Efficient Generation of Cancelable Face Templates Based on Quantum Image Hilbert Permutation

Hesham Alhumyani 1, Ghada M. El-Banby 2, Hala S. El-Sayed 3, Fathi E. Abd El-Samie 4,5 and Osama S. Faragallah 6,*

1 Department of Computer Engineering, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia; h.alhumyani@tu.edu.sa
2 Department of Industrial Electronics and Control Engineering, Faculty of Electronic Engineering, Menoufiya University, Menouf 32952, Egypt; ghadaelbanby75@gmail.com
3 Department of Electrical Engineering, Faculty of Engineering, Menoufiya University, Shebin El-Kom 32511, Egypt; hall_hhh@yahoo.com
4 Department of Electronics and Electrical Communication Engineering, Faculty of Electronic Engineering, Menoufiya University, Menouf 32952, Egypt; fathi_sayed@yahoo.com
5 Department of Information Technology, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia
6 Department of Information Technology, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia
* Correspondence: o.salah@tu.edu.sa

Abstract: The pivotal need to identify people requires efficient and robust schemes to guarantee high levels of personal information security. This paper introduces an encryption algorithm to generate cancelable face templates based on quantum image Hilbert permutation. The objective is to provide sufficient distortion of human facial biometrics to be stored in a database for authentication requirements through encryption. The strength of the proposed Cancelable Biometric (CB) scheme is guaranteed through the ability to generate cancelable face templates by performing the scrambling operation of the face biometrics after addition of a noise mask with a pre-specified variance and an initial seed. Generating the cancelable templates depends on a strategy with three basic steps: Initialization, Odd module, and Even module. Notably, the proposed scheme achieves high recognition rates based on the Area under the Receiver Operating Characteristic (AROC) curve, with a value up to 99.51%. Furthermore, comparisons with the state-of-the-art schemes for cancelable face recognition are performed to validate the proposed scheme.

Keywords: cancelable biometrics; quantum transformation; scrambling

1. Introduction

Document fraud, identity theft, terrorism, and cybercrime are serious issues that need to be considered and studied carefully. Therefore, security solutions have been extended widely to face unauthorized access to modern systems with abundant data communication. Biometric solutions are reliable security solutions that depend on physical or behavioral analysis for authentication of persons [1–3]. Biometric technologies are classified according to the required application as follows: physiological against behavioral, mono-modal against multimodal, cooperative against non-cooperative, contact against touchless, near against remote, server-based against mobile-based, and human against automated.

Universally, biometric systems are adopted for security in several applications such as forensics, surveillance, logical and physical access control, attendance management, etc. However, biometric systems are recommended wherever identification and authentication are critical. Recently, biometric technology has flourished greatly, particularly in identity...
documents based on individual specific characteristics in a short time. For distinguishing individuals, biometric identifiers involve statistical analysis for physiological and behavioral measurements [4–15].

Physiological patterns may be morphological, such as the iris, retina, face, hand shape, fingerprint, and vein pattern, or non-morphological such as the DNA, blood, saliva, urine, and police forensics. The most common behavioral measurements involve gesture, gait, voice, keystroke, signature dynamics, etc. Masek provided a well-known algorithm with its open-source code for iris recognition [16]. It depends on the circular Hough transform with some sort of pre-processing for initial iris localization. The science of biometric recognition is rapidly evolving in several applications using different modalities such as fingerprint, face, iris, hand geometry, ear, and gait, which are discussed and covered in detail in [17].

The main objective of this research is to present a CB recognition scheme based on quantum image Hilbert permutation. Flexible Quantum Image Representation (FRQI) is proposed to allow image representation on quantum computers in the form of a natural model. The FRQI captures and transforms image information into normalized quantum states based on colors and positions in order to allow better management of image information. The strategy adopted in this scheme is used to save the original biometrics from being stored in databases, and use their encrypted versions instead. The verification or identification task is implemented on the encrypted versions through correlation estimation and thresholding. Each user has the ability to change his templates through a user-specific operation. That is why the proposed CB scheme improves both biometrics security and users privacy. The proposed scheme also maintains high accuracy of operation.

