Optica Applicata, Vol. LIV, No. 2, 2024
DOI: 10.37190/oa240211

Multi-color-image compression-encryption scheme in the quaternion discrete Fresnel domain

Ze-Ting Hu[1], Ping-Ping Zeng[2], Hong-Xing Ding[1], Li-Hua Gong[3], Su-Hua Chen[1,*]

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

[2] College of Science and Technology, Nanchang University,
Jiujiang 332020, China

[3] School of Electronic and Electrical Engineering, Shanghai University of Engineering Science,
Shanghai 201620, China

[*] Corresponding author: chensuhua@ncu.edu.cn

A multiple color images compression-encryption scheme is designed with compressive sensing in the quaternion discrete Fresnel transform. To tackle multiple color images in a holistic manner, the discrete Fresnel transform is extended into the quaternion domain and the images are encrypted with the quaternion discrete Fresnel transform. In this scheme, the RGB color components of plaintext images are simultaneously compressed and encrypted in three mutually independent channels. Then the red, green and blue components are scrambled respectively by a chaos sequence generated by the 2D logistic-sine-coupling map. Each color component matrix is compressed with sparse representation and matrix measurement. Subsequently, the compressed matrices are integrated into the quaternion algebras and re-encrypted by the defined quaternion discrete Fresnel transform. The devised nonlinear cryptosystem originates from the asymmetric phase truncation operation. In decryption, the original color images are reconstructed by the gradient descent with a sparsification algorithm. The proposed multiple color images compression-encryption algorithm is feasible, effective, secure and robust.

Keywords: compressive sensing, quaternion discrete Fresnel transform, 2D-LSCM chaotic system, image compression-encryption algorithm.

1. Introduction

Secure storage and transmission of color images are of increasing importance in the Internet environment. The traditional cryptographic systems (such as DES, IDES and RSA) have some shortcomings in terms of storage space and robustness, thus they are not economical for the modern color image encryption. Image encryption algorithms [1,2] or multi-image encryption algorithms [3-5] have been presented to tackle this issue. Chaos systems were commonly integrated into image encryption algorithms for higher performance, especially security and key sensitivity/space. For instance, a new

1D chaos system was invented for image encryption [6], and a high-dimension chaos system was introduced into color image encryption [7]. To further enhance the performance of chaos systems, several logical maps were combined to constitute a higher-dimensional chaos system. A 2D Logistic-adjusted-sine map (2D-LASM) was designed for image encryption [8]. JASRA *et al.* explored a color image encryption scheme with the hyper-chaos system [9]. Nevertheless, the chaos systems employed in these schemes are all in the spatial domain, which may disrupt the chaotic performance to a certain degree.

Since storage space and transmission bandwidth are two inevitable issues for color images, it is necessary to compress them before further processing. Compressive sensing (CS) [10] has been widely adopted for image compression and encryption [11-14]. Some frequency domain transformations render the image encryption schemes linear, making them difficult to withstand some attacks. To solve this problem, a pioneering image encryption method was implemented with the asymmetric phase truncation (PT) operation [15]. The asymmetric PT can be combined with some orthogonal transforms to derive new nonlinear cryptosystems [16,17]. There still exist small encryption capacity and insufficient reconstruction accuracy in most color image compression and encryption algorithms, a nonlinear multi-color-image compression-encryption algorithm (MCICEA) is designed with the quaternion discrete Fresnel transform (QDFnT). A strong relationship between the keys and image matrices is established to counteract the common attacks. Furthermore, the effective gradient descent with sparsification (GDS) algorithm [18] is borrowed to enhance the reconstruction quality of decryption images.

The remainder of the article is arranged as follows. The detailed introduction of QDFnT is mentioned in Sec. 2. The main steps of the MCICEA are detailed in Sec. 3. In Sec. 4, simulation results are presented and discussed. Finally, a concise conclusion is provided in Sec. 5.

2. Quaternion discrete Fresnel transform

The quaternion discrete Fresnel transform is the combination of generalized discrete Fresnel transform [19] and quaternion algebra. Owing to the non-commutative multiplication of quaternions, there are left-side QDFnT $\hat{\mathbf{X}}_{\mathrm{QL}}$ and right-side one $\hat{\mathbf{X}}_{\mathrm{QR}}$,

$$\hat{\mathbf{X}}_{\mathrm{QL}} = \mathbf{\Psi}^{\mu}\mathbf{X}_{Q} \tag{1}$$

$$\hat{\mathbf{X}}_{\mathrm{QR}} = \mathbf{X}_{Q}^{\mathrm{T}}\mathbf{\Psi}^{\mu} \tag{2}$$

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 $\mu^2 = -1$, and $\mathbf{\Psi}$ denotes the kernel matrix of discrete Fresnel transform [20]. $\mathbf{X}_{\mathrm{Q}}$ is a 1D quaternion signal, *i.e.*,

$$\mathbf{X}_{\mathrm{Q}} = \mathbf{X}_0 + \mathbf{X}_1\mathbf{i} + \mathbf{X}_2\mathbf{j} + \mathbf{X}_3\mathbf{k} \tag{3}$$

After calculating the 1D-QDFnT along x-axis and y-axis, the 2D-QDFnT on a signal $\mathbf{Y}_\mathrm{Q} \in N \times N$ can be expressed as

$$\hat{\mathbf{Y}}_\mathrm{Q} = \mathbf{\Psi}\,\mathbf{Y}_\mathrm{Q}\mathbf{\Psi}^\mathrm{T} \tag{4}$$

The left-side QDFnT can be calculated with a basic algorithm of quaternion [21] and Euler's formula $\mathrm{e}^{\mathbf{j}x} = \cos x + \mathbf{j}\sin x$, and the calculation process is

$$\begin{aligned}\hat{\mathbf{X}}_\mathrm{QL} &= \mathbf{\Psi}^{\mu}\mathbf{X}_Q \\ &= \mathrm{Re}(\mathbf{\Psi}^{\mu}\mathbf{X}_0) + \mu\,\mathrm{Im}(\mathbf{\Psi}^{\mu}\mathbf{X}_0) + \left[\mathrm{Re}(\mathbf{\Psi}^{\mu}\mathbf{X}_1) + \mu\,\mathrm{Im}(\mathbf{\Psi}^{\mu}\mathbf{X}_1)\right]\mathbf{i} \\ &\quad + \left[\mathrm{Re}(\mathbf{\Psi}^{\mu}\mathbf{X}_2) + \mu\,\mathrm{Im}(\mathbf{\Psi}^{\mu}\mathbf{X}_2)\right]\mathbf{j} + \left[\mathrm{Re}(\mathbf{\Psi}^{\mu}\mathbf{X}_3) + \mu\,\mathrm{Im}(\mathbf{\Psi}^{\mu}\mathbf{X}_3)\right]\mathbf{k} \\ &= \lambda_1 + \beta_1\mathrm{i} + \chi_1\mathbf{j} + \delta_1\mathbf{k}\end{aligned} \tag{5}$$

