2016 Joint 8th International Conference on Soft Computing and Intelligent Systems and 2016 17th International Symposium on Advanced Intelligent Systems

An Efficient Random Unitary Matrix for Biometric Template Protection

Yuko SAITO, Ibuki NAKAMURA, Sayaka SHIOTA, and Hitoshi KIYA
Department of Information and Communication Systems, Tokyo Metropolitan University, Hino-shi, Tokyo 191-0065, Japan
Email:saito-yuko@ed.tmu.ac.jp, nakamura-ibuki@ed.tmu.ac.jp, sayaka@tmu.ac.jp, kiya@tmu.ac.jp

***Abstract*—This paper proposes a new way to generate random unitary matrices for biometric template protection. It is well known that the unitary transform-based template protection that is a class of cancelable biometrics systems, has some desirable properties such as being applicable to l^2-norm minimization problems. However, its performance and effectiveness depend on the variety of a unitary matrix. The aim of this paper is to generate an effective random unitary matrix and evaluate the effectiveness in terms of security, recognition performance and the complexity of the recognition system. The proposed random matrix consists of a random permutation matrix and a unitary matrix in which all elements have fixed values as the discrete Fourier transform(DFT). It is also applied to face recognition experiments to demonstrate the effectiveness.**

I. Introduction

Establishing the identity of a person is a critical task in any management systems. 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 studied various kinds of biometric recognition schemes not only to improve recognition performance but also to protect biometric templates [1], [2]. In addition, security and privacy evaluation metrics for biometric template protection are now under standardization process as ISO/IEC WD 30136 [3].

The template protection schemes proposed in literatures can be broadly classified into two categories, feature transformation approach and biometric cryptosystem [4], [5]. The unitary transform-based template protection on which we forcus, corresponds to a cancelable biometric protection [6], [7] in the feature transform approach [8]. The unitary transform-based protection provides a number of desirable properties. For example, the Euclidean distance between the protected templates is equal to that between original ones, and there is no degradation of the recognition performances against l^2-norm minimization [9]–[12]. However, it has been recently found that its performance and effectiveness depend on the type of a unitary matrix [11], [12].

Because of such a situation, the aim of this paper is to conduct effective random unitary matrices and evaluate the effectiveness in terms of security, recognition performance and the complexity of the recognition system. The proposed random matrix consists of a random permutation matrix and a unitary matrix with fixed elements as the discrete Fourier transform(DFT). Compared with conventional unitary matrices including that generated by the Gram-Schmidt approach [9], [13], the proposed matrix is easy to be designed and can be carried out by using some fast algorithms such as the fast Fourier transform(FFT), while keeping a high recognition performance.

II. Preparation

A. Recognition System

Fig. 1 illustrates a biometric recognition system as an example of the systems, on which we focus, where a parameter $\mathbf{p}_i$, $i = 1, 2, ..., K$, is used as either a user specific password or a common password in all users. In the enrollment, a feature vector $\mathbf{f}_{i,j} \in \mathbb{R}^N$, $j = 1, 2, ..., M$, called a template is extracted from a training image $\mathbf{g}_{i,j}$, and then a transform function $T(\cdot)$ is applied to the template to generate a protected template $\hat{\mathbf{f}}_{i,j} = T(\mathbf{f}_{i,j}, \mathbf{p}_i)$. 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 $T(\cdot)$ 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 system with a parameter $\mathbf{p}_i$, is well known as a class of cancelable biometrics systems [8].

When $\mathbf{p}_i$ is commonly used in all users as $\mathbf{p}_1 = \mathbf{p}_2 = ... = \mathbf{p}_k$, this system corresponds to a system that enables to classify users, where the key is safely managed in the enrollment system and the recognition system [14].

B. Template Protection

An ideal biometric template protection scheme should have the following four properties [4]. topsep=0pt

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.

