electronics

Article

Efficient Implementation of Homomorphic and Fuzzy Transforms in Random-Projection Encryption Frameworks for Cancellable Face Recognition

Abeer D. Algarni [1,*], Ghada M. El Banby [2], Naglaa F. Soliman [1,3], Fathi E. Abd El-Samie [4] and Abdullah M. Iliyasu [5,6,7,*]

[1] Department of Information Technology, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, Riyadh 84428, Saudi Arabia; nagla_soliman@yahoo.com
[2] Department of Industrial Electronics and Control Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt; ghadabanby@yahoo.com
[3] Department of Electronics and Communications, Faculty of Engineering, Zagazig University, Zagazig 44519, Egypt
[4] Department Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt; fathi_sayed@yahoo.com
[5] Electrical Engineering Department, College of Engineering, Prince Sattam Bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia
[6] School of Computing, Tokyo Institute of Technology, Yokohama 226-8502, Japan
[7] School of Computer Science and Technology, Changchun University of Science and Technology, Changchun 130022, China
* Correspondence: adalqarni@pnu.edu.sa (A.D.A.); a.iliyasu@psau.edu.sa (A.M.I.)

Received: 12 March 2020; Accepted: 8 June 2020; Published: 24 June 2020

Abstract: To circumvent problems associated with dependence on traditional security systems on passwords, Personal Identification Numbers (PINs) and tokens, modern security systems adopt biometric traits that are inimitable to each individual for identification and verification. This study presents two different frameworks for secure person identification using cancellable face recognition (CFR) schemes. Exploiting its ability to guarantee irrevocability and rich diversity, both frameworks utilise Random Projection (RP) to encrypt the biometric traits. In the first framework, a hybrid structure combining Intuitionistic Fuzzy Logic (IFL) with RP is used to accomplish full distortion and encryption of the original biometric traits to be saved in the database, which helps to prevent unauthorised access of the biometric data. The framework involves transformation of spatial-domain greyscale pixel information to a fuzzy domain where the original biometric images are disfigured and further distorted via random projections that generate the final cancellable traits. In the second framework, cancellable biometric traits are similarly generated via homomorphic transforms that use random projections to encrypt the reflectance components of the biometric traits. Here, the use of reflectance properties is motivated by its ability to retain most image details, while the guarantee of the non-invertibility of the cancellable biometric traits supports the rationale behind our utilisation of another RP stage in both frameworks, since independent outcomes of both the IFL stage and the reflectance component of the homomorphic transform are not enough to recover the original biometric trait. Our CFR schemes are validated on different datasets that exhibit properties expected in actual application settings such as varying backgrounds, lightings, and motion. Outcomes in terms standard metrics, including structural similarity index metric (SSIM) and area under the receiver operating characteristic curve (AROC), suggest the efficacy of our proposed schemes across many applications that require person identification and verification.

Keywords: cancellable biometrics; intuitionistic fuzzy logic; random projection; homomorphic transform; face recognition

1. Introduction

Biometric signals and images from persons are used across different domains and applications such as identification, verification, and authentication. The most common biometrics are fingerprints, faces, iris, palm/vein prints, and speech signals. The utilisation of biometric traits in identification has witnessed tremendous growth and sophistication making it ubiquitous for a wide range of applications. Today, institutions, companies, universities, banks, and airports have their own systems using different biometric traits. The basic idea of operation of these systems involves collection of biometrics from enrolled persons, extraction of discriminating features from the collated biometrics as a tool for data reduction, and storage of these features in a database. This registration or enrollment process is considered as the training phase. In the other phase, known as the testing phase, features from incoming biometrics for new persons are extracted and matched with the stored features [1,2]. This phase can be performed with or without classifiers.

Fingerprint recognition depends on the extraction of minutia, which are specific plot points on a fingerprint, to discriminate between different persons. On the other hand, facial recognition relies on discrimination of geometric markers of facial features including eyes, nose, and mouth for person identification and authentication. Meanwhile, in iris recognition, the initial focus is on the localisation of the iris region in the image, which is followed by the elimination of the effects of eyelids and eyelashes, which are considered as noise. Subsequently, transformations of polar or rectangular coordinates are used to isolate features that are extracted from the transformed patterns and then coded. As outlined, features extracted from fingerprint and face images are geometric features, while those extracted from iris images are transform domain features.

In contrast, speech recognition differs from face, fingerprint, and iris recognition as it deals with one-dimensional (1D) signals. Moreover, since speech signals have power distributed on the same frequency band, speakers can be distinguished based on their resolved power profile over this wide band. Most speaker identification systems adopt similar concepts to resolve speech signals of the speakers over the same band and obtain power distributions over the non-linearly segmented overlapping sub-bands required to extract discriminating features between speakers.

Traditional biometric systems depend on the acquisition of signals or images from the users or subscribers, extraction of features from these signals or images, and subsequent feature matching with a previously stored database. The main disadvantage of this traditional approach is that each person has to provide his original biometrics for enrollment as well as possible feature extraction and storage in the database. This means that, once the database is compromised, the integrity of the original biometrics will be lost forever and, hence, the whole system loses its confidentiality and credibility. Moreover, users whose biometrics have been compromised will not be able to use them again in other systems. Thus, traditional three-step biometric systems that depend on enrollment, feature extraction and feature matching are no longer credible.

Recently, the paradigm of cancellable biometrics has emerged as a motif to safeguard the important biometric data. A major advantage of Cancellable Biometric Systems (CBS) is their ability to support the protection of the original biometric data. In these systems, different biometric inputs can be revised or updated without affecting the entire system. To illustrate, in CBS that depend on geometric transforms, one-way geometric transforms can be used to modify the biometric patterns. Such transforms can be easily revised whilst maintaining the unidirectional security feature. For biometrics such as iris, feature extraction is very essential, and hence, for biometric security, operations such as bio-hashing can be executed at the feature level. Similarly, for 1D biometric signals, such as speech signals, operations such as bio-convolution can be executed.

Cancellable biometric frameworks provide templates to safeguard the integrity of biometric data for different applications [3–9]. In [3], Soliman et al. presented a CBS based on Double Random Phase Encoding (DRPE) for applications in both face and iris recognition. This approach depends on generation of feature matrices from either the face or iris to be encrypted by the DRPE technique. The simulation results reported an Equal Error Rate (EER) value of 0.17% and an Area under the

Receiver Operating Characteristic (AROC) of 99.3%. In [4], Savvides et al. presented a correlation filter-based CBS that depends on generating random user-specific convolution kernels. During the enrollment stage, a Personal Identification Number (PIN) is used to generate a random convolution kernel to be convolved with the training images in order to generate a Minimum Average Correlation Energy (MACE) filter. The MACE encrypted filter is subsequently used to measure correlation with the encrypted test images through the convolution process. Furthermore, in [5], Kaur and Khanna introduced a multi-level transformation-based CBS that depends on Log-Gabor filters and the RP technique to produce cancellable feature vectors to be used in person authentication and verification. In their contribution in [6], Maiorana et al. presented a convolution-based technique to generate new versions of original biometric templates based on template segmentation. The segmented sequences are subjected to a linear convolution process that produces transformed cancellable versions of the sequences. Moazz et al. presented a CBS for face recognition using Bloom filters in [7]. This system depends on the extraction of features from faces to be used in the generation of new templates. The feature bits are passed through Bloom filters with the help of PINs. In [8], Andrew et al. presented a bio-hashing CBS for face recognition. In this system, an extracted low-dimension feature matrix is re-projected randomly to generate a binary bit string. In another interesting contribution [9], Kaur and Khanna reported a CBS using Gaussian random vectors and one-way modulus hashing. This method was utilised in face and palm print identification. Simulation results reported in that study proved that the generated templates are non-invertible, easy to revoke, and they also give good performance.

While building on these efforts, among others, in this study, we present two new frameworks for generating efficient cancellable face templates. Like the studies highlighted, our proposed cancellable face recognition (CFR) frameworks utilise pre-processing stages to generate sophisticated patterns from the original biometrics. However, in this study, both pre-processing stages are non-invertible, a property that is further exploited to realise a random projection (RP) based encryption mechanism, which is subsequently used to mask the extracted patterns. Moreover, in the first framework (i.e., CFR1), a hybrid structure combining intuitionistic fuzzy logic (IFL) and random projection (RP) is used to accomplish full distortion and encryption of the original biometric traits to be saved in the database. In the second framework (i.e., CFR2), cancellable biometric traits are generated via homomorphic transform followed by application of the RP on the reflectance components which can be considered as signatures to evaluate the original biometric templates. Random kernel convolution and salting are considered in evaluating the performance of the RP encryption step, while the encrypted templates are stored in a database that is revocable via different random matrices. Furthermore, several quality tests and metrics are employed to provide an extensive evaluation of the robustness of the proposed frameworks when exposed to different types of attacks.

The rest of this paper is organised as follows. An overview of IFL, homomorphic transform, and Gaussian RP is provided in the next section (i.e., Section 2). This foundation motivates the design of the two proposed CFR biometric frameworks based on IFL and homomorphic transforms, whose rudiments are presented in Section 3. Experiments and performance evaluation of both CFR frameworks are presented and discussed in Section 4.

2. Materials and Methods

2.1. Intuitionistic Fuzzy Sets

Fuzzy processing is a common component employed in the pre-processing step of many image processing techniques [10]. The concept of fuzzy sets, where a degree of membership and its shape are used to denote a user's choice, was introduced by Zadeh in 1965. The shapes include Gaussian, triangular, trapezium and other shapes. In [11], Atanassov proposed a modified fuzzy set called intuitionistic fuzzy sets (IFS), which has both degrees of membership and non-membership that differ from the complements of the membership function. The IFS is considered as a powerful extension of Zadeh's fuzzy theory dealing with applications in vague and uncertain systems [12].

Consequently, it has found applications in numerous dynamic fields, such as industrial informatics, medical image diagnosis and machine learning [13–15] with intriguing prospects for extension to the field of cancellable biometrics.

Mathematically, the IFS representation of an image A can be described as:

$$A = \{< p, \mu_A(p), v_A(p) > | p \in P\} \tag{1}$$

where $\mu_A(p) : P \to [0, 1]$ is the degree of membership of pixel p in the finite set P and $v_A(p)$ can be computed using (2).

$$v_A(p) = 1 - \mu_s(p) \tag{2}$$

$v_A(p)$ is the non-membership function of pixel p in a finite set P with the condition that it can satisfy the relation in Equation (3).

$$0 \leq \mu_A(p) + v_A(p) \leq 1 \tag{3}$$

The third parameter π_A is called the hesitation degree, and it is represented by the Equation:

$$\pi_A(p) = 1 - \mu_A(p) - v_A(p) \tag{4}$$

where $0 \leq \pi_A(o) \leq 1$ for all $p \in P$. For images, the first step in the IFS depends on generating membership and non-membership degrees for each grey-scale value in the image. Vlachos and Sergiadis [16] proposed the determination of both functions, where an $M \times N$ sized image A is fuzzified according to the relationship in (5).

$$\mu_A(p) = \frac{p - p_{min}}{p_{max} - p_{min}} \tag{5}$$

where p is a grey level of the original image A, p_{min} and p_{max} are the minimum and maximum grey levels in the image, respectively.

