symmetry

MDPI

Article

A Cancelable Biometric System Based on Deep Style Transfer and Symmetry Check for Double-Phase User Authentication

Ahmed Sedik [1,2,*], Ahmed A. Abd El-Latif [3,4], Mohammed El-Affendi [3] and Hala Mostafa [5,*]

[1] Smart Systems Engineering Laboratory, College of Engineering, Prince Sultan University, Riyadh 11586, Saudi Arabia
[2] Department of the Robotics and Intelligent Machines, Kafrelsheikh University, Kafrelsheikh 33511, Egypt
[3] EIAS Data Science Lab, College of Computer and Information Sciences, Prince Sultan University, Riyadh 11586, Saudi Arabia
[4] Department of Mathematics and Computer Science, Faculty of Science, Menoufia University, Shebeen El-Kom 32511, Egypt
[5] Department of Information Technology, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia
* Correspondence: asedik@psu.edu.sa (A.S.); hfmostafa@pnu.edu.sa (H.M.)

Abstract: In recent times, there has been a noticeable increase in the application of human biometrics for user authentication in various domains, such as online banking. However, the use of biometric systems poses security risks and the potential for misuse, primarily due to the storage of original templates in databases. To tackle this issue, the concept of cancelable biometrics has emerged as a reliable method utilizing one-way encryption. Several algorithms have been developed to implement cancelable biometrics, incorporating visual representations of single or multiple biometrics. This research proposes a cancelable biometric system that utilizes deep learning techniques to generate two encrypted modalities, namely text and image, using facial and fingerprint biometrics acquired from a smartphone. The system consists of two main stages: a visual encoder and a text encoder. The visual encoder converts the fingerprint style into a facial representation, creating a cancelable template to ensure the potential for cancelation. The resulting visual template is then processed by the text encoder, which employs hashing techniques to generate a corresponding text template. User authentication is automatically verified by utilizing the generated templates through Siamese networks.

Keywords: cybersecurity; cancelable biometrics; user authentication; deep learning; similarity check; biometric recognition

Citation: Sedik, A.; El-Latif, A.A.A.; El-Affendi, M.; Mostafa, H. A Cancelable Biometric System Based on Deep Style Transfer and Symmetry Check for Double-Phase User Authentication. *Symmetry* **2023**, *15*, 1426. https://doi.org/10.3390/sym15071426

Academic Editor: Ki-Hyun Jung

Received: 1 June 2023
Revised: 2 July 2023
Accepted: 11 July 2023
Published: 15 July 2023

1. Introduction

1.1. Background Study

In the realm of recognition and identification methodologies, conventional approaches rely on the utilization of passwords, identification (ID) cards, or possession tokens as a means of granting access to systems. The underlying assumption is that an authorized user consistently maintains possession of a unique personal information number (PIN), cryptographic key, or password to facilitate authentication. Nevertheless, in practical terms, the efficacy of these systems in accurately providing the required PIN or password for authentication may be called into question.

With the advances in multimedia applications, biometric system technology has also been employed in our daily life and expanded precipitously. Because of many biometric features, it is essential to safeguard the biometrics confidentiality and manage access. The technology of the biometric system verifies and identifies personal characteristics in a fast, accurate, and expedient manner to manage the process of access to certain applications or systems [1]. The biometrics are considered the unique physical (fingerprints, hand

engineering, iris scan, retina, face position or recognition) or logical (keystroke pattern, voice recognition, walking, and signature) measured traits or features of a human body that are exploited to guarantee that only legal users have access to the offered applications [2]. In traditional systems, passwords are used to guarantee the cryptographic key privacy for a certain service. Sometimes, the same password is utilized by many persons through several applications and never adjusted to avert the difficulty of utilizing long, dissimilar passwords for various applications. Consequently, there is a probability of a violation of privacy for numerous applications due to the utilization of a single password that may be easily compromised [3].

Over the years, authentication procedures like passwords and PINs have been employed in security systems. Lately, for improved safety and privacy, the magnetic card has been utilized [4]. These conventional procedures of the security of information system come with the following disadvantages [5]: (1) They can realize some of the characters of a certain person instead of recognizing the actual person that produced these characters; (2) they can be lost, forgotten, or stolen; (3) they can be easily hacked or bypassed; and (4) they are not accurate. Therefore, a biometric recognition system that is adopted on the statistical evaluation of behavioral and physiological attributes of an individual is considered as a substitutional mechanism to achieve the recognition of persons. The biometric parameters that can be exploited and used to build an authentication system based on biometric traits are the human face, iris, fingerprint, ear, signature, voice, and other distinguishing characteristics. These biometrics are characterized by uniqueness for everyone. Hence, they are more efficient in authenticating one's identity than other authentication mechanisms based on knowledge-based procedures and token methods.

On the other hand, the databases used to store biometric traits are insecure, as these databases may be attacked by any hacker. If the database is compromised, this will result in a serious perpetual identity loss, as the utilized biological attributes are irreplaceable and irrevocable. Consequently, the biometric authentication systems need an effective solution for this specific harmful case [6]. A cancelable biometrics approach is considered as a new trend toward more secure biometrics. In cases of security issues, biometrics can be distorted easily without any change to the whole system. Different template protection techniques to generate a cancelable biometric template have been introduced. These techniques can be applied to all biometric types. The cancelable approach that depends on the employment of multiple biometrics represents a promising approach for achieving more secure systems. These systems utilize two or more biometrics to develop the confidence level during the authentication phase. Cancelable transformations, e.g., salting techniques, noninvertible transformations, and biometric cryptosystems have been applied to safeguard the stored biometric data in cloud databases [7].

1.2. Motivation, Contribution, and Organization of This Paper

The preceding discussion highlights certain limitations in the development of reliable authentication methods. The main objective is to establish a unique encrypted template for each user that can be used to verify their access to a system or platform. However, the existing methods described in the available literature lack the required level of resilience to prevent attacks. Therefore, the purpose of this research is to introduce a cancelable template system that can generate a robust encrypted template, ensuring secure authentication while remaining immune to attacks.

The proposed approach involves combining various biometric features, such as face and fingerprint, into a single representation. Multiple encrypted forms are then generated, encompassing both visual and text formats. To accomplish this goal, deep learning and hashing techniques are employed in this study. The objectives of this research can be summarized as follows:

(1) To utilize convolutional neural networks (CNNs) for extracting facial image features.
(2) To utilize convolutional neural networks (CNNs) for extracting unique features from fingerprint images.

(3) To train a model capable of transferring features from fingerprint images to face images.
(4) To investigate a deep learning architecture that focuses on generating an encrypted template based on the obtained feature map.
(5) To explore a loss function for the proposed system that produces an optimal template.
(6) To employ hashing algorithms for generating a textual representation of the cancelable template.

The remainder of the paper is structured as follows. Recent associated cancelable biometrics research is reviewed in Section 2. Section 3 introduces the proposed deep learning-based cancelable biometric system. The simulation results as well as the comparative investigation are introduced in Section 4. The concluding remarks are given in Section 5.

2. Related Work

The design of cancelable biometric transforms makes the recovery of the original biometric data a computationally hard process [8,9]. Several studies have been presented to generate cancelable biometrics [10–13]. Ratha et al. [14] proposed a method for identification based on a cancelable geometric fingerprint framework. This framework provides recommended performance and efficiency while achieving a high level of cancelability. In [15], authors introduced an improved cancelable fingerprint identification algorithm dependent on exploiting the fuzzy spiral curves. Their algorithm introduced a 1.17% equal error rate (EER).

In [16], a palmprint identification scheme dependent on a lookup table and Gabor filters was introduced. This scheme proved its success in presenting a recommended recognition rate of up to 99.92%, achieving strong protection of palmprint templates from attackers. In [17], authors introduced an efficient cancelable iris identification method dependent on a joint methodology for noninvertible transformations and encryption. The method accomplished a high and reliable recognition rate of 99.9%.

