



# Optical image encryption using chaos-based compressed sensing and phase-shifting interference in fractional wavelet domain

Qi Liu<sup>1</sup> · Ying Wang<sup>1</sup> · Jun Wang<sup>1</sup>  · Qiong-Hua Wang<sup>1</sup>

Received: 4 June 2017 / Accepted: 12 November 2017 / Published online: 22 November 2017  
© The Optical Society of Japan 2017

## Abstract

In this paper, a novel optical image encryption system combining compressed sensing with phase-shifting interference in fractional wavelet domain is proposed. To improve the encryption efficiency, the volume data of original image are decreased by compressed sensing. Then the compacted image is encoded through double random phase encoding in asymmetric fractional wavelet domain. In the encryption system, three pseudo-random sequences, generated by three-dimensional chaos map, are used as the measurement matrix of compressed sensing and two random-phase masks in the asymmetric fractional wavelet transform. It not only simplifies the keys to storage and transmission, but also enhances our cryptosystem nonlinearity to resist some common attacks. Further, holograms make our cryptosystem be immune to noises and occlusion attacks, which are obtained by two-step-only quadrature phase-shifting interference. And the compression and encryption can be achieved in the final result simultaneously. Numerical experiments have verified the security and validity of the proposed algorithm.

**Keywords** Compressed sensing · Fractional wavelet transform · Three-dimension chaos · Phase-shifting interference · Hologram

## 1 Introduction

In recent years, the optical image encryption has received more and more attentions. Refrainer and Javidi proposed the double-random-phase encoding (DRPE) method, involving two random phases mask keys in the input and Fourier domains in 1995 [1–3]. The optical implementation of this encryption scheme makes it widely applicable in the image encryption due to parallel processing and high speed. Unfortunately, the DRPE-based technique was found vulnerable to resist several kinds of attacks [4]. Subsequently, a novel multiple images encryption methods in the fractional Fourier transform (FRFT) [5] were introduced, which increases key numbers. However, the key space of fractional order is not big enough. Thus, fractional wavelet transform (FWT) [6, 7] was proposed to replace the FRFT in DRPE, which achieves double encryption in the fractional domain and wavelet domain. The fractional order and scale factors of

FWT can be selected as the additional keys to expand the key space and improve the security of the cryptosystem.

In order to transmit data in the channel effectively, it is far more important to reduce data of cryptosystem. Compressed sensing (CS) [8] is a fast emerging field in information security, which unifies compression and encryption in a simple linear measurement step. Therefore, some CS-based image compression–encryption algorithms (CEA) were proposed to improve the efficiency and security of the cryptosystem [9, 10]. The digital image encryption methods based on CS and DRPE technique were proposed to keep information secret more effectively [11]. To enhance security further, the image encryption scheme combined CS with Arnold transform was proposed [12]. However, in most CS-based CEA, regardless of whether the measurement matrix is a key, this whole matrix needs to be transmitted. In some image encryption combined CS with DRPE [13, 14] or its derivative algorithms such as FRFT [15] and fractional random transform [16], low-dimensional chaos was adopted to reduce their transmission bandwidth. Although one-dimensional (1D) chaotic map was employed to resist some common attacks in CEA [17], 1D chaotic algorithm has its limitations. The cycle of 1D chaotic sequence may degenerate because of the computers' finite precision, and

✉ Jun Wang  
jwang@scu.edu.cn

<sup>1</sup> School of Electronics and Information Engineering, Sichuan University, Chengdu 610065, China

its key space is relatively small, so the cipher-text has been widely analyzed or even been deciphered [18]. Thus, some CS-based cryptosystems using high-dimensional (HD) chaos like Lorenz system, hyper-chaos, and chaotic standard map were proposed [19–21], which can achieve the large parametric space and high security. Although the encryption efficiency and security have been improved in the previous approaches, there are still some space to improve in the robustness and security because of the growing demands for informational security.

In this paper, a robust image CEA based on two-step phase-shifting digital holography and FWT is proposed. Firstly, the cryptosystem has a good flexibility of optical realization and software implementation, which greatly reduces the complexity of achieving the encryption system. Besides, three pseudo-random sequences, which are generated by the 3D chaos, are used to be the measurement matrix of CS and two random-phase masks (RPM) in the FWT. It not only enhances the algorithms nonlinearity, but also enlarges the key numbers and space greatly. Lastly, in order to enhance the robustness of resisting noises and occlusion attacks, digital holograms are obtained by two-step-only quadrature phase-shifting interference (PSI). Numerical experiments have verified the security and validity of the proposed algorithm.

## 2 Fundamental knowledge

Here some basic knowledge related to our proposed scheme is introduced.

### 2.1 Fractional wavelet transform

Mendlovic and Zalevsky [22] defined the fractional wavelet transform (FWT), and the two-dimensional (2D) FWT [23] of 2D signal  $f(x, y)$  can be expressed as

$$W(a, \bar{b}) = \iint \iint U_{p_1}(x, x')U_{p_2}(y, y')H^*(x', y')f(x, y)dx dy dx' dy', \tag{1}$$

where  $p_1$  and  $p_2$  are the fractional orders. The  $f(x, y)$  is the input function. The  $U_{p_1}(x, x')$  and  $U_{p_2}(y, y')$  are the kernel functions, the “\*” means the complex conjugate, and  $H^*(x', y')$  is the wavelet function of mother wavelet function. And FWT in the fractional domains it can be expressed as

$$\begin{aligned} W(a_{mn}, \bar{b}) &= \text{FWT}_{\alpha_{1x}, \alpha_{1y}; \alpha_{2x}, \alpha_{2y}} \{f(x, y)\} \\ &= (a_m a_n)^{1/2} \iint H^*(a_m u, a_n v) \times \exp(j2\pi u b_{x'}, j2\pi v b_{y'}) \\ &\quad \times \text{FrFT}_{\alpha_{1x}, \alpha_{1y}} \{ \text{FrFT}_{\alpha_{2x}, \alpha_{2y}} [f(x, y)](x', y') \}(u, v) du dv, \end{aligned} \tag{2}$$

where  $a_{mn} = (a_m, a_n)$  is the discrete scaling vector,  $b = (b_{x'}, b_{y'})$  is the shift vector, and  $\alpha_{1x}, \alpha_{1y}, \alpha_{2x}, \alpha_{2y}$  is fractional order. It is an asymmetric system with fractional order on the  $x$  and  $y$  directions. The FrFT is expressed as the fractional Fourier transform.

