Trans. Tianjin Univ. (2017) 23:184–191
DOI 10.1007/s12209-017-0036-3

RESEARCH ARTICLE

Optical Image Encryption Based on Mixed Chaotic Maps and Single-Shot Digital Holography

Yonggang Su[1,2] · Chen Tang[1] · Xia Chen[1] · Biyuan Li[1] · Wenjun Xu[1] · Zhenkun Lei[3]

Received: 5 April 2016 / Revised: 14 June 2016 / Accepted: 9 August 2016 / Published online: 8 March 2017

Abstract Random phase masks play a key role in optical image encryption schemes based on double random phase technique. In this paper, a mixed chaotic method is proposed, which can efficiently solve some weaknesses that one-dimensional (1-D) single chaotic maps encounter to generate random phase masks. Based on the chaotic random phase masks, optical image encryption and decryption are realized with a single-shot digital holographic technique. In the proposed encryption scheme, the initial value and parameters of mixed chaotic maps serve as secret keys, which is convenient for the key management and transmission. Moreover, it also possesses high resistance against statistical attack, brute-force attack, noise attack and shear attack. Simulation results and security analysis verify the validity and security of the proposed encryption scheme.

Keywords Image encryption · Mixed chaotic maps · Digital holography · Chaotic random phase mask

✉ Chen Tang
tangchen@tju.edu.cn

[1] School of Electrical and Information Engineering, Tianjin University, Tianjin 300072, China

[2] Science and Technology on Electro-Optical Information Security Control Laboratory, Tianjin 300308, China

[3] State Key Laboratory of Structural Analysis for Industrial Equipment, Dalian University of Technology, Dalian 116024, China

Introduction

As one of the important issues in the information age, image security has received increasing attention. Among numerous technologies for image encryption, optical technique plays an important role owing to its high computation speed, high parallelism in applications and arbitrary parameter selection. In 1995, double random phase encoding (DRPE) technique in Fourier transform domain was proposed by Refregier and Javidi [1]. After that, DRPE was extended to other transform domains, such as fractional Fourier domain [2] and Fresnel domain [3]. Some other optical image encryption schemes based on joint transform correlators [4], digital holography [5–7], photon counting imaging [8] and compressive sensing [9, 10] were also proposed subsequently. It is worth mentioning that optical image encryption schemes based on DRPE technique can readily be performed using digital holography, owing to its excellent performance in recording and reconstructing the complex values. Phase-shifting techniques, such as four-step [5] and two-step [6] phase shift, are commonly used to retrieve the original complex information in digital holography. Nevertheless, these techniques need at least two interferograms to reconstruct the original complex object field. Unlike phase-shifting techniques, single-shot digital holography [7, 11] needs only one single-frame hologram to retrieve the original complex information.

Obviously, random phase masks play a key role in the optical image encryption schemes based on DRPE technique. When transmitting the encrypted images, effective and convenient management of secret keys is important for the encryption scheme. In most of the existing DRPE-based encryption schemes, the whole random phase masks with the same size as encrypted image have to be sent to the

authorized receiver side to decrypt the original image, which is inconvenient for the secret key management and transmission. The majority of previous studies focused on devising optical encryption systems, but few attention was paid to the new random phase encoding techniques.

Recently, the chaos-based encryption technique has become an interesting research topic. This technique can provide a good combination of speed, high security, complexity and computational power [12]. Chaotic maps have many fundamental properties, which can be considered analogous to some cryptographic properties of ideal ciphers, so they are widely used to encrypt digital images. In recent years, researchers have tried to propose some chaotic random phase encoding techniques. An image encryption scheme using fractional Fourier transform and chaos theory was proposed by Singh and Sinha [13], in which the random phase masks are generated by one single chaotic map such as Tent map. A double-image encryption scheme based on discrete multi-parameter fractional angular transform and two-coupled logistic maps was proposed by Sui et al. [14], in which the images are scrambled by two-coupled logistic maps before the optical processing step, and the random phase masks are generated by one single logistic map in the optical processing step. The 1-D single chaotic maps including logistic map and Tent map have the advantages of simplicity and low computational complexity. However, there are some drawbacks such as small key space and weak security [15] existing in the cryptosystem based on these chaotic maps. To avoid these problems, a novel mixed chaotic method is proposed to generate the random phase masks in this paper. In the proposed method, two 1-D single chaotic maps with distinct structures are combined to form a mixed chaotic map, and the two random phase masks are generated by two different mixed chaotic maps, respectively. Based on the chaotic random phase masks, optical image encryption and decryption are realized with a single-shot digital holographic technique. In the proposed encryption scheme, the initial value and parameters of mixed chaotic maps serve as secret keys, which is convenient for the key management and transmission. Moreover, the proposed encryption scheme possesses high resistance against statistical attack, brute-force attack, noise attack and shear attack. Simulation results and security analysis also verify the validity and security of the proposed scheme.

