An encryption scheme based on phase-shifting digital holography and amplitude-phase disturbance*

Hua Li-Li(花丽丽)[a], Xu Ning(徐 宁)[a]†, and Yang Geng(杨 庚)[b]

[a] College of Opto-Electronic Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210046, China
[b] College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210046, China

(Received 12 August 2013; revised manuscript received 30 October 2013; published online 10 April 2014)

In this paper, we propose an encryption scheme based on phase-shifting digital interferometry. According to the original system framework, we add a random amplitude mask and replace the Fourier transform by the Fresnel transform. We develop a mathematical model and give a discrete formula based on the scheme, which makes it easy to implement the scheme in computer programming. The experimental results show that the improved system has a better performance in security than the original encryption method. Moreover, it demonstrates a good capability of anti-noise and anti-shear robustness.

Keywords: optical encryption, phase-shifting holography, security, robustness

PACS: 42.30.–d, 42.15.Eq, 42.40.–i, 42.87.Bg **DOI:** 10.1088/1674-1056/23/6/064201

1. Introduction

The optical encryption technique has attracted more and more attention in recent years because of its superiority compared with traditional electronic encryption mechanism. When dealing with massive information, an electronic information system is inferior to an optical information system in the capability of parallel signal processing.[1–3] Besides, in the processing of data encryption and information hiding, the optical parameters such as wavelength, focal length, amplitude, intensity, phase, polarization state, spatial frequency, and the parameters of the optical element can be encoded by light interference, diffraction, filtering, imaging, and holography. Compared with the traditional computer cryptography and information security technology based on mathematics, optical information security has many advantages, such as multi-dimensions, a large capacity, high robustness, and an inherent nature of parallel processing.

The double random phase encryption method[4–6] proposed by Refregier and Javidi has opened new fields in optical information processing. In this encryption method, an input amplitude image is transformed into a white-noise-like image by disturbing the phase of the image to be encrypted randomly in the spatial and frequency domain by two random phase masks located in the input and the Fourier planes of the 4-f system. Many variations of this system have been introduced, including an encryption system based on the fractional Fourier transform[7–9] and a system in which the phase mask in the Fresnel domain is used.[10] However, the digital format of encrypted image data are plural in these systems. In order to solve this problem in the encryption systems based on a double random phase, Yamaguchi and Zhang[11] proposed a system based on a random phase and phase-shifting digital holography.

In Tajahuerce's scheme,[12,13] a technique of digital holography is used in optical encryption. It takes the focal length of the lens as a secret key and uses a random phase mask to disturb the plaintext. However, these processes have no influence in decrypting ciphertext; therefore, they have no effect on the security of the scheme. In this paper, the original system is improved by replacing the Fourier transform with the Fresnel transform and adding a random amplitude mask. The improvement increases the dimension of the key space and enhances the security of the system. The experimental results demonstrate a good performance of the scheme in terms of security and robustness.

2. An encryption system based on random amplitude-phase and phase-shifting digital holography

This section focuses on a detailed description of the proposed encryption system. The basic encryption scheme is depicted in Fig. 1. Conceptually, it is a Mach–Zender interferometer, with a plaintext image in one arm (denoted by arm 1 in Fig. 1) and a reference wave in the other arm (denoted by arm 2 in Fig. 1). Obviously, if the lens in arm 1 in the system is removed, the secret key is changed from the focal length of lens to the Fresnel diffraction distance. On the other hand, a random amplitude mask is inserted between the plaintext and the original random phase mask, making the distance between the random amplitude mask and the random phase mask z_3.

*Project supported by the National Basic Research Program of China (Grant No. 2011CB302903), the National Natural Science Foundation of China (Grant Nos. 61272084 and 61202004), and the Key Project of Natural Science Research of Jiangsu University, China (Grant No. 11KJA520002).

