Intelligent Automation & Soft Computing
DOI:10.32604/iasc.2021.014694
Article

Tech Science Press

Hybrid Multimodal Biometric Template Protection

Naima Bousnina[1], Sanaa Ghouzali[2,*], Mounia Mikram[1,3], Maryam Lafkih[1], Ohoud Nafea[4], Muna Al-Razgan[2] and Wadood Abdul[4]

[1]LRIT—CNRST URAC No. 29, IT Center, Faculty of Sciences, Mohammed V University, Rabat, 10000, Morocco
[2]Department of Information Technology, College of Computer and Information Sciences, King Saud University, Riyadh, 11451, Saudi Arabia
[3]Meridian Team, LYRICA Laboratory, School of Information Sciences, Rabat, 10000, Morocco
[4]Department of Computer Engineering, College of Computer and Information Sciences, King Saud University, Riyadh, 11451, Saudi Arabia
*Corresponding Author: Sanaa Ghouzali. Email: sghouzali@ksu.edu.sa
Received: 09 October 2020; Accepted: 01 November 2020

Abstract: Biometric template disclosure starts gaining an important concern in deploying practical biometric authentication systems, where an assailant compromises the database for illegitimate access. To protect biometric templates from disclosure attacks, biometric authentication systems should meet these four requirements: security, diversity, revocability, and performance. Different methods have been suggested in the literature such as feature transformation techniques and biometric cryptosystems. However, no single method could satisfy the four requirements, giving rise to the deployment of hybrid mechanisms. In this context, the current paper proposes a hybrid system for multimodal biometric template protection to provide robustness against template database attacks. Herein, a secure sketch method is first applied to secure the fingerprint modality. Subsequently, a Dual-Tree Complex Wavelet Transform Discrete Cosine Transform (DTCWT-DCT) based watermarking is employed to entrench the fingerprint sketch into the face image. However, a 3D chaotic-map-based encryption method is employed to protect the watermarked facial image in order to offer an added security level. The experimentation performed using the ORL face database and three Fingerprint Verification Competition (FVC) fingerprint databases showed the approach's efficiency in withstanding standard digital image watermarking attacks, brute force attacks, and information leakage. Moreover, the results revealed that the approach achieves high performance, and satisfies diversity and revocability requirements.

Keywords: Biometric template protection; secure sketch; watermarking; image; encryption; 3D chaotic map; hybrid

1 Introduction

Regarding to the rapid spread of digital technology that renders a large amount of digital information created and delivered many times in a second, a higher level of security is required. Hence, biometric

technology is presented as an alternative solution to replace the conventional token-based (e.g., passport, ID card) or knowledge-based (e.g., password, PIN code) personal identification techniques. Contrary to the traditional systems that cannot satisfy the increased security requirements, biometrics-based-authentication systems easily distinguish between fraudulent and authorized users, based on behavioral (e.g., speech, gait, signature dynamics) or physiological characteristics (e.g., face, iris, fingerprint) of the person. Generally, biometric authentication mechanisms include enrolment and authentication phases. While the enrolment phase acquires the biometric data from the genuine user, processes it, and stores it in the database as a reference, the authentication phase extracts the characteristics vector from the biometric inquiry data to be compared with reference features vector to grant or deny access.

Although biometric authentication systems provide a high level of performance, they are still vulnerable toward various sorts of attacks [1]: (1) *Attacks on the user sensor* (e.g., spoofing and mimicry attacks); (2) *Attacks on the interface between modules*; (3) *Attacks on software modules*; and (4) *Attacks on the system's database*. The devastating attack is the one on the templates database because the attacker gains illegitimate access to the database and can subsequently replace/usurp the biometric templates. To secure the biometric data, many methods are proposed in the literature. Primarily, the methods of protecting biometric template are classified into two classes: (1) *Feature transformation* [2]; and (2) *Biometric cryptosystems* [3]. Feature transformation approach transforms biometric features with a specific password/key producing a reference biometric model to be deposited in the system's database. Feature transformation methods are either invertible (salting) or non-invertible. Biometric cryptosystem technique links the biometric data with a secret key to generate a biometric data known as "helper data," kept as a reference in the database. Considering the secret key's generation mode, there exist two sorts of biometric cryptosystems: (1) *Key binding* (e.g., fuzzy commitment [4] and fuzzy vault [5,6]); and (2) *Key generation* (e.g., fuzzy extractors [7] and secure sketches [8–11]). A comprehensive survey of feature transformation and biometric cryptosystem approaches is introduced in [12].

Meanwhile, biometric watermarking has been considered as complementary techniques to secure biometric data in authentication systems [13]. Biometric watermarking methods offer a high-security level to the authentication system, where the embedded data would not be recovered using only a secret key. Moreover, the embedded data are kept linked to the cover image and thus no additional transfer resources or storage mechanisms are needed. However, watermarking directly affects the original image's perceptual transparency by making certain distortions on the image pixels during the watermark embedding process. Furthermore, cryptographic techniques also provide a higher level of security as it is computationally difficult to retrieve the original template from the generated one without knowing the encryption key. Therefore, conventional cryptography is not suitable for biometric templates, giving rise to numerous techniques for image encryption to cope with the speed and variability constraints [14].

Biometric template protection approaches should satisfy four criteria including security, revocability, diversity, and performance. However, no single technique fulfils the four constraints of biometric template protection at a time. Hence, several hybrid approaches that combine different methods, are proposed in the literature to achieve more requirements (e.g., [10,15–22]). An extensive review that analyzes different existing biometric template protection methods is presented in [23]. In this context, the current work proposes a multimodal biometric authentication-based hybrid approach to improve the effective security and efficiency of authentication systems against template database attacks. The underlying concept of this approach is to combine: (1) Dual-Tree Complex Wavelet Transform Discrete Cosine Transform-based watermarking; (2) secure sketch; and (3) 3D chaotic map image encryption. Fusing two biometric modalities (face and fingerprint) increases the authentication performance and security. Fingerprints are chosen because they provide a high verification rate, while face modality is typically used in our daily recognition tasks.

The process of the approach adheres to the following steps: first, the secure sketch is used to provide the security of the original fingerprint features. Next, because of secure sketch non-revocability and incapability to model intra-user variations, the blind DTCWT-DCT-based watermarking method is employed to entrench the fingerprint sketch (used as watermark) into the facial image (used as a cover image). The underlying concept in this technique is to fuse the fingerprint features and face images to relate each to other. The DTCWT domain frequency decomposition is used due to the high-frequency sub-bands that provide additional security level during the watermark integration. Further, the DCT scheme is used given its withstanding of various watermarking attacks such as noising, compressing, sharpening, and filtering. Finally, the 3D chaotic map image encryption method is employed to secure the facial watermarked image. This encryption method is chosen because of its sensitivity to initial status, control parameters, non-convergence, non-periodicity and robustness against brute force attacks.

The rest of the paper is organized as follows. Section 2 describes the proposed hybrid approach in detail. The experimental results are discussed in Section 3, providing an analysis of the four biometric requirements of the proposed hybrid approach. The conclusion is presented in Section 4.

2 Proposed Approach

The current section provides a description of the overall framework and a detailed overview of the suggested approach components.

