Optics Communications 297 (2013) 32–37

Contents lists available at SciVerse ScienceDirect

Optics Communications

journal homepage: www.elsevier.com/locate/optcom

Double images hiding by using joint transform correlator architecture adopting two-step phase-shifting digital holography

Xiaoyan Shi [a,b], Daomu Zhao [a,*], Yinbo Huang [c]

[a] Department of Physics, Zhejiang University, Hangzhou 310027, China
[b] College of Science, Hangzhou Dianzi University, Hangzhou 310018, China
[c] Key Laboratory of Atmospheric Composition and Optical Radiation, Chinese Academy of Sciences, Hefei 230031, China

ARTICLE INFO

Article history:
Received 29 November 2012
Received in revised form
10 January 2013
Accepted 30 January 2013
Available online 22 February 2013

Keywords:
Joint transform correlator (JTC) architecture
Two-step phase-shifting digital holography
Image hiding

ABSTRACT

Based on the joint Fresnel transform correlator, a new system for double images hiding is presented. By this security system, the dual secret images are encrypted and recorded as intensity patterns employing phase-shifting interference technology. To improve the system security, a dual images hiding method is used. By digital means, the deduced encryption complex distribution is divided into two subparts. For each image, only one subpart is reserved and modulated by a phase factor. Then these modified results are combined together and embedded into the host image. With all correct keys, by inverse Fresnel transform, the secret images can be extracted. By the phase modulation, the cross talk caused by images superposition can be reduced for their spatial parallel separation. Theoretical analyses have shown the system's feasibility. Computer simulations are performed to show the encryption capacity of the proposed system. Numerical results are presented to verify the validity and the efficiency of the proposed method.

1. Introduction

Nowadays, with the widespread of the internet and digital technology, searching efficient ways to protect information from illegal copying and unauthorized distribution are still challenging problems even with the most advanced technology and architecture. The optical encryption and security systems have been proposed and become the important issues in this domain for their properties of high speed and parallelism. Besides these advantages, they also provide a large degree of freedom for information security. In 1990s, Refregier and Javidi [1,2] proposed the optical image encryption system based on double random phase encoding (DRPE) method to transform an input image into a stationary white noise. Based on this DRPE system, encryption in transform domain [3,4], encryption and image hiding exploiting digital holography [5–11], multiple-image encryption and hiding [12–14], etc. have also been proposed. For the DRPE system, however, owing to the facts that conjugate phase and an accurate alignment should be made for decryption [1–4], so optical security solution based on JTC architecture is proposed [15]. Unlike the traditional DRPE system, no accurate alignment and no conjugate phase are demanded in this JTC system [15]. The real and nonnegative encoded result was recorded by the charge-couple device (CCD). And it is widely used for the real time processing for its high efficiency. In recent years, various kinds of security system based on the JTC architecture have been proposed [16–21]. Modified JTC system combing three-step phase-shifting interference technology was also proposed [21]. By this improved technology, noises caused by the zero and conjugate items can be eliminated by digital means in the output plane. This system is more compact and flexible for its lensless when comparing with the transitional one.

In this paper we realized the images hiding adopting two-step phase-shifting in the joint Fresnel transform correlator architecture. By this security system, double binary images are encrypted. For each image, by the phase-shifting technique, it is encrypted into two interference patterns which can be recorded by the CCD. By a digital operation, the encoded complex information is deduced from the recorded intensity patterns as discussed above. By the phase-shifting technology, better recovering quality can be obtained for its zeros-order and diffraction noises are eliminated. To further improve the system security, a digital division and combination operation is employed. By the division operation, each of the encrypted complex distributions deduced from interference intensities is then divided into two subparts. For each image, only one encrypted subpart is reserved and the other is set to be zero. Then the two reserved subparts are modulated by the phase factors and combined together. In the end, the final combined result containing double secret images obtained by digital processing is embedded into the host image. The watermarked host can be transmitted via

* Corresponding author. Tel.: +86 571 888 63887; fax: +86 571 87951328.
E-mail address: zhaodaomu@yahoo.com (D. Zhao).

0030-4018/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.optcom.2013.01.072

public channel with no one noticing the hiding information. Then by an inverse Fresnel transform, double secret images can be extracted. By the proposed method, the cross talk caused by image superposition can be reduced by the spatial parallel separation for their phase modulations. The extracted hiding images and the noise caused by the host image are recovered spatial separately in the output plane.

Compared to the previous multi-step system [21], less intensity patterns were recorded in our system and the information capacity was reduced. The modified JTC architecture allows for a more compact, versatile and security way to protect dates. For the attackers, it shows a disturbing way to extract the hiding information from the host image, for there's little difference between the original and watermarked host. Theoretical analyses have shown the system's feasibility. Computer simulations are performed to show the encryption capacity of the proposed system. Numerical results are presented to verify the validity and efficiency of our system.