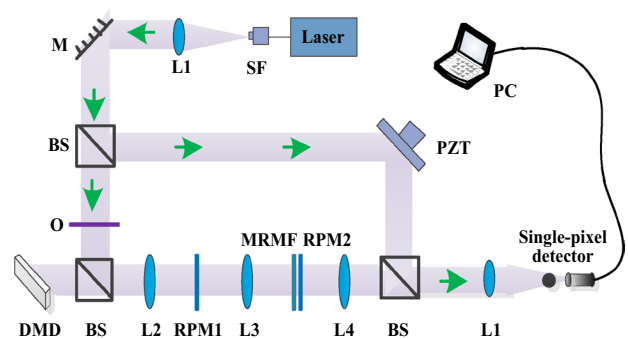
However, its back-reconstructing formula in the fractional wavelet domains is

$$\begin{aligned} f(x, y) &= \text{IFWT}_{(-\alpha_{1x}, -\alpha_{1y}; -\alpha_{2x}, -\alpha_{2y})} \{W(a_{mn}, \bar{b})\} \\ &= \frac{1}{C} \iint \text{FFT} \left\{ \sum_m \sum_n \iint \frac{1}{a_m a_n} W(a, \bar{b}) \right. \\ &\quad \times H(a_m u, a_n v) \exp(-j2\pi \mu b_{x'}, -2j\pi \nu b_{y'}) \\ &\quad \left. \times db_{x'} db_{y'} \right\} \times (x', y') U_{-\alpha_{1x}, -\alpha_{1y}; -\alpha_{2x}, -\alpha_{2y}} \\ &\quad (x, y; x', y') dx' dy', \end{aligned} \tag{3}$$

where IFWT is the inverse fractional wavelet transform,  $\text{FFT}\{\}$  denotes the Fourier transform, and  $C$  is a constant.

## 3 The process of encryption and decryption

Duarte et al. proposed a single-pixel imaging via compressed sampling and achieved optical implementation of CS in recent years [24]. Thus, the proposed encryption system is flexibility, which can be either optical realization or software implementation. The possible optical realization of image encryption scheme is shown in Fig. 1. The multi-reference matched filter (MRMF) is wavelet matched filter, and RPM1 and RPM2 are two random-phase masks (RPM), which are generated by three-dimensional chaotic systems. First of all, the laser is divided into two beams of light by the beam splitter (BS): a beam of light is used as a reference light, and the other is passed through an object as the object wave. The reference wave is controlled to generate different



**Fig. 1** The optical implementation of the proposed encryption method: *L1, L2, L3, L4* lens, *BS* beam splitter, *O* original image, *DMD* digital micro-mirror device, *RPM1, RPM2* random-phase masks, *MRMF* multi-reference matched filter, *PZT* piezo-electric transducer

phase reference waves by a PZT by an optical phase shifter. And the corresponding combined object wave is reflected off by a digital micro-mirror device (DMD) which consists of an array of tiny mirrors. Each mirror in DMD independently oriented either towards the optical path of the encryption by FWT or away from it, and the optical implementation devices of FWT consist of three lenses, a pair of RPM, and a MRMF closing to the RPM2. Thus, after encoded by the encrypted optical path of the fractional wavelet, the reflected light is interfered with the reference light through BS and then collected through the L1 and focused onto a single-pixel detector (SPD). Finally, the random samples can be recorded. And two holograms are obtained and saved in PC. The optical image decryption is the inverse applications of the optical encryption. In this process, the wavelet matched filter, two pieces of RPM, and fractional order can be used as a key, so the key space is enlarged greatly. Thus, the proposed encryption system can make the intruder attacks futile and reduce the bandwidth needed for data transmission.

Our method is based on CS and phase-shifting digital holography in FWT domain. The process of encryption and decryption are symmetrical as shown in Fig. 2. And main operations of encryption processes are introduced as follows.

Firstly, we construct three chaotic matrixes by 3D chaotic systems in PC. As chaotic system has good pseudo-randomness, in the proposed scheme, 3D chaotic system, namely Chen’s chaotic system [25], is employed in key generation, which is described by

$$\begin{aligned} x' &= a_1(y - x), \\ y' &= (c_1 - a_1)x - xz + c_1y, \\ z' &= xy - b_1z, \end{aligned} \tag{4}$$

where  $a_1$ ,  $b_1$ , and  $c_1$  are parameters. When  $a_1 = 35$ ,  $b_1 = 3$ , and  $c_1 \in [20, 28.4]$ , the system is chaotic. Thus, it can make our proposed cryptosystem nonlinear. The initial value  $x_0$ ,  $y_0$ ,  $z_0$  and the controls parameter  $a_1$ ,  $b_1$ ,  $c_1$  are acted as the secret keys.

We take the decimal part of all chaotic time series to limit its elements to the interval  $[0, 1]$  using the following operation:

$$\begin{cases} x'' = \text{abs}(x') - \text{floor}[\text{abs}(x')] \\ y'' = \text{abs}(y') - \text{floor}[\text{abs}(y')] \\ z'' = \text{abs}(z') - \text{floor}[\text{abs}(z')] \end{cases} \tag{5}$$

where the operation  $\text{abs}$  is used to obtain the absolute value,  $\text{floor}$  is used to obtain an integer outcome,  $x''$ ,  $y''$ , and  $z''$  is three random sequences, the sequence  $z''$  is to generate the measurement matrix  $\Phi$  of CS, and others sequences  $x''$  and  $y''$  are generated by two complex RPM in FWT.

