SECTORED RANDOM PROJECTIONS FOR CANCELABLE IRIS BIOMETRICS

[1]*Jaishanker K. Pillai,* [1]*Vishal M. Patel,* [1]*Rama Chellappa and* [2]*Nalini K. Ratha*

[1]Department Of Electrical & Computer Engineering
Center for Automation Research,
UMIACS, University of Maryland,
College Park, MD 20742.
{jsp,pvishalm,rama}@umiacs.umd.edu

[2]IBM Watson Research Center
19, Skyline Drive,
Hawthorne,
NY 10532.
ratha@us.ibm.com

ABSTRACT

Privacy and security are essential requirements in practical biometric systems. In order to prevent the theft of biometric patterns, it is desired to modify them through revocable and non invertible transformations called Cancelable Biometrics. In this paper, we propose an efficient algorithm for generating a Cancelable Iris Biometric based on Sectored Random Projections. Our algorithm can generate a new pattern if the existing one is stolen, retain the original recognition performance and prevent extraction of useful information from the transformed patterns. Our method also addresses some of the drawbacks of existing techniques and is robust to degradations due to eyelids and eyelashes.

Index Terms— Cancelable Biometrics, Secure Biometrics, Iris, Random Projections.

1. INTRODUCTION

With the rapid advancement of biometric technologies for personal authentication, issues such as privacy and protection of personal data become extremely relevant. To deal with them, the notion of Cancelable Biometrics has been introduced. The objectives of a Cancelable Biometric are as follows [1]:

- Different templates should be used in different applications to prevent cross matching.
- Template computation has to be non-invertible to prevent illegal recovery of biometric data.
- Revocation and reissue should be possible in the event of compromise and
- Recognition performance should not degrade when a cancelable biometric template is used.

Iris is one of the most promising biometric for personal verification. The texture patterns on the iris remain relatively stable through out one's life time and are found to be unique to each person. Designing a cancelable formulation for iris biometrics is an important step towards deploying it in practical applications. In this paper, we propose Sectored Random Projections (SRP) for Cancelable Iris Biometric (CIB). Our algorithm has the following novel features:

1. We study the effects of Random Projections (RP) for CIB and introduce sectored random projections.
2. Our algorithm can generate a different iris pattern for each application, create a new pattern if the existing one is stolen, maintain the original recognition performance and also prevent the extraction of useful information from the transformed patterns.
3. Since the only block to be added for cancelability is a matrix multiplication (using a precomputed matrix), our method can easily be incorporated into existing iris recognition systems.
4. Unlike existing techniques for cancelability, the proposed method does not suffer from a reduction in useful iris area and is also robust to common outliers in iris data due to the presence of eyelids, eyelashes and specular reflections.

The work of first three authors was supported by MURI from the Office of Naval Research under the Grant $N00014\_08\_I\_0638$

2. BACKGROUND

The concept of cancelable biometrics was first introduced by Ratha *et al.* in [2, 3]. In [4], RPs of discriminative features were used for cancelability in face biometrics. The pioneering work in the field of cancelable iris biometric was proposed in [5]. Other schemes have also been introduced to improve the security of iris biometric. See [1, 6, 7, 8, 9] and the references therein for more details.

In [5], four non invertible and revocable transformations were introduced for cancelability. The first method, namely GRAY-COMBO, transforms the Gabor features by circularly shifting and adding rows at random. BIN-COMBO, the second method, applies similar transformations on the iris codes by random shifting and XOR-ing. As pointed out by the authors, these methods gradually reduce the amount of information available for recognition. Since these methods employ linear transformations on the Gabor feature vectors, they are also sensitive to outliers in the form of eyelids, eye lashes and specular reflections. As perfect segmentation of iris images is difficult in practice, the performance of the recognition algorithm drops after transformation. Also different regions of the iris have different noise levels as demonstrated in [10]. Applying a global linear transform will combine the good and the bad regions, degrading the performance. On the other hand, as will be illustrated in the following sections, our method does not suffer from these limitations.

The other two methods introduced in [5] namely GRAY-SALT and BIN-SALT add random patterns or synthetic iris patterns to the Gabor features and iris codes, respectively. Though they do not suffer from the problem of outlier amplification and reduction of useful area, it is difficult to decide the relative strength of the noise patterns to be added. Adding very strong patterns will reduce the discriminative capacity of the original iris patterns and hence lead

to lower recognition results. Adding weaker patterns can lower the non-invertibility property, making it easier to extract useful information about the original iris biometric from the transformed patterns. Also, if the added patterns are compromised, the original iris patterns could be extracted from the transformed patterns by a simple subtraction operation. On the other hand, our method retains the non invertibility property even when the random matrix is compromised, as explained in Section 5.