$$\begin{cases}\lambda_1 = \mathrm{Re}(\mathbf{\Psi}^{\mu}\mathbf{X}_0) - a_0\,\mathrm{Im}(\mathbf{\Psi}^{\mu}\mathbf{X}_1) - a_1\,\mathrm{Im}(\mathbf{\Psi}^{\mu}\mathbf{X}_2) - a_2\,\mathrm{Im}(\mathbf{\Psi}^{\mu}\mathbf{X}_3) \\ \beta_1 = \mathrm{Re}(\mathbf{\Psi}^{\mu}\mathbf{X}_1) + a_0\,\mathrm{Im}(\mathbf{\Psi}^{\mu}\mathbf{X}_0) + a_1\,\mathrm{Im}(\mathbf{\Psi}^{\mu}\mathbf{X}_3) - a_2\,\mathrm{Im}(\mathbf{\Psi}^{\mu}\mathbf{X}_2) \\ \chi_1 = \mathrm{Re}(\mathbf{\Psi}^{\mu}\mathbf{X}_2) - a_0\,\mathrm{Im}(\mathbf{\Psi}^{\mu}\mathbf{X}_3) + a_1\,\mathrm{Im}(\mathbf{\Psi}^{\mu}\mathbf{X}_0) + a_2\,\mathrm{Im}(\mathbf{\Psi}^{\mu}\mathbf{X}_1) \\ \delta_1 = \mathrm{Re}(\mathbf{\Psi}^{\mu}\mathbf{X}_3) + a_0\,\mathrm{Im}(\mathbf{\Psi}^{\mu}\mathbf{X}_2) - a_1\,\mathrm{Im}(\mathbf{\Psi}^{\mu}\mathbf{X}_1) + a_2\,\mathrm{Im}(\mathbf{\Psi}^{\mu}\mathbf{X}_0)\end{cases} \tag{6}$$

Similarly, the right-side QDFnT can be calculated,

$$\hat{\mathbf{X}}_\mathrm{QR} = \mathbf{X}_Q^\mathrm{T}\mathbf{\Psi}^{\mu} = \lambda_2 + \beta_2\mathrm{i} + \chi_2\mathbf{j} + \delta_2\mathbf{k} \tag{7}$$

$$\begin{cases}\lambda_1 = \mathrm{Re}(\mathbf{\Psi}^{\mu}\mathbf{X}_0) - a_0\,\mathrm{Im}(\mathbf{\Psi}^{\mu}\mathbf{X}_1) + a_1\,\mathrm{Im}(\mathbf{\Psi}^{\mu}\mathbf{X}_2) - a_2\,\mathrm{Im}(\mathbf{\Psi}^{\mu}\mathbf{X}_3) \\ \beta_1 = \mathrm{Re}(\mathbf{\Psi}^{\mu}\mathbf{X}_1) + a_0\,\mathrm{Im}(\mathbf{\Psi}^{\mu}\mathbf{X}_0) + a_1\,\mathrm{Im}(\mathbf{\Psi}^{\mu}\mathbf{X}_3) - a_2\,\mathrm{Im}(\mathbf{\Psi}^{\mu}\mathbf{X}_2) \\ \chi_1 = \mathrm{Re}(\mathbf{\Psi}^{\mu}\mathbf{X}_2) + a_0\,\mathrm{Im}(\mathbf{\Psi}^{\mu}\mathbf{X}_3) - a_1\,\mathrm{Im}(\mathbf{\Psi}^{\mu}\mathbf{X}_0) + a_2\,\mathrm{Im}(\mathbf{\Psi}^{\mu}\mathbf{X}_1) \\ \delta_1 = \mathrm{Re}(\mathbf{\Psi}^{\mu}\mathbf{X}_3) - a_0\,\mathrm{Im}(\mathbf{\Psi}^{\mu}\mathbf{X}_2) + a_1\,\mathrm{Im}(\mathbf{\Psi}^{\mu}\mathbf{X}_1) - a_2\,\mathrm{Im}(\mathbf{\Psi}^{\mu}\mathbf{X}_0)\end{cases} \tag{8}$$

Likely, the 2D-QDFnT on signal $\mathbf{Y}_Q \in N \times N$ can be also computed. First of all, the left-side 1D-QDFnT ($\mathrm{QDFnT_L}$) is calculated on the x-axis, and then the subsequent result is put on y-axis to carry out the right-side 1D-QDFnT ($\mathrm{QDFnT_R}$) to generate the final calculation result,

$$\hat{\mathbf{Y}}_\mathrm{Q} = \mathrm{QDFnT_R}\left[\mathrm{QDFnT_L}(\mathbf{Y}_Q)\right] \tag{9}$$

3. Proposed multi-color-image CEA

3.1. Compression and encryption

Our MCICEA is given in Fig. 1, and its detailed steps are below.

Step 1: RGB separation. n original color images $\{f_i(x, y) | i = 1, 2, ..., n\}$ of size $N \times N$ are separated into R, G, B components respectively to yield $3n$ gray image matrices. The image matrices are grouped in terms of the color components for compression and encryption.

Step 2: Scrambling. Let the 2D-LSCM chaotic system produce three sets of chaos sequences of length n, and the three sets of chaos sequence are sorted to acquire their respective index sequences ε_1, ε_2, ε_3. Subsequently, each group of image matrices is scrambled by the index sequence.

Step 3: Images compression. Firstly, the curvelet transform is performed on n scrambled gray image matrices of red components $\{r_i(x, y) | i = 1, 2, ..., n\}$ for sparse processing, and then the independently distributed Gaussian random measurement matrix $\mathbf{\Phi} \in R^{M \times N}$ is selected for CS sampling to acquire four encryption image matrices $\mathbf{R}_1$, $\mathbf{R}_2$, $\mathbf{R}_3$, $\mathbf{R}_4$ of size $(N/4) \times N$. Similarly, $\mathbf{G}_1$, $\mathbf{G}_2$, $\mathbf{G}_3$, $\mathbf{G}_4$ ($\mathbf{B}_1$, $\mathbf{B}_2$, $\mathbf{B}_3$, $\mathbf{B}_4$) can also be generated from the green (blue) components.

Step 4: Quaternion representation (QR). First of all, the three groups of images are normalized. Subsequently, the quaternion representation of the three components can be expressed as

$$f_{\mathrm{QR}} = f_{R_1} + f_{R_2}\mathbf{i} + f_{R_3}\mathbf{j} + f_{R_4}\mathbf{k} \tag{10}$$

$$f_{\mathrm{QG}} = f_{G_1} + f_{G_2}\mathbf{i} + f_{G_3}\mathbf{j} + f_{G_4}\mathbf{k} \tag{11}$$

$$f_{\mathrm{QB}} = f_{B_1} + f_{B_2}\mathbf{i} + f_{B_3}\mathbf{j} + f_{B_4}\mathbf{k} \tag{12}$$

Step 5: Random phase mask (RPM) encoding and quaternion discrete Fresnel transform.

1) Fusion image of each group is right-multiplied with the quaternion RPM $\mathrm{RPM}_k = \exp(\boldsymbol{\mu} 2\pi \mathbf{m}_i)$, $k = 1, 2, 3$. $\boldsymbol{\mu}$ is a pure unit quaternion, $\mathbf{m}_i$ is a chaos matrix yielded by the 2D-LSCM chaotic system.

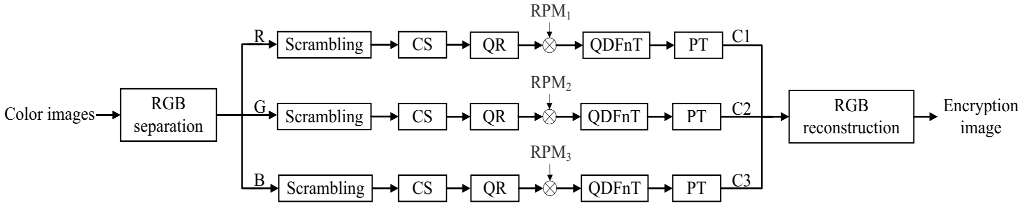


Fig. 1. Encryption process of proposed algorithm.