In [18], authors introduced an appreciated cancelable iris identification method dependent on multiple levels of thresholding. Then, a random projection process was employed for generating the encrypted iris templates utilized for user authentication. This method presented an EER of 0.58% and a good accuracy value of 99.67%. In addition, the same authors in [19] presented another efficient method dependent on employing a hybrid of chaotic maps and Gabor filters. This method achieved a recommended EER of 1.17% with 99.08% accuracy. Moreover, the same authors in [20] introduced a cancelable multiple biometric iris identification scheme dependent on combining several biometric data patterns. So, in their proposed scheme, the feature vectors resulting from both the right and left iris of the same individual were merged into a specific encrypted iris code. Then, the FrFt-based double random phase encoding (DRPE) approach was employed. This approach attained an accuracy of 99.75% and an EER of 0.63%. In [21], authors introduced a fingerprint identification system utilizing linear zone-based binary patterns. In this system, each fingerprint template is split into nine equal zones, and in each zone, the linear patterns are utilized for the identification process. This system reached 94.28% average identification accuracy.

Kaur and Khanna [3] suggested an efficient cancelable biometric system based on Log-Gabor filters and a random projection technique to generate a cancelable feature vector to access the user account. A cancelable face biometric adopted on bloom filters was proposed by Butt et al. [22]. Their methodology is based on feature extraction from facial images to be used as an efficient tool to produce a new distorted and encrypted template. In the next step, a bloom filter is employed using the personal identification number to be convolved with the feature matrix. Teoh et al. [23] introduced a bio-hashing scheme for the face biometric, where the extracted low-dimension feature value is reprojected randomly to create a binary bit string. Kho et al. [24] proposed a cancelable fingerprint system using a partial local structure descriptor and permutated randomized nonnegative least square. They applied the permutation to the PRNNLS dictionary and random projection scheme.

Their approach successfully achieved cancelable templates that are uncorrelated with the original fingerprint templates.

3. Proposed Approach

The primary goal of the proposed method is to generate a biometric image with the least amount of correlation to the original biometric image. Based on the style transfer technique, this paper proposes a multi-biometric cancelable system. Style transfer is utilized in this paper to convert the features of an artwork image to a photograph. The artwork image is considered as a texture image, such as a fingerprint biometric, and the photo image is used as a face biometric. As a result, the proposed style transfer technique is used to transfer the texture style of the fingerprint to the biometric face image. There are many phases of collection and generation in the proposed cancelable system. Collecting the necessary biometric images is the first step for the user. Then, the second phase uses the style transfer approach to generate the cancelable biometric images. The collection of the required biometric images can be handled by access control devices, whereas the generation of the cancelable image is handled by a computer device that is best supported by a GPU to reduce processing time. The image retrieval of the cancelable image is the second state. The proposed method is unique in that it involves deep style transfer to the security field. The main benefit is that the resulting image is regarded as the cancelable biometric of both the input fingerprint and face biometric images. The resulting image of traditional cancelable systems, on the other hand, is the cancelable image of only one biometric image using a technique such as the DRPE encryption technique. Figure 1 depicts the general framework of the proposed cancelable system.

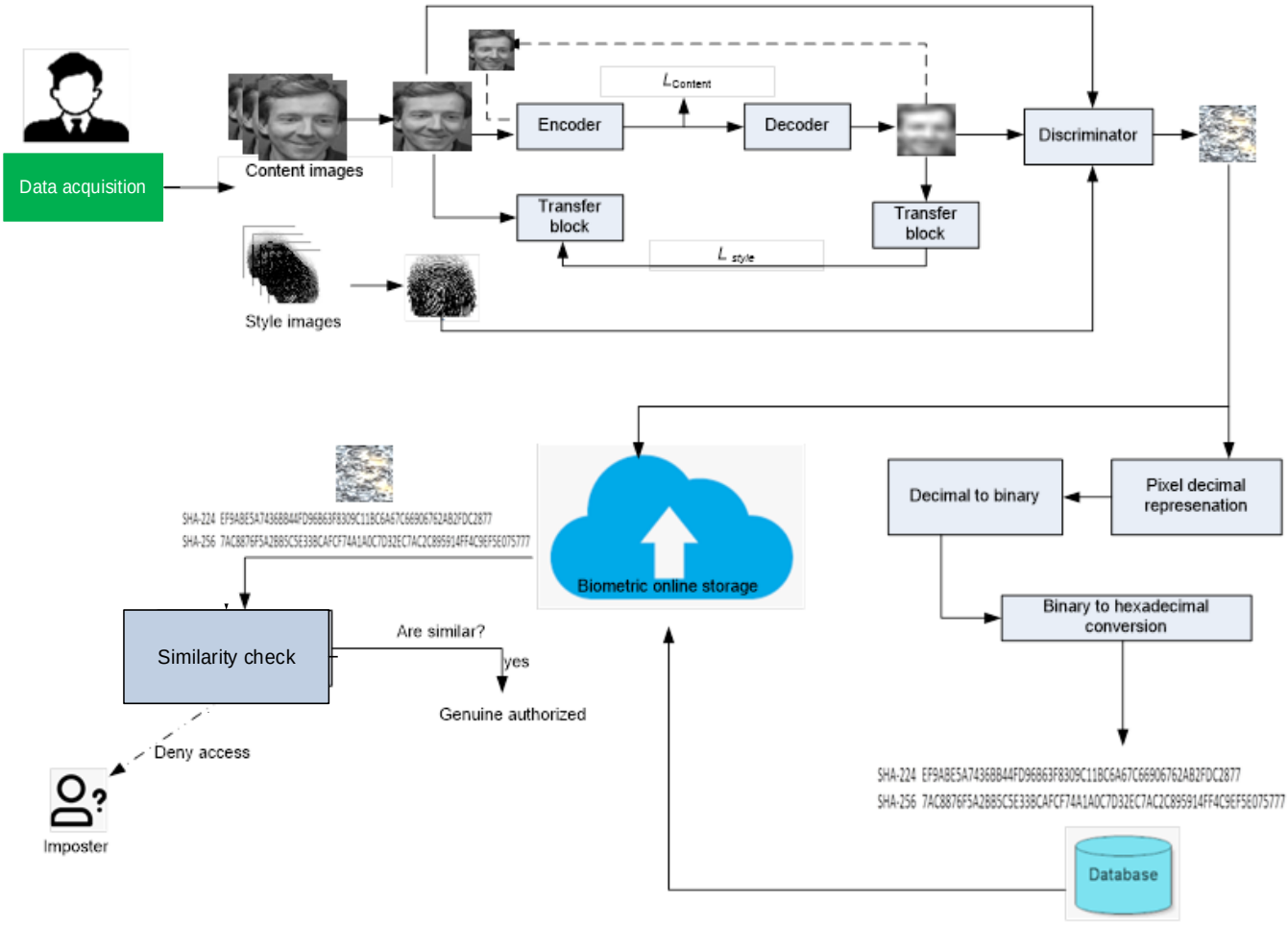


Figure 1. Block diagram of the proposed style transfer and bio-hash scheme.

As a result, a style transfer is used to create a photo that is like the artwork's style. The VGG network [25] is used to extract features from an image of artwork. This method has been selected for its efficiency in extracting features, as it is a widely used model in various applications. Furthermore, due to the limited availability of images for training, a pre-trained model was utilized for the feature extraction task. This feature extraction network model has been trained. This paper extracts features from the VGG-19 network model's normalized version of 16 convolutional layers and 5 pooling layers. To normalize the network, weights can be scaled. Scaling requires that the mean activation of each convolutional filter be equal to one. It is possible to rescale the VGG network without affecting its output. Because only linear activation functions (ReLU) are rectified, and feature maps are not pooled or normalized, this is the case. The proposed model lacks fully connected layers [26]. This model is applicable to anyone. In the proposed work, pooling averages rather than maximums is proposed to achieve slightly recommended and improved results. Furthermore, to ensure that the generated cancelable images cannot be reversed, they are hashed with SHA-256 and SHA-512. This is done to reduce the amount of storage required for biometrics.

3.1. Content Image Representation

The convolutional layer comes from several 2D digital filters, known as convolution filters. Features from the original biometric image are extracted and mapped using digital filters applied to the convolution of that data. The non-linear filter banks defined by each network layer are in general non-convex. As the number of layers in a network increases, the complexity of its filter bank also increases. Convolutional neural networks encode an input image $\widetilde{x}$ by responding to filters at successive layers. N_l feature maps can be created for a layer with N_l distinct filtering options. N_l, M_l is the height multiplied by the feature map width on each map of this sizing type. Responses in layer **l** can be represented in the matrix $F^l \in R^{N_l \times M_l}$, where F^l_{ij} indicates the activation of the ***ith*** filter in layer l at position j.

