Optica Applicata, Vol. LI, No. 3, 2021
DOI: 10.37190/oa210304

Color image encryption scheme based on quaternion discrete multi-fractional random transform and compressive sensing

Huo-Sheng YE, Jing-Yi DAI, Shun-Xi WEN, Li-Hua GONG, Wen-Quan ZHANG*

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

*Corresponding author: ndzwq@163.com

A color image compression-encryption algorithm by combining quaternion discrete multi-fractional random transform with compressive sensing is investigated, in which the chaos-based fractional orders greatly improve key sensitivity. The original color image is compressed and encrypted with the assistance of compressive sensing, in which the partial Hadamard matrix adopted as a measurement matrix is constructed by iterating Chebyshev map instead of utilizing the entire Guassian matrix as a key. The sparse images are divided into 12 sub-images and then represented as three quaternion signals, which are modulated by the quaternion discrete multi-fractional random transform. The image blocking and the quaternion representation make the proposed cryptosystem avoid additional data extension existing in many transform-based methods. To further improve the level of security, the plaintext-related key streams generated by the 2D logistic-sine-coupling map are adopted to diffuse and confuse the intermediate results simultaneously. Consequently, the final ciphertext image is attained. Simulation results reveal that the proposed cryptosystem is feasible with high security and has strong robustness against various attacks.

Keywords: color image encryption, quaternion discrete multi-fractional random transform, compressive sensing, confusion-diffusion strategy.

1. Introduction

Modern information technologies bring convenience to people, but also result in many information security issues. Encryption is an effective and classic strategy to address these problems. However, the conventional textual encryption methods are not directly suitable for images. To avoid the risk of image information leakage, many image encryption strategies have been designed based on chaotic system [1–3], cellular automata [4], fractional Fourier transform [5], *etc*. These encryption algorithms share a common purpose to transform a vivid image into a noise-like ciphertext image.

In practical applications, color images are more commonly adopted than gray images. Under such circumstance, color image encryption algorithms have been extensively stud-

ied. KANG *et al*. designed a color image encryption system with spatiotemporal chaotic system and deoxyribonucleic acid (DNA) operations [6]. CHAI *et al*. raised a color image cryptosystem with a dynamic DNA strategy [7]. KANG *et al*. defined a reality-preserving multiple parameter discrete fractional angular transform and encrypted three color components in the spatial and transform domains, respectively [8]. However, these color image encryption schemes deal with three color channels separately and the inherent correlations among three color channels were not well considered. To address this problem, quaternion, an extension of complex numbers to four dimensions, can be utilized to represent three color channels as a whole. Consequently, many transforms for real and complex signals have been expanded to quaternion signals [9–11]. WANG *et al*. proposed a color image encryption by combining discrete quaternion Fourier transform with double random phase encoding (DRPE) [9]. Motivated by this, CHEN expanded the conventional multiple-parameter fractional Fourier transform into quaternion domain and dwell on a new color encryption algorithm [10]. Nevertheless, these quaternion transform-based methods yield additional complex values, which are inconvenient for information storage and transmission.

Compressive sensing (CS), as a novel signal sampling-reconstruction technology, is considered to be able to compress and encrypt a signal simultaneously [12–16]. To facilitate the transmission of the keys, ZHOU *et al*. generated a measurement matrix in CS with the key-controlled chaotic map [12]. Subsequently, they combined a nonlinear transform called fractional Mellin transform with CS to compress and encrypt plaintext image [13]. A novel visually meaningful color image encryption based on 2D CS and multi-embedding technology was investigated, where the compressed images were firstly permuted and diffused in both bit-level and pixel-level and the intermediate results were embedded into a carrier image [14]. CHEN *et al*. put forward an asymmetric color cryptosystem based on CS and equal modulus decomposition to counteract the powerful chosen-plaintext attack [15].

Based on the above discussion, a CS-based color image compression-encryption algorithm is designed on the basis of the proposed QDMFRNT and a mechanism for updating keys. The three color components are compressed and encrypted simultaneously by CS. Then these sparse signals are divided and reorganized as three quaternion signals, which are modulated by the proposed QDMFRNT, respectively. Lastly the intermediate results are diffused and confused simultaneously with the update-keys-controlled chaotic sequences.

The rest of this paper is organized as follows. In Section 2, the quaternion discrete multi-fractional random transform is defined. In Section 3, the proposed CS-based color image encryption algorithm is described in detail. The simulation results and performance analyses are shown in Section 4. The conclusion is given in the last Section.

2. Quaternion discrete multi-fractional random transform

For a 1D quaternion signal $\mathbf{x}_q = \mathbf{x}_r + \mathbf{x}_i\mathbf{i} + \mathbf{x}_j\mathbf{j} + \mathbf{x}_k\mathbf{k}$ of size $N \times 1$, its left-side 1D quaternion discrete fractional random transform (QDFRNT) is defined as [11]

$$\mathbf{F}_{\mathrm{q}}^{\alpha} = \mathbf{R}^{\alpha,\mu}\mathbf{x}_{\mathrm{q}} \tag{1}$$

where the kernel transform matrix $\mathbf{R}^{\alpha,\mu}$ is

$$\mathbf{R}^{\alpha,\mu} = \mathbf{V}\mathbf{D}^{\alpha,\mu}\mathbf{V}^{\mathrm{T}} \tag{2}$$

α in QDFRNT is replaced by the order vector $\overline{\boldsymbol{\alpha}} = (\alpha_1, \alpha_2, ..., \alpha_{N-1})$ produced by the 1D logistic map, which extends the QDFRNT to the QDMFRNT. Chaos-based fractional orders make the proposed cryptosystem more sensitive to the key α_1 and enlarge the key space further. The logistic map is defined as

$$\alpha_{i+1} = x_0\alpha_i(1-\alpha_i) \tag{3}$$

where x_0 is the control parameter and the system in Eq. (3) has a chaotic performance if $x_0 \in (3.57, 4]$.

