Secure cancelable face recognition system based on inverse filter

Preprint *in* Journal of Optics · February 2024

DOI: 10.1007/s12596-023-01233-7

9 authors, including:

Mohammed Abd-Elnaby
Faculty of Electronic Engineering, Menoufia, University, Egypt
111 PUBLICATIONS **1,017** CITATIONS
SEE PROFILE

Walid El-Shafai
Menoufia University
353 PUBLICATIONS **4,196** CITATIONS
SEE PROFILE

Adel S. El-Fishawy
Menoufia University
166 PUBLICATIONS **682** CITATIONS
SEE PROFILE

M.I Ashiba
Menoufia University
11 PUBLICATIONS **33** CITATIONS
SEE PROFILE

J Opt
https://doi.org/10.1007/s12596-023-01233-7

RESEARCH ARTICLE

Secure cancelable face recognition system based on inverse filter

Abd El-Rahman Farouk[1] · Mohammed Abd-Elnaby[2] · Huda I. Ashiba[3] · Ghada M. El-Banby[4] · Walid El-Shafai[1,5] · Adel S. El-Fishawy[1] · Moawad I. Dessouky[1] · El-Sayed M. El-Rabaie[1] · Fathi E. Abd El-Samie[1,6]

Received: 1 September 2022 / Accepted: 18 November 2022

Abstract Biometric systems have recently become popular for modern security applications. Unfortunately, these systems have been the target of many hacking attempts. Biometrics in biometric databases will be lost forever if they are hacked and stolen. As a result, there is an urgent need to implement modern upgradable biometric systems. Cancelable biometrics is based on the principle of transforming biometric data to alternate templates that cannot be easily exploited by an impostor or attacker and can be discarded if violated. The idea in this paper depends on the inverse filter in a cancelable face recognition system. Masked biometric images are produced in the proposed cancelable face recognition system by blurring, noise addition, and then inverse filtering. In image restoration theory, it is well understood that inverse filtering contributes to noise enhancement, which is an undesirable effect. On the contrary, this result would be desired in cancelable biometric systems. When noise is magnified, it can obscure the original biometrics, resulting in cancelable templates. This is the philosophy that underpins the proposed system. The proposed system was tested on the Olivetti and Oracle (ORL) dataset, the Labeled Faces in the Wild (LFW) database, and the Face Recognition Technology (FERET) database. Simulation results using evaluation metrics such as non-invertibility, unlinkability, visual inspection, false positive rate, false negative rate, Equal Error Rate (EER), decidability, correlation coefficient, and Area under the Receiver Operating Characteristic curve (AROC) show that the proposed cancelable biometric recognition system is quite effective for several security applications.

Keywords Face images · Biometrics · Cancelable biometric recognition · Inverse filtering · Non-invertibility · Unlinlability

✉ Walid El-Shafai
eng.waled.elshafai@gmail.com;
walid.elshafai@el-eng.menofia.edu.eg; welshafai@psu.edu.sa

Abd El-Rahman Farouk
elrahman1086@yahoo.com

Mohammed Abd-Elnaby
maahmed@tu.edu.sa

Huda I. Ashiba
hudaashiba@gmail.com

Ghada M. El-Banby
ghadaelbanby75@gmail.com

Adel S. El-Fishawy
aelfishawy@hotmail.com

Moawad I. Dessouky
dr_moawad@yahoo.com

El-Sayed M. El-Rabaie
srabie1@yahoo.com

Fathi E. Abd El-Samie
feabdelhamid@pnu.edu.sa; fathi_sayed@yahoo.com

[1] Department of Electronics and Electrical Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt

[2] Department of Computer Engineering, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia

[3] Department of Electronics and Electrical Communications, Bilbis Higher Institute of Engineering, Bilbis, Sharqia, Egypt

[4] Department of Automatic Control, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt

[5] Security Engineering Lab, Computer Science Department, Prince Sultan University, Riyadh 11586, Saudi Arabia

[6] Department of Information Technology College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, Riyadh 11671, Saudi Arabia

Published online: 14 February 2024

Introduction

Biometric identification is known as the automatic identification of people based on their physical or behavioral characteristics. Fingerprints, ears, iris images, face images, and voice signals are the most commonly used biometrics. Some biometric properties are inextricably linked to persons; they provide clear proof of their identities. The basic operational principle of biometric systems is to capture biometrics for registered persons, extract discriminating features from the biometrics as a method for data reduction, and keep these features in a database. This is called the enrollment phase. In another biometric system phase, the verification can be executed with/without classifiers [1].

The external human body is essential in our social interactions, as it conveys titles and people's identities. Using the face as a key to protection, biometric face recognition innovation has received much attention in recent years due to its potential for a wide range of uses in both social regulation compliance and law enforcement. Face recognition has distinct advantages over other predictive methods that use palm prints/fingerprints and iris images, because of its non-contact form. Face images can be taken digitally without touching the person being identified; therefore, the identification does not require interaction with the person. Furthermore, face recognition serves as a crime deterrence tool, because face images that are captured and archived can later be used to identify persons [2].

Most biometric technology systems use equivalent fundamental standards of operation [2]. Therefore, the operation of biometric systems can be summarized as follows:

1. **Enrollment:** The procedure by which a client's biometric information is at first obtained, prepared, and put away as a layout for use in a biometric system is called enrollment. Consequent confirmation and ID verification are led against the template(s) created amid enrollment.
2. **Presentation:** Presentation is a procedure by which a client gives biometric information to a security gadget, the equipment used to gather biometric information. Contingent upon the biometric framework, presentation may require looking toward a camera, putting the finger on a platen, or presenting a pass phrase.
3. **Biometric data:** Biometric information are those that belong to human organs and are quantifiable, for instance, diagram or state of the hand, of fingers, their temperature, facial shape, veins, heartbeat, and iris images.
4. **Feature extraction:** Feature extraction is the process, which represents the encoding and localization of the biometric data features to produce the templates. Feature extraction can be provided during the enrollment/verification process. The process of feature extraction comprises filtration and optimization steps. For instance, the scan of voice technologies usually filter specific frequencies and templates. The higher the goodness of features, the greater the performance of the biometric system is.

All technical systems have drawbacks, and biometric systems are not exception. Biometric authentication has many benefits; however, the drawbacks of biometric authentication must be considered. Biometric features are irreversible, which is one of the biometric authentication cornerstones. Unfortunately, biometric identifiers like heat, gait, face, map, and others are critical, and can be taken without the owner's awareness. Biometric device technology advancements may be able to mitigate these drawbacks.

Cancelable biometric systems are introduced to solve these issues by generating distorted, meaningless templates to be stored in the database to avoid the impairments of biometric systems. However, the main advantage of these systems is that a person can generate another new cancelable template in case of attack or theft without updating the whole system.

This paper provides a new approach for cancelable face recognition. The proposed cancelable face recognition system is based on the generation of masked images using blurring, additive noise, and inverse filter technique. The verification is based on estimating the correlation coefficient between the masked feature matrix of the new subject face template and the masked feature matrices stored in the database. Finally, based on a threshold value, the matcher can decide and classify the new subject as being accepted or rejected. The quantitative evaluations of the proposed cancelable face recognition system have been performed using EER based on False Acceptance Rate (FAR), False Rejection Rate (FRR), AROC, correlation coefficient, non-invertibility, unlinability, and decidability.

The remainder of this paper is arranged as follows. Related work is presented in Sect. "Related work", In Sect. "Inverse filter", the inverse filter is presented. Sect. "The proposed cancelable biometric system" gives an explanation of the proposed cancelable face recognition system based on the inverse filter technique. Sect. "Evaluation metrics definitions" presents the evaluation metrics. The simulation results of the proposed system are investigated in Sect. "Simulations results". Finally, Sect. "Conclusion" gives the conclusion of this paper.

Related work

Many solutions are presented in the literature for cancelable biometric systems. In [3], Algarni et al. presented two methods for Cancelable Face Recognition (CFR) to ensure personal identification security. Both methods depend on the utilization of Random Projection (RP) for the biometric trait encryption. The first method depends on combining Intuitionistic Fuzzy Logic (IFL) with RP to generate encrypted biometric templates, while the second method depends on the homomorphic transform with RP to generate the encrypted template. Soliman et al. [4] used Double Random Phase Encoding (DRPE) to ensure the ability to generate cancelable biometric templates for both face and iris recognition.

Ratha et al. [5] used new transformation keys to give the user several biometric identifiers. When the identifiers are hacked, they can be deleted and replaced. Savvides et al. [6] generated encrypted biometric templates depending on the convolution of the training images with random kernels. BioHashing of Jin et al. [7] depends on the combination of two authentication tools, which can be implemented by an iterative mixture between the fingerprint biometrics and pseudo-random numbers. The Hadamard transform was used with Fourier transform for representing a series of binary biometric data to obtain complex vectors, while maintaining the distance between the vectors that was estimated before the transformation. For this approach, EER ranges from 1% up to 5% in various standard scenarios. Some attempts have been presented on multi-biometric systems with the possibility to use fingerprints and veins [8]. Wang and Hu offered a blind cancelable biometric recognition system based on generating secure pair-minutiae vectors and using these vector samples for identification [9]. This approach is valid for certain applications like mobile phones, smartcards, and drivers' licenses. Satisfactory results have been obtained on FVC2002 DB1, DB2, and DB3.

Abou Elazm et al. [10] presented a cancelable biometric system for fingerprint and face recognition based on optical encryption and 3D jigsaw transform. This system gives good results in terms of the ability to cancel and change templates if necessary and the good encryption characteristics. Abdellatef et al. [11] presented a new approach that depends on many Convolutional Neural Networks (CNNs) to generate deep features from various facial regions. This approach has been tested on the FERET, LFW, and PaSC datasets, and it gives excellent results. Soliman et al. [12] provided a biometric recognition system based on removing the effects of eyelids and eyelashes from the iris. Gabor filter is used for feature extraction, and finally, RP is used to increase security. CASIA-IrisV3-Interval database [13] has been used to test this system. Tarif et al. [14] offered

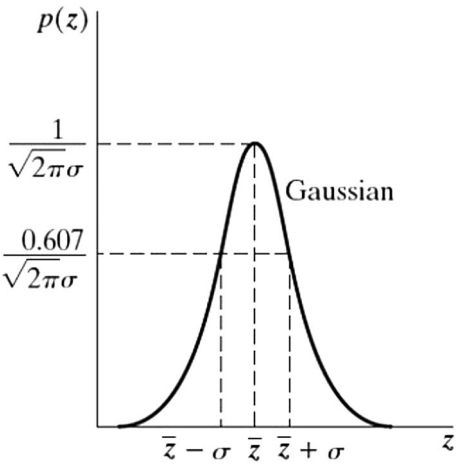

Fig. 1 PDF of Gaussian noise

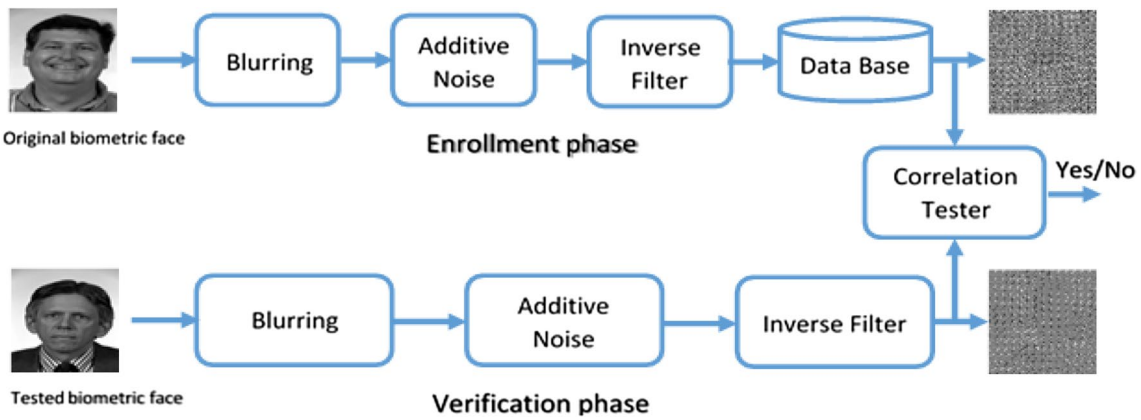

Fig. 2 Block diagram of the proposed cancelable face recognition system

an accelerated iterative approach for generating fingerprint and iris templates, and then implemented it in the Stanlet-SVD domain for face images. This approach is used within a multimodal biometric system. Georgia Tech face database [15] has been used to test this approach. Dang et al. [16] implemented a fuzzy vault with repeated sine transformation to generate cancelable templates. Principal Component Analysis (PCA) [17] and face features have been used for executing this algorithm.

Inverse filter

Generally, the inverse filter is one of the simplest restoration techniques used to reconstruct the original image from a degraded image, especially in the absence of noise. However, the restored image will become distorted if noise is present, especially at a low Signal-to-Noise Ratios (SNRs).

Gaussian noise

The Gaussian noise has a normal distribution. It results from natural sources like warm objects, radiation, and thermal vibration [18]. Generally, the Gaussian noise disturbs the gray values in digital images. The Probability Density Function (PDF) of Gaussian noise can be represented as [19]:

$$p(z) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(z-\bar{z})^2}{2\sigma^2}} \tag{1}$$

where z is the intensity, $\bar{z}$ represents the mean of z, and σ is the standard deviation. The square of the standard deviation is the variance σ^2.