The value of the certain pixel p_{new} is calculated as:

$$p_{new} = \sum_{i \in s} p_i . w_i \tag{1}$$

where p_i is the summation of the old surrounding pixels and w_i is the applied filter elements.

To execute gradient descent on a white noise image, one can visualize the encoded information at different levels of the hierarchy. The goal is to create a new image with response features identical to the previously processed one. It is important to note that $\widetilde{p}$ and $\widetilde{x}$ are the original and the produced picture, respectively; the feature representations at the layer of layer l are P^l**.** Then, the squared error loss between P^l and F^l is given as follows.

$$\mathcal{L}_{\text{content}}\left(\widetilde{p}, \widetilde{x}, l\right) = \frac{1}{2}\sum_{i,j}\left(F^l_{ij} - P^l_{ij}\right)^2 \tag{2}$$

The derivative $L_{Content}\left(\widetilde{p}, \widetilde{x}, l\right)$ at layer l, in terms of activations, is given as follows.

$$\frac{\partial \mathcal{L}_{\text{content}}}{\partial F^l_{ij}} = \begin{cases} F^l_{ij} - P^l_{ij} & if \quad F^l_{ij} > 0 \\ 0 & if \quad F^l_{ij} < 0 \end{cases}, \tag{3}$$

Utilizing standard error back-propagation, it is possible to compute the gradient of the image $\widetilde{x}$ initial random image $\widetilde{x}$ modified until it generates the same response as the original image . When taught to recognize an item, convolutional neural networks (CNNs) build a representation of the data that becomes increasingly explicit as the processing level increases. $\widetilde{x}$ is translated into representations that are more and more accurate. On the other hand, it becomes largely unchanging with respect to its certain form. Higher layers of the network collect high-level material, but they do not have enough control over pixel values to ensure a precise reconstruction of the input image with respect to objects and their arrangement. Reconstructions from lower layers can be used to obtain the precise

pixel values of the image. Consequently, the content representation refers to the feature responses at the higher layers of the network.

3.2. Style Image Representation

A style representation for an input image can be provided by a feature space designed to capture texture information. This feature space can be built using filter responses at any network layer. It consists of the correlations between the various filter responses, where the expectation is considered over the geographic area of the feature maps. For example, in layer l of the Gram matrix, feature correlations between the inner product of the vectorized feature maps can be found, $\boldsymbol{G^l} \in \boldsymbol{R^{N_l \times M_l}}$.

$$G_{ij}^{l} = \sum_{k} F_{ik}^{l} F_{ik}^{l} \tag{4}$$

With the texture information in the input image, a stationary multi-scale representation of the image can be obtained, but not the overall layout of the image. It is possible to create an image with the same style representation as an input image using these style feature spaces created at various network levels and thus visualize the information acquired. Gradient descents from a white noise image can be used to reduce the mean squared distance between the image's original Gram matrices and the image's generated Gram matrices. Let a and x represent the original and generated images, respectively, and A^l. and, G^l. represent the style representations of those images at layer l. In terms of overall loss, layer $\boldsymbol{l}$ contributes:

$$E_l = \frac{1}{4N_l^2 M_l^2} \sum_{i,j} \left(G_{ij}^2 - A_{ij}^2 \right)^2 \tag{5}$$

And the total style loss function, $\mathcal{L}_{\text{style}}$, is defined as:

$$\mathcal{L}_{\text{style}}\left(\vec{a}, \vec{x}\right) = \sum_{l=0}^{L} \omega_l E_l \tag{6}$$

where $\boldsymbol{\omega_l}$ represents the set of weighting factors of each layer contribution to the total loss. The derivative of E_l at layer l, in terms of the activations, is given as:

$$\frac{\partial E_l}{\partial F_{ij}^l} = \begin{cases} \frac{1}{N_l^2 M_l^2} \left(F^{l^T} (G^l - A^l)\right)_{ij} & if \quad F_{ij}^l > 0 \\ 0 & if \quad F_{ij}^l < 0 \end{cases} \tag{7}$$

Standard error back-propagation can be used to quickly compute the gradients of $\boldsymbol{E_l}$ with respect to the pixel values of the image $\vec{\boldsymbol{x}}$. We synthesize new data that matches both the style representation of the artwork and the content representation of the photograph. Using a convolutional neural network with multiple layers, we can reduce the distance between a white noise feature representation of the image and those of a content image and style. The main objective is to minimize the loss function:

$$\mathcal{L}_{\text{total}}\left(\vec{p}, \vec{a}, \vec{x}\right) = \alpha \mathcal{L}_{\text{content}}\left(\vec{p}, \vec{x}\right) + \beta \mathcal{L}_{\text{style}}\left(\vec{a}, \vec{x}\right) \tag{8}$$

In this equation, the weighting factors for style and content reconstruction are both the same. The gradient pixel values can be utilized as an input for various numerical optimization algorithms. L-BFGS can be utilized here, which was found to perform adequately in picture synthesis [27]. Before computing feature representations, it is necessary to extract picture information at comparable sizes to resize the style image to match the content image. Finally, image priors are not necessary for synthesis results to be regularized. It is possible to make the case that the texture features of lower network levels convey an image that comes before the style image. Using different optimization algorithms and network architecture is predicted to produce some changes in picture synthesis as well.

4. Simulation Results

The proposed cancelable system is carried out on a dataset that consists of both face and fingerprint biometric modalities. Each modality includes eighteen biometric images from different individuals. Figures 2 and 3 show a sample dataset for each biometric modality. Furthermore, this dataset is segmented into two segments; each one includes nine images of both face and fingerprint biometrics. This segmentation is performed to provide comparative analysis between the proposed approach and others in the literature.

Figure 2. Sample of the face images from the dataset.

Figure 3. Sample of fingerprint images from the dataset.

4.1. Evaluation Metrics

A different strategy for evaluation involves statistical analysis, encompassing both qualitative and quantitative measurements. The qualitative element entails evaluating the caliber of the cancelable template generated, while the quantitative aspect entails establishing statistical indicators like correlation and signal-to-noise ratio (SNR) for the template.

4.1.1. Quantitative Analysis

The effectiveness of the MBCS scheme is assessed through the application of three quantitative metrics: Number of Pixel Changes Rate (NPCR), Unified Average Changing Intensity (UACI), and Peak Signal to Noise Ratio (PSNR). Equations (9)–(11) are employed to compute NPCR, UACI, and PSNR for two images, namely I1 and I2. Here, M and N symbolize the dimensions of the images, denoting their width and height, respectively.

$$NPCR(\%) = \frac{1}{M \times N \times 3} \sum_{i=1}^{M} \sum_{j=1}^{N} \sum_{k=1}^{3} S(i,j,k) \times 100, \quad (9)$$

where

$$S(i,j,k) = \begin{cases} 1, & I_1(i,j,k) = I_2(i,j,k) \\ 0, & elsewhere \end{cases} \tag{10}$$

$$UACI(\%) = \frac{1}{M \times N \times 3} \sum_{i=1}^{M} \sum_{j=1}^{N} \sum_{k=1}^{3} \frac{|I_1(i,j,k) - I_2(i,j,k)|}{255} \times 100. \tag{11}$$

$$PSNR = 20\log_{10}\left[\frac{I_{MAX}}{\sqrt{MSE}}\right],$$

where I_{MAX} refers to the maximum possible pixel value, and MSE refers to mean square error, defined as:

$$MSE = \frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} [I_2(i,\ j) - I_1(i,\ j)]. \tag{12}$$

4.1.2. Qualitative Analysis

The qualitative evaluation process involves employing quality metrics to appraise the system's performance. In this particular scenario, the performance of the proposed MBCS scheme is assessed by analyzing the spectral distribution (SD) and universal image quality index (UIQ). These metrics are utilized to evaluate the cancelable template that has been generated.

