Optica Applicata, Vol. LIV, No. 3, 2024
DOI: 10.37190/oa240312

Corrigendum

Color image encryption with semi-tensor product compressive sensing and quaternion discrete fractional Krawtchouk transform

WEN-JUN YU[1], HONG-XING DING[2], LI-HUA GONG[1], ZHONG-HUA FANG[1,*]

1School of Electronic and Electrical Engineering, Shanghai University of Engineering Science, Shanghai 201620, China

[2]Department of Electronic Information Engineering, Nanchang University, Nanchang 330031, China

[*]Corresponding author: fzhh@sues.edu.cn

Corrigendum 1

In the online version of this article initially published, Eq. (2), (p. 437) was incorrect, and has been corrected as follows:

$$\mathbf{D}_{\mathrm{L}}^{\mu\alpha} = \begin{pmatrix} \exp(-\mu\alpha 0\pi) & 0 & \cdots & 0 \\ 0 & \exp(-\mu\alpha 1\pi) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \exp(-\mu\alpha(N-1)\pi) \end{pmatrix} \tag{2}$$

Corrigendum 2

In the online version of this article initially published, Eq. (4) (p. 437) was incorrect, and has been corrected as follows:

$$\mathbf{D}_{\mathrm{R}}^{\mu\beta} = \begin{pmatrix} \exp(-\mu\beta 0\pi) & 0 & \cdots & 0 \\ 0 & \exp(-\mu\beta 1\pi) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \exp(-\mu\beta(N-1)\pi) \end{pmatrix} \tag{4}$$

Corrigendum 3

In the online version of this article initially published, Eq. (11) (p. 440) was incorrect, and has been corrected as follows:

$$\mathbf{y} = \mathbf{\Phi}_{\mathrm{STP}} \ltimes \mathbf{x} = (\mathbf{\Phi}_{\mathrm{STP}} \otimes I_{P/N})\mathbf{x} = \begin{pmatrix} \Phi_{11} & \cdots & 0 & & \Phi_{1N} & \cdots & 0 \\ \vdots & \ddots & \vdots & \cdots & \vdots & \ddots & \vdots \\ 0 & \cdots & \Phi_{11} & & 0 & \cdots & \Phi_{1N} \\ & \vdots & & \ddots & & \vdots & \\ \Phi_{M1} & \cdots & 0 & & \Phi_{MN} & \cdots & 0 \\ \vdots & \ddots & \vdots & \cdots & \vdots & \ddots & \vdots \\ 0 & \cdots & \Phi_{M1} & & 0 & \cdots & \Phi_{MN} \end{pmatrix} \mathbf{x} \tag{11}$$

Corrigendum 4

In the online version of this article initially published, Ref. [1] (p. 451) was incorrect, and has been corrected as follows:

[1] Hu L.L., Chen M.X., Wang M.M., Zhou N.R., *A multi-image encryption scheme based on block compressive sensing and nonlinear bifurcation diffusion*, Chaos, Solitons & Fractals **188**, 2024: 115521. https://doi.org/10.1016/j.chaos.2024.115521

February 11, 2025

Optica Applicata, Vol. LIV, No. 3, 2024
DOI: 10.37190/oa240312

Color image encryption with semi-tensor product compressive sensing and quaternion discrete fractional Krawtchouk transform

Wen-Jun Yu[1], Hong-Xing Ding[2], Li-Hua Gong[1], Zhong-Hua Fang[1,*]

1School of Electronic and Electrical Engineering, Shanghai University of Engineering Science, Shanghai 201620, China

[2]Department of Electronic Information Engineering, Nanchang University, Nanchang 330031, China

[*]Corresponding author: fzhh@sues.edu.cn

A color image encryption scheme is investigated by integrating the semi-tensor product compressive sensing (STP-CS) with the quaternion discrete fractional Krawtchouk transform (QDFrKT). To process the color components of plaintext image as a whole, the discrete fractional Krawtchouk transform (DFrKT) is popularized into the quaternion domain and the color image is secured by the QDFrKT. The image matrices are compressed with the discrete wavelet transform (DWT) and the STP measurement matrix. Then the compressed matrices represented by quaternion algebra are re-encrypted by the double random phase encoding and the quaternion DFrKT. Subsequently, the nonlinear hyperchaotic Lorenz system is applied to pixel diffusion to obtain the encrypted image. The proposed reconstruction algorithm based on the grouping iterative reweighted least squares (GIRLS) can resume the decryption image with high precision. The efficiency, security and robustness of the image compression encryption algorithm for color images are evaluated.

Keywords: semi-tensor product; compressive sensing; quaternion discrete fractional Krawtchouk transform; chaotic system; image encryption.

1. Introduction

The secure storage and the transmission of color images are becoming increasingly important on the Internet. Numerous color image encryption algorithms have been raised [1-3]. Various kinds of chaos systems have been naturally imported into image encryption algorithms thanks to their pseudo-randomness and unpredictability. Gao *et al*. proposed an image encryption algorithm (IEA) by integrating a chaos system with single channel scrambled diffusion [4], and a fractional chaos system was designed for image encryption with better security [5]. Subsequently, coupled cascaded chaotic sys-

tems and hyperchaotic ones were constructed. For instance, a new image encryption algorithm was designed using a 2D logistic-sine chaotic system combined with dynamic DNA sequence coding [6]. NIE *et al*. introduced an image compression-encryption scheme (ICES) utilizing a nonlinear hyperchaotic system [7]. Additionally, an IEA with a delayed feedback dynamic hybrid coupled map was implemented, where the initial key is associated with the original images using the SHA-512 algorithm [8].

Besides security, storage space and transmission bandwidth are inevitable concerns during image processing. Consequently, it has become popular to compress-and-authenticate or compress-and-encrypt private images simultaneously [9-12]. LIU *et al*. introduced an ICES with compressed sensing (CS), where the measurement matrix formed by a hyper-chaos system significantly enhances the security [10]. HUANG *et al*. constructed a Hadamard measurement matrix dominated by a chaotic system to devise an ICES with the integer wavelet transform [11]. Subsequently, a color ICES was put forward with block CS and multi-objective particle swarm optimization [12]. Unfortunately, the reconstruction quality is unsatisfactory due to the sawtooth effect. This is because the reconstruction accuracy and the reconstruction efficiency of compressed images are inherently contradictory. Consequently, BABACAN *et al*. reconstructed the compressed images with a high degree of accuracy by estimating the prior probability density distribution function [13]. NI *et al*. developed a natural neural network to balance reconstruction accuracy and efficiency by translating deep learning into CS [14]. The high-dimensional property of quaternion algebra enables the extension of certain orthogonal transforms into the hypercomplex transform domain effectively, thus facilitating the investigation of several image processing methods based on quaternion transform. These include image watermarking [15], image fusion [16], image denoising [17] and image encryption [18-22]. ZHOU *et al*. invented a multi-image encryption scheme by defining quaternion discrete fractional Tchebyshev moment transformation [18]. The quaternion gyrator transform [19], the quaternion multi-parameter fractional Fourier transform [20], the quaternion discrete fractional random transform [21] and the quaternion master-slave neural networks [22] have been specifically designed to enhance the performance of IEAs.

With the semi-tensor product compressive sensing (STP-CS), a color ICES is designed by defining the quaternion discrete fractional Krawtchouk transform (QDFrKT). The storage space for the compressed image can be significantly reduced due to the use of the STP measurement matrix. Furthermore, the color components of the plaintext image are enciphered with the QDFrKT and double random phase encoding. The compressed images are reconstructed by the improved grouping iterative reweighted least squares (GIRLS), which produces high-quality reconstructions with an acceptable degree of efficiency.

The rest is arranged as follows. The QDFrKT is defined in Sec. 2. The ICES is detailed in Sec. 3. The simulation results are narrated in Sec. 4. And a conclusion is offered in Sec. 5.