2) The encoded 2D signal is subjected to the left-side QDFnT, and the result should be put on the y-axis. Then the right-side QDFnT is performed to obtain the final result,

$$\hat{f}_Q(u, v) = \mathbf{\Psi}\left[f_Q \exp(\boldsymbol{\mu} 2\pi \mathbf{m}_i)\right]\mathbf{\Psi}^{\mathrm{T}} \tag{13}$$

where $\mathbf{\Psi}$ is the kernel matrix of 1D QDFnT, and f_Q is f_{QR}, f_{QG} or f_{QB}.

Step 6: Asymmetric phase truncation. The nonlinear PT operation is executed on the enciphered images of each group $\hat{f}_Q(u, v)$. The phase information generated by the nonlinear PT can be treated as the private keys $k_{\mathrm{R}}(u, v)$, $k_{\mathrm{G}}(u, v)$, $k_{\mathrm{B}}(u, v)$, while the amplitudes produced by phase reservation are viewed as the ciphertext images. The final encryption image is generated by executing the RGB reconstruction algorithm on ciphertexts $\mathbf{C}_1$, $\mathbf{C}_2$ and $\mathbf{C}_3$.

3.2. Decryption process

Figure 2 illustrates the image decryption and decompression process.

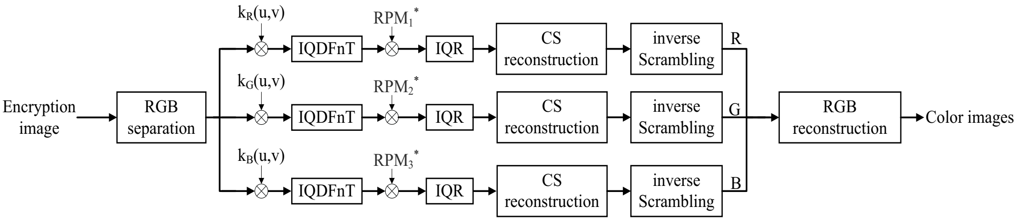


Fig. 2. Decryption process.

First of all, the encryption images are divided into three components through RGB separation. Taking ciphertext image 1 ($\mathbf{C}_1$) as an example, it is right-multiplied by the corresponding private key. Subsequently, the inverse quaternion discrete Fresnel transform (IQDFnT) is performed on the multiplication result. Secondly, the output of IQDFnT is left-multiplied with $\mathrm{RPM}_k^* = \exp(-\mu 2\pi \mathbf{m}_i)$, $k = 1, 2, 3$, and then four compressed matrices $\mathbf{R}_1'$, $\mathbf{R}_2'$, $\mathbf{R}_3'$, $\mathbf{R}_4'$ can be retrieved by the inverse quaternion representation (IQR) operation. Thirdly, the compression matrices are reconstructed based on the GDS algorithm. Finally, the correct index sequence ε_1 will be selected for the inverse scrambling operation to acquire the decryption image matrix of red component.

Similarly, the decryption image matrix of green (blue) components can be acquired with the corresponding key and the associated RPM. Finally, the decryption images $f_1(x, y)$, $f_2(x, y)$, ..., $f_n(x, y)$, can be retrieved one by one with correct indexes.

4. Simulation results and performance analyses

To demonstrate the feasibility of our proposed MCICEA, numerical experiments were carried out on a PC with Intel (R) Core (TM) i5-6300HQ CPU @2.30 GHz and the MATLAB (R2016a).

4.1. Encryption and decryption result

Four color test images are *Baboon*, *Airplane*, *Peppers* and *Tree* of size exhibited in Figs. 3 (a)–(d), respectively. The major control parameter w of the 2D-LSCM is 0.87, and the initial position parameters x_0 and y_0 are set as 0.25 and 0.125, respectively. During image compression based on CS, the sampling rate of each image takes as 0.25, and the independently distributed Gaussian random measurement matrix of size 64 × 256 is randomly generated by the computer. During the decryption, the initial parameters δ_{2s} and γ of the GDS algorithm for image reconstruction are 0.28 and 1.28, respectively. The fused encryption image of the four original images and its R, G and B components are shown in Figs. 3 (e)–(h), respectively. The corresponding deciphered images of the encryption one of the four original color images are demonstrated in Figs. 3 (i)–(l), respectively.

To quantify the quality of decryption images, the peak signal-to-noise ratio (PSNR) is utilized to measure the numerical relationship between original images and decryption ones.

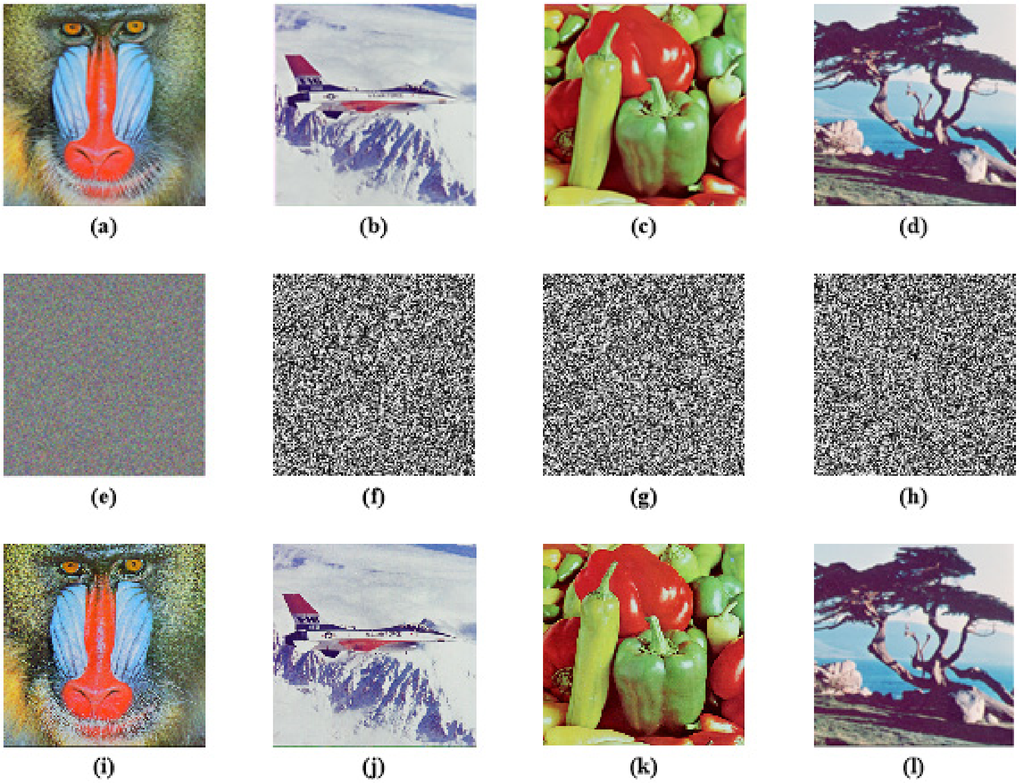


Fig. 3. Test results: (a) *Baboon*, (b) *Airplane*, (c) *Peppers*, (d) *Tree*; (e)–(h) Encryption images; (i)–(l) Corresponding decryption images.

$$\mathrm{PSNR} = 10\lg \frac{255^2 N^2}{\sum_{x=1}^{N}\sum_{y=1}^{N}\left[\mathbf{D}(x,y) - \mathbf{O}(x,y)\right]^2} \tag{14}$$

where $\mathbf{O}(x, y)$ and $\mathbf{D}(x, y)$ denote the gray pixel values of each color component in the plaintext images and the corresponding decryption images, respectively. As compiled in Table 1, most PSNR values of the four decryption images with our proposed algorithm are larger than 34 dB, so the proposed MCICEA is feasible.

Table 1. PSNR values of various decryption images.