The difference between the QDFRNT and the proposed QDMFRNT is the diagonal matrix $\mathbf{D}^{\bar{\alpha},\mu}$,

$$\mathbf{D}^{\bar{\alpha},\mu} = \mathrm{diag}\left\{1, \exp\left(-\frac{2\pi\mu\alpha_1}{T}\right), \exp\left(-\frac{4\pi\mu\alpha_2}{T}\right), ..., \exp\left[-\frac{2\pi\mu(N-1)\alpha_{N-1}}{T}\right]\right\} \tag{4}$$

where $\boldsymbol{\mu} = a\mathbf{i} + b\mathbf{j} + c\mathbf{k}$ and $|\boldsymbol{\mu}| = 1$. The expansion of the 2D QDMFRNT is straightforward as two 1D QDMFRNTs in the x-axis and the y-axis, respectively. The 2D QDMFRNT and its inverse version (IQDMFRNT) are defined respectively as

$$\aleph_{\mathrm{q}} = \mathbf{R}^{\bar{\alpha},\mu}\mathbf{y}_{\mathrm{q}}(\mathbf{R}^{\bar{\alpha},\mu})^{\mathrm{T}} \tag{5}$$

$$\mathbf{y}_{\mathrm{q}} = \mathbf{R}^{-\bar{\alpha},\mu}\aleph_{\mathrm{q}}(\mathbf{R}^{-\bar{\alpha},\mu})^{\mathrm{T}} \tag{6}$$

where $\mathbf{y}_{\mathrm{q}} = \mathbf{y}_{\mathrm{r}} + \mathbf{y}_{\mathrm{i}}\mathbf{i} + \mathbf{y}_{\mathrm{j}}\mathbf{j} + \mathbf{y}_{\mathrm{k}}\mathbf{k}$ is a 2D quaternion signal.

3. Color image compression-encryption algorithm

3.1. Key streams generation process

To guarantee the security of the proposed image encryption algorithm, a new method is designed to update the initial values $S_1(1)$, $S_2(1)$ and control parameter σ of 2D logistic-sine-coupling map (LSCM). The 2D LSCM is defined as [17]

$$\begin{cases} S_1(i+1) = \sin\left\{\pi\left[4\sigma S_{1i}\left(1-S_1(i)\right) + (1-\sigma)\sin\left(\pi S_2(i)\right)\right]\right\} \\ S_2(i+1) = \sin\left\{\pi\left[4\sigma S_2(i)\left(1-S_2(i)\right) + (1-\sigma)\sin\left(\pi S_1(i+1)\right)\right]\right\} \end{cases} \tag{7}$$

where σ ($\sigma \in [0, 1]$) is the control parameter. Thereafter, with the updated keys, pseudo -random numbers are obtained. The details are as follows.

Step 1. The sum of all pixel values of a color plaintext image is calculated and expressed as SU. In what follows, adopting the secret keys $S_1(1)$, $S_2(1)$, σ and SU as the input of hash function SHA-512, a 512-bit hash value H can be obtained. One can randomly select nine binary sequences (b_1, ..., b_9) with length 8 from 512-bit hash value H. Then each sequence is converted into an integer I_i by

$$I_i = \text{bin2dec}(b_i), \quad i = 1, ..., 9 \tag{8}$$

where function bin2dec(·) converts an 8-bit binary sequence into a decimal integer.

Step 2. The initial keys of 2D LSCM are updated as

$$S_1'(1) = S_1(1) + \frac{1}{2^{14}}\left[\text{mod}(I_1 + I_2, 256) \oplus I_3\right] \tag{9}$$

$$S_2'(1) = S_2(1) + \frac{1}{2^{14}}\left[\text{mod}(I_4 + I_5, 256) \oplus I_6\right] \tag{10}$$

$$\sigma' = \sigma + \frac{1}{2^{14}}\left[\text{mod}(I_7 + I_8, 256) \oplus I_9\right] \tag{11}$$

where $\oplus$ denotes bitwise OR operation.

Step 3. With the updated keys $S_1'(1)$, $S_2'(1)$, σ', the LSCM is iterated $N_0 + 3MN$ ($N_0 \in [1000, 2000]$) times. The former N_0 numbers are discarded and then two chaotic sequences S_1 and S_2 of length $3MN$ are obtained. Thereafter, the sequences S_1 and S_2 are further processed by

$$\mathbf{S}_i = \text{reshape}(\text{round}(S_i \times 10^{14}), M, 3N), \quad i = 1, 2 \tag{12}$$

$$\begin{cases} L(1: M) = S_2(1: M) \\ W(1: 3N) = S_2(3N(M-1): \text{end}) \end{cases} \tag{13}$$

To update the keys, the hash values are randomly chosen, which allows the proposed algorithm to generate different updated keys each time when the color plaintext image and original keys are the same.

3.2. Image encryption process

The encryption process of the proposed color image encryption scheme is shown in Fig. 1. The details of the encryption process are described as follows.

Step 1. Color image compression-encryption with compressive sensing.

1) Three components of color image P of size $N \times N \times 3$, namely, R, G, B, are sparsely represented in DWT domain with orthonormal basis φ: $\chi_i = \varphi^{\mathrm{T}} P_i \varphi$ (i = R, G, B).

2) The Chebyshev map, *i.e.*, $x_{n+1} = \cos(a \times \text{acos} x_n)$, is iterated MN times with the initial keys x_1 and $a = 4$ to obtain the pseudo-random sequence A. The last M ($M < N$)

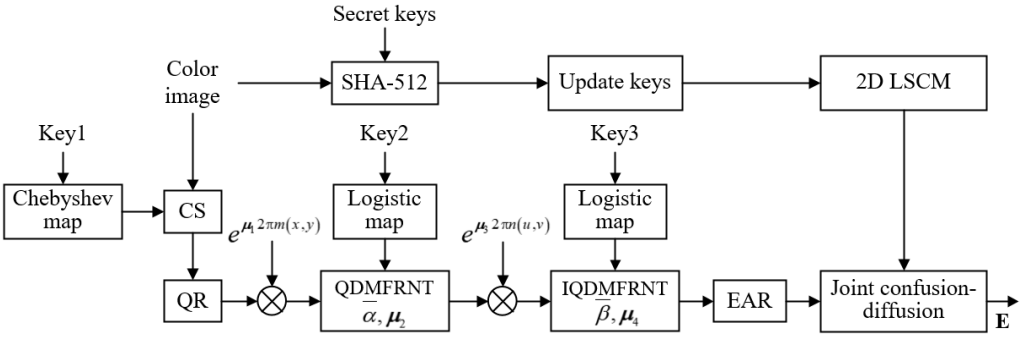


Fig. 1. Color image encryption algorithm.

elements are reserved and sorted. One can obtain the index sequence l from the obtained sequence and its sorted one, where the values of l represent the positions of the corresponding values in its sorted sequence.