2. Quaternion discrete fractional Krawtchouk transform

2.1. Definition

The QDFrKT is derived from DFrKT [23] and generalized into the quaternion domain. Let $\mathbf{T}_{\mathrm{L}}^{\alpha}$ and $\mathbf{T}_{\mathrm{R}}^{\beta}$ be designated as the left-side QDFrKT and the right-side one, respectively. The left-side 1D-QDFrKT on a quaternion sequence $\mathbf{x}(m) \in R^{N\times 1}$ of the α-th order, *i.e.*, $\mathbf{x} = \mathbf{x}_0 + \mathbf{x}_1\mathbf{i} + \mathbf{x}_2\mathbf{j} + \mathbf{x}_3\mathbf{k}$, can be defined as

$$\mathbf{T}_{\mathrm{L}}^{\alpha} = \mathbf{V}\,\mathbf{D}_{\mathrm{L}}^{\mu\alpha}\,\mathbf{V}^{\mathrm{T}}\mathbf{x} \tag{1}$$

where $\boldsymbol{\mu} = a_0\mathbf{i} + a_1\mathbf{j} + a_2\mathbf{k}$ is a pure unit quaternion satisfying the condition such that $|\boldsymbol{\mu}| = 1$, and the column vectors of $\mathbf{V}$ are the eigenvectors of the Krawtchouk matrix, the definition of this diagonal matrix $\mathbf{D}_{\mathrm{L}}^{\mu\alpha}$ is

$$\mathbf{D}_{\mathrm{L}}^{\mu\alpha} = \begin{pmatrix} \exp(-\mu\alpha 0\pi) & 0 & \cdots & 0 \\ 0 & \exp(-\mu\alpha 1\pi) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \exp(-\mu\alpha(N-1)\pi) \end{pmatrix} \tag{2}$$

Similarly, the right-side 1D-QDFrKT $\mathbf{T}_{\mathrm{R}}^{\beta}$ of the quaternion discrete sequence $\mathbf{y}(m) \in R^{N\times 1}$ with order β-th and the corresponding diagonal matrix $\mathbf{D}_{\mathrm{R}}^{\mu\beta}$ can be defined respectively as follows:

$$\mathbf{T}_{\mathrm{R}}^{\beta} = \mathbf{y}\,\mathbf{V}\,\mathbf{D}_{\mathrm{R}}^{\mu\beta}\,\mathbf{V}^{\mathrm{T}} \tag{3}$$

$$\mathbf{D}_{\mathrm{R}}^{\mu\beta} = \begin{pmatrix} \exp(-\mu\beta 0\pi) & 0 & \cdots & 0 \\ 0 & \exp(-\mu\beta 1\pi) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \exp(-\mu\beta(N-1)\pi) \end{pmatrix} \tag{4}$$

After calculating the left-side 1D-QDFrKT $\mathbf{T}_{\mathrm{L}}^{\alpha}$ and the right-side 1D-QDFrKT $\mathbf{T}_{\mathrm{R}}^{\beta}$ for the column and row vectors of a 2D quaternion discrete signal $\mathbf{Y}(m, n)$, the 2D-QDFrKT can be obtained as

$$\mathbf{T}^{\alpha,\beta} = \mathbf{V}\,\mathbf{D}_{\mathrm{L}}^{\mu\alpha}\,\mathbf{V}^{\mathrm{T}}\mathbf{Y}\,\mathbf{V}\,\mathbf{D}_{\mathrm{R}}^{\mu\beta}\,\mathbf{V}^{\mathrm{T}} \tag{5}$$

Due to the identity and additivity properties of the Krawtchouk matrix [24], the inverse quaternion discrete fractional Krawtchouk transform (IQDFrKT) can be obtained with the inverse fractional coefficients,

$$\mathbf{Y} = \mathbf{V}\,\mathbf{D}_{\mathrm{L}}^{-\mu\alpha}\,\mathbf{V}^{\mathrm{T}}\mathbf{T}^{\alpha,\beta}\,\mathbf{V}\,\mathbf{D}_{\mathrm{R}}^{-\mu\beta}\,\mathbf{V}^{\mathrm{T}} \tag{6}$$

2.2. Algorithm of QDFrKT

According to Eq. (1), the left-side 1D-QDFrKT can be calculated with a basic algorithm of quaternion $\boldsymbol{\mu} = a\mathbf{i} + b\mathbf{j} + c\mathbf{k}$, and the detailed calculation process of the α-th order left-side 1D-QDFrKT $\mathbf{T}_{\mathrm{L}}^{\alpha}$ is

$$\begin{aligned}\mathbf{T}_{\mathrm{L}}^{\alpha} &= \mathbf{V}\,\mathbf{D}_{\mathrm{L}}^{\mu\alpha}\,\mathbf{V}^{\mathrm{T}} = \lambda_{\mathrm{L}} + \gamma_{\mathrm{L}}\mathbf{i} + \chi_{\mathrm{L}}\mathbf{j} + \delta_{\mathrm{L}}\mathbf{k} \\ &= \mathrm{Re}(\mathbf{K}_{\mathrm{L}}^{\alpha}\mathbf{x}_0) + (a\,\mathbf{i} + b\,\mathbf{j} + c\,\mathbf{k})\,\mathrm{Im}(\mathbf{K}_{\mathrm{L}}^{\alpha}\mathbf{x}_0) \\ &\quad + \mathbf{i}\,\mathrm{Re}(\mathbf{K}_{\mathrm{L}}^{\alpha}\mathbf{x}_1) + (-a - b\,\mathbf{k} + c\,\mathbf{j})\,\mathrm{Im}(\mathbf{K}_{\mathrm{L}}^{\alpha}\mathbf{x}_1) \\ &\quad + \mathbf{j}\,\mathrm{Re}(\mathbf{K}_{\mathrm{L}}^{\alpha}\mathbf{x}_2) + (a\,\mathbf{k} - b - \mathbf{i})\,\mathrm{Im}(\mathbf{K}_{\mathrm{L}}^{\alpha}\mathbf{x}_2) \\ &\quad + \mathbf{k}\,\mathrm{Re}(\mathbf{K}_{\mathrm{L}}^{\alpha}\mathbf{x}_3) + (-a\,\mathbf{j} - b\,\mathbf{i} - c)\,\mathbf{k}\,\mathrm{Im}(\mathbf{K}_{\mathrm{L}}^{\alpha}\mathbf{x}_3)\end{aligned} \tag{7}$$

where

$$\begin{aligned}\lambda_{\mathrm{L}} &= \mathrm{Re}(\mathbf{K}_{\mathrm{L}}^{\alpha}\mathbf{x}_0) - a\,\mathrm{Im}(\mathbf{K}_{\mathrm{L}}^{\alpha}\mathbf{x}_1) - b\,\mathrm{Im}(\mathbf{K}_{\mathrm{L}}^{\alpha}\mathbf{x}_2) - c\,\mathrm{Im}(\mathbf{K}_{\mathrm{L}}^{\alpha}\mathbf{x}_3) \\ \gamma_{\mathrm{L}} &= a\,\mathrm{Im}(\mathbf{K}_{\mathrm{L}}^{\alpha}\mathbf{x}_0) + \mathrm{Re}(\mathbf{K}_{\mathrm{L}}^{\alpha}\mathbf{x}_1) - c\,\mathrm{Im}(\mathbf{K}_{\mathrm{L}}^{\alpha}\mathbf{x}_2) + b\,\mathrm{Im}(\mathbf{K}_{\mathrm{L}}^{\alpha}\mathbf{x}_3) \\ \chi_{\mathrm{L}} &= b\,\mathrm{Im}(\mathbf{K}_{\mathrm{L}}^{\alpha}\mathbf{x}_0) + \mathrm{Re}(\mathbf{K}_{\mathrm{L}}^{\alpha}\mathbf{x}_1) + c\,\mathrm{Im}(\mathbf{K}_{\mathrm{L}}^{\alpha}\mathbf{x}_2) - a\,\mathrm{Im}(\mathbf{K}_{\mathrm{L}}^{\alpha}\mathbf{x}_3) \\ \delta_{\mathrm{L}} &= c\,\mathrm{Im}(\mathbf{K}_{\mathrm{L}}^{\alpha}\mathbf{x}_0) + \mathrm{Re}(\mathbf{K}_{\mathrm{L}}^{\alpha}\mathbf{x}_1) - b\,\mathrm{Im}(\mathbf{K}_{\mathrm{L}}^{\alpha}\mathbf{x}_2) + a\,\mathrm{Im}(\mathbf{K}_{\mathrm{L}}^{\alpha}\mathbf{x}_3)\end{aligned}$$

In the same way as Eq. (7), the right-side 1D-QDFrKT on $\mathbf{y} = \mathbf{y}_0 + \mathbf{y}_1\mathbf{i} + \mathbf{y}_2\mathbf{j} + \mathbf{y}_3\mathbf{k}$ can be calculated as

$$\mathbf{T}_{\mathrm{R}}^{\beta} = \mathbf{y}\,\mathbf{V}\,\mathbf{D}_{\mathrm{R}}^{\mu\beta}\,\mathbf{V}^{\mathrm{T}} = \lambda_{\mathrm{R}} + \gamma_{\mathrm{R}}\mathbf{i} + \chi_{\mathrm{R}}\mathbf{j} + \delta_{\mathrm{R}}\mathbf{k} \tag{8}$$

where

$$\begin{aligned}\lambda_{\mathrm{R}} &= \mathrm{Re}(\mathbf{K}_{\mathrm{R}}^{\beta}\mathbf{y}_0) - a\,\mathrm{Im}(\mathbf{K}_{\mathrm{R}}^{\beta}\mathbf{y}_1) - b\,\mathrm{Im}(\mathbf{K}_{\mathrm{R}}^{\beta}\mathbf{y}_2) - c\,\mathrm{Im}(\mathbf{K}_{\mathrm{R}}^{\beta}\mathbf{y}_3) \\ \gamma_{\mathrm{R}} &= a\,\mathrm{Im}(\mathbf{K}_{\mathrm{R}}^{\beta}\mathbf{y}_0) + \mathrm{Re}(\mathbf{K}_{\mathrm{R}}^{\beta}\mathbf{y}_1) + c\,\mathrm{Im}(\mathbf{K}_{\mathrm{R}}^{\beta}\mathbf{y}_2) - b\,\mathrm{Im}(\mathbf{K}_{\mathrm{R}}^{\beta}\mathbf{y}_3) \\ \chi_{\mathrm{R}} &= b\,\mathrm{Im}(\mathbf{K}_{\mathrm{R}}^{\beta}\mathbf{y}_0) + \mathrm{Re}(\mathbf{K}_{\mathrm{R}}^{\beta}\mathbf{y}_1) - c\,\mathrm{Im}(\mathbf{K}_{\mathrm{R}}^{\beta}\mathbf{y}_2) + a\,\mathrm{Im}(\mathbf{K}_{\mathrm{R}}^{\beta}\mathbf{y}_3) \\ \delta_{\mathrm{R}} &= c\,\mathrm{Im}(\mathbf{K}_{\mathrm{R}}^{\beta}\mathbf{y}_0) + \mathrm{Re}(\mathbf{K}_{\mathrm{R}}^{\beta}\mathbf{y}_1) + b\,\mathrm{Im}(\mathbf{K}_{\mathrm{R}}^{\beta}\mathbf{y}_2) - a\,\mathrm{Im}(\mathbf{K}_{\mathrm{R}}^{\beta}\mathbf{y}_3)\end{aligned}$$

