UNITARY TRANSFORM-BASED TEMPLATE PROTECTION AND ITS PROPERTIES

Ibuki NAKAMURA[1], *Yoshihide TONOMURA*[2], *and Hitoshi KIYA*[1]

[1]Tokyo Metropolitan University, Hino, Tokyo 191-0065, Japan
[2]NTT 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 template protection schemes proposed in literatures can be broadly classified into two categories, feature transformation approach and biometric cryptosystem [1] [2]. The former [3] - [10] has a high degree of freedom for signal processing in the protected domain, compared to the latter [11] - [15]. Feature transform schemes can be further categorized as salting biometric [3] - [5] and non-invertible [6] - [10] transforms.

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 $\mathbf{p}_i$ as a user specific password or key. In the enrollment, a feature set $\mathbf{f}_i$, called a template is extracted from each biometric training sample, and then a transform function $\mathrm{T}(\cdot)$ is applied to the template to generate a protected template $\hat{\mathbf{f}}=\mathrm{T}(\mathbf{f}_i, \mathbf{p}_i)$. Next, only the protected template is stored into a database. The user i receives the parameter $\mathbf{p}_i$ from the enrollment system. On the other hand, in the authentication, the user i gives the parameter $\mathbf{p}_i$

978-0-9928626-3-3/15/$31.00 ©2015 IEEE

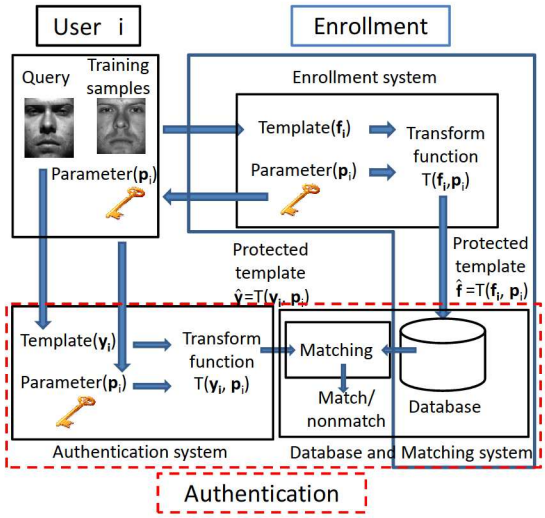


Fig. 1. Biometric authentication system

to the system and the same transform function T(·) is applied to a query feature $\mathbf{y}_i$. Finally the transformed query $T(\mathbf{y}_i, \mathbf{p}_i)$ is directly matched against the database.

The purpose of the paper is to consider the transform function in this system. In particular, some properties of the unitary transform-based template protection are discussed and a DFT-based template protection scheme is proposed as one of unitary transform schemes.

2.2. Template Protection

An ideal biometric template protection scheme should have the following four properties [1].

1. Performance: the biometric template protection scheme should not degrade the recognition performance of the biometric system.
2. Revocability: it should be possible to revoke a compromised template and generate a new one based on the same biometric data.
3. Security: it must be computationally hard to obtain the original biometric template from the secure template.
4. Diversity: the secure template must not allow cross-matching across databases.

We will evaluate the unitary transform-based template protection regarding these properties.

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

Generally, the template $\mathbf{f}_i \in \mathbb{R}^N$ is protected by a unitary matrix having randomness with a parameter $\mathbf{p}_i$, $\mathbf{Q}_p \in \mathbb{R}^{N\times N}$ as

$$\hat{\mathbf{F}} = T(\mathbf{f}_i, \mathbf{p}_i) = \mathbf{Q}_p \mathbf{f}_i, \tag{1}$$

where $\hat{\mathbf{F}}$ is the protected template. A lot of generation schemes of $\mathbf{Q}_p$ 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 $\mathbf{Q}_p$ [5]. However, generally, the conventional schemes are computationally expensive.

