Annals of Data Science
https://doi.org/10.1007/s40745-018-0172-1

A Modified Cancelable Biometrics Scheme Using Random Projection

Randa F. Soliman[1] · **Mohamed Amin**[1] · **Fathi E. Abd El-Samie**[2]

Received: 30 March 2018 / Revised: 27 July 2018 / Accepted: 30 July 2018

Abstract
This paper presents a random projection scheme for cancelable iris recognition. Instead of using original iris features, masked versions of the features are generated through the random projection in order to increase the security of the iris recognition system. The proposed framework for iris recognition includes iris localization, sector selection of the iris to avoid eyelids and eyelashes effects, normalization, segmentation of normalized iris region into halves, selection of the upper half for further reduction of eyelids and eyelashes effects, feature extraction with Gabor filter, and finally random projection. This framework guarantees exclusion of eyelids and eyelashes effects, and masking of the original Gabor features to increase the level of security. Matching is performed with a Hamming Distance (HD) metric. The proposed framework achieves promising recognition rates of 99.67% and a leading Equal Error Rate (EER) of 0.58%.

Keywords Iris recognition · Cancelable biometrics · Random projection

1 Introduction

Biometrics are adopted nowadays in most security systems. Biometric systems include signal-based systems as well as image-based systems. Signal-based systems include speaker identification and Electrocardiography (ECG) identification. Image-based systems include gesture, palmprint, fingerprint, handwritten signature, face, gait, hand geometry, and iris recognition. Iris recognition has been adopted as a widely-used biometric recognition system since 1987 by Leonard and Aran [1]. The basics of iris recognition have been developed and elaborated by Daugman in [2]. The work of Daugman

✉ Randa F. Soliman
randafouad2010@yahoo.com

1 Mathematics and Computer Science Department, Faculty of Science, Menoufia University, Shebin El-Kom 32511, Egypt

2 Department of Electronics and Electrical Communications Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt

Published online: 13 August 2018

is based on generating IrisCodes for the features extracted from iris images. The features extracted in this scheme are in the form of Gabor features and are coded in binary format. Hamming distance is adopted in this scheme for classification. Iris recognition systems comprise different steps; localization, normalization, coding, and classification. Different refinements have been presented on the steps of this framework. For example, the wavelet transform [2], and multi-resolution analysis of the localized iris have been used for more robust feature extraction [3, 4]. Another scheme developed by Wildes [5] and Masek [6] adopted the Hough transform for the determination of iris boundaries in the localization step. These methods have to search enormously in a three-dimensional parameter space, and hence they have a high computational cost.

In [7] and [8], the active contours are assumed for the non-circular shape of iris images to obtain the actual shape and perfect representation rather than the circle. Thresholding based on image histogram, particularly for pupil boundaries, was utilized by other approaches, because pupil boundaries are relatively darker than the rest of the image as introduced by Dey and Samanta [9].The technique proposed by An et al. [10] recognizes people by using distributed surveillance cameras for user re-identification application. In a coarse-to-fine algorithm that was introduced by Soliman et al. [11], thresholding is used as the first step instead of the weary search of a three-dimensional parameter space for a large number of image pixels. Although biometric recognition systems perform well in user authentication, they suffer intentionally or unintentionally compromises of biometric information. A solution to this privacy problem can be achieved through the utilization of cancelable biometric templates in recognition to save the biometric information from external attacks [12].

Cancelable biometrics have evolved as a solution for the hacking attacks on the biometric databases in the last decades. The basic concept of cancelable biometrics is the masking of either the signal or image or the extracted features from them in order to increase the security of biometric databases [13]. Some methods that develop a masking strategy for the original signals or images depend on encryption and hashing [14]. On the other hand, there exist other schemes that depend on geometric deformations of the original signals and images [12]. Unfortunately, these schemes have not been investigated on iris images. In this paper, we adopt a strategy for cancelable iris recognition based on encryption with random projection in the feature space. Nandakumar and Jain [15] claimed that the large degree of security achieved with cancelable biometrics may come at the cost of lower verification accuracy. On the contrary, the proposed approach for cancelable iris recognition maintains high accuracy results in the presence of cancelability.

To build a realistic cancelable biometric system, we need to achieve diversity, renewability, non-invertibility, and high recognition performance [16]. Diversity means the ability to generate different templates that can be used as cancelable biometric templates with different characteristics. Also, renewability is the ability of the cancelable biometric system to generate new templates for different new applications to avoid using the same cancelable template in different verification applications. Moreover, non-invertibility means that the used transform is non-invertible to increase the degree of security. Finally, the accuracy of detection needs to be close to the levels achieved by the normal biometric systems. These four mentioned criteria have been successfully achieved with the proposed scheme as will be highlighted later.