The membership degree of the IFS image is calculated according to (6).

$$\mu_{ifs}(p; \lambda) = 1 - (1 - \mu_A(p))^{\lambda - 1}, \tag{6}$$

and the non-membership degree of the IFS image is similarly denoted using:

$$v_{ifs}(p; \lambda) = (1 - \mu_{Iifs}(p; \lambda))^{\lambda} \tag{7}$$

Therefore, the hesitation degree of the IFS image can be deduced using:

$$\pi_{ifs}(p; \lambda) = (1 - \mu_{ifs}(p; \lambda) - v_{ifs}(p; \lambda)) \tag{8}$$

where $\lambda \geq 1$.

The biometric source image can be represented as an IFS image in the form:

$$A_{ifs} = \{< p, \mu_A(p, \lambda), v_A(p, \lambda) > \big| p \in 0, \ldots\ldots, l - 1\} \tag{9}$$

Moreover, Atanassov recommended a deconstruction methodology to convert the IFS image into the grey-scale domain using (10) and (11) [15].

$$p' = (l - 1)\mu_{D(ifs)}(p) \tag{10}$$

and

$$\mu_{D(ifs)}(p) = \alpha + (1 - \alpha)\mu_A(p; \lambda) - \alpha v_A(p; \lambda) \tag{11}$$

where p and p' are the initial and final intensity levels of the image, respectively, and α is a constant value selected in the range [0, 1].

The intuitionistic fuzzy process can be summarised in the form presented in Figure 1, which represents the decorrelation step for the image pixels prior to the subsequent encryption step [17,18].

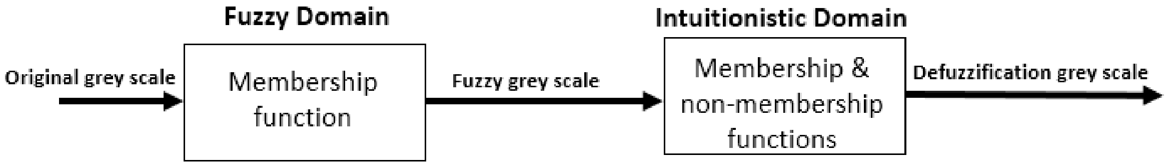


Figure 1. Representation of the intuitionistic fuzzy process of images.

2.2. Homomorphic Transform

Generally, an image is an aggregate of light reflected from objects such that any image $f(x,y)$ can be represented using two different components: one representing the light falling on the objects and the other representing the light reflected from the objects [19]. These two components are called the illumination and reflectance components denoted as $i(x,y)$ and $r(x,y)$, respectively. Consequently, an image can be represented in the form presented below:

$$f(x,y) = i(x,y) \times r(x,y) \tag{12}$$

where $f(x,y)$ represents the greyscale values of pixels in the image, $i(x,y)$ is the illumination component and $r(x,y)$ is the reflectance component.

Since the light falling over the scene is nearly constant and its distribution is approximately the same, changes occur in an image for the most important features in the reflectance component. Further, this component can be separated using a logarithmic operation defined in Equation (13) and a High-Pass Filter (HPF) as illustrated in Figure 2.

$$\log[f(x,y)] = \log(i(x,y)) + \log(r(x,y)) \tag{13}$$

Homomorphic transform is a popular image decomposition transform whose basic idea involves isolating details from the illumination component of an image as represented by the reflectance component [19]. In cancellable biometric applications, these details can be reused instead of the original biometrics. In our proposed cancellable face recognition framework, reflectance components of face images are encrypted with random projections (RP) to generate the cancellable face templates.

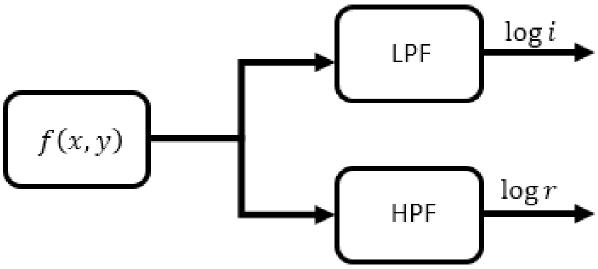


Figure 2. Homomorphic decomposition of an image.

2.3. Gaussian RP

The random projection (RP) is the process of projecting a signal or a feature vector onto a random space. It can be implemented through the multiplication of the signal or the feature vector by a random matrix. If the original data can be represented as $\mathbf{X}_{d\times N}$ multiplying it by some random matrix A (of dimensions $k \times d$) produces the RP output that is represented as:

$$\mathbf{Y}_{k\times N} = \mathbf{A}_{k\times d} \times \mathbf{X}_{d\times N} \tag{14}$$

The RP is adopted in this study as a tool to encrypt the extracted patterns from the original biometrics either with fuzzy processing or homomorphic transformation. In recent implementations of CBS, the RP has been applied on the original biometric templates directly [9,18,20–22]. Both Homomorphic and fuzzy transforms share the common feature of non-invertibility. Therefore, their use supports retention of details from the original biometric data.

We also note that, in computing (14), the relative distances between the original biometric templates should be unchanged or increased in the RP space. Moreover, the RP matrix must be selected to satisfy the Johnson and Lindenstrauss lemma (i.e., the JL lemma) [18], which helps to preserve the distances between encrypted biometric templates close to their original counterparts between original templates. Gaussian random matrices achieve the required distances in the random space.

3. Cancellable Face Recognition Frameworks

Building on the studies highlighted in the previous sections, the rudiments of our use of cancellable biometric systems (CBS) in face recognition, i.e., cancellable face recognition (CFR) schemes are presented in this section.

3.1. CFR Framework Based on Intuitionistic Fuzzy Logic and Random Projection

In this section, an efficient, robust, and revocable Gaussian RP process is proposed to safeguard biometric templates. The block diagram of the proposed CFR framework is presented in Figure 3 and, as seen therein, following fuzzy pre-processing of the images, Gaussian RP is used to encrypt the images. In the enrollment phase, IFS computation is performed on the raw biometric images of all users. More precisely, the greyscale values of the images are transformed to an intuitionistic fuzzy domain using the approach adduced by Handmandlu et al. in [23] according to the three-step EGE protocol presented in the sequel.

Step 1: E: Estimation of the membership function via (15).

$$\mu_{ij} = \left(X_{ij}\right) - (X_{\min})/(X_{\max} - X_{\min}) \tag{15}$$

where μ_{ij} refers to the degree of brightness of the grey level intensity at coordinates i and j.

Step 2: G: Generation of the membership and non-membership functions.

Using (15), the fuzzy membership of each pixel in the image is constructed. The membership and non-membership functions are generated according to Equations (6) and (7). Upon retrieving the intuitionistic components of the biometric image, a defuzzification phase is applied to convert the image from its fuzzy intuitionistic domain to a greyscale domain as dictated by Equations (10) and (11).

Step 3: E: Encryption based on Gaussian RP.

Finally, the intuitionistic output image is encrypted using the RP technique presented earlier in Section 2.3 to perform additional distortion of the biometric templates. A Gaussian random matrix with zero mean and a variance of 0.1 is used as provided in (14). Consequently, highly secure, revocable, and non-invertible biometric templates are generated and stored in the database. The outline of the proposed framework, i.e., CFR1, is presented in Figure 3.

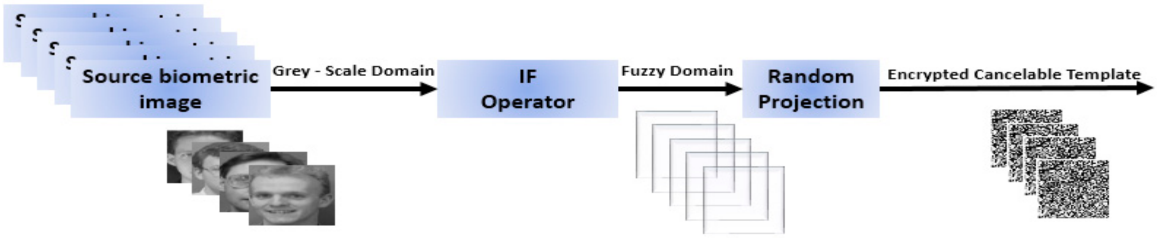


Figure 3. Proposed CFR framework based on intuitionistic fuzzy logic and Random Projection (RP) (i.e., CFR1).

3.2. CFR Framework Based on Homomorphic Transform and Random Projection

The reflectance components obtained from the homomorphic transform are adopted in the cancellable biometric framework as they contain most of the image details [22]. Furthermore, to generate cancellable biometric templates in conformity with (14), RP is applied on the reflectance components. Figure 4 presents the outline of the proposed cancellable face recognition framework based on homomorphic transform and RP (i.e., CFR2). Therefrom, it can be seen that, during the enrollment phase of the system, the original templates are processed to extract the reflectance components, which are then encrypted using RP to generate the cancellable biometric templates that are subsequently stored in the database. Meanwhile, in the authentication phase, the correlation score is used as matching criterion [24].

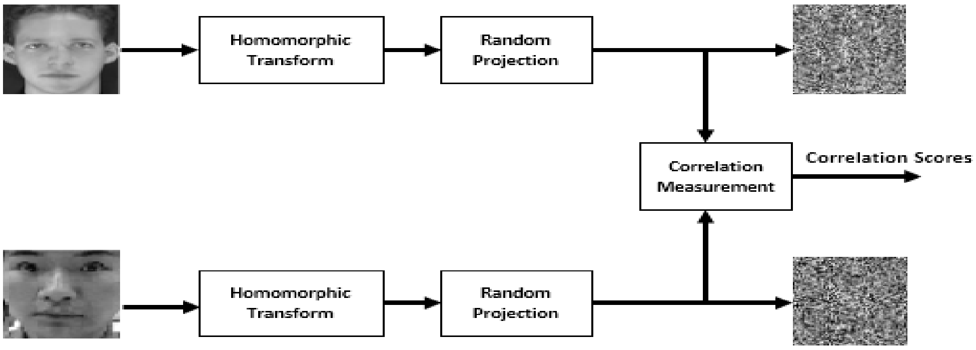


Figure 4. Proposed CFR framework based on homomorphic transform and RP (i.e., CFR2).

