Iris Template Protection Method Robust to Stolen Token Case

Youn Joo Lee and Jaihie Kim
School of Electrical and Electronic Engineering, Yonsei University
Biometric Engineering Research Center,
#401, Industry-University Research Center, Yonsei University 134
Shinchon-dong, Seodaemun-gu, Seoul 120-749, South Korea
E-mail: younjoo@yonsei.ac.kr, jhkim@yonsei.ac.kr

Abstract: Biometric authentication systems have been used in many security systems such as access contol, computer login, e-commers, and so on. However, biometric authentication systems have a critical problem. The problem is that if they are compromized once, biometric templates are permanantly compromized because biometric charicteristics cannot be changed. In order to solve this problem, the concept of cancelable biometrics was introduced. Cancelable biometrics method based on random projection is one of the various methods to produce revocable biometric templates. This method can easily reissue transformed biometric templates repeatedly and makes biometric features more distinquishable since original biometric signal is projected on random space that was derived from a user's token that embody the user-specific psuedorandom number (PRN). However, random projection method has a major limitation. In stolen-token senario, the recognition performance remains as single biometrics performance. This paper presents a biometric templates protection method based on random projection, which is robust to stolen-token case. We used multiple random projection (MRP) to produce cancelable biometric templates and extracted regualarized eigenfeatures in order to improve the recognition performance in the stolen token scenario. Experimental results showed that the performance of the proposed method was not greatly degraded in the stolen token scenario.

1. Introduction

Biometric authentication systems have been widely used in many security systems such as access contol, computer login, e-commerce, and so on. In general biometric authentication systems, the users' biometric templates are generated during an enrollment and are stored directly in a central database or storage devices such as smartcard. At authentication phase, the user enters a new data of the same biometrics and new biometric feature is produced from the data. Then, the user's new input biometric feature is matched against the corresponding template in database. Biometric charicteristics can not be changed since they are innate charicteristics of the users. Therefore, in most biometric authentication system, if biometric templates are compromised by attackers, these templates are permanently compromised [1].

For protecting biometric templates, the concept of cancelable biometrics was originally proposed by Ratha [2]. Its concept is to change a biometric signal into a new one using a repeatable distortion transform function for enrollment and for every authentication. In cancelable biometrics, a chosen transform function is non-invertible or is difficult to obtain original signal from transformed one. Therefore, if the transformed templates are compromised, the chosen transform function is changed and a new cancelable template is generated by a new chosen tranform function. Also, it is difficult for the attacker to obtain the original template from the stolen template.

Among various cancelable biometrics methods, random projection based methods has some advantages. They can easily reissued transformed biometric templates and has good recognition performance [3]. Teoh *et al*. [4] proposed a one-way transform method called BioHashing. Their scheme is based on iterated inner products between tokenized pseudo-random number and the user specific fingerprint feature. The authors reported that the performance has zero EER for palmprints [5-6] and faces [7] as well as fingerprints [4]. Subsequently, the authors [7] presented random multispace quantization as an analytic mechanism for BioHashing. They showed clean separation of the genuine and imposter populations in the recognition performance. Recently, Kong *et al*. [9] discussed that the BioHashing could have perfect accuracy (zero EER) only under the unpractical assumption that the tokenized pseudo-random number would never be lost, stolen, shared or duplicated. They showed that the performance of the BioHashing without the assumption was degraded over solely biometric.

In this paper, we focus on a cancelable biometrics based on random projection, which is robust to stolen token scenario. In the proposed method, original biometric signals are projected onto multiple random spaces and the randomized features are regularized by X. Jiang *et al*.[10]'s method to extract eigenfeatures that is robust to stolen token scenario. From the experimental results, we proved that the performance of proposed method (MRP-ERE) was better than the ones of simple MRP and MRP-PCA in the stolen token scenario.

The outline of this paper is given as follows. Section 2 describes the overview of the proposed method. Section 3 presents the experimental results and discussions. The conclusions are drawn in Section 4.

2. Proposed Method

2. 1 Overview

Figure 1 shows the overall process of the proposed method. At enrollment phase, the user's iris image is entered and the image is preprocessed to obtain 1D iris image vectors. 1D iris image vector is projected onto the multiple random spaces that are derived from a user-specific pseudorandom number (PRN).

