*Optica Applicata, Vol. LIII, No. 2, 2023*
DOI: 10.37190/oa230208

# Robust dual color images watermarking scheme with hyperchaotic encryption based on quaternion DFrAT and genetic algorithm

Hui-Xin Luo, Li-Hua Gong, Su-Hua Chen*

Department of Electronic Information Engineering, Nanchang University, Nanchang 330031, China

*Corresponding author: chensuhua@ncu.edu.cn

A robust dual color images watermarking algorithm is designed based on quaternion discrete fractional angular transform (QDFrAT) and genetic algorithm. To guarantee the watermark security, the original color watermark image is encrypted with a 4D hyperchaotic system. A pure quaternion matrix is acquired by performing the discrete wavelet transform (DWT), the block division and the discrete cosine transform on the original color cover image. The quaternion matrix is operated by the QDFrAT to improve the robustness and the security of the watermarking scheme with the optimal transform angle and the fractional order. Then the singular value matrix is obtained by the quaternion singular value decomposition (QSVD) to further enhance the scheme's stability. The encryption watermark is also processed by DWT and QSVD. Afterward, the singular value matrix of the encryption watermark is embedded into the singular value matrix of the host image by the optimal scaling factor. Moreover, the values to balance imperceptibility and robustness are optimized with a genetic algorithm. It is shown that the proposed color image watermarking scheme performs well in imperceptibility, security, robustness and embedding capacity.

Keywords: color image watermarking, hyperchaotic encryption, quaternion discrete fractional angular transform, quaternion singular value decomposition, genetic algorithm.

## 1. Introduction

Color image watermarking technology has become a research focus [1–3]. Dual-color image watermarking systems could achieve higher fidelity and greater amount of information capacity, where both watermark images and host ones are color [4, 5]. However, it is more challenging to realize three color channels of color images than single channel gray images.

Extending complex numbers into four dimensions, Hamilton introduced quaternion in 1843 [6]. By combining the quaternion theory with typical transform technologies, several effective and robust algorithms have been proposed [7–10]. Li *et al*. embedded the watermark by the scalar component of the quaternion discrete cosine transform [7]. Based on the quaternion discrete Fourier transform, Wang *et al*. investigated a new lossless watermarking algorithm of great visual quality with low-fre-

quency information [8]. LI *et al*. designed a new robust watermarking scheme with both the abundant phase information and the frequency coefficients of the host image obtained by the quaternion wavelet transform [9]. XIA *et al*. introduced a zero-watermarking algorithm based on the quaternion polar harmonic transforms [10].

Compared with the traditional transform methods, their corresponding fractional transforms with a free fractional parameter can reflect the dual characteristics of spatial domain and transform domain simultaneously. The performance of the digital watermarking algorithms can be enhanced by the additional fractional parameter of fractional Fourier transform [11], fractional wavelet transform [12], fractional random transform [13], *etc*. Therefore, quaternion and fractional transforms are combined together to design efficient and robust watermarking schemes. To verify the effectiveness of the proposed quaternion discrete fractional Krawtchouk transform, LIU *et al*. put forward a color image watermarking algorithm [14]. CHEN *et al*. designed a color image adaptive watermarking scheme by defining a quaternion discrete fractional random transform [15].

In this paper, a dual color images watermarking scheme is introduced based on the quaternion discrete fractional angular transform, the quaternion singular value decomposition and the genetic algorithm.

The rest of this paper is structured as follows. In Section 2, some key technologies are revisited, including the quaternion discrete fractional angular transform (QDFrAT), the quaternion singular value decomposition (QSVD), and the genetic algorithm. The detailed color watermark embedding and extraction algorithm is presented in Section 3. Experimental results and evaluations are presented in Section 4. Lastly, a short conclusion is drawn in Section 5.

## 2. Theoretical background

### 2.1. Quaternion discrete fractional angular transform

For an image $\mathbf{I}$ of size $M\times N$, the discrete fractional angular transform (DFrAT) is [16]

$$\mathbf{Y}_{\alpha,\beta} = \mathbf{\Phi}_M^{\alpha,\beta}\,\mathbf{I}\,\mathbf{\Phi}_N^{\alpha,\beta} \tag{1}$$

where $\alpha$ and $\beta$ denote the fractional order and the transform angle, respectively, and the kernel matrix $\mathbf{\Phi}_N^{\alpha,\beta}$ of the DFrAT is

$$\mathbf{\Phi}_N^{\alpha,\beta} = \mathbf{V}_N^{\beta}\,\mathbf{D}_N^{\alpha}(\mathbf{V}_N^{\beta})^{\mathrm{T}} \tag{2}$$

where $\mathbf{V}_N^{\beta}$ is an orthonormal matrix composed of the eigenvectors of the DFrAT, $\mathbf{D}_N^{\alpha} = \mathrm{diag}\{1, \exp(-2i\pi\alpha/T), \exp(-4i\pi\alpha/T), \ldots, \exp(-2(N-1)i\pi\alpha/T)\}$ is the eigenvalues matrix of the DFrAT, and $T$ denotes the period.

For a 1D signal $\mathbf{x}(n)$ with $N$ points, its $\alpha$-th order DFrAT is

$$\mathbf{X}_{\alpha,\beta} = \mathbf{\Phi}_N^{\alpha,\beta}\,\mathbf{x}(n) \tag{3}$$

According to the quaternion theory, a new QDFrAT can be defined. For a 1D quaternion signal $\mathbf{x}_q = \mathbf{x}_r + \mathbf{x}_i\mathbf{i} + \mathbf{x}_j\mathbf{j} + \mathbf{x}_k\mathbf{k}$, its $\alpha$-th order left-side and right-side QDFrATs are respectively

$$\mathbf{X}_{\alpha,\beta}^{\mu} = \mathbf{\Phi}_N^{\mu,\alpha,\beta}\mathbf{x}_q \tag{4}$$

$$\mathbf{X}'^{\mu}_{\alpha,\beta} = (\mathbf{x}_q)^{\mathrm{T}}\mathbf{\Phi}_N^{\mu,\alpha,\beta} \tag{5}$$

where the kernel matrix $\mathbf{\Phi}_N^{\mu,\alpha,\beta}$ of the QDFrAT is

$$\mathbf{\Phi}_N^{\mu,\alpha,\beta} = \mathbf{V}_N^{\beta}\mathbf{D}_N^{\mu,\alpha}(\mathbf{V}_N^{\beta})^{\mathrm{T}}$$

$$= \mathbf{V}_N^{\beta}\,\mathrm{diag}\left\{1,\ \exp\left(-\frac{2\mu\pi\alpha}{T}\right),\ \exp\left(-\frac{4\mu\pi\alpha}{T}\right),\ \ldots,\ \exp\left(-\frac{2(N-1)\mu\pi\alpha}{T}\right)\right\}(\mathbf{V}_N^{\beta})^{\mathrm{T}} \tag{6}$$

Unlike $\mathbf{\Phi}_N^{\alpha,\beta}$, the complex number $i$ is replaced by a quaternion number $\mu$.

The QDFrAT is designed to enhance the robustness and the security with parameters $\beta$ and $\alpha$, respectively.

### 2.2. Quaternion singular value decomposition

Suppose $Q \in \mu^{m\times n}$ is a quaternion matrix, where $\mu^{m\times n}$ is a set of quaternion matrices. Then $U = U_0 + U_1\mathbf{i} + U_2\mathbf{j} + U_3\mathbf{k} \in \mu^{m\times n}$ and $V = V_0 + V_1\mathbf{i} + V_2\mathbf{j} + V_3\mathbf{k} \in \mu^{m\times n}$ are two unitary quaternion matrices such that [17]

$$Q = U\Sigma V^*, \qquad \Sigma = \begin{bmatrix}\Sigma_1 & 0\\ 0 & 0\end{bmatrix} \tag{7}$$

where $V^* = V_0^{\mathrm{T}} - V_1\mathbf{i} - V_2\mathbf{j} - V_3\mathbf{k}$ represents the conjugate transpose of $V$, $\Sigma_1 = \mathrm{diag}(\sigma_1, \sigma_2, \ldots, \sigma_r)$, $\sigma_1 \geq \sigma_2 \geq \ldots \geq \sigma_r > 0$, and $\sigma_1, \sigma_2, \ldots, \sigma_r$ are the positive singular values of $Q$, and $r$ is the rank of matrix $Q$.