2 Related Work

Privacy concerns have raised up as the biometric template is a unique person identifier. If there is a database which ties the user to his unique biometric template, it could be used illegally to monitor the activities of the user. These threats have to be treated, and one prospective solution is the cancelable biometrics. Cancelable biometrics depend on template transformation schemes that utilize intentional repeated distortions to present security to biometric templates. The distortions can be performed either at feature level or at signal level to obtain transformed templates [13]. In this section, some of the previous researches on iris template protection are discussed.

Ratha et al. [17] first introduced the notion of biometrics cancelability. In their works, they rearranged the fingerprint minutiae in polar and Cartesian domains to obtain the cancelable templates. Although their work renders a satisfactory accuracy performance, the non-invertibility was seen weak [18]. Instead of utilizing the whole iris template as reported in [19], Pillai et al. [20] used sectored random projections for generating the cancelable iris templates. Their work secures the original template while maintaining the accuracy performance. Rathgeb et al. [21, 22] utilized Bloom filter to construct cancelable templates from IrisCodes with a comparison between the transformed biometric templates generated with Bloom filters. Zuo et al. [23] suggested the generation of cancelable iris templates by applying the row permutation on IrisCodes. In [24], a random key is utilized to convert an online signature data into discrete sequences that are convolved together to create the cancelable template. Other cancelable biometric methods have been presented by Syarif et al. [25] and Teoh et al. [26, 27] for increasing the recognition rates of cancelable templates. They employed secret random numbers to pattern the original biometric features into transformed templates.

Ouda et al. [28, 29] proposed a bio-encoding scheme for cancelable biometrics. They concluded that the accuracy performance is preserved compared to those of the unprotected counterparts. However, Lacharme [30] clarified that the non-invertible property of bio-encoding is violated. Hämmerle-Uhl et al. [31] utilized block remapping methods to perform non-invertible transformations. In spite of keeping high accuracy levels with block remapping methods, Jenisch et al. [32] proved that most of the original iris images can be recovered from the stolen patterns. The idea of generating a look-up table for cancelable templates was presented by Dwivedi and Somnath [33]. They guarantee the rotation invariance of the iris pattern by a shifting process of a reference iris template created from the same subject. In [34, 35], a resistant pre-image cancelable biometric method was introduced. An associative memory is used in this method for encoding the cancelable transformation parameters with high recognition rates.

This paper presents a cancelable iris recognition system that works on Gabor features extracted from iris images. These features are subject to random projection with Gaussian random kernels. The objective of the random projection process is to alter the generated features through multiplication with a random matrix under the constraint that the features extracted from different patterns remain distinctive. The recognition performance of the proposed system is comparable with those of traditional Gabor filter based iris systems.

For the rest of the paper, a brief introduction about the random projection is presented in the third section. The proposed scheme is explained in detail in Sect. 4. The experimental results and analysis are covered in Sect. 5. Section 6 gives a discussion of the security concerns. Finally, the conclusion of the paper is presented in Sect. 7.

3 Random Projection

Random projection can be utilized for creating cancelable biometric templates [36]. Random projection is performed through the multiplication of the obtained feature vector with a random matrix as follows.

$$\mathbf{y} = \mathbf{M}\mathbf{x} \tag{1}$$

where $\mathbf{x}$ is the feature vector extracted from the iris image, $\mathbf{M}$ is the Gaussian random projection matrix, and $\mathbf{y}$ is the cancelable feature vector. The heart of the random projection process is to guarantee that the estimated distance between two processed versions of the feature vectors generated through random projection is larger or equal to the estimated distance between the original corresponding feature vectors. This meaning coincides with Johnson–Lindenstrauss (JL) lemma [37].

Lemma 1 *For any integer p and any $0 < \epsilon < 1$, set n as a positive integer such that $n \geq O\left(\epsilon^{-2} \log p\right)$. For every set S of p points in $\mathbb{R}^N$, there is a map $f: \mathbb{R}^N \rightarrow \mathbb{R}^n$ such that, for all $\boldsymbol{g}$, $\boldsymbol{I} \in S$,*

$$(\mathbf{1} - \epsilon)||\mathbf{g} - \mathbf{I}||^2 \leq ||\boldsymbol{f}(\mathbf{g}) - \boldsymbol{f}(\mathbf{I})||^2 \leq (\mathbf{1} + \epsilon)||\mathbf{g} - \mathbf{I}||^2 \tag{2}$$

In our case of cancelable iris recognition with random projection, we have $\boldsymbol{g}$ and $\boldsymbol{I}$ as the two original feature vectors, and $f(\mathbf{g})$ and $f(\mathbf{I})$ as the new feature vectors generated after random projection. The requirements of Johnson-Lindenstrauss lemma can be satisfied with Bernoulli or Gaussian random matrices.

