2010 International Conference on Pattern Recognition

Cancelable Face Recognition using Random Multiplicative Transform

Yongjin Wang, Dimitrios Hatzinakos
Department of Electrical and Computer Engineering
University of Toronto, Canada
Email: {ywang, dimitris}@comm.utoronto.ca

***Abstract*—The generation of cancelable and privacy preserving biometric templates is important for the pervasive deployment of biometric technology in a wide variety of applications. This paper presents a novel approach for cancelable biometric authentication using random multiplicative transform. The proposed method transforms the original biometric feature vector through element-wise multiplication with a random vector, and the sorted index numbers of the resulting vector in the transformed domain are stored as the biometric template. The changeability and privacy protecting properties of the generated biometric template are analyzed in detail. The effectiveness of the proposed method is well supported by extensive experimentation on a face verification problem.**

***Keywords*-biometrics; changeability; privacy;**

I. Introduction

Biometrics refer to the technology of recognizing or confirming the identity of an individual based on the physiological (e.g., face, fingerprint) and/or behavioral (e.g., gait, keystroke) characteristics. It is superior to traditional password and token based methods in both security and convenience. However, there exist some problems yet to be addressed for widespread application of biometrics. Firstly, since biometric data reflects the physiological or behavioral characteristics of a person, the privacy concern arises. The biometric template should be generated in a way such that the privacy of the users can be protected even the template is known. Secondly, Biometrics can not be easily replaced if compromised due to the limited number of biometric traits that human has. To alleviate this problem, the biometric template should be changeable such that when a biometric template is compromised, the biometric signal itself is not lost forever, and a new one can be reissued.

A secure biometric system should offer both changeability and privacy protection. Moreover, the recognition performance of the system should not be deteriorated. Many tentative solutions have been introduced in the literature, which can be roughly categorized as biometric cryptosystems [1], and cancelable biometrics [2]. Comprehensive surveys of related works can be found in [1][3]. A biometric crypto-system aims at the combination of biometrics with cryptography to produce secure templates. In general, such methods are computationally complex and usually suffer performance degradation. The cancelable biometrics framework motivates the possibility of applying changeable and irreversible transforms on the biometric features. Using this method, every enrollment applies a different transform. When a biometric template is compromised, a new one can be generated by using a new transform. The major challenge here is to preserve the similarity in the transformed domain. A sorted index number (SIN) based approach has been introduced in [3], which demonstrates capability of being applied in conjunction with random transforms for producing secure templates. The SIN method is originated from the pairwise relation between vector elements, and it is capable of approximating the Euclidean distance. In this paper, we elaborate on the application of SIN method for changeable biometric authentication using random multiplicative transform (RMT). The effectiveness of the proposed method is supported by detailed changeability and privacy analysis, as well as extensive experimentation on a face verification problem.

II. Method Overview

The proposed method assumes the extracted biometric features being represented in continuous domain, and the similarity of the vectors can be evaluated by some (e.g. Euclidean) distance measures. Depending on different application context, the proposed method can be applied in two scenarios: user-independent (UI) and user-dependent (UD) transform. The UI scenario applies the same transform to all the users. The key is controlled by the service provider, and each individual does not need to carry a key. The UD scenario is a two-factor approach that requires both the correct biometrics and user-specific key for authentication. In both scenarios, the biometric template can be reproduced by simply changing the key. The procedure of generating a biometric template is as follows:

I Extract feature vector $\mathbf{w} \in \mathbb{R}^N$ from face image.

II Compute $\mathbf{u} = \mathbf{w} - \bar{\mathbf{w}}$, where $\bar{\mathbf{w}}$ is the mean feature vector calculated from the training data.

III Use a key $\mathbf{k}$ to generate a random vector $\mathbf{r} \in \mathbb{R}^N$, with each entry an i.i.d. Gaussian random variable of mean one and variance σ^2, $r_i \sim \mathbf{N}(1, \sigma^2)$. Compute $\mathbf{x} = (\mathbf{u} + \mathbf{d}) .* \mathbf{r}$, where $.*$ denotes multiplication by elements, and $\mathbf{d}$ is a translation vector.

IV Sort $\mathbf{x}$ in descending order, and store the corresponding index numbers in a new vector $\mathbf{g}$. The resulting SIN vector $\mathbf{g} \in \mathbb{Z}^M$ is stored as template.

