

An Efficient GCD-Based Cancelable Biometric Algorithm for Single and Multiple Biometrics

Naglaa F. Soliman^{1,2}, Abeer D. Algarni^{1,*}, Walid El-Shafai³, Fathi E. Abd El-Samie^{1,3}
and Ghada M. El Banby⁴

¹Department of Information Technology, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, Riyadh, 84428, Saudi Arabia

²Department of Electronics and Communications, Faculty of Engineering, Zagazig University, Zagazig, 44519, Egypt

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

⁴Department of Industrial Electronics and Control Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf, 32952, Egypt

*Corresponding Author: Abeer D. Algarni. Email: adalgarni@pnu.edu.sa

Received: 17 January 2021; Accepted: 10 April 2021

Abstract: Cancelable biometrics are required in most remote access applications that need an authentication stage such as the cloud and Internet of Things (IoT) networks. The objective of using cancelable biometrics is to save the original ones from hacking attempts. A generalized algorithm to generate cancelable templates that is applicable on both single and multiple biometrics is proposed in this paper to be considered for cloud and IoT applications. The original biometric is blurred with two co-prime operators. Hence, it can be recovered as the Greatest Common Divisor (GCD) between its two blurred versions. Minimal changes if induced in the biometric image prior to processing with co-prime operators prevents the recovery of the original biometric image through a GCD operation. Hence, the ability to change cancelable templates is guaranteed, since the owner of the biometric can pre-determine and manage the minimal change induced in the biometric image. Furthermore, we test the utility of the proposed algorithm in the single- and multi-biometric scenarios. The multi-biometric scenario depends on compressing face, fingerprint, iris, and palm print images, simultaneously, to generate the cancelable templates. Evaluation metrics such as Equal Error Rate (EER) and Area and Receiver Operator Characteristic curve (AROC) are considered. Simulation results on single- and multi-biometric scenarios show high AROC values up to 99.59%, and low EER values down to 0.04%.

Keywords: Cloud; IoT; cancelable biometrics; GCD; single- and multi-biometrics; security applications



This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

1 Introduction

Compared to authentication systems based on passwords, tokens, IDs, and biometrics, cancelable biometric recognition systems provide better security for human identification purposes. They are more suitable for remote access networks such as cloud and IoT networks. Cancelable biometric systems can be built with a single or uni-biometric, hence the name uCBS, or with multiple biometrics, hence the name mCBS. The uCBS are considered less secure compared to the mCBS [1]. The general framework of uCBAS is presented in Fig. 1, where the recognition process involves a sensor module for image capturing, a pre-processing module for data alignment and noise removal, and a segmentation module to extract the region of interest from the input image followed by the feature extraction process, which heralds the user identification.



Figure 1: Framework of typical uCBS

User validation schemes are impeded by overlapping facial biometrics as in twins, poor data acquisition in the case of dry fingerprints, or even missing data, in typical cases of occluded biometric images. Therefore, mCBS are required to enhance the outcomes of the recognition process. Human facial, iris, fingerprint, ear, signature, voice, and other biometric modalities are now widely exploited to build robust mCBS. At the same time, such behavioral biometrics suffer from unavailability or poor coverage over large databases, and they also exhibit poor recognition accuracy [2]. Meanwhile, several studies focusing on numerical approaches to secure biometric templates have been published [3–5]. Notwithstanding these efforts, safeguarding biometric templates from illicit tampering remains a top priority deserving improvement in the face of sophisticated techniques to violate their intensity.

For increasing the security, accuracy, and genuine acceptance rate, mCBS have been implemented [6]. Different studies on improving the accuracy of mCBS have been published [6–17]. Multimodal biometric systems take more than one biometric template to fuse them for the identification and validation purposes. An effective fusion scheme is an important step for effective mCBS. In this regard, Rathgeb et al. [7] presented a privacy preserving technique based on feature level fusion with bloom filter applied on face and iris biometrics. They reported an EER of 0.4%. Similarly, Paul et al. [8] presented a facial and ear cancelable biometric mechanism based on fusion. Both face and ear templates are partitioned into 25 blocks, and a random projection process is applied on each block. Subsequently, the average fused projected blocks are used to generate the cancelable templates. The results reported improvements of 12% and 14% in the recognition accuracy compared to those of the face and ear recognition systems, respectively. In their contribution, Dwivedi et al. [9] presented a two-level cancelable multi-biometric recognition system based on a score fusion technique. This system depends on a rectangular area weighting technique that is applied on scores from different modalities. It achieved a high authentication performance compared to those of the single-biometric recognition systems. Moreover, Kaur et al. [10] proposed a framework for multi-server biometrics that integrates a pseudo-biometric identity with a revoked version from a pseudo-template. The authors claimed enhanced security using pseudo-identities generated using a Random Distance Method (RDM).

Furthermore, Yang et al. [11] proposed an mCBS based on both fingerprint and finger-vein. Their method generates cancelable templates by combining feature sets extracted from both biometrics. They accomplished feature-level fusion using Partial Discrete Fourier Transform (PDFT). They reported a higher security level for the Enhanced Partial Discrete Fourier Transform (EPDFT) compared to that of the PDFT. Goswami et al. [12] proposed feature-level fusion and classification for multi-modality biometric recognition. They applied a Group Sparse Representation Classifier (GSRC) on feature vectors extracted from multi-biometrics, which yields biometric authentication with an accuracy of 99.1%. Likewise, Canuto et al. [13] investigated four fusion approaches for mCBS using voice and iris biometrics. Their work proves that cancelable biometric schemes based on more than one transformation could offer more security, since these transformations complicate the verification task. In their effort, a fusion structure in the feature level for fingerprint templates was proposed by Sandhy et al. [14]. Therein, two transformed features are computed from the fingerprint minutiae to produce a bit string to be used in the fusion process. They achieved an EER of 1.6% on the Fingerprint Verification Competition (FVC 2002) database. Meanwhile, Barrero et al. [15] introduced a multi-modality biometric recognition system based on homomorphic encryption. They applied three fusion levels: feature, score, and decision to safeguard their templates, and they reported a minimum EER of 0.12%.

Similarly, Lai et al. [16] proposed a cancelable iris recognition scheme based on hashing. It depends on a Hadamard product operation and a modulo threshold function. The authors claimed improved accuracy in addition to enhanced security. Finally, Umer et al. [17] introduced a bio-hashing approach with a spatial pyramidal feature extraction process. It depends on a user-specific independent token that can be generated by each user with his selected generation method.

This paper presents a new algorithm that can be applied for both uCBS and mCBS. The main idea of the proposed algorithm depends on the Greatest Common Divisor (GCD) to generate the cancelable templates. It is known that if two co-prime operators are used on the same biometric image to obtain two blurred versions of that image, the original biometric itself can be obtained again through the 2D GCD between the two blurred versions. If some intended change is induced in the biometric image prior to or after the application of one of the blurring operators, this will lead to a distorted output from the 2D GCD operation. This output can be used instead of the original biometric template as a cancelable template. This idea is adopted in this paper to build uCBS and mCBS. The remainder of this study is outlined as follows. The basics of the related 1-D and 2-D Sylvester GCD algorithms are discussed in Section 2. The proposed cancelable template generation algorithm for uCBS and mCBS is presented in Section 3. Extensive simulation experiments are presented in Section 4 to validate the proposed algorithm. Finally, the concluding remarks are summarized in Section 5.

2 Basics of the Sylvester GCD Algorithms

This section introduces the major fundamental theories of the 1-D and 2-D Sylvester GCD algorithms that will be exploited in the proposed cancelable biometric algorithm to create the distorted versions of the original biometrics.

2.1 One-Dimensional (1-D) Sylvester GCD Algorithm

Let $A(z)$ and $B(z)$ be two polynomials defined as:

$$A(z) = a_0 + a_1z + a_2z^2 + \dots + a_{n_2}z^{n_2} \quad (1)$$

and

$$B(z) = b_0 + b_1z + b_2z^2 + \dots + b_{n_1}z^{n_1} \quad (2)$$

Similarly, if the GCD between the two polynomials is equal to $P(z)$, which is of degree r , then it can be computed in the form:

$$\frac{A(z)}{C(z)} = \frac{B(z)}{D(z)} = P(z) \quad (3)$$

where

$$C(z) = c_0 + c_1z + c_2z^2 + \dots + c_{n_2-r}z^{n_2-r} \quad (4)$$

and

$$D(z) = d_0 + d_1z + d_2z^2 + \dots + d_{n_1-r}z^{n_1-r} \quad (5)$$

are two relatively co-prime polynomials. Consequently, it follows from [18] that

$$A(z)D(z) - B(z)C(z) = 0 \quad (6)$$

By equating the coefficients of like powers of z on both sides of Eq. (6), a matrix equivalence in the form in (7) is obtained [18]:

$$\mathbf{S}\mathbf{x} = 0 \quad (7)$$

where

$$\mathbf{x} = [d_{n_1-r}, \dots, d_2, d_1, d_0, -c_0, c_1, -c_2, \dots, -c_{n_2-r}] \quad (8)$$

Hence, \mathbf{S} is defined as presented in Eq. (9) [18].

$$\mathbf{S} = \begin{bmatrix} a_{n_2} & a_{n_2-1} & \cdots & \cdots & a_1 & a_0 & 0 & \cdots & 0 \\ 0 & a_{n_2} & a_{n_2-1} & \cdots & \cdots & a_1 & a_0 & \cdots & 0 \\ \vdots & \vdots \\ 0 & \cdots & 0 & a_{n_2} & a_{n_2-1} & \cdots & \cdots & a_1 & a_0 \\ 0 & 0 & \cdots & 0 & b_{n_1} & b_{n_1-1} & \cdots & b_1 & b_0 \\ 0 & \cdots & 0 & b_{n_1} & b_{n_1-1} & \cdots & b_1 & b_0 & 0 \\ \vdots & \vdots \\ b_{n_1} & b_{n_1-1} & \cdots & b_1 & b_0 & 0 & 0 & \cdots & 0 \end{bmatrix} \quad (9)$$

By analyzing the matrix \mathbf{S} in Eq. (9), it can be deduced that it has $n_2 + n_1 - 2r + 2$ rows and $n_2 + n_1 - r + 1$ columns. Therefore, given r , \mathbf{x} can be obtained via the application of Singular Value Decomposition (SVD) on \mathbf{S} . Furthermore, since $C(z)$ and $D(z)$ are two unique polynomials of degrees $n_2 - r$ and $n_1 - r$, it is deducible that \mathbf{x} has a unique solution, and consequently, \mathbf{S} must possess $n_2 + n_1 - 2r + 1$ linearly independent rows. As a result, the singular vector that corresponds to the zero singular value of \mathbf{S} is the least-squares solution of Eq. (7) for \mathbf{x} , and it contains the coefficient values of $C(z)$ and $D(z)$ as explained in [18].