The paper is organized as follows. In Section 2 the principle and realization of the proposed method of information encryption, hiding and decryption is presented theoretically in detail. To demonstrate our method, numerical simulations are presented in Section 3. Finally, conclusions are outlined in Section 4.

2. Theoretical analysis and implementing process

2.1. Encryption analysis based on the proposed method

Fig. 1(a) shows the optical schematic diagram of joint Fresnel transform correlator architecture, which is the modified JTC architecture we have used to encrypt and record the image to be hidden. As Fig. 1(a) shows, the interference patterns recording is realized in the Fresnel domain, for its lensless, it is more compact and simplified comparing with the traditional one [15]. The enhanced system based on the Fresnel JTC architecture, absorbing two-step phase-shifting technique, is similar to the prior one shown in [21]. As mentioned in the earlier work [21], the complex distribution, containing secret image and a random phase mask, is put side by side with the complex key mask in the input plane during the encryption stage. As is shown in Fig. 1(a),

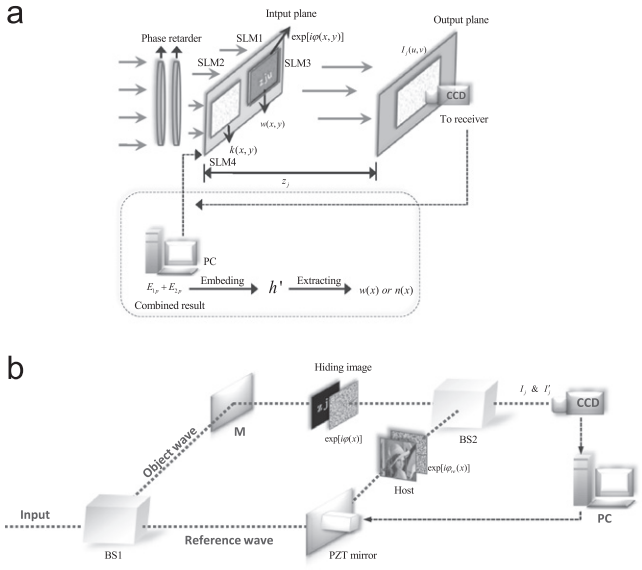

Fig. 1. Schematic of the proposed optical image security system (a) encryption and embedding process, (b) Mach–Zehnder interferometer architecture.

the phase of the reference beam can be changed when the parallel incident beam passes through the phase retarders with different phase shifting modulation. The key mask, wavelength and diffraction distance are all keys for decryption. By applying the phase-shifting technology, there are at least two interference patterns recorded by the CCD during the encryption procedure, and for decryption the key phase should also be recorded by the same way. These holograms are recorded and transferred via digital means. Post digital operation was used to get the encoded complex distribution of the original image. Thus by an inverse Fresnel transform with all correct keys, the decrypted complex distribution of the original image will be obtained. There's difference between our proposed system and the previous one [20] which will be introduced later.

In the following, the implementation details of the proposed method will be discussed. Let (x,y) and (u,v) denote coordinates at the input and transform plane. Double binary images $w(x,y)$ and $n(x,y)$ which will be encrypted and hidden are used as two input object waves, separately. $\varphi(x,y)$ and $\varphi_k(u,v)$ denote two independent white sequences uniformly distributed in $[0,2\pi]$. $\exp[i\varphi(x,y)]$ and $\exp[i\varphi_k(u,v)]$ are random phase masks used in the input and transform planes, respectively.

As is shown in Fig. 1(a), in the proposed system, random phase mask $\exp[i\varphi(x,y)]$ is attached to the real and positive object $w(x,y)$. This complex input is put side by side with the complex key distribution $k(x,y)$ defined by its Fresnel transform $K(u,v)=\exp[i\varphi_k(u,v)]$, which is used as the key code in this system. As is known, it is difficult to display complex-valued information on the SLM [15]. So both amplitude and phase SLMs should be used which are attached together to solve this problem. The optical operation can also be performed in a Mach–Zehnder interferometer architecture [15] as is shown in Fig. 1(b). In Fig. 1(b), the complex input $w(x,y)\cdot\exp[i\varphi(x,y)]$ is used as the object wave. In the input plane of the other optical path, the complex key $k(x,y)$, containing real positive host image "Lena" and a random phase mask $\exp[i\varphi_{re}(x,y)]$, is used as the reference wave. Let $W(u,v)$ be the diffraction distribution of the object wave, the complex diffraction distributions of the object and the reference waves in the CCD plane will be defined as