4. Results and Discussion

In this study, the facial recognition system is implemented via a workstation equipped with MATLAB Intel® Core ™ i5-4210U on a CPU with 1.7 GHz processor. The primary objective of any CBS scheme is to prove resistance to intrusion attacks. Therefore, we present a study of the robustness of the two proposed CFR frameworks to intrusion attacks. Samples of facial images obtained from the Research Laboratory for Olivetti and Oracle (ORL) database [25], the NiST Face Recognition Technology (FERET) dataset [26] and the Mass Labelled Faces in the Wild (LFW) dataset of the University of Massachusetts' Computer Vision laboratory [27] are used in our simulations. To evaluate the robustness of the proposed frameworks, i.e., CFR with IFL and Gaussian RP (or simply CFR1) and CFR with Homomorphic transform and Gaussian RP (or simply CFR2), several metrics are used. Additionally, we validate the effectiveness of the proposed frameworks by comparison with the random salting encryption in the homomorphic domain and random kernel convolution in the homomorphic domain.

4.1. Performance Evaluation for Encryption Mechanisms and Cancellable Schemes

The first set of results presented are those for the ORL dataset, whose sample images were presented in Figure 5. This dataset contains 40 subjects, with 10 images for each subject. The images were taken at different times, varying lighting, varying facial expressions and with small variations in the facial orientation [25]. Encrypted versions of the sample images in Figure 5 are presented in Figure 6.

Histogram distributions are used in evaluating the robustness of the encryption scheme to statistical attacks. Histogram distributions for sample test images in Figure 5 are presented in Figure 7. A comparison between the histogram distributions obtained in CFR1, CFR2, salting after homomorphic transform, and random kernel convolution after homomorphic transform are presented in Figure 8a–d. The figure reveals disparity in histogram distributions from those of the original face images, which is a property of good encryption schemes.

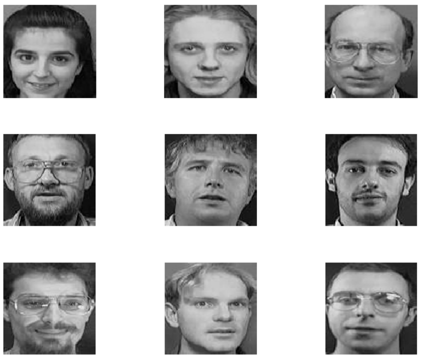


Figure 5. Sample facial images from Research Laboratory for Olivetti and Oracle (ORL) database used as original biometrics [25].

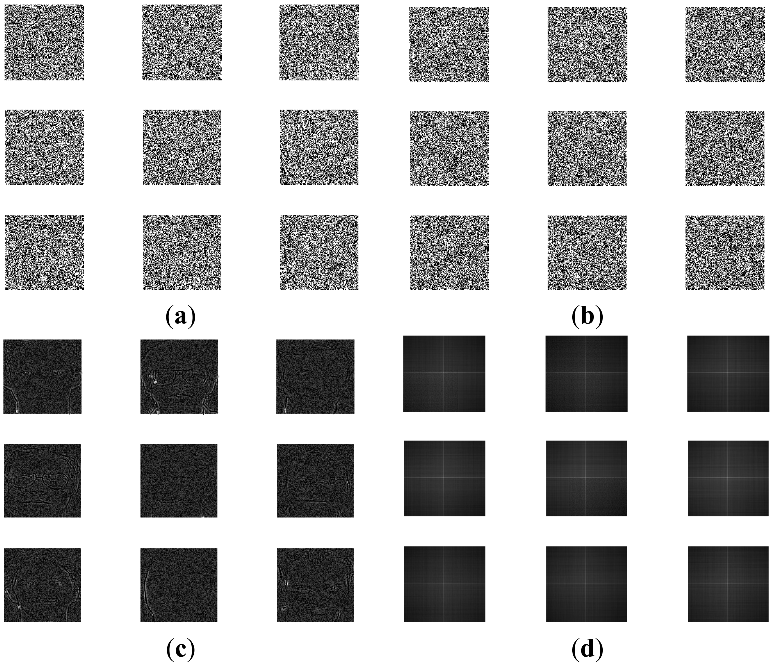


Figure 6. Encrypted versions of biometric faces in Figure 5 (from ORL dataset) for (**a**) CFR1 (**b**) CFR2, (**c**) homomorphic transform followed by salting and (**d**) homomorphic transform followed by random kernel convolution.

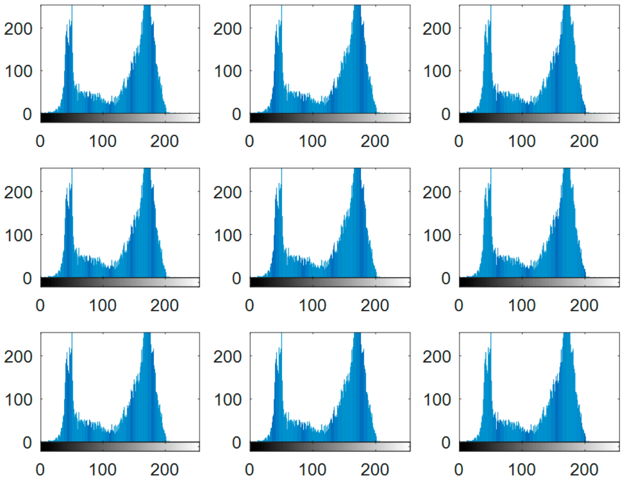


Figure 7. Histogram distributions of the sample facial images in Figure 5.

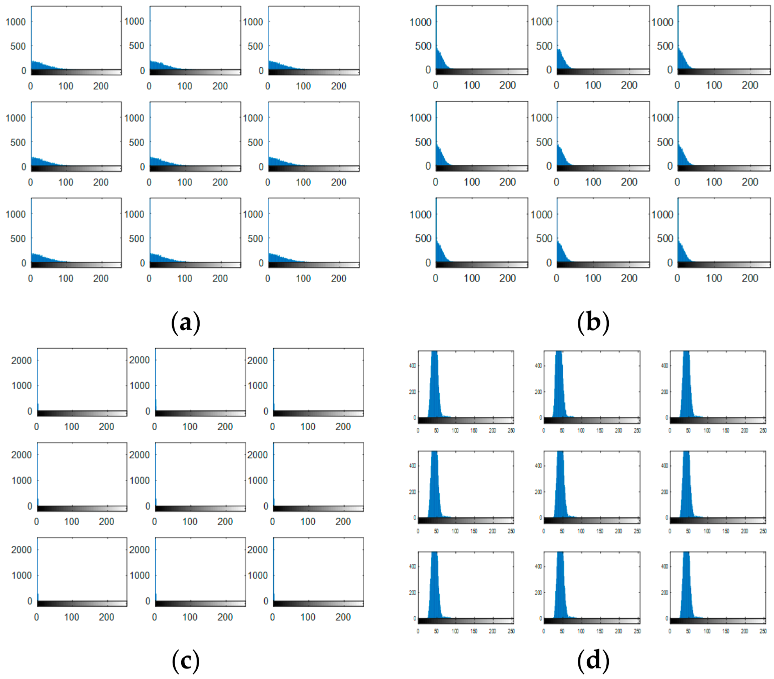


Figure 8. Histograms of encrypted images based on combinations in Figure 6, i.e., (**a**) CFR1, (**b**) CFR2, (**c**) homomorphic transform followed by salting and (**d**) homomorphic transform followed by random kernel convolution.

Another effective metric widely used in assessing the efficiency of encryption protocols is the correlation coefficient, which, in our case, measures the correlation between the encrypted images stored in the database and the encrypted versions of new subjects. Mathematically, the correlation coefficient is estimated as follows:

$$R_{xy} = \frac{\frac{1}{N}\sum_{i=1}^{N}(x_i - \overline{x})(y_i - \overline{y})}{\sigma_x \sigma_y} \tag{16}$$

where N is the total number of pixels, x and y are the encrypted templates stored in the database and the new subject encrypted template, respectively.

Figure 9 presents the correlation coefficient values estimated between authorised biometrics and their counterparts in the database in the presence of noise for all encryption schemes. Similarly, Figure 10 shows the correlation coefficient values estimated for unauthorised records with all records stored in the database. The results in both figures reveal that all correlation scores for authorised patterns are higher than 0.3, while those for unauthorised patterns are less than 0.05. Thus, a threshold can be easily set in the margin of 0.05 to 0.3 to effectively discriminate between authorised and unauthorised patterns. This indicates high security and performance of the proposed frameworks since a wide margin can be used to set the verification threshold.

Furthermore, to better understand the results, they are further interpreted in terms of statistical parameters of the Receiver Operating Characteristic (ROC) curves. Specifically, we study the False Acceptance Rate (FAR) versus the False Rejection Rate (FRR) [3,19,24]. The FAR reflects the misclassified imposters as being genuine, while the FRR represents the percentage of genuine examinations misunderstood and interpreted as being impostors. Figure 11 reports the ROC curves for all four CFR cancellable biometric frameworks reported in our experiments. From these curves, it can be deduced that the AROC values for both proposed frameworks are the highest, which points to the strength of these frameworks. Moreover, to further buttress this, the probability distributions of the correlation coefficients of the genuine and imposter tests are presented in Figure 12. Here, the rightmost Probability Distribution Functions (PDFs) are for the two proposed CFR frameworks.