Decryption images	PSNR [dB]			
	Red	Green	Blue	Average
Baboon	34.6638	35.4480	36.5129	35.5416
Airplane	32.6355	34.9189	34.8596	34.1380
Peppers	32.6907	34.4813	34.1074	33.7598
Tree	34.0793	36.3784	35.3276	35.2618

4.2. Compression performance

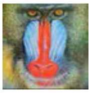
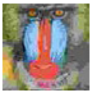
The SSIM value [22] of images is considered to measure the accurate statistical relationship between original images and decryption ones.

$$\mathrm{SSIM} = \frac{\sigma_{xy}}{\sigma_x \sigma_y}\,\frac{2\bar{x}\,\bar{y}}{\bar{x}^2 + \bar{y}^2}\,\frac{2\sigma_x\sigma_y}{\sigma_x^2 + \sigma_y^2} \tag{15}$$

where $\mathbf{x} \in R^{N \times N}$ $(\mathbf{y} \in R^{N \times N})$ is the original (decryption) image, while $\bar{x}$ $(\bar{y})$ is the average pixel value of corresponding image, σ_x (σ_y) is the standard deviation of $\mathbf{x}$ $(\mathbf{y})$, while σ_{xy} is the covariance between $\mathbf{x}$ and $\mathbf{y}$. The SSIM index ranges in [–1, 1]. Table 2 lists the decryption images and the corresponding average SSIM values of the original image *Baboon* under different compression ratios. The quality loss of decryption images is slight even though the compression ratio reaches 12.5%.

The GDS algorithm is picked up for image reconstruction. Compared with other traditional image reconstruction algorithms, for instance, NSL0 [13] and OMP [23], Fig. 4 displays the reconstruction quality of the three image reconstruction algorithms

Table 2. Average SSIM and decryption image under various compression ratios.

Original image	Compression ratio [%]	Decryption image	Average SSIM
	50/25/12.5/6.25	/  / / 	0.9614/0.9037/0.8352/0.7208

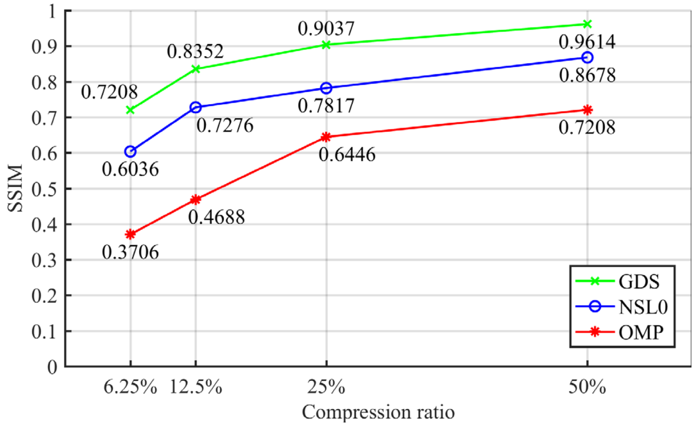


Fig. 4. SSIM values of different reconstruction algorithms.

under various compression ratios. Obviously, the GDS algorithm visibly outperforms the traditional reconstruction algorithms, *i.e.*, OMP and NSL0, in terms of the reconstruction quality of compressed images.

4.3. Histogram

The histograms of color components in the four original images are given in Figs. 5 and 6. One can observe that the histograms of the plaintext images fluctuate seriously and differ from each other. However, those of the three ciphertext images in Fig. 7 tend

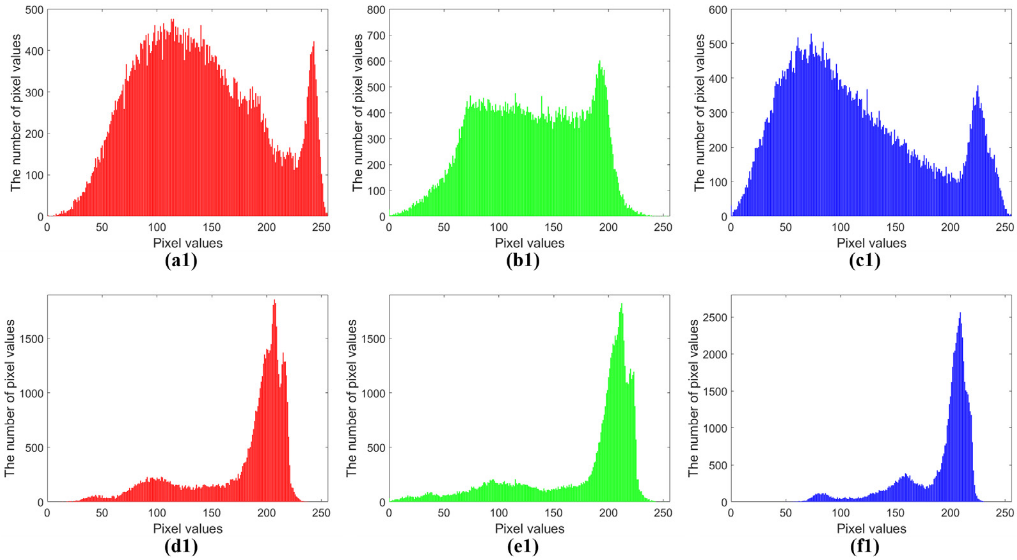


Fig. 5. Histograms: (a1)–(c1) are R, G, B components of *Baboon*; (d1)–(f1) are R, G, B components of *Airplane*.

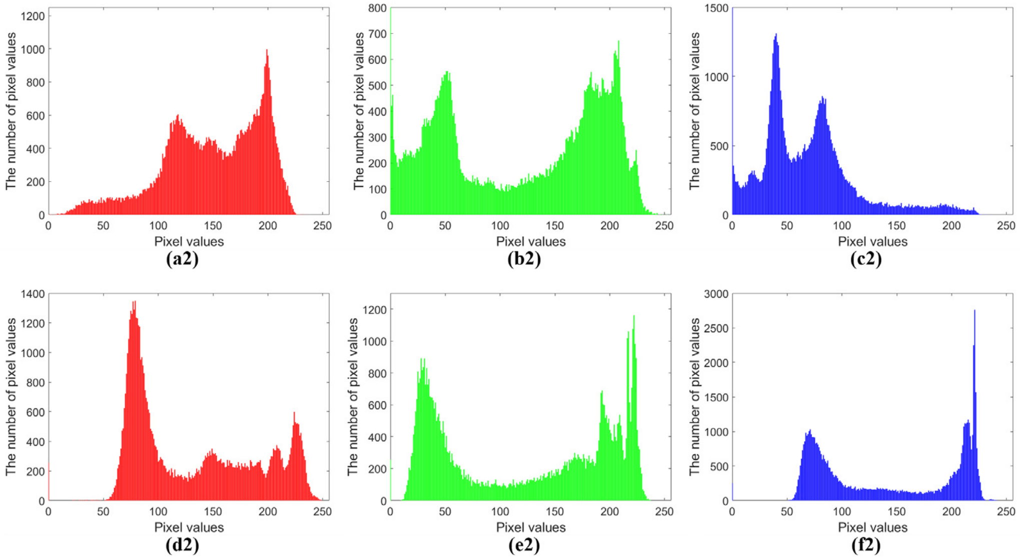


Fig. 6. Histograms: (a2)–(c2) are R, G, B components of *Peppers*; (d2)–(f2) are R, G, B components of *Tree*.

