



# Plaintext Related Optical Image Hybrid Encryption Based on Fractional Fourier Transform and Generalized Chaos of Multiple Controlling Parameters

Limin Tao · Xikun Liang · Zhijing Wu ·  
Lidong Han · Jiangping Zhu

Received: 12 October 2022 / Accepted: 28 February 2023 / Published online: 14 March 2023  
© Springer Nature B.V. 2023

**Abstract** Combining optical image encryption with digital image encryption, we propose a composed optical image hybrid encryption scheme in this paper. The scheme consists of two main parts. In the first part, the original image is encrypted in 4f optical system in the pattern of double random phase encoding. In the second stage, the result of optical encryption is divided into the real part image and the imaginary one. Then, pixels diffusion and confusion are successively carried out on the two images in parallel. Fractional Fourier transform and a generalized chaos, as well as nonlinear transform of matrices are composited to brace the core computation of the algorithm. Plaintext related cipher technology is fully applied to cryptosystem. Moreover, other tools including cumulative sum

and modular operation, random matrices, dot operation of matrices, sequence rearrangement, etc., are employed to support the algorithm. Cipher statistical analysis according to SP800 R1a shows that the cryptosystem is secure. Encryption simulations and performance analysis show that the algorithm performs well in effectiveness, feasibility, safety and robustness. The innovation of this work includes two aspects: firstly, the high-dimensional chaotic digital image encryption method is integrated into 4f optical image encryption system, and a new idea of optical image encryption is proposed; Secondly, a separate encryption paradigm of real and imaginary images in frequency domain is proposed, which greatly improves the security of image encryption and transmission. Other contributions of this paper consist in: a novel chaos with multiple free parameters is introduced to sustain the cryptosystem; the algorithm has a super large scale key space to ensure the security of the algorithm. Compared with other known schemes, the proposed algorithm shows relatively overall advantages. So, it is a nice candidate for image protection.

L. Tao · X. Liang (✉) · L. Han · J. Zhu  
School of Information Science and Technology, Hangzhou  
Normal University, Hangzhou 311121, China  
e-mail: schenken@hznu.edu.cn

L. Tao  
e-mail: tlm5460@hznu.edu.cn

L. Han  
e-mail: ldhan@hznu.edu.cn

J. Zhu  
e-mail: yz-zjp@hotmail.com

Z. Wu  
College of Zhejiang, Tongji University, Jiaxing 314051,  
China  
e-mail: 1160440752@qq.com  
e-mail: 1160440752@qq.com

**Keywords** Image Encryption · Fractional Fourier Transform · Chaos · Plaintext-related · Dot Operation

## 1 Introduction

As an important part of information security, image security has attracted extensive attention. For image

protection, it has been accepted that image encryption is the most effective means. So, image encryption has drawn much attention in cryptology [1, 2]. In general, image encryption can be divided into two main branches: optical image encryption and digital one. The former encrypts images from the perspective of image acquisition, which is usually implemented in optical system by using Fourier transformation and double Random Phase Mask (RPM) [3, 4]. The latter encrypts images in the sense of image storage, which is accomplished in digital computer by pixels diffusion and confusion (scrambling) [1, 2].

Since 1995, both Fourier Transformation (FT) [3] and Fractional Fourier Transformation (FRFT) [5–7] gradually applied to optical image encryption. Part of published research results include: cipher mechanism and encryption algorithm based on Fourier transform, chaotic map and double random phase masks [8, 9], multiple images encryption using discrete FRFT and novel chaos [10, 11], DNA and chaos image encryption [12], color image encryption applying hyper chaos [13], image encryption by employing a hidden attractor chaos [14], nonlinear optical image encryption making use of canonical transform [15], optical image encryption taking advantage of public key cryptography [16], optical image encryption with the support of chaos, phase masks and ptychography [17].

In the meantime, plaintext related cryptosystem is more and more applied to image encryption. Some representative achievements include: image cryptosystem based on chaos and S-box [18], image encryption using cosine transform [19], color image encryption combining chaos and plaintext related technology [20], plaintext related image encryption on the basis of chaos drove by sine transformation [21], image encryption utilizing hyper chaos and plaintext related cipher [22], image cryptosystem using perceptron-like network [23], gray image encryption combining Lagrange interpolation with nonlinear transformation [24]. Other researches related to the topic of this paper can be found in [25–28]. These works have either carried out interesting numerical calculation research in the field of fractional transformation or applied research in the field of optics and digital image processing. There is no doubt that these publications have provided useful help for our paper and important reference basis for our further work.

While affirming the theoretical significance and practice value of the existing achievements in image

encryption, attentions should be paid to some problems in image encryption. Firstly, some schemes, especially part of optical image encryption ones, completely ignore the argument of the security of cryptosystem. In fact, Mario, Thomas and Stefan et al. have studied the security of some chaotic-based image encryption schemes in 2018 [29]. They concluded that passing the statistical tests of various secure performance indicators is only a necessary but not a sufficient condition for the security of cryptosystem. After a large number of experiments, they found that the encryption algorithm based on unsecure ciphers can also pass the statistical testing. So, they suggested that the security of the cryptosystem should be demonstrated before it is applied to encrypting the image. For chaos-based cryptosystem, the security demonstration can be carried out either by the analysis of chaotic dynamic system or by the international standard evaluation of pseudo-random sequence. Secondly, the computing speed and storage capacity of modern computer systems are amazing, so those algorithms which have been proved to be secure under traditional conditions are no longer secure in modern computing environment due to their small key space. It is necessary to study the encryption algorithm with super large key space. This will inevitably involve the design and construction of multi parameter chaotic cryptosystem. Thirdly, the structures of some algorithms are not complex enough to guarantee the security of the encryption system confronting multiple malicious attacks.

On the whole, image encryption is divided into two relatively independent and parallel branches, namely optical image encryption and digital image encryption. Optical image encryption mostly uses the frequency domain encryption methods of wavelet transform, Fourier transform and other basic tools, while digital image encryption generally uses the pixel scrambling and pixel diffusion methods based on chaotic transformation. Of course, there are also a few digital image encryption schemes that combine cosine transform and chaotic transform. However, the combination of optical image encryption and digital image encryption tools has been a research gap in image comprehensive encryption. In fact, the cross-fusion application of the two branches is more conducive to carrying forward their respective advantages and avoiding each other's shortcomings. In order to effectively promote the integration of optical

image encryption methods and digital image encryption tools, this paper proposes an important idea of integrating time-domain encryption and frequency-domain encryption into optical image encryption. The main expression of this idea is combining chaos digital image encryption technologies with 4f optical encryption system to form a compound encryption mode. In addition, in the encryption algorithm, we propose a new mode, that is, the real part and the virtual part of the frequency domain image generated by the optical image system are encrypted by discrete chaotic encryption using pixel scrambling and diffusion. This mode multiplies the key space of the encryption scheme and improves the security of image transmission to twice the original. This greatly improves the overall security of the encryption algorithm.

In this paper, an optical image hybrid encryption scheme is proposed using 4f optical system with pixels diffusion and confusion. The mechanism of the algorithm is to implement the pixels operations of digital image based on the result of optical mask encoding. The encryption process includes two parts. In the first part, the original image is encoded in 4f double RPM based on FRFT with multiple parameters. In the second stage, the optical encrypting image is decomposed into real part and imaginary part images. And then, both the pixels diffusion and confusion, as well as pixels nonlinear transform are performed on the two parts to realize digital image encryption on the basis of the novel chaotic cryptosystem.

