



# Novel encryption for color images using fractional-order hyperchaotic system

Khalid M. Hosny<sup>1</sup> · Sara T. Kamal<sup>2</sup> · Mohamed M. Darwish<sup>2</sup>

Received: 20 July 2020 / Accepted: 15 December 2021 / Published online: 6 January 2022  
© The Author(s), under exclusive licence to Springer-Verlag GmbH Germany, part of Springer Nature 2022

## Abstract

The fractional-order functions show better performance than their corresponding integer-order functions in various image processing applications. In this paper, the authors propose a novel utilization of fractional-order chaotic systems in color image encryption. The 4D hyperchaotic Chen system of fractional-order combined with the Fibonacci Q-matrix. The proposed encryption algorithm consists of three steps: in step#1, the input image decomposed into the primary color channels, R, G, & B. The confusion and diffusion operations are performed for each channel independently. In step#2, the 4D hyperchaotic Chen system of fractional orders generates random numbers to permit pixel positions. In step#3, we split the permitted image into  $2 \times 2$  blocks where the Fibonacci Q-matrix diffused each of them. Experiments performed where the obtained results ensure the efficiency of the proposed encryption algorithm and its ability to resist attacks.

**Keywords** Color image encryption · Fractional-order chaotic system · 4D hyperchaotic Chen system · Fibonacci Q-matrix · Entropy

## 1 Introduction

Users of the Internet and other networks share and transmit millions of color images every day; these images are used in different applications such as telemedicine, distance learning, business, and military. Securing digital images is extremely important to prevent image content loss during transmission and hide image information from attackers.

Different techniques such as watermarking (Hosny et al. 2018; Hosny et al. 2019; Hosny et al. 2021a, b), image steganography (Zhou et al. 2019; Kadhim et al. 2020), and image encryption (Naskar et al. 2020) are frequently used for securing digital images. Image encryption technique is based on two main stages: encryption and decryption. In the encryption stage, the input image is converted into an unreadable image using a secret key. In the decryption stage, the contents are retrieved by using the same key. One main advantage of using encryption over other methods is that

the image is retrieved without losing information. The RGB color space is commonly used in color image encryption algorithms. Each pixel in the color image consists of three values, one in each channel. Most color image encryption algorithms encrypt each channel independently.

Scientists proposed different techniques of color image encryption. These techniques depend on a chaotic system (Wang et al. 2019a, b; Parvaz and Zarebnia 2018; Wang et al. 2019a, b; Xian et al. 2020; Liu et al. 2019a, b), DNA computing (Jithin and Sankar 2020; Nematzadeh et al. 2020), and compressive sensing (Yao et al. 2019). Also, deep learning approaches are applied in image encryption, (Abro et al. 2020; Ali et al. 2020; Chen et al. 2019), to increase the robustness of 2D/3D image encryption. This technique utilizes a fast and effective CNN denoiser based on the principle of deep learning. In Ding et al. (2020), the authors utilize the Cycle-GAN network as the primary learning network to encrypt and decrypt the medical image. Ding et al. (2021) proposed a new deep learning-based stream cipher generator, DeepKeyGen, designed to generate the private key to encrypt medical images.

Generally, color image encryption techniques involved confusion and diffusion of pixels. Confusion is the process of changing pixels' arrangement without changing the pixel value. This step individually does not give satisfactory

✉ Khalid M. Hosny  
k\_hosny@yahoo.com

<sup>1</sup> Information Technology Department, Zagazig University, Zagazig, Egypt

<sup>2</sup> Computer Science Department, Assiut University, Assiut, Egypt

results in encryption. For improved security, the confusion step is usually combined with the diffusion step, in which the values of pixels are changed based on specific mathematical operations.

Chaotic systems are divided into two main classes (low and high dimensions). These systems have many valuable characteristics, such as randomness, ergodicity, complex behavior, and sensitivity to control parameters and their initial conditions. Also, the keyspace generated by most of the chaotic systems is very large. Based on their ability to improve encryption algorithms' efficiency, various chaotic systems are utilized in color image encryption (Li et al. 2018; Li et al. 2019a, b; Yang and Liao 2018).

Pak and Huang (2017) show that low-dimensional (LD) chaotic systems contain a combination of one-dimensional chaotic maps. Teng et al. (2018) converted the color image to one bit-level image by combining the three primary channels, Red, Green, and Blue. Then, the combined image was scrambled using a skew tent map. Irani et al. (2019) designed the chaotic coupled-Sine map. This new map is used for scrambling color images. Despite the simple structure of low-dimensional systems, the keyspace is small, achieving a lower security level. Essaid et al. (2019) proposed a new method for encrypting both color and grey images using a secure variant of Hill cipher and an improved 1D chaotic maps (logistic map, sine map, and Chebyshev map). Wu et al. (2015) presented a color image encryption algorithm by combining DNA sequences with multiple improved 1D chaotic maps. Kamal et al. (2021) proposed a new algorithm for encrypting grey and color medical images. This algorithm is based on image blocks and a chaotic logistic map.

The high-dimension (HD) chaotic systems are characterized by having complex structures and multiple parameters. These properties enable HD systems to overcome the weaknesses of LD systems. Liu et al. (2019a, b) encrypted color images using dynamic DNA and the 4-D memristive hyper-chaos. Zhang and Han (2021) proposed a new color image encryption scheme based on dynamic DNA coding, six-dimensional (6D) hyperchaotic system, and image hashing. Kaur et al. (2020) presented minimax differential evolution-based 7D hyperchaotic map that is used for encrypting color images. Sahari and Boukemara (2018) combined two chaotic maps, piecewise and logistic, to design a 3D chaotic map. This 3D map is used in information security applications. Wu et al. (2016) proposed a new color image encryption method by combining the discrete wavelet transform with a 6D hyperchaotic system. Zhou et al. (2018) proposed quantum-based encryption of color images using quantum cross-exchange with a 5D hyperchaotic system.

The fractional-order polynomials and functions show better performance than the corresponding integer-order

ones in color image analysis Hosny et al. (2020a), pattern recognition Hosny et al. (2020b), Image-based Diagnosis of COVID-19 Abd Elaziz et al. (2020), Plant disease recognition Kaur et al. (2019), and improved recognition of bacterial species Chen et al. (2018). Generally, the chaotic systems of fractional orders are more complex and more accurate than the integer-orders chaotic systems. Accordingly, recent fractional-orders chaotic systems-based image encryption methods were proposed (Yang et al. 2019; Yang et al. 2020a, b; Yang et al. 2020a, b). These encryption algorithms are limited to encrypting gray-scale images.

Color images contain more information than grey images. So, encrypting color images with high efficiency in considerable time is a great challenge. Some recent color image encryption techniques have shortcomings, such as small keyspace; the key does not depend on the original image, making it weak against differential attacks. Other algorithms cannot resist different kinds of attacks. There is not much previous work that used fractional-order chaotic systems in encrypting color images. These shortages motivate the authors to propose a novel utilization of chaotic systems of fractional orders in the encryption of color images. The main contributions of this paper are:

1. A 4D fractional-order hyperchaotic Chen system is applied to generate the secret key used for scrambling the plain image, where the system's initial conditions are based on the plain image.
2. The diffusion step is based on the Fibonacci Q-matrix.
3. Integration between the 4D fractional-order hyperchaotic Chen system and Fibonacci Q-matrix assures a high level of security and can resist different kinds of attacks.

A new three-stage encryption algorithm for color images was proposed. In this algorithm, the 4D hyperchaotic Chen system of fractional orders is combined with the Fibonacci Q-matrix. Step#1: the input image decomposed into the primary color channels, R, G, & B. Step#2: the confusion and diffusion operations are performed independently for each channel, where the 4D hyperchaotic Chen system fractional-orders used to generate random numbers to permit pixel positions. Step#3: the permitted image is divided into small blocks where each of them is diffused by applying the Fibonacci Q-matrix. Various experiments were performed to demonstrate the efficiency and its ability to resist attacks.

The following subsections are: Sect. 2 includes the preliminaries of the 4D hyperchaotic Chen system of fractional-orders and the Fibonacci Q-matrix. The proposed method for color images is described in Sect. 3. The experiments, results, and discussion are presented in Sect. 4. The conclusion is presented in Sect. 5.

## 2 Preliminaries

### 2.1 4D hyperchaotic Chen system of Fractional-order

Li et al. (2005) defined the hyperchaotic Chen system of integer-order, while Hegazi and Matouk (2011) used the principles of fractional calculus to derive the hyperchaotic Chen system of fractional-order.

$$\begin{cases} D^\alpha x = a(y - x) + u \\ D^\alpha y = \gamma x - xz + cy \\ D^\alpha z = y - bz \\ D^\alpha u = yz + du \end{cases} \quad (1)$$

where  $\alpha$  is the fractional-order,  $a, b, c, d, \gamma$  are constants and  $x, y, z, u$  represent the state variable of the system. A chaotic system is hyperchaotic when the number of positive Lyapunov exponents is  $\geq 1$ . For  $a = 35, b = 3, c = 12, d = 0.3, \gamma = 7$ , and  $\alpha = 0.97$ , the system possesses two positive Lyapunov exponents, which means that it is hyperchaotic of fractional-order.