The rest of the paper is organized as follows. In Sect. 2, the construction of mixed chaotic maps will be described in detail. The optical image encryption scheme that combines single-shot digital holography with chaotic random phase masks will be presented in Sect. 3. Security analysis and numerical simulation results are given to verify the security and validity of the proposed encryption scheme in Sect. 4. Finally, conclusions are given in Sect. 5.

Mixed Chaotic Maps

Chaotic maps have many important properties, such as the sensitive dependence on the initial values and system parameters, pseudorandom property, nonperiodicity and topological transitivity. Most of these properties meet requirements such as permutation and diffusion in the sense of cryptography. Therefore, chaotic maps, especially the 1-D single chaotic maps, have more useful and practical applications in image encryption schemes. Though the 1-D single chaotic maps have the advantages of simplicity and low computational complexity, there are some drawbacks such as small key space and weak security existing in the cryptosystems based on these chaotic maps. With the logistic map [16] as an example, when the initial parameters are set as particular values, the security of cryptosystem based on logistic map will become very weak. Figure 1 shows the iterated results of logistic map when the initial parameters are set as $x_0 = 0.25, \mu = 4$. One can find that the iterated values are constant, and there are no random sequences generated. In this case, the logistic map cannot be used to encrypt the image. This is not a rare phenomenon in logistic map, but it happens in other 1-D single chaotic maps. Therefore, to avoid these problems, a novel mixed chaotic method is proposed to generate the random phase masks. In the proposed method, two 1-D single chaotic maps with distinct structures are combined to form a mixed chaotic map. The 1-D single chaotic maps used in this paper are chosen as logistic map [16], iterative chaotic map with infinite collapses (ICMIC) map [17] and Chebyshev map [18], respectively.

The discrete form of logistic map is defined as

$$x_{n+1} = \mu x_n(1 - x_n) \tag{1}$$

When the control parameter $\mu \in (3.5699, 4]$, the logistic map is chaotic.

The discrete form of ICMIC map is defined as

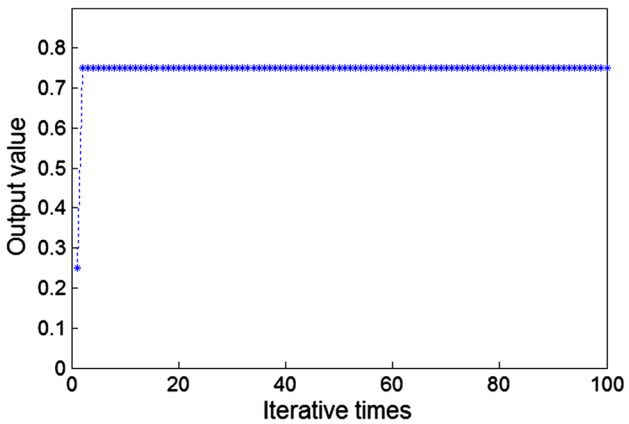

Fig. 1 Iterative results of logistic map

$$x_{n+1} = \sin(a/x_n) \tag{2}$$

When the control parameter $a \in (0, \infty)$, the ICMIC map is chaotic.

The discrete form of Chebyshev map is defined as

$$x_{n+1} = \cos\left(w\left(\cos^{-1} x_n\right)\right) \tag{3}$$

When the control parameter $w \in [2, \infty)$, the Chebyshev map is chaotic.

To construct the first mixed chaotic map, an appropriate initial value is firstly assigned to logistic map. Then, the output value of logistic map is used as the initial value of ICMIC map, and the random number sequence generated by ICMIC map will be used to generate the first random phase mask. The first mixed chaotic map can be written as

$$\begin{cases} x_{n+1} = \mu x_n(1 - x_n) \\ y_{n+1} = \sin(a/y_n) \end{cases} \tag{4}$$

Similarly, the appropriate initial value is firstly assigned to logistic map, and the output value of logistic map is then used as the initial value of Chebyshev map. The random number sequence generated by Chebyshev map will be used for generating the second random phase mask. The second mixed chaotic map can be written as

$$\begin{cases} x_{n+1} = \mu x_n(1 - x_n) \\ y_{n+1} = \cos(w(\cos^{-1} y_n)) \end{cases} \tag{5}$$

The proposed mixed chaotic maps can largely help avoid the problem that 1-D single chaotic maps encounter. In addition, the extended key space of mixed chaotic maps can further increase the security of cryptosystems. In this paper, two random phase masks are, respectively, generated by two different mixed chaotic maps. The chaotic random phase masks can be controlled by the initial value and parameters of mixed chaotic maps, which is convenient for the key transmission and management.

Proposed Optical Image Encryption Scheme

In this section, two chaotic random phase masks are introduced to the optical security system, as shown in Fig. 2. The original image is multiplied by the first chaotic random phase mask (CRPM) represented by $\exp[\mathrm{i}2\pi c_1(x_0, y_0)]$, where $c_1(x_0, y_0)$ is the random number sequence generated by the first mixed chaotic map. Then, the optical field distribution on the plane (x_1, y_1) can be written as

$$\mathrm{FrT}_{Z_1}\{U_0(x_0, y_0)\exp[\mathrm{i}2\pi c_1(x_0, y_0)]\} \tag{6}$$

where FrT_{Z_1} is the Fresnel transform of distance z_1; U_0 is the complex value of original image.