Then the original image is compacted by DMD, and it mainly has two steps in the process:

Step 1: An original image  $\alpha$  needs to be transformed to its sparse representation by wavelet basis  $\psi$ , and thus the  $N \times N$  sparse image  $X$  is formed by

$$X = \psi^T \alpha. \tag{6}$$

Step 2: Use the chaotic matrix  $\Phi$  to measure the sparse image; the measurement matrix is  $M \times N$  ( $M \ll N$ ), and the compressed image  $Y$  of  $M \times N$  matrix is calculated by

$$Y = \Phi X. \tag{7}$$

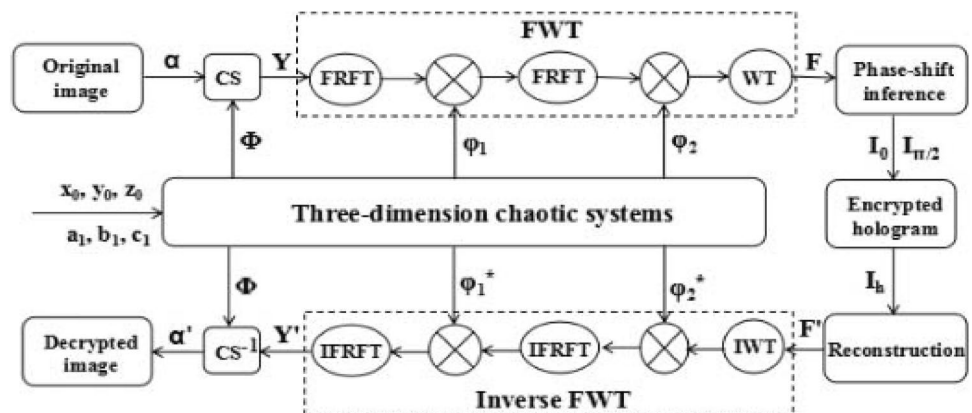
To recover the sparse signal  $X$  from the measurements  $\Phi$  although  $M \ll N$  correctly,  $\Phi$  should satisfy the restricted isometry property (RIP) [26]. Here the definition of RIP in  $k$  order is as follows:

$$(1 - \delta_k) \|X\|_2^2 \leq \|\Phi X\|_2^2 \leq (1 + \delta_k) \|X\|_2^2, \tag{8}$$

where  $\delta_k \in [0, 1]$  is an isometry constant.

Next all reflected (or transmissive) light from DMD is through optical encoding device to achieve the FWT based on DPRE; here  $\varphi_1$  and  $\varphi_2$  are loaded to the RPM, which are generated by chaotic system. In proposed method, the DPRE

Fig. 2 The process of encryption and decryption



in FWT domains can be implemented in Fig. 1, and a multi-reference matched filter (MRMF) is placed in the Fourier plane of the wavelet transform. After a one-level DWT with selected wavelet family, the information is decomposed into four parts.

The complex-amplitude distribution  $F$  after FWT can be represented by

$$\begin{aligned}
 F &= \text{FWT}_{\alpha_{1x}, \alpha_{1y}; \alpha_{2x}, \alpha_{2y}} \{Y\} = \text{MRMF}(u, v) \{ \text{FrTT}_{\alpha_{2x}, \alpha_{2y}} \\
 &\quad [ \text{FrFT}_{\alpha_{1x}, \alpha_{1y}} (Y \exp(i\varphi_1)) \exp(i\varphi_2) dudv ] \\
 &= (a_m a_n)^{1/2} \iint H^*(a_m u, a_n v) \times \exp(j2\pi b_{x'} u, j2\pi v b_{y'}) \\
 &\quad \times \text{FrFT}_{\alpha_{1x}, \alpha_{1y}} \{ \text{FrFT}_{\alpha_{2x}, \alpha_{2y}} [Y] \} (u, v) dudv, \tag{9}
 \end{aligned}$$

where  $H^*(x', y')$  is the wavelet function of mother wavelet function.  $a_{mn} = (a_m, a_n)$  is the discrete scaling vector,  $b = (b_{x'}, b_{y'})$  is the shift vector, and  $a_{1x}, a_{1y}, a_{2x}, a_{2y}$  are fractional

$$\begin{aligned}
 Y &= \text{IFWT}_{(-\alpha_{2x}, -\alpha_{2y}; -\alpha_{1x}, -\alpha_{1y})} \{F'\} = F^{-\alpha_{1x}, -\alpha_{1y}} \left\{ F_{-\alpha_{2x}, -\alpha_{2y}} [ \text{MRMF}(F') \exp(i\varphi_2^*) \exp(i\varphi_1^*) ] \right\} dx dy \\
 &= \frac{1}{C} \iint \text{FFT} \left\{ \sum_m \sum_n \iint \frac{1}{a_m a_n} F'(a, \bar{b}) \times H(a_m u, a_n v) \exp(-j2\pi \mu b_{x'}, -j2\pi v b_{y'}) \times db x' db y' \right\} \\
 &\quad \times (x', y') U_{-\alpha_{1x}, -\alpha_{1y}; -\alpha_{2x}, -\alpha_{2y}}(x, y; x', y') dx' dy', \tag{16}
 \end{aligned}$$

orders; they is an asymmetric system with fractional order on the  $x$  and  $y$  directions. FrFT represents the fractional Fourier transform, and MRMF ( $u, v$ ) can be calculated by

$$\text{MRMF}(u, v) = \sum_m \sum_n \{ H^*[a_{mn}(u - nu_0, v - nv_0)] \}, \tag{10}$$

where the parameters  $a_m, a_n$  are a series of scale factor, and  $H^*$  is a certain mother wavelet function.

Finally, two-step-only quadrature PSI holography is used to record the encoding image in Fig. 1. Two phases are 0 and  $\pi/2$  degree, and were introduced as two reference lights by PZT; the complex amplitudes of two holograms are  $I_0$  and  $I_{\pi/2}$ , respectively, which can be expressed as

$$I_0 = |F + R|^2 = F^2 + |R|^2 + R^* F + R F^*, \tag{11}$$

$$I_{\pi/2} = |F + R \exp(j\pi/2)|^2 = |F|^2 + |R|^2 - jR^* F + jR F^*, \tag{12}$$

where  $F$  and  $R$  denote the amplitude of the object wave and reference wave, respectively.  $|F|^2 + |R|^2$  is the zero-order light wave.

