Vol 14 No 10, October 2005
1009-1963/2005/14(10)/1996-08

Chinese Physics

© 2005 Chin. Phys. Soc.
and IOP Publishing Ltd

A new distribution scheme of decryption keys used in optical verification system with multiple-wavelength information

Niu Chun-Hui(牛春晖)[a], Zhang Yan(张 岩)[b]†, and Gu Ben-Yuan(顾本源)[a]

[a] *Institute of Physics, Chinese Academy of Sciences, Beijing* 100080, *China*

[b] *Department of Physics, Capital Normal University, Beijing* 100037, *China*

(Received 31 May 2005; revised manuscript received 16 June 2005)

A new distribution scheme of decryption keys used in optical verification systems is proposed. The encryption procedure is digitally implemented with the use of an iteration algorithm in computer. Three target images corresponding to three wavelengths are encoded into three sets of phase-only masks (POMs) by a special distributing method. These three sets of POMs are assigned to three authorized users as the personal identification. A lensless optical system is used as the verification system. In the verification procedure, every two of the three authorized users can pass the verification procedure cooperatively, but only one user cannot do. Numerical simulation shows that the proposed distribution scheme of decryption keys not only can improve the security level of verification system, but also can bring convenience and flexibility for authorized users.

Keywords: optical encryption technique, multiple-wavelength information, diffractive optical system
PACC: 4230V, 4278D, 4283

1. Introduction

Recently, optical technology has been widely employed in encryption and verification systems[1−8] because optical information processing technique possesses many advantages, for instance, the capability of parallel processing and fast computing speed. Moreover, optical wave carries not only the amplitude and phase information, but also contains other characteristic parameters, for instance, the polarization and wavelength.[9,10] These parameters may support more degrees of freedom and higher level of information security. Security level is an important factor for an encryption and verification system, which guarantees the validity and practicability of the system. One of the methods for obtaining high security level is to increase the capacity of key space. Refregier and Javidi [1] have proposed a double-random-phase encoding technique that encodes an original image into a stationary white noise. The two random-phase masks placed in the input and the Fourier plane of a 4-f correlator serve as the keys of the system. Information encryption techniques in the fractional-Fourier domain have also been presented.[2−6] It is well proved that higher security can be acquired in the fractional-Fourier domain because the scale factors and the fraction orders of the fractional-Fourier transform provide additional keys. Moreover, Matoba and Javidi [7] have experimentally demonstrated that the position of the phase masks in the Fresnel domain can also be used as the decrypting keys. More recently, Situ and Zhang[8] reported that the wavelength can play a role of a key in the Fresnel domain and the application of this key can increase the security level of the encryption system. Moreover, multiple wavelengths of the incident light can also be used as the additional decrypting keys. The increase of the number of the available wavelengths in information encryption can further improve the security level.

In all of the above mentioned methods, the decryption keys are distributed to different individual persons, and only when all the authorized persons meet together can the verification system be passed. This is not convenient for users. In this paper, we present a new distribution scheme of the decryption keys for a verification system in the Fresnel domain.

†E-mail: yzhang@mail.cnu.edu.cn

Three target images are digitally encoded into three sets of phase-only masks (POMs), which are served as the decryption keys by a special distributing method. A lensless optical system is used as the verification system, in which a set of POMs are located at the determined positions along the direction of propagation to decrypt the target image. Three sets of encrypted POMs are distributed to three users. Any two users can reconstruct all the three target images in the optical verification system by using their POMs, thus, they can pass the verification procedure cooperatively. However, any one of the three users can only produce two target images with the use of his own POMs and cannot pass the verification procedure. The distribution scheme of the decryption keys can not only increase the security level, but also increase flexibility of the verification procedure.

This paper is organized as follows. The description of the optical verification system, the relevant encryption algorithm, and the verification procedure are described in Section 2. Numerical simulations for demonstrating the advantage of the proposed distribution scheme are presented in Section 3 with some discussions. Finally, a brief conclusion is given in Section 4.

2. Encryption and verification procedure

We now describe in detail the optical verification system, the relevant encryption algorithm, and the verification procedure used in this work.