3) The partial Hadamard matrix $\mathbf{\Phi}$ of size $M \times N$, as the measurement matrix of CS, is established by selecting the row vector of the Hadamard matrix,

$$\mathbf{\Phi} = \left[Z_{l_1}(:), Z_{l_2}(:), ..., Z_{l_M}(:) \right] \tag{14}$$

where $Z_{l_i}(:)$ denotes the l_i-th row vector of the Hadamard matrix Z. Since the Hadamard matrix is an orthogonal matrix, the partial Hadamard matrix obtained after taking M rows from it still has strong non-correlation and partial orthogonality, which makes a better reconstruction effect to a certain extent.

4) The sparse signal χ_i is measured with the partial Hadamard matrix $\mathbf{\Phi}$, *i.e.*, $f_i = \mathbf{\Phi}\chi_i\mathbf{\Phi}^{\mathrm{T}}$ (i = R, G, B).

Step 2. Image blocking and quaternion representation (QR). To avoid the additional complex matrix, the three compressed components of color image are blocked into 12 sub-images. Consequently, these sub-images are represented as three quaternion signals, *i.e.*,

$$f_{Q_i}(x, y) = f_{i_1}(x, y) + f_{i_2}(x, y)\mathbf{i} + f_{i_3}(x, y)\mathbf{j} + f_{i_4}(x, y)\mathbf{k} \qquad (i = \mathrm{R, G, B}) \tag{15}$$

where f_{i_1}, f_{i_2}, f_{i_3} and f_{i_4} are the sub-images divided from the compressed component f_i.

Step 3. DRPE operation based on the proposed QDMFRNT.

$$h_{Q_i}(x, y) = \mathrm{IQDMFRNT}_{\overline{\beta}, \mu_4}\left\{ \mathrm{QDMFRNT}_{\overline{\alpha}, \mu_2}\left[f_{Q_i}(x, y) e^{\mu_1 2\pi m(x, y)} \right] e^{-\mu_3 2\pi n(u, v)} \right\} \tag{16}$$

where i = R, G, B.

Step 4. Extraction and reorganization (EAR) operations. The real part and the three imaginary parts of each quaternion signal $h_{Q_i}(x, y)$ (i = R, G, B) are extracted and reorganized into a new matrix $\mathbf{E}_1$ of size $M \times 3N$.

T a b l e 1. Algorithm 1: Joint confusion and diffusion strategy.

Input: The reorganized matrix $\mathbf{E}_1$; chaotic matrices $\mathbf{S}_1$ and $\mathbf{S}_2$.

$E_2 = \text{floor}[255 \times (E_1 - \min(E_1))/(\max(E_1) - \min(E_1))$
for $i = 1{:}M$
  for $j = 1{:}3N$
    $E_3(i, j) = \text{bitxor}\{\text{bitxor}[E_2(d_1(i), d_2(j)), S_1(i, j)], S_2(i, j)\}$
  end
end
$E = \text{reshape}(E_3, M, N, 3)$

Step 5. Joint confusion and diffusion strategy. With the sorting-based method described in Step 1 of Section 3.2, one can obtain two address sequences $d_1(m)$ and $d_2(n)$ from $L(m)$ and $W(n)$, respectively. The details of the confusion and the diffusion operations are listed in Table 1, in which the intermediate result is confused and diffused simultaneously with the plaintext-related key-streams. Consequently, the final ciphertext image **E** is attained.

Since the proposed scheme is a symmetric cryptosystem, the recipient who knows the whole correct keys can retrieve the decryption image with and inverse encryption process. Firstly, with the correct key-streams, the inverse diffusion and the confusion operations are applied to the ciphertext image. The intermediate result is divided into 12 sub-images and then represented into three quaternion signals. Then, the decoding of the QDMFRNT with the DRPE is performed to obtain quaternion signals. With signal separation and reorganization, three reconstructed color components are obtained and the plaintext image can be decrypted via the smooth l^0 norm algorithm [18] and the inverse DWT.

4. Simulation results and performance analyses

4.1. Encryption and decryption results

To demonstrate the feasibility of the designed cryptosystem, simulations are carried out with MATLAB 2016(a) platform. The original color images *Peppers*, *San Diego*, *Lena* and *Couple* of different sizes shown in Figs. 2**a1**–2**a4** are selected as the test images. The initial secret keys adopted in these simulations are arbitrarily chosen as: $S_1(1) = 0.6553$, $S_2(1) = 0.4944$, $\sigma = 0.5697$, $x_0 = 3.98$, $x_1 = 0.123$, $\alpha_1 = 0.6$ and $\beta_1 = 0.4$. Other parameters are given as: $\boldsymbol{\mu}_1 = (\mathbf{i} + \mathbf{j} + \mathbf{k})/\sqrt{3}$, $\boldsymbol{\mu}_2 = \mathbf{i}$, $\boldsymbol{\mu}_3 = \mathbf{j}$ and $\boldsymbol{\mu}_4 = \mathbf{k}$, respectively. Figures 2**b1**–2**b4** are encryption images while Figs. 2**c1**–2**c4** are corresponding decryption images. Table 2 shows the decryption results under different sizes of original images. For the original color image of size $8 \times 8 \times 3$, it is sparse and then measured with a partial Hadamard matrix to obtain intermediate encryption result of size $6 \times 6 \times 3$. Each color component is divided into four sub-images and represented as a quaternion signal. Consequently, three quaternion signals are modulated by the QDMFRNT and