2.1 Overall Framework Description

Fig. 1 illustrates a chart of the suggested template protection algorithm. As shown in this diagram, the algorithm comprises two phases: Enrolment and Authentication.

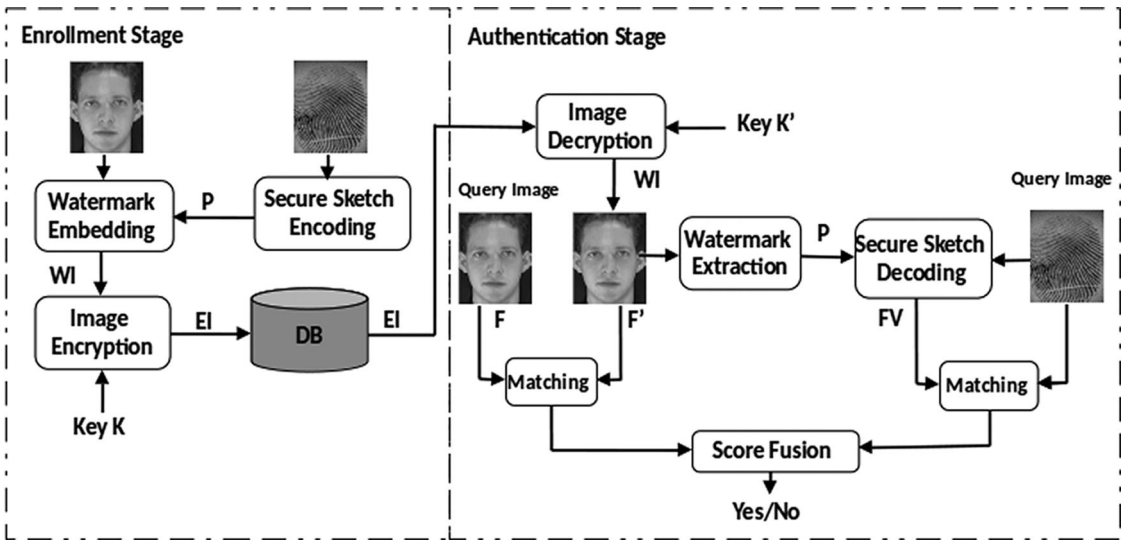

Figure 1: Proposed hybrid biometric template protection approach

- *Enrolment phase:* In this stage, we applied the secure sketch encoder to the extracted and preprocessed fingerprint features to ensure their security, thus, sketch P is generated. Next, we used the watermarking algorithm to embed the sketch P considered as a watermark into the facial image used as a cover image. Further, the watermarked facial image (WI) is then encrypted using a chaos-based simple encryption

technique via a user key K to enhance the security level. Furthermore, the encrypted watermarked facial image (EI) is warehoused in the database as a public reference.

- *Authentication phase:* Herein, the genuine user provides a key K' supposed to be the same as the enrolment key K. If the keys are not identical, it is asserted as an assailant. Otherwise, the user is requested to present her/his face, and fingerprint (query images). Subsequently, the reference image EI is restored from the system's database and decrypted using the key K' to recover the WI. Then, two parallel matching processes are carried out. The facial characteristics are taken out from both the query and reference facial images via the Orthogonal Locality Preserving Projections (OLPP) scheme introduced in [24], hence, two features sets F' and F are respectively obtained, binarized, and compared based on the Hamming distance metric, which generates the facial modality score S_{face}. Meanwhile, the watermark sketch P is extracted from the decrypted watermarked face image. Subsequently, the secure sketch decoder function is applied to generate a features vector FV to be matched with the features vector of the fingerprint query image using the Hamming distance metric that generates the fingerprint modality score $S_{fingerprint}$. To determine whether the authentication is successful, the score-level fusion method of the face and the fingerprint individual matching scores is employed. The Performance-Anchored Normalization method is used in this work to compute the scores of both modalities [25]. Next, the scores are merged via the weighted sum rule with an appropriate distribution of weights selected by the Equal Error Rate (EER) during the training stage. The weight, υ, is allocated to the score of the face modality S_{face}, while the weight, ω, is allocated to the score of the fingerprint modality $S_{fingerprint}$. Finally, the matching score of the multimodal biometric authentication system is computed as:

$$S_m = \upsilon S_{face} + \omega S_{fingerprint} \tag{1}$$

The biometric authentication system accepts or rejects an individual by comparing the matching score S_m to a threshold η.

2.2 Framework Components Description

In this section, the main components of the suggested approach are described, including secure sketch, watermarking, and image encryption algorithms.

2.2.1 Secure Sketch Algorithm

The secure sketch is a key generation biometric cryptosystem method that has been recently suggested to expand the conventional cryptographic metrics in biometric data (e.g., [8–11]). This scheme includes two blocks: encoder and decoder. While the encoder gets the authentic biometric data X as input and generates a sketch, the decoder combines the sketch with another biometric data Y to output a template X'. If Y and X are adequately identical, the equation $X = X'$ will be satisfied. The direct minutiae matching process is avoided in the proposed secure sketch algorithm due to two primary reasons. First, the proposed authentication system uses an extensive database, implying that, the minutiae-based matching strategy would not satisfy the fast-performance speed requirement. Second, fingerprint minutiae representation cannot be applied directly to a template-based secure sketch, since the minutiae extraction does not provide the same number of minutiae for different fingerprint images, whereas a fixed-length feature vector is needed as an input in a secure sketch algorithm. To solve these problems, the spectral minutiae representation is utilized rather than the minutiae sets. Hence, the minutiae points are depicted as a spectral characteristics' vector of fixed length after being elicited from the fingerprint image through the minutiae extraction system presented in [26]. More precisely, suppose that Z minutiae points are taken out from the fingerprint image, with (x_i, y_i, θ_i) the location and orientation of the i^{th} minutia and

$(\omega_x,\ \omega_y, \sigma_o^2)$ the frequencies and the parameters of the Gaussian kernel function, respectively. $m_i\ (x,\ y, \theta)$ the derivative of $m_i(x,\ y) = \delta(x\ -\ x_i,\ y\ -\ y_i)$ in the direction θ_i, and δ the Dirac Pulse metric. The minutiae exemplification is carried out using Eq. (2) [27]:

$$M_o(\omega_x,\ \omega_y, \sigma_o^2)\ =\ \left| e^{-\left(\frac{\omega_x^2\ +\ \omega_y^2}{2\sigma_o^2}\right)} \times \sum_{i=1}^{Z} \Gamma(m_i(x,\ y, \theta)) \right| \tag{2}$$

where Γ is the Fourier transform defined as:

$$\Gamma(m_i(x,\ y, \theta))\ =\ j(\omega_x \cos(\theta_i)\ +\ \omega_y \sin(\theta_i) \times e^{-j\left(\omega_x x_i\ +\ \omega_y y_i\right)} \tag{3}$$

As the obtained minutia representation is sizable dimensionality, the Column Principal Component Analysis (CPCA) features reduction approach addressed in [28] is utilized to reduce the spectral features vector size. This metric is used to obviate the large dimensionality problems such as template storage and computational burden requirements. Next, the minimized features vector is quantized based on the quantization technique presented in [27]. The engendered vector is joined with the Reed-Solomon codeword SR using the exclusive OR (XOR) to generate the sketch P.