Decryption is the inverse encryption process in Fig. 2.  $I_h$  is generated with no zero-order term and conjugate term by

$$I_h = (I_0 - |R|^2 - |F|^2) + j(I_{\pi/2} - |R|^2 - |F|^2) = 2R^* F. \tag{13}$$

The amplitude of the object wave can be calculated as follows:

$$F' = I_h / 2R^*. \tag{14}$$

Because there is no record of the intensity of object wave,  $|F|^2 + |R|^2$  should be calculated from two orthogonal phase-shift holograms. When the value of  $R$  reaches a certain value  $2R \geq \max(|F|) + \min(|F|)$ , which can be determined according to Eq. (11) and Eq. (12),  $|F|^2 + |R|^2$  can be calculated by

$$\begin{aligned}
 |F|^2 + |R|^2 &= (2R^2 + I_0 + I_{\pi/2}) / 2 \\
 &\quad - \left[ \sqrt{(2R^2 + I_0 + I_{\pi/2})^2 - 2(I_0^2 + I_{\pi/2}^2 + 4R^4)} \right] / 2. \tag{15}
 \end{aligned}$$

The light field of encryption image is obtained in Eq. (14). The inverse FWT algorithm in Eq. (16) is applied in a 4f optical inverse processor, which requires the complex conjugate Fourier phase ( $\varphi_1^*$  and  $\varphi_2^*$ ) to restore the encryption image:

where IFWT is the inverse fractional wavelet transform, FFT{ } denotes the Fourier transform, and C is a constant.

Thus, the measurement image  $\Phi$  is obtained by 3D chaotic systems. To improve the quality of decrypted image, the BP reconstruction algorithm is adopted to recover the wavelet coefficient matrix. The original image can be reconstructed through the inverse wavelet transform. The reconstructed image  $\alpha'$  is denoted as follows:

$$\alpha' = CS^{-1}(Y'). \tag{17}$$

Here,  $CS^{-1}$  is reconstructed process of CS, namely basis pursuit (BP) algorithm [26].

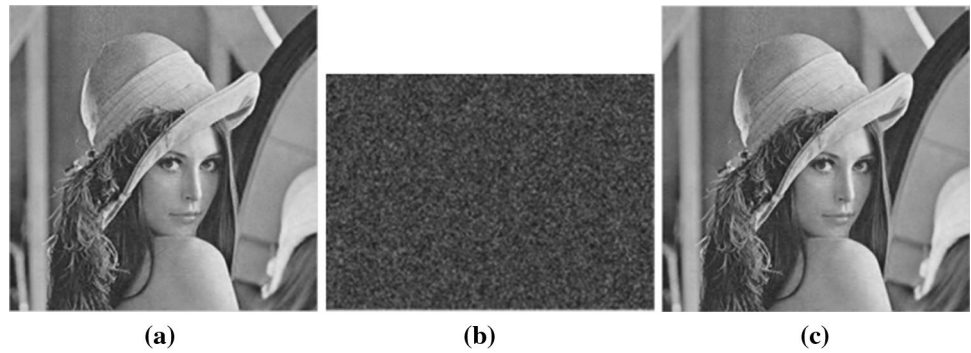
### 4 Simulation experiments and analysis

To check the performance of our proposed scheme, several numerical simulations have been performed. The gray image “Lena” is shown in Fig. 3a. It has  $256 \times 256$  pixels size and acts as the plain image in the experiment. In the proposed encryption system, the important parameters are (1)  $M=192, N=256$ , and a sampling rate of 75%, and the formula is expressed by

$$S_f = \frac{1}{r} = \frac{M \times N}{N \times N}, \tag{18}$$



**Fig. 3** Image encryption and decryption: **a** the original image “Lena”; **b** one of two encrypted holograms ( $I_0$ ); **c** the decrypted image



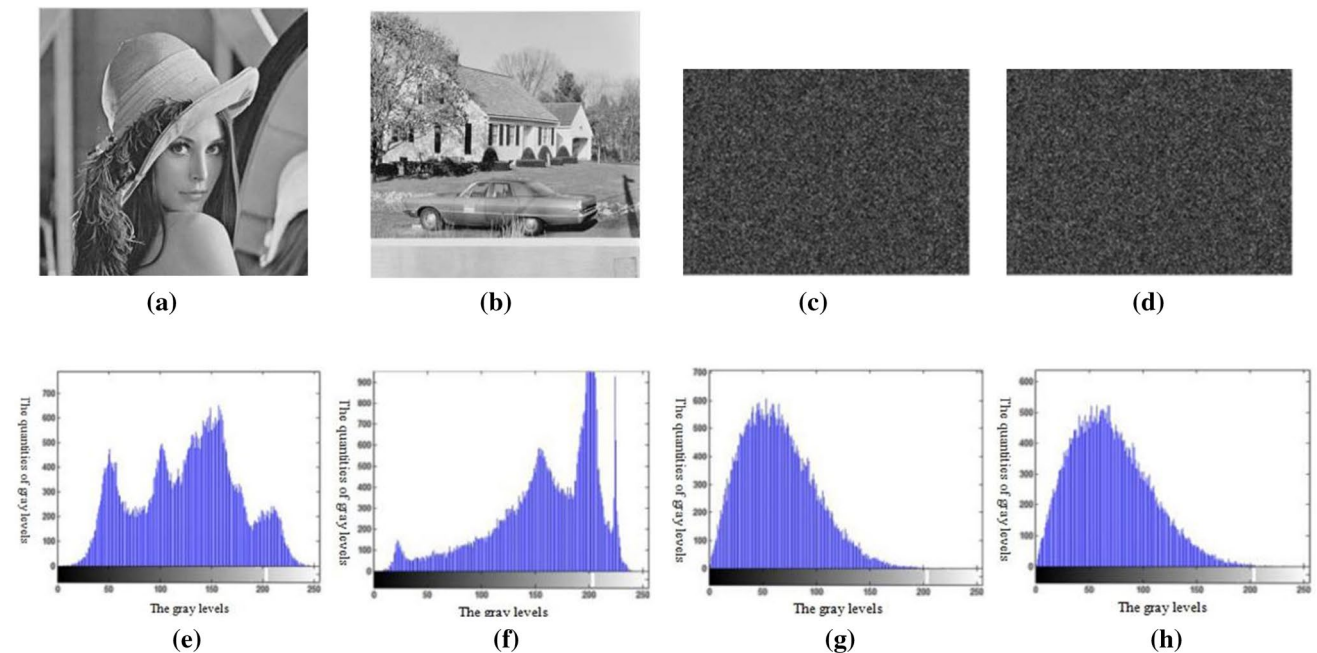
where  $S_f$  is the sampling rate, and it is the reciprocal of the comparison ratio  $r$ . The size of original image is  $N \times N$ , and the size of compressed image is  $M \times N$ ; (2)  $x_0 = 0.258$ ,  $y_0 = 0.368$ ,  $z_0 = 0.568$ , and  $a_1 = 35$ ,  $b_1 = 3$ ,  $c_1 = 28$  from the 3D chaos; (3) fractional orders  $a_1 = (a_{1x}, a_{1y}) = (1.5, 1.2)$ ,  $a_2 = (a_{2x}, a_{2y}) = (1.4, 1.6)$ , and scale factor  $s = 1$ ,  $b = \text{“haar”}$  mother wavelet from fractional wavelet transform. One of two encrypted holograms and decrypted image are displayed in Fig. 3b, c, respectively.

