

Received November 21, 2020, accepted December 6, 2020, date of publication December 9, 2020,  
date of current version December 21, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3043689

# Optical PTFT Asymmetric Cryptosystem-Based Secure and Efficient Cancelable Biometric Recognition System

ABDULAZIZ ALARIFI<sup>1</sup>, MOHAMMED AMOON<sup>1</sup>, MOUSTAFA H. ALY<sup>2</sup>,  
AND WALID EL-SHAFI<sup>3</sup>

<sup>1</sup>Department of Computer Science, Community College, King Saud University, Riyadh 11437, Saudi Arabia

<sup>2</sup>Electronics and Communications Engineering Department, College of Engineering and Technology, Arab Academy for Science, Technology and Maritime Transport, Alexandria 1029, Egypt

<sup>3</sup>Department of Electronics and Electrical Communications Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt

Corresponding author: Mohammed Amoon (mamoona@ksu.edu.sa)

This work was supported by the Deanship of Scientific Research, King Saud University, through the Research Group under Grant RG-1440-039.

**ABSTRACT** Recently, biometric systems are extensively and commonly utilized for authentication and verification applications. The security issue and the dependence on a specific biometric for the biometric verification process are the main challenges confronted in biometric systems. The security issue comes due to the exploitation of the original biometrics in stored servers. Therefore, if any attacks have been introduced to the stored biometrics, they will be missed indefinitely. Consequently, the stored original biometrics must be secured through maintaining and storing these templates away from exploitation in their servers. So, there is a need for designing a cancelable biometric recognition system (CBRS) that is a promising protection trend in biometric verification and authentication fields. The CBRS is based on the conversion of biometric data or its features to a different arrangement. In this article, a novel CBRS based on the suggested optical PTFT (Phase Truncated Fourier Transform) asymmetric encryption algorithm is introduced. In the proposed algorithm, two different distributions of phases in the output and Fourier planes are maintained as deciphering keys, and thus, the encryption keys will not be utilized for the decryption process. This leads to the advantage that the two ciphering keys may be utilized as public secret keys to encrypt distinct biometric images. Consequently, the suggested PTFT cryptosystem is an asymmetric encryption/decryption technique compared to the preceding related optical encryption techniques that are symmetric techniques such as Optical Scanning Holography (OSH) and Double Random Phase Encoding (DRPE). The suggested PTFT asymmetric encryption algorithm also has a wonderful practical performance in security applications. One of the main contributions of the proposed optical PTFT asymmetric encryption algorithm is that it removes the linearity features of the optical OSH and DRPE symmetric encryption algorithms through its great features of the phase truncation nonlinear operation. Subsequently, this produces an encrypted biometric template with two public keys, and the authenticated user can retrieve the original biometric template utilizing two private keys with achieving a high security and cancelability performance for the stored biometrics. To confirm the efficacy of the suggested optical encryption algorithm for developing a secure CBRS, various biometric datasets of face, ear, palmprint, fingerprint, and iris images are examined and analyzed. Extensive comparative analyses are performed amongst the suggested algorithm and the optical OSH and DRPE encryption algorithms. The experimental outcomes achieved for performance quality assessment assure that the suggested CBRS is reliable, robust, and realistic. It has great security and cancelability proficiency that expose excellent cancelable biometric recognition performance even in the existence of noise. Moreover, the performed experiments declare that the suggested CBRS guarantee an average FRR (False Reject Rate) of 0.0012, EER (Equal Error Rate) of 0.0019, and FAR (False Accept Rate) of 0.0030, and an average AROC (Areas under the Receiver Operating Characteristic) of 0.9996.

**INDEX TERMS** Optical encryption, cancelable biometrics, asymmetric encryption, OSH, DRPE, PTFT.

## I. INTRODUCTION

Due to the rapid advancement of digital knowledge, cloud, and Internet of Things (IoT) applications, the privacy and security of personal information have progressively received a great awareness [1], [2]. To bypass challenges related to the dependence on conventional authentication systems like tokens, Personal Identification Numbers (PINs), and passwords, advanced personal protection systems endorse biometric attributes that are unique to each person for authentication and identification [3]. Thus, recently, biometric images and signals from individuals are utilized across various authentication, verification, and identification applications. So, the biometric traits exploitation in identification and verification has observed incredible sophistication and expansion making it pervasive for a comprehensive variety of security applications [4].

These days, companies, institutions, banks, airports, and universities have their private security systems utilizing several biometric attributes. The fundamental function of these traditional biometric systems encompasses biometrics compilation from enrolled individuals, extraction of distinguishing traits from the gathered biometrics for data reduction purposes, and then stores these extracted traits in a secure database. This enrollment or registration procedure is deemed as the training stage. On the other hand, in the testing stage, traits from entering biometrics for new individuals are obtained and correlated with the previously accumulated traits [5], [6]. The major weakness of these conventional biometric systems is that each one of the subscribers has to deliver his unique biometrics for registration. This indicates that when the biometric storing server is embezzled, the main template veracity will be missed indefinitely and, for this reason, the complete biometric system misses its credibility and confidentiality. Furthermore, individuals whose personal biometrics have been purloined will not be capable to utilize them once more in other applications. Therefore, conventional biometric structures that are based on registration, extraction of main features, and matching of extracted features are no longer believable [7]–[10].


Consequently, in recent times, the theory of cancelable biometrics has arisen as a paradigm and an important processing tool to maintain the essential biometric information. A foremost benefit of cancellable biometric frameworks is their capability to sustain the immunization of the unique biometric information [11]. In these cancelable biometric frameworks, various biometric records can be modified or modernized without altering the whole system. So, cancelable biometric frameworks are based on the conversion of original biometric information into a different arrangement, so that individuals can supplant their unique biometric patterns in the same or various applications [12]. So, in such cancelable biometric frameworks, the original biometrics are distorted utilizing a one-way mathematical operation prior

to their storage in the database. Thus, the cancelable biometric procedures improve the unlinkability and diversity problem [13].

Various transformation schemes could be employed on the identical biometric pattern for various functions and applications to counteract the cross-correlation along with accumulated templates in several biometric databases. More transformations and mathematical operations can be utilized for the cancelable biometric applications [14]–[21]. Some of them are employed to combine two or more template protection techniques to build a single biometric cryptosystem. Also, one of the potential keys to construct cancelable biometric frameworks is the utilization of cryptography algorithms. Consequently, the main features in a biometric template could be hidden, secured, and encrypted using secret keys generated from any employed cryptography scheme like optical encryption schemes that have superior advantages and merits in enormous security applications [22], [23].

The technology of information and data processing in the optical domain has ingrained multidimensionality and the capability of high-speed parallel processing [24], [25]. The utilization of optical processing procedures to safeguard information and biometric templates has been developed to be an attractive trend for scholars. Lately, numerous research attempts have been introduced to improve the optical cryptography algorithms due to their immense advantages of multidimensional potency and ingrained optical parallel processing [24]–[29]. But the presented optical cryptography algorithms mostly belong to the class of symmetric cryptography algorithms that have similar ciphering and deciphering keys. The critical disadvantage of symmetric cryptography algorithms is that they yield numerous practical and implementation difficulties like key management and distribution [30]. Therefore, it is essential to build asymmetric cryptography algorithms for security applications to resolve and mitigate the challenges of the symmetric cryptography systems.

The implementation regulations of asymmetric cryptography systems in security applications have certain requirements that differ from symmetric cryptography systems [31]: (1) two different keys are required and should be simply determined for cryptosystem, a public key (ciphering key), and a private key (deciphering key), (2) it should be straightforward to produce a cipher biometric template with the availability of the ciphering key and the plain template, (3) it must be straightforward to retrieve the plain template with the availability of the deciphering key and the ciphered biometric template, (4) if an adversary (imposter) recognizes the ciphering key, it should nevertheless be difficult to assume the deciphering key, (5) if an adversary (imposter) recognizes the ciphering key and the ciphered biometric template, it must nonetheless be difficult to retrieve the plain template, which makes the calculations and estimation impossible for imposters. Therefore, from the implementation principles of asymmetric cryptography systems, it is observed that a key role that asymmetric cryptosystems perform is that they are considered as an efficient one-way ciphering operation.

The associate editor coordinating the review of this manuscript and approving it for publication was Chunsheng Zhu .

This prompted us to take the advantage of these great and tremendous features of asymmetric cryptosystems for CBRSs that mostly need such features in maintaining the original biometric templates of users from intruders.

In this article, a CBRS is suggested based on an optical PTFT asymmetric cryptography algorithm. In the suggested algorithm, the ciphering key is considered as two random independent phase operations that are completely different from those of the deciphering keys of another two random independent phase operations. So, in the suggested algorithm, the phase truncation process in the Fourier transform is exploited to generate an asymmetric ciphered biometric template by utilizing two arbitrary public keys of phases truncated keys, whereas a genuine (authenticated) user can recover the original biometric template utilizing alternative two diverse random private phases truncated keys. Therefore, the proposed optical PTFT cryptography algorithm has a wonderful benefit of phase truncation nonlinear process that can be employed for the stored and distributed biometric templates with exploiting its capability to ensure rich diversity and irrevocability and achieving superior robustness and security against intruders and imposters in IoT and cloud-based cancelable biometric applications. Moreover, numerous quality assessments and evaluation metrics are utilized to offer a widespread measurement of the strength of the suggested optical encryption based CBRS when exposed to several forms of assaults.

The remainder of this work is coordinated as follows. The reported cancelable biometric frameworks are presented in Section II. The preliminary studies for the basics of the DRPE and OSH encryption algorithms are introduced in Section III. The proposed optical PTFT asymmetric encryption based CBRS is explained in Section IV. More comparative studies and simulation analyses are displayed and discussed in Section V. The final observations and future trends are summarized in Section VI.

## II. RELATED CANCELABLE BIOMETRICS WORK

Biometrics data privacy and security have progressively received great consideration in the era of prompt progress in digital technologies and Internet services. The security processing technology using optical cryptography algorithms has ingrained multidimensionality and terrific capability of parallel processing. The deployment of digital and optical ciphering algorithms to protect biometrics data has become a hot movement of a lot of researchers [24]–[31].

In [11], the authors introduced a straightforward and influential CBRS established on an arbitrary scrambling scheme. They exploited the arithmetic eigenvectors and eigenvalues of the plain biometric template and its arbitrarily scrambled template for performing CBRS. Their cancelable framework worked ambiguously by recognizing the cancelable biometric image and a secret PIN code distributed to an enrolled user. They tested the introduced CBRS against comparison methods on three different datasets of face, iris, and ear. In [12], the authors suggested a novel CBRS defined as Random Slope

(RS) technique for producing non-invertible, revocable, and secured biometric templates. The presented cancelable RS technique achieved higher cancelability performance by providing biometric dimensionality decrement with improved ratios. The suggested CBRS performance was experimentally tested on numerous template modalities such as palmprint, face, finger-vein, and palm-vein. The comparison with the existing schemes proved the efficiency of the suggested work in terms of effectiveness, reliability, and considerable reduction in biometrics sizes.

In [13], a remote biometric verification and authentication framework is suggested for IoT network applications to achieve urgent biometric security requirements in digital smart cloud services in the presence of critical digital identity burglaries and cybercrimes. In the suggested cancelable biometric framework, the random distance technique is employed to create revocable, non-invertible, privacy-preserving, and dimensionally decreased pseudo template identities. The same authors in [12], [13] introduced an improved CBRS in [15] based on using a random polynomial transformation scheme for generating protected and secured biometric images identified as PolyCodes. These generated secured images are revocable, discriminability, and privacy safeguarding, and deliver considerable dimensionality diminution. To verify the applicability and security performance of the suggested CBRS, the authors carried out several experiments and comparisons on several biometric templates such as finger-vein, palm vein, and palmprint.

In [16], an applicable alignment-free scheme for generating cancelable fingerprint biometrics based on a circular curtailed convolution algorithm is presented. It is a one-way transform model. It can safeguard the binary biometric templates without the ability to recover them from the convolved and length-decreased output templates. The suggested scheme achieved improved revocability, non-invertibility, and diversity for the generated cancelable biometrics. Simulation studies on different fingerprint datasets were presented to verify the usefulness of the suggested model against existing schemes. The authors in [17] proposed a novel CBRS for creating cancelable templates utilizing the concept of secret visual sharing. Different shares related to each biometric template are generated. These generated secret visual shares are collected and stored in a disseminated way as alternatives to the original biometric templates. Simulations and performance analyses have been performed on the open-access IIT Iris Delhi database to demonstrate the effectiveness of the suggested framework [17]. The outcomes revealed that the accomplishment of the suggested work is superior to other existing proposed methodologies in terms of performance evaluation measures of average FRR, Correlation Coefficient ( $C_r$ ), FAR, TER (True Error Rate), TSR (True Success Rate), and GAR (Genuine Accept Rate).

The same authors in [11], [17] suggested another efficient CBRS in [18] for generating protected and cancelable templates based on employing a reverse XOR Boolean method. They suggested three various schemes for cancelable

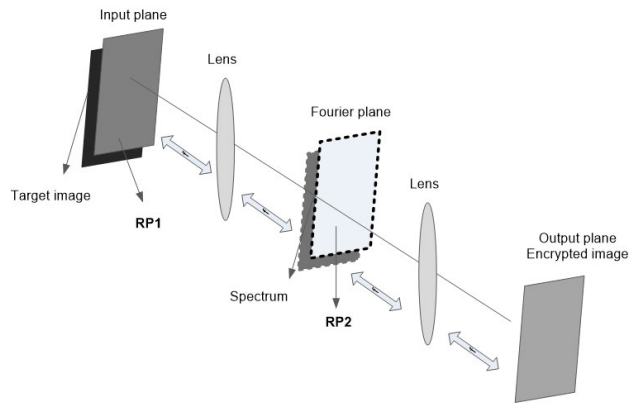


FIGURE 1. The basic concept of the DRPE algorithm.

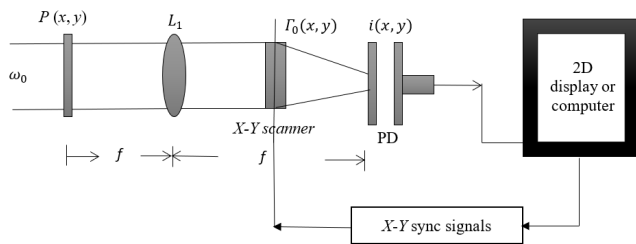


FIGURE 2. The basic concept of the OSH algorithm.

biometrics generation with the help of exploiting the secret visual sharing concept. The authors tested their suggested work performance on the open-access Iris IIT Delhi database and Face ORL database. A performance comparison between the three suggested schemes is introduced in terms of  $C_r$ , Peak Signal-to-Noise Ratio (PSNR), Structural Similarity (SSIM), and other distinct evaluation parameters. In [20], an efficient fingerprint cryptography technique is introduced that employs the space high-dimension projection algorithm to generate the protected encrypted biometric template. The suggested biometric cryptography technique incorporates the benefits of fuzzy commitment, dynamic key generation, and fuzzy vault schemes in its operation.

The authors in [21] suggested an improved CBRS for fingerprint biometrics, which comprises two different layers: an expendable layer and a core layer; to achieve consistent enrolment for crucial access control infrastructures. In the core layer, a non-invertible mathematical operation based random projection process is carried out to the feature set of fingerprint biometrics; to accomplish biometric template revocability and protection. In the expendable layer, the employed transformation key is protected to improve the whole CRBS security performance, and unquestionably, this additional protection is an improvement across the current CBRS frameworks. In [23], the authors proposed a hybrid biometric authentication system with the utilization of the OSH technique and asymmetric RSA (Rivest–Shamir–Adleman) cryptography algorithm. The proposed system comprises two main phases. Through the first employed

phase, the process of biometric ciphering is integrated into the OSH technique to transform the physical object image into an encrypted biometric hologram. On the other hand, in the second phase, the differential pulse code modulation (DPCM) is employed to encode the resulted encrypted biometric hologram, and then, the RSA algorithm is exploited to encrypt the DPCM data polarity.