1051-4651/10 $26.00 © 2010 IEEE
DOI 10.1109/ICPR.2010.314

For example, given $\mathbf{x} = \{x_1, x_2, x_3, x_4\}$, the sorted vector in descending order is $\hat{\mathbf{g}} = \{x_4, x_2, x_3, x_1\}$, then the template is $\mathbf{g} = \{4, 2, 3, 1\}$. The similarity measure between two SIN vectors $S(\mathbf{g}, \mathbf{p})$, denoted as SIN distance, can be computed as follows [3]:

1) Given two SIN vectors $\mathbf{g} \in \mathbb{Z}^M$ and $\mathbf{p} \in \mathbb{Z}^M$, start from the first element g_1 of $\mathbf{g}$.
2) Search for the corresponding element in $\mathbf{p}$, i.e., $p_i = g_1$. Record $\xi_1 = i - 1$, where i is the index number in $\mathbf{p}$.
3) Eliminate the obtained p_i in the previous step from $\mathbf{p}$, and obtain $\mathbf{p}^1 = \{p_1, p_2, ..., p_{i-1}, p_{i+1}, ..., p_M\}$.
4) Repeat step 2 and 3 on the subsequent elements of $\mathbf{g}$ until g_{M-1}. Record $\xi_2, \xi_3, ..., \xi_{M-1}$.
5) Computed $S(\mathbf{g}, \mathbf{p}) = \sum_{i=1}^{M-1} \xi_i$.

For example, let $\mathbf{g} = \{4, 2, 3, 1\}$ and $\mathbf{p} = \{3, 2, 1, 4\}$, we first search the 1^{st} element $g_1 = 4$, and find that $p_4 = 4$. Therefore $\xi_1 = 4 - 1 = 3$. Remove p_4 from $\mathbf{p}$ and form a new vector of $\mathbf{p}^1 = \{3, 2, 1\}$. Search the 2^{nd} element $g_2 = 2$ in $\mathbf{p}^1$, and find that $p_2^1 = 2$. Therefore $\xi_2 = 2 - 1 = 1$. Remove p_2^1 from $\mathbf{p}^1$ and form a new vector of $\mathbf{p}^2 = \{3, 1\}$. Search the 3^{rd} element $g_3 = 3$ in $\mathbf{p}^2$, and find that $p_1^2 = 3$. Therefore $\xi_3 = 1 - 1 = 0$. Compute $S(\mathbf{g}, \mathbf{p}) = \sum_{i=1}^{M-1} \xi_i = 3 + 1 + 0 = 4$.

III. Changeability Analysis

The proposed method employs RMT as a changeability mechanism, and in combination with SIN to produce privacy protection as well. Let $\mathbf{u} \in \mathbb{R}^N$ and $\mathbf{v} \in \mathbb{R}^N$ represent two biometric feature vectors. Let $\mathbf{r} \in \mathbb{R}^N$ and $\mathbf{s} \in \mathbb{R}^N$ denote two random vectors, and $r_i \sim \mathbf{N}(1, \sigma^2)$, $s_i \sim \mathbf{N}(1, \sigma^2)$. Let $\mathbf{x} = \mathbf{u}.*\mathbf{r}$, $\mathbf{y} = \mathbf{v}.*\mathbf{s}$. If the same key (SK) is applied, i.e., $\mathbf{r} = \mathbf{s}$, it can be shown that:

$$\mathbf{E}[\|\mathbf{x} - \mathbf{y}\|^2] = (\sigma^2 + 1)\|\mathbf{u} - \mathbf{v}\|^2, \tag{1}$$

$$\mathbf{Var}[\|\mathbf{x} - \mathbf{y}\|^2] = (2\sigma^4 + 4\sigma^2) \sum_{i=1}^{N} (u_i - v_i)^4, \tag{2}$$