4 Proposed Scheme

In this section, we present the proposed scheme for iris biometric cancelability based on random projection. The proposed scheme is illustrated in Fig. 1. It has two modes of operations; enrollment and verification. The enrollment mode comprises three major operations; pre-processing, feature extraction, and random projection to enroll biometric traits into the dataset. Also, the verification mode has three main steps, pre-processing, feature extraction, and feature matching with the enrolled IrisCodes.

4.1 Pre-processing

The pre-processing step acquires a couple of basic operations; localization and normalization. In localization, the iris image is segmented and for this purpose, we adopt a coarse-to-fine method [11]. The coarse stage relies on image thresholding to separate

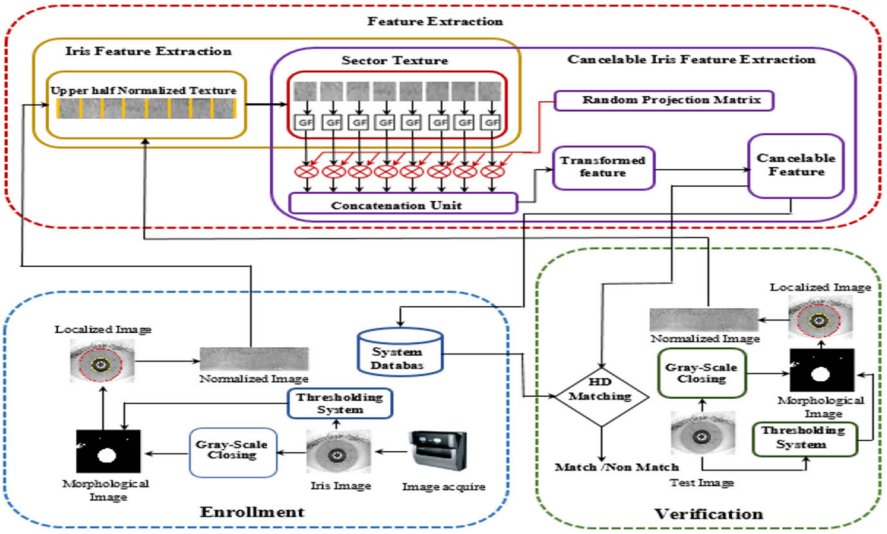

Fig. 1 Illustration of the workflow layout of the proposed cancelable recognition system

dark parts. The histogram analysis leads to the following empirical formula that builds a three-level thresholding system:

$$Threshold = \begin{cases} 115 : \sum_{i=150}^{255} h_i < 0.75MN \\ 50 : \sum_{i=0}^{100} h_i < 0.3MN \\ 85 : Otherwise \end{cases} \quad (3)$$

where h_i is the histogram value corresponding to pixel intensity i. M and N are the numbers of rows and columns of the image, respectively. The thresholding with three levels makes the proposed scheme suitable for various intensity conditions. Algorithm 1 illustrates the detailed procedure of the coarse stage.

Algorithm 1: Coarse Stage

Input: The iris image.
Output: The iris image subject to thresholding and morphological operations.
Step 1. Gray-scale closing with a disk structuring element.
Step 2. Selection of an appropriate threshold based on to Eq. (3).
Step 3. Gray image thresholding to obtain a binary image.
Step 4. Minimization of the specular reflections effect.
Step 5. Labeling of connected regions for obtaining the pupil.
Step 6. Setting the pupil initial center as the centroid of the area.

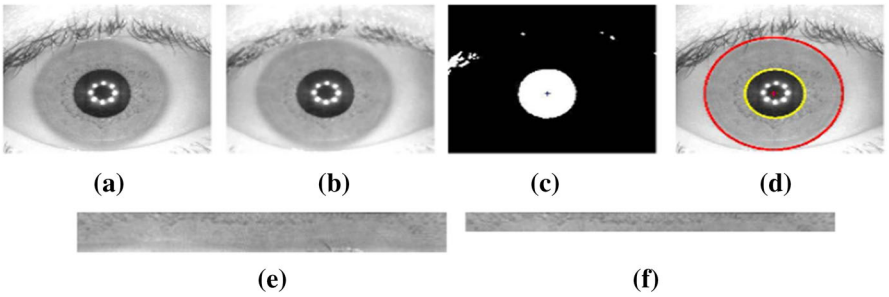

Fig. 2 Illustration of iris pre-processing: **a** Original image. **b** Image after gray-scale closing. **c** Image after thresholding and morphological processing with the centroid marked. **d** Localized iris. **e** Normalized iris. **f** Upper half of the normalized iris

Figure 2b demonstrates the gray-scale closing result of the sample image depicted in Fig. 2a. In Fig. 2c, the obtained image resulting from thresholding and morphological steps is given. Extraction of the initial central point, which represents the center for both iris and pupil boundaries, is performed with morphological processing. Algorithm 2 gives the steps of the fine stage.

