Frontiers of Information Technology & Electronic Engineering
www.jzus.zju.edu.cn; engineering.cae.cn; www.springerlink.com
ISSN 2095-9184 (print); ISSN 2095-9230 (online)
E-mail: jzus@zju.edu.cn

A novel hybrid cryptosystem based on DQFrFT watermarking and 3D-CLM encryption for healthcare services*

Fatma KHALLAF[1,2], Walid EL-SHAFAI[‡1,3], El-Sayed M. EL-RABAIE[1], Naglaa F. SOLIMAN[4], Fathi E. Abd EL-SAMIE[4]

[1]*Department of Electronics and Electrical Communications Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt*

[2]*Department of Electrical Engineering, Faculty of Engineering, Ahram Canadian University, 6th October City, Giza 12451, Egypt*

[3]*Security Engineering Lab, Computer Science Department, Prince Sultan University, Riyadh 11586, Saudi Arabia*

[4]*Department of Information Technology, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, Riyadh 11671, Saudi Arabia*

E-mail: fatma.mohammed333@gmail.com; eng.waled.elshafai@gmail.com; elsayedelrabaie@gmail.com; nfsoliman@pnu.edu.sa; fathi_sayed@yahoo.com

Received Sept. 2, 2022; Revision accepted Dec. 20, 2022; Crosschecked May 24, 2023

Abstract: Quaternion algebra has been used to apply the fractional Fourier transform (FrFT) to color images in a comprehensive approach. However, the discrete fractional random transform (DFRNT) with adequate basic randomness remains to be examined. This paper presents a novel multistage privacy system for color medical images based on discrete quaternion fractional Fourier transform (DQFrFT) watermarking and three-dimensional chaotic logistic map (3D-CLM) encryption. First, we describe quaternion DFRNT (QDFRNT), which generalizes DFRNT to handle quaternion signals effectively, and then use QDFRNT to perform color medical image adaptive watermarking. To efficiently evaluate QDFRNT, this study derives the relationship between the QDFRNT of a quaternion signal and the four components of the DFRNT signal. Moreover, it uses the human vision system's (HVS) masking qualities of edge, texture, and color tone immediately from the color host image to adaptively modify the watermark strength for each block in the color medical image using the QDFRNT-based adaptive watermarking and support vector machine (SVM) techniques. The limitations of watermark embedding are also explained to conserve watermarking energy. Second, 3D-CLM encryption is employed to improve the system's security and efficiency, allowing it to be used as a multistage privacy system. The proposed security system is effective against many types of channel noise attacks, according to simulation results.

Key words: Color medical image; Quaternion; Adaptive watermarking; Encryption; Fractional transform; Three-dimensional chaotic logistic map (3D-CLM)

https://doi.org/10.1631/FITEE.2200372 **CLC number:** TP391

1 Introduction

As the field of healthcare enters a new generation, biomedical data play a crucial role. However, when saved and transferred on broadcast networks, medical images are easily accessed and altered by individuals who lack proper authorization. Before being shared online, medical images must be encrypted if they include any especially sensitive information.

In the last two decades, color images have been handled extensively using the quaternion by encoding their three components into the quaternion representation (QR) components (Faragallah et al., 2020a). The fundamental benefit of QR is that a color image can be handled as a vector field in its entirety. Because of

‡ Corresponding author

* Project supported by the Princess Nourah bint Abdulrahman University Researchers Supporting Project (No. PNURSP2023R66)

ORCID: Fatma KHALLAF, https://orcid.org/0009-0008-1917-8251; Walid EL-SHAFAI, https://orcid.org/0000-0001-7509-2120

color images' low redundant data and straightforward inverse transforms, orthogonal transforms are a useful technique in signal processing. As a result, by applying quaternion algebra, several conventional orthogonal transforms for real or complex signals have been effectively adapted to quaternion signals. Wavelet transform (WT), polar harmonic transform (PHT), Fourier transform (FT), Hadamard transform (HT), discrete cosine transform (DCT), and orthogonal moments are examples of conventional orthogonal transforms (Faragallah et al., 2019, 2020b, 2021; Alarifi et al., 2020a; Huang and Zhou, 2022).

In recent decades, many fractional orthogonal transforms (FOTs) have been developed, such as discrete fractional random transform (DFRNT), fractional Fourier transform (FrFT), fractional sine transform (FrST), fractional cosine transform (FrCT), S transform (ST), fractional wavelet transform (FrWT), fractional Mellin transform (FrMT), and fractional Hartley transform (FrHT). These FOTs are a generalization of their equivalent classical orthogonal transforms in mathematics and can be seen as a signal revolution in the time–frequency plane for further applications. However, until now, only the fractional quaternion Fourier transform (FrQFT) has been used for quaternion signal processing. It has excellent mathematical characteristics retained from FrFT (Al-Afandy et al., 2018; Chen et al., 2018; El-Shafai et al., 2018a, 2018b, 2019; Duan et al., 2022). The inherent randomness of DFRNT enables watermarking and encryption to be easier and more efficient for image applications. As a result, this paper introduces quaternion DFRNT (QDFRNT), which extends DFRNT to successfully analyze quaternion signals before using QDFRNT for color image adaptive watermarking (Alarifi et al., 2020b; Elashry et al., 2020; Faragallah et al., 2020c; El-Shafai et al., 2021a; Salah et al., 2021; Soliman et al., 2021; Urynbassarova et al., 2022).

The use of chaotic cryptography for image encryption has been now widely recognized, and in various engineering fields researchers are very interested in the properties of chaos. The concept of using chaos in cryptography is attributed to Shannon's research (El-Shafai, 2015). Cryptography has used the chaotic logistic map (CLM) in a wide range of applications. The simplicity of generation, reliance on the initial conditions, and noise-like behaviour are only a few of the advantageous characteristics of chaotic logistic sequences. Because chaotic sequences have the appropriate features, applying chaos to cryptography has greatly improved data security.

Recently, Abdelwahab et al. (2020) presented a three-dimensional chaotic logistic map (3D-CLM) with deoxyribonucleic acid (DNA) encoding, which is used to confuse and diffuse image pixels. The initialization of 3D-CLM uses three symmetric keys, which strengthens the encryption technique. The 32-bit ASCII key, the Chebyshev chaotic key, and the prime key are the three symmetric keys that are employed. Algarni et al. (2020) described a system for chaotic encryption based on 3D-CLM with both a secure hash algorithm-3 (SHA-3) and an electrocardiogram (ECG) signal. El-Shafai et al. (2017) introduced the concept of reversible data hiding in 3D mesh models and CLM. They used the 3D mesh model to choose the values that would be used for embedding. This blind steganography technique is resistant to attacks such as translation, scaling, and rotation. Faragallah et al. (2022) proposed an image encryption method based on 3D-CLM. First, 3D-CLM is altered to produce a key stream. Second, 3D-CLM generates the chaos-based key stream, which has randomization qualities. El-Shafai et al. (2018c) suggested a simple method with a high level of output complexity and a quick processing. For image encryption, three nonlinear CLMs are used. The three different sequences are extracted and used for permutations of pixel columns and rows with the XOR operator.

Security has garnered considerable attention lately, especially with the rapid developments in information and communication systems. Watermarking has been in use for several years. Furthermore, due to recent improvements in multimedia data processing, developments in digital signal processing, and the accessibility of high-speed computational systems, the study of digital watermarking and its diverse applications has expanded exponentially over the last 30 years. The four kinds of watermarking techniques are text, image, audio, and video watermarking, depending on the type of data to be watermarked. The main applications of digital watermarking are fingerprinting, broadcast monitoring, copyright protection, digital signatures, medical applications, indexing, source tracking, and secure e-voting systems (El-Meadawy et al., 2021; El-Shafai et al., 2021b; Siam et al., 2021; Almomani et al., 2022a, 2022b; Alqahtani et al., 2022).

Since the development of inexpensive digital cameras, color images have become more prevalent. Compared to gray image watermarking, color image watermarking provides the following two significant advantages: (1) a color image can conceal more data; (2) a color image can achieve higher fidelity because color perception is influenced by both luminance and chrominance. As a result, we must investigate the color image watermarking algorithm. In terms of signal processing, watermark embedding can be considered embedding a poor signal into a strong background signal. Assuming that the inserted signal is more fragile than a simple recognizable distinction, it is challenging for the human vision system (HVS) to detect the watermark. Along these lines, the watermark strength should be adaptively determined by HVS to adjust the imperceptibility and vigor. Most current versatile watermarking strategies for a wide range of color images consider the HVS covering properties on the turning gray adaptation of a wide range of color host images.

There have been several papers thus far that deal with FrFT. Alarifi et al. (2020a) presented the quaternion discrete fractional Hartley transform (QDFrHT) as an expansion of the discrete FrHT to the quaternion transform domain, which was subsequently applied to multi-image encryption. Using DCT and zigzag operations, the plain images were compressed into four fusion images, which were then represented as quaternion algebra. Faragallah et al. (2020c) analyzed the properties of the polar quaternion discrete Fourier transform (PQDFT) and proposed lossless copyright protection of color images. Elashry et al. (2020) investigated a color image encryption algorithm based on the discrete trinion FT and random multiresolution singular value decomposition (SVD). A trinion matrix created from a color image was then applied to a blockwise discrete trinion FT. Then, a mapping from the trinion number domain to the real number domain was constructed to aid random multiresolution SVD.

In the adaptive process, many current techniques do not effectively use color information. As a result, this paper recovers the texture, edge, and color tone masking qualities immediately from color host images to adaptively choose the watermark strength, and then uses the adaptive strength to insert the watermark into the DQFrFT domain. After that, 3D-CLM is used to apply an encryption technique. The extraction of a binary watermark can be seen as a classification issue. Support vector machine (SVM) has been widely used in image watermarking because it has excellent learning capabilities and generalization performance even though the watermark image is heavily damaged. As a result, DQFrFT, SVM, and 3D-CLM are combined in this paper to create color image adaptive watermarking and encryption.

