IEEE Access
Multidisciplinary ⁝ Rapid Review ⁝ Open Access Journal

Received June 24, 2021, accepted July 12, 2021, date of publication July 16, 2021, date of current version July 27, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3097881

6D-Chaotic System and 2D Fractional Discrete Cosine Transform Based Encryption of Biometric Templates

DHANESH KUMAR[1], ANAND B. JOSHI[1], SONALI SINGH[1], VISHNU NARAYAN MISHRA[2], HAMURABI GAMBOA ROSALES[3], LIANG ZHOU[4], ARVIND DHAKA[5], AMITA NANDAL[5], HASMAT MALIK[6], (Senior Member, IEEE), AND SATYENDRA SINGH[7], (Member, IEEE)

[1]Department of Mathematics and Astronomy, University of Lucknow, Lucknow 226007, India
[2]Department of Mathematics, Indira Gandhi National Tribal University, Amarkantak 484886, India
[3]Faculty of Electrical Engineering, Autonomous University of Zacatecas, Zacatecas 98000, Mexico
[4]Center for Medicine Intelligent and Development, China Hospital Development Institute, Shanghai Jiao Tong University, Shanghai 200240, China
[5]Department of Computer and Communication Engineering, Manipal University Jaipur, Jaipur 303007, India
[6]Berkeley Education Alliance for Research in Singapore (BEARS) Research Center, University of California at Berkeley, University Town, NUS Campus, Singapore 138602
[7]School of Electrical Skills, Bhartiya Skill Development University, Jaipur 302037, India

Corresponding authors: Vishnu Narayan Mishra (vishnunarayanmishra@gmail.com), Liang Zhou (wenzhou6@sjtu.edu.cn), Hasmat Malik (hasmat.malik@gmail.com), and Arvind Dhaka (arvind.neomatrix@gmail.com)

This work was supported in part by the Universidad Autonoma de Zacatecas, Mexico, through the Consejo Nacional de Ciencia y Tecnología (CONACYT) Mexico and the Foundation of National Key Research and Development Program of China under Grant 2020YFC2008700, in part by the National Natural Science Foundation of China under Grant 82072228 and Grant 92048205, in part by the Foundation of Shanghai Municipal Commission of Economy and Informatization under Grant 202001007, in part by the Foundation of Shanghai Jiao Tong University under Grant CHDI-2019-C-02, and in part by the Council of Scientific and Industrial Research, New Delhi, India, under Grant 09/107(0385)/2017-EMR-I.

ABSTRACT A new algorithm for biometric templates using a 6D-chaotic system, and 2D fractional discrete cosine transform (FrDCT) is proposed in this paper. In this technique, the k biometric templates are represented into three groups. After representation, these three groups are converted into row vectors and scrambled by using keys generated by the 6D-chaotic system and after that, these row vectors are combined into three matrices. The three matrices are then mixed horizontally and divided into two halves, with the left half serving as the real part and the right half serving as the imaginary part of a complex-valued matrix (CVM). This CVM is further subjected to 2D FrDCT. The output of 2D FrDCT is separated into three parts. The robustness of the technique is further enhanced by substitution operation using keys generated by the 6D-chaotic system. Thus, the final encrypted template is obtained. The analysis like security, statistical, and attacks are given to authenticate the reliability of the proposed technique. The experimental values also show that the proposed technique is resistant to brute force attacks.

INDEX TERMS Biometric template encryption, decryption, 2D fractional discrete cosine transform, 6D-chaotic system.

I. INTRODUCTION

Biometrics [1] is the automatic assessment of the physical characteristics of human such as the face, fingerprint, iris, and so on. Researchers can now complete any task using different biometric devices due to advances in computerized knowledge. As a result, biometric data must be processed and compressed to ensure privacy and prevent unauthorized access to vital information. In recent years, most digital media including mobile phones and laptops use biometrics. Nowadays, the biometric-based smart attendance system is also getting popular. The biometric-based access granting system is widely used in restricted areas of various investigating agencies. Biometric techniques have inherent enrichment over personal identification number techniques, identification cards, and passwords.

In the present era, assuring the reliability and privacy of biometric data is a vital challenge. The digital biometric data for each human is different but still, it needs a secrecy mechanism. The secrecy risk associated with biometrics lies in biometric modification and reusing the biometric data when it is shared over unsecured open networks like the Internet.

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

That is the main reason to develop a biometric template encryption technique to secure biometric data from attackers. Few authors have used watermarking techniques, data hiding techniques, and encryption techniques to provide security for biometric data [2]–[8].

Cryptography is generally used for encryption, it is a branch of applied mathematics and computer science, contributes several algorithms to image protection. Traditional encryption techniques are ineffective for encrypting images for a variety of reasons, including a lot of similarity between adjacent pixels, a lot of info, and a lot of redundancy. As a result, biometric data security requires special attention, and we suggest an encryption algorithm that can aid in the efficient protection of biometric data.

In recent years, digital cryptosystem [9], [10], optical cryptosystem [11], [12] or a combination of both have been extensively used for encryption of digital biometric templates. Authors have used different transform domains such as hybrid transform [8], Fourier transform [13], [14], wavelet transform [15], [16], Arnold transform [17], and chaotic maps [18], [19] for encryption.

The fractional Fourier transform (FrFT) theorem is critical in the implementation of image encryption. The FrFT's key weakness is that it produces both true and imaginary coefficients, making processing more complex. As a result, this paper uses FrDCT that only produces real coefficients.

Encryption research continues to improve security features such as resistance to various attacks. The high similarity among the adjacent pixels, either horizontally (H), vertically (V), or diagonally (D), is one of the encryption's challenges. Based on the observation from state-of-art methods about encryption techniques, when a certain noise assaults the encrypted picture, several traditional methods suffer substantially. The encryption scheme must have a big keyspace to be healthier. It means that encrypting images in a domain with a higher degree of freedom reinforces the encryption process. Statistical attacks must be resistant to the encryption practice.

In addition to the above, the encryption technique's keys must be extremely sensitive, so that information cannot be recovered by an unauthorized person. Moreover, watermarking is often followed by image encryption. It's done to ensure that the data is sent correctly. As a result, our encryption method must be adaptable enough to accommodate the addition of a watermark signal.

This research paper proposes an encryption technique for biometric templates based on the 6D-chaotic system applied to the 2D-FrDCT coefficients, as a result of the above glimpse of encryption. In this technique, the k biometric templates are represented into three groups. After representation, the three groups are converted into row vectors and are scrambled by using keys generated by the 6D-chaotic system. Then, these scrambled row vectors are converted into three matrices. Further, these three matrices are horizontally concatenated and then divided into two half parts in which the first part is real, and the second is imaginary of a CVM. Then, the 2D FrDCT operation is performed on the CVM. The 2D FrDCT output is broken down into three parts. Each of these components represents a separate biometric template. The substitution operations using keys provided by the 6D-chaotic framework improve the scheme's robustness even further. Thus, the final encrypted template is obtained. To check the performance of the presented system, computer simulations and experimental results were performed on biometric templates. It's also worth noting that the proposed technique stands up to cropping and differential attacks remarkably well.

A. RELATED WORKS

For the security of fingerprint and face, Haddada *et al.* [2] advocated the use of watermarking based cryptosystem. In this process, the application of the twofold watermarking technology ensures a high level of security. Primarily, the local features watermark an individual's original biometric template face, minutia, of one biometric template fingerprint and then the predominantly watermarked biometric template face is placed as extra identifying information into the original biometric template fingerprint. Douglas *et al.* [4] reviewed the Steganography techniques for the preservation of biometric templates. The authors offer an overview of steganography approaches used to preserve biometric templates in fingerprints in this study.

For digital biometric templates security, Tarif *et al.* [5] proposed a encryption and concealing technique for providing security of biometric template in transmission through system for multi-modal biometric identification and authentication. In this method, the biometric (fingerprint and iris) templates are estimated using a stimulated iterative hard thresholding approach and then integrated in the face template's Slantlet-SVD field.

Barrero *et al.* [7] proposed a shared substructure for various biometric template protection based on a homomorphic probabilistic transform approach that only manipulates changed data. An iris template based double image encryption technique was suggested by Rakheja *et al.* [8]. In the frequency domain of the hybrid transform (HT), this technique used a 3D-Lorenz chaotic approach and modified equal modulus decomposition were utilised in this methodology. In this process, Walsh, Kekre, and fractional Fourier transforms of different orders were combined to create HT. The phase part of CVM was used to encrypt the iris template a double image. Rakheja *et al.* [15] later suggested a strategy for protecting hybrid iris templates. This methodology employed a 4D hyperchaotic method and a modified equal modulus decomposition tool in the multi resolution wavelet transform domain.

Barrero *et al.* [20] provided a statistical study of unprotected biometric models to estimate the key parameters of a digital biometric security system. In addition, the authors suggested a protected weighted feature level fusion to improve the efficiency and security of authentication. When compared to unsecured score level fusion, it was discovered that using weighted feature level fusion enhanced authentication accuracy. As a result, the weighted feature level fusion technique improved the system's privacy. Ajish and Kumar [21] proposed an iris template encryption technique using double bloom filter based feature function.

By inserting a different key sequence for each image sequence, the benefit of the pixels permutation to create a noise-resistant encryption scheme can be preserved, resulting in an encryption method that is immune to known image and brute-force attacks. The established image attack is rendered useless for attackers who do not know the initial key by using a different key sequence.

We used a 6D hyperchaotic method on an intermediate ciphertext image to improve the protection of a biometric template in this paper. The settings and beginning circumstances of the 6D hyperchaotic technique must first be considered by the attacker before performing a particular attack.

B. OUTLINE

The following are the remaining parts of this research paper. Section II presents the preliminary knowledge of the 6D-chaotic system, and 2D FrDCT. The proposed biometric template encryption and decryption technique is discussed in Section III. The computer simulation and experimental findings based on the proposed technique are discussed in Section IV. In section V, biometric prototype matching is addressed. The proposed technique's protection is discussed in Section VI. Sections VII and VIII include an attack overview and a comparison of the proposed technique to similar works, respectively. Finally, section IX concludes the proposed technique.

II. PRELIMINARY KNOWLEDGE

This section presents the preliminary knowledge of 6D-chaotic system, and 2D FrDCT.

A. THE 6D-CHAOTIC SYSTEM

The chaotic behavior with at least two positive Lyapunov exponents defines the hyper chaotic attractor. A continuous hyper chaotic structure has a minimum dimension of four. Grassi *et al.* [22] used two same 3D Lorenz chaotic systems and modeled a four wing hyper chaotic system which is represented by Eq. 1,

$$\begin{cases} \dot{u} = a_1(v-u) \\ \dot{v} = a_2u - v - uw + r_1(x-y) \\ \dot{w} = uv - a_3w \\ \dot{x} = a_1(y-x) \\ \dot{y} = a_2x - y - xz + r_2(u-v) \\ \dot{z} = xy - a_3z \end{cases} \tag{1}$$

where a_1, a_2, a_3, and r_1, r_2 are the positive and the coupling parameters. When $a_1 = 10$, $a_2 = 28$, $a_3 = 8/3$ and $r_1 = r_2 = 0.05$. The four wing attractors have been generated by Eq. 1 as shown in Fig. 1. In the proposed technique, the parameters a_1, a_2, a_3, r_1, r_2 and the initial conditions u, v, w, x, y and z are considered to be the secrete keys, to generate the keystream.

B. THE 2D FRACTIONAL DISCRETE COSINE TRANSFORM

A generalization of the DCT is the 2D FrDCT. In the DCT, the finite sequence of points is expressed in terms of the cosine function. The DCT, first proposed by Ahmed [23] in 1972, is the most useful transformation method in image processing and data security. The 2D DCT [24] of any 2D signal $I_{m,n}$ of size $M \times N$ is defined by Eq. 2,

$$I'_{s,t} = \alpha_s\alpha_t \sum_{m=0}^{M-1}\sum_{n=0}^{N-1} I_{m,n}\cos\frac{\pi(2m+1)s}{2M}\cos\frac{\pi(2n+1)t}{2N}, \tag{2}$$

where $I'_{s,t}$ is 2D DCT transformed signal and $0 \leq s \leq M-1$, $0 \leq t \leq N-1$, $0 \leq m \leq M-1$ and $0 \leq n \leq N-1$,

$$\alpha_s = \begin{cases} \frac{1}{\sqrt{M}} & \text{if } s=0 \\ \frac{2}{\sqrt{M}} & \text{otherwise,} \end{cases} \quad \alpha_t = \begin{cases} \frac{1}{\sqrt{N}} & \text{if } t=0 \\ \frac{2}{\sqrt{N}} & \text{otherwise.} \end{cases}$$

The frequency domain array $I'_{s,t}$ in Eq. 2 and spatial domain array $I_{m,n}$ both are of the same size. In the matrix form, it is represented by Eq. 3,

$$I'_{s,t} = C_cI_{m,n}, \tag{3}$$

where C_c is the IInd type DCT kernel matrix. Comparing Eqs. 2 and 3, the kernel of the DCT, C_c can be given by Eq. 4,

$$C_c = \left\| \frac{1}{\sqrt{M}}\beta_s\cos\left(2\pi\frac{(2m+1)s}{4M}\right)\right\|, \tag{4}$$

where $\|.\|$ represents $M \times M$ matrix, $0 \leq m, s \leq M-1$ and $\beta_0 = 1$, $\beta_s = \sqrt{2}$ for $s > 1$.