Algorithm 2: Fine Stage

Input: The iris image with the marked centroid.
Output: Localized iris
Step 1. Resizing of the iris image into a quarter of its original size.
Step 2. Setting of the course stage initial center.
Step 3. Specifying the neighborhood area of 10×10 pixels around.
Step 4. Searching in two iris boundary sectors only not in all the 360°
Step 5. Generating the initial central point that represents the origin for the two sectors.

After morphological processing, circles with their related centers are imbricated upon the iris region as seen in Fig. 2d. Clearly, the annular iris image is recognized and selected easily for the recognition process. For the normalization, all the points are re-mapped in the iris portion into a polar form as shown in Fig. 2e. In normalization, only the upper half iris portion is considered as seen in Fig. 2f.

4.2 Feature Extraction

In feature extraction, the normalized iris is convolved with a one-dimensional Log-Gabor wavelet for extracting features. The two-dimensional normalized trait is divided into a set of one-dimensional signals. The one-dimensional signals are convolved with a one-dimensional Gabor wavelet. The normalized two-dimensional pattern rows are considered as one-dimensional signals. After that, the output is phase quantized into four levels. The encoding process produces a bitwise IrisCode including a set of information bits equivalent to the angular resolutions multiplied by the radial resolutions.

4.2.1 Cancelable Template Generation

In this process, the extracted features from the biometric pattern are projected into a random subspace after feature extraction. The iris image undergoes a segmentation to obtain a sectored iris, which is unwrapped later. The unwrapped iris is divided into different sectors. The random projection is applied to the features extracted from the sectors, and then concatenation is performed. As a result of this scheme, the top and bottom iris images outliers cause deterioration to fewer sectors, not the whole iris. To avoid deterioration in performance, the lower half of the normalized iris is removed and only the features of the upper half are considered in the proposed scheme. The upper-half features correspond to the inner part close to the pupil boundary, which diminishes the noise created by eyelashes and eyelids. Finally, we attain better cancelable IrisCodes from the concatenated outputs. Algorithm 3 illustrates the cancelable template generation.

Algorithm 3: Cancelable Template Generation

Input: The upper unwrapped half of the iris image.
Output: The transformed template.
Step 1: Reading of the upper unwrapped half of the iris image.
Step 2: Converting the upper unwrapped half of iris image into the double format.
Step 3: Sectoring of the upper unwrapped half of iris image into blocks.
Step 4: Extracting Gabor features from each sector.
Step 5: Application of random projection separately on each sector.
Step 6: Concatenation of features to obtain the transformed IrisCodes.

4.3 Feature Matching

Hamming distance is used as the metric of matching. Hamming distance (HD) is the summation of non-equivalent bits between the query and stored templates. It can be estimated with the exclusive-OR as follows:

$$Hamming\ Distance\ (HD) = \frac{1}{K}\sum_{i=1}^{K} S_i \oplus Q_i \tag{4}$$

where Q_i and S_i are ith the bits of the query and stored templates, respectively. K is the total number of bits in the template.

5 Experimental Results and Discussion

In this section, details of the experimental results describing the performance of the proposed scheme are presented. Moreover, a comparison study between the proposed scheme and some existing approaches is given.

5.1 Performance Evaluation

To evaluate the performance of the proposed scheme, the CASIA-IrisV3-Interval database [38] has been used. The HD is used to determine the IrisCode class. This proposed scheme is evaluated using EER and Receiver Operating Characteristics (ROC) curve [39]. The ROC curve is obtained by plotting True Positive Rates (TPR) against the False Positive Rates (FPR). The EER is the point at which the false rejection rate (i.e., $1-\text{TPR}$) and FPR hold equality at particular threshold values. The area under curve (AROC) for the original IrisCodes is 0.99971, while this value for the proposed scheme is 0.9998, as depicted in Fig. 4. The TPR is also known as the sensitivity, while the TNR is known as the specificity. The FRR measures the probability of falsely rejecting an iris as an imposter (intra-class) iris pattern and the FPR measures the probability of falsely accepting an imposter iris pattern as genuine (inter-class) iris pattern. Negative and positive predictive values (NPV and PPV) are utilized to estimate the matching performance using Eqs. (5) and (6).