How pixels in an image are distributed by plotting the number of pixels at grayscale is illustrated with an image histogram. Specifically, it should hide the redundancy of plain-text and not leak any information about the plain-text or the relationship between plain-text and cipher-text.

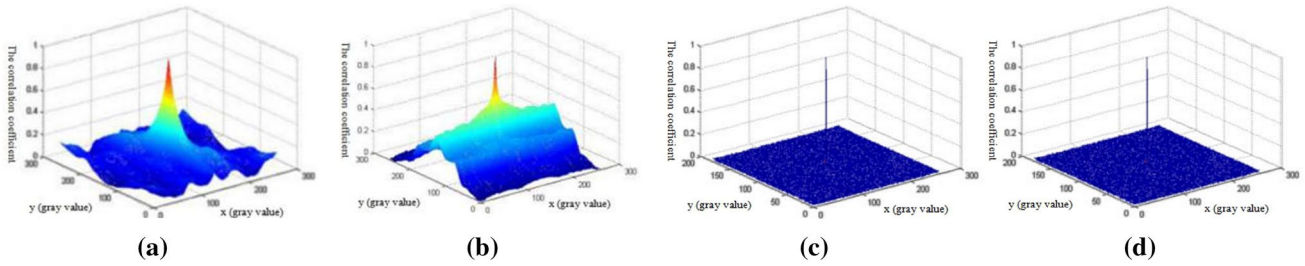
The histograms of “Lena” and “House” are shown in Fig. 4e, f. Their ciphered images produced by the proposed

scheme, and their histograms of ciphered images are shown in Fig. 4g, h, respectively. It is clear that the histograms of cipher images are significantly different from those of the plain images. Hence, it does not provide any clue to employ statistical attack.

The correlation coefficient of adjacent pixels is an important statistical feature of images. The correlation between two adjacent pixels in an original image is usually close to 1 in Fig. 5a, b. And an efficient image cryptosystem should produce the encrypted image with low correlation sufficiently. The correlation coefficients for adjacent pixels of their corresponding encrypted images are given in Fig. 5c, d, from which it is seen that the proposed scheme generally provides a satisfactory correlation performance.



**Fig. 4** The original image: **a** “Lena,” **b** “House”; the encrypted hologram: **c** “Lena,” **d** “House”; histogram of **e** “Lena,” **f** “House”; histogram of **g** encrypted hologram of “Lena,” **h** encrypted hologram of “House”

