IEICE TRANS. INF. & SYST., VOL.E99–D, NO.1 JANUARY 2016

PAPER Special Section on Enriched Multimedia—Creation of a New Society through Value-added Multimedia Content—

Unitary Transform-Based Template Protection and Its Application to l^2-norm Minimization Problems

Ibuki NAKAMURA[†a)], ***Nonmember***, **Yoshihide TONOMURA**[††b)], ***Member***, ***and*** **Hitoshi KIYA**[†c)], ***Fellow***

SUMMARY 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 study considers some properties of the unitary (including orthogonal) 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 study, 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.

key words: *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 study. 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. In addition, Security and privacy evaluation metrics for biometric template protection are now under standardization process as ISO/IEC WD 30136 [1]. Furthermore, it is pursued to fix the definition of metrics for measuring irreversibility, secrecy, and unlinkability and to devise methods for empirical evaluation of these metrics.

Manuscript received March 26, 2015.
Manuscript revised July 31, 2015.
Manuscript publicized October 21, 2015.

[†]The authors are with the Graduate School of System Design, Tokyo Metropolitan University, Hino-shi, 191–0065 Japan.
[††]The author is with NTT Network Innovation Laboratories, NTT Corporation, Yokosuka-shi, 239–0847 Japan.
a) E-mail: nakamura-ibuki@ed.tmu.ac.jp
b) E-mail: tonomura.yoshihide@lab.ntt.co.jp
c) E-mail: kiya@tmu.ac.jp

DOI: 10.1587/transinf.2015MUP0007

The template protection schemes proposed in literatures can be broadly classified into two categories, feature transformation approach and biometric cryptosystem [2], [3]. The former [4]–[16] has a high degree of freedom for signal processing in the protected domain, compared to the latter [17]–[21]. Feature transform schemes can be further categorized as salting biometric [4]–[8] and non-invertible [9]–[16] transforms.

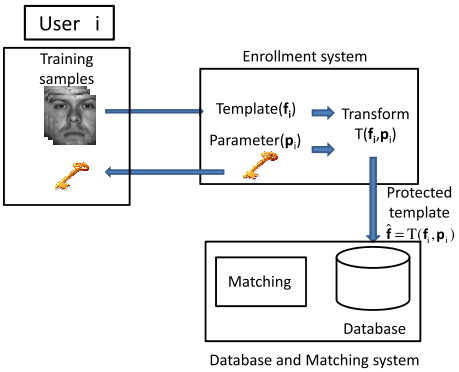
The unitary transform-based template protection in this study corresponds to a salting biometrics transformation in the feature transformation approach. In generally, non-invertible transforms are preferable in terms of security, but it is difficult to guarantee no degradation of recognition performance in a deterministic way. In addition, it has been pointed out that there are some risks 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 [14], [22]. Also, a template protection scheme with perfect security was proposed as a feature transform scheme [23], [24]. However the scheme focuses on only correlation-based matching. On the other hand, the unitary transform-based protection provides a few good properties, although parameters have to be securely managed as secret keys. For example, the Euclidean distance between the protected templates is equal to that between original ones [8].

This study 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.

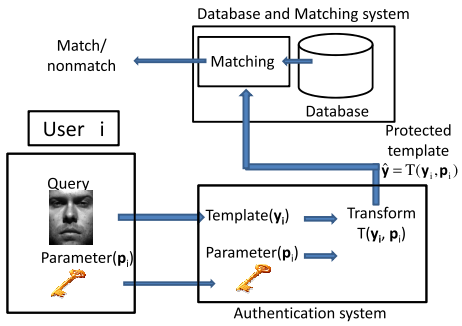
2. Preparation

2.1 Biometric Authentication System

In this study, 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



(a)Enrollment system



(b)Authentication system

Fig. 1 Biometric authentication system

to generate a protected template $\hat{\mathbf{f}}$=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 $\mathbf{p}_i$ 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 study 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 [2].

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 Scheme and Its Properties

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

3.1 Generation of Protected Templates

A. Unitary Transform-Based Template Protection

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

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

where $\hat{\mathbf{F}}_i$ is the protected template. A lot of generation schemes of $\mathbf{Q}_{p_i}$ have been studied to generate unitary or orthogonal random matrices [5], [6], [8]. For example, the Gram-Schmidt method is applied to a pseudo-random matrix to generate $\mathbf{Q}_{p_i}$ [8]. However, generally, the conventional schemes are computationally expensive [5], [6].

B. DFT-Based Template Protection

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

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

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

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

where $\mathbf{F}_i = [F_i(0), F_i(1)\ldots, F_i(N-1)]$. Next, N phase values $\theta_{p_i}(k) \in \{\frac{2\pi l}{L} + \alpha | l = 0, 1, \ldots, L-1, \alpha \in \mathbb{R}\}$, $k = 0, 1, \ldots, N-1$, are randomly generated by using a pseudo random generator [25], [26] and the phase vector $\boldsymbol{\theta}_{p_i}$ is used to define a diagonal matrix $\mathbf{H}_{p_i}$:

$$H_{p_i}(k,k) = e^{j\theta_{p_i}(k)},\ k = 0, 1, \ldots, N-1. \tag{4}$$

Note that the random phase matrix $\mathbf{H}_{p_i}$ satisfies

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

where $[\cdot]^*$ and $\mathbf{I}$ mean the Hermitian transpose operation and the identity matrix respectively, and $\boldsymbol{\theta}_{p_i}$ corresponds to $\mathbf{p}_i$ in Fig. 1. Then, $\mathbf{H}_{p_i}$ is multiplied to $\mathbf{F}_i$ as