In some cases, the degree r of the GCD is unknown, and hence, \mathbf{S} cannot be formed. In that case, we have [18]:

$$\mathbf{S}_0 \mathbf{x}_0 = \mathbf{0} \tag{10}$$

where

$$\mathbf{x}_0 = [d_{n_1-1}, \dots, d_2, d_1, d_0, -c_0, c_1, -c_2, \dots, -c_{n_2-1}] \tag{11}$$

with

$$d_{n_1-1} = \dots = d_{n_1-r+1} = c_{n_2-r+1} = \dots = c_{n_2-1} = 0 \tag{12}$$

Therefore, \mathbf{S}_0 can be computed using the standard Sylvester matrix presented in Eq. (13).

$$\mathbf{S}_0 = \begin{bmatrix} a_{n_2} & a_{n_2-1} & \cdots & \cdots & a_1 & a_0 & 0 & \cdots & 0 \\ 0 & a_{n_2} & a_{n_2-1} & \cdots & \cdots & a_1 & a_0 & \cdots & 0 \\ \vdots & \vdots \\ 0 & \cdots & 0 & a_{n_2} & a_{n_2-1} & \cdots & \cdots & a_1 & a_0 \\ 0 & 0 & \cdots & 0 & b_{n_1} & b_{n_1-1} & \cdots & b_1 & b_0 \\ 0 & \cdots & 0 & b_{n_1} & b_{n_1-1} & \cdots & b_1 & b_0 & 0 \\ \vdots & \vdots \\ b_{n_1} & b_{n_1-1} & \cdots & b_1 & b_0 & 0 & 0 & \cdots & 0 \end{bmatrix} \tag{13}$$

Using arguments in (9), it can be deduced that \mathbf{S}_0 has dimensions of $(n_2 + n_1) \times (n_2 + n_1)$. Meanwhile, the necessary and sufficient condition for $A(z)$ and $B(z)$ to have a non-constant GCD is that the resultant Sylvester matrix \mathbf{S}_0 is singular. The structural relation between \mathbf{S}_0 and \mathbf{S} is illustrated in Fig. 2. Furthermore, if we denote the sub-matrix of size $(n_2 + n_1 - 2k) \times (n_2 + n_1 - k)$ as \mathbf{S}_k , which is obtained by striking out the first k and last k rows of \mathbf{S}_0 and the first k columns of \mathbf{S}_0 , then for $GCD\{A(z), B(z)\} = P(z)$ with degree r , $\mathbf{S}_0, \mathbf{S}_1, \dots, \mathbf{S}_{r-1}$ must be singular and \mathbf{S}_{r-1} must be of rank $n_2 + n_1 - 2r + 1$.

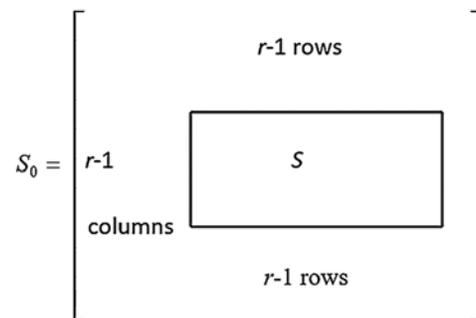


Figure 2: Structure of the Sylvester matrix used to estimate the GCD

2.2 Two-Dimensional (2-D) Sylvester GCD Algorithm

The direct extension of the 1-D Sylvester algorithm to the 2-D case in terms of constant matrices generated from the given 2-D polynomial coefficients leads to very large-size matrices. For $N \times N$ images, the matrix \mathbf{S} will be of size $2N^2 \times 2N^2$. Since the SVD computation produces matrices with a size proportional to the cube of the original matrix size, operations of $O(N^6)$ are required to execute the SVD, directly. Hence, a more efficient strategy is needed to extend the 1-D Sylvester algorithm to a 2-D algorithm.

In doing so, we assume that the two blurred versions $g_1(n_1, n_2)$ and $g_2(n_1, n_2)$ of the original image $f(n_1, n_2)$ are both $N_1 \times N_2$ matrices. The coefficients of these matrices are the coefficients of the z -transforms of their respective images. Using the Conventional Discrete Fourier Transform Least Squares (CDFT-LS) approach, we substitute $z_1 = e^{-j2\pi n_1/N_1}$, $n_1 = 0, 1, \dots, N_1 - 1$, into both $G_1(z_1, z_2)$ and $G_2(z_1, z_2)$. This results in two 1-D polynomials [17]:

$$G_k \left(e^{-j(2\pi n_1/N_1)}, z_2 \right) = F \left(e^{-j(2\pi n_1/N_1)}, z_2 \right) H_k \left(e^{-j(2\pi n_1/N_1)}, z_2 \right) \quad (14)$$

where $k = 1, 2$.

It is trivial that $F(e^{-j(2\pi n_1/N_1)}, z_2)$ is still a common factor of $G_1(e^{-j(2\pi n_1/N_1)}, z_2)$ and $G_2(e^{-j(2\pi n_1/N_1)}, z_2)$ in a single variable, z_2 . Consequently, the 1-D GCD produces the scaled quantity $c_0(e^{-j(2\pi n_1/N_1)})F(e^{-j(2\pi n_1/N_1)}, z_2)$. Furthermore, for each value of n_1 in Eq. (14), we substitute $z_2 = e^{-j2\pi n_2/N_2}$ in this GCD and form a matrix of discrete Fourier transform elements [18]:

$$A(n_1, n_2) = c(n_1) F \left(e^{-j(2\pi n_1/N_1)}, e^{-j(2\pi n_2/N_2)} \right) \quad (15)$$

We scale each row by a constant $c(n_1) = c_0(e^{-j(2\pi n_1/N_1)})$. So, we obtain:

$$A(n_1, n_2) a(n_1) = F \left(e^{-j(2\pi n_1/N_1)}, e^{-j(2\pi n_2/N_2)} \right) \quad (16)$$

Undertaking similar operations and substituting $z_2 = e^{\frac{-j2\pi n_2}{N_2}}$ in $G_1(z_1, z_2)$ and $G_2(z_1, z_2)$, whose 1-D GCD was obtained by substitution of $z_1 = e^{\frac{-j2\pi n_1}{N_1}}$, we obtain another matrix, $B(n_1, n_2)$ in Eq. (17), which is related to the discrete Fourier transform of the original image by column-wise scaling [18]:

$$B(n_1, n_2) b(n_2) = F \left(e^{-j(2\pi n_1/N_1)}, e^{-j(2\pi n_2/N_2)} \right) \quad (17)$$

From Eqs. (16) and (17), we have:

$$A(n_1, n_2) a(n_1) - B(n_1, n_2) b(n_2) = 0 \quad (18)$$

Eq. (18) can be written in matrix form as [18]:

$$\mathbf{\Gamma} \mathbf{y} = 0 \quad (19)$$

where

$$\mathbf{y} = [a(1), a(2), \dots, a(N_1), b(1), b(2), \dots, b(N_2)]^T \quad (20)$$

and

$$\Gamma = \begin{bmatrix} A(1, 1) & 0 & 0 & -B(1, 1) & 0 & 0 & 0 & 0 \\ A(1, 2) & 0 & 0 & 0 & -B(1, 2) & 0 & 0 & 0 \\ \dots & \dots \\ A(1, N_2) & 0 & 0 & 0 & 0 & 0 & 0 & -B(1, N_2) \\ 0 & A(2, 1) & 0 & -B(2, 1) & 0 & 0 & 0 & 0 \\ 0 & A(2, 2) & 0 & 0 & -B(2, 2) & 0 & 0 & 0 \\ \dots & \dots \\ 0 & A(2, N_2) & 0 & 0 & 0 & 0 & 0 & -B(2, N_2) \\ \vdots & \vdots \\ 0 & 0 & A(N_1, 1) & -B(N_1, 1) & 0 & 0 & 0 & 0 \\ 0 & 0 & A(N_1, 2) & 0 & -B(N_1, 2) & 0 & 0 & 0 \\ \dots & \dots \\ 0 & 0 & A(N_1, N_2) & 0 & 0 & 0 & 0 & -B(N_1, N_2) \end{bmatrix} \quad (21)$$

Multiplying Eq. (21) by Γ^T yields [18]:

$$\Gamma^T \Gamma \mathbf{y} = 0 \quad (22)$$

Eq. (22) can be solved using the least-squares solution to produce Eq. (23):

$$\Gamma^T \Gamma \mathbf{y} = \lambda \mathbf{y} \quad (23)$$

For an eigenvector \mathbf{y} corresponding to the smallest eigenvalue of $\Gamma^T \Gamma$ in Eq. (23), the estimated Fourier transform of the original image can be realized in the form [17]:

$$F\left(e^{-j(2\pi n_1/N_1)}, e^{-j(2\pi n_2/N_2)}\right) = \frac{1}{2} [A(n_1, n_2) a(n_1) + B(n_1, n_2) b(n_2)] \quad (24)$$

Finally, the inverse Fourier transform can be used to estimate the GCD. If we use two blurred images of the same biometric and estimate their 2D GCD, we can get the original biometric template. On the other hand, if we make a slight change induced by the user prior to or after blurring, we severely distort the 2D GCD result. The result of the GCD in this case can be used as a cancelable template. The minor changes can be induced in each biometric template in a user-specific manner.

3 Proposed GCD-Based Cancelable Biometric Algorithm

Fig. 3 presents the outlines of the proposed algorithm. As seen in the figure, the original biometric images are firstly compressed using the Discrete Cosine Transform (DCT) compression algorithm. After that, they are merged together to form a unified biometric template. This template is blurred with an operator $h_1(n_1, n_2)$. Simultaneously, another blurred version of the biometric template is generated with another operator $h_2(n_1, n_2)$.

We have:

$$g_1(n_1, n_2) = f(n_1, n_2) * h_1(n_1, n_2) \quad (25)$$

$$g_2(n_1, n_2) = f(n_1, n_2) * h_2(n_1, n_2) \quad (26)$$

Applying z -transform on (25) and (26), we get:

$$G_k(z_1, z_2) = F(z_1, z_2) H_k(z_1, z_2) \quad k = 1, 2 \quad (27)$$

where

$$G_1(z_1, z_2) = F(z_1, z_2) * H_1(z_1, z_2) \quad (28)$$

and

$$G_2(z_1, z_2) = F(z_1, z_2) * H_2(z_1, z_2) \quad (29)$$

If $H_1(z_1, z_2)$ and $H_2(z_1, z_2)$ are co-prime, then

$$GCD\{H_1(z_1, z_2), H_2(z_1, z_2)\} = 1 \quad (30)$$

and

$$GCD\{G_1(z_1, z_2), G_2(z_1, z_2)\} = F(z_1, z_2) \quad (31)$$

As shown in Fig. 3, if we induce some minimal change in the compressed template prior to blurring with $h_2(n_1, n_2)$, Eq. (31) does not hold. This leads to a distorted version of the fused templates that can be used as a cancelable template.

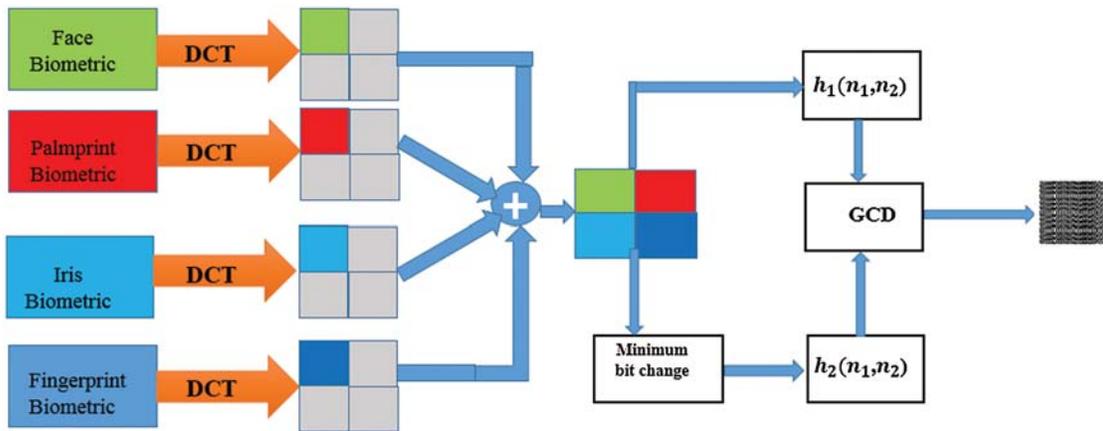


Figure 3: The proposed unified mCBS framework

4 Results and Discussion

In this section, the assessment of the suggested algorithm is introduced. Firstly, the security analysis of the suggested GCD-based algorithm as an encryption-like algorithm is presented in terms of visual analysis, correlation analysis, differential attack analysis, and entropy analysis [19] as provided in Tab. 1. It is well-known that the algorithm must break the correlation amongst the adjacent pixels. It is observed from the obtained outcomes that the suggested GCD-based algorithm succeeds in demolishing the very high correlation of pixels in the original biometric templates. Moreover, Tab. 1 demonstrates correlation, Unified Average Change Intensity (UACI), and Number of Changing Pixel Rate (NPCR) values [20] between two ciphered biometric templates. The outcomes reveal that the suggested GCD-based algorithm is robust and vulnerable to control

parameters and secret keys. So, all results confirm that the suggested GCD-based algorithm can be executed, cost-effectively, for constructing an efficient and secure cancelable biometric recognition system. As a result, this encouraged us to develop it in our suggested work.