Recently, securing color medical images in healthcare applications has become a challenging issue, which motivated us to design a novel hybrid cryptosystem based on DQFrFT watermarking and 3D-CLM encryption for healthcare services. The proposed technique is based on a combination of high-efficiency DQFrFT watermarking and the implementation of an effective medical image cryptography system based on higher-order chaos functions.

The following are the main contributions of this paper:

1. introducing a comprehensive survey of recent related studies,

2. developing DQFrFT, which expands DFRNT to handle quaternion signals effectively and holistically, especially for color image signals,

3. determining the connection between a quaternion signal's DQFrFT and DFRNT,

4. proposing a blind adaptive watermarking approach for color images based on SVM and QDFRNT,

5. developing the 3D-CLM encryption technique,

6. evaluating the effectiveness of the suggested approach using multiple security criteria on additional color medical images with varying attributes,

7. investigating the impact of communication noise and testing the proposed computational processing framework,

8. examining the suggested framework's resilience against additional attacks, and

9. conducting a comprehensive comparative analysis with recent works to prove the proposed solution's superiority.

2 Related works

2.1 Quaternion number and QR of color images

A complex number is a special case of a quaternion. A quaternion has three imaginary parts and

one real part that are determined by (Faragallah et al., 2020b)

$$\boldsymbol{q}=a+b\boldsymbol{i}+c\boldsymbol{j}+d\boldsymbol{k}, \tag{1}$$

where a, b, c, and $d\in\mathbb{R}$, and $\boldsymbol{i}$, $\boldsymbol{j}$, and $\boldsymbol{k}$ are three imaginary components that follow the principles below.

If $f(x, y)$ is an RGB image function with QR, each pixel can be described as a pure quaternion as follows (Pandey et al., 2014):

$$f(x,y)=f_{\mathrm{R}}(x,y)\boldsymbol{i}+f_{\mathrm{G}}(x,y)\boldsymbol{j}+f_{\mathrm{B}}(x,y)\boldsymbol{k}, \tag{2}$$

where $f_{\mathrm{R}}(x, y)$, $f_{\mathrm{G}}(x, y)$, and $f_{\mathrm{B}}(x, y)$ are the red, green, and blue channels of the pixel, respectively.

2.2 Discrete fractional random transform

Using the concept of discrete fractional Fourier transform (DFrFT), Faragallah et al. (2020c) proposed DFRNT for discrete signals without giving its continuous equivalent DFrFT. The α^{th}-order one-dimensional (1D) DFRNT of a 1D signal $\boldsymbol{x}$ with size $N\times1$ is given by

$$\boldsymbol{X}=\boldsymbol{R}^{\alpha}\boldsymbol{x}, \tag{3}$$

where $\boldsymbol{R}^{\alpha}$ is the kernel transform matrix.

2.3 QDFRNT fundamentals

2.3.1 QDFRNT definition

According to the definition of 1D conventional DFRNT in Eq. (3), a 1D quaternion signal of size $N\times1$ is given as $\boldsymbol{x}_{\mathrm{q}}=\boldsymbol{x}_{\mathrm{r}}+\boldsymbol{x}_i\boldsymbol{i}+\boldsymbol{x}_j\boldsymbol{j}+\boldsymbol{x}_k\boldsymbol{k}$, and its left-hand-side (LHS) of 1D QDFRNT is written as (Jin et al., 2013)

$$\boldsymbol{X}_{\mathrm{q}}=\boldsymbol{R}^{\alpha,\mu}\boldsymbol{x}_{\mathrm{q}}. \tag{4}$$

Two-dimensional (2D) quaternion signal $\boldsymbol{y}_{\mathrm{q}}$ of 2D QDFRNT and the inverse QDFRNT (IQDFRNT) are described by (Chen et al., 2018)

$$\boldsymbol{Y}_{\mathrm{q}}=\boldsymbol{R}^{\alpha,\mu}\boldsymbol{y}_{\mathrm{q}}(\boldsymbol{R}^{\alpha,\mu})^{\mathrm{T}}, \tag{5}$$

$$\boldsymbol{y}_{\mathrm{q}}=\boldsymbol{R}^{-\alpha,\mu}\boldsymbol{Y}_{\mathrm{q}}(\boldsymbol{R}^{-\alpha,\mu})^{\mathrm{T}}. \tag{6}$$

2.3.2 QDFRNT vs. DFRNT for the quaternion signal

1. One-dimensional formulation

The LHS 1D QDFRNT is given as (Chen et al., 2018)

$$\begin{aligned}
&\mathrm{LQDFRNT1D}^{\alpha,\mu}\left(\boldsymbol{x}_{\mathrm{q}}\right)\\
&=\boldsymbol{R}^{\alpha,\mu}\boldsymbol{x}_{\mathrm{r}}+\boldsymbol{R}^{\alpha,\mu}\boldsymbol{x}_i\boldsymbol{i}+\boldsymbol{R}^{\alpha,\mu}\boldsymbol{x}_j\boldsymbol{j}+\boldsymbol{R}^{\alpha,\mu}\boldsymbol{x}_k\boldsymbol{k}\\
&=\left(\mathrm{Re}\left(\boldsymbol{R}^{\alpha}\boldsymbol{x}_{\mathrm{r}}\right)+\mu\mathrm{Im}\left(\boldsymbol{R}^{\alpha}\boldsymbol{x}_{\mathrm{r}}\right)\right)\\
&+\left(\mathrm{Re}\left(\boldsymbol{R}^{\alpha}\boldsymbol{x}_i\right)+\mu\mathrm{Im}\left(\boldsymbol{R}^{\alpha}\boldsymbol{x}_i\right)\right)\boldsymbol{i}\\
&+\left(\mathrm{Re}\left(\boldsymbol{R}^{\alpha}\boldsymbol{x}_j\right)+\mu\mathrm{Im}\left(\boldsymbol{R}^{\alpha}\boldsymbol{x}_j\right)\right)\boldsymbol{j}\\
&+\left(\mathrm{Re}\left(\boldsymbol{R}^{\alpha}\boldsymbol{x}_k\right)+\mu\mathrm{Im}\left(\boldsymbol{R}^{\alpha}\boldsymbol{x}_k\right)\right)\boldsymbol{k},\\
&=\left(\mathrm{Re}\left(\mathrm{DFRNT1D}^{\alpha}(\boldsymbol{x}_{\mathrm{r}})\right)-a\mathrm{Im}\left(\mathrm{DFRNT1D}^{\alpha}(\boldsymbol{x}_i)\right)\right.\\
&\left.-b\mathrm{Im}\left(\mathrm{DFRNT1D}^{\alpha}(\boldsymbol{x}_j)\right)-c\mathrm{Im}\left(\mathrm{DFRNT1D}^{\alpha}(\boldsymbol{x}_k)\right)\right)\\
&+\left(\mathrm{Re}\left(\mathrm{DFRNT1D}^{\alpha}(\boldsymbol{x}_i)\right)+a\mathrm{Im}\left(\mathrm{DFRNT1D}^{\alpha}(\boldsymbol{x}_{\mathrm{r}})\right)\right.\\
&\left.-b\mathrm{Im}\left(\mathrm{DFRNT1D}^{\alpha}(\boldsymbol{x}_j)\right)+c\mathrm{Im}\left(\mathrm{DFRNT1D}^{\alpha}(\boldsymbol{x}_k)\right)\right)\boldsymbol{i}\\
&+\left(\mathrm{Re}\left(\mathrm{DFRNT1D}^{\alpha}(\boldsymbol{x}_j)\right)+a\mathrm{Im}\left(\mathrm{DFRNT1D}^{\alpha}(\boldsymbol{x}_{\mathrm{r}})\right)\right.\\
&\left.-b\mathrm{Im}\left(\mathrm{DFRNT1D}^{\alpha}(\boldsymbol{x}_k)\right)+c\mathrm{Im}\left(\mathrm{DFRNT1D}^{\alpha}(\boldsymbol{x}_i)\right)\right)\boldsymbol{j}\\
&+\left(\mathrm{Re}\left(\mathrm{DFRNT1D}^{\alpha}(\boldsymbol{x}_k)\right)+a\mathrm{Im}\left(\mathrm{DFRNT1D}^{\alpha}(\boldsymbol{x}_{\mathrm{r}})\right)\right.\\
&\left.-b\mathrm{Im}\left(\mathrm{DFRNT1D}^{\alpha}(\boldsymbol{x}_i)\right)+c\mathrm{Im}\left(\mathrm{DFRNT1D}^{\alpha}(\boldsymbol{x}_j)\right)\right)\boldsymbol{k}.
\end{aligned} \tag{7}$$

The RHS 1D QDFRNT relationship is determined as in Chen et al. (2018):

$$\begin{aligned}
&\mathrm{RQDFRNT1D}^{\alpha,\mu}\left(\boldsymbol{x}_{\mathrm{q}}\right)\\
&=\left(\mathrm{Re}\left(\mathrm{DFRNT1D}^{\alpha}(\boldsymbol{x}_{\mathrm{r}})\right)-a\mathrm{Im}\left(\mathrm{DFRNT1D}^{\alpha}(\boldsymbol{x}_i)\right)\right.\\
&\left.-b\mathrm{Im}\left(\mathrm{DFRNT1D}^{\alpha}(\boldsymbol{x}_j)\right)-c\mathrm{Im}\left(\mathrm{DFRNT1D}^{\alpha}(\boldsymbol{x}_k)\right)\right)\\
&+\left(\mathrm{Re}\left(\mathrm{DFRNT1D}^{\alpha}(\boldsymbol{x}_i)\right)+a\mathrm{Im}\left(\mathrm{DFRNT1D}^{\alpha}(\boldsymbol{x}_{\mathrm{r}})\right)\right.\\
&\left.+c\mathrm{Im}\left(\mathrm{DFRNT1D}^{\alpha}(\boldsymbol{x}_j)\right)-b\mathrm{Im}\left(\mathrm{DFRNT1D}^{\alpha}(\boldsymbol{x}_k)\right)\right)\boldsymbol{i}\\
&+\left(\mathrm{Re}\left(\mathrm{DFRNT1D}^{\alpha}(\boldsymbol{x}_j)\right)+b\mathrm{Im}\left(\mathrm{DFRNT1D}^{\alpha}(\boldsymbol{x}_{\mathrm{r}})\right)\right.\\
&\left.+a\mathrm{Im}\left(\mathrm{DFRNT1D}^{\alpha}(\boldsymbol{x}_k)\right)-c\mathrm{Im}\left(\mathrm{DFRNT1D}^{\alpha}(\boldsymbol{x}_i)\right)\right)\boldsymbol{j}\\
&+\left(\mathrm{Re}\left(\mathrm{DFRNT1D}^{\alpha}(\boldsymbol{x}_k)\right)+c\mathrm{Im}\left(\mathrm{DFRNT1D}^{\alpha}(\boldsymbol{x}_{\mathrm{r}})\right)\right.\\
&\left.+b\mathrm{Im}\left(\mathrm{DFRNT1D}^{\alpha}(\boldsymbol{x}_i)\right)-a\mathrm{Im}\left(\mathrm{DFRNT1D}^{\alpha}(\boldsymbol{x}_j)\right)\right)\boldsymbol{k}.
\end{aligned} \tag{8}$$