978-1-5090-2678-4/16 $31.00 © 2016 IEEE
DOI 10.1109/SCIS&ISIS.2016.47

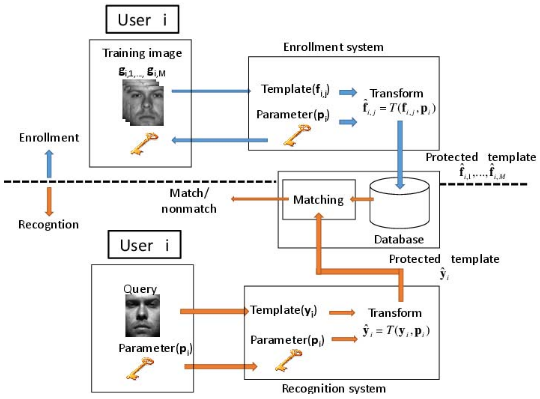

User i
Training image
$\mathbf{g}_{i,1}, ..., \mathbf{g}_{i,M}$
Enrollment system
Template($\mathbf{f}_{i,j}$)
Parameter($\mathbf{p}_i$)
Transform
$\hat{\mathbf{f}}_{i,j} = T(\mathbf{f}_{i,j}, \mathbf{p}_i)$
Enrollment
Protected template
$\hat{\mathbf{f}}_{i,1}, ..., \hat{\mathbf{f}}_{i,M}$
Match/
nonmatch
Matching
Database
Recognition
User i
Protected template
$\hat{\mathbf{y}}_i$
Query
Template($\mathbf{y}_i$)
Transform
$\hat{\mathbf{y}}_i = T(\mathbf{y}_i, \mathbf{p}_i)$
Parameter($\mathbf{p}_i$)
Parameter($\mathbf{p}_i$)
Recognition system

Fig. 1. Recognition system with protected templates.

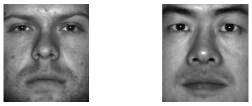

(a) template A (b) template B

Fig. 2. Original templates.

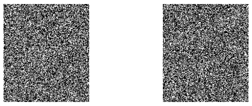

(a) template A (b) template B

Fig. 3. Protected templates.

4) Diversity: the secure template must not allow cross-matching across databases.

According to the above properties, the proposed scheme will be evaluated.

C. Properties of Unitary Transformation

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

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

where $\hat{\mathbf{f}}_{i,j}$ is the protected template. Fig. 2 shows template examples and Fig. 3 are their protected ones. It is certified that the original templates are difficult to be recognized from Fig. 3.

Note that the unitary matrix $\mathbf{Q}_{\mathbf{p}_i}$ satisfies

$$\mathbf{Q}^*_{\mathbf{p}_i}\mathbf{Q}_{\mathbf{p}_i} = \mathbf{I} \tag{2}$$

where $[\cdot]^*$ and $\mathbf{I}$ mean the Hermitian transpose operation and the identity matrix respectively. In addition to the unitarity, $\mathbf{Q}_{\mathbf{p}_i}$ needs to have randomness for generating protected templates. So far, a lot of studies on generating efficient random unitary matrices have been reported [7], [9], [11], [12], [14]. The Gram-Schmidt orthogonalization is a typical method for generating $\mathbf{Q}_{\mathbf{p}_i}$ [9]. However, matrices generated by the Gram-Schmidt orthogonalization have real value elements. In the hybrid approaches with a cryptosystem, the error-correcting coding techniques require integer values in template vectors such as integer vectors with limited range [15]. Further, it is well known that this orthogonalization requires a large amount of calculations to generate matrices. To overcome these problems, the phase scrambling-based method and the sign scrambling one have been also considered [16]–[18].