In the secure sketch decoding phase, the same process is carried out on the query fingerprint image to construct the features vector. This vector is subsequently XORed with the sketch P retrieved from the system's database. The result is further decoded using the Reed-Solomon decoder function to retrieve the codeword SR′ that is supposed to be near to the codeword SR with correct authentication. Finally, the features vector is restored by XORing P and SR′. To determine whether the authentication is successful, the obtained features' vector is compared to the query fingerprint image features vector according to the Hamming distance. Secure sketch encoding and decoding processes are illustrated in Fig. 2.

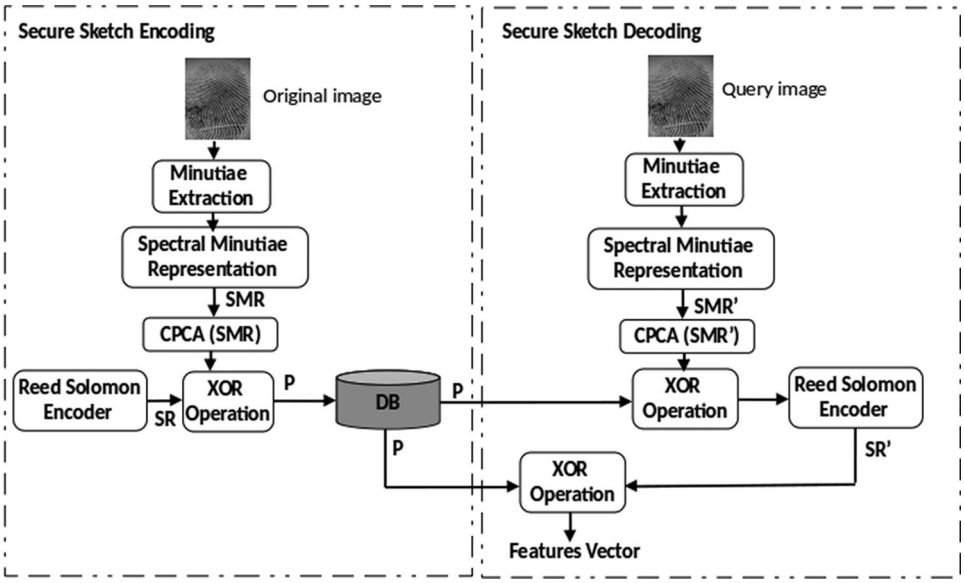

Figure 2: Block diagram of the secure sketch scheme for the fingerprint template

The security of secure sketch relies on the difficulty to estimate the original data, given that a small quantity of data is seeped out when the sketch is revealed. Therefore, an efficient solution is to restrain

assailants from determining the biometric template using a compromised sketch. In [7,29], the authors suggested the use of *entropy loss* to measure the sketch's information leakage, which gives an adversary the advantage to estimate the original information from a given sketch. In our study, the informal definition of *entropy loss*— also known as mutual information— is used. It measures the quantity of information communicated on average between the sketch P and the original fingerprint features vector F as follows:

$$\zeta(F;P) = \sum_{f\in F}\sum_{p\in P} H(f,\ p)\log\left(\frac{\mathrm{H(f,p)}}{\mathrm{H(f)H(p)}}\right) \tag{4}$$

where H(F) and H(P) are the marginal distributions of F and P.

2.2.2 Watermarking Algorithm

Digital watermarking is one of the leading protection expedients that has been effectively employed to protect the biometric templates (e.g., [30–38]). The watermarking algorithm used in this study relies on the DTCWT and DCT as two domain transform mechanisms. The concept used in this algorithm is to entrench the watermark with less disfigurement in the facial image while allowing blind watermark extraction via the correlation method. The DTCWT algorithm is designed to exhibit directional selectivity, which is reliable with the Human Visual System (HVS).

The watermark embedding stage starts by dismantling the facial image using one level DTCWT decomposition. Next, three high-frequency sub-bands are arbitrarily chosen and divided into 4×4 blocks. Then, the DCT transform is applied on each 4×4 block. After that, the watermark bits are integrated with a gain factor μ into the DCT transformed 4×4 blocks using two produced pseudorandom series PN_0 and PN_1 to integrate the 0 and 1 watermark bits, respectively. Finally, we execute the inverse DCT and inverse DTCWT to construct the watermarked facial image.

In the watermark extraction stage, the same procedure as in the watermark embedding stage is carried out on the watermarked facial image to obtain the DCT transformed blocks. Then, for each DCT transformed block, the mid-band coefficients are retrieved, and two correlations C_0 and C_1 are computed with PN_0 and PN_1, respectively. In case $C_0 < C_1$, the readout watermark bit is deemed 1; otherwise, it is deemed 0. The detailed information about the DTCWT-DCT-based watermarking algorithm used in this framework are found in [37].

Unlike the DTCWT-based watermarking algorithm indicated in [39] that inserts the watermark into coefficients of the sub-band with an angle of $\pm 45^o$, our approach's watermarking scheme enhances the security by randomly selecting three high-frequency sub-bands of the DTCWT decomposition. In [39], while the watermark is integrated directly into the DTCWT coefficients, the embedding is carried out in our approach by manipulating only the coefficients of the middle-frequency DCT sub-bands to affect less the lucidity of the watermarked cover image, and to prevent against compression attacks. This choice is due to two reasons: first, the high-frequency elements of the image are removed through noise attacks and compression. Second, most of the signal energy is located at low-frequency DCT sub-bands that contain the pertinent visual parts of the image.

2.2.3 Image Encryption Algorithm

Chaos-based image encryption is one of the most widely used image security for biometric template protection (e.g., [40–46]). The chaos map employed in the proposed approach is the logistic map. It is chosen due to its simplicity and reduced complexity. Eq. (5) illustrates the 1D logistic map and the 3D formula is given in Eq. (6), where $0 < x_n < 1$ and $\mu = 4$ are the conditions to render the equation chaotic; $0 < \beta < 0.022$, and $0 < \alpha < 0.015$ are the growth rates, and the initial values of x, y and z, respectively, in between 0 and 1.

$$x_{n+1} = \mu x_n(1 - x_n) \tag{5}$$

$$\begin{aligned} x_{n+1} &= \gamma x_n(1 - x_n) + \beta y_n^2 x_n + \alpha z_n^3 \\ y_{n+1} &= \gamma y_n(1 - y_n) + \beta \gamma z_n^2 y_n + \alpha x_n^3 \\ z_{n+1} &= \gamma y_n(1 - z_n) + \beta x_n^2 z_n + \alpha y_n^2 \end{aligned} \tag{6}$$

In this study, the 3D chaotic map encryption metric consists of a coupling of pixel value transformation, pixel position switching, and a nonlinear 3D chaos-based simple encryption scheme. Suppose $M \times N$ are the image dimensions. $[x_0, y_0, z_0, \alpha, \beta, \gamma, N1, N2, N3, N4, N5, N6]$ is the encryption/decryption key, where x_0, y_0, and z_0 are the initial values of the 3D logistic map population x, y, and z, respectively. $N2$, $N4$, $N6$ are large random numbers used to equalize the histogram of the generated logistic map (see Eq. (7)), while $N1$, $N3$, $N5$, are used as the first index to select the chaos x, y, and z, respectively. As illustrated in Fig. 3, the proposed encryption strategy comprises the following stages [47]:

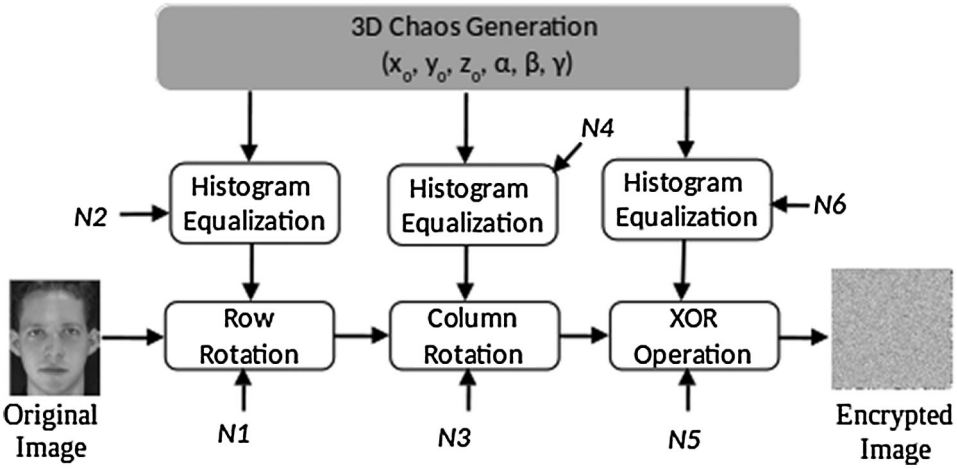

Figure 3: Encryption technique using 3D chaos

- Generate a 3D logistic map based on Eq. (6) to obtain the logistic map x, y, and z.
- Equalize the histogram of the logistic map using Eq. (7) to improve the security level. The histogram equalization is performed owing to the non-uniform distribution of the logistic map histogram.

$$\begin{aligned} x &= (integer(x \times N2))mod(N) \\ y &= (integer(y \times N4))mod(M) \\ z &= (integer(z \times N6))mod(512) \end{aligned} \tag{7}$$

- Permute the image pixels via a row rotation approach. This starts by arbitrary generating a considerable number $N1$; subsequently, choose M number of chaos x starting from index $N1$. Next, rotate the pixels based on chaos value x. If the x value is even, rotate to the left; if it is odd, rotate to the right.
- Permute the image pixels via a column rotation approach. This starts by generating a sizable random number $N3$; subsequently, select N numbers of chaos y from index $N3$. Perform rotation according to the y value. If the y value is even, rotate up; if it is odd, rotate down.

Applying row and column rotation generates an encrypted image with an unaltered histogram, that may fail toward histogram attacks. To overcome this issue, the XOR operation is applied as an added step. The underlying concept of this step is to change the image pixel value to a new value and prevent the retrieval of the original value without the chaos key. Therefore, a large random number $N5$ is generated; subsequently,

the $M \times N$ image is reshaped into a $1 \times MN$ vector. Finally, the XOR operation is applied between the $1 \times MN$ vector and the z chaos from the index $N5$ to obtain the encrypted image.

In the decryption stage, the encrypted image is first reshaped into a $1 \times MN$ vector. Then, it is XORed with the z chaos using $N5$. Next, the inverse column rotation and inverse row rotation are applied. In the inverse column rotation, the $1 \times MN$ vector is reshaped into an $M \times N$ image; subsequently, based on $N3$ and the y value, the rotation process is applied. If the y value is even, we rotate down; if it is odd, we rotate up. To get the original image, the inverse row rotation is applied using $N1$ and the x value. If the x value is even, we rotate to the right; if it is odd, we rotate to the left.

3 Experimental Results

3.1 Experiments Setting

Extensive tests have been carried out to assess the efficiency of the suggested hybrid approach using the ORL face database and three FVC databases: FVC2002 DB1, DB2, and FVC2000 DB1. 512×512 pixels facial images and fingerprint images of size 374×388,560 $\times 296$, and 300×300 pixels are obtained from FVC2002 DB1, DB2, and FVC2000 DB1, respectively. These images were divided into three datasets: *Dataset1* (ORL with FVC2002 DB1), *Dataset2* (ORL with FVC2002 DB2), *Dataset3* (ORL with FVC2000 DB1).

Stratifying the spectral minutiae representation on the extracted minutiae points, feature matrices of $128 \times 256 = 32768$ are obtained. After applying the CPCA features reduction metric, where only the pertinent features are selected, and the feature quantization method, a 10240-bits binary stream is generated (sketch P).

In the watermarking process, only three 256×256 high-frequency sub-bands are arbitrarily chosen from the six high-frequency sub-bands generated via the one level DTCWT decomposition. The decomposition of each selected high-frequency sub-band produces 64×64 blocks of dimension 4×4 each. Moreover, to get an optimal watermarking imperceptibility and good robustness against image watermarking attacks, the watermarking algorithm has been examined for various values of the gain factor μ among a range of 0 to 60. The conducted experiments demonstrated that the convenient values are $\mu = 20$, $\mu = 30$, and $\mu = 40$ for the first, second, and third high-frequency sub-bands. Besides, various values among a range of 0 to 1 are assigned to weights values υ allocated to the score of the facial system and ω allocated to the fingerprint system's score. The values of $\upsilon = 0.5$ and $\omega = 0.5$, which provide the maximum authentication performance, are chosen. Moreover, as the midb and frequencies of a DCT block have seven coefficients, pseudorandom sequences PN_0 and PN_1 of length seven are generated. To implement the encryption approach, $N2 = N4 = N6 = 100000$, $N1 = 500$, $N3 = 600$, and $N5 = 700$ are considered.

3.2 Results and Discussions

In this section, we put forward and discuss the evaluation results of the carried out tests to demonstrate the efficiency of the suggested approach in meeting the four requirements of biometric authentication systems.

3.2.1 Security Analysis

Three scenarios are considered below to assess the security of the suggested approach.

- *Compromised encrypted image scenario*

Suppose that the database is attacked and the encrypted facial image is stolen. It is typically computationally difficult for the attacker to estimate the key and decrypt the image due to the encryption key's large keyspace. The keyspace refers to the set of all possible permutations of a key; in other words, it is given as the span of distinct potential values of a key. It should be sufficiently large to minimize the

likelihood of an effective brute force attack. For instance, a password with n characters, where each of these characters assumes C different values, has a keyspace size of C^n [48].

In the suggested 3D chaotic map encryption method, six initial conditions x_0, y_0, z_0, α, β, and γ with precision 10^{-16} are used. Consequently, the keyspace size is $(10^{16})^6$. Additionally, $N1$, $N2$, $N3$, $N4$, $N5$ and $N6$ are used as random keys of precision 10^5, implying that the keyspace size is $(10^5)^6 = 10^{30}$. Consequently, the keyspace size is larger than 10^{126}, which is sufficiently immense to withstand exhaustive attacks. Moreover, the suggested image encryption method is sufficiently secure to be sensitive to slight changes in the decryption key.