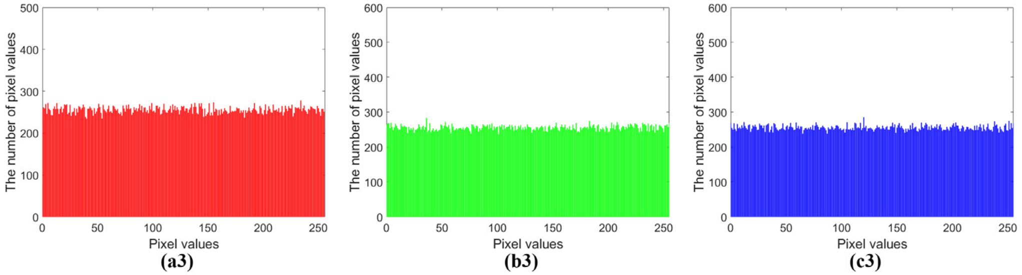


Fig. 7. Histograms: (a3)–(c3) are ciphertext 1, ciphertext 2, and ciphertext 3, respectively.

to be flat and similar to each other, without apparent fluctuations. In consequence, the proposed muti-color-image cryptosystem can withstand the statistical attacks.

4.4. Key space

The secret keys of the proposed MCICEA are three RPMs P_1, P_2, P_3, three random sequences ε_1, ε_2, ε_3, controlled by the initial values x_0, y_0, control parameter w of the 2D-LSCM chaos system, and pseudorandom phases k_R, k_G, k_B generated by the nonlinear PT.

Let the computing accuracy of a computer be 10^{-15}. For the pseudorandom phase image of size 256 × 256, the amounts of attempts required to retrieve three pseudorandom phase images are $(256 \times 256)^3$. Moreover, the range of control parameter w is (0.72, 1]. In total, the key space is about 7.8×10^{58} and greater than 2^{195}, which makes the brute-

Table 3. Key space comparison with other algorithms.

Scheme	Proposed scheme	[24]	[25]	[1]	[26]
Key space	$\geq 2^{195}$	$> 2^{100}$	$\geq 2^{130}$	$> 2^{138}$	$\geq 2^{149}$

force attack impossible. Besides, the key space comparisons with other typical algorithms are collected in Table 3. Table 3 clearly shows that the key space of the proposed MCICEA is significantly larger than those of the other classical algorithms, indicating a better resistance to the brute-force attack.

4.5. Correlation

To further verify the ability of the proposed MCICEA to counteract the statistical attacks, the correlation of adjacent pixels is considered. 32768 pairs of adjacent pixels along horizontal (vertical, diagonal) directions were randomly selected from the four original color images and the enciphered one. Subsequently, the correlation distributions of R, G and B components in the original images and the encryption one are shown in Figs. 8 and 9, respectively.

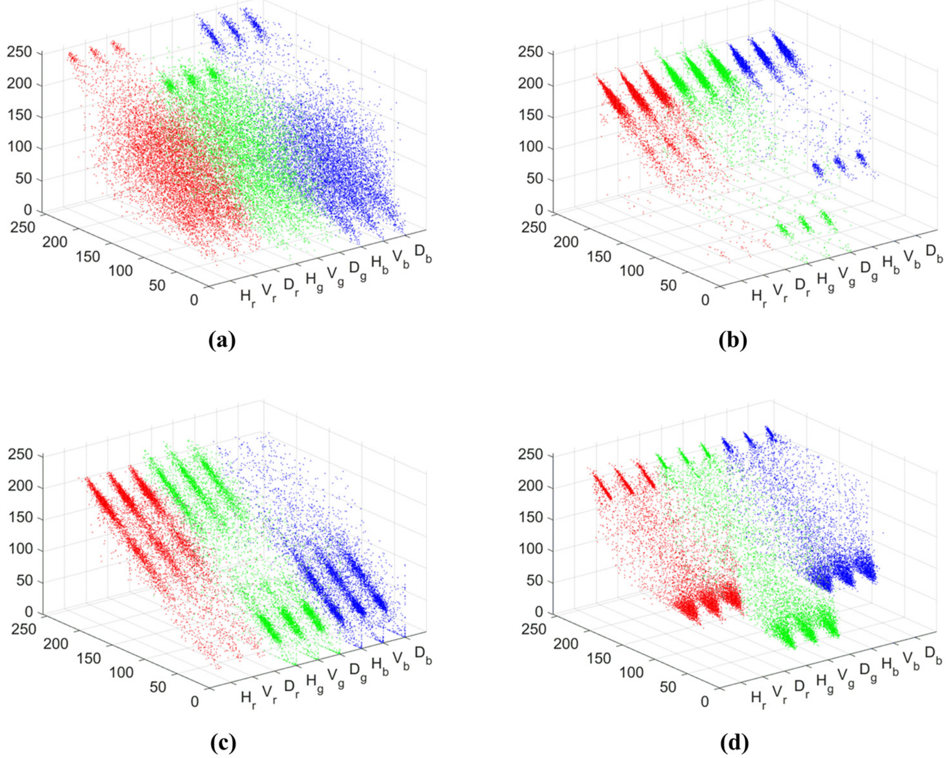
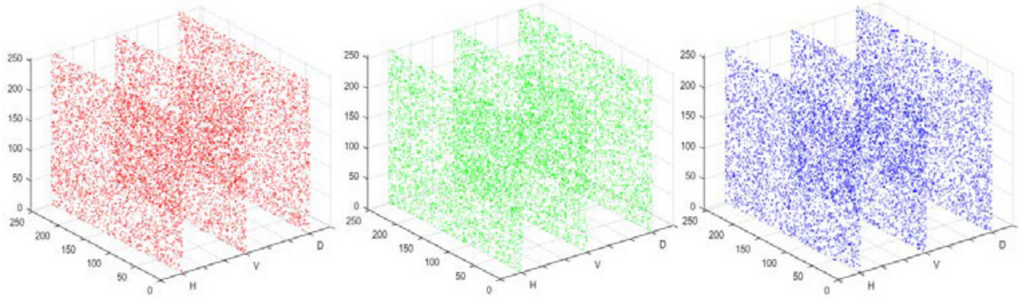


Fig. 8. Correlation distribution in the R, G and B components of plaintext images along horizontal, vertical and diagonal directions: (a) *Baboon*, (b) *Airplane*, (c) *Peppers*, (d) *Tree*.



(a) (b) (c)

Fig. 9. Correlation distribution in ciphertext image along horizontal, vertical and diagonal directions: (a) red, (b) green, and (c) blue.

$$\mathrm{CC} = \frac{\sum_{i=1}^{N}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{N}(x_i - \bar{x})^2 \sum_{i=1}^{N}(y_i - \bar{y})^2}} \tag{16}$$

$$\bar{x} = \frac{1}{N}\sum_{i=1}^{N} x_i, \quad \bar{y} = \frac{1}{N}\sum_{i=1}^{N} y_i \tag{17}$$

As gathered in Table 4, the CC values between adjacent pixels in the enciphered images are shown in Table 5. Although the R, G and B components in the original color images are tightly correlated, the CC values in the ciphertext decrease towards 0 significantly. Therefore, it is unlikely for an illegal attacker to grab enough information about the original images with the statistical attack.

Table 4. CC between adjacent pixels of original images.

Images	Components	Horizontal direction	Vertical direction	Diagonal direction
Baboon	R/G/B	0.9118/0.9399/0.9329	0.9640/0.9063/0.9153	0.9115/0.9247/0.9621
Airplane		0.9365/0.9295/0.9207	0.9105/0.9284/0.9100	0.9247/0.9205/0.9408
Peppers		0.9428/0.9492/0.9631	0.9343/0.9095/0.9599	0.9264/0.9285/0.9108
Tree		0.9452/0.9534/0.9502	0.9544/0.9679/0.9599	0.9225/0.9370/0.9361

Table 5. CC of the encryption images with different algorithms.