Here, some properties of the templates are shown below, on the assumption that two templates, $\mathbf{f}_{i,j} = \left[f_{i,j}(1), ..., f_{i,j}(N)\right]$ and $\mathbf{f}_{s,t} = [f_{s,t}(1), ..., f_{s,t}(N)]$ are protected by a common unitary matrix $\mathbf{Q}_{\mathbf{p}_i} = \mathbf{Q}_{\mathbf{p}_s}$ [11].

topsep=3pt

Property 1: Conservation of the Euclidean distances.

$$\sqrt{\textstyle\sum_k (f_{i,j}(k) - f_{s,t}(k))^2} = \sqrt{\textstyle\sum_k (\hat{f}_{i,j}(k) - \hat{f}_{s,t}(k))^2}$$

Property 2: Conservation of inner products.

$$\textstyle\sum_k f^*_{i,j}(k) f_{s,t}(k) = \sum_k \hat{f}^*_{i,j}(k)\hat{f}_{s,t}(k)$$

Property 3: Conservation of correlation coefficients.

$$\frac{\sum_k (f_{i,j}(k) - \bar{f}_{i,j})(f_{s,t}(k) - \bar{f}_{s,t})}{\sqrt{\sum_k (f_{i,j}(k) - \bar{f}_{i,j})^2}\sqrt{\sum_k (f_{s,t}(k) - \bar{f}_{s,t})^2}} = \frac{\sum_k (\hat{f}_{i,j}(k) - \bar{\hat{f}}_{i,j})(\hat{f}_{s,t}(k) - \bar{\hat{f}}_{s,t})}{\sqrt{\sum_k (\hat{f}_{i,j}(k) - \bar{\hat{f}}_{i,j})^2}\sqrt{\sum_k (\hat{f}_{s,t}(k) - \bar{\hat{f}}_{s,t})^2}}$$

Property 4: Conservation of results using the authentication via l^2-norm minimization.

In property 2, $f^*_{i,j}$ indicates the conjugate complex of $f_{i,j}$. $\hat{\mathbf{f}}_{i,j} = \left[\hat{f}_{i,j}(1), ..., \hat{f}_{i,j}(N)\right]$ and $\hat{\mathbf{f}}_{s,t} = \left[\hat{f}_{s,t}(1), ..., \hat{f}_{s,t}(N)\right]$ are protected templates of $\mathbf{f}_{i,j}$ and $\mathbf{f}_{s,t}$. All unitary transform-based protection schemes have the above properties.

III. Proposed Random Unitary Matrix

We propose efficient random unitary matrices.

A. Generation of Random Unitary Matrices

A method to generate $\mathbf{Q}_{\mathbf{p}_i}$ by using multiple unitary matrices was proposed [11] as

$$\mathbf{Q}_{\mathbf{p}_i} = \mathbf{H}(\mathbf{p}_i)\mathbf{A}, \tag{3}$$

where $\mathbf{A}$ is an unitary transform matrix such as the DFT, the discrete cosine transform (DCT), Hadamard transform etc. and $\mathbf{H}(\mathbf{p}_i)$ is an unitary matrix having randomness, which is generated by using a pseudo random generator. Note that $\mathbf{H}(\mathbf{p}_i)\mathbf{A}$ satisfies

$$(\mathbf{H}(\mathbf{p}_i)\mathbf{A})^*(\mathbf{H}(\mathbf{p}_i)\mathbf{A}) = \mathbf{I}. \tag{4}$$

Compared with the Gram-Schmidt-based orthogonalization, (3) enables to easily design $\mathbf{Q}_{\mathbf{p}_i}$ since $\mathbf{Q}_{\mathbf{p}_i}$ is structurally guaranteed to have orthogonality. In addition, some fast algorithms such as the FFT can be used for the transform $\mathbf{A}$. So far, the phase scrambling and the sign scrambling have been considered as a scheme for generating $\mathbf{H}(\mathbf{p}_i)$ [16]–[18]. For example, the random matrix called phase scrambling is illustrated by, for $N = 4$

$$\mathbf{H}_1(\mathbf{p}_i) = \begin{bmatrix} e^{j\theta_{\mathbf{p}_i(1)}} & 0 & 0 & 0 \\ 0 & e^{j\theta_{\mathbf{p}_i(2)}} & 0 & 0 \\ 0 & 0 & e^{j\theta_{\mathbf{p}_i(3)}} & 0 \\ 0 & 0 & 0 & e^{j\theta_{\mathbf{p}_i(4)}} \end{bmatrix} \tag{5}$$

where $\theta_{\mathbf{p}_i}(k)$ has randomness. Also, the sign scrambling is expressed as a matrix in which elements $e^{j\theta_{\mathbf{p}_i()}}$ in (5) are randomly replaced with -1 or 1. In this paper, we propose a new $\mathbf{H}(\mathbf{p}_i)$, referred to as a random permutation matrix, and evaluate the effectiveness.