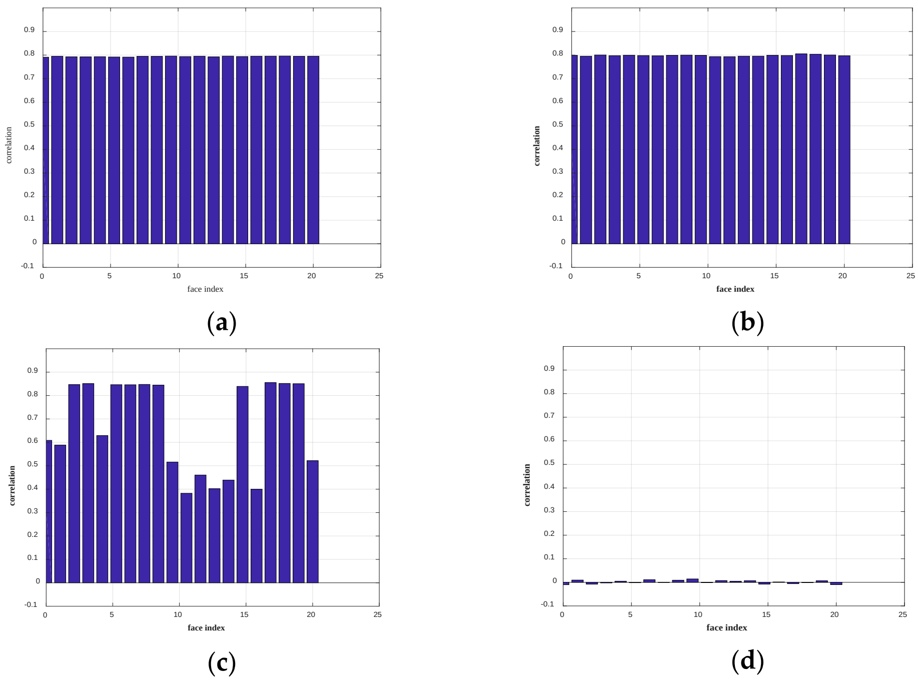


Figure 9. Correlation scores for authorised patterns (for ORL dataset) for (**a**) CFR1, (**b**) CFR2, (**c**) homomorphic transform followed by salting and (**d**) homomorphic transform followed by random kernel convolution.

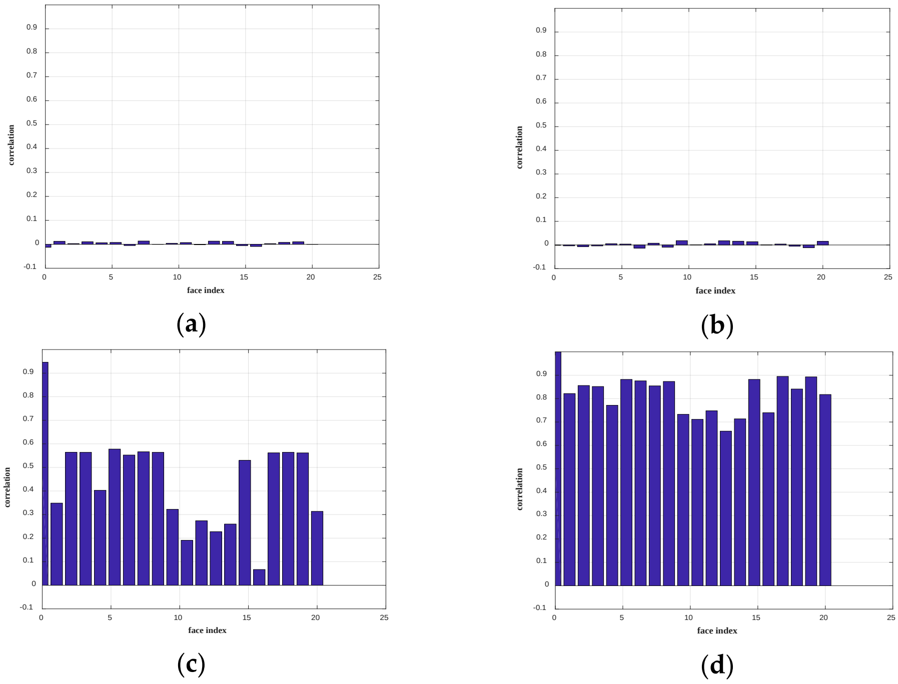
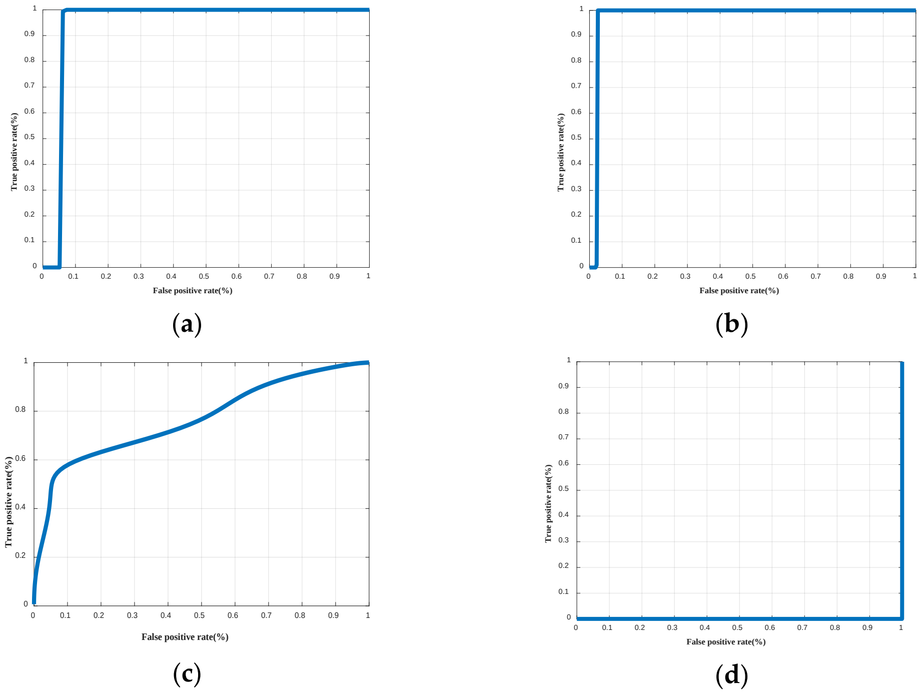


Figure 10. Correlation scores for unauthorised imposter patterns (for ORL dataset) for (**a**) CFR1, (**b**) CFR2, (**c**) homomorphic transform followed by salting and (**d**) homomorphic transform followed by random kernel convolution.

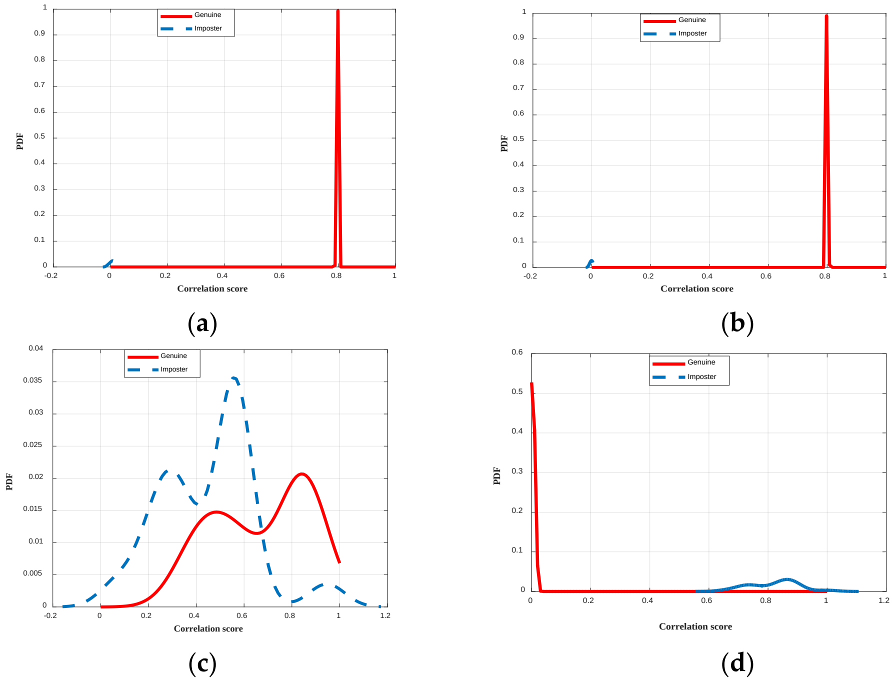
Structural Similarity Index Metric (SSIM) is a widely used tool that measures congruity between two images. In this study, the SSIM is utilised as a metric for encryption strength. A good encryption scheme should have SSIM values (between original and encrypted images) close to zero. Mathematically, we adopt the definition of SSIM in (17) [28] for assessment of encryption strength.



(**a**) (**b**)

(**c**) (**d**)

Figure 11. Receiver operating characteristic (ROC) curves for cancellable face recognition frameworks (for ORL dataset) for (**a**) CFR1, (**b**) CFR2, (**c**) homomorphic transform followed by salting and (**d**) homomorphic transform followed by random kernel convolution.



(**a**) (**b**)

(**c**) (**d**)

Figure 12. Probability distributions for cancellable face recognition frameworks (for ORL dataset) for (**a**) CFR1, (**b**) CFR2, (**c**) homomorphic transform followed by salting and (**d**) homomorphic transform followed by random kernel convolution.

$$SSIM = \frac{(2\mu_x\mu_y + S_1)(2\delta_{xy} \ + S_2)}{(\mu_x^2 \ + \mu_y^2 \ + S_1) + (\delta_x^2 \ + \delta_y^2 \ + S_2)} \tag{17}$$

where μ_x and μ_y are the mean values of the images x and y, respectively, δ_x^2 , and δ_y^2 are their variances, δ_{xy} is the cross-covariance between them, S_1 and S_2 are small values [10], and the value of SSIM is ideally less than 1.

Table 1 summaries the evaluation metrics of the proposed cancellable biometric frameworks. The area under the receiver operating characteristic (AROC) values, SSIM values between stored templates in the database and an imposter template as well as mean values of authorised and unauthorised correlation distributions are presented as metrics to establish the utility of the proposed scheme. The results indicate that both proposed CFR frameworks exhibit high encryption strength, while also retaining the ability to distinguish between authorised and unauthorised templates. The high AROC values of 0.9774 and 0.9720 and the corresponding low SSIM values of 0.058 and 0.0086 affirm the strength of the proposed frameworks (these are highlighted in bold in Table 1).

Table 1. Evaluation of CFR frameworks based on ORL dataset.

Method	AROC	SSIM	Mean of Authorised Correlation Score	Mean of Unauthorised Correlation Score
CFR1	**0.9720**	0.0086	0.7935	−0.0014
CFR2	**0.9774**	0.0580	0.7980	0.00000035
Homomorphic transform followed by salting	0.6600	0.9988	0.6705	0.5895
Homomorphic transform followed by random kernel convolution	0.00004	1.000	0.0021	0.8213

At this juncture, it is noteworthy that the ORL dataset whose results were reported above lacks the verity expected in actual application settings. Further, it is classified into a small database and has less variation. Consequently, to enrich the validation of our proposed CFR schemes, we consider the FERET [26] and LFW [27] datasets, which, in addition to all the properties of images in the ORL dataset, are taken with varying backgrounds and lighting as well as motion typical of actual application environments. However, both the FERET and LFW datasets consist of colour images; therefore, as a preprocessing stage, a transformation operation defined in (18) is used to generate greyscale versions of images in both datasets.

$$G = 0.3R + 0.59G + 0.11B \tag{18}$$

where R, G, and B are the colour components of the facial images.