2.1. Distribution scheme of decryption keys and optical verification system

In the encryption and verification system considered here, three sets of image information associated with three different wavelengths (e.g. λ_α, $\alpha = 1, 2, 3$) are encrypted into three sets of POMs by a special distribution method. The first set of POMs includes the information of images corresponding to λ_1 and λ_2. The second set of POMs includes the information to λ_2 and λ_3, and the last set of POMs includes the information to λ_3 and λ_1. Every set of POMs comprises two POMs (POM_1 and POM_2). Three sets of POMs are distributed to three users (called U_a, U_b and U_c) and serve as the decryption keys of the system. In the verification stage, two POMs held by one of the three users should be placed on the predesigned locations in the optical system shown in Fig.1 to reconstruct the target images.

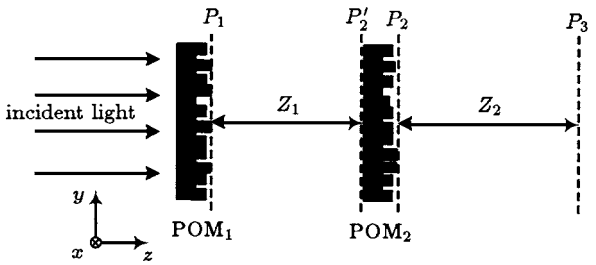


Fig.1. Schematic diagram of the optical verification system. POM_1 represents the first phase mask and POM_2 denotes the second one.

In Fig.1, the plane P_1 represents the plane immediately behind POM_1. The planes P_2' and P_2 are the planes before and behind POM_2, respectively. The output plane is denoted as P_3. The distance between P_1 and P_2' is z_1 and that between P_2 and P_3 is z_2. The optical field distribution on the adjacent planes, e.g. P_1 and P_2', are related by a Fresnel transform with the specified parameters of the distance between them and the incident wavelength λ_α. We denote the coordinate systems on the planes P_1, $P_2'(P_2)$, and P_3 to be (x_1, y_1), (x_2, y_2), and (x_3, y_3), respectively. When a uniform plane wave with wavelength λ_α illuminates the optical system, the wave function $u_1(x_1, y_1, \lambda_\alpha)$ after POM_1 can be expressed as

$$u_1(x_1, y_1, \lambda_\alpha) = \exp\left\{ \mathrm{i}\frac{2\pi}{\lambda_\alpha}[n_1(\lambda_\alpha) - 1]h_1(x_1, y_1) \right\}, \tag{1}$$

where $h_1(x_1, y_1)$ denotes the surface-relief depth distribution of the POM_1 and $n_1(\lambda_\alpha)$ is the refractive index of POM_1 at the incident wavelength λ_α.

Under the Fresnel approximation, the complex amplitude $u_2'(x_2, y_2, \lambda_\alpha)$ on the plane P_2' for the incident wavelength λ_α is expressed as

$$u_2'(x_2, y_2, \lambda_\alpha) = \int\int u_1(x_1, y_1, \lambda_\alpha) g(x_2, y_2; x_1, y_1; z_1, \lambda_\alpha) \mathrm{d}x_1 \mathrm{d}y_1. \tag{2}$$

The kernel function $g(x_2, y_2; x_1, y_1; z_1, \lambda_\alpha)$ is given by

$$g(x_2, y_2; x_1, y_1; z_1, \lambda_\alpha) = \frac{\exp(\mathrm{i}2\pi z_1/\lambda)}{\mathrm{i}\lambda_\alpha z_1} \times \exp\left\{ \frac{\mathrm{i}\pi}{\lambda_\alpha z_1}[(x_2 - x_1)^2 + (y_2 - y_1)^2] \right\}. \tag{3}$$

Equation (2) is essentially the Fresnel transform of the wave function $u_1(x_1, y_1, \lambda_\alpha)$ and it can be rewritten in a compact form

$$u_2'(x_2, y_2, \lambda_\alpha) = FrT_{\lambda\alpha}\{u_1(x_1, y_1, \lambda_\alpha); z_1\}, \tag{4}$$

where FrT_{λ_α} represents the Fresnel transform associated with λ_α.

The selected distance between P_2' and P_2 is quite short, therefore, the diffraction effect can be neglected and the optical field suffers only a phase-modulation caused by POM_2. Then, the wavefunction $u_2(x_2, y_2, \lambda_\alpha)$ on the plane P_2 can be expressed as

$$\begin{aligned} & u_2(x_2, y_2, \lambda_\alpha) \\ =& u_2'(x_2, y_2, \lambda_\alpha) \\ & \times \exp\left\{ \mathrm{i}\frac{2\pi}{\lambda_\alpha}[n_2(\lambda_\alpha) - 1]h_2(x_2, y_2) \right\}, \end{aligned} \tag{5}$$

where $h_2(x_2, y_2)$ denotes the depth distribution of the POM_2 and $n_2(\lambda_\alpha)$ is the refractive index of POM_2 at the wavelength λ_α.

