OPEN ACCESS
Fractals, Vol. 31, No. 6 (2023) 2340111 (16 pages)

DOI: 10.1142/S0218348X23401114

World Scientific
www.worldscientific.com

MULTI-IMAGE HYBRID ENCRYPTION ALGORITHM BASED ON PIXEL SUBSTITUTION AND GENE THEORY

XINYU GAO [*,†] JUN MOU [*,†,§,**] BO LI [*,†,¶,**]
SANTO BANERJEE [‡] and BO SUN [*,†,‖,**]

[*]*School of Management*
Dalian Polytechnic University
Dalian 116034, P. R. China

[†]*School of Information Science and Engineering*
Dalian Polytechnic University
Dalian 116034, P. R. China

[‡]*Department of Mathematical Sciences*
Giuseppe Luigi Lagrange, Politecnico di Torino
Corso Duca degli Abruzzi 24, Torino, Italy

[§]*moujun@csu.edu.cn*
[¶]*libolb@dlpu.edu.cn*
[‖]*sunbo-0709@126.com*

Received October 9, 2022
Accepted December 1, 2022
Published May 4, 2023

**Corresponding authors.

Abstract

A hybrid encryption scheme for multi-image is proposed in this paper, which can encrypt different types and different sizes of images simultaneously. First, the order of the discrete map is extended from integer order to unequal fractional order. By choosing suitable parameters, the map exhibits chaotic behavior, and using the map for the designed image encryption system can enlarge the key space of the cryptosystem. Then, the plain images are pixel substituted. The chaotic sequences produced from the unequal fractional-order discrete map are shaped and sorted; the index sequences generated by the sorting are used to replace plain image pixels. After plain image pixels are replaced, DNA encoding, selective diffusion, and gene exchange are performed. The statistical properties of the images are masked by the diffusion algorithm. Finally, simulation experiments and security test results show that the designed multi-image hybrid encryption algorithm is effective and secure.

Keywords: Multi-Image; Hybrid Encryption; Unequal Fractional Order; Gene Theory.

1. INTRODUCTION

The rise of mobile Internet and social networks has led to digital images being widely used around the world. The rapidly developing communication technology brings enormous advantages to people's daily life, but it also brings great challenges to information security, especially image and video security.[1] In daily life and work, images are often transmitted frequently from end to end because they carry rich information content.[2] Some images contain personal private information, while others contain important trade secrets, patient privacy, etc. More importantly, the massive front-end devices deployed in public and Internet environments can not only infringe on personal privacy and security, but also cause hacker attacks once they are exploited.[3] In this environment, how to protect the security of image information has become an important issue for all countries. In order to effectively protect image security, scholars from various countries are committed to researching secure and efficient image encryption schemes.[4–6] In real life, especially in commercial secrecy, military secrecy, images are often transmitted in bulk and vary in size. To meet the large number of image transmissions and applications in daily communication, business, military, education, and medical, multi-image encryption schemes have become a new research target and hot spot.[7,8]

Among the many image encryption methods, there are many scholars who study encryption methods based on chaos theory. This is because chaotic systems are extremely sensitive to both the initial situation and system parameters, and their random-like behavior and ergodic nature meet the needs of cryptography.[9–13] There are many types of chaotic systems, and the common ones are chaotic systems or chaotic maps of integer order.[9,14–17] In recent years, through continuous research on fractional order, it has been found that chaotic systems can still exhibit complex behavioral properties when extended from integer order to fractional order.[18–21] The system parameters are increased on this basis, which brings a larger key space for encryption algorithms.[22] The chaotic map is extended from integer order to unequal fractional order and unequal anomalous fractional order in this paper.[23] By choosing appropriate system parameters and initial conditions, the chaotic map of fractional order also exhibits rich dynamical behaviors.[24]

In recent years, the emergence of various multi-image encryption schemes has provided rich theoretical guidance for the application of image encryption.[25–27] Someone uses image stitching to stitch multi-image of the same size and then encrypt them[28,29]; someone uses optical means to encrypt multi-image, which is fast and efficient but highly-dependent on optical equipment and means[30–32]; someone uses quaternions to encrypt multi-image, and the number and size of images encrypted in a single pass will always be limited[33–35]; someone has segmented multi-image by blocks and fused and encrypted them in stereoscopic space, this scheme contributes to the further development of encryption of multi-image.[36,37] The design of multi-image encryption algorithm still has problems that need to be solved, for example, the type of encrypted images is relatively single, and many encryption

schemes only encrypt grayscale images or color images; the size of encrypted images is not flexible enough, and the general encryption scheme can only encrypt multi-image of the same size; the amount of encrypted images is limited, but in practical applications, it is often not constrained. In addition, the design of multi-image encryption algorithms can be extended from plane to three-dimensional space, which provides more possibilities for algorithm operation. The rich content of algorithm design can lead to better security of images. Based on these problems, a scheme that can hybridize the encryption of multiple color and grayscale images is proposed. By splitting and re-fusing the images, the size of the images that can be encrypted is more flexible and the number of images is not constrained. The encryption algorithm is implemented based on fractional-order chaos map, pixel substitution, and gene theory, the effectiveness and security of image encryption and decryption are guaranteed.

The structure of this paper is described as follows. Section 2 shows the dynamical behavior of fractional-order chaotic map. Section 3 describes the multi-image encryption scheme. Section 4 verifies the encryption and decryption effect of the designed scheme. Section 5 tests and analyzes the security of the algorithm. Section 6 summarizes the multi-image hybrid encryption work.

2. FRACTIONAL-ORDER CHAOTIC MAP

The chaotic map is expressed as

$$\begin{cases} x_{n+1} = e[ay_n^2 + b + c\sin(fn)]x_n, \\ y_{n+1} = dy_n + kx_n. \end{cases} \tag{1}$$

Extending the chaotic map from integer order to fractional order by introducing the Caputo difference operator, we have

$$\begin{cases} {}^{c}\Delta_{t_0}^{q} x(t) = \Delta_{t_0}^{-(m-q)} \Delta^m x(t) \\ \qquad\qquad = \dfrac{1}{\Gamma(m-q)} \displaystyle\sum_{s=t_0}^{t-(m-q)} (t-s-1)^{(m-q-1)} \\ \qquad\qquad \times \Delta^m x(s), \\ t^{(q)} = \dfrac{\Gamma(t+1)}{\Gamma(t+1-q)}, \end{cases} \tag{2}$$

where Δ denotes the forward difference operator, and m is the value rounded down for q. Then there is

$$\begin{cases} x(t) = \displaystyle\sum_{k=0}^{m-1} \frac{(t-t_0)^{(k)}}{k!} \Delta^k x(t_0) + f(q-1), \\ \Lambda^k x(t_0) = x_k, \quad k = 0, 1, \ldots, m-1, \\ f(q-1) = \dfrac{1}{\Gamma(q)} \displaystyle\sum_{s=tt}^{t-q} (t-s-1)^{(q-1)} ff(q-1), \\ ff(q-1) = f(s+q-1, x(s+q-1)), \\ tt = t_0 + m - q. \end{cases} \tag{3}$$