$$W(u,v)=FrT_{z_1}\{w(x,y)\cdot\exp[i\varphi(x,y)],\lambda_1\}=A_o\exp[i\varphi_o(u.v)] \tag{1}$$

$$\begin{aligned}K(u,v)&=FrT_{z_1}\{k(x,y),\lambda_1\}=FrT_{z_1}\{h(x,y)\times\exp[i\varphi_{re}(x,y)],\lambda_1\}\\&=\exp[i\varphi_k(u,v)]\end{aligned} \tag{2}$$

where $FrT_{z_1}\{\cdot\}$ denotes the Fresnel transform (FrT) over distance z_1 with wavelength λ_1. $h(x,y)$ represents the host image "Lena" which is defined as the amplitude of complex key $k(x,y)$. Pure phase distribution $\exp[i\varphi_{re}(x,y)]$, attached to $h(x,y)$ in the input plane, is obtained by use of the modified phase retrieval algorithm (PRA) [22] with $h(x,y)$ and the expected output $K(u,v)$ as the constraint conditions in the input and Fresnel diffraction plane by Fresnel transform over distance z_1 with wavelength λ_1. Let $K_1(u,v)$ and $K_2(u,v)$ be the Fresnel transform of the complex key code $k(x,y)$ with two phase shifts 0 and arbitrary value δ in $[0,\pi]$ introduced by the piezoelectric transducer (PZT) controlled mirror, respectively. The interference intensity patterns between an arbitrary input object $w(x,y)$ and reference beams for phase retarders 0 and δ can be written as I_j

$$I_j=\left|W(u,v)+K_j(u,v)\right|^2 \tag{3}$$

where j takes the value of 1 and 2 for phase retarders 0 and δ, respectively. Thus, from Eq. (3), we can obtain two intensity patterns I_1 and I_2, which are represented as

$$\begin{aligned}I_1&=\left|W(u,v)\right|^2+\left|K_1(u,v)\right|^2+2\times\left|W(u,v)\right|\left|K_1(u,v)\right|\cos(\varphi_o-\varphi_k)\\&=A_o^2+1+2A_o\cos(\varphi_o-\varphi_k)\end{aligned} \tag{4}$$

$$I_2 = |W(u,v)|^2 + |K_2(u,v)|^2 + 2 \times |W(u,v)||K_2(u,v)|\cos(\varphi_o - \varphi_k - \delta)$$
$$= A_o^2 + 1 + 2A_o\cos(\varphi_o - \varphi_k - \delta) \quad (5)$$

where it is assumed that $|K_j(u,v)|^2 = 1$, for it is a pure phase function. Thereafter applying the two-step phase shifting technique [11], the amplitude A_o and the phase $\varphi_e(u,v) = \varphi_o(u,v) - \varphi_k(u,v)$ can be calculated by a simple derivation from Eqs. (4) and (5). Denoting $\vartheta = A_o^2 + 1$, thus for input $w(x,y)$, the encrypted complex distribution can be written as [11]

$$E_1 = A_{ow}\exp[i\varphi_{ew}(u,v)]$$
$$= \frac{I_1 - \vartheta}{2} + i\frac{I_2 - I_1\cos\delta - (1-\cos\delta)\vartheta}{2\sin\delta} \quad (6)$$

where A_{ow} and $\varphi_{ew}(u,v) = \varphi_{ow}(u,v) - \varphi_k(u,v)$ represent, respectively, the encoded amplitude and phase distribution for the input $w(x,y)$. The subscript w is used to distinguish two encrypted results. The value of ϑ can be calculated from the following equation

$$\vartheta = \frac{-v - \sqrt{v^2 - 4uw}}{2u} \quad (7)$$

where

$$u = 2 - 2\cos\delta \quad (8a)$$

$$v = -u(I_1 + I_2) - 4\sin^2\delta \quad (8b)$$

$$w = I_1^2 + I_2^2 - 2I_1I_2\cos\delta + 4\sin^2\delta \quad (8c)$$

Substituting Eqs. (8) into (7), we can get the value of ϑ. And then substituting ϑ into Eq. (6), we can get the encrypted complex distribution for input $w(x,y)$. During the encryption procedure, random phase $K(u,v)$, Fresnel diffraction distance z_1 and wavelength λ_1 are all security keys. Note that it is impossible to recover the input image only by inverse Fresnel transform on the decrypted result E_1 in Eq. (6) unless one knows the phase distribution $\varphi_k(u,v)$ [11,23].