In [24], the authors suggested an optical cryptography algorithm for secure CBRS based on the optical 3D jigsaw and fractional Fourier transforms. The proposed CBRS framework was tested on the face and fingerprint biometrics to validate its performance compared to the optical DRPE algorithm. The obtained outcomes proved that the introduced CBRS is reliable, feasible, secured, and achieving recommended ciphering and cancelability performance. In [25], two DRPE based cancelable biometrics recognition systems (CBRSs) for iris and face biometric templates are introduced. In the CBRS for face templates, the feature scale-invariant algorithm is employed on the face biometrics. Then, the DRPE technique is employed to cipher the resulted and extracted features to produce protected and encrypted face templates. In the CBRS for iris templates, the main features of both iris templates for the same user are extracted. After that, the resulted and extracted features are ciphered with the DRPE technique to generate the cancelable iris templates. The outcomes proved the appreciated performance of the two suggested CBRSs even in the existence of channel noise.

In [32], a steganography scheme based CBRS for iris templates is presented to preserve user verification and safeguard the original unique iris information for IoT remote access applications. The main benefit of the suggested CBRS is that it integrates the data steganography process to generate the cancelable biometric templates to mitigate the issue of traditional CBRSs that depend on random projection and permutation techniques that are dependent on key-dependent transforms. In [33], the authors combined the least significant bit-based steganography algorithm and two-fish and triple data encryption-based cryptography algorithm to resolve the challenge of tackling or surviving biometric templates for a mischievous action, which has grown to be a massive dilemma in the iris authentication and recognition frameworks. In the suggested iris authentication system, the rubber-sheet Daugman approach, Hough transform, and Gabor Log filter were employed for the normalization, feature extraction, and segmentation purposes of the iris images. Then, the created iris features are ciphered utilizing the two-fish and triple DES encryption techniques. After that, the resulted and ciphered biometric image is incorporated into a host secret image to generate a stego image utilizing the LSB based hiding technique. The key benefit of the suggested iris authentication scheme is that it incorporated two security levels (steganography and cryptography), and thus, it will be capable to resist intruders and attackers.

In [34], the authors suggested deep learning-based CBRS for biometric authentication in cloud computing services. The suggested CBRS achieved high accuracy and efficiency



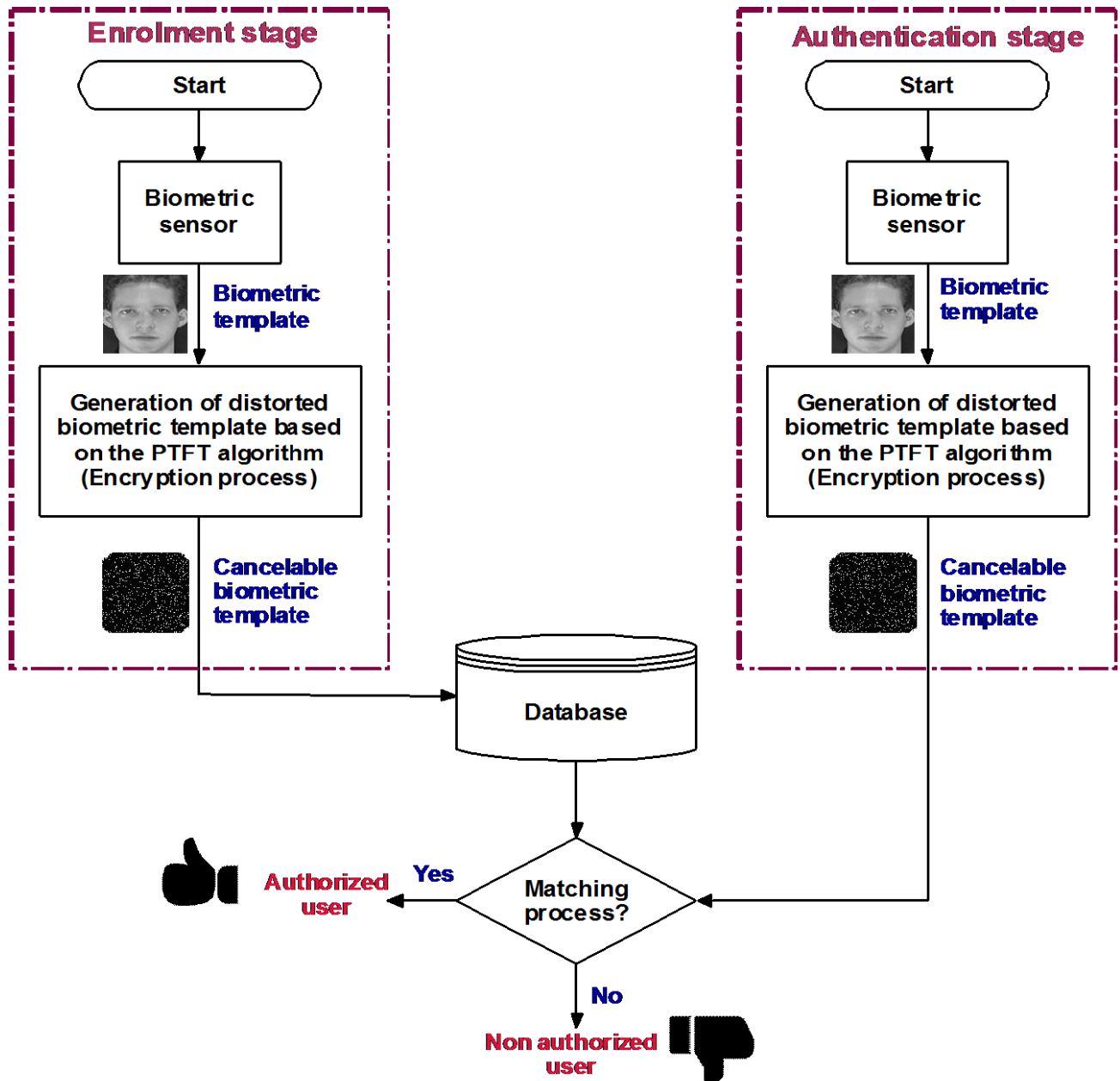


FIGURE 3. General flowchart of the suggested cancelable biometric recognition system.

to be a good solution for cloud-based biometric security systems achieving less computation. In [35], the authors introduced a CBRS for multi-biometric verification and authentication purposes. In the suggested CBRS, an efficient bit-wise ciphering algorithm is employed to transform a biometric image to a secured and cancelable biometric template utilizing a secret generated key from an alternative biometric image. The suggested CBRS completely maintains the bit errors number in the protected and original biometric templates to guarantee recognition efficacy corresponding to the unprotected framework performance. The comparison findings with the literature biometric security techniques on

numerous iris and face databases demonstrated that the suggested CBRS provided a good and significant recognition efficiency, whilst it delivered a high-level authentication and protection.

Although more mathematical transformations and encryption schemes have been introduced for achieving efficient and secure CBRS, however, many of these schemes fail to achieve authentication and confidentiality needs in the pilfered token situation and to be susceptible to turn into invertible with degraded accomplishment and efficiency. The key weaknesses identified in the associated CBRSs are as follows:

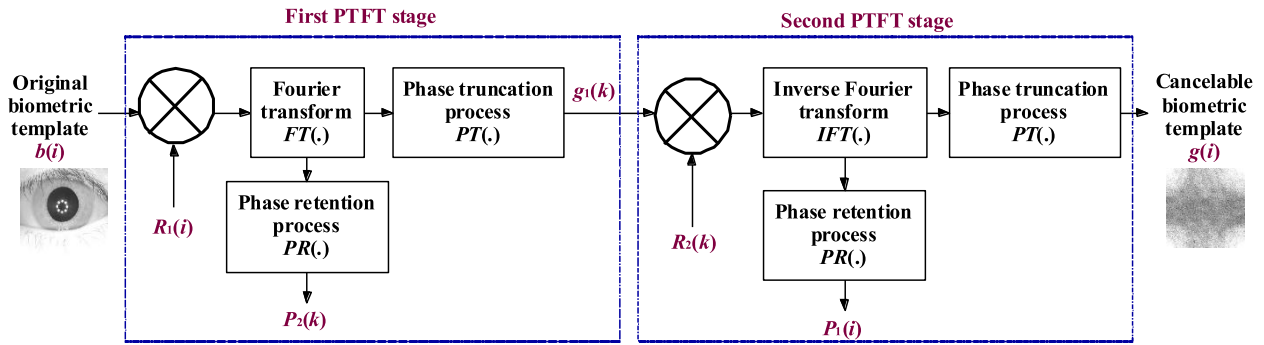


FIGURE 4. Block diagram of the suggested PTFT-based encryption algorithm.

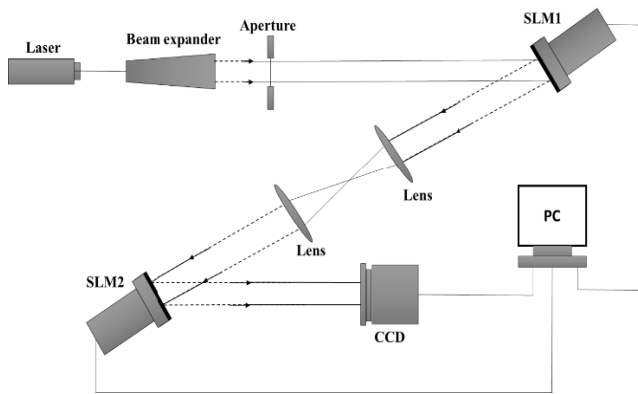


FIGURE 5. Optical implementation of the suggested PTFT algorithm.



FIGURE 6. Samples of nine faces of different persons of the first tested biometric dataset.



FIGURE 7. Samples of nine faces of different persons of the second tested biometric dataset.



FIGURE 8. Samples of nine ears of different persons of the third tested biometric dataset.

- Most of the reported cryptography-based CBRSs are simply depending on symmetric encryption schemes to generate the cancelable templates.
- No momentous progress is revealed in the estimated AROC curve and EER values (the extremely valuable security evaluation metrics in any CBRS) even in the recent related CBRSs.
- Almost related CBRSs assess their performance maximally on two or three biometric datasets for evaluation and investigation objectives.
- More security evaluation metrics and broad confidentiality assessments have not been considered and examined in detail in most of the related CBRSs.
- Almost related CBRSs did not consider the effect of the noise occurrence in their performance assessment investigations.
- The typical implementation time of the related CBRSs has not been studied.

Thus, in this work, we suggest a PTFT asymmetric cryptography algorithm for creating cancelable biometric images. The input biometric templates are ciphered using security keys that are considered two random independent phase operations (public keys) and are completely different from those of the deciphering keys (private keys) of another two random independent phase operations. Therefore, in the suggested

CBRS, the phase truncation process in the Fourier transform is exploited through utilizing the PTFT cryptography algorithm to generate cancelable templates with two arbitrary

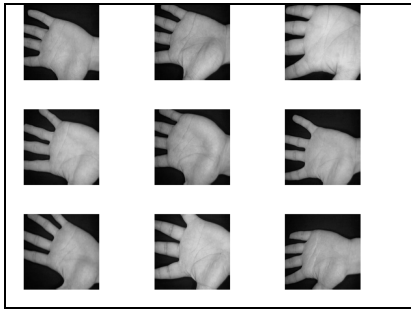


FIGURE 9. Samples of nine palmprints of different persons of the fourth tested biometric dataset.



FIGURE 10. Samples of nine fingerprints of different persons of the fifth tested biometric dataset.

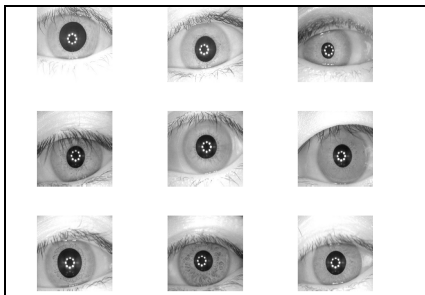


FIGURE 11. Samples of nine irises of different persons of the sixth tested biometric dataset.

public keys of phase truncated keys. The main contributions of the suggested CBRS algorithm are that:

- It has the nonlinear phase truncation feature that guarantees rich irrevocability and diversity to preserve greater security and robustness against intruders for the stored and distributed biometrics.
- The robustness performance of the suggested CBRS algorithm is tested on six different biometric datasets with numerous quality assessments and evaluation metrics such as visual ciphering inspection analysis, the impact of noise analysis, execution time analysis, PFD (Probability of False Distribution), EER, PTD (Probability of True Distribution), FAR, FRR, AROC, SSIM index, histogram analysis, correlation analysis.
- More comparison analyses are introduced to offer a broad evaluation of the potency of the suggested optical ciphering based CBRS algorithm against various possible attacks.

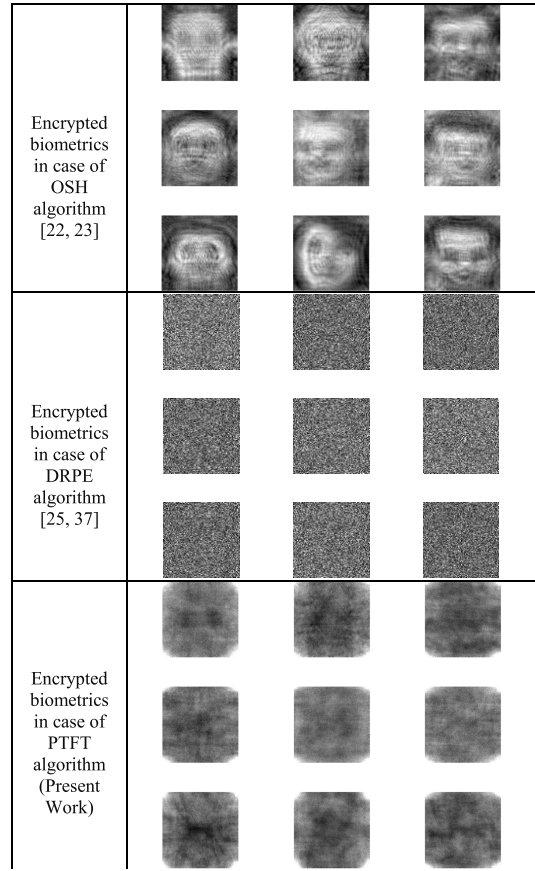


FIGURE 12. Results of the encrypted biometrics for the suggested PTFT algorithm contrasted to the literature OSH and DRPE algorithms for the first tested biometric dataset.

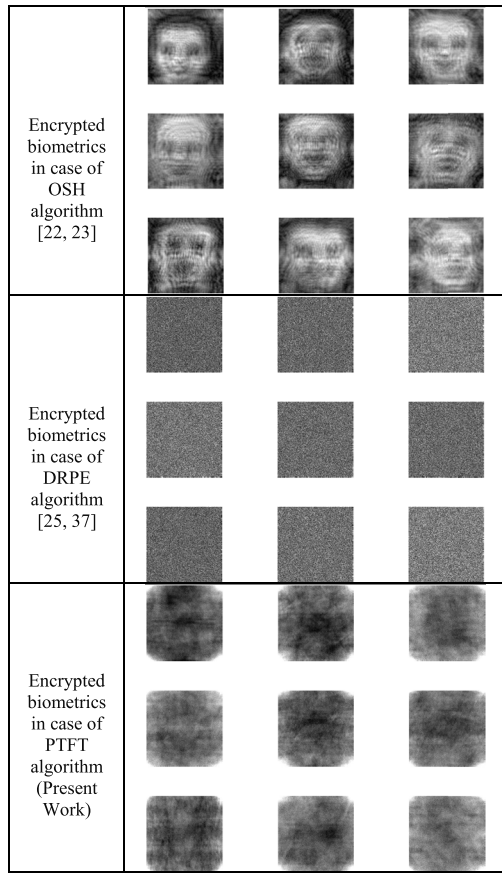
### III. PRELIMINARY STUDIES

The basics of the DRPE and OSH symmetric cryptography algorithms are described in this section.