2. Two-dimensional QDFRNT formulation

The 2D QDFRNT is given as follows:

$$\begin{aligned}
&\mathrm{QDFRNT2D}^{\alpha,\mu}(\boldsymbol{y}_{\mathrm{q}})\\
&=\mathrm{RQDFRNT1D}^{\alpha,\mu}(\mathrm{LQDFRNT1D}^{\alpha,\mu}(\boldsymbol{y}_{\mathrm{q}})),
\end{aligned} \tag{9}$$

where $\boldsymbol{y}_{\mathrm{q}}=\boldsymbol{y}_{\mathrm{r}}+\boldsymbol{y}_i\boldsymbol{i}+\boldsymbol{y}_j\boldsymbol{j}+\boldsymbol{y}_k\boldsymbol{k}$ is a 2D quaternion signal (Wang et al., 2019).

3 Multistage privacy system for color medical images based on DQFrFT, SVM watemarking, and 3D-CLM encryption

A blind adaptive watermarking and encryption system based on DQFrFT, SVM, and 3D-CLM is presented for color medical images to evaluate the efficiency of the proposed DQFrFT. Furthermore, the suggested method overcomes some of the limitations of conventional color adaptive watermarking techniques, such as the inefficient use of color information in the adaptive system or the failure to consider the holistic quality of the color host image channels. In this paper, the texture, edge, and color data are extracted from the color medical host images to fully use the color information. In addition, we investigated the quaternion-based method to process color host images holistically (Yamni et al., 2021).

3.1 Proposed color medical image watermarking scheme (stage 1)

A watermark approach is introduced into the medium frequency of QDFRNT coefficients using the integrated masking feature acquired in Section 2.3.1 to modify the watermark strength. Fig. 1 shows the block diagram of the proposed adaptive watermarking technique. This scheme has two parts, an online session for both watermark embedding and extraction

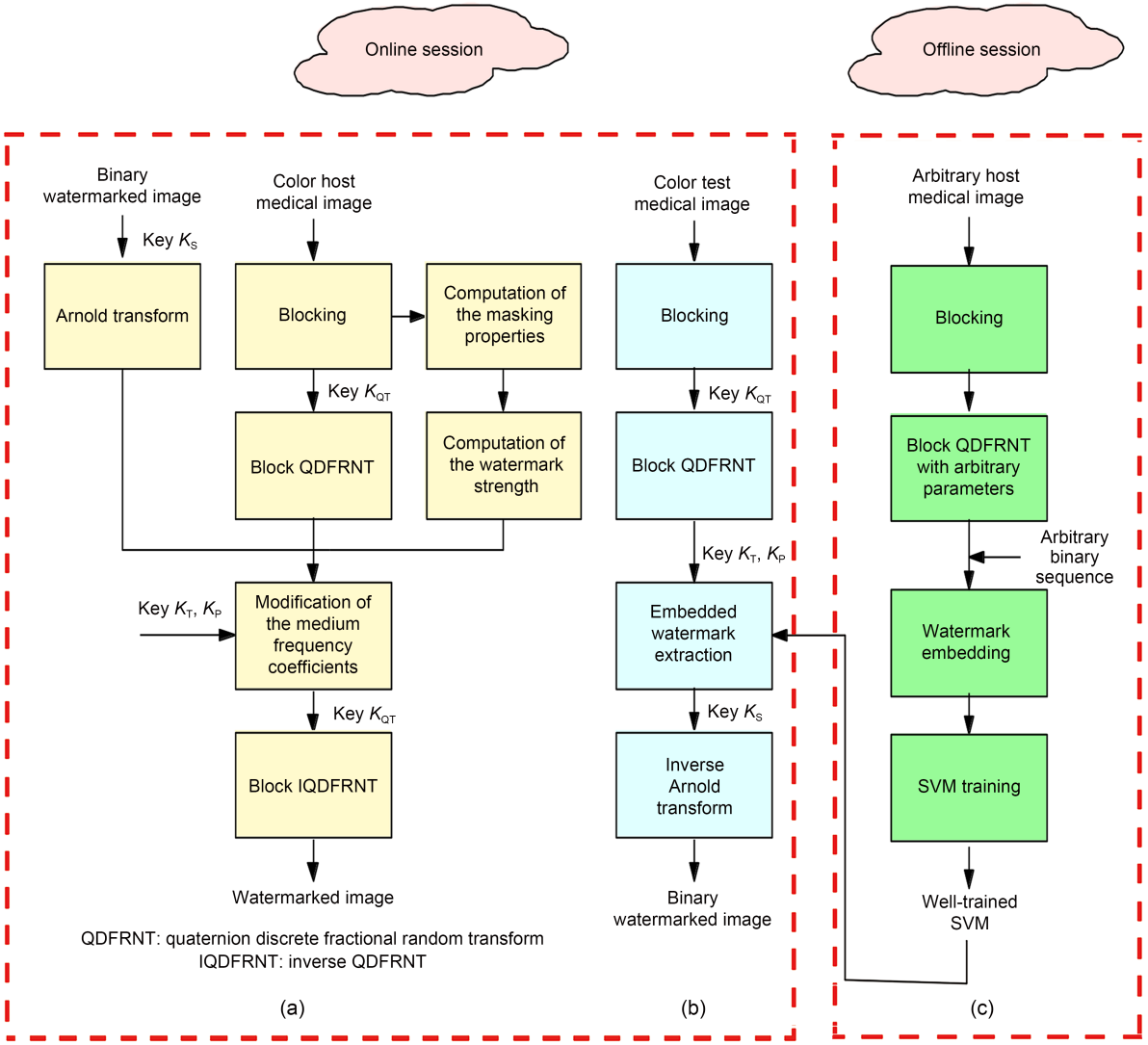

Fig. 1 Online and offline session diagrams for the proposed color medical image adaptive watermarking system: (a) watermark embedding; (b) watermark extraction; (c) support vector machine (SVM) training

and an offline SVM training session. The limitations of watermark embedding are initially discussed before introducing this approach.

3.1.1 Online watermark embedding

Fig. 1a shows a block diagram of watermark embedding. Let $\boldsymbol{W}$ be the image of a binary watermark. To improve the robustness, it is embedded K_{T} times as a key into a color host image $\boldsymbol{H}$ using a multiple redundant embedding approach as follows:

1. Watermark preprocessing

The binary watermark image $\boldsymbol{W}$ of size $N_{\mathrm{w}}\times N_{\mathrm{w}}$ is scrambled using an Arnold transform of s iterations to improve the security and robustness of resizing as follows:

$$\begin{pmatrix} x_s \\ y_s \end{pmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}^s \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} (\mathrm{mod}\, N_{\mathrm{w}}). \tag{10}$$

The parameter s is assigned to the key K_s. The bit stream **WS** is then generated from the scrambled binary watermark.

2. QDFRNT block and masking characteristic calculations

The host image $\boldsymbol{H}$ is divided into 8×8 nonoverlapping blocks. Next, for each block, the QDFRNT with order α, unit pure quaternion μ, periodicity M, and random matrix $\boldsymbol{P}$ is computed. The QDFRNT parameters α, μ, M, and $\boldsymbol{P}$ are configured as a key K_{QT}.

3. Position selection for embedding

Because the blocks with $\hat{J}=0$ have a plain texture, a rich edge, and a warm color, they are not candidates for embedding. By sorting the magnitude values of the QDFRNT coefficients, several medium-frequency locations of each block are privately chosen as candidates for embedding. The reason for this is that medium-frequency locations can ensure a better blend of invisibility and robustness. Furthermore, the 3×3 neighborhood of each embedding location should exist and does not overlap with other neighborhoods. A key $K_{\boldsymbol{P}}$ is assigned to the embedding position.

4. Embedding a watermark with adjustable watermark strength

According to the restrictions used for different types of unit pure quaternions, one to two of the four components ($Y_{\mathrm{qr}}(u, v)$, $Y_{\mathrm{q}\boldsymbol{i}}(u, v)$, $Y_{\mathrm{q}\boldsymbol{j}}(u, v)$, $Y_{\mathrm{q}\boldsymbol{k}}(u, v)$) of the QDFRNT coefficient $Y_{\mathrm{q}}(u, v)$ are adjusted to incorporate the watermark as follows:

$$Y'_{\mathrm{q}h}(u,v) = \mathrm{Avg}_h(u,v) + (2\mathrm{WS}(x)-1)\Delta, \tag{11}$$

$$\mathrm{Avg}_h(u,v)=\frac{1}{8}\sum_{y=-1}^{1}\sum_{z=-1}^{1}\left(Y_{\mathrm{q}h}(u+y,v+z)-Y_{\mathrm{q}}(u,v)\right), \tag{12}$$

where $Y_{\mathrm{q}h}(u,v)$, $h\in\{\mathrm{r}, \boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}\}$ is one of the four components, $Y'_{\mathrm{q}h}(u, v)$ is the modified component value, x is the location of the watermark bit in watermark **WS**, and Δ is the adaptive watermark strength equal to the masking property $\hat{J}$ multiplied by the basic strength Δ_0.