The QSVD will be performed to obtain the singular values matrices of the encryption watermark image and the host image by the SVD in the MATLAB Toolbox [18].

### 2.3. Genetic algorithm

In the proposed watermarking scheme, the optimal scaling factor $k$ and the optimal transform angle $\beta$ can be obtained with the genetic algorithm (GA), respectively. The fitness function of the GA is

$$\max\left\{\frac{1}{R}\sum_{t=1}^{R}\mathrm{NC}(\mathbf{W}, \mathbf{W}_{\mathrm{e}}) + \eta\,\mathrm{PSNR}(\mathbf{I}, \mathbf{I}_{\mathrm{w}}) + \frac{1}{R}\sum_{t=1}^{R}\mathrm{SSIM}(\mathbf{I}, \mathbf{I}_{\mathrm{w}})\right\} \tag{8}$$

where peak signal-to-noise ratio (PSNR) and structural similarity index measure (SSIM) are two important measures to evaluate the imperceptibility of the watermarked host image $\mathbf{I}_w$. $\mathbf{I}$ denotes the original host image. Normalized cross-correlation (NC) between the original watermark $\mathbf{W}$ and the extracted watermark $\mathbf{W}_e$ is a valid indicator to assess the robustness of the watermarking algorithm; $\eta$ is the weight coefficient; $R$ represents the number of the tested attacks.

PSNR is defined as

$$\mathrm{PSNR} = 10\lg\frac{255^2\times 3\times M\times M}{\sum_{z=1}^{3}\sum_{x=1}^{M}\sum_{y=1}^{M}\left[\mathbf{I}(x,y,z)-\mathbf{I}_w(x,y,z)\right]^2} \tag{9}$$

where $z$ taking 1, 2, 3 denotes the R, G, B components, respectively, $M\times M$ is the size of host image, $\mathbf{I}(x, y, z)$ and $\mathbf{I}_w(x, y, z)$ are the gray values of the pixel $(x, y)$ of component $z$ in the original host image and the corresponding watermarked host image, respectively. SSIM is described as

$$\mathrm{SSIM} = \frac{(2\mu_I\mu_{I_w}+b_1)(2\sigma_{II_w}+b_2)}{(\mu_I^2+\mu_{I_w}^2+b_1)(\sigma_I^2\sigma_{I_w}^2+b_2)} \tag{10}$$

where $\mu_I$ and $\mu_{I_w}$ represent the average pixel values of $\mathbf{I}$ and $\mathbf{I}_w$, respectively, $\sigma_I$ and $\sigma_{I_w}$ denote the standard deviations of $\mathbf{I}$ and $\mathbf{I}_w$, respectively, and $\sigma_{II_w}$ is the covariance between $\mathbf{I}$ and $\mathbf{I}_w$. What is more, $b_1 = (k_1L)^2$, $b_2 = (k_2L)^2$, $k_1 = 0.01$, $k_2 = 0.03$, $L$ represents the gray level of the original host image. NC is calculated as

$$\mathrm{NC} = \frac{\sum_{z=1}^{3}\sum_{x=1}^{N}\sum_{y=1}^{N}\mathbf{W}(x,y,z)\mathbf{W}_e(x,y,z)}{\sqrt{\sum_{z=1}^{3}\sum_{x=1}^{N}\sum_{y=1}^{N}\mathbf{W}^2(x,y,z)}\sqrt{\sum_{z=1}^{3}\sum_{x=1}^{N}\sum_{y=1}^{N}\mathbf{W}_e^2(x,y,z)}} \tag{11}$$

where $N\times N$ is the size of watermark image. $\mathbf{W}(x, y, z)$ and $\mathbf{W}_e(x, y, z)$ are the gray values of the pixel $(x, y)$ of component $z$ in the original watermark and the corresponding extracted watermark, respectively.

Take the parameter $k$ as an example, the detailed GA-based optimization process is displayed in Fig. 1, and the optimal transform angle $\beta$ can also be acquired by the same process. Noise attacks include salt-and-pepper noise attack, Gaussian noise attack and Speckle noise attack. Gaussian low-pass filtering attack and median filtering attack are also tested in the optimization process.

## 3. Proposed color image watermarking algorithm

As illustrated in Fig. 2, the image watermarking algorithm based on the QDFrAT and the GA is detailed as follows.

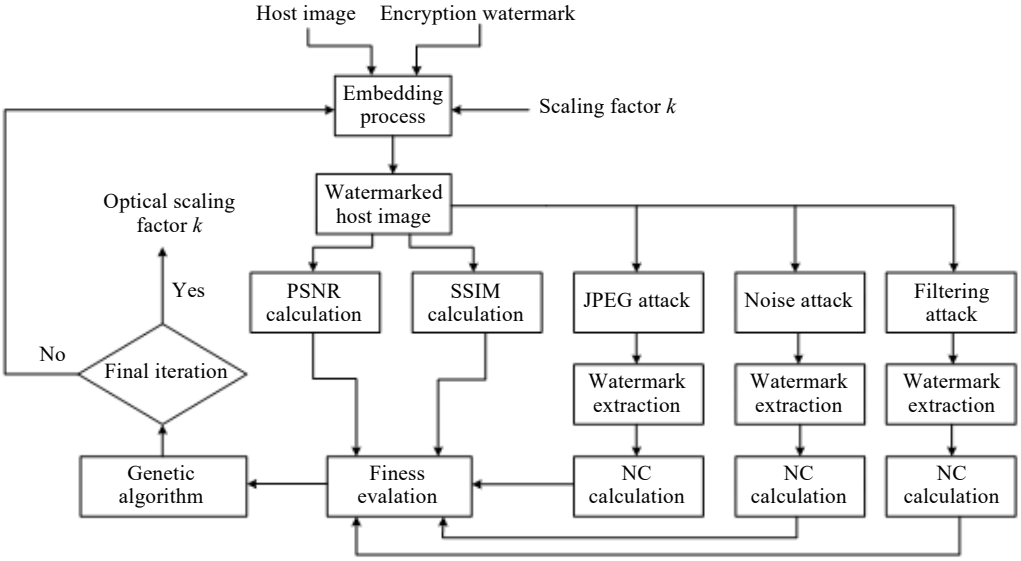



Fig. 1. GA-based optimization process of the scaling factor *k*.

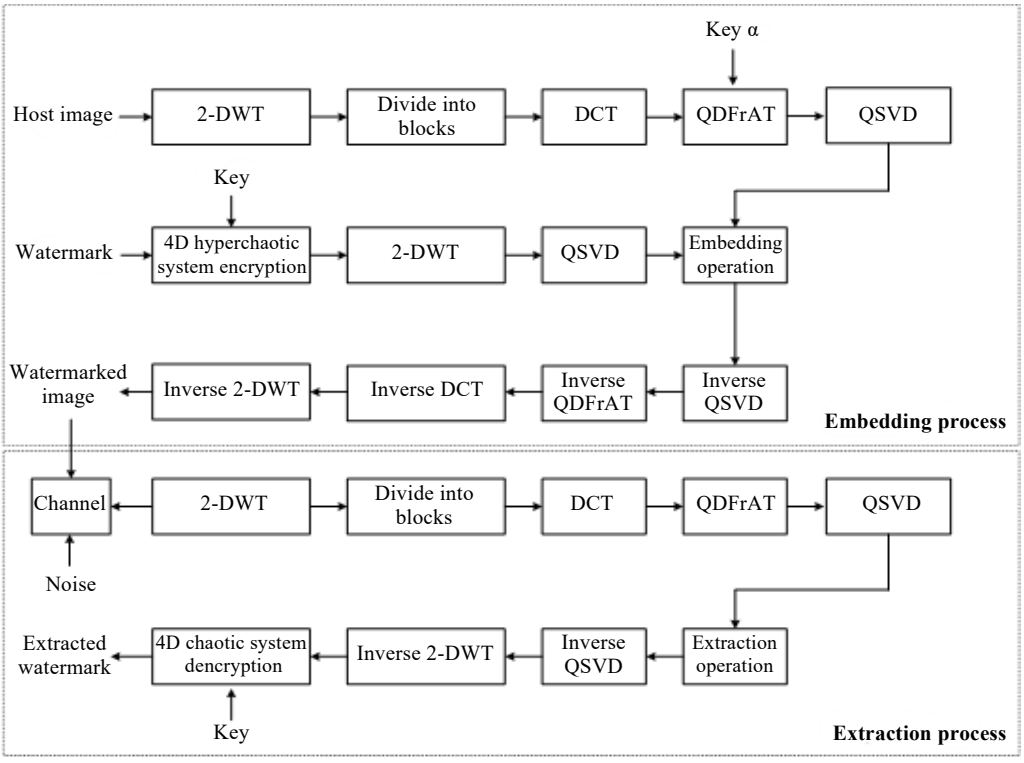



Fig. 2. Embedding and extraction processes.