### 2.2 Fibonacci Q-matrix

The Fibonacci sequence is defined by:

$$F_n = F_{n-1} + F_{n-2}, n > 2 \quad (2)$$

where  $F_n$  is Fibonacci number and  $F_1 = F_2 = 1$ . The Fibonacci  $Q$  matrix is a square matrix with size  $2 \times 2$  that is given by:

$$Q = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \quad (3)$$

The  $n$ th power of the  $Q$  matrix is defined by:

$$Q^n = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix} \quad (4)$$

The inverse matrix  $Q^{-n}$  has the following form:

$$Q^{-n} = \begin{bmatrix} F_{n-1} & -F_n \\ -F_n & F_{n+1} \end{bmatrix} \quad (5)$$

All symbols used in this section are defined in Table 1.

## 3 The proposed encryption algorithm

The input color image of size,  $M \times N \times 3$ , decomposed into three channels of the uni-size,  $M \times N$ , and then we encrypt each channel independently. Our encryption algorithm

**Table 1** Symbols descriptions

Symbol	Description
$\alpha$	fractional-order of the system
$a, b, c, d, \gamma$	Constants
$x, y, z, u$	Initial conditions of the system
$F_n$	Fibonacci number
$Q$	Fibonacci matrix

depends on three main steps. First: the fractional-order hyperchaotic sequence is generated. Second: the input color image is scrambled, and then diffusion of scrambled image is performed.

The scrambling and diffusion processes were executed twice to get the encrypted image. Figure 1 shows a visualized flowchart for one round. In this figure, the input color image “Lena” is decomposed into three grey images. Then, the fractional sequences are computed based on these images. After that, each grey image is scrambled by the generated sequence and diffused using the Fibonacci  $Q$  matrix. Finally, the three encrypted images are combined to obtain the encrypted color image. Also, the decryption process is illustrated in this section to retrieve the original image.

Figure 2 shows one round of the decryption process where the encrypted image is converted into three grey images. First, the diffusion steps using the Fibonacci  $Q$  matrix are applied. Then the same sequence ( $S$ ) generated in encryption is used in the scrambling step.

### 3.1 Generating a fractional hyperchaotic sequence

**Step#1:** the initial condition of the Chen hyperchaotic system of fractional-order, as defined in Eq. (1), is image-dependent. The image is converted into vector  $P$ , and then the initial condition is calculated by:

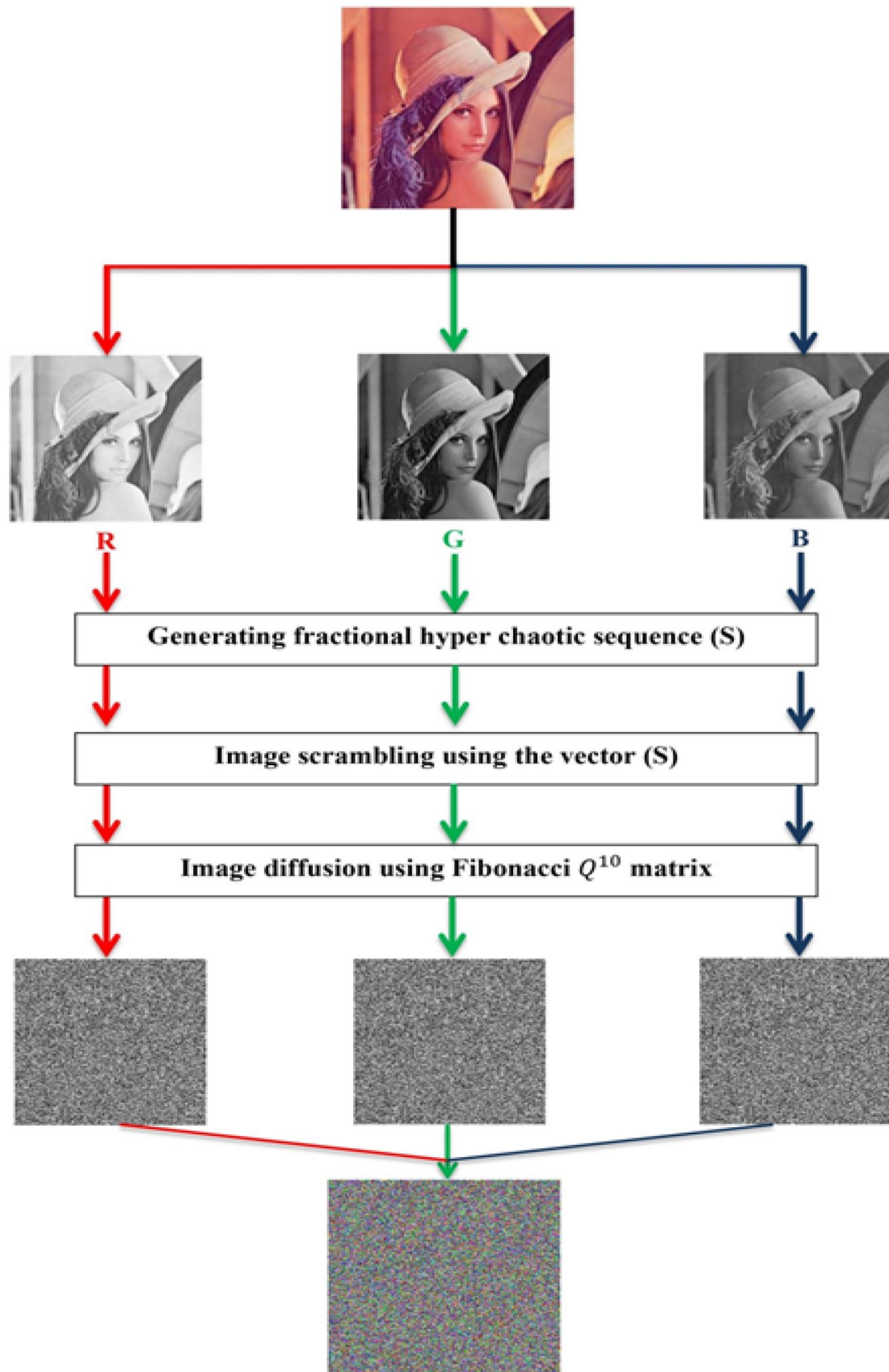
$$x_1 = \frac{\sum_{i=1}^{MN} P(i) + (M \times N)}{2^{23} + (M \times N)} \quad (6)$$

$$x_i = \text{mod}(x_{i-1} \times 10^6, 1) \quad i = 2, 3, 4 \quad (7)$$

where  $x_1, x_2, x_3, x_4$  refer to the initial conditions of the fractional hyperchaotic system,  $MN$  is the length of the image vector  $P$ , and the mod is the modulo operation.

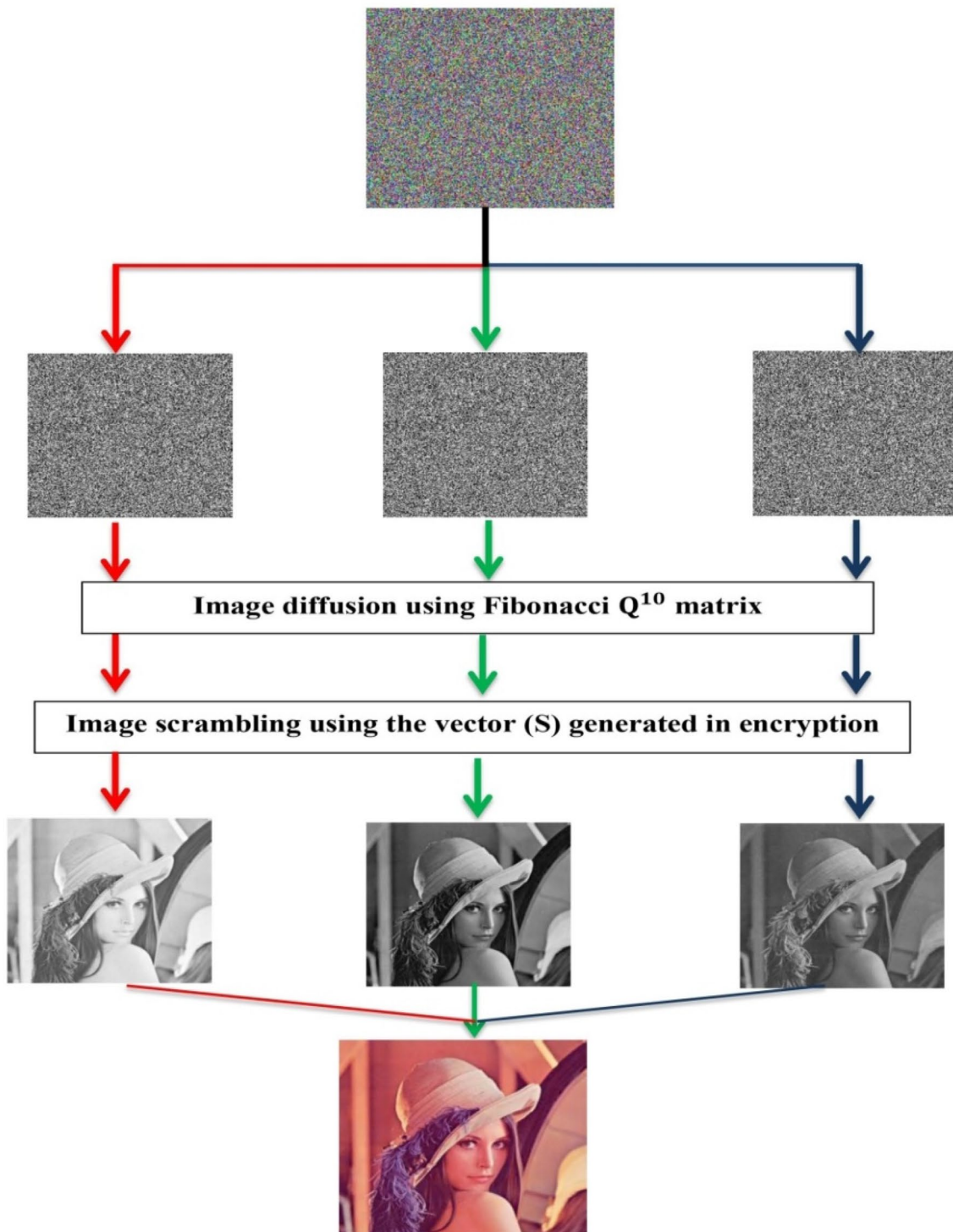
**Step#2:** get the sequence  $L$  by iterating the system in (1)  $N_0 + MN/4$  and then discard  $N_0$ .