Algorithms	Components	Horizontal direction	Vertical direction	Diagonal direction
Proposed scheme	R/G/B	−0.0019/0.0021/0.0017	0.0023/−0.0012/−0.0014	0.0024/0.0023/0.0016
[27]		0.0090/−0.0027/−0.0155	−0.0013/−0.0051/−0.0078	−0.0025/−0.0103/0.0099
[28]		0.0065/0.0053/0.0061	0.0018/0.0047/0.0028	0.0099/0.0044/0.0036

4.6. Key sensitivity

To estimate the key sensitivity of the current image cryptosystem, the mean square error (MSE) between encryption image and decryption one is usually adopted. Figure 10 displays the MSE curves with $w_0 + 0.28 \times 10^{-15}$, $x_0 + 10^{-15}$ and $y_0 + 10^{-15}$, respectively. One can see that the MSE values fluctuate dramatically even if the key deviates slightly. Moreover, Fig. 11 indicates that the rough contour of the original images cannot be reconstructed even though only one key has a subtle deviation while the other keys are kept intactly. In other words, the keys in the MCICEA are sensitive enough.

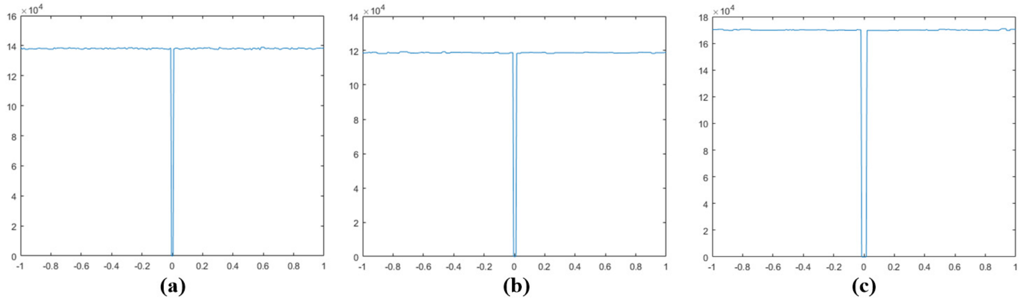


Fig. 10. MSE curves with deviated keys: (a) $w_0 + 0.28 \times 10^{-15}$, (b) $x_0 + 10^{-15}$, and (c) $y_0 + 10^{-15}$.

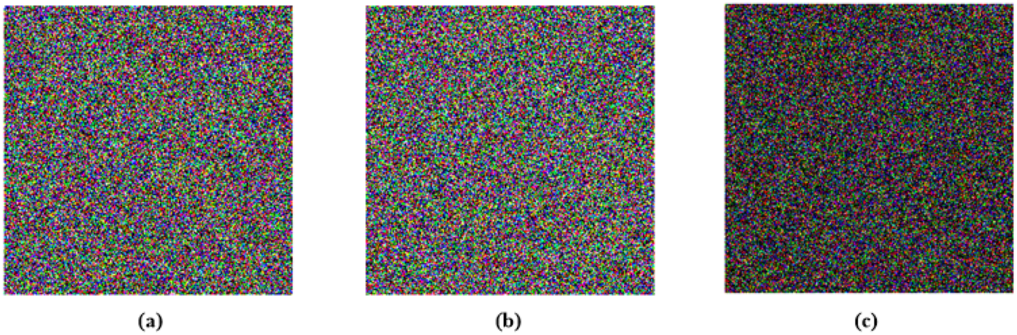


Fig. 11. Decryption image *Airplane* with the deviated keys: (a) $w_0 + 0.28 \times 10^{-15}$, (b) $\lambda_1 + 10^{-15}$, and (c) $p_1 + 10^{-5}$.

4.7. Noise attack

Three typical noise attacks, *i.e.*, white Gaussian noise attack, Salt-and-Pepper noise attack and Speckle noise attack are evaluated. To avoid contingency in the experiment, the PSNR values of different images are calculated under various noise intensities. The intensities of white Gaussian noise and Speckle noise are determined by their variances based on zero-mean, while the intensity of Salt-and-Pepper noise depends on its noise density.

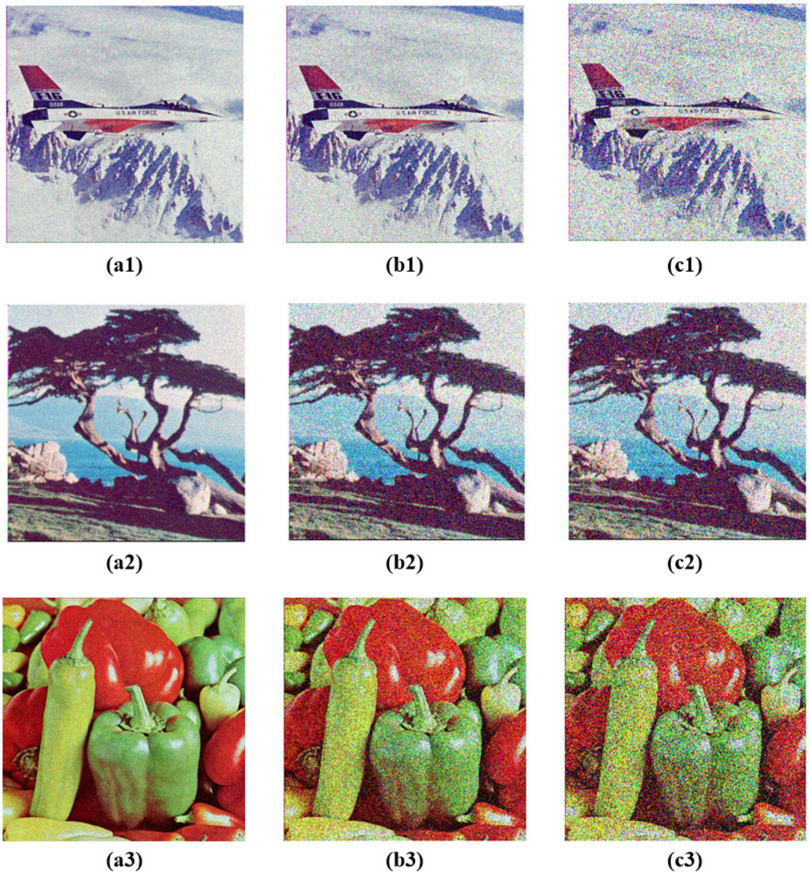


Fig. 12. Decryption images under different noises: (a1)–(c1) *Airplane* under Speckle noise of intensities 0.005, 0.01, and 0.05, respectively; (a2)–(c2) *Tree* under white Gaussian noise of intensities 0.001, 0.005, and 0.01, respectively; (a3)–(c3) *Peppers* under Salt-and-Pepper noise of intensities 0.005, 0.01, and 0.05, respectively.

The decryption images *Airplane* under the Speckle noise of different intensities are exhibited in Figs. 12(a1)–(c1). Similarly, the decryption images *Tree* under white Gaussian noise (*Peppers* under Salt-and-Pepper noise) of different intensities are displayed in Figs. 12 (a2)–(c2) (Fig. 12 (a3)–(c3)). Table 6 lists the average PSNR values of the three components of the original color image *Baboon* under different types of

Table 6. Average PSNR of *Baboon* under different noises of various noise intensities.

Noise type	Noise intensity	Average PSNR [dB]
Speckle noise	0.005/0.01/0.05	26.3323/19.4231/13.5597
White Gaussian noise	0.001/0.005/0.01	31.4107/22.5085/14.5376
Salt-and-Pepper noise	0.005/0.01/0.05	30.5922/18.7482/11.4223

noises and different noise intensities. As a consequence, the proposed MCICEA is sufficiently robust against the common noise attacks, since the decryption images from noisy encryption ones are still recognizable under certain degree of noise intensity.