The FrDCT is given by Eq. 5, which is derived from the Eq. 4.

$$C_c = U_cD_cU_c^* = \sum_m U_me^{i\phi_m}, \tag{5}$$

where U_c is a unitary matrix, composed of eigenvectors in the columns of u_m, $u_m^*u_n = \delta_{mn}$, $U_m = u_mu_m^*$ and D_c is a diagonal matrix with eigenvalues on the diagonal entries λ_m, $\lambda_m = e^{i\phi_m}$ with $0 < \phi_m < \pi$.

The FrDCT matrix C_α can be written by substituting the eigenvalues λ_m with their αth powers λ_m^α, given in Eq. 6,

$$C_\alpha = U_cD_c^\alpha U_c^*, \tag{6}$$

where α is an order of FrDCT.

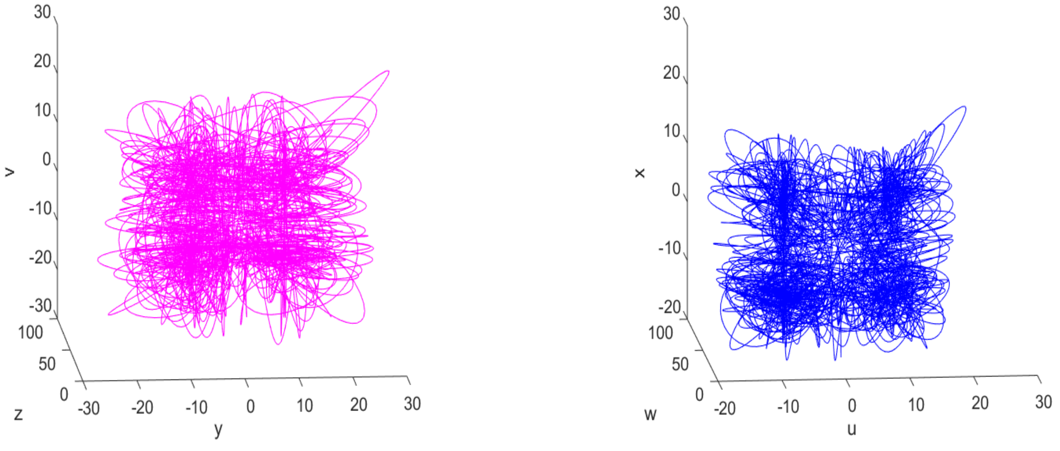
When $\alpha = 1$ the FrDCT behaves exactly similar as DCT, but when $\alpha = 0$ the FrDCT data output remains unchanged. For an image $I_{m,n}$, 2D FrDCT of fractional orders α, and β is defined by Eq. 7,

$$I'_{s,t} = C_\alpha I_{m,n}C_\beta^T, \tag{7}$$

where C_β^T is the transpose of C_β.

The 2D inverse fractional discrete cosine transform (IFrDCT) is computed by using Eq. 8,

$$I_{m,n} = C_{-\alpha}I'_{s,t}C_{-\beta}^T. \tag{8}$$



(a)

(b)

FIGURE 1. The 6D hyper-chaotic attractors of the system 1 when $a_1 = 10$, $a_2 = 28$, $a_3 = 8/3$ and $r_1 = r_2 = 0.05$: (a) in the (y, z, v) space and (b) in the (u, w, x) space.

III. BIOMETRIC TEMPLATE BASED ENCRYPTION AND DECRYPTION TECHNIQUE

Figs. 2 and 3, depict pictorial illustration of the proposed biometric template based encryption and decryption technique, respectively.

A. KEY GENERATION

Step 1: Iterate system 1, p times in advance to eliminate the transient response, to generate random sequences $u = \{u_1, u_2, u_3, \ldots, u_{MN}\}$, $v = \{v_1, v_2, v_3, \ldots, v_{MN}\}$, $w = \{w_1, w_2, w_3, \ldots, w_{MN}\}$, $x = \{x_1, x_2, x_3, \ldots, x_{MN}\}$, $y = \{y_1, y_2, y_3, \ldots, y_{MN}\}$ and $z = \{z_1, z_2, z_3, \ldots, z_{MN}\}$, respectively each of size $\max\{1 \times MN\}$.

Step 2: Converting the sequences u, v, w, x, y, and z into integers as:

$$U = \text{floor}(u \times 10^{15}) \bmod MN, \tag{9}$$

$$V = \text{floor}(v \times 10^{15}) \bmod MN, \tag{10}$$

$$W = \text{floor}(w \times 10^{15}) \bmod MN, \tag{11}$$

$$X = \text{floor}(x \times 10^{15}) \bmod MN, \tag{12}$$

$$Y = \text{floor}(y \times 10^{15}) \bmod MN, \tag{13}$$

$$Z = \text{floor}(z \times 10^{15}) \bmod MN, \tag{14}$$

where floor(p) returns p to the nearest integers less than or equal to p and mod defines modulo function.

Step 3: Sort the sequences 9–14 and get six sorted sequences $\overline{U}$, $\overline{V}$, $\overline{W}$, $\overline{X}$, $\overline{Y}$ and $\overline{Z}$. Find the positions of the values of $\overline{U}$, $\overline{V}$, $\overline{W}$, $\overline{X}$, $\overline{Y}$ and $\overline{Z}$ in U, V, W, X, Y and Z and mark down the transform positions i.e. $O = \{O(i) : i = 1, 2, 3, \ldots, MN\}$, $P = \{P(i) : i = 1, 2, 3, \ldots, MN\}$, $Q = \{Q(i) : i = 1, 2, 3, \ldots, MN\}$, $R = \{R(i) : i = 1, 2, 3, \ldots, MN\}$, $S = \{S(i) : i = 1, 2, 3, \ldots, MN\}$, $T = \{T(i) : i = 1, 2, 3, \ldots, MN\}$, where $U(O(i)) = \overline{U}(i)$, $V(P(i)) = \overline{V}(i)$, $W(Q(i)) = \overline{W}(i)$, $X(R(i)) = \overline{X}(i)$, $Y(S(i)) = \overline{Y}(i)$, and $Z(T(i)) = \overline{Z}(i)$.

Step 4: Now, the position sequences O, P, and Q are transform into row vectors M_1, M_2, and M_3, respectively, each of size $1 \times MN$ and R, S, and T are transform into matrices M_4, M_5, and M_6, respectively, each of size $M \times N$ and generate keys K_1, K_2, K_3, K_4, K_5, and K_6 as:

$$\begin{aligned}
K_1 &= M_1, \\
K_2 &= M_2, \\
K_3 &= M_3, \\
K_4 &= (M_4) \bmod 256, \\
K_5 &= (M_5) \bmod 256 \\
K_6 &= (M_6) \bmod 256.
\end{aligned}$$

B. BIOMETRIC TEMPLATE BASED ENCRYPTION ALGORITHM

The proposed technique of biometric templates encryption uses both permutation and substitution processes. The pictorial representation of the proposed encryption technique is shown in Fig. 2. The stepwise process of the technique is as follows:

Step 1: Let $I_1, I_2, I_3, \ldots, I_k$ be k biometric templates of size $m \times n$.

Step 2: In this step, all biometric templates are represented in form of three groups of templates which are G_1, G_2, and G_3 (as shown in Fig. 2). The order of each group is $M \times N$, where $m \leq M$ and $n \leq N$.

Step 3: Now, G_1, G_2, and G_3 are converted into row vectors Rv_1, Rv_2, and Rv_3 and are scrambled by using keys K_1, K_2, and K_3, respectively. After scrambling, these vectors are converted into matrices A_1, A_2, and A_3, each of size $M \times N$.

Step 4: This step combines A_1, A_2, and A_3 horizontally and generates a new matrix A. The matrix A is decomposed vertically into two half parts, i.e., H_l and H_r, where H_l is considered as the left part and H_r is considered as the right part (as shown in Fig. 2). The size of each part is $M \times \frac{3}{2}N$. When N is not an even number, then one column is padded

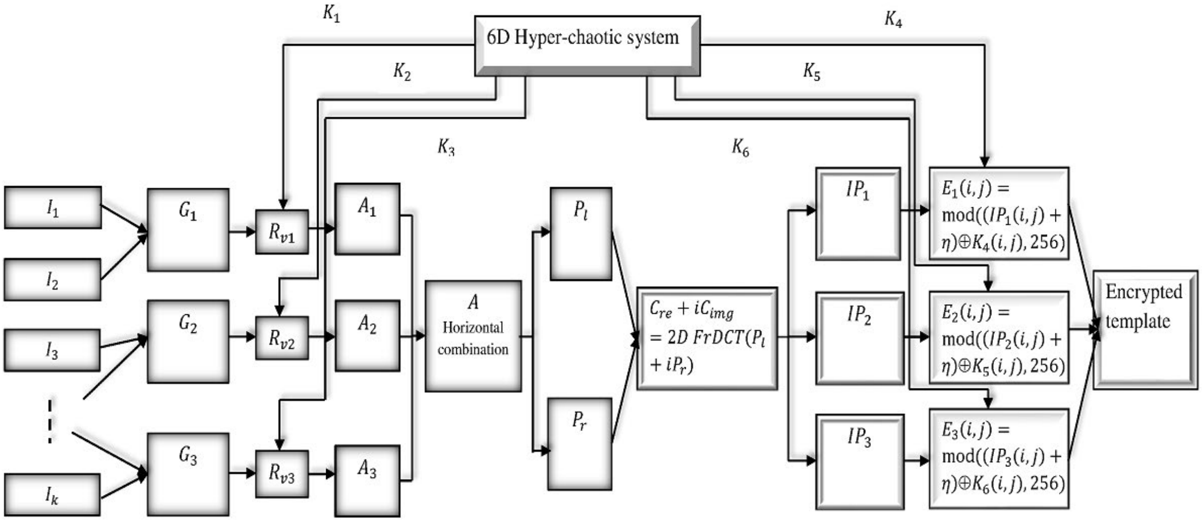

6D Hyper-chaotic system
K_1
K_2
K_3
K_4
K_5
K_6
I_1
I_2
I_3
I_k
G_1
G_2
G_3
R_{v1}
R_{v2}
R_{v3}
A_1
A_2
A_3
A
Horizontal combination
P_l
P_r
$C_{re} + iC_{img} = 2D\ FrDCT(P_l + iP_r)$
IP_1
IP_2
IP_3
$E_1(i,j) = \text{mod}((IP_1(i,j) + \eta)\oplus K_4(i,j), 256)$
$E_2(i,j) = \text{mod}((IP_2(i,j) + \eta)\oplus K_5(i,j), 256)$
$E_3(i,j) = \text{mod}((IP_3(i,j) + \eta)\oplus K_6(i,j), 256)$
Encrypted template

FIGURE 2. Block diagram of the proposed biometric template based encryption technique.

in the combined template and above steps are repeated on the padded template matrix.

Step 5: In this step, H_l and H_r as considered as the real and imaginary parts of CVM. We applied 2D FrDCT as illustrated in section II-B such that:

$$\begin{aligned} I &= H_l + iH_r \\ I' &= C_\alpha I C_\beta^T \end{aligned}$$

where α and β are the secret keys of the proposed technique.

Step 6: This step separates I' into real part C_{re} and imaginary part C_{img}. These real and imaginary parts are combined horizontally and a new matrix of size $M \times 3N$ is generated. Further, the new generated matrix is decomposed into three matrices IP_1, IP_2, and IP_3 of size $M \times N$.

Step 7: This step involve the substitution operation in IP_1, IP_2, and IP_3 using keys K_4, K_5, and K_6, respectively. The substitution process is given as:

Calculate the minimum values of the matrices IP_1, IP_2, and IP_3, let γ_1, γ_2, and γ_3 be the minimum values, respectively. Further, find the minimum value γ of γ_1, γ_2, and γ_3. Let $\eta = -\gamma + \lambda$, where $1 \leq \lambda \leq 5$. Calculate the corresponding pixel values of the encrypted template using Eq. 15,

$$\begin{cases} E_1(i,j) = \text{mod}((IP_1(i,j) + \eta) \oplus K_4(i,j), 256) \\ E_2(i,j) = \text{mod}((IP_2(i,j) + \eta) \oplus K_5(i,j), 256) \\ E_3(i,j) = \text{mod}((IP_3(i,j) + \eta) \oplus K_6(i,j), 256), \end{cases} \tag{15}$$

where $1 \leq i \leq M$, $1 \leq j \leq N$, and $\oplus$ represents the bitwise XOR operator. Thus, the encrypted template E is obtained after from E_1, E_2 and E_3, treating them the three components of this encrypted template.

