doi:10.3788/gzxb20144303.0310004

位置与波长并行复用技术下的光学干涉多图像加密系统

秦怡,刘旭焱,巩琼
(南阳师范学院 物理与电子工程学院,河南 南阳 473061)

摘 要:基于位置和波长参量的并行复用,提出一种高加密容量的光学干涉多图像加密系统.加密时,待加密图像分为两组,每组均利用位置复用技术解析地加密到两个纯相位板中,将所获取的四个相位板再经波长复用技术融合到两个光学相位元件中.加密过程采用数字技术,无需使用迭代算法,而解密过程既可以采用数字技术也可以采用纯光学方法.实验中利用波长与位置的并行复用及相关系数对系统的加密容量进行评估,同时研究了系统对于噪音攻击和剪切攻击的稳健性.结果表明:加密容量较已有方法有较大提高;对于噪音攻击的稳健性较强,但是对于剪切攻击的稳健性较弱.

关键词:多图像加密;波长复用;位置复用; 相位板;干涉原理
中图分类号:TP751 **文献标识码**:A **文章编号**:1004-4213(2014)03-0310004-7

Interference-based Multiple-image Encryption by Position and Wavelength Multiplexing

QIN Yi, LIU Xu-yan, GONG Qiong
(*College of physics and electronic Engineering, Nanyang Normal University, Nanyang, Henan* 473061, *China*)

Abstract: A novel interference-based multiple-image encryption method with high encryption capacity was proposed by position and wavelength multiplexing. For encryption, the original images to be encrypted were divided into two groups, and each group of target images was analytically hidden into two phase only masks by position multiplexing. Subsequently the obtained four phase only masks were further merged into two diffractive phase elements by wavelength multiplexing. The encryption process did not need iterative algorithm and should be implemented digitally, while the decryption process could be performed both digitally and optically. The encryption capacity of the system was evaluated with correlation coefficient, and it was shown that the capacity was greatly improved due to the introduction of both position and wavelength multiplexing. In addition, the robustness of the proposal against noise and occlusion was also investigated, and the results indicated that the proposal is of high robust against noise attack but a little vulnerable to occlusion attack.

Key words: Multiple-image encryption; Wavelength multiplexing; Position multiplexing; Phase-only mask; Interference principle
OCIS Codes: 060.4785; 070.0070; 100.2000

0 Introduction

Optical technology has been extensively explored and widely used in information security application, owing to its multiple parameters and parallel processing ability[1-2]. Since Refregier and Javidi firstly reported their pioneer work about optical encryption based on double random phase encoding (DRPE)[3], several optical encryption techniques have been proposed in recent years[4-8]. It was later found that the DRPE technique was not only vulnerable to several attacks[9-10] but also inconvenient for information transfer and

Foundation item: The National Natural Science Foundation of China (No. 61306007)
First author: QIN Yi (1981—), male, lecturer, M. S. degree, mainly focuses on optical information security. Email:641858757@qq.com
Received: Aug. 28, 2013; **Accepted**: Oct. 31, 2013

optical decryption, since the DRPE technique involves a complex ciphertext while the current spatial light modulators (SLMs) are not able to modify the amplitude and the phase at the same time. With this in mind, researchers began to commencing encrypting images into phase only masks[11-13]. In particular, the simple interference-based encryption (IBE) approach devoted by Zhang is noteworthy for it does not need the time-consuming iterative algorithm[14]. Based on the IBE method, new encrypting schemes with higher security levels are developed[15-16].

One major feature that improves optical encryption is the multiplexing technique. This procedure brings the possibility for storing multiple messages in a single medium without loss of information of primary images. As a consequence, the efficiency of secret-information transmission has been extremely improved. For instance, Situ and Zhang proposed to use wavelength multiplexing[17] and position multiplexing[18] for binary images. Barrera utilized polarization multiplexing to encrypt multiple images in a holographic architecture[19]. Liu et al. have devoted a frequency shift technique to achieve multiple-image encryption[20]. Jia and Liu proposed to encrypt double images by aid of random fractional Fourier transform[21], and so on. Afterwards, more and more multiplexing techniques are developed in various optical schemes[22-24]. However, a major problem facing these multiplexing techniques is the low hiding capacity associated with them. In the process of pursuing the solution of this problem, we noticed an important phenomenon in all of the above-mentioned works that there is only one type of multiplexing technique to achieve multiple-image encryption in each encryption system. We believe it is possible to combine two or more types of multiplexing technique in a single optical scheme, as a result of which the hiding capacity will be further enhanced. Therefore, in this paper, we present the implementation of simultaneously wavelength multiplexing and position multiplexing technique in an interference-based architecture. With the proposal one can analytically encrypt multiple images into two diffractive phase elements (DPEs). Since the proposed approach merges both wavelength multiplexing and position multiplexing techniques, the encryption capacity are hence greatly improved. To our best knowledge, this is the most efficiency encryption system cable of encrypting multiple images into to two DPEs without any iterative process.