$$\text{PPV} = \frac{\text{Number of true positives}}{\text{Number of true positives} + \text{Number of false positives}} \tag{5}$$

$$\text{NPV} = \frac{\text{Number of true negatives}}{\text{Number of true negatives} + \text{Number of false negatives}} \tag{6}$$

The values of these performance metrics are evaluated from the genuine and imposter scores. The EER is inversely proportional to the system performance. As seen in Table 2, EER (%) for the original IrisCodes is 0.83%; while it is 0.58% for the cancelable IrisCodes. A low EER value indicates a high recognition performance. Also, the separability between genuine and impostor distributions is measured by the decidability metrics $\acute{d}$ [28] which is computed as follows

$$\acute{d} = \frac{|\mu_i - \mu_g|}{\sqrt{(\sigma_i^2 + \sigma_g^2)/2}} \tag{7}$$

where μ_i and μ_g are the means and σ_i^2 and σ_g^2 are the variances of the impostor and genuine distributions, respectively. As shown in Table 1, the obtained values of the decidability metric for the original and proposed iris patterns are 4.31 and 4.37, respectively. The larger decidability values mean larger deviation between genuine and impostor distributions, which indicates a better recognition performance. The accuracy, NPV, PPV, specificity, and sensitivity of the proposed scheme are slightly increased with respect to the original counterparts.

Figure 3 shows a comparison between genuine and impostor HD distributions for the original and cancelable IrisCodes. It is obvious that the original IrisCode HD distributions are closer for both the genuine and imposter cases as shown in Fig. 3. On the other hand, the imposter distribution in the proposed scheme is obviously peaked and it is different from that of the original IrisCodes. Figure 4 gives the ROC curve for the proposed and original schemes. It is noticed that the proposed scheme performs better than the original one.

Table 1 Summary of performance metrics for the original and proposed schemes

Performance metric	Original IrisCodes [11]	Proposed scheme
Sensitivity (%)	99.5	99.8
Specificity (%)	99	99.5
NPV (%)	99.4975	99.8328
PPV (%)	99.005	99.5017
EER (%)	0.83	0.58
Accuracy (%)	99.25	99.6667
Decidability	4.3149	4.3667

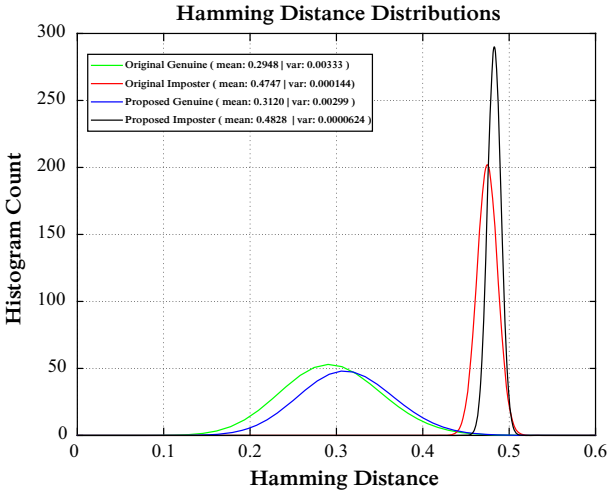

Fig. 3 Score distributions of the original and proposed cancelable schemes

In our experiments, we compared the proposed scheme with some state-of-the-art cancelable biometric schemes including Teoh et al. [27], Zuo et al. [23], Hammerle-Uhl et al. [31], Kumar et al. [39], Ouda et al. [28, 29], Rahulkar and Holambe [3]; Rathgeb et al. [21, 22], Tarek et al. [34, 35] schemes. From Table 2, the performance of the proposed scheme is better than those of the other considered schemes.

5.2 Robustness to Scaling and Rotation Effects

The robustness of the proposed scheme to rotation and scaling is tested. Using the CASIA-IrisV3 dataset, we randomly rescaled each test image with a scale factor s to examine its effect on the recognition rate. Table 3 shows the recognition rate results for the proposed scheme with $s \in [0.9, 1.1]$. One can see that the performance is slightly degraded when the images are subject to scale changes, which ensures that the proposed scheme preserves robustness to scaling effect.