B. Random Permutation Matrix

The permutation, σ, for shuffling elements in a template vector is defined as a two-line notation:

$$\sigma = \begin{pmatrix} 1 & 2 & ... & i & ... & N \\ z_1 & z_2 & ... & z_i & ... & z_N \end{pmatrix}, \quad (6)$$

where the first row represents the elements of i and the second row, which is $(z_1, z_2, ..., z_N)$, is a sequence generated by sequentially taking a pseudo-random number between 1 and N, ensuring that there are no repetitions. Further, (6) can be described as a permutation matrix. For example, the permutation matrix is illustrated by, for $N = 4$,

$$\mathbf{H}_P(\mathbf{p}_i) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}. \quad (7)$$

The permutation matrix is an unitary matrix having randomness. We propose to use a random permutation matrix as the matrix $\mathbf{H}_P(\mathbf{p}_i)$ in (3). The permutation matrix has the following advanced properties. topsep=1pt

(a) Unitarity(orthogonality)
(b) All elements have 1 or 0.
(c) There is one element having value 1 in every column.
(d) The matrix product, $\mathbf{H}_P(\mathbf{p}_k) = \mathbf{H}_P(\mathbf{p}_i)\mathbf{H}_P(\mathbf{p}_j)$ becomes a permutation matrix.

As described above, the permutation matrix has not only the unitarity, but also some desirable properties which are useful for reducing computation and memory cost and avoiding the effect of finite precision arithmetic in recognition systems.

C. Security Analysis for Brute-Force Attack

We evaluate the safety of the proposed system with its key space, assuming that an attacker performs the brute-force attack. The key space of the random unitary matrices is given as $N!$ where N is the dimension of the templates. Therefore, when $N!$ is larger than 2^{256}, i.e.

$$N! > 2^{256} \quad (8)$$

the key space of the proposed matrix is larger than that of the 256-bits key. It will be shown that (8) can be easily satisfied.

IV. Experimental Results and Evaluation

A number of random unitary matrices are applied to face recognition experiments.

A. Data Base

We use the Extended Yale Face Database B [19] that consists of 2432 frontal facial images with 192×168-pixels of 38 persons. 64 images for each person are divided into half randomly for training samples and queries. Namely, the number of persons is $K = 38$. Also, the number of training sample for each person is $M = 4$. To make the difference among random matrices clear, a small number as M is used for this simulation.

TABLE I
Type of $\mathbf{A}$ and $\mathbf{H}(\mathbf{p}_i)$.

$\mathbf{A}$		$\mathbf{H}(\mathbf{p}_i)$	
$\mathbf{A}_I$	Identity matrix	$\mathbf{H}_P(\mathbf{p}_i)$	permutation (proposed)
$\mathbf{A}_D$	DFT	$\mathbf{H}_1(\mathbf{p}_i)$	phase scrambling
$\mathbf{A}_C$	DCT	$\mathbf{H}_2(\mathbf{p}_i)$	sign scrambling
$\mathbf{A}_H$	Hadamard transformation		

TABLE II
Combination of $\mathbf{A}$ and $\mathbf{H}(\mathbf{p}_i)$.

