Optics Communications 359 (2016) 38–43

Contents lists available at ScienceDirect

Optics Communications

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

Multiple-image encryption based on computational ghost imaging

Jingjing Wu [a], Zhenwei Xie [a,b], Zhengjun Liu [c], Wei Liu [a], Yan Zhang [b], Shutian Liu [a,*]

[a] Department of Physics, Harbin Institute of Technology, Harbin 150001, PR China
[b] Department of Physics, Capital Normal University, Beijing 100048, PR China
[c] Department of Automation Measurement and Control, Harbin Institute of Technology, Harbin 150001, PR China

ARTICLE INFO

Article history:
Received 14 July 2015
Received in revised form
10 September 2015
Accepted 11 September 2015

Keywords:
Multiple-image encryption
Computational ghost imaging
Position multiplexing

ABSTRACT

We propose an optical multiple-image encryption scheme based on computational ghost imaging with the position multiplexing. In the encryption process, each plain image is encrypted into an intensity vector by using the computational ghost imaging with a different diffraction distance. The final ciphertext is generated by superposing all the intensity vectors together. Different from common multiple-image cryptosystems, the ciphertext in the proposed scheme is simply an intensity vector instead of a complex amplitude. Simulation results are presented to demonstrate the validity and security of the proposed multiple-image encryption method. The multiplexing capacity of the proposed method is also investigated. Optical experiment is presented to verify the validity of the proposed scheme in practical application.

1. Introduction

The optical image encryption technique is more and more attractive since Refrégiér and Javidi proposed an image encryption system based on double random phase encoding (DRPE) in 1995 [1]. Various security-enhanced methods were proposed [2–10] based on optical technology. To deal with multiple images simultaneously, various multiple-image encryption techniques were proposed [11–16]. Situ et al. proposed to use wavelength multiplexing [11] and position multiplexing [12] to realize the multiple-image encryption. However, the crosstalk among the encrypted images would tremendously reduce the quality of the decrypted images. Henao et al. [13] proposed an improved encryption method which can store multiple encrypted data into a single joint power spectrum by using plane reference waves with different incident angles. Except these, many multiple-image cryptosystems were proposed based on interference principle [17,18] and phase retrieval algorithm [19–21].

For most of these optical cryptosystems, the encoded results are complex amplitudes which increase the complexity of the recoding and transmission process. In 2010, Clemente et al. presented an optical encryption system based on computational ghost imaging [22]. In contrast to previous cryptosystems, the encrypted result of this scheme [22] is simply an intensity distribution instead of a complex-valued matrix. Ghost imaging is an intriguing optical technique and was experimentally realized by utilizing entangled two-photon pairs in 1995 [23]. Computational ghost imaging [24] is an ghost imaging arrangement that uses only a single-pixel detector by known speckle patterns. Several new image cryptosystems [25–29] and cryptanalysis schemes [30] based on computational ghost imaging were proposed in recent years.

In this work, we propose a multiple-image encryption scheme based on computational ghost imaging. In ghost imaging, the imaging result would be blurred if the difference in lengths between the object path and the reference path is larger enough [31,32]. Based on this property, in proposed scheme, each plain image is encrypted into an intensity vector by using the computational ghost imaging with different diffraction distances away from the source. All the intensity vectors are then superposed together to yield the final ciphertext. The proposed algorithm is quite straightforward and the ciphertext is simply an intensity vector. Numerical simulation and optical experiment are implemented to demonstrate the security and validity of proposed approach.

2. Proposed multiple-image encryption scheme

In conventional pseudothermal ghost imaging configuration, the pseudothermal light is generated by passing a laser beam through a rotating diffuser. The generated speckle beam is split into a signal beam and a reference beam. The signal beam passing through the object, which is located at a distance of z from the diffuser, is detected by a bucket detector with no spatial resolution. After propagating a distance z', the reference beam is

* Corresponding author. Fax: +86 451 86414335.
E-mail address: stliu@hit.edu.cn (Z. Liu).