Table 1: Security analysis for evaluating the suggested GCD-based algorithm

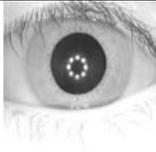
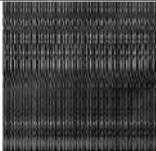
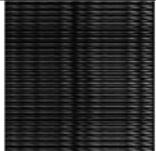
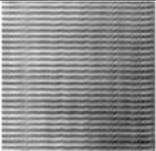
Original Biometrics	 Entropy = 7.3650.	 Entropy = 7.5638.	 Entropy = 7.4937.	 Entropy = 7.3856.
Cancelable Biometrics	 Correlation = 0.1283, Entropy = 7.8379, NPCR = 99.53, and UACI = 32.98.	 Correlation = 0.0937, Entropy = 7.9183, NPCR = 99.67, and UACI = 33.51.	 Correlation = 0.0439, Entropy = 7.9372, NPCR = 99.72, and UACI = 33.49.	 Correlation = 0.1070, Entropy = 7.8957, NPCR = 99.68, and UACI = 34.07.



Figure 4: Dataset 1 consisting of nine facial images [21]

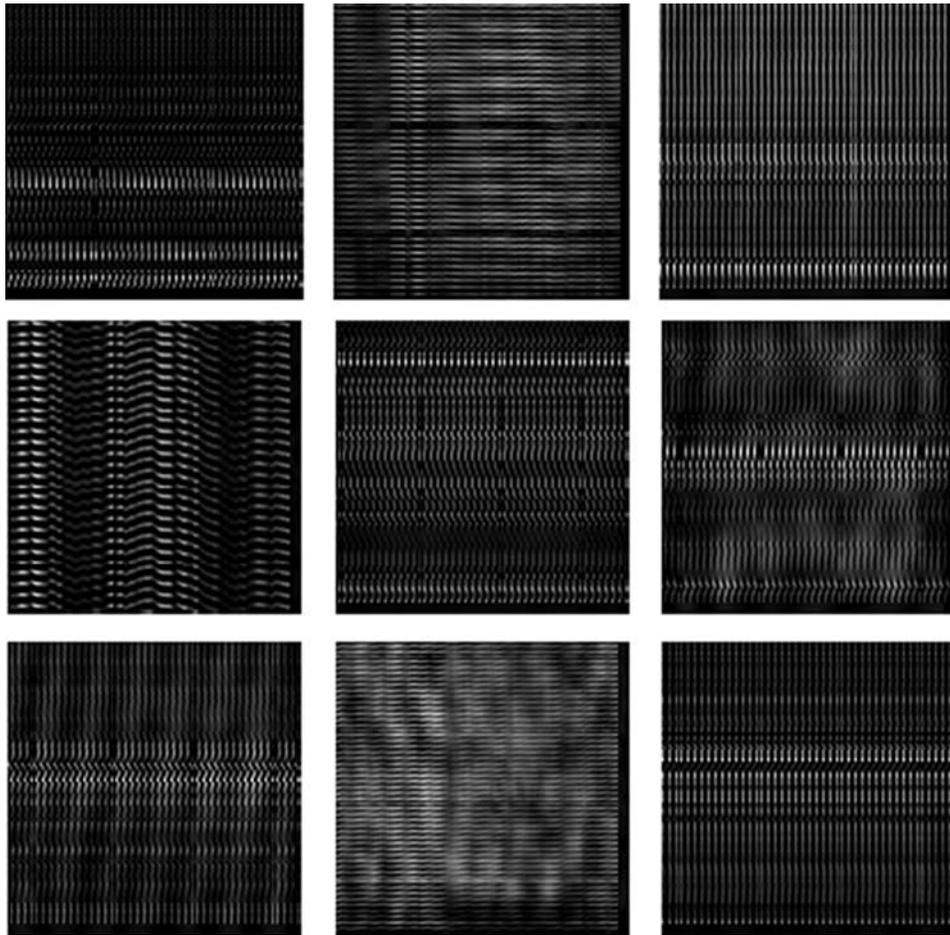


Figure 5: Cancelable facial images for those in Fig. 4 with GCD algorithm

Furthermore, in this section, several experiments are introduced to verify the validity of the proposed uCBS and mCBS that depend on 2D GCD. They have been implemented using a workstation equipped with MATLAB Intel® Core™i7-4210U on a CPU with a 1.7 GHz processor. Four datasets have been used in the uCBS experiments, namely ORL [21], FVC2000 DB1 [22], CASIA-IrisV3-Interval [23], and CASIA Palm print [24] for face, fingerprint, iris, and palm print images, respectively.

For the uCBS, the experiments are based on generating two blurred versions of each template and inducing a minor change in one of them prior to blurring. Hence, the 2D-GCD is implemented to generate the cancelable template of that biometric. The database of cancelable templates is composed, and hence the distance between new templates and those in the database is estimated based on the correlation score. Both EER and AROC values are estimated for the verification process. On the other hand, the proposed mCBS depends on estimating the DCTs of four biometric templates and generating a combined version based on the first quadrant of each DCT. This combined version is used as an initial template that is blurred twice. A minor change in one of these versions and the application of the 2D-GCD lead to the cancelable template.

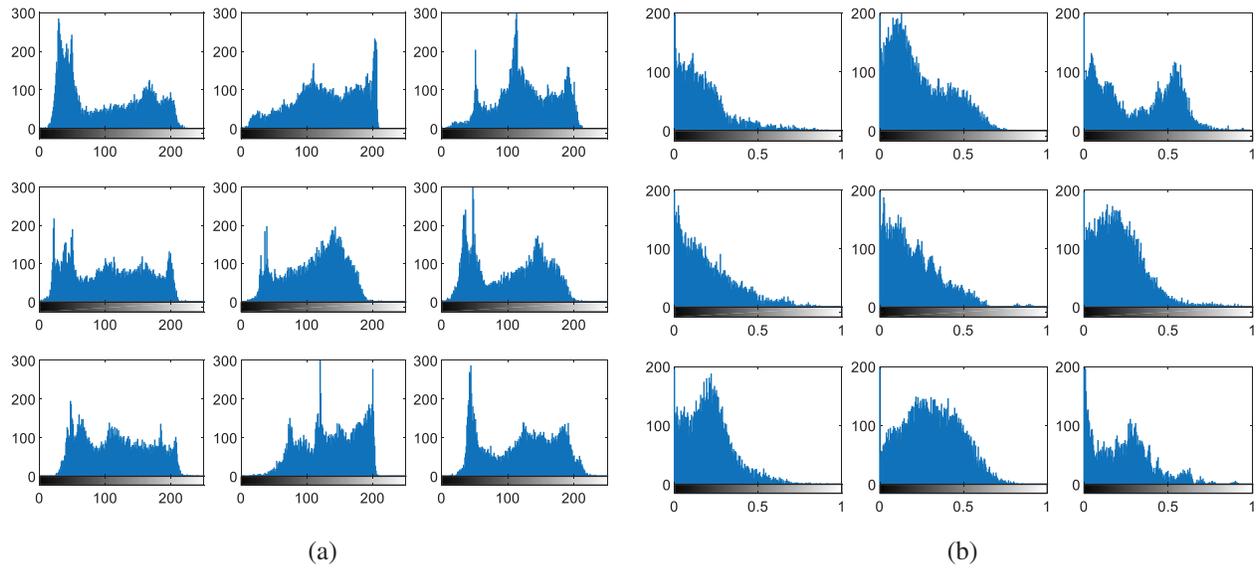


Figure 6: Histograms of facial images (a) original images (b) cancelable templates

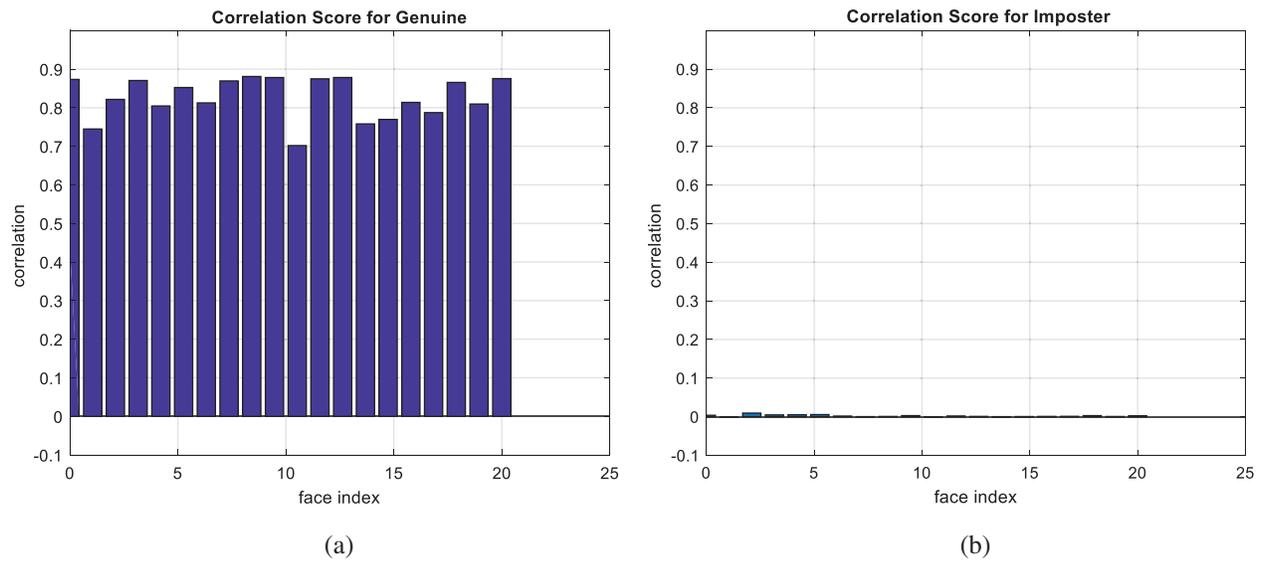


Figure 7: Correlation scores for original facial images (a) genuine (b) imposter

The Receiver Operating Characteristic (ROC) curve, which represents the relationship between the true-positive correlation and false-positive correlation [25,26], is used to assess the performance of the suggested CBS. The scores of all patterns are distributed around a mean score, which is higher for authorized patterns compared to unauthorized ones.