†Corresponding author. E-mail: xuning@njupt.edu.cn

© 2014 Chinese Physical Society and IOP Publishing Ltd

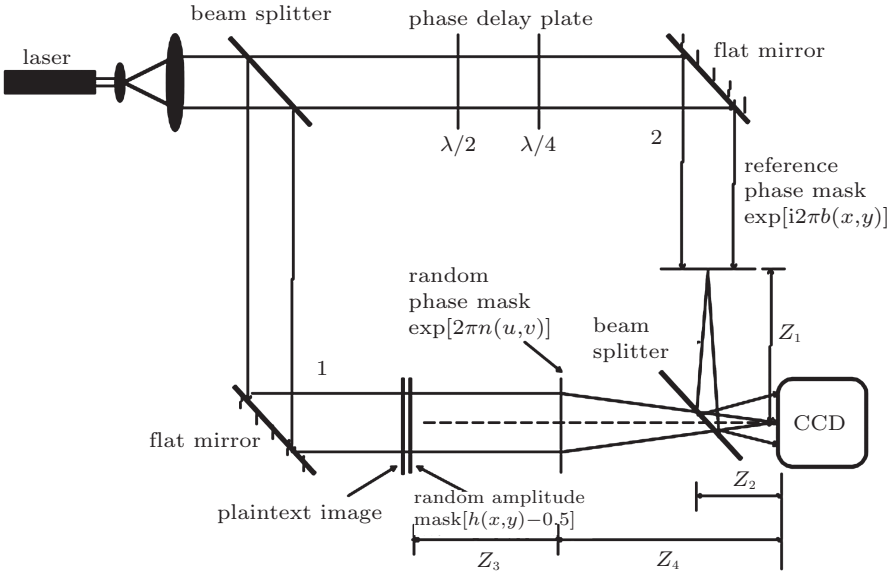


Fig. 1. Improved system.

In arm 2, we keep the original components, two phase delay plates, to generate phase delays of $\pi/2$ and π respectively. The different combinations of phase delays make the phase differences between the reference wave and the object wave 0, $-\pi/2$, $-\pi$, and $-3\pi/2$ to form phase-shifting interference fringes on the output plane. The encrypted optical signal is received by the CCD and converted into an electrical signal. The obtained digital holographic image can be digitally processed and transmitted through a communication link.

The system in Fig. 1 can be implemented by a real optical system. Fortunately, it can also be achieved by a virtual optical system, which contains only computer programs. In order to establish the virtual optical system, we must set up a mathematical model of the optical system and discrete the model in a programmable form.

2.1. Mathematical model

Suppose that x and y are the spatial domain coordinates, and u and v are the Fresnel domain coordinates. Let $f(x,y)$ denote the plaintext image, and let $\exp[\,\mathrm{j}2\pi n(u,v)]$ and $\exp[\mathrm{j}2\pi b(x,y)]$ represent the random phase mask placed in arm 1 and arm 2 respectively. Suppose that $[h(x,y)-0.5]$ is the random amplitude mask, where $n(u,v)$, $b(x,y)$, and $h(x,y)$ denote independent white sequences, which are uniformly distributed in the interval [0,1] respectively.

By using the Fresnel diffraction formula, the complex amplitude distribution of an object wave on the CCD plane can be expressed as follows:

$$\begin{aligned} U_{\mathrm{O}}(u,v) &= \frac{\exp(\mathrm{i}2\pi z_4/\lambda)}{\mathrm{i}\lambda z_4}\exp\left[\mathrm{i}\frac{\pi}{\lambda z_4}\left(u^2+v^2\right)\right] \\ &\times \iint_{-\infty}^{\infty} U_{\mathrm{f}}\left(u',v'\right)\exp\left[\frac{\pi}{\lambda z_4}\left(u'^2+v'^2\right)\right] \\ &\times \exp\left[-\mathrm{i}\frac{2\pi}{\lambda z_4}\left(uu'+vv'\right)\right]\mathrm{d}u'\,\mathrm{d}v', \end{aligned} \tag{1}$$

where

$$\begin{aligned} &U_{\mathrm{f}}\left(u',v'\right) \\ &= \exp\left[\mathrm{i}2\pi n\left(u',v'\right)\right]\frac{\exp(\mathrm{i}2\pi z_3/\lambda)}{\mathrm{i}\lambda z_3}\exp\left[\mathrm{i}\frac{\pi}{\lambda z_3}\left(u'^2+v'^2\right)\right] \\ &\times \iint_{-\infty}^{\infty} f(x,y)\times[h(x,y)-0.5]\exp\left[\frac{\pi}{\lambda z_3}\left(x^2+y^2\right)\right] \\ &\times \exp\left[-\mathrm{i}\frac{2\pi}{\lambda z_3}\left(xu'+yv'\right)\right]\mathrm{d}x\mathrm{d}y. \end{aligned} \tag{2}$$