In this paper, we introduce a new cancelable iris scheme based on random projections. Our method is comprised of two steps: feature extraction and random projections. In the feature extraction stage, Gabor features are extracted from the segmented iris image which form an N dimensional feature vector $\mathbf{g}$. This feature vector is then projected onto a random subspace by a random $n \times N$ matrix Φ, where $n \leq N$. This process is described as follows:

$$\mathbf{y} = \Phi \mathbf{g},$$

where $\mathbf{y}$ is the n dimensional RP vector. Entries in both $\mathbf{g}$ and Φ are complex numbers. We will show theoretically and empirically that our scheme based on RP meets all of the criteria required for a good cancelable iris scheme.

3. RANDOM PROJECTIONS

Since we are embedding N dimensional feature vectors in a space of a lower dimension n, for iris recognition to be effective, it is important that the relative distances between any two points in the feature space be preserved in the output random space. This is characterized by the Johnson-Lindenstrauss (JL) lemma [11, 12, 13].

Lemma 1. *(Johnson-Lindenstrauss) Let $\epsilon \in (0,1)$ be given. For every set S of $\sharp(S)$ points in $\mathbb{R}^N$, if n is a positive integer such that $n > n_0 = O\left(\frac{\ln(\sharp(S))}{\epsilon^2}\right)$, there exists a Lipschitz mapping $f : R^N \rightarrow R^n$ such that*

$$(1-\epsilon)\|\mathbf{u}-\mathbf{v}\|^2 \leq \|f(\mathbf{u})-f(\mathbf{v})\|^2 \leq (1+\epsilon)\|\mathbf{u}-\mathbf{v}\|^2 \quad (1)$$

for all $\mathbf{u}, \mathbf{v} \in S$.

This lemma essentially states that, a set S of points in $\mathbb{R}^N$ can be embedded into a lower-dimensional Euclidean space $\mathbb{R}^n$ such that the pairwise distance of any two points is approximately maintained. In fact, it can be shown that f can be taken as a linear mapping represented by an $n \times N$ matrix Φ whose entries are randomly drawn from certain probability distributions. This in turn implies that it is possible to change the original form of the data and still preserve its statistical characteristics useful for recognition.

In recent years, various improvements in the proof and the statement of the JL lemma have been made (see [12] and [13] for more details). Let Φ be an $n \times N$ random matrix with $n \leq N$ such that each entry $\phi_{i,j}$ of Φ is an independent realization of q, where q is a random variable on a probability measure space (Ω, ρ). It has been shown that given any set of points S, the following are some of the matrices that will satisfy (1) with high probability, provided n satisfies the condition of the Lemma 1 [12]:

- $n \times N$ random matrices Φ whose entries $\phi_{i,j}$ are independent realizations of Gaussian random variables $\phi_{i,j} \sim N\left(0, \frac{1}{n}\right)$.
- Independent realizations of ± 1 Bernoulli random variables

$$\phi_{i,j} \doteq \begin{cases} +1/\sqrt{n}, & \text{with probability } \frac{1}{2} \\ -1/\sqrt{n}, & \text{with probability } \frac{1}{2}. \end{cases}$$

- Independent realizations of related distributions such as

$$\phi_{i,j} \doteq \begin{cases} +\sqrt{3/n}, & \text{with probability } \frac{1}{6} \\ 0, & \text{with probability } \frac{2}{3} \\ -\sqrt{3/n}, & \text{with probability } \frac{1}{6}. \end{cases}$$

4. SECTOR BASED RANDOM PROJECTIONS

In practice, we have found that applying the random projections directly on the iris images leads to a degradation in performance due to the following reasons. First of all in real iris images, despite good segmentation algorithms, there will still be some outliers due to specular reflections, eye lashes and eyelids. Also, different parts of the iris have different quality [10]. By taking a linear transformation of the entire vector, we combine the good iris regions as well as the outliers and thereby corrupt the data. To avoid this, we divide the iris into different sectors, apply random projections on each sector separately and concatenate them to form the cancelable template (see Fig. 1). So outliers can corrupt only the corresponding sector