5. Watermarked image generation

The IQDFRNT function is run on each block to generate the watermarked image $\boldsymbol{H}'$.

3.1.2 Offline SVM training

Fig. 1c illustrates the block diagram. The following are the detailed steps:

1. Create a random binary sequential **BS** of length L. The length L should be greater than 50 to keep SVM efficient.

2. From step 2 to step 4, embed the sequence **BS** into an arbitrary host image using the embedding method, with random order α, periodicity M, random matrix $\boldsymbol{P}$, unit pure quaternion μ, and basic strength Δ_0, to produce the modifying QDFRNT coefficients $Y'_{\mathrm{q}}(u_l, v_l)$ (l = 1, 2, ..., L).

3. Calculate the set S_{u_1,v_1} for each embedding position (u_l, v_l) using

$$\begin{aligned} S_{u_1,v_1}=\{&\delta_{u_l-1,v_l-1},\delta_{u_l-1,v_l},\delta_{u_l-1,v_l+1},\delta_{u_l,v_l-1},\delta_{u_l,v_l},\\ &\delta_{u_l,v_l+1},\delta_{u_l+1,v_l-1},\delta_{u_l+1,v_l},\delta_{u_l+1,v_l+1}\}. \end{aligned} \tag{13}$$

Consider each set S_{u_1,v_1} as the input to a sample and BS(l) as the output. Then, these samples are trained, and the well-trained SVM model is used as a classifier. It can be sent to the recipient, or the receiver can train the SVM model using our technique and random parameters.

3.1.3 Online watermark extraction

Fig. 1b shows a block diagram of watermark extraction. The following are the detailed steps:

1. Calculate the QDFRNT coefficients for each block of 8×8 pixels using order K_{QT_α}, unit pure quaternion K_{QT_μ}, periodicity K_{QT_M}, and random matrix $K_{\mathrm{QT}\_\boldsymbol{P}}$. Note that all K_{QT_α}, K_{QT_μ}, K_{QT_M}, and $K_{\mathrm{QT}\_\boldsymbol{P}}$ are in the key K_{QT}.

2. Calculate the set S_{u_1,v_1} for all embedding positions (u_l, v_l) in $Y'_{qh}(u,v)$, $h\in\{r, \boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}\}$, according to the modification procedure under the constraint for the key unit pure quaternion K_{QT_μ} and the embedding position $K_{\boldsymbol{P}}$ as

$$\delta_{u_l+y,v_l+z}=\begin{cases}Y'_{qh}(u_l,v_l)-\mathrm{Avg}_h(u_l,v_l), & y=z=0,\\ Y'_{qh}(u_l,v_l)-Y'_{qh}(u_l+y,v_l+z), & \text{otherwise.}\end{cases}\tag{14}$$

Each set of S_{u_1,v_1} is fed into SVM using the well-trained SVM model, yielding the output d. The distances between d and {0, 1} are then computed, generating dis0 and dis1. The K_{T} bit streams $\mathrm{WS}'_t(x)$ (t=1, 2, ..., K_{T}) are extracted in the following way:

$$\mathrm{WS}'_t(x)=\begin{cases}1, & \mathrm{dis0}>\mathrm{dis1},\\ 0, & \text{otherwise.}\end{cases}\tag{15}$$

The watermark bit stream $\mathrm{WS}'(x)$ is then created as

$$\mathrm{WS}'(x)=\begin{cases}1, & \overline{\mathrm{WS}}(x)\geq 0.5,\\ 0, & \text{otherwise,}\end{cases}\tag{16}$$

where $\overline{\mathrm{WS}}(x)$ is the mean of the values of $\mathrm{WS}'_t(x)$, t=1, 2, ..., K_{T}.

3. Reconfigure the bits **WS** into a 2D binary watermark image of size $\sqrt{\mathrm{size}(K_{\mathrm{p}})/K_{\mathrm{T}}}\times\sqrt{\mathrm{size}(K_{\mathrm{p}})/K_{\mathrm{T}}}$. Then, for the extracted scrambled watermark image $(p-K_s)$ times, use the Arnold transform in Eq. (10) with the key repetition K_s to obtain the final watermark image $\boldsymbol{W}'$. Now, the period p can be obtained by using the watermark size $\sqrt{\mathrm{size}(K_{\mathrm{p}})/K_{\mathrm{T}}}$.

Here, the suggested approach in this case is blind because neither the original host image nor the original watermark is essential for watermark extraction.

3.2 Proposed 3D-CLM encryption scheme (stage 2)

In recent years, the chaos process has attracted much attention because its operation produces noise-like signals. The chaos-based encryption process has appreciated features of confusion, sensitivity to primary value, and diffusion. There are many chaotic maps in the most recent works, such as the Arnold map, logistic map, and cat map. Some studies (Arab et al., 2019; Belazi et al., 2019; Khan and Masood, 2019; Zhang et al., 2019) presented several image security and image cryptography methods based on chaotic systems. The use of lower-order chaos functions results in the main limitation of current chaotic-map-based encryption schemes. This motivated us to implement an effective medical image cryptography system based on a higher-order chaos function. Therefore, in this work, we employ 3D-CLM to encrypt transmitted color medical images to achieve reliable and robust security performance. Compared to traditional lower-order chaotic functions, 3D-CLM has better permutation and diffusion properties, allowing it to be significantly more robust to cryptanalytic attacks. Fig. 2 is the block diagram for the 3D-CLM encryption scheme suggested by Wen et al. (2016). El-Shafai et al. (2022a) discussed 3D-CLM in depth using detailed equations.

4 Simulation results

In this section, the first stage of the proposed system (watermarking) is evaluated. After that, the second stage of the full proposed system (encryption) is presented. These tests are implemented using Intel® Core™ i7-7700HQ CPU @2.80 GHz with 16 GB RAM and employing MATLAB 2020b. For 1D QDFRNT, five 512-bit 1D quaternion signals are created at random, whereas for 2D QDFRNT, five color medical images of size 512×512 are employed. Different metrics as summarized in El-Shafai and Hemdan (2021) and El-Shafai et al. (2022b) are considered to examine the effectiveness of the proposed method. The size of the color medical image is $m\times n$ in all the equations, where m represents height and n represents width.

4.1 Evaluation of the first stage of the proposed system (watermarking)

For the simulation results presented in this subsection, Fig. 3 presents the binary watermark image and its encrypted watermarked image using the Arnold scheme. Subjective results of the first stage for the examined five color medical images in the absence of attacks are shown in Fig. 4. It shows the original host medical image and its histogram, the watermarked medical image and its histogram, the difference between the original and watermarked images, and the extracted decrypted watermarked image. It is observed that the

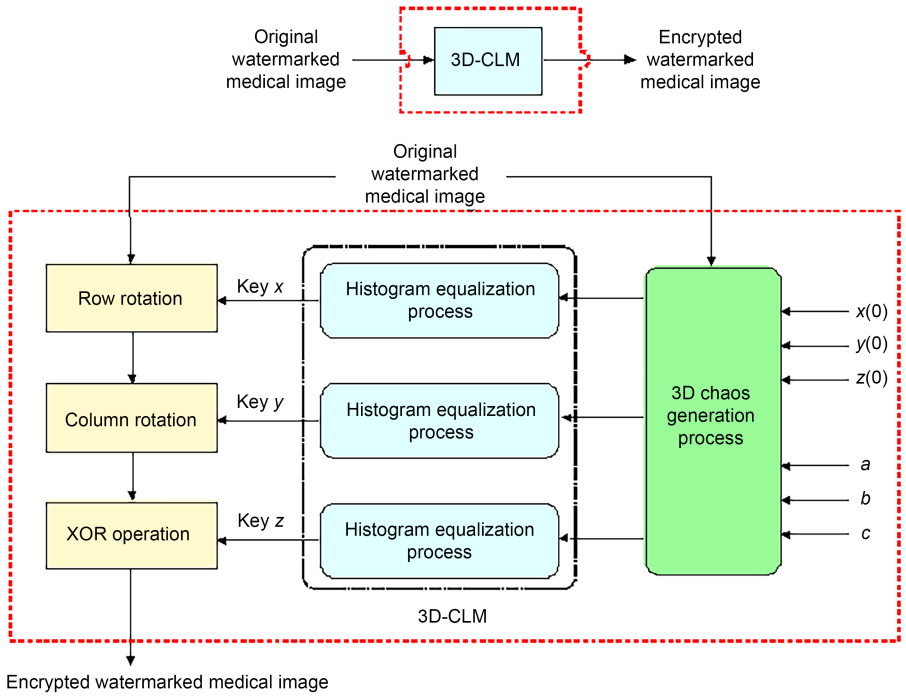

Fig. 2 Block diagram of the proposed three-dimensional chaotic logistic map (3D-CLM) encryption scheme

Fig. 3 Binary watermark image (a) and encrypted watermarked image (b) with the Arnold scheme

binary watermark image is completely encrypted using the Arnold scheme. In addition, the watermarked image is successfully hidden in the watermarked color medical image. It is also noted that the system can extract decrypted watermarked images, indicating its effectiveness and safety.

Objective results of the first stage for the examined color medical image 1 in the absence of attacks are shown in Table 1. The proposed extracted watermarked image is shown to provide high feature similarity (FSIM), structural similarity (SSIM), correlation, and low bit error rate (BER) values, indicating strong security. Table 2 presents the objective results of the extracted watermarked images for the examined medical image 1 in the case of rotation and Gaussian noise attacks. In addition, we examine different blurring attack types, different JPEG compression attack types, resizing attack, and crop attack (Table 3). The results demonstrate that the suggested system is effective against different channel noise threats. The average embedding time of the first stage for the examined medical image 1 in Table 4 indicates a quick processing.

