IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 20 July 2022, accepted 23 August 2022, date of publication 31 August 2022, date of current version 30 September 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3203067

RESEARCH ARTICLE

Biomedical Multimedia Encryption by Fractional-Order Meixner Polynomials Map and Quaternion Fractional-Order Meixner Moments

ACHRAF DAOUI[1], MOHAMED YAMNI[2], HICHAM KARMOUNI[1], MHAMED SAYYOURI[1], HASSAN QJIDAA[2], MUSHEER AHMAD[3], AND AHMED A. ABD EL-LATIF[4,5], (Senior Member, IEEE)

[1]Engineering, Systems and Applications Laboratory, National School of Applied Sciences, Sidi Mohamed Ben Abdellah University, Fez 30050, Morocco
[2]Laboratory of Electronic Signals and Systems of Information (LESSI), Dhar El Mahrez Faculty of Science, Sidi Mohamed Ben Abdellah University, Fez 30050, Morocco
[3]Department of Computer Engineering, Jamia Millia Islamia, New Delhi 110025, India
[4]EIAS Data Science Laboratory, College of Computer and Information Sciences, Prince Sultan University, Riyadh 11586, Saudi Arabia
[5]Department of Mathematics and Computer Science, Faculty of Science, Menoufia University, Shebin El-Kom, Menoufia 32511, Egypt

Corresponding author: Ahmed A. Abd El-Latif (aabdellatif@psu.edu.sa)

This work was supported by the EIAS Data Science Laboratory, College of Computer and Information Sciences, Prince Sultan University, Riyadh, Saudi Arabia.

ABSTRACT Chaotic systems are widely used in signal and image encryption schemes. Therefore, the design of new chaotic systems is always useful for improving the performance of encryption schemes in terms of security. In this work, we first demonstrate the chaotic behavior of fractional order Meixner polynomials (FrMPs) for introducing a new two-dimensional (2D) chaotic system called FrMPs map. This system is very sensitive to any variation by 10^{-15} of its control parameters (μandβ).Next, we use FrMPs to introduce a new type of orthogonal transforms called quaternion fractional order Meixner moments (QFrMMs). The latter generalize the existing fractional order Meixner moments. To demonstrate the relevance of the proposed FrMPs map and QFrMMs in the field of signal and image processing, they are applied in the development of a new encryption scheme. The main advantage of this scheme is its applicability to the encryption of different types of biomedical data such as multi-biomedical signals, multiple grayscale medical images, color medical image, and grayscale medical image. Several simulation analysis (visual, histogram, runtime, correlation, robustness, etc.) are conducted to verify the efficiency of the proposed scheme. Simulation and comparison results confirm that our encryption method is effective in terms of high security level, high quality of the decrypted information, strong resistance to different types of attacks, etc. These findings support the suitability of the proposed scheme for the secure exchange of biomedical multimedia via a public communication channel.

INDEX TERMS Quaternion theory, quaternion fractional order moments, fractional-order polynomials, multiple image encryption, medical image encryption.

I. INTRODUCTION

In order to detect pathology in a patient, specialists/physicians must analyze a variety of data that are collected from a patient. These data can be biomedical signals and images, which are usually collected in hospitals and/or in medical analysis centers. Biomedical data can be transmitted between medical analysis centers and between specialists/physicians for the purpose of diagnosis and analysis. The transmission of these data is typically done via unsecure communication channel such as the Internet [1]. The privacy of individuals can therefore be negatively affected if the private medical data are misused by unauthorized persons who use the Internet [2].

A literature survey on medical data security approaches [3], [4], [5], [6], [7], [8] indicates that encryption schemes

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

can provide a high security level when exchanging the medical data via unsecured channels. However, existing encryption schemes are designed for either medical images [9], [10], [11], [12] or biomedical signals (bio-signals) [13], [14], [15]. To the best of our knowledge, no encryption scheme applicable to both medical images and bio-signals has yet been developed. For this purpose, we develop a novel encryption scheme, which is applicable for the encryption of bio-signals and images. The importance of developing such encryption scheme is that it is unified and can be used to encrypt different types of biomedical multimedia. It is also important to state that no multi-biomedical signals encryption scheme is available in the literature. Therefore, we propose in this work an encryption scheme that can be applied to the encryption of multi-biomedical signals. Examples of bio-signals that can be used as inputs to the proposed encryption scheme include the electrocardiogram (ECG) [13], [14] fingertip photoplethysmogram (PPG) [16], arterial blood pressure (ABP), electroencephalogram (EEG), electromyogram (EMG) signals; galvanic skin response (GSR), etc. Figure 1 shows some bio-signals that can be measured from a person's body with the positions where they are measured.

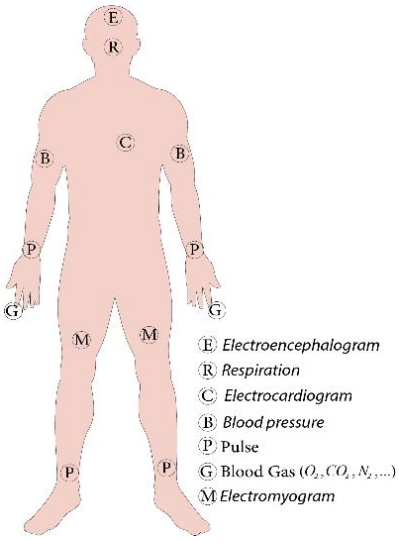


FIGURE 1. Some measurable bio-signals from the human body [17].

Encryption schemes are usually based on chaotic systems that are very sensitive to the variation of their initial conditions and parameters. The latter are used as security keys that are shared between the sender and the receiver via a secure communication channel.

Various chaotic systems can be found in the literature. However, the design of new chaotic systems remains an open research area. Starting from the idea that a high complexity level of the chaotic system can improve the security level of an encryption scheme [18], we put forward in this paper a new two-dimensional (2D) chaotic system called fractional order Meixner polynomials (FrMPs) map. The mathematical model of FrMPs map is complex in comparison to other models of existing 2D chaotic systems [19], [20], [21], [22], [23]. Therefore, a high level of security can be predicted by using FrMPs map in an encryption scheme. Moreover, the matrix form of FrMPs map is exploited in the introduction of a new type of discrete orthogonal moments called quaternion fractional order Meixner moments (QFrMMs). Then, FrMPs and QFrMMs are involved in the design of our unified encryption scheme. Indeed, QFrMMs are used in the diffusion phase of four inputs. Then, FrMPs map is used in the confusion phase. In both phases, QFrMMs and FrMPs map parameters are given as security keys. Finally, the encrypted data can be securely transmitted between different medical analysis centers. In the decryption phase, a reverse process of the encryption process is followed to recover the original data with negligible reconstruction/decryption errors. In both encryption and decryption phases, the same security keys must be used to correctly recover the original input data. The simulation results (see sections IV and VII.C) show that any variation by the order 10^{-15} of the security key parameters leads to the failure in recovering the original input data, which reflect the strong security level of our scheme.

The main contributions of the work presented in this paper are summarized as follows:

- ⋆ New 2D chaotic system called FrMPs map is proposed, which is very sensitive to any variation by the order 10^{-15} of its control parameters (μ and β).
- ⋆ New quaternion fractional order Meixner moments (QFrMMs) are proposed for the encryption of multiple inputs in a holistic and compact way.
- ⋆ Introduce a novel unified encryption scheme based on QFrMMs and FrMPs map for encrypting both bio-signal, grayscale medical image, color medical image, multi-biomedical signals and multi-grayscale medical images.
- ⋆ Provide experimental analysis and comparisons to prove the validity, efficiency and superiority of the proposed scheme.

The rest of the work is presented as follows: the second section covers the related work. The third section briefly presents the theoretical background of FrMPs. In the fourth section, we present the proposed FrMPs map. The proposed QFrMMs are presented in the fifth section. The details of the suggested unified encryption scheme are delivered in the sixth section. In the seventh section, the results of simulations and comparisons are offered to valid the efficiency of the designed scheme. Finally, conclusion and future work are outlined in the last section.

II. RELATED WORK

Discrete orthogonal moments (DOMs) are regarded as powerful descriptors in the field of digital signal and image processing. DOMs are computed based on discrete orthogonal polynomials (DOPs), like Tchebichef [24], Krawtchouk [2], Hahn [25], Meixner [26], Charlier [27], dual Hahn [28], [29] and Racah polynomials [30]. Lately, some discrete orthogonal polynomials involving fractional

order have been introduced in the literature. Many innovative discrete orthogonal moments of fractional order have been suggested based on these polynomials. Indeed, Liu *et al.* [31] derived the fractional order Krawtchouk polynomials (FrKPs) as a generalization of integer order Krawtchouk polynomials. Yamni *et al.* derived the fractional order Charlier polynomials (FrCPs) [32] and the fractional order Meixner polynomials (FrMPs) [33] as generalizations of Charlier and Meixner polynomials of integer order, respectively. Xiao *et al.* [34] derived the fractional order of Tchebichef polynomials (FrTPs) as generalization of Tchebichef polynomials of integer order. These authors used fractional order polynomials as kernel functions to express new discrete orthogonal moment transforms of fractional order. In addition, recent discrete orthogonal transforms of fractional order have been introduced that use two types of fractional order polynomials as kernel functions, such as the separable fractional order Charlier-Krawtchouk transform (FrCKTs) [2], and the separable fractional order Charlier-Meixner transform (FrCMTs) [35]. More recently, some fractional order transforms are extended to quaternion space using the quaternion theory. Indeed, Liu *et al.* extend the fractional order Krawtchouk transform to the quaternion fractional order Krawtchouk transform based on quaternion theory [36]. Yamni *et al.* extend the fractional-order Charlier and Hahn transforms to the quaternion fractional order Charlier transform [37] and quaternion fractional-order Hahn transform [38]. These transforms generalize the existing classical discrete orthogonal moments of integer order and provide excellent feasibility in various signal and image applications. However, the majority of the fractional-order transforms are designed for the analysis of single input (grayscale image or 1D signal). Motivated by the idea of introducing new discrete fractional order transforms that can be applied in the analysis of multiple inputs (color image channels, multiple 1D signals, multiple grayscale images, etc.), we introduce in the present work a new type of fractional order transforms called quaternion fractional order Meixner moments (QFrMMs). These moments are introduced on the one hand to generalize the existing fractional-order Meixner moments [33] and on the other hand to describe four input signals in a compact and simultaneous way. Table 1 presents a literature review on some discrete fractional order transforms including the proposed one with its applications.

From the analysis of the works illustrated in Table 1, it appears that the input data used in these works are either single or multiple. To overcome this limitation, we present in the current paper a generic framework that can be applied for the analysis of single or multiple inputs based on quaternion moments. Indeed, we introduce an unified encryption scheme using FrMPs and QFrMMs. This scheme is applicable to both single input and multiple inputs. The proposed scheme is applied for the encryption of biomedical multimedia (signals and images) that are transmitted via unsecured communication channels.

TABLE 1. Different discrete fractional order transforms and their applications.

Discrete orthogonal fractional order transforms	Applications	Single input	Multiple Inputs
Fractional-order Krawtchouk transform [31]	Image watermarking	✓	
Fractional order Charlier transform [32]	Image watermarking	✓	
Fractional order Charlier transform [27]	Signal encryption	✓	
Fractional order Meixner transform [33]	Image encryption	✓	
Fractional order Tchebichef transform [34]	Image encryption and watermarking	✓	
Fractional order discrete cosine transform [39]	Medical image encryption	✓	
Separable fractional order Charlier-Meixner [35]	Image watermarking	✓	
Separable fractional order Charlier-Krawtchouk [2]	Signal reconstruction and zero-watermarking	✓	
Quaternion fractional order Krawtchouk transform [36]	Color image encryption and watermarking		✓
Quaternion fractional order Charlier transform [37]	Color image zero-watermarking		✓
Quaternion fractional order Hahn transform [38]	Color image watermarking		✓
Proposed quaternion fractional order Meixner moments (QFrMMs)	**Encryption of single signal/image and multiple signals/images**	✓	✓

III. FRACTIONAL ORDER MEIXNER POLYNOMIALS

The well-known Meixner polynomials belong to the family of discrete orthogonal polynomials familiarized by Josef Meixner. The normalized Meixner polynomials (MPs) are defined as follows [40]:

$$\tilde{M}_n^{(\mu,\beta)}(x) = M_n^{(\mu,\beta)}(x)\sqrt{\frac{\omega(x)}{\rho(n)}} \tag{1}$$

where $M_n^{(\mu,\beta)}(x)$ is the n-th order Meixner polynomials well-defined by the following hyper-geometric function [41]:

$$M_n^{(\beta,\mu)}(x) = (\beta)_n {}_2F_1\left(-n, -x, \beta; 1-\frac{1}{\mu}\right) \tag{2}$$

where ${}_2F_1(.)$ is the hyper-geometric function given by:

$${}_2F_1\left(\begin{matrix} x_1, x_2 \\ y_1 \end{matrix} |z\right) = \sum_{k=0}^{\infty} \frac{(x_1)_k (x_2)_k}{(y_1)_k} \cdot \frac{z^k}{k!} \tag{3}$$

The weight $\omega(x)$ and the square norm $\rho(n)$ functions in Eq. (1) are defined as follows:

$$\omega(x) = \frac{\mu^x \Gamma(\beta + x)}{x!\Gamma(\beta)} \text{ with } \beta > 0 \text{ and } 0 < \mu < 1 \tag{4}$$

$$\rho(n) = \frac{n!(\beta)_n}{\mu^n (1-\mu)^\beta} = \frac{n!\Gamma(\beta+n)}{\mu^n (1-\mu)^\beta \Gamma(\beta)} \tag{5}$$