### 3.1. Watermark preprocessing

During watermark preprocessing, hyperchaotic encryption is a reliable way to enhance security. The detailed steps of watermark preprocessing are shown as follows.

1) The original color watermark image $\mathbf{W}$ of size $N \times N$ is divided into three color components, then these components are transformed into the corresponding 1D column vectors $\mathbf{R}'_{\mathrm{w}}$, $\mathbf{G}'_{\mathrm{w}}$, and $\mathbf{B}'_{\mathrm{w}}$.

2) A classical Lorenz hyperchaotic system is expressed as [19]

$$\begin{cases} \dot{x} = a(y-x)+w \\ \dot{y} = cx-y-xz \\ \dot{z} = xy-bz \\ \dot{w} = -yz+rw \end{cases} \tag{12}$$

where $a = 10$, $b = 8/3$, $c = 28$, $r = -1$, and the initial values $u_1$, $u_2$, $u_3$, $u_4$ are set as (1.1, 2.2, 3.3, 4.4). The hyperchaotic system can be solved with the classical one-step fourth-order Runge-Kutta method, and a hyperchaotic float sequence $S$ is obtained.

3) $S$ is converted into an integer sequence $I$, which is less than $10N$, then $I$ is split into two parts $I_1$ and $I_2$ on average.

$$I = \mathrm{mod}\left\{\mathrm{floor}\left[10^{10}(S+100)\right], 10N\right\}+1 \tag{13}$$

4) The coordinate conversion is described as

$$q = \mathrm{mod}\left[I_2(i)+I_1(i)\times i, \quad N\times N\right] \tag{14}$$

where the pixel position before transform $i$ varies from 1 to $N \times N$ and $q$ is the pixel position after transform. The pixel values of $\mathbf{R}'_{\mathrm{w}}$, $\mathbf{G}'_{\mathrm{w}}$, and $\mathbf{B}'_{\mathrm{w}}$ are substituted in order with the following rule:

$$\mathbf{R}'_{\mathrm{w}}(i) \leftrightarrow \mathbf{R}'_{\mathrm{w}}(q) \tag{15}$$

$$\mathbf{G}'_{\mathrm{w}}(i) \leftrightarrow \mathbf{G}'_{\mathrm{w}}(q) \tag{16}$$

$$\mathbf{B}'_{\mathrm{w}}(i) \leftrightarrow \mathbf{B}'_{\mathrm{w}}(q) \tag{17}$$

5) The scrambled matrices $\mathbf{R}^*_{\mathrm{w}}$, $\mathbf{G}^*_{\mathrm{w}}$, and $\mathbf{B}^*_{\mathrm{w}}$ of size $N \times N$ can be obtained by converting the substituted vectors $\mathbf{R}'_{\mathrm{w}}$, $\mathbf{G}'_{\mathrm{w}}$, and $\mathbf{B}'_{\mathrm{w}}$, then the encryption watermark image $\mathbf{W}'$ is reconstructed with the three scrambled matrices.

### 3.2. Watermark embedding

1) The color host image $\mathbf{I}$ of size $M \times M$ and $\mathbf{W}'$ are separated into color components $\mathbf{R}_1$, $\mathbf{G}_1$, $\mathbf{B}_1$, $\mathbf{R}_2$, $\mathbf{G}_2$, and $\mathbf{B}_2$.

2) With the 2D DWT, the six color components are converted into $\{\mathbf{LL}^{R_1}, \mathbf{LH}^{R_1}, \mathbf{HL}^{R_1}, \mathbf{HH}^{R_1}\}$, $\{\mathbf{LL}^{G_1}, \mathbf{LH}^{G_1}, \mathbf{HL}^{G_1}, \mathbf{HH}^{G_1}\}$, $\{\mathbf{LL}^{B_1}, \mathbf{LH}^{B_1}, \mathbf{HL}^{B_1}, \mathbf{HH}^{B_1}\}$, $\{\mathbf{LL}^{R_2}, \mathbf{LH}^{R_2}, \mathbf{HL}^{R_2}, \mathbf{HH}^{R_2}\}$, $\{\mathbf{LL}^{G_2}, \mathbf{LH}^{G_2}, \mathbf{HL}^{G_2}, \mathbf{HH}^{G_2}\}$, $\{\mathbf{LL}^{B_2}, \mathbf{LH}^{B_2}, \mathbf{HL}^{B_2}, \mathbf{HH}^{B_2}\}$, respectively.

3) $\mathbf{LL}^{R_1}$, $\mathbf{LL}^{G_1}$, and $\mathbf{LL}^{B_1}$ are divided into $M/N \times M/N$ non-overlapping blocks. Each block is executed by the DCT, then three new matrices $\mathbf{M}_\mathrm{R}$, $\mathbf{M}_\mathrm{G}$ and $\mathbf{M}_\mathrm{B}$ are constructed with the upper left coefficient of each block. Afterward, a pure quaternion matrix $\mathbf{M}$ can be obtained.

$$\mathbf{M} = \mathbf{M}_\mathrm{R}\mathbf{i} + \mathbf{M}_\mathrm{G}\mathbf{j} + \mathbf{M}_\mathrm{B}\mathbf{k} \tag{18}$$

4) $\mathbf{M}_1$ is acquired by operating the QDFrAT on $\mathbf{M}$ with $\alpha$ and $\beta$, where the fractional order $\alpha$ is the secret key while the optimal transform angle $\beta$ can be obtained by the GA.

$$\mathbf{M}_1 = \mathrm{QDFrAT}(\mathbf{M}, \alpha, \beta) \tag{19}$$

5) $\mathbf{LL}^{R_2}$, $\mathbf{LL}^{G_2}$, and $\mathbf{LL}^{B_2}$ and are chosen to form a pure quaternion matrix $\mathbf{W}^*$ and three matrices $\mathbf{U}_\mathrm{w}$, $\mathbf{S}_\mathrm{w}$ and $\mathbf{V}_\mathrm{w}$ can be obtained by performing the QSVD on $\mathbf{W}^*$.

$$\left[\mathbf{U}_\mathrm{w} \quad \mathbf{S}_\mathrm{w} \quad \mathbf{V}_\mathrm{w}^\mathrm{T}\right] = \mathrm{QSVD}(\mathbf{W}^*) \tag{20}$$

6) Matrix $\mathbf{M}_1$ is decomposed into three matrices $\mathbf{U}_\mathrm{m}$, $\mathbf{S}_\mathrm{m}$ and $\mathbf{V}_\mathrm{m}$ by the QSVD.

$$\left[\mathbf{U}_\mathrm{m} \quad \mathbf{S}_\mathrm{m} \quad \mathbf{V}_\mathrm{m}^\mathrm{T}\right] = \mathrm{QSVD}(\mathbf{M}_1) \tag{21}$$

7) The singular value matrix $\mathbf{S}_\mathrm{w}$ is embedded into $\mathbf{S}_\mathrm{m}$ with the optimal scaling factor $k$ produced by the GA, and the singular value matrix $\mathbf{S}$ of the watermarked image $\mathbf{I}_\mathrm{w}$ is acquired.

$$\mathbf{S} = \mathbf{S}_\mathrm{m} + k\,\mathbf{S}_\mathrm{w} \tag{22}$$

8) Matrix $\mathbf{M}_2$ can be generated by the matrices $\mathbf{U}_\mathrm{m}$, $\mathbf{S}$ and $\mathbf{V}_\mathrm{m}$.

$$\mathbf{M}_2 = \mathbf{U}_\mathrm{m}\,\mathbf{S}\,\mathbf{V}_\mathrm{m}^\mathrm{T} \tag{23}$$

9) $\mathbf{M}_2$ is executed by the inverse QDFrAT (IQDFrAT), and then the matrix $\mathbf{M}_3$ is

$$\mathbf{M}_3 = \mathrm{IQDFrAT}(\mathbf{M}_2, -\alpha, \beta) \tag{24}$$

10) $\mathbf{M}_3$ is returned to each block, then the new sub-bands $\mathbf{LL}_\mathrm{w}^{R_1}$, $\mathbf{LL}_\mathrm{w}^{G_1}$ and $\mathbf{LL}_\mathrm{w}^{B_1}$ are gained by operating the inverse DCT (IDCT) on each block.