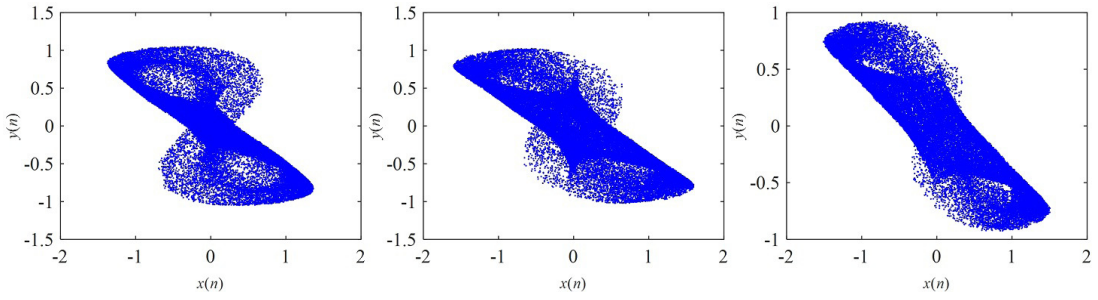
So,

$$\begin{cases} x(n) = x(0) + \dfrac{1}{\Gamma(q_1)} \displaystyle\sum_{i=1}^{n} \frac{\Gamma(n-i+q_1)}{\Gamma(n-i+1)} x(n)^*, \\ x(n)^* = e\begin{pmatrix} ay^2(i-1) + b \\ + c\sin(f(i-1)) \end{pmatrix} x(i-1) - x(i-1), \\ y(n) = y(0) + \dfrac{1}{\Gamma(q_2)} \displaystyle\sum_{i=1}^{n} \frac{\Gamma(n-i+q_2)}{\Gamma(n-i+1)} y(n)^*, \\ y(n)^* = [dy(i-1) + kx(i-1) - y(i-1)]. \end{cases} \tag{4}$$

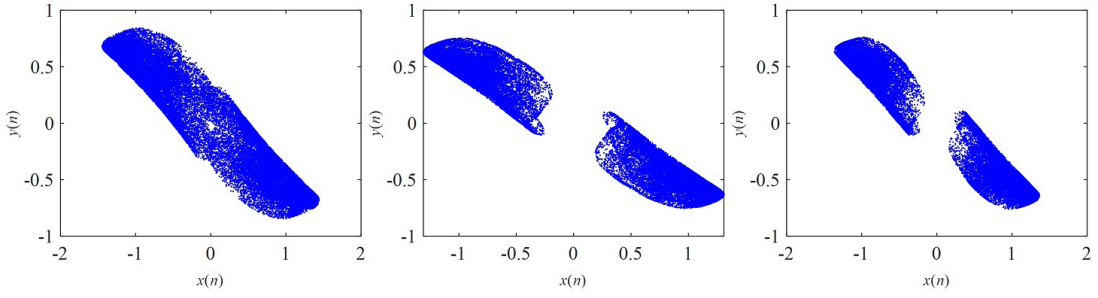
Let $(a, b, c, d, e, f, k, x_0, y_0) = (1.5, -1, 0.04, 1.72, 0.5, 0.9, 1, -0.1, 0.1)$, orders q_1 and q_2 take different values and the attractor changes, as shown in Fig. 1. When the two orders change, the trajectory of the attractor is changing with it. When the two orders change, the trajectory of the attractor is changing with it. The attractors of fractional order are shown in Fig. 1a, and the attractors of integer and anomalous fractional order are shown in Fig. 1b. The rich dynamical behavior of the fractional-order chaotic map can be seen from the change of attractors, which supports the design of the image encryption system.

3. MULTI-IMAGE HYBRID ENCRYPTION SCHEME

The scheme is divided into four main parts: image fusion, pixel substitution, diffusion and gene exchange. First, all plaintext images are split and fused into a plaintext cube. Then, the chaotic cube sequences are sorted by rows and the sorted index cubes are used for pixel substitution. The diffusion algorithm contains both Deoxyribonucleic Acid (DNA) addition and DNA subtraction operations. The choice of whether to use the addition or subtraction operation between the image cube and the



(a)



(b)

Fig. 1 Phase diagram at different orders **(a)** $q_1 = 0.9, q_2 = 0.5; q_1 = 0.9, q_2 = 0.85; q_1 = 0.95, q_2 = 0.9$ **(b)** $q_1 = 1, q_2 = 1; q_1 = 1.05, q_2 = 1; q_1 = 1.05, q_2 = 1.05$.

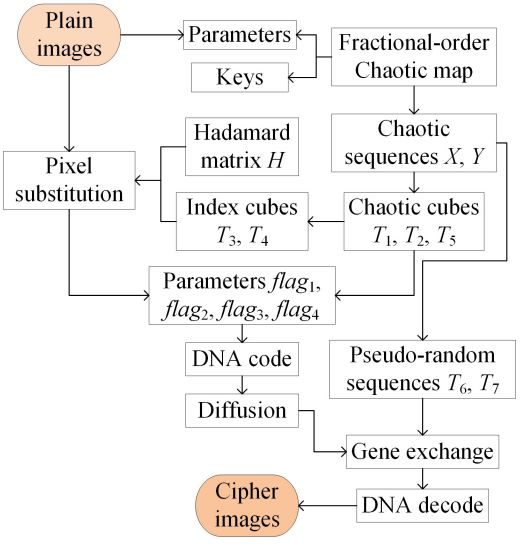


Fig. 2 Encryption procedure description diagram.

chaotic cubes is based on the addition and subtraction control sequences. Gene exchange is realized according to the principle of cross-swap between non-sister chromosomes, and the cross-swap of DNA in chromosomes is the coded image fragment swap after diffusion. The process of encryption is illustrated in Fig. 2, and the specific encryption operation is described as follows:

Step 1: Read in the plaintext images one by one and record the size of each image.

Step 2: Convert all the plaintext images into column vectors and stitch them together with length sl. Set the length, width and height of the fused plaintext cube as H, W, and L, respectively, where the length and width of the cube can be set by choice, L is calculated as follows:

$$L = \text{ceil}\left(\frac{sl}{HW}\right), \tag{5}$$

where ceil $(\bullet)$ is an upward rounding function.

Step 3: Shape the plaintext column vector into a plaintext cube of $H \times W \times L$, denoted as A.

Step 4: Calculate the information entropy of each cross-section of the plaintext cube, which yields eight parameters associated with the plaintext images.

$$\begin{cases} Hm = -\sum_{i=0}^{LL} p(i)\log_2 p(i), \\ hm_i = Hm_i - \text{floor}(Hm_i), \quad i = 1, \ldots, L, \\ h_i = \sum_{j=(i-1)\text{floor}(\frac{L}{8})}^{i\text{floor}(\frac{L}{8})} hm_j, \quad i = 1, \ldots, 8, \end{cases} \tag{6}$$

where floor $(\bullet)$ is a downward rounding function, $p(i)$ denotes the probability of pixel i, LL means pixel level.

Step 5: Enter all parameters, two chaotic sequences of length $H \times W \times L$, denoted as X and Y, can be obtained.

Step 6: Shape the chaotic sequences to obtain two chaotic cubes T_1 and T_2 of size $H \times W \times L$. Sort the chaotic cubes T_1 and T_2 by rows to obtain two index cubes T_3 and T_4.

$$\begin{cases} (\sim, T_3(i,:,k)) \\ \quad = \text{sort}(T_1(i,:,k)) - 1, \quad i = 1, \ldots, H, \\ (\sim, T_4(i,:,k)) \\ \quad = \text{sort}(T_2(i,:,k)) - 1, \quad k = 1, \ldots, L, \end{cases} \tag{7}$$

where sort $(\bullet)$ is a sorting function.

Step 7: Pixel substitution.