This optical field distribution is then encoded by the second CRPM represented by $\exp[\mathrm{i}2\pi c_2(x_1, y_1)]$, where

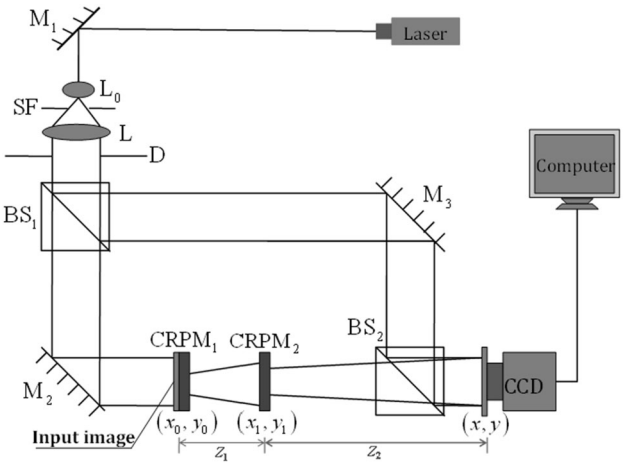

Fig. 2 Optical setup of the proposed cryptosystem. *M* mirror, L_0, *L* lens, *SF* spatial filter, *D* diaphragm, *BS* beam splitter, *CCD* charge-coupled device

$c_2(x_1, y_1)$ is the random number sequence generated by the second mixed chaotic map. The optical field distribution on the recording plane (x, y) can be written as

$$\begin{aligned} O_0(x, y) = \mathrm{FrT}_{Z_2}\{\mathrm{FrT}_{Z_1}\{U_0(x_0, y_0)\exp[\mathrm{i}2\pi c_1(x_0, y_0)]\} \\ \times \exp[\mathrm{i}2\pi c_2(x_1, y_1)]\} \end{aligned} \tag{7}$$

where O_0 is the object wave function on CCD camera plane; FrT_{Z_2} is the Fresnel transform of distance z_2.

Suppose that the reference wave is expressed as

$$R = |R|\exp(\mathrm{i}kx\sin\theta) \tag{8}$$

where k is the wave number; and θ is the angle between reference wave and object wave.

The reference wave and object wave intervene on the CCD plane to form a hologram, i.e., a noise-like encrypted image can be expressed as

$$H = |O_0|^2 + |R|^2 + R^* O_0 + O_0^* R \tag{9}$$

where $*$ stands for a complex conjugate.

To decrypt the original image, the single-shot digital holographic technique is adopted. This technique models the reconstruction of complex object field on the hologram plane as a constrained optimization problem, and the cost function to be minimized can be expressed as

$$C(O, O^*) = \frac{1}{2}\left\| H - \left(|O|^2 + |R|^2 + R^* O + O^* R\right)\right\|^2 + \alpha\psi(O, O^*) \tag{10}$$

where $\psi(O, O^*)$ is a penalty function for imposing a smoothness constraint on the complex object function O; and α is a control parameter. The optimization problem can be solved iteratively by steepest descent method. The

gradient of the cost function in Eq. (10) with respect to O^* may be calculated as

$$\nabla_{O^*} C(O, O^*) = -\left[H - \left(|O|^2 + |R|^2 + R^* O + O^* R\right)\right](O + R) + \alpha \nabla_{O^*} \psi(O, O^*) \quad (11)$$

Hence, the iterative solution is

$$\begin{aligned} O^{(n+1)} &= O^{(n)} - t[\nabla_{O^*} C]_{O=O^{(n)}} \\ &= O^{(n)} + t\left[H - \left(\left|O^{(n)}\right|^2 + |R|^2 + R^* O^{(n)} + O^{(n)*} R\right)\right] \\ &\quad \times \left(O^{(n)} + R\right) \end{aligned} \quad (12)$$

where t is step size. Operationally, α is set as zero.