Combination	$\mathbf{A}$	$\mathbf{H}(\mathbf{p}_i)$
C_0	$\mathbf{A}_I = \mathbf{I}$	$\mathbf{H}_P(\mathbf{p}_i)$
C_1(proposed)	$\mathbf{A}_D$, $\mathbf{A}_C$, $\mathbf{A}_H$	$\mathbf{H}_P(\mathbf{p}_i)$
C_2	$\mathbf{A}_D$	$\mathbf{H}_1(\mathbf{p}_i)$
C_3	$\mathbf{A}_D$, $\mathbf{A}_C$, $\mathbf{A}_H$	$\mathbf{H}_2(\mathbf{p}_i)$

B. Template

Random unitary matrices are applied to templates with dimension $N = 2048$, which are generated by the down-sampling method [20]. The down-sampling method divides an image into nonoverlapped blocks and then calculates the mean value in each block. Table I shows the variety of unitary matrices and random unitary matrices used as $\mathbf{A}$ and $\mathbf{H}(\mathbf{p}_i)$ respectively. Besides, Table II summarizes the combination of matrices used in the experiments. These combinations are applied to generate protected templates respectively.

C. Recognition Method via L^2-norm Minimization

The recognition method via l^2-norm minimization [10], [11], [20] is used. In the recognition, $\hat{\mathbf{f}}_{i,j}$ is defined as the j-th protected template for the i-th person where $j = 1, 2, ..., M$. For the i-th registered person in K registered persons, the set of training protected templates is given by $\hat{\mathbf{D}}_i = \left[\hat{\mathbf{f}}_{i,1}, ..., \hat{\mathbf{f}}_{i,M}\right]$. Let us assume that $\hat{\mathbf{y}}$, the protected feature vector of a query which belongs to i-th person is linearly approximated solely by the training vectors of the i-th person

$$\hat{\mathbf{y}} = \hat{\mathbf{f}}_{i,1}x_{i,1} + \hat{\mathbf{f}}_{i,2}x_{i,2} + ... + \hat{\mathbf{f}}_{i,M}x_{i,M} = \hat{\mathbf{D}}_i\mathbf{x}_i, \quad (9)$$

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

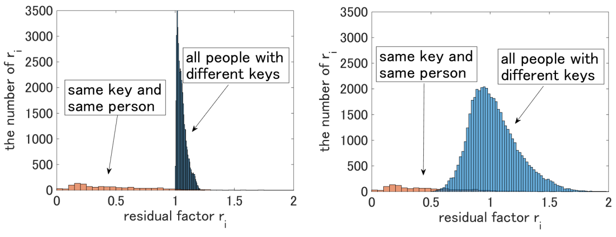
$$\hat{\mathbf{y}} = \hat{\mathbf{D}}_1\mathbf{0} + ... + \hat{\mathbf{D}}_{i-1}\mathbf{0} + \hat{\mathbf{D}}_i\mathbf{x}_i + \hat{\mathbf{D}}_{i+1}\mathbf{0} + ... + \hat{\mathbf{D}}_K\mathbf{0} = \hat{\mathbf{D}}\mathbf{x}_0, \quad (10)$$

where $\mathbf{x}_0 = \left[\mathbf{0}^T, ..., \mathbf{0}^T, {\mathbf{x}_i}^T, \mathbf{0}^T, ..., \mathbf{0}^T\right]^T$ and $\hat{\mathbf{D}} = \left[\hat{\mathbf{D}}_1, \hat{\mathbf{D}}_2, ..., \hat{\mathbf{D}}_K\right]$. To identify the i-th person, the l^2-norm minimization problem of (10) is carried out as

$$\tilde{\mathbf{x}}_0 = \arg\min_{\mathbf{x}} ||\mathbf{x}||_2 \ \textit{subject to} \ \hat{\mathbf{y}} = \hat{\mathbf{D}}\mathbf{x}. \quad (11)$$

By solving (11), an approximate solution $\tilde{\mathbf{x}}_0$ is obtained as $\tilde{\mathbf{x}}_0 = \left[\tilde{\mathbf{x}}_1^T, ..., \tilde{\mathbf{x}}_i^T, ..., \tilde{\mathbf{x}}_K^T\right]^T$. $\tilde{\mathbf{x}}_0$ 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:

$$\delta_i(\tilde{\mathbf{x}}_0) = \left[\mathbf{0}^T, ..., \mathbf{0}^T, {\tilde{\mathbf{x}}_i}^T, \mathbf{0}^T, ..., \mathbf{0}^T\right]^T. \quad (12)$$



C_1 : $\mathbf{A} = \mathbf{A}_D$ (6.17%) C_2 : $\mathbf{A} = \mathbf{A}_D$ (38.4%)

Fig. 4. Cross-matching evaluation(percentage of overlapped r_i between the red distribution and the blue one).