The computation of MPs using Eq. (1) is numerically unstable [26]. To overcome this problem, Daoui *et al.* use the following modified three-term recursive relation [26]:

$$\tilde{M}_n^{(\beta,\mu)}(x) = \psi \times \left[A\tilde{M}_n^{(\beta,\mu)}(x-1,N) + B\tilde{M}_n^{(\beta,\mu)}(x-2,N)\right]$$

with $\sigma(x) = x$; $\tau(x) = \beta\mu - x(1-\mu)$; $\lambda_n = n(1-\mu)$

$$\psi = \frac{1}{\sigma(x-1)+\tau(x-1)};$$

$$A = [2\sigma(x-1)+\tau(x-1)-\lambda_n]\sqrt{\frac{\mu(\beta+x-1)}{x}};$$

$$B = -\sigma(x-1)\sqrt{\frac{\mu^2(\beta+x-1)\beta+x-2)}{x(x-1)}} \quad (6)$$

where the initial PMs values for *x=0, 1* are calculated according to the next relations [26]:

$$\tilde{M}_n^{(\beta,\mu)}(0) = \sqrt{\frac{\mu(\beta+n-1)}{n}}\tilde{M}_{n-1}^{(\beta,\mu)}(0)$$

$$\text{with } \tilde{M}_0^{(\beta,\mu)}(0) = \sqrt{(1-\mu)^\beta} \quad (7)$$

$$\tilde{M}_n^{(\beta,\mu)}(1) = \left(\beta+n-\frac{n}{\mu}\right)\sqrt{\frac{\mu}{\beta}}\tilde{M}_n^{(\beta,\mu)}(0) \quad (8)$$

It is worth noting that Eqs. (6)-(8) represent the basic mathematical model that is used to generate MPs of orders $n = 0, 1, \ldots, N-1$, which are stored in a square matrix of size $N \times N$. Then, a spectral decomposition of this matrix is performed to obtain the following FrMPs [35]:

$$M^\alpha = \hat{V}D^\alpha\hat{V}^T = \sum_{k=0}^{N-1} e^{-jk\alpha\pi} v_k v_k^T \quad (9)$$

where M^α represents FrMPs matrix of size $N \times N$, $\hat{V}$ is a set of orthonormal eigenvectors of MPs that is specifically rearranged such that the MPs eigenvectors correspond to the eigenvalues of MPs, $v_k (k = 0, 1, \ldots, N-1)$ are the k-th column of $\hat{V}$, and D^α is defined as follows [35]:

$$D^\alpha = Diag\{1, e^{-j\alpha\pi}, e^{-j2\alpha\pi}, \ldots\ldots, e^{-j(N-1)\alpha\pi}\} \quad (10)$$

FrMPs have been used in the area of image processing with success [33], [35]. However, the chaotic behavior of these polynomials has not yet been studied or exploited. For this, we will highlight the chaotic character of FrMPs in the next section.

IV. PROPOSED CHAOTIC FrMPS MAP

In this section, we focus on highlighting the chaotic behavior of FrMPs in order to introduce a new 2D chaotic system called FrMPs map. First, FrMPs are computed for $\mu = 0.3$, $\beta = 128$, $\alpha = 0.5$, and *n, x = 0,1,...,255*. It should be mentioned that the parameters μ and β are set in Eqs. (6) - (8), and the fractional order parameter (α) is specified in Eq. (9). Then, the real and imaginary parts of FrMPs matrix of size 256×256 are demonstrated in Figure 2. From this figure, we can see that the values of FrMPs are almost randomly distributed in the polynomial matrix. This particularity of FrMPs can be successfully exploited for multimedia encryption.

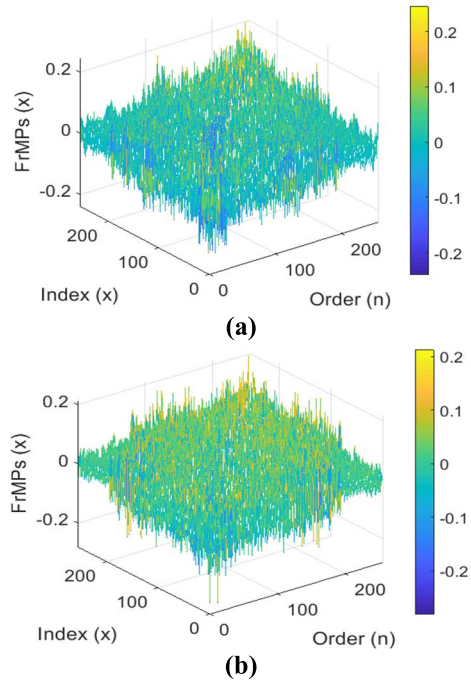


FIGURE 2. 3D plot of (a) real and (b) imaginary components of FrMPs calculated for $n, x = 0, 1, \ldots, 255$ with $\mu = 0.5$, $\beta = 128$ and $\alpha = 0.3$.

To display the chaotic behavior of FrMPs, one compute these polynomials up to a given order N for specified values of the parameters α, μ and β. Then, a slight variation is performed on one of these parameters to visualize the behavior of FrMPs to the performed variation. Indeed, FrMPs are computed for $n, x = 0, 1, \ldots, 15$ with $\mu = 0.8$, $\beta = 8$ and $\alpha = 1.3$, which allow to create a complex polynomial matrix of size 16×16. The latter is then decomposed into real and imaginary parts (matrices). The obtained matrices are then reshaped into *RV* and *IV* vectors each of size $N = 256$, respectively. Next, the value of the parameter μ is changed by a variation of the order $\Delta = 10^{-15}$ ($\mu* = \mu + \Delta$), and the process thus described to generate *RV* and *IV* is repeated to generate the vectors RV_μ (real part) and IV_μ (imaginary part) corresponding to FrMPs computed for $n, x = 0, 1, \ldots, 15$, $\mu^* = 0.8 + 10^{-15}$, $\beta = 8$ and $\alpha = 1.3$. *RV* and RV_μ vectors are shown in Figure 3 (a), and the vectors *IV* and IV_μ are shown in Figure 3 (b). In Figure 4, we display the influence of β parameter variation by the order 10^{-15} on FrMPs that are calculated for $n, x = 0, 1, \ldots, 15$, $\mu = 0.8, \beta = 8, \alpha = 1.3$ and $n, x = 0, 1, \ldots, 15$, $\mu = 0.8, \beta^* = 8 + 10^{-15}, \alpha = 1.3$, respectively. In Figure 5, we display the consequence of the fractional order (α) variation by the order 10^{-15} on FrMPs.

From the analysis of the results shown in Figures (4)-(6), we can see that the variation of the local parameters (μ and β) by the order 10^{-15} leads to a large variation of FrMPs values, while a variation by the order 10^{-15} of the fractional order parameter (α) does not lead to a significant variation on FrMPs. From these results, we can conclude that FrMPs displays a chaotic behavior. Therefore, FrMPs is considered

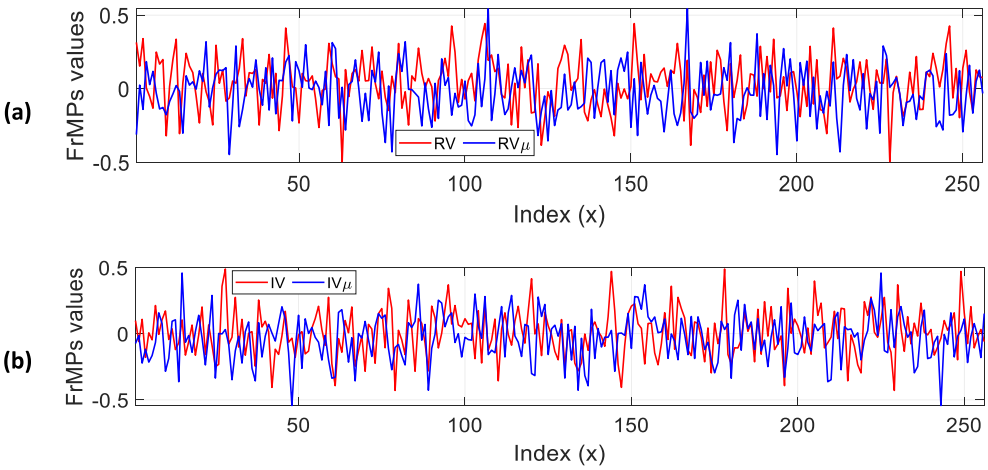


FIGURE 3. Influence of μ parameter variation by the order 10^{-15} on the (a) real (RV_μ) and (b) imaginary (IV_μ) parts of FrMPs.

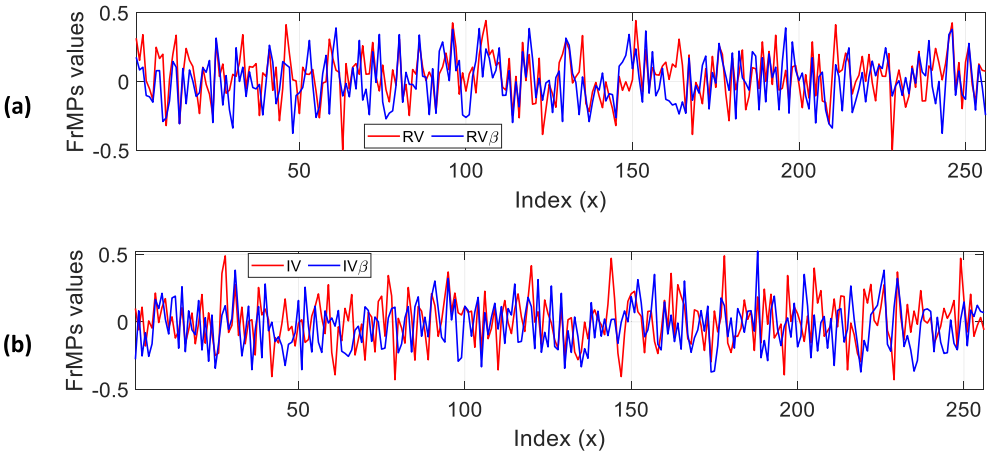


FIGURE 4. Influence of β parameter variation by the order 10^{-15} on the (a) real (RV_β) and (b) imaginary (IV_β) parts of FrMPs.

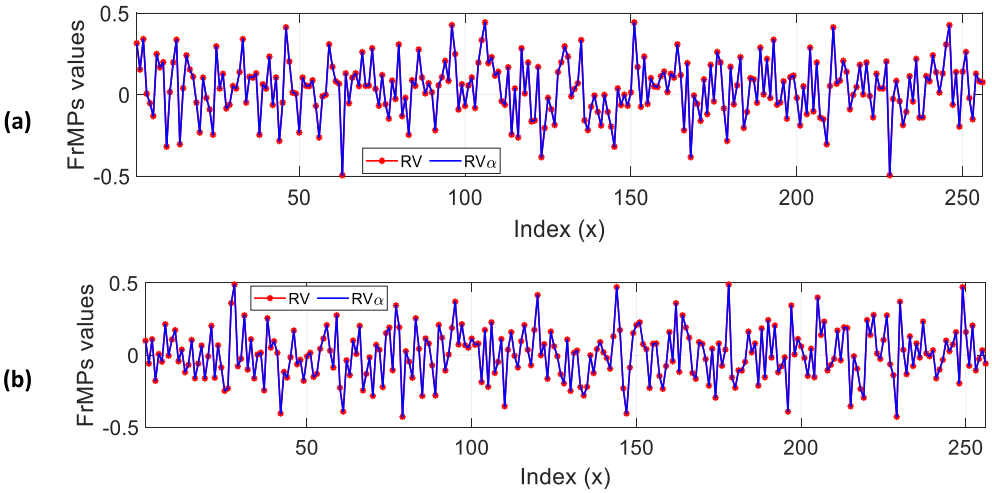


FIGURE 5. Influence of the fractional order α parameter variation by the order 10^{-15} on the (a) real (RV_α) and (b) imaginary (IV_α) parts of FrMPs.

as a new 2D chaotic system where the real part of FrMPs is the first dimension of this system and the imaginary part of FrMPs represents the second dimension of this system, which is called FrMPs map. The control parameters of this

map are the parameters $\mu(0 < \mu < 1)$ and $\beta(\beta > 0)$ with the fractional order α is set to a real value ($\alpha \in \mathbb{R}$). The mathematical model of the proposed FrMPs map is described by Eqs. (6)-(9). FrMPs map will be used in the confusion process of the proposed encryption scheme.

V. PROPOSED QUATERNION FRACTIONAL ORDER MEIXNER MOMENTS

Based on the quaternion algebra and FrMPs, a new discrete orthogonal transform called quaternion fractional order Meixner moments (QFrMMs) is proposed in this section. This transform can be used in the diffusion process of the proposed encryption scheme.

The quaternion number (q) is firstly introduced by Hamilton as follows: [42]:

$$q = a + bi + cj + dk \tag{11}$$

where a,b,c and d are real values with i,j and k are three imaginary numbers satisfying the following rules:

$$\begin{aligned} &i^2 = j^2 = k^2 = ijk = -1 \\ &ij = -ji = k, jk = -kj = i, ki = -ik = j \end{aligned} \tag{12}$$

If $a = 0$ in Eq. (11), q is called a pure quaternion.

The q number can be used to compactly represent four signals (S_1, S_2, S_3 and S_4) as follows [43]:

$$S = S_1 + S_2 i + S_3 j + S_4 k \tag{13}$$

Since the quaternion number is not commutative, we define the right-side QFrMMs as follows:

$$\begin{aligned} &QFrMM^R_{nm}(S) = \sum_{x=0}^{N-1}\sum_{y=0}^{M-1} S \times M_n^{\alpha_1}(x) \times M_m^{\alpha_2}(y)\mu \\ &\text{for } n = 0, \ldots, N-1 \text{ and } m = 0, \ldots, N-1 \end{aligned} \tag{14}$$

where μ is a pure unit quaternion selected in this paper as $\mu = -(i+j+k)/\sqrt{3}$. $M_n^{\alpha_1}$ and $M_m^{\alpha_2}$ represent FrMPs matrices of fractional orders $\alpha_1$and α_2, respectively.