Our main contributions are summarized as follows. Firstly, the high-dimensional chaos digital image encryption techniques are integrated into 4f optical image encryption system to construct a novel optical image hybrid encoding scheme. Secondly, the real and imaginary images in frequency domain are separately encrypted. This encryption paradigm greatly improves the overall security of the algorithm. Thirdly, a generalized chaos is formed to support the cryptosystem and a new pixel's diffusion mode is suggested. Fourthly, plaintext related technology and nonlinear transform of matrices are fully utilized in cipher generation and image encryption. Fifthly, the proposed algorithm has super large-scale key space. Therefore, it has relatively high security in resisting brute force attack.

The paper mainly includes the following contents: Part 2 summarizes the mathematical foundation of

the algorithm. Section 3 detailed expounds the image encryption algorithm. Section 4 implements the simulations. Section 5 tests the cryptosystem security. Section 6 exhibits the algorithm performance analysis. Section 7 gives the conclusions.

## 2 Mathematics Preliminaries

### 2.1 Fractional Fourier Transformation

FRFT is the rotation of coordinate axis in a time–frequency plane. The FRFT of order  $p$  is usually expressed as follows [30]:

$$F^p s(u) \equiv \int_{-\infty}^{\infty} K_p(t, u) s(t) dt, \quad (1)$$

$$K_p(t, u) = \begin{cases} \sqrt{\frac{1-j\cot\alpha}{2\pi}} \exp\left(j\frac{t^2+u^2}{2}\cot\alpha - j\frac{tu}{\sin\alpha}\right) & \alpha \neq n\pi \\ \delta(t-u) & \alpha = 2n\pi \\ \delta(t+u) & \alpha = (2n+1)\pi \end{cases}, \quad (2)$$

where,  $\alpha \equiv p\pi/2$ ,  $F^p$  is  $p$ -order FRFT,  $K_p$  is the kernel. In fact, FRFT is an extension of FT. It is obvious that FRFT has periodicity, i.e.  $F^{p+4n}s(u) = F^p s(u)$ ,  $n \in \mathbb{N}$ .

### 2.2 Chaos with Multiple Free Degrees

We know that Henon map is a commonly-used chaos to generate pseudo random sequence [1, 2]. One form of this chaos is denoted as follows:

$$\begin{cases} x(n+1) = 1 - a \cdot x^2(n) + y(n) \\ y(n+1) = b \cdot x(n) \end{cases},$$

where,  $a, b$  are the free parameters. Since the key space of Henon map is too small, the security of the ciphers generated by this chaos is limited. So we extend it to a novel form with multiple control parameters and additional items as follows:

$$\begin{cases} x(n+1) = 1 - t_1 \cdot x^2(n) + t_2 \cdot \cos(x(n)) \cdot y(n) + t_3 \cdot \sin(x(n)) \\ + t_4 \cdot \sin(y(n)) y(n+1) = t_5 \cdot x(n) \end{cases}. \quad (3)$$

where,  $t_1, t_2, t_3, t_4, t_5$  are the systematic parameters. In the following sections, we call this map as Cosine-sine Henon Map (CHM). When  $0.55 < t_1 < 2$ ,  $0 < t_2, t_3, t_4, t_5 < 1$ ,

CHM has one positive Lyapunov exponents, so it satisfies the sufficient condition of chaos. Since the nonlinear item and more free degrees are introduced in Eq. (3), the key space and structure complexity of this system is increasingly improved.

### 2.3 Nonlinear Transformations of Matrices

In matrix analysis, dot operation is oriented to the elements of a given matrix other than to the matrix. Suppose that  $I = (I_{ij})_{h \times k}$  represent the matrix of  $h$  rows and  $k$  columns. The dot power [31] of  $I$  is expressed as follows:

$$I.^{\wedge n} = ((I_{ij})^n)_{h \times k},$$

where,  $'.^{\wedge}$  stands for dot power operator. Based on this formula, we define the Nonlinear Transform about the Matrix (NTFM) $I_f$  as follows:

$$I_f = f(I) = \alpha \cdot I.^{\wedge} \beta + \gamma \cdot J.^{\wedge} \lambda + \mu \cdot \xi(R), \quad (4)$$

where,  $\alpha, \beta, \gamma, \lambda, \mu \in R^+$  are optional parameters,  $J$  is another matrix of the same size as  $I$ ,  $R$  is a nonzero random matrix, and  $\xi(\cdot)$  is a nonlinear function such as logarithmic, exponent, and trigonometric operators, etc. Obviously, it is not hard to deduce the Inverse of NTFM( $\text{NTFM}^{-1}$ ) as follows:

$$I = f^{-1}(I_f) = ((I_f - \gamma \cdot J.^{\wedge} \lambda + \mu \cdot \xi(R)) / \alpha).^{\wedge} (1/\beta). \quad (5)$$

## 3 Image Hybrid Encryption and Decryption

### 3.1 Image double RPM encoding based on FRFT

Using the inner function 'rand' of Matlab, we obtain two random matrices  $C_{S1}, C_{S2}$  with the size of  $h \times k$  as the image to be encrypted. Furthermore, we deduce the two random phase functions as follows:

$$C_{T1} = e^{2\pi i \cdot C_{S1}}, C_{T2} = e^{2\pi i \cdot C_{S2}}, \quad (6)$$

For the given plain image  $P_0$  and the specified parameter  $p$ , we perform the transform as follows:

$$\tilde{C}_{TP} = \text{FRFT}^p(P_0 * C_{T1}) * C_{T2}, \quad (7)$$

where,  $\text{FRFT}^p$  denotes the fractional Fourier transform of the order  $p$ . The matrix  $\tilde{C}_{TP}$  is referred to as

the masked image of  $P_0$ . Furthermore, we perform the following transform  $\bar{C}_{TP}$ :

$$\bar{C}_{TP} = a_0 \cdot \tilde{C}_{TP} + b_0 \cdot R_0.^c, \quad (8)$$

where,  $a_0, b_0, c_0 \in R^+$  are varied parameters,  $R_0$  is a nonzero random matrix.

In order to carry out digital image encryption successfully, we decompose the transformed result  $\bar{C}_{TP}$  into two real matrices as follows:

$$\bar{C}_{TPR} = \text{real}(\bar{C}_{TP}), \bar{C}_{TPI} = \text{imag}(\bar{C}_{TP}) \quad (9)$$

We can also implement another transform on the results of Eq. (9) as follows:

$$C_{TPR} = \bar{C}_{TPR} - \text{floor}(\bar{C}_{TPR}), \quad (10)$$

$$C_{TPI} = \bar{C}_{TPI} - \text{floor}(\bar{C}_{TPI}), \quad (11)$$

where,  $\text{floor}(\cdot)$  represents the operator of rounding downward. The matrices  $C_{TPR}$  and  $C_{TPI}$  are regarded as the encryption results of the first stage.

In this subsection, the key space is  $\Gamma_1 = \{a_0, b_0, c_0, p, C_{S1}, C_{S2}, R_0\}$ .

### 3.2 Pixels Diffusion

In this subsection and the subSect. 3.3, we take  $C_{TPR}$  as an example to elaborate the image encryption algorithm. The same algorithm should be performed on  $C_{TPI}$  in parallel.