The distance between the reference phase mask and the CCD in arm 2 is $z=z_1+z_2$, the complex amplitude distribution of the reference wave on the CCD plane is

$$\begin{aligned} U_{\mathrm{R}}(u,v;\alpha) &= \exp(\mathrm{i}\alpha)\frac{\exp(\mathrm{i}2\pi z/\lambda)}{\mathrm{i}\lambda z}\exp\left[\mathrm{i}\frac{\pi}{\lambda z}\left(u^2+v^2\right)\right] \\ &\times \iint_{-\infty}^{\infty}\exp[\mathrm{i}2\pi b(x,y)]\exp\left[\frac{\pi}{\lambda z}\left(x^2+y^2\right)\right] \\ &\times \exp\left[-\mathrm{i}\frac{2\pi}{\lambda z}(xu+yv)\right]\mathrm{d}x\mathrm{d}y, \end{aligned} \tag{3}$$

where α is controlled by two phase delay plates.

In the encryption process, the complex amplitude distribution of the object wave on the CCD is denoted by the function $U_{\mathrm{O}}(x,y)=A_{\mathrm{O}}\exp[\mathrm{i}\phi_{\mathrm{O}}(x,y)]$, and the complex amplitude distribution of the reference wave on the CCD is represented by the function $U_{\mathrm{R}}(x,y;\alpha)=A_{\mathrm{R}}\exp\{\mathrm{i}[\phi_{\mathrm{R}}(x,y)+\alpha]\}$. Then the intensity distribution on the CCD is

$$\begin{aligned} I(x,y;\alpha) &= |U_{\mathrm{O}}(x,y)+U_{\mathrm{R}}(x,y)|^2 \\ &= |U_{\mathrm{O}}(x,y)|^2+|U_{\mathrm{R}}(x,y)|^2 \\ &\quad + U_{\mathrm{O}}^*(x,y)U_{\mathrm{R}}(x,y)+U_{\mathrm{O}}(x,y)U_{\mathrm{R}}^*(x,y) \\ &= [A_{\mathrm{O}}(x,y)]^2+[A_{\mathrm{R}}(x,y)]^2+2A_{\mathrm{O}}(x,y)\times A_{\mathrm{R}}(x,y) \\ &\quad \times\cos[\phi_{\mathrm{O}}(x,y)-\phi_{\mathrm{R}}(x,y)-\alpha]. \end{aligned} \tag{4}$$

Based on the above algorithm, the phase of ciphertext can be expressed as follows:

$$\begin{aligned}\phi_{\mathrm{E}}(x,y) &= \phi_{\mathrm{O}}(x,y)-\phi_{\mathrm{R}}(x,y)\\ &= \arctan\left[\frac{I(x,y;-3\pi/2)-I(x,y;-\pi/2)}{I(x,y;0)-I(x,y;-\pi)}\right].\end{aligned} \quad (5)$$

The amplitude is

$$A_{\mathrm{E}}(x,y)=A_{\mathrm{O}}(x,y)A_{\mathrm{R}}(x,y)=\frac{1}{4}\frac{I(x,y;0)-I(x,y;-\pi)}{\cos\left[\phi_{\mathrm{O}}(x,y)-\phi_{\mathrm{R}}(x,y)\right]}. \quad (6)$$

The flow chart of encryption is shown in Fig. 2.

In the decrypting process, we remove the plaintext image, random amplitude mask, and random phase mask in arm 1 first. Then we obtain the amplitude $A_{\mathrm{R}}(x,y)$ and phase $\Phi_{\mathrm{R}}(x,y)$ of the reference wave on the CCD plane by a phase-shifting interference technique. By using the formulas (5) and (6), the amplitude and phase of the object light wave on the CCD plane are obtained. Finally, the decrypted information can be achieved by performing Fresnel inverse transform twice with the combination of random phase mask and random amplitude mask.