Step 7.1: Generate a Hadamard matrix H.

$$\begin{cases} ma = \max(H, W, L), \\ H = \text{hadamard}(ma). \end{cases} \tag{8}$$

Step 7.2: Using the pixel value of cube A as an index, find the corresponding value in cube T_3 or T_4, then substitute that value for the pixel value at the corresponding position. The cube after pixel substitution is noted as B.

$$B(i,j,k) = \begin{cases} T_3(i, A(i,j,k) + 1, k) \\ \quad \times (i+j+k) \mod 2 = 0 \ \& \\ H(i,j) = 1,255 - T_3(i, A(i,j,k) + 1, k) \\ \quad \times (i+j+k) \mod 2 = 0 \ \& \\ H(i,j) = -1, T_4(i, A(i,j,k) + 1, k) \\ \quad \times (i+j+k) \mod 2 = 1 \ \& \\ H(i,j) = 1,255 - T_4(i, A(i,j,k) + 1, k) \\ \quad \times (i+j+k) \mod 2 = 1 \ \& \\ H(i,j) = -1, \quad i = 1, \ldots, H, \\ \quad j = 1, \ldots, W, \ \ k = 1, \ldots, L. \end{cases} \tag{9}$$

Step 8: Diffusion.

Step 8.1: A new cube T_5 can be obtained by using cubes T_1 and T_2.

$$T_5 = abs(T_1 - T_2). \tag{10}$$

Step 8.2: Taking the remainder of the last value of cubes B, T_1, T_2, and T_5 yields the four DNA encoding rule parameters $\text{flag}_1, \text{flag}_2, \text{flag}_3$, and flag_4.

$$\begin{cases} \text{flag}_1 = B(H,W,L) \mod 8 + 1, \\ \text{flag}_2 = T_1(H,W,L) \mod 8 + 1, \\ \text{flag}_3 = T_2(H,W,L) \mod 8 + 1, \\ \text{flag}_4 = T_5(H,W,L) \mod 8 + 1. \end{cases} \tag{11}$$

Step 8.3: The cubes B, T_1, T_2, and T_5 are DNA encoded according to the rules $\text{flag}_1, \text{flag}_2, \text{flag}_3$, and flag_4, respectively. The encoded DNA cubes are noted as B_1, T_{11}, T_{21}, and T_{51}, respectively.

Step 8.4: Diffuse the first cross-section of cube B. The diffused cube is noted as C.

$$C(i,j,1) = B(i,j,1) = \begin{cases} +T_{11}(i,j,1), T_{51}(i,j,1) =' A', \\ -T_{11}(i,j,1), T_{51}(i,j,1) =' T', \\ +T_{21}(i,j,1), T_{51}(i,j,1) =' G', \\ -T_{21}(i,j,1), T_{51}(i,j,1) =' C', \\ i = 1, \ldots, H, \quad j = 1, \ldots, 4W. \end{cases} \tag{12}$$

Step 8.5: Diffuse the remaining cross-section of cube B.

$$C(i,j,k) = B(i,j,k) = \begin{cases} +T_{11}(i,j,1) + C(i,j,k-1), \\ \quad T_{51}(i,j,1) =' A', \\ -T_{11}(i,j,1) - C(i,j,k-1), \\ \quad T_{51}(i,j,1) =' T', \\ +T_{21}(i,j,1) + C(i,j,k-1), \\ \quad T_{51}(i,j,1) =' G', \\ -T_{21}(i,j,1) - C(i,j,k-1), \\ \quad T_{51}(i,j,1) =' C', \quad i = 1, \ldots, H, \\ \qquad j = 1, \ldots, 4W, \ \ k = 2, \ldots, L. \end{cases} \tag{13}$$

Step 9: Gene exchange.

Step 9.1: Based on the chaotic sequences X and Y, two pseudo-random number sequences T_6 and T_7

of length $(H \times L/4)$ can be obtained. Sequence T_6 is used to control the position of gene exchange and sequence T_7 is used to control the length of gene exchange.

$$\begin{cases} T_7(i) = Y(i) \mod 57 + 8, \\ T_6(i) = \begin{cases} X(i), X(i) \le \max(T_7), \\ X(i) - 64, X(i) > \max(T_7), \end{cases} \\ i = HWL - HL/4 + 1, \ldots, HWL. \end{cases} \tag{14}$$

Step 9.2: Consider the DNA coding sequences of two adjacent rows as a set of DNA with a double helix structure and the two adjacent sets of DNA as a pair of non-sister chromatids, and then exchange them. The cube after gene exchange is noted as D.

$$\begin{cases} D = C, \\ D(i+2 : i+3, T_6(t) : T_6(t) + T_7(t), k) \\ \quad = C(i : i+1, T_6(t) : T_6(t) + T_7(t), k), \\ D(i : i+1, T_6(t) : T_6(t) + T_7(t), k) \\ \quad = C(i+2 : i+3, T_6(t) : T_6(t) + T_7(t), k), \\ t = 1, \ldots, HL/4, \quad i = 1, 5, \ldots, H-3, \quad k = 1, \ldots L \end{cases} \tag{15}$$

Step 10: The cube D is DNA decoded to finally obtain the cipher cube E. The cube E is split according to the size of the image input to obtain the individual cipher images.

4. SIMULATION TEST

A good encryption algorithm needs to satisfy both effectiveness and security. To verify the encryption performance of the designed scheme, four sets of simulation test results are presented in Figs. 3–6. The first set of test contained six color images ($256 \times 256 \times 3$,$512 \times 512 \times 3$,$403 \times 610 \times 3$,$744 \times 518 \times 3$,$571 \times 842 \times 3$,$383 \times 510 \times 3$) and four grayscale images (200×200,256×256,512×512,1024×1024), the second set of test contained four color images ($289 \times 200 \times 3$,$200 \times 200 \times 3$,$130 \times 200 \times 3$,$150 \times 200 \times 3$) and four grayscale images (256×256,512×512,480×640,576×726), and the third and fourth sets of tests contained one grayscale image (1024×1024) and one color image ($512 \times 768 \times 3$), respectively. The decryption results in Figs. 4, 5c, 6c and 6f are exactly the same as Figs. 3a, 5a, 6a and 6d, cipher images in Figs. 3b, 5b, 6b and 6e are noise-like images. The simulation results indicate that the designed algorithm can successfully encrypt and decrypt multi-image simultaneously.

5. SECURITY TEST AND ANALYSIS

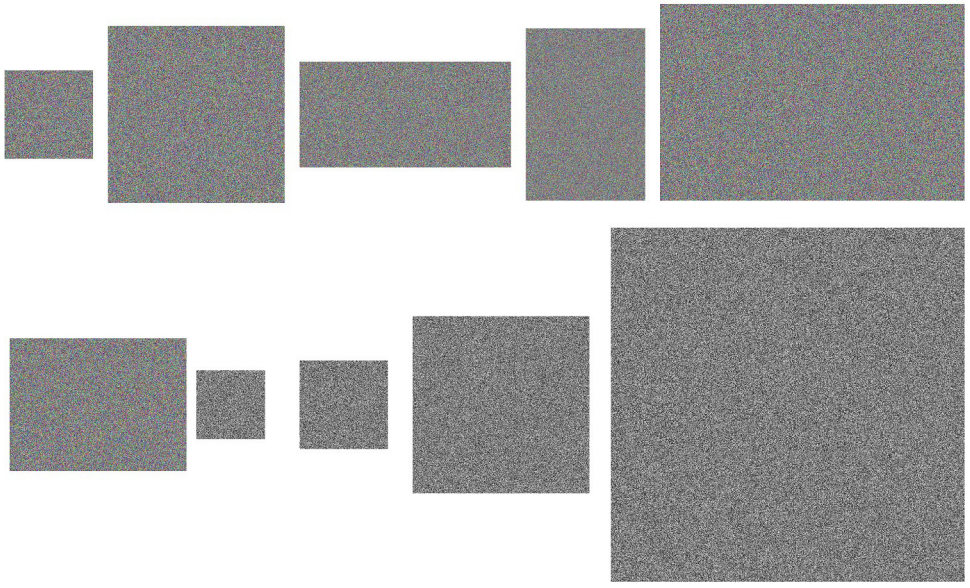
5.1. Key Security Test

5.1.1. *Key space*

The time cost of an attacker using brute force attacks increases as the key space increases, and