B. DFT-based template protection

DFT is applied to each template $\mathbf{f}_i = [f_i(0), f_i(1)..., f_i(N-1)]^T$, $i = 1, 2, ..., K$

$$F_i(k) = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} f_i(n) \cdot W_N^{nk}, \ k = 0, 1, ..., N-1 \tag{2}$$

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

$$\mathbf{F}_i = \mathbf{A}\mathbf{f}_i, \tag{3}$$

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

$$H_p(k,k) = e^{j\theta_p(k)}, \ k = 0, 1, ..., N-1. \tag{4}$$

Note that $\mathbf{H}_p$ satisfies

$$\mathbf{H}_p^* \mathbf{H}_p = \mathbf{I}, \tag{5}$$

where $[\cdots]^*$ and I mean the Hermitian transpose operation and the identity matrix respectively. Then, $\mathbf{H}_p$ is multiplied to $\mathbf{F}_i$ as

$$\hat{\mathbf{F}}_i = \mathbf{H}_p \mathbf{F}_i = \mathbf{H}_p \mathbf{A} \mathbf{f}_i. \tag{6}$$

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

$$\mathbf{Q}_p = \mathbf{H}_p \mathbf{A}. \tag{7}$$

Note that $\mathbf{H}_p\mathbf{A}$ is also a unitary matrix as well as $\mathbf{A}$. It is possible to obtain a protected template with real numbers by applying with inverse DFT:

$$\hat{\mathbf{f}}_i = \mathbf{A}^{-1} \hat{\mathbf{F}}_i = \mathbf{A}^{-1} \mathbf{H}_p \mathbf{A} \mathbf{f}_i, \tag{8}$$

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

Property 1 : Conservation of the Euclidean distances.
$\|\mathbf{f}_i - \mathbf{f}_j\|^2 = \|\hat{\mathbf{f}}_i - \hat{\mathbf{f}}_j\|^2$

Property 2 : Conservation of inner products.
$\mathbf{f}_i \cdot \mathbf{f}_j = \hat{\mathbf{f}}_i \cdot \hat{\mathbf{f}}_j$

Property 3 : Conservation of correlation coefficients.
$\frac{\|\mathbf{f}_i - \bar{\mathbf{f}}_i\| \|\mathbf{f}_j - \bar{\mathbf{f}}_j\|}{\sqrt{\|\mathbf{f}_j - \mathbf{f}_j\|^2} \sqrt{\|\mathbf{f}_j - \mathbf{f}_j\|^2}} = \frac{\|\hat{\mathbf{f}}_i - \bar{\hat{\mathbf{f}}}_i\| \|\hat{\mathbf{f}}_j - \bar{\hat{\mathbf{f}}}_j\|}{\sqrt{\|\hat{\mathbf{f}}_i - \hat{\mathbf{f}}_i\|^2} \sqrt{\|\hat{\mathbf{f}}_j - \hat{\mathbf{f}}_j\|^2}}$

The property 2 is provided by

$$\begin{aligned}\hat{\mathbf{f}}_i^*\hat{\mathbf{f}}_i &= (\mathbf{A}^{-1}\mathbf{H}_p\mathbf{A}\mathbf{f}_i)^*(\mathbf{A}^{-1}\mathbf{H}_p\mathbf{A}\mathbf{f}_i)\\ &= (\mathbf{f}_i^*\mathbf{A}\mathbf{H}_p^*\{\mathbf{A}^{-1}\}^*)(\mathbf{A}^{-1}\mathbf{H}_p\mathbf{A}\mathbf{f}_i)\\ &= (\mathbf{f}_i^*\mathbf{A}^{-1}\mathbf{H}_p^*\mathbf{A})(\mathbf{A}^{-1}\mathbf{H}_p\mathbf{A}\mathbf{f}_i) = \mathbf{f}_i^*\mathbf{f}_i. \end{aligned} \quad (9)$$

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 property is shown.

A.Authentication algorithm

First, $\mathbf{f}_{i,m_i}$ is defined as the m_i-th template for the i-th person where $m_i = 1, 2, ..., M_i$. For the i-th registered person among K registered persons, the set of M_i training templates is given by $\mathbf{D}_i = [\mathbf{f}_{i,1}, \mathbf{f}_{i,2}, ..., \mathbf{f}_{i,M_i}]$. Let us assume that $\mathbf{y}$, 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:

$$\mathbf{y} = \mathbf{f}_{i,1}x_{i,1} + \mathbf{f}_{i,2}x_{i,2} + ... + \mathbf{f}_{i,M_i}x_{i,M_i} = \mathbf{D}_i\mathbf{x}_i, \quad (10)$$