Spectral Distortion

The spectral distribution (SD) is a technique used to evaluate the likeness of spectral data between two images in a qualitative manner [28]. It is generally acknowledged that SD values can be used to determine the similarity of the images being compared [29]. The mathematical definition of SD is as follows:

$$SD = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} |x(i,j) - y(i,j)|}{MN} \tag{13}$$

Here, "M × N" denotes the total count of pixels present in the image, while the variables "X" and "Y" refer to the original image and the encrypted image, respectively.

- Universal image quality index

The Universal Image Quality Index (UIQ) is an additional measure utilized to evaluate the structural similarity between two images [30]. Mathematically, UIQ is computed using Equation (12), and the resulting values fall within the range of -1 to 1, with values closer to 1 indicating a higher level of consistency between the images being compared [30].

$$UQI(i,j) = \frac{Cov_{ij}}{\sigma_i \sigma_j} \cdot \frac{2\mu_i \mu_j}{\mu_i^2 + \mu_j^2} \cdot \frac{2\sigma_i \sigma_j}{\sigma_i^2 + \sigma_j^2} \tag{14}$$

The quantities referred to as "where and are the mean of i and j, variance i and j and the covariance of i and j respectively" denote specific statistical measures, namely the means, variances, and covariance of variables i and j.

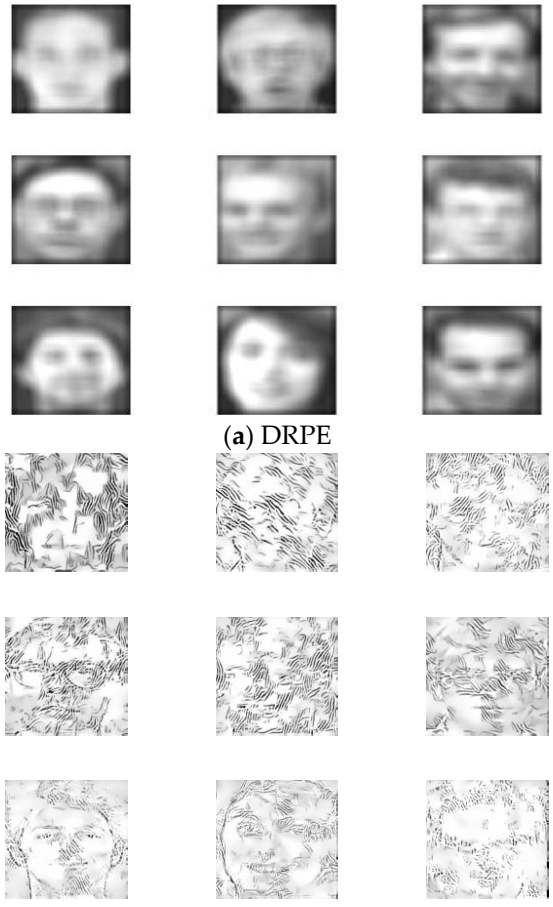
The quantitative and qualitative evaluation concludes with the tabular representation of the defined metrics for our proposed MBCS scheme.

4.2. Results of Visual Cancelable Templates

The proposed system, which is based on style transfer, is run on the dataset that was discussed in the previous subsection. To elucidate the impact of employing the suggested deep learning and style transfer scheme for the introduced cancelable biometric model, two sample datasets of faces and their corresponding fingerprint biometrics are tested. In simulation tests, the face biometrics are used as content images, and fingerprint biometrics

are used as style images. The original nine samples of the utilized content include faces and style fingerprint biometrics.

The proposed cancelable biometric model based on a deep style transfer scheme is compared to the DRPE ciphering technique [15]. Figures 4 and 5 show the results of the ciphering step for the proposed deep learning and style transfer scheme compared to the state-of-the-art DRPE technique for all analyzed biometrics. In contrast to the traditional DRPE method, the results of the proposed hybrid scheme are being praised and advocated for a more cost-effective cancelable biometric model. In all experiments, two biometric images have been used for authentication. Second, a person who is not authorized to access the information for the purposes of determining the level of system security is assumed to have access to the correct key during the testing process. Tested biometric patterns and two ciphered pictures are compared for their correlation coefficients.



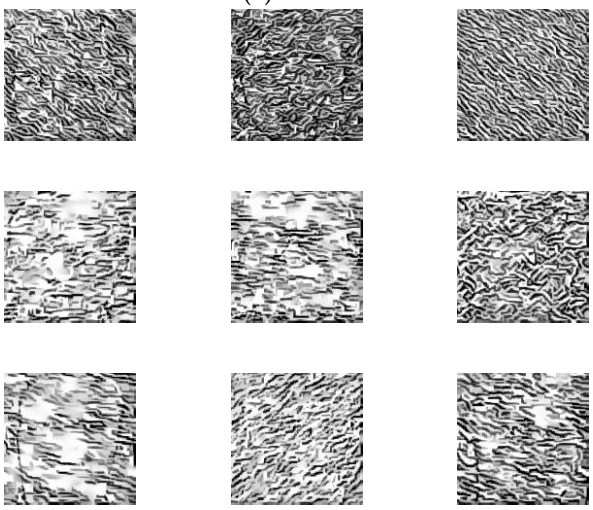
(**a**) DRPE

(**b**) Style Transfer

Figure 4. Cancelable biometrics generated by (**a**) DRPE and (**b**) style transfer for the first segment of the dataset.

The results of the authentication phase for the suggested method, in comparison to the related DRPE technique, are shown in Figures 6 and 7. These results include the receiver operating characteristic (ROC), probability of false distribution (PFD), and probability of true distribution (PTD) [31–34] for all the examined biometric patterns. In the authentication phase, these results determine the error probability and threshold. The threshold, which determines whether an input person is an authorized user, is obtained by analyzing the intersection of the PFD and PTD curves. The proposed deep learning plus style transfer scheme evaluates correlation values for nine biometric images in all datasets. The results are presented in Tables 1 and 2, respectively, in comparison to the current state-of-the-art DRPE method.

(**a**) DRPE

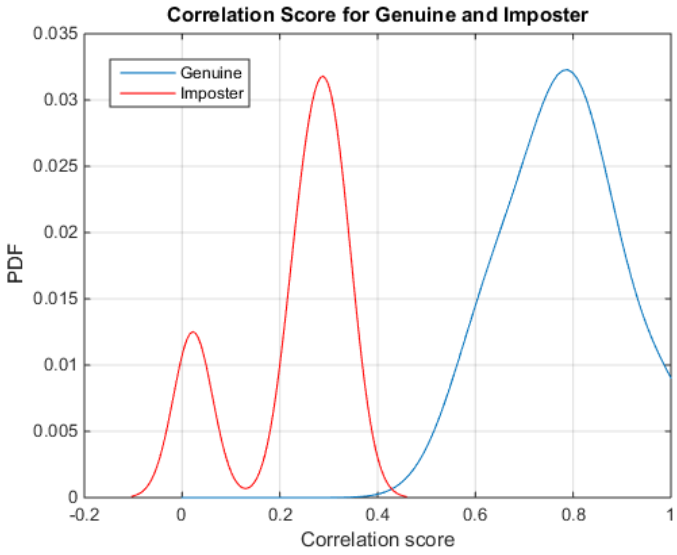


(**b**) Style Transfer

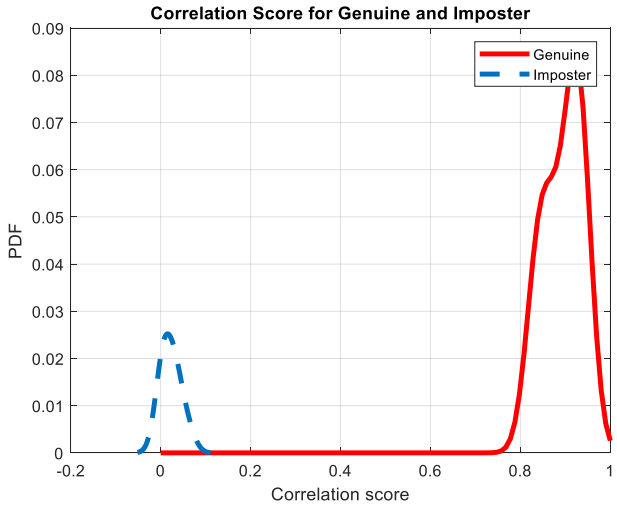
Figure 5. Cancelable biometrics generated by (**a**) DRPE and (**b**) style transfer for the second segment of the dataset.