Meanwhile, the 2D-QDFrKT on a quaternion signal $f \in R^{N\times N}$ can be calculated in accordance with the aforementioned methods. The left-side 1D-QDFrKT $\mathbf{T}_{\mathrm{L}}^{\alpha}$ is cal-

culated on the x-axis, and then the subsequent results are put on the y-axis to carry out the right-side 1D-QDFrKT to generate the final calculation result,

$$\mathbf{T}^{\alpha,\beta} = \mathbf{V}\,\mathbf{D}_{\mathrm{L}}^{\mu\alpha}\mathbf{V}^{\mathrm{T}}\mathbf{F}\,\mathbf{V}\,\mathbf{D}_{\mathrm{R}}^{\mu\beta}\mathbf{V}^{\mathrm{T}} = \mathbf{K}_{\mathrm{R}}^{\beta}\left[\mathbf{K}_{\mathrm{L}}^{\alpha}(\mathbf{F})\right] \tag{9}$$

3. Color image compression encryption algorithm

3.1. Compression-encryption process

Figure 1 is the flowchart of the proposed color ICES, whose detailed steps are described below.

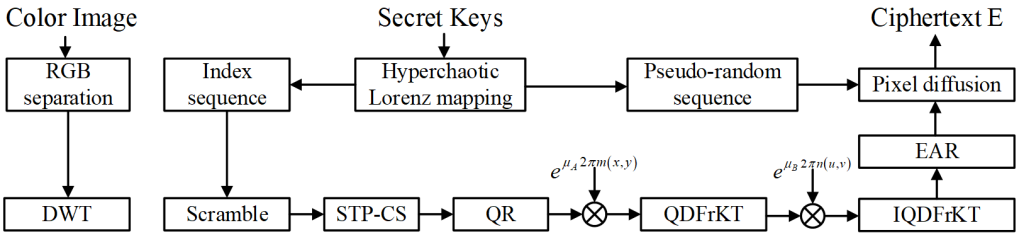


Fig. 1. Compression-encryption process of proposed algorithm.

Step 1: Compression and preliminary encryption with STP compressive sensing.

(1) The color plaintext image of size $M \times N \times 3$ is separated by R, G and B channels, yielding color component $\mathbf{P}_i$. These color components are then represented in the DWT domain to obtain the corresponding sparse coefficient matrix $\boldsymbol{\theta}_i = \boldsymbol{\Psi}^{\mathrm{T}}\mathbf{P}_i\boldsymbol{\Psi}$, $i \in \{\mathrm{R}, \mathrm{G}, \mathrm{B}\}$.

(2) Based on the nonlinear hyperchaotic Lorenz map, a pseudo-random sequence $(S_1, S_2, ..., S_N)$ is generated by iterating $M \times N$ times with the initial parameter values a_1, c_1, b_1, p_1. An index sequence ε is formed by sorting this pseudo-random sequence in ascending order. Subsequently, the sparse coefficient matrix $\boldsymbol{\theta}_i$ is scrambled by the index sequence ε.

(3) The first $(M/t)\times(N/t)$ elements in the sequence $(S_1, S_2, ..., S_N)$ are sorted by their column vectors to generate a low-order measurement matrix $\boldsymbol{\Phi}_{(M/t)\times(N/t)}$. The STP normalization is then performed on this matrix to yield the STP measurement matrix,

$$\boldsymbol{\Phi}_{\mathrm{STP}} = \sqrt{\frac{2t}{M}}\,(M - 2\boldsymbol{\Phi}_{(M/t)\times(N/t)}) \tag{10}$$

Subsequently, the scrambled sparse coefficient matrices $\boldsymbol{\theta}_i$ are measured to obtain the compression and preliminary encryption result

$$\mathbf{y} = \boldsymbol{\Phi}_{\mathrm{STP}} \ltimes \mathbf{x} = (\boldsymbol{\Phi}_{\mathrm{STP}} \otimes I_{P/N})\mathbf{x} = \begin{pmatrix} \Phi_{11} & \cdots & 0 & & \Phi_{1N} & \cdots & 0 \\ \vdots & \ddots & \vdots & \cdots & \vdots & \ddots & \vdots \\ 0 & \cdots & \Phi_{11} & & 0 & \cdots & \Phi_{1N} \\ & \vdots & & \ddots & & \vdots & \\ \Phi_{M1} & \cdots & 0 & & \Phi_{MN} & \cdots & 0 \\ \vdots & \ddots & \vdots & \cdots & \vdots & \ddots & \vdots \\ 0 & \cdots & \Phi_{M1} & & 0 & \cdots & \Phi_{MN} \end{pmatrix} \mathbf{x} \tag{11}$$

where $\ltimes$ and $\otimes$ are left side STP and Kronecker product, respectively, and $t = P/N$ is the descending ratio in the STP-CS.

Step 2: Quaternion representation (QR). The compressed image is first normalized, and then the three-color components in the compressed image are sliced into twelve sub-blocks. Subsequently, the quaternion representation of these sub-blocks can be represented as

$$f_{Q_i} = f_{i_1} + f_{i_2}\mathbf{i} + f_{i_3}\mathbf{j} + f_{i_4}\mathbf{k}, \qquad i \in \{\mathrm{R}, \mathrm{G}, \mathrm{B}\} \tag{12}$$

Step 3: Double random phase encoding based on the QDFrKT. Firstly, $f_{Q_i}(x, y)$ is post-multiplied by the quaternion random phase mask $\exp[\boldsymbol{\mu}_{\mathrm{A}} 2\pi m(x, y)]$. Then the defined QDFrKT is performed on the multiplication result to produce

$$g(u, v) = \mathrm{QDFKrT}^{\alpha}_{\boldsymbol{\mu}_1}\left[f_{Q_i}(x, y)\exp[\boldsymbol{\mu}_{\mathrm{A}} 2\pi m(x, y)]\right] \tag{13}$$

Then $g(u, v)$ is post-multiplied by the quaternion random phase mask $\exp[\boldsymbol{\mu}_{\mathrm{B}} 2\pi n(u, v)]$, and $c_{Q_i}(x, y)$ is established by carrying out the proposed IQDFrKT on $g(u, v)\exp[\boldsymbol{\mu}_{\mathrm{B}} 2\pi n(u, v)]$ with unit quaternion $\boldsymbol{\mu}_2$ and order β.

$$c_{Q_i}(x, y) = \mathrm{IQDFKrT}^{\beta}_{\boldsymbol{\mu}_2}\left\{\mathrm{QDFKrT}^{\alpha}_{\boldsymbol{\mu}_1}\left[f_{Q_i}(x, y)\exp[\boldsymbol{\mu}_{\mathrm{A}} 2\pi m(x, y)]\right]\exp[\boldsymbol{\mu}_{\mathrm{B}} 2\pi n(u, v)]\right\} \tag{14}$$

where $\boldsymbol{\mu}_1$, $\boldsymbol{\mu}_2$, $\boldsymbol{\mu}_{\mathrm{A}}$, and $\boldsymbol{\mu}_{\mathrm{B}}$ are random unit pure quaternions.

Step 4: Extraction and reorganization. By extracting the real part and the corresponding imaginary parts of quaternion from $c_{Q_i}(x, y)$, the reorganization matrix $\mathbf{C}$ of size $(M/t)\times(3N/t)$ is represented using the quaternion theory.

Step 5: Pixel diffusion. Each channel of the reorganization matrix $\mathbf{C}$ is diffused to generate the ciphered image $\mathbf{E}$, where the diffusion method utilized in each channel is

$$\mathbf{E}_i = \begin{cases} \left[\mathbf{C}_i + \mathbf{C}_L + \mathbf{C}_{L-1} + \mathrm{floor}(2^F S_i)\right] \bmod F, & i = 1 \\ \left[\mathbf{C}_i + \mathbf{E}_{L-1} + \mathrm{floor}(2^F S_i)\right] \bmod F, & i \in [2, L] \end{cases} \tag{15}$$

where L is the number of total pixels, while F is the image depth. The sequence S_i is generated by the pseudo-random sequence (S_1, S_2, ..., S_N) in descending order.