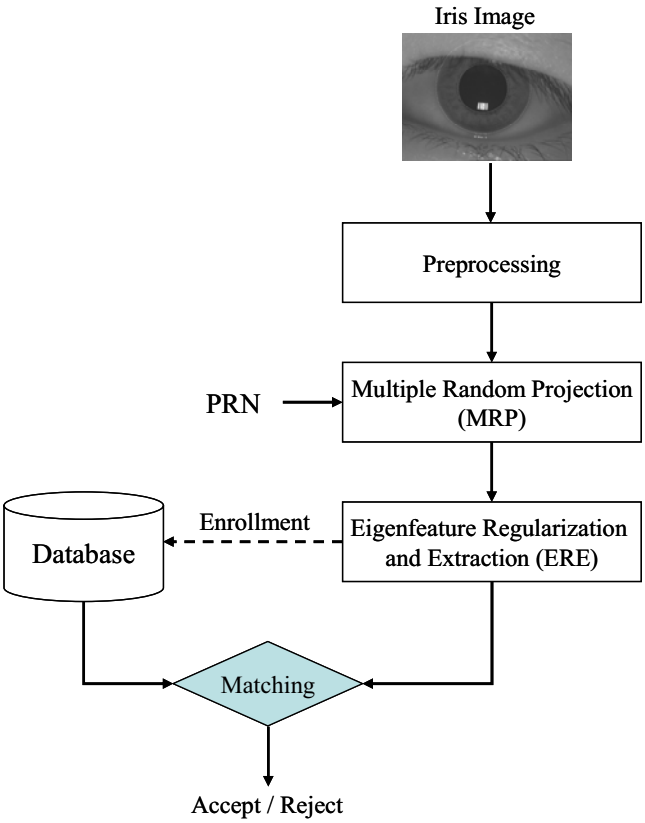

Figure 1. The overall flowchart of the proposed method.

Then, the randomized feature vectors are trained and regularized eigenfeatures are stored as cancelable templates in a central database. At verification phase, the user enters his iris image and 1D image vector is projected on the random space that is generated by the user's token. The randomized feature is multipied by regularization matrix that was derived during traning and a final feature vector is matched against the corresponding stored template. If the matching is successful, the user is identified as the legitimate user.

2. 2 Preprocessing

In the proposed method, it needs preprocessing of acquired eye images before extracting cancelable templates. An eye image is captured and we detect the interior boundary (between the pupil and the iris) and the exterior boundary (between the iris and the sclera) of the iris in the eye image. Then the localized iris part is normalized in a polar coordinate as shown in figure 2. To use only pure iris pattern, we selected the left and the right regions, which may partially or not be occluded by eyelids, eyelashes and specular reflections in the normalized iris image as Regions Of Interest (ROI). The size of each ROI is $p \times q$ and two ROIs are obtained in one iris image. Last, two ROIs are transformed into 1-dimensional image vectors in order to project onto the random space. To make 1-dimensional vector, row vectors of 2D ROI are concatenated into one row vector, $N \times 1$ vector ($N = p \times q$) as shown in figure 2.

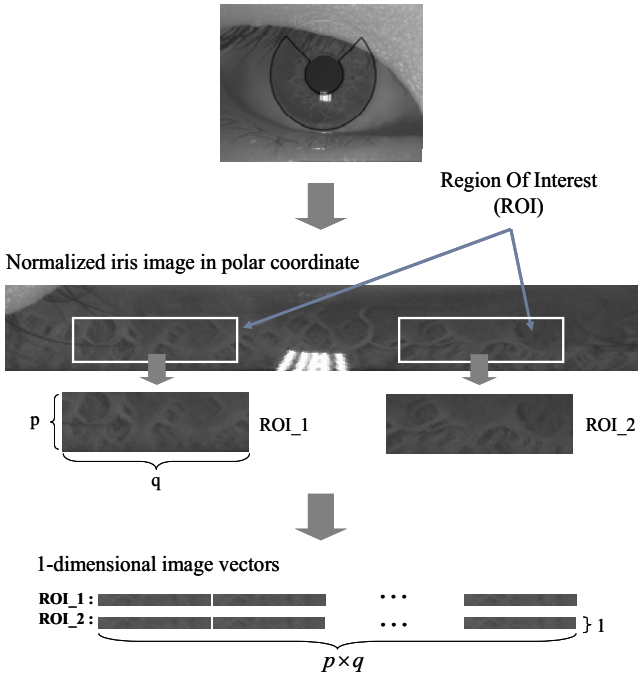

Figure 2. Preprocessing procedure.