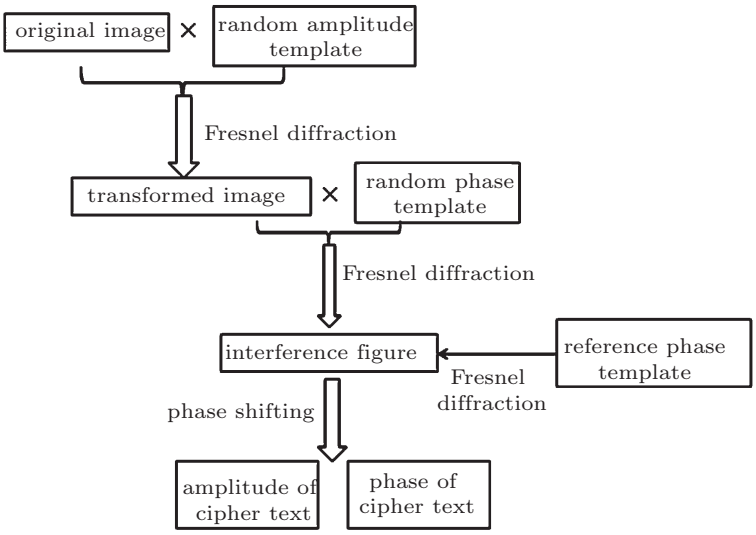


Fig. 2. Flow chart of encryption.

2.2. Discreted model

In order to implement the encryption and decryption process mentioned above in a programmable form, $f(x,y)$ and $\exp[\mathrm{j}2\pi b(x,y)]$ are sampled in $N\times N$ grids. The sampling intervals along the x and y axes are Δx and Δy respectively, then x and y can be replaced by $k\Delta x$ and $l\Delta y$, where k and l are integers ranging from 1 to N. Similarly, u and v can be replaced by $m\Delta u$ and $n\Delta v$. Therefore, the discrete variables and functions can be represented by the following formulas:

$$\begin{aligned}&x=k\Delta x,\ \ y=l\Delta y,\ \ k,l=1,2,\ldots,N,\\ &u=m\Delta u,\ \ v=n\Delta v,\ \ m,n=1,2,\ldots,N,\\ &f_x=m\Delta f_x=m\frac{\Delta u}{\lambda z},\ \ f_y=n\Delta f_y=n\frac{\Delta v}{\lambda z},\ \ m,n=1,2,\ldots,N.\end{aligned} \quad (7)$$

According to the Shannon theorem, we have

$$\Delta x=\frac{1}{N\Delta f_x}=\frac{\lambda z}{N\Delta u},\ \ \Delta y=\frac{1}{N\Delta f_y}=\frac{\lambda z}{N\Delta v}. \quad (8)$$

The discrete Fresnel diffraction (DFD) can be obtained according to Eqs. (7) and (8). The DFD of a two-dimensional information plane $U(k,l)$ can be expressed as follows:

$$\begin{aligned}&U'(m,n)\\ &=\mathrm{DFD}\left[U(k,l);\lambda,d\right]\\ &=\frac{\exp(\mathrm{j}2\pi d/\lambda)}{\mathrm{j}\lambda d}\exp\left[\mathrm{j}\frac{\pi}{\lambda d}\left(m^2\Delta u^2+n^2\Delta v^2\right)\right]\\ &\quad\times\sum_{k=1}^{N}\sum_{l=1}^{N}U(k,l)\exp\left[\mathrm{j}\frac{\pi}{\lambda d}\left(k^2\Delta x^2+l^2\Delta y^2\right)\right]\\ &\quad\times\exp\left[-\mathrm{j}2\pi\left(\frac{km}{N}+\frac{ln}{N}\right)\right]\\ &=\frac{\exp(\mathrm{j}2\pi d/\lambda)}{\mathrm{j}\lambda d}\exp\left[\mathrm{j}\frac{\pi}{\lambda d}\left(m^2\Delta u^2+n^2\Delta v^2\right)\right]\\ &\quad\times\mathrm{DFT}\left\{U(k,l)\exp\left[\mathrm{j}\frac{\pi}{\lambda d}\left(k^2\Delta x^2+l^2\Delta y^2\right)\right]\right\}.\end{aligned} \quad (9)$$

In Eq. (9), DFT[·] denotes the operation of discrete Fourier transform.