- *Compromised watermarked image scenario*

Suppose that the encrypted image is compromised and decrypted to get the watermarked facial image. The experimental results demonstrated the strength of the suggested watermarking algorithm against conventional digital image watermarking attacks, namely JPEG compression, Gaussian noise, speckle noise, salt and pepper noise, median filter, and additive white Gaussian noise. The evaluation is then reported using the correlation coefficient, Peak Signal-to-Noise Ratio (PSNR), and EER. The correlation coefficient and the PSNR are utilized to measure the quality of the extracted watermark and the integration deformation, respectively, whereas, the EER is employed to assess the authentication system's reliability after applying the attacks. Tab. 1 presents the average of the EER, PSNR, and correlation coefficient values under the aforementioned attacks. From this table, it can be observed that the authentication performance of the watermarking algorithm was not affected by the attacks, where the EER value has been slightly minimized for some attacks. Besides, the PSNR and correlation coefficient values are slightly changed after applying attacks, which demonstrate the watermarking algorithm's ability to withstand these attacks. However, the DTCWT-DCT-based watermarking algorithm does not preserve higher perceptual quality between the original and watermarked face images. This is due to the trade-off between the quality of the extracted watermark after embedding and the quality of the watermarked facial image. More precisely, improving the quality of the watermarked image decreases the quality of the extracted watermark and vice versa.

Table 1: Correlation coefficient, EER, and PSNR values before and after attacks

Attacks	Correlation coefficient	EER (%)	PSNR (dB)
No attack	1	0	30.88
Gaussian noise (Noise density = 0.2)	0.98	0.24	30.86
Salt & pepper (Noise density = 0.001)	0.99	0	29.69
Speckle noise (Noise density = 0.001)	1	0.14	29.92
JPEG compression (80%)	1	0	30.77
Median filter [3 × 3]	1	0.14	30.46
Median filter [5 × 5]	1	0	30.46
AWGNA (mean = 0 and variance = 0.0001)	1	0.14	29.45
AWGNA (mean = 0 and variance = 0.0003)	1	0.14	30.32

- *Compromised sketch scenario*

Assuming that the encrypted image is compromised and decrypted, and the embedded sketch is extracted. In this case, the attacker attempts to estimate the original fingerprint features vector, given that the sketch is revealed. Since sketch P is generated using the fingerprint images, the entropy loss is calculated only over the FVC databases. In our experiments, the mutual information is calculated for each

couple (F, P) of each image. Then the average of the mutual information is calculated for all images of each dataset. The average of the mutual information obtained for each dataset is 2.37×10^{-14}. The gained value shows that a tiny amount of mutual information is shared between the sketch and the original data, indicating that even when the sketch is extracted, the features vector information could not be leaked to the attacker.

3.2.2 Performance Analysis

Different curves are plotted for the three datasets to assess the performance of the proposed system, including the genuine and impostor matching score distribution curves, the False Acceptance Rate (FAR) against the False Reject rate (FRR) curves, and the Receiver Operating Characteristic (ROC) curves. The genuine and impostor scores are generated via the FVC standard protocol [49]. Fig. 4 presents the genuine and impostor distributions related to the suggested hybrid system for the three datasets. It is noteworthy from the sub-figures that the scores are not overlapped, demonstrating the presented approach's efficiency in discriminating between genuine and impostor users. The curves are well separated for *Dataset1* and *Dataset2* at the threshold's value 0.4517 and 0.4514, respectively, and slightly overlapped for *Dataset3* at the threshold range [0.8879,1.0521].

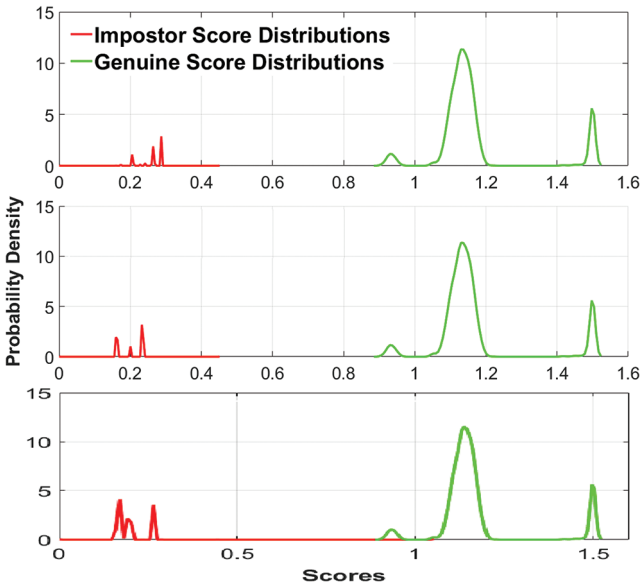

Figure 4: Genuine and impostor matching score distribution curves of the proposed hybrid system for the three datasets: *Dataset1*, *Dataset2*, and *Dataset3* from top to down

Besides, the approach's authentication performance is attested by computing the EER and the FAR as opposed to the FRR values. The smallest of the value of the EER is the preferable, proving that the system is less likely to falsely admit impostors as genuine or falsely reject genuine as impostors. Fig. 5 shows the FAR as opposed to the FRR curves of the proposed system for the three different datasets. As can be observed from this figure, the proposed method reached lower EER values of 0%, 0%, and 0.12% on *Dataset1*, *Dataset2*, and *Dataset3*, respectively. Also, FRR/FAR values of 0.0083/0.2140% for the threshold 0.4512, 0.0080/0.2141% for the threshold 0.4510, and 0.0095/0.2074% for the threshold 0.9184 are obtained over the three databases, respectively. These results demonstrated the high performance and reliability of the authentication approach.

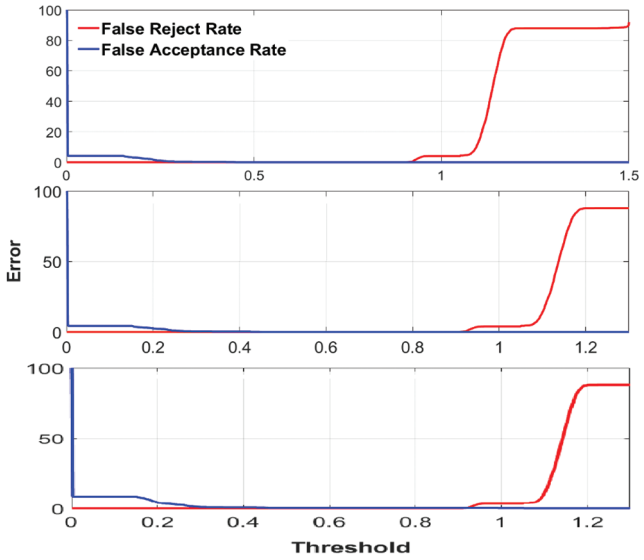

Figure 5: FAR *vs.* FRR curves of the proposed hybrid system, for the three datasets: *Dataset1*, *Dataset2*, and *Dataset3* from top to down

In Fig. 6, the ROC curves illustrated the authentication performance of the different approaches: face-based, fingerprint-based, and the proposed fingerprint-face-based multimodal. The three sub-figures in Fig. 6 show that the fingerprint-based authentication approach performs weaker than the face-based authentication approach since the minutiae extraction process does not provide the same number of minutiae for different fingerprint images of the same user. Additionally, significant performance improvement is shown for the fingerprint-face-based multimodal authentication system, as the accuracy of 100% is achieved, similar to the face-based authentication system. The obtained results indicated that the watermarking algorithm did not degrade the system's performance while improving the system's security due to the combination of two different modalities and the score fusion method's effectiveness.