4.8. Cropping attack

The images may be partially lost or even intercepted during the internet communication, so a cryptosystem should withstand the cropping attack. As shown in Figs. 13(a)–(d), 1/16, 1/8, 1/4, and 1/2 of the encryption image are clipped respectively. Correspondingly, the decryption images *Peppers* and *Baboon* are exhibited in Fig. 13, and their

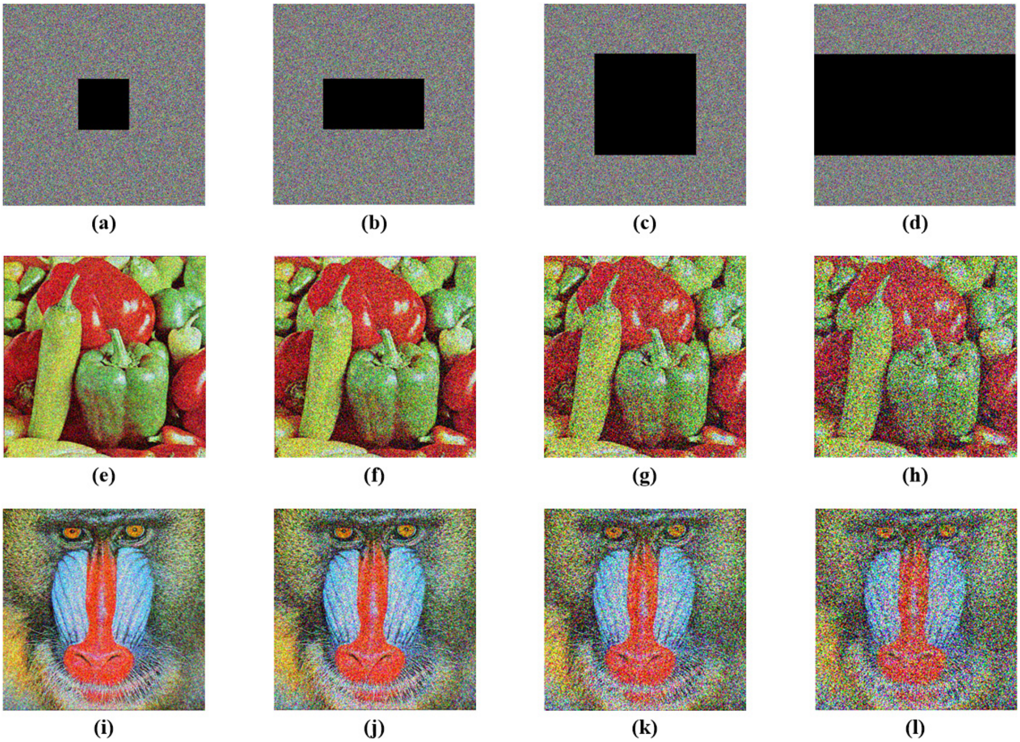


Fig. 13. Results of cropping attack: (a)–(d) Encryption images with 1/16, 1/8, 1/4, and 1/2 cropped, respectively; (e)–(h) Corresponding decryption images *Peppers* with 1/16, 1/8, 1/4, and 1/2 cropped, respectively; (i)–(l) Corresponding decryption images *Baboon* with 1/16, 1/8, 1/4, and 1/2 cropped, respectively.

Table 7. Average PSNR against cropping attack with different cropping proportions.

Images	Cropping proportion	Average PSNR [dB]
Peppers	$\frac{1}{16}/\frac{1}{8}/\frac{1}{4}/\frac{1}{2}$	24.1808/18.1883/15.5204/12.8360
Baboon		24.8238/18.5052/15.5947/11.9547
[29]		20.5700/17.5700/14.5900/11.5800
[30]	$\frac{1}{4}/\frac{1}{2}$	11.9500/8.9500

corresponding average PSNR values of the three color components are listed in Table 7. Compared with [29] and [30], one can observe that the main contours of the deciphered image remain visible even though the data loss is up to half. As a result, the MCICEA is robust enough against the cropping attack.

4.9. Chosen-plaintext attack

For the common chosen-plaintext attack, attackers usually choose some plaintexts and their corresponding ciphertexts to derive the secret key. Since the coefficients of the chaos sequence for scrambling in our scheme are strongly related to the selected plaintext images, it is impossible to obtain the actual key by the chosen-plaintext attack. The original images cannot be retrieved with the incorrect keystream, even if the attackers have intercepted the encryption image. Therefore, the MCICEA is secure enough to withstand the chosen-plaintext attack strategy and the other specific attack methods.

4.10. Efficiency

As presented in Fig. 14 (a), the encryption process of the proposed MCICEA mainly includes five parts: scrambling, compression, encoding and QDFnT, phase truncation. Apparently, the scrambling process takes the longest time since the random sequences used for scrambling need to be generated after a large number of iterations. Similarly, the decryption process can be divided into five parts, and their corresponding time and their respective percentages are given in Fig. 14(b). It is evident that the combined process of decoding and IQDFnT consumes the most time, primarily because generating the transpose of the kernel matrix in the discrete Fresnel domain is more time-consuming than in the time domain.

Besides, the proposed MCICEA can process multiple color images concurrently, and the total time for encryption and decryption *versus* the number of images processed

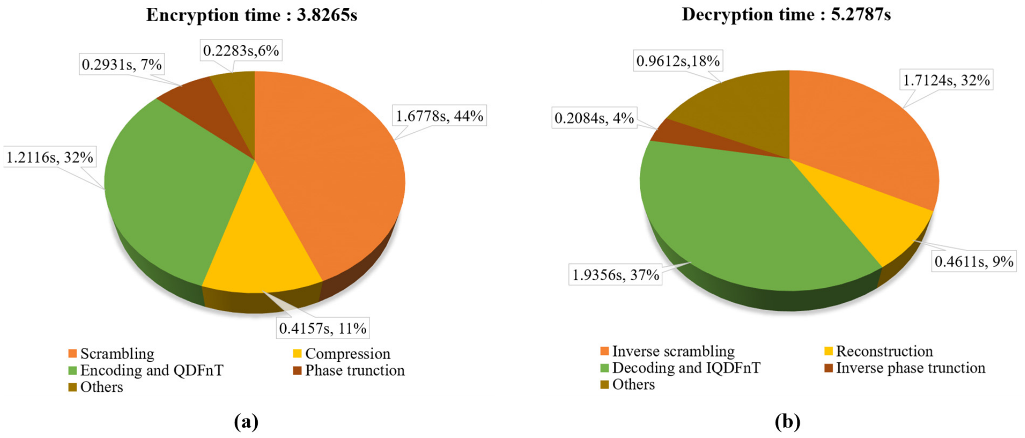


Fig. 14. Time and percentage of each part: (a) Encryption time, and (b) decryption time.

Table 8. Time *versus* different numbers of plaintext images.

Number of images	Encryption/decryption time [s]	Total time [s]
2	2.9352/3.6935	6.6287
4	3.8265/5.2787	9.1052
8	5.5734/6.5218	12.0952
16	7.9802/9.6724	17.6526
32	10.8716/12.2846	23.1562

is compiled in Table 8. It can be observed that the proposed MCICEA demonstrates acceptable performance in both encryption and decryption efficiency.

