in the authentication, the user $i$ gives the parameter $p_i$,
Generally, the template \( f_i \in \mathbb{R}^N \) is protected by a unitary matrix having randomness with a parameter \( p_r, Q_p \in \mathbb{R}^{N \times N} \) as

\[
\hat{F} = T(f_i, p_r) = Q_p f_i,
\]

(1)

where \( \hat{F} \) is the protected template. A lot of generation schemes of \( Q_p \) have been studied to generate unitary or orthonormal random matrices [5] [17]. For example, the Gram-Schmidt method is applied to a pseudo-random matrix to generate \( Q_p \) [5]. However, generally, the conventional schemes are computationally expensive.

B. DFT-based template protection

DFT is applied to each template \( f_i = [f_i(0), f_i(1), \ldots, f_i(N-1)]^T \), \( i = 1, 2, \ldots, K \)

\[
F_i(k) = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} f_i(n) \cdot W_N^{nk}, \quad k = 0, 1, \ldots, N-1
\]

(2)

where, \( W_N = e^{-j2\pi/n} \) and \([\cdots]^T\) means the transposed operation. When the DFT matrix is defined as \( A \in \mathbb{C}^{N \times N} \), eq(2) is expressed as:

\[
F_i = Af_i
\]

(3)

where \( F_i = [F_i(0), F_i(1), \ldots, F_i(N-1)] \). Next, \( N \) phase values \( \theta_p(k) \in [\frac{2\pi}{N} + \alpha l, 0, 1, \ldots, L-1, \alpha \in \mathbb{R}, k = 0, 1, \ldots, N-1 \) are randomly generated by using a pseudo random generator [18]-[20] and the phase vector \( \theta_p \) is used to define a diagonal matrix \( H_p \):

\[
H_p(k, k) = e^{j\theta_p(k)}, \quad k = 0, 1, \ldots, N-1
\]

(4)

Note that \( H_p \) satisfies

\[
H_p^* H_p = I
\]

(5)

where \([\cdots]^*\) and \( I \) mean the Hermitian transpose operation and the identity matrix respectively. Then, \( H_p \) is multiplied to \( F_i \) as

\[
\hat{F}_i = H_p F_i = H_p A f_i
\]

(6)

Comparing eq.(6) with eq.(1), the relation is given as,

\[
Q_p = H_p A
\]

(7)

Note that \( H_p A \) is also a unitary matrix as well as \( A \). It is possible to obtain a protected template with real numbers by applying with inverse DFT:

\[
\hat{f}_i = A^{-1} \hat{F}_i = A^{-1} H_p A f_i
\]

(8)

where \( \theta_p \) has to satisfy the relation \( \theta_p(k) = 2\pi - \theta_p(N-k), k = 1, \ldots, \lfloor \frac{N-1}{2} \rfloor \) if we want real values as \( \hat{f}_i \in \mathbb{R}^N \). In this case, \( \theta_p \) corresponds to \( p_r \) in Fig.1. Furthermore, the protected template has following properties.

Property 1 : Conservation of the Euclidean distances.

\[
||f_i - f_j||^2 = ||\hat{f}_i - \hat{f}_j||^2
\]

Property 2 : Conservation of inner products.

\[
f_i \cdot f_j = \hat{f}_i \cdot \hat{f}_j
\]

Property 3 : Conservation of correlation coefficients.

\[
\frac{|f_i \cdot f_j|}{\sqrt{||f_i||^2 \sqrt{||f_j||^2}}} = \frac{|\hat{f}_i \cdot \hat{f}_j|}{\sqrt{||\hat{f}_i||^2 \sqrt{||\hat{f}_j||^2}}} = \frac{|f_i \cdot f_j|}{\sqrt{||f_i||^2 \sqrt{||f_j||^2}}}
\]

3. PROPOSED SYSTEM

In this section, a new property of the unitary transform approach is presented and a DFT-based template protection is proposed.

3.1. Generation of Protected Templates

A. Unitary transform-based template protection
The property 2 is provided by
\[
\hat{f}_1^T \hat{f}_1 = (A^{-1}H_p A_f) (A^{-1}H_p A_f) = (f_1^T A H_p^T A_{-1}^T) (A^{-1}H_p A_f) = (f_1^T A H_p A_{-1}^T) = \hat{f}_1^T \hat{f}_1.
\] (9)

Also, the property 1 and 3 are obvious because they consist of inner products. In the section 3.2, another property is shown by using the property 2.