(a)

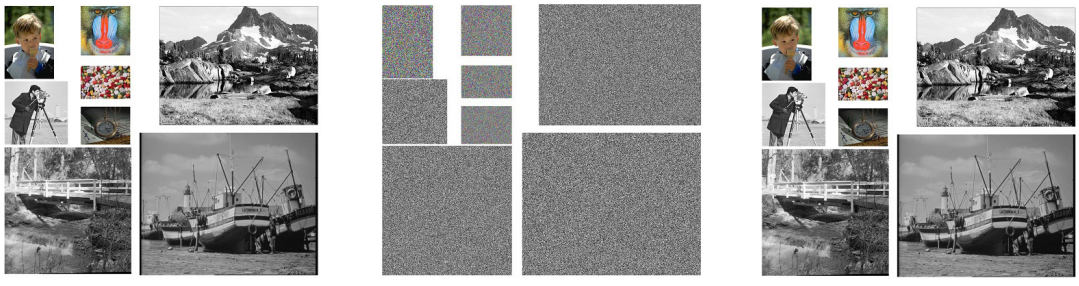
Fig. 3 Encryption simulation results **(a)** original images **(b)** encrypted images.



(a)

Fig. 3 (*Continued*)

Fig. 4 Decryption simulation results.



(a) **(b)** **(c)**

Fig. 5 Encryption simulation results **(a)** original images **(b)** encrypted images **(c)** decryption images.

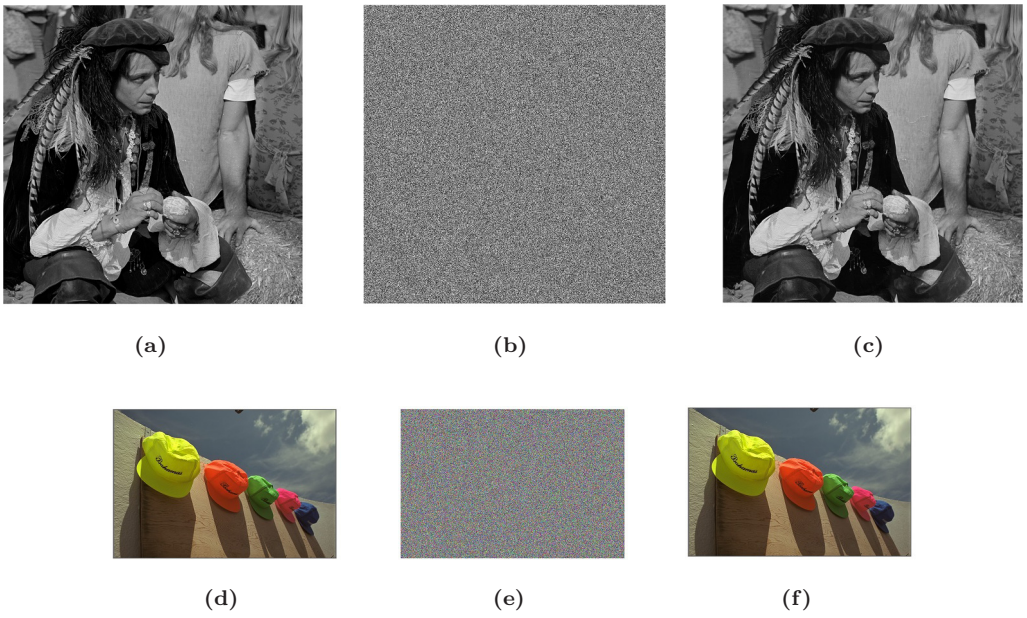


Fig. 6 Encryption simulation results **(a, d)** original images **(b, e)** encrypted images **(c, f)** decryption images.

Table 1 The Key Spaces of Different Algorithms.

Algorithm	Ref. 25	Ref. 28	Ref. 29	Ref. 35	Ref. 39	Proposed
Key space	2^{427}	2^{548}	2^{398}	2^{399}	2^{186}	2^{926}

the probability that the encryption system will be breached decreases. When the key space reaches 2^{100},[38] then the encryption and decryption system has the ability to resist brute force attacks. The key of the designed encryption system contains two parts: the parameters of the chaotic map and the parameters associated with plaintext images. The key space of each key is tested one by one, $h(i, i = 1, \ldots, 8)$ and c, x_0, y_0, q_1, q_2 have a key space of 10^{15}, and a, b, d, e, f, k have a key space of 10^{14}, so the total key space is $10^{(14\times6+15\times13)} \approx 2^{926}$. The key space test results reflect the resistance of the designed encryption algorithm to differential attacks. The key spaces of different algorithms are shown in Table 1,[25,28,29,35,39] and the designed multi-image encryption scheme has sufficient capability to resist differential attacks.

5.1.2. *Key sensitivity*

An image cryptosystem can be considered key-sensitive if a minor modification in the key during the decryption process will cause the decryption to fail. A secure encryption and decryption system needs to be sensitive to the key for the algorithm and the cipher images to be less vulnerable to breakage. A parameter c is randomly selected and a minor modification is added to the decryption process. The decryption results are shown in Fig. 7, which do not contain useful visual information. The test results in Fig. 7 illustrate that the presented multi-image cryptosystem is quite key-sensitive.

5.2. Statistical Characterization

5.2.1. *Histogram*

The histogram reflects the light and dark information of the plaintext image, but in the cipher image, the light and dark information of the images should be hidden to resist attacks. A color image and a grayscale image are randomly selected among the images tested by the algorithm to test the histograms of the plaintext and cipher images, respectively. The results are shown in Fig. 8, the histograms of plaintext images are tumbling, thus reflecting the overall lightness or darkness of the image. The histograms of cipher images are flat. The designed encryption scheme can successfully

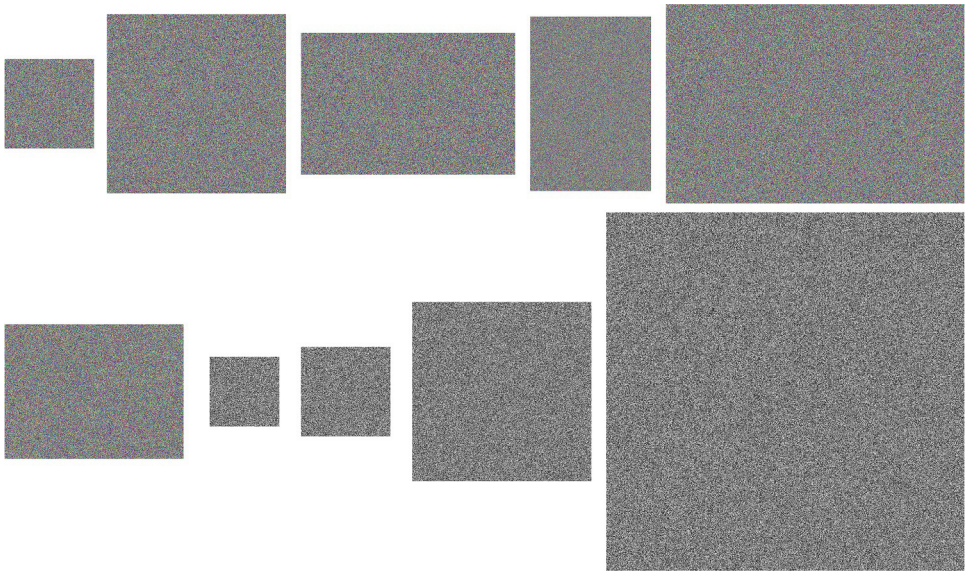


Fig. 7 Key sensitivity test results, $c = c + 10^{-15}$.