The remainder of this paper is sectioned as follows. The state-of-the-art work is explored in Section 1. Preliminaries of the FRQI, in addition to Hilbert image scrambling and quantum gates, are presented in Section 3. The design of the proposed CB recognition scheme based on quantum encryption is introduced in Section 4. Tests with quantitative and qualitative evaluation are given in Section 5. Conclusions are finally discussed in Section 6.

2. Related Work

The biometric authentication systems are more effective than conventional Personal Identification Number (PIN)/password-based authentication systems, which are not protected [18]. The authors of [19] presented a fusion-based multimodal system with enhanced verification accuracy, larger feature space, and higher security against spoofing than those of the unimodal biometric systems. This scheme depends on extracting features such as finger-vein, fingerprint, retina, and then key generation via the Rivest-Shamir-Adleman (RSA) algorithm. The system has been evaluated experimentally using MATLAB 2014, which showed high performance with a Genuine Acceptance Rate (GAR) of 95.3% and a False Acceptance Rate (FAR) of 0.01%.

A biometric template authentication scheme was presented by applying secret sharing [20]. This scheme stores the generated shared specifics of the biometric templates in the database and a Radio Frequency Identification (RFID) card, leading to a robust and secure database. A biometric system was initiated for personal authentication to provide digital security. The authors of [21] introduced a scheme for face recognition based on a patching technique and 2D Discrete Wavelet Transform (2D-DWT). A patching strategy was suggested to reflect the structural features of the face image and retain the integrity of local information for all samples. Patches of training and testing samples are obtained by applying a patch segmentation strategy. To examine the validity of the recognition method, several experiments were carried out on several face datasets such as FERET, Extended Yale B, and LFW. The results demonstrated that this scheme provides good performance compared to the recent conventional 2D-DWT and the state-of-the-art cancelable face recognition techniques. In [22], multimodal biometrics have been used to solve the problems of unimodal biometrics such as non-universality, effect of noise and low security. The partition-based DWT and the 2D Principal Component Analysis (2D PCA) were employed
for extracting image features. The obtained results for this unimodal scheme demonstrated an acceptable performance with Equal Error Rates (EERs) of 0.16 and 0.24 for face and palm print recognition, respectively. On the other hand, results obtained for the multimodal scheme are better with a 0.08 EER.

In [23], biometric features were used for implementing steganography via the image skin tone region. The Hue, Saturation and Value (HSV) color space is used for detecting the skin color tone. Furthermore, the DWT is employed for data embedding in a high-frequency sub-band through tracing the skin pixels in order to present a decoder key. This steganography achieved higher security with a satisfactory Peak Signal-to-Noise Ratio (PSNR).

Although biometric identification is a unique research field, it suffers from some problems, such as security and privacy limitations. Security limitations are represented in the ability of intruders to capture the original biometrics or their features. On the other hand, privacy limitations are represented in the inability of users to change or modify their biometrics, when using them in an identification or a verification system. To avoid these limitations, there is a need for biometric systems that allow the user to secure his biometrics either through non-invertible transforms or through encryption. Moreover, the user should have the ability to generate his user-specific templates from his biometrics. The CB recognition schemes are good candidates for this task. Both encryption and non-invertible transforms can be used in these schemes. With CB recognition schemes, the cancelable templates could be reissued if compromised.

Biometric template protection schemes are classified into biometric cryptosystems and intended distortion systems. The objective of template protection is to generate intentionally distorted templates for enrolling them in the authentication process. Such schemes are designed with the potential of meeting the irreversibility, high performance and unlinkability criteria [24].

In [25], a survey of CB recognition schemes was presented revealing their merits and drawbacks. This survey covered several challenges of the CB recognition schemes. In addition, this survey presented high-security CB recognition schemes depending on Discrete Cosine Transform (DCT), non-invertible functions and Huffman encoding. In [26], the authors presented alignment-free cancelable fingerprint recognition schemes with the aid of blind system identification. These schemes were studied on FVC2002 DB1, DB2, and DB3 datasets. Their results demonstrated good performance represented in alignment-free templates. However, the generated templates cannot be canceled and reissued, when the biometric authentication system is attacked. The authors of [27] introduced a CB recognition scheme with the potential of increasing privacy and security of biometric templates based on left and right irises as input biometric traits. Results showed that all template protection requirements were achieved with good recognition performance.