For the other binary image $n(x,y)$, the same encryption process can be done by the proposed method above. Normally, in order to reduce the information burden of the system, same encryption keys are usually used. However, different geometric key may be used in order to enhance the system security. Assuming that the encoding result of image $n(x,y)$ is given by E_2, it can be defined as

$$E_2 = A_{on}\exp[i\varphi_{en}(u,v)] \quad (9)$$

where A_{on} and $\varphi_{en}(u,v)$ represent, respectively, the amplitude and phase distribution of the encrypted complex distribution for image $n(x,y)$ which can be deduced from Eq. (6) by similar derivation used for $w(x,y)$. The subscript n is used to distinguish the encoded result for $n(x,y)$ from $w(x,y)$.

2.2. Decryption analysis based on the proposed method

Now, in this section, the decryption analysis is described. To decrypt the encrypted result shown in Eq. (6) and get the spatial distribution of the object, phase-shifting digital holography technique is performed here for recording the diffraction distribution of the key code. Note that the complex distribution $k(x,y)$ will be used as the object beam. By removing and replacing object $w(x,y) \times \exp[i\varphi(x,y)]$ with a constant diffraction complex values distribution $C(u,v)$ as the reference beam, we can represent the interference intensity patterns I_j' between the object and the reference beam for phase retarders 0 and δ as

$$I_j' = |C(u,v) + K_j(u,v)|^2 \quad (10)$$

where j takes the value of 1 and 2 for phase retarders 0 and δ, respectively. $C(u,v)$ is the complex distribution of the reference beam with the given constant amplitude A_c and phase $\varphi_c(u,v)$, respectively. From Eq. (10), we can obtain the intensity patterns I_1' and I_2', which are represented as

$$I_1' = A_c{}^2 + 1 + 2A_c\cos(\varphi_k - \varphi_c) \quad (11)$$

$$I_2' = A_c{}^2 + 1 + 2A_c\cos(\varphi_k - \varphi_c - \delta) \quad (12)$$

Thus by digital means we can deduce the key phase $K(u,v)$ from Eqs. (11) and (12). Performing digital calculation, the deduced result is given by

$$\cos(\varphi_k - \varphi_c) = \frac{I_1' - A_c{}^2 - 1}{2A_c} \quad (13)$$

$$\sin(\varphi_k - \varphi_c) = \frac{I_2' - I_1'\cos\delta - (1-\cos\delta)(A_c{}^2 + 1)}{2\sin\delta} \quad (14)$$

where φ_c is the constant phase which has no influence on the diffraction distribution. Let $\varphi_k{}' = \varphi_k - \varphi_c$, thus the encryption key code can be written as

$$R = \exp[i(\varphi_k - \varphi_c)] = \exp(i\varphi_k{}') \quad (15)$$

Then the reconstruction is carried out for any one of encryption images. For example, for input $w(x,y)$, the complex distribution of the original image in the input plane can be recovered by the following way

$$w(x,y) \times \exp[i\varphi(x,y)] = IFrT_{z_j}\{E_j \times R, \lambda_j\} = IFrT_{z_j}\{A_{ow}\exp[i\varphi_{ow}(u,v)], \lambda_i\} \quad (16)$$

where $IFrT_{z_j}\{\cdot\}$ denotes the inverse Fresnel transform (IFrT) over distance z_j for wavelength λ_j. j takes the value of 1 and 2, respectively, for the double secret images to be hidden. Since the phase distribution of the complex result can be removed by the intensity detective devices such as CCD camera, the constant phase factor φ_c can also be neglected in our discussion. Thus the intensity distribution of the image will be obtained. The reconstruction procedure can be done either by totally digital means or combining with optical means.

2.3. Embedding process

In order to improve the security of the system to confuse and resist the attack from the attackers, a double encrypted images hiding technique is further used. Same coordinate notation defined in Section 2.1 will be used here.

To achieve the double images embedding, the images division and combination operation exploiting digital means is introduced. Fig. 2 shows the principle of the double secret images embedding. Firstly, each of the encryption results E_1 and E_2 is divided into two subparts. In the following, as shown in Fig. 2, for the encrypted complex result E_1, maintaining the pixel values in the left subpart of the image unchanged, let the pixel values in the other subpart be replaced by zero. Meanwhile, another encrypted result E_2 is also divided into two subparts, let pixel values in the left subpart of E_2 be zero and maintain the other subpart unchanged. By this operation, two new complex distributions $E_1{}'$ and $E_2{}'$ which are called the subpart pixel-value modified images are derived.