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

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

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

Note that $\mathbf{H}_{p_i}\mathbf{A}$ is also a unitary matrix as well as $\mathbf{A}$, where $\mathbf{A}$ is a fixed unitary matrix and $\mathbf{H}_{p_i}$ is a diagonal one with randomness. Therefore, $\mathbf{H}_{p_i}$ can be easily designed, compared to the direct design of $\mathbf{Q}_{p_i}$. In addition, the FFT is available for the transformation. It is also possible to obtain a protected template with real numbers by calculating the inverse DFT:

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

where $\boldsymbol{\theta}_{p_i}$ has to satisfy the relation $\theta_{p_i}(k) = 2\pi - \theta_{p_i}(N-k)$, $k = 1, \ldots, \lfloor \frac{N-1}{2} \rfloor$ if we want real values as $\hat{\mathbf{f}}_i \in \mathbb{R}^N$. As with Eq. (1), Eq. (8) can be also expressed by

$$\hat{\mathbf{f}}_i = T(\mathbf{f}_i, \mathbf{p}_i). \tag{9}$$

The random phase matrix $\mathbf{H}_{p_i}$ in Eq. (4) is an example of random unitary matrices for the DFT-based template protection. The random phase matrix remains the power spectrum as the original one. To avoid this situation, for example, a random permutation matrix that permutes the order of elements of a vector, can be used as $\mathbf{H}_{p_i}$. Equation (10) is an example for N = 4.

$$\mathbf{H}_{p_i} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \tag{10}$$

Note that the random permutation matrix is a unitary (orthogonal) matrix.

The proposed protection is one of the unitary transform-based template protection. Therefore, the protected templates have the following properties under $\mathbf{p}_i = \mathbf{p}_j$ [6].

Property 1 : Conservation of the Euclidean distances.

$$\sqrt{\textstyle\sum_k (f_i(k) - f_j(k))^2} = \sqrt{\textstyle\sum_k (\hat{f}_i(k) - \hat{f}_j(k))^2}$$

Property 2 : Conservation of inner products.

$$\textstyle\sum_k f_i^*(k) f_j(k) = \sum_k \hat{f}_i^*(k)\hat{f}_j(k)$$

Property 3 : Conservation of correlation coefficients.

$$\frac{\sum_k (f_i(k)-\overline{f}_i)(f_j(k)-\overline{f}_j)}{\sqrt{\sum_k (f_i(k)-\overline{f}_i)^2}\sqrt{\sum_k (f_j(k)-\overline{f}_j)^2}} = \frac{\sum_k (\hat{f}_i(k)-\overline{\hat{f}}_i)(\hat{f}_j(k)-\overline{\hat{f}}_j)}{\sqrt{\sum_k (\hat{f}_i(k)-\overline{\hat{f}}_i)^2}\sqrt{\sum_k (\hat{f}_j(k)-\overline{\hat{f}}_j)^2}}$$

These properties may be expressed by vectors as

$$\mathbf{f}_i^*\mathbf{f}_j = \hat{\mathbf{f}}_i^*\hat{\mathbf{f}}_j \tag{11}$$

for the property 2.

The property 2 is provided by

$$\begin{aligned} \hat{\mathbf{f}}_i^*\hat{\mathbf{f}}_j &= (\mathbf{A}^{-1}\mathbf{H}_{p_i}\mathbf{A}\mathbf{f}_i)^*(\mathbf{A}^{-1}\mathbf{H}_{p_j}\mathbf{A}\mathbf{f}_j) \\ &= (\mathbf{f}_i^*\mathbf{A}\mathbf{H}_{p_i}^*\{\mathbf{A}^{-1}\}^*)(\mathbf{A}^{-1}\mathbf{H}_{p_j}\mathbf{A}\mathbf{f}_j) \\ &= (\mathbf{f}_i^*\mathbf{A}^{-1}\mathbf{H}_{p_i}^*\mathbf{A})(\mathbf{A}^{-1}\mathbf{H}_{p_j}\mathbf{A}\mathbf{f}_j) = \mathbf{f}_i^*\mathbf{f}_j. \end{aligned} \tag{12}$$

Also, the property 1 and 3 are obvious because they consist of inner products. In Sect. 3.2, another property will be given 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 as an l^2-norm minimization problem [9]–[15], and then 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 $m_i = 1, 2, \ldots, M_i$. For the i-th registered person among K registered persons, the set of M_i training templates is given by $\mathbf{D}_i = [\mathbf{f}_{i,1}, \mathbf{f}_{i,2}, \ldots, \mathbf{f}_{i,M_i}]$. 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:

$$\mathbf{y} = \mathbf{f}_{i,1}x_{i,1} + \mathbf{f}_{i,2}x_{i,2} + \ldots + \mathbf{f}_{i,M_i}x_{i,M_i} = \mathbf{D}_i\mathbf{x}_i, \tag{13}$$