The PDF of Gaussian noise is shown in Fig. 1, where this noise model for images has a zero mean, 0.1 variance, and 256 gray levels in its PDF.

Inverse filtering algorithm

The mathematical expression of the image degradation model is described using the following equation [20]:

$$\mathbf{g} = \mathbf{Hf} + \mathbf{n} \tag{2}$$

where $\mathbf{f}$ is an original image, $\mathbf{g}$ is the degraded image, $\mathbf{H}$ represents the blurring operator, and $\mathbf{n}$ represents the additive Gaussian noise. Lexicographic ordering is adopted in this equation.

Inverse filtering restoration model is established by assuming a known and invertible blurring operator. A direct solution to obtain a good restored image is by seeking $\widehat{\mathbf{f}}$ that minimizes the norm of the difference between the blurred

Fig. 3 Original face images

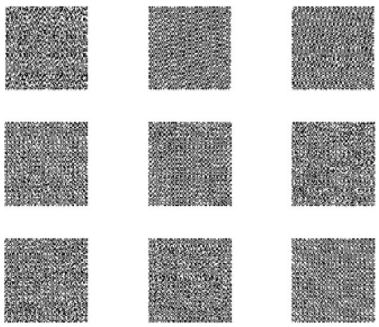

Fig. 4 Masked face images with 9×9 blurring operator, at − 10 dB

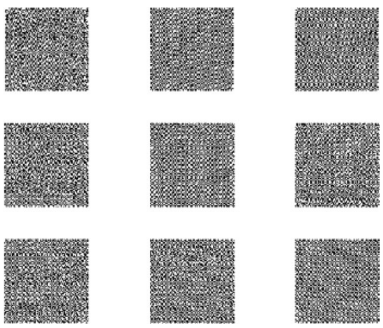

Fig. 5 Masked face images with 9×9 blurring operator, at 5 dB

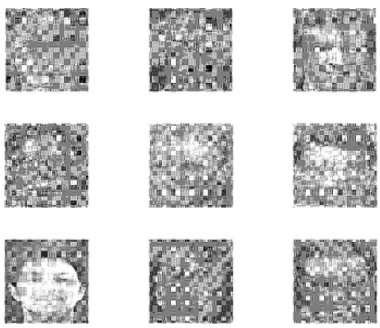

Fig. 6 Masked face images with 3×3 blurring operator, at 50 dB

Table 1 Correlation coefficient for different blurring operators and SNRs

SNR (dB)	Blurring operator	Correlation coefficient
50	3×3	0.1457
50	9×9	0.0895
5	3×3	–0.0069
5	9×9	–0.0086
− 10	3×3	–0.0090
− 10	9×9	–0.0045

estimated image $\mathbf{H}\hat{\mathbf{f}}$ and the degraded image $\mathbf{g}$. Mathematically, restoration is performed by seeking $\hat{\mathbf{f}}$ that minimizes the cost function [20]:

$$\Psi(\hat{\mathbf{f}}) = \|\mathbf{g} - \mathbf{H}\hat{\mathbf{f}}\|^2 \tag{3}$$

Taking the partial derivative of both sides of Eq. (3) with respect to $\hat{\mathbf{f}}$ and equating the result to zero yields [20]:

$$\frac{\partial \Psi\left(\hat{\mathbf{f}}\right)}{\partial \hat{\mathbf{f}}} = 0 = -2\mathbf{H}^t\left[\mathbf{g} - \mathbf{H}\hat{\mathbf{f}}\right] \tag{4}$$

Therefore,

$$\hat{\mathbf{f}} = \left[\mathbf{H}^t\mathbf{H}\right]^{-1}\mathbf{H}^t\mathbf{g} \tag{5}$$

Substituting from Eq. (2) into Eq. (5) and simplifying, we obtain the well-known solution for inverse filtering, which is defined as [20]:

$$\hat{\mathbf{f}} = \mathbf{H}^{-1}\mathbf{g} = \mathbf{f} + \mathbf{H}^{-1}\mathbf{n} \tag{6}$$

where $\mathbf{H}^t$ is the transpose of $\mathbf{H}$. By applying the frequency domain transformation, the formula will be:

$$\hat{F}(u,v) = \frac{G(u,v)}{H(u,v)} = F(u,v) + \frac{N(u,v)}{H(u,v)} \tag{7}$$

The proposed cancelable biometric system

In this system, the cancelable template is produced based on the low-pass nature of the blurring operator $\mathbf{H}$ according to Eq. (6). The inversion of the blurring operator leads to noise magnification in the cancelable biometric template. This becomes obvious when $\mathbf{H}$ is close to be singular, which is the inverse filter main concept. The proposed cancelable face recognition system illustrated in Fig. 2 can be implemented using the following steps:

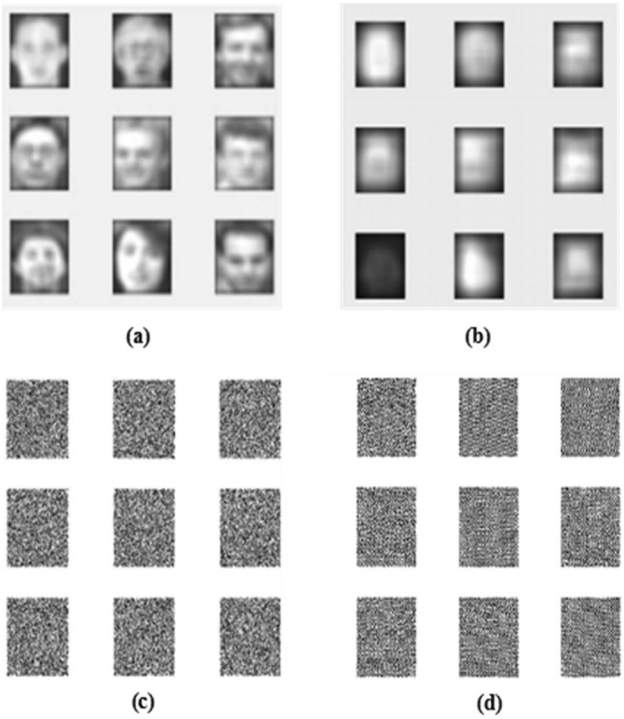

Fig. 7 Masked samples of biometric faces in Fig. 3 from the ORL dataset for **a** bio-convolving encryption, **b** DRPE, **c** CFR based on RP, **d** the proposed system

1) Blurring operation performed on the original biometric face image.
2) Adding Gaussian noise to the blurred biometric face image.
3) Applying an inverse filter to generate the cancelable template.

The obtained cancelable template is stored in the database during the enrollment phase to be compared with the new subject template in the verification phase using the correlation test.

Evaluation metrics definitions

- **False Positive Rate (FPR)**

The FPR gives the probability that the system blocks genuine subscribers.

$$FPR = \frac{FP}{FP + TN} \tag{8}$$

where FP is the number of false positives and TN is the number of true negatives.

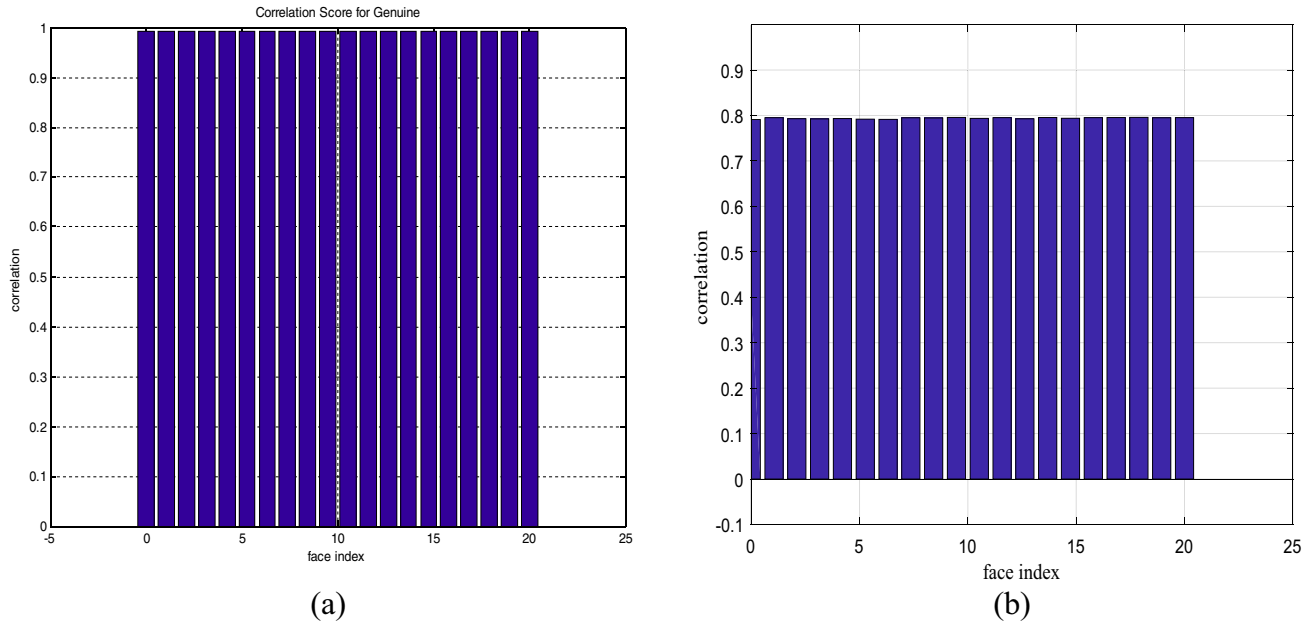

Fig. 8 Correlation scores of authorized face images (ORL dataset) for **a** the proposed system, **b** CFR based on RP

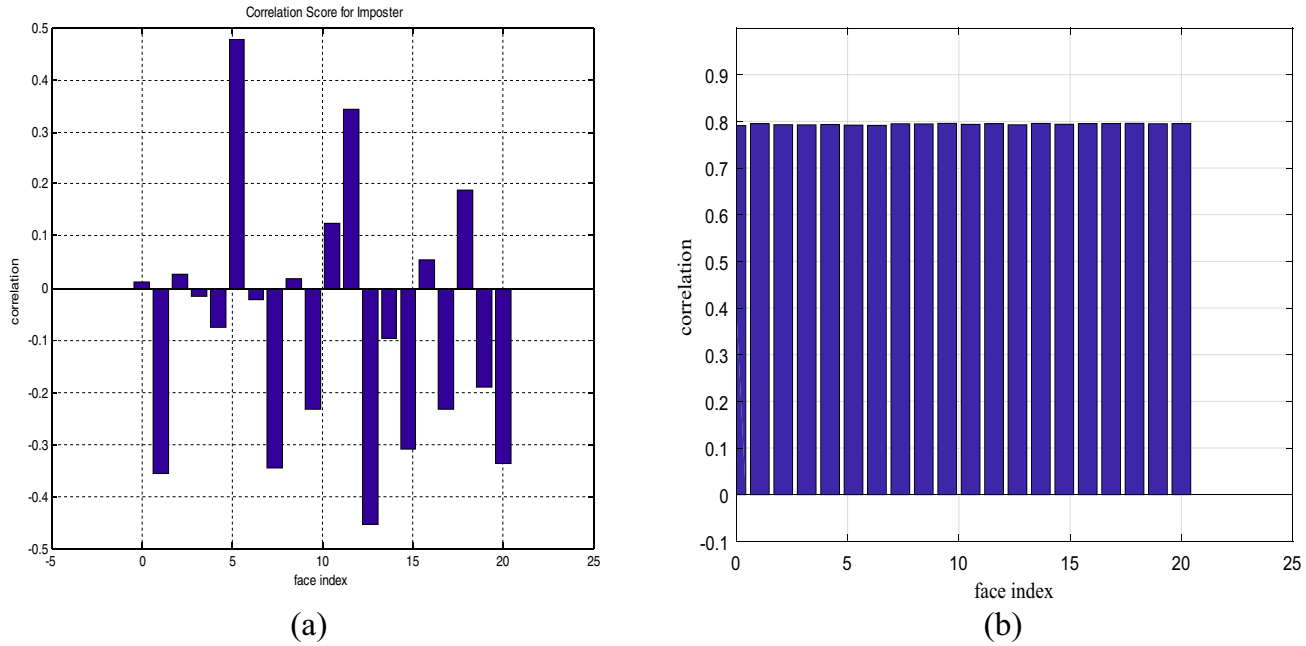

Fig. 9 Correlation scores of unauthorized face images (ORL dataset) for **a** the proposed system, **b** CFR based on RP

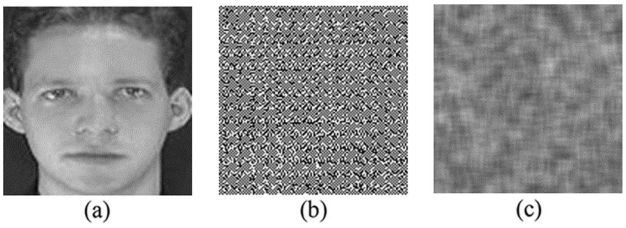

Fig. 10 Non-invertibility effect. **a** original face image, **b** masked face image, **c** inverted face image

- **False Negative Rate (FNR)**

The FNR is the probability that the system approves an impostor.

$$FNR = \frac{FN}{FN + TP} \tag{9}$$

where FN is the number of false negatives and TP is the number of true positives.