Eqn. 1 and Eqn. 2 show that the RMT preserves the mean of the squared Euclidean distance (SED) between two vectors in the transformed domain up to a scaling factor σ^2+1, and the variance is proportional to σ^2. In the different key (DK) case, i.e., $\mathbf{r} \neq \mathbf{s}$, we can derive that:

$$\mathbf{E}[\|\mathbf{x} - \mathbf{y}\|^2] = \sigma^2(\|\mathbf{u}\|^2 + \|\mathbf{v}\|^2) + \|\mathbf{u} - \mathbf{v}\|^2, \tag{3}$$

$$\mathbf{Var}[\|\mathbf{x} - \mathbf{y}\|^2] = 2\sigma^4 \sum_{i=1}^{N} p_i^2 + 4\sigma^2 \sum_{i=1}^{N} q_i p_i. \tag{4}$$

where $p_i = u_i^2 + v_i^2$ and $q_i = (u_i - v_i)^2$. To obtain changeability, we expect that the SK and DK distributions are well separated. Eqn. 1 can be rewritten as $\mathbf{E}[\frac{\|\mathbf{x}-\mathbf{y}\|^2}{\sigma^2+1}] = \|\mathbf{u} - \mathbf{v}\|^2$, and Eqn. 3 can be rewritten as $\mathbf{E}[\frac{\|\mathbf{x}-\mathbf{y}\|^2}{\sigma^2+1}] = \|\mathbf{u}-\mathbf{v}\|^2 + \frac{2\sigma^2\mathbf{u}^T\mathbf{v}}{\sigma^2+1}$. It can be seen that the separation of the distributions is dependent on the σ^2 and the inner product of the vectors. Since there is no guarantee that $\mathbf{u}^T\mathbf{v} > 0$, it is possible that the SED in the DK transformed domain is even smaller than the original SED, i.e., weak changeability. To solve this problem, we note that $\frac{2\sigma^2}{\sigma^2+1} > 0$, and the SED in the DK case can be enlarged by increasing $\mathbf{u}^T\mathbf{v}$. This can be achieved by adding a vector $\mathbf{d}$ to all the elements of $\mathbf{u}$ and $\mathbf{v}$, such that $\mathbf{u}^T\mathbf{v}$ is augmented, and the SED of the original vectors $\|\mathbf{u} - \mathbf{v}\|^2$ is unaltered. As such, the distributions of SK and DK cases can be well separated, and strong changeability can be obtained.

Since the SIN method also approximates the SED between two vectors [3], it is expected that similar property can be preserved by applying the SIN method on RMT transformed vectors. This is validated through two randomly selected unit-norm Principal Component Analysis (PCA) feature vectors of dimensionality 100 from our experimental data set, with each experiment performed 2000 trails. Fig. 1-a and -b depicts the distributions of SED and normalized SIN distance (NSD), where the NSD is obtained by dividing the SIN distance by the largest possible value $\frac{N(N-1)}{2}$. The results confirm that without vector translation, the SK and DK distributions are not well separated, and the variance of the distances increases as σ^2 increases. It is shown in Fig. 1-c and -d that after adding an appropriate vector $\mathbf{d}$ (the same value d for all the elements), the SK and DK distributions can be well separated, and hence it can produce strong changeability.

Note that in the UD application scenario, since different users utilize different keys for randomness generation, the above analysis implies that the inter-class and intra-class distributions can be well separated, hence zero false accept rate (FAR) and false reject rate (FRR) can both be obtained by selecting appropriate system threshold value. It also indicates that even the biometric is stolen, without the correct key, the authentication will not be successful. The stolen key case can be evaluated by setting the same key for all the users. This is equivalent to the UI scenario. Therefore, the performance of the system can be fully characterized and demonstrated by the UI and UD scenarios.

IV. Privacy Analysis

The proposed methods utilize the SIN vector of the RMT transformed features as template for biometric recognition. Obviously, it is impossible to recover the exact values of any element in the transformed feature vector. However, an adversary may be able to estimate the distribution of the features, generate a set of random numbers based on the distribution, and rearrange the random numbers based on the SIN vector. As such, it is possible to provide an approximate estimation of the original features. For simplicity, we assume the features are i.i.d. in this paper.