TABLE III
THE NUMBER OF OVERLAPPED r_i AND ITS PERCENTAGE.

	C_0	$C_1(proposed)$	C_2	C_3
$\mathbf{A}_I$	385 (31.7%)	-	-	-
$\mathbf{A}_D$	-	75 (6.17%)	467 (38.40%)	431 (35.4%)
$\mathbf{A}_C$	-	76 (6.25%)	-	575 (47.3%)
$\mathbf{A}_H$	-	76 (6.25%)	-	574 (47.2%)
Gram-Schmidt	76 (6.25%)			

Substituting $\delta_i(\tilde{\mathbf{x}}_0)$ into $\mathbf{x}_i$ in (9), the person C is estimated by

$$r_i = \|\hat{\mathbf{y}} - \hat{\mathbf{D}}\delta_i(\tilde{\mathbf{x}}_0)\|_2 \quad (13)$$

$$C = \arg\min_i r_i \quad (14)$$

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

D. Evaluation of Cross-matching Performance

Fig. 4 shows the relation between residual factor r_i and the number of r_i, where r_i should be ideally equal to zero when a query person is the same as a person of training samples, referred to as ”same person” in Fig.4 and the same key is provided to both of the query and training samples i.e. ”same key”. If there is almost no overlap between the red distribution and the blue one, the scheme has a sufficient performance for avoiding the cross-matching. From Fig.4, we can see that the cross-matching performance depends on the combination of unitary matrices. Table III summarizes the number of overlapping r_i and its percentage between the red distribution and the blue one for all combinations. It is shown from the table that the random permutation matrix has a better performance as well as the Gram-Schmidt than other combinations.

E. Evaluation of Recognition Accuracy

The proposed matrix is compared with the conventional ones in terms of recognition accuracy. To confirm the effectiveness of the proposed scheme, Receiver Operation Characteristic (ROC) curves are plotted as shown Figs.5 and 6, according to the relation of a residual factor r_i and a threshold value, τ:

$$if \;\; r_i \leq \tau \;\; then\ accept; \;\; else\ reject \quad (15)$$

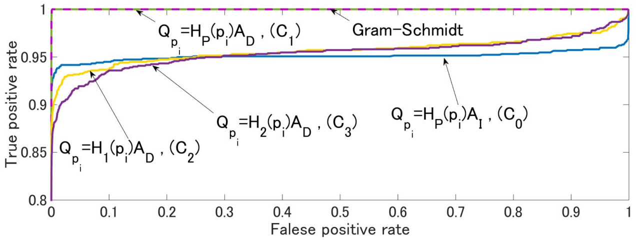


Fig. 5. ROC curves ($\mathbf{A} = \mathbf{A}_D$, No. of templates= 4).

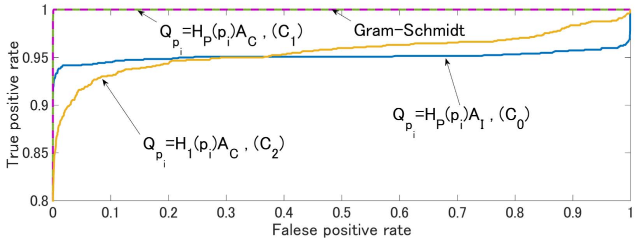


Fig. 6. ROC curves ($\mathbf{A} = \mathbf{A}_C$, No. of templates= 4).