C. DECRYPTION ALGORITHM

Figure 3 shows the pictorial representation of the decryption process that reveals the original biometric templates. The decryption process starts on the encrypted image using the same keystream K_4, K_5, and K_6 that are used in encryption. Using the reverse order of the encryption steps, the cipher image was successfully decrypted.

Step 1: Receiver obtains the encrypted image and decompose it into E'_1, E'_2, and E'_3 components. Receiver calculate IP'_1, IP'_2, and IP'_3 using Eq. 16,

$$\begin{cases} IP'_1(i,j) = \text{mod}((E_1(i,j) \oplus K_4(i,j)) - \eta, 256) \\ IP'_2(i,j) = \text{mod}((E_2(i,j) \oplus K_5(i,j)) - \eta, 256) \\ IP'_3(i,j) = \text{mod}((E_3(i,j) \oplus K_6(i,j)) - \eta, 256). \end{cases} \tag{16}$$

Step 2: Now, IP'_1, IP'_2, and IP'_3 are horizontally combined to form a matrix A' of dimension $M \times 3N$. Divide A' into two halves. To get a CVM B by treating the two components as real and imaginary parts, run 2D-iFrDCT with the correct keys.

Step 3: Divide the complex value B into its real and imaginary parts, C'_{re} and C'_{img}, respectively. To create a new matrix of size $M \times 3N$, horizontally combine these real and imaginary components. Further, break this matrix down into three distinct matrices. B_1, B_2, and B_3 of size $M \times N$.

Step 4: Now, B_1, B_2, and B_3 are converted into row vectors Rv'_1, Rv'_2, and Rv'_3 and scrambled by using keys K_1, K_2, and K_3, respectively. After scrambling, convert these vectors into matrices G'_1, G'_2, and G'_3, each of size $M \times N$.

Step 5: In this step, from the representation G'_1, G'_2, and G'_3, separates biometric templates I'_1, I'_2, $I'_3, \ldots, I'_k$.

IV. COMPUTER SIMULATION AND EXPERIMENTAL RESULTS

The proposed technique is implemented in personal computer (PC) using MATLAB R-2015a software. The configuration of PC's are Windows 10, Intel(R), Core(TM) i5-6200U CPU with a clock speed of 2.30 GHz and 8 GB RAM. For the experimental results, we have taken the biometric templates of different size shown in Fig. 4(a)–(f). Figure 4(g)–(i) shows

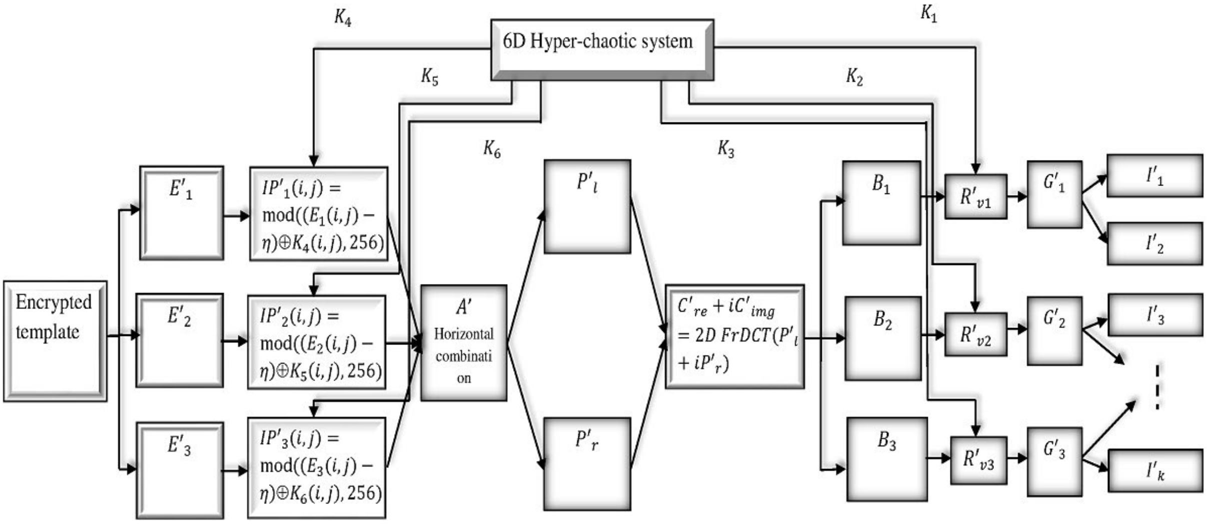

K_4
6D Hyper-chaotic system
K_1
K_5
K_2
K_6
K_3
Encrypted template
E'_1
E'_2
E'_3
$IP'_1(i,j) = \mathrm{mod}((E_1(i,j) - \eta)\oplus K_4(i,j), 256)$
$IP'_2(i,j) = \mathrm{mod}((E_2(i,j) - \eta)\oplus K_5(i,j), 256)$
$IP'_3(i,j) = \mathrm{mod}((E_3(i,j) - \eta)\oplus K_6(i,j), 256)$
A' Horizontal combination
P'_l
P'_r
$C'_{re} + iC'_{img} = 2D\ FrDCT(P'_l + iP'_r)$
B_1
B_2
B_3
R'_{v1}
R'_{v2}
R'_{v3}
G'_1
G'_2
G'_3
I'_1
I'_2
I'_3
I'_k

FIGURE 3. Block diagram of the proposed biometric template based decryption technique.

group representation of original biometric templates. The initial values and control parameters of the 6D-chaotic system are $u_0 = 2.543210007543721$, $v_0 = 3.674515623875401$, $w_0 = 1.235685120036054$, $x_0 = 1.6758174322200155643$, $y_0 = 4.785400011325467$, $z_0 = 2.3576335564327899543$, $a_1 = 10.000102302324532$, $a_2 = 28.004238236135784$, $a_3 = 2.424874598634125$, $r_1 = 0.036793421834854$ and $r_2 = 0.040002249502146$. The fractional order of the 2D-FrDCT are $\alpha = 2.2378500864321523$, $\beta = 3.338626723500651$. The encrypted template is shown in Fig. 4(j). The decrypted templates are shown in Fig. 4 (k)–(p).

A. MORE EXPERIMENTAL RESULTS

For more experimental results, we have taken different biometric templates as shown in Fig. 5(a)–(x). The encryption and decryption keys are same as given in section IV. Fig. 5(a)–(x) display the original biometric templates, Fig. 5(y)–(aa) display three groups of biometric templates, Fig. 4(ab) display encrypted template, and Fig. 5(ac)–(az) display corresponding decrypted biometric templates.

B. RUNNING TIME ANALYSIS

The proposed biometric templates encryption method is tested on templates of Figs. 4 of size 128 × 128, and 5 of size 256 × 256. The proposed technique is implemented in MATLAB R-2015a running on a PC having Windows 10, Intel(R), Core(TM) i5-6200U CPU with 2.30 GHz frequency and 8 GB RAM. The proposed technique consists of three main parts: (1) random sequence generator using 6D hyper-chaotic system, (2) Permutation and substitution, and (3) Pixel values transformation from the spatial or coordinate domain to the frequency domain. The proposed technique is a single-round multi-layer biometric template encryption technique that can be used for real-time online communication.

TABLE 1. Running time (in seconds) for encryption of biometric templates of different sizes.

Biometric templates	Proposed method	Zhu et al. [25]	Khan et al. [27]	Khan and Ahmad [28]
128 × 128	0.851	–	4.5962	–
256 × 256	2.811	0.464	–	0.65

Table 1 shows the running time in seconds for the encryption of biometric templates of different sizes. Table 1 indicates that the proposed technique has a lower encryption time than other algorithms.

V. BIOMETRIC TEMPLATE MATCHING

For biometric prototype matching, we employ hamming distance (HD), peak signal-to-noise ratio (PSNR), structural similarity index metric (SSIM), and mean square error (MSE).

A. HAMMING DISTANCE METHOD

The HD compares the two-bit patterns of the initial and decrypted biometric templates. A perfect match is indicated by an HD value of zero, while a perfect nonmatch is indicated by a value of one. The difference in HD between decrypted biometric templates $I'_1, I'_2, I'_3, \ldots, I'_k$ and the original templates $I_1, I_2, I_3, \ldots, I_k$, is stored in the database which is calculated by Eq. 17,

$$\mathrm{HD} = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N} I'_l(i,j) \oplus I_l(i,j), \tag{17}$$

where $1 \leq l \leq k$ and $\oplus$ the Boolean operator (XOR). The scale of the biometric prototype is M, N, and HD is the ratio of total differ bits to total bits.

B. MSE, AND PSNR METHOD

MSE identifies the error between the decrypted template and the original template. PSNR is a consistency metric that

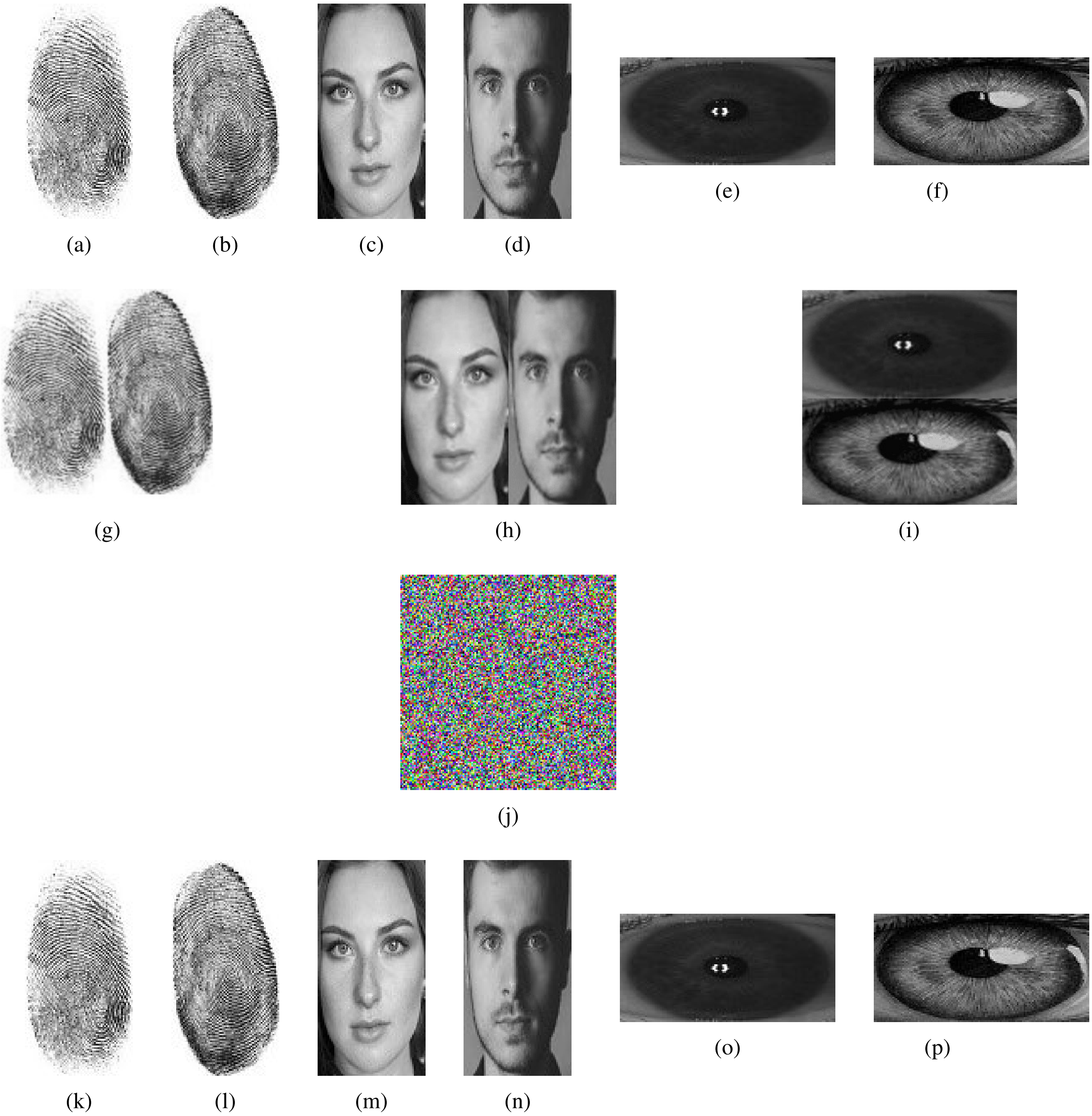


FIGURE 4. Experimental results of biometric templates: (a)–(f) original biometric templates, (g)–(i) three groups of original biometric templates, (j) encrypted template, and (k)–(p) decrypted biometric templates.

compares the decrypted template to its original counterpart. The higher the PSNR value, the higher the quality of the decrypted prototype.

The MSE, and PSNR [29] between I_l and I_l' are calculated by the Eqs. 18 and 19, respectively.

$$\text{MSE} = \frac{1}{MN}\sum_{m=1}^{M}\sum_{n=1}^{N}[I_l(m,n) - I_l'(m,n)]^2, \tag{18}$$

$$\text{PSNR} = 10\log_{10}\frac{(255)^2}{\text{MSE}}, \tag{19}$$

where $I_l(m, n)$ represents the original template and $I_l'(m, n)$ represents the decrypted template, M and N are the numbers of pixels of the frame.