In [28], a steganography-based CB recognition for iris images was introduced using non-invertible transforms. A non-invertible function is combined with Huffman encoding and DCT to perform some sort of modification of the iris coefficients extracted through the DCT. This scheme guarantees high security, since it is impossible to regenerate the source iris template from the stego iris template with an improved segmentation and normalization process.

The study in [29] presented a fingerprint template protection scheme based on feature-level fusion structures. This scheme depends on local and distant structures as bit strings to compute the transformed features. Bit-string feature-level-based fusion is employed to create the cancelable templates. This scheme achieved 2.19, 1.6 and 6.14% in ERR, when applied on FVC 2002 Database DB1 through DB3 and 11.89, 12.71, and 17.6% EER when applied on FVC 2004 DB1 through DB3. In [30], the authors addressed security and privacy issues arising from the use of CB templates. The introduced random distance transformation method changes the original user biometric identity to a pseudo-biometric identity to store and match. The experimental results proved good matching performance. In addition, this transformation was tested for unlinkability, non-invertibility, and resistance
to different types of attacks such as dictionary, record, false accept, multiplicity and brute-force attacks.

In [31], a comparative study, based on discrete transforms with matrix rotation, was presented to achieve revocability. The implemented tests for all transformations proved efficiency of the presented CB recognition schemes. The authors of [32] presented a face/fingerprint CB recognition scheme based on 3D jigsaw transformation with optical encryption. This scheme was validated using several groups of face and fingerprint images. The results obtained demonstrated that it is secure, feasible, and reliable. In [33], the Indexing-First-One (IFO) hashing-based cancelable iris recognition scheme was presented to achieve the balance between accuracy and privacy requirements. This scheme depends on two efficient mechanisms: modulo threshold function and P-order Hadamard product, to increase the IFO hashing strength. Experiments on the CASIA-v3 iris benchmark database ensured efficient performance in the presence of several security and privacy attacks. In [34], the authors proposed two secure key agreement protocols based on biometrics. They depend on the analysis of fingerprints to achieve security and complexity of reconstruction. These protocols were tested against complexity, brute-force, replay, and impersonation attacks to prove their quality.

Quantum image processing has some preliminaries including Qubit Lattice, quantum wavelet transform [35], quantum discrete cosine transform [36] and quantum Fourier transform [37], which are more efficient in quantum computations than classical ones. Based on quantum image representation methods [38–44], quantum image encryption approaches were investigated in both spatial domain and frequency domain [45]. In [46], Ye et al. proposed a cryptosystem based on an improved diffusion mechanism. It is designed with two stages. The first one is multi-image compression, and the second one is the encryption process based on quaternion discrete fractional Hartley transform. They achieved good results in the presence of different attacks. In [47], the authors presented an encoding system based on generalized Arnold transform with double random phase encoding. Their algorithm showed effective encryption with low complexity. Zhou et al. [48] designed an encryption scheme based on wavelet transform and 3D encryption. They achieved a high security level.

In [49], both wavelet fusion and fractional chaotic systems were exploited for digital face encryption. This scheme was experimentally verified on FERET, LFW, and ORL datasets. Evaluation metrics revealed EER close to zero and 100% AROC at low and mild noise scales. To protect face templates, a cancelable transform, namely Nonlinear Multi-dimension Spectral Hashing (NMDSH) was presented in [50]. The NMDSH transforms a real-valued deep face feature vector into a binary code with a strong non-inverting property. Experimental results with and without attacks proved that the NMDSH has no impact on the system accuracy. The authors of [51] built a CB recognition scheme based on a speeded-up robust features approach to extract and select features. Experiments were conducted on Yale and ORL datasets producing an acceptable performance.