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

$$\mathbf{y} = \mathbf{D}_1\mathbf{0} + \ldots + \mathbf{D}_{i-1}\mathbf{0} + \mathbf{D}_i\mathbf{x}_i + \mathbf{D}_{i+1}\mathbf{0} + \ldots + \mathbf{D}_K\mathbf{0} = \mathbf{D}\mathbf{x}_0, \tag{14}$$

where $\mathbf{D} = [\mathbf{D}_1, \mathbf{D}_2, \ldots, \mathbf{D}_K]$ and $\mathbf{x}_0 = [\mathbf{0}^T, \ldots, \mathbf{0}^T, \mathbf{x}_i^T, \mathbf{0}^T, \ldots, \mathbf{0}^T]^T$. To identify the i-th person, the l^2-norm minimization problem of Eq. (14) is carried out as

$$\tilde{\mathbf{x}}_0 = \arg\min_{\mathbf{x}} \|\mathbf{x}\|_2 \quad \textit{subject to} \quad \mathbf{y} = \mathbf{D}\mathbf{x}. \tag{15}$$

By solving Eq. (15), an approximate solution $\tilde{\mathbf{x}}_0$ is obtained as $\tilde{\mathbf{x}}_0 = [\tilde{\mathbf{x}}_1^T, \tilde{\mathbf{x}}_2^T, \ldots, \tilde{\mathbf{x}}_i^T, \ldots, \tilde{\mathbf{x}}_K^T]^T$. $\tilde{\mathbf{x}}_0$ 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:

$$\delta_i(\tilde{\mathbf{x}}_0) = [\mathbf{0}^T, \ldots, \mathbf{0}^T, \tilde{\mathbf{x}}_i^T, \mathbf{0}^T, \ldots, \mathbf{0}^T]^T. \tag{16}$$

Substituting $\delta_i(\tilde{\mathbf{x}}_0)$ into $\mathbf{x}_i$ in Eq. (13), the person C is estimated by

$$r_i = \|\mathbf{y} - \mathbf{D}\delta_i(\tilde{\mathbf{x}}_0)\|_2, \tag{17}$$

$$C = \arg\min_i r_i, \tag{18}$$

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

B. Authentication Algorithm with Protected Templates

Next, we replace original templates in the above discussion with templates protected by a common parameter $\mathbf{p}_i$ to show a new property. In this study, the parameter $\mathbf{p}_i$ is used for a templates set $\mathbf{D}$ or $\mathbf{D}_i$ globally as well as the conventional schemes [9], [10], [14], [15], although the entropy of the parameter $\mathbf{p}_i$ is reduced.

The solution of the l^2-norm minimization problem is represented as

$$\tilde{\mathbf{x}}_0' = \arg\min_{\mathbf{x}} \|\mathbf{x}\|_2 \quad \textit{subject to} \quad \hat{\mathbf{y}} = \hat{\mathbf{D}}\mathbf{x} \tag{19}$$

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

$$\mathbf{E}_2 = \|\hat{\mathbf{y}} - \hat{\mathbf{D}}\tilde{\mathbf{x}}'_0\|_2. \tag{20}$$

From $\frac{d\mathbf{E}_2}{d\tilde{\mathbf{x}}'_0} = 0$, $\tilde{\mathbf{x}}'_0$ which provides the minimum square error in Eq. (20), is represented by

$$\tilde{\mathbf{x}'}_0 = (\hat{\mathbf{D}}^*\hat{\mathbf{D}})^{-1}\hat{\mathbf{D}}^*\hat{\mathbf{y}}. \tag{21}$$

In addition, from the property 2 in Eq. (12), $\hat{\mathbf{D}}^*\hat{\mathbf{D}}$ and $\hat{\mathbf{D}}^*\hat{\mathbf{y}}$ can be also given by

$$\hat{\mathbf{D}}^*\hat{\mathbf{D}} = \mathbf{D}^*\mathbf{D},\ \hat{\mathbf{D}}^*\hat{\mathbf{y}} = \mathbf{D}^*\mathbf{y}. \tag{22}$$

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, that is the property 4

3.3 Reissue of Protected Templates

It was shown that the unitary transform-based template protection does not give any degradation of recognition performance in l^2-norm minimization problems in Sect. 3.2. This property enables to recursively generate protected templates without any performance degradation.

Equation (8) can be applied repeatedly with a different unitary transform $\mathbf{H}_{p'_i}$ as below.

$$\begin{aligned}\hat{\mathbf{f}}'_{p'_i} &= (\mathbf{A}^{-1}\mathbf{H}_{p'_i}\mathbf{A})(\mathbf{A}^{-1}\mathbf{H}_{p_i}\mathbf{A}\mathbf{f}_i)\\ &= \mathbf{A}^{-1}\mathbf{H}_{p'_{2i}}\mathbf{A}\mathbf{f}_i,\end{aligned} \tag{23}$$

where $\mathbf{H}_{p'_{2i}} = \mathbf{H}_{p'_i}\mathbf{H}_{p_i}$. The protected template $\hat{\mathbf{f}}_i$ can be reissued as a new template $\hat{\mathbf{f}}'_{p'_i}$ by simply repeating the same protection scheme. In the authentication system, the result of the templates $\hat{\mathbf{f}}'_{p'_i}$ is also equal to that of the original templates in l^2-norm minimization problems.