Eq. (14) is equivalent to:

$$QFrMM^R_{nm}(S) = A_0 + iA_1 + jA_2 + kA_3$$

where

$$\begin{aligned} A0 &= \frac{1}{\sqrt{3}}\left[\sum_{x=0}^{N-1}\sum_{y=0}^{M-1} A \times M_n^{\alpha_1}(x) \times M_m^{\alpha_2}(y)\right] \\ A_1 &= -\frac{1}{\sqrt{3}}\left[\sum_{x=0}^{N-1}\sum_{y=0}^{M-1} B \times M_n^{\alpha_1}(x) \times M_m^{\alpha_2}(y)\right] \\ A_2 &= -\frac{1}{\sqrt{3}}\left[\sum_{x=0}^{N-1}\sum_{y=0}^{M-1} C \times M_n^{\alpha_1}(x) \times M_m^{\alpha_2}(y)\right] \\ A_3 &= -\frac{1}{\sqrt{3}}\left[\sum_{x=0}^{N-1}\sum_{y=0}^{M-1} D \times M_n^{\alpha_1}(x) \times M_m^{\alpha_2}(y)\right] \end{aligned} \tag{15}$$

with

$$\begin{aligned} A &= S_2(x,y) + S_3(x,y) + S_4(x,y), \\ B &= S_1(x,y) + S_3(x,y) - S_4(x,y), \\ C &= S_1(x,y) + S_4(x,y) - S_2(x,y), \\ D &= S_1(x,y) + S_2(x,y) - S_3(x,y) \end{aligned}$$

It is worth mentioning that the proposed QFrMMs depend on six parameters ($\mu_1, \beta_1, \alpha_1, \mu_2, \beta_2, \alpha_2$). These parameters can be used as a security key of our encryption scheme.

The inverse transformation of the right-side of QFrMMs can be computed by the following relation:

$$\hat{S} = \hat{S}_1 + i\hat{S}_2 + j\hat{S}_3 + k\hat{S}_4$$

with

$$\begin{aligned} \hat{S}_1 &= \frac{-1}{\sqrt{3}}\left[\sum_{n=0}^{N-1}\sum_{m=0}^{M-1} (A_1 + A_2 + A_3)\, M_n^{\alpha_1}(x) M_m^{\alpha_2}(y)\right] \\ \hat{S}_2 &= \frac{1}{\sqrt{3}}\left[\sum_{n=0}^{N-1}\sum_{m=0}^{M-1} (A_0 + A_2 - A_3)\, M_n^{\alpha_1}(x) M_m^{\alpha_2}(y)\right] \\ \hat{S}_3 &= \frac{1}{\sqrt{3}}\left[\sum_{n=0}^{N-1}\sum_{m=0}^{M-1} (A_0 - A_1 + A_3)\, M^{\alpha_1}(x) M^{\alpha_2}(y)\right] \\ \hat{S}_4 &= \frac{1}{\sqrt{3}}\left[\sum_{n=0}^{N-1}\sum_{m=0}^{M-1} (A_0 + A_1 - A_2)\, M_n^{\alpha_1}(x) M_m^{\alpha_2}(y)\right] \end{aligned} \tag{16}$$

where $\hat{S}_1$, $\hat{S}_2$, $\hat{S}_3$ and $\hat{S}_4$ represent the reconstructed versions of the original signals S_1, S_2, S_3 and S_4, respectively.

To measure the reconstruction error between an original signal (S) and its reconstructed form ($\hat{S}$), we can use the following mean-square error (MSE) criterion:

$$MSE = \frac{1}{N \times M}\sum_{x=0}^{N-1}\sum_{y=0}^{M-1}\left[S(x,y) - \hat{S}(x,y)\right]^2 \tag{17}$$

The peak signal-to-noise ratio (PSNR) criterion is also utilized to compute the reconstruction error. This criterion is given by the next relation:

$$PSNR = 10\log_{10}\left(\frac{\sum_{x=1}^{N}\sum_{y=1}^{M}[S(x,y)]^2}{\sum_{x=1}^{N}\sum_{y=1}^{M}\left[S(x,y) - \hat{S}(x,y)\right]^2}\right) \tag{18}$$

If the MSE value tends to zero (high PSNR), it means that the original signal and its reconstructed form are very similar.

To quantity the difference between the reconstructed 1D signal $\hat{f}(i)$ and the original one $f(i)$, we can use the following Percentage Root Difference (PRD (%)) criterion [44]:

$$PRD(\%) = \sqrt{\frac{\sum_{i=1}^{N}\left[f(i) - \hat{f}(i)\right]^2}{\sum_{i=1}^{N}\left[\hat{f}(i)\right]^2}} \times 100 \tag{19}$$

The next section presents the proposed unified encryption scheme based on FrMPs and QFrMMs.

VI. PROPOSED ENCRYPTION SCHEME FOR BIOMEDICAL MULTIMEDIA

The diagram of the novel suggested encryption scheme is presented in Figure 6, which show that our scheme involves two main phases, namely (i) the holistically encryption of four biomedical data records in a storage device, and (ii) the decryption of the received data via the internet in another storage device. The details of the proposed scheme are presented in the next subsections.

A. BIOMEDICAL DATA ENCRYPTION PHASE

This phase is conducted at a storage device located in a medical analysis laboratory or in a hospital. The present phase includes the following steps:

Step 1: In this step of preprocessing, four inputs (I_1, I_2, I_3 and I_4) of biomedical data are used simultaneously. These data can be one bio-signal divided into four frames, four bio-signals reshaped in 2D matrices, four grayscale medical images, one color medical image represented in CMYK color space, or one grayscale medical image divided into four blocks. The dimensions of the inputs are stored in a matrix noted $Dim = [D_1, D_2, D_3, D_4]$ where D_1, D_2, D_3 and D_4 represent the dimensions of I_1, I_2, I_3 and I_4, respectively. Then the inputs are reshaped into four matrices S_1, S_2, S_3 and S_4 where the size of each matrix is $N \times M$. Note that the zero-padding method [45] can be used to make S_1, S_2, S_3 and S_4 of equal size. Next, Eq. (13) is used to represent the S_1, S_2, S_3 and S_4 by quaternion representation, which allows to obtain a quaternion matrix noted S of size $N \times M$. The latter is then divided into non-overlapping blocks each of size 8×8 to optimize the computation time of FrMPs matrix in the next step.

Step 2: This step represents the input data diffusion process of our scheme. For this purpose, the S matrix produced in the previous step is divided into blocks each of size 8×8. Next, Eq. (15) is used to compute QFrMMs of each block. Then, QFrMMs corresponding to each block are concatenated to produce a quaternion matrix named QM of size $N \times M$ (e.g. 512×512, 1024×768, 1800×1200, 1024×1024 etc.). The resulting QM matrix represents the diffused input data. It is worth mentioning that the parameters $\{\alpha_1, \alpha_2, \mu_1, \mu_2, \beta_1, \beta_2\}$ of QFrMMs (Eq. (15)) are provided as a security key noted *KEY1*. The optimal choice of these parameters is conducted according to the systematic method presented in [2], which is based on the Sine Cosine Algorithm (SCA) [46]. The use of this method guarantees the good quality of the reconstructed image when using our scheme. To illustrate the relevance of this method, three medical color images of various sizes are reconstructed by QFrMMs.Then, we display in Figure 7 the reconstructed images with the selected parameters by the method given in [2], and the reconstruction error (PSNR) that corresponds to each image.

From the results shown in Figure 7, we can notice that the PSNR values are high, which indicates that the medical images are reconstructed with high quality. These results

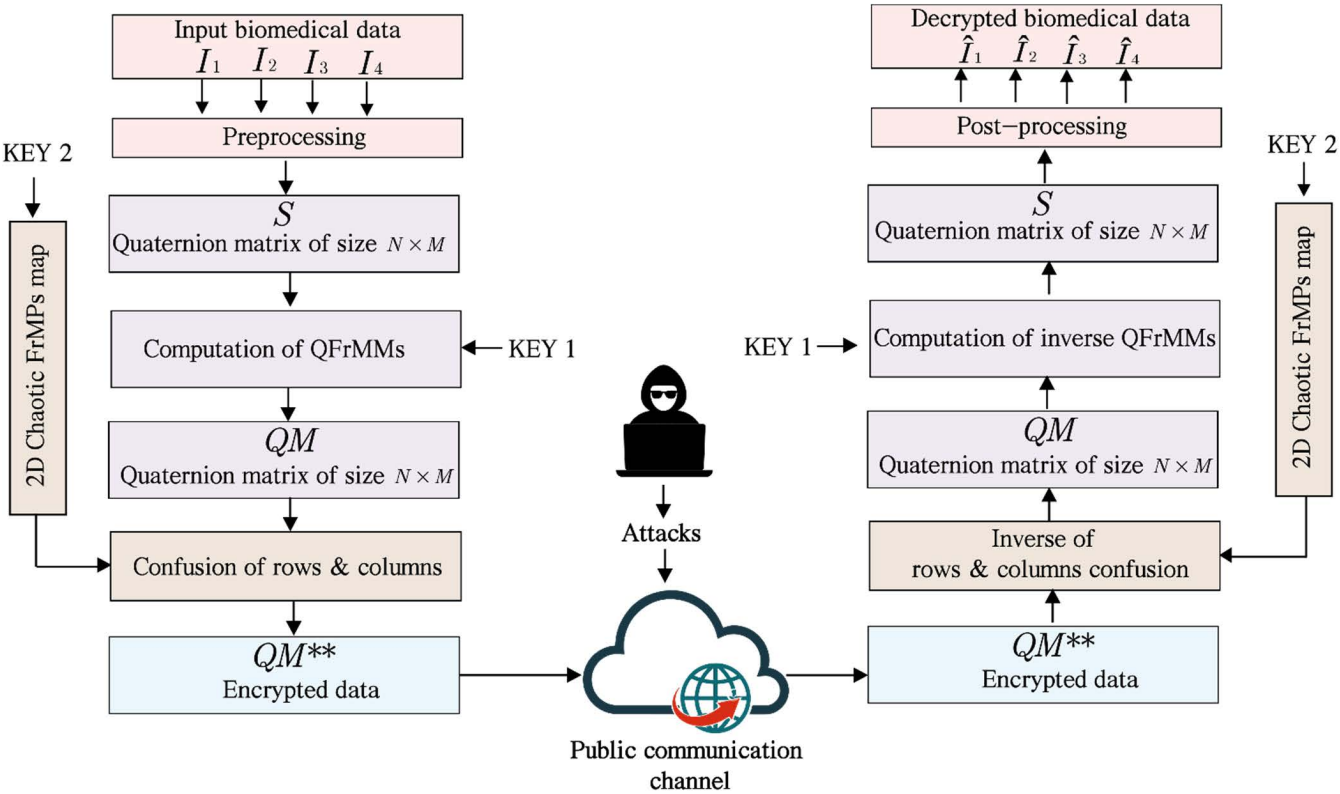


FIGURE 6. Diagram of the proposed scheme for multiple biomedical data encryption.

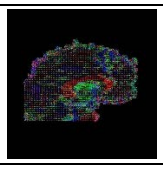
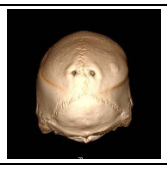
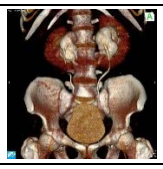
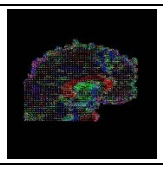
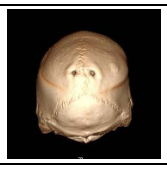
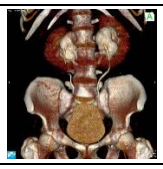
Test images			
Size	720×720	512×512	1024×1024
Reconstructed images			
Optimal QFrMMs parameter values	$\alpha_1 = 1.22; \alpha_2 = 2.13$ $\mu_1 = 0.58; \mu_2 = 0.95$ $\beta_1 = 6.01, \beta_2 = 3.21$	$\alpha_1 = 0.97; \alpha_2 = 3.12$ $\mu_1 = 0.45; \mu_2 = 0.70$ $\beta_1 = 4.02, \beta_2 = 4.17$	$\alpha_1 = 2.05; \alpha_2 = 6.16$ $\mu_1 = 0.75; \mu_2 = 0.43$ $\beta_1 = 7.05, \beta_2 = 3.98$
PSNR	PSNR = 292.15	PSNR = 291.79	PSNR=293.05

FIGURE 7. Color medical images reconstructed by QFrMMs with the optimal parameters of QFrMMs selected by the method given in [2].

confirm that the method presented in [2] is successful in selecting the optimal parameters of QFrMMs.

It is important to mention that FrMPs are computed only for $n,x = 0,1,\ldots,7$. Therefore, the runtime of QFrMMs basis polynomials is fast.

Step 3: This step is known as the scrambling process (confusion) and it is designed to increase the security level of our scheme. During this step, we use FrMPs map in the following way:

(a) Generate a 2D chaotic sequences (*C1* and *C2*) each of size L with $L \geq \max[N, M]$. Then, these sequences are normalized in the interval $[-N, N]$ with rounding their components to integer values.

(b) Use the elements of *C1* sequence to confuse each row of *QM* matrix via a circular shifting operation by k-positions with $k_i = C1(i), i = 1, 2, \ldots, N$ i.e. $QM * (i, :) = circshift\ (QM\ (i, :)\ , k_i)\ , i = 1, 2, \ldots, N$, where $Y = circshift(A,k)$ is a function that circularly shifts the elements of the A matrix by k positions [47].