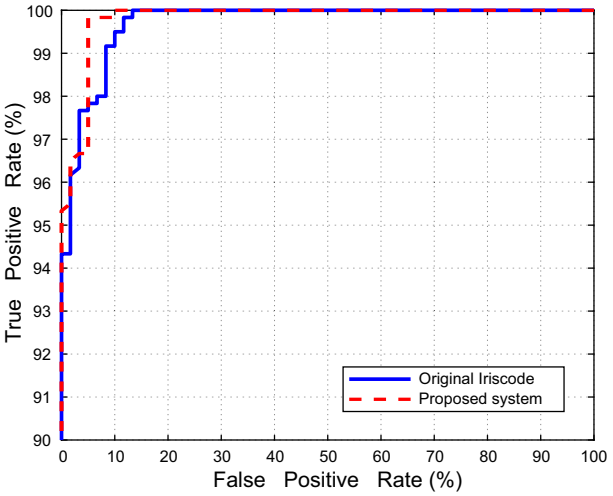

Fig. 4 ROC curve for the original and proposed cancelable schemes

Table 2 Summarized results of EER for different competing schemes on CASIA-IrisV3-Interval database

Scheme	Year	Performance (EER%)
Teoh et al. [27]	2004	4.81
Zuo et al. [23]	2008	4.41
Uhl et al. [31]	2009	1.30
Kumar et al. [39]	2010	1.48
Ouda et al. [29]	2010	5.54
Ouda et al. [28]	2011	6.27
Rahulkar et al. [3]	2012	1.91
Rathgeb et al. [21]	2015	1.14
Rathgeb et al. [22]	2014	8.98
Tarek et al. [34]	2016	3.56
Tarek et al. [35]	2017	2.001
Proposed		0.58

Table 3 Results of the scaling test

Recognition rate (%) for different scales				
$(s) = 0.9$	$(s) = 0.95$	$(s) = 1$	$(s) = 1.05$	$(s) = 1.1$
98.67	98.92	99.67	98.86	98.58

We randomly rotated each test image with an angle θ to examine the effect of θ on the accuracy. The results in Table 4 show the recognition rate for $\theta \in [-10°, 10°]$. We can observe that when the images are rotated with small angles, i.e.$-5°$ *or* $5°$, the proposed scheme is robust. In addition, when images are rotated with larger angles,

Table 4 Results of the rotation test

Recognition rate (%) for different rotation angles (θ)				
$(\theta) = -10°$	$(\theta) = -5°$	$(\theta) = 0°$	$(\theta) = 5°$	$(\theta) = 10°$
93.32	95.84	99.67	94.66	91.16

i.e.$-10°$ *or* $10°$, the proposed scheme performance deteriorates, but it is still the best in recognition rate.

6 Security Analysis

The cancelable biometric system requires security constraints as described, previously. In this section, analysis of renewability, diversity, non-invertibility, and distinctiveness constraints of the proposed scheme is presented. These security constraints ensure that the proposed system achieves the template protection schemes by keeping the recognition performance.

6.1 Renewability and Diversity

The cancelable scheme is revocable if it allows generation of a new key if the system storage is compromised to construct a new template for biometric data belonging to the same identity. During verification, both the test image and the random projection matrix are obtained from the user. Then, the cancelable template is estimated and a comparison with the dataset is performed. If a transformed iris template or a random projection matrix is compromised, a new random projection matrix can be easily generated to get a new cancelable template, which should be directly updated, in the application dataset. The user should not have to provide the random matrix through verification as the application is able to create the random matrix, and then it is stored in the cancelable IrisCodes database. It should be a simple technique for the user operation. On the other hand, with several random projection matrices, different IrisCodes for various applications can be issued. Thus, the property of diversity is also satisfied.

6.2 Non-invertibility

One of the most effective criteria in biometric cancelability is the non-invertibility. If the key has been lost and somehow a hacker gets access to that key, he may be able to form a random matrix from the information in that key. We have to guarantee that the hacker is not able to invert the cancelable IrisCodes. Also, if even the iris pattern is stolen by an observed scanner or from client systems, without having the random projection matrix, the hacker will not be able to create the transformed pattern needed by the application as it is an underdetermined issue due to dimensionality reduction resulting from the projection. So, the proposed scheme preserves the non-invertibility in the case of compromising the random Gaussian matrices. Figure 5 displays the