Let $x_1, x_2, ..., x_N$ denote N i.i.d. random variables, $x_{1:N}, x_{2:N}, ..., x_{N:N}$ denote the ordered variates, then the mean and variance of the jth order statistic are [4]: $u_{j:N} =$

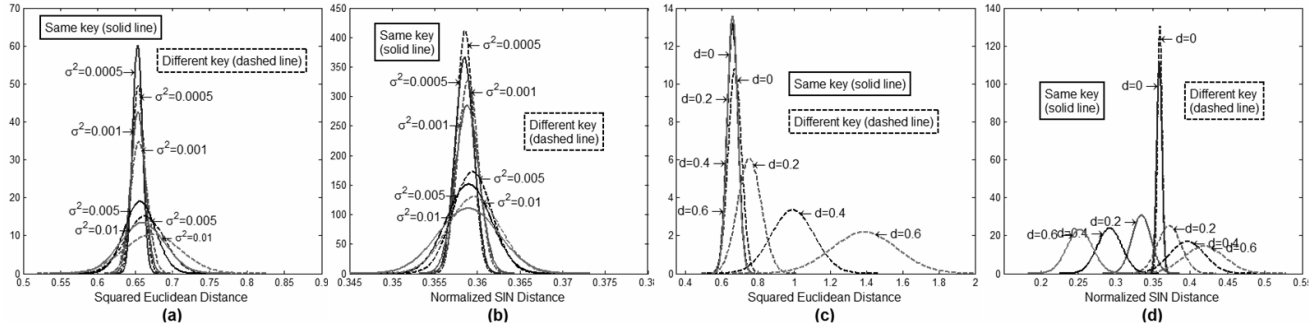

Figure 1. Distribution of (a) SED, (b) NSD, at different σ^2 values; and (c) SED, and (d) NSD, at different d values ($\sigma^2 = 0.01$).

$\int_{-\infty}^{+\infty} t f_{j:N}(t)dt$, and $\sigma^2_{j:N} = \int_{-\infty}^{+\infty}(t - u_{j:N})^2 f_{j:N}(t)dt$, where $f_{j:N}(t)$ is the probability density function (pdf) of $x_{j:N}$. Let $\widehat{x}_{j:N}$ denotes the estimation of $x_{j:N}$, then $\mathbf{E}[x_{j:N} - \widehat{x}_{j:N}] = u_{j:N} - \widehat{u}_{j:N}$, and $\mathbf{Var}[x_{j:N} - \widehat{x}_{j:N}] = \sigma^2_{j:N} + \widehat{\sigma}^2_{j:N}$. When the distribution of x is unknown, then the expected value of the estimation is not zero since $u_{j:N} \neq \widehat{u}_{j:N}$. In this case, the estimation will be less accurate and the user's privacy can be protected. However, it is possible that the attacker may estimate the distribution of the original features. Considering the worst case that the exact distribution is known, then we have: $\mathbf{E}[x_{j:N} - \widehat{x}_{j:N}] = u_{j:N} - \widehat{u}_{j:N} = 0$, and $\mathbf{Var}[x_{j:N} - \widehat{x}_{j:N}] = 2\sigma^2_{j:N}$. Therefore, the expected value of $x_{j:N} - \widehat{x}_{j:N}$ will be zero. Since the exact value of any element in the original feature vector can not be recovered, the variance of $x_{j:N} - \widehat{x}_{j:N}$ can be considered as a privacy measure. The larger the variance, the better the privacy protected. Fig. 2 plots the variance of the order statistics $\sigma^2_{j:N}$ as a function of vector dimensionality N (with $u_x = 0, \sigma^2_x = 1$), and variance of x, σ^2_x (with $N = 100$). It demonstrates that the $\sigma^2_{j:N}$ become greater at lower N and larger σ^2_x.

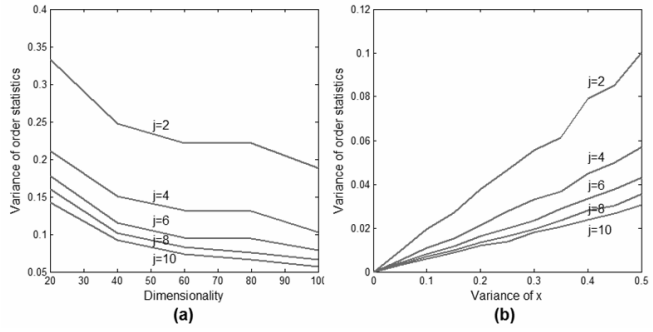

Figure 2. Variance $\sigma^2_{j:N}$ as function of (a) dimensionality N, and (b) variance σ^2_x.