3.2. Decryption process

In the process of decryption, the ciphertext image **E** is firstly implemented by RGB separation and the quaternion representation, thereby yielding the four sub-blocks of three channels, respectively. Subsequently, the inverse pixel diffusion is performed on these sub-blocks using the correct key, and the quaternion signals of each channel are produced with the double random phase decoding and the defined IQDFrKT. The measured results are then acquired by separation and reorganization. Finally, the compressed image is reconstructed by the improved GIRLS algorithm.

The commonly used IRLS algorithm lacks insufficient reconstruction efficiency and it is hard to process a larger number of color images. To tackle this issue, the IRLS algorithm is grouped to significantly elevate the efficiency of the reconstruction algorithm while ensuring the quality of image reconstruction. The specific process of the GIRLS algorithm is detailed below.

(1) Input: STP measurement matrix $\mathbf{\Phi}_{\mathrm{STP}}$, compression result **f**, and the image size $M \times N$.

(2) Output: reconstruction result $\hat{\boldsymbol{\theta}}_{N\times N}$.

(3) The initialization $i = j = 1$, $\varepsilon_0 = 1$ and the vector $\boldsymbol{\omega}^{(0)} = \hat{\boldsymbol{\theta}}^t_{(0)} = (1, ..., 1)$ of length $N \times 1$ are required. $\mathbf{D}_n$ is a diagonal matrix, where the p-th diagonal component depends on $1/\boldsymbol{\omega}_p^{(n)}$, and $\boldsymbol{\omega}_p^{(n)}$ denotes the n-th iteration of the reweighting operation, $p = 1, 2, ..., N/t$. Considering the L-q parametrization ($0 < q < 1$), the grouped operation on the compressed result **f** can be described as

$$\mathbf{f}^t_{(M/t)\times 1} = \left(f_1, f_2, ..., f_{\frac{Mt}{t-1}+t}\right)^{\mathrm{T}} \tag{16}$$

and then the iteration is performed on these grouped results,

$$\begin{cases} \hat{\boldsymbol{\theta}}^t_{n+1} = \mathbf{D}_n \mathbf{\Phi}^{\mathrm{T}}_{\mathrm{STP}} \left(\mathbf{\Phi}_{\mathrm{STP}} \mathbf{D}_n \mathbf{\Phi}^{\mathrm{T}}_{\mathrm{STP}}\right)^{-1} \mathbf{f}^t_{(M/t)\times 1} \\ \boldsymbol{\omega}_p^{(n)} = \left\{ \left[\left(\hat{\boldsymbol{\theta}}^{i,j}_p\right)^{(n)} \right]^2 + \varepsilon_n^{1+q} \right\}^{\frac{2-q}{q}} \end{cases} \tag{17}$$

where $\varepsilon_{n+1} = \rho \varepsilon_n$, and the sparse resolution $\hat{\boldsymbol{\theta}}^t_{n+1}$ is obtained until $\left\| \hat{\boldsymbol{\theta}}^t_{n+1} - \hat{\boldsymbol{\theta}}^t_n \right\| < \frac{\sqrt{\varepsilon}}{10}$.

(4) The grouped reconstruction process of the sparse resolution $\hat{\boldsymbol{\theta}}^t_{n+1}$ can be described as

$$\hat{\boldsymbol{\theta}}_{N\times 1}(pt+1 : pt+t) = (\hat{\boldsymbol{\theta}}^1_p, \hat{\boldsymbol{\theta}}^2_p, ..., \hat{\boldsymbol{\theta}}^t_p)^{\mathrm{T}} \tag{18}$$

where $\hat{\boldsymbol{\theta}}_{N\times 1}(pt+1:pt+t)$ denotes the $(pt+1)$-th to $(pt+t)$-th the elements in $\hat{\boldsymbol{\theta}}_{N\times 1}$. Subsequently, returning to the step (3), the reconstruction result $\hat{\boldsymbol{\theta}}_{N\times N}$ is obtained by performing N-th iterations with the sparse resolution $\hat{\boldsymbol{\theta}}_{N\times j}$. Eventually, the ciphered image is decrypted by the inverse DWT and RGB recombination.

4. Simulation results and analyses

The simulation is performed by the MATLAB (R2020a) on a computer with Intel (R) Core (TM) i5-6300HQ CPU @2.30 GHz.

4.1. Encryption and decryption result

Four color images "Car", "Cat", "Lake", "House" of size in Fig. 2(a)-(d) are considered as test images. The four Lyapunov exponents of the nonlinear hyperchaotic Lorenz system can serve as secret keys and their values are set as: $a = 0.3511$, $b = 0.1672$, $c = 0$, and $r = -1.2$. During the STP-CS, the sampling rate of each image takes 0.25, and the descending ratio is $P/N = 2$. The keys in double random phase encoding and QDFrKT are $\boldsymbol{\mu}_1 = \mathbf{i}$, $\boldsymbol{\mu}_2 = \mathbf{j}$, $\boldsymbol{\mu}_A = \mathbf{k}$, $\boldsymbol{\mu}_B = (\mathbf{i}+\mathbf{j}+\mathbf{k})/\sqrt{3}$, $\alpha = 0.4$, and $\beta = 0.5$. The four encryption and decryption images corresponding to the test image are displayed in Fig. 2(e)-(h) and (i)-(l), respectively. Based on the imperceptible difference between the original

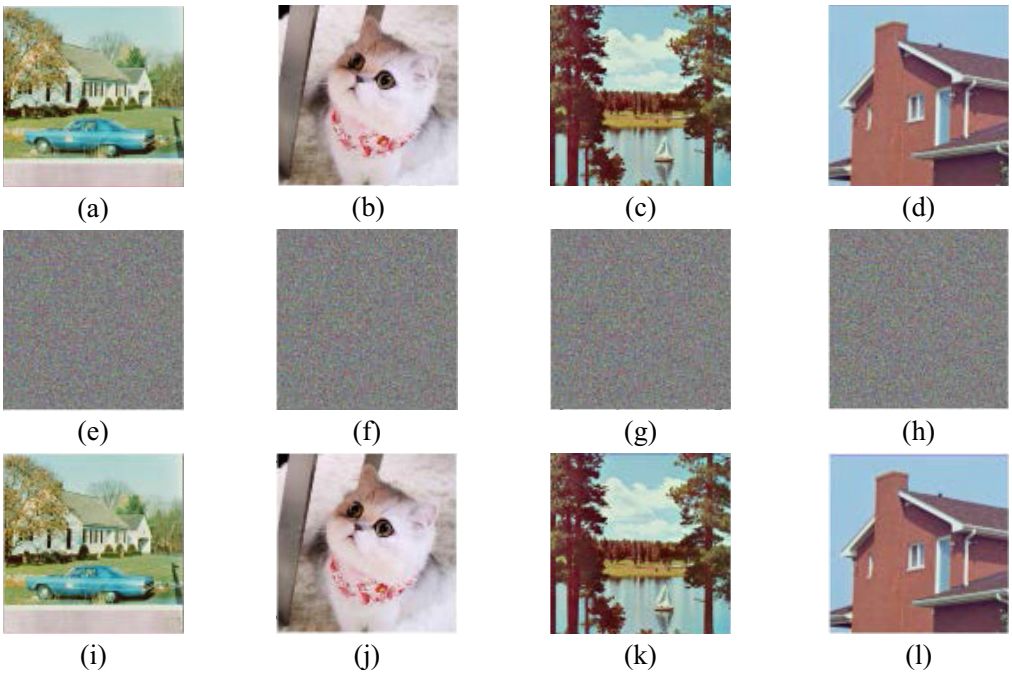


Fig. 2. Test results. Plaintext image: (a) "Car", (b) "Cat", (c) "Lake", (d) "House"; encryption image: (e) "Car", (f) "Cat", (g) "Lake", (h) "House"; decryption image: (i) "Car", (j) "Cat", (k) "Lake", (l) "House".

T a b l e 1. PSNR and average SSIM values of decryption images.

Decryption image	PSNR [dB]				Average SSIM value
	R	G	B	Average	
"Car"	37.9792	38.3409	39.1317	38.4839	0.9952
"Cat"	38.0321	38.2188	38.1781	38.1430	0.9931
"Lake"	38.2383	39.0288	38.3316	38.5329	0.9964
"House"	38.0127	38.3655	40.3006	38.8929	0.9977

image and its decryption one, the proposed color ICES is feasible. The PSNR and the average SSIM values of the four decryption images are summarized in Table 1.

$$\mathrm{PSNR} = 10\lg\frac{255^2 \times N \times N}{\sum_{x=1}^{N}\sum_{y=1}^{N}\left[D(x,y) - O(x,y)\right]^2} \tag{19}$$

$$\mathrm{SSIM} = \frac{\sigma_{\mathrm{OD}}}{\sigma_{\mathrm{O}}\sigma_{\mathrm{D}}} \cdot \frac{2\overline{\mathbf{O}}\,\overline{\mathbf{D}}}{\overline{\mathbf{O}}^2 + \overline{\mathbf{D}}^2} \cdot \frac{2\sigma_{\mathrm{O}}\sigma_{\mathrm{D}}}{\sigma_{\mathrm{O}}^2 + \sigma_{\mathrm{D}}^2} \tag{20}$$

where $O(x, y)$ and $D(x, y)$ are the pixel values of original plaintext image **O** and decryption image **D**, respectively; σ_{O} and σ_{D} are the standard deviations of images **O** and **D**, respectively, while σ_{OD} denotes the covariance of images **O** and **D**; $\overline{\mathbf{O}}$ and $\overline{\mathbf{D}}$ are the average pixel values of images **O** and **D**, respectively. The PSNR values of the majority of decryption images are greater than 37 dB, and the average SSIM values are near 1, which further confirms the excellent performance of our proposed scheme.