11) The watermarked host image $\mathbf{I}_\mathrm{w}$ can be obtained by executing the inverse DWT (IDWT) on $\mathbf{LL}_\mathrm{w}^{R_1}$, $\mathbf{LL}_\mathrm{w}^{G_1}$ and $\mathbf{LL}_\mathrm{w}^{B_1}$.

### 3.3. Watermark extraction

1) The watermarked image $\mathbf{I}_\mathrm{w}$ is split into three color components $\mathbf{R}_1^*$, $\mathbf{G}_1^*$, and $\mathbf{B}_1^*$.

2) Low-frequency sub-bands $\mathbf{LL}_\mathrm{R}^*$, $\mathbf{LL}_\mathrm{G}^*$ and $\mathbf{LL}_\mathrm{B}^*$ are obtained by performing the 2D DWT on the three components.

3) $\mathbf{LL}_{\mathrm{R}}^{*}$, $\mathbf{LL}_{\mathrm{G}}^{*}$ and $\mathbf{LL}_{\mathrm{B}}^{*}$ are divided into $M/N \times M/N$ blocks. Each block is transformed by the DCT, then the upper left coefficient is chosen to construct three matrices $\mathbf{M}_{\mathrm{R}}^{*}$, $\mathbf{M}_{\mathrm{G}}^{*}$ and $\mathbf{M}_{\mathrm{B}}^{*}$, respectively. A pure quaternion matrix $\mathbf{M}^{*}$ can be acquired eventually.

$$\mathbf{M}^{*} = \mathbf{M}_{\mathrm{R}}^{*}\mathbf{i} + \mathbf{M}_{\mathrm{G}}^{*}\mathbf{j} + \mathbf{M}_{\mathrm{B}}^{*}\mathbf{k} \tag{25}$$

4) Matrix $\mathbf{M}_{1}^{*}$ can be obtained by performing the QDFrAT on $\mathbf{M}^{*}$ with $\alpha$ and $\beta$.

$$\mathbf{M}_{1}^{*} = \mathrm{QDFrAT}(\mathbf{M}^{*}, \alpha, \beta) \tag{26}$$

5) Matrix $\mathbf{M}_{1}^{*}$ is decomposed into three matrices $\mathbf{U}_{\mathrm{m}}^{*}$, $\mathbf{S}'$ and $\mathbf{V}_{\mathrm{m}}^{*}$ by the QSVD.

$$\left[\mathbf{U}_{\mathrm{m}}^{*} \quad \mathbf{S}' \quad \mathbf{V}_{\mathrm{m}}^{*\,\mathrm{T}}\right] = \mathrm{QSVD}(\mathbf{M}_{1}^{*}) \tag{27}$$

6) With $k$ and $\mathbf{S}_{\mathrm{w}}$, the diagonal matrix $\mathbf{S}^{*}$ of the encryption watermark is obtained.

$$\mathbf{S}^{*} = \frac{\mathbf{S}' - \mathbf{S}_{\mathrm{w}}}{k} \tag{28}$$

7) Matrix $\mathbf{M}_{2}^{*}$ can be acquired by the matrices $\mathbf{U}_{\mathrm{w}}$, $\mathbf{S}^{*}$ and $\mathbf{V}_{\mathrm{w}}$.

$$\mathbf{M}_{2}^{*} = \mathbf{U}_{\mathrm{w}}\mathbf{S}^{*}\mathbf{V}_{\mathrm{w}}^{\mathrm{T}} \tag{29}$$

8) Matrix $\mathbf{M}_{3}^{*}$ is obtained by performing the IQDFrAT on $\mathbf{M}_{2}^{*}$.

$$\mathbf{M}_{3}^{*} = \mathrm{IQDFrAT}(\mathbf{M}_{2}^{*}, -\alpha, \beta) \tag{30}$$

9) After $\mathbf{M}_{3}^{*}$ is returned to each block, each block is performed by the IDCT to generate the new sub-bands $\mathbf{LL}_{1}^{R_1}$, $\mathbf{LL}_{1}^{G_1}$ and $\mathbf{LL}_{1}^{B_1}$.

10) The encryption watermark image $\mathbf{W}_{1}$ can be produced by performing the IDWT on $\mathbf{LL}_{1}^{R_1}$, $\mathbf{LL}_{1}^{G_1}$ and $\mathbf{LL}_{1}^{B_1}$.

11) Hyperchaotic decryption operations are reversed from the hyperchaotic encryption process in Section 3.1, and the extracted watermark image $\mathbf{W}_{\mathrm{e}}$ can be decrypted.

## 4. Experiment results and analysis

As shown in Fig. 3, the original host images are four RGB images of size 512×512, which are chosen from the USC-SIPI image database [20], and their bit depth is 24-bit. Furthermore, these images are representative, including the characteristics of texture, edge and smoothness, while the RGB image of size 64×64 and of bit depth 24-bit is selected as the original watermark. The simulation is implemented by a personal computer with Core i7, CPU @ 2.8GHz, 16 GB RAM, Windows 10 and MATLAB R2018b. The fractional order $\alpha$ is set as 0.1234. For the host images in Figs. 3(a)–(d), the values of the corresponding optimal embedding strength $k$ obtained by the GA are 0.1708,

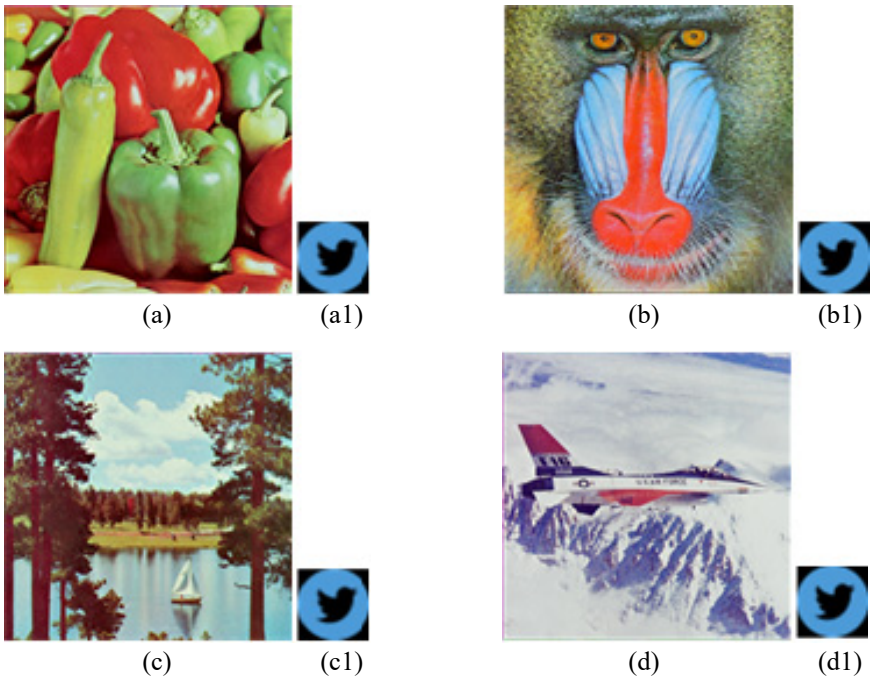
(a) (b) (c) (d) (e)

Fig. 3. Original test images: (a) *Peppers*, (b) *Baboon*, (c) *Sailboat*, (d) *Airplane*, and (e) watermark.