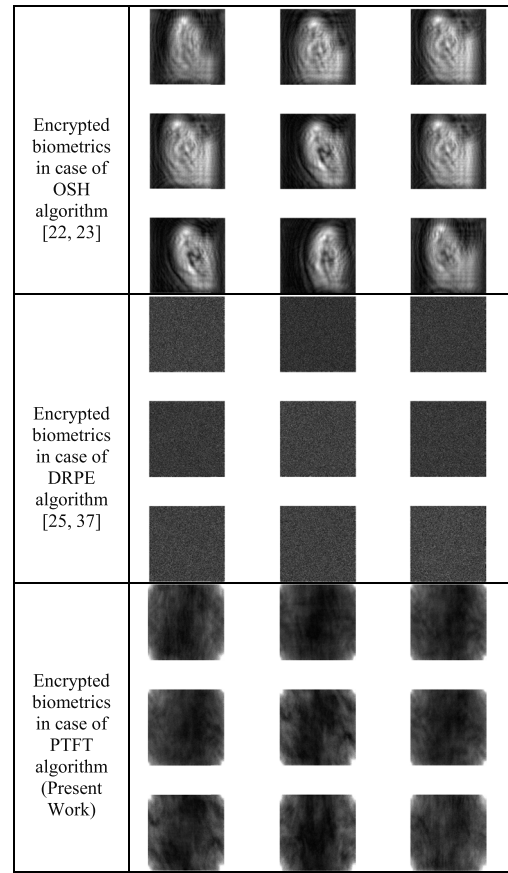
#### A. BASICS OF THE DRPE ENCRYPTION ALGORITHM

In 1995, Philippe *et al.* [36] suggested the optical Fourier transform-based DRPE algorithm. From that time, more optical cryptography algorithms have been developed precipitously. Various researchers have suggested other typical optical cryptography techniques based on the DRPE procedure, like the Fourier fractional transform-based DRPE algorithm [37], virtual optical cryptography algorithm [38], the DRPE algorithm based on Fresnel transform [39], and gyrator transformation based asymmetric cryptography algorithm [40].

The DRPE algorithm encompasses two random phase keys. One of these keys is deposited in the time domain and the other in the FT (Fourier transform) domain which applies the OFT (Optical Fourier Transform) as a superior optical biometric processing function. Thus, the DRPE algorithm setup is formed from two cascaded lenses for performing the OFT to the input biometric template object [25]. The DRPE algorithm is generally based on the modification of the spectral distribution of the input biometric template. The setup of the DRPE architecture depends on two Random



**FIGURE 13.** Results of the encrypted biometrics for the suggested PTFT algorithm contrasted with the literature OSH and DRPE algorithms for the second tested biometric dataset.



**FIGURE 14.** Results of the encrypted biometrics for the suggested PTFT algorithm contrasted with the literature OSH and DRPE algorithms for the third tested biometric dataset.

Phases (RP1 and RP2) in a  $4f$  imaging implementation as demonstrated in Fig. 1. The  $4f$  implementation comprises two cascaded lenses segregated by two focal lengths. Therefore, the operation of the DRPE algorithm can be discovered in three main steps:

1. The target biometric template is multiplied by the RP1 in the time domain for supplying the first adjustment to the target biometric template spectrum.
2. The target biometric template is then multiplied by the RP2 in the Fourier domain resulting in the second adjustment to the spectrum of the target biometric template.
3. An OFT is executed by the second lens to obtain the ciphered biometric template in 2D space.

**B. BASICS OF THE OSH ENCRYPTION ALGORITHM**

The OSH algorithm was firstly introduced by Korpel and Poon in [41]. The OSH is a formidable and fast scanning algorithm that utilizes a single-pixel sensor to capture the physical object hologram. The OSH can capture the dynamic scene and macroscopic holograms. So, it is a sufficient and fast scanning mechanism that does not have a strict restriction on the resolution and size of the captured hologram. The OSH algorithm has been employed in various applications such as

3D image recognition, scanning holographic microscopy, and cryptography systems [22], [23].

The optical scanning holography involves the principle of optical heterodyne scanning. So, the OSH is an electronic or digital scanning system that can interpret a 3D structure into 2D. The operation of this system involves active optical scanning and heterodyning [42]. Figure 2 illustrates a conventional system of the optical heterodyne scanning operation. Through the direction of the  $x$ - $y$  optical scanner, it is noticed that the collimated laser beam is projected to capture the target input biometric template stipulated by transparency  $\Gamma_o(x, y)$ . The light is converted to an electrical signal by the photodetector. This converted electrical signal comprises the processed data for the scanned biometric template. Then, the scanned electrical data is stored in a computer in a digital form and processed as a 2D digital image of the scanned input object. In Fig. 2, the  $i(x, y)$  is the biometric template to be encrypted, the PD is the photodetector, and the  $P(x, y)$  signifies the employed encryption key which is situated in the focal front plane of the lens ( $L_1$ ) with a focal length  $f$ . This key is illustrated by the laser wider beams with a temporal frequency of  $\omega_0$ . The encryption key is exploited to adjust the scanning beam shape in the operation of the OSH algorithm to provide the encrypted biometric template.



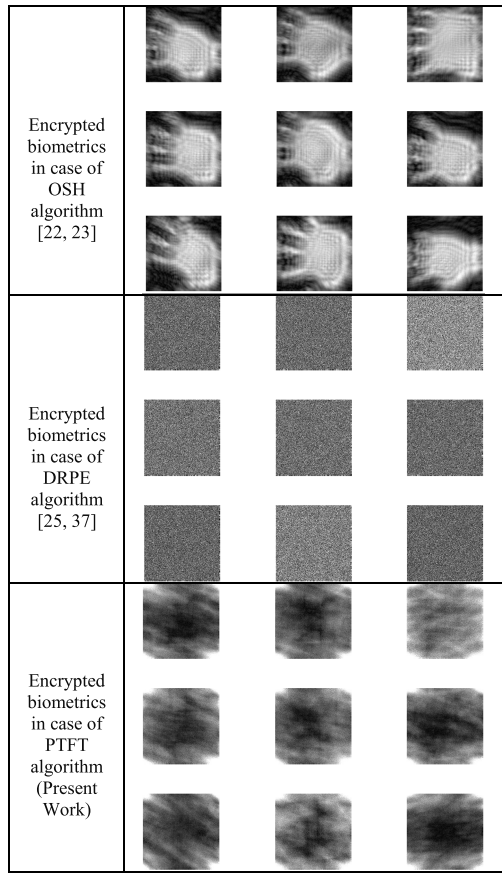


FIGURE 15. Results of the encrypted biometrics for the suggested PTFT algorithm contrasted with the literature OSH and DRPE algorithms for the fourth tested biometric dataset.

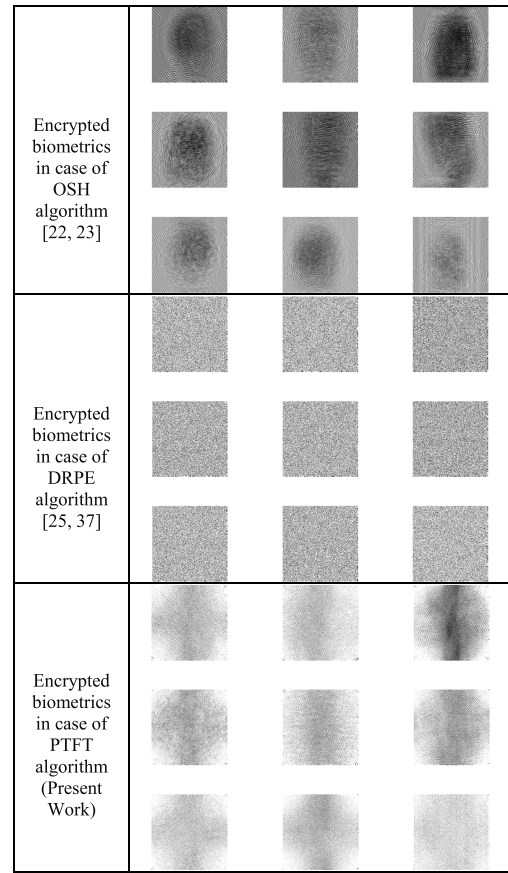


FIGURE 16. Results of the encrypted biometrics for the suggested PTFT algorithm contrasted with the literature OSH and DRPE algorithms for the fifth tested biometric dataset.

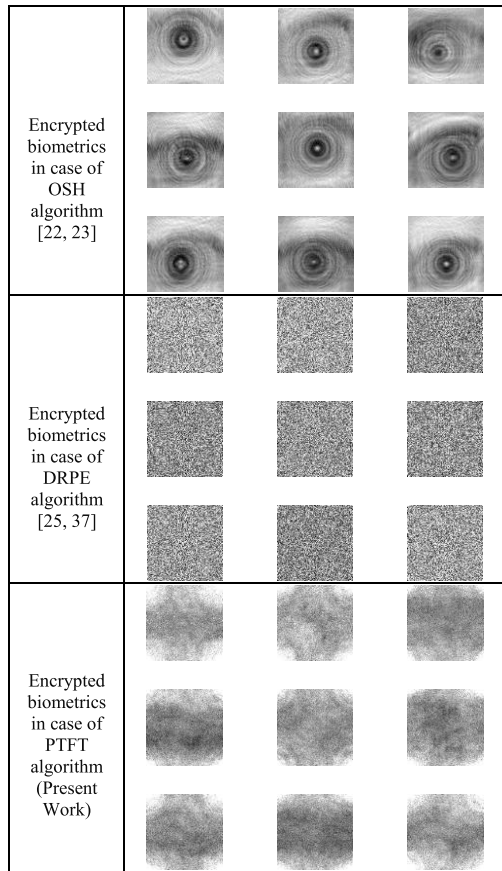
**IV. PROPOSED OPTICAL PTFT CRYPTOGRAPHY ALGORITHM BASED CBRS**

Targeting the challenge of guarantee distribution, storage, and transmission of biometric templates based on optical encryption and transformation, an inventive CBRS is suggested based on optical PTFT asymmetric cryptography algorithm. The suggested algorithm for biometric images focuses on the problem of key distribution with improved confidence and privacy in the optical cryptography procedure. In the suggested CBRS, the cryptography keys for the biometric templates incorporate optically generated keys of random phase masks of the PTFT algorithm. Therefore, if an authorized person tries to retrieve the plain biometric templates at the receiver side, the suggested system will satisfy the standards of asymmetric encryption with biometric data validation and authentication methodology.

The general flowchart of the suggested CBRS is presented in Fig. 3. The suggested system involves two modules: the authentication module and the enrolment module. In the enrolment stage, a user introduces her/his biometric to the biometric sensor to generate the biometric image. Afterward, the suggested PTFT cryptography algorithm is employed to generate the distorted and cancelable biometric image. Thereafter, the obtained cancelable biometric image is stored in the

database in a distorted form instead of an original form. In the authentication stage, the cancelable distorted biometric image is acquired through the same steps of the enrolment stage by utilizing the suggested PTFT cryptography algorithm. At the last step, a verification process is executed using a matching procedure which is performed among the already collected and distorted biometric images that are accumulated in the biometric server and the obtained cancelable biometric images from the authentication stage.

The most important feature of the suggested PTFT cryptography system is that it is an asymmetric ciphering process, where there are two different keys for the ciphering/deciphering processes. Therefore, during the authentication stage, if an imposter user knows the encryption key and the encrypted biometric template, it will still be challenging to reclaim the plain biometric template, forcing such an estimation infeasible. So, the optical PTFT cryptosystem is a one-way strategy. This terrific characteristic of the suggested algorithm has motivated us to employ it for achieving a robust and secure cancelable biometric recognition system. The PTFT procedure employs the Fourier transform of the input biometric image with the process of phase truncation, where the modular amplitude component of the FT spectrum is only utilized. Therefore, the amplitude (modular element) of the Fourier spectrum is only exploited, whereas the phase



**FIGURE 17.** Results of the encrypted biometrics for the suggested PTFT algorithm contrasted with the literature OSH and DRPE algorithms for the sixth tested biometric dataset.

component is amputated. The simple and effective mathematical model of the PTFT procedure that will be utilized in our suggested CBRS is discussed as follows.

Suppose the plain biometric template to be encrypted is denoted as  $b(i)$ ,  $FT$  is the FT operator,  $IFT$  is the inverse FT,  $PT$  is the phase truncation operator, and  $PR$  is the phase retention operator. So, the FT of the plain biometric image is given as:

$$F(k) = FT[b(i)] = |F(k)| \exp(j2\pi\phi(k)) \quad (1)$$

The phase retention is expressed as:

$$PR[F(k)] = \exp(j2\pi\phi(k)) \quad (2)$$

The phase truncation is provided as:

$$PT[F(k)] = |F(k)| \quad (3)$$

From this PTFT procedure, the suggested block diagram of the PTFT ciphering process is demonstrated in Fig. 4. It is noticed that the PTFT cryptography algorithm is similar to the DRPE cryptography algorithm, where both of them utilize a couple of random independent phase masks  $R_1(i)$  and  $R_2(k)$  as ciphering keys. But the proposed PTFT asymmetric cryptography algorithm removes the linear features of the optical symmetric cryptography algorithm through its great feature of the phase truncation nonlinear operation.

The ciphered cancelable biometric image  $g(i)$  can be acquired by Eqs. (4) and (5). In the same way, the subsequent supplementary two steps given by Eqs. (6) and (7) must also be accomplished to create a couple of random phase keys that are served as deciphering private keys  $P_1(i)$  and  $P_2(k)$ . So, the ciphering public keys  $R_1(i)$  and  $R_2(k)$  are different from the deciphering private keys  $P_1(i)$  and  $P_2(k)$ .

$$g_1(k) = PT[FT(b(i).R_1(i))] \quad (4)$$

$$g(i) = PT[IFT(g_1(k).R_2(k))] \quad (5)$$

$$P_2(k) = PR[FT(b(i).R_1(i))] \quad (6)$$

$$P_1(i) = PR[IFT(g_1(k).R_2(k))] \quad (7)$$

It is observed from Eqs. (4) – (7) that the  $g_1(k)$ ,  $g(i)$  and  $P_2(k)$ ,  $P_1(i)$  have straightforward and uncomplicated computations. So, it is demonstrated that:

$$g_1(k)P_2(k) = FT(b(i).R_1(i)) \quad (8)$$

$$g(i)P_1(i) = FT(g_1(k).R_2(k)) \quad (9)$$

Figure 4 and Eqs. (4) – (7) can be modified and rearranged to be employed for the deciphering process, but this is not required for cancelable biometric recognition systems as exhibited in Fig. 3, where the authentication procedure is presented in the ciphered domain. Because the ciphering keys are different from the deciphering keys in the PTFT asymmetric cryptography algorithm, the ciphering process cannot be inverted with the ciphering keys as the process of the phase truncation provides a one-way operation. Therefore, the deciphering process can be accomplished only by utilizing the private deciphering keys  $P_1(i)$  and  $P_2(k)$ . Thence, if the genuine user tries to repossess the plain biometric image from the ciphered one without having deciphering keys or even with having the ciphering keys, he will not succeed because of the nature of the PTFT asymmetric cryptography algorithm which is a one-way phase truncation operation. So, the PTFT cryptography algorithm is very robust and secure for biometric recognition applications.

As the PTFT asymmetric ciphering process is realized digitally as shown in Fig. 4, it can be applied in optics by utilizing certain optoelectronic devices. So, the phase truncation process can be simply performed using a CCD detector. Also, the phase retention process can be straightforwardly achieved utilizing the advantage of holographic recording and retrieved with the interferometry of the phase-shifting process. The optical implementation of the PTFT asymmetric ciphering algorithm is demonstrated in Fig. 5. This optical setup consists of a laser, a beam expander with aperture, two SLMs, CCD, a  $4f$  imaging system, and a computer (PC). The SLM1 is utilized as space amplitude-modulated light modulator, while the SLM2 is employed as a space phase-modulated light modulator. The objective of using the  $4f$  imaging model with a lens is to facilitate the optical contact between the employed two SLMs. The PC is utilized to control the CCD and the two SLMs.