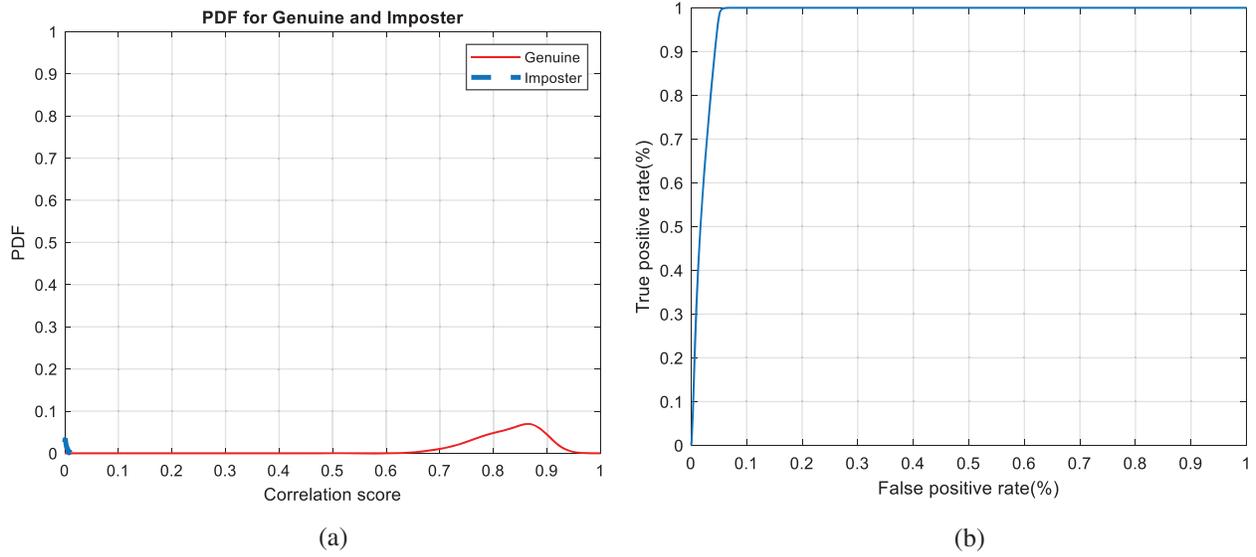


Figure 8: Authentication curves for facial biometrics (a) PFD curves (b) ROC curve



Figure 9: Dataset 2 consisting of nine fingerprint images [22]

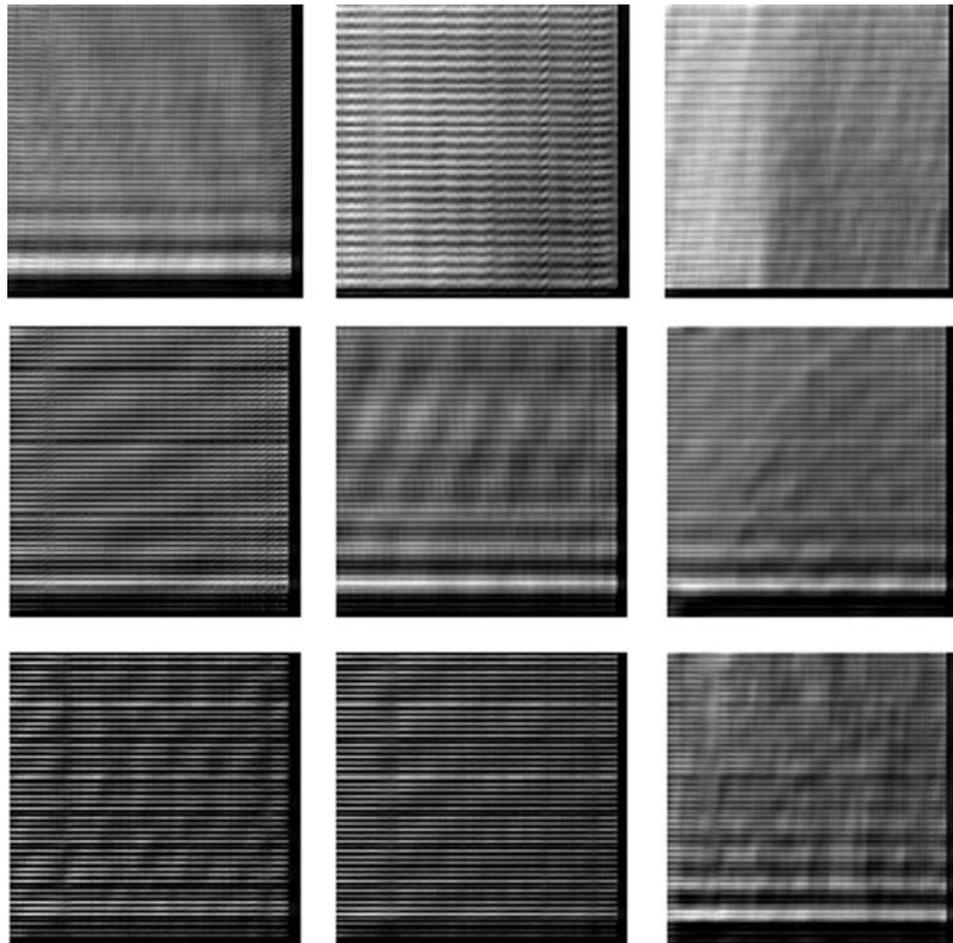


Figure 10: Cancelable fingerprint images for those in Fig. 9 with GCD algorithm

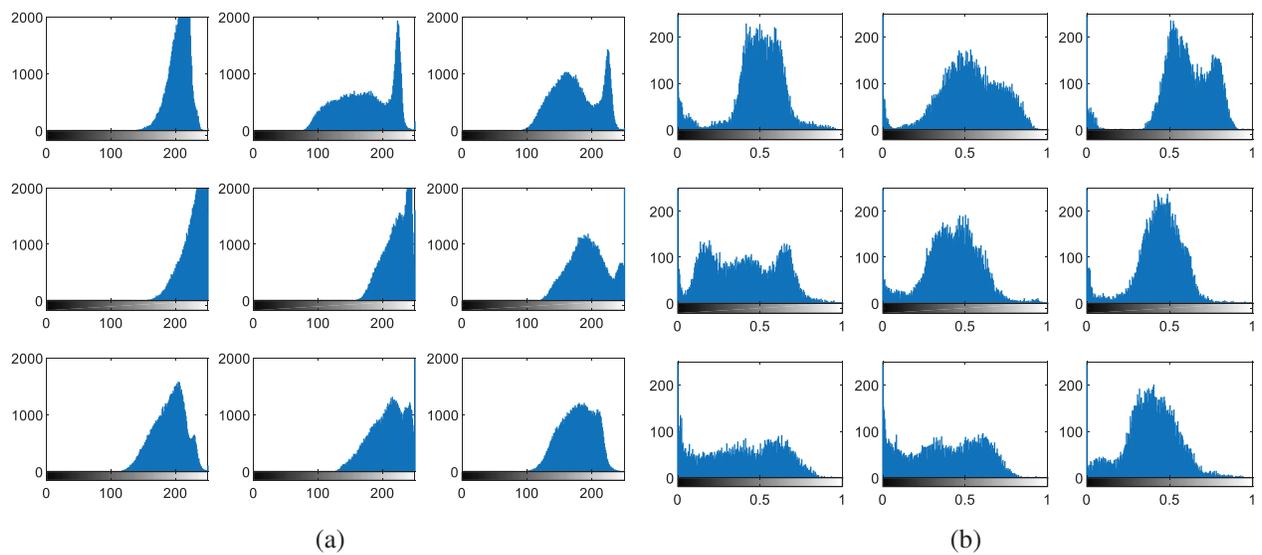


Figure 11: Histograms of fingerprint images (a) original images (b) cancelable templates

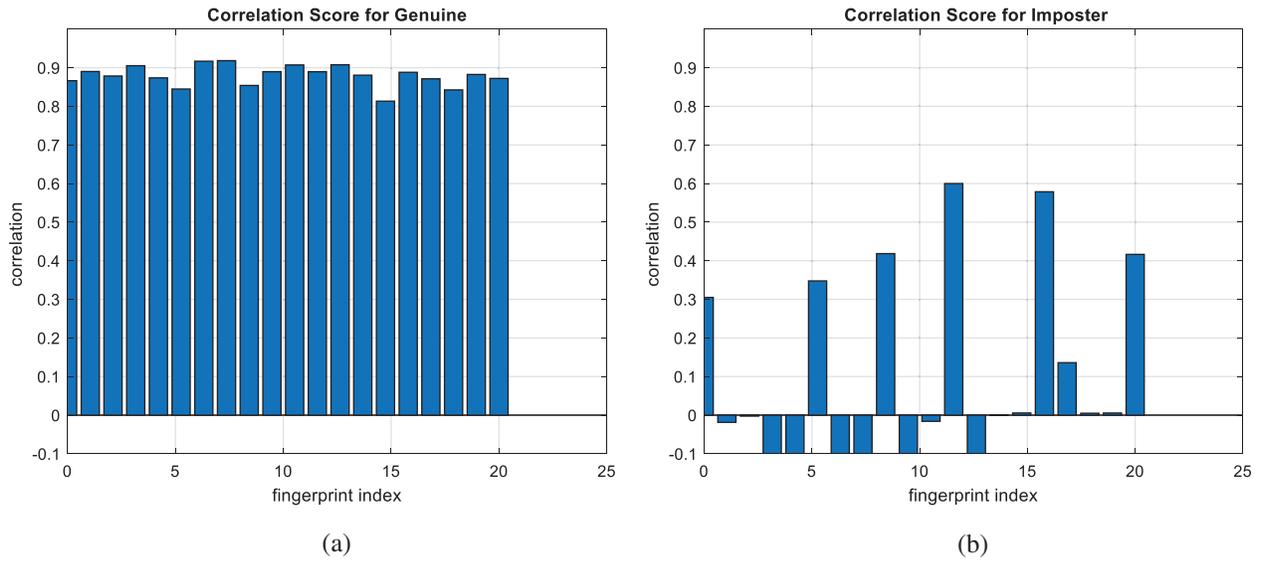


Figure 12: Correlation scores for original fingerprint images (a) genuine (b) imposter

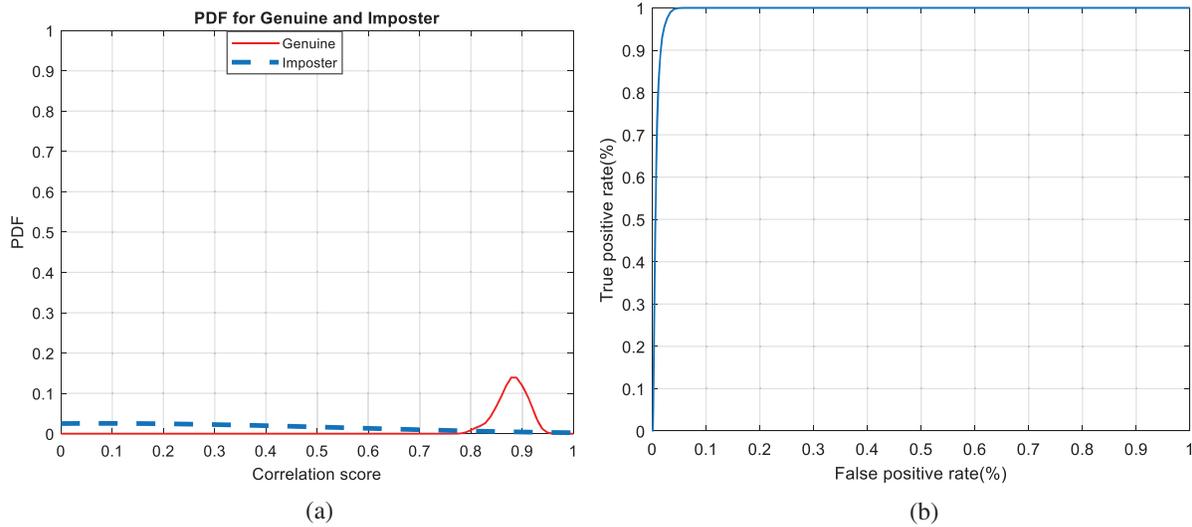


Figure 13: Authentication curves for cancelable fingerprint recognition (a) PFD curves (b) ROC curve

The multi-modal biometrics used to validate the proposed CBS consist of facial, fingerprint, iris, and palm print images as presented in Fig. 4 (Faces), Fig. 9 (Fingerprints), Fig. 14 (Iris), and Fig. 19 (Palm prints). Figs. 5, 10, 15, and 20 present the unimodal cancelable templates with 2D GCD. The histograms of the pristine unimodal biometrics are presented in Figs. 6, 11, 16, and 21 for facial, fingerprint, iris, and palm print biometrics, respectively.