Figures 13 and 14 present sample images from the FERET and LFW datasets, respectively. Furthermore, Figures 15–21 present simulation results implementing our two schemes (i.e., CFR1 and CFR2 in (a) and (b)) as well as homomorphic transform followed by salting (in (c)) and homomorphic transform followed by random kernel convolution (in (d)) for greyscale images from the FERET dataset.

Figure 13. Sample of greyscale facial images from Face Recognition Technology (FERET) database [26] used as original biometrics.

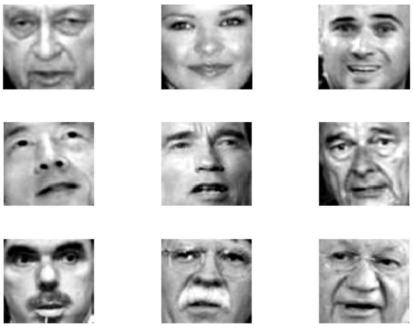


Figure 14. Sample of greyscale facial images from Labelled Faces in the Wild (LFW) database [27] used as original biometrics.

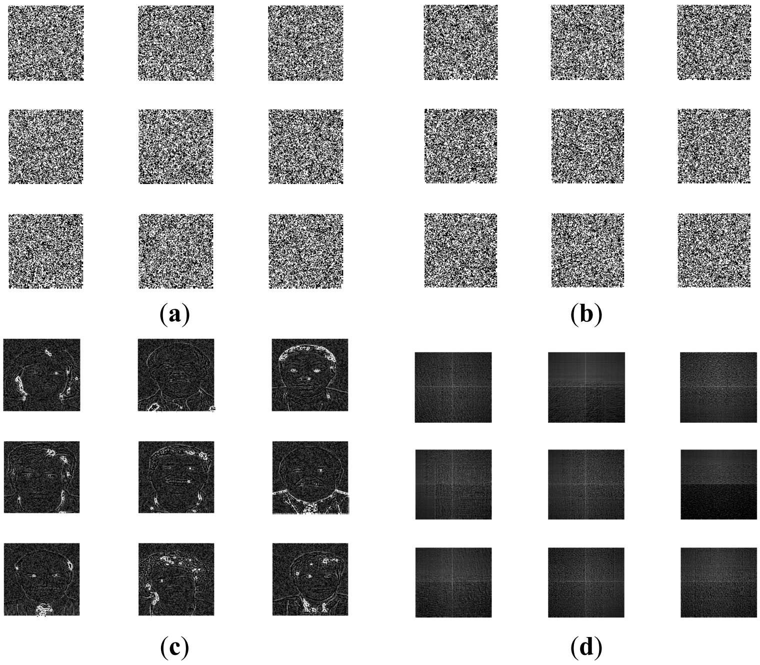


Figure 15. Encrypted versions of biometric faces in Figure 13 (i.e., from FERET dataset) for (**a**) CFR1 (**b**) CFR2, (**c**) homomorphic transform followed by salting and (**d**) homomorphic transform followed by random kernel convolution.

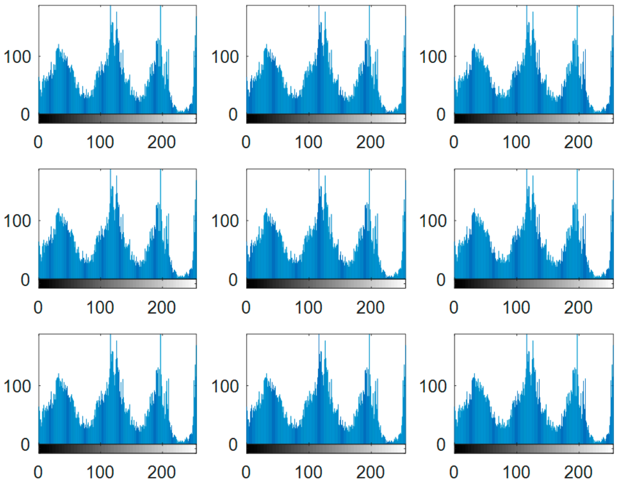
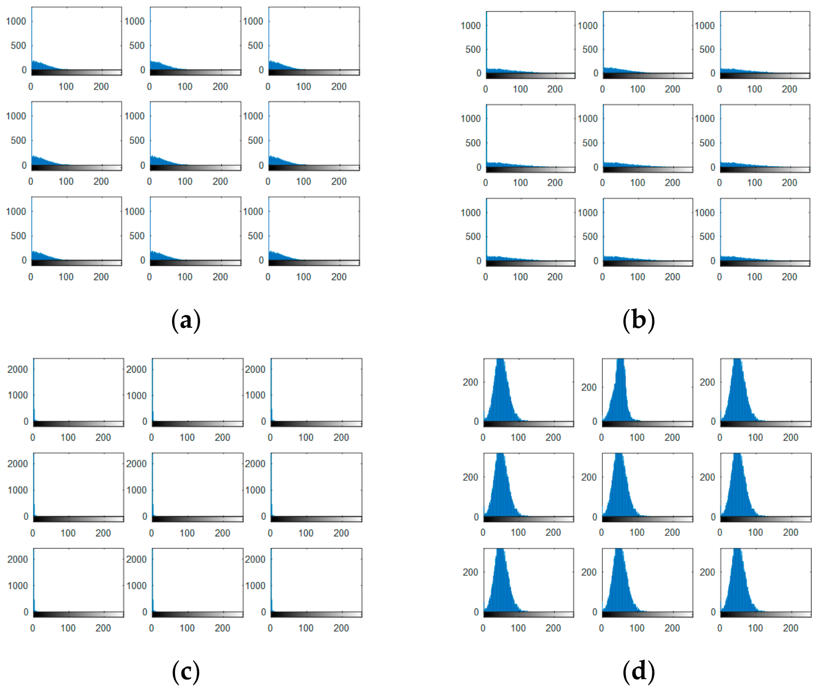


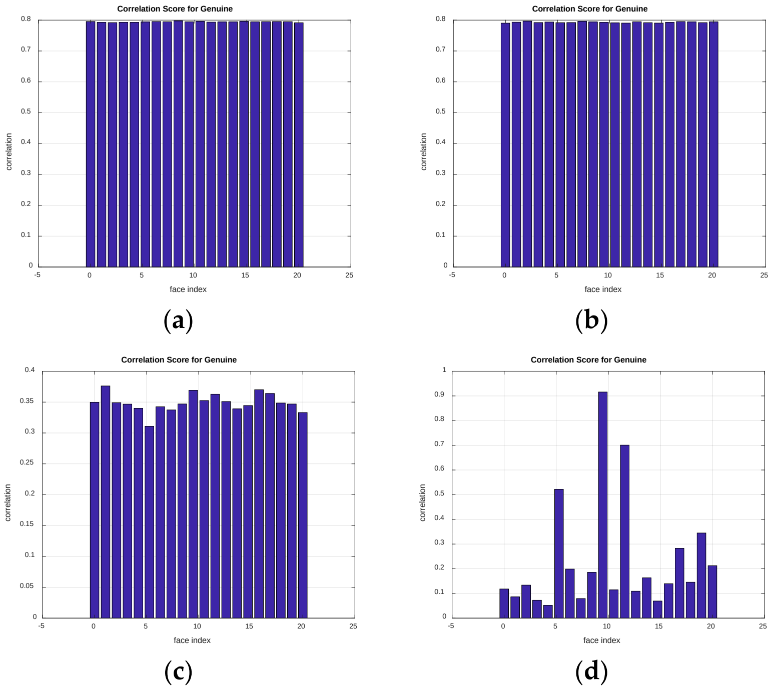
Figure 16. Histograms of the sample facial images in Figure 13.



(**a**) (**b**)

(**c**) (**d**)

Figure 17. Histograms of encrypted images based on combinations in Figure 15, i.e., (**a**) CFR1, (**b**) CFR2, (**c**) homomorphic transform followed by salting and (**d**) homomorphic transform followed by random kernel convolution.



(**a**) (**b**)

(**c**) (**d**)

Figure 18. Correlation scores for unauthorised imposter patterns (for FERET dataset) for (**a**) CFR1, (**b**) CFR2, (**c**) homomorphic transform followed by salting and (**d**) homomorphic transform followed by random kernel convolution.

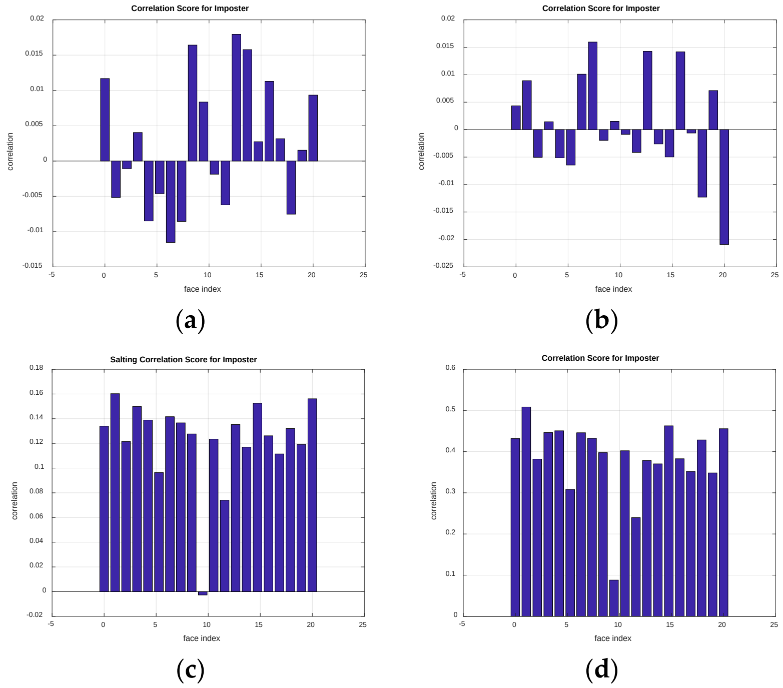


Figure 19. Correlation scores for unauthorised imposter patterns (for FERET dataset) for (**a**) CFR1, (**b**) CFR2, (**c**) homomorphic transform followed by salting and (**d**) homomorphic transform followed by random kernel convolution.