(c) Use the elements of *C2* sequence to confuse each column of MQ^* matrix by a circular shifting operation of h-positions with $h_j = C2(j), j = 1, 2, \ldots, M$ i.e. $QM^{**}\ (:, j) = circshift\ \left(QM^*\ (:, j)\ , h_j\right), j = 1, 2, \ldots, M$. Thus, the resulting QM^{**} matrix represents the encrypted medical data that will be communicated from one storage device to another one via the Internet.

In the present step, the values of the FrMPs map parameters are specified as a security key noted $KEY2$ with $KEY2 = \{\alpha_3, \mu_3, \beta_3\}$. It should be mentioned that the selection of *KEY2* parameters is made by the user in the definition domain of FrMPs parameters. Moreover, it is important to mention that the *Dim* matrix, and the security keys (*KEY1* and *KEY2*) are transferred from the sender to the receiver via a secure communication channel [48] to assure the confidentiality of the proposed encryption scheme.

B. DECRYPTION PHASE OF THE RECEIVED DATA

The present phase is performed at the storage device that receives the encrypted biomedical data. In this phase, we perform the inverse process of the steps given in the encryption phase to retrieve the original biomedical data. Indeed, the following steps are involved:

Step 1: In this step, the inverse process to that described in Step 2 of subsection VI.A is followed. Indeed, 2D chaotic sequences *C1* and *C2* each of size L are generated via the proposed FrMPs map using *KEY2* as initial conditions of this map. Then, *C2* and *C1* sequences are used to apply the inverse confusion of QM^{**} columns and rows, respectively, for recovering matrix.

Step 2: This step consists first of subdividing *QM* matrix into 8×8 blocks. Then, the inverse of QFrMMs (IQFrMMs) is computed for each block according to Eq. (16). Finally, the computed IQFrMMs of the blocs are concatenated to retrieve the quaternion matrix S of size $N \times M$. In the current step, *KEY 1* is used for computing IQFrMMs.

Step 3: This step begins with separating the quaternion matrix S into four components (S_1, S_2, S_3 and S_4). The latter are then reshaped into $\hat{I}_1, \hat{I}_2, \hat{I}_3$ and $\hat{I}_4$ matrices (or 1D signals) that represent the decrypted medical data of sizes D_1, D_2, D_3, D_4 (with $Dim = [D_1, D_2, D_3, D_4]$), respectively.

It is worth mentioning that the four biomedical input data are decrypted with very low reconstruction errors, which can be measured using the reconstruction error criteria (MSE, PRD, PSNR, etc.). It is also important to note that an efficient transform-based encryption scheme requires the reconstruction error to be close to zero ($MSE, PRD \simeq 0$).

VII. SIMULATION RESULTS AND PERFORMANCE ANALYSIS

In this section, we outline the strengths and capabilities of the suggested method for encrypting multi-biomedical signals and images. It should be noted that all the experiments of the actual work are realized using Matlab 9.6 installed on a 2.4 GHz processor PC with 4 GB of RAM.

A. RECONSTRUCTION ERRORS ANALYSIS OF BIOMEDICAL SIGNALS

To perform the following test, we use four biomedical signals of different types selected from the PhysioBank database [49] that contains more than 90,000 digitized physiological signal records. The types of the selected bio-signals are ECG, impedance pneumography respiratory (IPR), EEG and EMG, and the size of each signal is $N = 4096$ samples (Figure 8). The selected ECG signal is labeled as "Record 100" in the MIT-BIH arrhythmia database, where the recordings are digitized at 360 samples per second. The IPR signal is labeled as "bidmc01" in the BIDMC PPG and Respiration Dataset. This signal is sampled at 125 Hz. Regarding the EEG signal, it is denoted "chb01_01_edfm" in CHB-MIT Scalp EEG Database, which contains signals sampled at 256 samples per second with a resolution of 16 bits. The EMG signal is

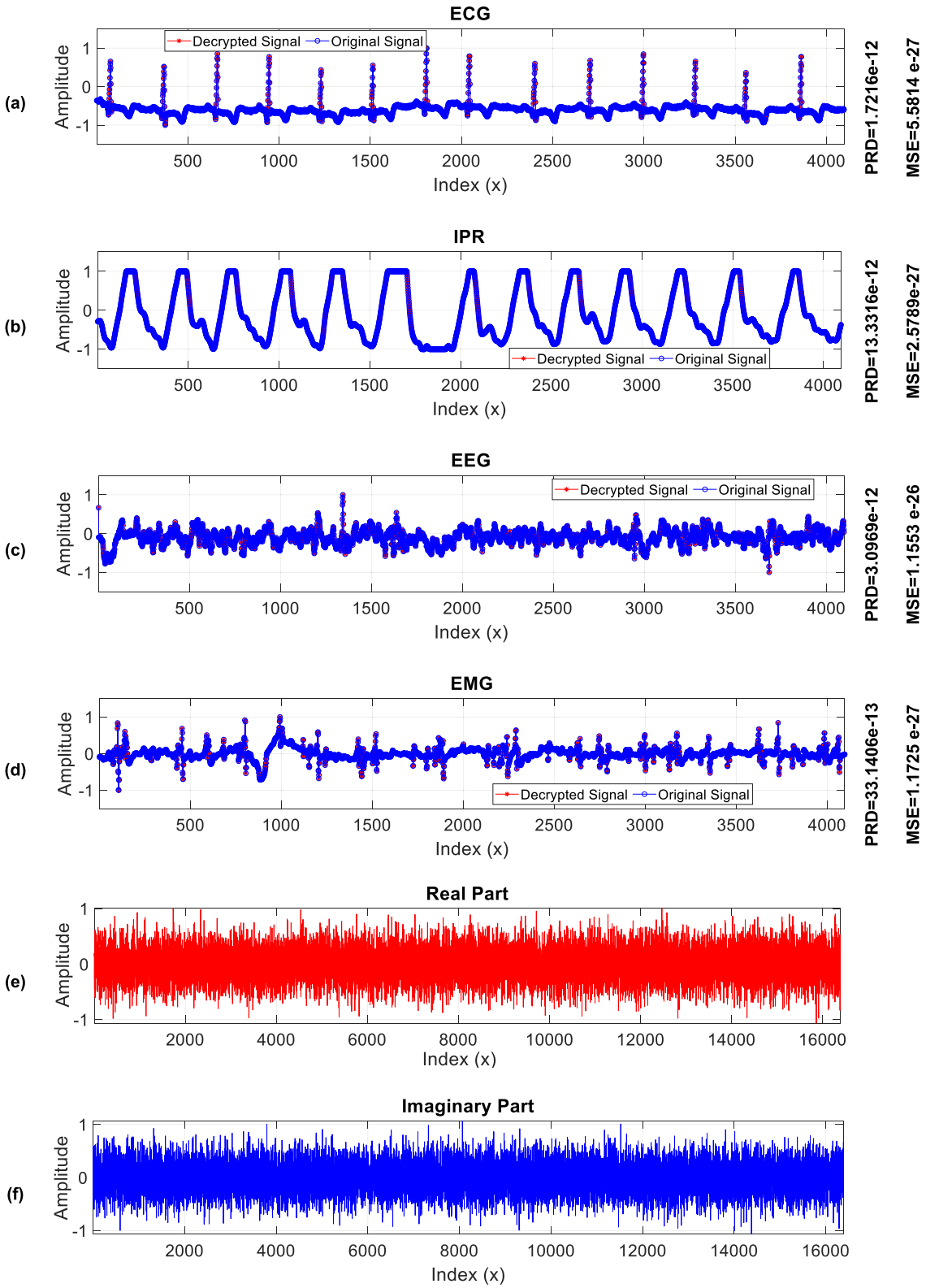


FIGURE 8. (a)-(d) Original and decrypted biomedical signals (ECG, PPG, EEG, and EMG) with the MSE and PRD values that correspond to the decrypted signals. (e) Real and (f) imaginary parts of the encrypted signals.

labeled "emg_healthy" in the Examples of Electromyograms database. The EEG signals of this dataset were recorded at 50 KHz and then downsampled to 4 KHz. It should be mentioned that the amplitudes of these signals are not normalized in

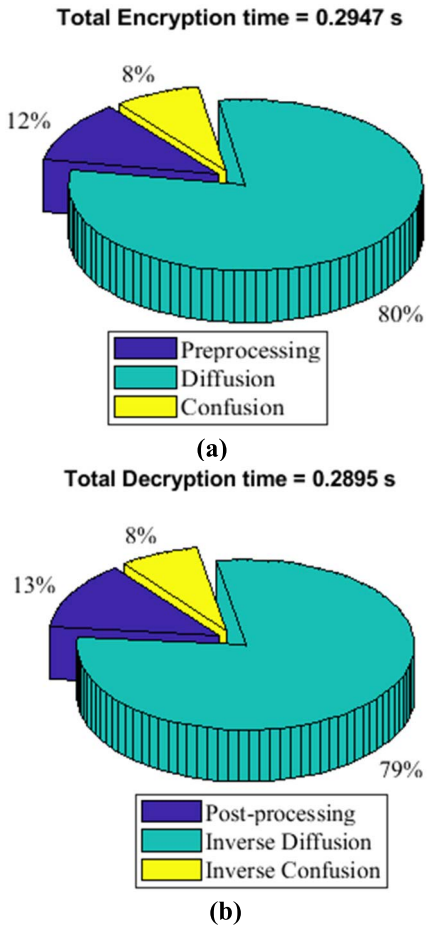


FIGURE 9. The average execution time details of (a) the encryption and (b) the decryption phases of the ECG, PPG, EEG, and EMG test signals, each of size $N = 4096$ samples.

the original database. For this reason, we normalize their amplitude to the interval $[-1, 1]$ for performing the numerical simulations. Then, the test signals are encrypted by the proposed method, generating a quaternion matrix ($QM**$) of size $N \times M$. The four components of this matrix are mapped to create a complex matrix of size $2N \times 2M$ in order to facilitate the presentation of the achieved results. Then, this matrix is reshaped into 1D vector that represents the encrypted bio-signals. The latter is of complex form, for that it is displayed in Figure 8 in two parties that represent the real part and the imaginary one of the complex vector. It can be seen from Figure 8 that there exists no visual likeness between the original signals and their encrypted form. This result indicates that the suggested scheme is able to hide all visual information of the input signals.

The decrypted signals with the corresponding PRD (%) values are given in the same Figure 8. The results achieved in this figure display that the four bio-signals are decrypted with reconstruction error tending to zero (MSE $< 10^{-27}$ and PRD (%) $< 10^{-12}$). This evidently specifies the high quality of the reconstructed bio-signals by the suggested method.

Noting that the present test is performed by using the following security key in both encryption and decryption phases:

$$\begin{aligned} KEY &= \{\alpha_1, \alpha_2, \mu_1, \mu_2, \beta_1, \beta_2, \alpha_3, \mu_3, \beta_3\} \\ &= \{1.3, 1.45, 0.8, 0.75, 8, 7.5, 1.25, 0.77, 8.1\} \end{aligned}$$

B. RUNTIME ANALYSIS

To show the execution speed of our scheme, one measures the execution time of the encryption and decryption phases the four test signals (ECG, PPG, EEG, and EMG). Indeed, each phase is executed 100 runs, and then the average time of both phases is obtained and shown in Figure 9. From the achieved results, we can observe that the average time to encrypt and then decrypt the four input signals each of size N = 4096 is 0.5842 sec. This encouraging result makes our method promising for use in the encryption of bio-signals.

C. KEY SENSITIVITY AND KEY SPACE ANALYSIS

This section analyses the influence of the security KEY parameters modification on the reconstruction quality of the decrypted bio-signals. Indeed, a slight variation by the order $\Delta = 10^{-15}$ is performed in the decryption phase on one of the following KEY parameters:

$\{\mu_1, \mu_2, \beta_1, \beta_2, \mu_3, \beta_3\} = \{0.8, 0.75, 8, 7.5, 0.77, 8.1\}$. Then, we observe the effect of the performed deviation on the quality of the decrypted signal. It should be noted that the KEY parameters $\{\alpha_1, \alpha_2, \alpha_2\}$ are not very sensitive to a slight variation by the order Δ. For this reason, they are not considered in the present test. The original signals as well as the decrypted ones are demonstrated in Figure 10. From this figure, it is obvious that the quality and the visual representation of the decrypted signal are significantly degraded when a slight variation by the order $\Delta = 10^{-15}$ is performed on one parameter value of the security key (KEY). This result clearly designates that the proposed map is quite sensitive to the slight deviation of the security key.

By considering the precision order of about 10^{-15} for real type value of double precision, the KEY size of our scheme comes approximately equal to $(10^{15})^6 = 10^{90} \simeq 2^{294}$. This key space is sufficiently higher than the minimum recommended key size that is 2^{100} [50], which delivers adequate security against exhaustive brute-force assaults.

D. HISTOGRAM ANALYSIS

Histogram analysis is frequently used to illustrate the toughness of an encryption scheme against statistical attacks. The histograms of the original, encrypted and decrypted signals are displayed in Figure 11. From this figure, we can clearly note that the original and the decrypted signals histograms are quite same, which specifies that the anticipated scheme does not change the statistical characteristics of input signals. On the other hand, we notice that the histograms of the real and imaginary parts of encrypted signal are very different from the histograms of the original/decrypted signals, which means that our scheme can efficiently resist statistical attacks,

TABLE 2. Correlation analysis results of the proposed scheme using various bio-signals.

Bio-signals	r_{XY} value for the original and encrypted signals	r_{XY} value for the original and decrypted signals
ECG	-0.0101	1
IPR	0.0092	1
EEG	0.0102	1
EMG	-0.0032	1

so any useful information can be obtained by analyzing the histograms of the encrypted signal.