C. SSIM METHOD

The SSIM [30] is a perceptual metric for determining image quality. The SSIM value obtained is a decimal value between 0 and 1, with value 1 indicating perfect structural similarity only in the case of two equivalent sets of data. The SSIM index between I_l and I_l' is calculated by Eq. 20,

$$\text{SSIM} = \frac{(2\mu_{I_l}\mu_{I_l'} + J_1)(2\sigma_{I_lI_l'} + J_2)}{(\mu_{I_l}^2 + \mu_{I_l'}^2 + J_1)(\sigma_{I_l}^2 + \sigma_{I_l'}^2 + J_2)}, \tag{20}$$

where μ_{I_l} and $\mu_{I_l'}$ are mean of the original template and decrypted template, respectively. σ_{I_l} and $\sigma_{I_l'}$ are the standard deviation of the original template and decrypted template, respectively. $\sigma_{I_lI_l'}$ is the covariance between the original

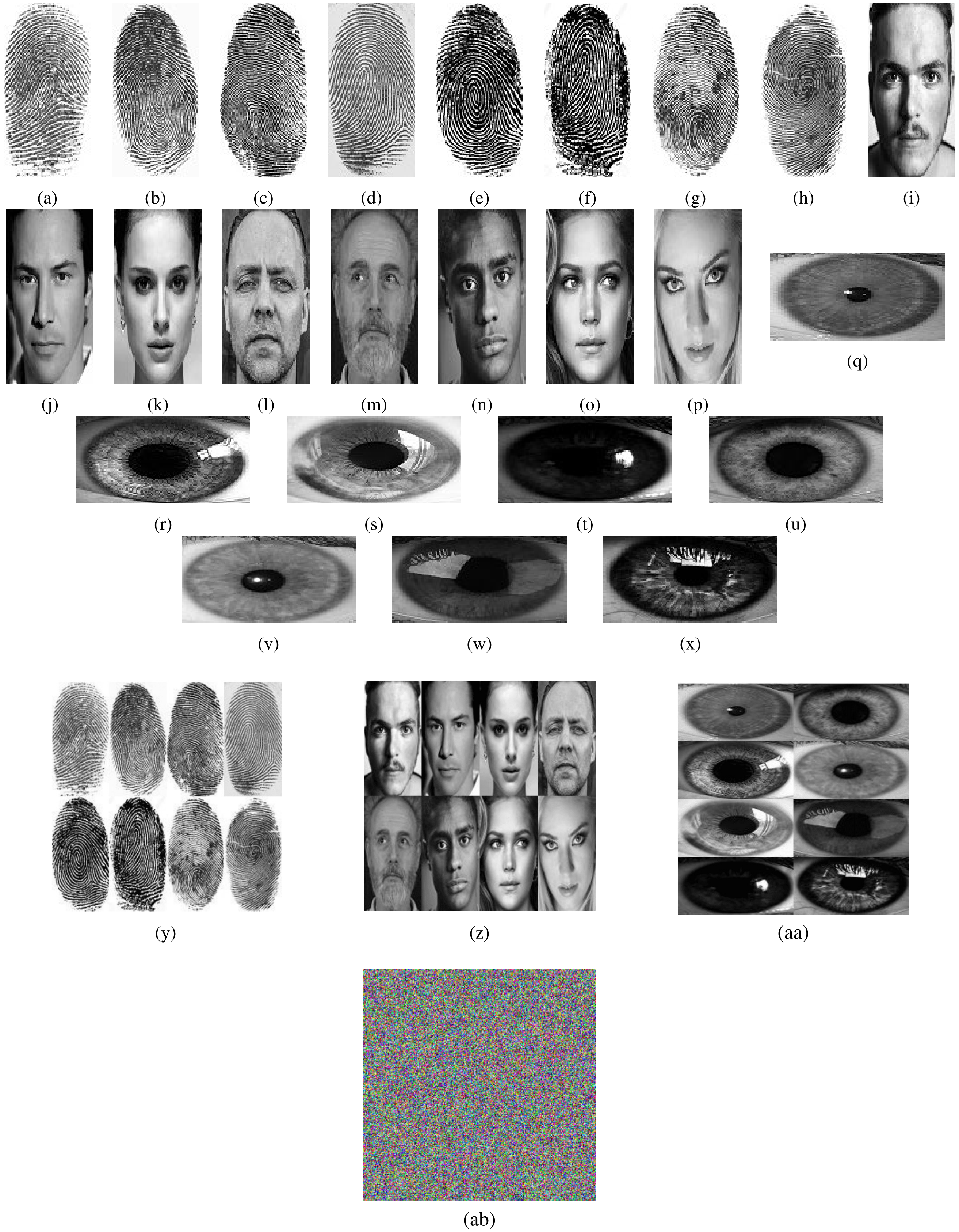


FIGURE 5. Experimental results of biometric templates: (a)–(x) original biometric templates, (y)–(aa) three groups of original biometric templates, and (ab) encrypted template.

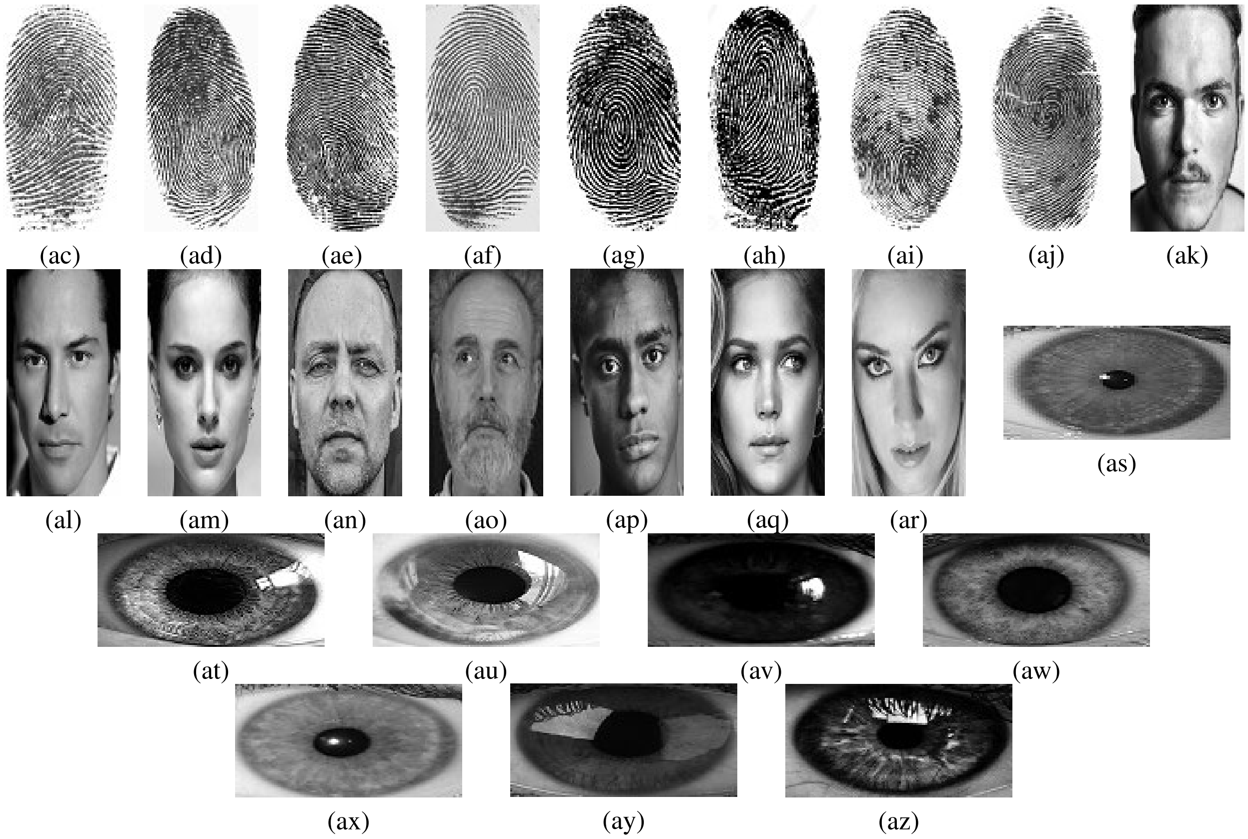


FIGURE 5. *(Continued.)* Experimental results of biometric templates: (ac)–(az) decrypted biometric templates.

template and the decrypted template, $J_1 = (k_1L)^2$, $J_2 = (k_2L)^2$ and $k_1 = 0.01$, $k_2 = 0.03$ and $L = 2^{\text{number of bits per pixel}} - 1$.

Table 2 shows the measured HD, MSE, PSNR, and SSIM values for original and decrypted biometric templates. From Table 2, one can see that the HD is 0, MSE is also 0, PSNR is ∞ and SSIM is 1 for all templates. It means that the decrypted templates are perfectly matched with the original one, i.e., there is no loss of data during transmission.

VI. SECURITY ANALYSIS

In this section, we have discussed some security parameters to check the validity and toughness of the presented technique.

A. KEY SPACE AND KEY SENSITIVITY ANALYSIS

In the presented technique, 6D-chaotic system have control parameters a_1, a_2, a_3, r_1, r_2 and initial values u_0, v_0, w_0, x_0, y_0 and z_0 as secret keys and also fractional order α and β of 2D FrDCT are secret keys. For the control parameters, initial values of 6D hyper chaotic system and fractional order of 2D FrDCt, if the precision is 10^{-15} the key space will be $10^{(15+15+\ldots+15)_{11-\text{times}}} \times 10^{15+15} = 10^{195} \approx 2^{648}$, which is much sufficient to resists the brute-force attacks.

For key sensitivity analysis, we are slightly changing the keys. For a slight change in keys, we add $\Delta = 10^{-15}$ in the control parameters, initial values and fractional order. Due to the chaotic properties, a slight change in control parameters and initial values leads to a dramatic change in the sequences i.e., in keys. From Fig. 6, one can see that the decrypted templates are absolutely different from the original one.

TABLE 2. Experimental values of HD, MSE, PSNR, and SSIM between original and decrypted templates of Fig. 4.

Original templates	Decrypted templates	HD	MSE	PSNR	SSIM
Fig. 4(a)	Fig. 4(k)	0	0	∞	1
Fig. 4(b)	Fig. 4(l)	0	0	∞	1
Fig. 4(c)	Fig. 4(m)	0	0	∞	1
Fig. 4(d)	Fig. 4(n)	0	0	∞	1
Fig. 4(e)	Fig. 4(o)	0	0	∞	1
Fig. 4(f)	Fig. 4(p)	0	0	∞	1

Fig. 6(a)–(f) is the decrypted templates of Fig. 4(j) with slight change in control parameter a_1 i.e., $a_1' = a_1 + \Delta$. Fig. 6(g)–(l) is the decrypted templates of Fig. 4(j) with slight change in control parameter a_2 i.e., $a_2' = a_2 + \Delta$. Fig. 6(m)–(r) is the decrypted templates of Fig. 4(j) with slight change in control parameter a_3 i.e., $a_3' = a_3 + \Delta$. Fig. 6(s)–(x) is the decrypted templates of Fig. 4(j) with slight change in control parameter r_1 i.e., $r_1' = r_1 + \Delta$. Fig. 6(y)–(ad) is the decrypted templates of Fig. 4(j) with slight change in control parameter r_2 i.e., $r_2' = r_2 + \Delta$. Fig. 6(ae)–(aj) is the decrypted templates of Fig. 4(j) with slight change in initial value u_0 i.e., $u_0' = u_0 + \Delta$. Fig. 6(ak)–(ap) is the decrypted templates of Fig. 4(j) with slight change in initial value v_0 i.e., $v_0' = v_0 + \Delta$.