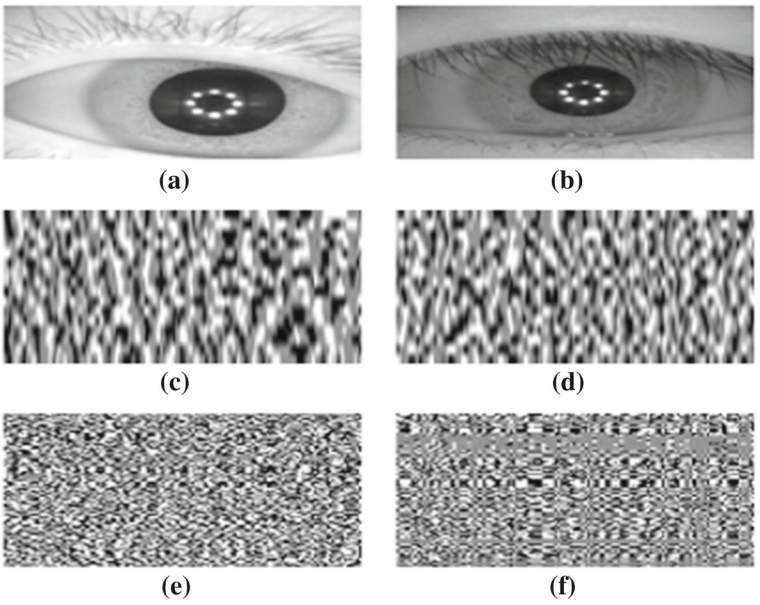

Fig. 5 Non-invertibility analysis. **a**, **b** Original eye images; **c**, **d** Transformed IrisCodes; **e**, **f** Inverted IrisCodes images

original eye traits, the transformed IrisCodes and their corresponding inverted images, respectively. Clearly, the inverted images are distinct from their corresponding original eye images.

6.3 Distinctiveness

A set of the cancelable IrisCodes of the same pattern is created with various random projection matrices and submitted to distinctive analysis to guarantee template uniqueness. This is verified by the correlation (C) as follows:

$$C(\boldsymbol{I}_1, \boldsymbol{I}_2) = \frac{\sum\sum(\boldsymbol{I}_1 - \overline{\boldsymbol{I}_1})(\boldsymbol{I}_2 - \overline{\boldsymbol{I}_2})}{\sqrt{(\boldsymbol{I}_1 - \overline{\boldsymbol{I}_1})^2(\boldsymbol{I}_2 - \overline{\boldsymbol{I}_2})^2}} \tag{8}$$

where $\boldsymbol{I}_1$ and $\boldsymbol{I}_2$ are cancelable IrisCodes. The coefficients of correlation for the IrisCodes of the same traits with different random projection matrices have been computed to be close to zero. This ensures the IrisCodes uniqueness.

7 Conclusion

A novel cancelable iris recognition scheme has been proposed in this paper. The proposed scheme preserves the characteristics of cancelable biometric systems. Using the

three-level thresholding as an initial stage enhances the recognition rate. Moreover, Johnson-Lindenstrauss (JL) lemma supplies a theoretical justification for using the random projection method for cancelability. This yields a superior recognition performance with cancelability guarantees and a robustness to rotation and scaling effects compared to other schemes. Moreover, the proposed scheme achieves a high accuracy of 99. 67% and a superior EER of 0.58% on the CASIA-IrisV3 dataset.