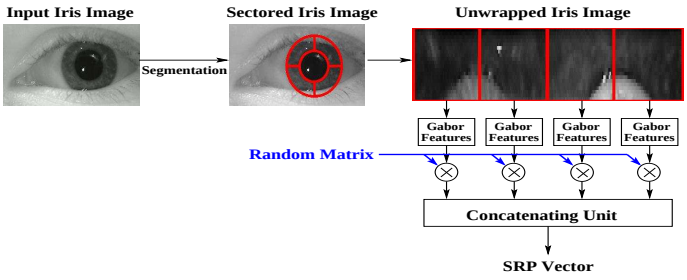
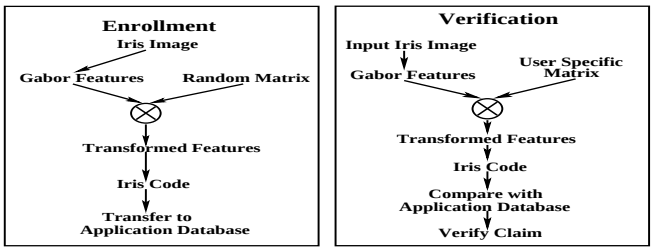


Fig. 1. Block Diagram Of Sectored Random Projections

and not the entire iris vector. Since outliers due to eyelids and eye lashes are present only at the top and bottom of the iris images, only a small number of sectors get corrupted in practice. This mitigates the problem of reduction in useful information, mentioned in [5].

5. CANCELABLE IRIS BIOMETRIC SYSTEM

In this section, we explain the proposed CIB system. The enrollment system extracts the iris pattern of the user, computes the Gabor features, applies a different RP for each application and transfers the new pattern to the application database. Note that even if the transformed pattern and the key (i.e. the projection matrix) are stolen, it is difficult for a hacker to get a pattern close to the original iris pattern since it is an underdetermined problem due to the dimension reduction caused by the projection. Also even if a hacker steals the user's iris pattern either from the client system or using a hidden scanner, without knowing the random projection he/she cannot generate the transformed patterns required by the application. During the verification stage, the application obtains the iris image and the RP matrix from the user, computes the transformed pattern and compares it with the ones in its database. In case, the RP matrix or the transformed patterns are compromised, one can create a new RP matrix and obtain a new transformed pattern which can be updated into the application database. Instead of the user providing the random matrix during verification, the application can generate and store it along with the cancelable template in its database. Though this will be an easier scheme for the user to operate, it is less secure as a hacker can get both the random projection matrices and the transformed patterns by breaking into the application database.



(a) (b)

Fig. 2. Block Diagram of the proposed system.

6. EXPERIMENTS AND DISCUSSION

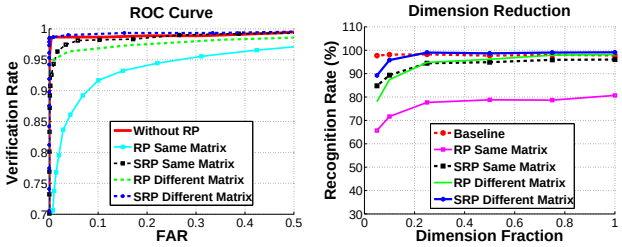
We present the results of our algorithm on the MMU dataset [14]. Out of the 5 images available per class, 4 were used as part of the gallery and the fifth one was used as the probe. To illustrate the robustness of our method to outliers in the iris data in the form of eyelids, eye lashes and specular reflections, we used a simple segmentation scheme extracting just the circles corresponding to the pupil and iris using the publicly available code of Masek *et al.* [15]. We assume that the iris images are registered correctly. The iris region thus obtained were unwrapped into a rectangular image of size 10×80. Its Gabor features were obtained and concatenated to form an iris vector of length 800.

We used the random Gaussian matrix in our experiments, though other random matrices mentioned in Section 3 also give similar results. Since the Gabor features are complex vectors, the random projection involves multiplying the Gabor vector with a complex matrix, whose real and imaginary entries are Gaussian random variables. We multiply the iris vector either with the same random Gaussian matrix for all the users or different random matrices for different users to obtain the RP "Same Matrix" and "Different Matrix" vectors, respectively. Similarly, we multiply each sector of the iris vector with the same random Gaussian matrix to obtain the SRP "Same Matrix" vector. To get the SRP "Different Matrix" vector, still all the sectors of one user are multiplied with the same random Gaussian matrix. However this matrix is different for different users. In our experiments, we fixed the number of sectors to eight. Increasing the number of sectors did not improve the performance significantly.

Once the random vectors are obtained from the Gabor features of the iris image, we compute the iris codes using [15] and use the Hamming distance to decide the class of the probe iris image. We present the Receiver Operating Characteristic (ROC) curves and the Hamming distance distributions for RP and SRP in the subsections below.