Suppose that  $P = C_{TPR}$ . For the given parameters  $t_{11}, t_{21}, t_{31}, t_{41}, t_{51}$ , apply Eq. (3) to generate the chaotic sequence  $C_{S3}$  in the length of  $n = h \cdot k$  and convert it into the matrix  $\bar{C}_{S3}$  of the same size as  $P$ . For the known parameters  $a_1, b_1, c_1, d_1, e_1$ , the matrices  $P, \bar{C}_{S3}$ , and the random matrix  $R_1$ , we implementing the NTFM in Eq. (4) and obtain the matrix  $C_d$  as follows:

$$C_d = a_1 \cdot P.^{\wedge} b_1 + c_1 \cdot \bar{C}_{S3}.^{\wedge} d_1 + e_1 \cdot \xi_1(R_1) \quad (12)$$

where,  $\xi_1(\cdot) = \cos(\cdot)$  is called operator key. The matrix  $C_d$  is referred to as the Diffusion Cipher Related to the Plaintext (DCRP).

It is well known that the traditional pixel diffusion is performed based on XOR operation or addition and modular operation. To improve the computing efficiency, we introduce a new diffusion mode combining

cumulative sum with modulus arithmetic. The forward and backward diffusing calculations and their inverse of this mode are, respectively, expressed as follows:

$$\begin{aligned} D_i &= \left( \sum_{j=0}^{i-1} D_{i-1} + S_i + P_i \right) \bmod 256, D_i \\ &= \left( \sum_{j=1}^{i+1} D_{i+1} + S_i + P_i \right) \bmod 256 \end{aligned} \quad (13)$$

$$\begin{aligned} P_i &= \left( n \times 256 + D_i - \sum_{j=0}^{i-1} D_{i-1} - S_i \right) \bmod 256, \\ P_i &= \left( n \times 256 + D_i - \sum_{j=1}^{i+1} D_{i+1} - S_i \right) \bmod 256 \end{aligned} \quad (14)$$

where,  $D$  is the diffused pixels matrix,  $P$  is the image to be diffused, and  $S = C_d$  is the DCRP.

In this subsection, the key space is  $\Gamma_2 = \{t_{11}, t_{21}, t_{31}, t_{41}, t_{51}, a_1, b_1, c_1, d_1, e_1, \xi_1, R_1\}$ .

### 3.3 Pixels Confusion

For the selected parameters  $t_{12}, t_{22}, t_{32}, t_{42}, t_{52}$ , we use the chaos in Eq. (3) to generate the chaotic matrix  $C_{S4}$ . After setting the values of  $a_2, b_2, c_2, d_2, e_2$ , we carry out the transform in Eq. (4) on the diffused image  $D$ , the matrix  $C_{S4}$ , and another random matrix  $R_2$  and derive the matrix  $M$  as follows:

$$M = a_2 \cdot D \wedge b_2 + c_2 \cdot C_{S4} \wedge d_2 + e_2 \cdot \xi_2(R), \quad (15)$$

where,  $\xi_2(\cdot) = \sin(\cdot)$  is another operator key. Then, we sort  $M$  into  $M_S$  in ascending order. According to the sequence  $N_{new}$ , that is the number of the elements after sorting, we rearrange  $D$  into  $D_f$ . The matrix  $D_f$  is the confused image.

### 3.4 Decryption

Firstly, according to the sequence  $N_{old}$ , that is the number of the elements after sorting, we rearrange the encrypted image  $D_f$  into the matrix  $D$ . Secondly, we make use of Eq. (14) to compute the matrix  $P$  and recover the images  $C_{TPR}, C_{TPI}$ . Thirdly, we use the inverses of Eqs. (11), (10), (9) and (8) to derive  $\tilde{C}_{TP}$ . And finally, we implement the inverse of  $\text{FRFT}^p$  as follows:

$$IC_{TP} = \text{FRFT}_p^{-1} \left( \tilde{C}_{TP} * \text{conj}(C_{T2}) \right), \quad (16)$$

where,  $\text{FRFT}_p^{-1}$  is the inverse of  $\text{FRFT}^p$ ,  $\text{conj}(\cdot)$  represent the conjugate operator, and  $IC_{TP}$  denotes the final decrypted image. So far, the image decryption is completed.

### 3.5 Algorithm Description

#### (1) Preprocessing

- <sub>1</sub> Suppose that the original gray image is  $P_0$ ;

#### (2) Double random phases mask encryption

- <sub>2</sub> Use Matlab function to generate the matrices  $C_{S1}, C_{S2}$ ;
- <sub>3</sub> Use Eq. (6) to work out the double phase masking functions  $C_{T1}, C_{T2}$ ;
- <sub>4</sub> Set the parameters  $p, a_0, b_0, c_0, R_0$ , and carry out the transforms in Eqs. (7), (8), (9), (10) and (11), successively, to derive the images  $C_{TPR}, C_{TPI}$ ;

#### (3) Diffusion encryption

- <sub>5</sub> Select the keys  $t_{11}, t_{21}, t_{31}, t_{41}, t_{51}$ , and employ Eq. (3) to calculate the chaotic matrix  $\bar{C}_{S3}$ ;
- <sub>6</sub> Use Eq. (12) to deduce the cipher  $C_d$  based on the known parameters  $a_1, b_1, c_1, d_1, e_1, R_1$ ;
- <sub>7</sub> Make use of Eq. (13) to conduct the pixels diffusion;

#### (4) Confusion Encryption

- <sub>8</sub> Compute the chaotic matrix  $C_{S4}$ , carry out the transform in Eq. (15), and rearrange the transform result into the matrix  $D_f$ ;

#### (5) Decryption

- <sub>9</sub> Convert the encrypted image  $D_f$  into the matrix  $D$ , use Eqs. (14), (11), (10), (9) and (8) successively,

to derive the matrix  $\tilde{C}_{TP}$ , and then perform  $\text{FRFT}_p^{-1}$  in Eq. (16) to obtain the decrypted image  $IC_{TP}$ .

### 3.6 The Algorithm Flow Chart

The image encryption and decryption process is displayed in Fig. 1. The encryption process consists of optical image encryption and digital image encryption in sequence. The part of optical image encryption includes the following steps: firstly, use Matlab inner function to generate two random matrices  $R_{01} = C_{S1}, R_{02} = C_{S2}$ ; secondly, use Eq. (6) to obtain the double phase masking functions  $C_{T1}, C_{T2}$ ; thirdly, use  $C_{T1}, C_{T2}$  to implement Fractional Fourier Transform on plaintext, as mentioned in Eqs. (7), (8), (9), (10) and (11), successively, to deduce the optical image encryption results. The results include real part encrypted image and imaginary part

encrypted image which denoted by  $C_{TPR}, C_{TPI}$ , respectively. The part of digital image encryption is carried out on the basis of optical image encryption results. This part includes two stages, i.e., pixels diffusion and pixels confusion. In the first stage, Eq. (3) is firstly used to calculate the chaotic matrix CHM\_01; then, NTFM\_01 in Eq. (12) is applied to deduce the cipher  $C_d$ ; finally, Eq. (13) is implemented to conduct the pixels diffusion. In the second stage, Eq. (3) is firstly used again to compute the chaotic matrix CHM\_02; then, the transform in Eq. (15) is conducted to obtain a new matrix; finally, the transform result is rearranged into another matrix, it is the confused image, i.e., the final encrypted image. Decryption is the reverse process of encryption. Firstly, the encrypted image  $D_f$  is converted into the matrix  $D$ ; then, Eqs. (14), (11), (10), (9) and (8) is used, successively, to derive the matrix  $\tilde{C}_{TP}$ ; Finally,  $\text{FRFT}_p^{-1}$  in Eq. (16) is performed to obtain the decrypted image  $IC_{TP}$ .