2. 3 Multiple Random Projection (MRP)

The random projection (RP), $f : \Re^n \rightarrow \Re^m$ is a technique of projecting a set of data points to a randomly selected low-dimensional space [11]. Therfore, RP method is generally used as a dimensionality reduction technique while preserving the structure of data points [3][11]. RP method is a linear orthogonal transform. Any point x is projected onto a random subspace $R \in \Re^{mn}$, where R is a $m \times n$ ($m \leq n$) random matrix such that each entry r_{ij} of R is independent and identically (i.i.d) drawn from $N(0, \sigma^2)$. This effect is based on the Johnson-Lindenstrauss Lemma [12]. This Lemma states that any k data points in n-dimensional Euclidean space can be mapped down to $m = O(\log k / \varepsilon^2)$ dimensional space without distorting the pair-wise distance of any two points by more than $(1+\varepsilon)$.

In this paper, multiple random projection (MRP) technique was used to produce cancelable iris templates. In the proposed method, random space consists of multiple random matrices as shown in figure 3(a). To obtain one random matrix, we generate multiple different $d \times N$ random matrices. Then, these random matrices are combined as shown in figure 3(a) and $D \times N$ random matrix is obtained. Here, N is the dimension of 1-D image vector and D is the dimension of the randomized feature vector. Randomized feature vectors(f) are obtained by product of random matrix R and 1-D image vector(V), $f = RV$ as shown in figure 3(b).

2. 4 Eigenfeature Regularization and Extraction

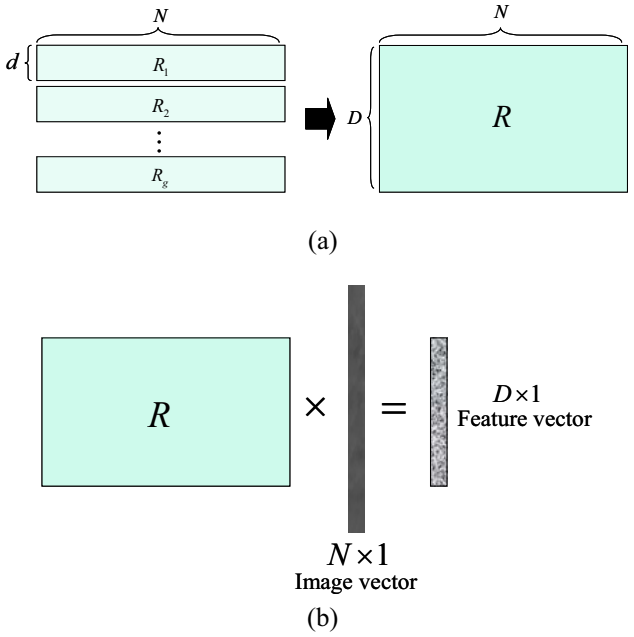

Figure 3. Multiple random projection procedure; a) generating multiple random matrix, b) randomized feature vector generation by product of mulitple random matrix with image vector

Eigenfeature regularization and extraction (ERE) method was proposed by X. Jiang *et al.*[10]. ERE method can extract discriminant eigenfeatures since it addresses the performance degradation caused by noise disturbance and finite number of training samples compared with Principal Component Anlysis (PCA). Therefore, we applied this method for randomized iris features in order to improve the performance in stolen-token scenairo. In this method, eigenspace of the within-class scatter matrix is decomposed into three subspaces and eigenfeatures are regularized differently in these subspaces by using eigenspectrum modelling as shown in Figure 4. The procedure of the ERE method is as follows.

At training,

1) Given a training set of randomized iris feature vectors $\{X_{ij}\}$, compute within scatter matix S^w by eq. (1) and solve the eigenvalue problem as eq. (2).

$$S^w = \sum_{i=1}^{p} \frac{c_i}{q_i} \sum_{j=1}^{q} (X_{ij} - \bar{X}_i)(X_{ij} - \bar{X}_i)^T \qquad (1)$$

where, $\bar{X}_i = \frac{1}{q_i} \sum_{j=1}^{q_i} X_{ij}$.

$$\Lambda^g = \Phi^{gT} S^g \Phi^g \qquad (2)$$

where, $\Phi^g = \left[\phi_1^g, ..., \phi_n^g\right]$ and eigenvalues are $\lambda_1^g, ..., \lambda_n^g$.