Similarly, the wavefunction $u_2(x_2, y_2, \lambda_\alpha)$ on the plane P_2 and the wavefunction $u_3(x_3, y_3, \lambda_\alpha)$ on the plane P_3 can be expressed in the following compact form:

$$u_3(x_3, y_3, \lambda_\alpha) = FrT_{\lambda_\alpha}\{u_2(x_2, y_2, \lambda_\alpha); z_2\}, \tag{6}$$

or

$$u_2(x_2, y_2, \lambda_\alpha) = IFrT_{\lambda_\alpha}\{u_3(x_3, y_3, \lambda_\alpha); z_2\}, \tag{7}$$

where $IFrT_{\lambda_\alpha}$ denotes the inverse Fresnel transform with the wavelength parameter λ_α.

2.2. The encryption procedure

Two target images associated with two different wavelengths (e.g. λ_1 and λ_2) are encrypted into two POMs of one user via a computer. This procedure corresponds to an optimization problem for determining two depth distributions of two POMs. That is, if we have already known the amplitude distributions of the incident light field and output light field, how can we search for the optimal depth distributions of $h_1(x_1, y_1)$ and $h_2(x_2, y_2)$ to satisfy the predefined convergent criterion?

An iterative algorithm with the aid of the conjugate-gradient method (CGM)[11] is employed to solve this optimization problem. Initially, the depth distribution $h_1(x_1, y_1)$ of POM_1 is generated from a random number generator. Thus, the wavefunction on the plane P_1 at the wavelength λ_α can be obtained according to Eq.(1). After performing a Fresnel transform, the wavefunction $u_2'(x_2, y_2, \lambda_\alpha)$ on the plane P_2' at λ_α can be obtained by Eq.(4).

We denote $\rho_2(x_2, y_2, \lambda_\alpha)$ as the amplitude distribution of $u_2'(x_2, y_2, \lambda_\alpha)$ and $f_\alpha(x_3, y_3)$ as the amplitude distribution of the target image at the wavelength λ_α. By the known amplitude distribution $\rho_2(x_2, y_2, \lambda_\alpha)$ and the corresponding $f_\alpha(x_3, y_3)$, we can optimize the depth distribution $h_2(x_2, y_2)$ of POM_2 with the use of the CGM algorithm. For simplicity, we only give a brief description here.

We introduce the following error function to evaluate the performance of the designed depth distribution of the POM_2:

$$\begin{aligned} E = \sum_\alpha \Bigg\{ \sum_{x_3, y_3} \Bigg[& f_\alpha(x_3, y_3) \\ & - \Bigg| \sum_{x_2, y_2} g(x_3, y_3; x_2, y_2; z_2, \lambda_\alpha) \\ & \times \rho_2(x_2, y_2, \lambda_\alpha) \\ & \times \exp\left\{ \mathrm{i}\frac{2\pi}{\lambda_\alpha}[n_2(\lambda_\alpha) - 1]h_2(x_2, y_2) \right\} \Bigg| \Bigg]^2 \Bigg\}. \end{aligned} \tag{8}$$

The problem of designing the depth distribution of the POM_2 is attributed to minimize the error function E with respect to the unknown argument $\boldsymbol{h}_2$, i.e., the distribution of $h_2(x_2, y_2)$. In the CGM, the solution of the depth distribution $\boldsymbol{h}_2$ can be iteratively obtained from Ref.[11]:

$$\boldsymbol{h}_2^{(l+1)} = \boldsymbol{h}_2^{(l)} + \tau^{(l)} \boldsymbol{d}^{(l)}, \quad \text{for } l = 0, 1, 2, 3, \ldots \tag{9}$$

where $\boldsymbol{h}_2^{(l)}$,$\tau^{(l)}$, and $\boldsymbol{d}^{(l)}$ denote the depth distribution, the step size, and the search direction, respectively, in the lth iteration. The search direction $\boldsymbol{d}^{(l)}$ reads

$$\boldsymbol{d}^{(l)} = -\nabla E(\boldsymbol{h}_2^{(l)}) + \beta^{(l-1)} \boldsymbol{d}^{(l-1)}, \quad \text{for } l = 1, 2, 3, \ldots \tag{10}$$

where $\nabla E(\boldsymbol{h}_2^{(l)})$ is the gradient of the error function and $\beta^{(l-1)}$ is a factor defined by

$$\beta^{(l-1)} = \frac{|\nabla E(\boldsymbol{h}_2^{(l)})|^2}{|\nabla E(\boldsymbol{h}_2^{(l-1)})|^2}, \quad \text{for } l = 1, 2, 3, \ldots \tag{11}$$