3.2. Authentication via \( l^2 \)-norm minimization

We review the authentication algorithm based on Linear combination of templates computed by \( l^2 \)-norm minimization [6] - [9], and the 4th out is shown.

\( \text{A. Authentication algorithm} \)

First, \( f_{i,m} \) is defined as the \( m \)-th template for the \( i \)-th person where \( m = 1, 2, ..., M_i \). For the \( i \)-th registered person among \( K \) registered persons, the set of \( M_i \) training templates is given by \( D_i = \{ f_{i,1}, f_{i,2}, ..., f_{i,M_i} \} \). Let us assume that \( y \), the template of a query which belongs to the \( i \)-th person, is linearly approximated solely by the training vectors of the \( i \)-th person:
\[
y = f_{i,1} x_{i,1} + f_{i,2} x_{i,2} + ... + f_{i,M_i} x_{i,M_i} = D_i x_i,
\] (10)

where \( x_{i,j} \) is a coefficient value. Therefore, with all templates of \( K \) registered persons, \( y \) can be represented as:
\[
y = D_1 x_1 + ... + D_{i-1} x_{i-1} + D_{i+1} x_{i+1} + ... + D_K x_K = D x_0.
\] (11)

To identify the \( i \)-th person, the \( l^2 \)-norm minimization problem of eq. (11) is carried out as:
\[
x_0 = \arg \min_{x} ||x||_2 \quad \text{subject to} \quad y = D x.
\] (12)

By solving eq. (12), an approximate solution \( \hat{x}_0 \) is obtained as \( \hat{x}_0 = [\hat{x}_1^T, \hat{x}_2^T, ..., \hat{x}_K^T]^T \). \( \hat{x}_0 \) is used to authenticate a person \( C \). We define the function \( \hat{\delta}(\cdot) \) that replaces the coe\( ficients \) with zeros for each of the \( i \)-th person:
\[
\hat{\delta}(\hat{x}_0) = [0^T, ..., 0^T, \hat{x}_i^T, 0^T, ..., 0^T]^T.
\] (13)

Substituting \( \hat{\delta}(\hat{x}_0) \) into \( x_i \) in eq. (10), the person \( C \) is estimated by
\[
r_i = ||y - D \hat{\delta}(\hat{x}_0)||_2,
\] (14)

\[C = \arg \min_i r_i.
\] (15)

where \( r_i \) is called residual factor of \( i \)-th person.

\( \text{B. Authentication algorithm with protected templates} \)

Next, we replace original templates in the above discussion with protected templates to show a new property. The solution of the \( l^2 \)-norm minimization problem is represented as
\[
x_0 = \arg \min_{x} ||x||_2 \quad \text{subject to} \quad y = D x
\] (16)

The square error between a protected query and training templates is represented as
\[
E_2 = ||\hat{y} - \hat{D} \hat{x}_0||_2^2. \quad \text{(17)}
\]

From \( \frac{\partial E_2}{\partial \hat{x}_0} = 0 \), \( \hat{x}_0 \) which provides the minimum square error in eq. (17) is represented by
\[
\hat{x}_0 = (D^* D)^{-1} D^* \hat{y}.
\] (18)

In addition, the property 2 in eq. (9), \( D^* D \) and \( D^* \hat{y} \) can be also given by
\[
D^* D = D^* D, \quad D^* \hat{y} = D^* y.
\] (19)

Therefore, the relation \( \hat{x}_0 = \hat{x}_0 \) is satisfied. That is, the unitary transform-based templates give the same results as in original templates, which is the property 4.

C. Reissuing of the protected template

This scheme can be applied repeatedly with a different parameter \( H_{p'} \), as below:
\[
\hat{f}_1' = (A^{-1}H_{p'} A)(A^{-1}H_p A_f) = A^{-1}H_{p'} A_f.
\] (20)

where \( H_{p'} = H_{p} \). The protected template \( \hat{f}_1 \) can be reissued as the new template \( \hat{f}_1' \) with the parameter \( H_{p'} \) by simply repeating the same protection scheme. In the authentication system, the result of the templates \( \hat{f}_1' \) is also equal to that of the original templates in \( l^2 \)-norm minimization problem.

4. EXPERIMENTAL RESULTS

First, the proposed scheme is applied to face recognition experiments. Furthermore, the proposed scheme is discussed about the security analysis and compared with the random orthogonal transformation [5].