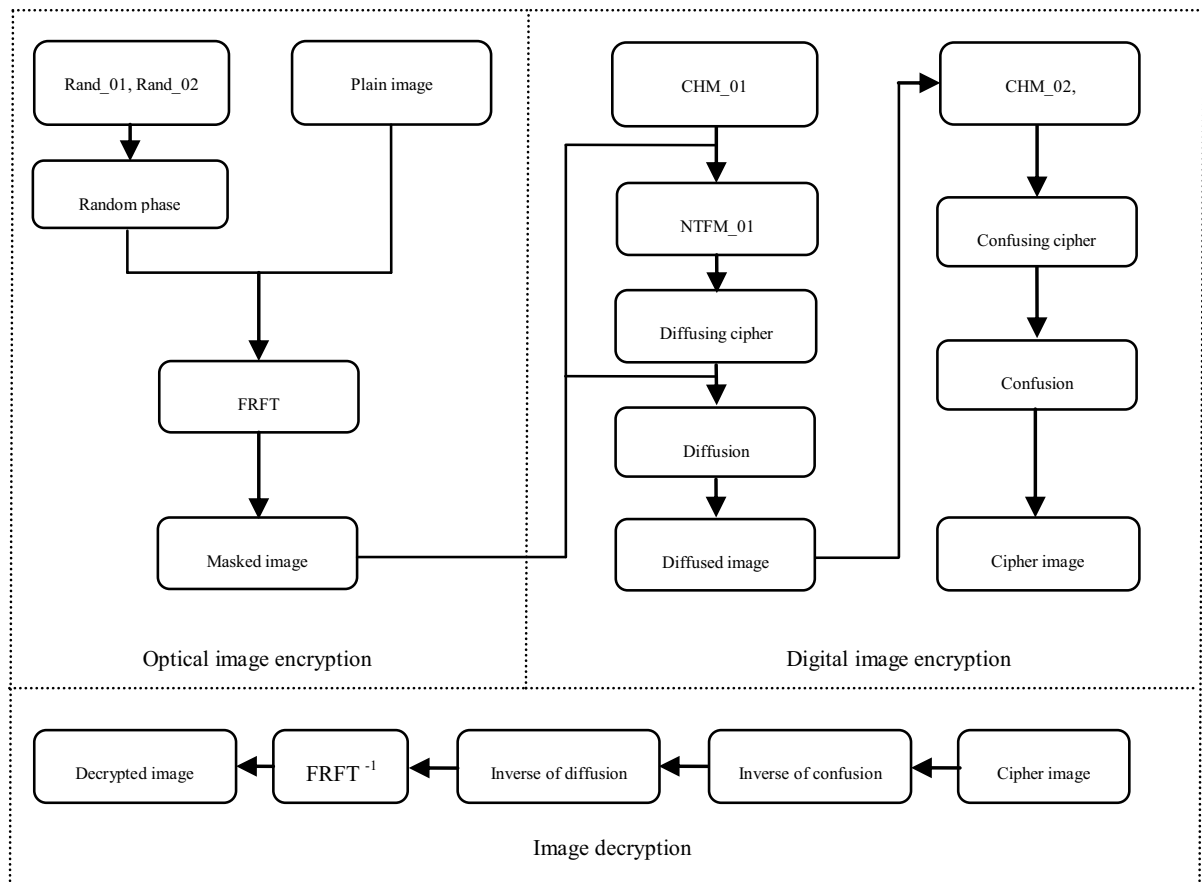


**Fig. 1** The encryption and decryption flow chart

## 4 Encryption and Decryption Simulations

We randomly pick up three sample images, i.e., Mushroom ( $256 \times 384$ ), Dragonfly ( $481 \times 321$ ), and Jaguar ( $512 \times 348$ ), from the universal datasets BSD-S500 (Berkeley Segmentation Dataset and Benchmark 500) [32] and Caltech (the California Institute of Technology) 101 [33]. The simulations are conducted on the platform of Matlab 2019a. The system configuration is Intel Core i7 2.4 GHz CPU, 8.0 GB RAM, and Win10.

In this section, the data and conclusions are obtained from the encrypted image  $C_{TPR}$ , the similar data and conclusions are also applicable to  $C_{TPI}$ .

The key space is  $\Gamma_1 \times \Gamma_2 \times \Gamma_3$ . Besides  $R_0, R_1, R_2$  are random matrices and  $\xi_1(\cdot) = \cos(\cdot), \xi_2(\cdot) = \sin(\cdot)$ , the other keys are assigned as in Table 1. The experimental results are shown in Fig. 2.

Figure 2 shows the plain images (a), the encrypted real (b) and imaginary (c) images and the decrypted images (d). It is obvious that the ciphertext is disorder. From the cipher image, little useful information can be obtained. So, from the visual intuition, the proposed algorithm is valuable.

Table 2 shows the similarity index of two images. PSNR (Peak Signal to Noise Ratio) is an objective standard for evaluating image similarity, the higher its value, the stronger the similarity between the two images. SSIM (Structural Similarity) is another index to measure the similarity of two images. Its value range is  $[0, 1]$ . The bigger the value is, the higher the similarity is. The data in Table 2 reveals that the practical effect of the algorithm is quite ideal. In addition, the data indicate that the algorithm can be realized without losing any information of the original image.

## 5 The Security Test of the Cryptosystem

We know that the base of the proposed algorithm cryptosystem is CHM in Eq. (3). To meet the demand of applied cryptography, the cipher stream generated by CHM should be proved to be secure. For the parameters

$t_{11} = 1.20, t_{21} = 0.50, t_{31} = 0.78, t_{41} = 0.30, t_{51} = 0.40$  used in Sect. 4, we calculate the 15 indicators of SP800-22 Revision 1a [34] and list them in Table 3.

Table 3 is composed of four columns: the first one is the security index, the second one is the reasonable range of the security index, the third one is the test value of the security index of the cryptographic system in this paper, and the fourth one is the test result of the security index.

Table 3 shows that, the chaotic sequence can smoothly pass the tests of SP80022. In fact, as long as the parameters are within the reasonable range, the similar results can be obtained from other parameters sets. Thus, we conclude that cryptosystem used in this paper is secure and applicable.

## 6 Performance Analysis of the Algorithm and the Comparison with Other Encryption Schemes

As previously mentioned, the innovation of this paper includes two aspects: i) the high-dimensional chaotic digital image encryption method is integrated into 4f optical image encryption system, and a new idea of optical image encryption is proposed; ii) a separate encryption paradigm of real and imaginary images in frequency domain is proposed, which greatly improves the security of image encryption and transmission. And also, the encryption simulation in Sect. 4 has proved the feasibility of encryption scheme. To verify the security and superiority of the proposed algorithm, we analyze the common security indicators of image encryption in this section. These indicators include: Key space and Keys sensitivity, Information entropy, Gray surface, Pixels correlation, Plaintext sensitivity. Besides, we also compare our algorithm with the existing algorithms of the same kind.