To ensure the convergence of the iteration process, the step size $\tau^{(l)}$ should be selected to be small enough to satisfy the following relationship:

$$|\nabla E(\boldsymbol{h}_2^{(l+1)})| < |\nabla E(\boldsymbol{h}_2^{(l)})|.$$

The iteration process in the CGM can be started with a random initial depth distribution $\boldsymbol{h}_2^{(0)}$ and this process is continued until one of the following conditions is satisfied: (a) the modulus of the gradient of $E(\boldsymbol{h}_2^{(l)})$ reaches a small value less than ε, i.e. $|\nabla E(\boldsymbol{h}_2^{(l)})| \leq \varepsilon$, where ϵ is a given small quantity for the control of the calculation accuracy of the gradient, or (b) the number of iteration exceeds a given integer L.

Note that the above iteration process only involves an inner loop in the whole encryption procedure. Finally, the desired depth $h_2(x_2, y_2)$ is obtained. Then, we can acquire the wavefunction on the output plane P_3 according to Eqs.(5) and (6).

Let the phase distribution of $u_3(x_3, y_3, \lambda_\alpha)$ unchanged and adopt the expected normal distribution $f_\alpha(x_3, y_3)$ to replace the calculated amplitude distribution and compose a new field distribution

$$u_3'(x_3, y_3, \lambda_\alpha) = f_\alpha(x_3, y_3)\exp[\mathrm{i}\varphi_3(x_3, y_3, \lambda_\alpha)], \quad (12)$$

we then obtain a wavefunction $u_2(x_2, y_2, \lambda_\alpha)$ on the plane P_2 from an inverse Fresnel transform of the $u_3'(x_3, y_3, \lambda_\alpha)$ (see, Eq.(7)). The wavefunction on the plane P_2' is

$$\begin{aligned} & u_2'(x_2, y_2, \lambda_\alpha) \\ =& u_2(x_2, y_2, \lambda_\alpha) \\ & \times \exp\left\{ -\mathrm{i}\frac{2\pi}{\lambda_\alpha}[n_2(\lambda_\alpha) - 1]h_2(x_2, y_2)\right\}. \end{aligned} \quad (13)$$

The corresponding wavefunction on the plane P_1 at λ_α can be obtained:

$$u_1(x_1, y_1, \lambda_\alpha) = IFrT_{\lambda_\alpha}\{u_2'(x_2, y_2, \lambda_\alpha); z_1\}. \quad (14)$$

The depth distribution of POM_1 in the first iteration can be determined as

$$\begin{aligned} & h_1(x_1, y_1) \\ =& \frac{1}{2}\sum_{\alpha=1}^{2}\frac{\lambda_\alpha}{2\pi[n_1(\lambda_\alpha) - 1]}\mathrm{ang}\{u_1(x_1, y_1, \lambda_\alpha)\}, \end{aligned} \quad (15)$$

where $\mathrm{ang}\{\cdot\}$ denotes the phase-portion of the relevant function.

So far, a whole iterative encryption procedure is completed. The same procedure is repeated until the iteration times is larger than a predesigned number K. Finally, the optimal depth distributions of $h_1(x_1, y_1)$ and $h_2(x_2, y_2)$ of the POM_1 and POM_2 are determined. Two images corresponding to two different wavelengths are encoded into POMs held by one of three users. The POMs of the two other users can be obtained by using the same iteration algorithm.

2.3. Description of the verification procedure

Three sets of POMs are assigned to three users, every user holds two POMs which serve as his own decryption keys in the verification procedure. Meanwhile, every user uses four parameters, i.e., two wavelengths and two position parameters z_1 and z_2, as his personal identification numbers (PINs). In the verification stage, one user places his own two POMs in the optical verification system shown in Fig.1. Then, this user inputs his own four PINs into the system. Firstly, the verification system will adjust the correctness of the locations of the two POMs according to the two position parameters included in the input PINs. After this step, a plane wave with a given wavelength in the input PINs is used to illuminate the verification system, thus an image which denotes the verification information of the user is displayed on the P_3 plane. Similarly, a plane wave with the other given wavelength, in the input PINs will produce another image on the P_3 plane. Note that there are three target images which should be verified in the system, therefore, even two produced images of the verification user identify two target images, the user still cannot pass through the verification procedure. In this case, one of the other two authorized users can help him to open the lock in the verification system with the use of his own POMs and PINs because his POMs include the information of the third target image. That is to say, every two of the three authorized users can pass the verification procedure cooperatively. This distribution scheme of the decryption keys would definitely upgrade the security level of the verification system and it is convenient and flexible for users.