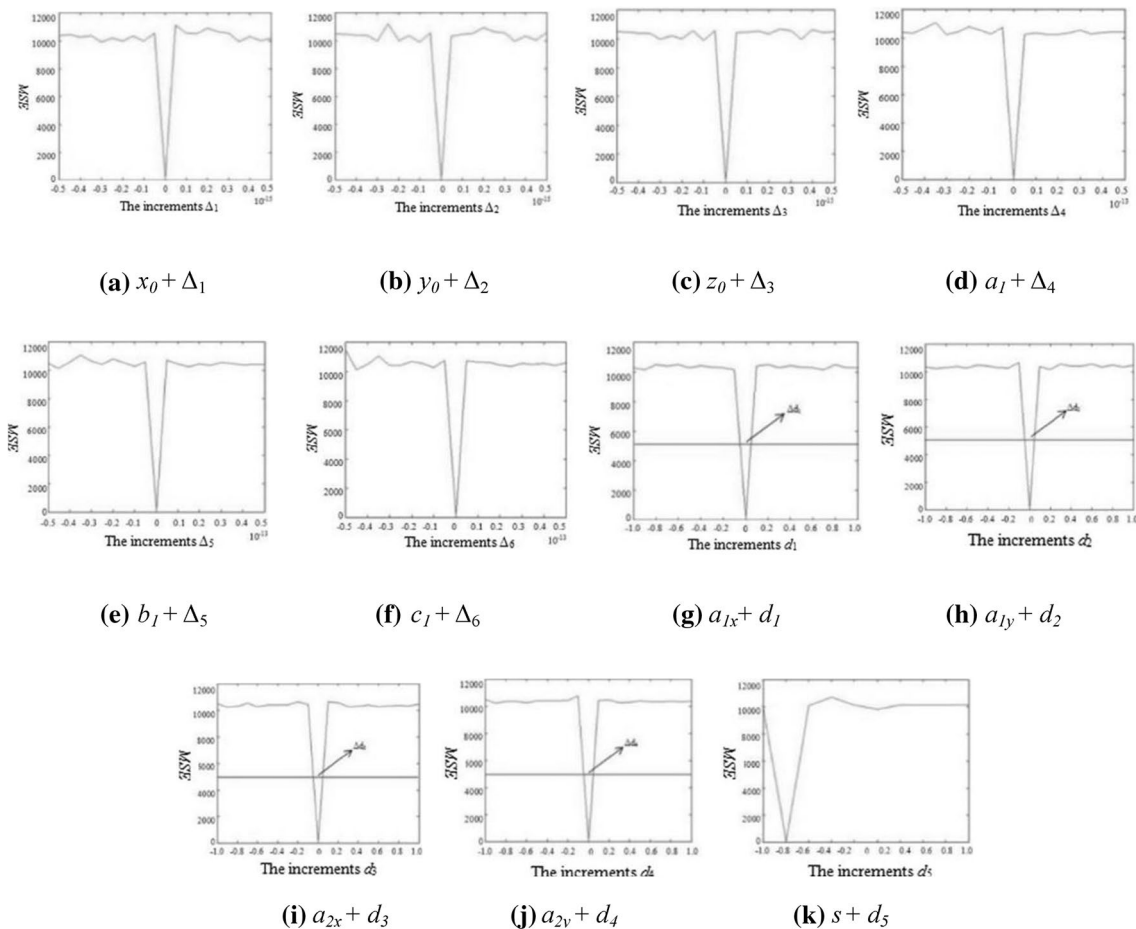


**Fig. 5** The autocorrelation coefficient distribution of adjacent pixels in original image of **a** “Lena,” **b** “House”; encrypted hologram of **c** “Lena,” **d** “House”

In our proposed scheme, there are 12 keys in total, namely six initial values  $x_0, y_0, z_0$  and  $a_1, b_1, c_1$  from the 3D chaos, four fractional orders  $a_{1x}, a_{1y}, a_{2x}, a_{2y}$ , the wavelet base type  $b$ , and the wavelet decomposition progression  $s$  in fractional wavelet domain.

We give the mean square error (MSE) curves in relation to increments  $\Delta_i$  and  $d_i$ , which are added to  $x_0, y_0, z_0, a_1, b_1, c_1$  and  $a_{1x}, a_{1y}, a_{2x}, a_{2y}, s$ , respectively. The MSE changes

versus each deviation are drawn in Fig. 6a–k, and it is clear that the proposed system is sensitive to keys, which means a tiny change of keys can result in a great visual distortion in recovered images. Usually, the MSE and peak signal-to-noise ratio (PSNR) is used to evaluate the quality of recovered images. Their formula is described as follows:



**Fig. 6** MSE curves for **a**  $x_0 + \Delta_1$ , **b**  $y_0 + \Delta_2$ , **c**  $z_0 + \Delta_3$ , **d**  $a_1 + \Delta_4$ , **e**  $b_1 + \Delta_5$ , **f**  $c_1 + \Delta_6$ , **g**  $a_{1x} + d_1$ , **h**  $a_{1y} + d_2$ , **i**  $a_{2x} + d_3$ , **j**  $a_{2y} + d_4$ , **k**  $s + d_5$

$$MSE = 1/MN \sum_{i=1}^M \sum_{j=1}^N (Y(i,j) - X(i,j))^2, \tag{19}$$

$$PSNR = 10 \log \left( \frac{255^2}{MSE} \right), \tag{20}$$

where  $Y(i, j)$  and  $X(i, j)$  denote pixel values of recovered image and original image at location  $(i, j)$ , respectively, and  $M, N$  denote the height and width of these images, respectively.

To provide high security of the encryption system, the key space should be large enough to make any brute-force attack ineffective. In our approach, the number of keys and their spaces are both expanded greatly. The total key space includes two processes of confusion and diffusion.

Since  $x_0, y_0, z_0$ , and  $a_1, b_1, c_1$  are from the 3D chaos, their key spaces could be computed by the help of MSE curve, when  $\Delta_1, \Delta_2, \Delta_3, \Delta_4, \Delta_5$ , or  $\Delta_6$  in initial values  $x_0 + \Delta_1, y_0 + \Delta_2, z_0 + \Delta_3$  and  $a_1 + \Delta_4, b_1 + \Delta_5, c_1 + \Delta_6$  drops down to  $1 \times 10^{-16}$ . The effective ranges of  $\Delta_i (i = 1, 2, 3)$  are all real number, and according to the IEEE floating-point standard [27], their computational precision of 64-bit double-precision number is about more than  $2^{64}$ , while the scope of  $\Delta_i (i = 4, 5, 6)$  is only a few set of values. So we can calculate that the key space from  $x_0, y_0, z_0$  and  $a_1, b_1, c_1$  is about  $10^{16 \times 3} \times 10^{14 \times 3} \times 2^{64} \times 3 = 5.534 \times 10^{109}$ .

As for the fractional orders  $a_{1x}, a_{1y}, a_{2x}$ , and  $a_{2y}$ , their key space could be analyzed as follows. In Fig. 6g–i, we know the maximum value of  $\Delta d_i (i = 1, 2, 3, 4, 5, 6)$  (the distances between the two cross-points on the red lines) is about 0.02 when the MSE is equal to  $5 \times 10^3$ . Since the effective range of  $d_i$  is  $[-2]$ , the number of possible intervals of  $d_i$  is  $4/0.02 = 200$ . So the key space from four fractional orders is  $200^4 = 4 \times 10^8$ . Besides, the wavelet base type  $b$  and the

wavelet decomposition progression  $s$  for fractional wavelet transform, the key space is more than  $2^{64}$ . Thus, the key space  $S$  of the entire encryption system is

$$S = \prod_{i=1}^{12} K_i > 4 \times 5.534 \times 10^{109} \times 10^8 \times 2^{64} = 4.08 \times 10^{137}, \tag{21}$$

which indicates heavy work for the opponents to decrypt the image by exhausting the keys.




To evaluate the performance of the encryption system, two other methods are used to compare with our proposed method. Thus, the encryption method [15] based on the CS and FRFT by multiple 1D chaotic map is called CS-FRFT. And the encryption method based on the CS and FWT by 3D chaotic map is called CS-FWT, which is a part of the proposed method without adopting holographic technology. In addition, all recovered images are rebuilt by the basis pursuit (BP) algorithm in three encryption methods. In Table 1, it is shown that the key space of our proposed method is greater than that of other methods, and thus it has a stronger ability to resist brute-force attacks for the proposed methods without reducing the quality of decrypted image.