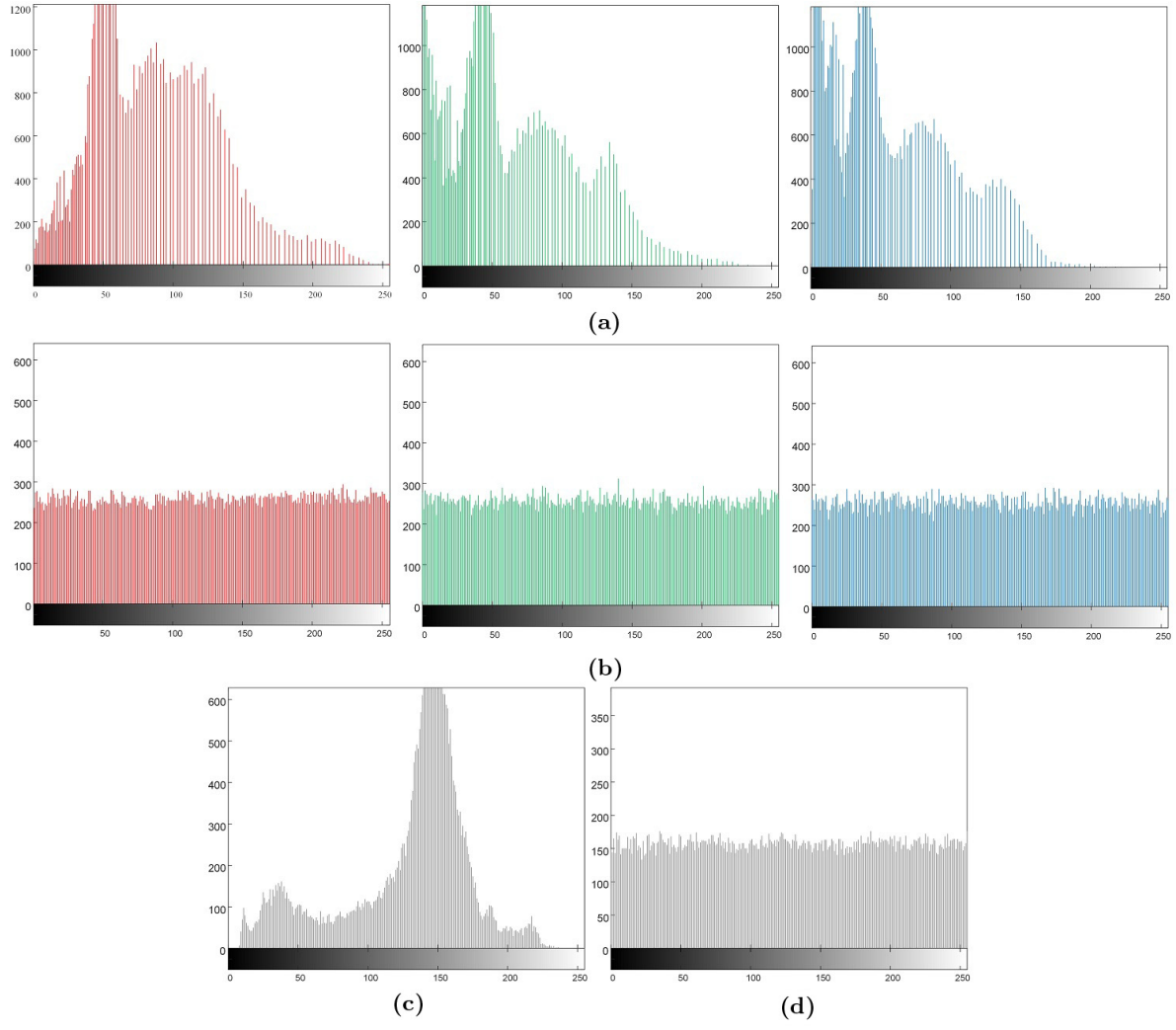


Fig. 8 Histogram of different images **(a)** histogram of color original image "4.1.01" **(b)** histogram of color cipher image **(c)** histogram of grayscale original image "fishingboat" **(d)** histogram of grayscale cipher image.

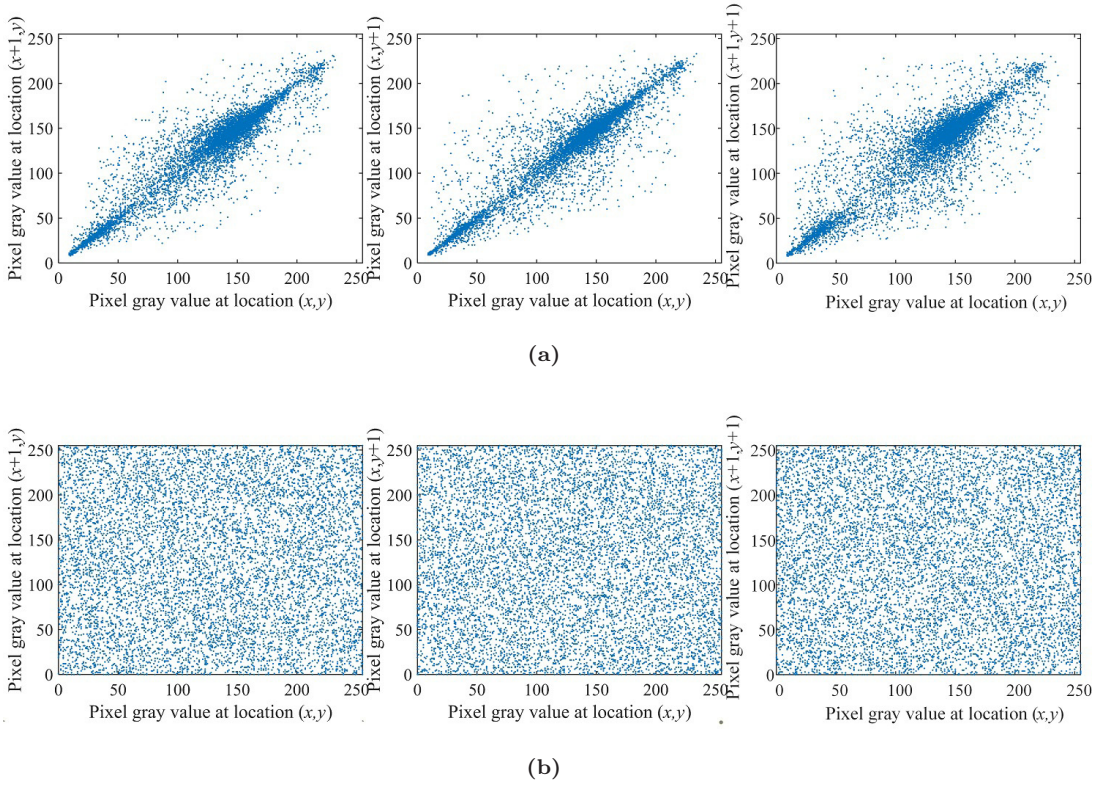


Fig. 9 Adjacent pixel correlation **(a)** Adjacent pixel correlation in horizontal, vertical and diagonal directions for grayscale image "fishingboat" **(b)** Adjacent pixel correlation of the corresponding cipher image.

protect against attacks by hiding the light and dark information of the images.