The results of the iterative procedure in Eq. (12) give a complex object function $O(x, y)$, and then, the original image can be retrieved as

$$\begin{aligned} U_0^{\dagger}(x_0, y_0) &= \mathrm{IFrT}_{Z_1}\{\mathrm{IFrT}_{Z_2}[O(x, y)] \exp[-\mathrm{i}2\pi c_2(x_1, y_1)]\} \\ &\quad \times \exp[-\mathrm{i}2\pi c_1(x_0, y_0)] \end{aligned} \quad (13)$$

Security Analysis and Experiment Results

To verify the feasibility and effectiveness of the proposed scheme, numerical simulations are performed on two plain images of "TEST" and "Peppers," as shown in Fig. 3a, b. In these numerical simulations, the proposed encryption scheme is compared with the method in Ref. [13] in terms of key sensitivity and correlation coefficient analysis of adjacent pixels. The numerical simulations are completed by MATLAB R2011a on a PC with Core i3-2120, 3.3 GHz CPU and 2 GB RAM memory. In the proposed encryption scheme, the initial value and parameters of the mixed chaotic maps are set as $x_0 = 0.3141$, $\mu = 3.8956$, $a = 12.5098$ and $w = 4$, and the parameters of the optical system are set as $\lambda = 632.8$ nm, $z_1 = 500$ mm, $z_2 = 300$ mm, $n = 20$ and $t = 0.005$, respectively. For the method in Ref. [13], the initial values and parameters of logistic map are set as $x_1 = 0.241$, $\mu_1 = 3.85$ and $x_2 = 0.341$, $\mu_2 = 3.96$ to generate the first and second random phase masks, and the fractional orders of the first and second fractional Fourier transform systems are set as $(0.75, 0.9)$ and $(1.25, 1.1)$, respectively. Figure 3c, d shows the encrypted image of "TEST" and "Peppers," respectively. The decrypted images with correct keys are shown in Fig. 3e, f, from which one can find that the original image can be retrieved from the encrypted image well.

Key Space Analysis

The set of all initial values and parameters of mixed chaotic maps compose the main key space. The main key space of the proposed encryption scheme has four secret key values, i.e., $x_0 = 0.3141$, $\mu = 3.8956$, $a = 12.5098$ and $w = 4$. As stated in the IEEE floating-point standard, the computational precision of the 64-bit double-precision number is about 10^{-15}. Therefore, the main key space of the proposed encryption scheme is $(10^{15})^4 = 10^{60} \approx \leftarrow 2^{199}$. Furthermore, the parameters of optical encryption system such as diffraction distance and incident wavelength can also be used as one part of the key size. From the above analysis,

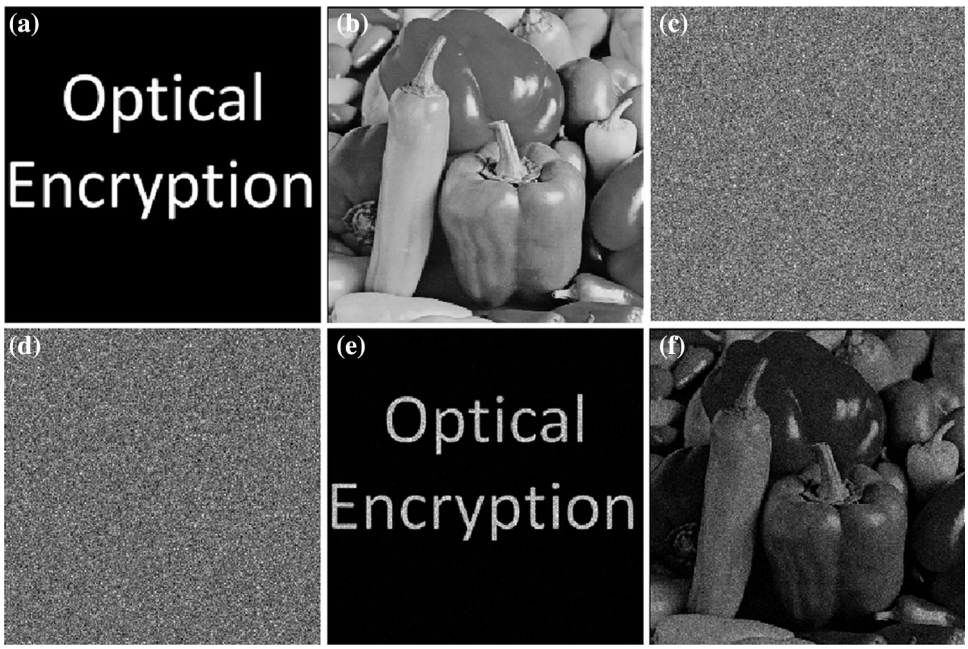

Fig. 3 Two plain images and their encryption and decryption results. **a** Plain image "TEST," **b** plain image "Peppers," **c** encrypted image "test," **d** encrypted image "peppers," **e** decrypted image "test" and **f** decrypted image "Peppers"

one can find that the key space of the proposed encryption scheme is large enough to resist the brute-force attack.