### 6.1 Key Space and Keys Sensitivity

Applied cryptography has concluded that, for 8-bit integer images, only when the key space is no less than 128bit, the algorithm is considered to be secure. As we

**Table 1** The original keys

| Key   | $a_0$ | $b_0$ | $c_0$    | $p$      | $t_{11}$ | $t_{21}$ | $t_{31}$ | $t_{41}$ | $t_{51}$ | $a_1$ | $b_1$ | $c_1$ |
|-------|-------|-------|----------|----------|----------|----------|----------|----------|----------|-------|-------|-------|
| Value | 2.00  | 4.00  | 2.00     | 2.50     | 1.20     | 0.50     | 0.78     | 0.30     | 0.40     | 6.00  | 4.00  | 3.00  |
| Key   | $d_1$ | $e_1$ | $T_{12}$ | $t_{22}$ | $t_{32}$ | $t_{42}$ | $t_{52}$ | $a_2$    | $b_2$    | $c_2$ | $d_2$ | $e_2$ |
| Value | 2.00  | 5.00  | 1.25     | 0.48     | 0.72     | 0.32     | 0.45     | 2.00     | 3.00     | 2.00  | 4.00  | 5.00  |

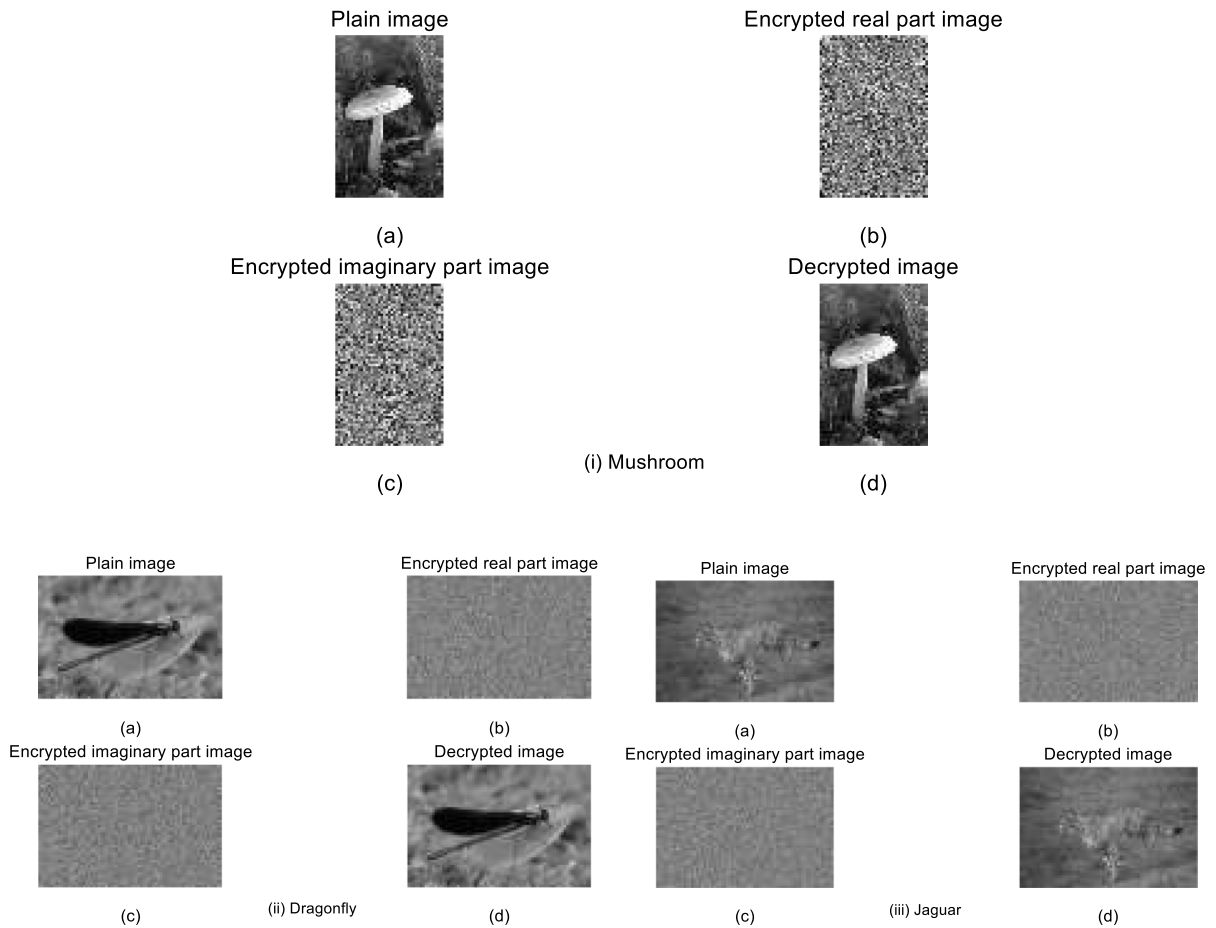


**Fig. 2** The encryption and decryption results of experimental images

**Table 2** PSNR and SSIM of two images

| Index                                                | Mushroom | Dragonfly | Jaguar   | Expected value |
|------------------------------------------------------|----------|-----------|----------|----------------|
| Size                                                 | 256×384  | 481×321   | 512×348  | —              |
| $P_1$ —the PSNR of the ciphertext and plaintext      | 7.7421   | 7.7634    | 7.7644   | —              |
| $S_1$ —the SSIM of the ciphertext and plaintext      | 0.0044   | 0.0072    | 0.0030   | 0.0000         |
| $P_2$ —the PSNR of the decrypted image and plaintext | $\infty$ | $\infty$  | $\infty$ | —              |
| $S_2$ —the SSIM of the decrypted image and plaintext | 1.0000   | 1.0000    | 1.0000   | 1.0000         |

known, the key space totally includes 29 keys. Even though those parameters in special form, including  $R_0, R_1, R_2$  and  $\xi_1(\cdot), \xi_2(\cdot)$ , are not taken into account, there are 24 common numerical keys to brace the key space. Thus, the theoretical size of the key space is  $\log_2(10^{336}) \approx 1162$  bit. Even though all the keys are valued on the conservative interval  $[10^{-4}, 10^4]$ , the key space is not less than  $\log_2(10^{192}) \approx 638$  bit.

Without loss of generality, we select three keys  $a_0, t_{21}, c_1$ , respectively, from the key space to measure the key sensitivity. Suppose that the group of keys in Table 1 is denoted as  $K_0$ . Keeping the other parameters invariant, we assign an increment of  $10^{-12}$  to the key  $a_0$  in  $K_0$ , and write down the new keys set as  $K_1$ . In the meantime, applying the operation to the keys  $t_{21}, c_1$  in  $K_0$ , we obtain another two sets of keys  $K_2, K_3$ , respectively.

**Table 3** Statistical testing of randomness for the chaotic sequence

| Number | Index                                        | Criterion       | Result         | Conclusions |
|--------|----------------------------------------------|-----------------|----------------|-------------|
| 1      | The frequency test                           | $\geq 0.01$     | 0.8893         | pass        |
| 2      | Frequency test with a block                  | $\geq 0.01$     | 0.5822         | pass        |
| 3      | The runs test                                | $\geq 0.01$     | 0.7328         | pass        |
| 4      | Tests for the longest-run-of-ones in a block | $\geq 0.01$     | 0.1114         | pass        |
| 5      | The binary matrix rank test                  | $\geq 0.01$     | 0.4399         | pass        |
| 6      | The discrete Fourier transform test          | $\geq 0.01$     | 0.5423         | pass        |
| 7      | The non-overlapping template matching test   | $\geq 0.01$     | 0.5985         | pass        |
| 8      | The overlapping template matching test       | $\geq 0.01$     | 0.0302         | pass        |
| 9      | Maurer's 'Universal Statistical' test        | $\geq 0.01$     | 0.1795         | pass        |
| 10     | The linear complexity test                   | $\geq 0.01$     | 0.1333         | pass        |
| 11     | The serial test                              | $\geq 0.01$     | 0.3275, 0.1132 | pass        |
| 12     | The approximate entropy test                 | $\geq 0.01$     | 0.8989         | pass        |
| 13     | The cumulative sums test                     | $\geq 0.01$     | 1.0000         | pass        |
| 14     | The random excursions test                   | all $\geq 0.01$ | D_01           | pass        |
| 15     | The random excursions variant test           | all $\geq 0.01$ | D_02           | pass        |