Performance Of RP And SRP: Fig. 3(a) plots the ROC characteristics for the iris images in the MMU dataset for the original and transformed iris patterns. As can be observed, the SRP performs better than RP for both the same matrix and different matrix cases. Also using different matrices for each class gives better performance than using the same matrix for all classes. In Fig. 4(c), we compare the distribution of the genuine and impostor normalized Hamming distance for the original and transformed iris patterns. We can observe that the distribution of the genuine Hamming distance remains almost the same after applying the SRP. The original and Same Matrix SRP cases have similar impostor Hamming distance distributions. But the Different Matrix SRP case has an impostor distribution which is more peaked and farther from the genuine distribution, indicating superior performance.

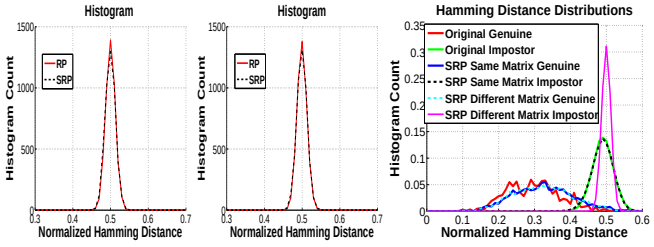
We believe that these observations can be explained as follows. Since RP obtains the random vector by applying a linear transform on the entire iris vector, it combines the different regions of the iris which have different quality measures. In particular, the image regions corresponding to the eyelids and eye lashes, which occlude the iris vector is combined with the good iris regions, thereby corrupting the whole iris vector. On the other hand, SRP takes linear transform on each sector separately and hence does not corrupt the good iris regions by combining them with the bad ones. The bad regions can corrupt only their corresponding sectors, which will occupy only a small region in the output iris vector and hence do not significantly degrade the recognition performance. Also, using different matrices per class increases the between class distance without changing the within class distance and hence gives superior performance.



(a) (b)

Fig. 3. (a) ROC Characteristics For The MMU Dataset. SRP performes better than the RP. Also using different matrices for each class gives better performance. (b) Plot of the recognition rate with dimension reductions for the MMU dataset. Note that the performance remains the same up to 30% of the original dimension.

Normalized Hamming distance comparison between the original and the transformed patterns: In Fig. 4(a) and (b), we illustrate the normalized Hamming distance between the iris codes from the original and the transformed iris vectors for the "Same Matrix" and "Different Matrix" cases, respectively. Ideally we want the two iris codes to be independent and hence the Normalized Hamming distance should be 0.5. The figure shows that the histogram of the hamming distance peaks at 0.5, empirically verifying that the random projected iris vectors are significantly different from the originals ones. So a hacker cannot get any direct information about the original iris patterns from the transformed patterns. Note that the hacker may still be able to develop a transformation which takes the projected patterns close to the original iris patterns, but the effect of such transformations is not investigated in this paper.



(a) (b) (c)

Fig. 4. Plot of the histograms of the Normalized Hamming Distance between the original and transformed vectors for (a) Same Matrix, (b) Different Matrix. (c) Comparison of the distribution of the Genuine and Impostor normalized Hamming distances for the original and transformed patterns.

Table 1 provides the statistics of the normalized Hamming dis-

tance for RP and SRP. As can be seen, both the cases have mean normalized Hamming distance very close to 0.5 with a very low standard deviation. The mean for the RP case is closer to 0.5 when compared to SRP. This is expected as RP applies a global linear transform and hence the transformed vectors will be farther from the original vectors when compared to a local linear transformation, as done in SRP.

Table 1. Statistics Of The Normalized Hamming Distance.

Methods	Mean	Standard Deviation
Without RP	0	0
RP, Same Matrix	0.4999	0.0124
SRP, Same Matrix	0.4993	0.0124
RP, Different Matrix	0.5001	0.0126
SRP, Different Matrix	0.4997	0.0136

Comparison with Salting: In Table. 2, we present the recognition rates and the corresponding mean Hamming distance for the salting method [5] for various noise levels. The best recognition rate and the best Hamming distance for the Salting method are 96.6% and 0.494 respectively. For SRP, we obtained a recognition rate of 97.7% at a hamming distance of $.499$. Thus both the recognition performance and security (non-invertibility) are higher for SRP when compared to the Salting method.