0.1538, 0.1660 and 0.1816, respectively, while the values of the corresponding optimal transform angle $\beta$ are 2.7856°, 3.3615°, 1.8897° and 2.5715°, respectively.

### 4.1. Imperceptibility

By comparing Figs. 4(a)–(d) with Figs. 3(a)–(d), there exists no noticeable difference between the original host images and the watermarked host ones visually. It is feasible to extract the watermarks from the watermarked images with the proposed watermarking scheme, as shown in Figs. 4(a1)–(d1).



(a) (a1) (b) (b1)

(c) (c1) (d) (d1)

Fig. 4. Results of embedding and extraction processes: (a)–(d) watermarked *Peppers*, *Baboon*, *Sailboat* and *Airplane*, (a1)–(d1) corresponding extracted watermark images without attack.

T a b l e 1. PSNR values and SSIM values of the watermarked host images, and NC values of the extracted watermarks without attack.

| Images | PSNR | SSIM | NC |
|---|---|---|---|
| *Peppers* | 45.0443 | 0.9883 | 0.9998 |
| *Baboon* | 45.2271 | 0.9965 | 1 |
| *Sailboat* | 45.3151 | 0.9930 | 1 |
| *Airplane* | 44.2376 | 0.9907 | 1 |

PSNR values and SSIM values of the four watermarked host images and their corresponding extracted watermarks without attack are compiled in Table 1. The PSNR values are higher than 40 dB, and the SSIM values are greater than 0.9880. Therefore, the imperceptibility of the proposed watermarking scheme can be guaranteed. On the other hand, the NC values in Table 1 verify that the watermark extraction process is valid.

Figures 5(a)–(d) and (e)–(h) display the histograms of color components in the original host images and the corresponding watermarked host ones, respectively. The histo-

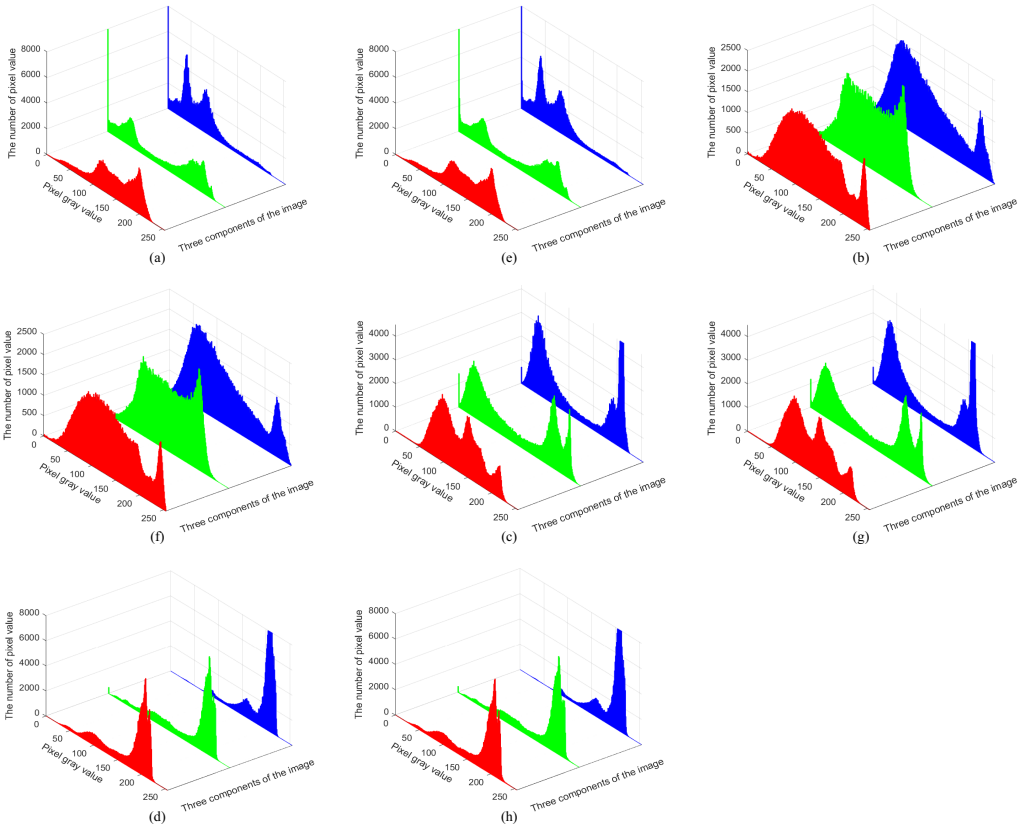



Fig. 5. Histograms: (a)–(d) *Peppers*, *Baboon*, *Sailboat*, and *Airplane*, (e)–(h) watermarked *Peppers*, *Baboon*, *Sailboat*, and *Airplane*.

grams of the original host images and the corresponding watermarked ones are similar. Consequently, the proposed scheme has a good imperceptibility and can withstand the statistical analysis attack.

### 4.2. Security

Take the color host image *Sailboat* as an example, if only one key is slightly modified and the other keys are intact, the decryption watermark images are shown in Figs. 6(b)–(e). Since the above decryption watermarks are hard to recognize, the extracted watermark can be correctly decrypted only with all the right keys, as shown in Fig. 6(f). Whatis more, to improve the security of the proposed watermarking scheme further, the coefficients of the host image in the transform domain are encrypted by the QDFrAT.

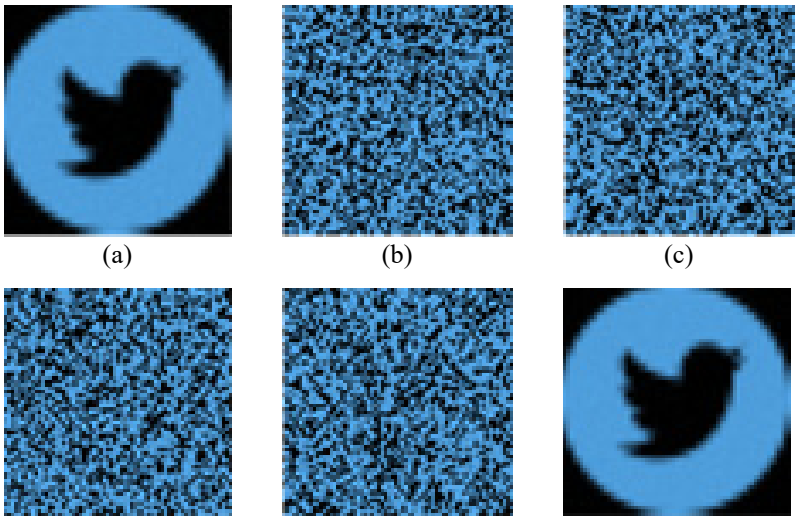



Fig. 6. (a) Original watermark image, (b)–(f) decryption watermark images with $u_1 + 10^{-13}$, $u_2 + 10^{-14}$, $u_3 + 10^{-14}$, $u_4 + 10^{-11}$ and all the right keys, respectively.

### 4.3. Robustness

JPEG compression attack, salt-and-pepper noise attack, Gaussian noise attack, Speckle noise attack, scaling attack, rotation attack, cutting attack, filtering attack, brightness change attack and contrast variation attack are also evaluated, as shown in Figs. 7–12. For all tested watermarked images, NC values between the original watermarks and the extracted ones are displayed in Tables 2–7.

#### 4.3.1. JPEG compression attack

The watermarked image is executed with the JPEG compression of quality factors 90, 60 and 30, and the attacked results are shown in Fig. 7. Table 2 exhibits the corre-

(a) (a1) (b) (b1) (c) (c1)

Fig. 7. Results of JPEG compression attack. (a)–(c) Watermarked host images *Airplane* with quality factors 90, 60, and 30, repectively. (a1)–(c1) Extracted watermark images.