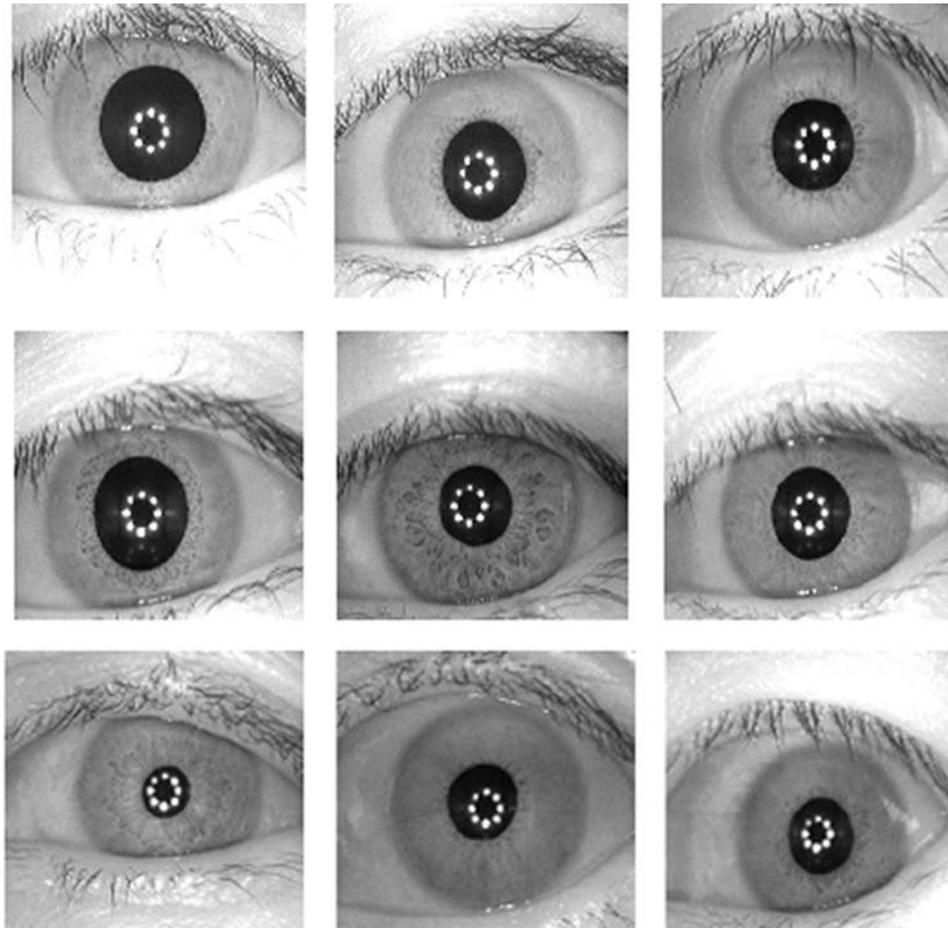


Figure 14: Dataset 3 consisting of nine biometric iris images [23]

Figs. 7, 12, 17, and 22 present the correlation scores for all nine unimodal biometric images used in the uCBS experiments. The PTD, PFD, and ROC curves for these biometrics are presented in Figs. 8, 13, 18, and 23. These curves display the threshold values used to distinguish authorized users from unauthorized ones. Fig. 24 presents the composite multi-biometric templates. Samples of the GCD cancelable multi-biometric templates and their respective histograms are presented in Fig. 25. Correlation scores for both authorized and unauthorized patterns are introduced in Fig. 26. Authentication curves for the proposed mCBS are presented in Fig. 27.

Finally, the average A ROC, mean correlation scores, False Acceptance Rate (FAR), False Rejection Rate (FRR), and ERR for the GCD-based mCBS are presented in Tab. 2.

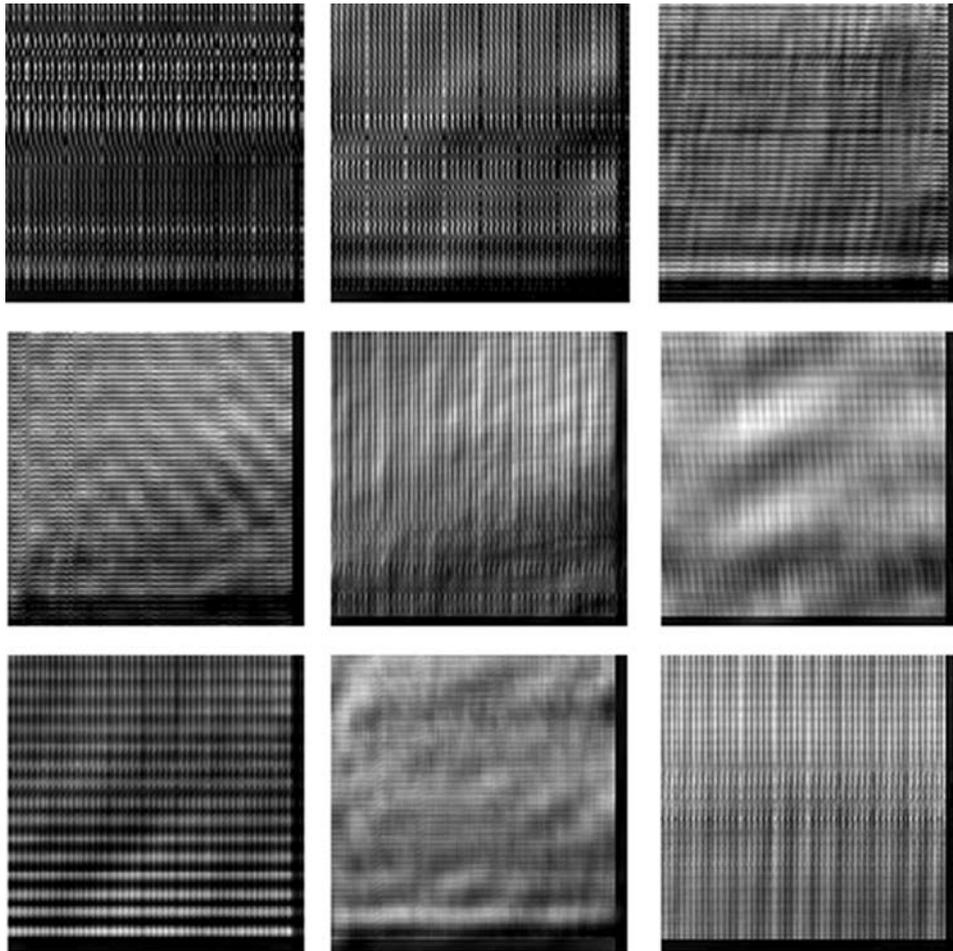


Figure 15: Cancelable iris images for those in Fig. 14 with GCD algorithm

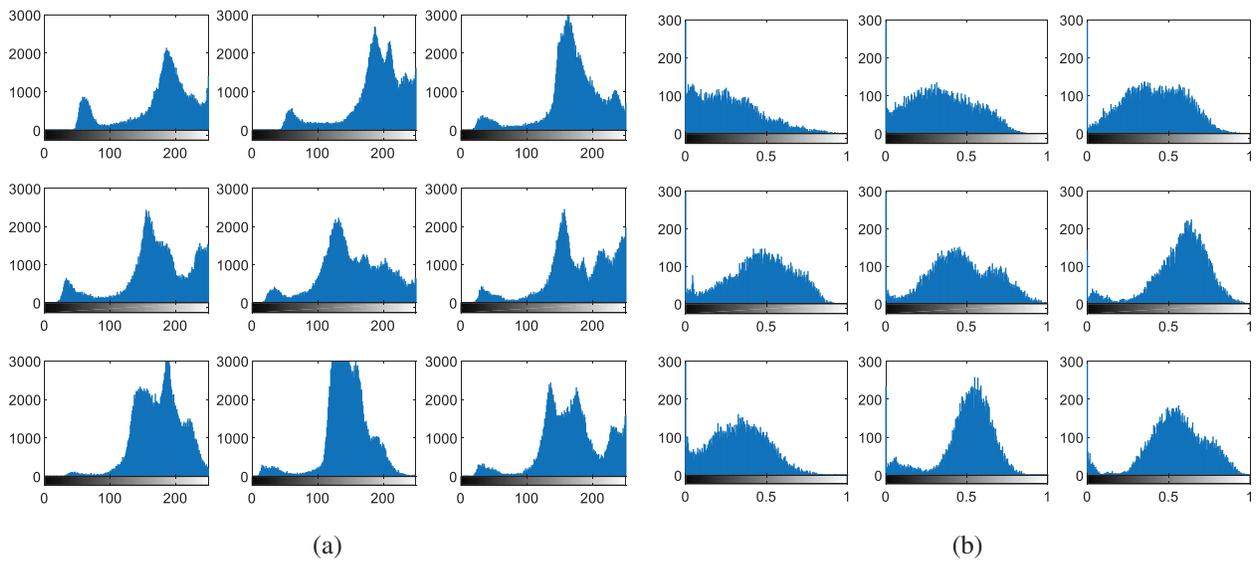


Figure 16: Histograms of iris images (a) original images (b) cancelable templates