(Note: D\_01: {0.9105, 0.3086, 0.1484, 0.4654, 0.4937, 0.6669, 0.9518, 0.9763}; D\_02: {0.9805, 0.6589, 0.6222, 0.5243, 0.5688, 0.6123, 0.6208, 0.5615, 0.6875, 0.1152, 0.1413, 0.5290, 0.7805, 0.2834, 0.1541, 0.2490, 0.4996, 0.5916})

Using  $K_0, K_1, K_2, K_3$ , we encrypt the image Mushroom respectively. The four cipher images are displayed in Fig. 3. In order to find the difference among the four ciphertexts, we compute the five metrics between the first cipher image and the later three ones, respectively. Which are recorded in Table 4. Where, CORR is the Correlation Coefficient of two images. The closer its value is to zero, the smaller the correlation between the two images. NPCR (the Number of Pixels Change Rate) represents the ratio of different ciphertext images with different gray values at the same position. UACI (the Unified Average Changing Intensity) represents the average change density between different ciphertext images. BACI (Block Average Changing Intensity) reflects the average change intensity of image block pixels. These three indicators are used to represent the images' ability to resist differential attacks. The data in Table 4 indicates that the proposed algorithm is quite sensitive to the keys.

## 6.2 Statistic Security

### 6.2.1 Information Entropy

Information entropy is an important indicator to reflect the chaos or disorder of an independent information system. The maximum value of information entropy of an 8-bit integer image is 8.0000. The cipher images entropies are now listed in Table 5. Table 5 shows that the data of ciphertexts are not only larger than that of plaintexts, but also very close to the optimal value.

### 6.2.2 Gray Surface

In general, a secure and robust encryption scheme can make the cipher pixels gray present uniform distribution. The common tool to reflect this feature is the gray histogram. Another tool to reveal this characteristic is gray surface. Suppose that the abscissas and ordinates of all pixels form a grid in the  $xoy$  plane. For each vertex of the grid, we assign the pixel gray as the third coordinate and obtain the gray surface  $z = g(x, y)$ . In general, the

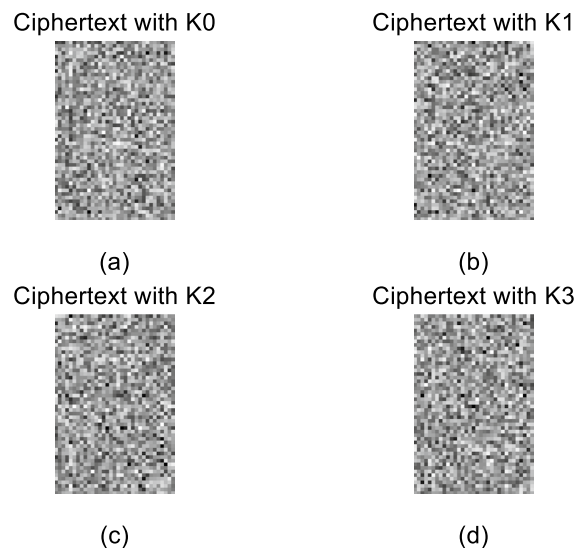


**Fig. 3** Ciphers corresponding to the four groups of keys with slight difference

smoother the grayscale surface, the more uniform the pixel grayscale distribution. Figure 4 exhibits the gray surfaces of the first two experimental images.

Figure 4 indicates that all the gray surfaces of plain images are obviously fluctuating, whereas those of the cipher images have equal height almost everywhere. This means that little useful information of the plaintext's images can be obtained through ciphertexts gray statistical analysis.

### 6.2.3 Pixels Correlation

For a plain image with specific meaning, there usually is a certain correlation among the pixels. After a secure and robust encryption, this correlation should be completely eliminated.

For the original image Mushroom, we randomly pick up 4000 pixels in three different directions, respectively.

Table 6 records the pixels correlation coefficients before and after encryption. Figure 5 gives their distributions.

Figure 5 reveals that the plain pixels appear an approximate linear distribution in three directions, but the cipher pixels distribution is irregular. This means that the encryption operating successfully destroys the plain pixels correlation. Thus, we conclude that our algorithm is secure against pixels statistical attacks. Table 6 also supports this conclusion.

### 6.3 Plaintext Sensitivity

Suppose that the pixels increment is  $10^{-12}$ . For the three initial images, Table 7 records the five indexes of the two ciphers before and after the plaintext variation. Table 7 states clearly that all the indicators are almost equal to the expected values. This manifests that our encryption scheme has plaintext sensitivity.

**Table 4** The five metrics of two ciphertexts before and after the keys variation

| Metrics | $K_1-K_0$               | $K_2-K_0$                | $K_3-K_0$               | Theoretical value |
|---------|-------------------------|--------------------------|-------------------------|-------------------|
| CORR    | $5.4407 \times 10^{-4}$ | $-8.3595 \times 10^{-4}$ | $2.5124 \times 10^{-4}$ | 0.0000            |
| SSIM    | 0.0072                  | 0.0051                   | 0.0061                  | 0.0000            |
| NPCR    | 99.6073%                | 99.6155%                 | 99.6399%                | 99.6094%          |
| UACI    | 33.4441%                | 33.5181%                 | 33.4607%                | 33.4636%          |
| BACI    | 26.7713%                | 26.7866%                 | 26.7161%                | 26.7712%          |

**Table 5** Entropies of the plaintext and cipher images

| Image                       | Mushroom         | Dragonfly        | Jaguar           | Optimal value |
|-----------------------------|------------------|------------------|------------------|---------------|
| Size (Pixels)               | $256 \times 384$ | $481 \times 321$ | $512 \times 348$ | —             |
| Entropy of the plain imager | 7.3031           | 6.4999           | 6.1668           | 8.0000        |
| Entropy of the cipher image | 7.9981           | 7.9989           | 7.9989           | 8.0000        |

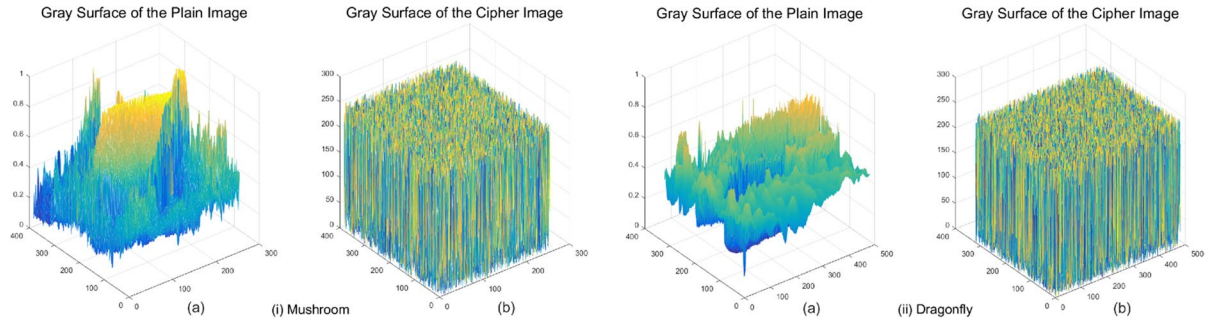


**Fig. 4** Gray surfaces of plain and cipher images

6.4 Comparison with Other Schemes

In this subsection, we compare some metrics of our algorithm with those of Refs. [14, 35, 36] and [37] based on the image Jaguar. The experiment data are shown in Table 8.