1 Theoretical analysis

1.1 Principle of the System

In the proposed optical interference-based multiple-image encryption system, the ciphertexts are two diffractive phase elements DPE_1 and DPE_2. In the present encryption scheme, we multiplex multiple distances but only two wavelengths (λ_1 and λ_2) for the reason explicated in the end of Section 2. To explain more fully the encryption process, it is desirable to introduce the decryption schemes of our proposal, which are shown in Fig. 1(a) and Fig. 1(b), respectively. Where f represents plaintexts, g represents the intermediate function, λ represents wavelength, BS represents beam splitter. The two schemes are completely the same with each other except the wavelengths of the illuminating light sources, so only Fig. 1(a) is taken for example to interpret the decryption process. The two DPEs are both illuminated by a parallel light beam with a wavelength of λ_1, then the two diffraction fields are combined by the half mirrors, thereafter the interference of the two beams will generate the original plaintexts, which are denoted as $f_k^{\lambda_1}, k=1,2,\cdots,N^{\lambda_1}$, at different axial positions. Those decrypted images could be directly accepted by Charge Coupled Device (CCD). It should be emphasized that when the identical two DPEs are illuminated by another parallel light beam with a wavelength of λ_2, as shown in Fig. 1(b), another group of original plaintexts $f_k^{\lambda_2}, k=1,2,\cdots,N^{\lambda_2}$ could be obtained.

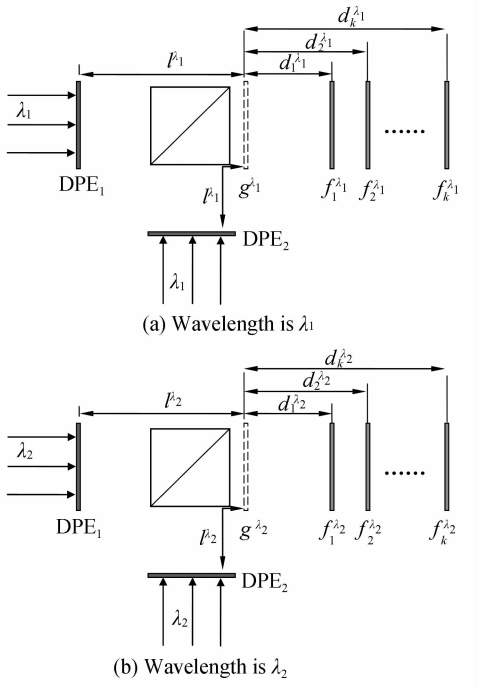


Fig. 1 Schematic of the optical decryption system

Compared with the decryption process, the encryption process is not so straightforward and could only be implemented with digital method. According to the decryption process, the encryption task is to encrypt the multiple target images into DPE_1 and

DPE$_2$. So we propose to separate the encryption task into two steps. First of all, for each $\lambda_i (i=1,2)$, we encrypt the corresponding plaintexts into two phase distributions by position multiplexing. Secondly, the four obtained phase distributions are merged into two DPEs (DPE$_1$ and DPE$_2$) by wavelength multiplexing. These two steps are described in detail in Subsection 1.1.1 and Subsection 1.1.2 below.

1.1.1 *Position multiplexing process in the IBE scheme*

As the first encryption step for both λ_1 and λ_2 is similar, we also only describe the position-multiplexing encryption process of plaintext $f_k^{\lambda_1}, k=1,2,\cdots,N^{\lambda_1}$ that associated with λ_1.

Let the function $f_k^{\lambda_1}(x_o,y_o)$ represent the intensity distribution of the k^{th} target image. We can create a new function expressed as

$$f_k^{\lambda_1}(x_o,y_o)=\sqrt{f_k^{\lambda_1}(x_o,y_o)}\exp[\mathrm{j}2\pi\mathrm{rand}(x_o,y_o)] \quad (1)$$

where rand(x_o, y_o) denotes a random distribution between 0 and 1. Then we calculate the inverse Fresnel propagation of this complex image with a distance d_k and have

$$g_k^{\lambda_1}(x,y)=\mathrm{FrT}_{\lambda_1}[f_k^{\lambda_1}(x_o,y_o);-d_k^{\lambda_1}] \quad (2)$$

where FrT_λ represents the Fresnel transform with respect to λ[4]. Then we can superpose these $g_k(x,y)$ to form an intermediate function