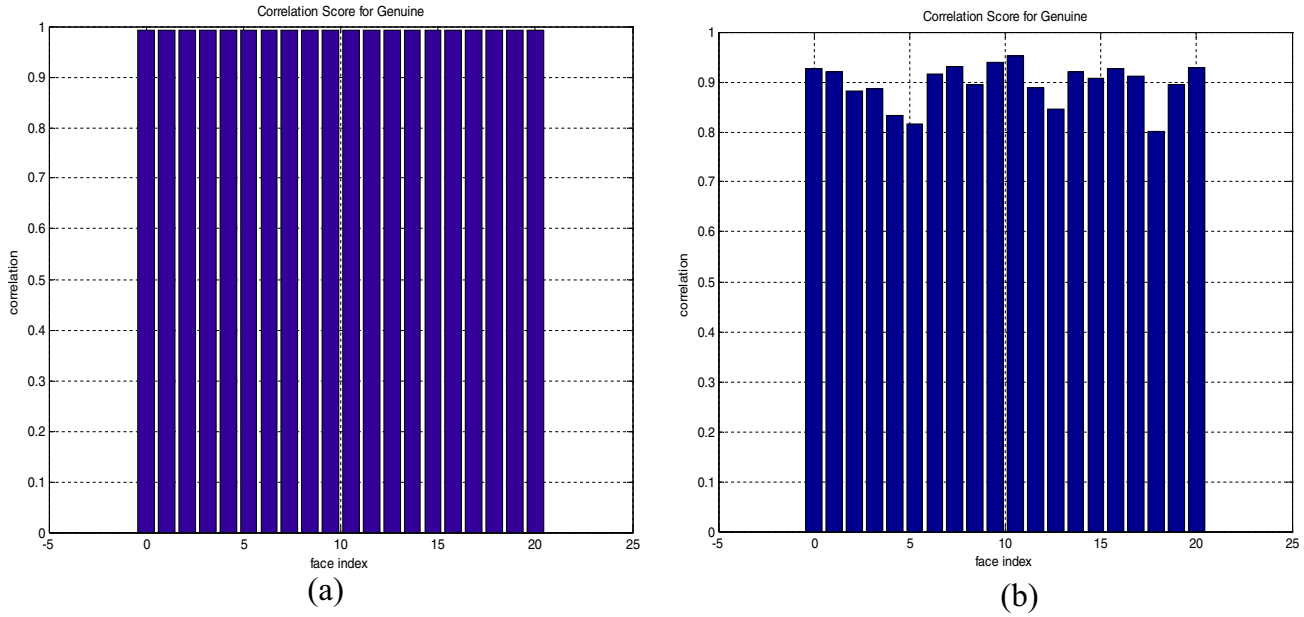

Fig. 11 Unlinkability results for **a** authorized biometric face images, **b** regenerated authorized biometric face images

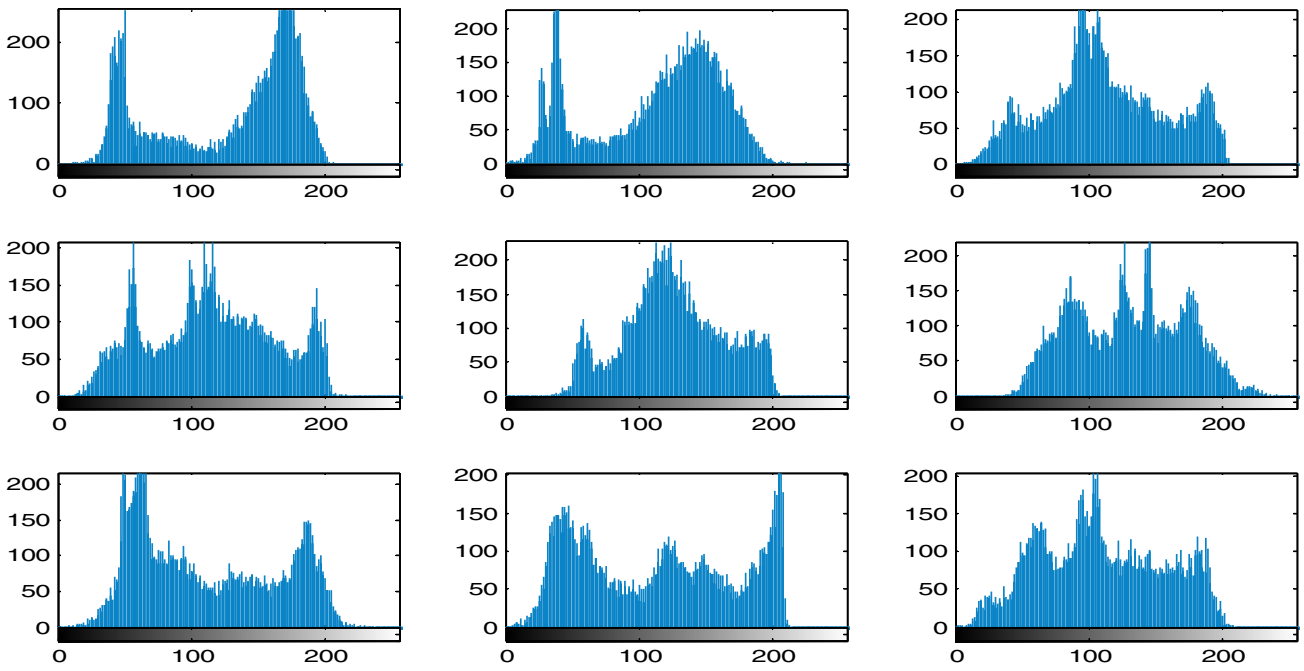

Fig. 12 Histogram distributions of the original biometric face images presented in Fig. 3

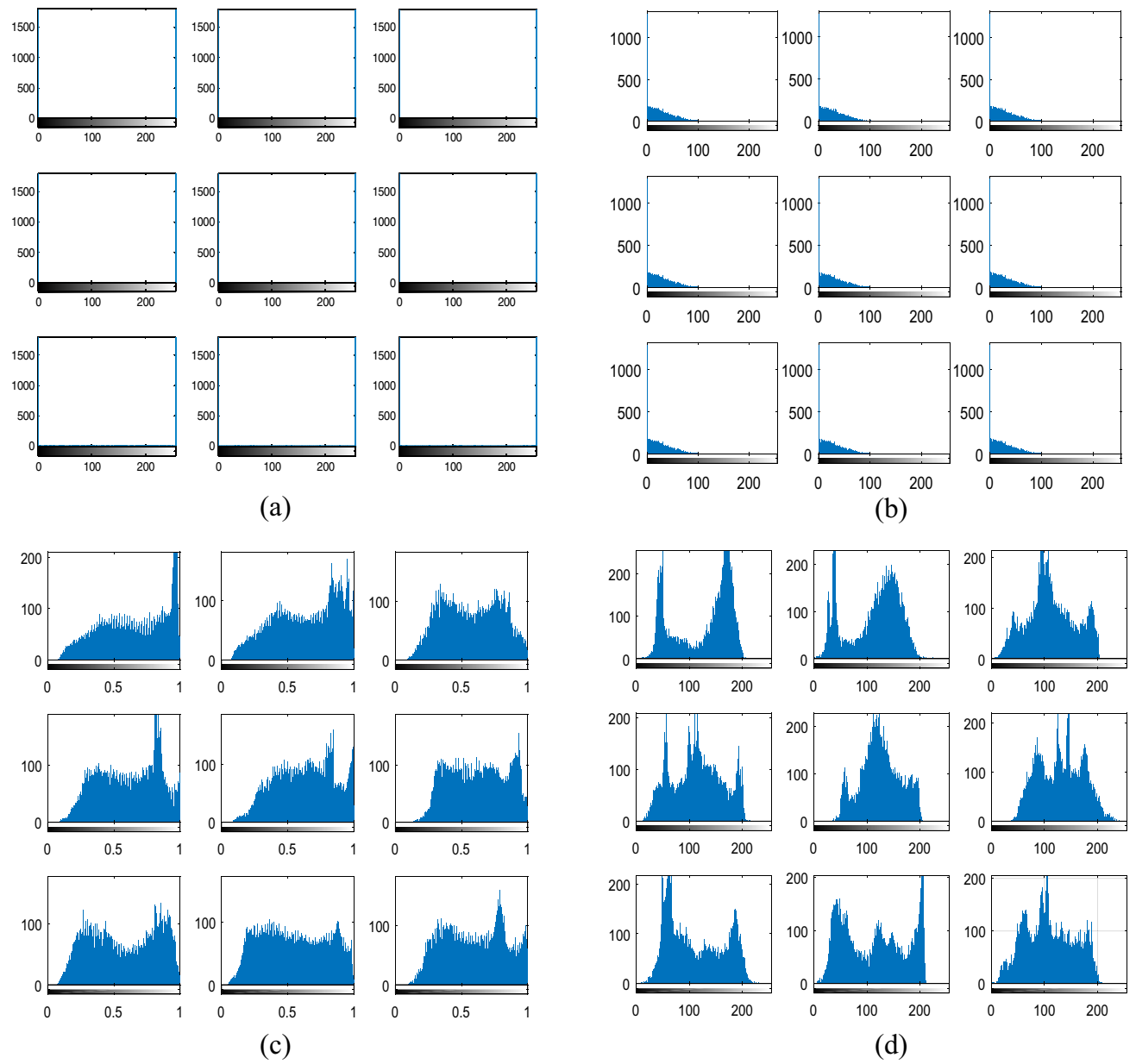

Fig. 13 Histograms of masked samples of biometric faces for **a** the proposed system, **b** CFR based on RP, **c** DRPE, **d** bio-convolving encryption

- **Equal Error Rate (EER)**

The EER is estimated at the point at which the FPR and the FNR are equal at the intersection between the distributions of genuine and impostor correlation values. Therefore, the lower the value of EER, the greater the security level of the system is.

- **Receiver Operating Characteristic (ROC) curve**

The ROC curve is acquired by calculating the relationship between the $FPR\ (T)$ and the $TPR\ (T)$ for every threshold value T.

- **Area under ROC curve (AROC)**

Area under ROC curve is a discrimination parameter that demonstrates the system capability to distinguish the genuine users and impostors. If the AROC value is close to one, the system is more secure.

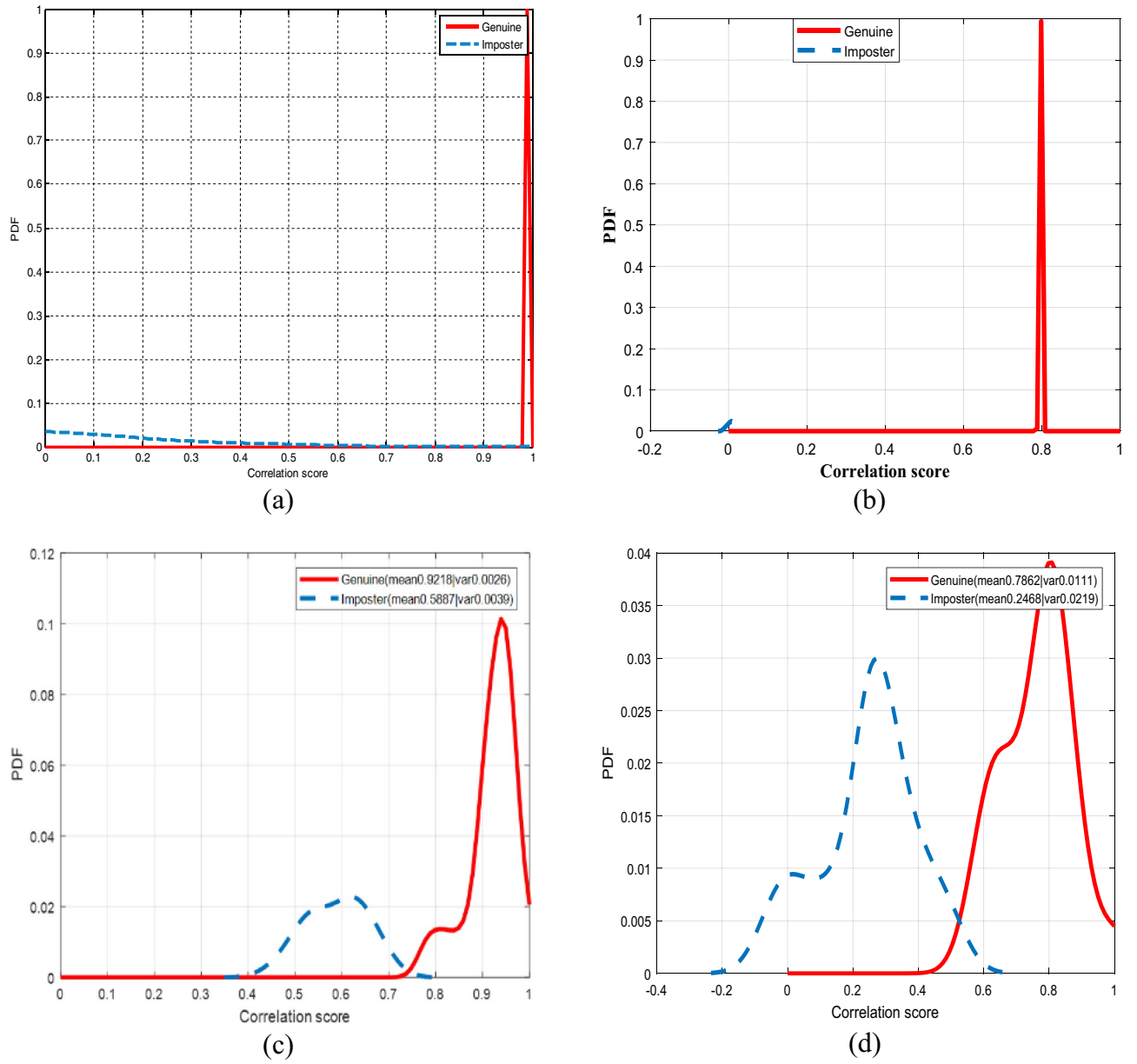

Fig. 14 Distributions of genuine and impostor scores for **a** the proposed system, **b** CFR based on RP, **c** DRPE, **d** bio-convolving

Simulation results

Firstly, we will study the effect of the blurring operator and the additive noise on the face image masking for different blurring operators and SNRs. Figure 3 shows the original face images. Figures 4, 5 and 6 show the masked face images for different blurring operators and SNRs. From these figures, it is obvious that the masking of face images increases at high levels of blurring and low SNRs.