http://dx.doi.org/10.1016/j.optcom.2015.09.039
0030-4018/

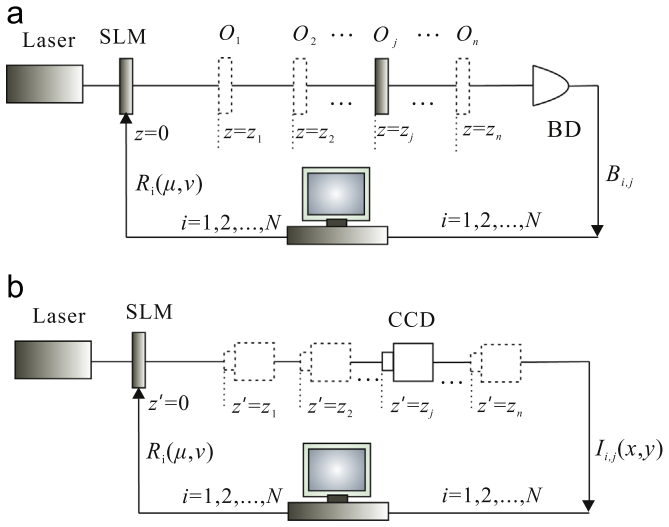

Fig. 1. Optical setup for proposed scheme. (a) Encryption procedure. (b) Decryption procedure. SLM represents spatial light modulator and BD represents bucket detector.

captured by a CCD camera. Here the CCD camera and the bucket detector are synchronized to ensure that the captured speckle image and the total intensity are correlated. If the distances z and z' are equal, after capturing and detecting a number of times, the image of the object could be obtained by the cross correlation of the speckle field and the total intensity [31]. While if $\Delta z_0 = z - z'$ is larger enough, the resolution of ghost imaging would comparable with the size of object, and the imaging result would be blurred [31,32]. We propose a multiple-image encryption method based on this property of ghost imaging.

In this work, the speckle field is generated by modulating a laser beam with a series of random phases introduced by an SLM, which is called computational ghost imaging [24]. The optical architecture of encryption process is shown in Fig. 1(a). The intensity transmission functions of the n images to be encrypted are represented by $O_j(x, y)$ ($j = 1, \ldots, n$). Firstly, to encrypt the first image, we put O_1 in the object path at position z_1 independently. The random phases introduced by pure phase SLM at ith time is represented by $R_i(\mu, \nu)$ ($i = 1, \ldots, N$). Hence the detect intensity sequence of BD is $B_{i,1}$

$$B_{i,1} = \sum_{x,y} I_{i,1}(x, y) O_1(x, y) \quad (i = 1, \ldots, N), \tag{1}$$

where $I_{i,1}(x, y)$ are the generated speckle fields illuminating on the object:

$$I_{i,j}(x, y) = \left| \mathrm{FrT}_{z_j}[R_i(\mu, \nu)] \right|^2 \quad (i = 1, \ldots, N), \tag{2}$$

where $\mathrm{FrT}_z[\cdot]$ denote the Fresnel transformation of distance z. Then remove O_1 from the object path and put O_2 at position z_2 to encrypt the second image with the same $R_i(\mu, \nu)$ ($i = 1, \ldots, N$). The detected intensity sequence of BD is $B_{i,2}$. Repeat the processes mentioned above until all n images are encrypted. The entire recoded results are $B_{i,j}$ ($i = 1, \ldots, N$; $j = 1, \ldots, n$). At last we superpose $B_{i,j}$ of every plaint image together to generate the final ciphertext

$$C_i = \sum_{j=1}^{n} B_{i,j} \quad (i = 1, \ldots, N). \tag{3}$$

The ciphertext C_i ($i = 1, \ldots, N$) is stored in an N-component positive number vector form and n images are encoded in it. $R_i(\mu, \nu)$ ($i = 1, \ldots, N$) and z_j ($j = 1, \ldots, n$) can be employed as keys.