T a b l e 2. NC values of the extracted watermarks after JPEG compression attack.

| Quality factor | *Peppers* | *Baboon* | *Sailboat* | *Airplane* |
|---|---|---|---|---|
| 90 | 0.9991 | 0.9998 | 0.9998 | 1 |
| 60 | 0.9989 | 0.9996 | 0.9995 | 0.9998 |
| 30 | 0.9992 | 0.9991 | 0.9994 | 0.9998 |

sponding NC values of the extracted watermarks. When the quality factor of the watermarked images is 30, the watermarks can be still extracted validly and the NC values are all larger than 0.9990. It shows that the proposed watermarking scheme based on the DCT and the block division could stand up to the JPEG compression attack.

#### 4.3.2. Noise attack

Suppose the watermarked host images are attacked by salt-and-pepper noise with intensities 0.01, 0.05 and 0.1, Gaussian noise with variances 0.01, 0.05 and 0.1, and Speckle noise with densities of 0.01, 0.05 and 0.1, respectively. The attacked watermarked images and the extracted watermarks are presented in Fig. 8. And the NC values of the

(a) (a1) (b) (b1) (c) (c1)

Fig. 8. Results of noise attack. Watermarked host images *Airplane*: (a)–(c) salt-and-pepper noise with intensities 0.01, 0.05 and 0.1, respectively, (d)–(f) Gaussian noise with variances 0.01, 0.05 and 0.1, respectively, (g)–(i) Speckle noise with densities 0.01, 0.05 and 0.1, respectively. (a1)–(i1) Corresponding extracted watermark images.

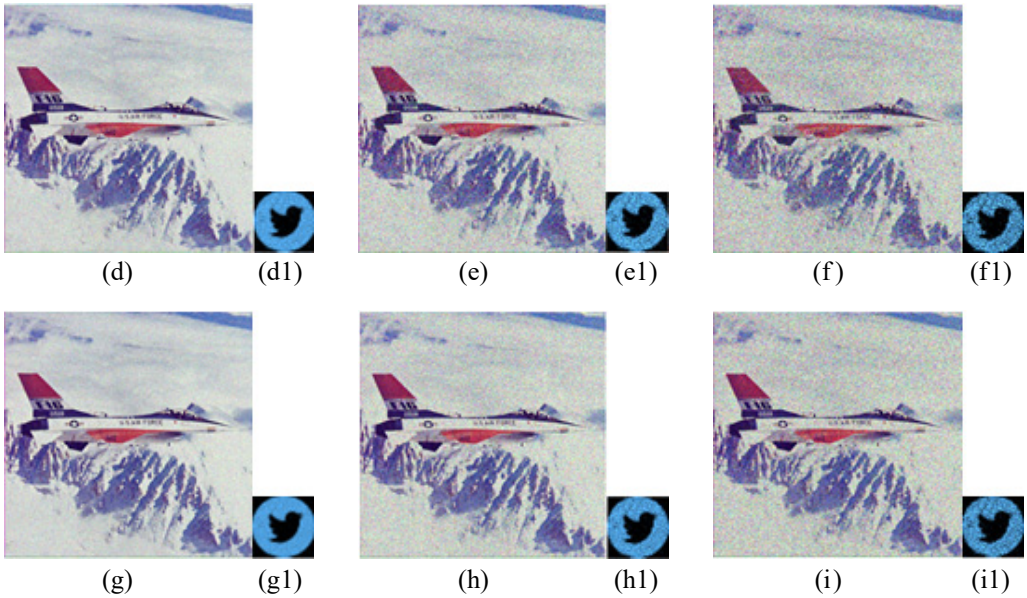



Fig. 8. Continued.

T a b l e 3. NC values of the extracted watermarks after noise attack.

| Noise attack | *Peppers* | *Baboon* | *Sailboat* | *Airplane* |
|---|---|---|---|---|
| Salt-and-pepper noise (0.01) | 0.9996 | 0.9978 | 0.9997 | 0.9996 |
| Salt-and-pepper noise (0.05) | 0.9984 | 0.9976 | 0.9987 | 0.9977 |
| Salt-and-pepper noise (0.1) | 0.9975 | 0.9972 | 0.9976 | 0.9950 |
| Gaussian noise (0.01) | 0.9992 | 0.9985 | 0.9990 | 0.9992 |
| Gaussian noise (0.05) | 0.9961 | 0.9910 | 0.9973 | 0.9857 |
| Gaussian noise (0.1) | 0.9756 | 0.9573 | 0.9875 | 0.9579 |
| Speckle noise (0.01) | 0.9998 | 0.9997 | 0.9997 | 0.9993 |
| Speckle noise (0.05) | 0.9986 | 0.9989 | 0.9986 | 0.9963 |
| Speckle noise (0.1) | 0.9966 | 0.9945 | 0.9968 | 0.9805 |

extracted watermarks are displayed in Table 3. It is shown that the designed watermarking algorithm can resist the noise attack, since the NC values are all above 0.9550.

#### 4.3.3. Scaling attack

Figure 9 depicts the test results of the attacks with scaling 0.5 and scaling 2. Furthermore, the NC values of the corresponding extracted watermarks are shown in Table 4. All the NC values are over 0.9980, implying the watermarks can be well extracted from the attacked host images. The embedding information is the singular value of the encryption watermark, resulting in the watermarking system owning a better stability.


(a) (a1) (b) (b1)

Fig. 9. Results of scaling attack. Watermarked host images *Airplane*: (a), (b) with scaling 0.5 and 2, respectively. (a1), (b1) Extracted watermark images.

T a b l e 4. NC values of the extracted watermarks after scaling attack.

| Scaling attack | *Peppers* | *Baboon* | *Sailboat* | *Airplane* |
|---|---|---|---|---|
| Scaling 0.5 | 0.9983 | 0.9994 | 0.9993 | 0.9985 |
| Scaling 2 | 0.9993 | 0.9997 | 0.9997 | 0.9998 |

Consequently, the proposed method based on the QSVD has a good performance in defending the scaling attack.

#### 4.3.4. Cutting attack

Cutting attack is performed on the watermarked host images, including 1/8 center cutting, 1/8 left upper corner cutting, 1/8 row cutting and 1/8 column cutting. The attacked watermarked images and the corresponding extracted watermarks are presented in Fig. 10. In addition, all the NC values of the extracted watermarks are illustrated in Table 5. When confronting different kinds of cutting attacks, the extracted watermarks can still be identified by the human visual system and the NC values of the extracted watermarks are larger than 0.8090. It mostly benefits from the watermark preprocessed by the hyperchaotic encryption, which reduces the correlation between the adjacent pixels of the watermark image. Hence, the proposed color image watermarking scheme based on hyperchaotic encryption is robust against the cutting attack.

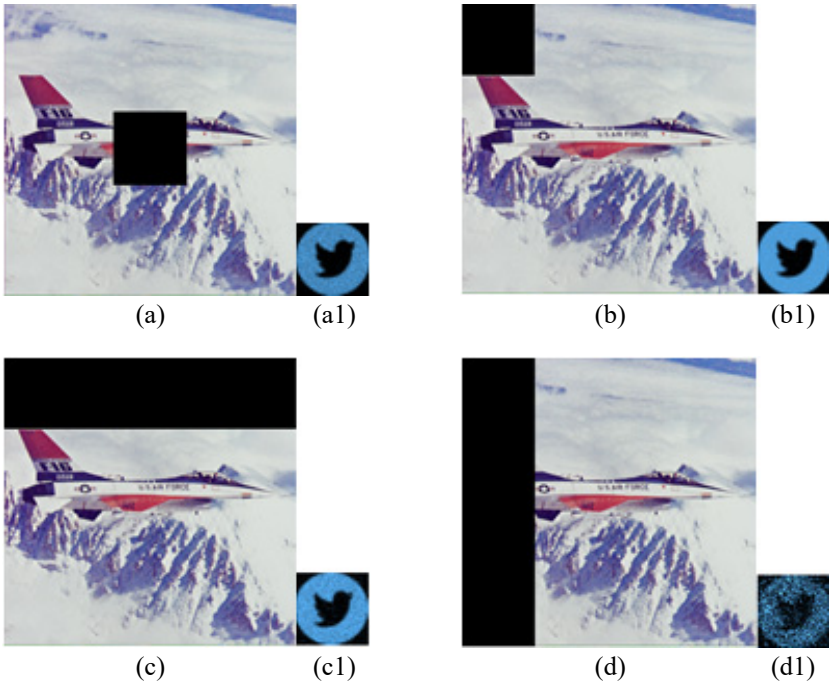



Fig. 10. Results of cutting attack. Watermarked host images *Airplane*: (a) with 1/8 center cutting, (b) 1/8 left upper corner cutting, (c) 1/8 row cutting and (d) 1/8 column cutting. (a1)–(d1) Extracted watermark images.