Based on the correlation values obtained from the tested simulation cases, it can be concluded that the proposed deep learning + style transfer scheme is a good candidate for the cancelable biometric system to perform better than the traditional DRPE method.

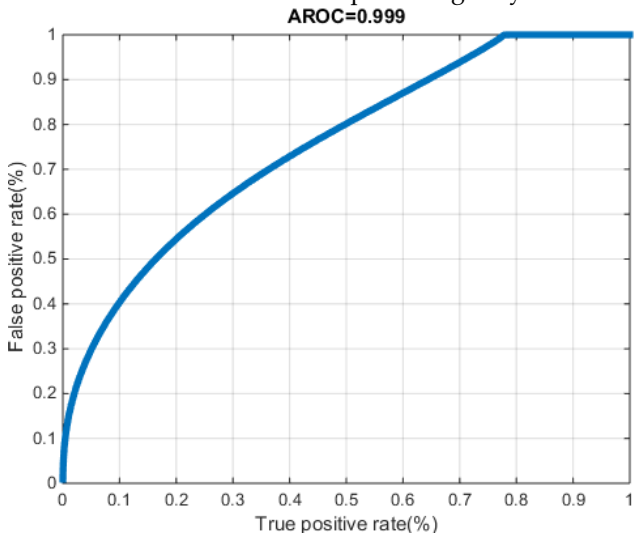
Table 1 presents the results of the statistical analysis conducted on the proposed MBCS. The analysis involved comparing the generated cancelable templates with the original images using various metrics. The proposed MBCS was found to exhibit a high level of efficiency based on the evaluated metrics, achieving an average NPCR of 99.26, PSNR of 23.28, SSIM of 0.0405, UIQ of 0.7492, SD of 60.442, and UACI of 24.268. The evaluation metrics suggest that the proposed MBCS can be confidently employed for cybersecurity applications that rely on human biometrics.



(**a**) The PFD and PTD results of the DRPE scheme.

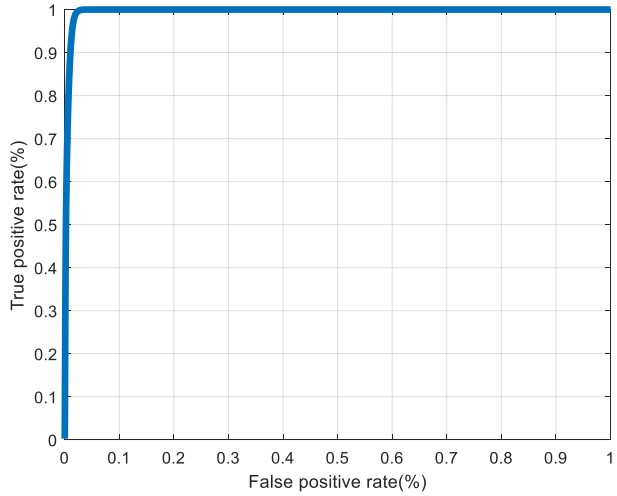


(**b**) The PFD and PTD results of the deep learning + style transfer scheme.



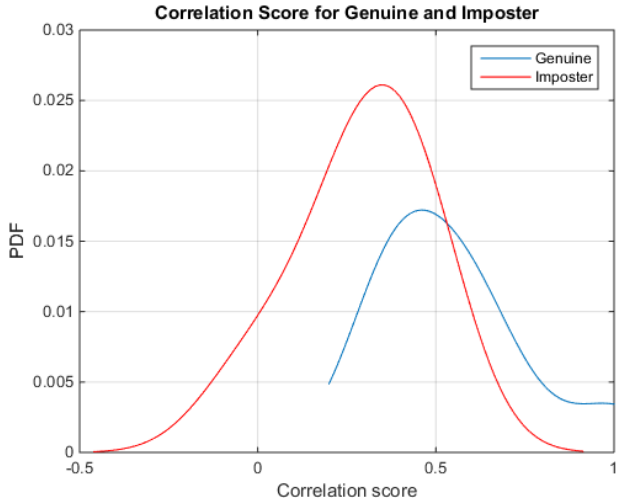
(**c**) ROC of the DRPE scheme.

Figure 6. *Cont*.

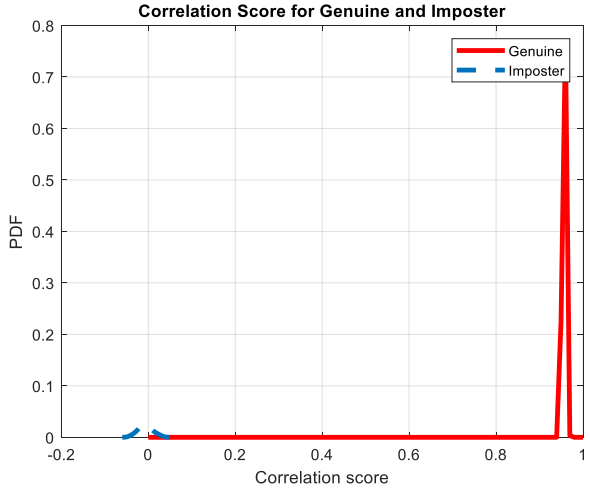


(**d**) The ROC of the deep learning + style transfer scheme.

Figure 6. The ROC, PFD, and PTD results of the authentication stage output for the proposed deep learning + style transfer scheme contrast to the DRPE scheme of the nine analyzed biometric face images as content images and nine biometric fingerprint images as style images of sample 1 dataset.

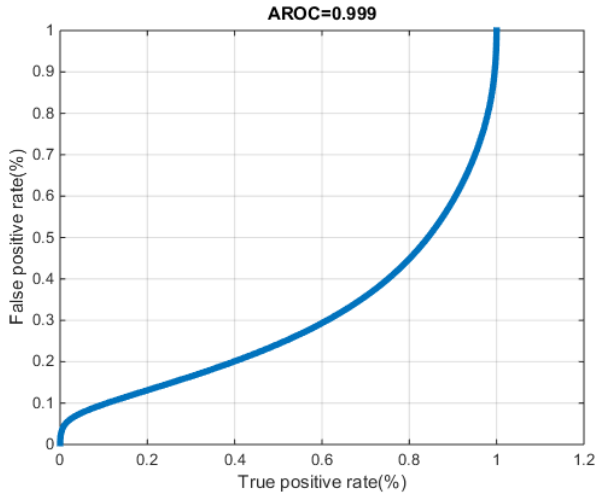


(**a**) The PFD and PTD results of the DRPE scheme.

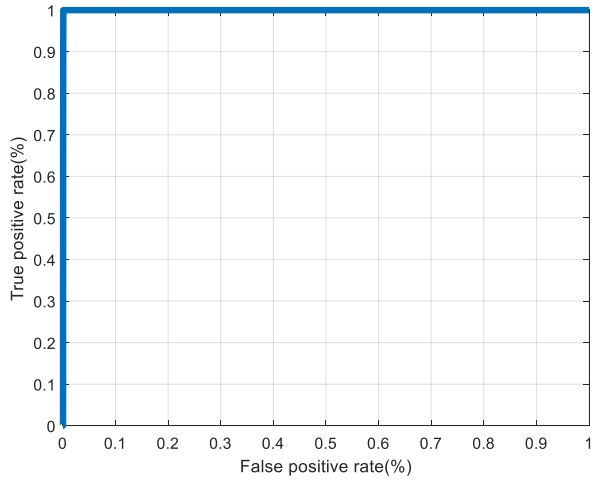


(**b**) The PFD and PTD results of the deep learning + style transfer scheme.

Figure 7. *Cont.*



(**c**) The ROC of the DRPE scheme.



(**d**) The ROC of the deep learning + style transfer scheme.

Figure 7. The ROC, PFD, and PTD results of the authentication stage output for the proposed deep learning + style transfer scheme contrast to the DRPE scheme of the nine analyzed biometric face images as content images and nine biometric fingerprint images as style images of sample 2 dataset.