5.2.2. *Adjacent pixel correlation*

In digital images, individual pixels do not exist independently, so there is a strong correlation between adjacent pixels of an image. To prevent attackers from using the correlation to attack the images and the algorithm, the encryption algorithm needs to disrupt the correlation. The results of the proposed scheme for disrupting the correlation of an image are shown in Fig. 9 and Table 2. A grayscale image is randomly selected among the images tested by the algorithm. The correlation coordinates of the original image and cipher image in all directions are shown in Figs. 9a and 9b. From Fig. 9, the plaintext image exhibits strong correlation and the distribution of neighboring pixels of the cipher image is spread over the whole coordinate area. In Table 2, the adjacent pixel correlation coefficients of the plaintext images are close to 1, and the absolute values of the adjacent pixel correlation coefficients of the cipher images are close to 0. Figure 9 and Table 2 together illustrate that the encryption scheme can reduce the correlation between adjacent pixels to protect the image.

5.2.3. *Information entropy*

When the information entropy of an image is large enough, the effective information of the image is difficult to be recognized, and the theoretical value of information entropy is 8. The information entropies of different images are tabulated in Table 3, and the information entropies of different sizes of cipher images reach 7.99, they are very nearly to the theoretical value. The information entropies of different algorithms are shown in Table 4.[25,40–43] The designed algorithm can effectively obfuscate the original images so that the images cannot be broken by statistical analysis.

5.3. Differential Attack Resistance Test

An attacker encrypts the same image twice and observes how minor variations in the plaintext image result in variations in the cipher image to attack the encryption and decryption system. When

Table 2 Adjacent Pixel Correlation Coefficients of the Plaintext Images and Cipher Images.

Images		Plaintext Images			Cipher Images		
		Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
4.1.01	R	0.9584	0.9740	0.9459	−0.0065	−0.0076	0.0011
	G	0.9687	0.9731	0.9514	−0.0063	−0.0016	−0.0065
	B	0.9524	0.9598	0.9384	0.0035	0.0048	0.0038
baboon	R	0.8670	0.9217	0.8550	0.0014	0.0028	0.0016
	G	0.7700	0.8621	0.7404	0.0025	0.0013	−0.0023
	B	0.8813	0.9038	0.8384	−0.0028	0.0046	−0.0043
bandon	R	0.9858	0.9965	0.9841	−0.0020	−0.0025	−0.0039
	G	0.9662	0.9946	0.9626	−0.0022	0.0047	0.0076
	B	0.9558	0.9773	0.9433	−0.0044	−0.0072	0.0010
brandyrose	R	0.9935	0.9928	0.9914	0.0051	−0.0053	0.0037
	G	0.9862	0.9868	0.9748	−0.0037	−0.0037	0.0029
	B	0.9612	0.9575	0.9444	0.0054	−0.0055	0.0059
newyork	R	0.9279	0.9379	0.8948	0.0039	0.0011	0.0016
	G	0.8995	0.9094	0.8679	−0.0069	0.0042	−0.0025
	B	0.8996	0.9130	0.8659	−0.0018	−0.0036	−0.0039
pool	R	0.9690	0.9557	0.9048	−0.0029	−0.0026	0.0032
	G	0.9681	0.9818	0.9522	0.0083	0.0021	0.0013
	B	0.9718	0.9802	0.9626	0.0078	0.0046	0.0072
fishingboat		0.9276	0.9215	0.8661	0.0044	−0.0041	0.0019
5.1.12		0.9729	0.9569	0.9388	−0.0035	0.0053	−0.0049
5.2.08		0.9122	0.9279	0.8628	0.0013	−0.0017	0.0026
5.3.01		0.9799	0.9770	0.9650	0.0053	0.0024	0.0016

Table 3 Information Entropy of Different Images.

Images	Sizes	Plaintext Images			Cipher Images		
		R	G	B	R	G	B
4.1.01	256 × 256 × 3	6.4200	6.4457	6.3807	7.9973	7.9975	7.9970
baboon	512 × 512 × 3	7.7067	7.4744	7.7522	7.9994	7.9993	7.9994
bandon	403 × 610 × 3	5.9395	5.9194	4.9755	7.9993	7.9992	7.9994
brandyrose	744 × 518 × 3	7.1988	7.5829	6.8277	7.9994	7.9996	7.9996
newyork	571 × 842 × 3	6.9021	6.6460	6.5450	7.9996	7.9996	7.9996
pool	383 × 510 × 3	4.5418	5.5702	4.4569	7.9992	7.9991	7.9990
fishingboat	200 × 200		7.1349			7.9953	
5.1.12	256 × 256		6.7057			7.9972	
5.2.08	512 × 512		7.2010			7.9994	
5.3.01	1024 × 1024		7.5237			7.9998	

Table 4 Information Entropy of Different Images.

Algorithms	Image Size	Information Entropy
Ref. 25	512 × 512	7.9993
Ref. 40	512 × 512	7.9992
Ref. 41	512 × 512	7.9994
Ref. 42	512 × 512	7.9993
Ref. 43	512 × 512	7.9993
Proposed	512 × 512	7.9994

there is a minor variation in the original image, the s reliable encryption system can generate an entirely different cipher image. The image change is measured by the number of pixels change rate and the unified average changing intensity (NPCR and UACI). During the differential attack test, the multi-image is fused into a plaintext image cube for the first encryption; a pixel point in the plaintext cube is randomly selected for a small change

Table 5 NPCR and UACI of Different Images.

Images	NPCR (%)			UACI (%)		
	R	G	B	R	G	B
4.1.01	99.6124	99.6099	99.6158	33.4521	33.4687	33.4667
baboon	99.6217	99.6182	99.6179	33.4721	33.4784	33.4560
bandon	99.6153	99.6202	99.6196	33.4812	33.4625	33.4706
brandyrose	99.6263	99.6192	99.6201	33.4514	33.4566	33.4608
newyork	99.6180	99.6098	99.6134	33.4497	33.4523	33.4618
pool	99.6125	99.6113	99.6206	33.4714	33.4835	33.4767
fishingboat		99.6286			33.4531	
5.1.12		99.6213			33.4677	
5.2.08		99.6174			33.4693	
5.3.01		99.6096			33.4509	
Average value		99.6172			33.4643	

Table 6 NPCR and UACI of Different Algorithms.

Algorithms	NPCR (%)	UACI (%)
Ref. 27	99.6060	33.5126
Ref. 34	99.6077	33.4398
Ref. 36	99.6100	33.4800
Ref. 40	99.5900	33.4100
Ref. 42	99.6161	33.4794
Ref. 44	99.6138	33.4809
Proposed	99.6172	33.4643

and then encrypted a second time. The cipher images obtained from the two encryptions are put together for comparison. The test results are shown in Table 5, where the NPCR is greater than its theoretical value of 99.6094% and the UACI is close to its ideal value of 33.4635%. The test results of different algorithms are shown in Table 6,[27,34,36,40,42,44] and the designed multi-image encryption algorithm has an advantage in resisting differential attacks compared with other algorithms.