**Step#3:** sort the sequence  $L$  in ascending order and return sorted pixels position in vector  $S$  with size  $MN$ .



**Fig. 1** Flow chart of one round of color image encryption





**Fig. 2** Flow chart of one round of color image decryption

### 3.2 Image scrambling

Image scrambling is the process of changing the position of the pixels without changing their value. In our algorithm, the image vector  $P$  scrambled by the sequence  $S$  that is defined by:

$$R_i = P(S_i), i = 1 : MN \quad (8)$$

where  $R$  is the scrambled vector obtained from changing the pixel's position in  $P$  using the values in the vector  $S$ .

### 3.3 Diffusion

In diffusion, the Fibonacci Q-matrix is used to change image pixels value as follows:

**Step#1:** reshape scrambled vector  $R$  into the matrix  $R'$  with size  $M \times N$ .

**Step#2:** divide the matrix  $R'$  into sub-blocks of sizes  $2 \times 2$

**Step#3:** obtain the encrypted image  $E$  by multiplying each sub-block in the scrambled image  $R'$  with the Fibonacci Q matrix ( $Q^{10}$ ) defined in Eq. (4) as follows:

$$\begin{bmatrix} E_{ij} & E_{i,j+1} \\ E_{i+1,j} & E_{i+1,j+1} \end{bmatrix} = \begin{bmatrix} R'_{ij} & R'_{i,j+1} \\ R'_{i+1,j} & R'_{i+1,j+1} \end{bmatrix} \begin{bmatrix} 89 & 55 \\ 55 & 34 \end{bmatrix} \bmod 256 \quad (9)$$

where  $i = 1 : M$ ,  $j = 1 : N$  with a unified step 2.

---

#### Algorithm 1. The proposed algorithm for one round of color image encryption

---

**Input:** The color image  $I$  with size  $M \times N \times 3$ , constant of the fractional system  $a, b, c, d, \gamma, \alpha$  and  $N_0$

1. Read the plain image  $I$ , then divided it into three channels ( $I_R, I_G, I_B$ ) each with size  $M \times N$ .

2. Do the following steps for each channel:

1. Convert the matrix  $I$  into vector  $P$

2. Calculate the first initial condition of the fractional system by

$$3. x_1 = \frac{\sum_{i=1}^{MN} P_i + (M \times N)}{2^{23} + (M \times N)}$$

4. For  $i = 2: 4$  do

$$5. x_i = \text{mod}(x_{i-1} \times 10^6, 1)$$

6. End for

7. Iterate the system in (1)  $N_0 + MN/4$  and then discard  $N_0$  to obtain the sequence  $L$ .

8.  $[t, S] = \text{sort}(L)$

9. For  $i = 1: MN$  do

$$10. R_i = P(S_i)$$

11. End for

12. Convert  $R$  into the 2D matrix  $R'$

13. For  $i = 1: 2: M$

14. For  $j = 1: 2: N$

$$15. \begin{bmatrix} E_{ij} & E_{i,j+1} \\ E_{i+1,j} & E_{i+1,j+1} \end{bmatrix} = \begin{bmatrix} R'_{ij} & R'_{i,j+1} \\ R'_{i+1,j} & R'_{i+1,j+1} \end{bmatrix} \begin{bmatrix} 89 & 55 \\ 55 & 34 \end{bmatrix} \bmod 256$$

16. End for

17. End for

3. Combine the three encrypted channels to obtain the encrypted image  $C$

**Output:** The encrypted image  $C$

---

### 3.4 Decryption

The inverse process of encryption is decryption. This process aims to retrieve the input image from the encrypted one. In the proposed algorithm, the diffusion Eq. (9) changed:


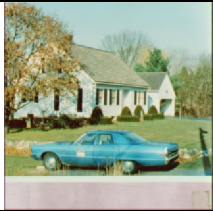



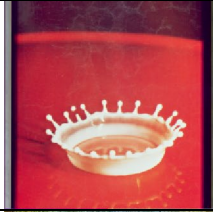

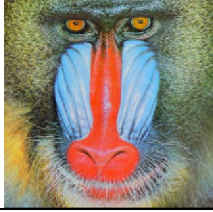
$$\begin{bmatrix} R_{ij} & R_{i,j+1} \\ R_{i+1,j} & R_{i+1,j+1} \end{bmatrix} = \begin{bmatrix} E_{ij} & E_{i,j+1} \\ E_{i+1,j} & E_{i+1,j+1} \end{bmatrix} \begin{bmatrix} 34 & -55 \\ -55 & 89 \end{bmatrix} \bmod 256 \quad (10)$$

where  $i = 1 : M$ ,  $j = 1 : N$  with a unified step 2.

Also, the sequence  $S$  that generated in Sect. 3.1 used to retrieve the original image by replacing Eq. (8) in the scrambling process with the following equation:

$$P(S_i) = R_i, i = 1 : MN \quad (11)$$

**Table 2** Standard color images

Image name	Size	Original image	Image name	Size	Original image
Lena	$256 \times 256$		House	$512 \times 512$	
Couple	$256 \times 256$		AirPlane	$512 \times 512$	
Tree	$256 \times 256$		Splash	$512 \times 512$	
Female	$256 \times 256$		Baboon	$512 \times 512$	

**Table 3** Entropy for different color images in three channels

Test Image	R	G	B
Lena	7.9974	7.9971	7.9973
Couple	7.9967	7.9966	7.9977
Tree	7.9971	7.9972	7.9971
Female	7.9969	7.9968	7.9968
House	7.9993	7.9993	7.9993
Airplane	7.9992	7.9993	7.9993
Splash	7.9992	7.9991	7.9993
Baboon	7.9993	7.9992	7.9993

**Table 4** Comparison of entropy of Lena

Method	R	G	B	Average
Proposed	7.9974	7.9971	7.9973	7.9973
Chai et al.(2019)	7.9973	7.9969	7.9971	7.9971
Li et al. (2019a, b)	7.9991	7.9973	7.9967	7.9977
Rehman et al.(2018)	7.9966	7.9972	7.9967	7.9968
Wu et al. (2018)	7.9892	7.9898	7.9899	7.9896
Zhang et.al (2020)	7.9917	7.9912	7.9918	7.9916
Hosny et al. (2021a, b)	7.9974	7.9976	7.9974	7.9975
Xuejing and Zihui (2020)	7.9980	7.9979	7.9978	7.9979

## 4 Experiments and results

Various experiments were conducted to show the efficiency of the proposed method in color image encryption. These experiments are based on computing information entropy and the correlation between adjacent pixels to show the high randomness of the image encrypted using our proposed algorithm.

Also, the efficiency of our algorithm in resisting differential attacks, brute force attacks, noise, and data attacks is presented. In these experiments, the authors used standard color images that are available in SIPI datasets. The experiments were performed using MATLAB (R2015a) with a Laptop computer equipped with Core i5-2430 M 2.4GH CPU and 4 GB RAM. Table 2 shows all test images used for evaluating our algorithm. In Table 2, there is an eight-color test

image with two sizes ( $256 \times 256$  and  $512 \times 512$ ). Also, the names of all the test images are stated in Table 2.