Table 1. Quantitative and qualitative evaluation of proposed MBCS scheme.

Image	NCRP (%)	PSNR (dB)	SSIM	UIQ	SD	UACI
1	98.76	21.95	0.042	0.78	75.21	30.14
2	98.72	24.05	0.034	0.74	56.55	22.78
3	98.12	22.57	0.05	0.72	57.84	24.43
4	98.19	22.45	0.04	0.77	58.89	25.29
5	98.28	23.83	0.034	0.73	57.24	26.33
6	98.98	22.88	0.032	0.71	59.06	26.54
7	99.25	22.35	0.039	0.75	56.92	24.96
8	98.31	21.61	0.057	0.79	57.49	23. 19
9	99.28	23.71	0.031	0.79	60. 39	24.46
10	98.67	21.35	0.051	0.76	75.95	28.74
11	98.47	22.53	0.036	0.74	57.39	22.78
12	98.12	23.73	0.06	0.72	56.84	23.33
13	99. 29	21.58	0.033	0.77	60.99	26.81
14	98.23	24.23	0.04	0.70	60.28	27.03

Table 1. *Cont.*

Image	NCRP (%)	PSNR (dB)	SSIM	UIQ	SD	UACI
15	98.78	24.08	0.038	0.71	58.0688	26.54
16	98.71	22.34	0.031	0.76	57.2120	23. 69
17	98.91	22.08	0.059	0.78	56.4679	24. 12
18	99.07	24.28	0.0315	0.72	61.7939	26.86

Table 2. Execution time (in seconds).

Method	Total
IFL followed by Gaussian RP [35]	13.14
Homomorphic transform followed by Gaussian RP [35]	12.19
The proposed MBCS method	16.52

4.3. Results of Bio-Hash Templates

The current investigation proposes an alternative approach to cancelable templates by employing hashing algorithms. This class of cancelable templates represents the hashed representation of the input biometric data. These forms possess a limited storage capacity, which is highly valuable in real-time applications that lack extensive storage resources, such as those commonly found in Internet of Things (IoT) applications. The suggested technique utilizes hashing algorithms on the visual templates produced by the style transfer algorithm. To evaluate the effectiveness of this technique, pairwise distances, including Hamming and correlation, are utilized. Figures 8 and 9 depict the Hamming distance and correlation between the generated bio-hash templates and a hypothetical intruder who attempts to compromise the system by generating a bio-hash. The findings demonstrate that the proposed cancelable biometric system generates hashed templates with a Hamming distance close to 1, indicating optimal performance, and correlation values close to zero, which is also considered optimal performance.

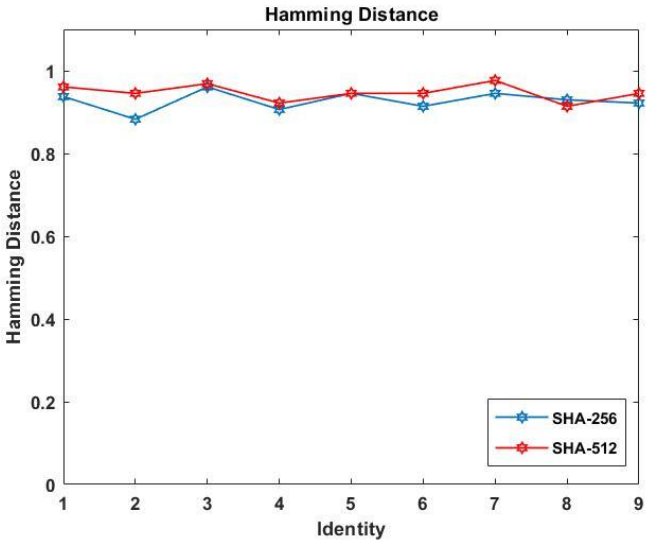


Figure 8. *Cont.*

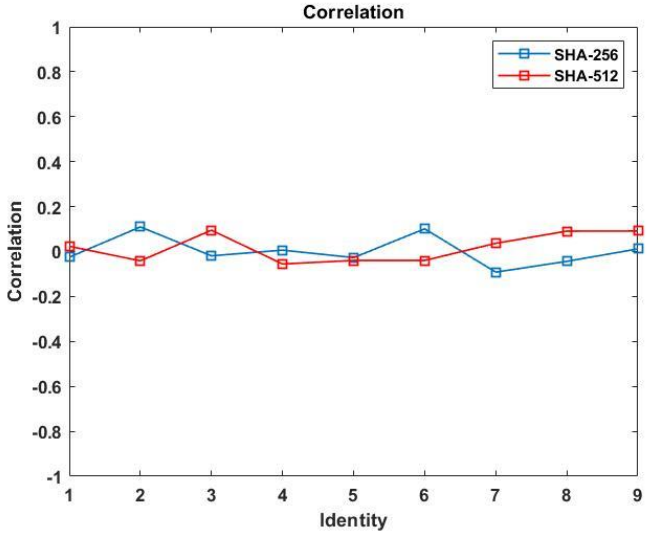


Figure 8. Hamming distance and correlation of the proposed bio-hash templates of the first segment of dataset.

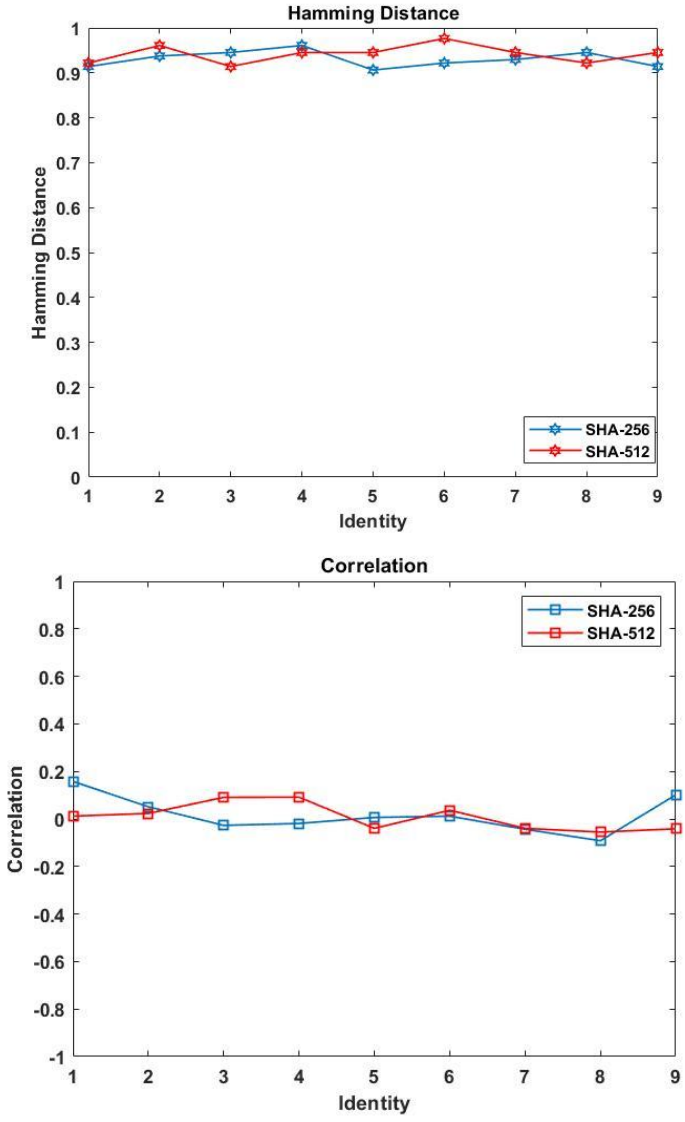


Figure 9. Hamming distance and correlation of the proposed template protection scheme of the second segment of dataset.

5. More Analysis and Discussion

5.1. Robustness Justification

A good strategy for assessing the system's robustness is to simulate a spoofing attack and evaluate it by analyzing the autocorrelation and cross-correlation between the selected spoofer and the other subjects.