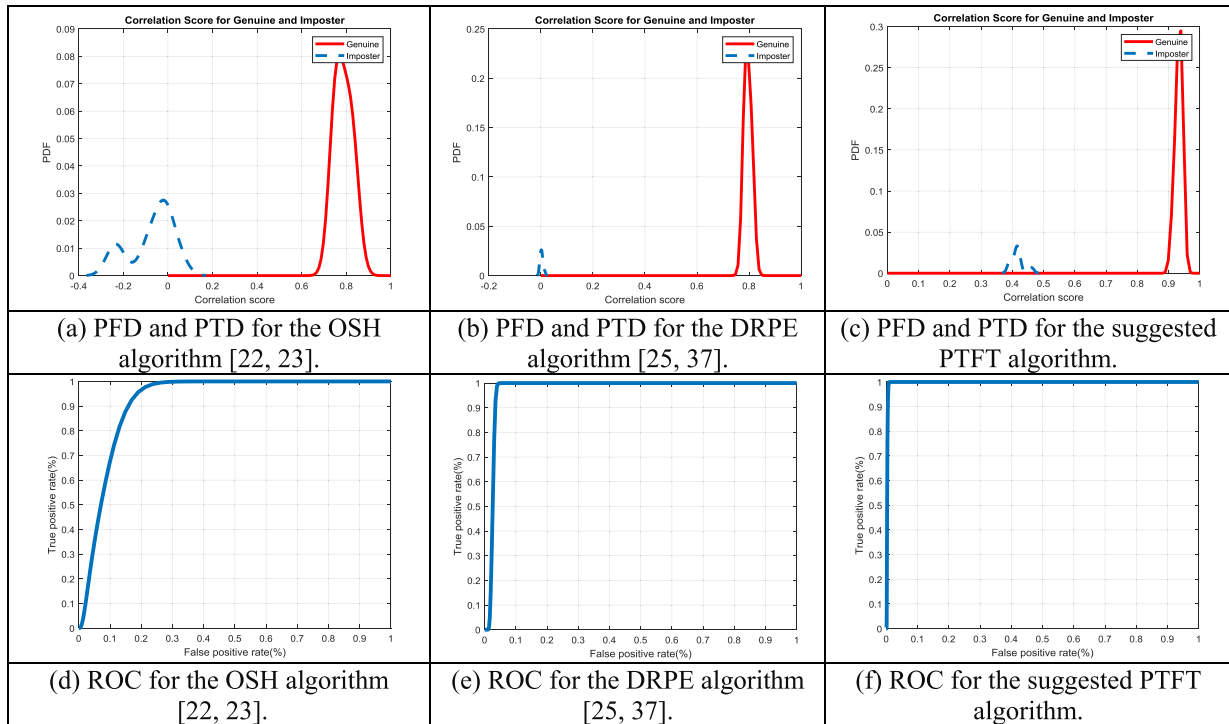


FIGURE 18. PFD, PTD, and ROC for the suggested PTFT algorithm contrasted with the literature OSH and DRPE algorithms of the first tested biometric dataset.

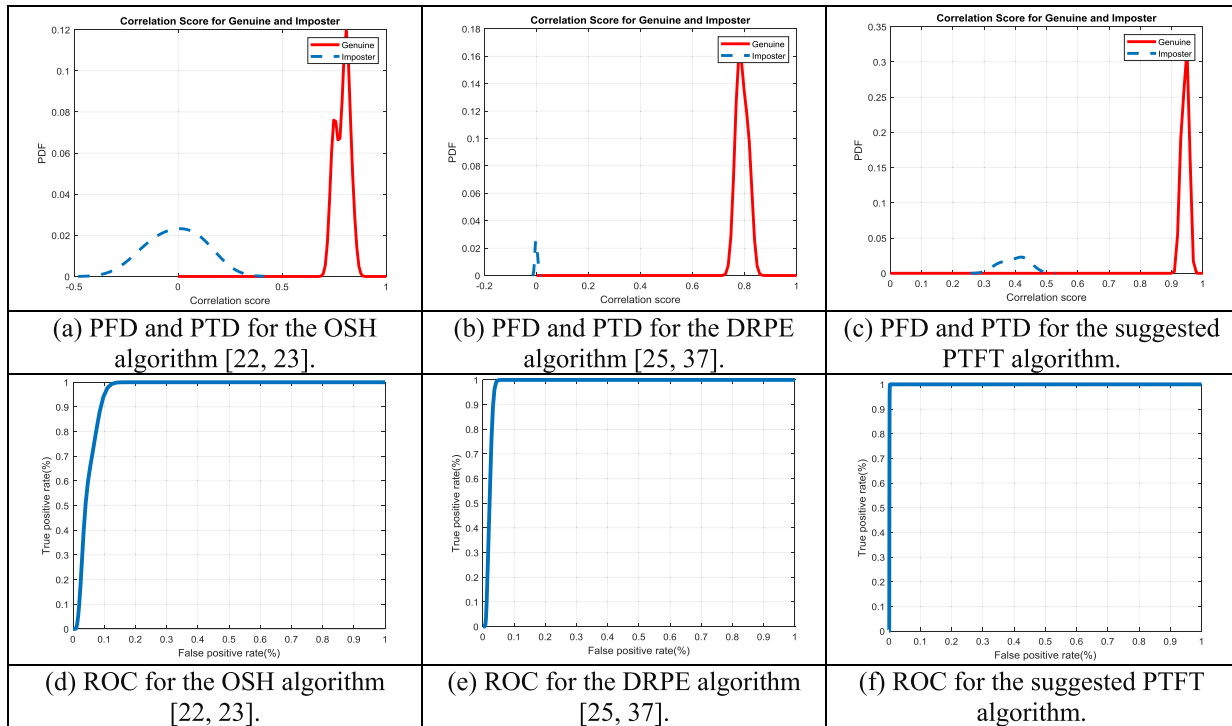


FIGURE 19. PFD, PTD, and ROC for the suggested PTFT algorithm contrasted with the literature OSH and DRPE algorithms of the second tested biometric dataset.

### V. SIMULATION RESULTS AND COMPARATIVE ANALYSIS

More simulation assessments are carried out and performed in this section to clarify and test the impact of employing

the suggested CBRS based on the optical PTFT asymmetric encryption algorithm. In the simulation tests, we utilize different samples of biometric datasets that demonstrate

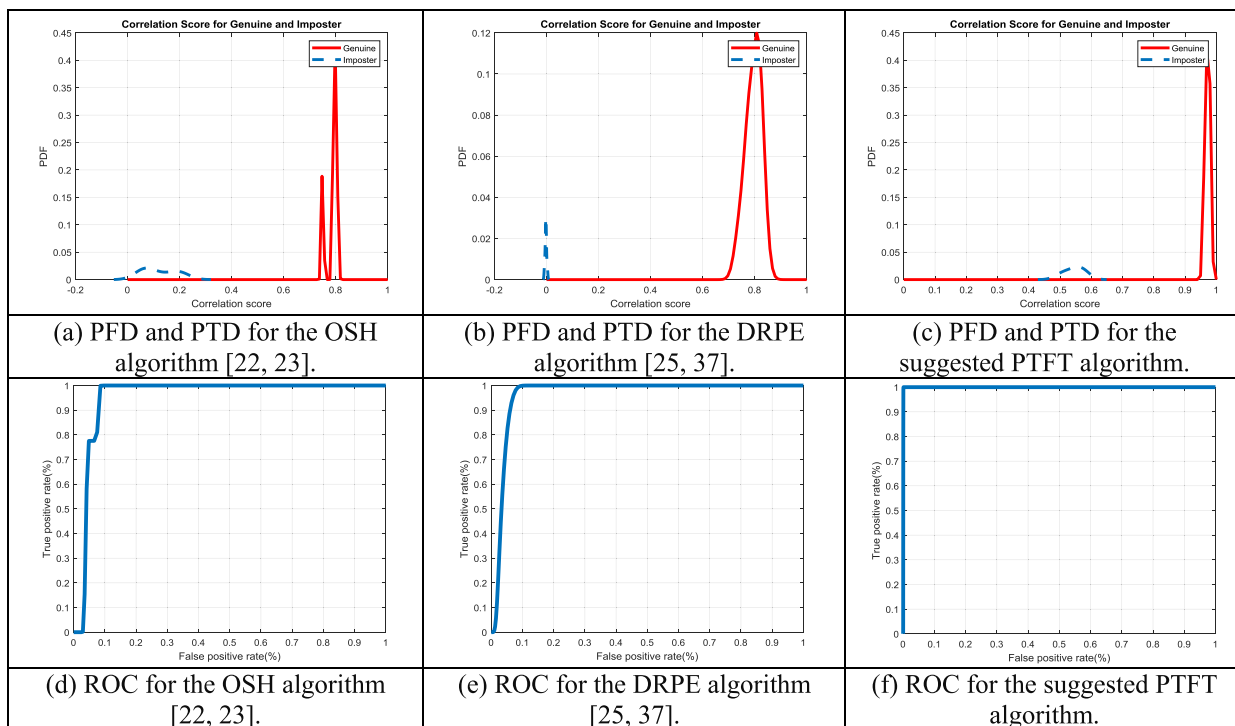


FIGURE 20. PFD, PTD, and ROC for the suggested PTFT algorithm contrasted with the literature OSH and DRPE algorithms of the third tested biometric dataset.

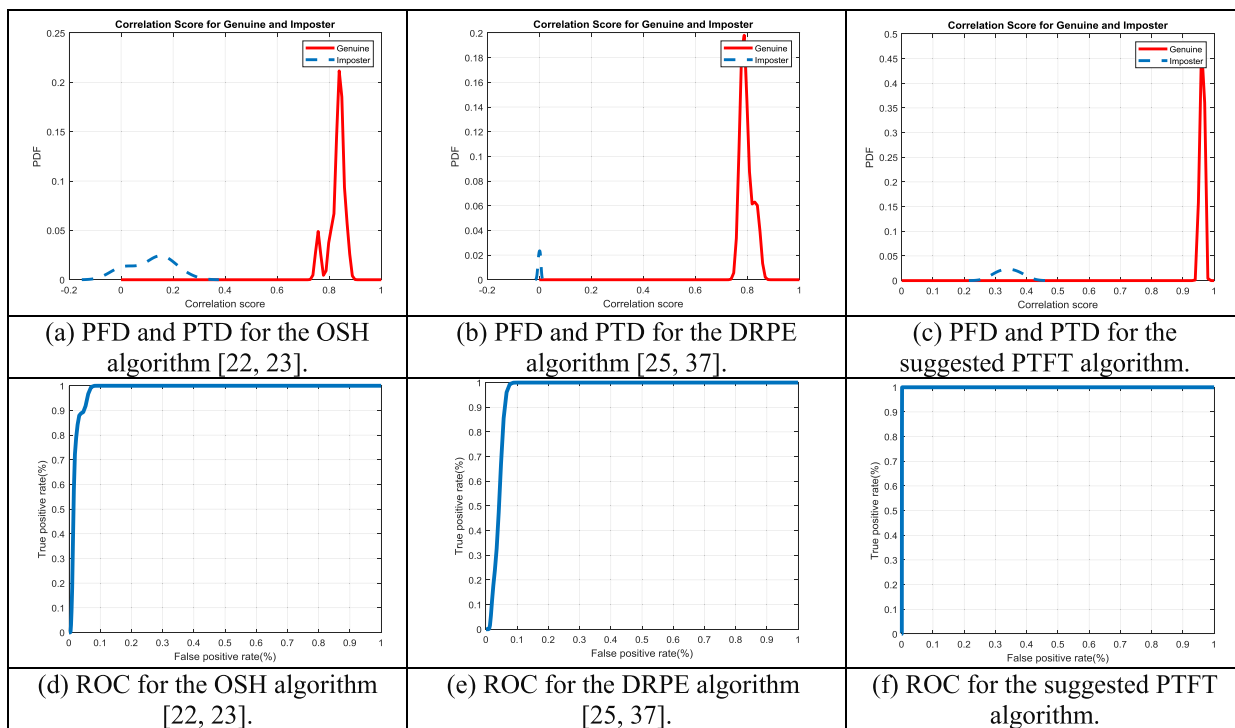
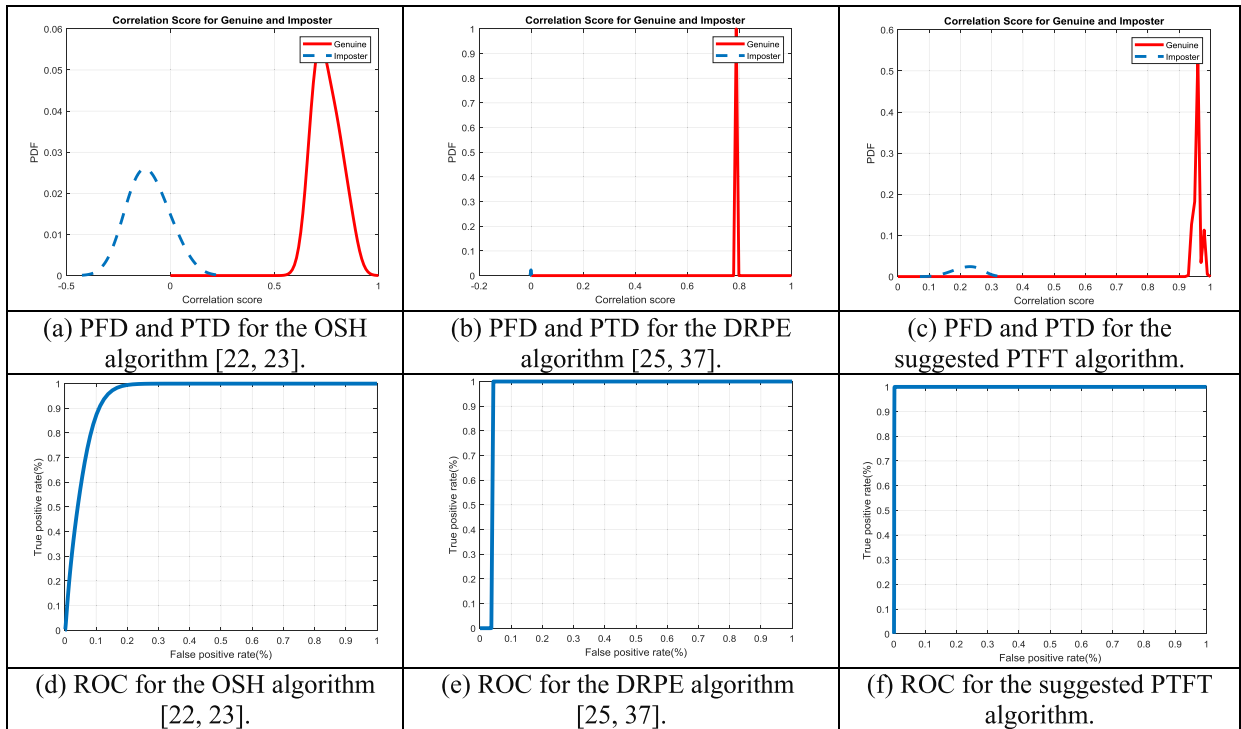


FIGURE 21. PFD, PTD, and ROC for the suggested PTFT algorithm contrasted with the literature OSH and DRPE algorithms of the fourth tested biometric dataset.