4.2 Evaluation of the full proposed system (encryption)

In this subsection, the full proposed system based on encryption is shown as a second stage. Fig. 5 presents the subjective results of the second stage for medical image 1. This figure also shows the original, encrypted, and decrypted watermarked medical images, the difference between the original and decrypted watermarked images, and the extracted decrypted watermarked image after the decryption process. For the encrypted watermarked medical images, the main details of the plain medical images can be observed. Furthermore, the proposed system performs decryption operations effectively. Histogram results of the original, encrypted, and decrypted watermarked medical image 1 are illustrated in Fig. 6. The histograms of the original images differ from each other, and these histograms are concentrated on certain gray levels. However, the

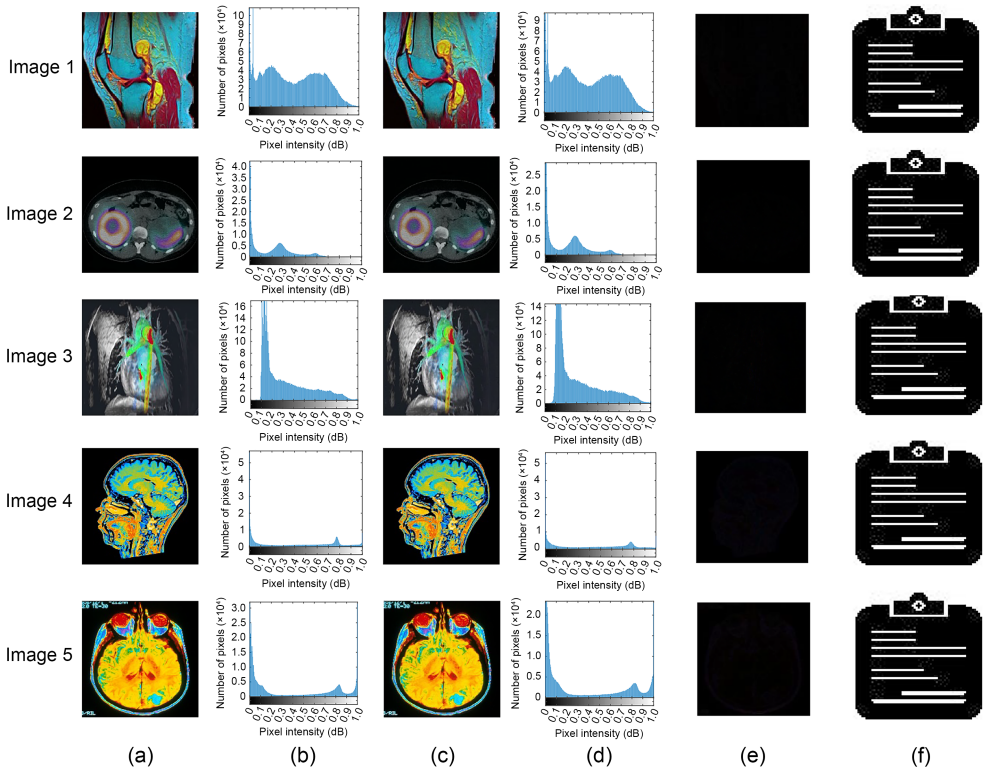

Fig. 4 Subjective results of the first stage for the examined color medical images in the absence of attacks: (a) original host medical image; (b) histogram of the original host medical image; (c) watermarked medical image; (d) histogram of the watermarked medical image; (e) difference between the original and watermarked images; (f) extracted decrypted watermarked image

Table 1 Objective results of the first stage for the examined color medical image 1 in the absence of attacks

Watermarked medical image			Extracted watermarked image			
PSNR (dB)	SSIM	FSIM	SSIM	FSIM	BER	Correlation
82.63	1.0000	0.9999	1.0000	0.9999	0.0050	0.9987

PSNR: peak signal-to-noise ratio; SSIM: structural similarity; FSIM: feature similarity; BER: bit error rate

Table 2 Objective results of the extracted watermarked images for the examined medical image 1 in the case of rotation and Gaussian noise attacks

Parameter	Rotation attack			Gaussian noise attack		
	5°	10°	20°	σ=0.02	σ=0.04	σ=0.06
SSIM	0.9462	0.9451	0.9397	0.9752	0.9738	0.9712
FSIM	0.9262	0.9207	0.9168	0.9604	0.9591	0.9564
BER	0.0098	0.0108	0.0137	0.0067	0.0073	0.0087
Correlation	0.9384	0.9337	0.9217	0.9704	0.9615	0.9553

SSIM: structural similarity; FSIM: feature similarity; BER: bit error rate

Table 3 Objective results of the extracted watermarked images for the examined medical image 1 with different attacks

Parameter	Motion blur	Disk blur	Average blur	JPEG 20%	JPEG 40%	JPEG 60%	Resizing attack	Crop attack
SSIM	0.9864	0.9829	0.9860	0.9833	0.9836	0.9839	0.9907	0.9897
FSIM	0.9859	0.9831	0.9853	0.9842	0.9846	0.9849	0.9896	0.9886
BER	0.0052	0.0073	0.0064	0.0058	0.0056	0.0053	0.0053	0.0069
Correlation	0.9759	0.9727	0.9749	0.9742	0.9744	0.9747	0.9957	0.9943

SSIM: structural similarity; FSIM: feature similarity; BER: bit error rate

histograms of the encrypted medical images are nearly identical. Each gray level has a fixed number of pixels corresponding to it.

The original and encrypted watermarked color medical images from the examined medical image 1 are shown in Fig. 7, which shows the effects of two neighboring pixels' horizontal (H), vertical (V), and diagonal (D) correlations. The correlation coefficients of two adjacent pixels in the original, encrypted, and decrypted watermarked medical images are presented in Table 5. Fig. 7 and Table 5 show that the suggested system has low correlation values, indicating that the proposed cryptosystem is more secure and robust. As the correlation value decreases in the encryption algorithm, the encryption algorithm becomes stronger.

Table 6 shows the information entropies of the tested plain, ciphered, and deciphered watermarked color medical images. The results demonstrate that the entropy levels are extremely near the optimum value of 8, indicating that the suggested ciphering technique performs better.

Table 4 Average embedding time of the first stage for the examined color medical image 1

Medical image	Average embedding time (s)
Image 1	2.52

Table 7 compares the peak signal-to-noise ratio (PSNR), FSIM, and SSIM results of the plain and encrypted watermarked medical images. The estimated PSNR for the ciphered color images is lower, as shown in the data obtained in Table 7. This demonstrates how effective the proposed medical image encryption algorithm is. Table 8 presents the number of pixel change rate (NPCR) and unified average changing intensity (UACI) values of the ciphered watermarked color medical images. The high NPCR and UACI values close to the ideal values show that the suggested medical imaging system has excellent characteristics in resisting differential attacks. Moreover, Table 8 shows the histogram and irregular deviation results of the ciphered watermarked medical images. As shown, both H_D and D_I have low values, indicating that the plain and ciphered images are totally irrelevant.

Table 8 also illustrates the edge detection ratio (EDR) values of the encrypted watermarked medical images. They almost equal one, indicating that the

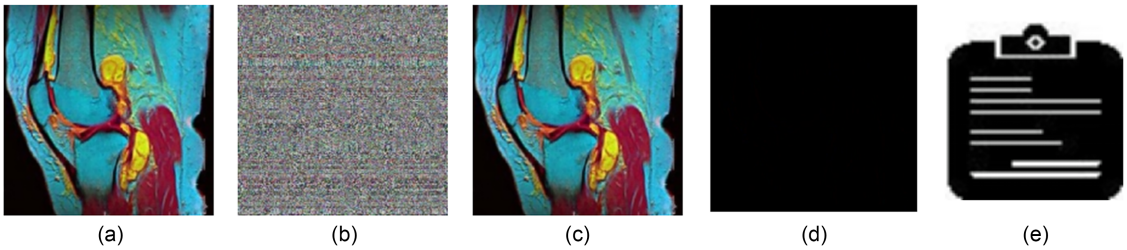

Fig. 5 Subjective results of the second stage for the examined medical image 1: (a) original watermarked medical image; (b) encrypted watermarked medical image; (c) decrypted watermarked medical image; (d) difference between the original and decrypted watermarked images; (e) extracted decrypted watermarked image after the decryption process

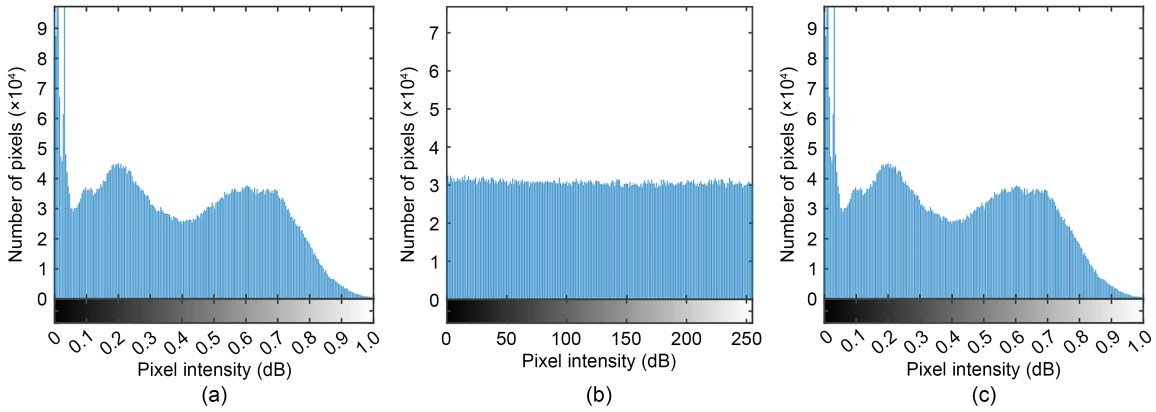

Fig. 6 Histogram of the original (a), encrypted (b), and decrypted (c) watermarked medical image 1