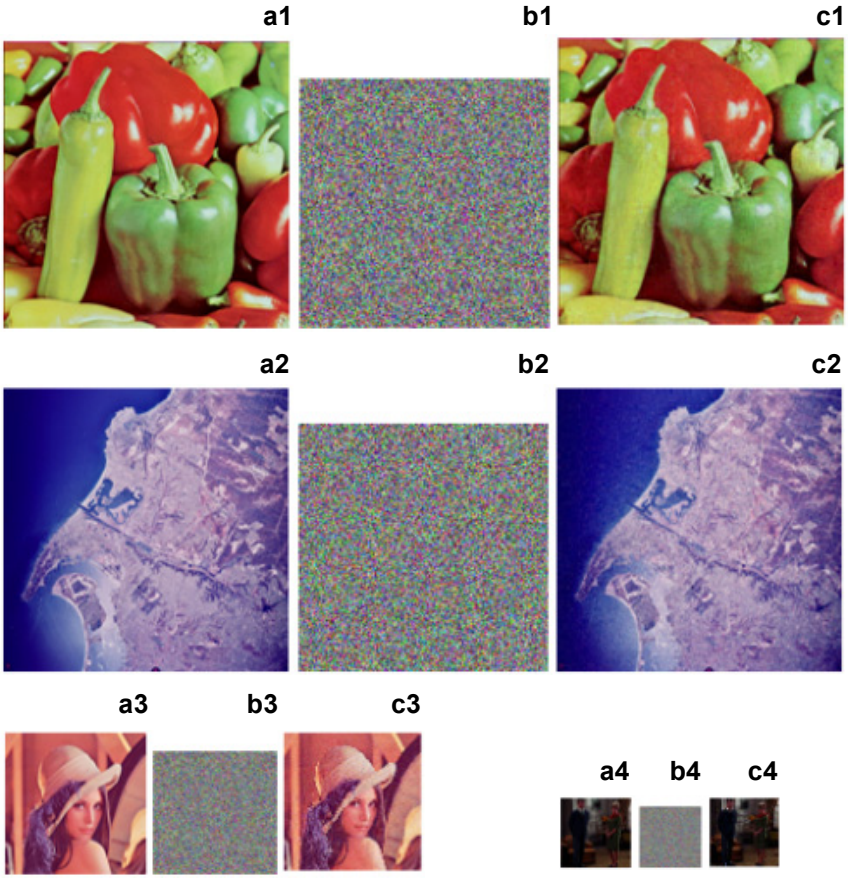
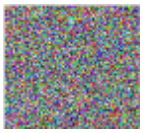


Fig. 2. Simulation results: (**a1**–**a4**) *Peppers* of size 256 × 256, *San Diego* of size 256 × 256, *Lena* of size 128 × 128, *Couple* of size 64 × 64, respectively. (**b1**–**b4**) corresponding encryption images with 75.56% compression ratio. (**c1**–**c4**) corresponding decryption images.

T a b l e 2. Simulation results for different sizes of original image.

Original size	Compression ratio	Encryption image	Decryption image	PSNR [dB]
256 × 256 × 3	75.56%			33.3790
64 × 64 × 3	75.56%			24.9560
8 × 8 × 3	56.25%			27.9941

then simultaneous confusion and diffusion strategy is performed to obtain the final ciphertext image. Simulation results show that the encryption images are noise-like while the corresponding decryption images are visible. It indicates that the designed color image compression-encryption algorithm is feasible with satisfactory encryption and decryption performance.

4.2. Comparison with existing works

In the proposed color cryptosystem, three color components are performed by combining the high-dimensional properties of quaternion with image blocking operation. Accordingly, compared with some similar color image encryption schemes in [5, 9, 10], the proposed algorithm cannot yield additional complex matrix. Data storage comparison results collected in Table 3 indicate that the total amount of ciphertext data and the consumption of keys are smaller in our proposed algorithm. Therefore, the proposed color image encryption algorithm is more applicable.

T a b l e 3. Data storage comparison results.

Algorithm	Original image	Ciphertext image	Private keys
Ref. [5]	$256 \times 256 \times 3$	$256 \times 256 \times 3$	$256 \times 256 \times 3$
Ref. [9]		$256 \times 256 \times 3 + 256 \times 256$	Transform parameters; initial keys
Ref. [10]		$256 \times 256 \times 3 + 256 \times 256$	Transform parameters; initial keys
Our scheme		$224 \times 224 \times 3$	$S_1(1)$, $S_2(2)$, σ, x_1, α_1, β_1

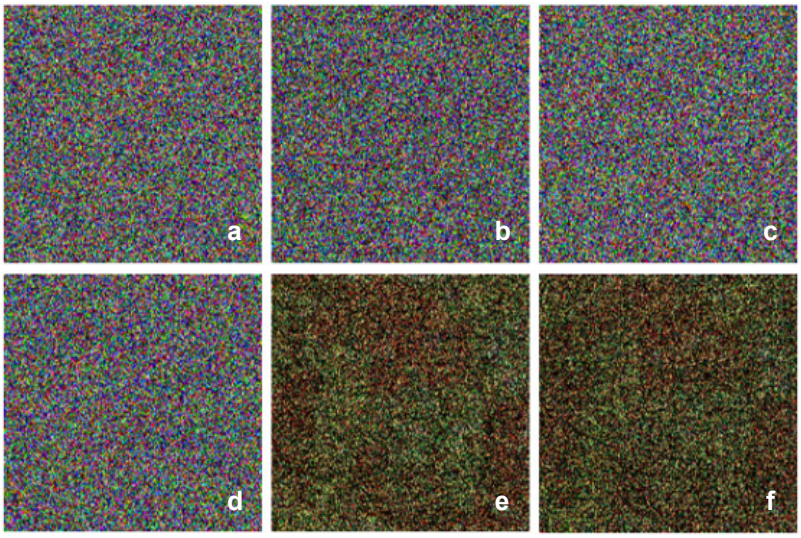


Fig. 3. Decryption image *Peppers* with modified key: (**a**) $S_1(1) + 10^{-16}$, (**b**) $S_2(1) + 10^{-16}$, (**c**) $\sigma + 10^{-16}$, (**d**) $x_1 + 10^{-16}$, (**e**) $\alpha_1 + 10^{-16}$, and (**f**) $\beta_1 + 10^{-16}$.