where $x_{i,j}$ is a coefficient value. Therefore, with all templates of K registered persons, $\mathbf{y}$ can be represented as

$$\mathbf{y} = \mathbf{D}_1\mathbf{0} + ... + \mathbf{D}_{i-1}\mathbf{0} + \mathbf{D}_i\mathbf{x}_i + \mathbf{D}_{i+1}\mathbf{0} + ... + \mathbf{D}_K\mathbf{0} = \mathbf{D}\mathbf{x}_0, \quad (11)$$

where $\mathbf{D} = [\mathbf{D}_1, \mathbf{D}_2, ..., \mathbf{D}_K]$, $\mathbf{x}_0 = [\mathbf{0}^T, ..., \mathbf{0}^T, \mathbf{x}_i^T, \mathbf{0}^T, ..., \mathbf{0}^T]^T$. To identify the i-th person, the l^2-norm minimization problem of eq.(11) is carried out as

$$\tilde{\mathbf{x}}_0 = \arg\min_{\mathbf{x}} ||\mathbf{x}||_2 \quad subject\ to \quad \mathbf{y} = \mathbf{D}\mathbf{x}. \quad (12)$$

By solving eq.(12), an approximate solution $\tilde{\mathbf{x}}_0$ is obtained as $\tilde{\mathbf{x}}_0 = [\tilde{\mathbf{x}}_1^T, \tilde{\mathbf{x}}_2^T, ..., \tilde{\mathbf{x}}_i^T, ..., \tilde{\mathbf{x}}_K^T]^T$. $\tilde{\mathbf{x}}_0$ is used to authenticate a person C. We define the function $\delta_i(\cdot)$ that replaces the coefficients with zeros except for those of the i-th person:

$$\delta_i(\tilde{\mathbf{x}}_0) = [\mathbf{0}^T, ..., \mathbf{0}^T, \tilde{\mathbf{x}}_i^T, \mathbf{0}^T, ..., \mathbf{0}^T]^T. \quad (13)$$

Substituting $\delta_i(\tilde{\mathbf{x}}_0)$ into $\mathbf{x}_i$ in eq.(10), the person C is estimated by

$$r_i = ||\mathbf{y} - \mathbf{D}\delta_i(\tilde{\mathbf{x}}_0)||_2, \quad (14)$$

$$C = \arg\min_i r_i, \quad (15)$$

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

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

$$\tilde{\mathbf{x}}_0' = \arg\min_{\mathbf{x}} ||\mathbf{x}||_2 \quad subject\ to \quad \hat{\mathbf{y}} = \hat{\mathbf{D}}\mathbf{x} \quad (16)$$

The square error between a protected query and training templates is represented as

$$\mathbf{E}_2 = ||\hat{\mathbf{y}} - \hat{\mathbf{D}}\tilde{\mathbf{x}}_0'||^2. \quad (17)$$

From $\frac{d\mathbf{E}_2}{d\tilde{\mathbf{x}}_0'} = 0$, $\tilde{\mathbf{x}}_0'$ which provides the minimum square error in eq.(17), is represented by

$$\tilde{\mathbf{x}'}_0 = (\hat{\mathbf{D}}^*\hat{\mathbf{D}})^{-1}\hat{\mathbf{D}}^*\hat{\mathbf{y}}. \quad (18)$$

In addition, from the property 2 in eq.(9), $\hat{\mathbf{D}}^*\hat{\mathbf{D}}$ and $\hat{\mathbf{D}}^*\hat{\mathbf{y}}$ can be also given by

$$\hat{\mathbf{D}}^*\hat{\mathbf{D}} = \mathbf{D}^*\mathbf{D}, \ \hat{\mathbf{D}}^*\hat{\mathbf{y}} = \mathbf{D}^*\mathbf{y}. \quad (19)$$

Therefore, the relation $\tilde{\mathbf{x}}_0 = \tilde{\mathbf{x}}_0'$ 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 $\mathbf{H}_{p_i'}$ as below.

$$\begin{aligned}\hat{\mathbf{f}}_i' &= (\mathbf{A}^{-1}\mathbf{H}_{p_i'}\mathbf{A})(\mathbf{A}^{-1}\mathbf{H}_{p_i}\mathbf{A}\mathbf{f}_i)\\ &= \mathbf{A}^{-1}\mathbf{H}_{p2_i}\mathbf{A}\mathbf{f}_i, \end{aligned} \quad (20)$$

where $\mathbf{H}_{p2_i} = \mathbf{H}_{p_i'}\mathbf{H}_{p_i}$. The protected template $\hat{\mathbf{f}}_i$ can be reissued as the new template $\hat{\mathbf{f}}_i'$ with the parameter $\mathbf{H}_{p2_i}$ by simply repeating the same protection scheme. In the authentication system, the result of the templates $\hat{\mathbf{f}}_i'$ 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 orthonormal transformation [5].