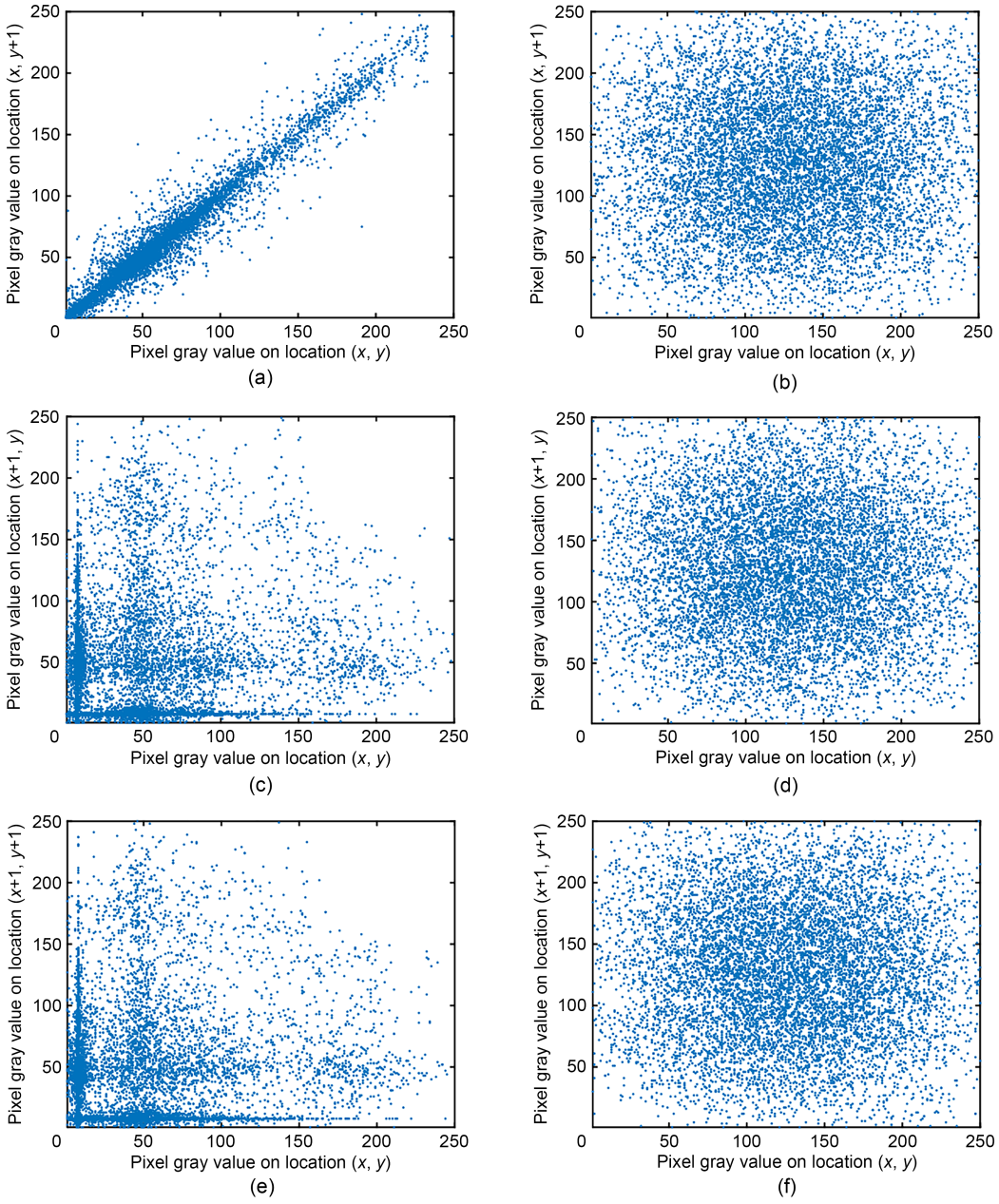

Fig. 7 Horizontal (H), vertical (V), and diagonal (D) correlation results of two adjacent pixels in the original and encrypted watermarked medical images of the tested medical image 1: (a) H direction in the original watermarked medical image; (b) H direction in the encrypted watermarked medical image; (c) V direction in the original watermarked medical image; (d) V direction in the encrypted watermarked medical image; (e) D direction in the original watermarked medical image; (f) D direction in the encrypted watermarked medical image

Table 5 Correlation coefficients in the original, encrypted, and decrypted watermarked medical image 1

Image	Correlation coefficient		
	Horizontal	Vertical	Diagonal
Original	0.9413	0.9819	0.9262
Encrypted	0.1666	0.0445	0.0892
Decrypted	0.9413	0.9819	0.9262

original and encrypted color medical images are completely different. The Laplacian edge detection results of watermarked medical images are shown in Fig. 8. As seen, the edges are observed in the encrypted forms of the images are entirely different from those in the original versions. Note that the observed edges in the deciphered images are identical to the original ones.

Table 6 Information entropies of the tested plain, ciphered, and deciphered watermarked medical image 1

Image	Information entropy
Original	7.6715
Encrypted	7.7849
Decrypted	7.6715

Table 7 PSNR, SSIM, and FSIM results between plain and ciphered watermarked medical image 1

PSNR (dB)	SSIM	FSIM
8.7738	0.0107	0.5506

PSNR: peak signal-to-noise ratio; SSIM: structural similarity; FSIM: feature similarity

Table 8 Results of ciphered watermarked medical image 1

NPCR	UACI	H_D	D_I	EDR
0.9960	0.3346	6.1023	0.0076	0.9095

NPCR: number of pixel change rate; UACI: unified average changing intensity; EDR: edge detection ratio

These results confirm the efficiency of the proposed color medical image system.

Chaos sequences require a large key space and high sensitivity to preparatory conditions. Key sensitivity refers to the notion that an output can vary significantly when one or more input values are slightly changed. As a result, the plain image is no longer recoverable. The sensitivity of an encryption algorithm to key changes should be high. The important sensitivity analysis results for the examined medical images are shown in Fig. 9. According to the results, the suggested encryption algorithm has high key sensitivity for small changes in the secret key. Table 9 presents the processing time of the encrypted watermarked medical images. Furthermore, the ciphering algorithm's computational complexity is low for all medical images tested. Therefore, the suggested technique is applicable for real-time applications.

4.3 Noise attack analysis

In this subsection, the performance analysis of various noise threats, in addition to the effects on encrypted medical images, is examined. Various noise sources are evaluated: Gaussian, Poisson, salt-and-pepper, speckle, and occlusion attacks are all examples of attacks. White noise is another name for Gaussian noise. An example of a transmission threat is salt-and-pepper channel noise, which occurs when the image has noise made up of black and white pixels. Artificial aperture radar, satellite, and medical images all have speckle noise,

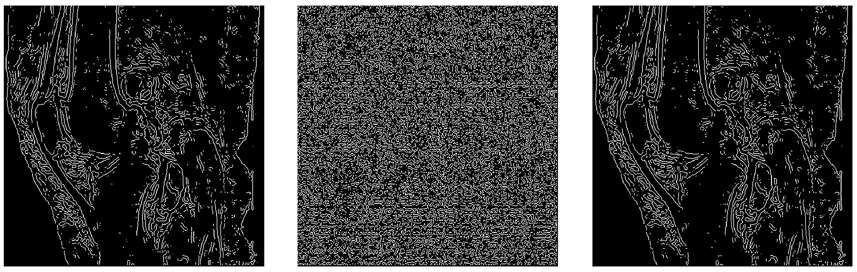

Fig. 8 Laplacian of Gaussian edge detection results of watermarked medical image 1: (a) original; (b) encrypted; (c) decrypted

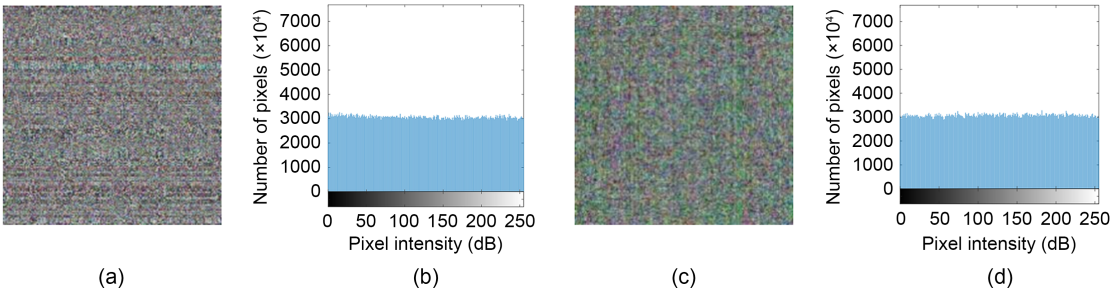

Fig. 9 Key sensitivity results for the examined medical image 1: (a) encrypted image using the correct key; (b) histogram of the encrypted image using the correct key; (c) decrypted image using an incorrect key; (d) histogram of the decrypted image using an incorrect key

which is an additive distortion. Poisson noise, also known as photon or shot noise, is a fundamental type of uncertainty in light measurement caused by the quantized structure of light and the independence of photon detection. An occlusion attack occurs when something is closed or blocked. A blood clot blocking a coronary artery is the main cause of heart attacks in almost all cases.

Encrypted and decrypted watermarked medical images in the presence of Gaussian noise with different noise variances are presented in Fig. 10. Gaussian noise with variances of 0.02, 0.04, and 0.06 is added to the encrypted image to test the proposed encryption algorithm against noise attacks. The results show the strength of the suggested system versus noise attack, where the decrypted watermarked medical images could be retrieved with clarity.

Fig. 11 shows the encrypted and decrypted watermarked medical images in the presence of Poisson noise on the encrypted images. The encrypted watermarked images for all tests are completely hidden. Moreover, it gives good outcomes for the decrypted watermarked images.

Table 9 Processing time of encrypted watermarked medical image 1

Medical image	Time (s)
Image 1	3.92

The watermarked medical images that have been encrypted and decrypted, along with salt-and-pepper noise with various noise variances, are shown in Fig. 12. To evaluate the proposed encryption algorithm against noise attacks, salt-and-pepper noise with variances of 0.02, 0.04, and 0.06 is introduced to encrypted and decrypted images. The strength of the suggested cryptosystem against noise attack is demonstrated by the results, showing that in the presence of channel noise, decrypted watermarked images are restored with high performance.