5.4. Robustness Test

5.4.1. *Noise attack resistance test*

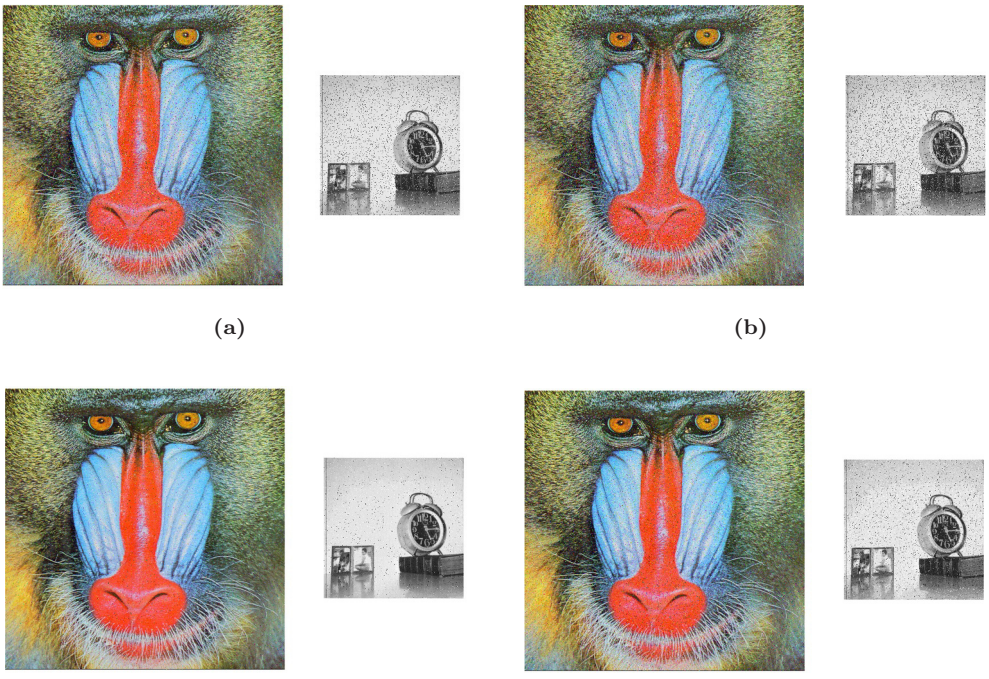
Cipher images are susceptible to noise contamination when transmitted in the channel, and whether the contaminated images can be decrypted depends on the robustness of the encryption and decryption system. The cipher cubes are added with salt and pepper noise (SPN) of intensity 0.05 and 0.07, Gaussian noise (GN) of variance 10^{-4} and 10^{-6}, respectively. A color image and a grayscale image are randomly selected to show the decryption results, as shown in Fig. 10. By observing the decryption results, it is easy to see that the main visual information about the original images can be discerned in the decrypted images even if the cryptographic images are contaminated with different intensities and types of noise. The results in Fig. 10 show that the designed multi-image encryption scheme has a certain ability to restore the cipher images when it encounters noise contamination.

5.4.2. *Shear attack resistance rest*

Clipping attack is one of the common attacks in which the attacker removes and replaces the contents of the cipher images. A robust image encryption system can recover the visual information about the original images when a portion of the cipher content is modified. After multi-image are fused and encrypted, the decryption result is shown in Fig. 11 after clipping 12.5% in the center of the cipher cube. Despite the noise in the decrypted images, the main information of the original images can still be recognized. From Fig. 11, the designed multi-image encryption and decryption system can be unaffected by the visual information of the images when subjected to a slight noise attack, demonstrating the capability of the encryption and decryption system to withstand shear attacks.

5.5. Speed Analysis

Encryption speed is an important factor for images to be used for real-time secure transmission. The designed multi-image hybrid encryption scheme contains three components: pixel replacement,



(a) **(b)**

(c) **(d)**

Fig. 10 Results of noise pollution decryption **(a)** SPN, 0.05 **(b)** SPN, 0.07 **(c)** GN, 10^{-6} **(d)** GN, 10^{-4}.

Fig. 11 Results of shearing attack.

Table 7 Test Results of Encryption Speed.

Procedure	Pixel Replacement	Diffusion	Gene Exchange	Total
Time (s)	1.54	47.32	2.41	51.27
Speed (MB/s)	3.94	0.13	2.52	0.12

diffusion and gene exchange. The running time and speed of each part of the algorithm are shown in Table 7. The test results in Table 7 show that the diffusion process decreases the running speed of the whole encryption process, which is due to the judgment link designed by the diffusion algorithm. In future algorithm research, process optimization of diffusion algorithms is an important goal of algorithm design.

6. CONCLUSIONS

A scheme to hybridize multiple color and grayscale images for encryption is devised in this paper. Multiple color or grayscale images of different sizes are fed into the encryption system, and after image fusion, key generation, pseudo-random sequence generation, pixel substitution, DNA selective diffusion, and gene exchange steps, a set of noise-like encrypted images can be obtained. In the simulation test part, color and grayscale images with different sizes are selected for encryption at the same time. The simulation results not only verify the effectiveness of the algorithm, but also reflect the wide applicability of the algorithm, i.e. the algorithm is applicable to both color and grayscale images, and to images of different sizes at the same time. In terms of security, the results of key space and key sensitivity tests demonstrate the ability of the encryption and decryption system to resist brute force attacks; the results of statistical analysis show that the designed encryption and decryption system can conceal the statistical characteristics of the original images successfully and strongly resist the attacker's statistical analysis attacks; differential attacks and robustness tests results together reflect the ability of the designed encryption and decryption system to protect both the images and the algorithm, whether the attacks are performed on the algorithm or on the images. The simulation experiments and security tests together reflect the application value of the designed multi-image encryption and decryption algorithm. In future research work, while investigating more secure multi-image encryption algorithm, the encryption speed of the algorithm needs to be further improved to meet the demand for real-time secure transmission of multiple images.

ACKNOWLEDGMENTS

This work was supported by the National Natural Science Foundation of China (Grant No. 62061014); The Basic Scientific Research Projects of Colleges and Universities of Liaoning Province (Grant No. LJKZ0545).

ORCID

X. Gao https://orcid.org/0000-0002-1609-5548
J. Mou https://orcid.org/0000-0002-7774-2833
B. Li https://orcid.org/0000-0002-4384-7418
S. Banerjee https://orcid.org/0000-0002-2135-695X
B. Sun https://orcid.org/0000-0002-1192-1185

REFERENCES

1. X. Li, J. Mou, S. Banerjee, Z. Wang and Y. Cao, Design and DSP implementation of a fractional-order detuned laser hyperchaotic circuit with applications in image encryption, *Chaos Solitons Fractals* **159** (2022) 112133.
2. L. N. Wang, Y. H. Cao, H. Jahanshahi, Z. S. Wang and J. Mou, Color image encryption algorithm based on Double layer Josephus scramble and laser chaotic system, *Optik* **275** (2023) 170590.
3. Z. Tang, J. Song, X. Zhang and R. Sun, Multiple-image encryption with bit-plane decomposition and chaotic maps, *Opt. Lasers Eng.* **80** (2016) 1.
4. X. Bi, C. Shuai, B. Liu, B. Xiao, W. Li and X. Gao, Privacy-preserving color image feature extraction by quaternion discrete orthogonal moments, *IEEE Trans. Inf. Forensics Secur.* **17** (2022) 1655.
5. X. L. Chai, Y. J. Wang, Z. H. Gan, X. H. Chen and Y. S. Zhang, Preserving privacy while revealing thumbnail for content-based encrypted image retrieval in the cloud, *Inform. Sci.* **604** (2022) 115.
6. X. L. Chai, Y. J. Wang, X. H. Chen, Z. H. Gan and Y. S. Zhang, TPE-GAN: Thumbnail preserving encryption based on GAN with key, *IEEE Signal Process. Lett.* **29** (2022) 972.
7. X. Y. Gao, J. Mou, S. Banerjee, Y. H. Cao, L. Xiong and X. Y. Chen, An effective multiple-image encryption algorithm based on 3D cube and hyperchaotic map, *J. King Saud Univ.* **34**(4) (2022) 1535.
8. X. Gao, J. Mou, L. Xiong, Y. Sha, H. Yan and Y. Cao, A fast and efficient multiple images encryption based on single-channel encryption and chaotic system, *Nonlinear Dynam.* **88** (2022) 613.
9. X. C. Liu, J. Mou, J. Wang, S. Banerjee and P. Li, Dynamic analysis of a novel fractional-order chaotic system based on memcapacitor and meminductor, *Fractal Fract.* **6**(11) (2022) 671.
10. T. M. Liu, J. Mou, L. Xiong, X. T. Han, H. Z. Yan and Y. H. Cao, Hyperchaotic maps of a discrete memristor coupled to trigonometric function, *Phys. Scripta* **96**(12) (2021) 15242.
11. Y. W. Sha, B. Sun, X. Y. Chen, J. Mou and H. Jahanshahi, A chaotic image encryption scheme