In this context, subject number one is assumed to be the spoofer, and both its autocorrelation and cross-correlation with the other subjects are measured. Figure 10 presents a bar plot illustrating the correlation between the spoofer and all the subjects. Notably, the correlation between the assumed spoofer and subject 1 is close to 1, indicating a strong correlation. Conversely, the correlation between the assumed spoofer and the other subjects is close to 0, suggesting minimal correlation. Consequently, these findings support the conclusion that the proposed system serves as a robust solution against spoofing attacks.

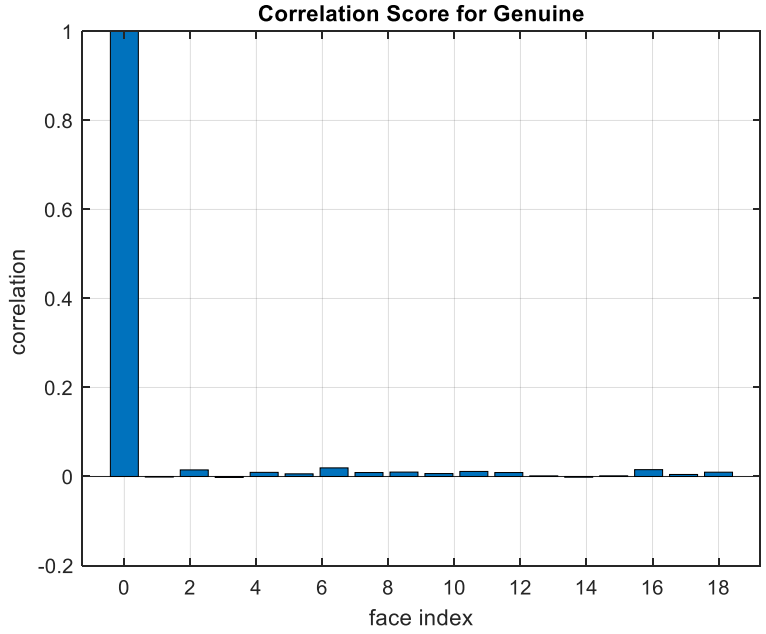


Figure 10. Correlations among a spoofer and the subjects included in the dataset.

5.2. Time Complexity and Execution Time

The assessment of an algorithm's complexity involves evaluating the interactions and resources necessary for its implementation. In this study, we measure the effectiveness of the proposed MBCS scheme by analyzing its execution time and its inherent constraining aspect, namely, the big *O* analysis.

The computation of the implementation time for our MBCS scheme, measured in seconds, is determined based on the execution steps needed for each user, with each user's biometric being represented as an *M* by *N* image, as outlined in the following enumeration. Steps performed for each user are given below:

1- (O(1)) operations to register current biometrics of the user.
2- (O(n $\times$ (M $\times$ N)) operations to perform feature extraction on an M $\times$ N image, where n is an integer.
3- (O(2 $\times$ n $\times$ (M $\times$ N))) operations to fuse the features.
4- (O(M $\times$ N)) operations to reconstruct the fused image.
5- (O(5 $\times$ n $\times$ M $\times$ N)) operations to perform the deep dream (where 5 is the number of steps).
6- (O(n $\times$ (M $\times$ N))) operations to perform the authentication process to accept or reject the user.

Furthermore, the time required to execute the proposed scheme is tabulated in Table 2. The reported time is considered acceptable since generation of the cancelable template is an off-line process [35].

5.3. Discussion and Comparisons

To confirm the productivity of the proposed reliable cancelable biometric approach based on a hybrid deep learning and style transfer scheme, a comparison was made with the results of recent previous schemes [8,18,29,31,36–38]. The performance of the proposed hybrid deep learning plus style transfer scheme-based cancelable biometric model was evaluated in terms of false acceptance rate (FAR), equal error rate (EER), area under the receiver operating characteristic curve (AROC), and false rejection rate (FRR), and compared with other ciphering-based cancelable biometric related systems in the literature. The results of the comparison are presented in Table 3, which shows that the proposed hybrid deep learning and style transfer scheme-based cancelable biometric system performed favorably in terms of EER, FAR, AROC, and FRR, compared to other systems published in the literature.

Table 3. Statistical analysis (EER, FAR, FRR, and AROC) of the proposed method and other methods in the literature.

Method	EER	FAR	FRR	AROC
Proposed (Style Transfer)	7.6842×10^{-13}	2.1573×10^{-15}	1.0295×10^{-11}	0.9999
Ref. [18]	0.0058	0.0985	1.6822×10^{-4}	0.8630
Ref. [31]	9.5647×10^{-5}	0.0056	2.5216×10^{-3}	0.8684
Ref. [36]	0.0046	2.3550×10^{-4}	0.9292	0.8837
Ref. [8]	0.0178	0.0017	0.8769	0.8967
Ref. [29]	5.6942×10^{-10}	3.0414×10^{-7}	0.9671	0.9076
Ref. [37]	0.0016	0.1955	4.5354×10^{-4}	0.8737
Ref. [38]	8.7546×10^{-9}	0.0435	6.1101×10^{-3}	0.7187

6. Conclusions

This study introduces a novel approach for developing a cancelable biometric system, suitable for IoT applications, that combines deep learning and style transfer techniques. The primary contribution of this research lies in the integration of deep learning with the style transfer scheme, resulting in a robust biometric model that can effectively withstand potential attacks from hackers. By incorporating both deep learning and style transfer, the proposed approach enhances the security and introduces distortion to the original biometric patterns, leading to the generation of altered biometric patterns. The effectiveness of the hybrid deep learning and style transfer scheme was verified through extensive experimentation involving encryption and distortion of stored biometric data. The results demonstrate that this approach offers superior suitability for securing biometric patterns compared to previously proposed methods. Additionally, the proposed system exhibits the ability to encrypt and distort various types of biometric datasets, further reinforcing the cancelability of stored biometric templates. Overall, the introduced cancelable identification biometric framework achieves remarkable objective and subjective outcomes, surpassing the performance of previous approaches.

Author Contributions: Conceptualization, A.S. and A.A.A.E.-L.; methodology, A.S.; validation, A.S.; formal analysis, A.S. and A.A.A.E.-L.; investigation, A.S. and H.M.; resources, M.E.-A. and H.M.; data curation, M.E.-A. and H.M.; writing—original draft preparation, A.S. and A.A.A.E.-L.; supervision, M.E.-A. and H.M. All authors have read and agreed to the published version of the manuscript.

Funding: Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2023R137), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Data Availability Statement: Data is available on demand.

Acknowledgments: The authors would like to acknowledge the support of Prince Sultan University for paying the Article Processing Charges (APC) for this publication.