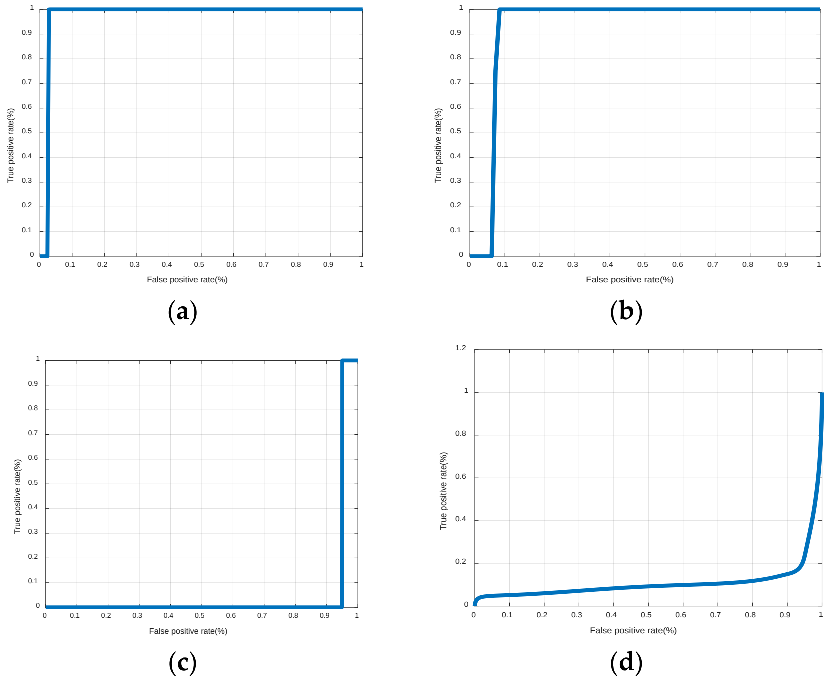


Figure 20. ROC curves for cancellable face recognition frameworks (for FERET dataset) for (**a**) CFR1, (**b**) CFR2, (**c**) homomorphic transform followed by salting and (**d**) homomorphic transform followed by random kernel convolution.

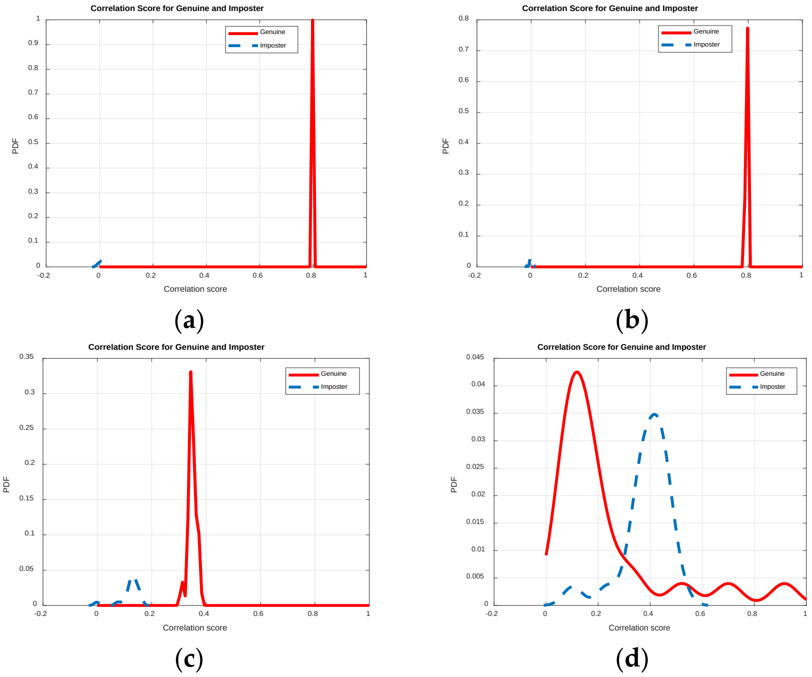


Figure 21. Probability distributions for cancellable face recognition frameworks (for FERET dataset) for (**a**) CFR1, (**b**) CFR2, (**c**) homomorphic transform followed by salting and (**d**) homomorphic transform followed by random kernel convolution.

Likewise, Figures 22–28 present similar results for greyscale sample images from the LFW dataset.

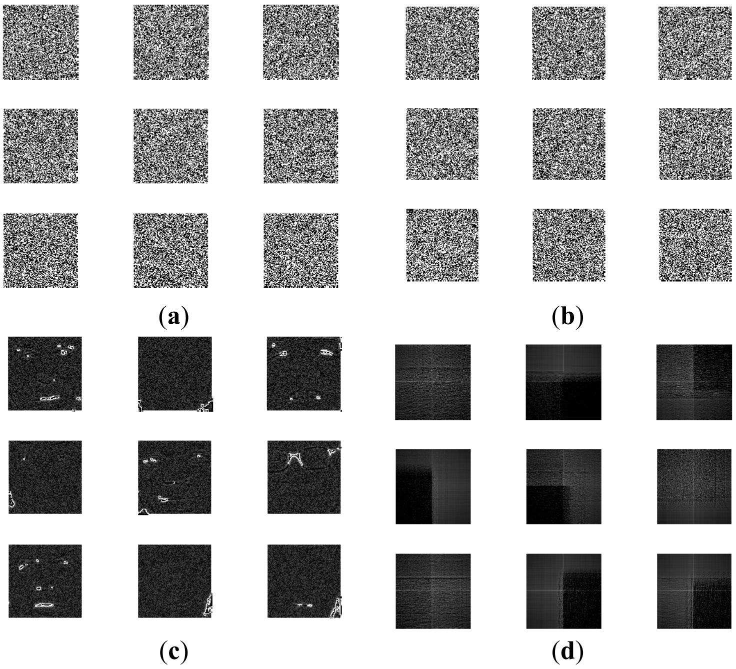


Figure 22. Encrypted versions of biometric faces in Figure 14 (i.e., from LFW dataset) for (**a**) CFR1 (**b**) CFR2, (**c**) homomorphic transform followed by salting and (**d**) homomorphic transform followed by random kernel convolution.

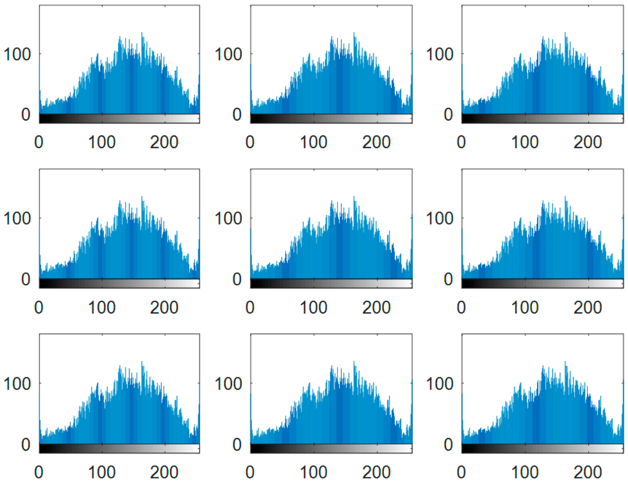
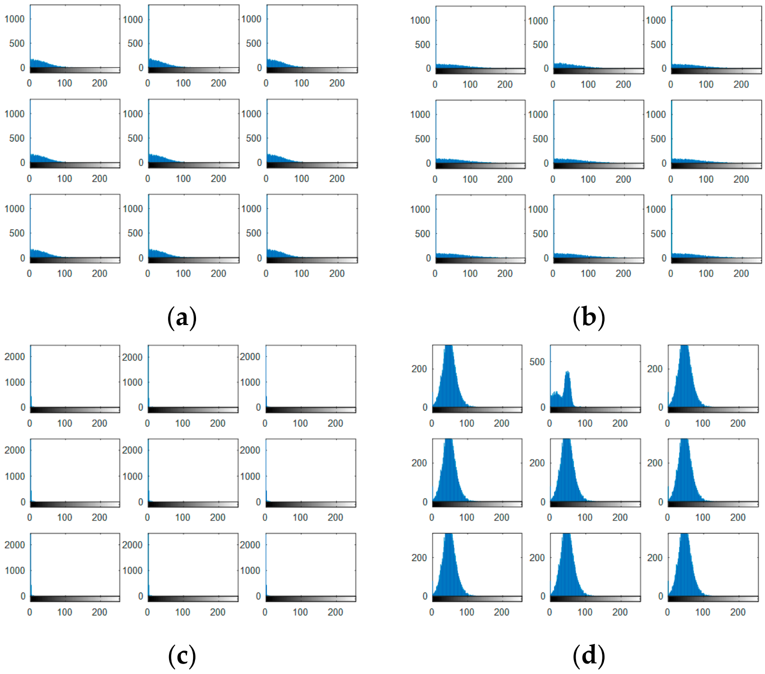
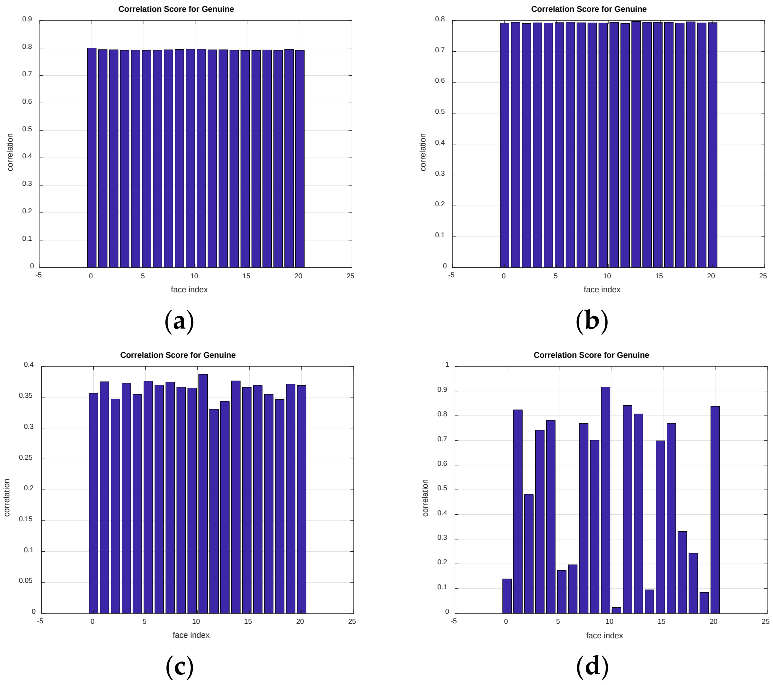


Figure 23. Histograms of the sample facial images in Figure 14.