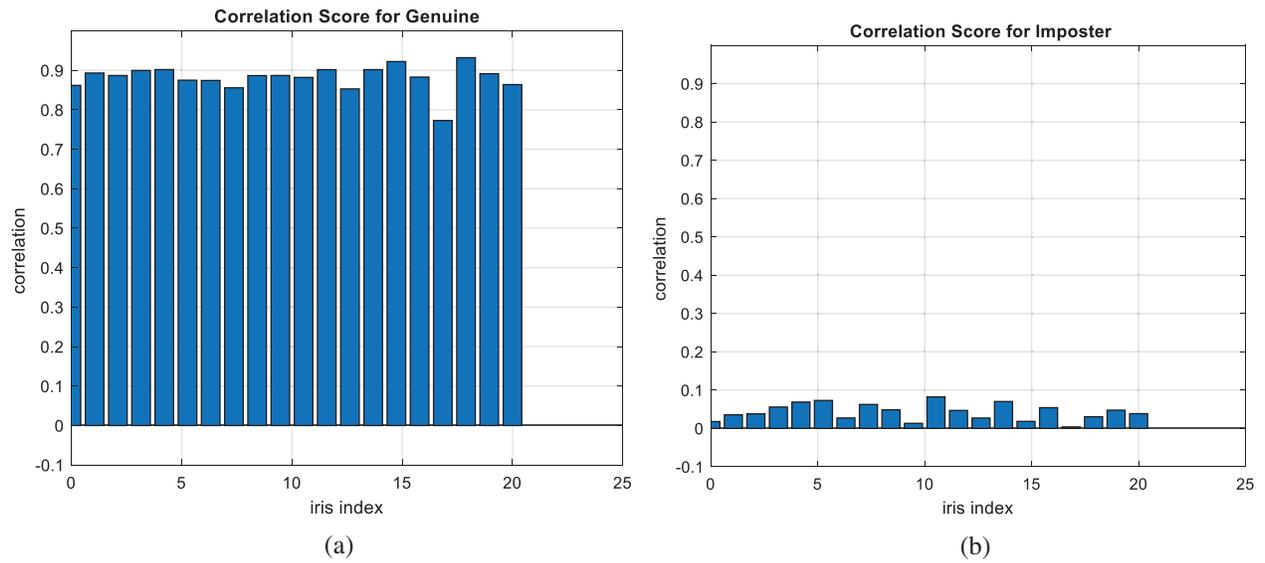


Figure 17: Correlation scores for original iris images (a) genuine (b) imposter

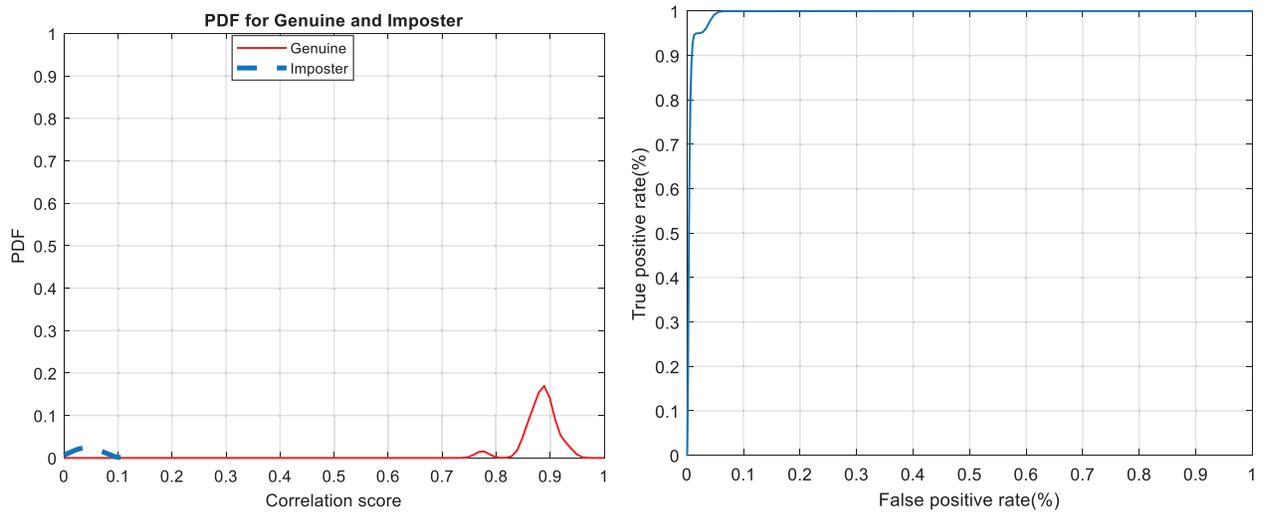


Figure 18: Authentication curves for cancelable iris recognition (a) PFD curves (b) ROC curve

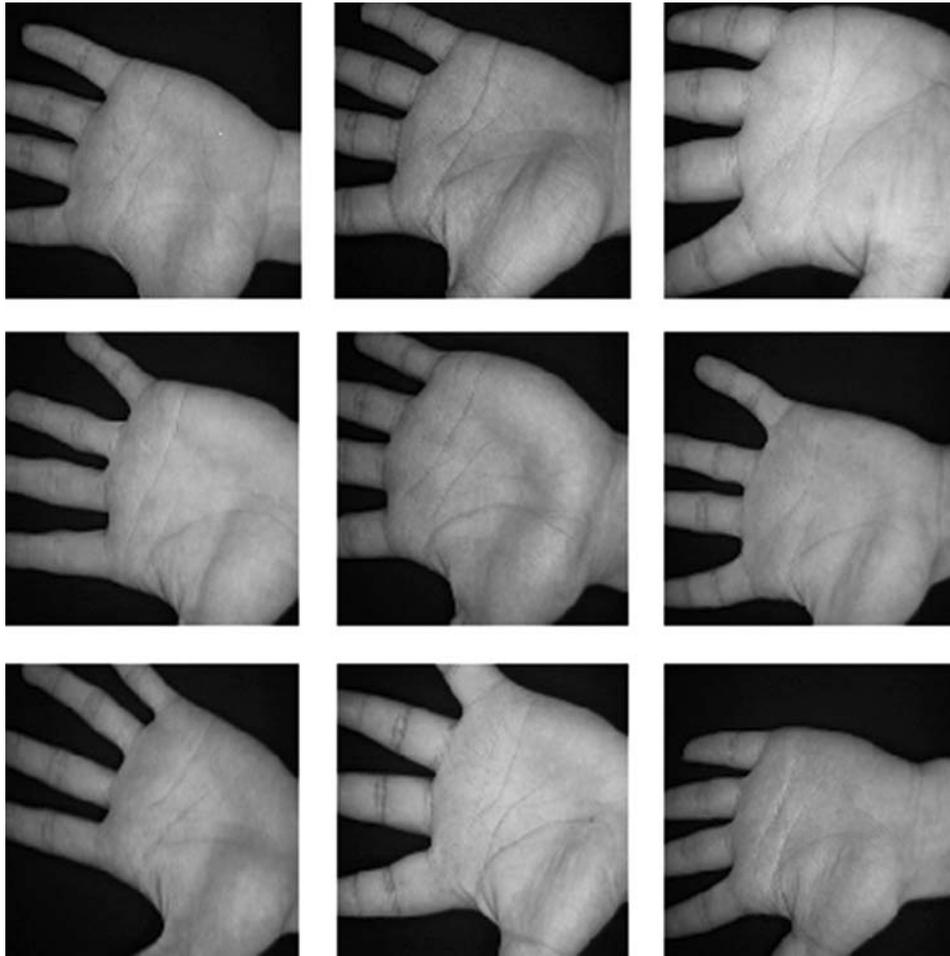


Figure 19: Dataset 4 consisting of nine palm print images [24]

- **Comparison with Other Related Works**

To validate the suggested CBS, more test investigations have been carried out for comparison of the suggested CBS with the latest algorithms [25–32]. We compared the average FAR, EER, AROC, and FRR of the suggested CBS with those of the CBS in [25–32] as presented in Tab. 3. From the introduced comparative study in Tab. 3, we ensure that the FAR, EER, AROC, and FRR of the suggested CBS are better than those of the other traditional CBS.

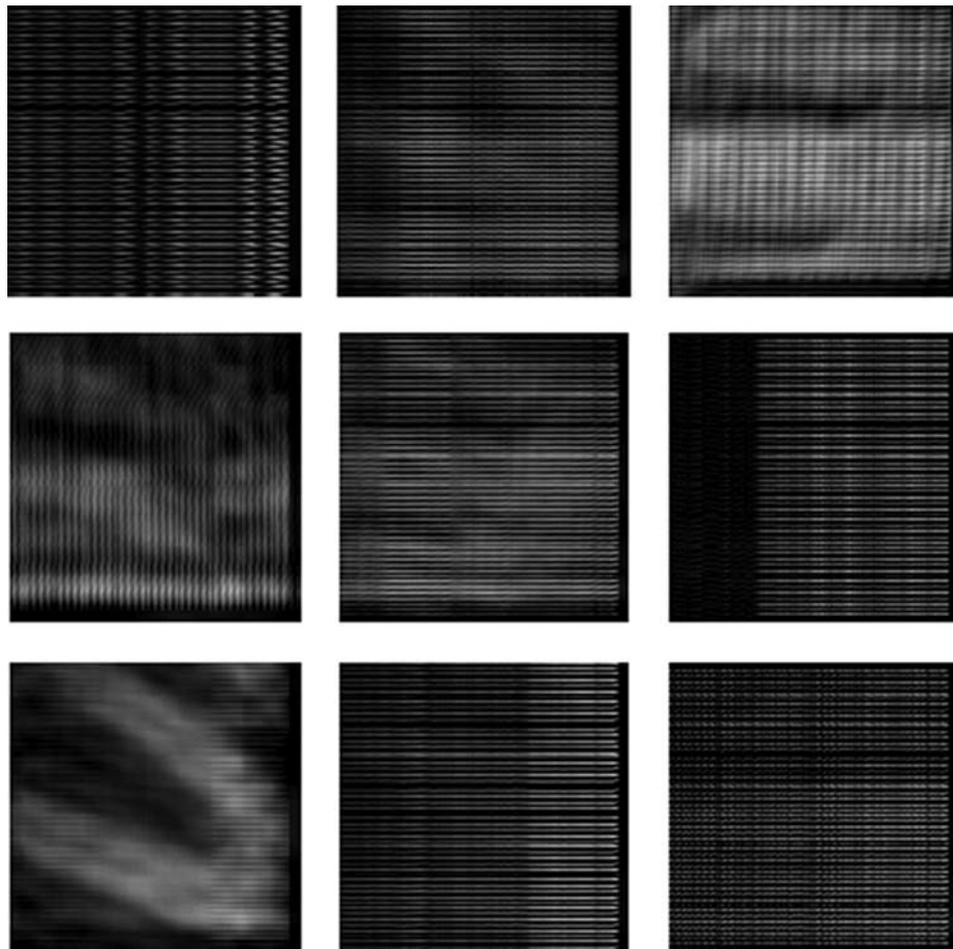


Figure 20: Cancelable palm print images for those in Fig. 19 with GCD algorithm

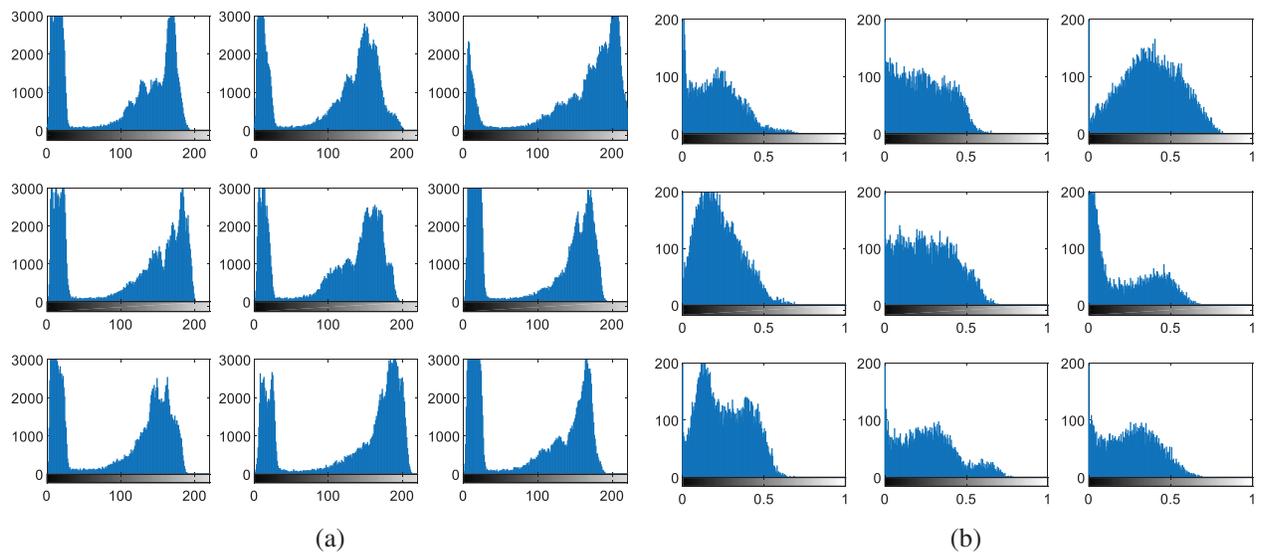


Figure 21: Histograms of palm print images (a) original images (b) cancelable templates