2) Decompose the eigenspace into feature-, noise-, and null-spaces by determining the *m* value using eq. (3) and eq. (4).

$$\lambda_{med}^g = median\left\{\forall \lambda_k^g \mid k \le r\right\} \qquad (3)$$

$$\lambda_{m+1}^g = \max\left\{\forall \lambda_k^g \mid \lambda_k^g < (\lambda_{med}^g + \mu(\lambda_{med}^g - \lambda_r^g))\right\} \qquad (4)$$

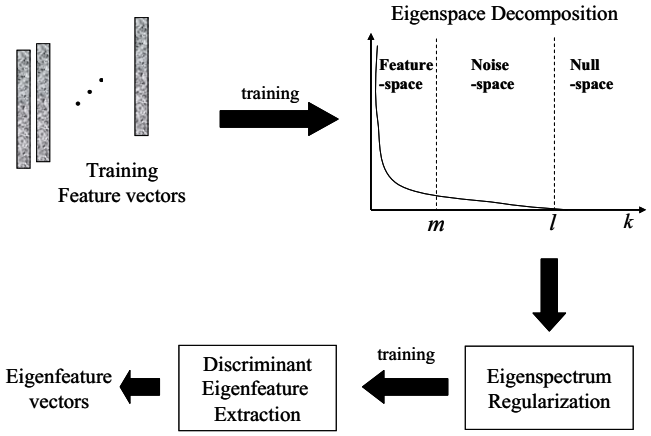

Figure 4. Eigenfeature regularization and extraction

3) Transform the training feature vectors represented by X_{ij} into $\tilde{Y}_{ij}$ by eq. (5) with the weighting function eq. (6) determined by eq. (7).

$$\tilde{Y}_{ij} = \tilde{\Phi}_n^{wT} X_{ij} \; \tilde{\Phi}_n^w = \left[\tilde{w}_k^w \phi_k^w\right]_{k=1}^n \qquad (5)$$

$$\bar{w}_k^w = \frac{1}{\sqrt{\tilde{\lambda}_k^w}}, \; k = 1, 2, ..., n \qquad (6)$$

$$\tilde{\lambda}_k^w = \begin{cases} \lambda_k^w, & k < m \\ \dfrac{\alpha}{k+\beta}, & m \le k \le r \\ \dfrac{\alpha}{r+1+\beta}, & r < k \le n \end{cases} \qquad (7)$$

4) Compute within scatter matrix $\tilde{S}^t$ with $\tilde{Y}_{ij}$ and solve the eigenvalue problem.

5) Obtain the final feature regularization and extraction matrix.

At the feature extraction, each randomized feature vector *X* is transformed into final feature vector *F* using the feature regularization and extraction matrix U obtained in the training such as $F = U \times X$

3. Experimental Results

We used BERC iris database (version 1) [14] to evaluate the performance of the proposed method. BERC database consists of 990 images: 10 images for 99 individuals. Figure 5 shows some sample images in this database. All images have a resolution of 640×480 pixels with gray information of 8 bits. In our experiments, five iris images per class were used for training and the remaining five images were used for testing. The criteria used for evaluating the performance was Equal Error Rate (EER) and we otained the results for stolen token scenario. Stolen token scenario means a case that an imposter stole the genuine token, which is used by the imposter to attempt to access security system as a genuine user.

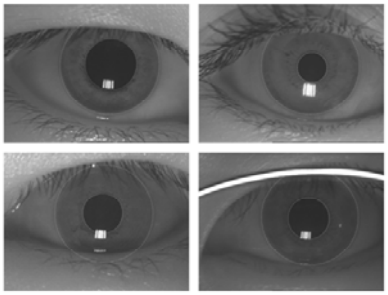

Figure 5. Images in BERC iris database.