3.2.3 Diversity and Revocability Analysis

A template protection approach meets the diversity criteria if it generates multiple uncorrelated templates from the same original features vectors, allowing users to register in distinct applications based on the same features without the risk of cross-matching between the corresponding databases. In comparison, the revocability requirement indicates the capability to revoke a template that has been breached and generate a novel one. The typical means to verify that a template protection method meets both properties is by producing multiple protected templates from the same original templates and different keys, and subsequently attempting to match the resulting sets of protected templates. Regarding the diversity criterion, the matching is derived using the True Rejection Rate (TRR) that measures the percentage of time the system (correctly) rejects a user with a distinct key. In our experiments, the obtained TRR values are 99.50%, 99.35%, and 98.94% for *Dataset1*, *Dataset2*, and *Dataset3*, respectively, which proves the suggested approach to be embedded into various applications without databases cross-matching. Regarding the revocability property, the matching is accomplished using the EER metric, where an EER value of 0% is obtained for each of the three datasets, indicating that the intra-class variation is preserved. Therefore, canceling a template that has been breached and generating a novel one will not change or affect the authentication system.

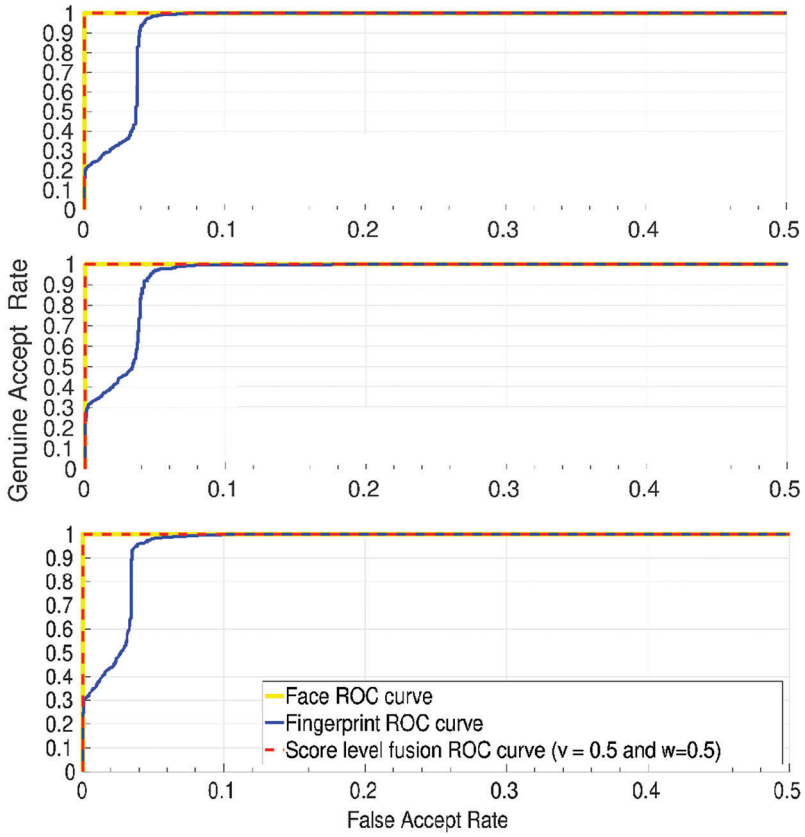

Figure 6: ROC curves of the face-based unimodal authentication system, the fingerprint-based unimodal authentication system, and the fingerprint-face-based multimodal authentication system for the three datasets *Dataset1*, *Dataset2*, and *Dataset3* from top to down

3.2.4 Computational Complexity

To examine the computational complexity of the suggested hybrid approach, the run time has been recorded during the authentication stage, which is the most crucial phase required to be carried out in real time. As illustrated in Fig. 1, this phase includes the image decryption, watermark extraction, and secure sketch decoding. All the algorithms were implemented in MATLAB and run on an Intel Core(TM) 2 Duo CPU P7450 at 2.13 GHz with 4 GB of memory. The run time is recorded during the experiments carried out over all the databases of 320 images. The average time obtained is 2.11 s for the image decryption, 1.36 s for the watermark extraction, and 3.28 s for the sketch decoding process. By adding the average time needed to perform the matching process of 0.31 s, a total average of 7.06 s is attained for the overall authentication phase.

3.2.5 Comparison with Previous Studies

In the current section, a comparison of the suggested approach and the existing studies is presented. However, related studies used various databases and biometric modalities to endorse the efficiency of their suggested methods. Consequently, a useful comparison with our hybrid approach cannot be carried out. Tab. 2 outlines the biometric template protection methods suggested in the literature (based on watermarking, secure sketch, and image encryption methods), and their biometric modalities, criteria satisfaction, and performance results. It can be seen from this table that the suggested hybrid approach has evident advantages over the existing studies in terms of satisfying all the four requirements of biometric authentication systems.

Table 2: Summary of different biometric template protection approaches

Reference	Biometric modality	Database	Performance	Requirements (S: Security, R: Revocability, D: Diversity)
[9]	Fingerprint	FVC2000	EER = 1.4 %	S
		University of Twente database	EER = 1.6 %	
[15]	Face	Face94	FRR< 0.2% FAR< 0.2%	S R
[18]	Face	CMU PIE	GAR = 78.43%	S
		FEI	GAR = 55.7%	
		Extended Yale B	GAR = 66.5%	
[20]	Face & Fingerprint	FVC2002 DB1 & ORL	EER = 0%	S R D
[21]	Face & Fingerprint	FVC2002 DB1 & ORL	EER = 3.87%	S D
[22]	Iris	CASIA	FAR = 0% GAR = 98.70 %	S
[29]	Fingerprint & Face	Essex Faces94 & NIST	FRR = 1.4% FAR = 0.58%	S
[30]	Fingerprint & Face	ORL & FVC2002 DB2	EER = 0.96%	S
[31]	Iris & Fingerprint	FVC2004 & CASIA	EER = 1.2%	S
[35]	Face & Fingerprint	Biosecure	EER = 6.5%	S
[37]	Face & Fingerprint	ORL & FVC2002 DB1	EER = 0%	S
[38]	Face & Fingerprint	Biosecure	EER = 7.77%	S
Proposed Hybrid Approach	Face & Fingerprint	ORL & FVC2002 DB1	EER = 0% FRR = 0.0083 % FAR = 0.2140 % GAR = 99.99 %	S R D
		ORL & FVC2002 DB2	EER = 0% FRR = 0.0080 % FAR = 0.2141 % GAR = 99.99 %	
		ORL & FVC2000 DB1	EER = 0.12% FRR = 0.0095 % FAR = 0.2074 % GAR = 99.99 %	

The algorithms presented in [22,30,37] satisfied only the security and performance requirements. In [22], the authors combined cryptography and steganography to secure the storage of iris templates. The work discussed in [37] employed the same DTCWT-DCT-based watermarking algorithm used in the current work to improve the performance and security of the authentication system. Moreover, the methods presented in [9,18,29,31,35,38] achieved lower performance than the presented work, while

ensuring the security criteria. These approaches used a single protection technique based on watermarking [31,35,38] or secure sketch [9,29].