Sensitivity of Keys

In the proposed encryption scheme, the initial value and parameters of mixed chaotic maps serve as the main keys. In Ref. [13], the initial value x_2 and parameter μ_2 of logistic map serve as the main keys. To evaluate the key sensitivity, the encryption and decryption are repeated with a tiny alteration introduced to one of the correct keys each time. To demonstrate the difference between the two encrypted images C_1 and C_2 which are obtained from the same plain image by using two similar encryption keys, the number of pixels change rate (NPCR) and the unified average changing intensity (UACI) are computed. The NPCR and UACI are defined as follows:

$$\mathrm{NPCR} = \frac{\sum_{i=0}^{W-1}\sum_{j=0}^{H-1} D(i,j)}{WH} \times 100\% \tag{14}$$

$$\mathrm{UACI} = \frac{1}{WH}\left(\sum_{i=0}^{W-1}\sum_{j=0}^{H-1}\frac{|C_1(i,j) - C_2(i,j)|}{255}\right) \times 100\% \tag{15}$$

where D is a two-dimensional set with the same size as image C_1 or C_2; W and H are the width and height of the image, respectively. The set $D(i,j)$ is defined by $C_1(i,j)$ and $C_2(i,j)$: if $C_1(i,j) \neq C_2(i,j)$ then $D(i,j) = 1$; otherwise, $D(i,j) = 0$. The NPCR and UACI test results from the proposed encryption algorithm and the method in Ref. [13] are listed in Table 1. It can be seen that the proposed encryption algorithm is sensitive with respect to small changes of secret keys, and the proposed encryption algorithm outperforms the method in Ref. [13].

To demonstrate the difference between the original image U_0 and the decrypted image $U_0^{\dagger}$ numerically, the correlation coefficient (CC) is calculated as follows

$$\mathrm{CC} = \frac{E\left\{\left[U_0^{\dagger} - E\left[U_0^{\dagger}\right]\right]\left[U_0 - E[U_0]\right]\right\}}{\sqrt{E\left\{\left[U_0^{\dagger} - E\left[U_0^{\dagger}\right]\right]^2\right\}E\left\{\left[U_0 - E[U_0]\right]^2\right\}}} \tag{16}$$

where $E\{\cdot\}$ is an expectation operator. Note that the higher the value of CC, the smaller the difference between the decrypted and original images.

The images of "TEST" and "Peppers" are decrypted under the condition that one key is incorrect while the other keys are correct, and the decrypted images are shown in Figs. 4 and 5, respectively. Figures 4a–d and 5a–d show the decrypted images "TEST" and "Peppers" by the proposed encryption scheme with incorrect keys $x_0^{\dagger} = x_0 + 1 \times 10^{-15}$, $\mu^{\dagger} = \mu + 1 \times 10^{-15}$, $a^{\dagger} = a + 1 \times 10^{-15}$ and $w^{\dagger} = w + 1 \times 10^{-15}$, respectively. These decrypted images with incorrect keys do not show the information about the original images visually. Figures 4e, f and 5e, f show the decrypted images "TEST" and "Peppers" by the method in Ref. [13] with incorrect keys $x_2^{\dagger} = x_2 + 1 \times 10^{-15}$ and $\mu_2^{\dagger} = \mu_2 + 1 \times 10^{-15}$, respectively. The CC of Figs. 4a–f and 5a–f is 0.0043, 0.0005, 0.0018, 0.0041, 0.0300, 0.0144 and 0.0165, 0.0151, 0.0155, 0.0138, 0.0183, 0.0171, respectively, which means that the proposed encryption scheme outperforms the method in Ref. [13].

The above results indicate that the proposed encryption scheme is highly sensitive to the secret keys. Even an almost perfect guess of the key does not reveal any valuable information about the plain image. In addition, the results also indicate that the proposed encryption scheme outperforms the method in Ref. [13] in terms of key sensitivity.

Correlation Coefficient Analysis of Adjacent Pixels

In order to test the correlation of adjacent pixels, 1 000 pairs of adjacent pixels are randomly selected in the vertical,

Table 1 NPCR and UACI results of the two encrypted images with similar secret keys (k, k^*)

Index	(k, k^*)	Image "TEST"		Image "Peppers"	
		Ref. [13]	Proposed method	Ref. [13]	Proposed method
NPCR	(x, x^*)	88.1830	95.5615	91.8170	98.2181
	(μ, μ^*)	87.4973	95.1022	91.0876	96.6571
	(a, a^*)	–	96.9272	–	97.3884
	(w, w^*)	–	94.1776	–	95.6943
UACI	(x, x^*)	28.9156	32.2641	30.5950	32.5065
	(μ, μ^*)	28.6523	32.1290	30.2600	32.1128
	(a, a^*)	–	32.6025	–	32.1538
	(w, w^*)	–	31.8061	–	32.1072