(**a**) (**b**) (**c**) (**d**)

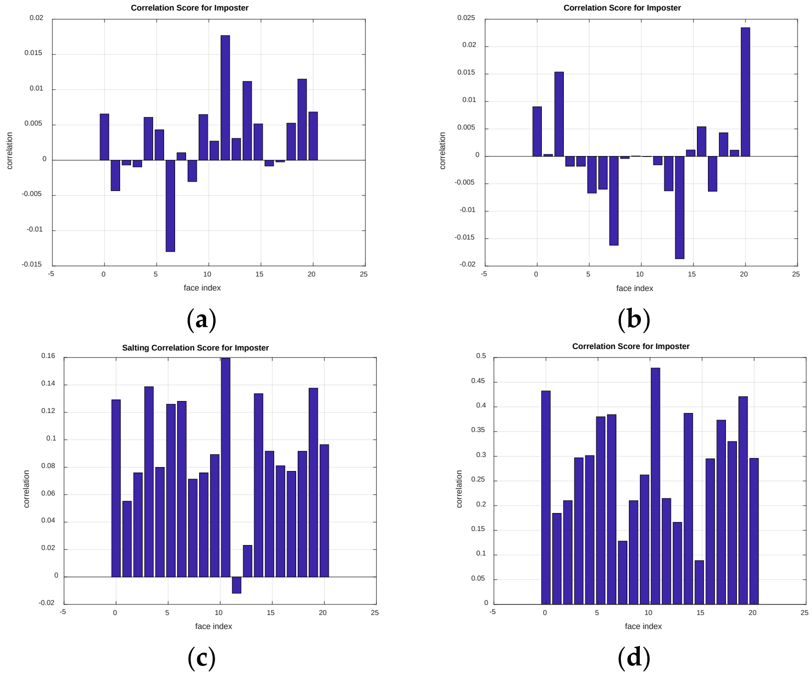
Figure 24. Histograms of encrypted images based on combinations in Figure 22, i.e., (**a**) CFR1, (**b**) CFR2, (**c**) homomorphic transform followed by salting and (**d**) homomorphic transform followed by random kernel convolution.



(**a**) (**b**)

(**c**) (**d**)

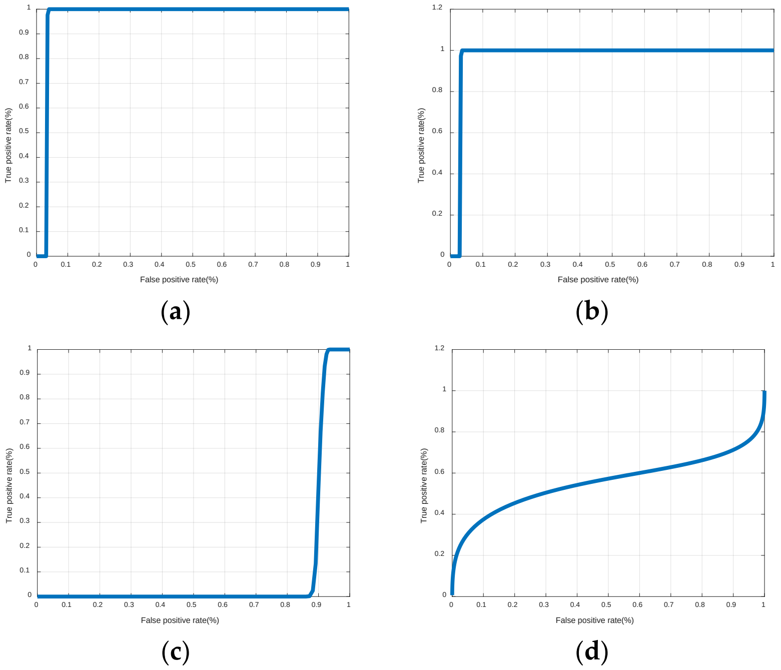
Figure 25. Correlation scores for unauthorised imposter patterns (for LFW dataset) for (**a**) CFR1, (**b**) CFR2, (**c**) homomorphic transform followed by salting and (**d**) homomorphic transform followed by random kernel convolution.



(**a**) (**b**)

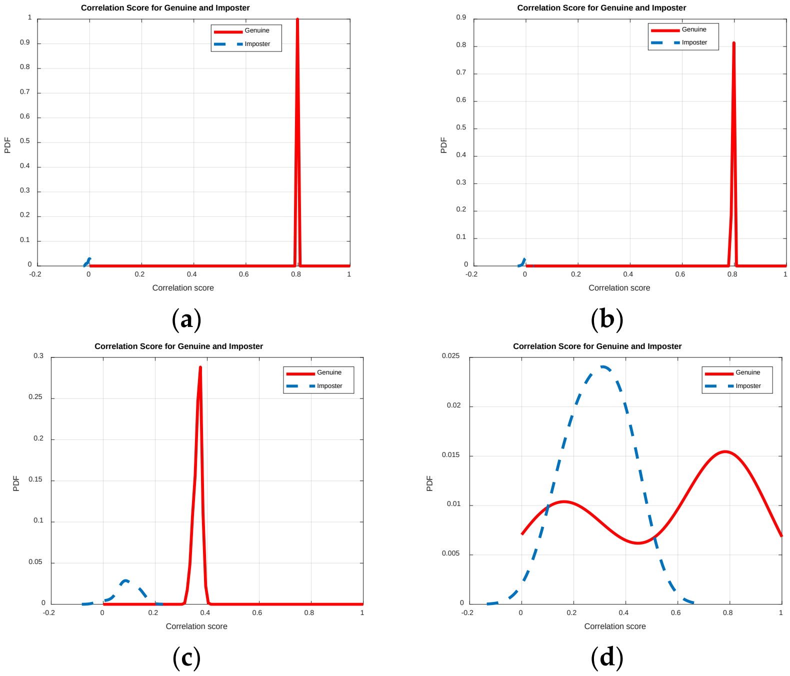
(**c**) (**d**)

Figure 26. Correlation scores for unauthorised imposter patterns (for FERET dataset) for (**a**) CFR1, (**b**) CFR2, (**c**) homomorphic transform followed by salting and (**d**) homomorphic transform followed by random kernel convolution.



(**a**) (**b**) (**c**) (**d**)

Figure 27. ROC curves for cancellable face recognition frameworks (for LFW dataset) for (**a**) CFR1, (**b**) CFR2, (**c**) homomorphic transform followed by salting and (**d**) homomorphic transform followed by random kernel convolution.



(**a**) (**b**) (**c**) (**d**)

Figure 28. Probability distributions for cancellable face recognition frameworks (for LFW dataset) for (**a**) CFR1, (**b**) CFR2, (**c**) homomorphic transform followed by salting and (**d**) homomorphic transform followed by random kernel convolution.

Tables 2 and 3 present summaries of the performance indices in terms of SSIM, AROC as well as mean values of authorised and unauthorised correlation distributions for images in the FERET and LFW datasets, respectively with the best AROC results highlighted in bold.

Table 2. Evaluation of CFR frameworks based on FERET dataset (where bold entries indicate best AROC results recorded).

Framework	AROC	SSIM	Mean of Authorised Correlation Distribution	Mean of Unauthorised Correlation Distribution
CFR1	**0.9744**	0.0108	0.7944	0.0024
CFR2	**0.9294**	0.0019	0.7930	6.4323×10^{-4}
Homomorphic transform followed by salting	0.0501	0.9710	0.3491	0.1226
Homomorphic transform followed by random kernel convolution	0.1092	0.2298	0.2323	0.3862

Table 3. Evaluation of CFR frameworks based on LFW dataset (where bold entries indicate best AROC results recorded).

Framework	AROC	SSIM	Mean of Authorised Correlation Distribution	Mean of Unauthorised Correlation Distribution
CFR1	**0.9668**	0.0058	0.7936	0.0032
CFR2	**0.9694**	0.0029	0.7934	2.7577×10^{-4}
Homomorphic transform followed by salting	0.0977	0.9727	0.3635	0.0925
Homomorphic transform followed by random kernel convolution	0.5569	0.2582	0.5225	0.2920

Finally, Table 4 presents a summary of the performance of our CFR schemes, i.e., CFR1 (i.e., IFL followed by Gaussian random projection) and CFR2 (i.e., Homomorphic transform followed by Gaussian random projection) for images in the three datasets (i.e., ORL, FERET and LFW) alongside results reported for similar techniques.

Table 4. Comparison of AROC between proposed schemes and state-of-the-art cancellable schemes.

Method (Dataset)	AROC
CFR1 (ORL)	**0.9720**
CFR2 (ORL)	**0.9774**
CFR1 (FERET)	**0.9744**
CFR2 (FERET)	0.9294
CFR1 (LFW)	**0.9668**
CFR2 (LFW)	0.9694
FERFT only [29,30]	0.8837
Jigsaw only [31]	0.8967
[32]	0.9076
[33]	0.8737
[34]	0.7187
[35]	0.8630
[29]	0.8684

As seen from the table, AROC values for our cancellable schemes vary between 0.9668 to 0.9744 for CFR1 and 0.9294 to 0.9774 for CFR2 (with best results for CFR1 (ORL), CFR2 (ORL), CFR1 (FERET), and CFR1 (LFW) highlighted in bold in Table 4). Relative to the similar studies reported in the table, AROC values for our two CFR schemes outperform those in [29–35].

4.2. Execution Time and Complexity Analysis

The average execution times required for the implementation of both CFR frameworks are recorded in Table 5. These temporal requirements are considered acceptable since the process of generating cancellable templates is undertaken off-line. In addition to execution time tests, we also undertook a complexity analysis, where, for uniformity and level playing ground [35], the analysis is introduced in terms of CPU operations required to execute the different frameworks. Therefore, we estimate the running time for each step in the process of recognition required for each user. The steps performed for every user are enumerated as follows:

1. ($O(1)$) to register its current face;
2. ($O(n \times (M \times N))$) to retrieve the function (IF) and perform distortion number 1 using the intuitionistic fuzzy transformation;
3. ($O(n \times (M \times N))$) to retrieve the function (RP) and perform the second distortion number 2 using random projection;
4. ($O(M \times N)$) to apply random noise on the final distorted template;
5. ($O(M \times N)$) to compute the correlation coefficient between the distorted template of the current user with the dataset stored in the database, which was distorted via the same sequence;
6. ($O(n \times (M \times N))$) based on the value of correlation coefficient required to execute the authentication process producing an outcome accept or reject.

Table 5. Comparison of execution time (in seconds).

Method	Time (s)
CFR1	13.14
CFR2	12.19

Therefore, adding it all up, the complexity of the algorithm proposed to execute the recognition procedure is $O(max(n, (n \times (M \times N)))$ which compares with those reported in similar studies [27–34], as summarised in Table 6.

Table 6. Comparison of computational complexity between the proposed approach and other approaches.