In the proposed RIM-SIN method, the SIN vector $\mathbf{g}$ of RMT transformed vector $\mathbf{x}$ is stored as template, with each element of $\mathbf{x}$ obtained by $x_i = r_i(u_i + d), i = 1, 2, ..., N$, where $r_i \sim \mathbf{N}(1, \sigma^2_r)$, u_i is the ith element of feature vector $\mathbf{u}$ of mean zero and variance σ^2_u, and d is a translation value. It is straightforward to derive that $\mathbf{E}[x_i] = \mathbf{E}[r_i(u_i + d)] = d$, $\mathbf{E}[x^2_i] = \mathbf{E}[r^2_i(u_i + d)^2] = (\sigma^2_r + 1)(\sigma^2_u + d^2)$, and the variance of x_i is $\sigma^2_x = \mathbf{E}[x^2_i] - \mathbf{E}[x_i]^2 = \sigma^2_u(\sigma^2_r + 1) + d^2\sigma^2_r$.

Assuming the worst case that an attacker knows the distribution of $\mathbf{r}$, $\mathbf{u}$, and the value of d, he can generate a set of N random numbers of mean d and variance σ^2_x, estimate $\widehat{\mathbf{x}}$ by mapping the numbers according to the SIN vector $\mathbf{g}$, perform element-wise division followed by subtraction of d to obtain an estimate of u_i as $\widehat{u_i} = \widehat{x_i}/r_i - d$. As shown in Fig. 2, $\sigma^2_{j:N}$ increases as the variance of σ^2_x increases. In the RMT-SIN method, σ^2_x is proportional to σ^2_r and d, hence the larger the σ^2_r and d, the greater the $\sigma^2_{j:N}$, and hence the better the privacy.

V. Experimental Results

The effectiveness of the proposed method is evaluated through experiments on a generic data set that consists of 4666 face images from several well-known databases: FERET, PIE, AR, Aging, and BioID. The detailed configuration of the data set can be found in [3]. In our experiments, we randomly select 2388 image samples from 520 subjects as the training set, while 2278 samples of the rest 500 subjects as the testing set. The evaluation is performed on an exhaustive basis, where every image is used as a template once, and the rest of the images as the probe set. All the experiments are performed 5 times, and the average of the results are reported. To study the effects of different feature extractors, we adopt PCA [5] and Kernel Direct Discriminant Analysis (KDDA) [6] for comparison.

Fig. 3 depicts the obtained Equal Error Rate (EER, the operating point where FAR and FRR are equal) of RMT-SIN method as functions of variance of the multiplicative vector σ^2 and translation value d. The dimensionality of the feature vector is set to $N = 100$ based on empirical results. It can be observed from Fig. 3-b and -d that without translation, zero EER can not be produced in UD scenario, which indicates weak changeability. This is consistent with our analysis in Section 3 and the plot in Fig. 1-b, that by using RMT directly, clear separation of SK and DK distribution can

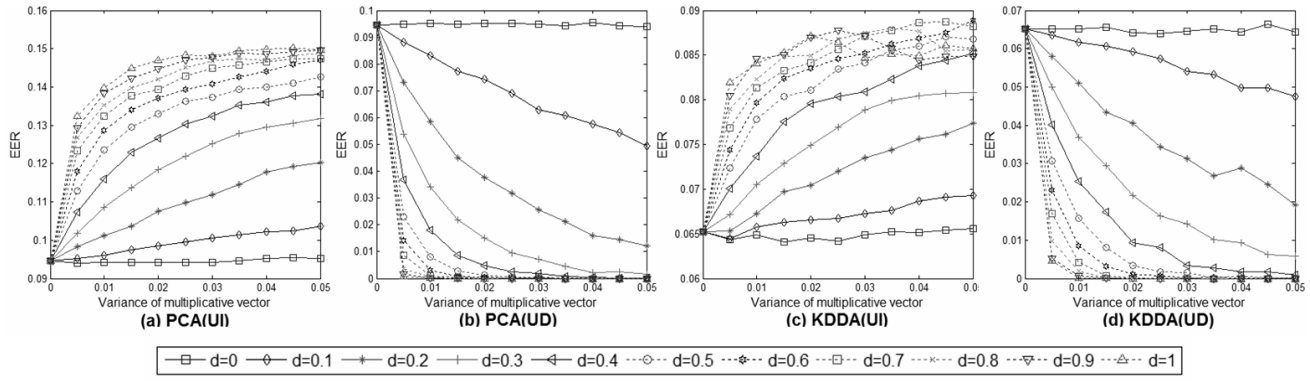

Figure 3. Obtained EER of RMT-SIN method: (a) PCA UI, (b) PCA UD, (c) KDDA UI, (d) KDDA UD.