References

1. Leonard F, Aran S (1987) Iris recognition system. Patent, US4641349 A
2. Daugman J (1993) High confidence visual recognition of persons by a test of statistical independence. IEEE Trans Pattern Anal Mach Intell 15:1148–1161
3. Rahulkar AD, Holambe RS (2012) Half-iris feature extraction and recognition using a new class of biorthogonal triplet half-band filter bank and flexible k-out-of-n: a postclassifier. IEEE Trans IFS 7:230–240
4. Tsai CC, Lin HY, Taur J, Tao CW (2012) Iris recognition using possibilistic fuzzy matching on local features. IEEE Trans SMC (Part B) 42:150–162
5. Wildes RP (1997) Iris recognition: an emerging biometric technology. In: Proceedings of the IEEE, pp 1348–1363
6. Masek L (2003) Recognition of human iris patterns for biometric identification. M.Sc. thesis, The University of Western Australia
7. Daugman J (2007) New methods in iris recognition. IEEE Trans Syst Man Cybern B 37:1167–1175
8. Shah S, Ross A (2009) Iris segmentation using geodesic active contours. IEEE Trans Inf Forensics Secur 4:824–836
9. Dey S, Samanta D (2007) A novel approach to iris localization for iris biometric processing. Int J Biomed Biol Eng 1(5):293–304
10. An L, Chen X, Yang S, Bhanu B (2016) Sparse representation matching for person re-identification. Inf Sci 355:74–89
11. Soliman NF, Mohamed E, Magdi F, Abd El-Samie FE, AbdElnaby M (2017) Efficient Iris localization and recognition. Opt Int J Light Electron Opt 140:469–475
12. Patel VM, Ratha NK, Chellappa R (2015) Cancelable biometrics: a review. IEEE Signal Process Mag 32(5):54–65
13. Punithavathi P, Subbiah G (2017) Can cancellable biometrics preserve privacy? Biom Technol Today 2017(7):8–11
14. Lai Y, Jin J, Teoh ABJ, Goi B, Yap W, Chai T, Rathgeb C (2017) Cancellable iris template generation based on indexing-first-one hashing. Pattern Recognit 64:105–117
15. Nandakumar K, Jain AK (2015) Biometric template protection: bridging the performance gap between theory and practice. IEEE Signal Process Mag 32(5):88–100
16. Jain AK, Nandakumar K (2008) Nagar A (2008) Biometric template security. EURASIP J Adv Signal Proc 113:1–17 **(Special issue on Biometrics)**
17. Ratha NK, Chikkerur S, Connell JH, Bolle RM (2007) Generating cancelable fingerprint templates. IEEE Trans Pattern Anal Mach 29(4):561–572
18. Harjoko A, Hartati S, Dwiyasa H (2009) A method for iris recognition based on 1d coiflet wavelet. World Acad Sci Eng Technol 56:126–129
19. Chong SC, Jin ATB, Ling DNC (2006) High security iris verification system based on random secret integration. Comput Vis Image Underst 102(2):169–177
20. Pillai JK, Patel VM, Chellappa R, Ratha NK (2010) Sectored random projections for cancelable iris biometrics. In: IEEE international conference on acoustics speech and signal processing, pp 1838–184
21. Rathgeb C, Breitinger F, Baier H, Busch C (2015) Towards bloom filter-based indexing of iris biometric data. In: 15th IEEE international conference on biometrics, pp 422–429
22. Rathgeb C, Breitinger F, Busch C, Baier H (2014) On the application of bloom filters to iris biometrics. IET J Biom 3(4):207–218
23. Zuo J, Ratha NK, Connel JH (2008) Cancelable iris biometric. In: Proceedings of the 19th international. Conference on pattern recognition, pp 1–4

24. Maiorana E, Campisi P, Fierrez J, Ortega-Garcia J, Neri A (2010) Cancelable templates for sequence-based biometrics with application to on line signature recognition. IEEE Trans Syst Man Cybern 40(3):525–538
25. Syarif MA, Ong TS, Teoh ABJ, Tee C (2014) Improved biohashing method based on most intensive histogram block location. In: International conference of neural information processing, pp 644–652
26. Teoh ABJ, Chong LY (2010) Secure speech template protection in speaker verification system. Speech Commun 52(2):150–163
27. Teoh ABJ, Ngo DCL, Goh A (2004) Biohashing: two factor authentication featuring fingerprint data and tokenised random number. Pattern Recognit 37(11):2245–2255
28. Ouda O, Tsumura N, Nakaguchi T (2011) On the security of bioencoding based cancelable biometrics. IEICE Trans Inf Syst 94-D(9):1768–1777
29. Ouda O, Tsumura N, Nakaguchi T (2010) A reliable tokenless cancelable biometrics scheme for protecting iriscodes. IEICE Trans Inf Syst E93-D(7):1878–1888
30. Lacharme P (2012) Analysis of the iriscodes bioencoding scheme. Int J Comput Sci Softw Eng 6(5):315–321
31. Hammerle-Uhl J, Pschernig E, Uhl A (2009) Cancelable iris biometrics using block re-mapping and image warping. In: International conference on information security, pp 135–142
32. Jenisch S, Uhl, A (2011) Security analysis of a cancelable iris recognition system based on block remapping. In: Proceedings of the IEEE international conference on image processing, pp 3274–3277
33. Dwivedi R, Somnath D (2015) Cancelable iris template generation using look-up table mapping. In: 2nd international conference on signal processing and integrated network, pp 785–790
34. Tarek M, Ouda O, Hamza T (2016) Robust cancelable biometrics scheme based on neural networks. IET J Biom 5(3):220–228
35. Tarek M, Ouda O, Hamza T (2017) Pre-image resistant cancelable biometrics scheme using bidirectional memory model. Int J Netw Secur 19(4):498–506
36. Evans N, Marcel S, Ross A, Teoh ABJ (2015) Biometrics security and privacy protection. IEEE Signal Process Mag 32(5):17–18
37. Johnson W, Lindenstrauss J (1984) Extensions of Lipschitz maps into a hilbert space. Contemp Math 26:189–206
38. CASIA-IrisV3 Database. http://www.cbsr.ia.ac.cn/english/IrisDatabase.asp. Accessed June 2017
39. Kumar A, Passi A (2010) Comparison and combination of iris matchers for reliable personal authentication. Pattern Recognit 43:1016–1026