Table 1 presents the correlation coefficient values between the original face image and the masked face image for different blurring operators and SNRs. The table shows that the correlation coefficient decreases with the increase of blurring degree and the reduction of SNR. In our study, the human face images are distorted with a 9×9 blurring operator and additive noise with SNR = 5 dB to generate degraded face images. Then, inverse filtering is applied o generate the cancelable templates.

Performance evaluation of the cancelable face recognition system relies on the evaluation metrics that measure the relation between the template of the user who wants to access the system and the templates kept in the database. To ensure that the proposed system is working properly, we test it and

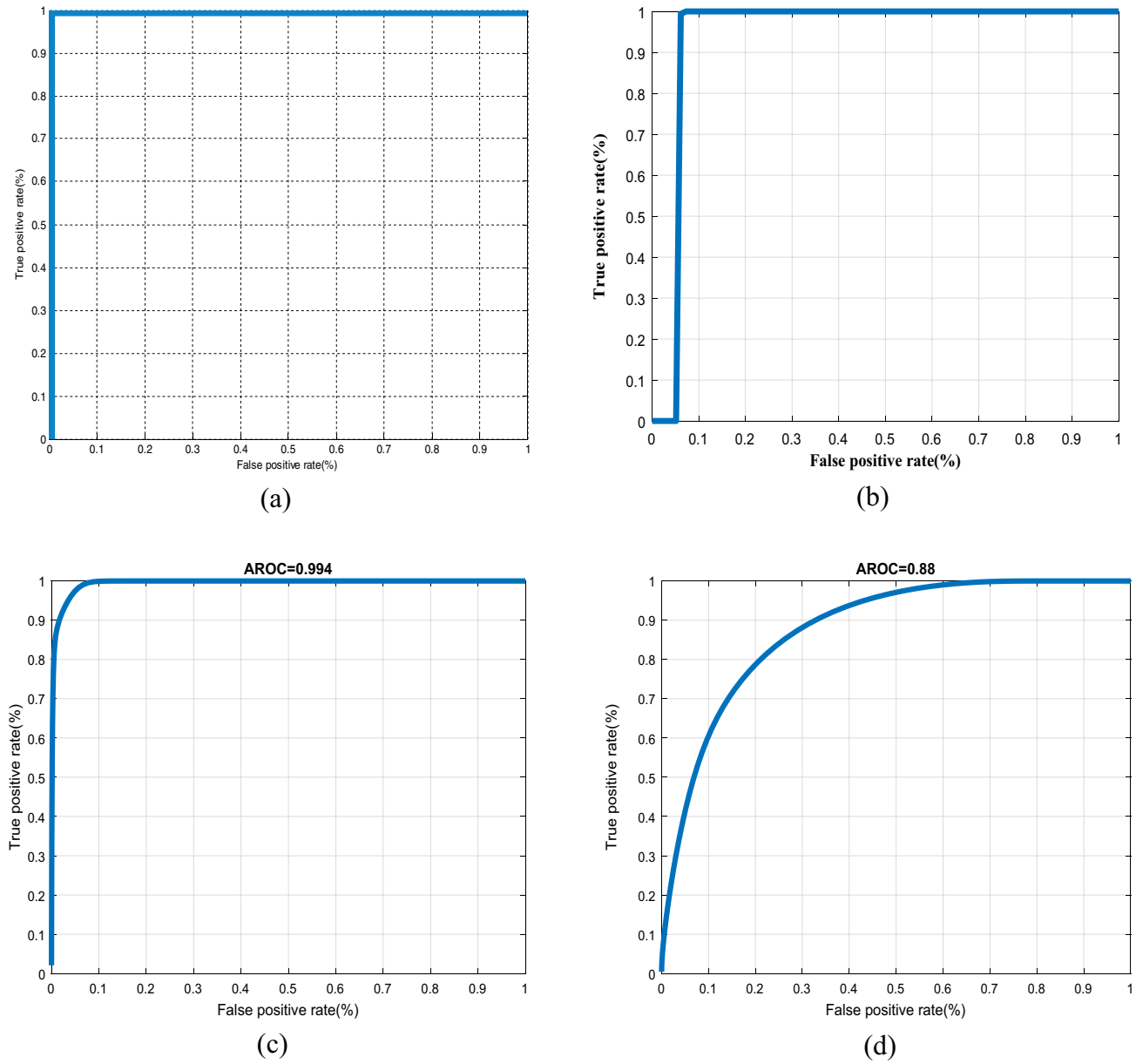

Fig. 15 Receiver Operating Characteristics (ROC) curves for **a** the proposed system, **b** CFR based on RP, **c** CFR based on DRPE, **d** CFR based on bio-convolving

Table 2 Evaluation metrics of the proposed and other biometric systems on ORL database

Evaluation metric	CFR based on bio-convolving	CFR based on DRPE	CFR based on RP scheme	Proposed system
AROC	0.88	0.993	0.9720	1
EER	0.005	0.0017	–	0.0011
Decidability	4.2	26.5	–	5.79
Mean of genuine distribution	–	–	0.7935	0.9921

Fig. 16 Samples of face biometric images from the LFW dataset

Fig. 17 Samples of face biometric images from the FERET dataset

compare it with other existing systems (optical encryption system, bio-convolving, CFR based on RP) using twenty face images of the ORL dataset. The ORL dataset includes 40 subjects, and each subject has 10 images taken at different conditions, times, facial features, and lighting conditions.

Visual inspection

One of the essential image quality assessment tools is the visual inspection. The more the hidden details of images, the better the masking scheme is. The masked face images using bio-convolving, DRPE, CFR based on RP, and the proposed cancelable face recognition system are shown in Fig. 7a–d. It is clear that the proposed system has masked the image features.

Correlation coefficient

The correlation coefficient is one of the evaluation metrics used to estimate the efficiency of biometric encryption or masking systems. It measures the relationship between the masked biometric images kept in the device database and the new masked images. The formula of the correlation coefficient is written as:

$$C_r = \frac{\mathrm{cov}(x, y)}{\sigma_x \sigma_y} \tag{10}$$

where x is a cancelable biometric template kept in the device database and y is a new cancelable biometric template.

The correlation scores of authorized biometric templates in the presence of noise are shown in Fig. 8(a and b). Likewise, the correlation scores of the unauthorized biometric templates are shown in Fig. 9(a and b). It is clear from the figures that the correlation coefficient values for all authorized biometric templates are greater than 0.9 and the correlation coefficient values for all unauthorized biometric templates are less than 0.5. Therefore, a threshold value can be set between 0.5 and 0.9 to distinguish the authorized biometric templates from the unauthorized ones. This is an indicator of the security of the proposed system.

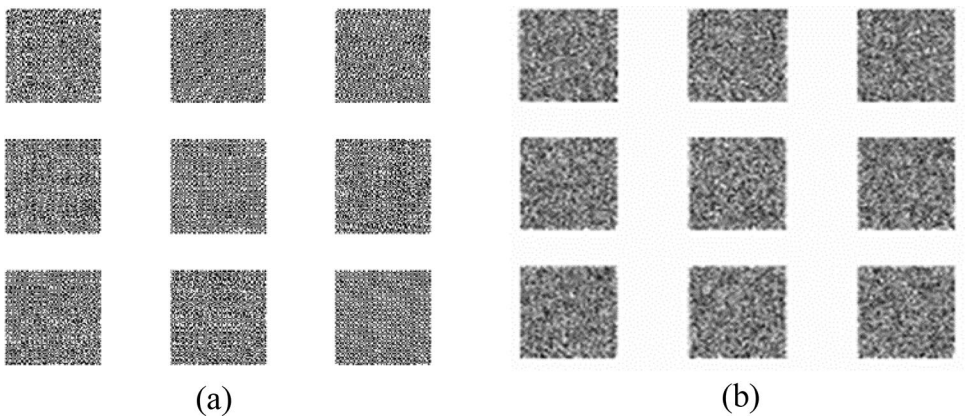

Fig. 18 Masked patterns of biometric faces in Fig. 17 from the FERET dataset for **a** the proposed system, **b** CFR based on RP

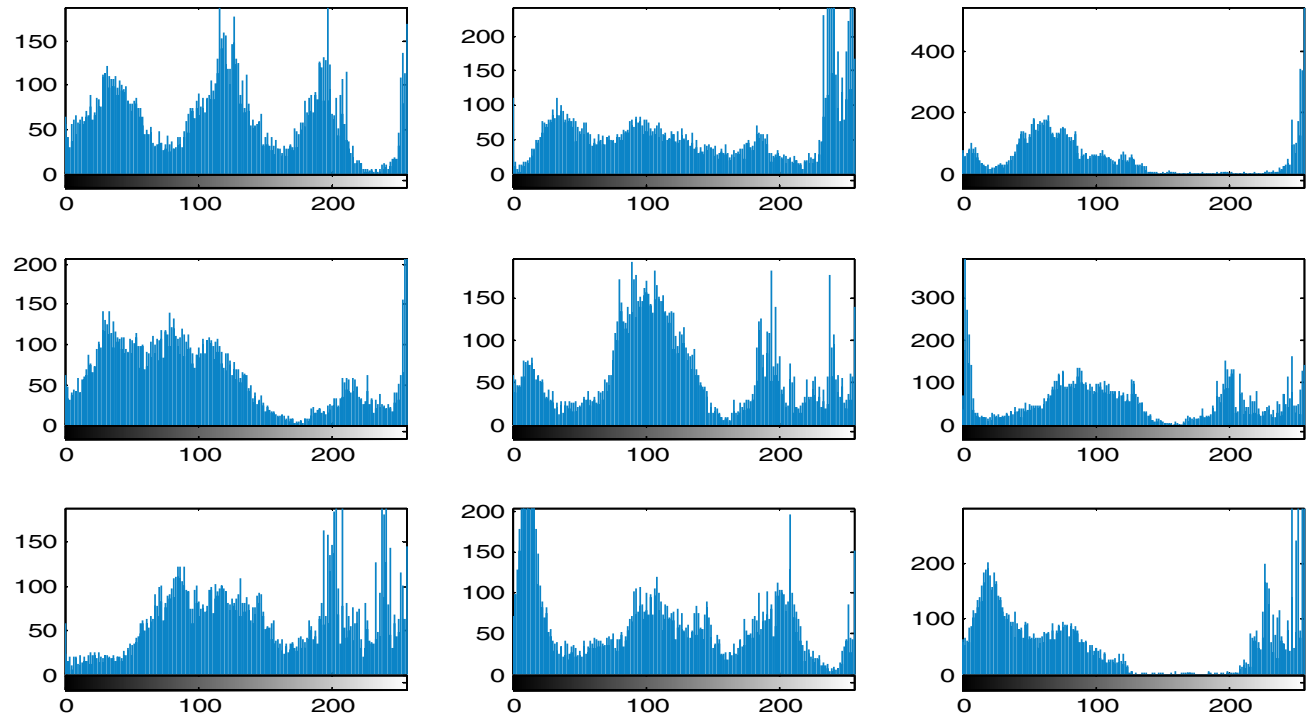

Fig. 19 Histograms of original biometric faces in Fig. 17

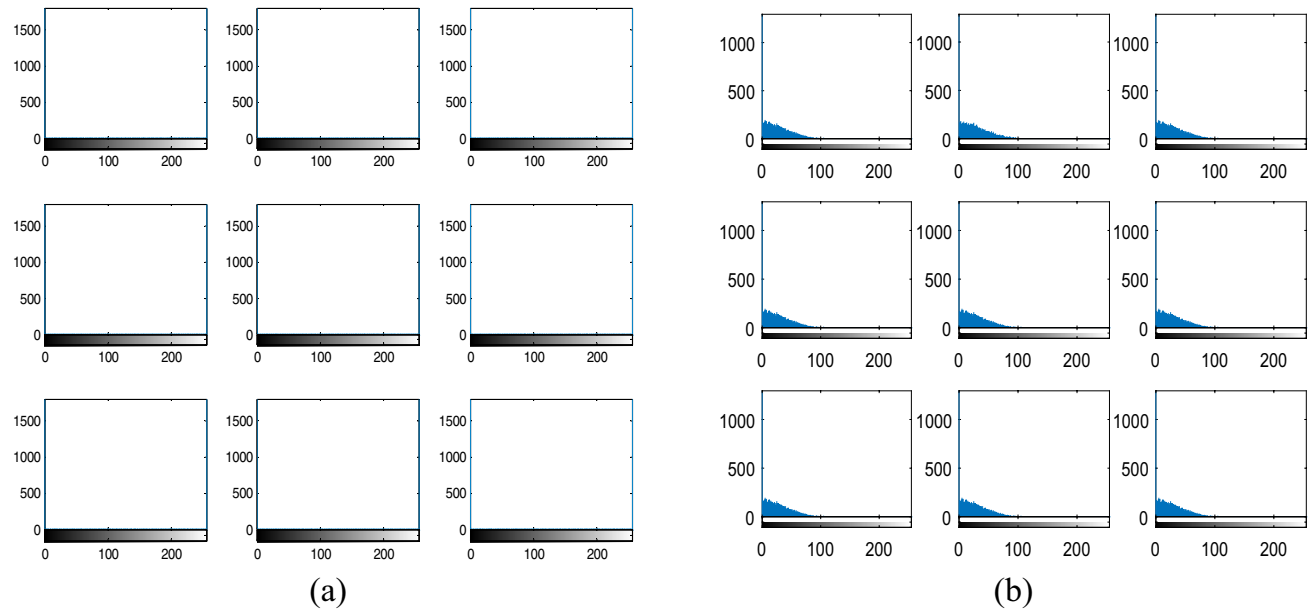

Fig. 20 Histograms of masked face images (FERET dataset) in Fig. 17 for **a** the proposed system, **b** the CFR scheme