4.1. Database

We use The Extended Yale Face Database B [21] that consists of \( \mathcal{24} \times \mathcal{24} \) frontal facet images of \( \mathcal{38} \) persons. Also, \( \mathcal{192} \times \mathcal{168} \) pixel images are captured various illumination condition. 64 images for each person are divided into half randomly for training samples and queries.

Here, DFT is used as an unitary transformation to generate protected templates, where \( \theta_p \in \{ \frac{\pi}{4}, -\frac{\pi}{4} \} \).

4.2. Results and Discussion

A. Face recognition experiment

The proposed protection is applied to templates generated by the down-sampling method [7] and the random projection method [22]. The down-sampling method divides an image into non-overlapped blocks and then calculates the mean value in each block. Also, the random projection method transforms a vector into the dimension reduced vector by a random matrix with a standard normal distribution.
Figure 2 shows a template example and the protected template generated by proposed scheme. From Fig.2 the protected template has no visual information, while the template is still visible. As shown in Fig 3 (b), the template has no visual information before applying the proposed protection to it. The protected template in Fig.3 (c) was generated by the proposed scheme.

In order to confirm the effectiveness of the proposed scheme, Receiver Operating Characteristic (ROC) curves were plotted as shown in Fig.4, according to the relation of a residual factor $r_i$ and a threshold value, $\tau$:

$$\text{if } r_i \leq \tau \text{ then accept; else reject.}$$  \hspace{1cm} (21)  

In the Fig4, True positive rate is the acceptance rate of the correct person. Also, False positive rate is the acceptance rate of people that are different from the query person. From Fig.4, it is shown that the use of the proposed scheme provides the same performance as that of the original templates when a common secret key is used for both query and training templates. That is, there is no degradation of recognition performance in solving the problem of $\ell$-norm minimization. On the other hand, when different secret keys are used for queries and training templates respectively, the true positive rate approximately equals the false positive rate. The results mean that the cross-matching performance is good.

B. Security Analysis

Security analysis for Brute-Force Attack

The key of the proposed scheme is a phase vector $\theta_p$. The key space of the phase vector $\theta_p$ has to meet $\theta_p(k) = 2\pi - \theta_p(N - k)$, $k = 1, ..., \left\lfloor \frac{N}{2} \right\rfloor$. Therefore, the key space is $\mathbb{L}^{\left\lfloor \frac{N}{2} \right\rfloor}$. In the experiments, the length $N$ of the template becomes 1254 and the number $L$ of elements becomes 2. The key space of protection in the experiments is $2^{\left\lfloor \frac{1254}{2} \right\rfloor} \approx 2^{626}$. This key space is larger than the key space of 256-bit encryption. Thus, this scheme has a large key space enough to prevent Brute-Force Attack.

Security analysis for Diversity

C. Comparing with the random orthonormal transformation

The DFT-based protection is compared with the random orthonormal transformation(ROT) [5]. The ROT is the scheme that protects templates by an orthonormal matrix generated by using the Gram-Schmidt method. Furthermore, the calculation order for generation the random orthonormal matrix from an pseudo-random matrix of the size $N \times N$ is $O(N^3)$ at least and the calculation order for the product of the random orthonormal matrix and a feature vector is $O(N^2)$. Thus, the calculation order of the protected template generation based on the ROT is $O(N^3)$. In contrast, the procedure of the protection by the proposed scheme of FFT(IFTF) and the product of a matrix $H_r$ and a feature vector transformed by FFT. The calculation order of $N$ point FFT(IFTF) is $O(N \log N)$ and for the product of the diagonal matrix of the size $N \times N$ and a vector of the length $N$ is $O(N)$. Therefore, the calculation order of the proposed scheme is $O(N \log N)$. Thus, the protection of the proposed scheme is faster than that of ROT.

5. CONCLUSIONS

This paper considered some useful properties of the unitary transform-based template protection and proposed a DFT-based one. It was shown that the unitary transform-based template protection does not affect not only the Euclidean distance but also the solution of the $\ell$-norm minimization. The proposed scheme was also applied to face recognition experiments to verify the effectiveness of the proposed one.
We confirmed that the proposed scheme has the sufficient performance for the security. Finally, we compared with the ROT method and demonstrated that the proposed scheme is faster than the ROT method.

6. ACKNOWLEDGMENT
This research was partly supported by Grant-in-Aid for Research on Priority Areas, Tokyo Metropolitan University, "Research on social big data."

REFERENCES