The detailed implementation of the DFD algorithm is shown in Fig. 3.

The intermediate variables in Fig. 3 are described by:

$$\alpha_1=\frac{\pi}{\lambda d}\left(k^2\Delta x^2+l^2\Delta y^2\right),\ \ \alpha_2=\frac{\pi}{\lambda d}\left(m^2\Delta u^2+n^2\Delta v^2\right).$$

By taking $U(k,l)=f(k,l)\times[h(k,l)-0.5]$ and $d=z_3$ in the algorithm in Fig. 3, we obtain the discrete result $U_{\mathrm{f}}(m,n)$ of formula (2). Similarly, we can obtain the discrete result $U_{\mathrm{O}}(m,n)$ of the formula (1) by taking $U(k,l)=U_{\mathrm{f}}(k,l)\times \mathrm{e}^{\mathrm{j}2\pi n(k,l)}$ and $d=z_4$. Finally, we have the discrete result $U_{\mathrm{R}}(m,n)$ of formula (3) when $U(k,l)=\mathrm{e}^{\mathrm{j}2\pi b(k,l)}$ and $d=z=z_1+z_2$. With the obtained $U_{\mathrm{O}}(m,n)$ and $U_{\mathrm{R}}(m,n)$, according to

the discrete formulas (4)–(6), the ciphertext can be obtained, where the plaintext is $f(k,l)$. The decrypting is a reverse process.

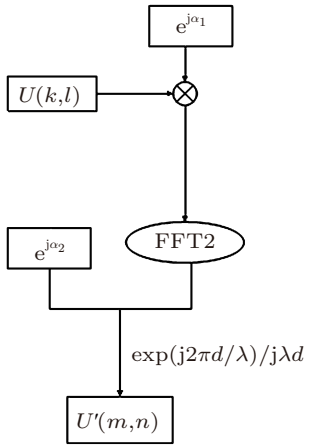


Fig. 3. Flow chart of the DFD algorithm implementing.

3. Experimental results and analysis

3.1. Security analysis

We analyze the security of the proposed system by testing a gray-scale picture (Lena's picture) with 512×512 pixels. Simulation is implemented with the Matlab tool for the proposed encryption system based on random amplitude-phase and phase-shifting digital holography. The parameters are $\lambda = 632.8$ nm, $z_1 + z_2 = 1000$ mm, $z_3 = 1200$ mm, and $z_4 = 1400$ mm. The experimental results are shown in Fig. 4.

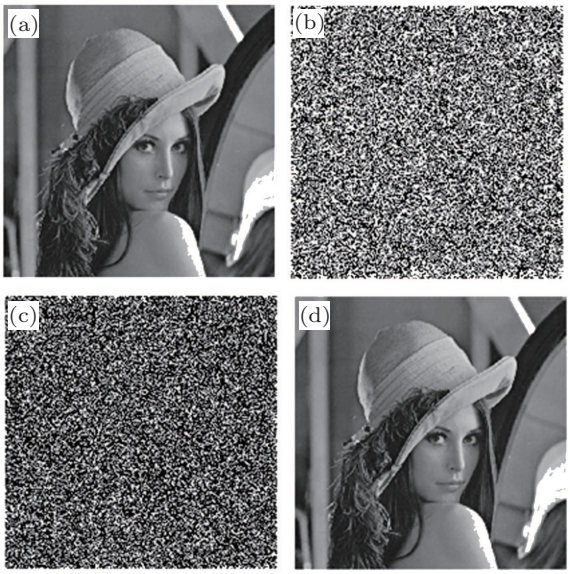


Fig. 4. Experimental results using the proposed scheme, showing (a) the original image, (b) the amplitude of the cipher text, (c) the phase of the cipher text, and (d) the decrypted image.