In addition, the encrypted and decrypted watermarked medical images in the presence of speckle noise with different noise variances are shown in Fig. 13. Variances of 0.02, 0.04, and 0.06 are applied to the encrypted image to test the proposed encryption algorithm versus speckle noise threats. As shown, the suggested

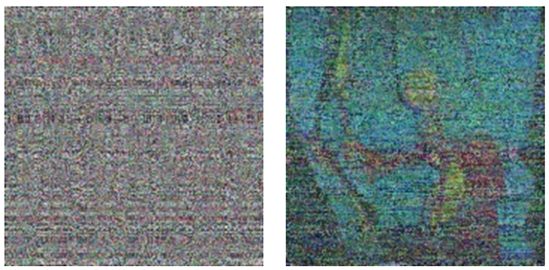

Fig. 11 Encrypted (a) and decrypted (b) watermarked image 1 in the presence of Poisson noise

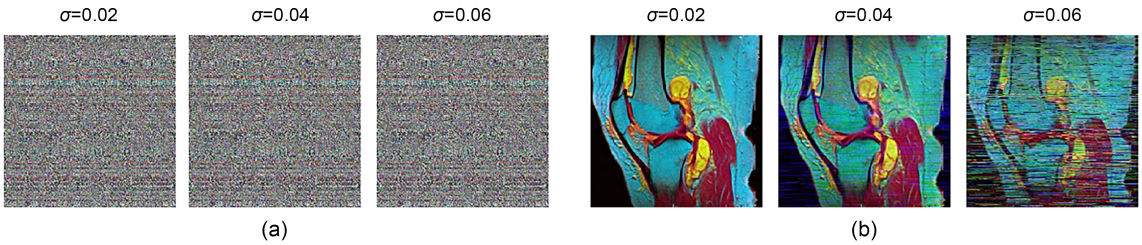

Fig. 10 Encrypted (a) and decrypted (b) watermarked medical image 1 in the presence of Gaussian noise with different noise variances (μ=0)

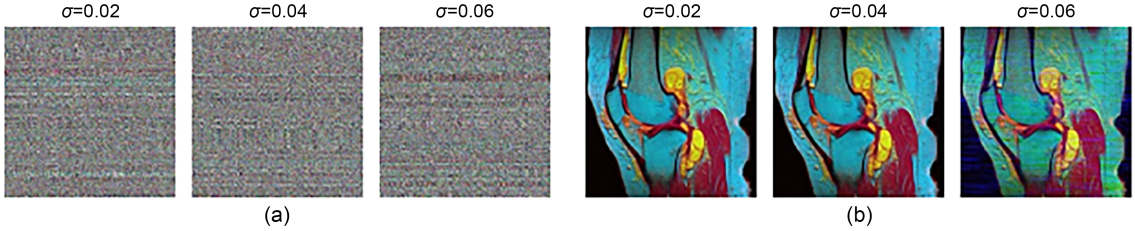

Fig. 12 Encrypted (a) and decrypted (b) watermarked medical image 1 in the presence of salt-and-pepper noise with different noise variances

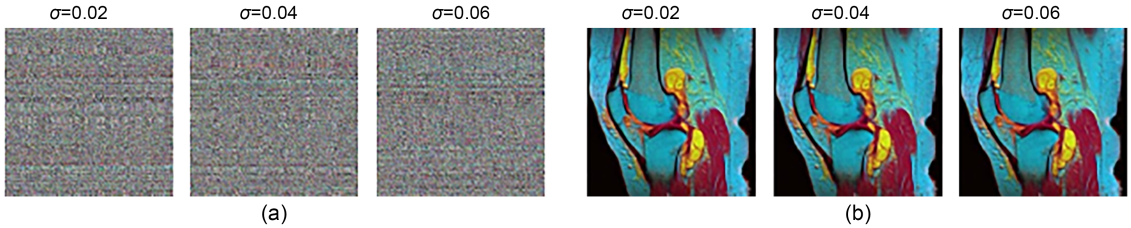

Fig. 13 Encrypted (a) and decrypted (b) watermarked medical image 1 in the presence of speckle noise with different noise variances

cryptosystem is strong against different noise attacks, and decrypted watermarked medical images can be recovered in excellent shape.

Furthermore, Fig. 14 presents the encrypted and decrypted watermarked medical images in the presence of occlusion attack on the encrypted images. The encrypted watermarked medical images are fully concealed, and for the decrypted watermarked medical images, the tested images are reconstructed with good quality. Finally, it is noticed from all the visual results of different types of attack that both speckle noise and salt-and-pepper noise have the lowest impression of the decrypted images.

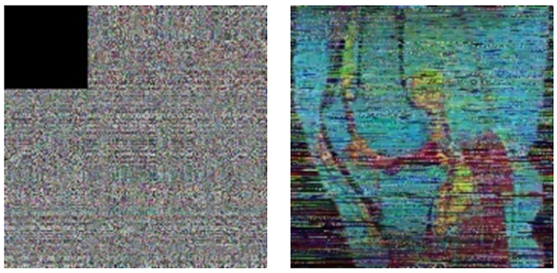

Fig. 14 Encrypted (a) and decrypted (b) watermarked medical images in the presence of occlusion attack on the encrypted images

5 Competitive study

Furthermore, more simulation tests are carried out to compare the proposed security algorithm with state-of-the-art techniques (Faragallah et al., 2019; Yamni et al., 2021; Daoui et al., 2022; Khafaga et al., 2022) to validate the security and robustness efficiency of the multilevel security algorithm. Table 10 presents the evaluation results of the full proposed system (encryption) in comparison with the related work without the presence of attacks. Comparison results show that the suggested security work achieves lower average runtime values for the examined color medical images than conventional techniques. Moreover, it shows that this paper studies all evaluation metrics with and without noise attack, unlike other papers.

6 Conclusions and future work

This paper presents a novel multistage privacy scheme for color medical images based on DQFrFT watermarking and 3D-CLM encryption. To extend DFRNT to quaternion signal processing, QDFRNT has been developed. Theoretical analysis demonstrates that the QDFRNT of a quaternion signal can be easily determined by obtaining the DFRNT of each component. The computational complexity of this effective computation method is only 1/2 that of the direct method. The suggested QDFRNT-based approach performs better than some other systems regarding the implementation of QDFRNT in color image adaptive watermarking:

1. It examines the masking characteristics directly on the color host image rather than on the grayscale version.

2. It processes the three channels of the color image using a quaternion-based method rather than individually.

In addition, QDFRNT's random matrix and fractional order both enhance the security of the suggested technique. Simulation results demonstrate that the proposed security system is effective against various types of channel noise attacks.

In our future work, we will expand the suggested work to other signals to further validate the security results. In addition, we intend to implement a real hardware system for the proposed cryptosystem. Also, there is a plan to use GPUs for this type of computation.

Table 10 Comparisons with related works

Reference	Correlation coefficient*			PSNR (dB)	Entropy**	NPCR
	Horizontal	Vertical	Diagonal			
Daoui et al. (2022)	0.0082	−0.0035	−0.0036	–	–	–
Faragallah et al. (2019)	–	–	–	54.2100	–	–
Khafaga et al. (2022)	–	–	–	–	–	–
Yamni et al. (2021)	–	–	–	20.8050	–	–
This paper (image 2)	0.0466	0.0599	−0.0413	6.3120	7.9410	0.9962

Reference	UACI	SSIM	FSIM	H_D	D_I	EDR	Average runtime (s)
Daoui et al. (2022)	–	–	–	–	–	–	5.4653
Faragallah et al. (2019)	–	–	–	–	–	–	–
Khafaga et al. (2022)	–	–	–	–	–	–	11.7690
Yamni et al. (2021)	–	–	–	–	–	–	13.4568
This paper (image 2)	0.3352	0.0088	0.4317	2.9431	0.0075	0.8938	4.1700

* Encrypted watermarked medical image. ** Encrypted image. PSNR: peak signal-to-noise ratio; NPCR: number of pixel change rate; UACI: unified average changing intensity; SSIM: structural similarity; FSIM: feature similarity; EDR: edge detection ratio

Contributions

All authors designed the research. Fatma KHALLAF, Walid EL-SHAFAI, and Naglaa F. SOLIMAN processed the data and drafted the paper. Fatma KHALLAF and Walid EL-SHAFAI helped organize the paper. Walid EL-SHAFAI, El-Sayed M. EL-RABAIE, Naglaa F. SOLIMAN, and Fathi E. Abd EL-SAMIE revised and finalized the paper.

Compliance with ethics guidelines

Fatma KHALLAF, Walid EL-SHAFAI, El-Sayed M. EL-RABAIE, Naglaa F. SOLIMAN, and Fathi E. Abd EL-SAMIE declare that they have no conflict of interest.

Data availability

The data that support the findings of this study are available from the corresponding author upon reasonable request.

References

Abdelwahab KM, El-Atty SMA, El-Saied M, et al., 2020. Efficient SVD-based audio watermarking technique in FRT domain. *Multim Tools Appl*, 79(9):5617-5648. https://doi.org/10.1007/s11042-019-08023-z

Al-Afandy KA, El-Shafai W, El-Rabaie ESM, et al., 2018. Robust hybrid watermarking techniques for different color imaging systems. *Multim Tools Appl*, 77(19):25709-25759. https://doi.org/10.1007/s11042-018-5814-y

Alarifi A, Sankar S, Altameem T, et al., 2020a. A novel hybrid cryptosystem for secure streaming of high efficiency H.265 compressed videos in IoT multimedia applications. *IEEE Access*, 8:128548-128573. https://doi.org/10.1109/ACCESS.2020.3008644

Alarifi A, Amoon M, Aly MH, et al., 2020b. Optical PTFT asymmetric cryptosystem-based secure and efficient cancelable biometric recognition system. *IEEE Access*, 8:221246-221268. https://doi.org/10.1109/ACCESS.2020.3043689

Algarni AD, El Banby G, Ismail S, et al., 2020. Discrete transforms and matrix rotation based cancelable face and fingerprint recognition for biometric security applications. *Entropy*, 22(12):1361. https://doi.org/10.3390/e22121361

Almomani I, Alkhayer A, El-Shafai W, 2022a. A crypto-steganography approach for hiding ransomware within HEVC streams in Android IoT devices. *Sensors*, 22(6):2281. https://doi.org/10.3390/s22062281

Almomani I, AlKhayer A, El-Shafai W, 2022b. Novel ransomware hiding model using HEVC steganography approach. *Comput Mater Contin*, 70(1):1209-1228. https://doi.org/10.32604/cmc.2022.018631