4.3. Key sensitivity analysis

Figures 3**a**–3**f** show the decryption images *Peppers* under the condition that only one secret key is modified with a tiny change while other keys are correct. It can be observed that the decryption images are unrecognizable and an unauthorized user cannot obtain any useful information unless she knows all correct keys. The average mean square error (MSE) curves with different initial fractional orders α_1 and β_1 are exhibited in Figs. 4**a** and 4**b**. Especially, compared with the typical algorithms based on fractional random transform [19, 20], the sensitivity to the fractional keys is enhanced by three decimal levels at least, since the fractional orders of the proposed QDMFRNT are generated with the chaotic system. Therefore, the proposed color image compression-encryption algorithm is very sensitive to the keys.

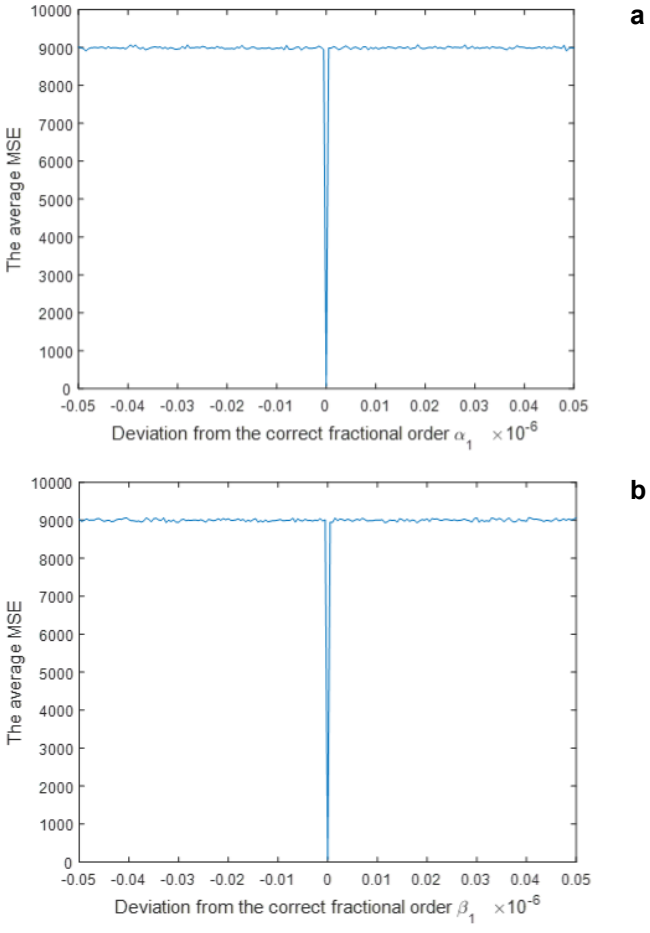


Fig. 4. Average MSE *versus* disturbance of initial fractional order: (**a**) α_1, and (**b**) β_1.

4.4. Key space analysis

To resist the brute-force attack, the key space of a secure cryptosystem is considered to be at least 2^{100}. In our algorithm, the precision of $S_1(1)$, $S_2(1)$, σ or x_1 is about 10^{-16}. The key space of fractional order α_1 or β_1 is around 10^6. Thus, the total key space is 2^{259} at least, which indicates that the proposed color image encryption algorithm possesses enough key space to withstand the brute-force attack.

4.5. Histogram analysis

Figure 5**a** shows the histograms of three components of color plaintext image *Peppers*. The histograms of the corresponding encryption image encrypted with the proposed algorithm are shown in Fig. 5**b**. Apparently, the histograms of the RGB components of plaintext image are significantly different, while the histograms of ciphertext images

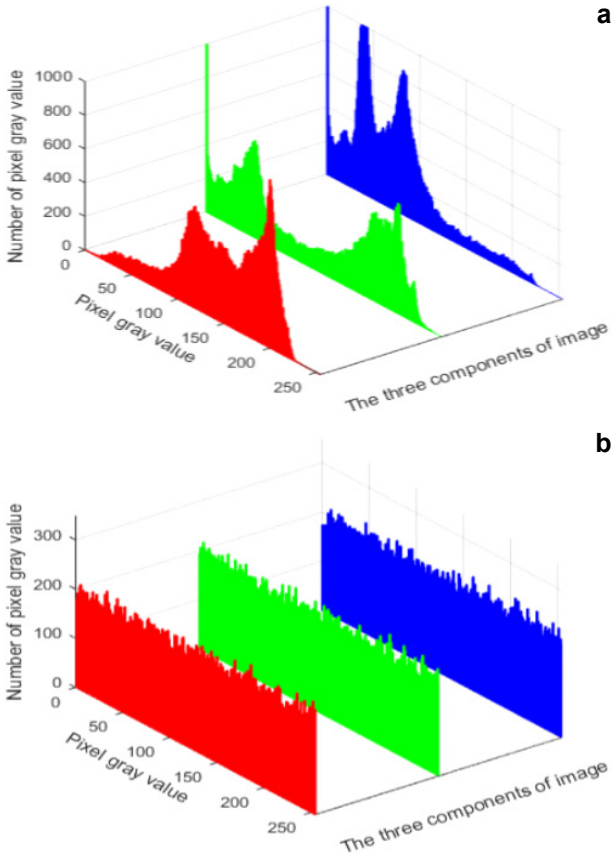


Fig. 5. Histogram: (**a**) R, G, B components of original image *Peppers*, (**b**) R, G, B components of encryption *Peppers*.

are flat enough. Therefore, the proposed color image compression-encryption algorithm can effectively withstand the histogram analysis attack.

4.6. Correlation analysis

The correlation coefficient between adjacent pixels is

$$C = \frac{\sum_{j=1}^{N}(m_j - \overline{m})(n_j - \overline{n})}{\sqrt{\sum_{j=1}^{N}(m_j - \overline{m})^2 \sum_{j=1}^{N}(n_j - \overline{n})^2}} \tag{17}$$

where

$$\overline{m} = \frac{1}{N}\sum_{j=1}^{N} m_j$$

$$\overline{n} = \frac{1}{N}\sum_{j=1}^{N} n_j$$

12 000 adjacent pixel pairs of the original color images *Peppers* and *San Diego* are selected randomly in horizontal, vertical and diagonal directions, respectively. Table 4 lists the correlation coefficients of these adjacent pixel pairs. The correlation coefficients in original color image are near 1, while those in encryption images are close

T a b l e 4. Correlation coefficients of adjacent pixels.