Table 1. Performance of MRP

Dim	100	500	1000	1500	2000
EER (%)	24.58	16.919	13.11	13.73	13.53

Table 2. Performance comparisons of MRP-PCA and MRP-ERE

Dim	20	40	60	80	100
MRP-PCA	10.10	10.05	10.03	10.05	10.04
MRP-ERE	5.54	7.24	10.43	11.89	13.07

Table 1 shows the performances of MRP when the dimension of feature vectors is chaged. From Table 1, we found that the performance was not good in stolen token scenario, when using simple MRP. Table 2 shows the performances of MRP-PCA and MRP-ERE. MRP-PCA method means a combination of MRP and PCA. After performing MRP, we applied PCA for randomized feature vectors. In Table 2, we found that the performance of MRP-ERE was better than one of MRP-PCA. In the case of MRP-PCA, the performances were similar for all given dimensions. In the case of MRP-ERE, the EER value was smaller as the dimension was reduced.

From the experimental results, the performance of the proposed method was 5.54% EER. This result showed that the proposed method was robust to the stolen token scenario compared to MRP and MRP-PCA.

4. Conclusions

This paper presented an iris template protection method robust to stolen token case. In th proposed method, original biometric signal was projected onto the multiple random spaces that was derived from a user-specific token to make easily revocable iris templates and then, the ERE method was used to extract discriminant features from feature vectors that were obtained by MRP. The experimental results showed that the proposed method had a better performance compared to simple MRP and MRP-PCA in the stolen token scenario.

Acknowledgements

This work was supported by the Korea Science and Engineering Foundation (KOSEF) through the Biometrics Engineering Research Center (BERC) at Yonsei University. (R112002105080020(2008))

References

[1] A. K. Jain, A. Ross and S. Prabhakar, “An Introduction to Biometric Recognition,” *IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics*, vol. 14, no. 1, pp. 4-20, January 2004.

[2] N. K. Ratha, J. H. Connell and R. M. Bolle, “Enhancing Security and Privacy in Biometrics-based Authentication Systems,” *IBM* Systems Journal, vol. 40, no. 3, 2001.

[3] Y. Kim, and K. -A. Toh, “A method to enhance face biometric security,” proc. IEEE conference on biometrics: Theory, Applications (ICIEA) pp. 815-833, 2006.

[4] B. J. Andrew Teoh, C. L. David Ngo, and A. Goh, “Biohashing: two factor authentication featuring fingerprint data and tokenized random number,” *Pattern Recognition*, Vol. 37, pp. 2245-2255, 2004.

[5] T. Connie, B. J. Andrew Teoh, M. Goh, and D. Ngo, “PalmHashing: a novel approach for dual-factor authentication,” *Pattern Analysis and Applications*, Vol. 7, No. 3, pp.255-268, 2004.

[6] T. Connie, B. J. Andrew Teoh, M. Goh, and C. L. David Ngo, “PalmHashing: a novel approach for cancelable biometric,” *Information Processing Letter*, Vol. 93, No.1, pp. 1-5, 2005.

[7] B. J. Andrew Teoh, C. L. David Ngo, and A. Goh, “Personalised cryptographic key generation based on FaceHashing,” *Computers and Security*, Vol. 23, No. 7, pp. 606-614, 2004.

[8] B. J. Andrew Teoh, A. Goh, and C. L. David Ngo, “Random Multispace Quantization as an Analytic Mechanism for Biohashing of Biometric and Random Identity Inputs,” IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 28, No. 12, 2006.

[9] A. Kong, K. Cheung, D. Zhang, M. Kamel, and J. You, “An analysis of BioHashing and its variants,” *Pattern Recognition*, In Press, Corrected Proof, Available online, 27 December 2005.

[10] Xudong Jiang, Bappaditya Mandal and Alex Kot, “Egenfeature Regularization and Extraction in Face recognition”, IEEE trans. on Pattern Analysis and Machine Intelligence, May, 23, 2007.

[11] A. B. J. Teoh and C. T. Yuang, “Cancelable Biometrics Realization With Multispace Random Projections,” IEEE Transactions on Systems, Man, and Cybernetics – Part B, vol. 37, no. 5, October 2007.

[12] S. Dasgupta and A. Gupta, “An elementary proof of the Johnson-Lindenstrauss Lemma,” International Computer Science Institute, TR-99-006.

[13] S. Kaski, “Dimensionality Reduction by Random Mapping: Fast Similarity Computation for Clustering,” *IEEE International Joint Conference on Neural Networks*, Anchorage, Alaska, May 1998.

[14] http://berc.yonsei.ac.kr (accessed on 2008. 5. 26).