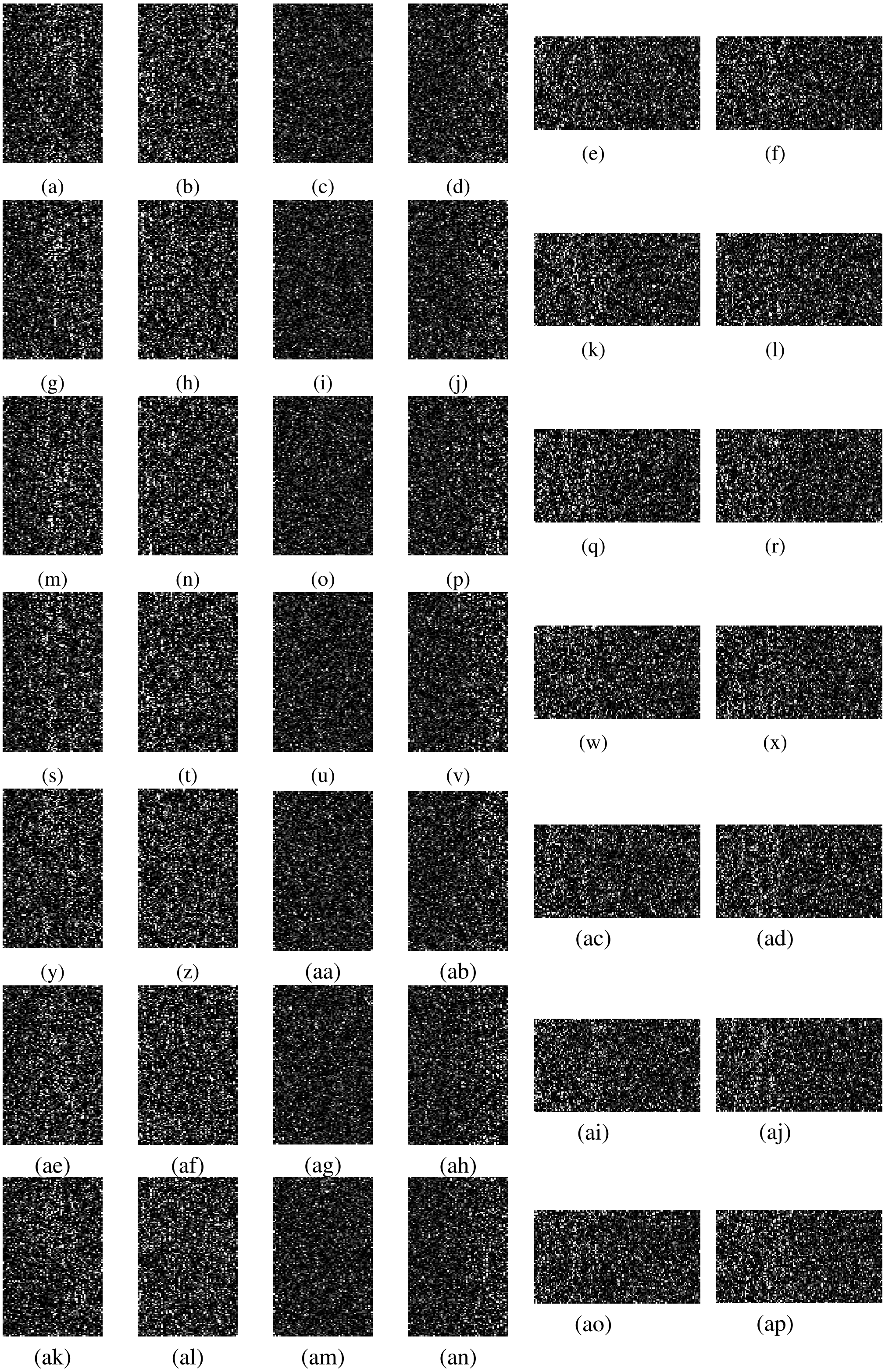


FIGURE 6. **Experimental results of key sensitivity analysis. Each row from top to bottom: decrypted templates of Fig. 4(j) with wrong keys.**

Fig. 6(aq)–(av) is the decrypted templates of Fig. 4(j) with slight change in initial value w_0 i.e., $w_0' = w_0 + \Delta$. Fig. 6(aw)–(bb) is the decrypted templates of Fig. 4(j) with slight change in initial value x_0 i.e., $x_0' = x_0 + \Delta$. Fig. 6(bc)–(bh) is the decrypted templates of Fig. 4(j) with slight change in initial value y_0 i.e., $y_0' = y_0 + \Delta$.

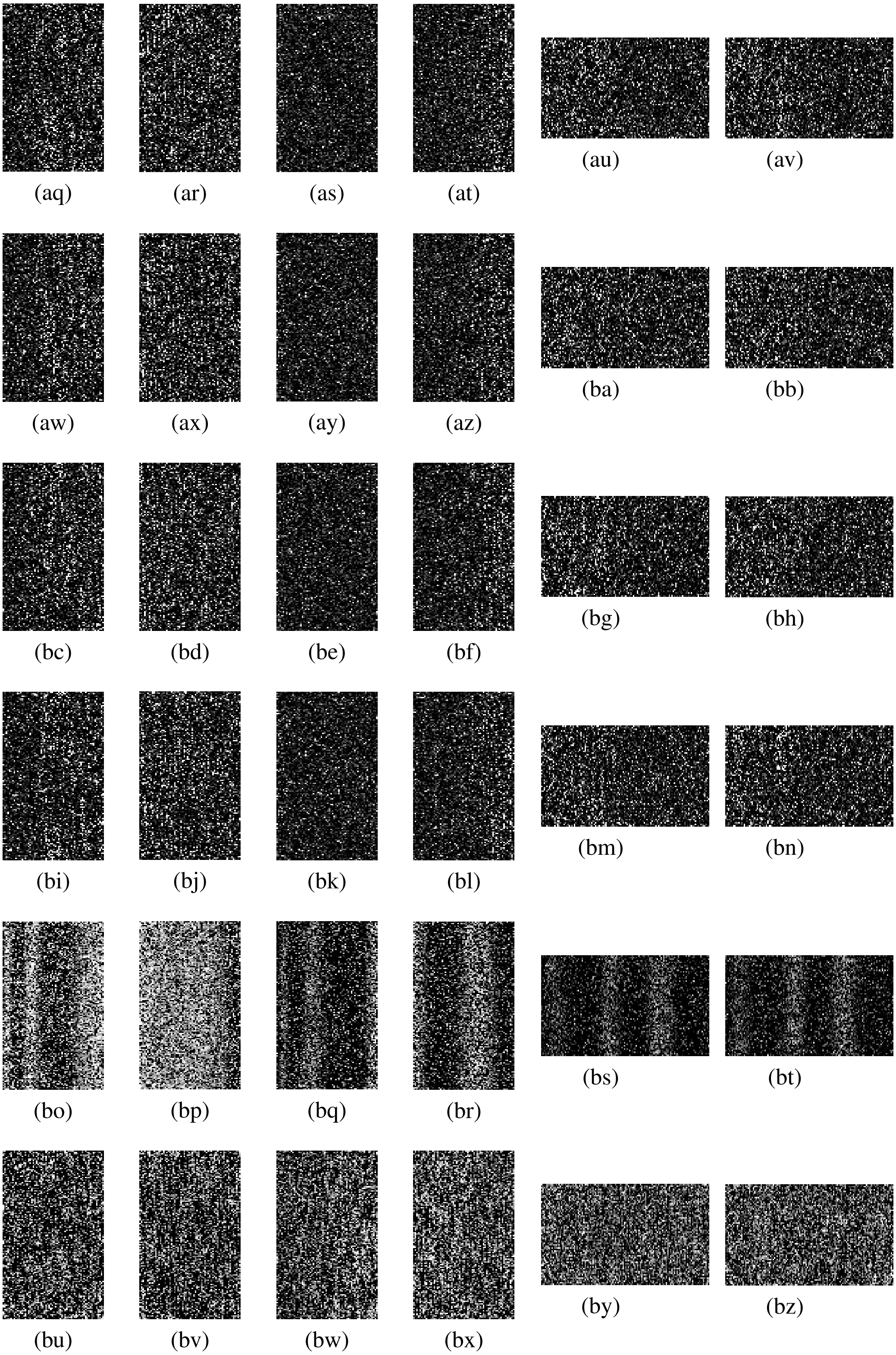

(aq) (ar) (as) (at) (au) (av)
(aw) (ax) (ay) (az) (ba) (bb)
(bc) (bd) (be) (bf) (bg) (bh)
(bi) (bj) (bk) (bl) (bm) (bn)
(bo) (bp) (bq) (br) (bs) (bt)
(bu) (bv) (bw) (bx) (by) (bz)

FIGURE 6. ***(Continued.)*** **Experimental results of key sensitivity analysis. Each row from top to bottom: decrypted templates of Fig. 4(j) with wrong keys.**

Fig. 6(bi)–(bn) is the decrypted templates of Fig. 4(j) with slight change in initial value z_0 i.e., $z_0' = z_0 + \Delta$. Fig. 6(bo)–(bt) is the decrypted templates of Fig. 4(j) with slight change in fractional order value α i.e., $\alpha' = \alpha + \Delta$. Fig. 6(bu)–(bz) is the decrypted templates of Fig. 4(j) with slight change in fractional order value β i.e., $\beta' = \beta + \Delta$.

TABLE 3. Experimental results for entropy; entropy value of biometric templates of Fig. 4(a)–(f), and encrypted template (Fig. 4(j)).

Templates	Entropy	
	Biometric templates	Encrypted
Fig. 4	6.9041	7.9894
Fig. 4	7.2273	
Fig. 4	7.4794	
Fig. 4	7.1964	
Fig. 4	6.0009	
Fig. 4	7.3409	

TABLE 4. Encryption quality analysis using the variance of the histogram test for original and encrypted templates.

Template	V_H of the Original template	V_H of the encrypted template
Fig. 4	$3.1959e+03$	$5.4550e+02$
Fig. 5	$5.1661e+03$	$5.4672e+02$

B. ENTROPY ANALYSIS

The entropy of the digital data z is considered by Eq. 21.

$$H(z) = -\sum_{i=1}^{N} P(z_i)log_2P(z_i) \tag{21}$$

where $P(z_i)$ is the probability for occurrence of z_i.

The suggested technique's entropy for an encrypted template is extremely close to 8, and is demonstrated in Table 3.

C. HISTOGRAM ANALYSIS VIA GRAPHICAL METHOD

In the case of digital biometric data, a histogram is a graph that shows the relationship between the number of pixels and their intensity. The histogram of original biometric templates is advertised in Fig. 7(a)–(c), and the histogram of the encrypted template is advertised in Fig. 7(d). The proposed technique is resistant to histogram analysis, and no information about the initial biometric template is leaked.

D. HISTOGRAM ANALYSIS VIA VARIANCE METHOD

We have measured the quality of the encryption technique by calculating the variance of the histogram V_H [27]. It is defined by Eq. 22,

$$V_H(A) = \frac{1}{M^2}\sum_{i=0}^{M-1}\sum_{j=0}^{M-1}\frac{(a_i - a_j)^2}{2}, \tag{22}$$

where $A = \{a_0, a_1, a_2, \ldots, a_{M-1}\}$ is an array and a_i and a_j are pixel values. The variance of the histogram is calculated for original and encrypted templates. Table 4 displays the calculated values of the variance of the histogram.

E. MAXIMUM, AND IRREGULAR DEVIATION TESTS

The maximum deviation (MD) [26] among the original and encrypted templates were used to determine the encryption technique's superiority. The encryption approach is more effective if the encrypted template deviates from the original template. To calculate MD, follow the steps given below:

TABLE 5. Encryption quality analysis using maximum and irregular deviation tests between original and encrypted templates.

Original and encrypted templates	MD	ID
Fig. 4	$1.9663e+04$	15390
Fig. 5	$1.9141e+04$	15113

1) Plot the histogram of the original and encrypted template.
2) Determine the difference in absolute deviation between the two graphs.
3) Now calculates MD, which is given Eq. 23,

$$\text{MD} = \frac{b_0 + b_{255}}{2} + \sum_{i=1}^{254} b_i, \tag{23}$$

where b_i is the amplitude of the absolute deviation between two graphs at value i.

From the Eq. 23, we analyze that the higher value of MD shows that, the encrypted template deviates from the original template.

The irregular deviation (ID) [27] measures the deviation effected by the encryption technique on the encrypted template is irregular. To calculate ID, follow the steps given below:

1) Let I be the original template and E be the encrypted template. Calculate the absolute difference matrix A_D as: $A_D = |E - I|$.
2) Plot the graph of histogram distribution H_D of the A_D i.e., $H_D = \text{histogram}(A_D)$.
3) Calculate the average value A_V using Eq. 24,

$$A_V = \frac{1}{M \times N}\sum_{i=0}^{255} b_i, \tag{24}$$

where b_i is the amplitude of the H_D at the value i.