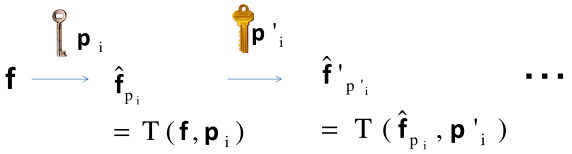
Figure 2 (a) shows the recursive parameter generation where $\hat{\mathbf{f}}_{p_i}$ is the protected template generated from a template $\mathbf{f}$ with a parameter $\mathbf{p}_i$, and $\hat{\mathbf{f}}'_{p'_i}$ is provided from $\hat{\mathbf{f}}_{p_i}$ with $\mathbf{p}'_i$ as,

$$\begin{aligned}\hat{\mathbf{f}}_{p'_i} &= T(\hat{\mathbf{f}}_{p_i}, \mathbf{p}'_i)\\ &= T(\mathbf{f}, \mathbf{p}'_{2i}),\end{aligned} \tag{24}$$

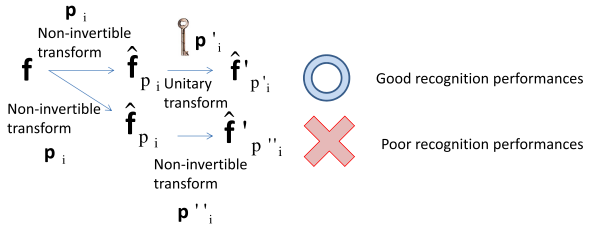
where $\mathbf{p}'_{2i}$ is the synthesis parameter of $\mathbf{p}_i$ and $\mathbf{p}'_i$. In the case of the DFT-based protection, from Eq. (23), the synthesis parameter $\boldsymbol{\theta}_{p'_{2i}}$ is given by

$$\boldsymbol{\theta}_{p'_{2i}} = \boldsymbol{\theta}_{p_i} + \boldsymbol{\theta}_{p'_i}. \tag{25}$$

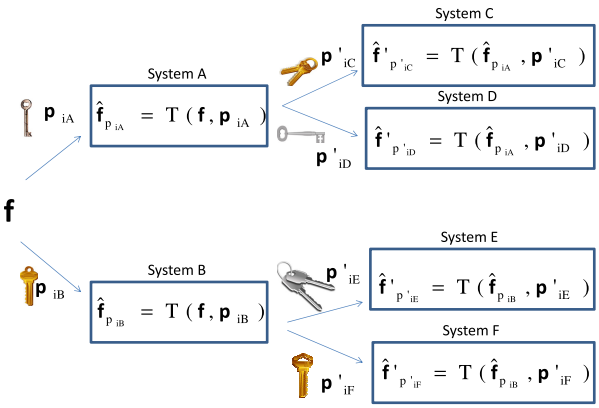
The unitary transform-based protection can be combined with a non-invertible transform as shown in Fig. 2 (b). In generally, the recursive use of a non-invertible transform degrades recognition performance. On the other hand, the proposed scheme enables to reissue templates protected by a non-invertible transform, without any performance degradation. The recognition performance of the doubly protected templates $\hat{\mathbf{f}}_{p'_i}$ is the same as that of $\hat{\mathbf{f}}_{p_i}$.



(a)Recursive parameter generation



(b)Combination with non-invertible protection



(c)Distributed management system

Fig. 2 Recursive parameter generation

Finally, we introduce a distributed management system in Fig. 2 (c). This system enables to manage a template with a number of parameters. Each protected template with a different parameter has the same recognition performance, while this management can decrease the damage for the leakage of some secret parameters.

4. Experimental Results and Evaluation

The proposed scheme is applied to face recognition experiments. Furthermore, it is evaluated for the reasonability of the security and compared with the Gram-Schmidt method [8].

4.1 Database

We use The Extended Yale Face Database B [27] that consists of 2432 frontal facial images with 192×168-pixels of 38 persons. 64 images for each person are divided into half

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

Fig. 3 An example of the down-sampling method

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

Fig. 4 An example of the random projection method

randomly for training samples and queries.

Here, the DFT is used as an unitary transformation to generate protected templates, where $\boldsymbol{\theta}_{p_i} \in \{\frac{\pi}{2}, -\frac{\pi}{2}\}$.

4.2 Results and Discussion

A. Face Recognition Experiment

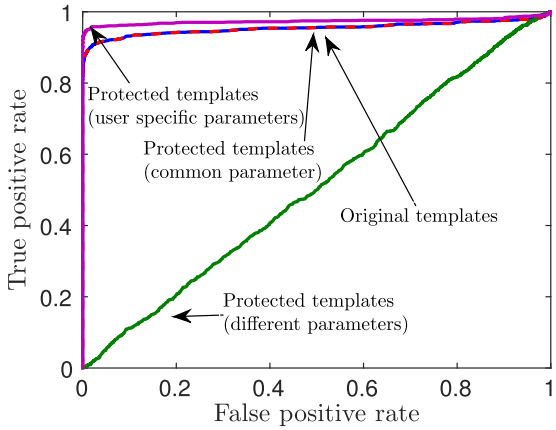
The proposed protection is applied to templates with 1254 dimensions generated by the down-sampling method [10] and the random projection method [28] respectively. The down-sampling method divides an image into non-overlapped blocks and then calculates the mean value in each block. Also, the random projection method, which is not a unitary transformation, transforms a vector into a dimension-reduced vector by a random matrix with a standard normal distribution.