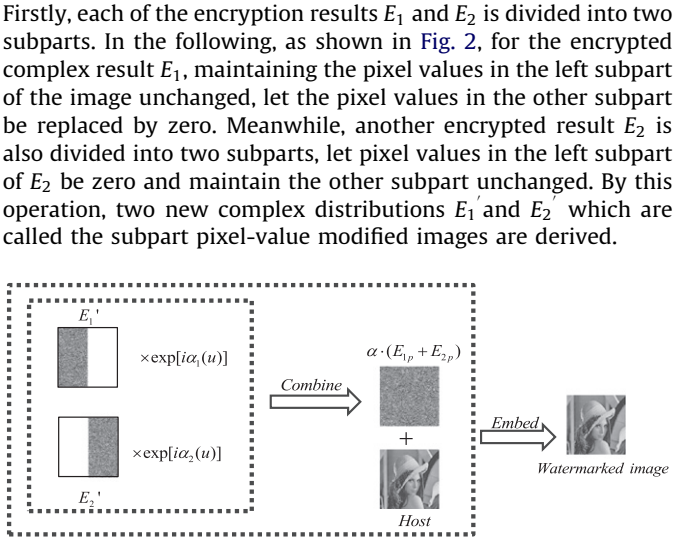

Fig. 2. Diagram of the proposed double images hiding procedure.

Further operation is introduced to reduce the cross talk caused by image embedding for multiple images superposition. As an improved method, we performed the operation of phase modulation on E_1' and E_2' just before the image combination. Under this condition, as is shown in Fig. 2, E_1' and E_2' are multiplied by the phase functions $\exp[i\alpha_1(u,v)]$ and $\exp[i\alpha_2(u,v)]$, respectively. The phase modulation process can be expressed as

$$E_{jp} = PM\left\{E_j'\right\} = E_j' \times \exp[i\alpha_j(u,v)] = E_j' \times \exp\left[i\frac{2\pi}{\lambda_j z_j}(x_j \times u + y_j \times v)\right] \quad (17)$$

where $PM\{\cdot\}$ represents the phase modulation operation. Coordinate (x_j,y_j) is the spatial shift distance of the recovered images in the output plane. j takes the value of 1 and 2 for E_1' and E_2', respectively. To realize the spatial separation between the extracted results, the coordinates (x_1,y_1) and (x_2,y_2) should be chosen carefully to avoid the images overlap. Using the displacement rule, phase modulation will result in spatial shifting which will help to reduce the cross talk caused by multiple images superposition.

Fig. 2 illustrates the combination and embedding procedure. As is shown in Fig. 2, the results E_{jp} obtained by Eq. (17) will be combined together and be embedded in the host image "Lena" with proper weighting factor α. This procedure can be expressed as

$$h' = h + \alpha \times (E_{1p} + E_{2p}) \quad (18)$$

where α is an arbitrary constant, which is chosen varying between $[0 \sim 1]$ to ensure the invisibility and robustness of the embedded image. The watermarked image embedded with noise like information will be transmitted via public channel.

As the phase key has been recorded in Section 2.1 above, knowing the geometric parameters, the double secret images decryption (extraction) process will be easily performed. By Eq. (16) the extraction procedure will be generated as

$$IFrT_{z_j}\{h' \times R,\lambda_j\} = IFrT_{z_j}\{h \times R,\lambda_j\} + IFrT_{z_j}\{E_1' \times \exp[i\alpha_1(u,v)] \times R,\lambda_j\} + IFrT_{z_j}\{E_2' \times \exp[i\alpha_2(u,v)] \times R,\lambda_j\} \quad (19)$$

There are mainly three parts in the right side of the Eq. (19) which are spatially separated in the output plane. The first noise like item is at the coordinate $x = y = 0$. The second and the third terms are two extracted images, which are spatially separated when all right keys are used. Their center positions depend on the coordinates (x_1,y_1) and (x_2,y_2). The extraction procedure is shown in Fig. 3.

3. Numerical simulation

We now give some numerical simulation results in this section to verify the validity of the proposed method. In our simulation, the original double images chosen to be encrypted are the binary "zju" and "OPT", which have size of 128×128 pixels as shown in Fig. 4(a) and (b). Fig. 4(c) and (d) are the key phase masks

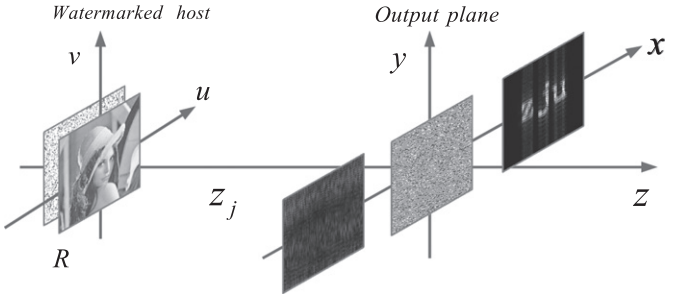

Fig. 3. Extraction sketch for double secret images.