4.1. Database

We use The Extended Yale Face Database B [21] that consists of 2432 frontal facial images of 38 persons. Also, 192×168-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 $\boldsymbol{\theta}_p \in \{\frac{\pi}{2}, -\frac{\pi}{2}\}$.

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.

(a)Original (b)Template (c)Protected template

Fig. 2. An example of the down-sampling method

(a)Original (b)Template (c)Protected template

Fig. 3. An example of the random projection method

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, τ:

$$if\ r_i \leq \tau\ then\ accept;\ else\ reject. \tag{21}$$

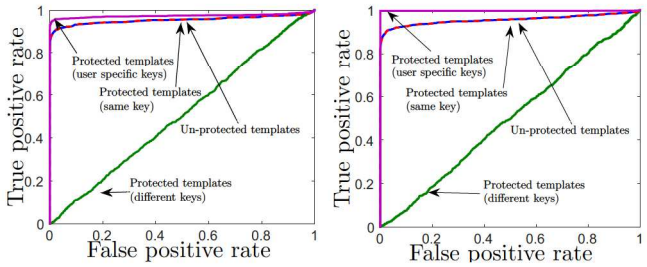
In the Fig4, True positive rate is the acceptance rate of the correct person. Also, False positive rate is the acceptance rate of people that are different from the query person. From Fig.4, it is shown that the use of the proposed scheme provides the same performance as that of the original templates 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 l^2-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 $\boldsymbol{\theta}_p$. The key space of the phase vector $\boldsymbol{\theta}_p$ depends on the length of the template, N and the number of elements, L. If real number templates are required, $\boldsymbol{\theta}_p$ has to meet $\theta_p(k) = 2\pi - \theta_p(N-k)$, $k = 1, ..., \lfloor \frac{N-1}{2} \rfloor$. Therefore, the key space is $L^{\lfloor \frac{N-1}{2} \rfloor}$. 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 $2^{\lfloor \frac{1254-1}{2} \rfloor} = 2^{626}$. 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



(a) down-sampling (b) random projection

Fig. 4. ROC curves(Templates with 1254 dimensions)

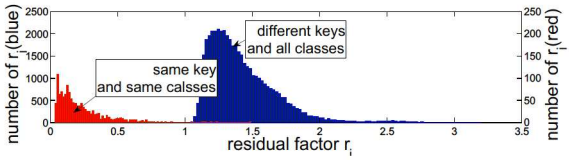


Fig. 5. Cross-matching evaluation of the proposed scheme with templates extracted by the random projection method

The cross-matching performance of the proposed scheme is evaluated. Fig.5 shows the relation between residual factor r_i and the number of r_i, where same classes means same persons. Note that there is almost no overlap between the red distribution and the blue one. Therefore, the proposed scheme has the sufficient performance for avoiding the cross-matching.

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(IFFT) and the product of a matrix H_p and a feature vector transformed by FFT. The calculation order of N point FFT(IFFT) is $O(NlogN)$ 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 $O(NlogN)$. 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 l^2-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

[1] A.K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," EURASIP J. Adv. Signal Processing, vol.2008, no.579416, Jan. 2008.

[2] C. Rathgeb, and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," EURASIP J. Information Security, vol.2011, no.1, pp.1-25, 2011.

[3] A. Goh, A. B. J. Teoh and D. C. L. Ngo, "Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs," IEEE Trans. Pattern Anal Mach Intell, vol.28, no.12, pp.1892-1901, Dec 2006.

[4] S. Marios, B. V. K. Vijaya Kumar, and P. K. Khosla, "Cancelable biometric filters for face recognition," in Proc. of the 17th International Conference on Pattern recognition, vol.3, pp.922-925, 2004.