In [52], two CB recognition schemes for template protection were presented. A trous Wavelet Transform (AWT) is applied to divide the face image into seven sub-bands, followed by Homomorphic Filter Masking (HFM) encoding. The second scheme is applied for features detection of Facial Expression Recognition (FER). This is performed through a segmentation procedure using Canny edge detection and Hough Transform (HT). Simulation results proved success of both schemes.

3. Preliminaries: Quantum Image Processing (QIP)

Quantum Image Processing (QIP) is a research area that depends on the image representation using quantum information and quantum operators. Unlike classical theory, quantum theory concepts depend on qubits [53]. The FRQI model involves information
about the color and the corresponding pixel position in an image. The general quantum representation of an image of size $2^n \times 2^n$ is given by the following mathematical relation:

$$ I(\theta) = \frac{1}{2^n} \sum_{i=0}^{2^n-1} |c_i\rangle \otimes |i\rangle $$  \hspace{1cm} (1)

where

$$ |c_i\rangle = \cos \theta_i |0\rangle + \sin \theta_i |1\rangle, \quad \theta_i \in \left[0, \frac{\pi}{4}\right], \quad i = 0, 1, \ldots, 2^n - 1 $$  \hspace{1cm} (2)

The Hilbert scanning matrix is vital to allow image scrambling by performing permutation on each pixel to a new position to transform a meaningful image into a distorted non-meaningful encrypted image. Therefore, the Hilbert scanning matrix is given by the following relations [54]:

$$ H_{n+1} = \left\{ \begin{array}{ll}
H_n & \text{if } n \text{ is even} \\
(4^n+1)E_n + H_n^T & \text{if } n \text{ is odd}
\end{array} \right. $$  \hspace{1cm} (5)

where $n$ represents a positive integer. The initial matrix is

$$ H_1 = \begin{pmatrix}
1 & 2 \\
4 & 3
\end{pmatrix} $$

and

$$ E_n = \begin{pmatrix}
1 & 1 & \cdots & 1 \\
1 & 1 & \cdots & 1 \\
\vdots & \vdots & \ddots & \vdots \\
1 & 1 & \cdots & 1
\end{pmatrix} $$

For $n = 1$, the $2 \times 2$ FRQI template image will be described by the following equation:

$$ |I\rangle = \frac{1}{2} \left( (\cos \theta_0 |0\rangle + \sin \theta_0 |1\rangle) \otimes |00\rangle + (\cos \theta_1 |0\rangle + \sin \theta_1 |1\rangle) \otimes |01\rangle + (\cos \theta_2 |0\rangle + \sin \theta_2 |1\rangle) \otimes |10\rangle + (\cos \theta_3 |0\rangle + \sin \theta_3 |1\rangle) \otimes |11\rangle \right) $$  \hspace{1cm} (4)

The geometric transformation of the matrix image $A$ in the form $2^m \times 2^m$ is given as follows:

$$ A = \begin{pmatrix}
a_{1,1} & a_{1,2} & \cdots & a_{1,m} \\
a_{2,1} & a_{2,2} & \cdots & a_{2,m} \\
\vdots & \vdots & \ddots & \vdots \\
a_{m,1} & a_{m,2} & \cdots & a_{m,m}
\end{pmatrix} $$
Then,

\[
A^T = \begin{pmatrix}
    a_{1,1} & a_{2,1} & \cdots & a_{m,1} \\
    a_{1,2} & a_{2,2} & \cdots & a_{m,2} \\
    \vdots & \vdots & \ddots & \vdots \\
    a_{1,m} & a_{2,m} & \cdots & a_{m,m}
\end{pmatrix}
\]

\[
A^{0l} = \begin{pmatrix}
    a_{1,1} & a_{1,2} & \cdots & a_{1,m} \\
    a_{2,1} & a_{2,2} & \cdots & a_{2,m} \\
    \vdots & \vdots & \ddots & \vdots \\
    a_{m,1} & a_{m,2} & \cdots & a_{m,m}
\end{pmatrix}
\]