In order to evaluate the result of the decrypted image theoretically, we define the mean square error (MSE) as a standard to measure the difference in pixel value between the decrypted image and the original image (we assume 4 bits to be used as the calculation precision in the simulation):

$$\mathrm{MSE} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} |f(x,y) - f_{\mathrm{D}}(x,y)|^2 . \tag{10}$$

Here, $f(x,y)$ denotes the plaintext image, $f_{\mathrm{D}}(x,y)$ the decrypted image, and $M \times N$ the number of pixels of the image. Functions $f(x,y)$ and $f_{\mathrm{D}}(x,y)$ are normalized. According to formula (10) and the results in Fig. 4, the MSE value is 0.

To verify the security of the keys in the improved system, we evaluate first the quality of decryption result with the value of MSE when one of the four keys, i.e., the wavelength of light and three diffraction distances has a deviation. Figure 5 shows the curves of MSE for Lena image.

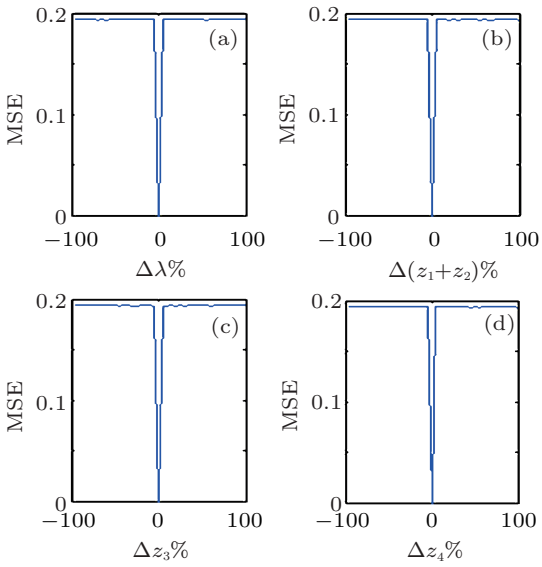


Fig. 5. (color online) Curves of MSE of decryption results with the original image when there is deviation in the decryption keys. (a) MSE∼λ%, (b) MSE∼(z_1+z_2)%, (c) MSE∼z_3%, and (d) MSE∼z_4%.

Figure 5 shows that MSE tends to 0.1950 with the increase of the deviation. Compared with the original system, the focal length of the lens in the original system is actually replaced with z_4 in the improved system. Figure 6 shows that the MSE value keeps 0 (in fact, it is about 10^{-26}) when the offset of the focal length changes from 0 to 100%. The result demonstrates a great change compared with that in Fig. 5(d). This implies that the change of key from the focal length of the lens to the Fresnel diffraction distance provides us with a lot of key adjusting flexibility and also enhances the security of the system.

Moreover, if the offset of the focal length of the lens in the original system and z_4 in the proposed system are both about 1%, the corresponding values of MSE are 0 and 0.1939 respectively. The experimental results are shown in Fig. 7, indicating that the three diffraction distances and the wavelength play an important role in security in the encryption process.

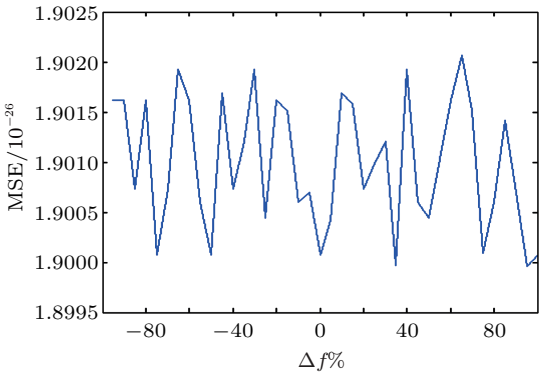


Fig. 6. (color online) MSE∼f%.