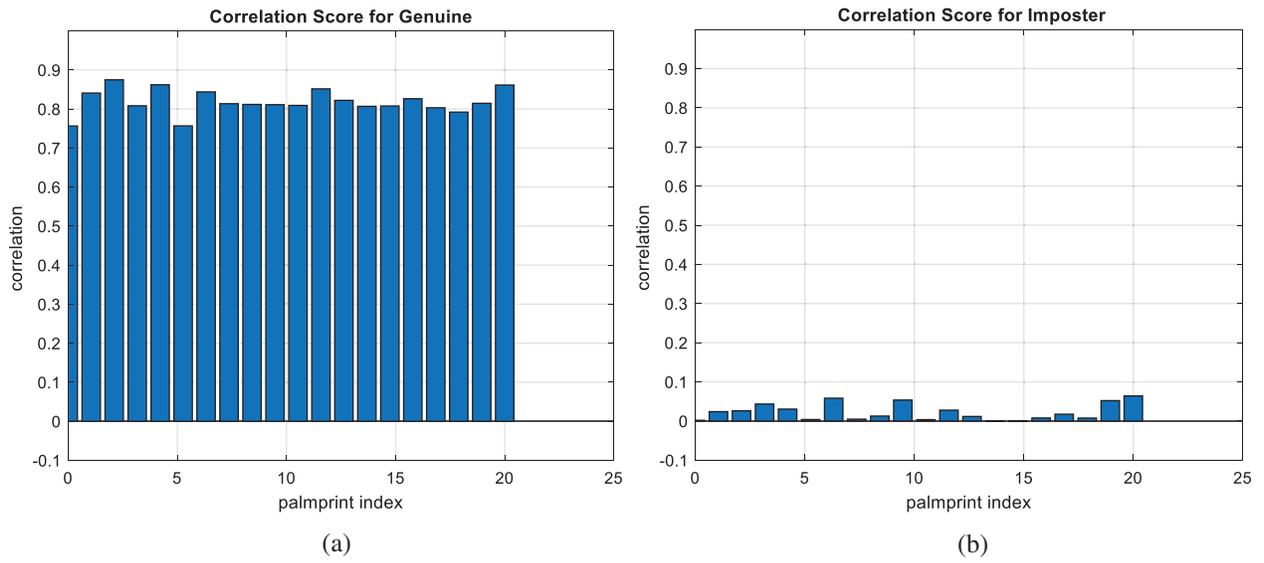


Figure 22: Correlation scores for original palm print images (a) genuine (b) imposter

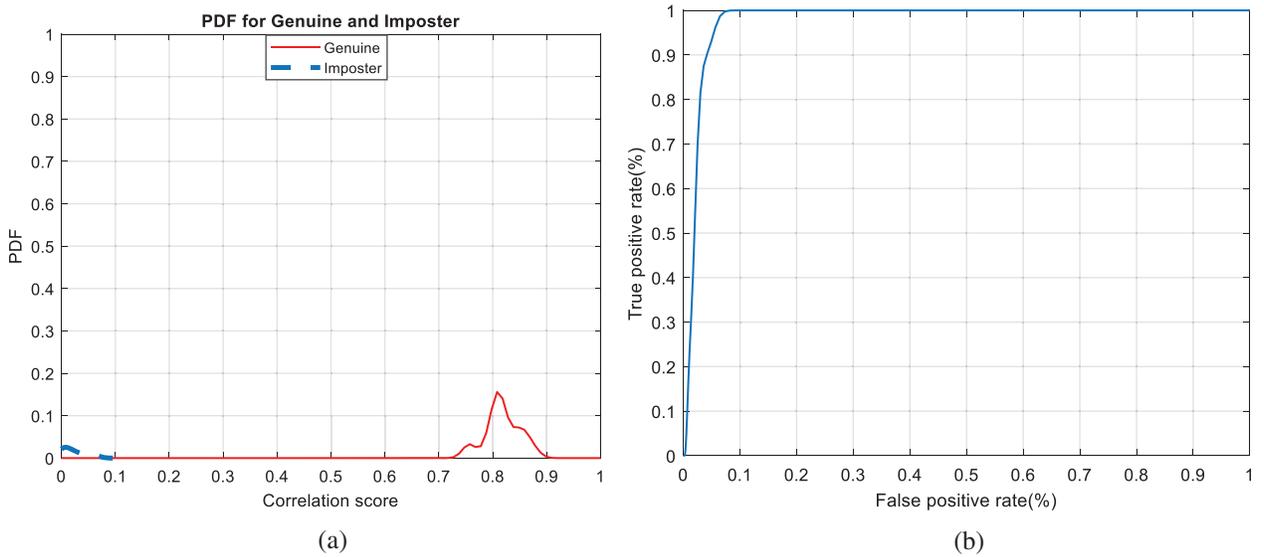


Figure 23: Authentication curves for cancelable palm print recognition (a) PFD curves (b) ROC curve