4) Now, Subtract A_V from the H_D, and then take the absolute value of the result we obtain A_R i.e., $A_R = |H_D - A_V|$.
5) Calculate the area under the A_R value curve, which is ID given by Eq. 25,

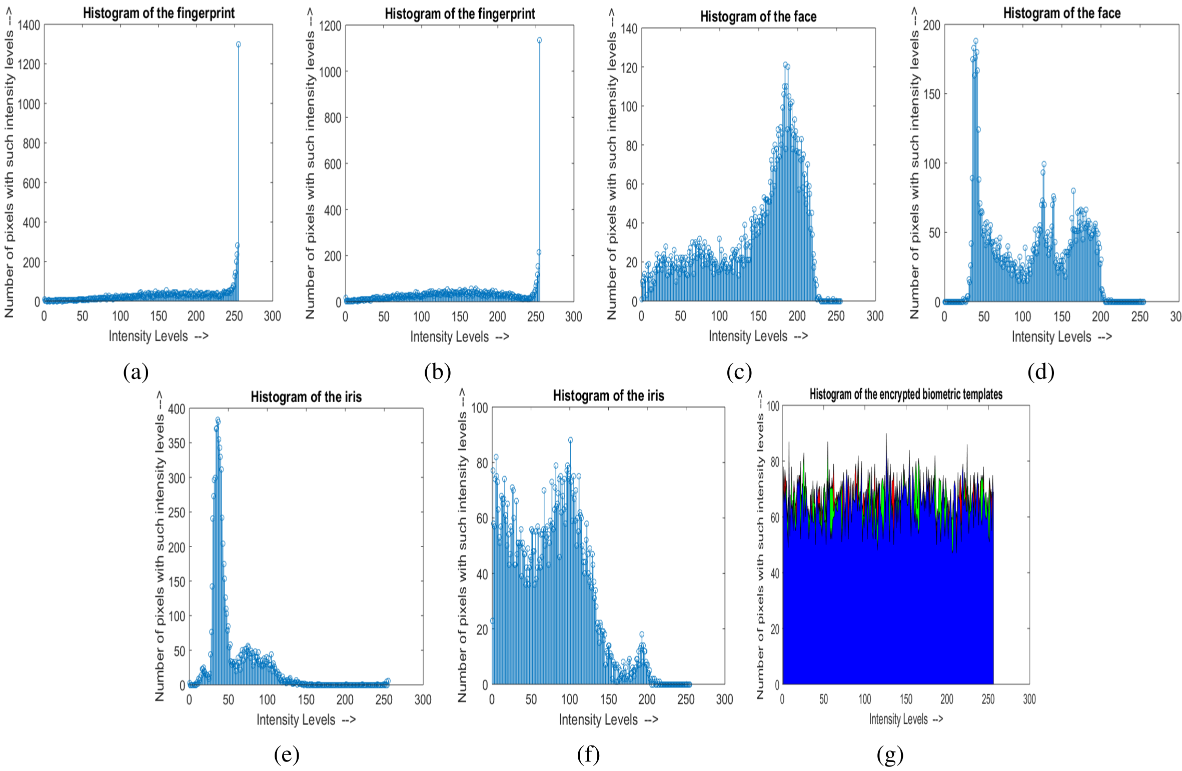
$$\text{ID} = \sum_{i=0}^{255} A_R(i). \tag{25}$$

From the Eq. 25, we analyze that the lower value of ID shows that, the encrypted template deviates from the original template.

Table 5 shows the MD and ID values between original and encrypted biometric templates.

F. ENERGY TEST

This test measures the aggregate of all elements squared in the ''Grey Level Co-occurrence Matrix'' (GLCM) [27], which is used to detect disorders in the encrypted template. For a high



(a) (b) (c) (d)

(e) (f) (g)

FIGURE 7. Histogram analysis via graphical method of the proposed technique; (a) histogram of Fig. 4(a), (b) histogram of Fig. 4(b), (c) histogram of Fig. 4(c), (d) histogram of Fig. 4(d), (e) histogram of Fig. 4(e), (f) histogram of Fig. 4(f), and (g) histogram of Fig. 4(j).

TABLE 6. Encryption quality analysis using energy test for original and encrypted templates.

Template	Original template energy	encrypted template energy
Fig. 4	0.0074	$8.1523e-05$
Fig. 5	0.0085	$2.0376e-05$

quality encryption technique, the energy level should be low. The energy is calculated by using Eq. 26,

$$\text{Energy} = \sum_{i=0}^{M-1}\sum_{j=0}^{N-1} I^2(i,j), \tag{26}$$

where $I(i,j)$ represents the pixel value at (i,j)th position.

Table 6 shows calculated energy values for original and encrypted templates. From Table 6, the sufficient less value of energy for encrypted template with respect to original template shows a maximum disorder in the encrypted template and so the encryption technique is of high quality.

G. CONTRAST TEST

The number of local variations present in the biometric template is measured by contrast test. The encrypted templates generated by a high quality encryption technique will show high contrast due to randomness. The contrast is calculated by using Eq. 27,

$$\text{Contrast} = \sum_{i,j} |i-j|^2 I(i,j), \tag{27}$$

where $I(i,j)$ represents GLCM.

TABLE 7. Experimental values for encryption quality analysis using contrast test in original and encrypted templates.

Template	Original template contrast	encrypted template contrast
Fig. 4	374.5	2725.2
Fig. 5	1234	10923

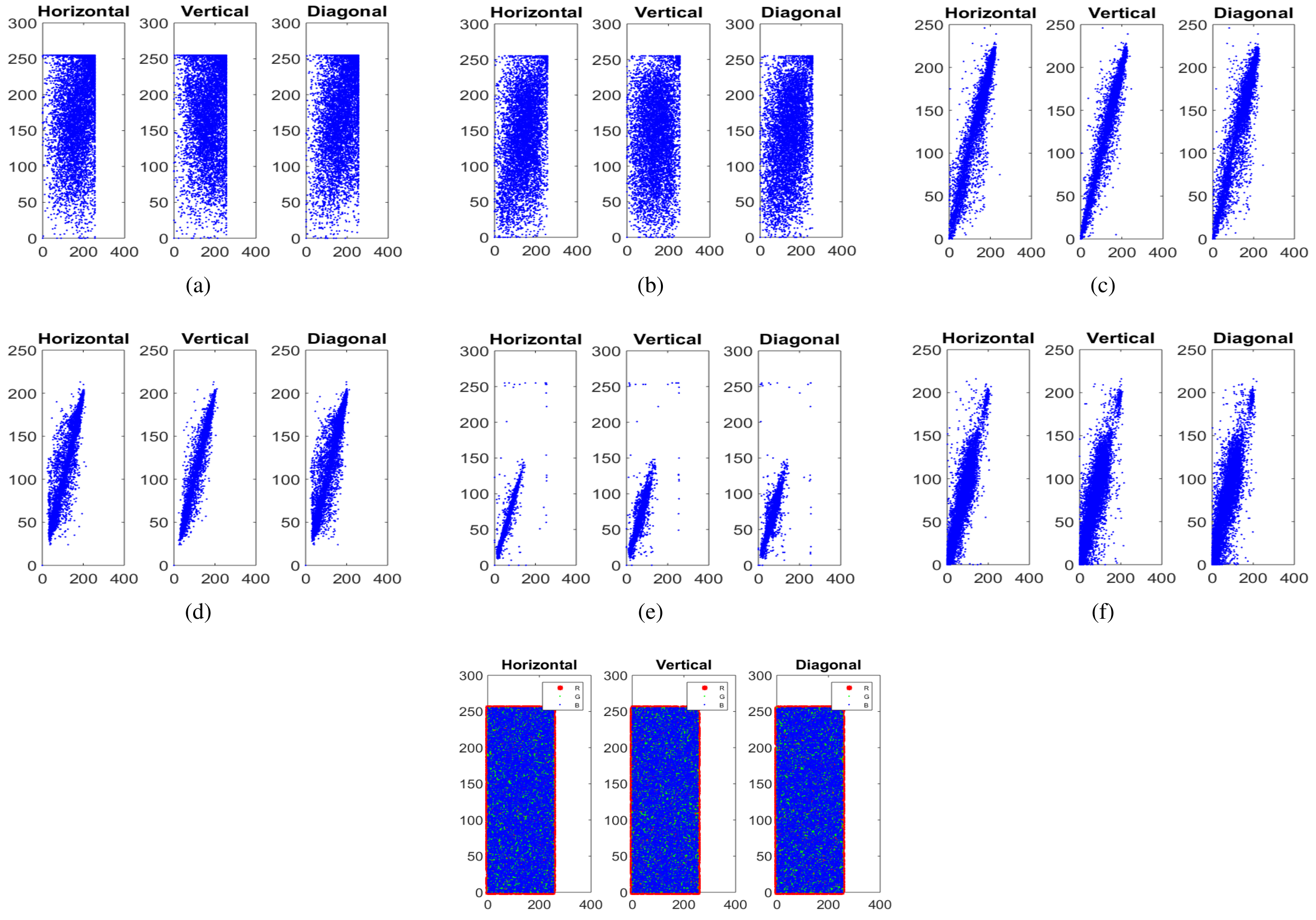
Table 7 shows the calculated contrast values of original and encrypted templates, which shows that this encryption technique is efficient and offers higher security.

H. HOMOGENEITY TEST

It measures the proximity quantification of the biometric template pixels distributed in the GLCM. In the template pixels near diagonal, homogeneity test values are more sensitive. It has maximum value, when all pixels in the biometric template are same. The homogeneity is calculated by using Eq. 28,

$$\text{Homogeneity} = \sum_{i,j} \frac{I(i,j)}{1+|i-j|}. \tag{28}$$

Table 8 displays the calculated homogeneity values for the original and encrypted templates. From Table 8, one can see that, the homogeneity values for original templates are high and for encrypted templates are low, it confirms the encryption technique's security, quality, and efficiency.



(a)

(b)

(c)

(d)

(e)

(f)

(g)

FIGURE 8. Graphical analysis of pixel intensity distributions in biometric templates: (a) pixel intensity distributions at H, V, and D direction of Fig. 4(a), (b) pixel intensity distributions at H, V, and D direction of Fig. 4(b), (c) pixel intensity distributions at H, V, and D direction of Fig. 4(c), (d) pixel intensity distributions at H, V, and D direction of Fig. 4(d), (e) pixel intensity distributions at H, V, and D direction of Fig. 4(e), (f) pixel intensity distributions at H, V, and D direction of Fig. 4(f), and (g) pixel intensity distributions at H, V, and D direction of Fig. 4(j).

TABLE 8. Encryption quality analysis using homogeneity test for original and encrypted templates.

Template	Original template homogeneity	encrypted template homogeneity
Fig. 4	0.7234	0.0623
Fig. 5	0.5768	0.0362

TABLE 9. Experimental result of CC values of Fig. 4(a)–(f) in H, V, and D directions.

Biometric	Direction		
template	H	V	D
Fig. 4(a)	0.4846	0.3719	0.5589
Fig. 4(b)	0.6020	0.4903	0.5834
Fig. 4(c)	0.9491	0.9690	0.9353
Fig. 4(d)	0.9474	0.9795	0.9400
Fig. 4(e)	0.9313	0.8930	0.8565
Fig. 4(f)	0.9021	0.8481	0.8439

TABLE 10. Experimental result of CC values of Fig. 4(j) in H, V, and D directions.

Encrypted template	Component	Direction		
		H	V	D
Fig. 4(j)	R	−0.0106	−0.0094	−0.0032
	G	0.0167	0.0061	0.0142
	B	−0.0009	0.0104	−0.0007

TABLE 11. NPCR and UACI results performed on Figs. 4 and 5.

Standard image	Experimental values	
	NPCR(%)	UACI(%)
Fig. 4	99.6422	33.3854
Fig. 5	99.6543	33.4235

I. CORRELATION ANALYSIS

The proposed technique's performance against the pixel intensity distribution of neighboring pixels in the H, V, and D directions is assessed by computing the correlation coefficient (CC) [27] between the original biometric template (I) and the encrypted template (E) using Eq. 29,

$$CC_{IE} = \frac{\sum_{i=1}^{u}\sum_{j=1}^{v}(I_{i,j}-\overline{I})(E_{i,j}-\overline{E})}{\sqrt{[\sum_{i=1}^{u}\sum_{j=1}^{v}(I_{i,j}-\overline{I})]^2[\sum_{i=1}^{u}\sum_{j=1}^{v}(E_{i,j}-\overline{E})]^2}}, \tag{29}$$

where $\overline{I}$ and $\overline{E}$ are mean of original and encrypted templates.

TABLE 12. Comparison of our technique with other relevant techniques: Rakheja *et al.* technique [8], Barrero *et al.* technique [20], Khan *et al.* technique [27], Khan and Ahmad technique [28], and Singh technique [34].

S.No.	Performance parameters	Rakheja et al. [8]	Barrero et al. [20]	Khan et al. [27]	Khan and Ahmad [28]	H. Singh [34]	Proposed method
1.	Data	Iris templates	Biometric templates	Image	Image	Grayscale image	Biometric templates
2.	Applied procedure	Optical or digital	Digital	Digital	Digital	Optical or digital	Digital
3.	Transform domain	Hybrid transform	Bloom Filters	DNA and Wavelet	Chaos based	Gyrator transform	2D FrDCT domain
4.	Permutation method	Yes	No	Yes	Yes	No	Yes
5.	Substitution method	Yes	No	Yes	Yes	Yes	Yes
6.	Number of keys	RPM+10	–	6	6	9	13
7.	Sensitivity to secret keys	Yes	Yes	Yes	Yes	Yes	Yes
8.	Keyspace	–	–	2^{299}	2^{299}	–	2^{648}
9.	Entropy	7.9977	–	7.9897	7.9925	6.647	7.9899
10.	PSNR of decrypted image in dB	image1=190dB image2=infinity	Not mention	Not mention	Not mention	310.9292dB	infinity
11.	Attack analysis	Noise and Special attacks	–	Differential, noise, and occlusion	Differential attack	Cropping and noise attack	Cropping and Differential attack

Tables 9 and 10 display the CC values that were measured. For each direction (H, V, or D) and color variable, the CC in the encrypted template is very close to zero (R, G, or B). As a result, though adjacent pixels in the original models are more correlated, adjacent pixels in the biometric template encrypted by our technique have a slight correlation.