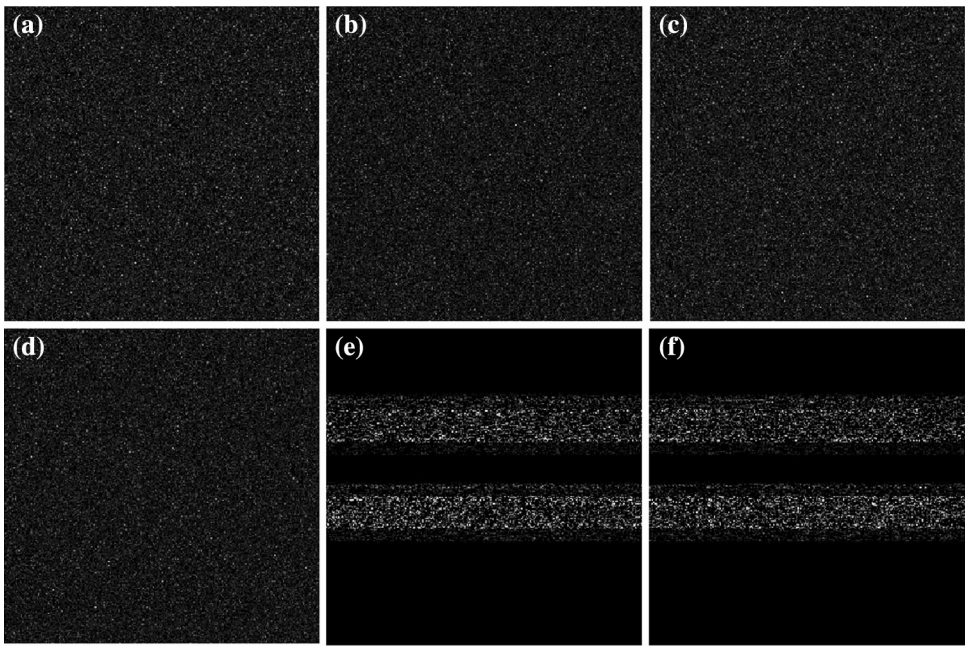

Fig. 4 Decrypted results of image "TEST" with incorrect keys. **a** Decrypted image with $x_0 + 10^{-15}$, **b** decrypted image with $\mu + 10^{-15}$, **c** decrypted image with $a + 10^{-15}$, **d** decrypted image with $w + 10^{-15}$, **e** decrypted image with $x_2 + 10^{-15}$ and **f** decrypted image with $\mu_2 + 10^{-15}$

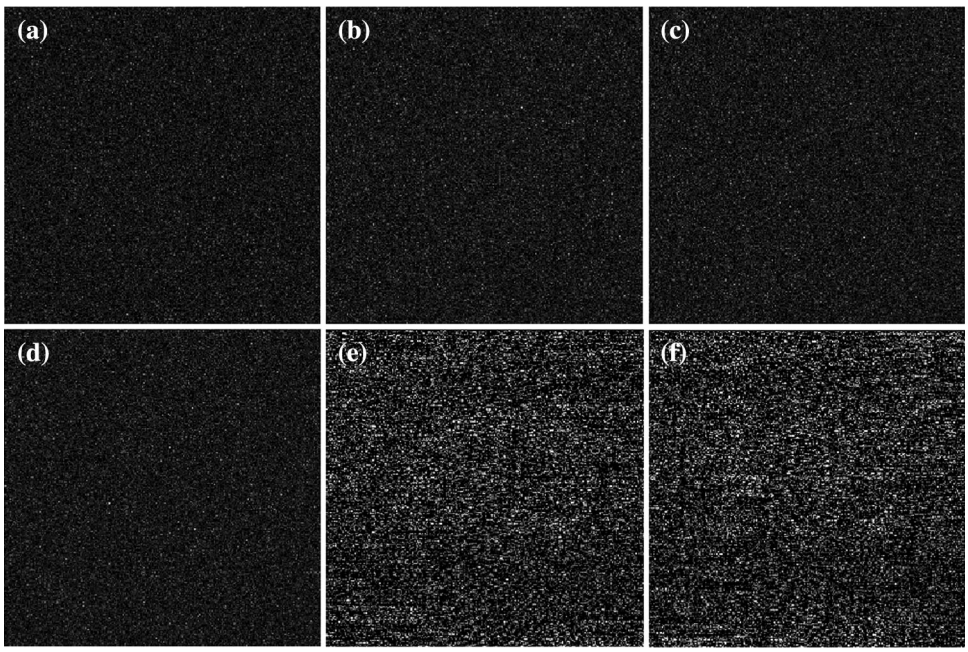

Fig. 5 Decrypted results of image "Peppers" with incorrect keys. **a** Decrypted image with $x_0 + 10^{-15}$, **b** decrypted image with $\mu + 10^{-15}$, **c** decrypted image with $a + 10^{-15}$, **d** decrypted image with $w + 10^{-15}$, **e** decrypted image with $x_2 + 10^{-15}$ and **f** decrypted image with $\mu_2 + 10^{-15}$

horizontal and diagonal directions from the plain images "TEST" and "Peppers" as well as from the corresponding cipher images encrypted by the proposed encryption scheme and the method in Ref. [13]. The correlation coefficient of two adjacent pixels (x_i, y_i) is calculated as

$$\mathrm{Cor} = \frac{\mathrm{cov(x,y)}}{\sqrt{D(x)}\sqrt{D(y)}} \tag{17}$$

where

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - \bar{x})^2 \tag{18}$$

$$D(y) = \frac{1}{N}\sum_{i=1}^{N}(y_i - \bar{y})^2 \tag{19}$$

$$\mathrm{cov}(x,y) = \sum_{i=1}^{N}(x_i - \bar{x})(y_i - \bar{y}) \tag{20}$$

Table 2 Horizontal, vertical and diagonal correlation coefficients of adjacent pixels in the plain and encrypted images