Non-invertibility analysis

One of the foremost important security characteristics in cancelable biometric systems is the non-invertibility of templates. If an intruder compromises the key management operation of the biometric template encryption, he can invert the encrypted template of the biometric face, which is stored in the database. Therefore, he can get the original biometric face image. In our proposed system, we have

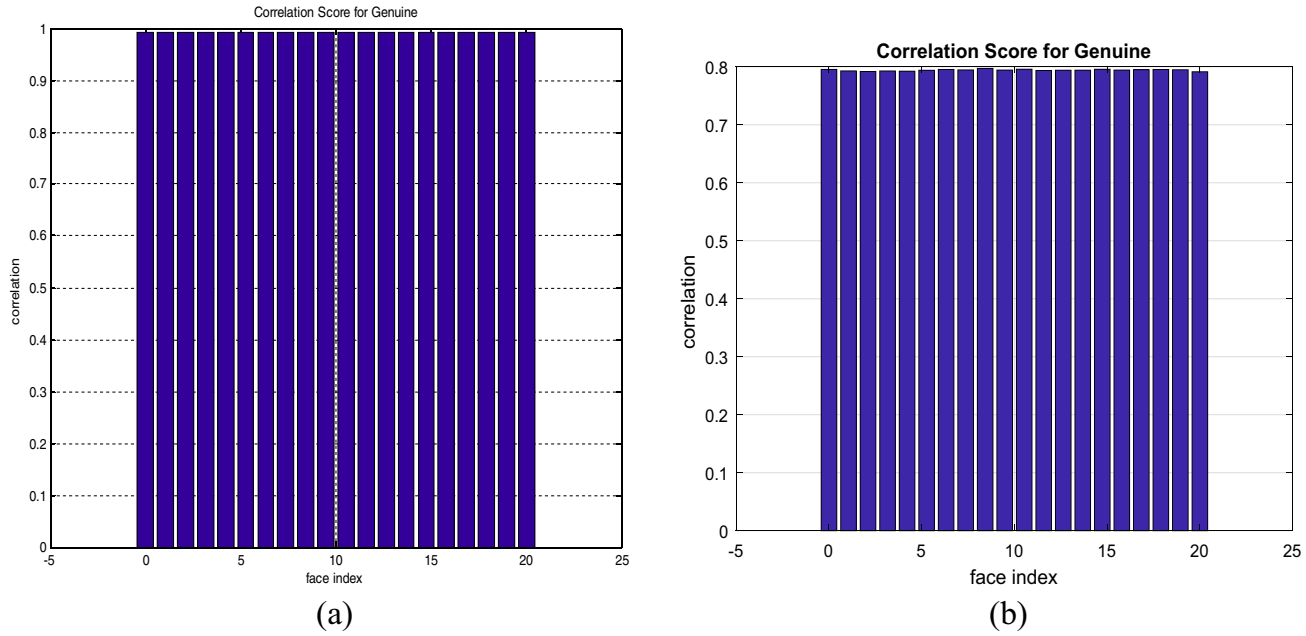

Fig. 21 Correlation scores of authorized face images (FERET dataset) for **a** the proposed system, **b** the CFR based on RP

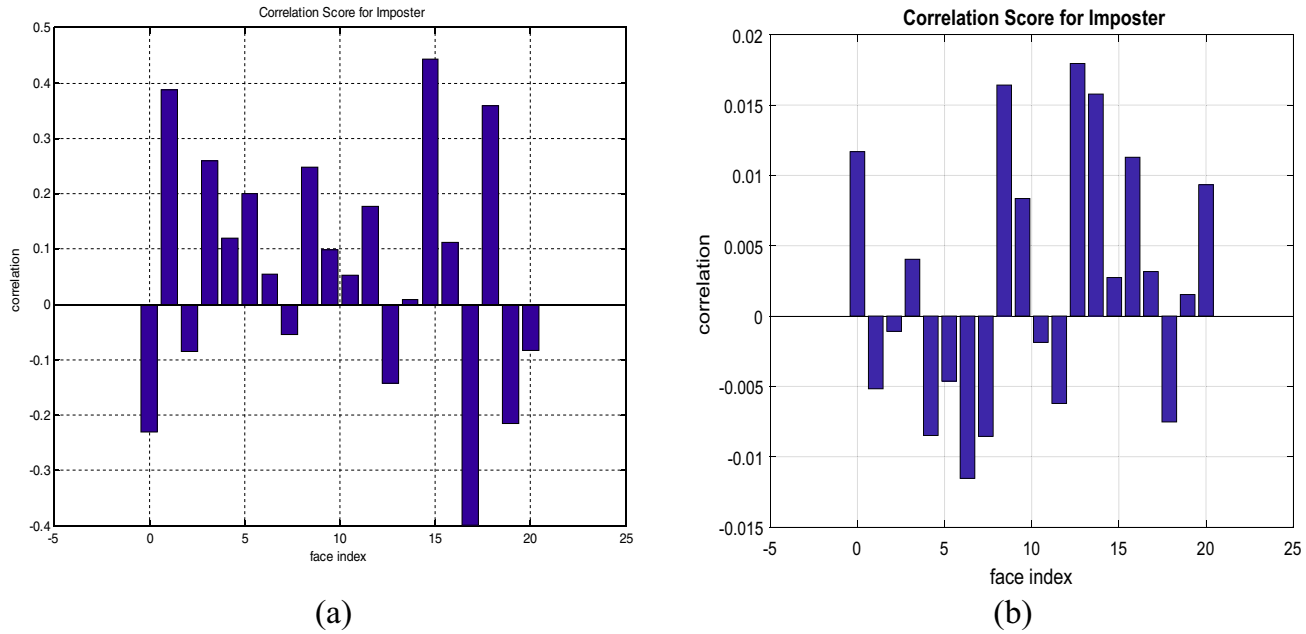

Fig. 22 Correlation scores of unauthorized face images (FERET dataset) for **a** the proposed system, **b** the CFR based on RP

to prevent the intruders from obtaining the original biometric face images. Figure 10a–c illustrates the original face image, the masked template, and the inverted image. From the figures, there is obviously no relation between the inverted face image and the original face image.

Changeability/Unlinkability analysis

The templates of the cancelable biometric system are changeable/unlinkable if the system is capable of generating a new random template for the same user in case of

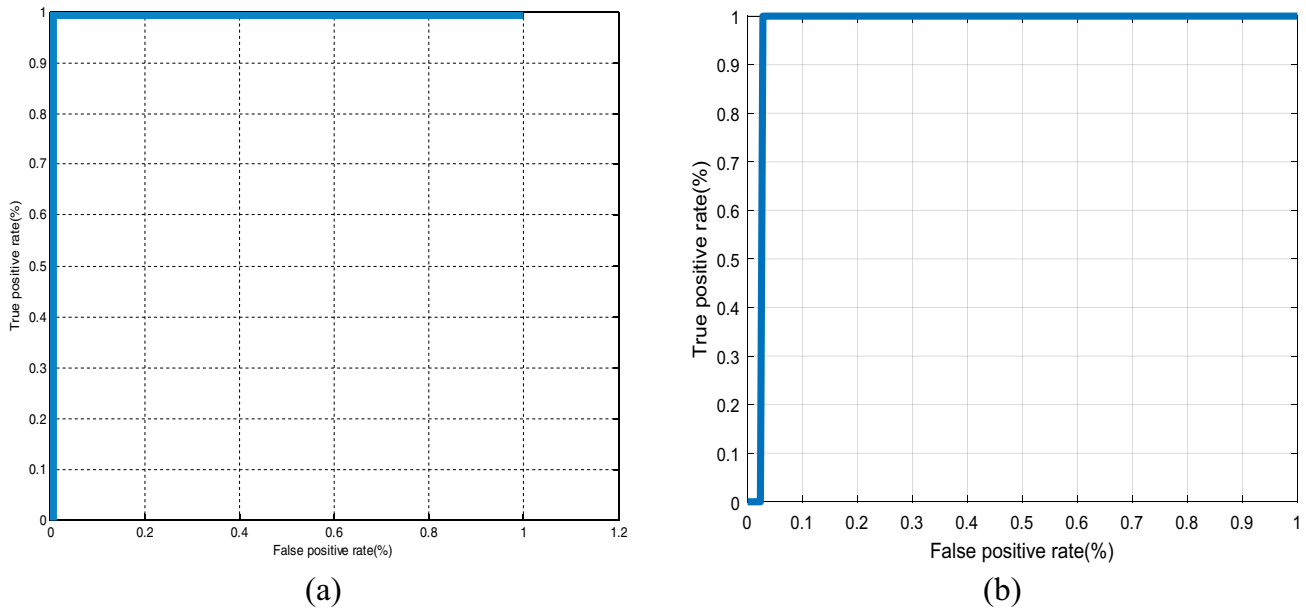

Fig. 23 Receiver Operating Characteristic (ROC) curves (FERET dataset) for **a** the proposed system, **b** the CFR based on RP

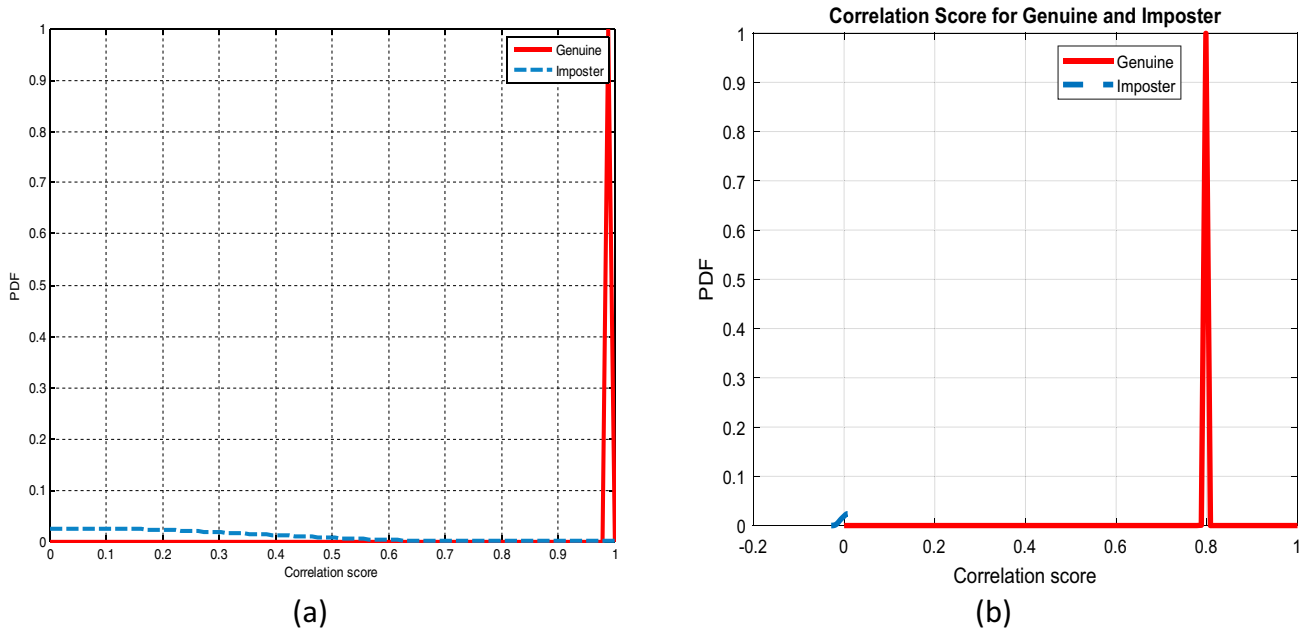

Fig. 24 Distributions of genuine and impostor scores (FERET dataset) for **a** the proposed system, **b** the CFR based on RP

compromising the system storage database. Mean Square Error (MSE) is an evaluation metric that can illustrate the changeability/unlinkability of templates. The MSE equation can be expressed as:

$$MSE = \frac{1}{n}\sum_{i=1}^{n}\left(X_i - \hat{X}_i\right)^2 \tag{11}$$

where X_i is the masked biometric image which have been compromised, and $\widehat{X}_i$ is the regenerated masked biometric image. In the proposed system, the average MSE values between the masked templates and the regenerated masked templates are around 63.2. This means that the proposed system allows unlikability of templates.