Table 2. Comparison with Salting method. The Recognition Rate(RR) and mean Hamming Distance(HD) are provided for the Salting and SRP methods. The recognition rate obtained using SRP is higher than that of the Salting method. Also SRP gives mean Hamming distance closer to .5 when compared to the Salting method.

Quantity	Salting					SRP
RR(%)	94.2	94.7	95.3	96.6	94.0	97.7
HD	0	.467	.480	.491	.494	.499

Effect of dimension reduction: In Fig. 3(b), we demonstrate the robustness of random projections to reduction in the original dimension of the feature vector. The SRP vectors retain their original performance for up to 30% reduction in the original dimension for both the same and different matrix cases. Dimension reduction further strengthens the non-invertibility of our transformation as there will be infinite possible iris vectors corresponding the reduced dimension random vectors obtained by RP or SRP.

Note that our SRP method meets the various constraints mentioned in Section 1. By using different RP matrices, we can issue different templates for different applications. The dimension reduction as well as the empirical results demonstrate that original iris patterns cannot be obtained from the randomly projected patterns. If a transformed pattern is compromised, we can reissue a new pattern by applying a new random projection to the iris vector. From the JL lemma and the experiments, we see that SRPs preserve the original recognition performance. Furthermore, since our method is based on pseudo-random number generation, we only consider the state space corresponding to the value taken by the seed of the random number generator. Hence, instead of storing the entire matrix, one only needs to store the seed used to generate the RP matrix.

7. CONCLUSIONS

We have proposed an efficient algorithm for CIB based on Sectored Random Projections. Experiments show that the proposed method meets the criteria of cancelability. Moreover, the JL Lemma provides a theoretical justification for using RPs for cancelability. Since the only block to be added for cancelability is a matrix multiplication, our method can easily be incorporated into existing iris recognition systems, thereby improving the security. Future work include analyzing the possible transformations which can extract useful information from the random projected patterns and the effect of misalignment of iris patterns on the performance.

8. REFERENCES

[1] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric Template Security," *EURASIP Journal on Advances in Sig. Proc., Special issue on Biometrics*, vol. 2008, no. 113, pp.1–17, 2008.

[2] N.K. Ratha, J.H. Connel and R.M. Bolle "Enhancing security and privacy in biometrics-based authentication systems," *IBM Systems Journal*, vol. 40, no. 3, pp.614–634, 2001.

[3] R.M. Bolle, J.H. Connel and N.K. Ratha, "Biometrics Perils and Patches," *Pattern Recognition*, vol. 35, no. 12, pp.2727–2738, 2002.

[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 Analysis and Machine Intelligence* ,vol. 28, no. 12, pp.1892–1901, Dec. 2006.

[5] J. Zuo, N.K. Ratha and J.H. Connell, "Cancelable Iris Biometric," *Proc. International Conference on Pattern Recognition*, pp.1–4, Dec. 2008.

[6] G. I. Davida, Y. Frankel and B. J. Matt, "On enabling secure applications through off-line biometric identification," *IEEE Symposium on Security and Privacy*, pp.148–157, 1998.

[7] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," *IEEE Trans. Computers*, vol. 55, no. 9, pp.1081–1088,2006.

[8] S. Kanade, D. Petrovska-Delacretaz and B. Dorizzi, "Cancelable iris biometrics and using error correcting codes to reduce variability in biometric data," *CVPR*, 2009.

[9] A. Juels and M. Wattenberg, "A fuzzy commitment scheme,"*ACM Conference on Computers and Communications Security*, pp.28–36, 1999.

[10] Y. Chen, S. C. Dass, A. K. Jain, "Localized iris image quality using 2-D wavelets", *Springer LNCS 3832: International Conference on Biometrics*, 2005, pp. 373381.

[11] W.B. Johnson and J. Lindenstrauss, "Extensions of Lipschitz maps into a Hilbert space," *Contemp. Math.*, pp.189–206, 1984.

[12] D. Achlioptas, "Database-friendly Random Projections," *ACM SIGACT-SIGMOD-SIGART Symp. on Principles of Database Systems*,pp.274–281, 2001.

[13] R. Baraniuk, M. Davenport, R. DeVore and M. Wakin, "A Simple Proof of the Restricted Isometry Property for Random Matrices,"*Constructive Approximation*, vol. 28, no. 3, pp.253–263,Dec. 2008.

[14] Malaysia Multimedia University. MMU1 iris image database. http://pesona.mmu.edu.my/ccteo.

[15] L. Masek, P. Kovesi, "MATLAB Source Code for a Biometric Identification System Based on Iris Patterns", The University of Western Australia. 2003.