3. Numerical simulations of encryption and verification procedure

Suppose that three target images contain three different numeric-information, respectively, as shown in Fig.2.



(a) λ_1=0.5378μm (b) λ_2=0.6328μm (c) λ_3=0.6943μm

Fig.2. Three target images corresponding to three different wavelengths.

Three images correspond to three different wavelengths, e.g., $\lambda_1 = 0.5378\mu$m for the first picture, $\lambda_2 = 0.6328\mu$m for the second picture, and $\lambda_3 = 0.6943\mu$m for the third picture. We encrypt two of these images into the POMs of one user by using the encryption algorithm described in section 2.2. We suppose that every target picture possesses 200×200 pixels with 64 grey scale and the size of the image is 8 mm×8 mm. The spacing between planes P_1 and P_2' in Fig.1 is chosen to be $z_1 = 1000$ mm, and the distance between planes P_2 and P_3 is $z_2 = 1000$ mm. K5 glass is adopted as the material for fabricating these POMs. The refractive index of the K5 glass at room temperature is evaluated by[12]

$$\begin{aligned} n(\lambda) =& 2.2850299 - 8.6010725 \times 10^{-3}\lambda^2 + 1.1806783 \times 10^{-2}\lambda^{-2} + 2.0765657 \times 10^{-4}\lambda^{-4} \\ & - 2.1314913 \times 10^{-6}\lambda^{-6} + 3.2131234 \times 10^{-7}\lambda^{-8}, \end{aligned} \tag{16}$$

where λ is the incident wavelength and the unit of λ is μm. After passing 15 iteration loops, the depth distributions of two POMs for one user are determined. The depth distributions of the POMs for other two users can also be obtained by similar operation. So, three sets of POMs are produced for three users. The detailed distribution scheme is described as follows: The user U_a holds a set of POMs which comprise the information of two images associated with $\lambda_1 = 0.5378\,\mu m$ and $\lambda_2 = 0.6328\,\mu$m, the POMs of user U_b contain the image information associated with $\lambda_2 = 0.6328\,\mu$m and $\lambda_3 = 0.6943\,\mu$m; the user U_c holds the information associated with $\lambda_3 = 0.6943\,\mu$m and $\lambda_1 = 0.5378\,\mu$m. The obtained depth distributions of all the POMs are displayed in Fig.3.

The depth distributions in Figs.3(a_1) and (a_2) correspond to POM_1 and POM_2 of user U_a, respectively. Figures 3(b_1) and (b_2) represent the depth distributions of POM_1 and POM_2 of user U_b. Figures 3(c_1) and (c_2) display the depth distributions of POM_1 and POM_2 of user U_c. The grey level is proportional to the surface-relief depth in pixel. It is clearly seen that all these POMs are noise-like distributions and one cannot observe any information about the target images. Only when two POMs of one user are placed at the correct positions in the optical verification system and illuminated by the plane wave with the correct wavelength, a target image can then be displayed on the plane P_3. First, let us place two designed POMs of user U_a [i.e., the POMs as shown in Figs.3(a_1) and (a_2)] in the correct locations, which are illuminated by a plane wave with the wavelength $\lambda = 0.5378\,\mu$m in the optical verification system. The image in Fig.4(a) is displayed on the plane P_3.