E. CORRELATION ANALYSIS

To assess the statistical dependence between input, encrypted and decrypted signals, the correlation coefficient r_{XY} is widely used. The following relation defines this coefficient for two input signals X and Y of the same size:

$$r_{XY} = \frac{C(X, Y)}{\sqrt{V(X)}\sqrt{V(Y)}} \tag{20}$$

where $C(X, Y)$ represents the covariance of X and Y, with $V(X)$ and $V(Y)$ are the variance of X and Y signals, respectively. If r_{XY} tends to zero, this implies that there is no statistical dependence between X and Y. In contrast, when $|r_{XY}|$ tends towards one, there is a strong statistical dependence between X and Y.

Since the size of each original/decrypted signal is N, and the encrypted signals size is $4N$, we select arbitrary sequences of size N from the encrypted signal to compute r_{XY} values in the following test. The same test signals demonstrated in Figure 8 are used in the present test. The results of this test are given in Table 2 that indicate,on the one hand, that the values of r_{XY} corresponding to the original signals and the encrypted one tend towards zero, which specifies that there is no statistical dependency between the original signals and the encrypted ones. It is also noticeable that the r_{XY} values are equal to one for the original and decrypted signals, which designates that our scheme provides a perfect reconstruction of the decrypted signals with an insignificant reconstruction error.

The following test is provided for a comparison between the suggested method and other excellent bio-signal signal (ECG and EEG) encryption methods presented in [14], [51], and [52]. The comparison is conducted in terms of the correlation coefficient and the average runtime for both encryption and decryption phases of each method. For this perseverance, the test signals demonstrated in Figure 8 are used. The average $|r_{XY}|$ value corresponding to the original and the encrypted signals is premeditated for each encryption scheme and then reported in Table 3. Similarly, the average $|r_{XY}|$ values corresponding to the original and the decrypted signals are presented in the same table. It is worth mentioning that the

TABLE 3. Comparison in terms of average values of $|r_{XY}|$ between our scheme and recent schemes given in [14], [51], [52], and [53].

Encryption scheme	Average $\lvert r_{XY}\rvert$ value of the original and encrypted signals	Average $\lvert r_{XY}\rvert$ value of the original and encrypted signals	Average time in (sec) for the encryption & decryption phases
Scheme [51]	0.0095	1	1.0236
Scheme [14]	0.0205	0.9902	1.6411
Scheme [52]	0.0102	0.9921	1.3872
Scheme [53]	0.0098	1	1.8257
Proposed	**0.0085**	**1**	**0.5842**

bio-signal encryption methods provided in [14], [51], [52], and [53] are suitable for encrypting a single input bio - signal. For this purpose, the average time of 100 executions is calculated for each method and then multiplied by four to compare the obtained time with the mean running time of the projected method, which is used for the simultaneous encryption of four input bio-signals. From the comparison results achieved in Table 3 it appears that, the suggested scheme achieves improved performance than the competitive approaches in terms of statistical dependence between the original, encrypted and decrypted signals. This can be explained by the fact that FrMPs exhibit chaotic characters on the one hand, and QFrMMs generate a decrypted signal with negligible reconstruction errors on the other hand. Moreover, we notice that the execution time of the suggested encryption method is lower than the compared methods. The reason for this can be explicated by the circumstance that our scheme is block-based method, which reduces the computational time in comparison to the compared methods.

After confirming the usefulness of our scheme for the encryption of multi-biomedical signals, we show in the next section the usefulness of our scheme in the encryption of multiple grayscale medical images.

F. VISUAL AND HISTOGRAM ANALYSIS

This section presents the tests that justify the competence of the suggested scheme in the encryption of multiple medical images. For this purpose, we arbitrary select four Magnetic resonance imaging (MRI) from the [54] dataset and four Computed Tomography (CT) images from the [55] dataset, which contains over 32,000 labelled lesions detected on CT images.

In the present test, the selected images of size 512×512 are encrypted via the suggested method. Then, the four input test images, encrypted and decrypted ones are displayed in Figure 12. The results presented in this figure specify that the quality of the decrypted CT images is very high (PSNR$>$290). Therefore, the diagnosis of a specific pathology cannot be influenced by this very low degradation of the derypted images. On the other hand, we can see that the real and imaginary parts of the encrypted image fully hide the visual information of the plaintext CT images. Therefore, the

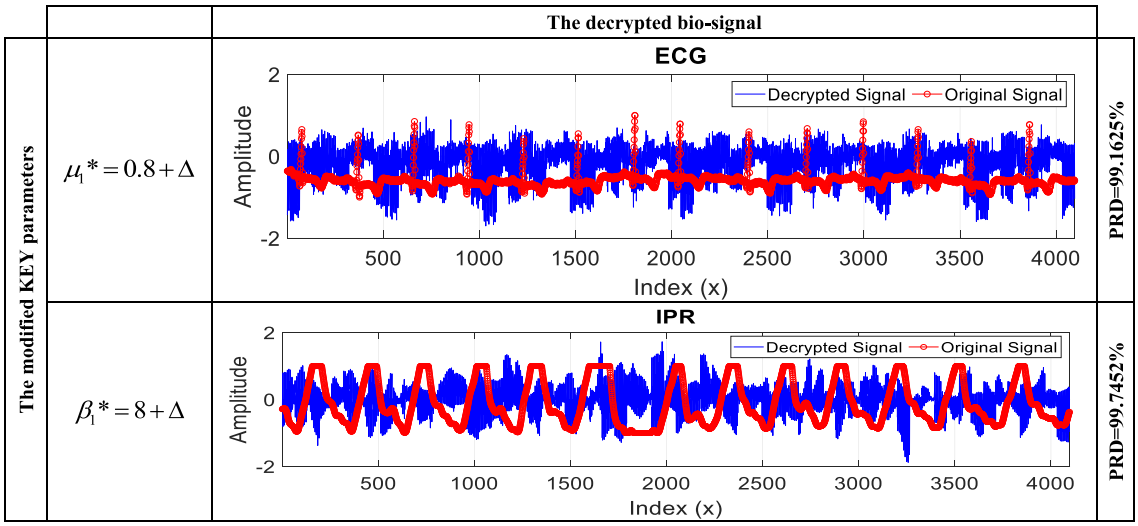


FIGURE 10. Influence of μ_1 and β_1 KEY parameters variation by the order $\Delta = 10^{-15}$ on the quality of decrypted bio- signals.

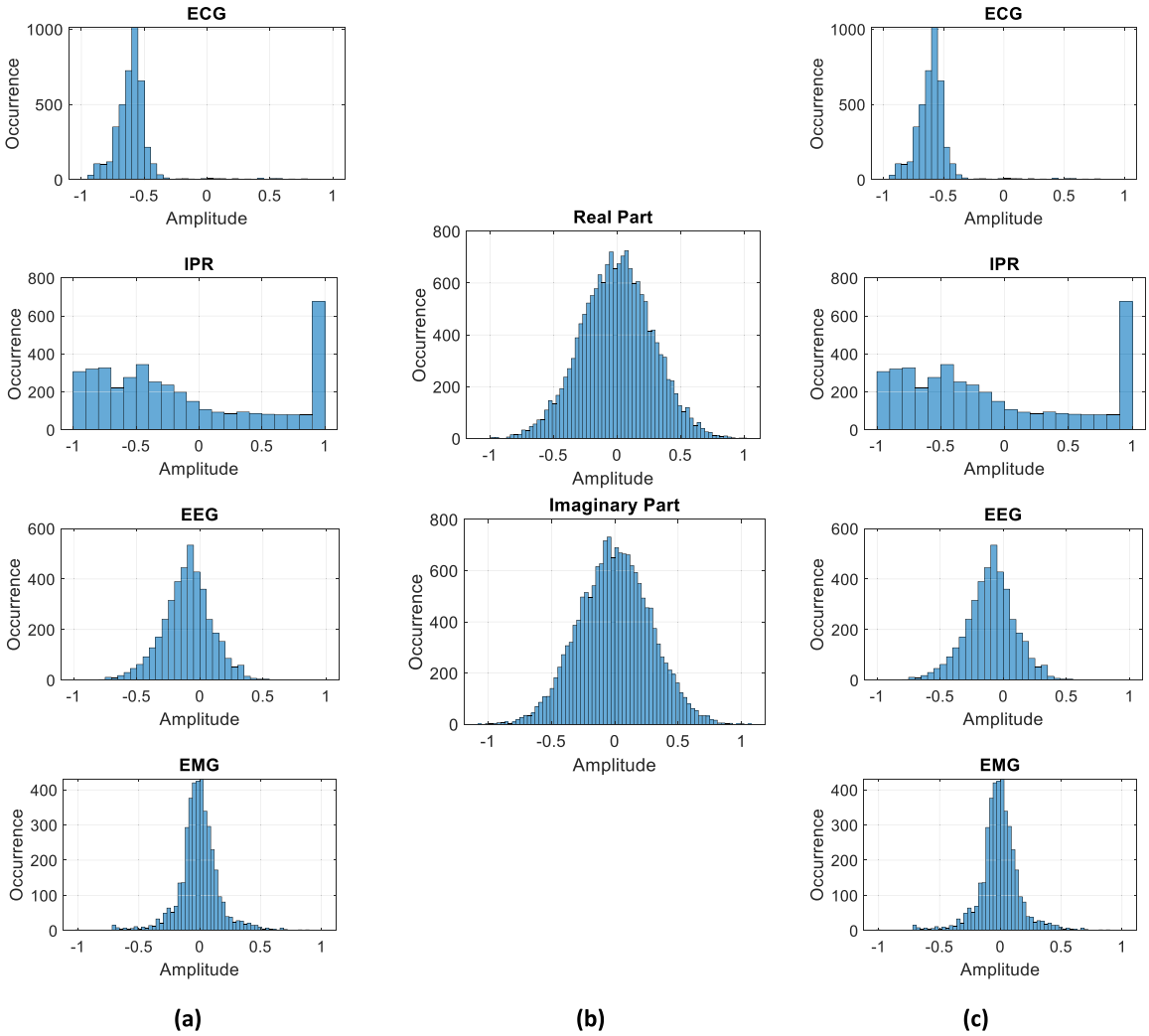


FIGURE 11. Histograms of the (a) original, (b) the encrypted and (c) the decrypted bio-signals.

attacker cannot predict the content of the original images via a visual analysis of the encrypted image.

Moreover, we can see the large difference between the histograms of the encrypted and decrypted CT images

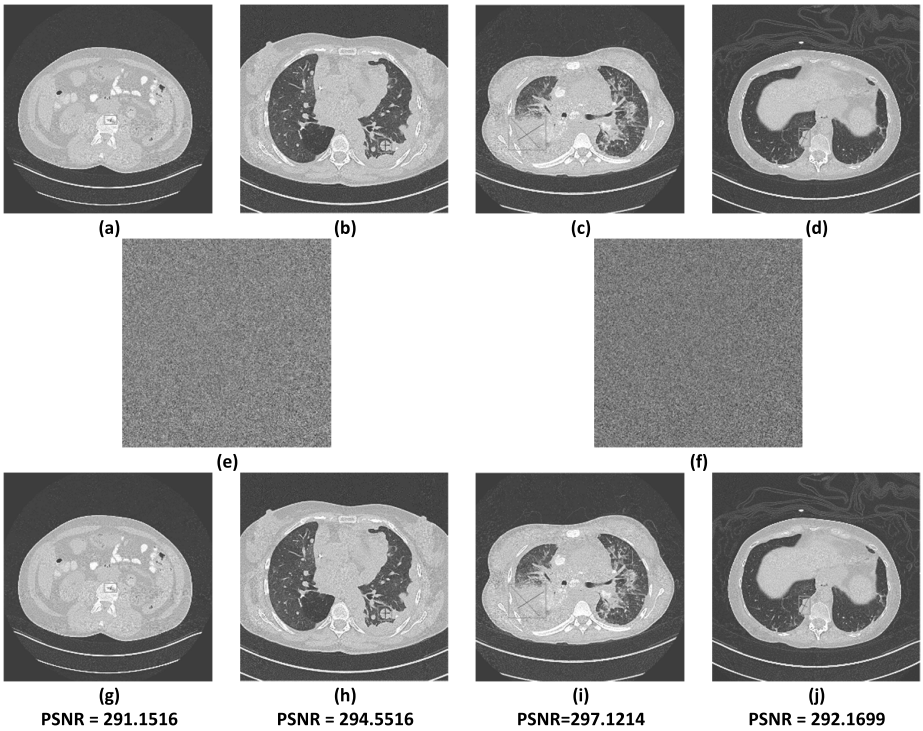


FIGURE 12. Original CT images. (e) - (f) Real and imaginary parts of the encrypted images, respectively. (g) - (j) Decrypted images with the PSNR values.