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

References

1. Choudhury, B.; Then, P.; Issac, B.; Raman, V.; Haldar, M.K. A Survey on Biometrics and Cancelable Biometrics Systems. *Int. J. Image Graph.* **2018**, *18*, 1850006. [CrossRef]
2. Khan, M.K.; Xie, L.; Zhang, J. Chaos and NDFT-Based Spread Spectrum Concealing of Fingerprint-Biometric Data into Audio Signals. *Digit. Signal Process.* **2010**, *20*, 179–190. [CrossRef]
3. Kaur, H.; Khanna, P. Cancelable Features Using Log-Gabor Filters for Biometric Authentication. *Multimed. Tools Appl.* **2017**, *76*, 4673–4694. [CrossRef]
4. Nandakumar, K.; Jain, A.K. Biometric Template Protection: Bridging the Performance Gap between Theory and Practice. *IEEE Signal Process. Mag.* **2015**, *32*, 88–100. [CrossRef]
5. Rane, S. Standardization of Biometric Template Protection. *IEEE Multimed.* **2014**, *21*, 94–99. [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, 4–7 April 2011; IEEE: New York, NY, USA; pp. 495–500.
7. Jin, Z.; Teoh, A.B.J.; Goi, B.-M.; Tay, Y.-H. Biometric Cryptosystems: A New Biometric Key Binding and Its Implementation for Fingerprint Minutiae-Based Representation. *Pattern Recognit.* **2016**, *56*, 50–62. [CrossRef]
8. 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]
9. Sedik, A.; El-Latif, A.A.A.; Wani, M.A.; El-Samie, F.E.A.; Bauomy, N.A.-S.; Hashad, F.G. Efficient Multi-Biometric Secure-Storage Scheme Based on Deep Learning and Crypto-Mapping Techniques. *Mathematics* **2023**, *11*, 703. [CrossRef]
10. Elazm, L.A.A.; El-Shafai, W.; Ibrahim, S.; Egila, M.G.; Shawkey, H.; Elsaid, M.K.H.; Soliman, N.F.; AlEisa, H.N.; El-Samie, F.E.A. Efficient Hardware Design of a Secure Cancellable Biometric Cryptosystem. *Intell. Autom. Soft Comput.* **2023**, *36*, 929–955. [CrossRef]
11. El-Shafai, W.; Elsayed, M.; Rashwan, M.; Dessouky, M.; El-Fishawy, A.; Soliman, N.F.; Alhussan, A.A.; Abd El-Samie, F.E. Optical Ciphering Scheme for Cancellable Speaker Identification System. *Comput. Syst. Sci. Eng.* **2023**, *45*, 563–578. [CrossRef]
12. Salama, G.M.; El-Gazar, S.; Omar, B.; Nassar, R.M.; Khalaf, A.A.M.; El-Banby, G.M.; Hamed, H.F.A.; El-Shafai, W.; Abd El-Samie, F.E. Cancelable Biometric System for IoT Applications Based on Optical Double Random Phase Encoding. *Opt. Express* **2022**, *30*, 37816–37832. [CrossRef] [PubMed]
13. Faragallah, O.S.; Naeem, E.A.; El-Shafai, W.; Ramadan, N.; Ahmed, H.E.H.; Elnaby, M.M.A.; Elashry, I.; El-khamy, S.E.; El-Samie, F.E.A. Efficient Chaotic-Baker-Map-Based Cancelable Face Recognition. *J. Ambient. Intell. Humaniz. Comput.* **2023**, *14*, 1837–1875. [CrossRef]
14. Takahashi, K.; Hitachi, S.H. Generating Provably Secure Cancelable Fingerprint Templates Based on Correlation-Invariant Random Filtering. In Proceedings of the 2009 IEEE 3rd International Conference on Biometrics: Theory, Applications, and Systems, Washington, DC, USA, 28–30 September 2009; IEEE: New York, NY, USA, 2009; pp. 1–6.
15. Sandhya, M.; Prasad, M.V.N.K. Cancelable Fingerprint Cryptosystem Using Multiple Spiral Curves and Fuzzy Commitment Scheme. *Int. J. Pattern Recognit. Artif. Intell.* **2017**, *31*, 1756004. [CrossRef]
16. Qiu, J.; Li, H.; Dong, J. Design of Cancelable Palmprint Templates Based on Look up Table. *IOP Conf. Ser. Mater. Sci. Eng.* **2018**, *322*, 52050. [CrossRef]
17. Ali, M.A.M.; Tahir, N.M. Cancelable Biometrics Technique for Iris Recognition. In Proceedings of the 2018 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE), Penang, Malaysia, 28–29 April 2018; IEEE: New York, NY, USA, 2018; pp. 434–437.
18. Soliman, R.F.; Amin, M.; Abd El-Samie, F.E. A Modified Cancelable Biometrics Scheme Using Random Projection. *Ann. Data Sci.* **2019**, *6*, 223–236. [CrossRef]
19. Soliman, R.F.; Ramadan, N.; Amin, M.; Ahmed, H.H.; El-Khamy, S.; Abd El-Samie, F.E. Efficient Cancelable Iris Recognition Scheme Based on Modified Logistic Map. *Proc. Natl. Acad. Sci. India Sect. A Phys. Sci.* **2020**, *90*, 101–107. [CrossRef]
20. Soliman, R.F.; Amin, M.; Abd El-Samie, F.E. A Double Random Phase Encoding Approach for Cancelable Iris Recognition. *Opt. Quantum Electron.* **2018**, *50*, 326. [CrossRef]
21. Gowthami, A.T.; Mamatha, H.R. Fingerprint Recognition Using Zone Based Linear Binary Patterns. *Procedia Comput. Sci.* **2015**, *58*, 552–557. [CrossRef]
22. Butt, M.; Damer, N. Helper Data Scheme for 2D Cancelable Face Recognition Using Bloom Filters. In Proceedings of the IWSSIP 2014 Proceedings, Dubrovnik, Croatia, 12–15 May 2014; IEEE: New York, NY, USA, 2014; pp. 271–274.
23. Teoh, A.B.J.; Kuan, Y.W.; Lee, S. Cancellable Biometrics and Annotations on Biohash. *Pattern Recognit.* **2008**, *41*, 2034–2044. [CrossRef]
24. Kho, J.B.; Kim, J.; Kim, I.-J.; Teoh, A.B.J. Cancelable Fingerprint Template Design with Randomized Non-Negative Least Squares. *Pattern Recognit.* **2019**, *91*, 245–260. [CrossRef]

25. Simonyan, K.; Zisserman, A. Very Deep Convolutional Networks for Large-Scale Image Recognition. *arXiv* **1409**, arXiv:1409.1556.
26. Jia, Y.; Shelhamer, E.; Donahue, J.; Karayev, S.; Long, J.; Girshick, R.; Guadarrama, S.; Darrell, T. Caffe: Convolutional Architecture for Fast Feature Embedding. In Proceedings of the 22nd ACM International Conference on Multimedia, Orlando FL, USA, 3–7 November 2014; pp. 675–678.
27. Zhu, C.; Byrd, R.H.; Lu, P.; Nocedal, J. Algorithm 778: L-BFGS-B: Fortran Subroutines for Large-Scale Bound-Constrained Optimization. *ACM Trans. Math. Softw.* **1997**, *23*, 550–560. [CrossRef]
28. Elshazly, E.A.; Hashad, F.G.; Sedik, A.; Abd El-Samie, F.E.; Abdel-Salam, N. Compression-Based Cancelable Multi-Biometric System. *Res. Sq.* 2022; *in press*. [CrossRef]
29. Tarif, E.B.; Wibowo, S.; Wasimi, S.; Tareef, A. A Hybrid Encryption/Hiding Method for Secure Transmission of Biometric Data in Multimodal Authentication System. *Multimed. Tools Appl.* **2018**, *77*, 2485–2503. [CrossRef]
30. Benrhouma, O.; Hermassi, H.; Abd El-Latif, A.A.; Belghith, S. Chaotic Watermark for Blind Forgery Detection in Images. *Multimed. Tools Appl.* **2016**, *75*, 8695–8718. [CrossRef]
31. Refregier, P.; Javidi, B. Optical Image Encryption Based on Input Plane and Fourier Plane Random Encoding. *Opt. Lett.* **1995**, *20*, 767–769. [CrossRef]
32. Lai, Y.-L.; Jin, Z.; Teoh, A.B.J.; Goi, B.-M.; Yap, W.-S.; Chai, T.-Y.; Rathgeb, C. Cancellable Iris Template Generation Based on Indexing-First-One Hashing. *Pattern Recognit.* **2017**, *64*, 105–117. [CrossRef]
33. Tarek, M.; Ouda, O.; Hamza, T. Pre-Image Resistant Cancelable Biometrics Scheme Using Bidirectional Memory Model. *Int. J. Netw. Secur.* **2017**, *19*, 498–506.
34. Wu, J.; Zhu, Z.; Guo, S. A Quality Model for Evaluating Encryption-as-a-Service. In Proceedings of the International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage, Guangzhou, China, 12–15 December 2017; Springer: Cham, Switzerland, 2017; pp. 557–569.
35. Algarni, A.D.; El Banby, G.M.; Soliman, N.F.; El-Samie, F.E.A.; Iliyasu, A.M. Efficient Implementation of Homomorphic and Fuzzy Transforms in Random-Projection Encryption Frameworks for Cancellable Face Recognition. *Electronics* **2020**, *9*, 1046. [CrossRef]
36. Sinha, A.; Singh, K. Image Encryption by Using Fractional Fourier Transform and Jigsaw Transform in Image Bit Planes. *Opt. Eng.* **2005**, *44*, 57001. [CrossRef]
37. 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), Coimbatore, India, 7–9 January 2016; IEEE: New York, NY, USA, 2016; pp. 1–6.
38. 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]