Also, the correlation score is another metric that can be used to investigate unlinkability of the biometric templates.

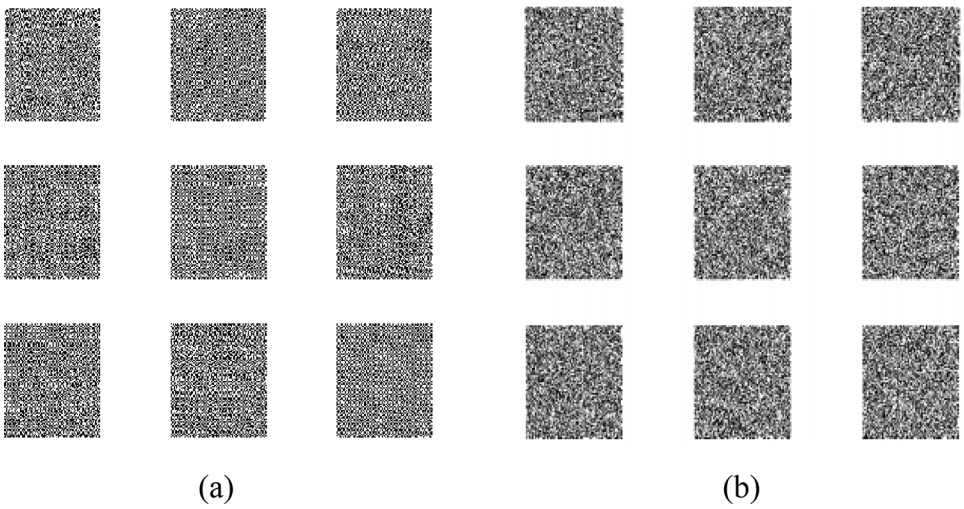

Fig. 25 Masked patterns of biometric face images in Fig. 16 from the LFW dataset for **a** the proposed system, **b** the CFR based on RP

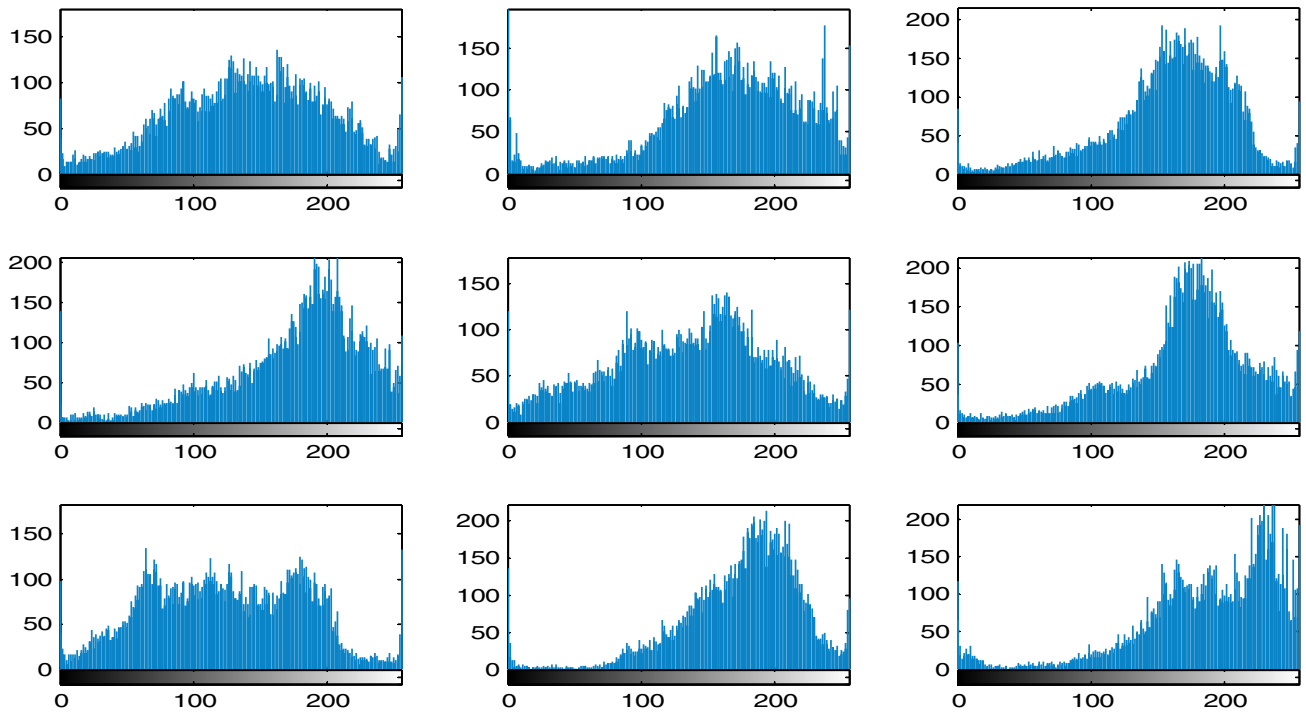

Fig. 26 Histograms of original biometric faces in Fig. 16

Figure 11 illustrates the correlation score distribution for the authorized biometric face images and the regenerated biometric face images. It is clear from the figure that the proposed system achieves the unlinkability criterion.

Histogram distribution analysis

Histogram distributions are commonly used to estimate the masking system robustness against intrusions and attacks. Figure 12 shows the histogram distributions of the original biometric face images. The histogram distributions of masked biometric images using bio-convolving, DRPE, CFR

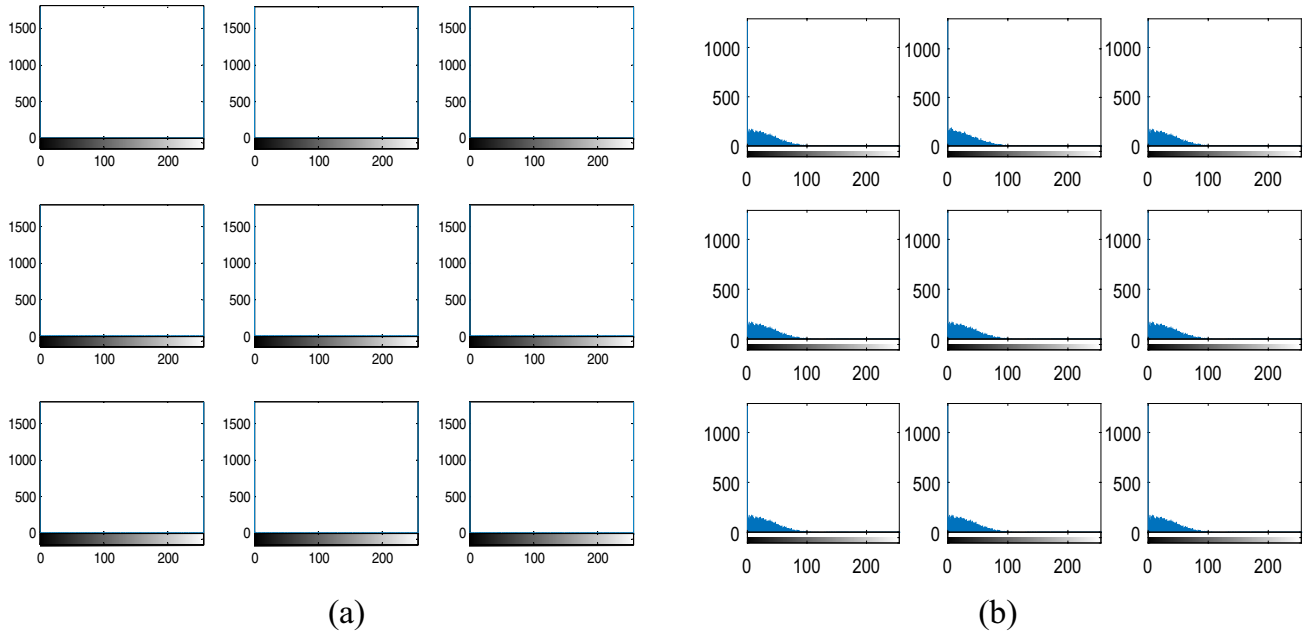

Fig. 27 Histograms of encrypted face images (LFW dataset) in Fig. 24 for **a** the proposed system, **b** the CFR based on RP

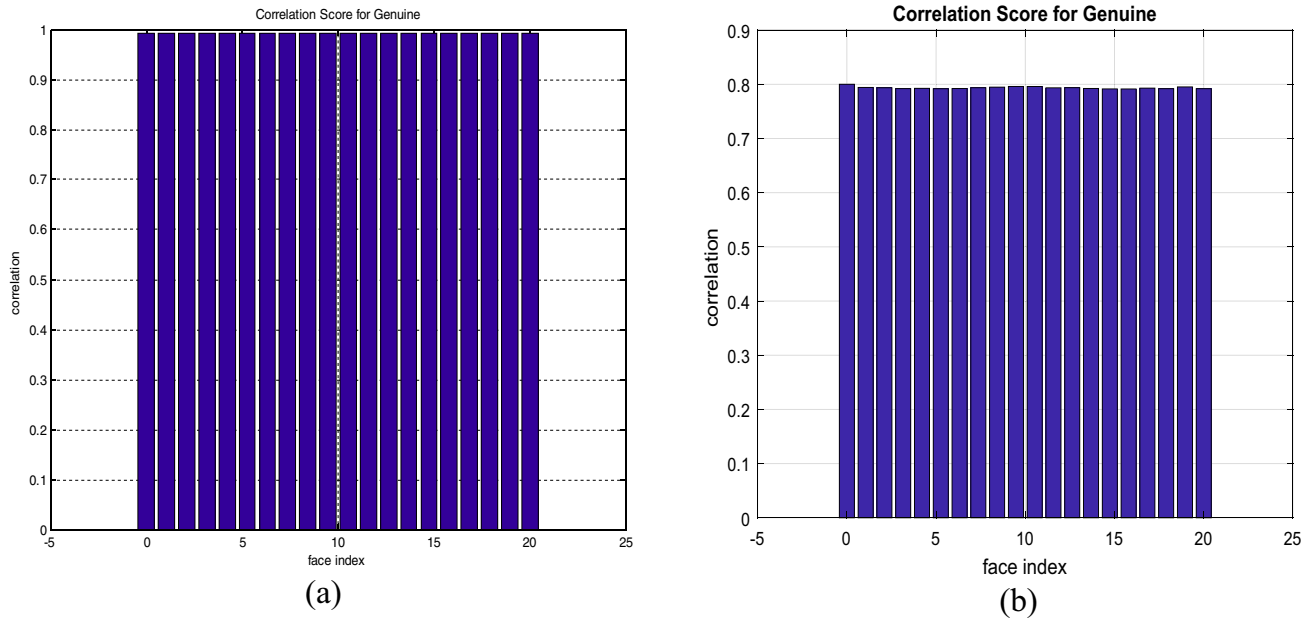

Fig. 28 Correlation scores of authorized face images (LFW dataset) for **a** the proposed system, **b** the CFR based on RP

based on RP encryption, and the proposed system presented in Fig. 7a–d are given in Fig. 13a–d. It is obvious from the figure that the deviation between the original biometric faces and the masked ones is high enough.