Figures 3 and 4 show template examples and the protected templates generated by the proposed scheme. In Fig. 3, the protected template generated by the down-sampling method has no visual information, while the template is still visible. As shown in Fig. 4 (b), the template has no visual information before applying the proposed protection to it. The protected template in Fig. 4 (c) was generated by the proposed scheme.

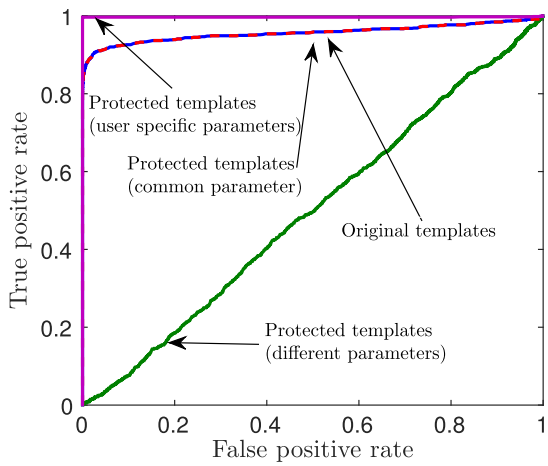
In order to confirm the effectiveness of the proposed scheme, Receiver Operating Characteristic (ROC) curves were plotted as shown in Fig. 5, according to the relation of a residual factor r_i and a threshold value, τ:

$$\textit{if } r_i \leq \tau \textit{ then accept; else reject.} \tag{26}$$

In Fig. 5, 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. 5, it is shown that the use of the proposed scheme provides the same performance as that of the original templates (non-protected templates) when a common secret parameter is used for all of queries and training templates. That is, there is no degradation of the recognition performance



(a) down-sampling



(b) random projection

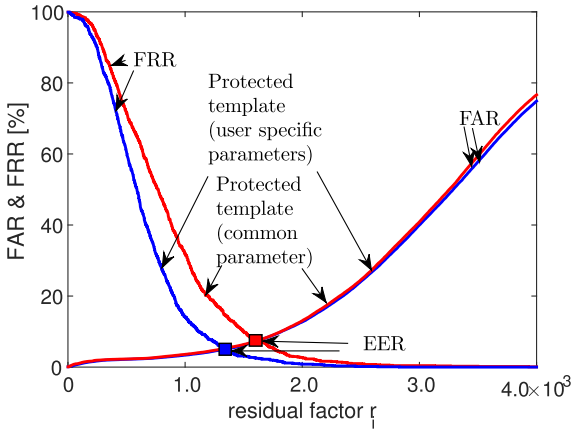
Fig. 5 ROC curves (Templates with 1254 dimensions)

in solving the problem of l^2-norm minimization. On the other hand, when different secret parameters among queries and training templates are used, the true positive rate approximately equals the false positive rate. The results mean that the cross-matching performance is reasonable. Furthermore, when user specific parameters are used for each person as Fig. 1, the recognition performance is improved due to its better cross-matching performance than that of original templates.

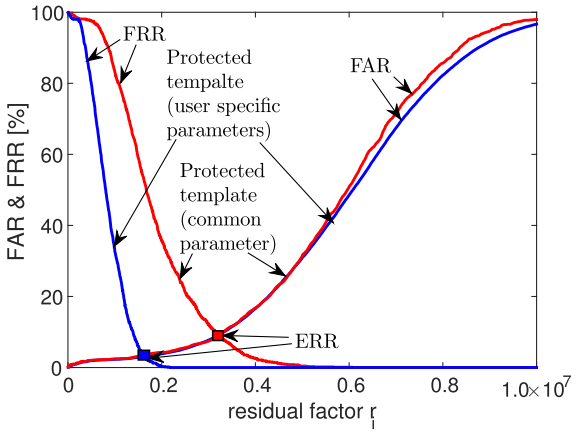
In Fig. 6, it is shown that the relation of FAR (False Accept Rate), FRR (False Reject Rate) and a residual factor, where FAR means the acceptance rate of the false person and FRR is the reject rate of false person. Furthermore, the intersection of FAR and FRR is called EER (Equal Error Rate) and EER is used to evaluate the recognition performance. Table 1 shows EER values of Fig. 6. The EER values for the user specific parameters is improved due to the improvements of the cross-matching performance compared to the use of a common parameter.

B. Comparing with the Random Projection Method

We compare the proposed scheme with the random



(a) down-sampling



(b) random projection

Fig. 6 FAR and FRR (Templates with 1254 dimensions)

Table 1 EER

	Down sampling	Random projection
common parameter	7.48%	9.21%
user specific parameters	5.02%	3.04%

projection method, which is a non-invertible transformation, in terms of the reissue of protected templates. As shown in Sect. 3.3, the proposed scheme can reissue protected templates without any performance degradation. However, the random projection method, which is not an unitary transformation, has not the property. We repeat applying the random projection method to confirm this point. First, to obtain a template $\mathbf{f}_i$ with 1254-dimensions from 32256-pixels image $\mathbf{g}_i$, the image is multiplied by a 1254×32256 matrix $\mathbf{R}_1$ which consists of random values and the Euclidean length of each column has been normalized to unity as.