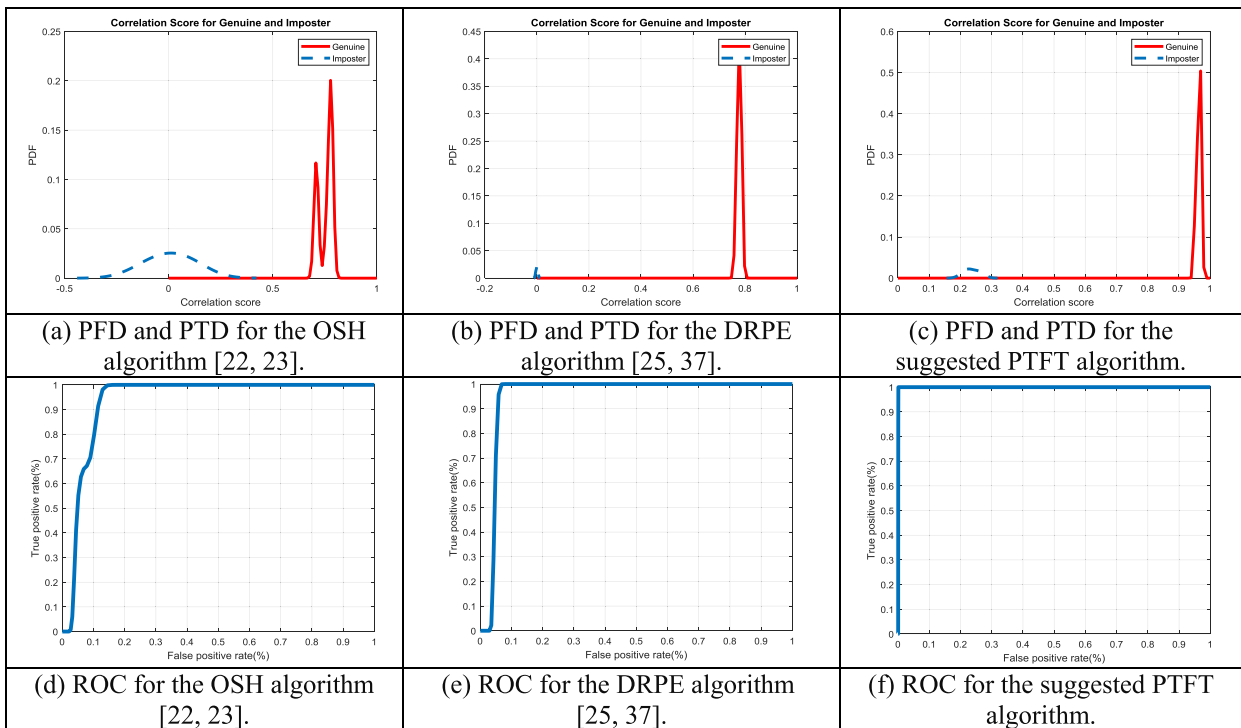
properties anticipated in concrete application situations for instance lightings, contrasting backgrounds, and motion [43]–[48]. Two samples of biometric datasets of faces are used. Also, one sample biometric dataset of each ear, palm-print, fingerprint, and iris are investigated.

For simplicity, only nine different biometric images of different persons of each tested biometric dataset are introduced as given in Figs. 6–11. Consequently, six various experimental cases for the examined biometric datasets are assessed. In every simulated case, the tested biometrics are





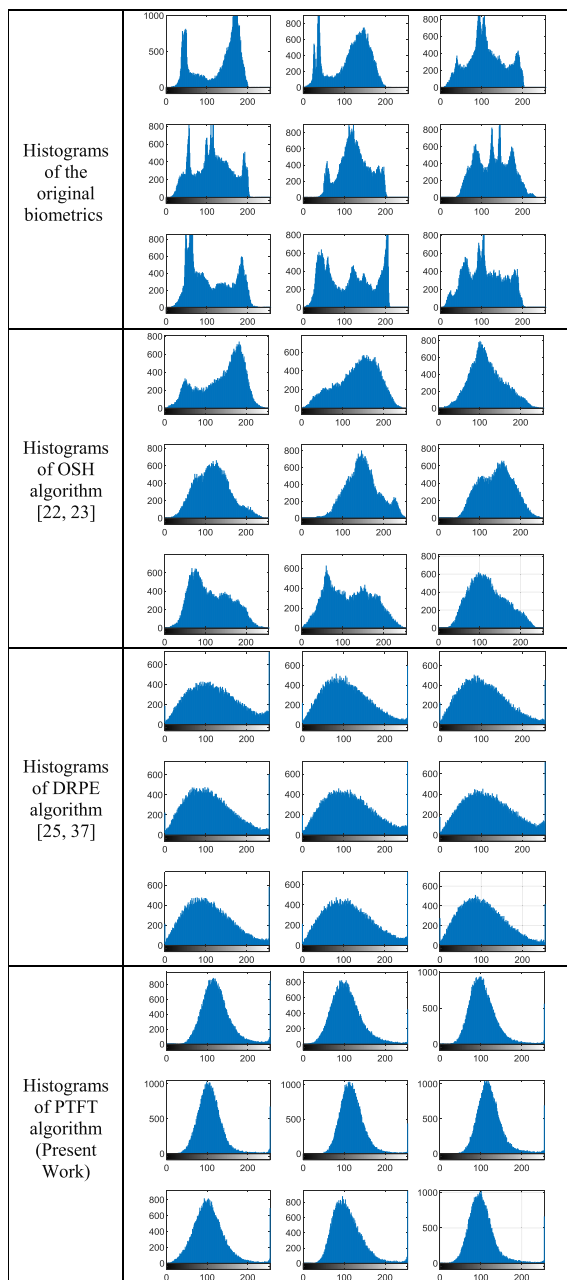
**FIGURE 22.** PFD, PTD, and ROC for the suggested PTFT algorithm contrasted with the literature OSH and DRPE algorithms of the fifth tested biometric dataset.



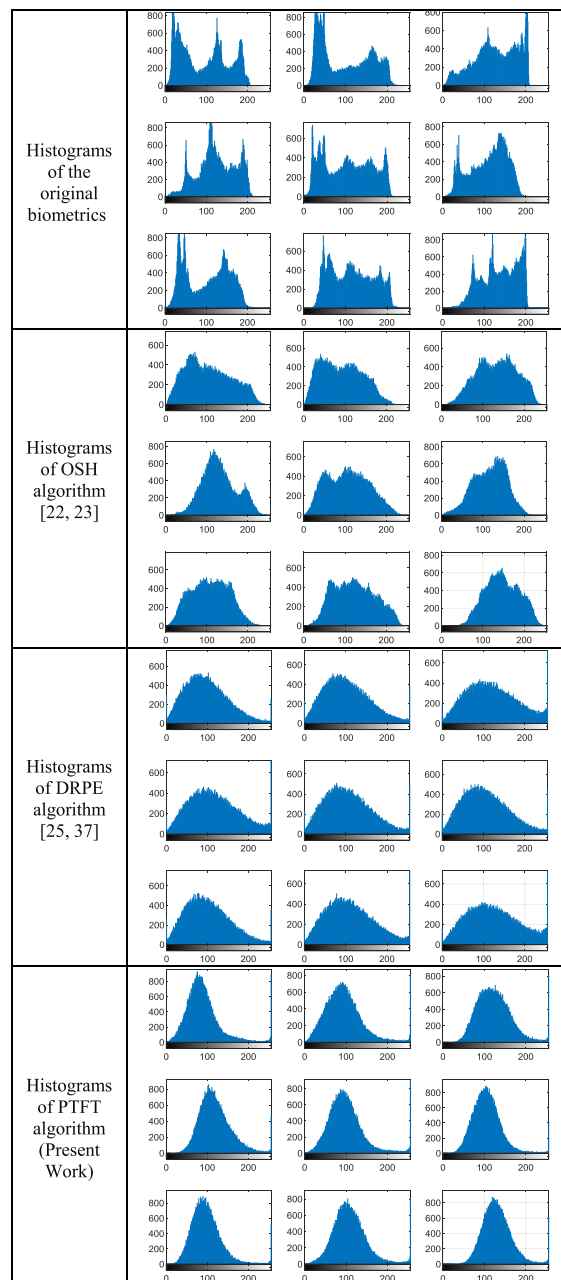
**FIGURE 23.** PFD, PTD, and ROC for the suggested PTFT algorithm contrasted with the literature OSH and DRPE algorithms of the sixth tested biometric dataset.

encrypted with the suggested optical PTFT encryption algorithm. For each tested experiment, more simulations and experiments are investigated. Different evaluation metrics

are employed to measure the performance efficiency of the suggested CBRS such as visual inspection, execution time, PFD, EER, FAR, PTD, FRR, SSIM, AROC, histogram, and



**FIGURE 24.** Histograms of the original biometrics and the encrypted biometrics for the suggested PTFT algorithm contrasted with the literature OSH and DRPE algorithms for the first tested biometric dataset.



**FIGURE 25.** Histograms of the original biometrics and the encrypted biometrics for the suggested PTFT algorithm contrasted with the literature OSH and DRPE algorithms for the second tested biometric dataset.

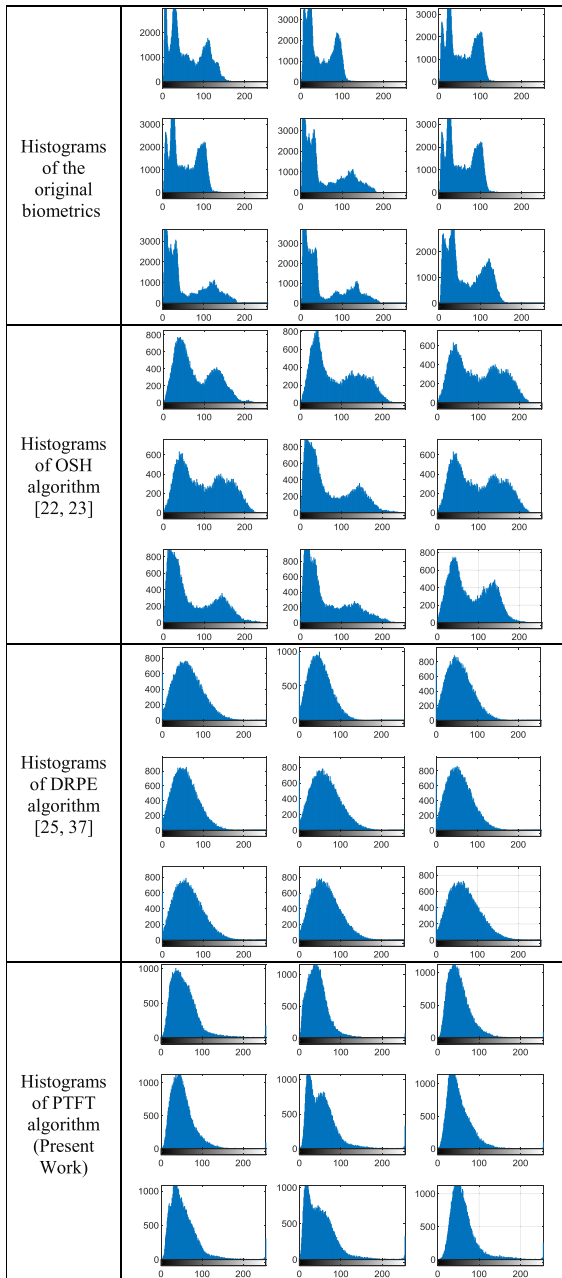
correlation coefficient. But for simplicity, the results of only nine encrypted biometrics are presented in this section to evaluate and confirm the cancelability accomplishment and efficiency of the suggested optical PTFT encryption algorithm. The achievement of the suggested PTFT asymmetric algorithm based CBRS is compared with the optical OSH and DRPE symmetric encryption algorithms based CBRSs [22], [23], [25], [37].

In the next sub-sections, the proposed CBRS algorithm is evaluated in terms of different eight perspectives: (A) Visual encryption analysis, (B) PFD, PTD, and ROC analysis, (C),

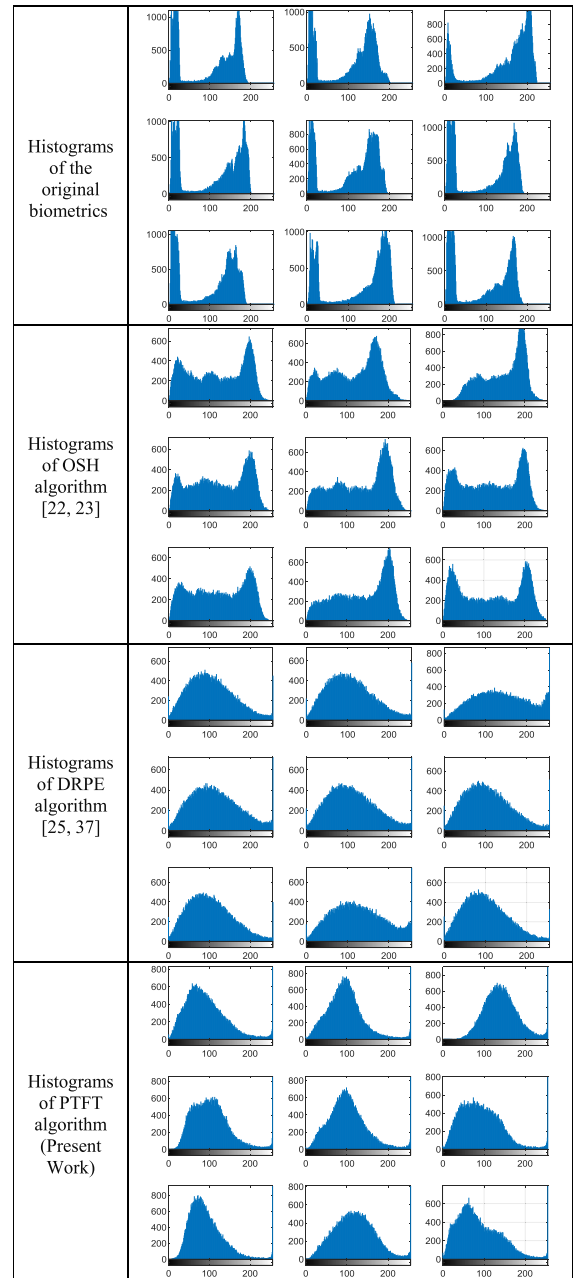
Histogram security analysis, (D) Correlation and SSIM analysis, (E) EER, FAR, FRR, and AROC analysis, (F) Computational processing analysis, (G) Noise analysis, and (H) Comparative analysis.

**A. VISUAL ENCRYPTION ANALYSIS**

In this section, the objective is to justify and investigate the encryption effectiveness of the suggested optical PTFT cryptography algorithm. Figures 12–17 present the encrypted biometrics for the suggested optical PTFT encryption algorithm contrasted to the literature optical OSH and DRPE



**FIGURE 26.** Histograms of the original biometrics and the encrypted biometrics for the suggested PTFT algorithm contrasted with the literature OSH and DRPE algorithms for the third tested biometric dataset.



**FIGURE 27.** Histograms of the original biometrics and the encrypted biometrics for the suggested PTFT algorithm contrasted with the literature OSH and DRPE algorithms for the fourth tested biometric dataset.

encryption algorithms [22], [23], [25], [37] of all tested biometric datasets.

For the six examined and tested biometric cases, it is observed that the suggested algorithm is advised and recommended for effective encryption and cancelable template recognition systems contrasted to the traditional optical OSH and DRPE encryption algorithms [22], [23], [25], [37]. It is demonstrated and recognized that the suggested algorithm accomplishes complete encryption and distortion of the plain biometric features to be safely stored in the protected storage server, which supports counteract unapproved access to the biometric information.

### B. PFD, PTD, AND ROC ANALYSIS

Moreover, to well recognize the simulation outcomes, the results are additionally clarified through the ROC measurements. Precisely, the FAR versus the FRR is studied as in [24], [25]. The FRR characterizes the proportion of genuine tests misinterpreted and understood as being impostors, whilst the FAR signifies the misclassified imposters as being genuine. Furthermore, the PFD and PTD probabilities of the genuine and imposter correlation coefficients are tested to buttress the evaluation of the suggested CBRS.