$$g^{\lambda_1}(x,y)=\sum_{k=1}^{N}g_k^{\lambda_1}(x,y) \quad (3)$$

Moreover, From Fig. 1(a) we can obtain

$$g^{\lambda_1}(x,y)=[M_1^{\lambda_1}(x_i,y_i)+M_2^{\lambda_1}(x_i,y_i)] * h(x_i,y_i,l^{\lambda_1},\lambda_1) \quad (4)$$

where

$$h(x_i,y_i,l,\lambda)=\frac{\exp(\frac{\mathrm{j}2\pi l}{\lambda})}{\mathrm{j}\lambda l}\exp[\frac{\mathrm{j}\pi(x_i+y_i)}{\lambda l}] \quad (5)$$

represents the point pulse function of the Fresnel transform. $M_1^{\lambda_1}(x_i,y_i)$ and $M_2^{\lambda_1}(x_i,y_i)$ represent the phase distribution introduced by DPE$_1$ and DPE$_2$, respectively. $*$ indicates the convolution operation and l^{λ_1} represents the distance between the phase masks and the plane where locates $g(x,y)$. With the approach illustrated in Ref. [14], we could finally obtain the phase distributions of DPE$_1$ and DPE$_2$ as

$$M_1^{\lambda_1}=\arg(D^{\lambda_1})-\arccos[\mathrm{abs}(D^{\lambda_1})/2] \quad (6)$$

$$M_2^{\lambda_1}=\arg[D^{\lambda_1}-\exp(\mathrm{i}M_1^{\lambda_1})] \quad (7)$$

where $D^{\lambda_1}=\mathrm{F}^{-1}\{\mathrm{F}[g^{\lambda_1}(x,y)]/\mathrm{F}[h(x_i,y_i,l^{\lambda_1},\lambda_1)]\}$, and F and F^{-1} denote the Fourier transform and inverse Fourier transform, respectively. Similarly, for the wavelength of λ_2, we could also get two phase distributions, which contain the information of the plaintext $f_k^{\lambda_2}(x_o,y_o)$, $k=1,\cdots,N$.

$$M_1^{\lambda_2}=\arg(D^{\lambda_2})-\arccos[\mathrm{abs}(D^{\lambda_2})/2] \quad (8)$$

$$M_2^{\lambda_2}=\arg[D^{\lambda_2}-\exp(\mathrm{i}M_1^{\lambda_2})] \quad (9)$$

where $D^{\lambda_2}=\mathrm{F}^{-1}\{\frac{\mathrm{F}[g^{\lambda_2}(x,y)]}{\mathrm{F}[h(x_i,y_i,l^{\lambda_2},\lambda_2)]}\}$.

1.1.2 *Wavelength multiplexing*

Now we have two phase distributions $M_1^{\lambda_1}$ and $M_2^{\lambda_1}$ for λ_1 and another two phase distributions $M_1^{\lambda_2}$ and $M_2^{\lambda_2}$ for λ_2. However, there are only two DPEs according to the decryption principle. Is it possible to generated two designated phase distributions (e. g. $M_1^{\lambda_1}$ and $M_1^{\lambda_2}$) with the identical DPE for λ_1 and λ_2? Niu *et al*. has demonstrated that the answer is yes[25]. It is worth recalling the fact that the phase distribution of a DPE is a function of the height distribution, the refractive index as well as the wavelength. If we denote the surface height distribution of DPE$_1$ as h_1, the phase distribution with respect to λ_1 can be mathematically expressed as

$$M_1^{\lambda_1}=\frac{2\pi}{\lambda_1}[n(\lambda_1)-1]h_1 \quad (10)$$

where $n(\lambda_1)$ denotes the refractive index of DPE$_1$ for λ_1. For the phase retardation for λ_2 with the identical DPE$_1$ is expected to be $M_2^{\lambda_2}$, we can similarly obtain

$$M_1^{\lambda_2}=\frac{2\pi}{\lambda_2}[n(\lambda_2)-1]h_1 \quad (11)$$

where $n(\lambda_1)$ denotes the refractive index of DPE$_1$ with respect to λ_2. Apparently, it is hard to fulfill Eq. (10) and Eq. (11) simultaneously, because $M_1^{\lambda_1}$ and $M_2^{\lambda_1}$ are completely independent with each other. Considering that $M_1^{\lambda_1}$ and $M_2^{\lambda_1}$ are both phase distributions, the addition of an integral number of 2π to them does not affect the decryption results. Therefore, if we carefully select two integers P and Q, Eq. (12) may be satisfied which is expreesed as

$$h_1=\frac{M_1^{\lambda_1}+2P\pi}{2\pi[n(\lambda_1)-1]}\lambda_1\cong\frac{M_1^{\lambda_2}+2Q\pi}{2\pi[n(\lambda_2)-1]}\lambda_2 \quad (12)$$