T a b l e 5. NC values of the extracted watermarks after cutting attack.

| Cutting attack | *Peppers* | *Baboon* | *Sailboat* | *Airplane* |
|---|---|---|---|---|
| 1/8 center cutting | 0.9988 | 0.9989 | 0.9977 | 0.9981 |
| 1/8 left upper corner cutting | 0.9991 | 0.9966 | 0.9978 | 0.9999 |
| 1/8 row cutting | 0.8718 | 0.8396 | 0.8093 | 0.9907 |
| 1/8 column cutting | 0.9316 | 0.8978 | 0.8831 | 0.8945 |

#### 4.3.5. Transform attacks of brightness and contrast

Simulation results on brightness change attack and contrast variation attack are demonstrated in Fig. 11 and Table 6. Figure 11 shows that transform attack affects the extracted watermarks slightly. However, the NC values in Table 6 indicate that the proposed watermarking method could withstand the above transform attacks effectively.

#### 4.3.6. Other common attacks

Other common attacks are also executed on the watermarked host images and the corresponding experimental results are displayed in Table 7 and Fig. 12. The robustness

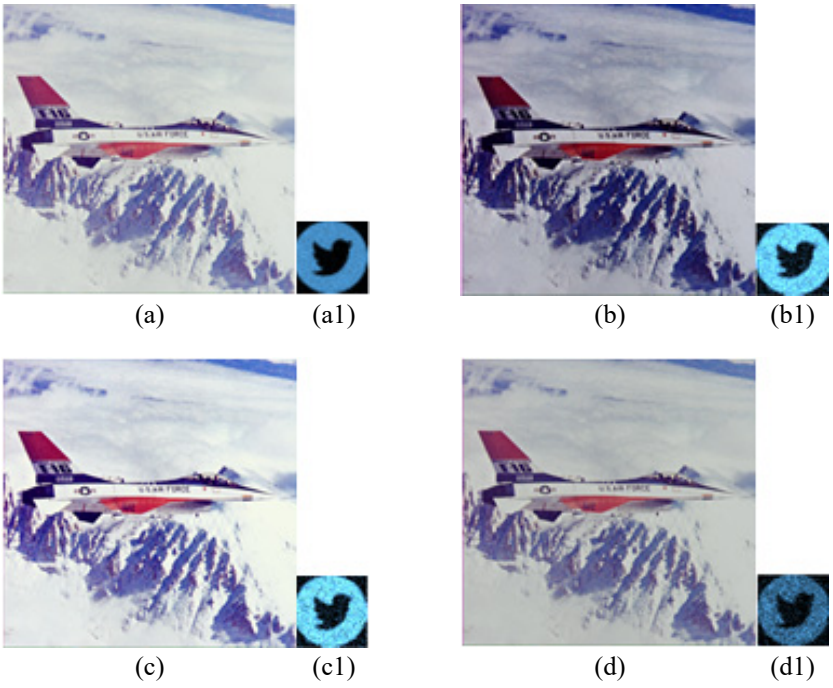



Fig. 11. Results of transform attack. Watermarked host images *Airplane*: (a) with image brightening, (b) image darkening, (c) contrast enhancement and (d) contrast weakening. (a1)–(d1) Corresponding extracted watermark images.

T a b l e 6. NC values of the extracted watermarks after transform attack

| Transform attack | *Peppers* | *Baboon* | *Sailboat* | *Airplane* |
|---|---|---|---|---|
| Image brightening | 0.9999 | 0.9990 | 0.9998 | 0.9984 |
| Image darkening | 0.9987 | 0.9967 | 0.9980 | 0.9939 |
| Contrast enhancement | 0.9882 | 0.9610 | 0.9638 | 0.9754 |
| Contrast weakening | 0.9791 | 0.9379 | 0.9277 | 0.9949 |

T a b l e 7. NC values of the extracted watermarks after other attacks.

| Attack | *Peppers* | *Baboon* | *Sailboat* | *Airplane* |
|---|---|---|---|---|
| Histogram equalization | 0.9982 | 0.9344 | 0.9953 | 0.9066 |
| Motion blur | 0.9892 | 0.9327 | 0.9782 | 0.9993 |
| Gaussian low-pass filtering 3×3 | 0.9978 | 0.9974 | 0.9979 | 0.9986 |
| Median filtering 3×3 | 0.9965 | 0.9986 | 0.9982 | 0.9967 |

of the proposed digital image watermarking scheme is acceptable, since the NC values of the extracted watermarks are all larger than 0.9000.

According to the above simulation results on the robustness, the proposed color image watermarking algorithm could be effectively resistant to the different attacks.

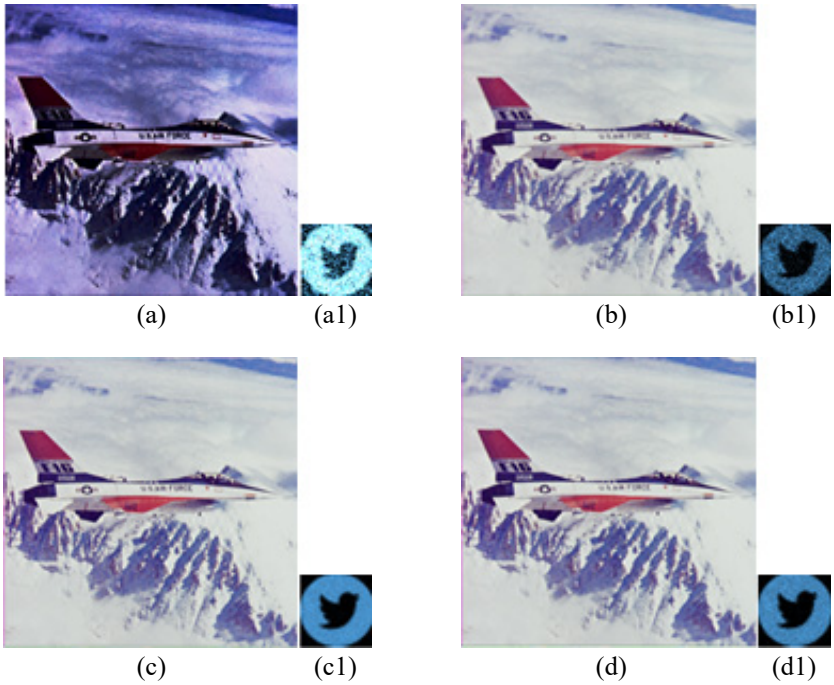


Fig. 12. Results of other attacks. Watermarked host images *Airplane*: (a) with histogram equalization, (b) motion blur, (c) Gaussian low-pass filtering and (d) median filtering. (a1)–(d1) Corresponding extracted watermark images.

### 4.4. Embedding capacity

The embedding capacities of the schemes in [3,5] and the proposed scheme are collected in Table 8. Since the embedded watermark is a 24-bit color image, while the watermarks of the other schemes are binary, the embedding capacity of our proposed scheme is higher than the other two schemes listed in Table 8.