The distributions of genuine and imposter scores are evaluated for the proposed cancelable biometric recognition system based on some selected metrics. The proposed system performance efficiency is estimated by computing FPR, FNR, EER, AROC and ROC curves. For numerical evaluation of the proposed system and other existing biometric systems, Figs. 14a–d show these systems' genuine and imposter distributions, and the ROC curves are plotted in Fig. 15a–d. Table 2 gives a comparison of the proposed

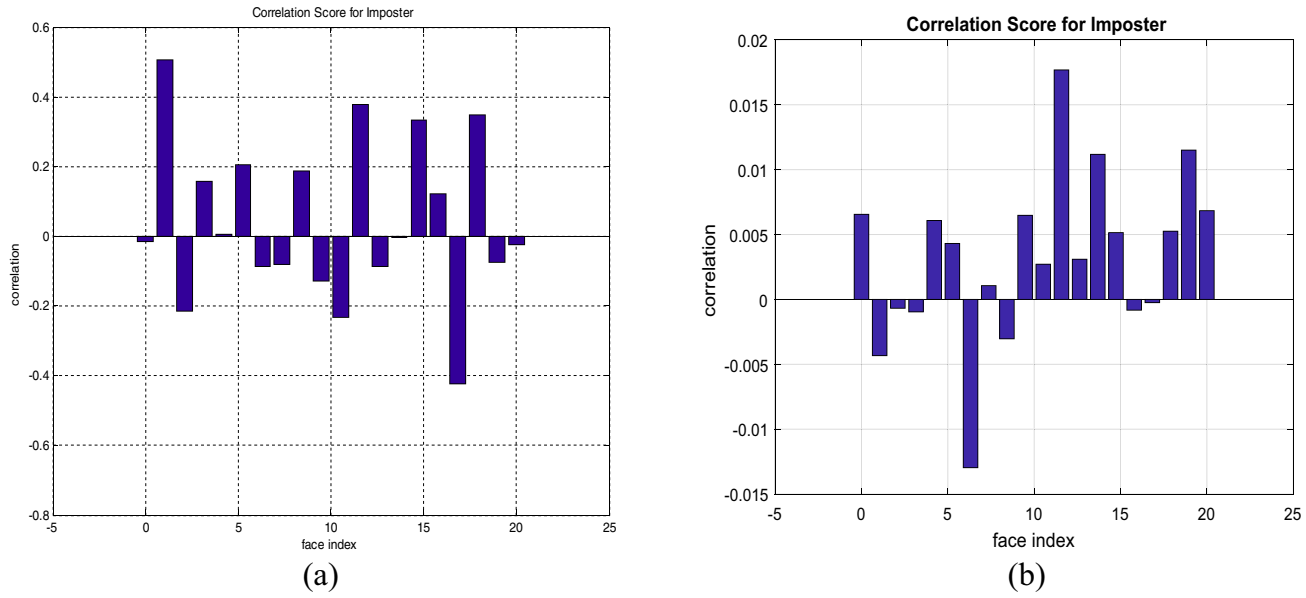

Fig. 29 Correlation scores of unauthorized face images (LFW dataset) for **a** the proposed system, **b** the CFR based on RP

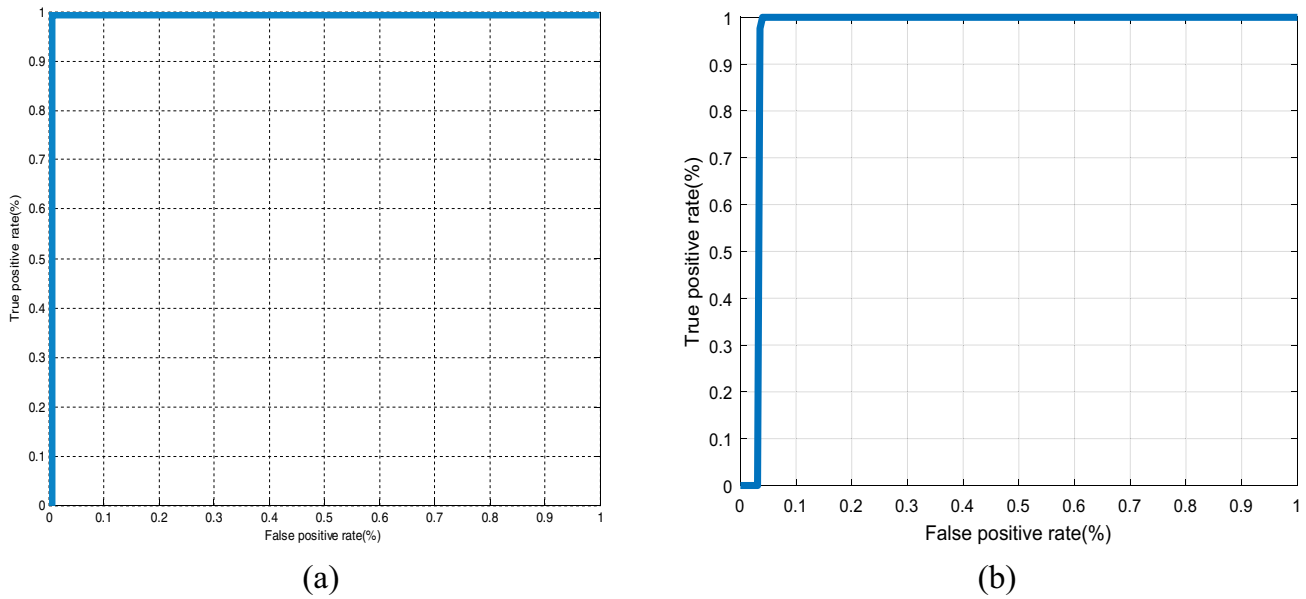

Fig. 30 Receiver Operating Characteristics (ROC) curves (LFW dataset) for **a** the proposed system, **b** the CFR based on RP

cancelable biometric system and other existing biometric systems using AROC, EER, mean of authorized correlation scores, and decidability metrics. From the table values, it is obvious that the proposed system achieves high performance and high levels of security.

Decidability is an evaluation metric used to differentiate between genuine and imposter distributions. The formula of the decidability can be expressed as:

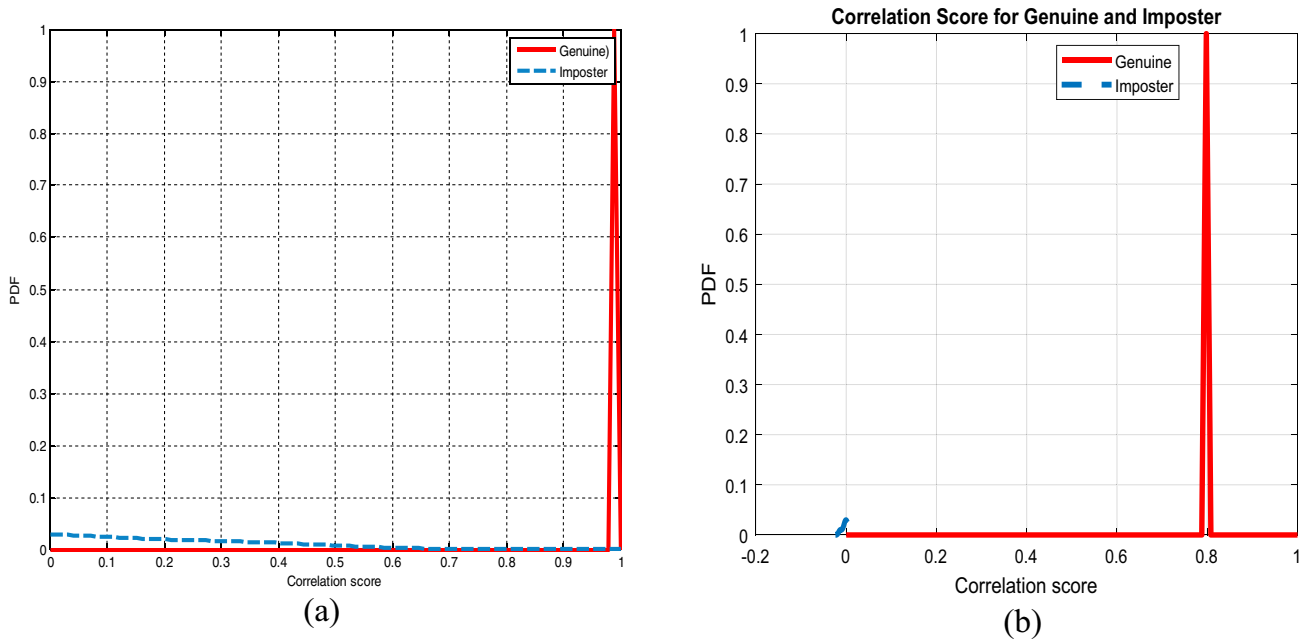

Fig. 31 Distributions of genuine and impostor scores (LFW dataset) for **a** the proposed system, **b** the CFR based on RP

$$D = \frac{\left|\mu_i - \mu_g\right|}{\sqrt{(\sigma_i^2 + \sigma_g^2)/2}} \tag{12}$$

where μ_i and μ_g represent the means, and σ_i^2 and σ_g^2 represent the variances of the impostor and genuine distributions, respectively. Larger values of decidability reflect a better performance of the biometric system. The higher the decidability values, the higher the biometric system performance is.

To ensure the efficiency of the proposed system, it was applied to other datasets, namely LFW [21] and FERET [22]. The images of both datasets are captured at different times, and different light and motion effects are also present. The original image samples of the LFW and FERET datasets are presented in Figs. 16 and 17, respectively. Figures 18, 19, 20, 21, 22, 23 and 24 illustrate the proposed and the CFR based on RP systems' simulation results on FERET dataset images. Also, Figs. 25 26, 27, 28, 29, 30 and 31 illustrate the simulation results of the proposed system and the CFR system based on RP on the LFW dataset images. Another-indicator to test the performance of the proposed system is to implement it on a dataset of similar images.

In fact, the cancelable biometric systems are offline systems that the user controls. So, he can control the initial image he introduces. Moreover, the noise mask generated depends on the initial image. If the user changes his image, he changes the mask totally, and hence he can generate a totally different cancelable template that can be used for a different application. That is why the proposed system is very sensitive to the initial images presented by the users. Figure 32 presents samples of similar images, and their histograms are present in Fig. 33. Figures 34a–f present the simulation results of the proposed system on similar images.

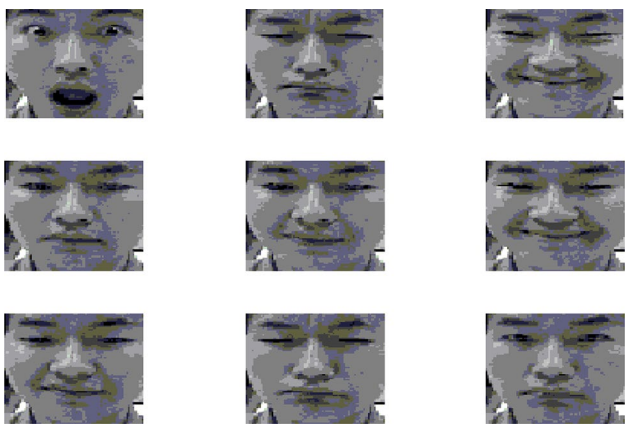

Fig. 32 Samples of similar images

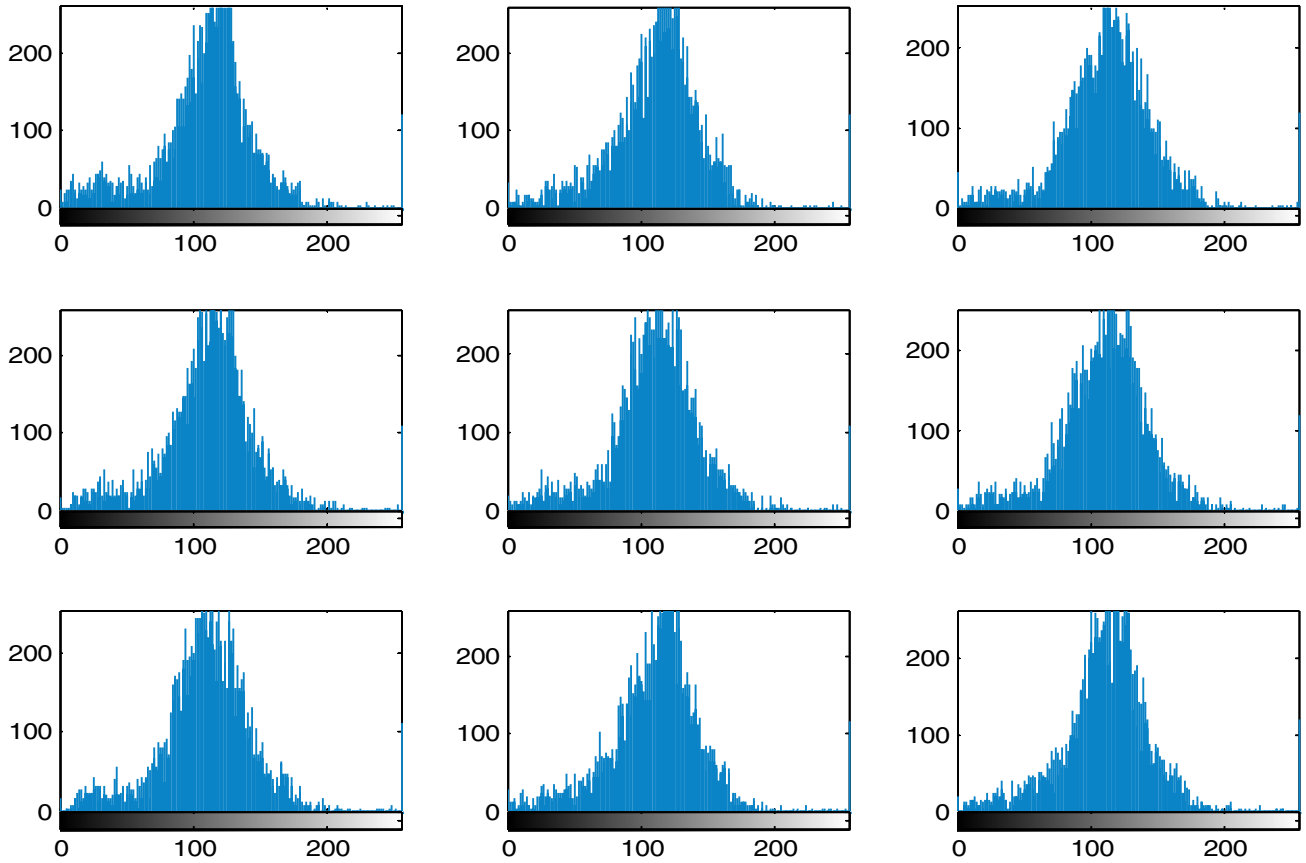

Fig. 33 Histograms of the similar images in Fig. 32

Tables 3 and 4 illustrate a comparison between the proposed system and the CFR based on RP using AROC, the mean of authorized correlation distribution, and the mean of unauthorized correlation distribution on the LFW and FERET datasets, respectively.