In other words, the height distribution of DPE$_1$ could be obtained if we make the two items in right of Eq. (12) as close as possible to each other by varying P and Q simultaneously. If we calculate in such a way that we assure the phase retardation of DPE$_1$ for λ_1 is exactly equal to $M_1^{\lambda_1}$, then there will be inevitable errors between the phase retardation of DPE$_1$ for λ_2 and $M_1^{\lambda_2}$. However, these errors would become negligible if the value scope of P and Q is large enough. Thereafter we can identify the height distribution of DPE$_2$ for realization of $M_2^{\lambda_1}$ and $M_2^{\lambda_2}$ with a similar procedure.

1.2 The decryption process

The optical architecture for decryption has already been illustrated in Fig. 1. From the encryption principle it is easy to know that the decryption process for λ_1 and λ_2 are similar. Thus we also take only the decryption process with λ_1 for example to mathematically interpret the decryption process, which is shown in Fig. 1(a). By a similar deduction with the approach described in Ref. [24], we can reconstruct the k^{th} decrypted image at the output expressed as follows

$$\hat{f}_k^{\lambda_1}(x_o,y_o)=f_k^{\lambda_1}(x_o,y_o)+n_k^{\lambda_1}(x_o,y_o) \tag{13}$$

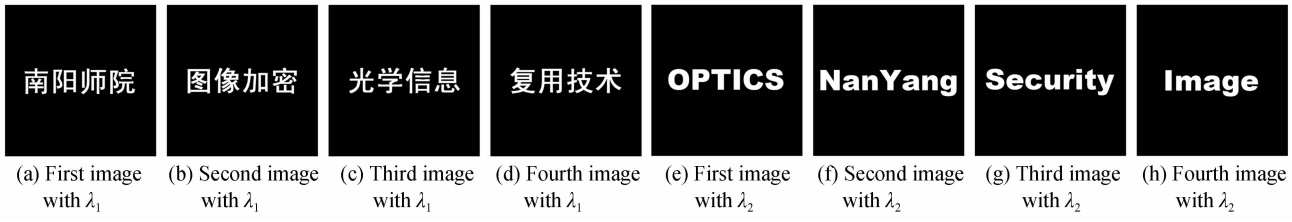
where

$$n_k^{\lambda_1}(x_o,y_o)=\sum_{q\neq k}n_q^{\lambda_1}(x_o,y_o)=\sum_{q\neq k}\mathrm{FrT}_{\lambda_1}\{\mathrm{FrT}_{\lambda_1}[f_q^{\lambda_1}(x_o,y_o);-d_q^{\lambda_1}];d_k^{\lambda_1}\} \tag{14}$$

It could be seen from Eq. (13) that the actual retrieved image includes the desired primary image plus an annoying noise $n_k^{\lambda_1}(x_o,y_o)$. Fortunately, it was shown in a previous study that the original image could be well reconstructed if we sufficiently increasing the distance mismatch $d_{kq}^{\lambda_1}=|d_k^{\lambda_1}-d_q^{\lambda_1}|$ to render $n_k^{\lambda_1}(x_o,y_o)$ down to random noise[24]. In fact, this is also the basic principle for position multiplexing.