Algorithm	Image		Horizontal direction	Vertical direction	Diagonal direction
	Peppers	R	0.9503	0.9379	0.9030
		G	0.9641	0.9488	0.9220
		B	0.9380	0.9219	0.8932
	San Diego	R	0.8955	0.9057	0.8869
		G	0.8992	0.8978	0.8795
		B	0.8821	0.8772	0.8491
Proposed algorithm	Encryption *Peppers*	R	–0.0007	0.0115	0.0060
		G	–0.0123	–0.0053	–0.0079
		B	–0.0148	–0.0152	0.0066
	Encryption *San Diego*	R	0.0058	–0.0191	0.0132
		G	–0.0011	0.0012	0.0006
		B	0.0172	–0.0230	0.0118
Ref. [13]	Encryption *Peppers*	R	0.0526	0.0729	0.0871
		G	0.0537	0.0649	0.0736
		B	0.0648	0.0599	0.8113

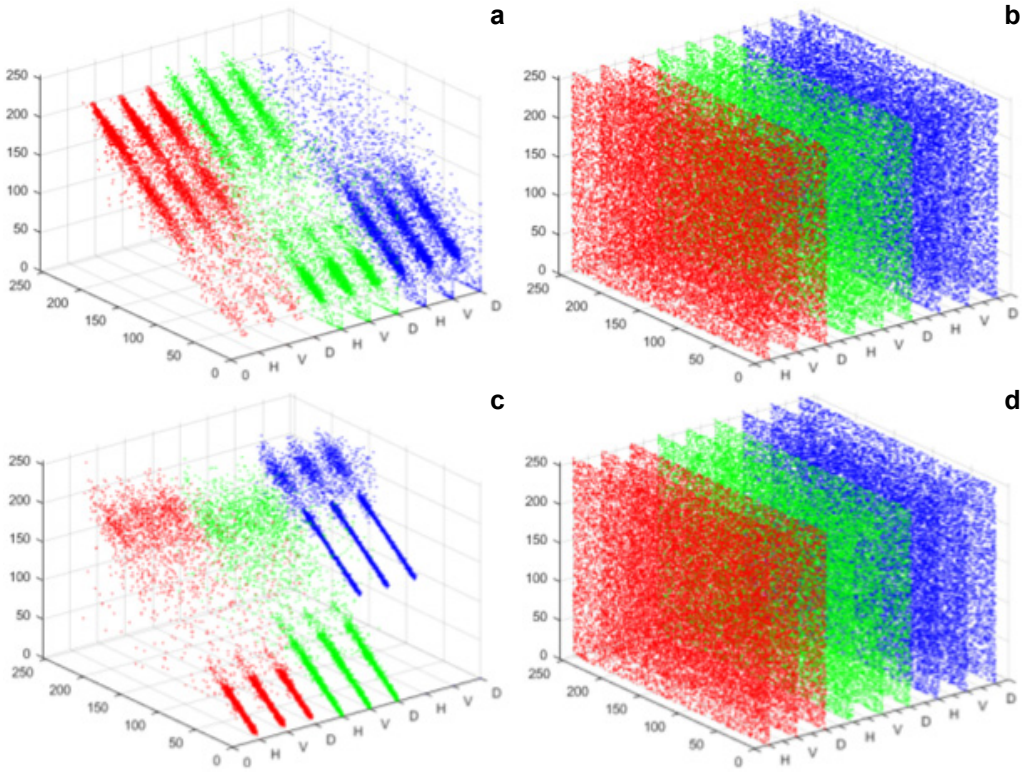


Fig. 6. Correlation distributions of adjacent pixels in the horizontal, vertical, diagonal directions: R, G, B components of *Peppers* (**a**), R, G, B components of encryption *Peppers* (**b**), R, G, B components of *San Diego* (**c**), and R, G, B components of encryption *San Diego* (**d**).

to 0. Figures 6**a** and 6**c** depict the correlation distributions between the adjacent pixels of *Peppers* and *San Diego*. Figures 6**b** and 6**d** are the correlation distributions of the corresponding encryption images, respectively. It is shown that the correlations in original images are similar to linear distribution while the correlations in encryption images are destroyed efficiently with the proposed algorithm. Therefore, the proposed color image compression and encryption algorithm is immune to the statistical analysis attack.

4.7. Robustness against noise attack and occlusion attack

The ciphertext image is easily corrupted by various types of noises during transmission. Figure 7 shows the decryption results after adding Gaussian noise and Salt-and-Pepper noise to the ciphertext image. In addition, the PSNR values of decryption images under different noise parameters are shown in Fig. 8. As the simulation results show, the quality of the retrieved images is still in acceptable range with the increase of noise intensity. Therefore, the proposed algorithm has strong robustness against noise attack. To eval-