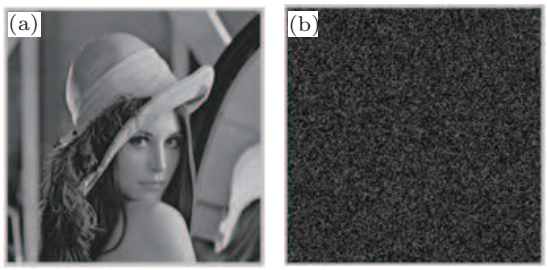


Fig. 7. Comparison of decryption result between (a) when $\Delta f = 1\%$ and (b) when $\Delta z_4 = 1\%$.

On the other hand, we analyze the influences of two phase masks and one amplitude mask on security respectively. The experimental results are shown in Fig. 8. They imply that the decrypting cannot be successful if only one random mask is wrong. The result is random white noise.

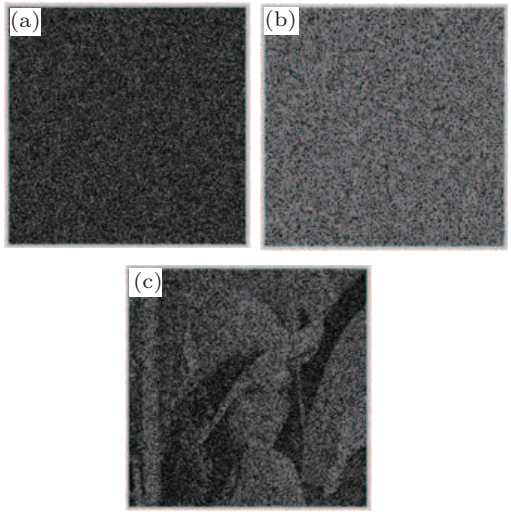


Fig. 8. Decryption results when (a) the random phase mask in arm 1 is wrong and MSE = 0.1940; (b) the random phase mask in arm 2 is wrong and MSE = 0.1937; (c) the random amplitude mask in arm 1 is wrong and MSE = 0.1927.

However, in Tajahuerce's scheme, the plaintext can be obtained even without the random phase mask corresponding to it, because the pixel value of the image to be encrypted is real. Let $f(x,y)$ and $\exp[\mathrm{j}\varphi(x,y)]$ denote the plaintext image and the random phase mask respectively. In the decrypting process, the amplitude and phase of object light waves are obtained. Then we have $f(x,y)\exp[\mathrm{j}\varphi(x,y)]$ after a Fourier inverse transform. By using the CCD we can obtain the intensity of the plaintext $|f(x,y)|^2$. Figure 9 shows the encryption result without the random phase mask corresponding to the plaintext in the traditional system, the MSE value is 0.

The above simulation and analysis show that each secret key in the proposed system plays a crucial role in the encrypting and decrypting processes. The decryption cannot be performed correctly with any change of secret keys. So the security of the system has been greatly improved and guaranteed.



Fig. 9. Encryption result without the random phase mask bonded to the plaintext in the traditional system.

3.2. Robustness analysis

3.2.1. Capability of anti-noise

We add Gaussian white noise and Rayleigh noise in the ciphertext separately. The mean and variance of Gaussian white noise are 0 and 0.05, and the parameter of Rayleigh noise is 0.1. The decryption results are shown in Fig. 10. The values of MSE are 0.1848 and 0.1644 in Figs. 10(a) and 10(b), respectively, demonstrating that the proposed system has a strong robustness in anti-noise.

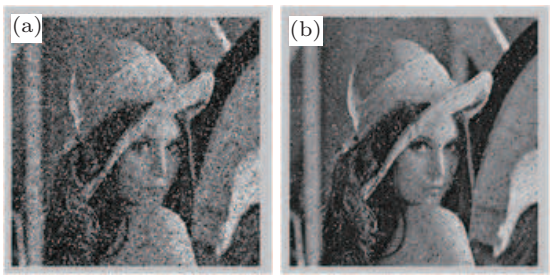


Fig. 10. Decryption results with (a) Gaussian and (b) Rayleigh noise attack.