T a b l e 8. Comparison of embedding capacity (bit/pixel).

| Scheme | Watermark image | Host image | Embedding capacity |
|---|---|---|---|
| [3] | 64×64 | 512×512×3 | 0.0052 |
| [5] | 64×64 | 512×512×3 | 0.0052 |
| Proposed scheme | 64×64×24 | 512×512×3 | 0.1250 |

### 4.5. Robustness comparison

The PSNR value of the watermarked host image in the proposed scheme is 45.2271 dB, which is larger than 36.4600 dB [3] and 43.2199 dB [5], thus the imperceptibility of this scheme is the best. The NC values after different attacks are displayed in Table 9. Obviously, most of the NC values of the extracted watermarks are higher than those

T a b l e 9. Comparison of NC values.

| Attack | [3] | [5] | Proposed scheme |
|---|---|---|---|
| No attack | 0.9819 | 1 | 1 |
| Salt-and-pepper noise (0.01) | 0.9547 | 0.9890 | 0.9978 |
| Gaussian noise (0.01) | 0.8550 | 0.9886 | 0.9985 |
| JPEG compression (30) | 0.9562 | 0.7614 | 0.9991 |
| JPEG compression (60) | 0.9916 | 0.8456 | 0.9996 |
| Median filtering (3×3) | 0.8652 | 0.9880 | 0.9986 |
| Gaussian low-pass filtering (3×3) | 0.9958 | 0.9968 | 0.9974 |
| Image brightening | 0.9634 | 0.9987 | 0.9990 |
| Image darkening | 0.9611 | 0.9921 | 0.9967 |
| Scaling 0.5 | 0.8936 | 0.9778 | 0.9994 |
| Histogram equalization | 0.9097 | 0.9987 | 0.9344 |

of the other two algorithms mentioned. It indicates that the proposed watermarking algorithm performs better under these tested attacks.

## 5. Conclusion

A robust color image watermarking method based on the DWT, the DCT, the QFrAT, the QSVD and the genetic algorithm is put forward. To ensure the security of the embedding information, the original watermark image is encrypted by a hyperchaotic system. Furthermore, the color watermark image can offer a larger embedding capacity for the watermarking scheme. The transform coefficients are encrypted by the QDFrAT and the stability of this scheme is improved by the QSVD further. More importantly, the robustness and the imperceptibility of the watermarked host image are balanced by the GA algorithm. It is demonstrated that the dual color images watermarking scheme is effective and secure against different common attacks, including JPEG compression attack, noise attack, filtering attack, brightness variation attack, contrast change attack, scaling attack, cutting attack, *etc*. The designed watermarking algorithm is non-blind, since the information of the host image is demanded in the watermark extraction process. In the future, a blind dual color images watermarking method based on the quaternion theory will be discussed.

**Acknowledgments**
This work is supported by the National Natural Science Foundation of China (Grant no. 61861029) and the Innovation Special Foundation of Graduate Student of Jiangxi Province (Grant no. YC2021-S148).

## References

[1] SHAO Z.H., SHANG Y.Y., ZENG R., SHU H.Z., COATRIEUX G.N., WU J.S., *Robust watermarking scheme for color image based on quaternion-type moment invariants and visual cryptography*, Signal Processing: Image Communication **48**, 2016: 12-21. https://doi.org/10.1016/j.image.2016.09.001

[2] Pandey M.K., Parmar G., Gupta R., Sikander A., *Lossless robust color image watermarking using lifting scheme and GWO*, International Journal of System Assurance Engineering and Management **11**(2), 2020: 320-331. https://doi.org/10.1007/s13198-019-00859-w

[3] Zhang H., Li Z.Y., Liu X.L., Wang C.P., Wang X.Y., *Robust image watermarking algorithm based on QWT and QSVD using 2D Chebyshev-Logistic map*, Journal of the Franklin Institute **359**(2), 2022: 1755-1781. https://doi.org/10.1016/j.jfranklin.2021.11.027

[4] Sun Y.A., Su Q.T., Wang H.Y., Wang G., *A blind dual color images watermarking based on quaternion singular value decomposition*, Multimedia Tools and Applications **81**(5), 2022: 6091-6113. https://doi.org/10.1007/s11042-021-11815-x

[5] Ahmadi S.B.B., Zhang G.X., Rabbani M., Boukela L., Jelodar H., *An intelligent and blind dual color image watermarking for authentication and copyright protection*, Applied Intelligence **51**(3), 2021: 1701-1732. https://doi.org/10.1007/s10489-020-01903-0

[6] Hamilton W.R., *Elements of Quaternions*, Longmans, Green & Company, London. 1866.

[7] Li J.Z., Lin Q., Yu C.Y., Ren X.C., Li P., *A QDCT- and SVD-based color image watermarking scheme using an optimized encrypted binary computer-generated hologram*, Soft Computing **22**(1), 2018: 47-65. https://doi.org/10.1007/s00500-016-2320-x

[8] Wang C.P., Wang X.Y., Zhang C., Xia Z.Q., *Geometric correction based color image watermarking using fuzzy least squares support vector machine and Bessel K form distribution*, Signal Processing **134**, 2017: 197-208. https://doi.org/10.1016/j.sigpro.2016.12.010

[9] Li D.S., Che X.Y., Luo W., Y. Hu, Wang Y.N., Yu Z.Y., Yuan L.W., *Digital watermarking scheme for colour remote sensing image based on quaternion wavelet transform and tensor decomposition*, Mathematical Methods in the Applied Sciences **42**(14), 2019: 4664-4678. https://doi.org/10.1002/mma.5668

[10] Xia Z.Q., Wang X.Y., Zhou W.J., Li R., Wang C.P., Zhang C., *Color medical image lossless watermarking using chaotic system and accurate quaternion polar harmonic transforms*, Signal Processing **157**, 2019: 108-118. https://doi.org/10.1016/j.sigpro.2018.11.011

[11] Lang J., Zhang Z.G., *Blind digital watermarking method in the fractional Fourier transform domain*, Optics and Lasers in Engineering **53**, 2014: 112-121. https://doi.org/10.1016/j.optlaseng.2013.08.021

[12] Elshazly E.H., Faragallah O.S., Abbas A.M., Ashour M.A., El-Rabaie E.-S.M., Kazemian H., Alshebeili S.A., El-Samie F.E.A., El-sayed H.S., *Robust and secure fractional wavelet image watermarking*, Signal, Image and Video Processing **9**, 2015: 89-98. https://doi.org/10.1007/s11760-014-0684-x

[13] Kim M., Li D., Hong S., *A robust digital watermarking technique for image contents based on DWT-DFRNT multiple transform method*, International Journal of Multimedia and Ubiquitous Engineering **9**(1), 2014: 369-378. https://doi.org/10.14257/ijmue.2014.9.1.34

[14] Liu X.L., Wu Y.F., Zhang H., Wu J.S., Zhang L.M., *Quaternion discrete fractional Krawtchouk transform and its application in color image encryption and watermarking*, Signal Processing **189**, 2021: 108275. https://doi.org/10.1016/j.sigpro.2021.108275

[15] Chen B.J., Zhou C.F., Jeon B., Zheng Y.H., Wang J.W., *Quaternion discrete fractional random transform for color image adaptive watermarking*, Multimedia Tools and Applications **77**(16), 2018: 20809-20837. https://doi.org/10.1007/s11042-017-5511-2

[16] Liu Z.J., Ahmad M.A., Liu S., *A discrete fractional angular transform*, Optics Communications **281**(6), 2008: 1424-1429. https://doi.org/10.1016/j.optcom.2007.11.012

[17] Zhang F.Z., *Quaternions and matrices of quaternions*, Linear Algebra and its Applications **251**, 1997: 21-57. https://doi.org/10.1016/0024-3795(95)00543-9

[18] Sangwine S.J., Le Bihan N., *Quaternion singular value decomposition based on bidiagonalization to a real or complex matrix using quaternion Householder transformations*, Applied Mathematics and Computation **182**(1), 2006: 727-738. https://doi.org/10.1016/j.amc.2006.04.032

[19] WANG X.Y., WANG M.J., *Hyperchaotic Lorenz system*, Acta Physica Sinica **56**(9), 2007: 5136-5141. https://doi.org/10.7498/aps.56.5136

[20] *USI-SIPI image database for research in image processing, image analysis, and machine vision*. http://sipi.usc.edu/database/.2019 (accessed August, 2022).

*Received August 18, 2022*
*in revised form September 21, 2022*