The methods described in [13,20,21] satisfied more requirements, which demonstrated the advantage of using the hybrid approach. In [20], a DWT-SVD-based watermarking approach is employed to fuse the face and fingerprint features. Subsequently, a shuffling algorithm is carried out on the watermarked image, which is then XORed with a chaotic map and a Hadamard code to achieve the randomization and orthogonality of protected biometric features. This approach satisfied all the four requirements. However, its main drawback is that it is applicable only for biometric modality represented as an ordered set (e.g., face). This issue of using an ordered set of biometric modalities is improved in our proposed work as we used a fingerprint image as a cover image and manipulated its features using a face image. The results in [20] and our current work indicated a high recognition rate for all conditional cases, except when the noise levels are too high. In [21], the authors demonstrated how to integrate the fingerprint traits into various directional DWT sub-bands of the face image. Subsequently, each user is associated with a unique key and a hyper-chaotic map is employed to generate a keystream to encipher the watermarked image. This approach satisfied the security and diversity requirements. However, a lower level of performance (EER = 3.87%) is reached compared to our method.

4 Conclusion

A hybrid multimodal biometric template protection approach to provide robustness against template database attacks in biometric authentication systems is proposed in this work. Herein, the approach combines three techniques to satisfy jointly four requirements of biometric authentication systems, including security, diversity, revocability, and performance. The concept underlying the suggested approach starts by securing the fingerprint features using the secure sketch method. Subsequently, the obtained sketch is embedded in the face image based on a DTCWT-DCT watermarking approach. Finally, the watermarked face image is secured via a 3D chaotic map-based image encryption method.

Extensive experiments were carried out on the ORL face dataset and three FVC databases, including FVC2002 DB1, DB2, and FVC2000 DB1, to evaluate the suggested system. The experimental results showed a high level of security. An excellent matching performance is also achieved with EER values of 0%, 0%, and 0.12% for the three datasets, respectively. Moreover, the diversity and revocability constraints are achieved, indicating the approach's ability to be embedded into various applications without databases cross-matching. Hence, our work makes a significant improvement compared with the existing related studies in meeting the four requirements at a time, due to its use of four potential points: multimodality, secure sketch, biometric watermarking, and chaotic map-based image encryption.

Nevertheless, as biometric authentication systems become familiar to the general public, they become frail to spoofing attacks where an assailant can readily get the biometric data from social networks to generate sophisticated models to deceive the authentication system. This attack raises the challenge of dealing with systems database attacks as well as imposters. In this regard, we intend in the future work to investigate in developing an anti-spoofing approach to distinguish between genuine and fake users.

Acknowledgement: Researchers Supporting Project No. (RSP-2020/206), King Saud University, Riyadh, Saudi Arabia.

Funding Statement: Researchers Supporting Project No. (RSP-2020/206), King Saud University, Riyadh, Saudi Arabia.

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

References

[1] A. K. Jain, K. Nandakumar and A. Nagar, "Biometric template security," *EURASIP Journal on Advances in Signal Processing*, vol. 2008, no. 1, 579416, 2008.

[2] A. Nagar, K. Nandakumar and A. K. Jain, "Biometric template transformation: A security analysis," in *Media Forensics and Security II, Part of the IS&T-SPIE Electronic Imaging Symposium*, San Jose, California, USA, 2010.

[3] U. Uludag, S. Pankanti, S. Prabhakar and A. K. Jain, "Biometric cryptosystems: Issues and challenges," *Proceedings of the IEEE*, vol. 92, no. 6, pp. 948–960, 2004.

[4] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *6th ACM Conf. on Computer and Communications Security*, pp. 28–36, 1999.

[5] A. Juels and M. Sudan, "A fuzzy vault scheme," *Designs, Codes and Cryptography*, vol. 38, no. 2, pp. 237–257, 2006.

[6] H. M. Patel, C. N. Panuwala and A. Vora, "Hybrid feature level approach for multi-biometric cryptosystem," in *Int. Conf. on Wireless Communications, Signal Processing and Networking*, Chennai, India, pp. 1087–1092, 2016.

[7] Y. Dodis, L. Reyzin and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *Int. Conf. on the Theory and Applications of Cryptographic Techniques. Proceedings: Lecture Notes in Computer Science*, Interlaken, Switzerland, pp. 523–540, 2004.

[8] Q. Li, Y. Sutcu and N. Memon, "Secure sketch for biometric templates," in *int. conf. on the Theory and Application of Cryptology and Information Security. Proceedings: Lecture Notes in Computer Science*, Shanghai, China, pp. 99–113, 2006.

[9] C. Fang, Q. Li and E. C. Chang, "Secure sketch for multiple secrets," in *Int. Conf. on Applied Cryptography and Network Security. Proc.: Lecture Notes in Computer Science*, Beijing, China, pp. 367–383, 2010.

[10] J. Bringer, H. Chabanne and B. Kindarji, "The best of both worlds: Applying secure sketches to cancelable biometrics," *Science of Computer Programming*, vol. 74, no. 1–2, pp. 43–51, 2008.

[11] Y. Sutcu, Q. Li and N. Memon, "Protecting biometric templates with sketch: theory and practice," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 3, pp. 503–512, 2007.

[12] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP Journal on Information Security*, vol. 2011, no. 1, pp. 42011.

[13] J. Hämmerle-Uhl, K. Raab and A. Uhl, "Watermarking as a means to enhance biometric systems: A critical survey," in *Int. Workshop on Information Hiding. Proc.: Lecture Notes in Computer Science*, Prague, Czech Republic, pp. 238–254, 2011.

[14] M. Kumari, S. Gupta and P. Sardana, "A survey of image encryption algorithms," *3D Research*, vol. 8, no. 4, pp. 567, 2017.

[15] T. K. Dang, Q. C. Truong, T. T. B. Le and H. Truong, "Cancellable fuzzy vault with periodic transformation for biometric template protection," *IET Biometrics*, vol. 5, no. 3, pp. 229–235, 2016.

[16] Y. J. Chin, T. S. Ong, A. B. J. Teoh and K. O. M. Goh, "Integrated biometrics template protection technique based on fingerprint and palmprint feature-level fusion," *Information Fusion*, vol. 18, pp. 161–174, 2014.

[17] H. Kaur and P. Khanna, "Biometric template protection using cancelable biometrics and visual cryptography techniques," *Multimedia Tools and Applications*, vol. 75, no. 23, pp. 16333–16361, 2016.

[18] S. Nazari, M. S. Moin and H. R. Kanan, "Securing templates in a face recognition system using error-correcting output code and chaos theory," *Computers & Electrical Engineering*, vol. 72, pp. 644–659, 2018.