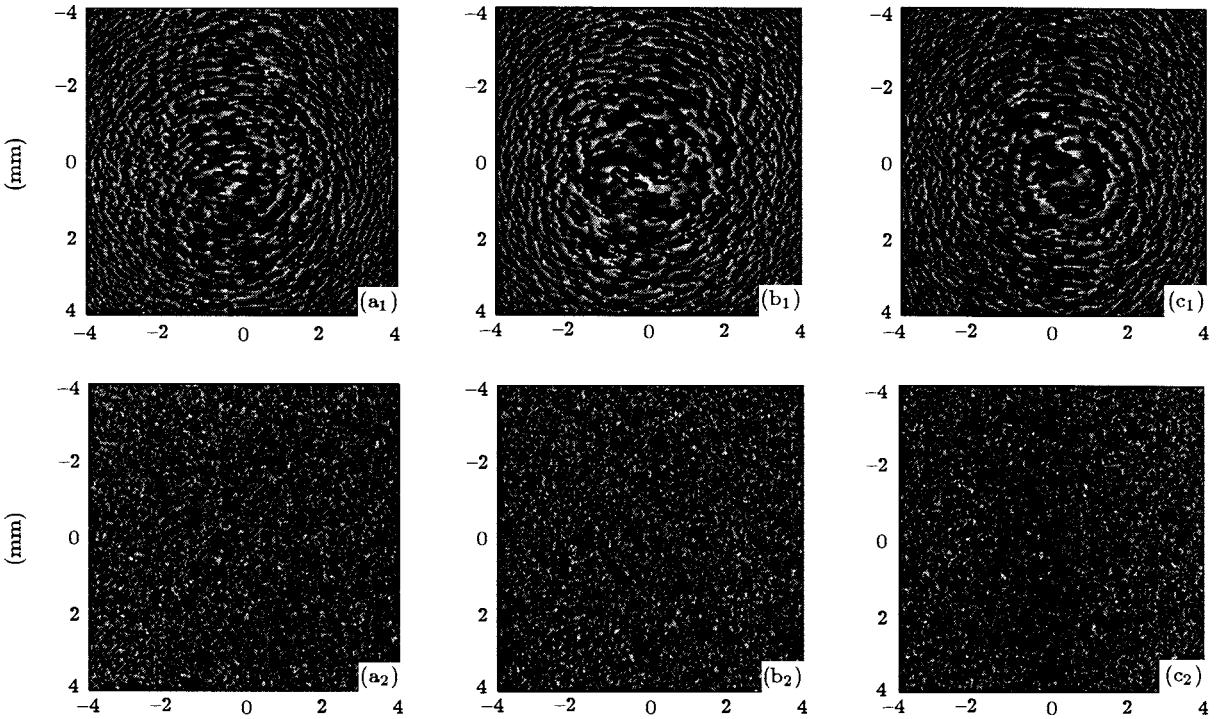
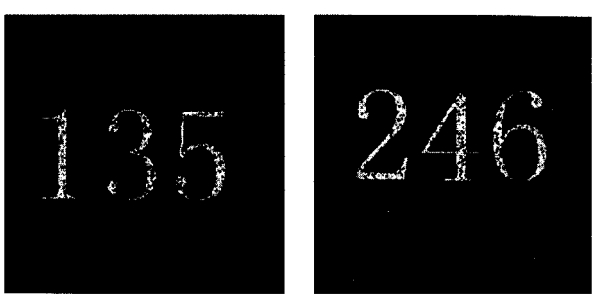


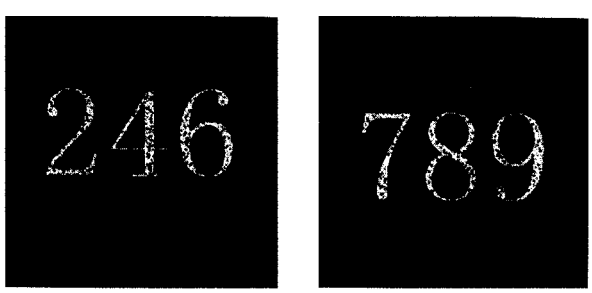
Fig.3. Depth distributions of three sets of designed POMs: (a_1) and (a_2) correspond to the first mask POM_1 and the second mask POM_2 of user U_a; (b_1) and (b_2) correspond to POM_1 and POM_2 of user U_b; (c_1) and (c_2) to POM_1 and POM_2 of user U_c. Note that the depth variations are [–1.8 μm, 1.8 μm] for POM_1 and [–1.5 μm, 1.5 μm] for POM_2.



(a) λ=0.5378μm (b) λ=0.6328μm

Fig.4. Reconstructed images by using the designed POMs and inputting all the correct PINs of user U_a: (a) The illumination wavelength is $\lambda_1 = 0.5378\,\mu$m; (b) the illumination wavelength is $\lambda_2 = 0.6328\,\mu$m.