**TABLE 1.** False and true correlation and SSIM for the sample nine templates for the first tested biometric dataset.

The nine templates of the first biometric dataset	Correlation/SSIM with false face			Correlation/SSIM with true face		
	OSH [22, 23]	DRPE [25, 37]	PTFT (Present Work)	OSH [22, 23]	DRPE [25, 37]	PTFT (Present Work)
Face1	0.4219/0.1265	0.0049/0.0819	-0.0186/0.0148	0.8290/0.4714	0.8157/0.7750	0.9378/0.9742
Face2	0.4144/0.0968	0.0051/0.07180	-0.0315/0.0173	0.8105/0.5561	0.7876/0.7760	0.9419/0.9683
Face3	0.4102/0.1450	0.0007/0.0832	0.0489/0.0116	0.7582/0.4097	0.7838/0.7762	0.9315/0.9675
Face4	0.4159/0.1279	-0.0040/0.0872	-0.0119/0.0066	0.7580/0.4805	0.7894/0.7548	0.9264/0.9690
Face5	0.3908/0.1398	-0.0008/0.0869	-0.0992/0.0057	0.7443/0.4069	0.8044/0.7670	0.9118/0.9717
Face6	0.3911/0.1209	0.0141/0.0717	-0.2253/0.0215	0.7478/0.4636	0.8109/0.7983	0.9238/0.9736
Face7	0.4221/0.1122	0.0015/0.0882	-0.0716/0.0086	0.8050/0.4808	0.7890/0.7573	0.9444/0.9690
Face8	0.4617/0.1147	-0.0039/0.0873	-0.2240/0.0124	0.8392/0.4195	0.8001/0.7425	0.9439/0.9711
Face9	0.4090/0.1380	0.0051/0.0932	0.0004/0.0198	0.7773/0.4425	0.7784/0.7479	0.9311/0.9669
Average	<b>0.4152/0.1246</b>	<b>0.0025/0.0834</b>	<b>-0.0726/0.0013</b>	<b>0.7855/0.4590</b>	<b>0.7955/0.7649</b>	<b>0.9325/0.9701</b>

**TABLE 2.** False and true correlation and SSIM for the sample nine templates for the second tested biometric dataset.

The nine templates of the second biometric dataset	Correlation/SSIM with false face			Correlation/SSIM with true face		
	OSH [22, 23]	DRPE [25, 37]	PTFT (Present Work)	OSH [22, 23]	DRPE [25, 37]	PTFT (Present Work)
Face1	0.4501/0.1097	-0.1929/0.0889	-0.0039/0.0125	0.8387/0.4905	0.7618/0.7315	0.9505/0.9633
Face2	0.4307/0.1076	-0.1185/0.0885	0.0034/0.0131	0.8089/0.4950	0.7778/0.7447	0.9565/0.9665
Face3	0.3612/0.1364	0.0741/0.0734	0.0074/0.0159	0.7987/0.4478	0.8147/0.7955	0.9461/0.9744
Face4	0.3866/0.1322	0.0444/0.0720	-0.0045/0.0040	0.7553/0.4620	0.8059/0.7928	0.9400/0.9725
Face5	0.4185/0.1076	-0.0276/0.0872	-0.0001/0.0074	0.7373/0.5336	0.7859/0.7661	0.9530/0.9675
Face6	0.4219/0.1151	-0.1055/0.0870	-0.0052/0.0049	0.7847/0.4990	0.7805/0.7579	0.9290/0.9671
Face7	0.4126/0.1015	-0.0240/0.0901	-0.0023/0.0106	0.8108/0.5634	0.7729/0.7415	0.9366/0.9650
Face8	0.3363/0.1326	0.1246/0.0792	0.0022/0.0088	0.8145/0.4729	0.7963/0.7782	0.9493/0.9703
Face9	0.3536/0.1426	0.1279/0.0698	-0.0005/0.0059	0.7534/0.4622	0.8233/0.8084	0.9285/0.9754
Average	<b>0.3969/0.1205</b>	<b>-0.0108/0.0817</b>	<b>-0.0004/0.0092</b>	<b>0.7892/0.4918</b>	<b>0.7910/0.7684</b>	<b>0.9433/0.9691</b>

**TABLE 3.** False and true correlation and SSIM for the sample nine templates for the third tested biometric dataset.

The nine templates of the third biometric dataset	Correlation/SSIM with false ear			Correlation/SSIM with true ear		
	OSH [22, 23]	DRPE [25, 37]	PTFT (Present Work)	OSH [22, 23]	DRPE [25, 37]	PTFT (Present Work)
Ear1	0.5773/0.1155	0.1448/0.1059	0.0034/0.0174	0.7491/0.4346	0.8127/0.5341	0.9760/0.9243
Ear2	0.5093/0.1050	0.1003/0.0970	-0.0026/0.0134	0.7934/0.4597	0.7411/0.4343	0.9624/0.8856
Ear3	0.5238/0.1121	0.0623/0.1085	-0.0030/0.0182	0.7918/0.4677	0.7752/0.4780	0.9665/0.9072
Ear4	0.4967/0.1121	0.0624/0.1022	-0.0031/0.0109	0.7919/0.4644	0.7797/0.4761	0.9658/0.9245
Ear5	0.5461/0.1015	0.1949/0.1025	-0.0008/0.0152	0.8072/0.4462	0.8134/0.5214	0.9777/0.9083
Ear6	0.5578/0.1121	0.0625/0.1043	-0.0052/0.0145	0.7510/0.4627	0.7776/0.4857	0.9674/0.9255
Ear7	0.5436/0.1015	0.1947/0.1020	-0.0021/0.0148	0.8020/0.4453	0.8146/0.5067	0.9761/0.9254
Ear8	0.5675/0.0860	0.2052/0.0927	-0.0077/0.0094	0.7967/0.4293	0.8119/0.5213	0.9803/0.9323
Ear9	0.5814/0.1104	0.0734/0.1064	-0.0006/0.0163	0.7971/0.4395	0.8314/0.5672	0.9749/0.9076
Average	<b>0.5448/0.1062</b>	<b>0.1223/0.1023</b>	<b>-0.0025/0.0144</b>	<b>0.7867/0.4499</b>	<b>0.7953/0.5027</b>	<b>0.9719/0.9156</b>

**TABLE 4.** False and true correlation and SSIM for the sample nine templates for the fourth tested biometric dataset.

The nine templates of the fourth biometric dataset	Correlation/SSIM with false palmprint			Correlation/SSIM with true palmprint		
	OSH [22, 23]	DRPE [25, 37]	PTFT (Present Work)	OSH [22, 23]	DRPE [25, 37]	PTFT (Present Work)
Palmprint1	0.3172/0.1129	0.0509/0.0823	0.0042/0.0137	0.7813/0.4800	0.8477/0.7384	0.9672/0.9671
Palmprint2	0.3836/0.1318	0.1266/0.0772	-0.0023/0.0132	0.7885/0.4590	0.8048/0.7583	0.9600/0.9683
Palmprint3	0.3589/0.1188	0.1245/0.0630	0.0016/0.0105	0.8420/0.4833	0.7572/0.8385	0.9521/0.9794
Palmprint4	0.3443/0.1220	0.1673/0.0843	0.0046/0.0163	0.8046/0.4935	0.8395/0.7435	0.9610/0.9720
Palmprint5	0.3841/0.1297	0.1566/0.0840	-0.0013/0.0094	0.7958/0.4645	0.8305/0.7576	0.9617/0.9707
Palmprint6	0.3307/0.1079	-0.0082/0.0855	0.0020/0.0123	0.7850/0.4895	0.8478/0.7219	0.9658/0.9678
Palmprint7	0.3497/0.1296	0.2332/0.0860	0.0055/0.0137	0.7778/0.5000	0.8430/0.7067	0.9539/0.9659
Palmprint8	0.3045/0.1335	0.1736/0.0691	-0.0058/0.0068	0.8257/0.5097	0.8286/0.8089	0.9652/0.9767
Palmprint9	0.2970/0.1039	0.0043/0.0800	-0.0020/0.0054	0.7706/0.4803	0.8684/0.7046	0.9684/0.9645
Average	<b>0.3411/0.1211</b>	<b>0.1143/0.0790</b>	<b>0.0007/0.0112</b>	<b>0.7968/0.4844</b>	<b>0.8297/0.7531</b>	<b>0.9617/0.9702</b>

Figures 18–23 display the results of the PFD, PTD, and ROC curves of the verification process for the suggested optical PTFT encryption algorithm contrasted to the literature optical OSH and DRPE encryption algorithms of the whole

examined biometric datasets. These curves define the error probability and threshold values in the verification process, where the threshold value is determined by indicating the intersection point amongst the curves of PFD and PTD. This



**TABLE 5.** False and true correlation and SSIM for the sample nine templates for the fifth tested biometric dataset.

The nine templates of the fifth biometric dataset	Correlation/SSIM with false fingerprint			Correlation/SSIM with true fingerprint		
	OSH [22, 23]	DRPE [25, 37]	PTFT (Present Work)	OSH [22, 23]	DRPE [25, 37]	PTFT (Present Work)
Fingerprint1	0.2224/0.0993	-0.1430/0.0354	-0.0032/0.0031	0.7422/0.6837	0.7952/0.8887	0.9570/0.9827
Fingerprint2	0.1870/0.0884	-0.0935/0.0334	-0.0007/0.0019	0.7053/0.7208	0.7926/0.8992	0.9542/0.9828
Fingerprint3	0.2641/0.0796	-0.0878/0.0446	-0.0015/0.0088	0.8617/0.7238	0.7860/0.8806	0.9807/0.9823
Fingerprint4	0.2436/0.0812	-0.0922/0.0376	-0.0028/0.0050	0.8101/0.7532	0.7931/0.8885	0.9602/0.9825
Fingerprint5	0.2087/0.0884	-0.1765/0.0355	-0.0013/0.0087	0.7042/0.6869	0.7904/0.8997	0.9598/0.9824
Fingerprint6	0.2525/0.0880	-0.1997/0.0447	0.0002/0.0095	0.7945/0.6915	0.7880/0.8799	0.9629/0.9826
Fingerprint7	0.2019/0.1007	-0.1686/0.0400	-0.0005/0.0060	0.7115/0.6516	0.7933/0.8722	0.9472/0.9826
Fingerprint8	0.2507/0.0947	0.0284/0.0422	-0.0016/0.0076	0.7622/0.6975	0.7920/0.8707	0.9578/0.9824
Fingerprint9	0.1538/0.0992	-0.0193/0.0431	0.0009/0.0076	0.6683/0.7277	0.7930/0.8922	0.9388/0.9827
Average	0.2205/0.0910	-0.1058/0.0936	-0.0012/0.0064	0.7511/0.7040	0.7915/0.8857	0.9576/0.9825

**TABLE 6.** False and true correlation and SSIM for the sample nine templates for the sixth tested biometric dataset.

The nine templates of the sixth biometric dataset	Correlation/SSIM with false iris			Correlation/SSIM with true iris		
	OSH [22, 23]	DRPE [25, 37]	PTFT (Present Work)	OSH [22, 23]	DRPE [25, 37]	PTFT (Present Work)
Iris1	0.2315/0.1103	-0.1329/0.0496	-0.0050/0.0015	0.7826/0.5206	0.7858/0.8534	0.9653/0.9821
Iris2	0.2215/0.1182	-0.0813/0.0481	-0.0002/0.0061	0.7077/0.5139	0.7849/0.8727	0.9592/0.9818
Iris3	0.2265/0.1197	-0.0299/0.0548	-0.0041/0.0028	0.7142/0.4447	0.7743/0.8414	0.9547/0.9801
Iris4	0.2045/0.1247	0.0757/0.0552	0.0024/0.0062	0.7055/0.5131	0.7686/0.8512	0.9714/0.9798
Iris5	0.2617/0.1229	-0.0255/0.0537	0.0025/0.0112	0.7575/0.4956	0.7792/0.8561	0.9536/0.9809
Iris6	0.2701/0.1304	-0.0363/0.0524	0.0026/0.0112	0.7781/0.4538	0.7758/0.8509	0.9645/0.9805
Iris7	0.2577/0.1257	0.1145/0.0515	0.0043/0.0075	0.7721/0.4769	0.7783/0.8530	0.9677/0.9811
Iris8	0.2155/0.1293	0.0857/0.0563	0.0002/0.0087	0.7522/0.4704	0.7663/0.8409	0.9695/0.9790
Iris9	0.2436/0.1307	0.0862/0.0475	-0.0018/0.0069	0.7818/0.4609	0.7842/0.8557	0.9674/0.9820
Average	0.2370/0.1235	0.0063/0.0521	0.0008/0.0069	0.7535/0.4833	0.7775/0.8528	0.9637/0.9808

threshold value is utilized to decide if the input tested user is an authorized or unauthorized user. From the introduced PFD, PTD, and ROC results of the six examined and tested biometric cases, it is noticed that the suggested algorithm is advised and recommended for effective cancelable template recognition systems contrasted to the traditional optical OSH and DRPE encryption algorithms [22], [23], [25], [37]. Therefore, the proposed cancelable recognition system based on an optical PTFT encryption algorithm can efficiently classify authorized and unauthorized users better than the related optical encryption algorithms.

### C. HISTOGRAM ANALYSIS

In this section, to further investigate the effectiveness of the suggested optical PTFT cryptography algorithm for developing and achieving secure CBRS, the histogram security analysis is examined. The evaluation histogram distributions metric is utilized in assessing the strength of the cryptography technique to statistical assaults and attacks [24]. Figures 24 – 29 show the results of histograms of the original biometrics and the encrypted biometrics for the suggested algorithm contrasted to the literature optical OSH and DRPE encryption algorithms [22], [23], [25], [37] of the whole tested biometric datasets.

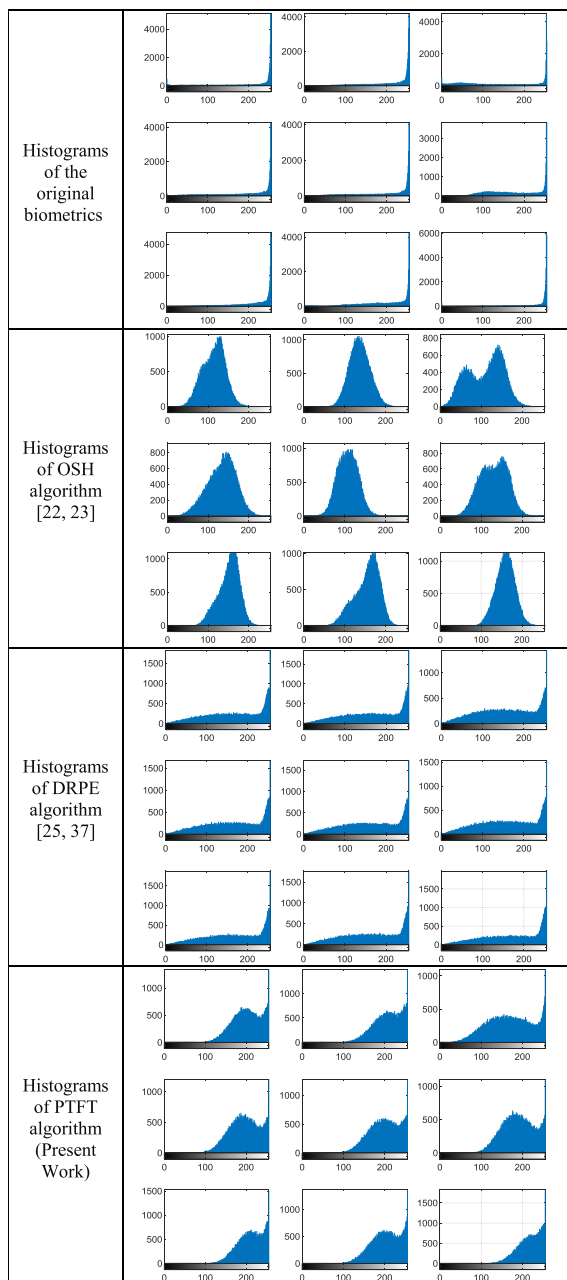
From the examined histograms, it is noticed that the suggested optical encryption algorithm and the literature optical encryption algorithms present different distributions for the encrypted biometric histograms from the original biometric histograms for the whole examined images. This

means that the performance of the suggested encryption algorithm is quite good for accomplishing significant encryption efficiency and a secure CBRS. Consequently, the achieved outcomes of the whole examined simulation tests confirm the superiority of the application of the optical PTFT encryption algorithm for cancelable biometric recognition purposes.