#### 4.1 Information entropy

Image randomness is usually measured using the information entropy, where a successful image encryption method can generate an encrypted image with high randomness. The entropy is computed for each primary color channel, R, G, and B in color images. If the entropy for each channel is near 8, this means the high randomness of the color image. The mathematical formulation for entropy is:

$$H(s) = - \sum_{i=1}^k P(s_i) \log_2 P(s_i) \quad (12)$$

where  $k$  refers to the total number of pixels in the image,  $P(s_i)$  refers to the probability of  $s_i$ . The entropy is computed for eight standard color images in the three channels, where the three primary channels of these images are encrypted using the proposed method. Obtained values are shown in Table 3. The values of entropy for all color images in all channels are almost identical to the optimum value.

In another experiment, the color image of Lena was encrypted by using our method and the recent algorithms

(Chai et al. 2019; Li et al. 2019a, b; Rehman et al. 2018; Wu et al. 2018; Zhang et al. 2020; Hosny et al. 2021a, b; Xuejing and Zihui 2020). The values of the entropy are calculated and shown in Table 4. Generally, the average entropy (encrypted image) using our technique outperforms the methods (Rehman et al. 2018; Wu et al. 2018; Zhang et al. 2020) and is very similar to the results of the methods (Chai et al. 2019; Li et al. 2019a, b; Hosny et al. 2021a, b; Xuejing and Zihui 2020). The results indicate that our algorithm can produce an encrypted image with high randomness as all values are near 8.

#### 4.2 Correlation analysis

Typically original image has a high correlation between adjacent pixels. A good encryption algorithm should remove this correlation between neighboring pixels. In successfully encrypted images, the correlation between adjacent pixels in the encrypted image should 0. For any two adjacent pixels  $x$  and  $y$ , their correlation is:

**Table 6** Comparison of correlation coefficients for lena

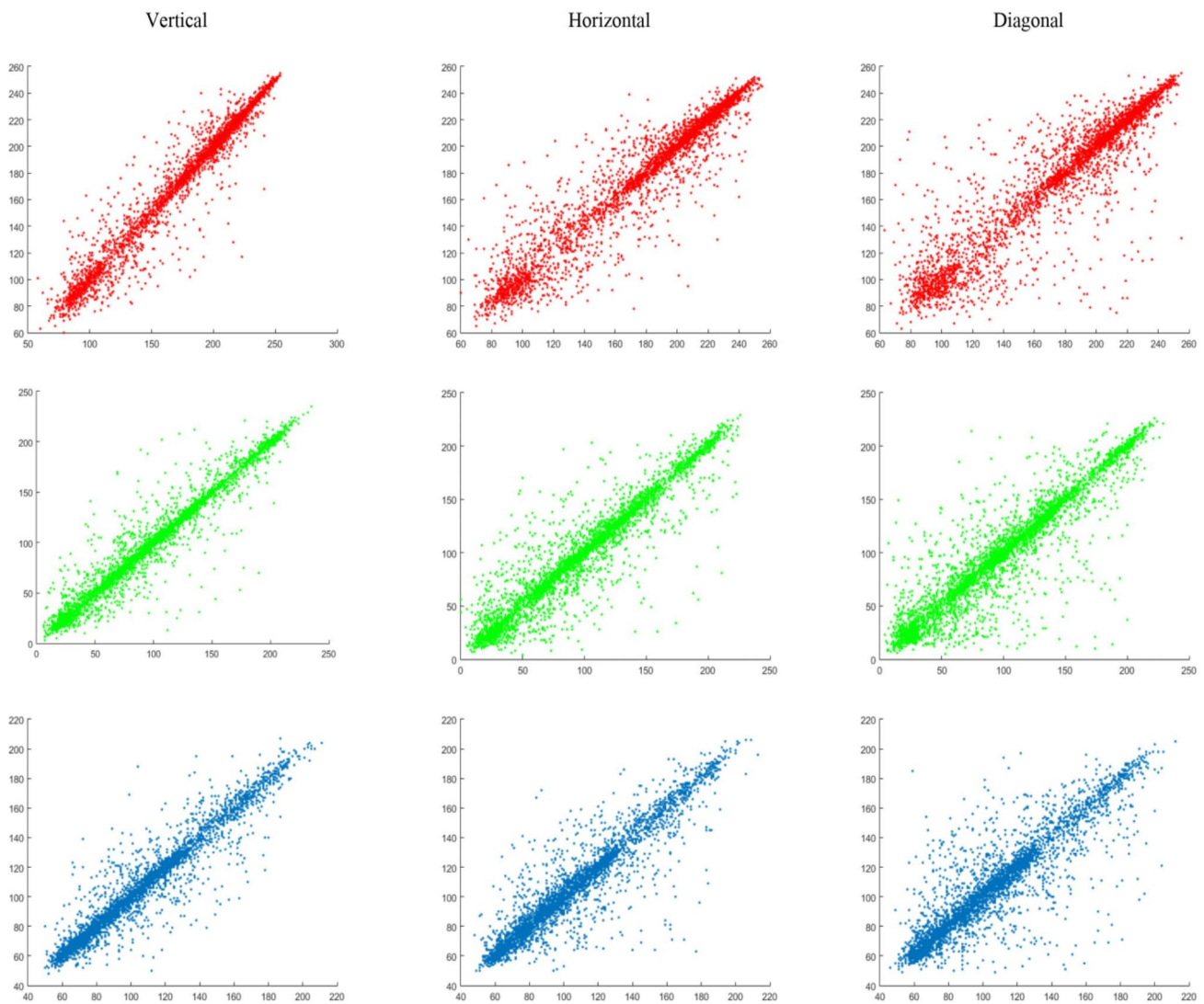
Methods	Directions	R	G	B
Proposed	H	− 0.0154	− 0.0096	− 0.0030
	V	− 0.0102	0.0027	0.0117
	D	0.0159	− 0.0162	− 0.0026
Chai et al.(2019)	H	− 0.0029	− 0.0032	0.0040
	V	0.0013	− 0.0032	− 0.0018
	D	− 0.0026	− 0.0039	0.0012
Li et al.(2019a, b)	H	− 0.0025	0.0058	− 0.0058
	V	0.0913	− 0.0372	0.0036
	D	0.0011	− 0.0014	2.1180e− 04
Rehman et al. (2018)	H	− 0.0073	0.0011	− 0.0061
	V	0.0010	− 0.002	0.0058
	D	− 0.0013	0.0078	− 0.0003
Wu et al. (2018)	H	0.0137	− 0.0246	− 0.0137
	V	− 0.0237	− 0.0170	0.0023
	D	0.0109	− 0.0133	− 0.0013
Zhang et al. (2020)	H	0.0014	0.0033	0.0021
	V	0.0048	− 0.0006	0.0002
	D	0.0002	0.0048	− 0.0040
Hosny et al. (2021a, b)	H	0.0064	0.0009	0.0091
	V	0.0160	0.0034	− 0.0045
	D	− 0.0026	0.0125	− 0.0090
Xuejing and Zihui (2020)	H	0.0092	0.0002	0.0076
	V	0.0203	− 0.0025	0.0006
	D	− 0.0073	− 0.0131	0.0111

V ertical; H Horizontal, D Diagonal

**Table 5** Correlation coefficients for a different color image in three directions

Images	Directions	R	G	B
Couple	V	− 0.0318	0.0115	0.0243
	H	− 0.0056	3.1995e− 04	0.0219
	D	− 0.0012	0.0111	− 0.0046
Tree	V	− 0.0161	0.0307	0.0110
	H	0.0124	0.0081	0.0278
	D	0.0058	− 0.0039	0.0035
Female	V	− 0.0011	0.0147	0.0037
	H	0.0176	0.0024	− 0.0033
	D	− 0.0046	0.0074	− 0.0147
House	V	− 0.0046	0.0140	0.0229
	H	− 0.0067	− 0.0024	0.0234
	D	0.0129	0.0044	0.0341
Airplane	V	0.0238	− 0.0068	− 0.0044
	H	0.0020	0.0096	− 0.0133
	D	− 0.0038	− 0.0047	0.0106
Splash	V	0.0032	0.0152	0.0195
	H	0.0012	0.0415	− 0.0199
	D	− 0.0019	− 0.0027	0.0099
Baboon	V	0.0191	− 0.0070	0.0076
	H	0.0064	0.0110	0.0056
	D	0.0132	0.0056	0.0190

V Vertical, H Horizontal, D Diagonal



**Fig. 3.** Correlation analysis of Lena in three directions for the three channels

$$r_{x,y} = \frac{E((x - E(x))(y - E(y)))}{\sqrt{D(x)D(y)}} \quad (13)$$

where

$$E(x) = \frac{1}{N} \sum_{i=1}^N x_i, D(x) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))^2 \quad (14)$$

The correlation in diagonal, horizontal, & vertical is computed for each primary channel. Table 5 shows the obtained results. All correlation values of the different color images are near 0, indicating that our algorithm broke the strong correlation.