Table 8 reveals that, in absolute terms, all the indexes of the five encryption schemes are approximate to the theoretical values. This means that all the five schemes can meet the security requirements of image encryption. From a relative point of view, among the 8 data items involved in the comparison, our scheme has four items ranked first, two item ranked second, and two items ranked third. This demonstrates that the proposed algorithm in this paper has relatively comprehensive comparative advantages over the other four schemes.

The above analysis shows that the optical image encryption paradigm proposed by us, which combines digital image and optical image encryption methods, has good feasibility and security. The proposed encryption scheme has a good application prospect in the field of optical image encryption engineering.

7 Conclusions

In this paper, both optical image encryption method and digital image encryption technology are used

to construct a compound optical image encryption scheme to protect the image information. Fractional Fourier transform, a novel chaos with multiple adjustable parameters, and multiple nonlinear transforms are united to constitute the theoretical basis of the algorithm. Other tools including plaintext related ciphers, dot operation, random matrix, modular arithmetic, sequence rearrangement, rounding arithmetic, etc. are also introduced to support the algorithm. The security of the cryptosystem is test by SP800. The feasibility, effectiveness, security and robustness of the algorithm are evaluated comprehensively. The main novelties of the paper consist in: the high-dimensional chaos digital image encryption techniques are integrated into 4f optical image encryption system to construct a novel optical image hybrid encoding scheme; the real and imaginary images in frequency domain are separately encrypted. This encryption paradigm greatly improves the overall security of the algorithm. It should be recognized that compared with the individual optical image encryption or digital image encryption, the disadvantage of the proposed encryption scheme in this paper is that the running time is slightly increased, but this additional

Table 6 Correlations of the pixels before and after encryption

| Direction  | Horizontal | vertical | diagonal |
|------------|------------|----------|----------|
| Plaintext  | 0.9478     | 0.9481   | 0.9175   |
| Ciphertext | 0.0044     | 0.0015   | 0.0079   |

Table 7 The indicators of the two ciphers before and after the variation of the plaintext

| Index       | Mushroom | Dragonfly | Jaguar   | Theoretical value |
|-------------|----------|-----------|----------|-------------------|
| correlation | -0.0020  | 0.0009    | 0.0011   | 0.0000            |
| SSIM        | 0.0032   | 0.0069    | 0.0071   | 0.0000            |
| NPCR        | 99.5921% | 99.6004%  | 99.5982% | 99.6094%          |
| UACI        | 33.4697% | 33.4620%  | 33.4604% | 33.4636%          |
| BACI        | 26.7779% | 26.7816%  | 26.7707% | 26.7712%          |

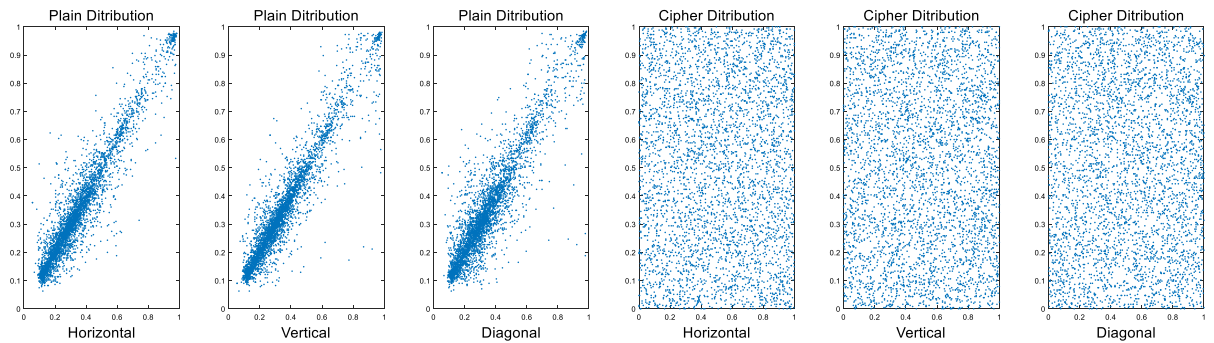


Fig. 5 Distributions of the plaintext and ciphertext pixels

**Table 8** Performance data of different encryption schemes

|                          |            | Ref. [14] | Ref. [35] | Ref. [36] | Ref. [37] | Ref. [38] | Our algorithm | Theoretical value |
|--------------------------|------------|-----------|-----------|-----------|-----------|-----------|---------------|-------------------|
| Key space                |            | 128bit    | 259 bit   | 449bit    | 199bit    | 512bit    | 1162 bit      | $\geq 128$ bit    |
| Information entropy      | —          | 7.9976    | 7.9988    | 7.9913    | 7.9973    | 7.9965    | 7.9988        | 8.0000            |
| CORR of ciphertext image | Horizontal | 0.0068    | 0.0127    | 0.0136    | 0.0072    | 0.0068    | 0.0060        | 0.0000            |
|                          | Vertical   | 0.00112   | 0.0081    | 0.0023    | 0.0026    | 0.0080    | 0.0078        | 0.0000            |
|                          | Diagonal   | 0.0056    | 0.0119    | 0.0128    | -0.0045   | -0.0072   | 0.0069        | 0.0000            |
| Differential analysis    | NPCR       | 99.6321%  | 99.5983%  | 99.5722   | 99.6348%  | 99.5990%  | 99.5982%      | 99.6094%          |
|                          | UACI       | 33.6742%  | 33.4543%  | 33.4463   | 33.5633%  | 33.4722%  | 33.4604%      | 33.4636%          |
|                          | BACI       | —         | 26.7636%  | 26.7633%  | —         |           | 26.7707%      | 26.7712%          |

consumption of time is insignificant for modern computer systems. Moreover, compared with the significant improvement of security, this small cost in time is completely worthy. Compared with other known encryption methods, the proposed algorithm demonstrates overall advantages including: Creative idea of image encryption, novelty of password generation tool, and high security of encryption scheme. It is expected to be candidate tool in the field of image information hiding such as: military map protection, commercial image security and private image encryption.

**Abbreviations** *RPM*: Random Phase Mask; *FT*: Fourier Transformation; *FRFT*: Fractional Fourier transformation; *CHM*: Cosine-sine Henon Map; *NTFM*: The Nonlinear Transform about the Matrix; *NTFM<sup>-1</sup>*: The Inverse of NTFM; *DCRP*: Diffusion cipher related to the plaintext; *PSNR*: Peak Signal to Noise Ratio; *SSIM*: Structural Similarity; *CORR*: The Correlation Coefficient; *NPCR*: The Number of Pixels Change Rate; *UACI*: The Unified Average Changing Intensity; *BACI*: Block Average Changing Intensity

**Acknowledgements** This work was supported by National Natural Science Foundation of China [No. 61702153]. We express our sincere gratitude to those who have provided helps for our work.

**Authors' contributions** Limin Tao: Conceived overall structure of the paper and performed the experiment.

Xikun Liang: Performed design and analysis of algorithms and wrote the paper.

Zhijing Wu: Performed the data analyses.

Lidong Han: Collected the data.

Jiangping Zhu: Helped perform the analysis with constructive discussions.

**Funding** National Natural Science Foundation of China [No. 61702153].

**Data Availability** The datasets used and analyzed during the current study are available from the corresponding author on reasonable request.

## Declarations

**Ethics Approval and Consent to Participate** Not applicable.

**Consent for Publication** Not applicable.

**Competing Interest** The authors declare that there is no conflict of interests regarding the publication of this paper.