Direction	Image "TEST"			Image "Peppers"		
	Plain image	Ref. [13]	Proposed method	Plain image	Ref. [13]	Proposed method
Horizontal	0.8641	0.2263	0.0084	0.9414	0.0484	0.0132
Vertical	0.8707	0.2706	−0.0047	0.9438	0.1119	0.0154
Diagonal	0.7564	0.1947	0.0011	0.8969	−0.0553	−0.0105

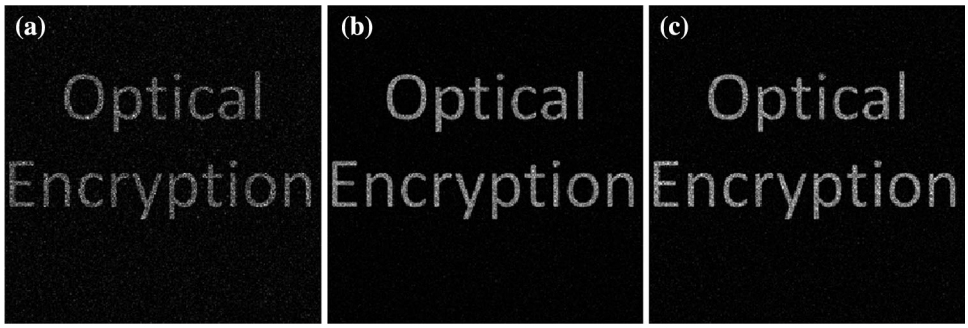

Fig. 6 Robustness against noise attacks. **a** Decrypted image with Gaussian noise, **b** decrypted image with salt and pepper noise and **c** decrypted image with speck noise

where N is the total number of couples (x_i, y_i); and $\bar{x}$, $\bar{y}$ are the mean values of x_i and y_i, respectively.

Table 2 shows the results of correlation computations of two adjacent pixels in the plain images and the corresponding cipher images encrypted by different encryption methods. It is clear that the two adjacent pixels of the plain images are highly correlated in the three directions. And for the cipher images encrypted by the proposed encryption scheme, there is a negligible correlation between the two adjacent pixels in three directions. In addition, the correlation between two adjacent pixels in the cipher images encrypted by the method in Ref. [13] is higher than those encrypted by the proposed encryption scheme. The results indicate that the proposed encryption scheme outperforms the method in Ref. [13], and the unauthorized users cannot get any valid information from the statistical data.

Noise Attack

During the transmission, the encrypted images may be polluted by various types of noises. In order to investigate the performance of the proposed encryption scheme against noise attack, three different kinds of noises, i.e., Gaussian noise with zero mean, salt and pepper noise and speckle noise, are added to the encrypted image of "TEST" by using the imnoise function in MATLAB. Figure 6a–c is the decrypted image of "TEST" retrieved from the encrypted data polluted by Gaussian noise, salt and pepper noise and speckle noise at 0.10 noise level, respectively. And the corresponding values of CC are 0.5938, 0.8748 and 0.9127, respectively. The results demonstrate that the decrypted images can be recognized despite of some noise interference, and the proposed encryption scheme can tolerate a certain range of noise level.

Shear Attack

During the transmission, the encrypted image may also be partially lost. Therefore, the robustness against shear attack should be considered. Figure 7a–c shows the encrypted images of "TEST" damaged by 12.5, 25 and 50%, respectively. The decryption process is performed on these damaged cipher images with all correct keys. The corresponding decrypted results are shown in Fig. 7d–f, from which the main information of the original image can be recognized visually. The CCs of Fig. 7d–f are 0.8612, 0.6409 and 0.2581, respectively, indicating that the proposed encryption scheme has high robustness against the shear attack.

Conclusions

A novel mixed chaotic method for generating the random phase masks is proposed. Based on CRPM, optical image encryption and decryption are realized with a single-shot digital holography. In the proposed optical encryption scheme, the plain images fail to be recovered unless all of the correct keys are known. Moreover, the proposed encryption scheme has high resistance against potential