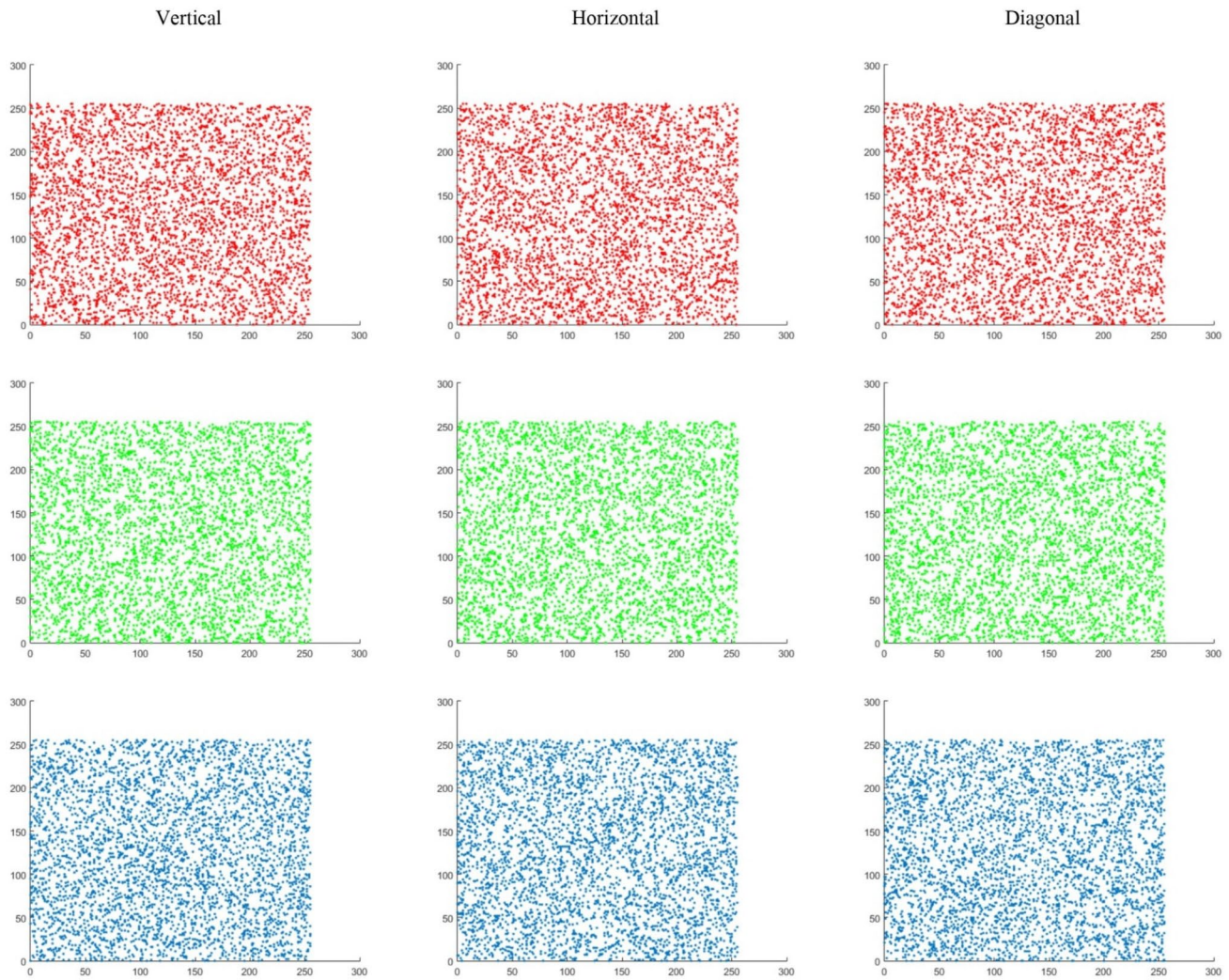
Additional experiments were performed to calculate the correlation coefficients of the novel encryption methods

(Chai et al. 2019; Li et al. 2019a, b; Rehman et al. 2018; Wu et al. 2018; Zhang et al. 2020; Hosny et al. 2021a, b; Xuejing and Zihui 2020), where the obtained results are shown in Table 6. As displayed in Fig. 3, a visualized correlation analysis proves the concept of a strong correlation between adjacent pixels as all pixels clustered in the diagonal direction. However, in Fig. 4, the selected adjacent pixels from the encrypted image occupied the whole space, indicating a weak correlation.

### 4.3 Differential attack

The efficiency of image encryption algorithms depends on their high sensitivity to minimal image changes. The algorithm is considered more efficient when a minimal input





**Fig. 4.** Correlation analysis of encrypted image Lena in three directions for the three channels

**Table 7** NPCR and UACI for different color images

Images	NPCR			UACI		
	R	G	B	R	G	B
Couple	99.5926	99.6170	99.6094	33.4336	33.4296	33.5116
Tree	99.6490	99.6231	99.6155	33.4965	33.4607	33.4270
Female	99.6170	99.6353	99.5926	33.4380	33.4572	33.4994
House	99.6006	99.6071	99.6124	33.4563	33.4374	33.4559
Airplan	99.6128	99.6071	99.6124	33.4356	33.4988	33.4658
Splash	99.5949	99.5987	99.6399	33.4530	33.4741	33.4589
Baboon	99.6048	99.6162	99.5937	33.4024	33.4443	33.4964

image change produces a distinguishable encrypted image. Attackers try to trace differences between two images, which are encrypted using the exact encryption method from the input images with only a one-pixel difference. This process enables attackers to find a relation between the input and

encrypted image to guess the secret key. This kind of attack is known as a differential attack. The higher efficiency of an algorithm makes it more difficult for attackers to guess image information. The resistance to this attack was measured quantitatively using NPCR and UACI:

**Table 8** NPCR and UACI for Lena using different methods

Method	NPCR				UACI			
	R	G	B	Average	R	G	B	Average
Proposed	99.6017	99.6063	99.6368	99.6149	33.4128	33.4980	33.4974	33.4694
Chai et al. (2019)	99.60	99.61	99.61	99.61	33.56	33.45	33.49	3.5
Li et al. (2019a, b)	99.6016	99.6205	99.6095	99.6105	33.2483	33.4977	33.3877	33.3779
Rehman et al. (2018)	99.6078	99.6088	99.6081	99.6082	33.4291	33.4252	33.4219	33.4254
Wu et al. (2018)	99.6137	99.6053	99.6079	99.609	33.4655	33.4781	33.4746	33.4727
Zhang et al. (2020)	99.6243	99.6185	99.6281	99.6236	33.4224	33.4362	33.4604	33.4397
Hosny et al. (2021a, b)	99.6094	99.6124	99.6307	99.6215	33.4666	33.4241	33.4212	33.4373
Xuejing and Zihui (2020)	99.6531	99.6522	99.6518	99.6524	33.4572	33.4715	33.4384	33.4557

$$\text{NPCR} = \frac{1}{M \times N} \sum_{i=1}^N \sum_{j=1}^M D(i, j) \times 100(\%) \quad (15)$$

where NPCR is the number of pixels change rate while NPCR is the unified average Change intensity.

$$D(i, j) = \begin{cases} 0, & \text{if } E_1(i, j) = E_2(i, j), \\ 1, & \text{if } E_1(i, j) \neq E_2(i, j), \end{cases} \quad (16)$$

$$\text{UACI} = \frac{1}{M \times N} \sum_{i=1}^N \sum_{j=1}^M \frac{|E_1(i, j) - E_2(i, j)|}{255} \times 100(\%) \quad (17)$$

where  $E_1$  and  $E_2$  refer to encrypted images from the same input image by changing a single pixel.

In the literature of image encryption, 99.6094 %, 33.4635 % are the typical values of NPCR and UACI. An experiment was performed where we randomly changed on pixels in the input image then encrypted both the original input image and the modified one using our algorithm. The NPCR and UACI were computed for both encrypted images. As shown in Table 7, the obtained results show that all NPCR and UACI for the three primary channels are almost equal to the typical values. Also, Table 8 compares the results of our algorithm and the methods (Chai et al. 2019; Li et al. 2019a, b; Rehman et al. 2018; Wu et al. 2018; Zhang et.al 2020;

Hosny et al. 2021a, b; Xuejing and Zihui 2020). The average values of NPCR and UACI are ideal. Thus, encrypted images produced using our algorithm are secured against differential attacks.