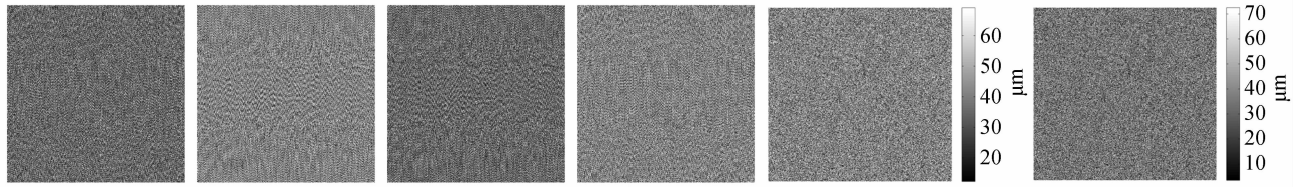
2 Simulation results and discussions

Numerical simulations are performed for showing the validity of the encryption scheme. First of all, eight binary images of size 512×512 pixels, which are shown in Fig. 2, are introduced into the encryption scheme. They are further divided into two groups for encryption: the first group of Figs. 2(a)～(d) and the second group of Figs. 2(e)～(h). By use of the method described in Subsection 1.1, the two groups of images are firstly encrypted by position multiplexing with λ_1 and λ_2, respectively. The wavelengths of the illuminating light are set as $\lambda_1=632.8$ nm and $\lambda_2=555$ nm. For brevity, the distances l^{λ_1} and l^{λ_2} are both equal to 50mm and the axial distances are set as $d_1^{\lambda_1}=d_1^{\lambda_2}=50$ mm, $d_2^{\lambda_1}=d_2^{\lambda_2}=50$ mm, $d_3^{\lambda_1}=d_3^{\lambda_2}=110$ mm, and $d_4^{\lambda_1}=d_4^{\lambda_2}=140$ mm. The analytically obtained four phase distributions are shown in Figs. 3(a)～(d). Among them the phase distributions of $M_1^{\lambda_1}$ and $M_2^{\lambda_1}$ are shown in Fig. 3(a) and Fig. 3(b) while that of $M_1^{\lambda_2}$ and $M_2^{\lambda_2}$ are shown in Fig. 3(c) and Fig. 3(d), respectively.



(a) First image with λ_1 (b) Second image with λ_1 (c) Third image with λ_1 (d) Fourth image with λ_1 (e) First image with λ_2 (f) Second image with λ_2 (g) Third image with λ_2 (h) Fourth image with λ_2

Fig. 2 The primary images for encryption



(a) $M_1^{\lambda_1}$ (b) $M_2^{\lambda_1}$ (c) $M_1^{\lambda_2}$ (d) $M_2^{\lambda_2}$ (e) DPE_1 (f) DPE_2

Fig. 3 The analytically obtained phase masks

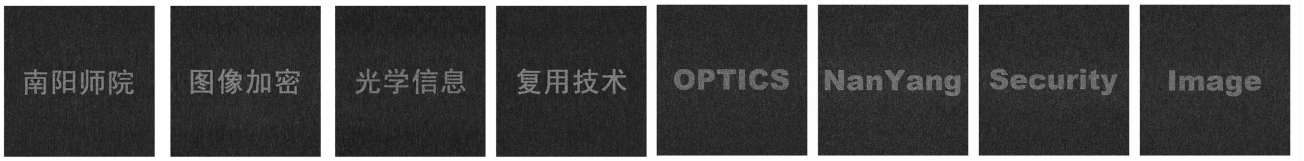
Then by aid of Eq. (12), we could identify the final ciphertexts, namely the height distribution of DPE_1 for generalization of $M_1^{\lambda_1}$ and $M_2^{\lambda_1}$ and the height distribution of DPE_2 for generalization of $M_1^{\lambda_2}$ and $M_2^{\lambda_2}$, which are displayed in Fig. 3(e) and Fig. 3(f), respectively. It should be emphasized we limit the values of P and Q to be integers between 0 and 8 in simulations. The reconstructed images with DPE_1 and DPE_2 as well as correct parameters are shown in Fig. 4, where Figs. 4(a)～(d) correspond to λ_1 and Figs. 4(e)～(h) correspond to λ_2. It is obvious that the original plaintexts are successfully retrieved, although they suffer from some degradation in quality as a result of cross talk. The decryption results with incorrect DPE_1 and DPE_2 but correct wavelengths λ_1 and λ_2, from which one can get no information about the primary images, are shown in Fig. 5. To objectively estimate these decryption results, we calculate the correlation coefficient (CC) between the recovered image $|\hat{f}_k(x_o,y_o)|$ and the primary image $f_k(x_o,y_o)$. It is defined as

$$\mathrm{CC}=\frac{E\{[f-E(f)][|\hat{f}_k|-E(|\hat{f}_k|)]\}}{\sqrt{E\{[f-E(f)]^2\}E\{[|\hat{f}_k|-E(|\hat{f}_k|)]^2\}}} \tag{15}$$

where $E[\cdot]$ is the expectation value. The coordinates are omitted here for brevity.

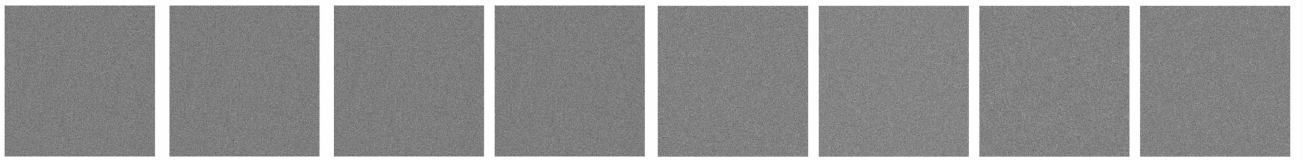
The corresponding CCs for Figs. 4(a)～(d) are 0.648 2, 0.6558, 0.612 1, and 0.634 0, respectively. By comparison, the CCs for Figs. 4(e)～(h) are 0.444 3, 0.473 0, 0.443 1, and 0.396 8, respectively. It can be found that the decryption results with λ_2 have lower quality than that with λ_1. This is because of the reason stated in Subsection 1.1. Namely, since the integer P and Q are limited between 0 and 8, the phase retardations generated by the DPE_1 and DPE_2 with λ_2 are not equal to the ideal phase distribution $M_1^{\lambda_2}$ and $M_2^{\lambda_2}$ analytically computed with Eq. (8) and Eq. (9). However, the quality of the retrieved images with λ_1 is still not satisfied due to the low values of CC. In factual, this problem could be dealt with by postprocessing the directly decrypted images with a