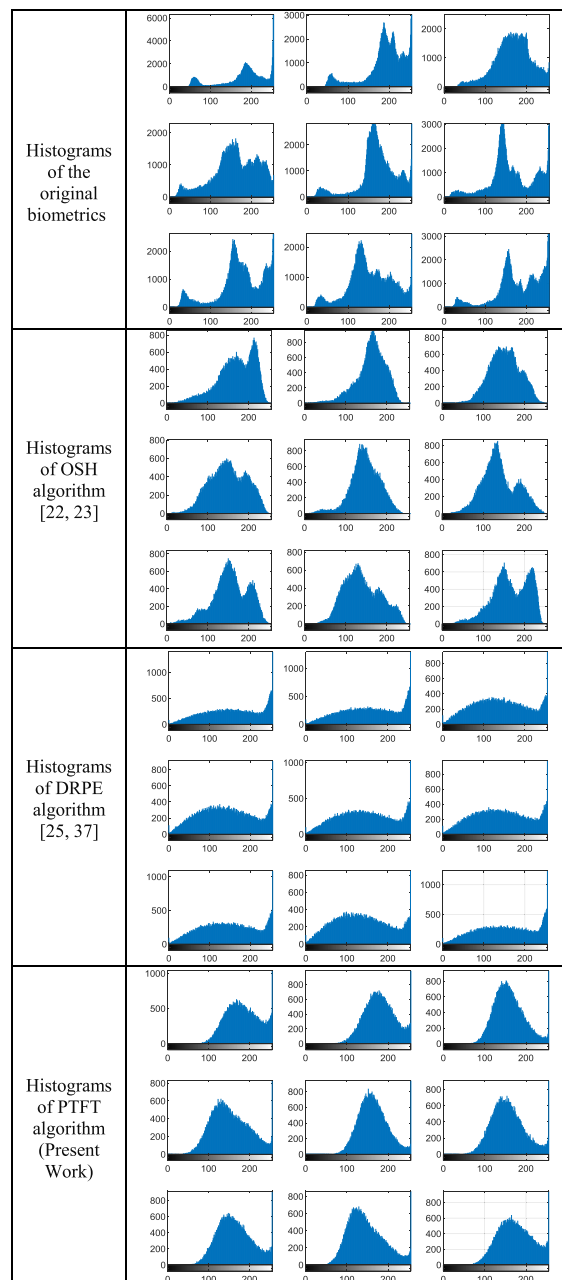
### D. CORRELATION AND SSIM ANALYSIS

For verification and authentication, two encrypted templates of biometrics have been examined. The first one is for the unauthorized user and the other one is for the authorized user. The correlation and SSIM values are estimated amongst the two examined (authorized and unauthorized) encrypted templates and the original stored encrypted biometric templates to assess the verification accomplishment of the suggested optical encryption algorithm.

The correlation coefficient [18] is an extra useful evaluation metric extensively utilized in assessing the effectiveness of cryptography procedures. It is used in our proposed work to determine the correlation between the ciphered biometric templates stored in the biometric database and the ciphered ones of new enrolments. Also, the SSIM metric [18] is utilized for the evaluation purpose in our work. It is a commonly utilized evaluation tool that evaluates congruity amongst two biometric images. In our proposed work, the SSIM metric is employed as an assessment tool for the strength of the encryption process. It is measured between the ciphered biometric



**FIGURE 28.** Histograms of the original biometrics and the encrypted biometrics for the suggested PTFT algorithm contrasted with the literature OSH and DRPE algorithms for the fifth tested biometric dataset.



**FIGURE 29.** Histograms of the original biometrics and the encrypted biometrics for the suggested PTFT algorithm contrasted with the literature OSH and DRPE algorithms for the sixth tested biometric dataset.

templates collected in the biometric server and the ciphered ones of new enrollments.

Tables 1 to 6 present the false and true correlation comparison results and SSIM comparison results for the sample of nine templates of the whole six tested biometrics datasets for the suggested optical PTFT encryption algorithm contrasted to the literature optical encryption algorithms [22], [23], [25], [37]. For the six examined and tested biometric cases, these tables confirm that the suggested CBRS achieves the highest correlation coefficients and SSIM values in the case of true biometrics enrolment and the lowest values in the case of

false biometrics enrolment contrasted to the other comparison CBRSs. Therefore, the suggested optical PTFT encryption algorithm is advised and recommended for effective cancelable template recognition systems when compared to the traditional optical OSH and DRPE encryption algorithms for robust and secure biometric security applications and services. Thus, from the obtained results in Tables 1 to 6, it is confirmed that the proposed cancelable recognition system based on an optical PTFT encryption algorithm can efficiently classify authorized and unauthorized users compared to the literature algorithms [22], [23], [25], [37].

**TABLE 7.** EER and AROC of the first tested biometric dataset in the noise presence.

Noise variance	OSH [22, 23]		DRPE [25, 37]		PTFT (Present Work)	
	EER	AROC	EER	AROC	EER	AROC
0.0	0.0271	0.9181	0.0078	0.9742	0.0068	0.9972
0.01	0.0273	0.9163	0.0089	0.9721	0.0072	0.9969
0.02	0.0277	0.9132	0.0094	0.9689	0.00734	0.9957
0.03	0.0282	0.9098	0.0105	0.9624	0.00738	0.9934
0.04	0.0328	0.9092	0.0174	0.9597	0.00751	0.9897
0.05	0.0345	0.9084	0.0196	0.9586	0.00756	0.9892

**TABLE 8.** EER and AROC of the second tested biometric dataset in the noise presence.

Noise variance	OSH [22, 23]		DRPE [25, 37]		PTFT (Present Work)	
	EER	AROC	EER	AROC	EER	AROC
0.0	0.0151	0.9516	0.0067	0.9778	0.0016	0.9991
0.01	0.0154	0.9504	0.0071	0.9771	0.0019	0.9987
0.02	0.0159	0.9489	0.0078	0.9765	0.0027	0.9984
0.03	0.0187	0.9478	0.0083	0.9742	0.0041	0.9976
0.04	0.0208	0.9435	0.0094	0.9713	0.0069	0.9970
0.05	0.0237	0.9417	0.0108	0.9683	0.0097	0.9963

**TABLE 9.** EER and AROC of the third tested biometric dataset in the noise presence.

Noise variance	OSH [22, 23]		DRPE [25, 37]		PTFT (Present Work)	
	EER	AROC	EER	AROC	EER	AROC
0.0	0.0995	0.9521	0.0093	0.9637	0.0037	0.9996
0.01	0.1089	0.9514	0.0098	0.9624	0.0046	0.9987
0.02	0.1175	0.9499	0.0125	0.9617	0.0061	0.9981
0.03	0.1367	0.9492	0.0164	0.9589	0.0083	0.9974
0.04	0.1459	0.9483	0.0197	0.9578	0.0098	0.9969
0.05	0.1624	0.9478	0.0236	0.9562	0.0117	0.9963

**TABLE 10.** EER and AROC of the fourth tested biometric dataset in the noise presence.

Noise variance	OSH [22, 23]		DRPE [25, 37]		PTFT (Present Work)	
	EER	AROC	EER	AROC	EER	AROC
0.0	0.0220	0.9592	0.0187	0.9803	0.0008	0.9993
0.01	0.0228	0.9588	0.0192	0.9796	0.0017	0.9989
0.02	0.0242	0.9583	0.0218	0.9790	0.0023	0.9981
0.03	0.0264	0.9576	0.0324	0.9788	0.0034	0.9969
0.04	0.0282	0.9565	0.0360	0.9781	0.0073	0.9963
0.05	0.0312	0.9549	0.0395	0.9772	0.0147	0.9957

**TABLE 11.** EER and AROC of the fifth tested biometric dataset in the noise presence.

Noise variance	OSH [22, 23]		DRPE [25, 37]		PTFT (Present Work)	
	EER	AROC	EER	AROC	EER	AROC
0.0	0.3031	0.9489	0.0145	0.9604	0.0020	0.9993
0.01	0.3037	0.9484	0.0149	0.9598	0.0023	0.9987
0.02	0.3042	0.9479	0.0157	0.9594	0.0027	0.9981
0.03	0.3053	0.9472	0.0163	0.9586	0.0031	0.9974
0.04	0.3064	0.9463	0.0171	0.9576	0.0035	0.9969
0.05	0.3092	0.9457	0.0179	0.9564	0.0042	0.9958

**TABLE 12.** EER and AROC of the sixth tested biometric dataset in the noise presence.

Noise variance	OSH [22, 23]		DRPE [25, 37]		PTFT (Present Work)	
	EER	AROC	EER	AROC	EER	AROC
0.0	0.0257	0.9357	0.0161	0.9533	0.0005	0.9995
0.01	0.0264	0.9349	0.0172	0.9529	0.0012	0.9992
0.02	0.0273	0.9341	0.0181	0.9526	0.0024	0.9989
0.03	0.0289	0.9329	0.0197	0.9521	0.0031	0.9984
0.04	0.0318	0.9317	0.0217	0.9517	0.0039	0.9979
0.05	0.0357	0.9302	0.0241	0.9509	0.0048	0.9972

**E. EER, FAR, FRR, AND AROC ANALYSIS**

To confirm the efficacy of the suggested optical encryption algorithm for robust CBRS, more simulations are performed for evaluating the EER, FAR, FRR, and AROC results of

the suggested optical encryption algorithm based CBRS and the literature OSH and DRPE encryption algorithms based CBRSs [22], [23], [25], [37]. The numerical assessment security evaluation of the EER, FAR, FRR, and AROC results

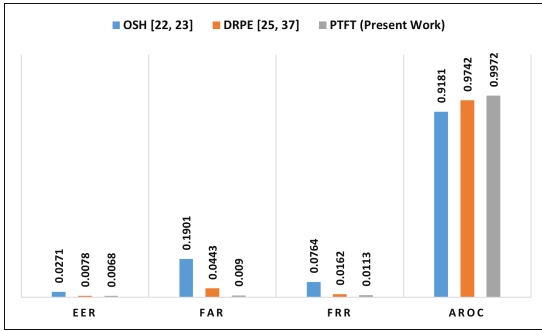


FIGURE 30. AROC, FRR, EER, and FAR of the first tested biometric dataset.

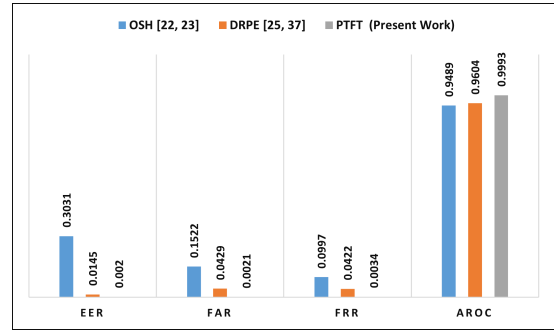


FIGURE 34. AROC, FRR, EER, and FAR of the fifth tested biometric dataset.

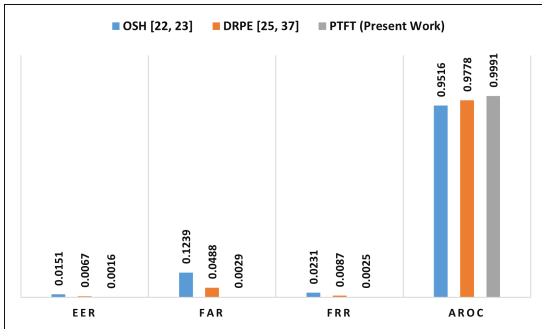


FIGURE 31. AROC, FRR, EER, and FAR of the second tested biometric dataset.

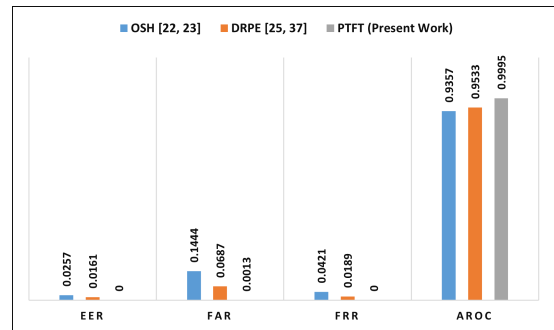


FIGURE 35. AROC, FRR, EER, and FAR of the sixth tested biometric dataset.

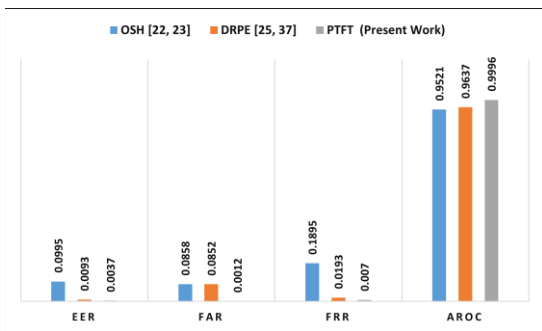


FIGURE 32. AROC, FRR, EER, and FAR of the third tested biometric dataset.

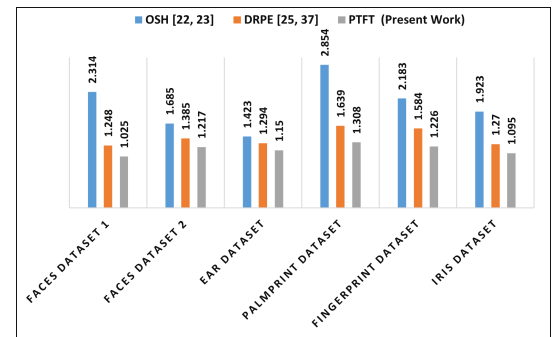


FIGURE 36. Average execution time (s) of the tested biometric datasets.

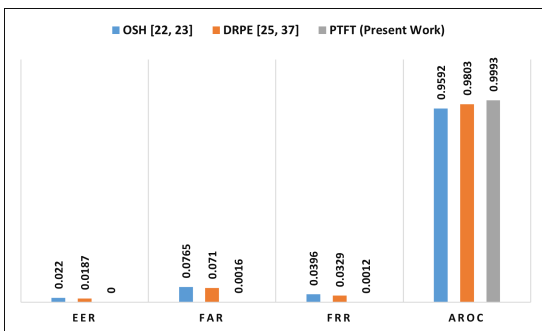


FIGURE 33. AROC, FRR, EER, and FAR of the fourth tested biometric dataset.

of the suggested optical encryption based CBRS with the literature encryption-based CBRSs in [22], [23], [25], [37] are presented in Figs. 30–35. It is observed that the FRR, FAR, AROC, and EER of the cancelable templates for the

suggested CBRS are more appreciated and recommended because it achieves the highest AROC values and the lowest EER, FAR, and FRR values contrasted to the preceding related CBRSs.

### F. PROCESSING TIME ANALYSIS

Moreover, the computational performance of the suggested optical encryption-based CBRS with the literature encryption-based CBRSs in [22], [23], [25], [37] is investigated. The experimental comparisons are carried out with MATLAB R2019a on a workstation with Microsoft Windows 10 with Intel(R) CPU @ 2.40GHz/1.80GHz Core(TM) i7-4500 and 8 GB RAM. Figure 36 shows the average execution time required to generate the encrypted biometric templates using the proposed optical PTFT encryption algorithm compared to those of the literature OSH and DRPE algorithms



**TABLE 13.** Average comparison for the suggested cancelable template recognition system and the previous cancelable recognition works.

Cancelable recognition system	FAR	EER	AROC	FRR
Proposed	0.0030	0.0019	0.9996	0.0012
Ref. [12]	0.0296	0.0039	0.9236	0.1139
Ref. [13]	0.0946	0.0219	0.8920	0.2983
Ref. [15]	0.0527	0.0086	0.9416	0.0372
Ref. [16]	0.0632	0.0436	0.9592	0.0279
Ref. [17]	0.0741	0.0622	0.9343	0.0667
Ref. [21]	0.0359	0.0862	0.9274	0.0129
Ref. [24]	0.0071	0.0178	0.8967	0.0579
Ref. [32]	0.0038	0.0096	0.9372	0.0926
Ref. [33]	0.0167	0.0195	0.9728	0.0134
Ref. [35]	0.0263	0.0096	0.9673	0.0192
Ref. [49]	0.0497	0.0351	0.9583	0.2836

for the whole examined biometric datasets. It is clear that the processing time of the proposed CBRS is recommended for both online and offline biometric authentication applications because it achieves the lowest execution time results in contrast to the other related comparison algorithms.

### G. NOISE ANALYSIS

It is not conceivable to abandon this performance investigation without studying and examining the sensitivity of the suggested CBRS to the occurrence of noise. Tables 7–12 offer the average EER and AROC values obtained from the Gaussian noise analysis with distinct noise variances of the suggested optical encryption-based CBRS with the literature encryption-based CBRSs for the whole examined biometric datasets. It is highly demonstrated that the suggested CBRS has minimal noise sensitivity with introducing acceptable EER and AROC compared to the literature schemes.

### H. COMPARATIVE ANALYSIS

For additional verification for the competence of the suggested algorithm for consistent cancelable recognition model, further comparisons are carried out for contrasting the outcomes of the suggested cancelable system with the recent literature CBRSs in [12], [13], [15]–[17], [21], [24], [32], [33], [35], [49]. We contrasted the average numerical security assessment of the FAR, EER, AROC, and FRR findings of the suggested CBRS with the previous recent CBRSs in [12], [13], [15], [16], [17], [21], [24], [32], [33], [35], [49] as summarized in Table 13. The offered outcomes in Table 13 demonstrated that the FAR, EER, AROC, and FRR of the suggested optical cryptography algorithm based CBRS are superior and highly contrasted as compared to the previous CBRSs.