\[
A^{ud} = \begin{pmatrix}
    a_{1,1} & a_{2,1} & \cdots & a_{m,1} \\
    a_{1,2} & a_{2,2} & \cdots & a_{m,2} \\
    \vdots & \vdots & \ddots & \vdots \\
    a_{1,m} & a_{2,m} & \cdots & a_{m,m}
\end{pmatrix}
\]

\[
A^{pp} = \begin{pmatrix}
    a_{1,1} & a_{2,1} & \cdots & a_{m,1} \\
    a_{1,2} & a_{2,2} & \cdots & a_{m,2} \\
    \vdots & \vdots & \ddots & \vdots \\
    a_{1,m} & a_{2,m} & \cdots & a_{m,m}
\end{pmatrix}
\]

The scrambling process of the original image is composed of the three basic operations as illustrated in Figure 1, including initialization, Even and Odd modules. The size of the Hilbert scanning matrix begins with \(2 \times 2\) and increases gradually with each operation step. The scrambling starts with partitioning of the image into blocks and working on each block according to Equation (1). PARTITION (0) is performed in the initialization step to divide the \(2^n \times 2^n\) input image into \(2^{n-1} \times 2^{n-1}\) sub-images with size \(2 \times 2\). Then, each block is denoted by \(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\). Next, swapping operation is performed on the last two pixels of every sub-image to be \(\begin{pmatrix} a & b \\ d & c \end{pmatrix}\). Then, PARTITION (1) divides the output image into \(4 \times 4\) sub-images. This is followed by an Odd module that changes every block into \(\begin{pmatrix} a & \text{d}_{pp} \\ b^T & c^T \end{pmatrix}\). Then, the Even module is performed to generate \(\begin{pmatrix} a & \text{d}_{pp} \\ b^T & c^T \end{pmatrix}\). The Odd and Even modules are performed, alternatively, until Even \((n-1)/\text{Odd}(n-1)\) that is if \((n-1)\) is an even value, the final operation is Even \((n-1)\); otherwise, the final operation will be Odd \((n-1)\).

Figure 1. The general Hilbert scrambling quantum scheme.

4. Cancelable Face Recognition Based on Quantum Image Distortion

This section introduces the methodology to accomplish our proposed scheme to generate robust cancelable templates to achieve a high security level for the original biometric templates against thefts and attacks. The proposed scheme is illustrated in Figure 2, where the scrambling approach is performed on the raw images in the enrollment stage. The generated encrypted templates are stored in the database for further matching.
processes in the authentication phase. The generated cancelable templates are obtained through the Hilbert scrambling strategy with three basic steps: Initialization, Odd and Even modules. The cancelable templates are produced as follows:

Step 1: The procedure starts with PARTITION (0) to generate $2 \times 2$ sub-images in the form $(i, i+1, i+2, i+3)$.

Step 2: Swapping operation is performed for the last two pixels of every sub-image by the C-Not gate.

Step 3: $4 \times 4$ sub-images are generated through PARTITION (1). Odd and Even modules are used to complete the scrambling process.

If a generated distorted template is compromised, the proposed CB recognition scheme can generate a new different distorted template that completely differs from the compromised one by adding a noise mask to the original biometric image according to an initial seed and a certain variance. The newly generated template will be totally different from the other stored templates in the database.

Figure 2. The proposed QIP-based CB recognition scheme.

5. Performance Evaluation and Test Results

Quantitative and qualitative analysis are introduced in this work. The proposed facial recognition scheme is implemented using MATLAB running on Intel Core™ i5-4210U with 1.7 GHz CPU. The goal is to overcome illegal access and attacks. Therefore, we propose an efficient scheme based on QIP to be resistant to intrusion attacks. Samples of biometric face images used in this study are selected from the Mass Labeled Faces in the Wild (LFW) dataset [55], Olivetti and Oracle (ORL) dataset [56], and NIST Face Recognition Technology (FERET) dataset [57]. Different evaluation metrics are used for investigating the proposed scheme robustness. Furthermore, a comparison is introduced between the proposed scheme and other existing ones based on fuzzy domain and homomorphic domain to demonstrate and ensure the effectiveness of the proposed scheme.