#### 4.4 Histogram analysis

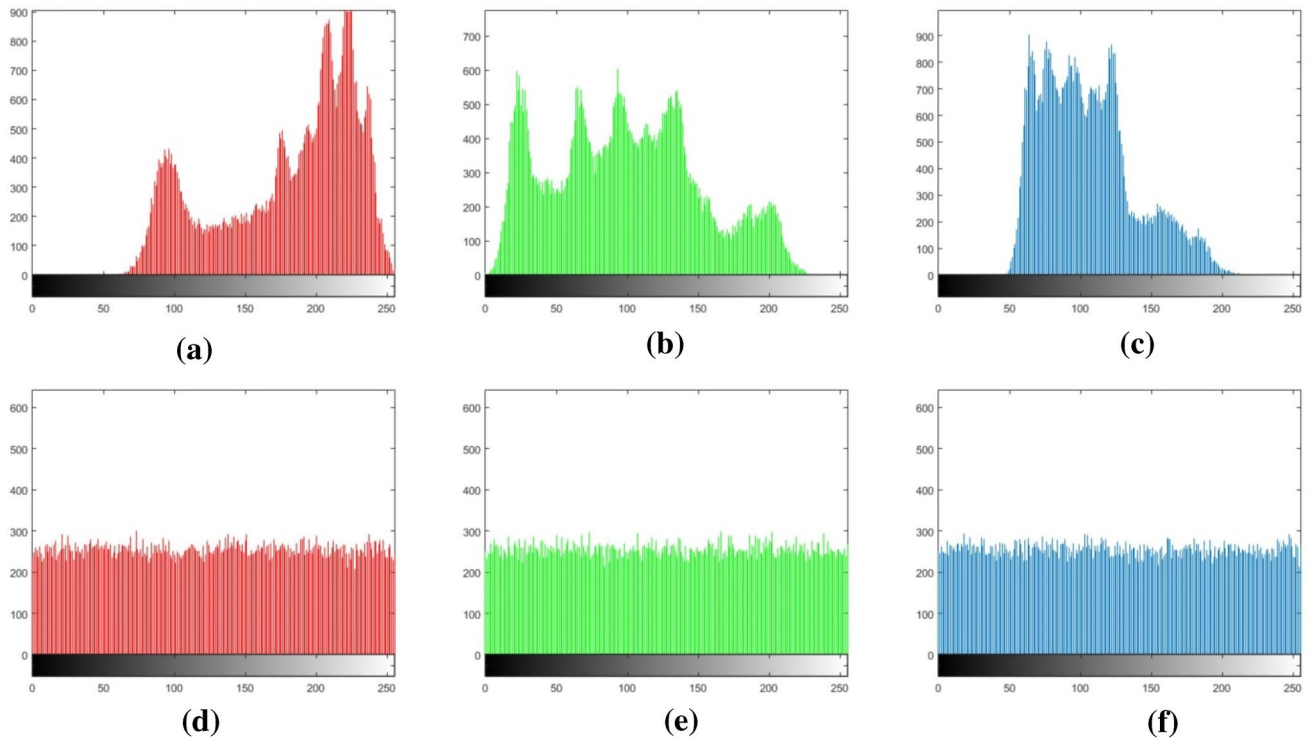
The histogram for each grey level of the color image shows its pixel value distribution. The histogram of both original and encrypted images must be entirely different. Also, the histogram of the original image is usually distributed randomly. However, the histogram of an encrypted image should be uniform. Mathematically, the variances of histograms are calculated by:

$$\text{Var}(Y) = \frac{1}{n^2} \sum_{i=1}^n \sum_{j=1}^n \frac{1}{2} (Y_i - Y_j)^2 \quad (18)$$

The variance of the histogram reflects the histogram uniform distribution for the encrypted image, where both are inversely proportional. Low variance means a uniform histogram. Table 9 shows the variances of histograms for the test color images. The variances of the encrypted images are smaller than the variances of the original images. Figure 5 shows the histogram of the original and encrypted primary channels of the Lena color image. The histograms of the

**Table 9** Variances of histograms for both Original and encrypted images

Image		Original image			Encrypted image		
		R	G	B	R	G	B
256 × 256	Lena	$6.24 \times 10^4$	$2.64 \times 10^4$	$8.5 \times 10^4$	240.7059	264.1255	245.1765
	Couple	$2.1 \times 10^5$	$3.37 \times 10^5$	$2.89 \times 10^5$	299.4902	309.0745	214.1490
	Tree	$8.13 \times 10^4$	$5.7 \times 10^4$	$1.29 \times 10^5$	268.0471	258.0392	262.4941
	Female	$7.9 \times 10^5$	$8.61 \times 10^5$	$6.2 \times 10^5$	281.0980	289.3490	294.6039
512 × 512	House	$7.68 \times 10^5$	$1.33 \times 10^6$	$9.92 \times 10^5$	1014.8	991.9765	1005.8
	Airplane	$2.72 \times 10^6$	$2.74 \times 10^6$	$4.44 \times 10^6$	1114.7	956.1961	1057.4
	Splash	$2.43 \times 10^6$	$3.09 \times 10^6$	$5.94 \times 10^6$	1101.5	1331.2	1005.8
	Baboon	$3.33 \times 10^5$	$5.73 \times 10^5$	$3.21 \times 10^5$	1031.3	1103.4	984.8235



**Fig. 5** Histograms of Lena and its encrypted image using the proposed algorithm. Original image in the first row: **a** R-channel. **b** G-channel. **c** B-channel. The encrypted image in the second row: **d** R-channel. **e** G-channel. **f** B-channel

encrypted channels are uniform, while the histograms of the original channels are not uniform.

#### 4.5 Data cut and noise attacks

Encrypted images may be exposed to data loss or noise when transmitted over the network. An encryption method is successful when efficiently restoring the encrypted image after noise and data cut attacks. This ability is measured by peak signal to noise ratio (PSNR), which is calculated by:

$$PSNR = 10 \times \log_{10} \left( \frac{255^2}{MSE} \right) (db) \quad (19)$$

The MSE is defined by:

$$MSE = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N |I_o(i,j) - I_d(i,j)|^2 \quad (20)$$

where  $I_o$  &  $I_d$  refer to original and encrypted images.

The value of PSNR is directly proportional to image quality, where high values reflect a high similarity between the decrypted and the original image. When the value of PSNR is above 35, it is challenging to distinguish between the original image and the decrypted image. To test the ability of

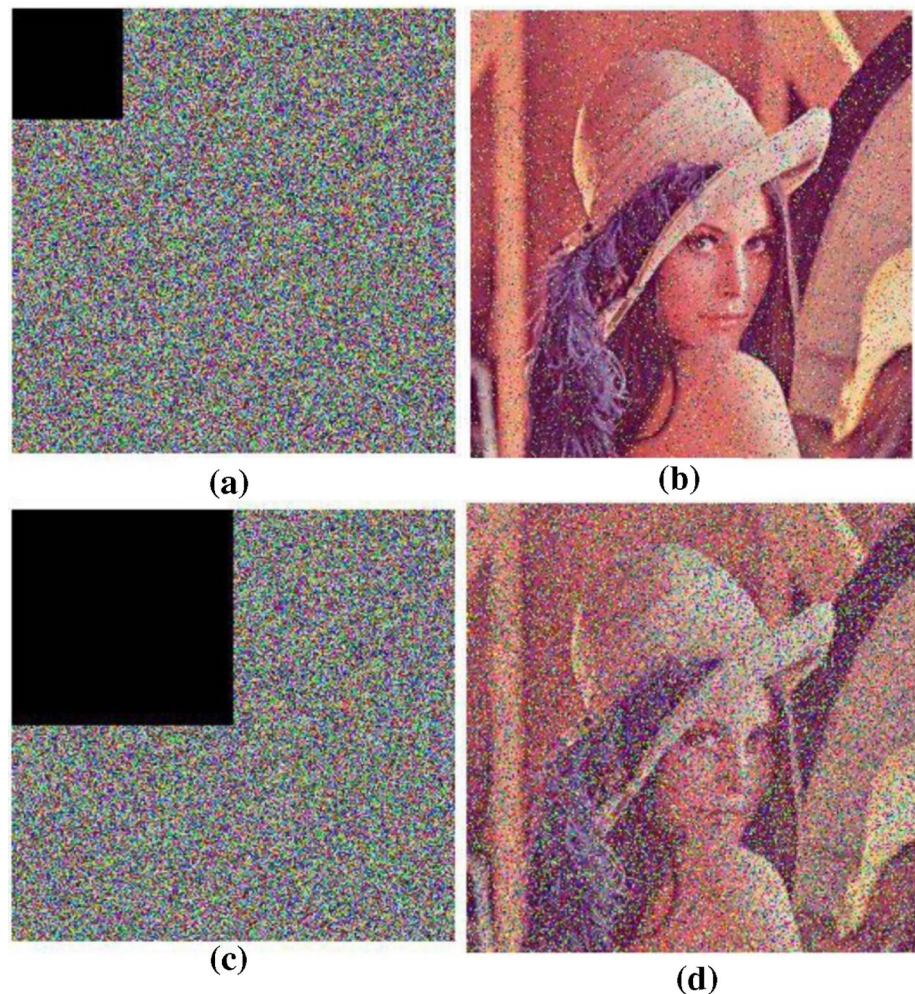
our algorithm in resisting these attacks, we do the following experiments on the encrypted image:

- (1) Add “salt & pepper” noise (SPN) with density 0.002 and 0.005.
- (2) Cut attack by cropping with size  $64 \times 64$  and  $128 \times 128$  at the left corner.