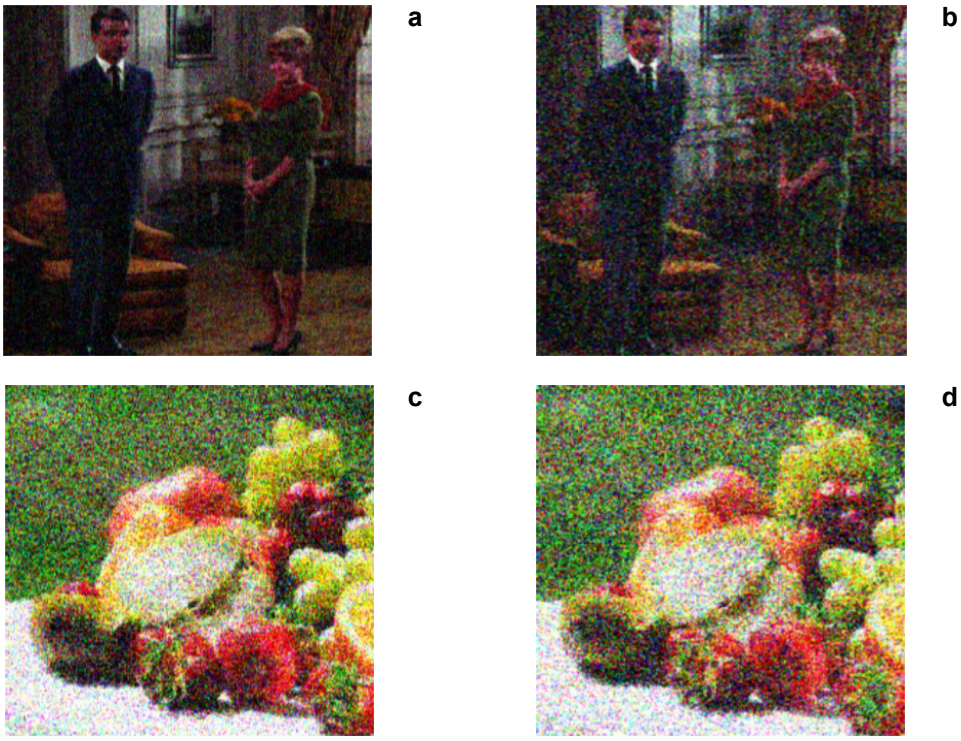


Fig. 7. Decryption results with different noise attacks: decryption *Couple* with Gaussian noise with intensity (**a**) $k = 5$, and (**b**) $k = 10$; decryption *Fruits* with Salt-and-Pepper noise with the density of noise distribution (**c**) 5, and (**d**) 10.

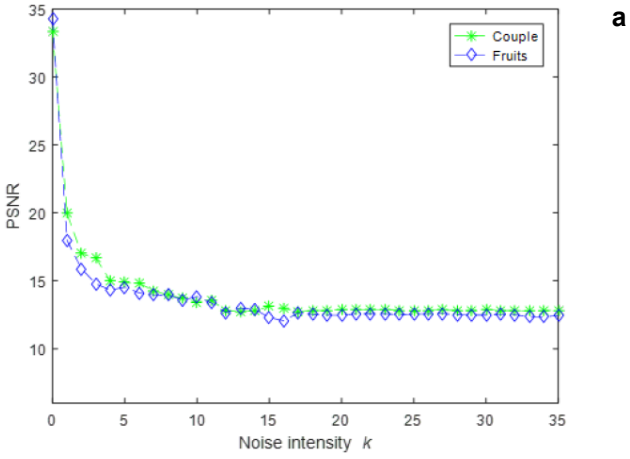


Fig. 8. Average PSNR values *versus* noise parameter (**a**) Gaussian noise, and (**b**) Salt-and-Pepper noise.

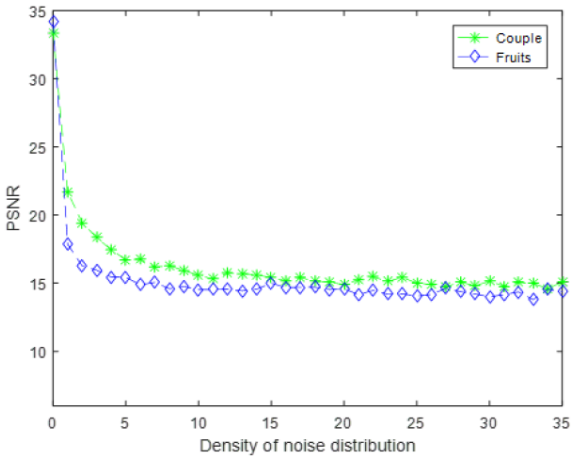


Fig. 8. Continued.

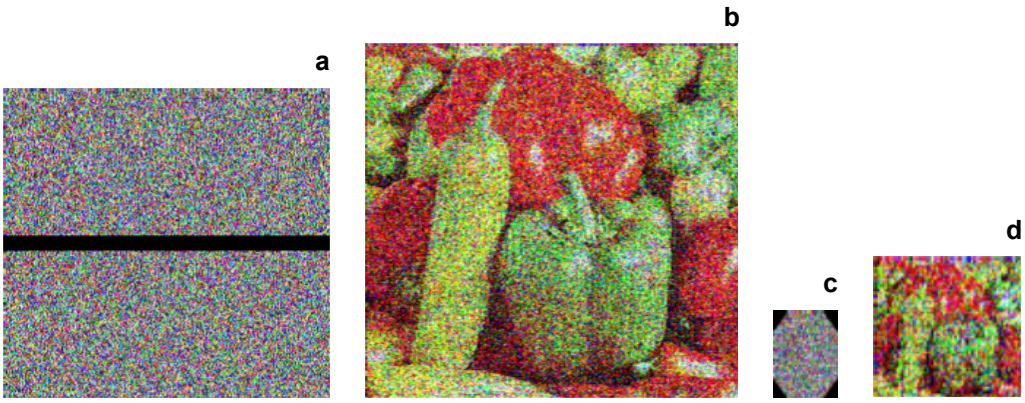


Fig. 9. Results of occlusion attack: encryption images with (**a**) 5%, and (**c**) 10% data loss, and (**b**, **d**) corresponding decryption images.

uate the robustness of the presented cryptosystem against the occlusion attack, the encryption images of size 256 × 256 and 64 × 64 are cropped with 5% and 10%, respectively, and the corresponding decryption results are shown in Fig. 9. The reconstructed images show acceptable decryption effect. In conclusion, the proposed color image algorithm could withstand the occlusion attack to a certain degree.

5. Conclusion

A secure CS-based color image encryption algorithm by combining quaternion discrete multi-fractional random transform with the hash function SHA-512 is proposed. The input of SHA-512 is set to associate with the color plaintext image and the secret keys. The initial keys and the parameter of 2D LSCM are updated via randomly selected hash

values, which allows the proposed algorithm to generate different updated keys each time when the color plaintext image and the original keys are same. The quaternion discrete random transform is extended to the quaternion discrete multi-fractional random transform, which not only increases the key space, but also significantly improves the sensitivity of the fractional key. Experiment results verify that the designed color image encryption algorithm possesses high security and strong robustness against the statistical analyses attack, noise attack and occlusion attack.