From all quantitative and visual results, one can confirm that the suggested optical PTFT encryption algorithm is recommended and appreciated for accomplishing robust and reliable CBRS contrasted to the traditional optical OSH and DRPE encryption algorithms and other preceding CBRSs. Additionally, it is depicted that the suggested optical encryption algorithm presents satisfactory investiga-

tional findings for various biometric template datasets which have various characteristics. Therefore, all findings in terms of different standard evaluation metrics involving correlation coefficients, SSIM, FAR, EER, AROC, execution time, visual encryption, noise analysis, and FRR indicate the effectiveness of our suggested optical cryptography algorithm based cancelable system across numerous biometric security applications that necessitate individual verification and identification.

## VI. CONCLUSION AND FUTURE WORK

An effective and enhanced optical encryption procedure is suggested for reliable and secure CBRS. The foremost impact of this suggested work is the employment and utilization of the optical PTFT asymmetric ciphering for accomplishing a strong CBRS. Consequently, the suggested algorithm introduces both diffusion and confusion encryption effects to the biometric templates. Simulation examinations are carried out to validate the promising accomplishment of the suggested optical ciphering algorithm in effectively scrambling the biometric templates. The obtained simulation results show that the suggested algorithm is suitable and recommended for reliable biometric images compared to the literature optical encryption algorithms. The proposed CBRS offers valued ROC, PFD, EER, FAR, FRR, SSIM, PTD, visual, histogram, execution time, and correlation results. The suggested algorithm has demonstrated its potential capability to satisfactorily scramble different biometric template datasets with various features. Therefore, the suggested CBRS bolsters the cancelability performance of the biometric images and as well as developing significant quantitative and visual outcomes compared to the literature algorithms. Additionally, experiments and comparative findings achieved for the suggested CBRS guarantee an average FRR, EER, and FAR of 0.0012, 0.0019, and 0.0030, correspondingly, and an average AROC of 0.9996.

For the forthcoming investigation strategy, we suggest building a CBRS framework that combines efficient encryption, steganography, and watermarking schemes to achieve higher fidelity and robustness storage for biometric templates. Additionally, we are encouraged to investigate modern deep learning-based cancelable biometric security techniques for efficient storage and distribution of biometric templates.

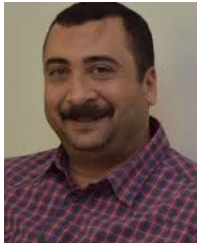
## REFERENCES

- [1] D. Orme, "Can biometrics secure the Internet of Things?" *Biometric Technol. Today*, vol. 2019, no. 5, pp. 5–7, May 2019.
- [2] S. K. Sharma and B. Khuntia, "Service layer security architecture for IoT using biometric authentication and cryptography technique," in *Intelligent Manufacturing and Energy Sustainability*. Singapore: Springer, 2020, pp. 827–837.
- [3] M. Gomez-Barrero and J. Galbally, "Reversing the irreversible: A survey on inverse biometrics," *Comput. Secur.*, vol. 90, Mar. 2020, Art. no. 101700.
- [4] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, "Security and accuracy of fingerprint-based biometrics: A review," *Symmetry*, vol. 11, no. 2, p. 141, Jan. 2019.
- [5] A. Manisha and N. Kumar, "Cancelable biometrics: A comprehensive survey," *Artif. Intell. Rev.*, vol. 53, pp. 3403–3446, Oct. 2019.

- [6] W. Yang, S. Wang, G. Zheng, J. Yang, and C. Valli, "A privacy-preserving lightweight biometric system for Internet of Things security," *IEEE Commun. Mag.*, vol. 57, no. 3, pp. 84–89, Mar. 2019.
- [7] G. Panchal, D. Samanta, and S. Barman, "Biometric-based cryptography for digital content protection without any key storage," *Multimedia Tools Appl.*, vol. 78, pp. 26979–27000, Oct. 2019.
- [8] G. S. Walia, S. Rishi, R. Asthana, A. Kumar, and A. Gupta, "Secure multimodal biometric system based on diffused graphs and optimal score fusion," *IET Biometrics*, vol. 8, no. 4, pp. 231–242, Jul. 2019.
- [9] J. Chaki, N. Dey, F. Shi, and R. S. Sherratt, "Pattern mining approaches used in sensor-based biometric recognition: A review," *IEEE Sensors J.*, vol. 19, no. 10, pp. 3569–3580, May 2019.
- [10] V. Kakkad, M. Patel, and M. Shah, "Biometric authentication and image encryption for image security in cloud framework," *Multiscale Multidisciplinary Model., Exp. Des.*, vol. 2, no. 4, pp. 233–248, Dec. 2019.
- [11] N. Kumar and M. Rawat, "RP-LPP: A random permutation based locality preserving projection for cancelable biometric recognition," *Multimedia Tools Appl.*, vol. 79, nos. 3–4, pp. 2363–2381, Jan. 2020.
- [12] H. Kaur and P. Khanna, "Random slope method for generation of cancelable biometric features," *Pattern Recognit. Lett.*, vol. 126, pp. 31–40, Sep. 2019.
- [13] H. Kaur and P. Khanna, "Privacy preserving remote multi-server biometric authentication using cancelable biometrics and secret sharing," *Future Gener. Comput. Syst.*, vol. 102, pp. 30–41, Jan. 2020.
- [14] V. K. Gunjan, P. S. Prasad, and S. Mukherjee, "Biometric template protection scheme-cancelable biometric," in *ICCCE 2019*. Singapore: Springer, 2020, pp. 405–411.
- [15] H. Kaur and P. Khanna, "PolyCodes: Generating cancelable biometric features using polynomial transformation," *Multimedia Tools Appl.*, vol. 79, pp. 20729–20752, Aug. 2020.
- [16] S. Wang and J. Hu, "Design of alignment-free cancelable fingerprint templates via curtailed circular convolution," *Pattern Recognit.*, vol. 47, no. 3, pp. 1321–1329, Mar. 2014.
- [17] N. Kumar, "On generating cancelable biometric templates using visual secret sharing," in *Proc. Sci. Inf. Conf.* Cham, Switzerland: Springer, 2020, pp. 532–544.
- [18] N. Kumar, "On generating cancelable biometric template using reverse of Boolean XOR," in *Proc. IEEE Int. Conf. Emerg. Trends Commun., Control Comput. (ICONC3)*, Lakshmanagarh, India, 2020, pp. 1–4.
- [19] X. Wang, Y. Chen, C. Dai, and D. Zhao, "Discussion and a new attack of the optical asymmetric cryptosystem based on phase-truncated Fourier transform," *Appl. Opt.*, vol. 53, no. 2, pp. 208–213, 2014.
- [20] Z. Wu, B. Liang, L. You, Z. Jian, and J. Li, "High-dimension space projection-based biometric encryption for fingerprint with fuzzy minutia," *Soft Comput.*, vol. 20, no. 12, pp. 4907–4918, Dec. 2016.
- [21] W. Yang, S. Wang, G. Zheng, J. Chaudhry, and C. Valli, "ECB4CI: An enhanced cancelable biometric system for securing critical infrastructures," *J. Supercomput.*, vol. 74, no. 10, pp. 4893–4909, Oct. 2018.
- [22] A. Yan, T.-C. Poon, Z. Hu, and J. Zhang, "Optical image encryption using optical scanning and fingerprint keys," *J. Mod. Opt.*, vol. 63, no. 3, pp. S38–S43, Dec. 2016.
- [23] P. W. M. Tsang, A. Yan, T.-C. Poon, and H. Lam, "Asymmetrical and biometric encrypted optical scanning holography (ABE-OSH)," *IEEE Trans. Ind. Informat.*, vol. 16, no. 2, pp. 1094–1101, Feb. 2020.
- [24] S. Ibrahim, M. G. Egila, H. Shawky, M. K. Elsaid, W. El-Shafai, and F. E. A. El-Samie, "Cancelable face and fingerprint recognition based on the 3D jigsaw transform and optical encryption," *Multimedia Tools Appl.*, vol. 79, pp. 14053–14078, Feb. 2020.
- [25] R. F. Soliman, G. M. El Banby, A. D. Algami, M. Elsheikh, N. F. Soliman, M. Amin, and F. E. A. El-Samie, "Double random phase encoding for cancelable face and iris recognition," *Appl. Opt.*, vol. 57, no. 35, pp. 10305–10316, 2018.
- [26] B. Ganeshan, D. Theckedath, R. Young, and C. Chatwin, "Biometric iris recognition system using a fast and robust iris localization and alignment procedure," *Opt. Lasers Eng.*, vol. 44, no. 1, pp. 1–24, Jan. 2006.
- [27] Y. Du and C.-I. Chang, "3D combinational curves for accuracy and performance analysis of positive biometrics identification," *Opt. Lasers Eng.*, vol. 46, no. 6, pp. 477–490, Jun. 2008.
- [28] E. C. Lee and K. R. Park, "Image restoration of skin scattering and optical blurring for finger vein recognition," *Opt. Lasers Eng.*, vol. 49, no. 7, pp. 816–828, Jul. 2011.
- [29] S. Banerjee, S. Mukhopadhyay, and L. Rondoni, "Multi-image encryption based on synchronization of chaotic lasers and iris authentication," *Opt. Lasers Eng.*, vol. 50, no. 7, pp. 950–957, Jul. 2012.
- [30] N. Saini and A. Sinha, "Biometrics based key management of double random phase encoding scheme using error control codes," *Opt. Lasers Eng.*, vol. 51, no. 8, pp. 1014–1022, Aug. 2013.
- [31] G. Verma, M. Liao, D. Lu, W. He, X. Peng, and A. Sinha, "An optical asymmetric encryption scheme with biometric keys," *Opt. Lasers Eng.*, vol. 116, pp. 32–40, May 2019.
- [32] W. Yang, S. Wang, J. Hu, A. Ibrahim, G. Zheng, M. J. Macedo, M. N. Johnstone, and C. Valli, "A cancelable iris-and steganography-based user authentication system for the Internet of Things," *Sensors*, vol. 19, no. 13, p. 2985, Jul. 2019.
- [33] O. C. Abikoye, U. A. Ojo, J. B. Awotunde, and R. O. Ogundokun, "A safe and secured iris template using steganography and cryptography," *Multimedia Tools Appl.*, vol. 79, pp. 23483–23506, Jun. 2020.
- [34] T. Sudhakar and M. Gavrilova, "Cancelable biometrics using deep learning as a cloud service," *IEEE Access*, vol. 8, pp. 112932–112943, 2020.
- [35] D. Chang, S. Garg, M. Hasan, and S. Mishra, "Cancelable multi-biometric approach using fuzzy extractor and novel bit-wise encryption," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3152–3167, 2020.
- [36] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Opt. Lett.*, vol. 20, no. 7, pp. 767–769, 1995.
- [37] G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain," *Opt. Lett.*, vol. 25, no. 12, pp. 887–889, 2000.
- [38] X. Peng, Z. Cui, and T. Tan, "Information encryption with virtual-optics imaging system," *Opt. Commun.*, vol. 212, nos. 4–6, pp. 235–245, Nov. 2002.
- [39] G. Situ and J. Zhang, "Double random-phase encoding in the Fresnel domain," *Opt. Lett.*, vol. 29, no. 14, pp. 1584–1586, 2004.
- [40] M. R. Abuturab, "An asymmetric color image cryptosystem based on Schur decomposition in gyrator transform domain," *Opt. Lasers Eng.*, vol. 58, pp. 39–47, Jul. 2014.
- [41] T. C. Poon and J. P. Liu, *Introduction to Modern Digital Holography: With MATLAB*. Cambridge, U.K.: Cambridge Univ. Press, 2014.
- [42] T. C. Poon, "On the fundamentals of optical scanning holography," *Amer. J. Phys.*, vol. 76, no. 8, pp. 738–745, 2008.
- [43] AT&T. (1994). *ORL Database of Faces*. Accessed: Jun. 15, 2020. [Online]. Available: <http://www.cl.cam.ac.uk/>
- [44] B. I. Test. (2005). *CASIA Palmprint*. [Online]. Available: <http://www.biometrics.idealtest.org>
- [45] B. I. Test. (2005). *CASIA-Facev5*. Accessed: Jun. 15, 2020. [Online]. Available: <http://www.biometrics.idealtest.org>
- [46] (2002). *IIT Delhi Ear Database Version 1*. Accessed: Jun. 15, 2020. [Online]. Available: [http://webold.iitd.ac.in/biometrics/Database\\_Ear.htm](http://webold.iitd.ac.in/biometrics/Database_Ear.htm)
- [47] M. Dobes and L. Machala. (2004). *Upol Iris Image Database*. Accessed: Jun. 15, 2020. [Online]. Available: <http://phoenix.inf.upol.cz/iris/>
- [48] (2004). *Fingerprint Verification Competition*. Accessed: Jun. 15, 2020. [Online]. Available: <http://bias.csr.unibo.it/fvc2004>
- [49] W. He, X. Peng, W. Qin, and X. Meng, "The keyed optical hash function based on cascaded phase-truncated Fourier transforms," *Opt. Commun.*, vol. 283, no. 11, pp. 2328–2332, Jun. 2010.



**ABDULAZIZ ALARIFI** received the Ph.D. degree in information security from the University of Wollongong, Australia. He is currently an Assistant Professor with the Department of Computer Science, Community College, King Saud University (KSU), Saudi Arabia. He is also the Head of the Research Unit, Community College, KSU. His main research interests include information security, information technology management, cloud computing, big data, information privacy, risk assessment and management, e-governance, and mobile applications.



**MOHAMMED AMOON** received the B.Sc. degree in electronic engineering and the M.Sc. and Ph.D. degrees in computer science and engineering from Menoufia University, in 1996, 2001, and 2006, respectively. He is currently a Professor of computer science and engineering with the Department of Computer Science and Engineering, Menoufia University. He is also a Professor of computer science with the Department of Computer Science, King Saud University. His research interests include agent-based systems, fault tolerance techniques, scheduling algorithms, green computing, distributed computing, grid computing, cloud computing, fog computing, and the Internet of Things (IoT).



**MOUSTAFA H. ALY** was born in Alexandria, Egypt, in 1953. He received the B.Sc., M.Sc., and Ph.D. degrees from the Faculty of Engineering, Alexandria University, Alexandria, in 1976, 1983, and 1987, respectively. He is currently a Professor of optical communications with the Electronics and Communications Engineering Department, College of Engineering and Technology, Arab Academy for Science, Technology and Maritime Transport, Alexandria. He was a Co-Supervisor of 135 M.Sc. and Ph.D. students and published 290 journal and conference papers. His research interests include optical communications, optical amplifiers, and optical networks.



**WALID EL-SHAFAI** was born in Alexandria, Egypt. He received the B.Sc. degree (Hons.) in electronics and electrical communication engineering from the Faculty of Electronic Engineering (FEE), Menoufia University, Menouf, Egypt, in 2008, the M.Sc. degree from the Egypt-Japan University of Science and Technology (E-JUST), in 2012, and the Ph.D. degree from FEE, Menoufia University, in 2019. He is currently working as a Lecturer and an Assistant professor with the Department of Electronics and Electrical Communications Engineering, FEE, Menoufia University. His research interests include wireless mobile and multimedia communications systems, image and video signal processing, efficient 2D video/3D multi-view video coding, multi-view video plus depth coding, 3D multi-view video coding and transmission, quality of service and experience, digital communication techniques, cognitive radio networks, adaptive filters design, 3D video watermarking, steganography, and encryption, error resilience and concealment algorithms for H.264/AVC, H.264/MVC and H.265/HEVC video codecs standards, cognitive cryptography, medical image processing, speech processing, security algorithms, software defined networks, the Internet of Things, medical diagnoses applications, FPGA implementations for signal processing algorithms and communication systems, cancellable biometrics and pattern recognition, image and video magnification, artificial intelligence for signal processing algorithms and communication systems, modulation identification and classification, image and video super-resolution and denoising, deep learning in signal processing, and communication systems applications.

• • •