The optical schematic of decryption is shown in Fig. 1(b) (this process can also be realized numerically). To decrypt the jth image, $R_i(\mu, \nu)$ ($i = 1, \ldots, N$) are introduced into the pure phase SLM one by one. The CCD is placed at $z' = z_j$. The detect results of CCD are equal to the speckle fields $I_{i,j}(x, y)$ representing in Eq. (2). The decrypted result of jth image $D_j(x, y)$ is the normalized second-order correlation of C_i and $I_{i,j}(x, y)$

$$D_j(x, y) = \frac{\langle I_{i,j}(x, y) C_i \rangle}{\langle I_{i,j}(x, y) \rangle \langle C_i \rangle} = \frac{\left\langle I_{i,j}(x, y) \sum_{j'=1}^{n} B_{i,j'} \right\rangle}{\langle I_{i,j}(x, y) \rangle \left\langle \sum_{j''=1}^{n} B_{i,j''} \right\rangle} \tag{4}$$

where $\langle \cdot \rangle \equiv (1/N) \sum_i \cdot$ denotes the average of N measurements. The $j' = j$ part in Eq. (4) is contributing to the correct ghost imaging O'_j, while $j' \neq j$ part will bring cross-talk noise because of the property of ghost imaging mentioned above. So Eq. (4) can be represented as

$$\begin{aligned} D_j(x, y) &= \frac{\langle I_{i,j}(x, y) B_{i,j} \rangle}{\langle I_{i,j}(x, y) \rangle \langle \sum_{j''=1}^{n} B_{i,j''} \rangle} + \frac{\langle I_{i,j}(x, y) \sum_{j' \neq j} B_{i,j'} \rangle}{\langle I_{i,j}(x, y) \rangle \langle \sum_{j''=1}^{n} B_{i,j''} \rangle} \\ &= r_j O'_j(x, y) + n(x, y), \end{aligned} \tag{5}$$

in which r_j is a constant equal to $\langle B_{i,j} \rangle / \langle \sum_{j''=1}^{n} B_{i,j''} \rangle$. $n(x, y)$ is cross-talk noise. Eq. (5) is actually a superposition of the ghost imaging result and the cross-talk noise. Although the cross-talk cannot be avoided in the decryption result, it can be dramatically reduced by utilizing a Gaussian low pass filter. All the plaint images can be decrypted through this way.

The finial ciphertext is an intensity vector. The results need to detect and record in the encrypting process are also intensity values. Hence the detecting process of proposed scheme is more convenient than other multiple images' encryption systems. This is the characteristic of proposed multiple-image encryption scheme.

3. Simulation and discussion

In this part, we firstly confirm the minimum distance Δz between two images under the simulation condition. Then the appropriate z_j ($j = 1, \ldots, n$) are used to encrypt n images by simulation. At last the security and the multiplexing capacity are analyzed by simulation results.

Firstly, a binary image with the size of 50×50 pixels (shown in Fig. 2(a)) is used to investigate the influence of Δz_0 on the imaging quality. The measurement times are $N = 5000$. $z = 5 \times 10^{-2}$ m. When Δz_0 is 2×10^{-4} m, 4×10^{-4} m, 6×10^{-4} m, 8×10^{-4} m, 1×10^{-3} m, the ghost imaging results are shown in Fig. 2(b)–(f), respectively. Fig. 2(g) shows the correlation coefficient (CC) between the original image and the recovered image versus Δz_0. CC between the original image O and the decrypted result D is defined as

$$\mathrm{CC} = \left| \frac{E\{[O - E(O)][D - E(D)]\}}{\{E\{[O - E(O)]^2\} E\{[D - E(D)]^2\}\}^{1/2}} \right| \tag{6}$$

in which $E\{\cdot\}$ is an expectation operator. The CC value is used to weighting the quality of recovered image. If CC = 1, it means that O and D are the same. It can be learning from Fig. 2 that the CC decrease rapidly with the increase of $|\Delta z_0|$ and the imaging result will be noise-like when $\Delta z_0 \geq 1 \times 10^{-3}$ m. Hence the minimum distance between two images Δz should satisfy $\Delta z \geq 1 \times 10^{-3}$ m under the same simulation condition in this paper.

We now consider encrypting $n = 15$ binary images and the size of each is 50×50 pixels. The wavelength of the light source is $\lambda = 632.8$ nm. The actual size of the images is 8 mm × 8 mm in the simulation. The measurement times are $N = 30{,}000$. The position of