Acknowledgment – This work is supported by the National Natural Science Foundation of China (Grant Nos. 61866024 and 61861029), and the Cultivation Plan of Applied Research of Jiangxi Province (Grant No. 20181BBE58022).

References

[1] Linqing Huang, Shuting Cai, Xiaoming Xiong, Minging Xiao, *On symmetric color image encryption system with permutation-diffusion simultaneous operation*, Optics and Lasers in Engineering **115**, 2019, pp. 7–20, DOI: 10.1016/j.optlaseng.2018.11.015.

[2] Parvaz R., Zarebnia M., *A combination chaotic system and application in color image encryption*, Optics and Laser Technology **101**, 2018, pp. 30–41, DOI: 10.1016/j.optlastec.2017.10.024.

[3] Xiangjun Wu, Kunshu Wang, Xingyuan Wang, Haibin Kan, Kurths J., *Color image DNA encryption using NCA map-based CML and one-time keys*, Signal Processing **148**, 2018, pp. 272–287, DOI: 10.1016/j.sigpro.2018.02.028.

[4] Niyat A.Y., Moattar M.H., Torshiz M.N., *Color image encryption based on hybrid hyper-chaotic system and cellular automata*, Optics and Lasers in Engineering **90**, 2017, pp. 225–237, DOI: 10.1016/j.optlaseng.2016.10.019.

[5] Hang Chen, Zhengjun Liu, Li Zhu, Tanougast C., Blondel W., *Asymmetric color cryptosystem using chaotic Ushiki map and equal modulus decomposition in fractional Fourier transform domains*, Optics and Lasers in Engineering **112**, 2019, pp. 7–15, DOI: 10.1016/j.optlaseng.2018.08.020.

[6] Xuejing Kang, Zihui Guo, *A new color image encryption scheme based on DNA encoding and spatiotemporal chaotic system*, Signal Processing: Image Communication **80**, 2020, article 115670, DOI: 10.1016/j.image.2019.115670.

[7] Xiuli Chai, Xianglong Fu, Zhihua Gan, Yang Lu, Yiran Chen, *A color image cryptosystem based on dynamic DNA encryption and chaos*, Signal Processing **155**, 2019, pp. 44–62, DOI: 10.1016/j.sigpro.2018.09.029.

[8] Xuejing Kang, Anlong Ming, Ran Tao, *Reality-preserving multiple parameter discrete fractional angular transform and its application to color image encryption*, IEEE Transactions on Circuits and Systems for Video Technology **29**(6), 2019, pp. 1595–1607, DOI: 10.1109/TCSVT.2018.2851983.

[9] Xiaolei Wang, Hongchen Zhai, Zhilei Li, Qi Ge, *Double random-phase encryption based on discrete quaternion Fourier-transforms*, Optik **122**(20), 2011, pp. 1856–1859, DOI: 10.1016/j.ijleo.2010.11.016.

[10] Beijing Chen, Ming Yu, Yuhang Tian, Leida Li, Dingcheng Wang, Xingming Sun, *Multiple-parameter fractional quaternion Fourier transform and its application in colour image encryption*, IET Image Processing **12**(12), 2018, pp. 2238–2249, DOI: 10.1049/iet-ipr.2018.5440.

[11] Beijing Chen, Chunfei Zhou, Byeungwoo Jeon, Yuhui Zheng, Jinwei Wang, *Quaternion discrete fractional random transform for color image adaptive watermarking*, Multimedia Tools and Applications **77**(2), 2018, pp. 20809–20837, DOI: 10.1007/s11042-017-5511-2.

[12] Nanrun Zhou, Aidi Zhang, Fen Zheng, Lihua Gong, *Novel image compression–encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing*, Optics and Laser Technology **62**, 2014, pp. 152–160, DOI: 10.1016/j.optlastec.2014.02.015.

[13] NANRUN ZHOU, HAOLIN LI, DI WANG, SHUMIN PAN, ZHIHONG ZHOU, *Image compression and encryption scheme based on 2D compressive sensing and fractional Mellin transform*, Optics Communications **343**, 2015, pp. 10–21, DOI: 10.1016/j.optcom.2014.12.084.

[14] XIULI CHAI, HAIYANG WU, ZHIHUA GAN, YUSHU ZHANG, YIRAN CHEN, *Hiding cipher-images generated by 2-D compressive sensing with a multi-embedding strategy*, Signal Processing **171**, 2020, article 107525, DOI: 10.1016/j.sigpro.2020.107525.

[15] HANG CHEN, TANOUGAST C., ZHENGJUN LIU, SIELER L., *Asymmetric optical cryptosystem for color image based on equal modulus decomposition in gyrator transform domains*, Optics and Lasers in Engineering **93**, 2017, pp. 1–8, DOI: 10.1016/j.optlaseng.2017.01.005.

[16] HAO JIANG, ZHE NIE, NANRUN ZHOU, WENQUAN ZHANG, *Compressive-sensing-based double-image encryption algorithm combining double random phase encoding with Josephus traversing operation*, Optica Applicata **49**(3), 2019, pp. 445–459, DOI: 10.5277/oa190307.

[17] ZHONGYUN HUA, FAN JIN, BINXUAN XU, HEJIAO HUANG, *2D logistic-sine-coupling map for image encryption*, Signal Processing **149**, 2018, pp. 148–161, DOI: 10.1016/j.sigpro.2018.03.010.

[18] 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, pp. 289–301, DOI: 10.1109/TSP.2008.2007606.

[19] LIHUA GONG, CHENZHI DENG, SHUMIN PAN, NANRUN ZHOU, *Image compression-encryption algorithms by combining hyper-chaotic system with discrete fractional random transform*, Optics and Laser Technology **103**, 2018, pp. 48–58, DOI: 10.1016/j.optlastec.2018.01.007.

[20] ANNABY M.H., RUSHDI M.A., NEHARY E.A., *Color image encryption using random transforms, phase retrieval, chaotic maps, and diffusion*, Optics and Lasers in Engineering **103**, 2018, pp. 9–23, DOI: 10.1016/j.optlaseng.2017.11.005.

Received June 5, 2020
in revised form August 1, 2020