The robustness of our proposed encryption system was checked against the attack using the noise and the occlusion. In the image transmission and processing, it is inevitable that the cipher-text will be affected by noise. Therefore, we need to test the ability of resisting noise attack, and different intensity random noises adjusted by parameter  $k$  are added into the cipher-text  $I$  as follows:










$$I' = I(1 + kG), \tag{22}$$

where  $I'$  is the noise-affected encrypted amplitude images,  $k$  is a coefficient that represents the noise strength, and  $G$  is a noise type, which is random noise. Accordingly, their

**Table 1** The key space comparison of three methods in the 75% sampling rate

	The proposed method	The part of the proposed method CS-FWT	CS-FRFT [15]
Key space	$> 4.08 \times 10^{137}$	$> 4.08 \times 10^{137}$	$10^{42} - 10^{91}$
Reconstruction image quality ( $M = 192$ )			
	PSNR = 33.45 dB	PSNR = 33.43 dB	PSNR = 32.68 dB

**Table 2** The anti-noise performance comparison of three methods in the 75% sampling rate

	Random noise attack $k = 0.1$	Random noise attack $k = 0.3$	Random noise attack $k = 0.6$
The proposed method	 PSNR = 25.13 dB	 PSNR = 14.61 dB	 PSNR = 10.52 dB
The part of the proposed method CS-FWT	 PSNR = 20.65 dB	 PSNR = 12.25 dB	 PSNR = 9.37 dB
CS-FRFT [15]	 PSNR = 20.09 dB	 PSNR = 12.27 dB	 PSNR = 9.58 dB

restored images of the proposed methods, CS-FWT and CS-FRFT, are illuminated in Table 2, from which it can be shown that the restored images of the proposed method have a higher image quality under the same intensity of noise. Therefore, compared with two other methods, the proposed method has a better robustness of anti-noise attacks.

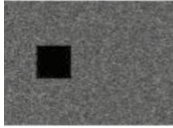
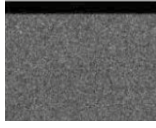






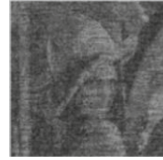



As a digital evaluation to measure the performance of resisting occlusion attack, peak signal-to-noise ratio (PSNR) is mathematically used to evaluate the quality of image. Compression has much effect on the reconstruction of original image. In generally, it cannot effectively resist occlusion attack well. In three encryption methods of the proposed, CS-FWT and CS-FRFT, the basic information of recovered images can all be identified in Table 3, and their PSNR values of the proposed methods are higher than those of two others, indicating that the proposed encryption system has a better robustness against occlusion attack with the aid of the holography.

An image encryption system can adopt the CS technique to save and process the compressed versions of encrypted images in order to decrease volume in transmission and

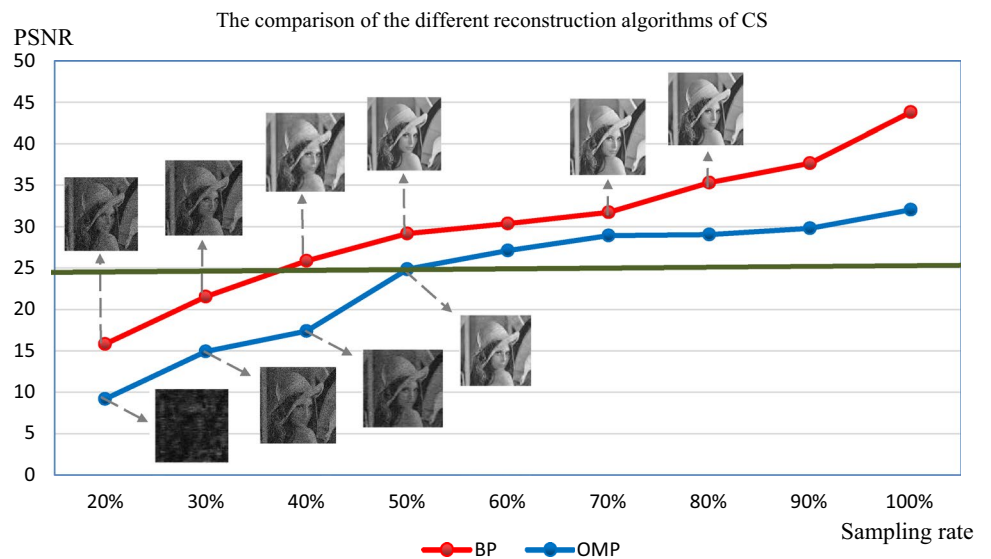
storage. To evaluate the compression performance of the proposed encryption system, “Lena” was chosen as the original image, and Fig. 7 is the decrypted image PSNR values in different sampling rates through the different reconstruction algorithms of CS. In basis pursuit (BP) [26] reconstruction algorithms of CS, when the sampling rate is about 40%, the PSNR value is 25.04 dB. At this time, we can see subjectively that the decrypted image is basically not distorted, and all the information of the original image is almost recognized, while the information is seriously lost when the PSNR value is 21.54 dB at a sampling rate of 30%. Besides, in orthogonal matching pursuit (OMP) [28] reconstruction algorithms of CS, the change curve can also be clearly seen. And when the PSNR of recovered image exceeds 25 dB (blue green line in Fig. 7), the recovered image has a good quality. Therefore, it can be seen that the quality of recovered image is acceptable when the sampling rate is lower than or equal to 50%. Even when the sampling rate reaches 40%, the PSNR is still not bad.



**Table 3** The comparison of performance against cropping of three methods in the 75% sampling rate

				
		5% data loss	10% data loss	20% data loss
The proposed method				
		PSNR = 19.78 dB	PSNR = 12.52 dB	PSNR = 9.82 dB
The part of the proposed method CS-FWT				
		PSNR = 13.33 dB	PSNR = 10.98 dB	PSNR = 8.37 dB
CS-FRFT [15]				
		PSNR = 12.51 dB	PSNR = 10.67 dB	PSNR = 8.72 dB

**Fig. 7** The decrypted image PSNR values of different sampling rates in the different reconstruction algorithms of CS



## 5 Conclusions

In this paper, an efficient and secure image cryptosystem, based on CS and PSI in asymmetric fractional wavelet domain by 3D Chen's chaos map, is proposed. It not only can overcome problems of the small key space and low security in resisting nonlinear attacks, but also decreases a large number of encrypted data greatly. In order to simplify the transmission and storage, the keys generated by 3D chaos map replace the enormous RPM and measurement matrix. With the help of digital holography, the proposed method has a good robustness against occlusion and noise attacks. And the higher security of our cryptosystem is demonstrated by evaluating key space analysis. In addition, for efficiency analysis, the compression performance analysis shows that the PSNR is high enough to recognize the information of original image when the sampling rate is lower than or equal to 50%, and it is acceptable even at 40%. Thus, the proposed encryption system may be a reference for data security transmission and effective storage in encryption.