4.2. Compression performance

The images are compressed with different sizes by the STP measurement matrix. PSNR is employed to assess the quality of the recovered images under different compression rates. Figure 3 shows the decryption images of "Car" under compression ratios 0.75, 0.5, 0.25 and 0.125. Even if the compression ratio reaches 0.125, major content of the reconstruction image can be clearly identified. The PSNR values of the

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

Fig. 3. Decryption "Car" under different compression ratios: (a) 0.75, (b) 0.5, (c) 0.25, (d) 0.125.

T a b l e 2. PSNR of decryption "Car" under different compression ratios.

Algorithms	PSNR [dB]		
	0.75	0.5	0.25
Proposed algorithm	42.2167	38.4839	35.3488
[25]	41.0852	36.7034	32.2037
[26]	36.1415	32.1471	28.0615
[27]	29.2200	29.2300	26.5200
[28]	32.3500	32.1000	26.7800

T a b l e 3. Speed performance before and after compression.

	Time [s]	
	Encryption	Decryption
Before compression	0.5041	0.4028
After compression	0.5588	0.7625

decryption images at different compression ratios are presented in Table 2. The proposed ICES performs excellent performance in both compression and reconstruction accuracy.

The speed performance of this algorithm before and after compression when fully sampled is shown in Table 3. It can be observed from Table 3 that the efficiency of the proposed image compression-encryption algorithm is acceptable, adequately meeting the requirements for real-time compression and encryption.

4.3. Histogram

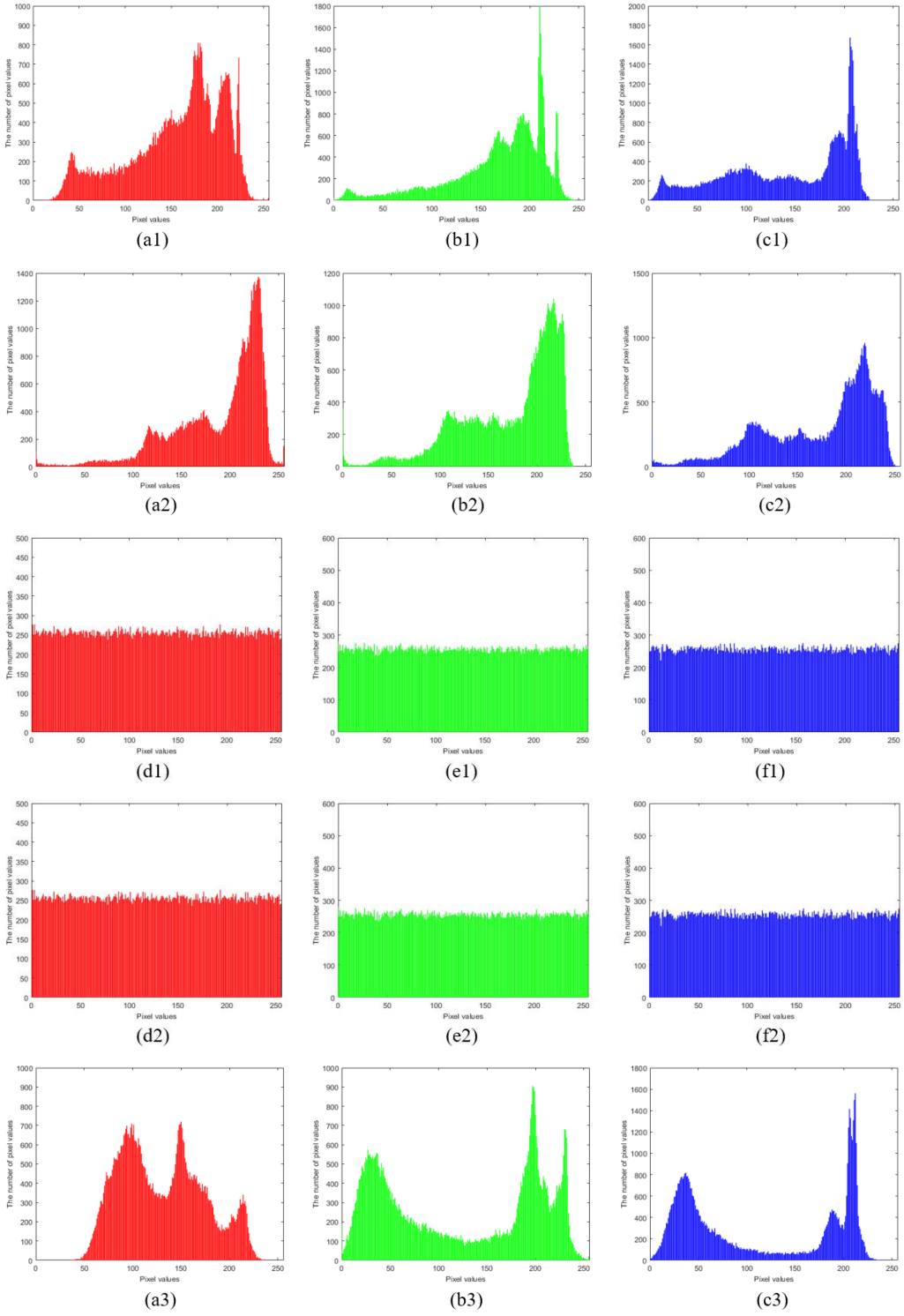
Figure 4 presents the histograms of four test images and their corresponding encryption ones. The histograms of the four test images exhibit apparent differences. However, the histograms of their encryption images are similar with each other to withstand the statistical attack and histogram attack on the proposed ICES.

4.4. Correlation

The correlation coefficients (CCs) of RGB components in the original images and the encryption ones are illustrated in Fig. 5.

$$\mathrm{CC} = \frac{\sum_{i=1}^{N}(x_i - \overline{x})(y_i - \overline{y})}{\sqrt{\sum_{i=1}^{N}(x_i - \overline{x})^2 \sum_{i=1}^{N}(y_i - \overline{y})^2}} \tag{21}$$

$$\overline{x} = \frac{1}{N}\sum_{i=1}^{N} x_i \quad \text{and} \quad \overline{y} = \frac{1}{N}\sum_{i=1}^{N} y_i \tag{22}$$


The number of pixel values
Pixel values
(a1)
(b1)
(c1)
(a2)
(b2)
(c2)
(d1)
(e1)
(f1)
(d2)
(e2)
(f2)
(a3)
(b3)
(c3)