[19] A. Sardar, S. Umer, C. Pero and P. Nappi, "A novel cancelable FaceHashing technique based on non-invertible transformation with encryption and decryption template," *IEEE Access*, vol. 8, pp. 105263–105277, 2020.

[20] O. Nafea, S. Ghouzali, W. Abdul and E. H. Qazi, "Hybrid multi-biometric template protection using watermarking," *Computer Journal*, vol. 59, no. 9, pp. 1392–1407, 2016.

[21] W. Abdul, O. Nafea and S. Ghouzali, "Combining watermarking and hyper-chaotic map to enhance the security of stored biometric templates," *Computer Journal*, vol. 63, no. 3, pp. 479–493, 2020.

[22] 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 and Applications*, vol. 79, no. 31–32, pp. 23483–23506, 2020.

[23] A. Sarkar and B. Singh, "A review on performance, security and various biometric template protection schemes for biometric authentication systems," *Multimedia Tools and Applications*, vol. 79, no. 37–38, pp. 27721–27776, 2020.

[24] D. Cai, X. He, J. Han and H. J. Zhang, "Orthogonal laplacianfaces for face recognition," *IEEE Transactions on Image Processing*, vol. 15, no. 11, pp. 3608–3614, 2006.

[25] N. Damer, A. Opel and A. Nouak, "Performance anchored score normalization for multi-biometric fusion," in *Int. Sym. on Visual Computing. Proc.: Lecture Notes in Computer Science*, Rethymnon, Crete, Greece, pp. 68–75, 2013.

[26] A. El-Sisi, "Design and implementation biometric access control system using fingerprint for restricted area based on Gabor filter," *International Arab Journal of Information Technology*, vol. 8, no. 4, pp. 355–363, 2011.

[27] Haiyun Xu, R. N. J. Veldhuis, A. M. Bazen, T. A. M. Kevenaar, T. A. H. M. Akkermans *et al.,* "Fingerprint verification using spectral minutiae representations," *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 3, pp. 397–409, 2009.

[28] Haiyun Xu, Veldhuis R. N. J., Kevenaar T. A. M. and Akkermans T. A. H. M., "A fast minutiae-based fingerprint recognition system," *IEEE Systems Journal*, vol. 3, no. 4, pp. 418–427, 2009.

[29] Y. Sutcu, Q. Li and N. Memon, "Secure biometric templates from fingerprint-face features," in *IEEE Conf. on Computer Vision and Pattern Recognition*, Minneapolis, MN, USA, pp. 1–7, 2007.

[30] N. Bousnina, S. Ghouzali, M. Lafkih, O. Nafea and M. M. *et al.,* "Watermarking for protected fingerprint authentication," in *12th Int. Conf. on Innovations in Information Technology,* Al-Ain, United Arab Emirates, pp. 1–5, 2016.

[31] B. Ma, C. Li, Y. Wang, Z. Zhang and Y. Wang, "Block pyramid based adaptive quantization watermarking for multimodal biometric authentication," in *20th Int. Conf. on Pattern Recognition*, Istanbul, Turkey, pp. 1277–1280, 2010.

[32] M. Paunwala and S. Patnaik, "Biometric template protection with DCT-based watermarking," *Machine Vision and Applications*, vol. 25, no. 1, pp. 263–275, 2014.

[33] S. Ghouzali, "Watermarking based multi-biometric fusion approach," in *Int. Conf. on Codes, Cryptology, and Information Security. Proc.: Lecture Notes in Computer Science*, Rabat, Morocco, pp. 342–351, 2015.

[34] M. A. M. Abdullah, S. S. Dlay, W. L. Woo and J. A. Chambers, "A framework for iris biometrics protection: A marriage between watermarking and visual cryptography," *IEEE Access*, vol. 4, pp. 10180–10193, 2016.

[35] L. R. Haddada, B. Dorizzi and N. E. Ben-Amaraa, "A combined watermarking approach for securing biometric data," *Signal Processing: Image Communication*, vol. 55, pp. 23–31, 2017.

[36] M. R. M. Isa, S. Aljareh and Z. Yusoff, "A watermarking technique to improve the security level in face recognition systems," *Multimedia Tools and Applications*, vol. 76, no. 22, pp. 23805–23833, 2017.

[37] N. Bousnina, S. Ghouzali, M. Mikram and W. Abdul, "DTCWT-DCT watermarking method for multimodal biometric authentication," in *2nd Int. Conf. on Networking, Information Systems & Security*, Rabat, Morocco, pp. 1–7, 2019.

[38] L. R. Haddada and N. E. Ben-Amara, "Double watermarking-based biometric access control for radio frequency identification card," *International Journal of RF and Microwave Computer-Aided Engineering*, vol. 29, no. 5, pp. 1–11, 2019.

[39] K. Zebbiche, F. Khelifi and K. Loukhaoukha, "Robust additive watermarking in the dtcwt domain based on perceptual masking," *Multimedia Tools and Applications*, vol. 77, no. 16, pp. 21281–21304, 2018.

[40] H. I. Hsiao and J. Lee, "Fingerprint image cryptography based on multiple chaotic systems," *Signal Processing*, vol. 113, pp. 169–181, 2015.

[41] S. Ghouzali and W. Abdul, "Private chaotic biometric template protection algorithm," in *IEEE Second Int. Conf. on Image Information Processing*, Shimla, India, pp. 655–659, 2013.

[42] S. Rajendran and M. Doraipandian, "Biometric template security triggered by two dimensional logistic sine map," *Procedia Computer Science*, vol. 143, pp. 794–803, 2018.

[43] M. A. Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez and R. M. López-Gutiérrez, "A robust embedded biometric authentication system based on fingerprint and chaotic encryption," *Expert Systems with Applications*, vol. 42, no. 21, pp. 8198–8211, 2015.

[44] C. Moujahdi, S. Ghouzali, M. Mikram, M. Rziza and G. Bebis, "Spiral Cube for biometric template protection," in *Int. Conf. on Image and Signal Processing. Proc.: Lecture Notes in Computer Science*, Agadir, Morocco, pp. 235–244, 2012.

[45] C. Moujahdi, G. Bebis, S. Ghouzali, M. Mikram and M. Rziza, "Biometric template protection using spiral Cube: performance and security analysis," *International Journal on Artificial Intelligence Tools*, vol. 25, no. 01, pp. 1550027, 2016.

[46] N. A. Hikal and M. M. Eid, "A new approach for palmprint image encryption based on hybrid chaotic maps," *Journal of King Saud University-Computer and Information Sciences*, vol. 32, no. 7, pp. 870–882, 2020.

[47] M. B. Hossain, M. T. Rahman, A. B. M. S. Rahman and S. Islam, "A new approach of image encryption using 3D chaotic map to enhance security of multimedia component," in *Int. Conf. on Informatics*, Dhaka, Bangladesh: Electronics & Vision, pp. 1–6, 2014.

[48] L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication," in *Proc. of the IEEE*, vol. 91, no. 12, pp. 2021–2040, 2003.

[49] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman and A. K. Jain, "FVC2000: Fingerprint verification competition," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 24, no. 3, pp. 402–412, 2002.