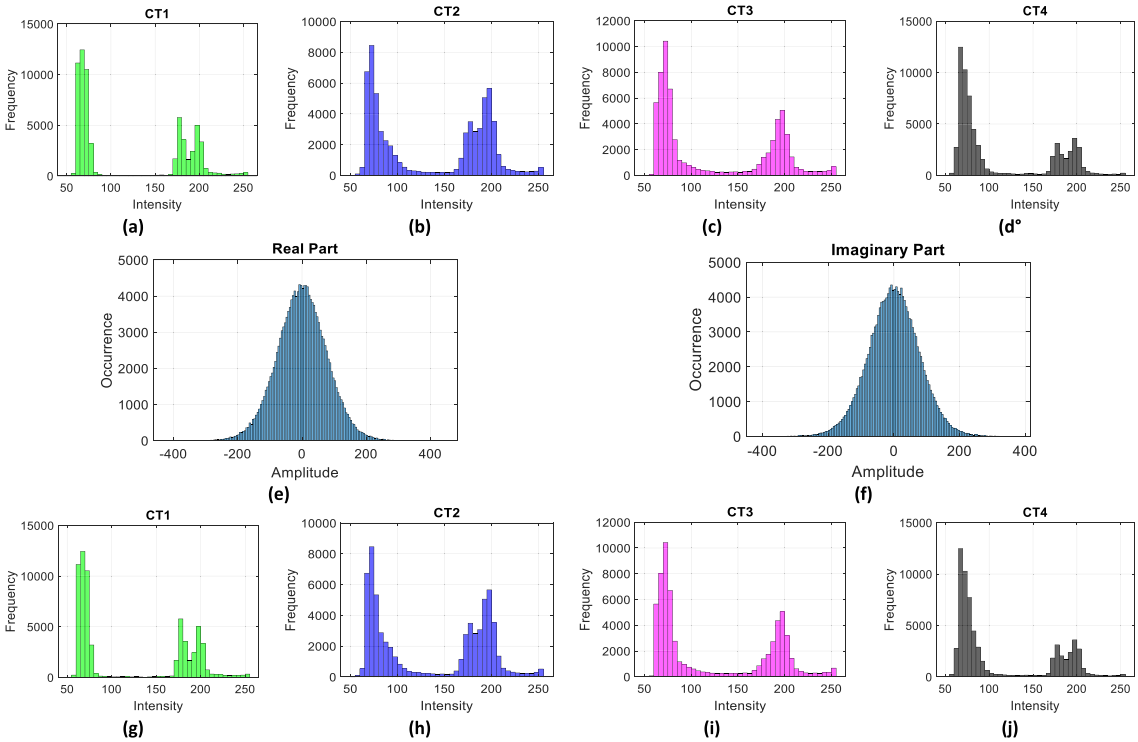


FIGURE 13. Histograms of (a)–(d) the original CT images, (e)–(f) the encrypted images, and (g)–(j) decrypted images.

(Figure 13). Therefore, the statistical analysis is not successful when it is applied to the proposed scheme.

The present analysis is not sufficient to corroborate the efficacy of the suggested scheme. For this, we perform statistical analysis in the following tests

G. ROBUSTNESS TO DIFFERENTIAL ATTACKS ANALYSIS

In attack analysis, the assailant employs two alike images with a minor change in one pixel of these images. Then, the attacker attempts to identify the resemblances between the encrypted images trying to identify the used security key in

the encryption scheme [56]. The number of pixels change rate (NPCR) and the unified average changed intensity (UACI) criteria are used to appraise the robustness of an encryption scheme against differential attacks. NPCR and UACI criteria can be defined as [57], [58] :

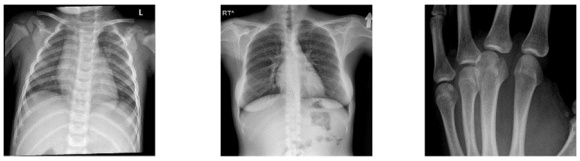
$$NPCR = \frac{\sum_{i,j} D_f(i,j)}{N \times M} \times 100$$
$$\text{with} D_f(i,j) = \begin{cases} 0 C(i,j) = C'(i,j) \\ 1 C(i,j) \neq C'(i,j) \end{cases} \quad (21)$$
$$UACI = \frac{\sum_{i,j} \left| C(i,j) - C'(i,j) \right|}{255 \times N \times M} \times 100 \quad (22)$$

where C and C' are the original image and the changed one of size $N \times M$, respectively.

It should be reported that a well-performing encryption scheme must meet the following criteria: NPCR $>$ 99.50% and UACI $>$ 33.33% for 8-bit grayscale images, as indicated in [59]. Furthermore, the ideal values of NPCR and UACI for 8-bit gray scale images are 99.6094% and 33.4635%, respectively [60].

As previously stated in this work, a variation of the order 10^{-15} in any value of QFrMMs and FrMPs map parameters $(\mu_1, \mu_2, \mu_3, \beta_1, \beta_2, \beta_3)$ leads to the failure in decrypting the input biomedical data. Therefore, we can rely on this property to resist differential attacks. Indeed, we can define a constant value (i.e. $\gamma = 2.6 \times 10^{-15}$) that is added to only one of the above KEY parameters (i.e. $\mu_1 = 0.34 + \gamma$) while the rest of the parameters remain unchanged. Then, at each execution of the encryption algorithm, the value of γ is incremented by a slight value (i.e. $\gamma = 2.6 \times 10^{-15} + 10^{-15}$). That is, each input image is encrypted/decrypted with its own security key. The use of this method guarantees the resistance of suggested system against differential attacks. That is, for the same input, the proposed algorithm generates two different outputs in two successive iterations. In this way, it is expected that the suggested encryption process can avoid differential attacks. To test the efficiently of this method against differential attacks, we use the test the images "X-ray1", "X-ray2" and "X-ray3" of size 1024 $\times$ 1024 (Figure 14). Then, we modify one pixel by 1 bit in the original images at arbitrary positions in these images. Next, the values of NPCR and UACI are deliberated, assessed and reported in Tables 4 and 5, respectively. The achieved results in these tables show that the suggested encryption method is able to resist differential attacks because the average values of NPCR and UACI criteria achieved by the proposed method are very close to the ideal values of these criteria as indicated in [60].

In the following test, we compare the UACI and NPCR values obtained by our scheme versus recent transform-based encryption schemes, which are presented in [33], [34], [61], and [62]. To perform the current test, we use 8-bit grayscale medical images of various size that are shown in Figure 15. Then, one pixel is changes by a 1-bit variation at the arbitrary positions in all the test images. Next, the values of NPCR and UACI are calculated and reported in Tables 6 and 7, respectively.



X-ray1 X-ray2 X-ray3

FIGURE 14. Original X-ray images of size 1024 × 1024 used in the test.

TABLE 4. NPCR values for 1-bit variation of various pixels.

Image	Position of the changed pixel			Average NPCR
	(2,3)	(500,300)	(1000,4)	
"X-ray1"	99.6115%	99.5912%	99.6015%	99.6014%
"X-ray2"	99.6050%	99.5989%	99.6068%	99.6036%
"X-ray3	99.5991%	99.6025%	99.6104%	99.6040%

TABLE 5. UACI values for 1-bit variation of various pixels.

Image	Position of the changed pixel			Average NPCR
	(2,3)	(500,300)	(1000,4)	
"X-ray1"	33.4578%	33.4615%	33.4625%	33.4606%
"X-ray2"	33.4644%	33.4589%	33.4619%	33.4617%
"X-ray3	33.4579%	33.4605%	33.4624%	33.4603%

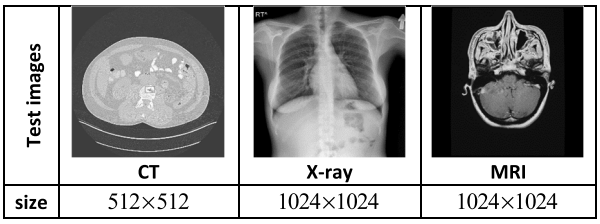


FIGURE 15. 8-bit grayscale test images of different sizes used in the comparative analysis of NPCR and UACI criteria.

The results of the current test show on the one hand that all the compared methods meet the NPCR and UACI criteria according to work presented in [59] since NPCR $>$ 99.50% and UACI $>$ 33.33%. On the other hand, we can notice that our method provides superior performance with respect to the compared schemes. This superiority can be explained by the fact that our scheme is based on FrMPs map and QFrMMs that demonstrated a good chaotic behavior. In contrast, the compared schemes are not very sensitive to the variation of their control and fractional order parameters.

H. NOISE ROBUSTNESS ANALYSIS

The encrypted image/signal can be affected by different noise types during communication or processing. Therefore, it is

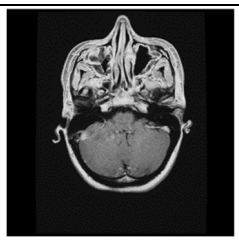
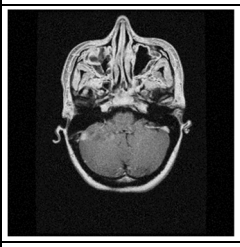
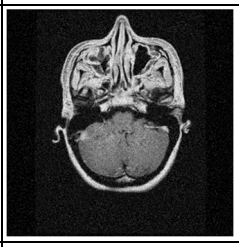
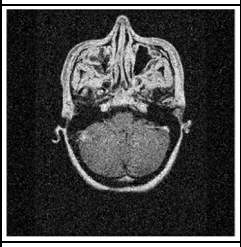
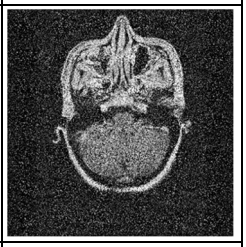
Original image				
Noise strength (k)	5	10	15	20
Decrypted image				
PSNR value	38.1478	29.2365	21.25	15.9852

FIGURE 16. Decrypted MRI image with PSNR values for various noise strengths (k).

TABLE 6. NPCR values for 1-bit variation of various pixels.

Test Image	Encryption scheme				
	Proposed	[61]	[62]	[34]	[33]
« CT »	**99.6021%**	99.5914%	99.5922%	99.6025%	99.6015%
« X-ray »	**99.5988%**	99.5814%	99.5871%	99.5930%	99.5900%
« MRI »	**99.6012%**	99.5863%	99.5912%	99.5908%	99.5882%

TABLE 7. UACI values for 1-bit variation of various pixels.

Test Image	Encryption scheme				
	Proposed	[61]	[62]	[34]	[33]
« CT »	**33.4609%**	33.4402%	33.4421%	33.4502%	33.4318%
« X-ray »	**33.4618%**	33.4303%	33.4598%	33.4585%	33.4414%
« MRI »	**33.4598%**	33.4415%	33.4502%	33.4569%	33.4412%

essential to test the toughness of our planned scheme against noise. Let's consider that I is the original encrypted image contaminated by a noise (G) as follows:

$$I_N = I + kG \tag{23}$$

where I_N is the noisy image, G represents a "Gaussian" noise with zero-mean and identity standard deviation, and k indicates the strength of the noise. To perform the present test, a MRI medical image of size 1024×1024 is taken from the database [63]. This image is encrypted by the proposed method and then affected by a noise a "Gaussian" noise (Eq. (23)) with different values of k. The original image and the decrypted ones are presented in Figure 16. From this figure, it appears that the quality of the decrypted images decreases proportionally to the increasing of k value. However, the visual content of the decrypted images seems identifiable. The archived results designate that the suggested scheme can counterattack noise contamination.

I. CROPPING ATTACKS ROBUSTNESS ANALYSIS

Congestion or failure of a communication channel can occur during the transmission of medical data (images, signals, videos, etc.), which can lead to partial loss (cropping) of the transmitted data. Therefore, it is requirement to assess the robustness of our scheme against cropping. For this purpose, we use an MRI image (Figure 17) of size 512×512, which is taken from the database [63]. This image is encrypted by the proposed method. Then, the real and imaginary parts of the encrypted image are cropped in the same area by various occlusion values. Finally, the cropped images are decrypted via our scheme. The results of the actual test are offered in Figure 17, which show that the quality of the decrypted image reduces (decrease PSNR) when the occlusion ratio increases. However, we can see that the visual content of the decrypted images is still presented, which specifies that the suggested system can withstand cropping attacks.

J. COMPARISON ANALYSIS WITH SIMILAR WORK

In the following test, we use DTI images shown in Figure 18 to calculate the correlation coefficient values according to the proposed method and other similar approaches presented in [33], [34], [61], and [62]. The test results are given in Table 5. From this table, we can observe that the coefficients are tending towards 1 for the original images, which shows the strong dependence between the adjacent pixels

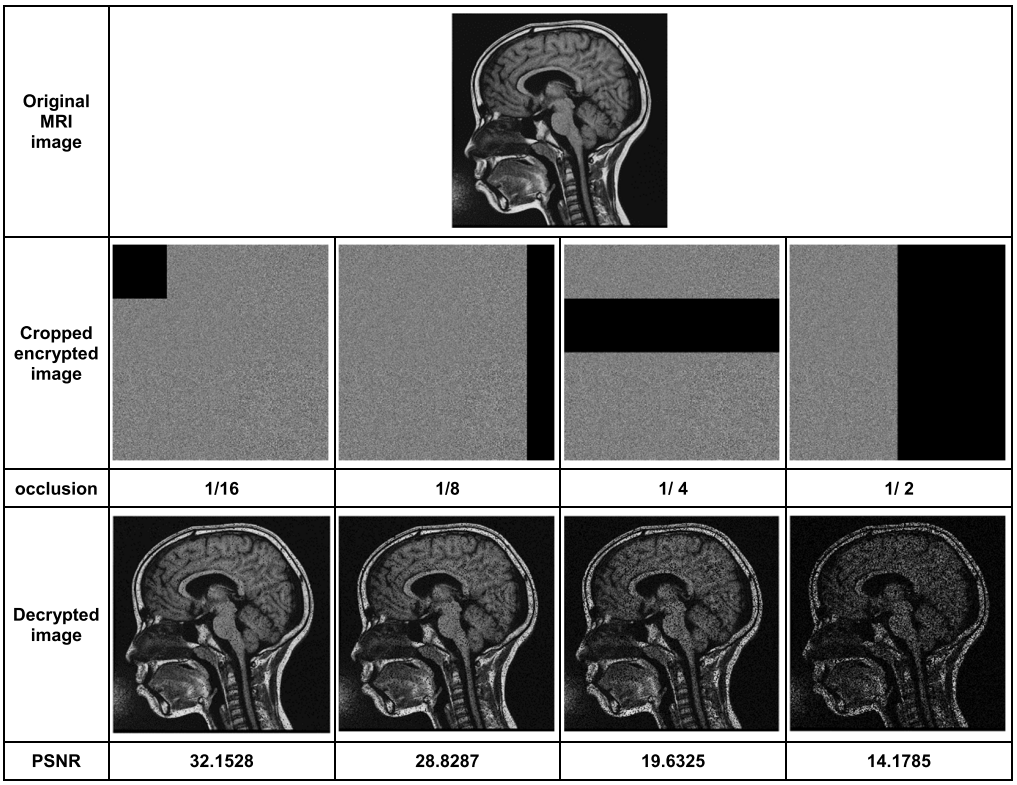


FIGURE 17. Decrypted MRI medical image from the attacked encrypted one for various occlusions.