Image contents still recognized that prove the robustness of our algorithm against noise and data cut attacks. Figure 6 shows the decryption results after attacking the encrypted image with different sizes of data cut—the decryption of Lena after adding Salt and Pepper noise with different densities presented in Fig. 7. Also, Table 10 shows the PSNR values for two-color images in the three channels. When we add noise with density 0.002 and 0.005, the average PSNR of the three images' three channels is 29db and 26 dB. While in the case of data cut of size 128, the average PSNR for Lena is 12, and for Baboon is 18. When the data cut is size 64, PSNR average values for Lena and Baboon are 18 and 24, respectively. The experimental results indicate that our algorithm has an excellent performance in restoring encrypted images after noise and data cut attacks.



**Fig. 6** Data cut attack. **a** Encrypted Lena with a cut of size  $64 \times 64$ . **b** The decryption of **a**. **c** Encrypted Lena with a cut of size  $128 \times 128$ . **d** Decrypted image of **c**



#### 4.6 Keyspace

Attackers try all possible keys in the keyspace of an encryption algorithm to know the correct secret key. If the keyspace is large, it is more difficult for attackers to guess it correctly. This kind of attack is known as a brute force attack. The efficiency of the encryption method depends on having a large keyspace to resist this attack. When the keyspace is larger than  $2^{100}$  the algorithm can achieve a higher level of security. In our encryption algorithm for color images, the secret key constructed by the four initial conditions of the fractional hyperchaotic system,  $a, b, c, d, \gamma, \alpha$  and  $N_0$ . If we consider the computation precision is  $10^{15}$ , the size of the keyspace is  $N_0 \times 10^{150}$ . Therefore, the keyspace of this method is sufficient to resist this attack.

#### 4.7 Key sensitivity

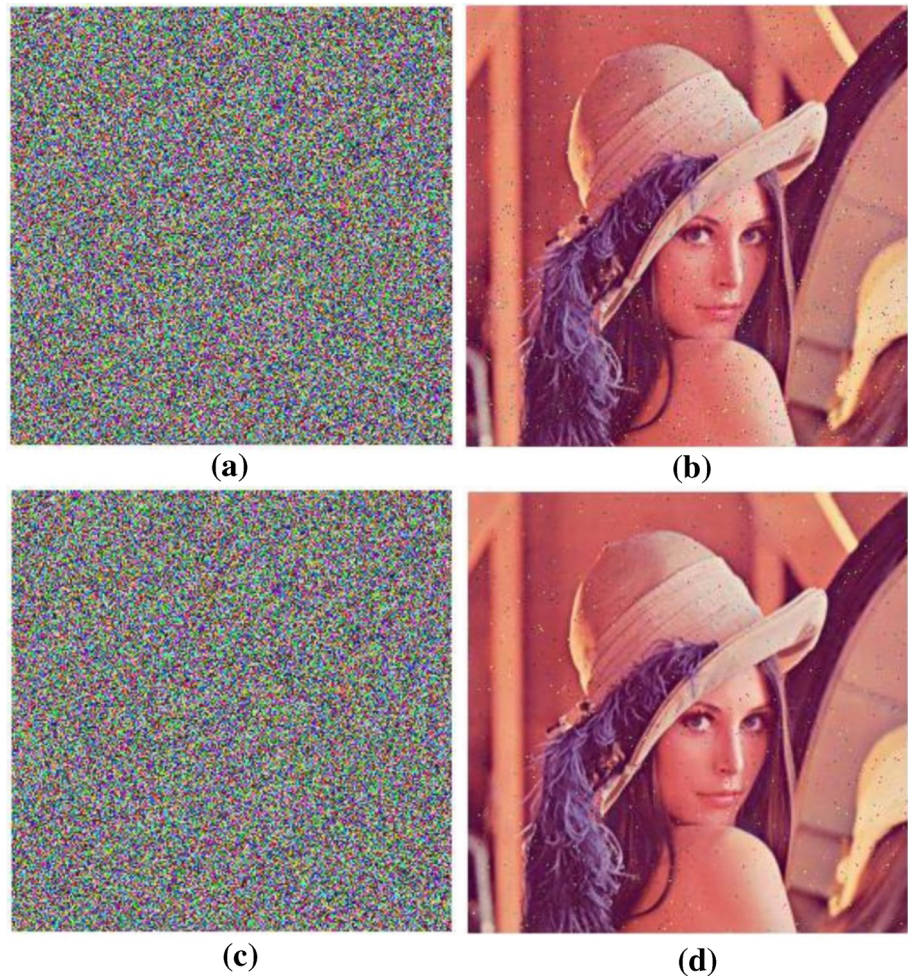
The robustness of the encryption algorithm depends on its sensitivity to the secret key. In other words, minimal

changes in the generation process of the secret key result in another key. Therefore, the modified key cannot be utilized in decrypting the encrypted image by the original key. The decrypted image should be a noisy image without any information about the original image. In this experiment, the original key was used in encrypting the image of Lena, and the encrypted image using this key is shown in Fig. 8b. When we decrypt the image in Fig. 8b with changing  $x_4$  in the initial conditions to  $x_4 + 0000000001$  the plain image is not restored as in Fig. 8c. The original secret key will only restore the plain image, as seen in Fig. 8d.

## 5 Conclusion

Novel utilization of hyperchaotic systems of fractional-order in encrypting color images proposed. In this three-stage encryption algorithm, the 4D hyperchaotic Chen system of fractional-order is used in changing the pixel position. The diffused color image is divided into a group of  $2 \times 2$  blocks,

**Fig. 7** noise attack. **a** Noisy encrypted image (0.005, Salt and Pepper noise). **b** Decrypted image of **a**. **c** Noisy encrypted image (0.002, Salt and Pepper noise). **d** Decrypted image of **c**



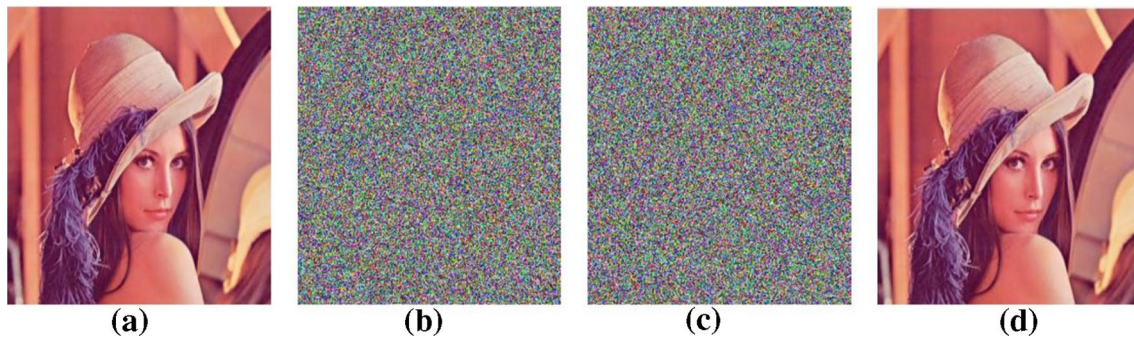
**Table 10** The PSNR uses different attacks

Attack	PSNR (dB)							
	Lena				Baboon			
	R	G	B	Average	R	G	B	Average
SPN with density 0.002	29.2715	29.6508	29.9875	29.6366	29.5367	30.1769	29.7010	29.80487
SPN with a density of 0.005	24.7114	26.0815	26.7650	25.8526	25.7811	26.2857	25.2280	25.76493
Data cut with block size 128X128	11.4779	12.4165	13.5832	12.4925	17.9969	18.5111	17.6164	18.04147
Data cut with block size 64X64	17.0396	17.7707	18.9603	17.9235	23.9470	24.3719	23.5335	23.9508

and then the Fibonacci Q-matrix with  $n = 10$  is used in changing the pixels values for each block. The new encryption algorithm showed high sensitivity to any minimal modifications to the secret key and the pixel distribution where an entirely different encrypted image was obtained. The obtained results ensure the success of the proposed color image encryption algorithm to resist all frequent attacks.

The future work will focus on improving the running speed of our proposed algorithm. Also, we will study applying the proposed algorithm in video encryption and super-resolution images. The emerging deep learning-based encryption approach for color images is another future work.