low-pass filter, e. g. a median filter. The decrypted images are presented in Figs. 6(a)～(h) when a median filter with 4 × 4 neighborhood is adopted, and the corresponding CC values for Figs. 6(a)～(h) are 0.890 9, 0.890 6, 0.864 8, 0.891 3, 0.818 5, 0.830 1, 0.812 0, and 0.772 8, respectively.



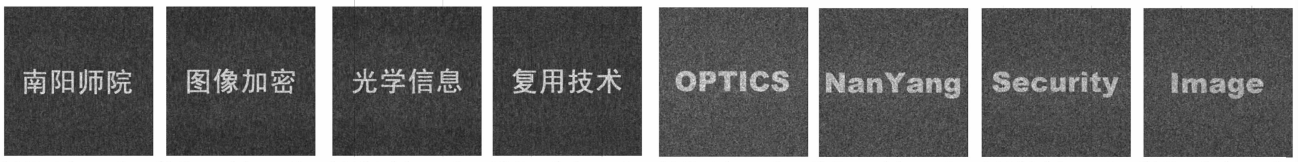
(a) First decryption with λ_1 (b) Second decryption with λ_1 (c) Third decryption with λ_1 (d) Fourth decryption with λ_1 (e) First decryption with λ_2 (f) Second decryption with λ_2 (g) Third decryption with λ_2 (h) Fourth decryption with λ_2

Fig. 4 Decryption results by use of the correct DPEs



(a) First decryption with λ_1 (b) Second decryption with λ_1 (c) Third decryption with λ_1 (d) Fourth decryption with λ_1 (e) First decryption with λ_2 (f) Second decryption with λ_2 (g) Third decryption with λ_2 (h) Fourth decryption with λ_2

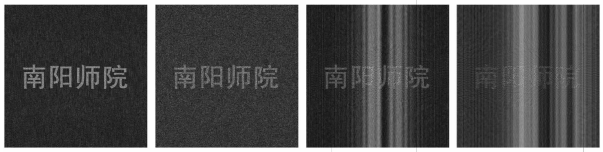
Fig. 5 Decryption results by the use of the incorrect DPEs



(a) First decryption with λ_1 (b) Second decryption with λ_1 (c) Third decryption with λ_1 (d) Fourth decryption with λ_1 (e) First decryption with λ_2 (f) Second decryption with λ_2 (g) Third decryption with λ_2 (h) Fourth decryption with λ_2

Fig. 6 Decryption results by the use of the correct POMs with median filtering

During data storage or transmission, the DPEs may be contaminated, and robustness against noise is further tested. To test the reconstruction of the primary image in the presence of multiplicative input noise, we multiply the DPEs by a realization of the random white noise that uniformly distributed in [0; α], where α is a positive number. For brevity, only the decryption results corresponding to Fig. 2(a) are presented. The decoded images are shown in Figs. 7(a) and 7(b) when α takes the values of 0.01 and 0.1, respectively. We also test the robustness of the proposed method against occlusion attack. Figs. 7(c) and 7(d) show the decrypted images when 30% and 50% occlusions exist at the DPEs. it can be seen From Fig. 7 that the proposal is highly robust against noise attacks but a little vulnerable to occlusion attacks. Therefore it is important to prevent the DPEs from occlusion attack during storage or transmission of them.



(a) α=0.01 (b) α=0.1 (c) 30% occlude (d) 50% occluded

Fig. 7 Robustness of the proposal against attacks

For multiple-image encryption, the multiplexing capacity is considered to be an important index for evaluating the encryption system. It is referred as to the maximum number $N_{\max}$ of the total encrypted images that the system can tolerate. Since the proposed method includes both wavelength multiplexing and position multiplexing, then if we denote $N_{\max}^{\lambda_1}$ and $N_{\max}^{\lambda_2}$ the position multiplexing capacity corresponding to λ_1 and λ_2, the total multiplexing capacity of the proposed encryption system should be

$$N_{\max} = N_{\max}^{\lambda_1} + N_{\max}^{\lambda_2} \tag{16}$$

It has been shown in the previous work devoted by Qin[24] that the position multiplexing capacity could be determined by introducing the correlation coefficient. Here we employ a similar approach to analyze the proposed proposal with simulation. In this simulation, the same images shown in Fig. 2(a) are encrypted with a fixed $l^{\lambda_i} = 50$ mm, $i = 1, 2$ and variable $d_k^{\lambda_i} = 50 + 30(k - 1)$mm, $k = 1, 2, \cdots, N^{\lambda_i}$. Then the behavior of the correlation coefficient versus the total number N^{λ_i} of the encrypted images recorded with in the two DPEs is drawn in Fig. 8.