not be accomplished. As shown in Fig. 1-d, with proper translation, the DK distribution shifts to the right towards 0.5, and clear separation of SK and DK distributions can be obtained. This is confirmed in Fig. 3-b and -d that zero EER can be achieved in UD scenario by proper translation. On the other hand, since the SK distribution in Fig. 1-d also shifts to the left as the translation value increases, which indicate deviation from the characteristics of the original features, the performance in the UI scenario will possibly degrades as d increases, as shown in Fig. 3-a and -c. Therefore, the proposed method has a tradeoff between privacy and performance.

To provide a comparison with the performance of the original feature extractors, Fig. 4 plots the receiver operating characteristic (ROC) curve of different methods, as a function of Genuine Accept Rate (complement of FRR) and FAR. For the original features, Euclidean distance and Cosine distance are used as similarity measures. For the RMT-SIN method, the parameters are set to $\sigma_r^2 = 0.03$ and $d = 2$ as a balance point between privacy and accuracy. It can be seen that the proposed method outperforms that of the original features in the UI scenario. In the UD scenario, it produces FAR=0 at all selections of the system threshold values, which demonstrates strong changeability.

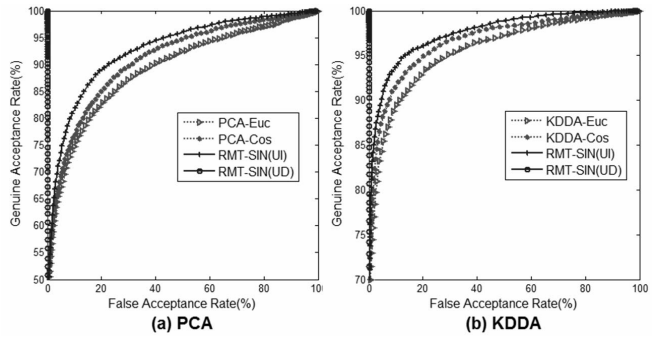

Figure 4. ROC curve: (a) PCA, (b) KDDA .

VI. Conclusion

This paper has presented a new approach for cancelable face recognition using random multiplicative transform in conjunction with a sorted index number approach. The changeability and privacy protecting properties of the proposed method is analyzed in detail. Extensive experimentation demonstrates that the introduced solution outperforms the original features, and is capable of producing biometric template with strong changeability. Although we focus on face based biometric verification in this paper, the analysis is general for features in continuous domain, and it is expected that such method can also be applied to other biometrics.

Acknowledgment

This work is supported in part by the Natural Sciences and Engineering Research Council of Canada (NSERC).

References

[1] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric Cryptosystems: Issues and Challenges", Proceedings of the IEEE, vol. 92, no. 6, pp. 948-960, 2004

[2] R. M. Bolle, J. H. Connel, N. K. Ratha, "Biometric perils and patches", Pattern Recognition, vol. 35, pp. 2727-2738, 2002

[3] Y. Wang, and D. Hatzinakos, "Sorted index numbers for privacy preserving face recognition", EURASIP Journal on Advances in Signal Processing, vol. 2009, Article ID 260148, 16 pages, 2009. doi: 10.1155/2009/260148.

[4] H. A. David, H. N. Nagaraja, Order Statistics, 3rd Edition, Wiley, 2003, Chapter 2 and 3.

[5] M. Turk, A. Pentland, "EigenFaces for recognition", Journal of Cognitive Neuroscience 13(1) (1991) 71-86

[6] J. Lu, K.N. Plataniotis, and A.N. Venetsanopoulos, "Face Recognition Using Kernel Direct Discriminant Analysis Algorithms", IEEE Transactions on Neural Networks, Vol. 14, No. 1, Page: 117-126, January 2003.