$\exp[i\varphi(x,y)]$ and $\exp[i\varphi_{re}(x,y)]$. The size of the phases is same as that of the original image shown in Fig. 4(a) and (b). The transform parameters used for the double binary images shown in Fig. 4(a) and (b) are $\lambda_1 = 540$ nm, $z_1 = 40$ mm and $\lambda_2 = 600$ nm, $z_2 = 50$ mm, respectively. The phase shift value is $\delta = \pi/8$. Fig. 4(e) shows the amplitude and phase distributions of the final encrypted result derived from Eq. (6) by the two intensities shown in Eqs. (4) and (5) for the original image "zju", respectively. Similar result is shown in Fig. 4(f) for the other binary image "OPT".

Fig. 5(a) shows the original host image "Lena" (gray image with 128×128 pixels). In order to decrypt the original image, holography technology is used to record the key phase information. Fig. 5(b) shows one of the interference patterns of the key phase $K(u,v)$ recorded by the CCD derived from Eq. (10) which is convenient to be recoded and transmitted via digital means. Fig. 5(c) gives the amplitude and phase distributions of the combined phase modulated result $E_{1p} + E_{2p}$. As an embedding result, the watermarked host with weighting factor $\alpha = 0.01$ is

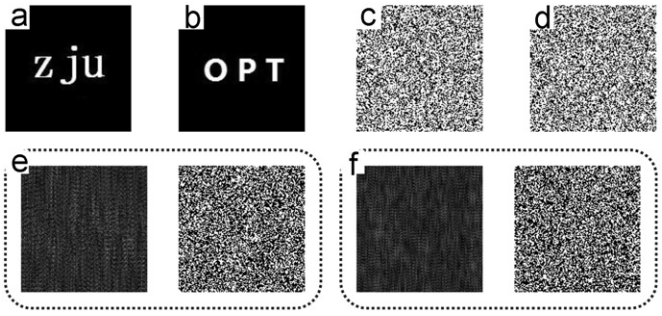

Fig. 4. Binary images (a) zju and (b) OPT, random phase masks (c) $\exp[i\varphi(x)]$ and (d) $\exp[i\varphi_{re}(x)]$, the encrypted amplitude and phase distributions of the images (e) zju and (f) OPT.

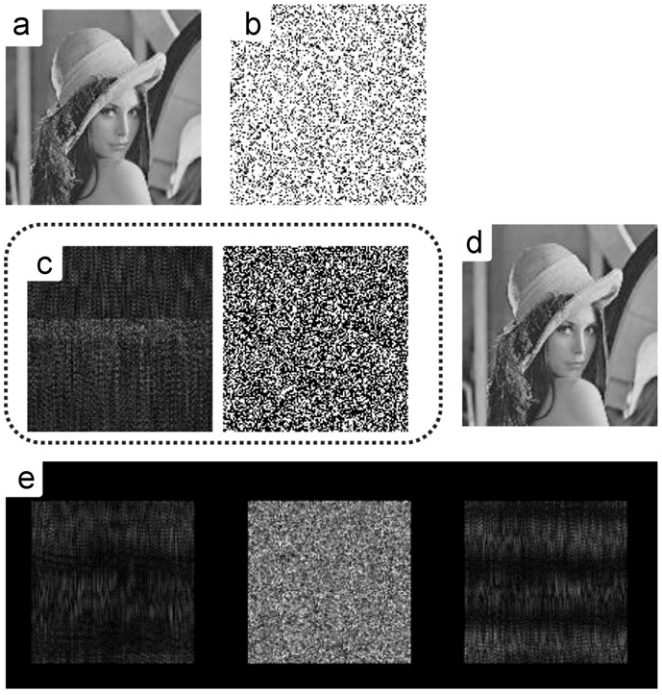

Fig. 5. (a) Host image Lena, (b) one of the interference intensity patterns of the key phase recorded, (c) the amplitude and phase distributions of the combined result $E_{1p} + E_{2p}$, (d) watermarked host Lena, (e) decrypted result with only correct geometric keys.

shown in Fig. 5(d). The decryption result by inverse Fresnel transform directly from the watermarked host in Fig. 5(d) is shown in Fig. 5(e) with only correct geometric parameters. It shows that without the key phase, the spatially separated, noise-like results are obtained in the output plane. So without knowing the key phase, one cannot recover the original images.

As is shown in Fig. 6(a), with all correct keys, by inverse Fresnel transform on the watermarked image shown in Fig. 5(d), fully decrypted result "zju" can be obtained. With all correct keys, by inverse Fresnel transform, the other secret image "OPT" can also be recovered as is shown in Fig. 6(b). If the same encryption keys are used for the double secret images encryption, as a decryption result, the two images will be obtained in the output plane simultaneously as is shown in Fig. 6(c).