based on genetic central dogma and KMP method, *Internat. J. Bifur. Chaos Appl. Sci. Engrg.* **32**(12) (2022) 2250186.
12. X. Han, J. Mou, H. Jahanshahi, Y. Cao and F. Bu, A new set of hyperchaotic maps based on modulation and coupling, *Eur. Phys. J. Plus* **137**(4) (2022) 523.
13. X. Y. Gao, B. Sun, Y. H. Cao, S. Banerjee and J. Mou, A color image encryption algorithm based on hyperchaotic map and DNA mutation, *Chinese Phys. B* **32** (2023) 030501.
14. G. Dou, K. X. Zhao, M. Guo and J. Mou, Memristor-based LSTM network for text classification, *Fractals*, doi:10.1142/S0218348X23400406.
15. T. Ma, J. Mou, B. Li, S. Banerjee and H. Z. Yan, Study on the complex dynamical behavior of the fractional-order hopfield neural network system and its implementation, *Fractal Fract.* **6**(11) (2022) 637.
16. T. Ma, J. Mou, H. Yan and Y. Cao, A new class of Hopfield neural network with double memristive synapses and its DSP implementation, *Eur. Phys. J. Plus* **137**(10) (2022) 1135.
17. X. C. Liu, J. Mou, H. Z. Yan and X. Bi, Memcapacitor-coupled Chebyshev hyperchaotic map, *Internat. J. Bifur. Chaos Appl. Sci. Engrg.* **32**(12) (2022) 2250180.
18. L. J. Ren, J. Mou, S. Banerjee and Y. S. Zhang, A hyperchaotic map with a new discrete memristor model: design, dynamical analysis, implementation and application, *Chaos Solitons Fractals* **159** (2023) 112133.
19. Y. X. Chen, J. Mou, H. Jahanshahi, Z. S. Wang and Y. H. Cao, A new mix chaotic circuit based on memristor-memcapacitor, *Eur. Phys. J. Plus* **138**(1) (2023) 78.
20. C. Ma, J. Mou, P. Li and T. Liu, Dynamic analysis of a new two-dimensional map in three forms: Integer-order, fractional-order and improper fractional-order, *Eur. Phys. J. Spec. Top.* **230**(7) (2021) 1945.
21. C. Ma, J. Mou, Y. Cao, T. Liu and J. Wang, Multistability analysis of a conformable fractional-order chaotic system, *Phys. Scripta* **95**(7) (2020) 075204.
22. F. Yu, X. X. Kong, H. F. Chen, Q. L. Yu, S. Cai, Y. Y. Huang and S. C. Du, A 6D fractional-order memristive hopfield neural network and its application in image encryption, *Front. Phys.* **10** (2022) 847385.
23. Y. Deng and Y. Li, Bifurcation and bursting oscillations in 2D non-autonomous discrete memristor-based hyperchaotic map, *Chaos Solitons Fractal* **150** (2021) 111064.
24. T. Liu, J. Mou, H. Jahanshahi, H. Yan and Y. Cao, A class of fractional-order discrete map with multistability and its digital circuit realization, *Phys. Scripta* **97**(7) (2022) 075201.
25. K. A. K. Patro, A. Soni, P. K. Netam and B. Acharya, Multiple grayscale image encryption using cross-coupled chaotic maps, *J. Inf. Secur. Appl.* **52** (2020) 102470.
26. X. Sun, Z. Shao, Y. Shang, M. Liang and F. Yang, Multiple-image encryption based on cascaded gyrator transforms and high-dimensional chaotic system, *Multimed. Tools. Appl.* **80**(10) (2021) 15825.
27. X. Zhang and Y. Hu, Multiple-image encryption algorithm based on the 3D scrambling model and dynamic DNA coding, *Opt. Lasers Technol.* **141** (2021) 107073.
28. D. S. Malik and T. Shah, Color multiple image encryption scheme based on 3D-chaotic maps, *Math. Comput. Simulation* **178** (2020) 646.
29. M. Zarebnia, R. Kianfar and R. Parvaz, Multicolor image compression-encryption algorithm based on chaotic system and fuzzy transform, *Multimed. Tools. Appl.* **78**(8) (2018) 10491.
30. X. Y. Li, X. F. Meng, X. L. Yang, Y. R. Wang, Y. K. Yin, X. Peng, W. Q. He, G. Y. Dong and H. Y. Chen, Multiple-image encryption via lifting wavelet transform and XOR operation based on compressive ghost imaging scheme, *Opt. Lasers Eng.* **102** (2018) 106.
31. Y. Gao, S. Jiao, J. Fang, T. Lei, Z. Xie and X. Yuan, Multiple-image encryption and hiding with an optical diffractive neural network, *Opt. Commun.* **463** (2020) 125476.
32. L. Liu, M. Shan, Z. Zhong and B. Liu, Multiple-image encryption and authentication based on optical interference by sparsification and space multiplexing, *Opt. Laser Technol.* **122** (2020) 105858.
33. Z. Shao, X. Liu, Q. Yao, N. Qi, Y. Shang and J. Zhang, Multiple-image encryption based on chaotic phase mask and equal modulus decomposition in quaternion gyrator domain, *Signal Process. Image Commun.* **80** (2020) 115662.
34. H. S. Ye, N. R. Zhou and L. H. Gong, Multi-image compression-encryption scheme based on quaternion discrete fractional Hartley transform and improved pixel adaptive diffusion, *Signal Process.* **175** (2020) 107652.
35. J. Y. Dai, Y. Ma and N. R. Zhou, Quantum multi-image compression-encryption scheme based on quantum discrete cosine transform and 4D hyperchaotic Henon map, *Quantum Inf. Process.* **20**(7) (2021) 246.
36. A. Sahasrabuddhe and D. S. Laiphrakpam, Multiple images encryption based on 3D scrambling and hyper-chaotic system, *Inform. Sci.* **55** (2021) 252.
37. X. Zhang and X. Wang, Multiple-image encryption algorithm based on the 3D permutation model and chaotic system, *Symmetry* **10**(11) (2018) 660.

38. F. Yang, X. An and L. Xiong, A new discrete chaotic map application in image encryption algorithm, *Phys. Scripta* **97**(3) (2022) 035202.
39. X. Zhang and X. Wang, Multiple-image encryption algorithm based on mixed image element and chaos, *Comput. Electr. Eng.* **62** (2017) 401–413.
40. L. Zhang and X. Zhang, Multiple-image encryption algorithm based on bit planes and chaos, *Multimed. Tools. Appl.* **79**(29–30) (2020) 20753.
41. K. A. K. Patro and B. Acharya, A novel multi-dimensional multiple image encryption technique, *Multimed. Tools Appl.* **79**(19–20) (2020) 12959.
42. M. Hanif, R. A. Naqvi, S. Abbas, M. A. Khan and N. Iqbal, A novel and efficient 3D multiple images encryption scheme based on chaotic systems and swapping operations, *IEEE Access* **8** (2020) 123536–123555.
43. X. Zhang and X. Wang, Multiple-image encryption algorithm based on DNA encoding and chaotic system, *Multimed. Tools. Appl.* **78**(6) (2018) 7841.
44. Y. J. Sun, H. Zhang, C. P. Wang, Z. Y. Li and X. Y. Wang, Networked chaotic map model and its applications in color multiple image encryption, *IEEE Photon. J.* **12**(5) (2020) 1.