In the H, V, and D directions, the graph depicts the pixel intensity distribution of neighboring pixels in the initial biometric templates and encrypted as shown in Fig. 8.

VII. ATTACK ANALYSIS

A. CROPPING ATTACK ANALYSIS

For this analysis, we deal with the encrypted template (Fig. 4(j)) cropped with different formats to test the robustness of the proposed technique as shown in Fig. 9((a), (h), (o), (v), and (ac)). The encrypted template (Fig. 4(j)) is cropped with block size of 16 × 16, 32 × 32, 64 × 64 from left top corner, and 16×16, 32×32 from middle, which are displayed in Fig. 9((a), (h), (o), (v), and (ac)), respectively. The corresponding decrypted templates are shown in Fig. 9((b)–(g), (i)–(n), (p)–(u), (w)–(ab), and (ad)–(ai)). As shown in Fig. 9, our proposed encryption technique is resistant to cropping attacks.

B. DIFFERENTIAL ATTACK ANALYSIS

Biham and Shamir [31], [32] are usually attributed to the discovery of differential cryptanalysis attack to various ciphers. In the differential attack, the adversary may change one pixel of the original biometric template to find purposeful relationships between the original biometric template and corresponding encrypted template. If a single pixel shift in the original template induces a major change in the encrypted template, then the encryption method is immune to differential attack. The number of pixels change rate (NPCR) and unified average changing intensity (UACI) [33] tests, both of which are defined in Eqs. 30 and 31, respectively, are widely used to determine the encryption technique's strength in differential attacks.

$$\text{NPCR} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)}{M \times N} \times 100\%, \tag{30}$$

$$\text{UACI} = \frac{1}{MN}\left[\frac{\sum_{i=1}^{M}\sum_{j=1}^{N} |E(i,j) - E'(i,j)|}{255}\right] \times 100\%, \tag{31}$$

where E and E' are two encrypted biometric templates corresponding to the original biometric templates with the difference of only one pixel. M and N are the size of the biometric templates and $D(i,j)$ is a bipolar array given by Eq. 32,

$$D(i,j) = \begin{cases} 0 & \text{if } E(i,j) = E'(i,j) \\ 1 & \text{if } E(i,j) \neq E'(i,j). \end{cases} \tag{32}$$

To check the resistance against differential attack on the presented technique, the NPCR and UACI tests are executed on Fig. 4 and Fig. 5 using the Eqs. 30 and 31. The results of NPCR and UACI are given in Table 11. For two random templates, the expected values of NPCR and UACI [33] are 99.6094% and 33.4635%, respectively. From Table 11, the proposed method has high NPCR and suitable UACI

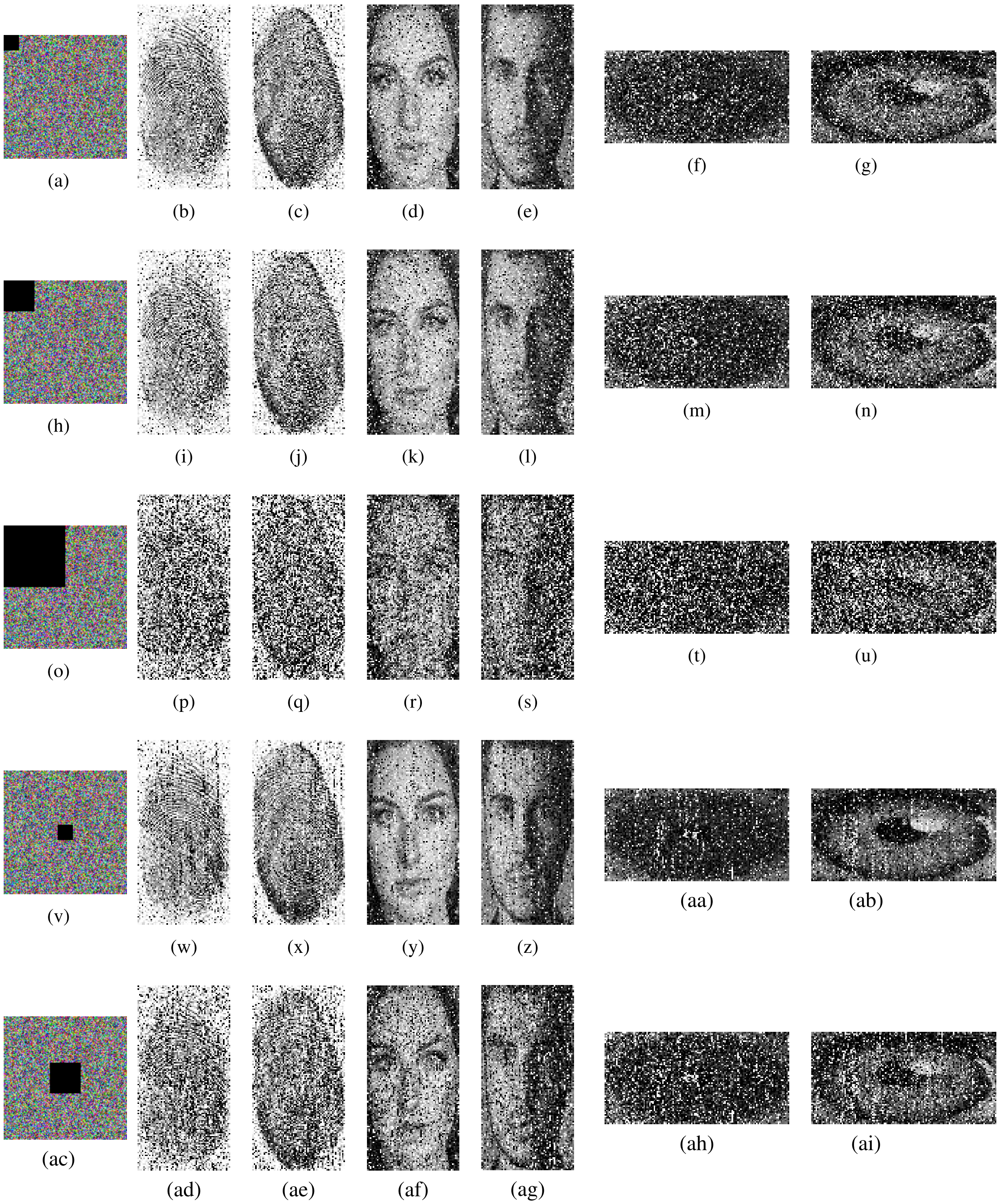


FIGURE 9. Experimental result of cropping attack: each row from the second column to the last column show decrypted templates under different levels of cropping attack.

values, which are close to standard values. On the basis of comparison of the experimental and the standard values, we can say that our method passes both NPCR and UACI tests, so the proposed method is resistant to differential attack.

VIII. COMPARISON WITH THE RELATED WORKS

A comparative analysis against existing methods was performed to check the authenticity, accuracy, and originality of the presented biometric templates encryption technique for real-time applications. We have compared our presented technique with other existing techniques [8], [20], [27], [28], [34]. The type of data, applied process, transform domain, permutation and substitution methods, the number of keys, sensitivity to secret keys, keyspace, entropy, PSNR of the decrypted image, and attack analysis are among the parameters considered for comparison, as described in Table 12.

The proposed approach advances research in the 2D FrDCT domain, as shown in Table 12. It also does well in terms of keyspace, key sensitivity, entropy, PSNR, cropping attack, and differential attack robustness.

IX. CONCLUSION

This paper presents a new encryption and decryption technique for the protection of biometric templates using the 6D-chaotic system and 2D FrDCT. Due to the sensitivity of the key (fractional orders) used, using 2D FrDCT in biometric template encryption significantly improves the safety parameters in the encrypted biometric template; however, the 6D-chaotic method is used to improve protection even further for any cryptanalyst attempting to decrypt the biometric templates without authorization, since the 6D-chaotic system is highly sensitivity with respect to initial and its control parameters. To exhibit the feasibility and stability of the proposed technique, computer simulations and experimental results are given. The proposed technique's robustness against statistical attacks is confirmed by security analyses such as entropy, histogram, and correlation analyses. The proposed technique is also resistant to brute-force attacks, according to the findings of the experiments. Furthermore, the proposed technique is resistant to cropping and differential attacks. On the basis of experimental results and security analysis, we can say that the proposed technique is fast and efficient encryption and decryption technique for biometric templates security.

ACKNOWLEDGMENT

The authors extend their appreciation to the supporters. This work was supported in part by the Universidad Autonoma de Zacatecas, Mexico, through the Consejo Nacional de Ciencia y Tecnología (CONACYT) Mexico and the Foundation of National Key Research and Development Program of China under Grant 2020YFC2008700, in part by the National Natural Science Foundation of China under Grant 82072228 and Grant 92048205, in part by the Foundation of Shanghai Municipal Commission of Economy and Informatization under Grant 202001007, in part by the Foundation of Shanghai Jiao Tong University under Grant CHDI-2019-C-02, and in part by the Council of Scientific and Industrial Research, New Delhi, India, under Grant 09/107(0385)/2017-EMR-I. Moreover, the anonymous reviewers are thanked for careful reading of their manuscript and their comments and suggestion that greatly improved the quality of the manuscript.

REFERENCES

[1] A. K. Jain, R. Bolle, and S. Pankanti, Eds., *Biometrics: Personal Identification in Networked Society*, vol. 479. New York, NY, USA: Springer, Apr. 2006, doi: 10.1007/b117227.

[2] L. R. Haddada, B. Dorizzi, and N. E. B. Amara, "A combined watermarking approach for securing biometric data," *Signal Process., Image Commun.*, vol. 55, pp. 23–31, Jul. 2017, doi: 10.1016/j.image.2017.03.008.

[3] S. Li, X. Chen, Z. Wang, Z. Qian, and X. Zhang, "Data hiding in iris image for privacy protection," *IETE Tech. Rev.*, vol. 35, no. 1, pp. 34–41, Dec. 2018, doi: 10.1080/02564602.2018.1520153.

[4] M. Douglas, K. Bailey, M. Leeney, and K. Curran, "An overview of steganography techniques applied to the protection of biometric data," *Multimedia Tools Appl.*, vol. 77, no. 13, pp. 17333–17373, Jul. 2018, doi: 10.1007/s11042-017-5308-3.

[5] 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 Appl.*, vol. 77, no. 2, pp. 2485–2503, Jan. 2018, doi: 10.1007/s11042-016-4280-7.

[6] B. Choudhury, P. Then, V. Raman, B. Issac, and M. K. Haldar, "Cancelable iris biometrics based on data hiding schemes," in *Proc. IEEE Student Conf. Res. Develop.*, Kuala Lumpur, Malaysia, Dec. 2016, pp. 1–6, doi: 10.1109/SCORED.2016.7810049.

[7] M. Gomez-Barrero, E. Maiorana, J. Galbally, P. Campisi, and J. Fierrez, "Multi-biometric template protection based on homomorphic encryption," *Pattern Recognit.*, vol. 67, pp. 149–163, Jul. 2017, doi: 10.1016/j.patcog.2017.01.024.

[8] P. Rakheja, P. Singh, R. Vig, and R. Kumar, "Double image encryption scheme for iris template protection using 3D Lorenz system and modified equal modulus decomposition in hybrid transform domain," *J. Mod. Opt.*, vol. 67, no. 7, pp. 592–605, May 2020, doi: 10.1080/09500340.2020.1760384.

[9] H.-S. Ye, N.-R. Zhou, and L.-H. Gong, "Multi-image compression-encryption scheme based on quaternion discrete fractional Hartley transform and improved pixel adaptive diffusion," *Signal Process.*, vol. 175, Oct. 2020, Art. no. 107652, doi: 10.1016/j.sigpro.2020.107652.

[10] N. Zhou, H. Jiang, L. Gong, and X. Xie, "Double-image compression and encryption algorithm based on co-sparse representation and random pixel exchanging," *Opt. Lasers Eng.*, vol. 110, pp. 72–79, Nov. 2018, doi: 10.1016/j.optlaseng.2018.05.014.

[11] Z.-J. Huang, S. Cheng, L.-H. Gong, and N.-R. Zhou, "Nonlinear optical multi-image encryption scheme with two-dimensional linear canonical transform," *Opt. Lasers Eng.*, vol. 124, Jan. 2020, Art. no. 105821, doi: 10.1016/j.optlaseng.2019.105821.

[12] N. Zhou, Y. Wang, and L. Gong, "Novel optical image encryption scheme based on fractional Mellin transform," *Opt. Commun.*, vol. 284, no. 13, pp. 3234–3242, Jun. 2011, doi: 10.1016/j.optcom.2011.02.065.

[13] A. B. Joshi, D. Kumar, A. Gaffar, and D. C. Mishra, "Triple color image encryption based on 2D multiple parameter fractional discrete Fourier transform and 3D Arnold transform," *Opt. Lasers Eng.*, vol. 133, Oct. 2020, Art. no. 106139, doi: 10.1016/j.optlaseng.2020.106139.