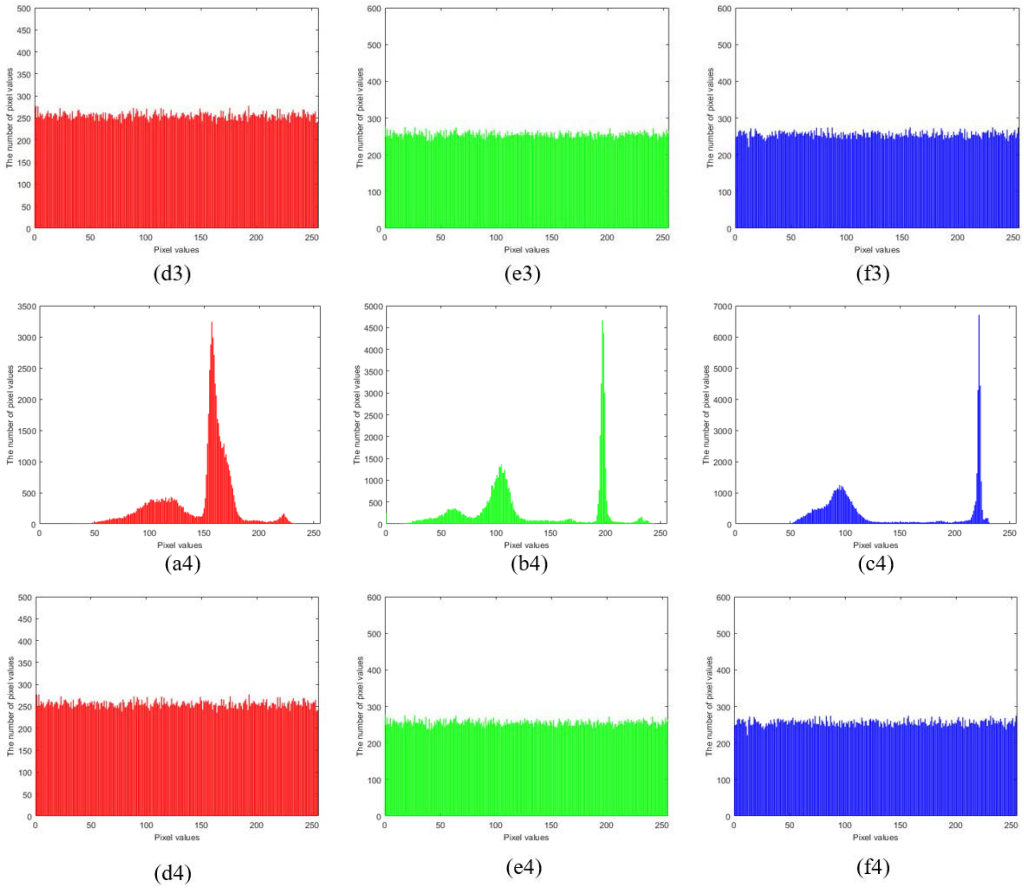
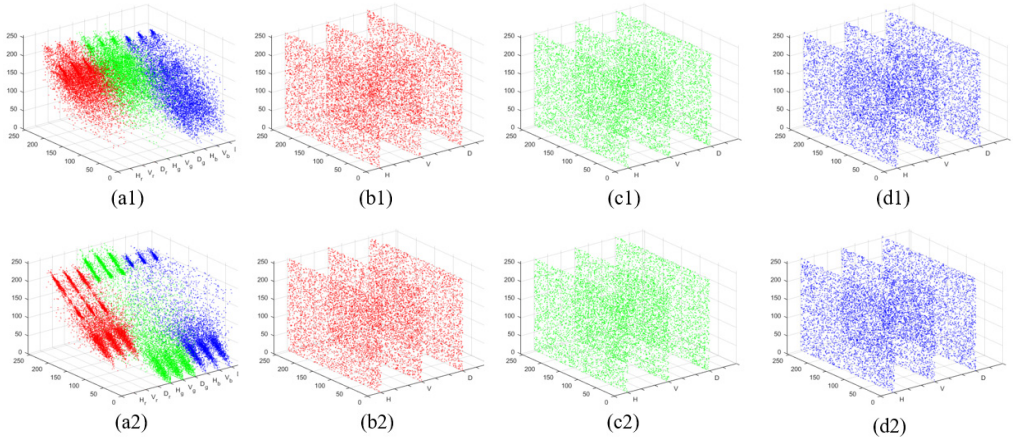


Fig. 4. Histogram of R, G, B components: (a1)–(c1) “Car”, (d1)–(f1) encryption “Car”, (a2)–(c2) “Cat”, (d2)–(f2) encryption “Cat”, (a3)–(c3) “Lake”, (d3)–(f3) encryption “Lake”, (a4)–(c4) “House”, (d4)–(f4) encryption “House”.



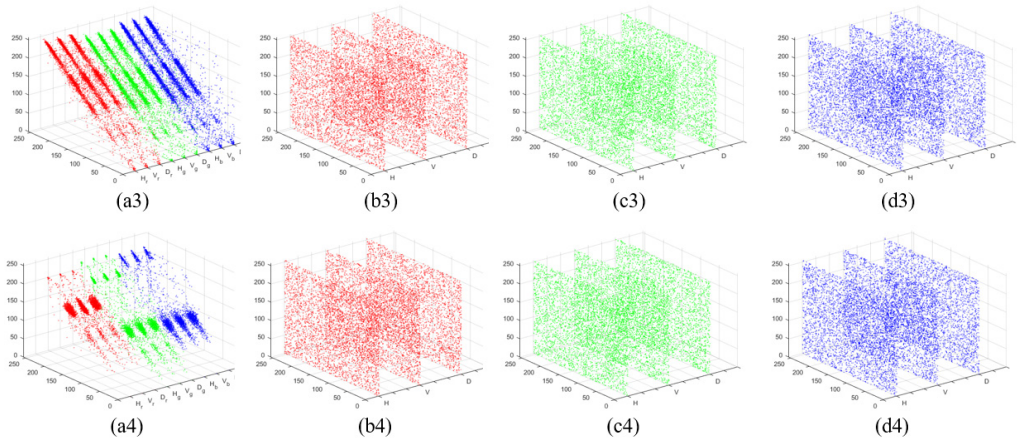


Fig. 5. Correlation distribution between adjacent pixels of the RGB components in original images: (a1)-(d1) "Car" and encryption "Car", (a2)-(d2) "Cat" and encryption "Cat", (a3)-(d3) "Lake" and encryption "Lake", (a4)-(d4) "House" and encryption "House".

T a b l e 4. CC between adjacent pixels in the original images.

Images	Color components	Original image			Encryption image		
		Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
"Car"	R	0.9240	0.9250	0.9136	−0.0045	0.0063	0.0123
	G	0.9188	0.9086	0.8994	0.0057	−0.0082	0.0124
	B	0.8852	0.8873	0.8798	−0.0117	0.0066	0.0032
"Cat"	R	0.9611	0.9570	0.9361	−0.0032	0.0144	0.0103
	G	0.9666	0.9561	0.9462	0.0052	−0.0054	−0.0017
	B	0.9713	0.9687	0.9528	−0.0035	0.0071	−0.0059
"Lake"	R	0.9208	0.9229	0.9423	0.0018	−0.0032	−0.0048
	G	0.9223	0.9261	0.8920	0.0102	−0.0027	−0.0017
	B	0.9319	0.9336	0.9087	0.0091	0.0051	0.0045
"House"	R	0.9398	0.9660	0.9124	−0.0023	0.0034	0.0018
	G	0.9417	0.9799	0.9261	0.0027	−0.0011	−0.0103
	B	0.9721	0.9832	0.9595	−0.0075	0.0077	0.0142

In Table 4, the CC values between adjacent pixels in the encryption images are significantly weakened, despite the RGB components in the color plaintext images are highly correlated. Therefore, the proposed color ICES ensures against the statistical attack.

4.5. Key space

The keys are four Lyapunov exponents a, b, c, and r of the nonlinear hyperchaotic Lorenz map, the unit quaternion $\boldsymbol{\mu}_A$, $\boldsymbol{\mu}_B$ and the control parameters of QDFrKT $\boldsymbol{\mu}_1$, $\boldsymbol{\mu}_2$, a_0, b_0, c_0, α, and β. Considering the computational accuracy 10^{-15}, the number of at-

T a b l e 5. Key space for various algorithms.

Algorithms	Ours	[10]	[29]	[30]	[31]
Key space	$\geq 2^{285}$	$\geq 2^{233}$	$> 2^{210}$	$> 2^{192}$	$\geq 2^{130}$

tempts to retrieve three pseudorandom phase images is $M^3 \times N^3$ for the pseudorandom phase image of size 256 × 256. The total key space is 8.3×10^{85}, *i.e.*, about 2^{285}. From Table 5, the proposed color ICES can resist the brute-force attack.

4.6. Key sensitivity

Figure 6 displays the decryption image of "Cat" with $\alpha = 0.4 + 10^{-15}$, $\beta = 0.5 + 10^{-15}$, $b = 0.1672 + 10^{-15}$, and $r = -1.2 + 10^{-15}$, respectively. The primary content of the image "Cat" is hard to obtain even if there exists only a tiny change of these keys. In other words, the keys are sufficiently sensitive to the ICES.

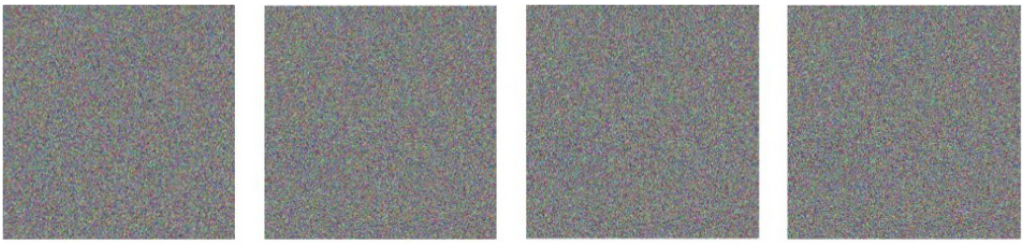


Fig. 6. Decryption "Cat" with tiny deviations of the key: (a) $\alpha = 0.4 + 10^{-15}$, (b) $\beta = 0.5 + 10^{-15}$, (c) $b = 0.1672 + 10^{-15}$, and (d) $r = -1.2 + 10^{-15}$.

4.7. Differential attack

The number of changing pixel rate (NPCR) and the unified averaged changed intensity (UACI) are respectively expressed as [33]

$$\mathrm{NPCR} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} F(i,j) \times 100\% \tag{23}$$

$$\mathrm{UACI} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{\left| F_1(i,j) - F_2(i,j) \right|}{255} \times 100\% \tag{24}$$

$$F(i,j) = \begin{cases} 1, & F_1(i,j) \neq F_2(i,j) \\ 0, & F_1(i,j) = F_2(i,j) \end{cases} \tag{25}$$

where $F_1(i,j)$ and $F_2(i,j)$ are the values of pixels at (i,j) in images $\mathbf{F}_1$ and $\mathbf{F}_2$, respectively. As demonstrated in Table 6, the average NPCR (99.6172%) and the av-

T a b l e 6. NPCR and UACI values.