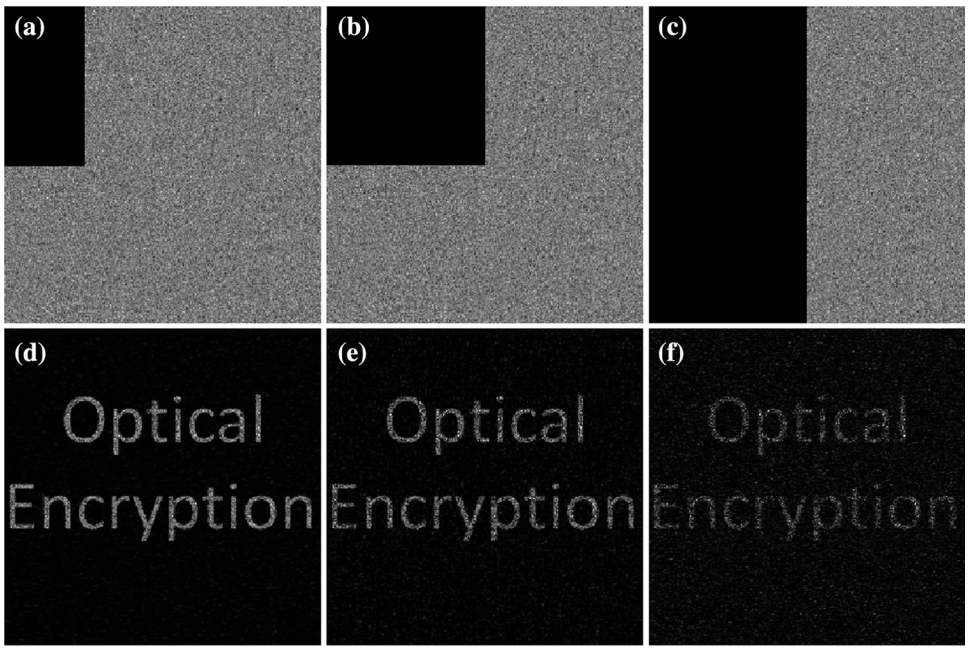

Fig. 7 Robustness against shear attacks. **a** Encrypted image with damaged 12.5%, **b** encrypted image with damaged 25%, **c** encrypted image with damaged 50%, **d** decrypted image from (**a**), **e** decrypted image from (**b**) and **f** decrypted image from (**c**)

attacks, such as brute-force attack, statistical attack, noise attack and shear attack. In addition, the proposed encryption scheme does not use any phase keys in the encryption and decryption process, which is convenient for the transmission and management of secret keys. Numerical simulations illustrate the feasibility and effectiveness of the proposed encryption scheme.

Acknowledgements This study was supported by the National Natural Science Foundation of China (Nos. 61177007 and 11472070).

References

1. Refregier P, Javidi B (1995) Optical image encryption based on input plane and Fourier plane random encoding. Opt Lett 20:767–769
2. Gong LB, Liu XB, Zheng F et al (2013) Flexible multiple-image encryption algorithm based on log-polar transform and double random phase encoding technique. J Mod Opt 60:1074–1082
3. Situ G, Zhang J (2004) Double random-phase encoding in the Fresnel domain. Opt Lett 29:1584–1586
4. Amaya D, Tebaldi M, Torroba R et al (2008) Multichanneled encryption via a joint transform correlator architecture. Appl Opt 47:5903–5907
5. Tajahuerce E, Matoba O, Verrall SC et al (2000) Optoelectronic information encryption with phase-shifting interferometry. Appl Opt 39:2313–2320
6. Jeon SH, Gil SK (2011) 2-step phase-shifting digital holographic optical encryption and error analysis. J Opt Soc Korea 15:244–251
7. Li XY, Tang C, Zhu XJ et al (2015) Image/video encryption using single shot digital holography. Opt Commun 342:218–223
8. Cho M, Javidi B (2013) Three-dimensional photon counting double-random-phase encryption. Opt Lett 38:3198–3201
9. Zhou NR, Zhang AD, Zheng F et al (2014) Novel image compression-encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing. Opt Laser Technol 62:152–160
10. Zhou NR, Li HL, Wang D et al (2015) Image compression and encryption scheme based on 2D compressive sensing and fractional Mellin transform. Opt Commun 343:10–21
11. Khare K, Samsheer Ali PT, Joseph J (2013) Single shot high resolution digital holography. Opt Express 21:2581–2591
12. Kocarev L (2002) Chaos-based cryptography: a brief overview. IEEE Circuits Syst Mag 1:6–21
13. Singh N, Sinha A (2008) Optical image encryption using fractional Fourier transform and chaos. Opt Lasers Eng 46:117–123
14. Sui LS, Duan KK, Liang JL (2015) Double-image encryption based on discrete multiple-parameter fractional angular transform and two-coupled logistic maps. Opt Commun 343:140–149
15. Arroyo D, Rhouma R, Alvarez G et al (2008) On the security of a new image encryption scheme based on chaotic map lattices. Chaos 18:033112
16. Wang B, Wei XP, Zhang Q (2013) Cryptanalysis of an image cryptosystem based on logistic map. Optik 124:1773–1776
17. He D, He C, Jiang LG et al (2001) Chaotic characteristics of a one-dimensional iterative map with infinite collapses. IEEE Trans Circuits Syst I Fundam Theory Appl 48:900–906
18. Liao XF, Li XM, Pen J et al (2004) A digital secure image communication scheme based on the chaotic Chebyshev map. Int J Commun Syst 17:437–445