We consider three different datasets to examine the encryption algorithm performance and enrich the validation scheme. The size of all templates is $128 \times 128$. The original samples of the three datasets are presented in Figure 3, with distorted versions shown in Figure 4. The distributions of histograms for the original samples and the encrypted samples illustrated in Figures 5 and 6 prove that the scrambling process based on Swapping
operation, Odd module and Even module permutes and shuffles sufficiently each pixel position to perform effectual distortion without changing pixel gray levels.

Another important metric used to evaluate the performance of the encryption algorithm is the correlation coefficient, which is used for measuring the correlation between distorted output templates in the enrollment phase and the new distorted facial images. The correlation coefficient can be evaluated as follows:

\[ R_{xy} = \frac{1}{N} \sum_{i=1}^{N} (x_i - \bar{x})(y_i - \bar{y}) \frac{\sigma_x \sigma_y}{\sigma_x \sigma_y} \]  

(6)

where \( N \), \( x \) and \( y \) are the number of pixels, the current stored distorted encrypted version, and the newly distorted template.

Figure 3. Cont.
Figure 3. Samples of face images used as original biometrics [55–57]. (a) LFW dataset [55]. (b) FERET dataset [57]. (c) ORL dataset [56].

Figure 4. Cont.
Figure 4. Encrypted versions of biometric faces in Figure 3 based on QIP. (a) Samples of LFW encrypted templates. (b) Samples of FERET encrypted templates. (c) Samples of ORL encrypted templates.

Figure 5. Cont.
Figure 5. Histograms of facial image samples for (a) LFW dataset, (b) FERET dataset, (c) ORL dataset.

Figure 6. Cont.
where $\mu_{AROC}$ is as high as possible, revealing more robustness and strength of the proposed FERET dataset, (Figure 6. Histograms of encrypted facial image samples based on QIP for (a) LFW dataset, (b) FERET dataset, (c) ORL dataset.

Figure 7 illustrates the correlation coefficient values evaluated among the authorized biometrics and their corresponding counterparts stored in the enrollment phase with noise for all encrypted templates. In addition, Figure 8 illustrates the calculated correlation coefficient scores for all impostor and unauthorized records. The output scores in both Figures 7 and 8 demonstrate that all correlation values for authorized patterns are greater than 0.7, while those correlation values for unauthorized patterns are lower than 0.25. Hence, a threshold score may be adopted ranging from 0.25 to 0.7 to distinguish between authorized and unauthorized patterns. Using such a wide range for setting the threshold, the proposed scheme achieves a high security level.

The ROC curves are shown in Figure 9 for better grasping and understanding of the results. The True Positive Rate (TPR) versus the False Positive Rate (FPR) was studied in [58–61]. The TPR and the FPR are used to assess the authentication performance. The AROC is as high as possible, revealing more robustness and strength of the proposed scheme. The probability distributions of the correlation scores for both authorized and unauthorized tests are given in Figure 10.

The congruity evaluation metrics, such as Structural Similarity Index Metric (SSIM), are employed to measure the similarity between two templates. For example, an acceptable SSIM value to test the encryption quality between original and encrypted images should be close to zero. Mathematically, SSIM can be computed as in Equation (7) [62] to evaluate the distortion strength.

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

where $\mu_x$ and $\mu_y$ are the means of the images $x$ and $y$, respectively, $\delta_x^2$, and $\delta_y^2$ denote the two images variances, $\delta_{xy}$ is the cross-covariance between them, $S_1$ and $S_2$ are selected as small as possible according to [63].
Figure 7. Correlation scores for authorized patterns based on QIP for (a) LFW dataset, (b) FERET dataset, (c) ORL dataset.
Figure 8. Correlation scores for unauthorized impostor patterns based on QIP for (a) LFW dataset, (b) FERET dataset, (c) ORL dataset.
Figure 9. ROC curves for the proposed CB recognition scheme based on QIP for (a) LFW dataset, (b) FERET dataset, (c) ORL dataset.
Figure 10. Probability distributions for the proposed CB recognition scheme based on QIP for (a) LFW dataset, (b) FERET dataset, (c) ORL dataset.
Table 1 ensures the high performance and the robustness of the proposed CB recognition scheme by displaying the scores of evaluation metrics. These metrics include the AROC and SSIM scores among the stored and impostor patterns, and the correlation score distribution for authorized and unauthorized patterns. These presented metrics are used to demonstrate and prove the superiority of the proposed CB recognition scheme. The obtained results of high AROC values of 0.9951 on average for the three different datasets in addition to the low values of SSIM indicate the strength of the proposed scheme to be applied for authentication applications. Finally, Table 2 presents a comparison with state-of-the-art CB recognition schemes from the AROC perspective. The suggested CB recognition scheme is superior compared to the others.