$$\hat{\mathbf{f}}_i = \mathbf{R}_1 \mathbf{g}_i. \tag{27}$$

Then, random matrices with 1254×1254 size, $\mathbf{R}_2$ and $\mathbf{R}_3$ are also generated and used to generate the 2nd and the 3rd protected templates. Figure 7 shows the ROC curves in the random projection method. From Fig. 7, it is shown that it is different to avoid the degradation of the recognition

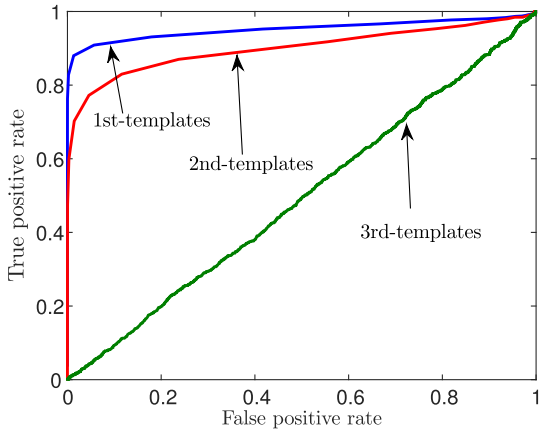


Fig. 7 ROC curves (the random projection method)

performance under the random projection method.

4.3 Evaluation

A. 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 dimension of the template, N and the number of elements, L. If real number templates are required, $\boldsymbol{\theta}_p$ has to meet $\theta_p(k) = 2\pi - \theta_p(N-k)$, $k = 1, \ldots, \lfloor \frac{N-1}{2} \rfloor$. 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, e.g. $\boldsymbol{\theta}_p \in \{\frac{\pi}{2}, -\frac{\pi}{2}\}$. The key space in the experiments is reduced to $2^{\lfloor \frac{1254-1}{2} \rfloor} = 2^{626}$. Also, the key space of the random permutation matrix is given as $(\lfloor \frac{N-1}{2} \rfloor)!$ when real number templates are used. Thus, the key space in the experiments is $(\lfloor \frac{1254-1}{2} \rfloor)! = 626!$. These key space are 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

The cross-matching performance of the proposed scheme is evaluated. Figure 8 shows the relation between residual factor r_i and the number of r_i, where same classes means that a query person is the same as one for training samples. 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.

Security Analysis for Irreversibility

We consider irreversibility that is difficulty to recover the original information from a protected template, in terms of resistance against recovery from parameter, from authentication result and from template respectively.

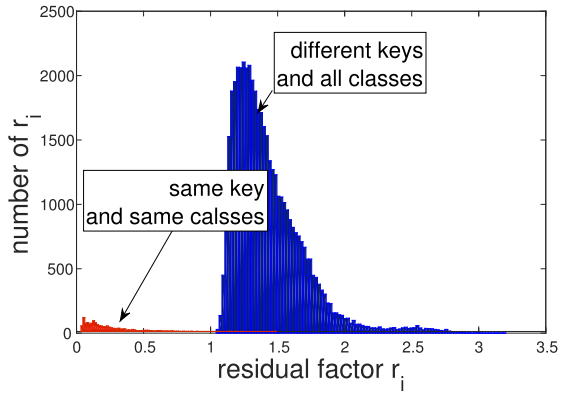


Fig. 8 Cross-matching evaluation of the proposed scheme with templates extracted by the random projection method

(1) Resistance against Recovery from Parameter

We assume that an attacker accesses only the parameter $\mathbf{p}_i$. The parameter $\mathbf{p}_i$ is uniformly random and independent from the original template $\mathbf{f}_i$. Thus, it is impossible to recover the template $\mathbf{f}_i$ from the parameter $\mathbf{p}_i$ without the protected template $\hat{\mathbf{f}}_i$. In addition, even if the attacker collects two or more different parameters, he can not recover $\mathbf{f}_i$ because the parameters does not have any information of $\mathbf{f}_i$.

(2) Resistance against Recovery from Authentication Result

we assume that an attacker accesses only authentication results, which include inner products in the authentication via l^2-norm minimization. In order to recover the original template $\mathbf{f}_i$, the attacker regards Eq. (21) as a simultaneous equation, where inner products of a protected query template with dimension N and M protected training templates with dimension N are calculated. This simultaneous equation consists of $NM + N + \lfloor \frac{N-1}{2} \rfloor$ variables and NM equations. Since the number of equations is less than the number of variables, the solution is underspecified. Therefore, the attacker can not estimate the original template from only authentication results.

(3) Resistance against Recovery from Template

We assume that an attacker accesses only protected templates. As described in Sect. 4.3 A, the proposed scheme has a large key space enough to prevent Brute-Force Attack on a random phase matrix or a random permutation matrix. However, the proposed scheme does not satisfy "perfect security" defined by Shannon [23], [29], as well as other protection schemes [5]–[16]. The use of schemes with perfect security is the most secure option. In addition, the entropy of the parameter $\mathbf{p}_i$ is generally reduced by applying $\mathbf{p}_i$ to a templates set, $\mathbf{D}$ or $\mathbf{D}_i$ globally. Many researchers have been seeking a trade-off between irreversibility and recognition performance as described in [30]–[32], because high recognition performance can be achieved only when the protected biometric reference retains all the discriminatory information contained in the original template. This study shows a new result, namely templates protected by a unitary transform can provide the same recognition performance in l^2-norm minimization as that of original templates, although the templates do not satisfy "perfect security". As far as we can see, any schemes with "perfect security" do not have this recognition performance.