## References

1. Zhang, Y.: Chaotic Digital Image Cryptosystem. Tsinghua University Press, Beijing (2016)
2. Guo, F.M., Tu, L.: Application of Chaos Theory in Cryptography. Beijing Institute of Technology Press, Beijing (2015)
3. Refregier, P., Javidi, B.: Optical image encryption based on input plane and Fourier plane random encoding. *Opt. Lett.* **20**(7), 767–769 (1995)
4. Ben Farah, M.A., Guesmi, R., Kachouri, A., et al.: A novel chaos based optical image encryption using fractional Fouriertransform and DNA sequence operation. *Opt. Laser Technol.* **121**, 105777 (2020)
5. Sui, L., Xin, M., Tian, A., Jin, H.: Single-channel color imageencryption using phase retrieve algorithm in fractional fourier domain. *Opt. Lasers Eng.* **51**(12), 1297–1309 (2013)
6. Liu, Z., Li, S., Liu, W., Liu, S.: Opto-digital image encryption by usingbaker mapping and 1-d fractional fourier transform. *Opt. Lasers Eng.* **51**(3), 224–229 (2013)
7. Liu, Z., Li, S., Liu, W., Wang, Y., Liu, S.: Image encryption algorithmby using fractional fourier transform and pixel scrambling operation basedon double random phase encoding. *Opt. Lasers Eng.* **51**(1), 8–14 (2013)
8. Singh, N., Sinha, A.: Optical image encryption using fractional Touriertransform and chaos. *Opt. Lasers Eng.* **46**(2), 117–123 (2008)

9. Singh, N., Sinha, A.: Gyrator transform-based optical image encryption using chaos. *Opt. Lasers Eng.* **47**(5), 539–546 (2009)
10. Li, H., Wang, Y.: Double-image encryption based on discrete fractional random transform and chaotic maps. *Opt. Lasers Eng.* **49**(7), 753–757 (2011)
11. Liu, Z., Gong, M., Dou, Y., et al.: Double image encryption by using Arnold transform and discrete fractional angular transform. *Opt. Lasers Eng.* **50**(2), 248–255 (2012)
12. Chai, X., Chen, Y., Broyde, L.: A novel chaos-based image encryption algorithm using DNA sequence operations. *Opt. Lasers Eng.* **88**, 197–213 (2017)
13. Xue, H., Du, J., Li, S., et al.: Region of interest encryption for color images based on a hyper chaotic system with three positive Lyapunov exponents. *Opt. Laser Technol.* **106**, 506–516 (2018)
14. Wang, S., Wang, C., Xu, C.: An image encryption algorithm based on a hidden attractor chaos system and the Knuth-Durstenfeld algorithm. *Opt. Lasers Eng.* **128**, 105995 (2019)
15. Huang, Z., Cheng, S., Gong, L., et al.: Nonlinear optical multi-image encryption scheme with two-dimensional linear canonical transform. *Opt. Lasers Eng.* **124**, 105821 (2019)
16. Liu, Y., Jiang, Z., Xu, X., et al.: Optical image encryption algorithm based on hyper-chaos and public-key cryptography. *Opt. Laser Technol.* **127**, 106171 (2020)
17. Su, Y., Xu, W., Zhao, J.: Optical image encryption based on chaotic fingerprint phase mask and pattern-illuminated Fourier ptychography. *Opt. Lasers Eng.* **128**, 106020 (2020)
18. Zhang, Y.: The unified image encryption algorithm based on chaos and cubic S-Box. *Inf. Sci.* **450**, 361–377 (2018)
19. Hua, Z., Zhou, Y., Huang, H.: Cosinetransformbased chaotic system for image encryption. *Inf. Sci.* **480**, 403–419 (2019)
20. Chai, X., Fu, X., Gan, Z., et al.: A color image cryptosystem based on dynamic DNA encryption and chaos. *Signal Process.* **155**, 44–62 (2019)
21. Mansouri, A., Wang, X.: A novel one-dimensional sine powered chaotic map and its application in a new image encryption scheme. *Inf. Sci.* **520**, 46–62 (2020)
22. Zhou, W.: A novel image encryption scheme based on conservative hyper chaotic system and closed-loop diffusion between blocks. *Signal Process.* **171**, 107484 (2020)
23. Zhang, Y., Chen, A., Tang, Y., et al.: Plaintext-related image encryption algorithm based on perceptron-like network. *Inf. Sci.* **526**, 180–202 (2020)
24. Liang, X., Tan, X., Tao, L.: Plaintext related image hybrid encryption scheme using algebraic interpolation and generalized chaotic map. *Multimed. Tools Appl.* **79**, 2719–2743 (2020)
25. Abdollahi, Z., Mohseni Moghadam, M., Saeedi, H., Ebadi, M.J.: A computational approach for solving fractional Volterra integral equations based on two-dimensional Haar wavelet method. *Int. J. Comput. Math.* **99**(7), 1488–1504, 0020-716 (2022)
26. Radmanesh, M., Ebadi, M.J.: A local mesh-less collocation method for solving a class of time-dependent fractional integral equations: 2D fractional evolution equation. *Eng. Anal. Bound. Elem.* **113**, 372–381, 0955-7997 (2020)
27. Nazari, K., Ebadi, M.J., Berahmand, K.: Diagnosis of Alternaria disease and leaf miner pest on tomato leaves using image processing techniques. *J. Sci. Food Agric.* **P1**, 0022–5142 (2022)
28. Alimohammadirokni, M., Emadlou, A., Yuan, J.J.: The Strategic Resources of a Gastronomy Creative City: The Case of San Antonio, Texas. *J. Gastron. Tour.* **5**(4), P237-252, 2169–2971 (2021)
29. Preishuber, M., Hütter, T., Katzenbeisser, S.: Depreciating Motivation and Empirical Security Analysis of Chaos-Based Image and Video Encryption. *IEEE Trans. Inf. Forensics Secur.* **13**(9), 2137–2150 (2018)
30. Kamalakannan, R., Roopkumar, R., Zayed, A.: On the extension of the coupled fractional Fourier transform and its properties. *Integral Transforms and Special Functions* **33**(1), 65–80 (2022)
31. Zhao, B., Chen, M., Zou, F.S., et al.: Proficiency in MATLAB-Science computation and the application of data statistics. Posts and Telecommunications Press, Beijing (2018)
32. Contour Detection and Image Segmentation Resources. <https://www2.eecs.berkeley.edu/Research/Projects/CS/vision/grouping/resources.html>, March, 2023.
33. Ranzato, M.A., Li, F.-F., Andreetto, M.: Caltech101 image dataset. <https://academictorrents.com/details/410206b2624ab243b0fa-87058f73927fc44a5b7c>, March, 2023.
34. Rukhin, A., Nechvatal, J., Smid, M. et al.: A statistical test suite for random and pseudorandom number generator for cryptographic applications. <https://xueshu.baidu.com/usercenter/paper/show?paperid=7fd4e905ff21d31c99cd52c1f61f9a26>, March, 2023.
35. Zhen, P., Zhao, G., Min, L., Jin, X.: Chaos-Based Image Encryption Scheme Combining DNA Coding and Entropy. *Multimed. Tools Appl.* **75**(11), 6303–6319 (2016)
36. Jin, X., Yin, S., Liu, N., Li, X., Zhao, G., Ge, S.: Color Image Encryption in Non-RGB Color Spaces. *Multimed. Tools Appl.* **77**(12), 15851–15873 (2018)
37. Zhou, K., Fan, J., Fan, H., et al.: Secure image encryption scheme using double random-phase encoding and compressed sensing. *Opt. Laser Technol.* **121**, 105769 (2020)
38. Zhou, Q., Wang, X., Jin, M., Zhang, L., Xu, B.: Optical image encryption based on two-channel detection and deep. *Opt. Lasers Eng.* **162**, P107415, 0143–8166 (2023)

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

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.