3.2.2. Capability of anti-cipher text damage

A ciphertext is cut off 25% in both amplitude and phase, which are shown in Figs. 11(a) and 11(b) respectively. The value of MSE is 0.1922. In order to evaluate the performance of the proposed scheme quantitatively, figure 12 shows the curve of MSE changing with the cipher text shear-rate. The result shows that the proposed system also has a capability of anti-shear robustness.

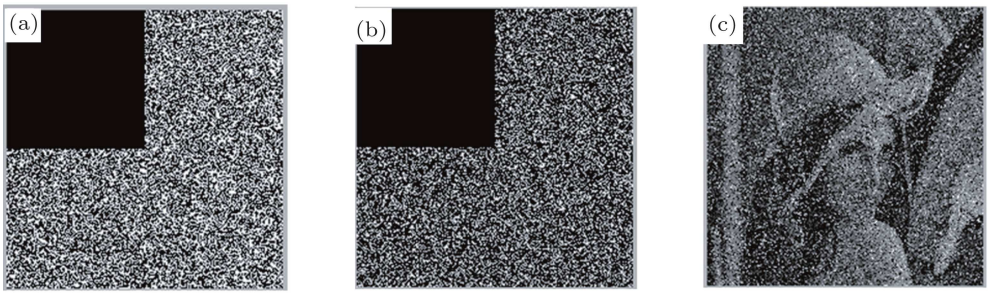


Fig. 11. Cutting 25% of amplitude (a) and phase (b) of cipher text and (c) decrypted image.

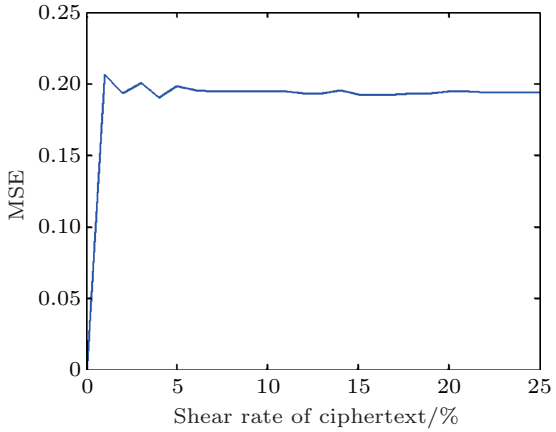


Fig. 12. (color online) MSE changing with cipher text shear-rate.

4. Conclusion

In this paper, we proposed a novel encryption scheme based on random phase and phase-shifting digital holography. In the scheme, the phase of disturbance used in Tajahuerce's scheme is retained and a random amplitude mask to encode the amplitude of the plaintext is added. Moreover, in the scheme, the Fourier transform is replaced by the Fresnel transform. These modifications not only increase the dimension of the key space, but also enhance the security of the system. Experimental results show that the security of the proposed system is raised and the system has a certain performance in anti-noise and anti-shear robustness.

References

[1] Javidi B 1997 *Phys. Today* **50** 27
[2] Xu N, Chen X L and Yang G 2013 *Acta Phys. Sin.* **62** 084202 (in Chinese)
[3] Zhao T Y, Liu Q X and Yu F H 2012 *Chin. Phys. B* **21** 064203
[4] Matoba O, Nomura T and Perez-Cabre E, *et al.* 2009 *Proc. IEEE* **97** 1128
[5] Zhu Y C, Zhang J S and Gong Q H 2008 *Chin. Phys. Lett.* **25** 2037
[6] Refregier P and Javidi B 1995 *Opt. Lett.* **20** 767
[7] Tao R, Lang J and Wang Y 2008 *Opt. Lett.* **33** 581
[8] Hennelly B and Sheridan J T 2003 *Opt. Lett.* **28** 269
[9] Jia L and Liu Z 2009 *Acta Photon. Sin.* **38** 1020 (in Chinese)
[10] Situ G and Zhang J 2004 *Opt. Lett.* **29** 1584
[11] Yamaguchi I and Zhang T 1997 *Opt. Lett.* **22** 1268
[12] Tajahuerce E, Matoba O, Verrall S and Javidi B 2000 *Appl. Opt.* **39** 2313
[13] Javidi B and Nomura T 2000 *Opt. Lett.* **25** 28