TABLE 8. Correlation coefficient values obtained by the proposed method and other similar ones.

Method	*Image*	*Testing direction*			*Average Runtime in (sec)*
		Horizontal	Vertical	Diagonal	
	Original « DTI 1 »	0.9274	0.9829	0.9405	
Proposed		**-0.0023**	**0.0017**	**0.0034**	5.4654
Method [61]		-0.0156	-0.0149	0.0151	4.4622
Method [62]	Encrypted « DTI 1 »	0.0254	0.0256	-0.0234	4.3589
Method [34]		0.0186	-0.0198	-0.0179	**4.2195**
Method [33]		-0.0045	-0.0052	0.0036	5.0187
	Original « DTI 2 »	0.9204	0.9636	0.9700	--
Proposed method		**0.0028**	**-0.0035**	**-0.0036**	**5.4653**
Method [61]		-0.0174	0.0165	-0.0145	4.4621
Method [62]	Encrypted « DTI 2 »	0.0232	0.0240	-0.0228	4.3591
Method [34]		-0.0138	-0.0140	0.0159	**4.2194**
Method [33]		0.0048	0.0050	0.0046	5.0185
	Original « DTI 3 »	0.9400	0.9531	0.9620	--
Proposed		**0.0034**	**-0.0031**	**0.0030**	5.4650
Method [61]		0.0182	-0.0172	0.0184	4.4620
Method [62]	Encrypted « DTI 3 »	-0.0235	0.0228	-0.0219	4.3589
Method [34]		-0.0138	-0.0140	0.0152	**4.2192**
Method [33]		0.0052	-0.0049	-0.0041	5.0184

of these images. We also see that the correlation coefficients tend towards zero for the encrypted images by the different encryption methods with a clear superiority of the proposed method since it allows generating correlation

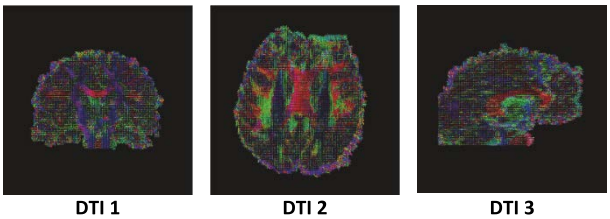


FIGURE 18. Original color DTI images of size 720 × 720.

coefficient values very close to zero. The results validate that the projected method delivers decent diffusion and confusion characteristics. It is prominent that the execution time of our suggested method is relatively higher than the compared methods (Table 8). This limitation remains an open problem to be addressed in future work.

VIII. CONCLUSION

In this paper, a new type of chaotic systems is introduced, namely FrMPs map. Then, a novel discrete orthogonal transform is called QFrMMs is also introduced. Next, a new encryption scheme applicable for biomedical data is proposed based on QFrMMs and FrMPs map. This scheme is designed to be adaptable to several biomedical multimedia (bio-signals, grayscale medical images, color medical images, multi-biomedical signals and multiple medical images). To support the validity of the of the proposed scheme, several analysis tests are performed in terms of the decrypted data quality, key sensitivity, correlation, robustness to statistical attacks, robustness to noise addition and cropping, timing, etc. The results clearly demonstrated the efficiently and good robustness of the suggested encryption method. Comparisons with similar methods are also provided to show the validity and of the proposed scheme for the secure transmission of various biomedical data over the Internet. In the future, the planned scheme will be developed to be applied in 3D medical image encryption.

CONFLICT OF INTEREST STATEMENT

The authors declare that there is no conflict of interest.

ACKNOWLEGMENT

This work was supported by the EIAS Data Science Lab, College of Computer and Information Sciences, Prince Sultan University, Riyadh, Saudi Arabia.

REFERENCES

[1] G. Zheng, R. Shankaran, W. Yang, C. Valli, L. Qiao, M. A. Orgun, and S. C. Mukhopadhyay, "A critical analysis of ECG-based key distribution for securing wearable and implantable medical devices," *IEEE Sensors J.*, vol. 19, no. 3, pp. 1186–1198, Feb. 2019, doi: 10.1109/JSEN.2018.2879929.

[2] A. Daoui, M. Yamni, H. Karmouni, M. Sayyouri, and H. Qjidaa, "Biomedical signals reconstruction and zero-watermarking using separable fractional order Charlier–Krawtchouk transformation and sine cosine algorithm," *Signal Process.*, vol. 180, Mar. 2021, Art. no. 107854, doi: 10.1016/j.sigpro.2020.107854.

[3] L. D. Singh and K. M. Singh, "Medical image encryption based on improved ElGamal encryption technique," *Optik*, vol. 147, pp. 88–102, Oct. 2017, doi: 10.1016/j.ijleo.2017.08.028.

[4] W. Cao, Y. Zhou, C. L. P. Chen, and L. Xia, "Medical image encryption using edge maps," *Signal Process.*, vol. 132, pp. 96–109, Mar. 2017, doi: 10.1016/j.sigpro.2016.10.003.

[5] Z. Hua, S. Yi, and Y. Zhou, "Medical image encryption using high-speed scrambling and pixel adaptive diffusion," *Signal Process.*, vol. 144, pp. 134–144, Mar. 2017, doi: 10.1016/j.sigpro.2017.10.004.

[6] A. Belazi, M. Talha, S. Kharbech, and W. Xiang, "Novel medical image encryption scheme based on chaos and DNA encoding," *IEEE Access*, vol. 7, pp. 36667–36681, 2019, doi: 10.1109/ACCESS.2019.2906292.

[7] J. Z. Liu, Y. D. Ma, S. L. Li, J. Lian, and X. Zhang, "A new simple chaotic system and its application in medical image encryption," *Multimedia Tools Appl.*, vol. 77, no. 17, pp. 22787–22808, Sep. 2018, doi: 10.1007/s11042-017-5534-8.

[8] X. Chen and C. J. Hu, "Adaptive medical image encryption algorithm based on multiple chaotic mapping," *Saudi J. Biol. Sci.*, vol. 24, no. 8, pp. 1821–1827, 2017, doi: 10.1016/j.sjbs.2017.11.023.

[9] A. Banik, Z. Shamsi, and D. S. Laiphrakpam, "An encryption scheme for securing multiple medical images," *J. Inf. Secur. Appl.*, vol. 49, Dec. 2019, Art. no. 102398, doi: 10.1016/j.jisa.2019.102398.

[10] R. Thanki and A. Kothari, "Multi-level security of medical images based on encryption and watermarking for telemedicine applications," *Multimedia Tools Appl.*, vol. 80, no. 3, pp. 4307–4325, Jan. 2021, doi: 10.1007/s11042-020-09941-z.

[11] V. S. Lima, F. Madeiro, and J. B. Lima, "Encryption of 3D medical images based on a novel multiparameter cosine number transform," *Comput. Biol. Med.*, vol. 121, Jun. 2020, Art. no. 103772, doi: 10.1016/j.compbiomed.2020.103772.

[12] J. Zhou, J. Li, and X. Di, "A novel lossless medical image encryption scheme based on game theory with optimized ROI parameters and hidden ROI position," *IEEE Access*, vol. 8, pp. 122210–122228, 2020, doi: 10.1109/ACCESS.2020.3007550.

[13] T. Y. Liu, K. J. Lin, and H. C. Wu, "ECG data encryption then compression using singular value decomposition," *IEEE J. Biomed. Health Inform.*, vol. 22, no. 3, pp. 707–713, May 2018.

[14] A. D. Algarni, N. F. Soliman, H. A. Abdallah, and F. E. A. El-Samie, "Encryption of ECG signals for telemedicine applications," *Multimedia Tools Appl.*, vol. 80, no. 7, pp. 10679–10703, Mar. 2021, doi: 10.1007/s11042-020-09369-5.

[15] M. E. Hameed, M. M. Ibrahim, N. A. Manap, and A. A. Mohammed, "A lossless compression and encryption mechanism for remote monitoring of ECG data using Huffman coding and CBC-AES," *Future Gener. Comput. Syst.*, vol. 111, pp. 829–840, Oct. 2020, doi: 10.1016/j.future.2019.10.010.

[16] S. Dhar, S. K. Mukhopadhyay, S. Pal, and M. Mitra, "An efficient data compression and encryption technique for PPG signal," *Meas., J. Int. Meas. Confederation*, vol. 116, pp. 533–542, Feb. 2018, doi: 10.1016/j.measurement.2017.11.006.

[17] G. Cho, *Smart Clothing: Technology and Applications*. Boca Raton, FL, USA: CRC Press, 2009.

[18] E. Y. Xie, C. Li, S. Yu, and J. Lü, "On the cryptanalysis of Fridrich's chaotic image encryption scheme," *Signal Process.*, vol. 132, pp. 150–154, Mar. 2017.

[19] M. Benedicks and L. Carleson, "The dynamics of the Henon map," *Ann. Math.*, vol. 133, no. 1, pp. 73–169, 1991.

[20] X. Han, J. Mou, T. Liu, and Y. Cao, "A new fractional-order 2D discrete chaotic map and its DSP implement," *Eur. Phys. J. Special Topics*, vol. 230, nos. 21–22, pp. 3913–3925, Dec. 2021, doi: 10.1140/epjs/s11734-021-00331-6.

[21] Z. Hua, Y. Chen, H. Bao, and Y. Zhou, "Two-dimensional parametric polynomial chaotic system," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 52, no. 7, pp. 4402–4414, Jul. 2022, doi: 10.1109/TSMC.2021.3096967.

[22] Z. Hua, Z. Zhu, Y. Chen, and Y. Li, "Color image encryption using orthogonal Latin squares and a new 2D chaotic system," *Nonlinear Dyn.*, vol. 104, no. 4, pp. 4505–4522, May 2021, doi: 10.1007/s11071-021-06472-6.

[23] H. Huang, S. Yang, and R. Ye, "Efficient symmetric image encryption by using a novel 2D chaotic system," *IET Image Process.*, vol. 14, no. 6, pp. 1157–1163, May 2020, doi: 10.1049/iet-ipr.2019.0551.

[24] C. Camacho-Bello and J. S. Rivera-Lopez, "Some computational aspects of Tchebichef moments for higher orders," *Pattern Recognit. Lett.*, vol. 112, pp. 332–339, Sep. 2018, doi: 10.1016/j.patrec.2018.08.020.

[25] A. Daoui, H. Karmouni, M. Sayyouri, and H. Qjidaa, "Fast and stable computation of higher-order Hahn polynomials and Hahn moment invariants for signal and image analysis," *Multimedia Tools Appl.*, vol. 80, nos. 21–23, pp. 32947–32973, Sep. 2021, doi: 10.1007/s11042-021-11206-2.

[26] A. Daoui, M. Sayyouri, and H. Qjidaa, "Efficient computation of high-order Meixner moments for large-size signals and images analysis," *Multimedia Tools Appl.*, vol. 80, no. 2, pp. 1641–1670, Jan. 2021, doi: 10.1007/s11042-020-09739-z.

[27] A. Daoui, H. Karmouni, M. Sayyouri, and H. Qjidaa, "Efficient methods for signal processing using Charlier moments and artificial bee colony algorithm," *Circuits, Syst., Signal Process.*, vol. 41, no. 1, pp. 166–195, Jan. 2022, doi: 10.1007/s00034-021-01764-z.

[28] A. Daoui, H. Karmouni, M. Yamni, M. Sayyouri, and H. Qjidaa, "On computational aspects of high-order dual Hahn moments," *Pattern Recognit.*, vol. 127, Jul. 2022, Art. no. 108596, doi: 10.1016/j.patcog.2022.108596.

[29] E. G. Karakasis, G. A. Papakostas, D. E. Koulouriotis, and V. D. Tourassis, "Generalized dual Hahn moment invariants," *Pattern Recognit.*, vol. 46, no. 7, pp. 1998–2014, Jul. 2013, doi: 10.1016/j.patcog.2013.01.008.

[30] A. Daoui, H. Karmouni, M. Sayyouri, and H. Qjidaa, "Stable analysis of large-size signals and images by Racah's discrete orthogonal moments," *J. Comput. Appl. Math.*, vol. 403, Mar. 2022, Art. no. 113830, doi: 10.1016/j.cam.2021.113830.

[31] X. Liu, G. Han, J. Wu, Z. Shao, G. Coatrieux, and H. Shu, "Fractional Krawtchouk transform with an application to image watermarking," *IEEE Trans. Signal Process.*, vol. 65, no. 7, pp. 1894–1908, Apr. 2017, doi: 10.1109/TSP.2017.2652383.

[32] M. Yamni, A. Daoui, O. El Ogri, H. Karmouni, M. Sayyouri, H. Qjidaa, and J. Flusser, "Fractional Charlier moments for image reconstruction and image watermarking," *Signal Process.*, vol. 171, Jun. 2020, Art. no. 107509, doi: 10.1016/j.sigpro.2020.107509.

[33] O. E. Ogri, H. Karmouni, M. Sayyouri, and H. Qjidaa, "A novel image encryption method based on fractional discrete Meixner moments," *Opt. Lasers Eng.*, vol. 137, Feb. 2021, Art. no. 106346.