Table 5 presents the evaluation metrics, namely AROC, EER, decidability, and mean of authorized correlation score for the database of similar images. The table shows that the proposed system is very efficient for the dataset of similar images.

Finally, Table 6 provides a comparison of systems based on AROC metric on the three datasets (ORL, LFW, FERET) and the dataset of similar images. From the table, it is clear that the proposed system gives larger values of AROC for all mentioned datasets compared to other systems. This ensures higher performance and efficiency of the proposed system and its ability to secure all biometric applications.

Conclusion

This paper presented a new system for cancelable face recognition. It has many applications in improving security in airports, banking, and other substantial sectors by saving the data of authorized customers and subscribers. The proposed system is based on blurring, noise addition, and applying the inverse filter. The original face images are masked by blurring and addition of noise. The noise enhancement property of the inverse filter is exploited to mask faces. The masked face templates can be used as cancelable biometric templates. The proposed system has confirmed its validity on four datasets (ORL database, LFW dataset, FERET dataset, and the dataset of similar images). The results show that the proposed system performs efficiently as a cancelable face recognition system compared with the other methods. In future work, we intend to apply different types of inverse filters with different orders and noise patterns. Also, a cancelable biometric system based on optimized deep learning algorithms is aimed to be examined.

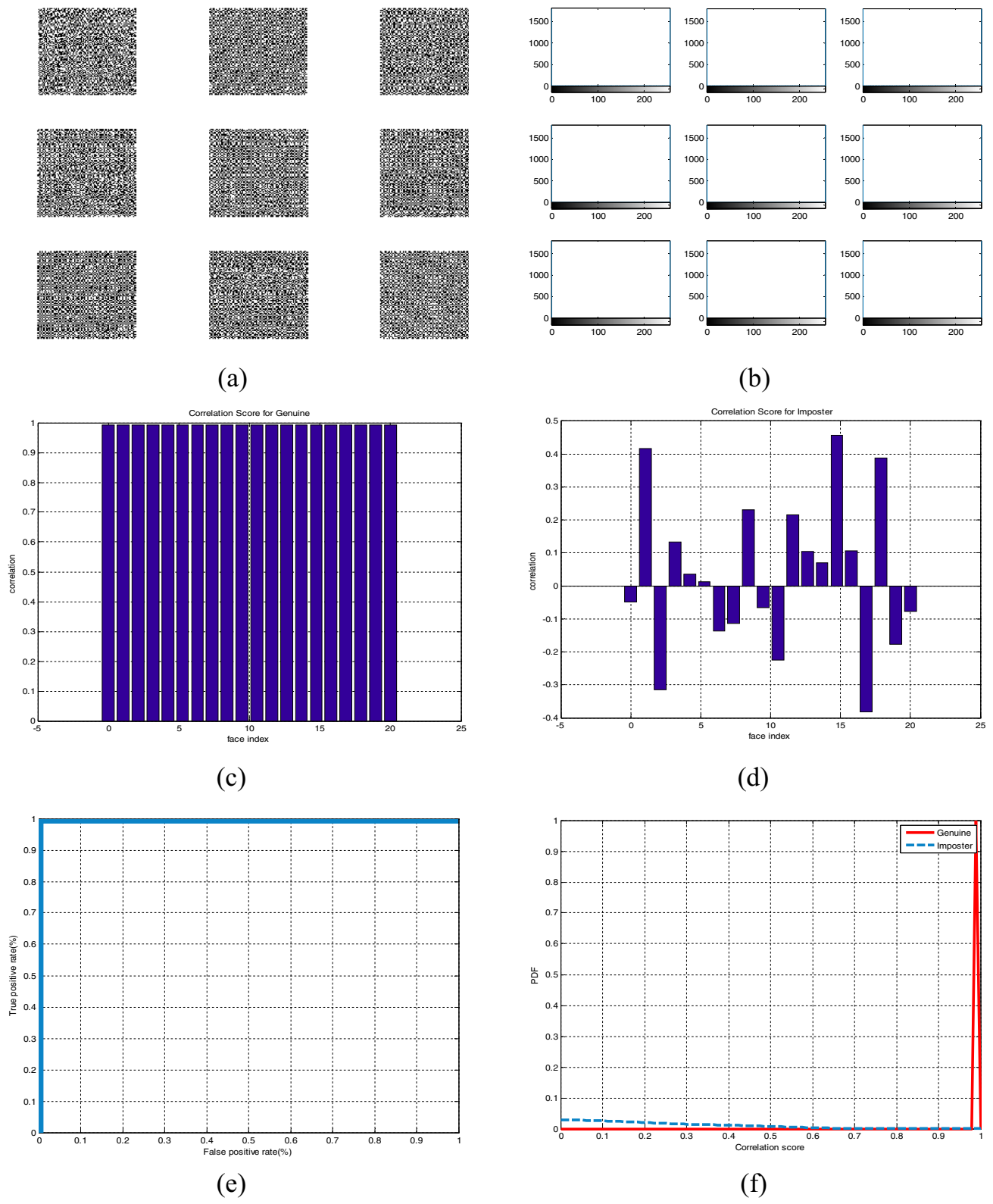

Fig. 34 Evaluation metrics for similar images based on the proposed system. **a** Masked templates for the similar images in Fig. 31, **b** Histograms of masked images, **c** correlation scores of authorized face images, **d** correlation score of unauthorized face images, **e** ROC curves, **f** genuine and impostor distributions

Table 3 Evaluation metrics of the CFR based on RP and the proposed system on LFW dataset

Evaluation metric	CFR based on RP	Proposed system
AROC	0.9668	1
Mean of authorized scores correlation scores	0.7936	0.9921
Mean of unauthorized correlation scores	0.0032	0.0435

Table 4 Evaluation metrics of the CFR based on RP and the proposed system on FERET dataset

Evaluation metric	CFR based on RP	Proposed system
AROC	0.9744	1
Mean of authorized correlation scores	0.7944	0.9921
Mean of unauthorized correlation scores	0.0024	0.0658

Table 5 Evaluation metrics for similar images based on the proposed system

AROC	EER	Decidability	Mean of authorized correlation scores
1	0.0013	5.8346	0.9921

Table 6 Comparison between systems on three datasets based on AROC metric

Method (dataset)	AROC
Proposed system (ORL)	1
Proposed system (LFW)	1
Proposed system (FERET)	1
Proposed system (Similar images)	1
Jigsaw only [23]	0.8967
FERFT only [24, 25]	0.8837
PCA [16]	0.7187
CASIA-IrisV3 database [12]	0.8630
Georgia Tech face database [14]	0.9067

Acknowledgement The researchers would like to acknowledge Deanship of Scientific Research, Taif University for funding this work.

Funding The researchers would like to acknowledge Deanship of Scientific Research, Taif University for funding this work.

References

1. W. El-Shafai, I. Almomani, A. Alkhayer, Optical bit-plane-based 3D-JST cryptography algorithm with cascaded 2D-FrFT encryption for efficient and secure HEVC communication. IEEE Access **2**(9), 35004–35026 (2021)
2. A. Alarifi, M. Amoon, M. Aly, W. El-Shafai, W, Optical PTFT asymmetric cryptosystem-based secure and efficient cancelable biometric recognition system. IEEE Access **3**(8), 221246–221268 (2020)
3. O. Faragallah, A. Afifi, H. El-Sayed, M. Alzain, J. Al-Amri, F. Abd El-Samie, W. El-Shafai, Efficient HEVC integrity verification scheme for multimedia cybersecurity applications. IEEE Access **7**(8), 167069–167089 (2020)
4. I. Elashry, W. El-Shafai, E. Hasan, S. El-Rabaie, A. Abbas, A. El-Samie, O. Faragallah, Efficient chaotic-based image cryptosystem with different modes of operation. Multimed. Tools Appl. **79**(29), 20665–20687 (2020)
5. N. Soliman, M. Khalil, A. Algarni, S. Ismail, R. Marzouk, W. El-Shafai, Efficient HEVC steganography approach based on audio compression and encryption in QFFT domain for secure multimedia communication. Multimed. Tools Appl. **80**(3), 4789–4823 (2021)
6. W. El-Shafai, Joint adaptive pre-processing resilience and post-processing concealment schemes for 3D video transmission. 3D Res. **6**(1), 1–13 (2015)
7. K. Abdelwahab, A. El-atty, M. Saied, W. El-Shafai, S. El-Rabaie, A. El-Samie, Efficient SVD-based audio watermarking technique in FRT domain. Multimed. Tools Appl. **79**(9), 5617–5648 (2020)
8. A. Algarni, G. El Banby, S. Ismail, W. El-Shafai, F. El-Samie, N.F. Soliman, Discrete transforms and matrix rotation based cancelable face and fingerprint recognition for biometric security applications. Entropy **22**(12), 1361 (2020)
9. N. El-Hag, A. Sedik, W. El-Shafai, H. El-Hoseny, A. Khalaf, A. El-Fishawy, G. El-Banby, Classification of retinal images based on convolutional neural network. Microsc. Res. Tech. **84**(3), 394–414 (2021)
10. L. Abou Elazm, S. Ibrahim, M. Egila, H. Shawky, M. Elsaid, W. El-Shafai, F. Abd El-Samie, Cancellable face and fingerprint recognition based on the 3D jigsaw transform and optical encryption. Multimed Tools Appl. **7**(9), 14053–14078 (2020)
11. W. El-Shafai, S. El-Rabaie, M. El-Halawany, F. El-Samie, Enhancement of wireless 3d video communication using color-plus-depth error restoration algorithms and Bayesian Kalman filtering. Wirel Pers. Commun. **97**(1), 245–268 (2017)
12. O. Faragallah, W. El-Shafai, A. Sallam, I. Elashry, E. El-Rabaie, A. Afifi, H. El-sayed, Cybersecurity framework of hybrid watermarking and selective encryption for secure HEVC communication. J. Ambient Intell. Humanid Comput. **13**(2), 1215–1239 (2022)
13. I. Badr, A. Radwan, E. El-Rabaie, L. Said, G. El Banby, W. El-Shafai, F. Abd El-Samie, Cancellable face recognition based on fractional-order Lorenz chaotic system and Haar wavelet fusion. Digital Sign. Process **11**(6), 103103 (2021)
14. W. El-Shafai, F. Mohamed, H. Elkamchouchi, M. Abd-Elnaby, A. Elshafee, Efficient and secure cancelable biometric authentication framework based on genetic encryption algorithm. IEEE Access **2**(9), 77675–77692 (2021)
15. F. Abd El-Samie, R. Nassar, M. Safan, M. Abdelhamed, A. Khalaf, G. El Banby, W. El-Shafai, Efficient implementation of optical scanning holography in cancelable biometrics. Appl. Opt. **60**(13), 3659–3667 (2021)
16. S. Ibrahim, M. Egila, H. Shawkey, M. Elsaid, W. El-Shafai, F. Abd El-Samie, Hardware implementation of cancellable biometric

systems, in *Fourth IEEE International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*, pp. 1145-1152 (October) (2020)
17. H. El-Hameed, N. Ramadan, W. El-Shafai, A. Khalaf, H. Ahmed, S. Elkhamy, F. El-Samie, Cancelable biometric security system based on advanced chaotic maps. The V Comput **38**(6), 2171–2187 (2021)
18. I. Almomani, W. El-Shafai, A. AlKhayer, A. Alsumayt, S. Aljameel, Proposed biometric security system based on deep learning and chaos algorithms. Comput., Mater. Contin. **74**(2), 3515–3537 (2023)
19. L. Elazm, W. El-Shafai, S. Ibrahim, M. Egila, H. Shawkey, Efficient hardware design of a secure cancellable biometric cryptosystem. Intell. Autom. Soft Comput. **36**(1), 929–955 (2023)
20. W. El-Shafai, M. Elsayed, M. Rashwan, M. Dessouky, A. El-Fishawy, Optical ciphering scheme for cancellable speaker identification system. Comput. Syst. Sci. Eng. **45**(1), 563–578 (2023)
21. A. Ayoup, A. Khalaf, W. El-Shafai, F. Abd El-Samie, F. Alraddady, S. Eldin, Cancellable multi-biometric template generation based on arnold cat map and aliasing. CMC-Comp. Mater. Continua **72**(2), 3687–3703 (2022)
22. S. El-Gazar, W. El Shafai, G. El Banby, H. Hamed, G. Salama, M. Abd-Elnaby, F. Abd El-Samie, Cancelable speaker identification system based on optical-like encryption algorithms. Comput. Syst. Sci. Eng. **43**(1), 87–102 (2022)
23. A. Ayoup, A. Khalaf, F. Alraddady, F. Abd El-Samie, W. El-Shafai, Cancelable multi-biometric template generation based on dual-tree complex wavelet transform. Intell. Autom Soft Comput. **33**(2), 1289–1304 (2022)
24. I. Almomani, A. AlKhayer, W. El-Shafai, Novel ransomware hiding model using HEVC steganography approach. CMC Comput. Mater. Cont **70**(2), 1209–1228 (2021)
25. A. Alarifi, S. Sankar, T. Altameem, K. Jithin, M. Amoon, W. El-Shafai, A novel hybrid cryptosystem for secure streaming of high efficiency H. 265 compressed videos in IoT multimedia applications. IEEE Access **8**(2), 128548–128573 (2020)