For the incident plane wave with the wavelength $\lambda = 0.6328\,\mu$m, the expected image in Fig.4(b) can be displayed on the plane P_3. It can be found from Figs.2 and 4 that the generated images coincide with the expected target images quite well. According to the normal verification scheme, the user U_a can pass through the verification procedure, however, there is the third target image, as shown in Fig.2(c), should be verified in our proposed verification scheme, consequently, the user U_a is not allowed to pass the verification procedure. We put the two POMs of user U_b in the correct location of verification system, and use a plane wave with wavelength $\lambda = 0.6943\,\mu$m to illuminate the system, then an image appears, shown as in Fig.5(b).



(a) λ=0.6328μm (b) λ=0.6943μm

Fig.5. Reconstructed images by using the designed POMs and taking all the correct PINs of user U_b: (a) The illumination wavelength is $\lambda_1 = 0.6328\,\mu$m; (b) the illumination wavelength is $\lambda_2 = 0.6943\,\mu$m.

Up till now, all the three target images are reconstructed in the verification system correctly. So, the verification procedure is over and the users U_a and U_b can pass through together. That is, two users U_a and U_b can open the lock of the system and pass the verification system cooperatively, but one of them cannot do. There exists another scheme that can make user U_a open the lock, for instance, the third target image can also be generated by using the two POMs of user U_c, as shown in Fig.6(b).



Fig.6. Reconstructed images by using the designed POMs and chosen all the correct PINs of user U_c: (a) The illumination wavelength is $\lambda_1 = 0.5378\,\mu$m; (b) the illumination wavelength is $\lambda_2 = 0.6943\,\mu$m.

Similarly, the users U_b and U_c can also pass the verification procedure cooperatively. Three target images can be generated with the use of the POMs of U_b and U_c, e.g., the reconstructed images shown in Figs.5(a), 6(a), and 6(b), or, those shown in Figs.5(a), 5(b), and 6(a). Every two of the three users can pass through the verification procedure, which makes the verification system more convenient and flexible for users.

To describe the closeness of the reconstructed image to the target image quantitatively, we introduce a mean square error (MSE) defined as

$$\mathrm{MSE} = \frac{1}{M \times N} \sum_{m=1}^{M} \sum_{n=1}^{N} |r(m,n) - o(m,n)|^2, \quad (17)$$

where $M \times N$ is the number of the pixels. $r(m,n)$ and $o(m,n)$ denote the intensities of the reconstructed image and the target image on pixel (m,n), respectively. We analyse the influence of the wavelength deviation on the verification system, the obtained results are shown in Fig.7.

The results in Figs.7(a) and 7(b) are obtained by using the POMs of user U_a with the predesigned wavelengths $\lambda = 0.5378\,\mu$m and $\lambda = 0.6328\,\mu$m, respectively. It is evident from Fig.7(a) that the MSE is increased with the increase of the deviation of the illumination wavelength from the predesigned wavelength. The MSE reaches the smallest value of 0.01 when the illumination wavelength is just identical to the predesigned wavelength. The deviation of wavelength will lead to the worse qualities of the reconstructed images. The reconstructed image for $\lambda = 0.5478\,\mu$m is shown in Fig.8.

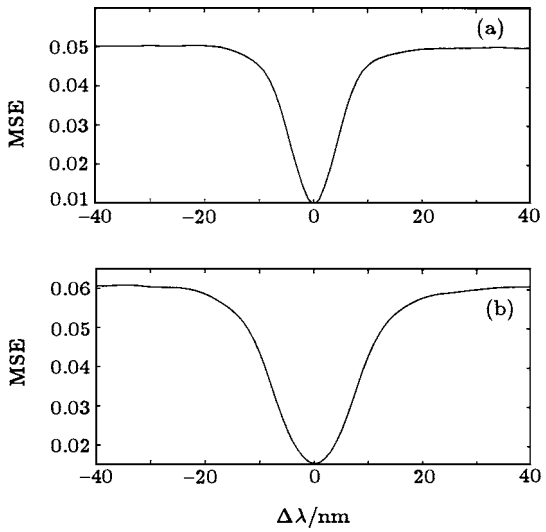


Fig.7. Variation of the MSEs versus $\Delta\lambda$: (a) Corresponding to a centre wavelength of $\lambda = 0.5378\,\mu$m; (b) corresponding to a centre wavelength of $\lambda = 0.6328\,\mu$m.