If we set a threshold value CC = 0.7 to judge whether the original image is successfully retrieved, it could be seen from Fig. 8 the position multiplexing capacity is $N_{\max}^{\lambda_1} = 3$ for λ_1 and $N_{\max}^{\lambda_2} = 1$ for λ_2 in case of no postprocessing, and the total capacity of the proposal is $N_{\max} = 4$. However, the two number will become $N_{\max}^{\lambda_1} = 9$ and $N_{\max}^{\lambda_2} = 5$ while applying median filtering to the decrypted images, in this case the total

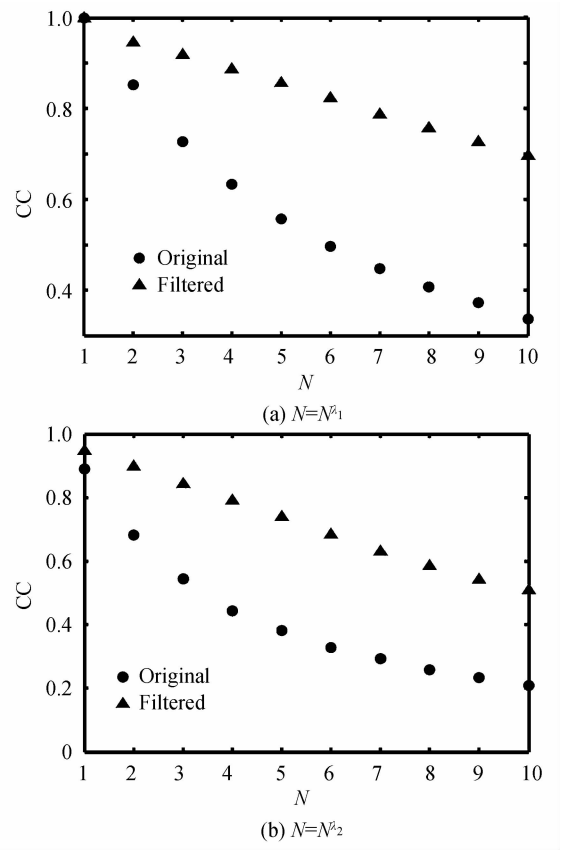


Fig. 8 Behavior of CC versus N

capacity of the proposal is up to $N_{\max}=14$, which is large enough for actual applications.

As a matter of course, one may expect this technique can also be adopted to multiplex three or more wavelengths in a single scheme so the multiplexing capacity could be further improved. However, this goal could hardly be approached. Assuming that another phase distribution $M_1^{\lambda_3}$ corresponding a third wavelength λ_3 is obtained from a similar process with the acquisition of $M_1^{\lambda_1}$ and $M_2^{\lambda_2}$, and one want to multiplex the three wavelengths by using the aforementioned method, he must find three integers P, Q and R which are determined by

$$h_1=\frac{M_1^{\lambda_1}+2P\pi}{2\pi[n(\lambda_1)-1]}\lambda_1\cong\frac{M_1^{\lambda_2}+2Q\pi}{2\pi[n(\lambda_2)-1]}\lambda_2\cong\frac{M_1^{\lambda_3}+2Q\pi}{2\pi[n(\lambda_3)-1]}\lambda_3 \tag{17}$$

However, from a mathematical point of view, it will be much more difficulty to identify the three integers P, Q and R that make the equation true.

Advantages of the proposed optical encoding system compared to previous work can be briefly enumerated as follows: 1) simplicity of the implementation, the encryption process is completely free from iterative algorithm and the decryption process can be performed in a pure optical manner, therefore the proposal is suitable for high speed image encryption; 2) high encryption capacity, compared with some previous multiple-image encryption methods[17-19], the encryption capacity of our approach is significantly enhanced due to the employment of two multiplexing techniques.

3 Conclusions

In conclusion, a novel method for multiple-image hiding by combination of position multiplexing and wavelength multiplexing has been proposed. The encryption process should be implemented in a digital manner, while the decryption process can be carried out in a pure optical manner or a digital manner. With the proposed system one can analytically hide multiple images into only two diffractive phase elements. The encryption capacity is greatly enhanced compared with previous devoted approach which utilizes only one multiplexing technique in a single encryption system. The feasibility and effectiveness of the proposal have been verified by computer simulations.