Method	Complexity
Proposed	$O(max(n, (n \times (M \times N)))$
[31]	$O(n)$
[32]	$O(n)$

5. Conclusions

The study presented two revocable and non-invertible cancellable face recognition (CFR) frameworks that have potential applications in enhancing security in banking, airports, and other important sectors by safeguarding identity and data of authorised users and customers. Both frameworks share the Gaussian random projection stage for encryption, which is preceded by a pre-processing phase to extract an uninvertible signature from each biometric. Such non-invertible signatures secure the biometric templates even if the random projection process is inverted. Moreover, both the intuitionistic fuzzy and homomorphic transforms used provide a first level security that is further strengthened using random projections. Furthermore, the proposed frameworks satisfy the JL lemma, which guarantees a large distance between encrypted templates in the random space. This guarantees a high level of accuracy in the verification process of both CFR frameworks. The two schemes are validated using three datasets that exhibit properties expected in real-life scenarios, such as varying backgrounds, lightings, motion, etc. Outcomes based on standard metrics support claims that the proposed schemes would enhance many applications that require person identification, authentication, and verification. Efforts to improve outcomes from our study are being pursued along two directions. First, in ongoing work, the study is being refined via integration of new recognition and encryption approaches that will be validated using larger and more robust datasets. Second, in future work, inputs from real-time cameras where dynamic images will be used evaluate the proposed CFR frameworks for deployment across multiple application scenarios.

Author Contributions: Conceptualisation, A.D.A., G.M.E.B. and N.F.S.; methodology, A.D.A., F.E.A.E.-S. and A.M.I.; software, A.D.A. and N.F.S.; validation, A.D.A., G.M.E.B. and F.E.A.E.-S.; formal analysis, G.M.E.B., N.F.S. and F.E.A.E.-S.; investigation, A.D.A., G.M.E.B., and F.E.A.E.-S.; resources, A.D.A., N.F.S., and A.M.I.; data curation, G.M.E.B. and N.F.S.; writing—original draft preparation, A.D.A., N.F.S., F.E.A.E.-S. and A.M.I.; writing—review and editing, A.D.A., G.M.E.B. and A.M.I.; visualisation, G.M.E.B. and F.E.A.E.-S.; supervision, A.D.A. and A.M.I.; project administration, A.D.A. and A.M.I.; funding acquisition, A.D.A. and A.M.I. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Deanship of Scientific Research at Princess Nourah bint Abdulrahman University (Grant No. 39/S/249).

Acknowledgments: The authors would like to thank the support of Deanship of Scientific Research at Princess Nourah bint Abdulrahman University.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. El-Latif, A.A.; Hossain, M.S.; Wang, N. Score level multibiometrics fusion approach for healthcare. *Clust. Comput.* **2017**, *22*, 2425–2436. [CrossRef]
2. Gad, R.; Talha, M.; El-Latif, A.A.; Zorkany, M.; El-Sayed, A.; El-Fishawy, N.; Muhammade, G.; Talha, M. Iris Recognition Using Multi-Algorithmic Approaches for Cognitive Internet of things (CIoT) Framework. *Future Gener. Comput. Syst.* **2018**, *89*, 178–191. [CrossRef]
3. Soliman, R.F.; El Banby, G.M.; Algarni, A.D.; Elsheikh, M.; Soliman, N.F.; Amin, M.; El-Samie, F.E.A. Double random phase encoding for cancelable face and iris recognition. *Appl. Opt.* **2018**, *57*, 10305–10316. [CrossRef] [PubMed]
4. Savvides, M.; Kumar, B.V.K.V.; Khosla, P. Cancelable biometric filters for face recognition. In Proceedings of the 17th International Conference on Pattern Recognition, Cambridge, UK, 26 August 2004; Volume 3, pp. 922–925.
5. Kaur, H.; Khanna, P. Cancelable features using log-Gabor filters for biometric authentication. *Multimed. Tools Appl.* **2016**, *76*, 4673–4694. [CrossRef]
6. Maiorana, E.; Campisi, P.; Neri, A. Bioconvolving: Cancelable templates for a multi-biometrics signature recognition system. In Proceedings of the 2011 IEEE International Systems Conference, Montreal, QC, Canada, 3–6 April 2011; pp. 495–500.
7. Butt, M.; Damer, N. Helper Data Scheme for 2D Cancelable Face Recognition using Bloom Filters. In Proceedings of the International Conference on Systems, Signals and Image Processing (IWSSIP), Dubrovnik, Croatia, 12–15 May 2014; pp. 271–274.
8. Teoh, A.B.J.; Kuan, Y.W.; Lee, S. Cancellable biometrics and annotations on BioHash. *Pattern Recognit.* **2008**, *41*, 2034–2044. [CrossRef]
9. Kaur, H.; Khanna, P. Gaussian Random Projection Based Non-invertible Cancelable Biometric Templates. *Procedia Comput. Sci.* **2015**, *54*, 661–670. [CrossRef]
10. Wang, Z.; Simoncelli, E.P.; Bovik, A.C. Multiscale structural similarity for image quality assessment. In Proceedings of the Thirty-Seventh Asilomar Conference on Signals, Systems & Computers, Pacific Grove, CA, USA, 9–12 November 2003; pp. 1398–1402. [CrossRef]
11. Atanassov, K.T. Intuitionistic fuzzy sets. *Fuzzy Sets Syst.* **1986**, *20*, 87–96. [CrossRef]
12. Ejegwa, P.A.; Akowe, S.O.; Otene, P.M.; Ikyule, J.M. An overview on intuitionistic fuzzy sets. *Int. J. Sci. Technol. Res.* **2014**, *3*, 142–145.
13. Verma, H.; Gupta, A.; Kumar, D. A modified intuitionistic fuzzy c-means algorithm incorporating hesitation degree. *Pattern Recognit. Lett.* **2019**, *122*, 45–52. [CrossRef]
14. Akram, M.; Dudek, W.A. Intuitionistic fuzzy hypergraphs with applications. *Inf. Sci.* **2013**, *218*, 182–193. [CrossRef]
15. Kaushik, R.; Bajaj, R.K.; Kumar, T. On Intuitionistic Fuzzy Divergence Measure with Application to Edge Detection. *Procedia Comput. Sci.* **2015**, *70*, 2–8. [CrossRef]

16. Vlachos, I.K.; Sergiadis, G.D. The Role of Entropy in Intuitionistic Fuzzy Contrast Enhancement. In Proceedings of the International Fuzzy Systems Association World Congress, Cancun, Mexico, 18–21 June 2007.
17. Chaira, T. *Medical Image Processing: Advanced Fuzzy Set Theoretic Techniques*; CRC Press: Boca Raton, FL, USA, 2015.
18. Matoušek, J. On variants of the Johnson-Lindenstrauss lemma. *Random Struct. Algorithms* **2008**, *33*, 142–156. [CrossRef]
19. Wang, N.; Li, Q.; El-Latif, A.A.; Peng, J.; Niu, X. An enhanced thermal face recognition method based on multiscale complex fusion for Gabor coefficients. *Multimed. Tools Appl.* **2013**, *72*, 2339–2358. [CrossRef]
20. Ashiba, H.I.; Mansour, H.M.; Ahmed, H.M.; Dessouky, M.I.; El-Kordy, M.F.; Zahran, O.; El-Samie, F.E.A. Enhancement of IR images using histogram processing and the Undecimated additive wavelet transform. *Multimed. Tools Appl.* **2018**, *78*, 11277–11290. [CrossRef]
21. Pillai, J.K.; Patel, V.M.; Chellappa, R.; Ratha, N.K. Secure and Robust Iris Recognition Using Random Projections and Sparse Representations. *IEEE Trans. Pattern Anal. Mach. Intell.* **2011**, *33*, 1877–1893. [CrossRef] [PubMed]
22. Patel, V.M.; Ratha, N.K.; Chellappa, R. Cancelable Biometrics: A review. *IEEE Signal Process. Mag.* **2015**, *32*, 54–65. [CrossRef]
23. Handmandlu, M.; Jha, D.; Sharma, R. Color image enhancement using fuzzy intensification. *Pattern Recognit. Lett.* **2004**, *24*, 81–87.
24. Benrhouma, O.; Hermassi, H.; El-Latif, A.A.; Belghith, S. Chaotic watermark for blind forgery detection in images. *Multimed. Tools Appl.* **2015**, *75*, 8695–8718. [CrossRef]
25. ORL Database. Available online: https://www.cl.cam.ac.uk/research/dtg/attarchive/facedatabase.html (accessed on 1 June 2020).
26. FERET Database. Available online: https://www.nist.gov/itl/products-and-services/color-feret-database (accessed on 1 June 2020).
27. LFW Database. Available online: http://vis-www.cs.umass.edu/lfw/ (accessed on 1 June 2020).
28. Wang, Z.; Bovik, A.C.; Sheikh, H.R.; Simoncelli, E.P. Image Quality Assessment: From Error Visibility to Structural Similarity. *IEEE Trans. Image Process.* **2004**, *13*, 600–612. [CrossRef]
29. Réfrégier, P.; Javidi, B. Optical image encryption based on input plane and Fourier plane random encoding. *Opt. Lett.* **1995**, *20*, 767. [CrossRef]
30. Sinha, A.; Singh, K. Image encryption by using fractional Fourier transform and jigsaw transform in image bit planes. *Opt. Eng.* **2005**, *44*, 057001. [CrossRef]
31. Kumar, P.; Joseph, J.; Singh, K. Optical image encryption using a jigsaw transform for silhouette removal in interference-based methods and decryption with a single spatial light modulator. *Appl. Opt.* **2011**, *50*, 1805–1811. [CrossRef] [PubMed]
32. Ben Tarif, E.; Wibowo, S.; Wasimi, S.; Tareef, A. A hybrid encryption/hiding method for secure transmission of biometric data in multimodal authentication system. *Multimed. Tools Appl.* **2017**, *77*, 2485–2503. [CrossRef]
33. Sree, S.R.S.; Radha, N. Cancellable multimodal biometric user authentication system with fuzzy vault. In Proceedings of the 2016 International Conference on Computer Communication and Informatics (ICCCI), Coilmbatore, India, 7–9 January 2016; pp. 1–6.
34. Dang, T.K.; Truong, Q.C.; Le, T.T.B.; Truong, H. Cancellable fuzzy vault with periodic transformation for biometric template protection. *IET Biom.* **2016**, *5*, 229–235. [CrossRef]
35. Soliman, R.F.; Amin, M.; El-Samie, F.E.A. A Modified Cancelable Biometrics Scheme Using Random Projection. *Ann. Data Sci.* **2018**, *6*, 223–236. [CrossRef]