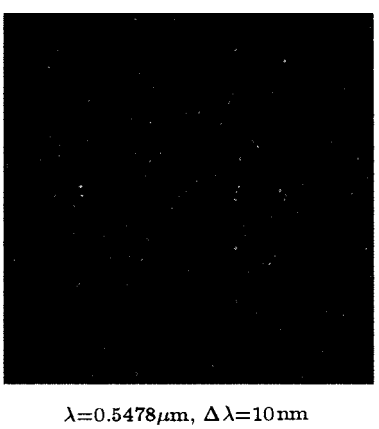


Fig.8. Incorrectly reconstructed images with the correct POMs of user U_a by using the incorrect illumination wavelength $\lambda = 0.5478\,\mu$m with $\Delta\lambda = 10$nm.

Although the deviation is only $\Delta\lambda = 10$nm, it is clearly seen that useful information now no longer appears in this reconstructed image. The similar results can be seen in Fig.7(b) although the change of MSE is smaller than that in Fig.7(a). Therefore, the wavelength information is very important for the verification procedure. Moreover, it is well-known that the correct position parameters are also important for passing the verification system.[7,8] The target image cannot be reconstructed correctly if the user does not hold the correct wavelength and position parameter information.

Moreover, we can extend the presented scheme to more users for further security of system. Suppose that there are five target images (denoted by I_k, k=1, 2, 3, 4, 5) associated with five different wavelengths.

Two of the five target images are encrypted into a set of POMs, and each set of POMs is distributed to one of the five authorized users (denoted by U_a, U_b, U_c, U_d, and U_e). The distribution scheme of information is chosen as follows: the user U_a holds the image information of I_1 and I_2; U_b carries that of I_2 and I_3; U_c retains that of I_3 and I_4; U_d has that of I_4 and I_5; and U_e possesses that of I_5 and I_1. Then, the following combinations of users can successfully reconstruct all the five target image information by using their own POMs co-operatively: 1) group of U_a, U_c, and U_d; 2) group of U_b, U_d, and U_e; 3) group of U_c, U_e, and U_a; 4) group of U_d, U_a, and U_b; 5) group of U_e, U_b, and U_c. This means that no less than three of the five authorized users can open the lock co-operatively. The security level of the verification system is improved.

The proposed distribution scheme can be used for authenticity verification of some banks, security departments, network, etc. The POMs can be embedded into the personal identification (ID) cards and assigned to all legal users that can be a group or some of the staff of a company. Every authorized user holds several PINs, which are equivalent to a set of passwords and should be the input into the system in the verification stage. None of these users can pass the verification procedure alone; only when several of the authorized users work together can they open the lock of system and pass the verification procedure. The proposed distribution scheme is convenient and flexible for all the authorized users. It is expected that this distribution scheme may be useful for further improving information and data security.

4. Conclusion

In summary, we have proposed a new distribution scheme of decryption keys for multi-wavelength information encryption technique in the Fresnel domain. The encryption procedure is digitally implemented with the use of an iteration algorithm in the computer. Three images are encoded into three sets of POMs, serving as the decryption keys by a special distribution method. Three sets of POMs are assigned to three authorized users. The verification procedure is performed in a lensless optical system. Every two of the three authorized users can pass the verification procedure cooperatively, but one user alone cannot do. The extended distribution scheme is also suited to a group of up to five users. Numerical simulations indicate that the proposed distribution scheme of decrypting keys can improve the security level of the verification system and it is more convenient and flexible for all the authorized users.

References

[1] Refregier P and Javidi B 1995 *Opt. Lett.* **20** 767
[2] Unnikrichnan G and Singh K 2000 *Opt. Eng.* **39** 2853
[3] Liu S, Yu L and Zhu B 2001 *Opt. Commun.* **187** 57
[4] Zhang Y, Zheng C H and Tanno N 2002 *Opt. Commun.* **202** 277
[5] Zhu B and Liu S 2001 *Opt. Commun.* **195** 371
[6] Zhu B and Liu S 2001 *Opt. Lett.* **26** 1242
[7] Matoba O and Javidi B 1999 *Opt. Lett.* **24** 762
[8] Situ G H and Zhang J J 2004 *Opt. Lett.* **29** 1584
[9] Ge D *et al* 2005 *Chin. Phys.* **14** 128
[10] Cao N W *et al* 2000 *Acta Phys. Sin.* **49** 61 (in Chinese)
[11] Avriel M 1976 *Nonlinear Programming: Analysis and Methods* (Prentice-Hall, Englewood Cliffs, N.J.) p299
[12] Michael B, Eric W V S, David R W and William L W 1995 *Handbook of Optics: Devices, Measurements, and Properties* 2st edn (McGraw-Hill, New York) p67