Alqahtani F, Amoon M, El-Shafai W, 2022. A fractional Fourier based medical image authentication approach. *Comput Mater Contin*, 70(2):3133-3150. https://doi.org/10.32604/cmc.2022.020454

Arab A, Rostami MJ, Ghavami B, 2019. An image encryption method based on chaos system and AES algorithm. *J Supercomput*, 75(10):6663-6682. https://doi.org/10.1007/s11227-019-02878-7

Belazi A, Talha M, Kharbech S, et al., 2019. Novel medical image encryption scheme based on chaos and DNA encoding. *IEEE Access*, 7:36667-36681. https://doi.org/10.1109/ACCESS.2019.2906292

Chen BJ, Zhou CF, Jeon B, et al., 2018. Quaternion discrete fractional random transform for color image adaptive watermarking. *Multim Tools Appl*, 77(16):20809-20837. https://doi.org/10.1007/s11042-017-5511-2

Daoui A, Yamni M, Karmouni H, et al., 2022. Biomedical multimedia encryption by fractional-order Meixner polynomials map and quaternion fractional-order Meixner moments. *IEEE Access*, 10:102599-102617. https://doi.org/10.1109/ACCESS.2022.3203067

Duan CF, Zhou J, Gong LH, et al., 2022. New color image encryption scheme based on multi-parameter fractional discrete Tchebyshev moments and nonlinear fractal permutation method. *Opt Lasers Eng*, 150:106881. https://doi.org/10.1016/j.optlaseng.2021.106881

Elashry IF, El-Shafai W, Hasan ES, et al., 2020. Efficient chaotic-based image cryptosystem with different modes of operation. *Multim Tools Appl*, 79(29):20665-20687. https://doi.org/10.1007/s11042-019-08322-5

El-Meadawy SA, Farghal AE, Shalaby HMH, et al., 2021. Efficient and secure bit-level chaos security algorithm for orbital angular momentum modulation in free-space optical communications. *IEEE Access*, 9:74817-74835. https://doi.org/10.1109/ACCESS.2021.3074894

El-Shafai W, 2015. Joint adaptive pre-processing resilience and post-processing concealment schemes for 3D video transmission. *3D Res*, 6(1):10. https://doi.org/10.1007/s13319-015-0042-y

El-Shafai W, Hemdan EED, 2021. Robust and efficient multi-level security framework for color medical images in tele-healthcare services. *J Amb Intell Human Comput*, 14:3675-3690. https://doi.org/10.1007/s12652-021-03494-1

El-Shafai W, El-Rabaie S, El-Halawany M, et al., 2017. Enhancement of wireless 3D video communication using color-plus-depth error restoration algorithms and Bayesian Kalman filtering. *Wirel Pers Commun*, 97(1):245-268. https://doi.org/10.1007/s11277-017-4503-x

El-Shafai W, El-Rabaie S, El-Halawany MM, et al., 2018a. Efficient hybrid watermarking schemes for robust and secure 3D-MVC communication. *Int J Commun Syst*, 31(4):e3478. https://doi.org/10.1002/dac.3478

El-Shafai W, El-Rabaie ESM, El-Halawany M, et al., 2018b. Efficient multi-level security for robust 3D color-plus-depth HEVC. *Multim Tools Appl*, 77(23):30911-30937. https://doi.org/10.1007/s11042-018-6036-z

El-Shafai W, El-Rabaie S, El-Halawany MM, et al., 2018c. Recursive Bayesian filtering-based error concealment scheme for 3D video communication over severely lossy wireless channels. *Circ Syst Signal Process*, 37(11):4810-4841. https://doi.org/10.1007/s00034-018-0786-8

El-Shafai W, El-Rabaie S, El-Halawany MM, et al., 2019. Security of 3D-HEVC transmission based on fusion and watermarking techniques. *Multim Tools Appl*, 78(19):27211-27244. https://doi.org/10.1007/s11042-019-7448-0

El-Shafai W, Almomani IM, Alkhayer A, 2021a. Optical bit-plane-based 3D-JST cryptography algorithm with cascaded 2D-FrFT encryption for efficient and secure HEVC communication. *IEEE Access*, 9:35004-35026. https://doi.org/10.1109/ACCESS.2021.3062403

El-Shafai W, Khallaf F, El-Rabaie ESM, et al., 2021b. Robust medical image encryption based on DNA-chaos cryptosystem for secure telemedicine and healthcare applications. *J Amb Intell Human Comput*, 12(10):9007-9035. https://doi.org/10.1007/s12652-020-02597-5

El-Shafai W, Mesrega AK, Ahmed HEH, et al., 2022a. An efficient multimedia compression-encryption scheme using latin squares for securing Internet-of-things networks. *J Inform Secur Appl*, 64:103039. https://doi.org/10.1016/j.jisa.2021.103039

El-Shafai W, Khallaf F, El-Rabaie ESM, et al., 2022b. Proposed neural SAE-based medical image cryptography framework using deep extracted features for smart IoT healthcare applications. *Neur Comput Appl*, 34(13):10629-10653. https://doi.org/10.1007/s00521-022-06994-z

El-Shafai W, Khallaf F, El-Rabaie ESM, et al., 2022c. Proposed 3D chaos-based medical image cryptosystem for secure cloud-IoMT eHealth communication services. *J Amb Intell Human Comput*, p.1-28. https://doi.org/10.1007/s12652-022-03832-x

Faragallah OS, Alzain MA, El-Sayed HS, et al., 2019. Block-based optical color image encryption based on double random phase encoding. *IEEE Access*, 7:4184-4194. https://doi.org/10.1109/ACCESS.2018.2879857

Faragallah OS, Afifi A, El-Shafai W, et al., 2020a. Investigation of chaotic image encryption in spatial and FrFT domains for cybersecurity applications. *IEEE Access*, 8:42491-42503. https://doi.org/10.1109/ACCESS.2020.2974226

Faragallah OS, Afifi A, El-Sayed HS, et al., 2020b. Efficient HEVC integrity verification scheme for multimedia cybersecurity applications. *IEEE Access*, 8:167069-167089. https://doi.org/10.1109/ACCESS.2020.3019840

Faragallah OS, AlZain MA, El-Sayed HS, et al., 2020c. Secure color image cryptosystem based on chaotic logistic in the FrFT domain. *Multim Tools Appl*, 79(3):2495-2519. https://doi.org/10.1007/s11042-019-08190-z

Faragallah OS, El-Sayed HS, Afifi A, et al., 2021. Efficient and secure opto-cryptosystem for color images using 2D logistic-based fractional Fourier transform. *Opt Lasers Eng*, 137:106333. https://doi.org/10.1016/j.optlaseng.2020.106333

Faragallah OS, El-Shafai W, Sallam AI, et al., 2022. Cybersecurity framework of hybrid watermarking and selective encryption for secure HEVC communication. *J Amb Intell Human Comput*, 13(2):1215-1239. https://doi.org/10.1007/s12652-020-02832-z

Huang ZW, Zhou NR, 2022. Image encryption scheme based on discrete cosine Stockwell transform and DNA-level modulus diffusion. *Opt Laser Technol*, 149:107879. https://doi.org/10.1016/j.optlastec.2022.107879

Jin LH, Song EM, Li L, et al., 2013. A quaternion gradient operator for color image edge detection. IEEE Int Conf on Image Processing, p.3040-3044. https://doi.org/10.1109/ICIP.2013.6738626

Khafaga DS, Karim FK, Darwish MM, et al., 2022. Robust zero-watermarking of color medical images using multi-channel Gaussian-Hermite moments and 1D Chebyshev chaotic map. *Sensors*, 22(15):5612. https://doi.org/10.3390/s22155612

Khan M, Masood F, 2019. A novel chaotic image encryption technique based on multiple discrete dynamical maps. *Multim Tools Appl*, 78(18):26203-26222. https://doi.org/10.1007/s11042-019-07818-4

Pandey R, Gamit N, Naik S, 2014. Non-destructive quality grading of mango (Mangifera Indica L) based on CIELab colour model and size. IEEE Int Conf on Advanced Communications, Control and Computing Technologies, p.1246-1251. https://doi.org/10.1109/ICACCCT.2014.7019298

Salah E, Amine K, Redouane K, et al., 2021. A Fourier transform based audio watermarking algorithm. *Appl Acoust*, 172:107652. https://doi.org/10.1016/j.apacoust.2020.107652

Siam AI, Almaiah MA, Al-Zahrani A, et al., 2021. Secure

health monitoring communication systems based on IoT and cloud computing for medical emergency applications. *Comput Intell Neurosci*, 2021:8016525. https://doi.org/10.1155/2021/8016525

Soliman NF, Khalil MI, Algarni AD, et al., 2021. Efficient HEVC steganography approach based on audio compression and encryption in QFFT domain for secure multimedia communication. *Multim Tools Appl*, 80(3):4789-4823. https://doi.org/10.1007/s11042-020-09881-8

Urynbassarova D, Teali AA, Zhang F, 2022. Discrete quaternion linear canonical transform. *Dig Signal Process*, 122:103361. https://doi.org/10.1016/j.dsp.2021.103361

Wang H, Hu XJ, Xu H, et al., 2019. No-reference quality assessment method for blurriness of SEM micrographs with multiple texture. *Scanning*, 2019:4271761. https://doi.org/10.1155/2019/4271761

Wen WY, Zhang YS, Fang YM, et al., 2016. A novel selective image encryption method based on saliency detection. Visual Communications and Image Processing, p.1-4. https://doi.org/10.1109/VCIP.2016.7805456

Yamni M, Karmouni H, Sayyouri M, et al., 2021. Robust zero-watermarking scheme based on novel quaternion radial fractional Charlier moments. *Multim Tools Appl*, 80(14): 21679-21708. https://doi.org/10.1007/s11042-021-10717-2

Zhang XC, Wang LF, Zhou Z, et al., 2019. A chaos-based image encryption technique utilizing Hilbert curves and H-fractals. *IEEE Access*, 7:74734-74746. https://doi.org/10.1109/ACCESS.2019.2921309