[5] Y. Wang and K. Plataniotis "Face based biometric authentication with changeable and privacy preservable templates," in Proc. IEEE Biometrics Symposium, pp.1-6 2007.

[6] J.K. Pillai, V.M. Patel, R. Chellappa, and N.K. Ratha, "Secure and robust iris recognition using random projections and sparse representation," IEEE Trans. Pattern Analysis and Machine Intelligence, vol.33, no.9, pp.1877-1893, Sep. 2011.

[7] J. Wright, A. Yang, A. Ganesh, S. Sastry, and Y. Ma, "Robust face recognition via sparse representation," IEEE Trans. Pattern Analysis and Machine Intelligence, vol.31, no.2, Feb. 2009.

[8] Y. Muraki, M. Furukawa, M. Fujiyoshi, Y. Tonomura, and H. Kiya, "A Compressible Template Protection Scheme for Face Recognition Based on Sparse Representation," in Proc. European Signal Processing Conference, no.TH-P5, Sep. 2014.

[9] M. Furukawa, Y. Muraki, M. Fujiyoshi, and H. Kiya, " A Secure Face Recognition Scheme Using Noisy Images Based on Kernel Sparse Representation, " in Proc. APSIPA Annual Summit and Conference, no.OS.20-IVM.9-4, October, 2013.

[10] A.B.J. Teoh and C.T. Yuang, "Cancelable biometrics realization with multispace random projections," IEEE Trans. Sys., Man, and Cybernetics Part B: Cybernetics, vol.37, pp.1096-1106, Mon. 2007.

[11] A. Juels, and M. Wattenberg, "A fuzzy commitment scheme," in Proc. ACM conference on Computer and communications security, no.9, pp.28-36, 1999.

[12] Y.C. Feng, P.C. Yuen, and A.K. Jain, "A hybrid approach for generating secure and discriminating face template," IEEE Trans. Info. Forensic Security, vol.5, pp.103-117, Mar. 2010.

[13] U. ludag, S. Pankanti, S. Prabhakar, and K. Jain. "Biometric cryptosystems: issues and challenges," Proceedings of the IEEE, vol.92, no.6, pp.948-960, Jun, 2004.

[14] E. Maiorana, P. Campisi, A. Neri, "Iris template protection using a digital modulation paradigm," in Proc. IEEE International Conference on Acoustics, Speech and Signal Processing, pp.3787-3791, 2014

[15] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," IEEE Trans. Pattern Analysis and Machine Intelligence, vol.29, no.4, pp.561-572, Apr. 2011.

[16] Y. Muraki, M. Furukawa, M. Fujiyoshi, and H. Kiya, "Robustness Analysis of Cancelable Biometrics Systems in Terms of Visual Recognizability," in Proc. International Workshop on Advanced Image Technology, no.A2-145, pp.24-27, Jan. 2014.

[17] S. Jassim, H.Al-assam, H.Sellahewa, "Improving performance and security of biometrics using efficient and stable random projection techniques," in Proc. International Symposium on Image and Signal Processing and Analysis, pp. 556-561, 2009.

[18] I. Ito and H. Kiya, "One-Time Key Based Phase Scrambling for Phase-Only Correlation between Visually Protected Images," EURASIP J. Information Security, vol.2009, no.841045, Jan. 2010.

[19] I. Ito and H. Kiya, "A new class of image registration for guaranteeing secure data management"in Proc. IEEE International Conference on Image Processing, no.MA-PA.5, pp.269-272, Oct. , 2008.

[20] I. Ito and H. Kiya, " Phase Scrambling for Blind Image Matching, " in Proc. IEEE International Conference on Acoustics, Speech and Signal Processing, no.IFS-P2.9, pp.1521-1524, April, 2009.

[21] A.S. Georghiades, P.N. Belhumeur, and D.J. Kriegman, "From few to many: Illumination cone models for face recognition under variable lighting and pose," IEEE Trans. Pattern Analysis and Machine Intelligence, vol.23, no.6, pp.643-660, Jun. 2001.

[22] S. Kaski, "Dimensionality Reduction by Random Mapping," in Proc. IEEE Int'l Joint Conf. Neural Networks, vol. 1, pp. 413-418, 1998.