[14] A. B. Joshi and D. Kumar, "A new method of multi color image encryption," in *Proc. IEEE Conf. Inf. Commun. Technol.*, Allahabad, India, Dec. 2019, pp. 1–5, doi: 10.1109/CICT48419.2019.9066198.

[15] P. Rakheja, R. Vig, P. Singh, and R. Kumar, "An iris biometric protection scheme using 4D hyperchaotic system and modified equal modulus decomposition in hybrid multi resolution wavelet domain," *Opt. Quantum Electron.*, vol. 51, no. 6, p. 204, Jun. 2019, doi: 10.1007/s11082-019-1921-x.

[16] A. B. Joshi, D. Kumar, D. C. Mishra, and V. Guleria, "Colour-image encryption based on 2D discrete wavelet transform and 3D logistic chaotic map," *J. Mod. Opt.*, vol. 67, no. 10, pp. 933–949, Jul. 2020, doi: 10.1080/09500340.2020.1789233.

[17] A. B. Joshi, D. Kumar, and D. C. Mishra, "Security of digital images based on 3D arnold cat map and elliptic curve," *Int. J. Image Graph.*, vol. 21, no. 1, pp. 2150006–2150026, Dec. 2020, doi: 10.1142/S0219467821500066.

[18] H. Liu and X. Wang, "Color image encryption using spatial bit-level permutation and high-dimension chaotic system," *Opt. Commun.*, vol. 284, nos. 16–17, pp. 3895–3903, 2011, doi: 10.1016/j.optcom.2011.04.001.

[19] J. S. Khan and S. K. Kayhan, "Chaos and compressive sensing based novel image encryption scheme," *J. Inf. Secur. Appl.*, vol. 58, May 2021, Art. no. 102711, doi: 10.1016/j.jisa.2020.102711.

[20] M. Gomez-Barrero, C. Rathgeb, G. Li, R. Ramachandra, J. Galbally, and C. Busch, "Multi-biometric template protection based on Bloom filters," *Inf. Fusion*, vol. 42, pp. 37–50, Jul. 2018, doi: 10.1016/j.inffus.2017.10.003.

[21] S. Ajish and K. S. AnilKumar, "Iris template protection using double Bloom filter based feature transformation," *Comput. Secur.*, vol. 97, Oct. 2020, Art. no. 101985, doi: 10.1016/j.cose.2020.101985.

[22] G. Grassi, F. L. Severance, and D. A. Miller, "Multi-wing hyperchaotic attractors from coupled Lorenz systems," *Chaos, Solitons Fractals*, vol. 41, no. 1, pp. 284–291, Jul. 2009, doi: 10.1016/j.chaos.2007.12.003.

[23] N. Ahmed, T. Natarajan, and K. R. Rao, "Discrete cosine transform," *IEEE Trans. Comput.*, vol. C-23, no. 1, pp. 90–93, Jan. 1974, doi: 10.1109/T-C.1974.223784.

[24] S. Kumar, B. Panna, and R. Kumar, "Medical image encryption using fractional discrete cosine transform with chaotic function," *Med. Biol. Eng. Comput.*, vol. 57, no. 11, pp. 2517–2533, Sep. 2019, doi: 10.1007/s11517-019-02037-3.

[25] S. Zhu, G. Wang, and C. Zhu, "A secure and fast image encryption scheme based on double chaotic S-boxes," *Entropy*, vol. 21, no. 8, p. 790, Aug. 2019, doi: 10.3390/e21080790.

[26] A. Hamid, M. Ragab, O. S. F. Alla, and A. Y. Noaman. (2014). *Encryption Quality Analysis of the RCBC Block Cipher Compared With RC6 and RC5 Algorithms*. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.465.8187

[27] J. S. Khan, W. Boulila, J. Ahmad, S. Rubaiee, A. U. Rehman, R. Alroobaea, and W. J. Buchanan, "DNA and plaintext dependent chaotic visual selective image encryption," *IEEE Access*, vol. 8, pp. 159732–159744, Sep. 2020, doi: 10.1109/ACCESS.2020.3020917.

[28] J. S. Khan and J. Ahmad, "Chaos based efficient selective image encryption," *Multidimensional Syst. Signal Process.*, vol. 30, no. 2, pp. 943–961, Apr. 2019, doi: 10.1007/s11045-018-0589-x.

[29] Z. Wang and A. C. Bovik, "Modern image quality assessment," *Synth. Lect. Image, Video Multimedia Process.*, vol. 2, no. 1, pp. 1–156, Dec. 2006, doi: 10.2200/S00010ED1V01Y200508IVM003.

[30] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," *IEEE Trans. Image Process.*, vol. 13, no. 4, pp. 600–612, Apr. 2004, doi: 10.1109/TIP.2003.819861.

[31] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *J. Cryptol.*, vol. 4, no. 1, pp. 3–72, Jan. 1991.

[32] E. Biham and A. Shamir, "Differential cryptanalysis of the full 16-round DES," in *Proc. Annu. Int. Cryptol. Conf.* Heidelberg, Germany: Springer, Aug. 1992, pp. 487–496, doi: 10.1007/3-540-48071-4_34.

[33] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption," *Cyber J., Multidisciplinary J. Sci. Technol., J. Sel. Areas Telecommun.*, vol. 1, pp. 31–38, Apr. 2011.

[34] H. Singh, "Hybrid structured phase mask in frequency plane for optical double image encryption in gyrator transform domain," *J. Mod. Opt.*, vol. 65, no. 18, pp. 2065–2078, Oct. 2018, doi: 10.1080/09500340.2018.1496286.

DHANESH KUMAR received the M.Sc. degree in mathematics from Chhatrapati Shahu Ji Maharaj University Kanpur. He is currently pursuing the Ph.D. degree with the University of Lucknow, Lucknow, India. He qualified CSIR-JRF with AIR-39, UGC-JRF with AIR-84, and GATE with AIR-779. He has actively participated in several conferences and workshop held across India, in cryptography and network security, and has published more than nine research articles in the various national and international journals. His research interests include security and cryptography.

ANAND B. JOSHI received the Ph.D. degree in mathematics from the Department of Mathematics, Indian Institute of Technology Delhi (IIT Delhi). He had been working as an Assistant Professor with the Department of Mathematics, Dayalbag Education Institute, deemed University Agra, for more than three years. He had also been working as a Visiting Researcher with the Institute for Theoretical Information Technology, RWTH Aachen University, Germany, for one and half years. He is currently working as an Assistant Professor with the Department of Mathematics with the University of Lucknow, Uttar Pradesh, India. He has delivered a talk in many conferences and refresher programs for teachers. He has supervised many M.Phil. and has been guiding many Ph.D. students. He has published many research articles in various reputed journals of Springer, Elsevier, IEEE, and Taylor and Francis. His research interests include the area of cryptography, number theory, algebra, Boolean functions, image security, and digital image processing. He is a member of many professional societies, such as the Cryptography Research Society of India and the Bharata Ganita Parisad. He received the prestigious ERASMUS MUNDUS Scholarship from the European Commission.

SONALI SINGH received the B.Sc. and M.Sc. degrees in mathematics from the University of Lucknow, where she is currently pursuing the Ph.D. degree. She qualified GATE with AIR-951. Her research interests include cryptography and digital image security.

VISHNU NARAYAN MISHRA received the Ph.D. degree in mathematics from the Indian Institute of Technology at Roorkee, Roorkee, in 2007. He held academic positions as an Associate Professor at IGNTU, Amarkanta, an Assistant Professor with the AMHD, SVNIT, Surat, and a Guest Lecturer at MNNIT, Prayagraj. He is currently working as a Professor and the Head of the Department of Mathematics, Indira Gandhi National Tribal University, Amarkantak, Madhya Pradesh, India. He is actively involved in teaching undergraduate and postgraduate students and Ph.D. students. He is a referee and an editor of several international journals in frame of pure and applied mathematics, and applied economics. He has authored more than 280 research articles to his credit published in several journals and conference proceedings of repute and guided many postgraduate, and Ph.D. students (nine Ph.D.). His research interests include the areas of pure and applied mathematics, including approximation theory, variational inequality, fixed point theory, operator theory, Fourier approximation, non-linear analysis, special functions, q-series and q-polynomials, signal analysis, and image processing, and optimization. He is a member of many professional societies, such as the Indian Mathematical Society (IMS), the International Academy of Physical Sciences (IAPS), the Gujarat Mathematical Society, the International Society for Research and Development (ISRD), the Indian Academicians and Researchers Association (IARA), the Society for Special Functions and their Applications (SSFA), and the Bharat Ganit Parishad. Citations of his research contributions can be found in many books and monographs, Ph.D. thesis, and scientific journal articles, much too numerous to be recorded here. He awarded as Prof. H. P. Dikshit Memorial Award at Hisar, Haryana, in December 2019. Moreover, he serves voluntarily as a Reviewer for *Mathematical Reviews* (USA) and *Zentralblatt Math* (Germany). He received the Gold Medal in B.Sc., the Double Gold Medal in M.Sc., the V. M. Shah Prize in IMS, and the Young Scientist Award in CONIAPS, Allahabad University, Prayagraj, and the Best Paper Presentation Award at Ghaziabad. He has delivered talks at several international conferences, workshops, refresher programmes, and STTPs, as a resource person.

HAMURABI GAMBOA ROSALES received the bachelor's degree in electronics and communications engineering from the Faculty of Engineering, University of Guadalajara, in 2000, the master's degree in electrical engineering from the University of Guanajuato, in 2003, with a focus on the digital signal processing, and the Ph.D. degree in the area of voice processing from the Technical University of Dresden, Germany, in 2010. He is currently working as a Professor and a Researcher in the area of research digital signal processing with the Academic Unit of Electrical Engineering, Autonomous University of Zacatecas, Mexico.

LIANG ZHOU is currently working with the Center for Medicine Intelligent and Development, China Hospital Development Institute, Shanghai Jiao Tong University, Shanghai, China. His main research interests include Big data analysis and decision support.

ARVIND DHAKA received the Ph.D. degree in computer science and engineering from NIT Hamirpur, India (an institute of national importance), in 2018. Since 2018, he has been working as an Assistant Professor with the Department of Computer and Communication Engineering, Manipal University Jaipur. His research interests include wireless communication, wireless sensor networks, *ad-hoc* networks, medical image processing, and machine leaning and deep learning in image processing.

AMITA NANDAL received the Ph.D. degree in electronics and communication engineering from SRM University, Chennai, in 2014. Since 2018, she has been working as an Associate Professor with the Department of Computer and Communication Engineering, Manipal University Jaipur. Her research interests include digital signal processing, machine learning and deep learning for medical image processing, wireless communication, circuits systems, and FPGA implementation.

HASMAT MALIK (Senior Member, IEEE) received the M.Tech. degree in electrical engineering from the National Institute of Technology (NIT) Hamirpur, Himachal Pradesh, India, and the Ph.D. degree in electrical engineering from the Indian Institute of Technology (IIT), Delhi.

He has served as an Assistant Professor, for more than five years at the Division of Instrumentation and Control Engineering, Netaji Subhas Institute of Technology (NSIT), Delhi, India. He has been a Research Fellow with BEARS, University-Town, NUS Campus, Singapore, since January 2019. He has supervised 23 PG students. He involves in several large research and development projects. He has published widely in international journals and conferences, where his research findings related to intelligent data analytics, artificial intelligence, and machine learning applications in power systems, power apparatus, smart building and automation, smart grid, forecasting, prediction and renewable energy sources. He has authored/coauthored more than 100 research articles, eight books, and thirteen chapters in nine other books, published by IEEE, Springer, and Elsevier. His principal area of research interests include artificial intelligence, machine learning, and big-data analytics for renewable energy, smart building and automation, condition monitoring, and online fault detection and diagnosis (FDD). He is a fellow of Institution of Electronics and Telecommunication Engineering (IETE), a Life Member of the Indian Society for Technical Education (ISTE) and the International Society for Research and Development (ISRD), London, and a member of the Computer Science Teachers Association (CSTA), USA, the Association for Computing Machinery (ACM) EIG, and the Mir Labs, Asia. He is a chartered engineer and professional engineer. He received the POSOCO Power System Award (PPSA-2017) for his Ph.D. work for research and innovation in the area of the power systems. He has received the Best Research Paper Awards at IEEE INDICON-2015, and the Full Registration Fee Award at IEEE SSD-2012, Germany. He organized five international conferences, and proceedings have been published by Springer Nature.

SATYENDRA SINGH (Member, IEEE) received the B.E. degree in electrical engineering from the Government Engineering College Bikaner, Rajasthan, India, in 2008, the master's degree in power systems from the National Institute of Technology (NIT), Hamirpur, Himachal Pradesh, India, in 2011, and the Ph.D. degree in electrical engineering from the Malaviya National Institute of Technology (MNIT) at Jaipur, Jaipur, India, in 2019. He is currently working as an Assistant Professor with the School of Electrical Skills, Bhartiya Skill Development University, Jaipur, Rajasthan. His research interests include power systems, power system economics, electricity market, renewable energy modeling, FACTs devices, multi-agent systems, and nature-inspired algorithms.