**Acknowledgements** The work is supported by the National Science Foundation of China (NSFC) (61405130 and 61320106015).

## References

1. Refregier, P., Javidi, B.: Optical image encryption based on input plane and Fourier plane random encoding. *Opt. Lett.* **20**, 767–769 (1995)
2. Nakano, K., Takeda, M., Suzuki, H., et al.: Encrypted imaging based on algebraic implementation of double random phase encoding. *Appl. Opt.* **53**, 2956–2963 (2014)
3. Wang, X., Chen, W., Chen, X.: Optical information authentication using compressed double random phase encoded images and quick-response codes. *Opt. Express.* **23**, 6239–6253 (2015)
4. Zhao, T., Ran, Q., Yuan, L., et al.: Manipulative attack using the phase retrieval algorithm for double random phase encoding. *Appl. Opt.* **54**, 7115–7119 (2015)
5. Rajput, S.K., Nishchal, N.K.: Optical double image security using random phase fractional Fourier domain encoding and phase-retrieval algorithm. *Opt. Commun.* **388**, 38–46 (2017)
6. Dinç, E., Ragno, G., Baleanu, D., et al.: Fractional wavelet transform-continuous wavelet transform for the quantification of melatonin and its photo degradation product. *Spectrosc. Lett.* **45**, 337–343 (2012)
7. Singh, H.: Optical cryptosystem of color images using random phase masks in the fractional wavelet transform domain. *Am. Inst. Phys. Conf. Ser.* **12**, 767–769 (2016)
8. Orsdemir, A., Altun, H.O., Sharma, G., Bocko, M.F.: On the security and robustness of encryption via compressed sensing. *IEEE Milit. Commun. Conf.* 1–7 (2008)
9. Gong, Q., Wang, Z., Lv, X., et al.: Interference-based image encryption with silhouette removal by aid of compressive sensing. *Opt. Commun.* **359**, 290–296 (2016)
10. Cambareri, V., Mangia, M., Pareschi, F., et al.: Low-complexity multiclass encryption by compressed sensing. *IEEE Trans. Signal Process.* **63**, 2183–2195 (2015)
11. Deepan, B., Quan, C., Wang, Y., et al.: Multiple-image encryption by space multiplexing based on compressive sensing and the double-random phase-encoding technique. *Appl. Opt.* **53**, 4539–4547 (2014)
12. Rawat, N., Kim, B., Kumar, R.: Fast digital image encryption based on compressive sensing using structurally random matrices and Arnold transform technique. *Opt. Int. J. Light Electron Opt.* **127**, 2282–2286 (2016)
13. Lang, J., Zhang, J.: Optical image cryptosystem using chaotic phase-amplitude masks encoding and least-data-driven decryption by compressive sensing. *Opt. Commun.* **338**, 45–53 (2015)
14. Liu, H., Xiao, D., Liu, Y., et al.: Securely compressive sensing using double random phase encoding. *Opt. Int. J. Light Electron Opt.* **126**, 2663–2670 (2015)
15. Liu, X., Mei, W., Du, H.: Optical image encryption based on compressive sensing and chaos in the fractional Fourier domain. *J. Mod. Opt.* **61**, 1–8 (2014)
16. Deng, J., Zhao, S., Wang, Y., et al.: Image compression-encryption scheme combining 2D compressive sensing with discrete fractional random transform. *Multimed. Tools Appl.* **86**, 1–21 (2016)
17. Liu, X., Mei, W., Du, H.: Simultaneous image compression, fusion and encryption algorithm based on compressive sensing and chaos. *Opt. Commun.* **366**, 22–32 (2016)
18. Tong, X.J., Wang, Z., Zhang, M., et al.: An image encryption algorithm based on the perturbed high-dimensional chaotic map. *Nonlinear Dyn.* **80**, 1–16 (2015)
19. Zhou, N., Pan, S., Cheng, S., et al.: Image compression-encryption scheme based on hyper-chaotic system and 2D compressive sensing. *Opt. Laser Technol.* **82**, 121–133 (2016)
20. George, S.N., Pattathil, D.P.: A novel approach for secure compressive sensing of images using multiple chaotic maps. *J. Opt.* **43**, 1–17 (2014)
21. Fridrich, A.: A novel 1D hybrid chaotic map-based image compression and encryption using compressed sensing and Fibonacci-Lucas transform. *Math. Probl. Eng.* **3**, 1–15 (2016)
22. Mendlovic, D., Zalevsky, Z., Mas, D.: Fractional wavelet transform. *Appl. Opt.* **20**, 4801–4806 (1997)
23. Kong, D., Shen, X., Lin, C., et al.: Optical image encryption based on fractional wavelet transform with double random phases. *Opt. Instrum.* **35**, 17–21 (2013)
24. Duarte, M., Davenport, M., Takbar, D., Laska, J., Sun, T., Kelly, K., Baraniuk, R.: Single-pixel imaging via compressive sampling. *IEEE Signal Process. Mag.* **25**, 83–91 (2008)
25. Guan, Z.H., Huang, F.J., Guan, W.J.: Chaos-based image encryption algorithm. *Phys. Lett. A.* **346**, 153–157 (2005)
26. Chen, S., Donoho, D.L., Saunders, M.A.: Atomic decomposition by basis pursuit. *Siam J. Sci. Comput.* **20**, 33–61 (1998)
27. IEEE: IEEE standard for binary floating-point arithmetic. *Lecture Notes on the Status of IEEE*, pp. 86–118 (1985)
28. Liu, E., Temlyakov, V.N.: The orthogonal super greedy algorithm and applications in compressed sensing. *Inf. Theory IEEE Trans.* **58**, 2040–2047 (2012)