**Fig. 8.** **a** Original image. **b** Encrypted image of **a** with the original key. **c** Decrypted image of **b** with the modified key. **d** decrypted image of **b** with the original key

## Declarations

**Conflict of Interest** The authors declare that they have no conflict of interest.

## References

- Abd Elaziz MA, Hosny KM, Salah A, Darwish MM, Lu S, Sahlol AT (2020) New machine learning method for image-based diagnosis of COVID-19. *PLoS One* 15(6):e0235187. <https://doi.org/10.1371/journal.pone.0235187>
- Abro WA, Qi G, Ali Z, Feng Y, Aamir M (2020) Multi-turn intent determination and slot filling with neural networks and regular expressions. *Knowl Based Syst* 208:106428
- Ali Z, Qi G, Muhammad K, Ali B, Abro WA (2020) Paper recommendation based on heterogeneous network embedding. *Knowl Based Syst* 210:106438
- Chai X, Fu X, Gan Z, Lu Y, Chen Y (2019) A color image cryptosystem based on dynamic DNA encryption and chaos. *Signal Process* 155:44–62
- Chen B, Yu M, Su Q, Shim HJ, Shi YQ (2018) Fractional quaternion Zernike moments for robust color image copy-move forgery detection. *IEEE Access* 6:56637–56646
- Chen J, Li XW, Wang QH (2019) Deep learning for improving the robustness of image encryption. *IEEE Access* 7:181083–181091
- Ding Y, Wu G, Chen D, Zhang N, Gong L, Cao M, Qin Z (2020) A deep learning-based image encryption and decryption network for internet of medical things. *IEEE Internet Things* 8:1504–1518
- Ding Y, Tan F, Qin Z, Cao M, Choo KKR, Qin Z (2021) DeepKeyGen: a deep learning-based stream cipher generator for medical image encryption and decryption. *IEEE Trans Neural Netw Learn Syst*. <https://doi.org/10.1109/TNNLS.2021.3062754> (Online first)
- Essaid M, Akharraz I, Saaidi A (2019) Image encryption scheme based on a new secure variant of Hill cipher and 1D chaotic maps. *J Inform Secur Appl* 47:173–187
- Hegazi AS, Matouk AE (2011) Dynamical behaviors and synchronization in the fractional-order hyperchaotic Chen system. *Appl Math Lett* 24(11):1938–1944
- Hosny KM, Darwish MM (2019) Resilient color image watermarking using quaternion radial substituted chebychev moments. *ACM Trans Multimed Comput Commun Appl* 15(2):46
- Hosny KM, Darwish MM, Li K, Salah A (2018) Parallel multi-core CPU and GPU for fast and robust medical image watermarking. *IEEE Access* 6:77212–77225
- Hosny KM, Darwish MM, Aboelenen T (2020a) Novel fractional-order generic Jacobi–Fourier moments for image analysis. *Signal Processing* 172:107545
- Hosny KM, Darwish MM, Aboelenen T (2020b) New fractional-order legendre-fourier moments for pattern recognition applications. *Pattern Recogn* 103:1–19
- Hosny KM, Darwish MM, Fouda MM (2021a) Robust color images watermarking using new fractional-order exponent moments. *IEEE Access* 9:47425–47435
- Hosny KM, Kamal ST, Darwish MM (2021b) A color image encryption technique using block scrambling and chaos. *Multimed Tools Appl*. <https://doi.org/10.1007/s11042-021-11384-z> (Online first)
- Irani BY, Ayubi P, Jabalkandi FA, Valandar MY, Barani MJ (2019) Digital image scrambling based on a new one-dimensional coupled Sine map. *Nonlinear Dyn* 97(4):2693–2721
- Jithin KC, Sankar S (2020) Colour image encryption algorithm combining Arnold map, DNA sequence operation, and a Mandelbrot set. *J Inf Secur Appl*. 50:102428
- Kadhim IJ, Premaratne P, Vial PJ (2020) Improved image steganography based on super-pixel and coefficient-plane-selection. *Signal Process* 171:107481
- Kamal ST, Hosny KM, Elgindy TM, Darwish MM, Fouda MM (2021) A new image encryption algorithm for grey and color medical images. *IEEE Access* 9:37855–37865
- Kaur P, Pannu HS, Malhi AK (2019) Plant disease recognition using fractional-order Zernike moments and SVM classifier. *Neural Comput Appl* 31:8749–8768
- Kaur M, Singh D, Kumar V (2020) Color image encryption using minimax differential evolution-based 7d hyper-chaotic map. *Appl Phys B* 126(9):1–19
- Li Y, Tang WK, Chen G (2005) Generating hyperchaos via state feedback control. *Int J Bifurcat Chaos* 15(10):3367–3375
- Li M, Lu D, Wen W, Ren H, Zhang Y (2018) Cryptanalyzing a color image encryption scheme based on hybrid hyper-chaotic system and cellular automata. *IEEE Access* 6:47102–47111
- Li M, Wang P, Liu Y, Fan H (2019a) Cryptanalysis of a novel bit-level color image encryption using improved 1D chaotic map. *IEEE Access* 7:145798–145806
- Li P, Xu J, Mou J, Yang F (2019b) Fractional-order 4D hyperchaotic memristive system and application in color image encryption. *EURASIP J Image Video Process* 2019(1):22
- Liu H, Kadir A, Liu J (2019a) Color pathological image encryption algorithm using arithmetic over Galois field and coupled hyper-chaotic system. *Opt Lasers Eng* 122:123–133
- Liu Z, Wu C, Wang J, Hu Y (2019b) A color image encryption using dynamic DNA and 4-D memristive hyper-chaos. *IEEE Access* 7:78367–78378

- Naskar PK, Bhattacharyya S, Nandy D, Chaudhuri A (2020) A robust image encryption scheme using chaotic tent map and cellular automata. *Nonlinear Dyn* 100:2877–2898
- Nematzadeh H, Enayatifar R, Yadollahi M, Lee M, Jeong G (2020) Binary search tree image encryption with DNA. *Optik* 202:163505
- Pak C, Huang L (2017) A new color image encryption using combination of the 1D chaotic map. *Signal Process* 138:129–137
- Parvaz R, Zarebnia M (2018) A combination chaotic system and application in color image encryption. *Opt Laser Technol* 101:30–41
- Rehman A, Liao X, Ashraf R, Ullah S, Wang H (2018) A color image encryption technique using exclusive-OR with DNA complementary rules based on chaos theory and SHA-2. *Optik* 159:348–367
- Sahari ML, Boukemara I (2018) A pseudo-random numbers generator based on a novel 3D chaotic map with an application to color image encryption. *Nonlinear Dyn* 94(1):723–744
- Teng L, Wang X, Meng J (2018) A chaotic color image encryption using integrated bit-level permutation. *Multimed Tools Appl* 77(6):6883–6896
- Wang X, Feng L, Li R, Zhang F (2019a) A fast image encryption algorithm based on non-adjacent dynamically coupled map lattice model. *Nonlinear Dyn* 95:2797–2824
- Wang X, Qin X, Liu C (2019b) Color image encryption algorithm based on customized globally coupled map lattices. *Multimed Tools Appl* 78(5):6191–6209
- Wu X, Kan H, Kurths J (2015) A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps. *Appl Soft Comput* 37:24–39
- Wu X, Wang D, Kurths J, Kan H (2016) A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system. *Inf Sci* 349:137–153
- Wu X, Wang K, Wang X, Kan H, Kurths J (2018) Color image DNA encryption using NCA map-based CML and one-time keys. *Signal Process* 148:272–287
- Xian Y, Wang X, Yan X, Li Q, Wang X (2020) Image encryption based on chaotic sub-block scrambling and chaotic digit selection diffusion. *Opt Lasers Eng* 134:106202
- Xuejing K, Zihui G (2020) A new color image encryption scheme based on DNA encoding and spatiotemporal chaotic system. *Signal Process Image Commun* 80:115670
- Yang B, Liao X (2018) A new color image encryption scheme based on logistic map over the finite field  $\mathbb{Z}_N$ . *Multimed Tools Appl* 77(16):21803–21821
- Yang YG, Guan BW, Li J, Li D, Zhou YH, Shi WM (2019) Image compression-encryption scheme based on fractional-order hyperchaotic systems combined with 2D compressed sensing and DNA encoding. *Opt Laser Technol*. <https://doi.org/10.1016/j.optlastec.2019.105661>
- Yang F, Mou J, Liu J, Ma C, Yan H (2020a) Characteristic analysis of the fractional-order hyperchaotic complex system and its image encryption application. *Signal Process*. <https://doi.org/10.1016/j.sigpro.2019.107373>
- Yang F, Mou J, Ma C, Cao Y (2020b) Dynamic analysis of an improper fractional-order laser chaotic system and its image encryption application. *Opt Lasers Eng*. <https://doi.org/10.1016/j.optlaseng.2020.106031>
- Yao S, Chen L, Zhong Y (2019) An encryption system for color image based on compressive sensing. *Opt Laser Technol*. <https://doi.org/10.1016/j.optlastec.2019.105703>
- Zhang Q, Han J (2021) A novel color image encryption algorithm based on image hashing, 6D hyperchaotic and DNA coding. *Multimed Tools Appl* 80(9):13841–13864
- Zhang YQ, He Y, Li P, Wang XY (2020) A new color image encryption scheme based on 2DNLCML system and genetic operations. *Opt Lasers Eng*. <https://doi.org/10.1016/j.optlaseng.2020.106040>
- Zhou N, Chen W, Yan X, Wang Y (2018) Bit-level quantum color image encryption scheme with quantum cross-exchange operation and hyper-chaotic system. *Quantum Inf Process* 17(6):1–24
- Zhou Z, Mu Y, Wu QJ (2019) Coverless image steganography using partial-duplicate image retrieval. *Soft Comput* 23(13):4927–4938

**Publisher's Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.