Schemes	Images	NPCR [%]	UACI [%]
Ours	"Car"	99.6087	33.5741
	"Cat"	99.6170	33.4719
	"Lake"	99.6219	33.6671
	"House"	99.6212	33.7745
	Average	99.6172	33.6219
[25]	Average	99.6066	34.4654
[32]	Average	99.7509	34.7577

erage UACI one (33.6219%) achieved with the proposed CIES approach their theoretical values 99.6094% and 33.4635%, respectively. Consequently, differential attack is invalid for the proposed color ICES.

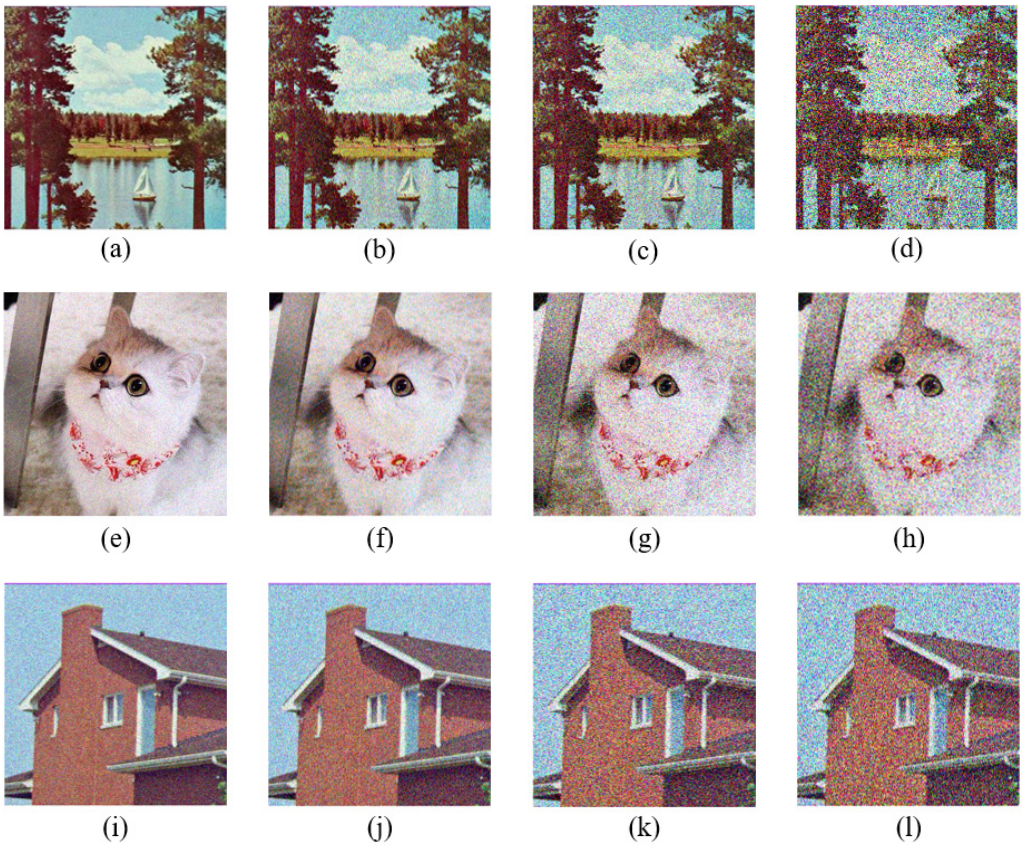


Fig. 7. Decryption images under different noises: (a)-(d) "Lake" with speckle noise with intensities 0.001, 0.005, 0.01, and 0.05, respectively, (e)-(h) "Cat" under white Gaussian noise with intensities 0.001, 0.005, 0.01, and 0.05, respectively, (a3)-(c3) "House" under salt-and-pepper noise with intensities 0.005, 0.01, 0.05, and 0.1, respectively.

4.8. Noise attack

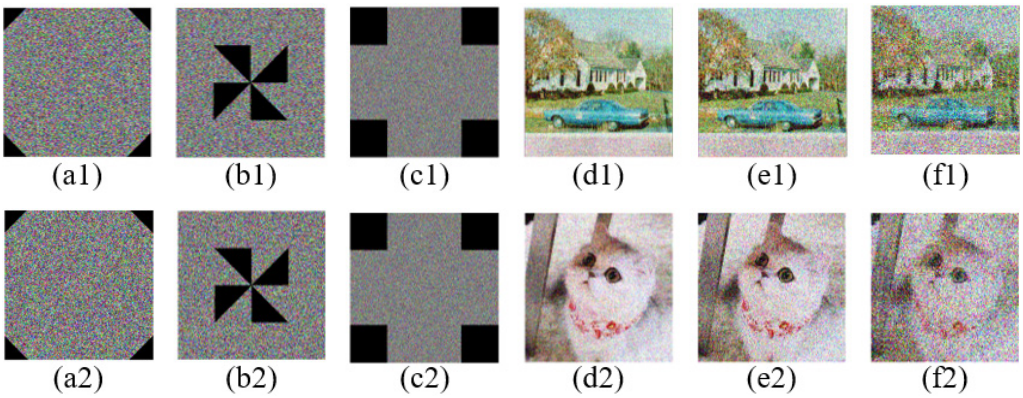
Figure 7(a)-(d) display the decryption images of "Lake" under the speckle noise attack with distinct noise intensities, respectively. Similarly, the decryption images "Cat" under white Gaussian noise attack ("House" under salt-and-pepper noise attack) are exhibited in Fig. 7(e)-(h) (Fig. 7(i)-(l)). Table 7 shows the average PSNR values of the RGB channels of the color test image "Car" under different noise types and intensities. The proposed color ICES is sufficiently robust against the common noise attacks, since the quality of decryption images from noisy encryption images is acceptable under certain noise intensity.

T a b l e 7. Average PSNR of "Car" under different noises with different noise intensities.

Noise type	Noise intensity	Average PSNR [dB]
Speckle noise	0.001	24.5699
	0.005	20.1354
	0.01	15.8670
	0.05	10.8374
White Gaussian noise	0.001	28.3263
	0.005	23.3251
	0.01	16.8885
	0.05	11.3296
Salt-and-pepper noise	0.005	30.0832
	0.01	23.5199
	0.05	18.7580
	0.1	12.5104

4.9. Cropping attack

As shown in Fig. 8, the four encryption images are cropped at 6.25%, 12.5% and 25% cropping ratios, respectively, and the corresponding decryption images are presented simultaneously at the same ratios. The primary content of the decrypted images can



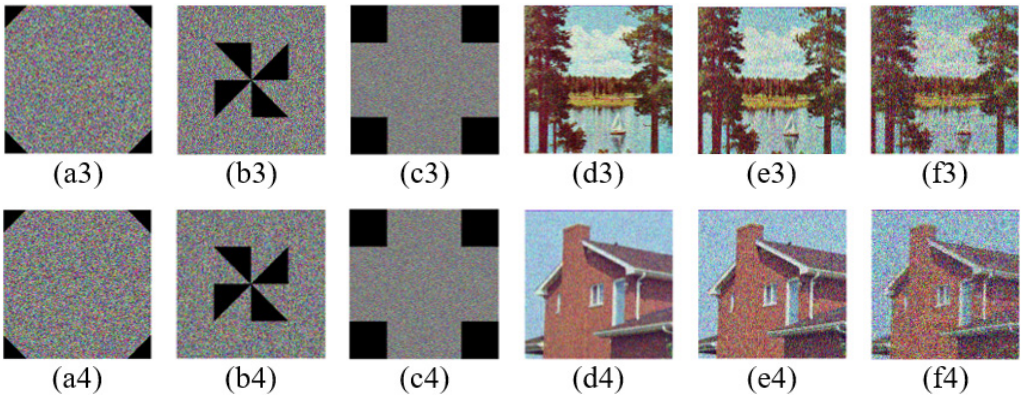


Fig. 8. Results of cropping attack with 6.25%, 12.5% and 25% ratio: (a1)-(c1) encryption "Car", (d1)-(f1) decryption "Car", (a2)-(c2) encryption "Cat", (d2)-(f2) decryption "Cat", (a3)-(c3) encryption "Lake", (d3)-(f3) decryption "Lake", (a4)-(c4) encryption "House", (d4)-(f4) decryption "House".

be distinguished yet even if the data loss in the encryption images reaches 25%. Therefore, the proposed color ICES is robust against the cropping attack.

5. Conclusion

According to the definition of the QDFrKT, a color image compression encryption algorithm is designed with the STP-CS. The color components of the original image are initially compressed and then encrypted by the DWT and the STP measurement matrix. And the compressed image is then re-secured with the double random phase coding and the defined QDFrKT, and the resulting pixels are diffused to reduce the correlation between adjacent pixels further. The simulation results demonstrate the efficiency and the robustness of the color image compression-encryption scheme is as expected.