Table 2 Calculation times

	Proposed scheme	Gram-Schmidt method
transformation and generation time	0.0007 [sec/template]	1.5153 [sec/template]
verification time	0.3774 [sec/query]	0.3872 [sec/query]

Table 3 The platform used in the experiment

Software	Processor	RAM
MATLAB R2015a	Intel Core i7-3540M 3.00GHz	8.0GB

B. Comparing with the Gram-Schmidt Method

The proposed DFT-based protection is compared with the Gram-Schmidt method [8] in terms of the calculation amount of the registration which consists of the transformation and the generation of $\mathbf{Q}_p$. The Gram-Schmidt method is the protection scheme that is based on an random orthogonal matrix generated by using the Gram-Schmidt orthogonalization. Furthermore, the calculation order for generation the orthogonal 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 orthogonal matrix and a feature vector is $O(N^2)$. Thus, the calculation order of the protected template generation based on the Gram-Schmidt method is $O(N^3)$. In contrast, the procedure of the proposed scheme consists of the FFT (IFFT) and the product of a diagonal matrix $\mathbf{H}_{p_i}$ and a template vector. 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 has lower calculation amount than that of the Gram-Schmidt method.

On the other hand, the calculation amount of the verification is almost the same, when a verification scheme is used in common and the dimension of templates is the same. Table 2 is represented about the experimental processing times of the transformation and the verification. Also, this experiment was carried out on platform in Table 3. It is shown that the proposed scheme is faster than Gram-Schmidt method in the transformation and the generation time.

C. Comparing with CIRF

The proposed scheme is compared with CIRF (correlation-invariant random filtering) [23], [24], which is based on the number theoretic transform (NTT) and a random filter. The similarities between both schemes are that matching operations are carried out in a transform domain and a random matrix is used securely to protect templates. By contrast,

the differences are that CIRF can satisfy the perfect security condition and focuses on correlation-based matching. In contrast, the proposed scheme has a high freedom degree of applicable authentication algorithms, because there is no restriction imposed by the use of a finite field. As a result, it can provide the same results in l^2-norm minimization problems as those of original templates.

5. Conclusions

This study 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 the proposed scheme with the Gram-Schmidt method and demonstrated that the proposed scheme has lower calculation amount than the Gram-Schmidt method.