In our numerical simulations, the peak signal-to-noise ratio (PSNR) is chosen as a metric to evaluate the quality of watermarked host image for different weighting factor α. The PSNR value between the original image $h(x,y)$ and the noise introduced image $h'(x,y)$ can be defined as

$$\mathrm{PSNR} = 10\ \lg \frac{(2^n-1)^2}{\frac{1}{M\times N}\sum_{x=1}^{N}\sum_{y=1}^{M}[h(x,y)-h'(x,y)]^2}\ \mathrm{dB} \tag{20}$$

where $M \times N$ represents the total number of pixels of images. $h(x,y)$ and $h'(x,y)$ represent the original host image and the watermarked host image, respectively.

Fig. 7 shows the PSNR for host image at different weighting factor α. It is shown that when α varies from 0 to 1.2 the quality of the host goes down rapidly from 56 dB to 16 dB. To ensure the recovered quality for the host image, small value of α will be an optimum. Considering the invisible and robustness of the hidden images, as the spatial separation results are obtained, by a simple division calculation on the watermarked host, the hidden images will be obtained for an arbitrary value of α.

To further test the performance of our proposed method, we have also checked the robustness of the system against noise attacks. Fig. 8(a) shows the watermarked "Lena" which is distorted by the Gaussian noise when the variance equals 0.01. Fig. 8(b) shows the recovered hiding images from Fig. 8(a) when the same encryption keys are used for double images encryption which is similar to Fig. 6(c). The results of making occlusion on the watermarked host were not given here, for it is evident that part of the encoding result can be used to reconstruct the original images as we can see from the analyses in Section 2.3 and the similar results were also given in the early work [7].

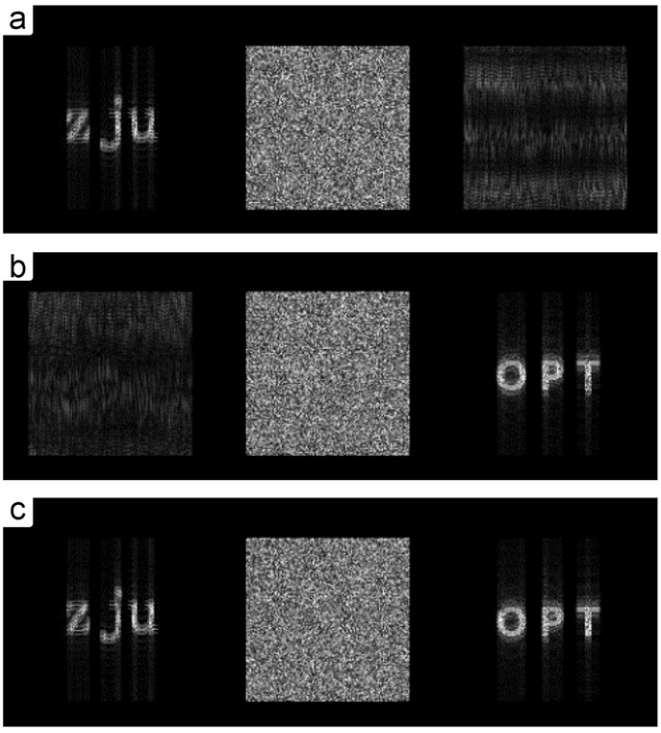

Fig. 6. Decryption results by inverse Fresnel transform over watermarked host Lena with all correct key (a) decryption zju (b) decryption OPT, (c) two extraction images using same encoding keys.

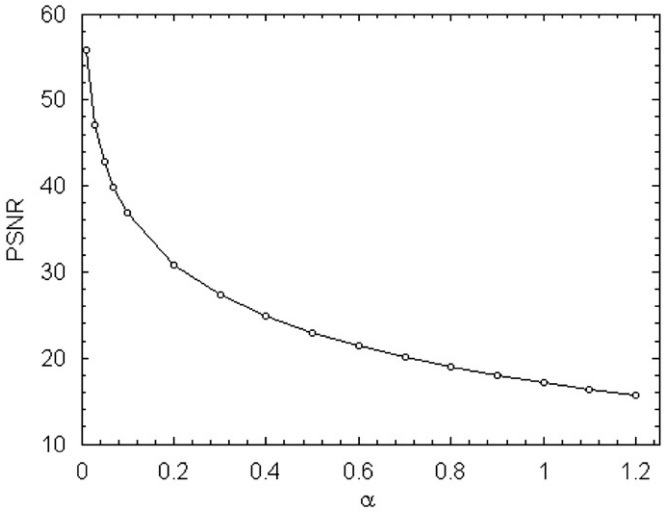

Fig. 7. PSNR for the host image for different α.