5. Conclusion

The quaternion discrete Fresnel transform is defined firstly. A multi-color-image compression-encryption scheme is presented by combining the quaternion discrete Fresnel transform with compressive sensing. The images separated by the RGB components are then scrambled by the 2D-LSCM. The compressed images are further re-encrypted by the quaternion discrete Fresnel transform, and the subsequent results are manipulated with the nonlinear phase truncation. Moreover, the decryption process mainly contains the inverse scrambling, the inverse quaternion discrete Fresnel transform and the image reconstruction. Simulation results verify the feasibility as well as the efficiency of the presented multi-color-image encryption scheme. The presented scheme with enough key sensitivity and key space can stand up to typical noise attack, statistical attack, cropping attack, even the chosen-plaintext attack. Especially, the quality of the reconstructed images by the GDS algorithm outperforms those of the reconstructed images with the traditional methods.

Declaration of competing interest

The authors declare that there are no conflict of interests.

Acknowledgement

This work is supported by the National Natural Science Foundation of China (Grant No. 61861029), the Science & Technology Planning Project of Shanghai (Grant No. 23010501800), and the Science and Technology Research Project of Jiangxi Education Department (GJJ2203915).

References

[1] HUA Z.Y., ZHU Z.H., YI S., ZHANG Z., HUANG H.J., *Cross-plane colour image encryption using a two -dimensional logistic tent modular map*, Information Sciences **546**, 2021: 1063-1083. https://doi.org/10.1016/j.ins.2020.09.032

[2] LAI Q., HU G.W., ERKAN U., TOKTAS A., *A novel pixel-split image encryption scheme based on 2D Salomon map*, Expert Systems with Applications **213**, 2023: 118845. https://doi.org/10.1016/j.eswa.2022.118845

[3] LUAN G.Y., ZHONG Z., SHAN M.G., *Optical multiple-image encryption in discrete multiple-parameter fractional Fourier transform scheme using complex encoding, theta modulation and spectral fusion*, Optica Applicata **51**(1), 2021: 121-134. https://doi.org/10.37190/oa210110

[4] 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

[5] Zhou N.R., Hu L.L., Huang Z.W., Wang M.M., Luo G.S., *Novel multiple color images encryption and decryption scheme based on a bit-level extension algorithm*, Expert Systems with Applications **238**, 2024: 122052. https://doi.org/10.1016/j.eswa.2023.122052

[6] Zhou W.J., Wang X.Y., Wang M.X., Li D.Y., *A new combination chaotic system and its application in a new Bit-level image encryption scheme*, Optics and Lasers in Engineering **149**, 2022: 106782. https://doi.org/10.1016/j.optlaseng.2021.106782

[7] 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

[8] Hua Z.Y., Zhou Y.C., *Image encryption using 2D Logistic-adjusted-Sine map*, Information Sciences **339**, 2016: 237-253. https://doi.org/10.1016/j.ins.2016.01.017

[9] Jasra B., Moon A.H., *Color image encryption and authentication using dynamic DNA encoding and hyper chaotic system*, Expert Systems with Applications **206**, 2022: 117861. https://doi.org/10.1016/j.eswa.2022.117861

[10] Donoho D.L., *Compressed sensing*, IEEE Transactions on Information Theory **52**(4), 2006: 1289 -1306. https://doi.org/10.1109/TIT.2006.871582

[11] Ye G.D., Liu M., Wu M.F., *Double image encryption algorithm based on compressive sensing and elliptic curve*, Alexandria Engineering Journal **61**(9), 2022: 6785-6795. https://doi.org/10.1016/j.aej.2021.12.023

[12] 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

[13] Mohimani H., Babaie-Zadeh M., Jutten C., *A fast approach for overcomplete sparse decomposition based on smoothed ℓ^0 norm*, IEEE Transactions on Signal Processing **57**(1), 2009: 289-301. https://doi.org/10.1109/TSP.2008.2007606

[14] Li X.L., Zhang B., Wang K., Li Z.D., *A multi-image encryption-then-compression scheme based on parallel compressed sensing*, Optik **290**, 2023: 171304. https://doi.org/10.1016/j.ijleo.2023.171304

[15] Qin W., Peng X., *Asymmetric cryptosystem based on phase-truncated Fourier transforms*, Optics Letters **35**(2), 2010: 118-120. https://doi.org/10.1364/OL.35.000118

[16] Huang Z.J., Cheng S., Gong L.H., Zhou N.R., *Nonlinear optical multi-image encryption scheme with two-dimensional linear canonical transform*, Optics and Lasers in Engineering **124**, 2020: 105821. https://doi.org/10.1016/j.optlaseng.2019.105821

[17] Yadav A.K., Singh P., Saini I., Singh K., *Asymmetric encryption algorithm for colour images based on fractional Hartley transform*, Journal of Modern Optics **66**(6), 2019: 629-642. https://doi.org/10.1080/09500340.2018.1559951

[18] Garg R., Khandekar R., *Gradient descent with sparsification: an iterative algorithm for sparse recovery with restricted isometry property*, Proceedings of the 26th Annual International Conference on Machine Learning, 2009: 337-344. https://doi.org/10.1145/1553374.1553417

[19] Aizenberg I., Astola J.T., *Discrete generalized Fresnel functions and transforms in an arbitrary discrete basis*, IEEE Transactions on Signal Processing **54**(11), 2006: 4261-4270. https://doi.org/10.1109/TSP.2006.881189

[20] Xing O.Y., Antony C., Gunning F., Zhang H.Y., Guan Y.L., *Discrete Fresnel transform and its circular convolution*, arXiv:1510.00574, 2015. https://doi.org/10.48550/arXiv.1510.00574

[21] Hamilton W.R., *Elements of Quaternions*, Longmans, Green(London), 1866.

[22] 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

[23] Chen S.S.B., Donoho D.L., Saunders M.A., *Atomic decomposition by basis pursuit*, SIAM Review **43**(1), 2001: 129-159. https://doi.org/10.1137/S003614450037906X

[24] ZHOU N.R., JIANG H., GONG L.H., XIE X.W., *Double-image compression and encryption algorithm based on co-sparse representation and random pixel exchanging*, Optics and Lasers in Engineering **110**, 2018: 72-79. https://doi.org/10.1016/j.optlaseng.2018.05.014

[25] PAK C., AN K., JANG P., KIM J. KIM S., *A novel bit-level color image encryption using improved 1D chaotic map*, Multimedia Tools and Applications **78**(9), 2019: 12027-12042. https://doi.org/10.1007/s11042-018-6739-1

[26] CHEN J.X., ZHANG Y., QI L., FU C., XU L.S., *Exploiting chaos-based compressed sensing and cryptographic algorithm for image encryption and compression*, Optics and Laser Technology **99**, 2018: 238-248. https://doi.org/10.1016/j.optlastec.2017.09.008

[27] WANG X.Y., ZHANG H.L., BAO X.M., *Color image encryption scheme using CML and DNA sequence operations*, Biosystems **144**, 2016: 18-26. https://doi.org/10.1016/j.biosystems.2016.03.011

[28] WANG L.Y., SONG H.J., LIU P., *A novel hybrid color image encryption algorithm using two complex chaotic systems*, Optics and Lasers in Engineering **77**, 2016: 118-125. https://doi.org/10.1016/j.optlaseng.2015.07.015

[29] REHMAN A.U., LIAO X.F., ASHRAF R., ULLAH S., WANG H.W., *A color image encryption technique using exclusive-OR with DNA complementary rules based on chaos theory and SHA-2*, Optik **159**, 2018: 348-367. https://doi.org/10.1016/j.ijleo.2018.01.064

[30] SURYANTO Y., SURYADI, RAMLI K., *A new image encryption using color scrambling based on chaotic permutation multiple circular shrinking and expanding*, Multimedia Tools and Applications **76**(15), 2017: 16831-16854. https://doi.org/10.1007/s11042-016-3954-5

Received February 4, 2023
in revised form March 15, 2024