Acknowledgement
This work is supported by the National Natural Science Foundation of China (Grant No. 61861029).

Disclosures
The first two authors had equal contribution.

References

[1] Hu L.L., Chen M.X., Wang M.M., Zhou N.R., *A multi-image encryption scheme based on block compressive sensing and nonlinear bifurcation diffusion*, Chaos, Solitons & Fractals **188**, 2024: 115521. https://doi.org/10.1016/j.chaos.2024.115521
[2] Pak C., Huang L.L., *A new color image encryption using combination of the 1D chaotic map*, Signal Processing **138**, 2017: 129-137. https://doi.org/10.1016/j.sigpro.2017.03.011
[3] Malik D.S., Shah T., *Color multiple image encryption scheme based on 3D-chaotic maps*, Mathematics and Computers in Simulation **178**, 2020: 646-666. https://doi.org/10.1016/j.matcom.2020.07.007

[4] GAO X.Y., MOU J., XIONG L., SHA Y.W., YAN H.Z., CAO Y.H., *A fast and efficient multiple images encryption based on single-channel encryption and chaotic system*, Nonlinear Dynamics **108**(1), 2022: 613-636. https://doi.org/10.1007/s11071-021-07192-7

[5] WU G.C., DENG Z.G., BALEANU D., ZENG D.Q., *New variable-order fractional chaotic systems for fast image encryption*, Chaos **29**(8), 2019: 083103. https://doi.org/10.1063/1.5096645

[6] ZHENG J.Y., LIU L.F., *Novel image encryption by combining dynamic DNA sequence encryption and the improved 2D logistic sine map*, IET Image Processing **14**(11), 2020: 2310-2320. https://doi.org/10.1049/iet-ipr.2019.1340

[7] NIE Z., LIU Z.X., HE X.T., GONG L.H., *Image compression and encryption algorithm based on advanced encryption standard and hyper-chaotic system*, Optica Applicata **49**(4), 2019: 545-558. https://doi.org/10.37190/oa190402

[8] WANG X.Y., CHEN S.N., ZHANG Y.Q., *A chaotic image encryption algorithm based on random dynamic mixing*, Optics and Laser Technology **138**, 2021: 106837. https://doi.org/10.1016/j.optlastec.2020.106837

[9] GUO Z., CHEN S.H., ZHOU L., GONG L.H., *Optical image encryption and authentication scheme with computational ghost imaging*, Applied Mathematical Modelling **131**, 2024: 49-66. https://doi.org/10.1016/j.apm.2024.04.012

[10] LIU J.L., ZHANG M., TONG X.J., WANG Z., *Image compression and encryption algorithm based on 2D compressive sensing and hyperchaotic system*, Multimedia Systems **28**(2), 2022: 595-610. https://doi.org/10.1007/s00530-021-00859-6

[11] HUANG X.L., DONG Y.X., YE G.D., SHI Y., *Meaningful image encryption algorithm based on compressive sensing and integer wavelet transform*, Frontiers of Computer Science **17**(3), 2023: 173804. https://doi.org/10.1007/s11704-022-1419-8

[12] CHAI X.L., FU J.Y., GAN Z.H., LU Y., ZHANG Y.S., *An image encryption scheme based on multi-objective optimization and block compressed sensing*, Nonlinear Dynamics **108**(3), 2022: 2671-2704. https://doi.org/10.1007/s11071-022-07328-3

[13] BABACAN S.D., MOLINA R., KATSAGGELOS A.K., *Bayesian compressive sensing using Laplace priors*, IEEE Transactions on Image Processing **19**(1), 2010: 53-63. https://doi.org/10.1109/TIP.2009.2032894

[14] NI R.J., WANG F., WANG J., HU Y.H., *Multi-image encryption based on compressed sensing and deep learning in optical gyrator domain*, IEEE Photonics Journal **13**(3), 2021: 7800116. https://doi.org/10.1109/JPHOT.2021.3076480

[15] GONG L.H., LUO H.X., *Dual color images watermarking scheme with geometric correction based on quaternion FrOOFMMs and LS-SVR*, Optics and Laser Technology **167**, 2023: 109665. https://doi.org/10.1016/j.optlastec.2023.109665

[16] CHAI P.F., LUO X.Q., ZHANG Z.C., *Image fusion using quaternion wavelet transform and multiple features*, IEEE Access **5**, 2017: 6724-6734. https://doi.org/10.1109/ACCESS.2017.2685178

[17] YU Y.B., ZHANG Y.L., YUAN S.F., *Quaternion-based weighted nuclear norm minimization for color image denoising*, Neurocomputing **332**, 2019: 283-297. https://doi.org/10.1016/j.neucom.2018.12.034

[18] ZHOU N.R., TONG L.J., ZOU W.P., *Multi-image encryption scheme with quaternion discrete fractional Tchebyshev moment transform and cross-coupling operation*, Signal Processing **211**, 2023: 109107. https://doi.org/10.1016/j.sigpro.2023.109107

[19] SHAO Z.H., SHANG Y.Y, TONG Q.B., DING H., ZHAO X.X., FU X.Y., *Multiple color image encryption and authentication based on phase retrieval and partial decryption in quaternion gyrator domain*, Multimedia Tools and Applications **77**(19), 2018: 25821-25840. https://doi.org/10.1007/s11042-018-5818-7

[20] CHEN B.J., YU M., TIAN Y.H., LI L.D., WANG D.C., SUN X.M., *Multiple-parameter fractional quaternion Fourier transform and its application in colour image encryption*, IET Image Processing **12**(12), 2018: 2238-2249. https://doi.org/10.1049/iet-ipr.2018.5440

[21] Ye H.S., Dai J.Y., Wen S.X., Gong L.H., Zhang W.Q., *Color image encryption scheme based on quaternion discrete multi-fractional random transform and compressive sensing*, Optica Applicata **51**(3), 2021: 349-364. https://doi.org/10.37190/oa210304

[22] Liu L.R., Lei M.L., Bao H.B., *Event-triggered quantized quasisynchronization of uncertain quaternion-valued chaotic neural networks with time-varying delay for image encryption*, IEEE Transactions on Cybernetics **53**(5), 2023: 3325-3336. https://doi.org/10.1109/TCYB.2022.3176013

[23] Liu X.L., Han G.N., Wu J.S., Shan Z.H., Coatrieux G., Shu H.Z., *Fractional Krawtchouk transform with an application to image watermarking*, IEEE Transactions on Signal Processing **65**(7), 2017: 1894-1908. https://doi.org/10.1109/TSP.2017.2652383

[24] 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

[25] Nan, S.X., Feng, X.F., Wu, Y.F., Zhang H., *Remote sensing image compression and encryption based on block compressive sensing and 2D-LCCCM*, Nonlinear Dynamics **108**(3), 2022: 2705-2729. https://doi.org/10.1007/s11071-022-07335-4

[26] Wei J.J., Zhang M., Tong X.J., *Multi-image compression–encryption algorithm based on compressed sensing and optical encryption*, Entropy **24**(6), 2022: 784. https://doi.org/10.3390/e24060784

[27] Xu Q.Y., Sun K.H., Cao C., Zhu C.X., *A fast image encryption algorithm based on compressive sensing and hyperchaotic map*, Optics and Lasers in Engineering **121**, 2019: 203-214. https://doi.org/10.1016/j.optlaseng.2019.04.011

[28] Xu Q.Y., Sun K.H., He S.B., Zhu C.X., *An effective image encryption algorithm based on compressive sensing and 2D-SLIM*, Optics and Lasers in Engineering **134**, 2020: 106178. https://doi.org/10.1016/j.optlaseng.2020.106178

[29] Gan Z.H., Chai X.L., Bi J.Q., Chen X.H., *Content-adaptive image compression and encryption via optimized compressive sensing with double random phase encoding driven by chaos*, Complex and Intelligent Systems **8**(3), 2022: 2291-2309. https://doi.org/10.1007/s40747-022-00644-6

[30] Man Z.L., Li J.Q., Di X.Q., Liu X., Zhou J., Wang J., Zhang X.X., *A novel image encryption algorithm based on least squares generative adversarial network random number generator*, Multimedia Tools and Applications **80**(18), 2021: 27445-27469. https://doi.org/10.1007/s11042-021-10979-w

[31] Wang X.Y., Zhang J.J., Cao G.H., *An image encryption algorithm based on ZigZag transform and LL compound chaotic system*, Optics and Laser Technology **119**, 2019: 105581. https://doi.org/10.1016/j.optlastec.2019.105581

[32] Setyaningsih E., Wardoyo R., Sari A.K., *Securing color image transmission using compression -encryption model with dynamic key generator and efficient symmetric key distribution*, Digital Communications and Networks **6**(4), 2020: 486-503. https://doi.org/10.1016/j.dcan.2020.02.001

[33] Singh A.K, Chatterjee K., Singh A., *An image security model based on chaos and DNA cryptography for IIoT images*, IEEE Transactions on Industrial Informatics **19**(2), 2023: 1957-1964. https://doi.org/10.1109/TII.2022.3176054

Received June 6, 2024
in revised form December 12, 2024