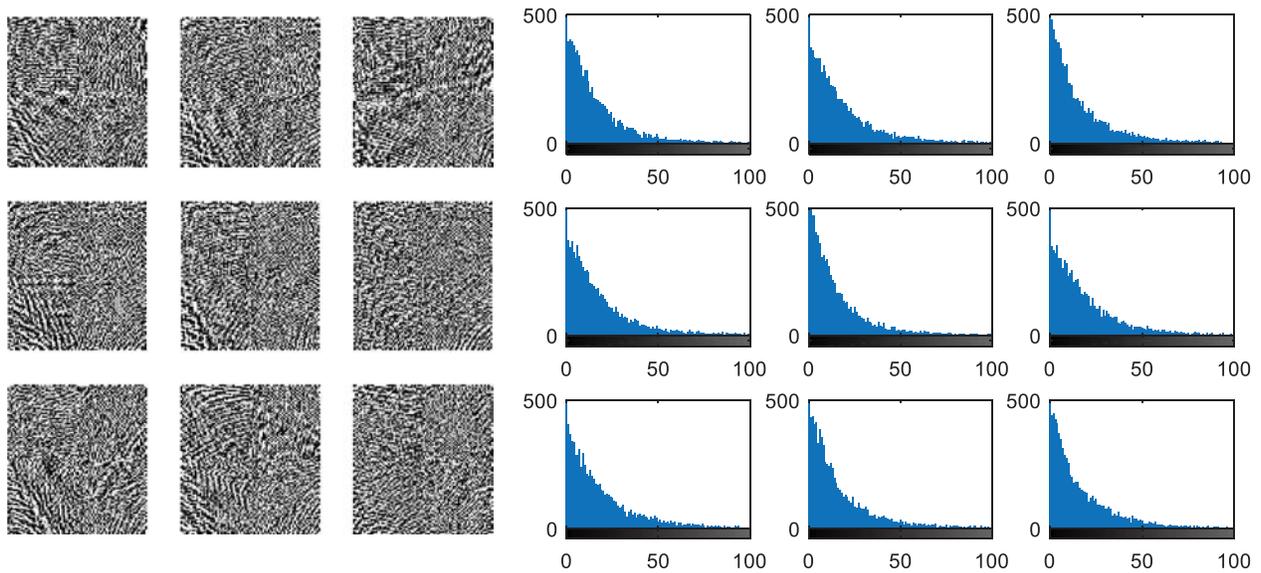


Figure 24: Composite DCT outputs of multi-biometric inputs and their histograms

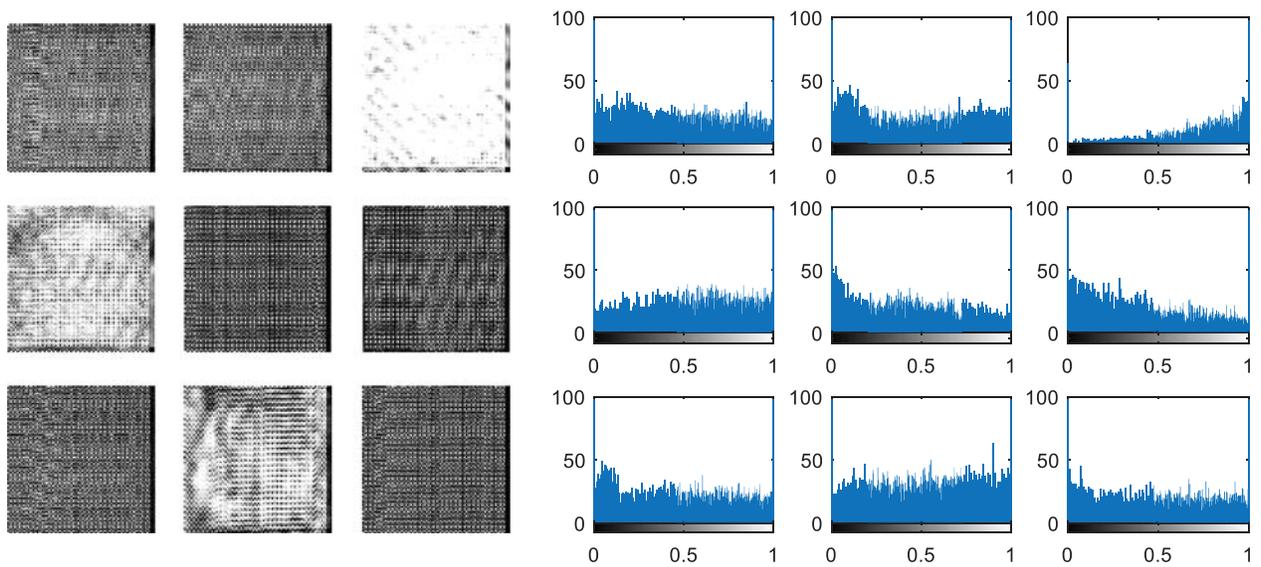


Figure 25: Cancelable templates for the proposed mCBS and their histograms

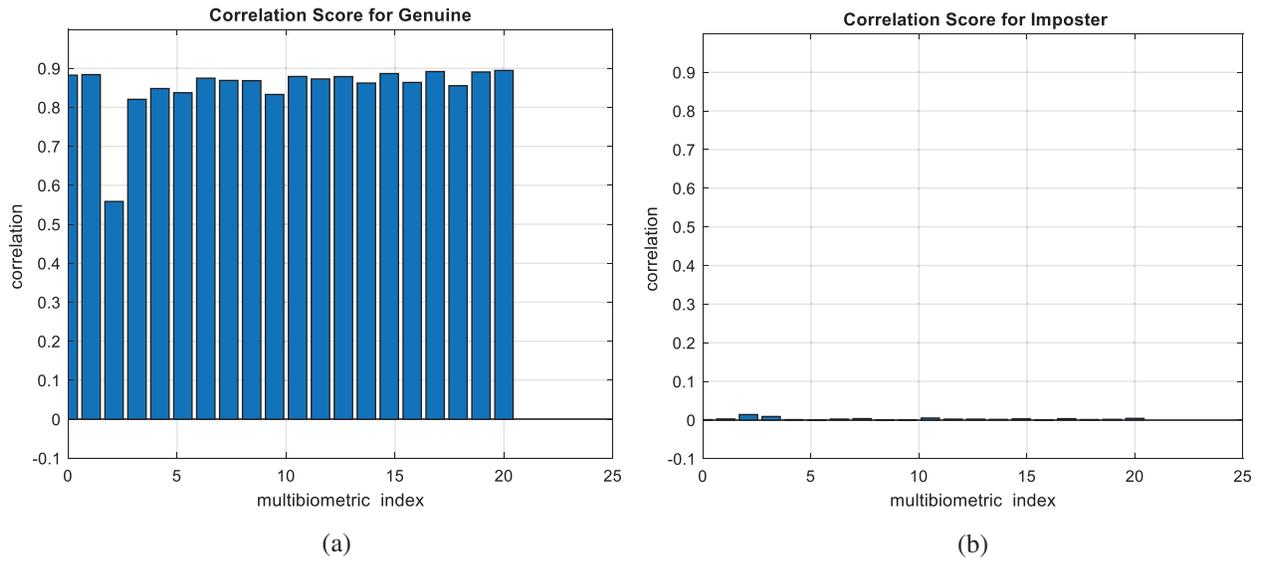


Figure 26: Correlation scores for the proposed mCBS (a) genuine (b) imposter

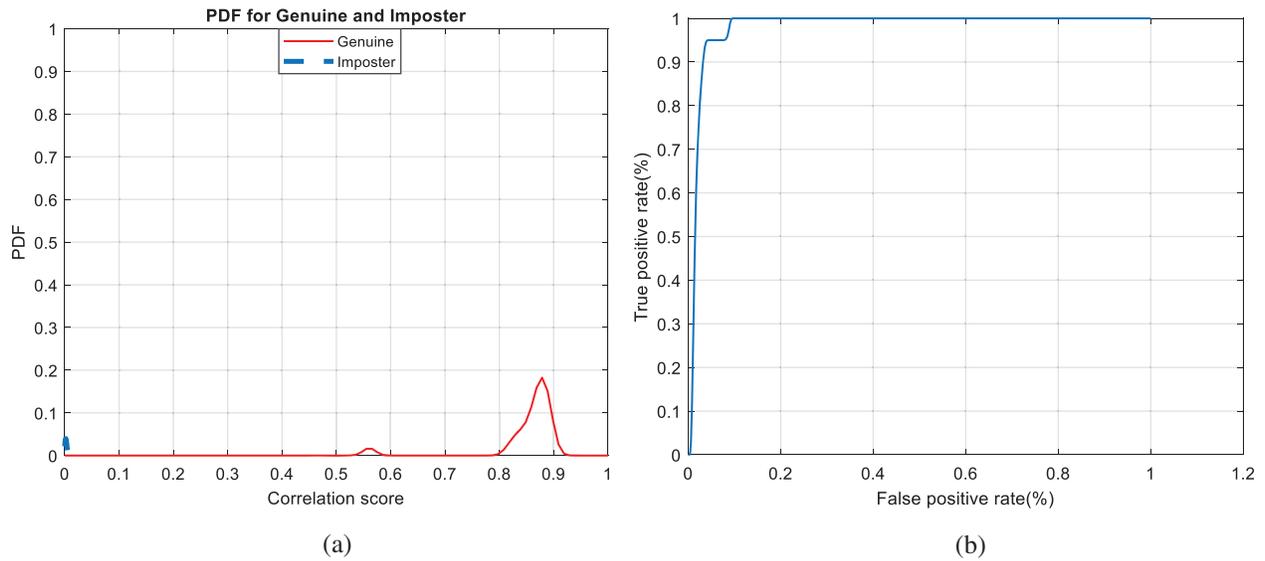


Figure 27: Authentication curves for the proposed mCBS (a) PFD curves (b) ROC curve

Table 2: Results of the proposed uCBS and mCBS

System	AROC	Mean of authorized correlation score	Mean of un-authorized correlation score	FAR	FRR	ERR
Proposed uCBS for face images	0.9806	0.8278	0.0302	0.0916	0.0328	0.0098
Proposed uCBS for fingerprint images	0.9922	0.8799	0.0417	0.0401	0.0107	0.0071
Proposed uCBS for iris images	0.9943	0.8817	0.0430	0.0476	0.0230	0.0107
Proposed uCBS for palm print images	0.9780	0.8186	0.0225	0.0735	0.0129	0.0096
Proposed mCBS	0.9802	0.8529	0.0031	0.0933	0.0092	0.0049

Table 3: Average metric values for the proposed and traditional CBS [25–32]

CBAS	EER	FAR	FRR	AROC
Proposed	0.0023	0.0182	0.0024	0.968
[25]	0.0046	0.0235	0.0929	0.883
[26]	0.0357	0.0985	0.0612	0.863
[27]	0.0859	0.0435	0.0627	0.718
[28]	0.0416	0.1955	0.0489	0.873
[29]	0.1081	0.0927	0.0967	0.907
[30]	0.0924	0.0562	0.0257	0.868
[31]	0.0178	0.0571	0.0876	0.896
[32]	0.0098	0.0104	0.018	0.952

5 Conclusions and Future Work

This paper presented a new approach to build efficient CBS using single- and multi-biometric inputs for cloud and IoT biometric applications. Pre-determined distortions are induced in the biometric images for single- and multi-biometric inputs with the GCD algorithm. As a self-dependent approach, the need for auxiliary data or images is eliminated. The GCD with some minimal changes can be used efficiently in the generation of cancelable biometric templates. We validated the proposed uCBS and mCBS on inputs consisting of facial, fingerprint, iris, and palm print images. AROC values above 99% were recorded for all the examined biometrics. This work can be easily implemented for cloud, IoT, and wireless access applications. In addition, it can be enhanced with the utilization of encryption algorithms with the GCD algorithm. In the future, we can incorporate deep learning algorithms for compressing and encrypting the biometric images for enhancing the cancelable biometric system performance.

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

Funding Statement: This research was funded by the Deanship of Scientific Research at Princess Nourah Bint Abdulrahman University through the Fast-track Research Funding Program to support publication in the top journal (Grant No. 42-FTTJ-13).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

- [1] B. Choudhury, P. Then, B. Issac, V. Raman and M. Haldar, "A survey on biometrics and cancelable biometrics systems," *International Journal of Image and Graphics*, vol. 18, no. 1, pp. 1850006, 2018.
- [2] A. Algarni, G. El Banby, S. Ismail, W. El-Shafai, F. El-Samie *et al.*, "Discrete transforms and matrix rotation based cancelable face and fingerprint recognition for biometric security application," *Entropy*, vol. 22, no. 12, pp. 1–40, 2020.
- [3] A. Alarifi, M. Amoon, M. Aly and W. El-Shafai, "Optical PTFT asymmetric cryptosystem based secure and efficient cancelable biometric recognition system," *IEEE Access*, vol. 8, pp. 221246–221268, 2020.
- [4] A. Jegede, N. Udzir, A. Abdullah and R. Mahmood, "Cancelable and hybrid biometric cryptosystems: Current directions and open research issues," *International Journal of Advanced and Applied Sciences*, vol. 4, no. 11, pp. 65–77, 2017.
- [5] S. Ibrahim, M. Egila, H. Shawky, M. Elsaid, W. El-Shafa *et al.*, "Cancelable face and fingerprint recognition based on the 3D jigsaw transform and optical encryption," *Multimedia Tools and Applications*, pp. 1–26, 2020.
- [6] N. Soliman, M. Khalil, A. Algarni, S. Ismail, R. Marzouk *et al.*, "Efficient HEVC steganography approach based on audio compression and encryption in QFFT domain for secure multimedia communication," *Multimedia Tools and Applications*, vol. 80, no. 3, pp. 1–35, 2020.
- [7] C. Rathgeb, M. Gomez-Barrero, C. Busch, J. Galbally and J. Fierrez, "Towards cancelable multi-biometrics based on bloom filters: A case study on feature level fusion of face and iris," in *Proc. 3rd IEEE Int. Workshop on Biometrics and Forensics*, Gjøvik, Norway, pp. 1–6, 2015.
- [8] P. Paul and M. Gavrilova, "Multimodal biometrics using cancelable feature fusion," in *Proc. IEEE Int. Conf. on Cyberworlds*, Santander, Spain, pp. 279–284, 2014.
- [9] R. Dwivedi and S. Dey, "Score-level fusion for cancelable multi-biometric verification," *Pattern Recognition Letters*, vol. 126, no. 3, pp. 58–67, 2019.
- [10] H. Kaur and P. Khanna, "Privacy preserving remote multi-server biometric authentication using cancelable biometrics and secret sharing," *Future Generation Computer Systems*, vol. 102, no. 11, pp. 30–41, 2020.
- [11] W. Yang, S. Wang, J. Hu, G. Zheng and C. Valli, "A fingerprint and finger-vein based cancelable multi-biometric system," *Pattern Recognition*, vol. 78, pp. 242–251, 2018.
- [12] G. Goswami, P. Mittal, A. Majumdar, M. Vatsa and R. Singh, "Group sparse representation based classification for multi-feature multimodal biometrics," *Information Fusion*, vol. 32, no. 2, pp. 3–12, 2015.
- [13] A. Canuto, F. Pintro and J. Xavier-Junior, "Investigating fusion approaches in multi-biometric cancelable recognition," *Expert Systems with Applications*, vol. 40, no. 6, pp. 1971–1980, 2013.
- [14] M. Sandhya and M. Prasad, "Securing fingerprint templates using fused structures," *IET Biometrics*, vol. 6, no. 3, pp. 173–182, 2017.
- [15] M. Barrero, E. Maiorana, J. Galbally, P. Campisi and J. Fierrez, "Multi-biometric template protection based on Homomorphic encryption," *Pattern Recognition*, vol. 67, no. 10, pp. 149–163, 2017.
- [16] Y. Lai, Z. Jin, A. Teoh, B. Goi, W. Yap *et al.*, "Cancelable iris template generation based on indexing-first-one hashing," *Pattern Recognition*, vol. 64, no. 1, pp. 105–117, 2017.

- [17] S. Umer, B. Dhara and B. Chanda, "A novel cancelable iris recognition system based on feature learning techniques," *Information Sciences*, vol. 406, no. 407, pp. 102–118, 2017.
- [18] S. El-Khamy, M. Hadhoud, M. Dessouky, B. Salam and F. Abd El-Samie, "Blind multichannel reconstruction of high-resolution images using wavelet fusion," *Journal of Applied Optics*, vol. 44, no. 34, pp. 7349–7356, 2005.
- [19] A. Alarifi, S. Sankar, T. Altameem, K. Jithin, M. Amoon *et al.*, "Novel hybrid cryptosystem for secure streaming of high efficiency H.265 compressed videos in IoT multimedia applications," *IEEE Access*, vol. 8, pp. 128548–128573, 2020.
- [20] O. Faragallah, A. Afifi, W. El-Shafai, H. El-Sayed, E. Naeem *et al.*, "Investigation of chaotic image encryption in spatial and FrFT domains for cybersecurity applications," *IEEE Access*, vol. 8, pp. 42491–42503, 2020.
- [21] ORL database, [Online]. Available: <https://www.cl.cam.ac.uk/research/dtg/attarchive/facedatabase.html> (Accessed on 1 November 2020).
- [22] Fingerprint verification competition, (FVC2000 DB1:Secure desktop scanner by keytronic), [Online]. Available: <http://bias.csr.unibo.it/fvc2000/databases.asp> (Accessed on 1 November 2020).
- [23] CASIA-IrisV3 database, [Online]. Available: <http://www.cbsr.ia.ac.cn/english/IrisDatabase.asp> (Accessed on 1 November 2020).
- [24] CASIA palm print image database, [Online]. Available: <http://biometrics.idealtest.org/dbDetailForUser.do?id=5> (Accessed on 1 November 2020).
- [25] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Optics Letters*, vol. 20, no. 7, pp. 767–769, 1995.
- [26] P. Kumar, J. Joseph and K. Singh, "Optical image encryption using a jigsaw transform for silhouette removal in interference-based methods and decryption with a single spatial light modulator," *Applied Optics*, vol. 50, no. 13, pp. 1805–1811, 2011.
- [27] T. Dang, Q. Truong, T. Le and H. Truong, "Cancellable fuzzy vault with periodic transformation for biometric template protection," *IET Biometrics*, vol. 5, no. 3, pp. 229–235, 2016.
- [28] S. Sree and N. Radha, "Cancellable multimodal biometric user authentication system with fuzzy vault," in *Proc. IEEE Int. Conf. on Computer Communication and Informatics*, Coimbatore, India, pp. 1–6, 2016.
- [29] E. B. Tarif, S. Wibowo, S. Wasimi and A. Tareef, "A hybrid encryption/hiding method for secure transmission of biometric data in multimodal authentication system," *Multimedia Tools and Applications*, vol. 77, no. 2, pp. 2485–2503, 2019.
- [30] R. F. Soliman, G. M. El Banby, A. D. Algarni, M. Elsheikh, N. F. Soliman *et al.*, "Double random phase encoding for cancelable face and iris recognition," *Applied Optics*, vol. 57, no. 35, pp. 10305–10316, 2018.
- [31] R. F. Soliman, M. Amin and F. E. Abd El-Samie, "A modified cancelable biometrics scheme using random projection," *Annals of Data Science*, vol. 6, no. 2, pp. 223–236, 2019.
- [32] A. D. Algarni, G. M. El Banby, N. F. Soliman, F. E. A. El-Samie and A. M. Iliyasu, "Efficient implementation of homomorphic and fuzzy transforms in random-projection encryption frameworks for cancellable face recognition," *Electronics*, vol. 9, no. 6, pp. 1046, 2020.