References

[1] JAVIDI B. Securing information with optical technologies[J]. *Physics Today*, 1997, **50**: 27-32.

[2] ALFALOU A, BROSSEAU C. Optical image compression and encryption methods[J]. *Advance in Optics and Photonics*, 2009, **1**(3): 589-636.

[3] REFREGIER P, JAVIDI B. Optical image encryption based on input plane and Fourier plane random encoding[J]. *Optics Letters*, 1995, **20**(7): 767-769.

[4] UNNIKRISHNAN G, JOSEPH J, SINGH K. Optical encryption by double-random phase encoding in the fractional Fourier domain[J]. *Optics Letters*, 2000, **25**(12): 887-889.

[5] SITU G, ZHANG J. Double random-phase encoding in the Fresnel domain[J]. *Optics Letters*, 2004, **29**(14): 1584-1586.

[6] NOMURA T, JAVIDI B. Optical encryption using a joint transform correlator architecture[J]. *Optical Engineering*, 2000, **39**(8): 2031-2035.

[7] QIN Y, GONG Q. Optical encryption in a JTC encrypting architecture without the use of an external reference wave[J], *Optics and Laser Technology*, 2013, **51**: 5-10.

[8] ZHOU N, WANG Y, WU J. Image encryption algorithm based on the multi-order Discrete fractional Mellin transform [J]. *Optics Communications*, 2011, **284**: 5588-5597.

[9] PENG X, ZHANG P, WEI H, *et al*. Known-plaintext attack on optical encryption based on double random phase keys[J]. *Optics Letters*, 2006, **31**(8): 1044-1046.

[10] PENG Xiang, TANG Hong-qiao, TIAN Jing-dong. Ciphertext only attack on double random phase encoding optical encryption system[J]. *Acta Physica Sinica*, 2007, **56**(5): 2629-2636.

[11] CHANG H T, LU W C, KUO C J. Multiple-phase retrieval for optical security systems by use of random-phase encoding [J]. *Applied Optics*, 2002, **41**(23): 4825-4834.

[12] SITU G, ZHANG J. A lensless optical security system based on computer-generated phase only masks [J]. *Optics Communications*, 2004, **232**: 115-122.

[13] LI Y, KRESKE K, ROSEN J. Security and encryption optical systems based on a correlator with significant output images[J]. *Applied Optics*, 2000, **39**(29): 5295-5301.

[14] ZHANG Y, WANG B. Optical image encryption based on

interference[J]. *Optics Letters*, 2008, **33**(21): 2443-2445.

[15] WANG X, ZHAO D. Optical image hiding with silhouette removal based on the optical interference principle [J]. *Applied Optics*, 2012, **51**(6): 686-691.

[16] ZHANG Y, WANG B, DONG Z. Enhancement of image hiding by exchanging two phase masks[J]. *Journal of Optics A: Pure and Applied Optics*, 2009, **11**(12): 125406.

[17] SITU G, ZHANG J. Multiple-image encryption by wavelength multiplexing[J]. *Optics Letters*, 2005, **30**(11): 1306-1308.

[18] SITU G, ZHANG J. Position multiplexing for multiple-image encryption[J]. *Journal of Optics A: Pure and Applied Optics*, 2006, **8**(5): 391-397.

[19] BARRERA J F, HENAO R, TEBALDI M, *et al*. Multiplexing encrypted data by using polarized light [J]. *Optics Communications*, 2006, **260**: 109-112.

[20] LIU Z, ZHANG Y, ZHAO H, *et al*. Optical multi-image encryption based on frequency shift[J]. *Optik*, 2011, **122**: 1010-1013.

[21] JIA Li-juan, LIU Zheng-jun. Double image encryption algorithm based on random fractional Fourier transform[J]. *Acta Photonica Sinica*, 2009, **38**(4): 1020-1024.

[22] XIAO Y, SU X, LI S, *et al*. Key rotation multiplexing for multiple-image optical encryption in the Fresnel domain[J]. *Optics and Laser Technology*, 2011, **43**(4): 889-894.

[23] HWANG H E, CHANG H T, LIE W N. Multiple-image encryption and multiplexing using a modified Gerchberg-Saxton algorithm and phase modulation in Fresnel transform domain[J]. *Optics Letters*, 2009, **34**(24): 3917-3919.

[24] QIN Y, GONG Q. Interference-based multiple-image encryption with silhouette removal by position multiplexing [J]. *Applied Optics*, 2013, **52**(17): 3987-92

[25] NIU C H, WANG X L, LV N G, *et al*. An encryption method with multiple encrypted keys based on interference principle[J]. *Optics Express*, 2010, **18**(8): 7827-7834.