Table 1. Evaluation metrics of the QIP-based cancelable face recognition scheme on three different datasets.

<table>
<thead>
<tr>
<th>Dataset</th>
<th>AROC</th>
<th>SSIM</th>
<th>Authorized Mean Correlation</th>
<th>Unauthorized Mean Correlation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quantum encryption for LFW</td>
<td>0.9963</td>
<td>0.021</td>
<td>0.9026</td>
<td>0.0522</td>
</tr>
<tr>
<td>Quantum encryption for FERET</td>
<td>0.9992</td>
<td>0.121</td>
<td>0.9569</td>
<td>0.0527</td>
</tr>
<tr>
<td>Quantum encryption for ORL</td>
<td>0.9897</td>
<td>0.011</td>
<td>0.8882</td>
<td>0.0414</td>
</tr>
</tbody>
</table>

Table 2. Comparison with state-of-the-art CB recognition schemes from the AROC perspective.

<table>
<thead>
<tr>
<th>Method</th>
<th>AROC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quantum encryption scheme</td>
<td>0.9951</td>
</tr>
<tr>
<td>IFL followed by Gaussian RP [64]</td>
<td>0.9720</td>
</tr>
<tr>
<td>Homomorphic transform followed by Gaussian RP [63]</td>
<td>0.9774</td>
</tr>
<tr>
<td>FRFT only [64,65]</td>
<td>0.8837</td>
</tr>
<tr>
<td>Jigsaw only [66]</td>
<td>0.8967</td>
</tr>
</tbody>
</table>

6. Conclusions

This paper presented a cancelable biometric recognition scheme that depends on QIP concepts. A scrambling and permutation algorithm was proposed to generate the cancelable encrypted templates to be stored in the database for authentication. The proposed scheme allows securing of biometric templates from unauthorized access. In addition, it allows changing the biometric templates if compromised through the addition of a user-specific noise mask. The proposed scheme was evaluated and tested on three distinct datasets to take into consideration the anticipated variations in lighting conditions, and background. Simulation and comparison results revealed an average AROC of 0.9951 and an average SSIM of 0.051 for the proposed scheme. These findings reveal that the proposed scheme is a good candidate for biometric security in remote access systems. In future work, our research plan is to work on multiple biometrics to generate robust cancelable templates. In addition, deep learning will be considered for robust feature extraction in CB recognition systems.

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

Funding: This study was funded by the Deanship of Scientific Research, Taif University Researchers Supporting Project number (TURSP-2020/216), Taif University, Taif, Saudi Arabia.


Acknowledgments: The authors would like to thank the Deanship of Scientific Research, Taif University Researchers Supporting Project number (TURSP-2020/216), Taif University, Taif, Saudi Arabia for supporting this research work.

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

References


46. Ye, H.; Zhou, N.; Gong, L. Multi-image compression-encryption scheme based on quaternion discrete fractional Hartley transform and improved pixel adaptive diffusion. *Signal Processing* 2020, 175, 107652. [CrossRef]

47. Zhou, N.R.; Hua, T.X.; Gong, L.H.; Pei, D.J.; Liao, Q.H. Quantum image encryption based on generalized Arnold transform and double random-phase encoding. *Quantum Inf. Processing* 2015, 14, 1193–1213. [CrossRef]


52. Ashiba, H.I. Proposed framework for cancelable face recognition system. *Multimed. Tools Appl.* 2021, 80, 13677–13705. [CrossRef]