[34] B. Xiao, J. Luo, X. Bi, W. Li, and B. Chen, "Fractional discrete Tchebyshev moments and their applications in image encryption and watermarking," *Inf. Sci.*, vol. 516, pp. 545–559, Apr. 2020.

[35] M. Yamni, H. Karmouni, M. Sayyouri, and H. Qjidaa, "Image watermarking using separable fractional moments of Charlier–Meixner," *J. Franklin Inst.*, vol. 358, no. 4, pp. 2535–2560, Mar. 2021, doi: 10.1016/j.jfranklin.2021.01.011.

[36] X. Liu, Y. Wu, H. Zhang, J. Wu, and L. Zhang, "Quaternion discrete fractional Krawtchouk transform and its application in color image encryption and watermarking," *Signal Process.*, vol. 189, Dec. 2021, Art. no. 108275, doi: 10.1016/j.sigpro.2021.108275.

[37] M. Yamni, H. Karmouni, M. Sayyouri, and H. Qjidaa, "Robust zero-watermarking scheme based on novel quaternion radial fractional Charlier moments," *Multimedia Tools Appl.*, vol. 80, pp. 21679–21708, Mar. 2021.

[38] M. Yamni, H. Karmouni, M. Sayyouri, and H. Qjidaa, "Quaternion Cartesian fractional Hahn moments for color image analysis," *Multimedia Tools Appl.*, vol. 81, no. 1, pp. 737–758, Jan. 2022, doi: 10.1007/s11042-021-11432-8.

[39] 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, Nov. 2019, doi: 10.1007/s11517-019-02037-3.

[40] H. Zhu, M. Liu, H. Shu, H. Zhang, and L. Luo, "General form for obtaining discrete orthogonal moments," *IET Image Process.*, vol. 4, no. 5, pp. 335–352, Oct. 2010, doi: 10.1049/iet-ipr.2009.0195.

[41] T. Jahid, A. Hmimid, H. Karmouni, M. Sayyouri, H. Qjidaa, and A. Rezzouk, "Image analysis by Meixner moments and a digital filter," *Multimedia Tools Appl.*, vol. 77, no. 15, pp. 19811–19831, Aug. 2018.

[42] W. R. Hamilton, *Elements of Quaternions*. Harlow, U.K.: Longmans, Green, & Company, 1866.

[43] S. J. Sangwine and T. A. Ell, "Hypercomplex Fourier transforms of color images," in *Proc. Int. Conf. Image Process.*, vol. 1, 2001, pp. 137–140.

[44] M. Pooyan, A. Taheri, M. Moazami-Goudarzi, and I. Saboori, "Wavelet compression of ECG signals using SPIHT algorithm," *Int. J. Signal Process.*, vol. 1, no. 3, p. 4, 2004.

[45] M. Hashemi, "Enlarging smaller images before inputting into convolutional neural network: Zero-padding vs. Interpolation," *J. Big Data*, vol. 6, no. 1, pp. 1–13, Dec. 2019.

[46] S. Mirjalili, "SCA: A sine cosine algorithm for solving optimization problems," *Knowl.-Based Syst.*, vol. 96, pp. 120–133, Mar. 2016.

[47] *Shift Array Circularly—MATLAB Circshift*. Accessed: Mar. 4, 2022. [Online]. Available: https://www.mathworks.com/help/MATLAB/ref/circshift.html

[48] M. Liyanage, A. Braeken, A. D. Jurcut, M. Ylianttila, and A. Gurtov, "Secure communication channel architecture for software defined mobile networks," *Comput. Netw.*, vol. 114, pp. 32–50, Feb. 2017, doi: 10.1016/j.comnet.2017.01.007.

[49] *PhysioBank ATM*. Accessed: Jul. 13, 2021. [Online]. Available: https://archive.physionet.org/cgi-bin/atm/ATM

[50] G. Alvarez and L. I. Shujun, "Some basic cryptographic requirements for chaos-based cryptosystems," *Int. J. Bifurcation Chaos*, vol. 16, no. 8, pp. 2129–2151, Aug. 2006, doi: 10.1142/S0218127406015970.

[51] C.-H. Lin, J.-X. Wu, P.-Y. Chen, C.-M. Li, N.-S. Pai, and C.-L. Kuo, "Symmetric cryptography with a chaotic map and a multilayer machine learning network for physiological signal infosecurity: Case study in electrocardiogram," *IEEE Access*, vol. 9, pp. 26451–26467, 2021, doi: 10.1109/ACCESS.2021.3057586.

[52] P. Mathivanan, A. B. Ganesh, and R. Venkatesan, "QR code–based ECG signal encryption/decryption algorithm," *Cryptologia*, vol. 43, no. 3, pp. 233–253, May 2019.

[53] C.-F. Lin, S.-H. Shih, and J.-D. Zhu, "Chaos based encryption system for encrypting electroencephalogram signals," *J. Med. Syst.*, vol. 38, no. 5, p. 49, May 2014, doi: 10.1007/s10916-014-0049-6.

[54] *3.0T GE Discovery 750W MRI Scanner Images | Magnetic Resonance Research Facility*. Accessed: Mar. 11, 2022. [Online]. Available: https://medicine.uiowa.edu/mri/30t-ge-discovery-750w-mri-scanner-images

[55] National Institutes of Health (NIH). (Jul. 20, 2018). *NIH Clinical Center Releases Dataset of 32,000 CT Images*. Accessed: Aug. 19, 2021. [Online]. Available: https://www.nih.gov/news-events/news-releases/nih-clinical-center-releases-dataset-32000-ct-images

[56] A. Belazi, A. A. A. El-Latif, and S. Belghith, "A novel image encryption scheme based on substitution-permutation network and chaos," *Signal Process.*, vol. 128, pp. 155–170, Nov. 2016, doi: 10.1016/j.sigpro.2016.03.021.

[57] X. Liao, S. Lai, and Q. Zhou, "A novel image encryption algorithm based on self-adaptive wave transmission," *Signal Process.*, vol. 90, no. 9, pp. 2714–2722, Sep. 2010, doi: 10.1016/j.sigpro.2010.03.022.

[58] Y. Wu, "NPCR and UACI randomness tests for image encryption," *Cyber J., J. Sel. Areas Telecommun.*, vol. 1, pp. 31–38, Apr. 2011.

[59] Y. Wang, K.-W. Wong, X. Liao, and G. Chen, "A new chaos-based fast image encryption algorithm," *Appl. Soft Comput.*, vol. 11, no. 1, pp. 514–522, 2011.

[60] M.-M. Wang, N.-R. Zhou, L. Li, and M.-T. Xu, "A novel image encryption scheme based on chaotic apertured fractional Mellin transform and its filter bank," *Expert Syst. Appl.*, vol. 207, Nov. 2022, Art. no. 118067, doi: 10.1016/j.eswa.2022.118067.

[61] S.-S. Yu, N.-R. Zhou, L.-H. Gong, and Z. Nie, "Optical image encryption algorithm based on phase-truncated short-time fractional Fourier transform and hyper-chaotic system," *Opt. Lasers Eng.*, vol. 124, Jan. 2020, Art. no. 105816, doi: 10.1016/j.optlaseng.2019.105816.

[62] J. Wu, F. Guo, P. Zeng, and N. Zhou, "Image encryption based on a reality-preserving fractional discrete cosine transform and a chaos-based generating sequence," *J. Mod. Opt.*, vol. 60, no. 20, pp. 1760–1771, Nov. 2013, doi: 10.1080/09500340.2013.858189.

[63] Radiopaedia. *The Wiki-Based Collaborative Radiology Resource*. Accessed: Jul. 29, 2021. [Online]. Available: https://radiopaedia.org/

ACHRAF DAOUI was born in Taounate, Morocco, in 1991. He received the B.Eng. degree in electrical engineering and the M.S. degree in engineering science from the Faculty of Science, Sidi Mohammed Ben Abdellah University, Fez, Morocco, in 2013 and 2018, respectively. He is currently pursuing the Ph.D. degree with the Laboratory of Engineering, Systems and Applications, National School of Applied Sciences, Sidi Mohamed Ben Abdellah University. His research interests include signal processing, image processing, and pattern recognition.

MOHAMED YAMNI was born in Fez, Morocco, in 1993. He received the B.Eng. degree in electrical engineering and the M.S. degree in engineering science from the Faculty of Science, Sidi Mohammed Ben Abdellah University, Fez, in 2014 and 2018, respectively. He is currently pursuing the Ph.D. degree with the Department of Physics, Sidi Mohammed Ben Abdellah University. His research interests include image watermarking, signal processing, and pattern classification.

HICHAM KARMOUNI was born in Fez, Morocco, in 1992. He received the M.S. degree in signals, systems and informatics and the Ph.D. degree in electrical engineering from the Faculty of Science, Sidi Mohammed Ben Abdellah University, Fez, in 2013 and 2019, respectively. He currently works as a Research Scientist with the Laboratory of Electronics, Signals, Systems and Computers (LESSI), Faculty of Science, Sidi Mohammed Ben Abdellah University. His current research interests include image processing, pattern recognition, and machine intelligence.

MHAMED SAYYOURI received the M.S. degree in engineering science and the Ph.D. degree in signals, systems and informatics from the Faculty of Science, Sidi Mohammed Ben Abdellah University, Fez, Morocco, in 2002 and 2014, respectively. Since 2016, he has been working as a Research Scientist at the Department of Industrial Engineering, National School of Applied Sciences, Sidi Mohamed Ben Abdellah University. He has been a Professor with the Department of Industrial Engineering. His research interests include image processing, pattern classification, signals and systems.

HASSAN QJIDAA received the M.S. and Ph.D. degrees in electrical engineering from the Nuclear Physics Institute of Lyon, France, in 1984 and 1987, respectively. Since 1987, he has been working as a Research Scientist at the Faculty of Science, Sidi Mohammed Ben Abdellah University, Fez, Morocco. He has been a Professor with the Department of Physics. He is currently the Director of the Information Analysis and Micro-System Teams (IAMS), and the Vice Director of the Electronic Signal and Systems Laboratory (LESSI). His current research interests include image processing, pattern recognition, data analysis, and machine intelligence.

MUSHEER AHMAD received the B.Tech. and M.Tech. degrees from the Department of Computer Engineering, Aligarh Muslim University, India, in 2004 and 2008, respectively, and the Ph.D. degree in chaos-based cryptography from the Department of Computer Engineering, Jamia Millia Islamia, New Delhi, India. From 2007 to 2010, he worked with the Department of Computer Engineering, Aligarh Muslim University. Since 2011, he has been working as an Assistant Professor with the Department of Computer Engineering, Jamia Millia Islamia. He has published over 90 research papers in internationally reputed refereed journals and conference proceedings of the IEEE/Springer/Elsevier. He has more than 2200 citations of his research works with an H-index of 29, i-10 index of 60, and cumulative impact factor of more than 200. Recently, he is listed among World's Top 2% Scientists in a study conducted by Elsevier and Stanford University and report published by Elsevier. His research interests include multimedia security, chaos-based cryptography, cryptanalysis, machine learning for security, image processing, and optimization techniques. He has served as a reviewer and a technical program committee member of many international conferences. He has also served as a Referee of some renowned journals, such as *Information Sciences*, *Signal Processing*, *Journal of Information Security and Applications*, IEEE Journal on Selected Areas in Communications, IEEE Transactions on Cybernetics, IEEE Transactions on Circuits and Systems for Video Technology, IEEE Transactions on Industrial Informatics, IEEE Transactions on Pattern Analysis and Machine Intelligence, IEEE Transactions on Neural Networks and Learning Systems, IEEE Transactions on Intelligent Transportation Systems, IEEE Transactions on Network Science and Engineering, IEEE Transactions on Nanobioscience, IEEE Transactions on Circuits and Systems—I: Regular Papers, IEEE Transactions on Big Data, IEEE Transactions on Reliability, IEEE Internet of Things Journal, IEEE Multimedia, IEEE Access, *Expert Systems with Applications*, *Wireless Personal Communications*, *Neural Computing and Applications*, *International Journal of Bifurcation and Chaos*, *Chaos Solitons & Fractals*, *Physica A*, *Signal Processing: Image Communication*, *Neurocomputing*, *IET Information Security*, *IET Image Processing*, *Security and Communication Networks*, *Optik*, *Optics and Laser Technology*, *Complexity*, *Computers in Biology and Medicine*, *Computational and Applied Mathematics*, and *Concurrency and Computation*.

AHMED A. ABD EL-LATIF (Senior Member, IEEE) received the B.Sc. degree (Hons.) in mathematics and computer science and the M.Sc. degree in computer science from Menoufia University, Egypt, in 2005 and 2010, respectively, and the Ph.D. degree in computer science and technology from the Harbin Institute of Technology, Harbin, China, in 2013. He is currently a Research Professor at the EIAS Data Science Laboratory, College of Computer and Information Sciences, Prince Sultan University, Riyadh, Saudi Arabia. He is the author or coauthor of more than 200 papers, including refereed IEEE/ACM/Springer/Elsevier journals, conference papers, books, and book chapters. His research interests include multimedia content encryption, secure wireless communication, the IoT, applied cryptanalysis, perceptual cryptography, secret media sharing, information hiding, biometrics, forensic analysis in digital images, and quantum information processing. He is a member of ACM. He is a fellow of the Academy of Scientific Research and Technology, Egypt. He received many awards, including the State Encouragement Award in Engineering Sciences in 2016, Arab Republic of Egypt; the Best Ph.D. Student Award from the Harbin Institute of Technology in 2013; and the Young Scientific Award, Menoufia University, Egypt, in 2014. He is an editor/guest editor in several reputed SCI journals. He had many books, more than ten books, in several publishers for process in Springer, IET, CRC press, IGI-Global, Wiley, and IEEE.