References

[1] S. Rane, "Standardization of Biometric Template Protection," IEEE Multimedia Mag., vol.21, no.4, pp.94–99, Oct. 2014.
[2] A.K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," EURASIP J. Adv. Signal Processing, vol.2008, no.1, p.579416, Jan. 2008.
[3] 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.
[4] A.B.J. Teoh, A. Goh, 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.
[5] S. Jassim, H. Al-Assam, and H. Sellahewa, "Improving performance and security of biometrics using efficient and stable random projection techniques," Proc. of the 6th International Symposium on Image and Signal Processing and Analysis, ISPA '09, pp.556–561, 2009.
[6] H. Al-Assam, H. Sellahewa, and S. Jassim, "A lightweight approach for biometric template protection," SPIE Defense, Security, and Sensing. International Society for Optics and Photonics, 73510P-73510P-12, 2009.
[7] S. Marios, B.V.K. Vijaya Kumar, and P.K. Khosla, "Cancelable biometric filters for face recognition," Proc. 17th International Conference on ICPR 2004, vol.3, pp.922–925, 2004.
[8] Y. Wang and K.N. Plataniotis, "Face based biometric authentication with changeable and privacy preservable templates," Proc. IEEE Biometrics Symposium, pp.1–6, 2007.
[9] 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 Anal. Mach. Intell., vol.33, no.9, pp.1877–1893, Sept. 2011.
[10] J. Wright, A.Y. Yang, A. Ganesh, S.S. Sastry, and Y. Ma, "Robust face recognition via sparse representation," IEEE Trans. Pattern Anal. Mach. Intell., vol.31, no.2, pp.210–227, Feb. 2009.
[11] L.-W. Kang, C.-Y. Hsu, H.-W. Chen, and C.-S. Lu, "Secure SIFT-based sparse representation for image copy detection and recognition," Proc. IEEE Int. Conf. Multimedia and Expo, pp.1248–1253, July 2010.
[12] N.K. Ratha, J.H. Connell, and R.M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," Ibm. Syst. J., vol.40, no.3, pp.614–634, 2001.
[13] J. Zuo, N.K. Ratha, and J.H. Connell, "Cancelable iris biometric," ICPR 2008 19th International Conference on IEEE, pp.1–4, 2008.
[14] Y. Muraki, M. Furukawa, M. Fujiyoshi, Y. Tonomura, and H. Kiya, "A Compressible Template Protection Scheme for Face Recognition Based on Sparse Representation," Proc. EURASIP, no.TH-P5, Sept. 2014.
[15] M. Furukawa, Y. Muraki, M. Fujiyoshi, and H. Kiya, "Secure Face Recognition Scheme Using Noisy Images Based on Kernel Sparse Representation," Proc. APSIPA Annual Summit and Conference, no.OS.20-IVM.9-4, Kaohsiung, Taiwan, R.O.C., Oct. 2013.
[16] A.B.J. Teoh and C.T. Yuang, "Cancelable biometrics realization with multispace random projections," IEEE Trans. Syst. Man, Cybern. B, Cybern., vol.37, no.5, pp.1096–1106, Mon. 2007.
[17] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," Proc. of the 6th ACM conference on Computer and communications security, no.9, pp.28–36, 1999.
[18] Y.C. Feng, P.C. Yuen, and A.K. Jain, "A hybrid approach for generating secure and discriminating face template," IEEE Trans. Inf. Forensics Security, vol.5, no.1, pp.103–117, March 2010.
[19] U. Uludag, S. Pankanti, S. Prabhakar, and A.K. Jain, "Biometric cryptosystems: issues and challenges," Proc. IEEE, vol.92, no.6, pp.948–960, June 2004.
[20] E. Maiorana, P. Campisi, and A. Neri, "Iris template protection using a digital modulation paradigm," Proc. IEEE International Conference on Acoustics, Speech and Signal Processing, pp.3787–3791, 2014.
[21] N.K. Ratha, S. Chikkerur, J.H. Connell, and R.M. Bolle, "Generating cancelable fingerprint templates," IEEE Trans. Pattern Anal. Mach. Intell., vol.29, no.4, pp.561–572, April 2007.
[22] Y. Muraki, M. Furukawa, M. Fujiyoshi, and H. Kiya, "Robustness Analysis of Cancelable Biometrics Systems in Terms of Visual Recognizability," Proc. International Workshop on Advanced Image Technology, no.A2-145, pp.24–27, Jan. 2014.
[23] S. Hirata and K. Takahashi, "Cancelable Biometrics with Perfect Secrecy for Correlation-Based Matching," Advances in Biometrics, Lecture Notes in Computer Science, vol.5558, pp.868–878, 2009.
[24] K. Takahashi, "Unconditionally provably secure cancelable biometrics based on a quotient polynomial ring," International Joint Conference on Biometrics (IJCB), pp.1–8, 11-13 Oct. 2011.
[25] 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.
[26] I. Ito and H. Kiya, "A new class of image registration for guaranteeing secure data management," Proc. IEEE International Conference on Image Processing, no.MA-PA.5, pp.269–272, Oct. 2008.
[27] 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 Anal. Mach. Intell., vol.23, no.6, pp.643–660, June 2001.
[28] S. Kaski, "Dimensionality Reduction by Random Mapping," Proc. IEEE Int'l Joint Conf. Neural Networks, vol.1, pp.413–418, 1998.
[29] J.A. Buchmann, Introduction to Cryptography, Springer, Heidelberg, 2004.
[30] K. Nandakumar and A.K. Jain, "Biometric Template Protection: Bridging the Performance Gap Between Theory and Practice," IEEE Signal Process. Mag., vol.32, no.5, pp.77–87, 2015.
[31] A. Nagar, K. Nandakumar, and A.K. Jain, "Biometric Template Transformation: A Security Analysis," Proc. SPIE Media Forensics and Security, Electronic Imaging, pp.75410O-1–75410O-15, 2010.
[32] Y. Wang, S. Rane, S.C. Draper, and P. Ishwar, "A Theoretical Analysis of Authentication, Privacy, and Reusability Across Secure Biometric Systems," IEEE Trans. Inf. Forensics Security, vol.7, no.6, pp.1825–1840, Dec. 2012.

Ibuki Nakamura received his B.Eng. degree from Tokyo Metropolitan University, Japan in 2014. From 2014, he is currently a Master course student at Tokyo Metropolitan University. His research interests include biometrics and image processing.

Yoshihide Tonomura received his B.S. and M.S. degrees in electronics engineering from Nagaoka University of Technology, and a Ph.D. from Tokyo Metropolitan University in 2002, 2004, and 2010, respectively. Hi joined NTT Network Innovation Laboratories in 2004. From 2012 to 2013, he was a visiting scientist at MIT Media Lab, USA. His research is focused on image processing theories and applications. He is a member of IEICE.

Hitoshi Kiya received his B.Eng. and M.Eng. degrees from Nagaoka University of Technology, Japan, in 1980 and 1982, respectively, and his D.Eng. degree from Tokyo Metropolitan University in 1987. In 1982, he joined Tokyo Metropolitan University as an Assistant Professor, where he became a Full Professor in 2000. From 1995 to 1996, he attended the University of Sydney, Australia as a Visiting Fellow. He was/is the Chair of IEEE Signal Processing Society Japan Chapter, an Associate Editor for IEEE Trans. Image Processing, IEEE Trans. Signal Processing and IEEE Trans. Information Forensics and Security, respectively. He also served as the President of IEICE Engineering Sciences Society (ESS), the Editor-in-Chief for IEICE ESS Publications, a Vice President of APSIPA, and the Editor-in-Chief for IEICE ESS publications. His research interests are in the area of signal and image processing including multirate signal processing, wavelets, video coding, compressed-domain video manipulation, and security for multimedia. He received the IWAIT Best Paper Award in 2014 and 2015, the ITE Niwa-Takayanagi Best Paper Award in 2012, the Telecommunications Advancement Foundation Award in 2011, the IEICE ESS Contribution Award in 2010, and the IEICE Best Paper Award in 2008. He is a Fellow Member of the IEICE and the ITE, and a Senior Member of the IEEE.