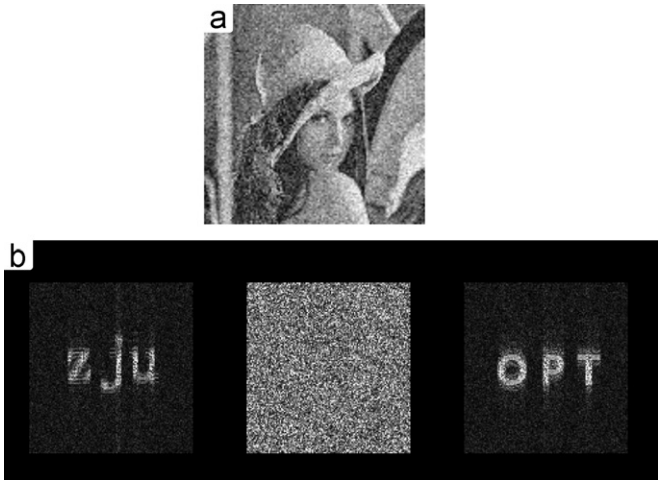

Fig. 8. Noise attacking (a) watermarked Lena with Gaussian noise, (b) hidden image recovered from (a).

4. Conclusions

In conclusion, we have presented an optical system for image encryption by use of joint Fresnel transform correlator architecture adopting two-step phase-shifting interference technology. To enhance the system security, a digital process is used to realize double encrypted images hiding and extracting. In our proposed method, the secret image attached with a phase mask is used as the object beam. The complex mask with two constant phase shifts 0 and δ are used as two different reference beams, respectively. Both of the encryption result and the key phase can be recorded as interference intensity patterns by the CCD. The

complex encryption result can be derived from the intensities recorded by the CCD. Compared with previous works [15–20], for its lensless, the improved system is more compact and versatile. By the two-step phase-shifting, fewer number of intensity patterns need to be delivered via digital means, it is helpful to reduce the information load and make the system more efficient. Digital operation is further used to realize the images hiding to improve the security. By the extraction procedure, the recovered images can be spatially separated from noise for their phase modulation. And each time when different encoding keys are used, there's only one meaningful image can be extracted. The quality of the recovered hidden image will be better for the cross talk can be eliminated by this way. Theoretical analyses and computer simulations indicate the feasibility of our system. Numerical results are also given to verify the performance and robustness when there is noise attack on the watermarked host.

Acknowledgments

This work was supported by the Zhejiang Provincial Natural Science Foundation of China (R1090168 and Y6090220), the National Natural Science Foundation of China (11274273, 11074219 and 10874150), and the Open Research Fund of Key Laboratory of Atmospheric Composition and Optical Radiation, Chinese Academy of Sciences (JJ-09-10D).

References

[1] P. Refregier, B. Javidi, Optics Letters 20 (1995) 767.
[2] B. Javidi, Physics Today 50 (1997) 27.
[3] G. Unnikrishnan, J. Joseph, K. Singh, Optics Letters 25 (2000) 887.
[4] G. Situ, J. Zhang, Optics Letters 29 (2004) 1584.
[5] B. Javidi, T. Nomura, Optics Letters 25 (2000) 28.
[6] E. Tajahuerce, O. Matoba, S. Verrall, B. Javidi, Applied Optics 39 (2000) 2313.
[7] S. Kishk, B. Javidi, Applied Optics 41 (2002) 5462.
[8] N. Takai, Y. Mifune, Applied Optics 41 (2002) 865.
[9] S. Kishk, B. Javidi, Optics Letters 28 (2003) 167.
[10] H. Chang, C. Tsan, Applied Optics 44 (2005) 6211.
[11] X. Meng, L. Cai, X. Xu, X. Yang, X. Shen, G. Dong, Y. Wang, Optics Letters 31 (2006) 1414.
[12] Y. Shi, G. Situ, J. Zhang, Optics Letters 32 (2007) 1914.
[13] H. Hwang, H. Chang, W. Lie, Optics Letters 34 (2009) 3917.
[14] H. Chang, H. Hwang, C. Lee, M. Lee, Applied Optics 50 (2011) 710.
[15] T. Nomura, B. Javidi, Optical Engineering 39 (2000) 2031.
[16] D. Abookasis, O. Arazi, J. Rosen, B. Javidi, Optical Engineering 40 (2001) 1584.
[17] H. Chang, C. Chen, Optical Review 11 (2004) 165.
[18] D. Abookasis, O. Montal, O. Aramson, J. Rosen, Applied Optics 55 (2005) 3019.
[19] X. Shi, D. Zhao, Applied Optics 50 (2011) 766.
[20] H. Chang, C. Chen, Optics Express 14 (2006) 1458.
[21] C. Mela, C. Iemmi, Optics Letters 31 (2006) 2562.
[22] J.R. Fienup, Applied Optics 22 (1982) 2758.
[23] E. Tajahuerce, O. Matoba, S. Verrall, B. Javidi., Applied Optics 39 (2000) 2313.