TABLE IV
PLATFORM USED IN THE EXPERIMENT

Processor	Intel Core i7-4810MQ 2.80GHz
RAM	16.0GB
OS	Windows7
Software	MATLAB R2014b

TABLE V
TIME OF MATRIX GENERATION AND TRANSFORMATION[SEC/TEMPLATE]

	C_1(DFT)	C_1(DCT)	Gram-Schmidt
calculation times (relative value)	0.0001 (1)	0.0005 (5)	0.0059 (59)

In the figures, 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. It is shown that the proposed combination(C_1) provides a high recognition accuracy as well as the Gram-Schmidt, compared with the other ones. This is the reason why the proposed one has a better cross-matching performance.

F. Evaluation of Calculation Times

Next, the proposed matrix is compared with the conventional ones in terms of calculation time. This experiment was carried out on the platform in table IV.

Table V summarizes processing time for the matrix generation and transformation. The proposed scheme was about 60 times faster than the Gram-Schmidt approach. In addition to processing time, the Grand-Schmidt approach needs a large amount of memory to manage unitary matrices, because the matrix has $N \times N$ elements with real numbers for one person. In contrast, the random unitary matrix has N elements with integer numbers.

V. CONCLUSION

In this study, we proposed an efficient random unitary matrix and showed the performance of the matrix. First, this paper described the properties of the unitary transformation, and showed kinds of random unitary matrices. Further, by doing some face recognition experiments, various random unitary matrices are compared in terms of cross-matching performance, processing time and security. It was shown that the use of the random permutation matrix has some efficient properties. And, we compared the proposed generation scheme with the Gram-Schmidt method, and it was shown that the scheme can generate the unitary matrix with more superiority easily.

References

[1] K. Nandakumar, A. K. Jain, "Biometric Template Protection: Bridging the Performance Gap Between Theory and Practice." Signal Processing Magazine, IEEE, vol.32, no.5, pp.88-100, 2015.

[2] Y. Wang, S. Rane, S. C. Draper, and P. Ishwar, "A Theoretical Analysis of Authentication, Privacy, and Reusability Across Secure Biometric Systems," IEEE Trans. Information Forensics and Security, vol. 7, no. 6, pp. 1825-1840, Dec, 2012.

[3] S. Rane., "Standardization of Biometric Template Protection, "IEEE Multimedia Magazine, Vol. 21, No. 4, pp. 94–99, Oct. 2014.

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

[5] 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.

[6] 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.

[7] 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, p.73510P-73510P-12, 2009.

[8] L. MengHui, A. Beng, J. Teoh and J. Kim, "Biometric Feature-Type Transformation: Making templates compatible for secret protection," Signal Processing Magazine, IEEE, vol32, no.5, pp.77-87, 2015

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

[10] 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 European Signal Processing Conference, no.TH-P5-4, Lisbon, Portugal, 4th Sep., 2014.

[11] I. Nakamura, Y. Tonomura, and H. Kiya, "Unitary Transform-Based Template Protection and Its Properties," Proc. European Signal Processing Conference, vol.SIPA-P3.4, pp.2466-2470, 2015.

[12] I. Nakamura, Y. Tonomura, and H. Kiya, "Unitary Transform-Based Template Protection and Its Application to l_2-norm Minimization Problems," IEICE Trans. Inf. & Sys., vol.E99-D, no.1, pp.60-68, Jan.2016.

[13] A. T. B. Jin, D. N. C. Ling, A. Goh, "Biohashing: two factor authentication featuring fingerprint data and tokenised random number," Pattern recognition, vol.37, no.11: pp2245-2255, 2004,.

[14] S. Jassim, H.Al-assam, 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, pp. 556-561, 2009.

[15] 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, Mar.2010.

[16] 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.

[17] 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, 2008.

[18] I Ito and H Kiya, "Phase-only correlation based matching in scrambled domain for preventing illegal matching," Transactions on data hiding and multimedia security V, pp.51-69,2010.

[19] 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.

[20] 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.