Optik 126 (2015) 3210–3214

Contents lists available at ScienceDirect

Optik

journal homepage: www.elsevier.de/ijleo

Optical multiple-image encryption based on fully phase encoding and interference

Xiaopeng Deng*, Wei Wen

Department of Physics and Information Engineering, Huaihua University, Huaihua 418008, China

ARTICLE INFO

Article history:
Received 18 June 2014
Accepted 19 July 2015

Keywords:
Multiple-image encryption
Fully phase encoding
Interference

ABSTRACT

We propose a new method for multiple-image encryption based on fully phase encoding and interference. Firstly, all images to be encrypted are encoded separately into a phase-only image with the help of the fully phase encoding rather then the sophisticated and time-consuming iterations in computer, and then these phase-only images are intermodulated into a single phase-only image by multiplication. Finally, the single phase-only image is used as the input image to be encrypted by the double random phase encoding system. In the process of the decryption, all plaintexts can be accurately recovered from the ciphertext with the corresponding decryption keys based on interference rather than the complicated phase-contrast technique. Simulation results are presented to demonstrate the feasibility and effectiveness of the proposed method.

1. Introduction

Optical image encryption techniques have played an important role in the field of information security because of high-speed processing two-dimensional complex data in parallel. In the past two decades, many techniques have been proposed for optical image encryption and hiding [1–8] since the double random phase encoding algorithm was proposed by Réfrégier and Javidi in 1995 [8]. However, most of the encryption techniques proposed in the above-mentioned papers are not suited for multiple-image encryption. In order to transmit more information and increase encryption efficiency, Situ and Zhang first proposed the multiple-image encryption technique based on wavelength multiplexing [9]. After that, many approaches, such as position multiplexing [10], key rotation multiplexing [11], random phase matching [12], and spread-space spread-spectrum multiplexing [13], have been proposed for multiple-image encryption. However, these techniques are in fact much more suitable for binary image encryption because of the cross-talk noise, which usually cannot be avoided in these encryption methods because the final encrypted image is obtained by direct superposition and recorded on a single medium. In addition, the encryption capacity is also limited in these encryption methods. To overcome the cross-talk problem and increase encryption capacity, many improved multiple-image encryption techniques have been proposed [14–21]. In the encryption process of these improved methods, all images to be encrypted are required to be encoded separately into one or more phase-only masks with all kinds of phase retrieval algorithms. As we know, the iterative process is a time-consuming process, which will drastically reduce the efficiency of the encryption. So although in these improved methods the encryption capacity is considerably enhanced without the cross-talk noise, the time-consuming computation becomes an inevitable problem. In addition, all plaintexts can only be approximately recovered because of applying phase retrieval algorithm in these methods.

In this paper, we propose a new method for multiple-image encryption based on fully phase encoding and interference. Similar to the above improved multiple-image encryption method based on all kinds of phase retrieval algorithm [14–21], in our method all images to be encrypted also are first encoded separately into a phase-only image with the help of the fully phase encoding in computer. Then these phase-only images are intermodulated into a single phase-only image by multiplication. Finally, the single phase-only image is used as the input image to be encrypted by the double random phase encoding system [8]. In the process of the decryption, all plaintexts can be accurately recovered from the ciphertext with the corresponding decryption keys based on interference. Compared with the methods proposed in Refs. [9–13], our method can overcome the problems of cross-talk noise and encryption capacity. Also, compared with the improved methods in Refs. [14–21], our method does not require sophisticated and time-consuming iteration computation and all plaintexts can be

* Corresponding author. Tel.: +86 0745 2851011; fax: +86 0745 2851011.
E-mail address: dxpzqh@163.com (X. Deng).

http://dx.doi.org/10.1016/j.ijleo.2015.07.148
0030-4026/

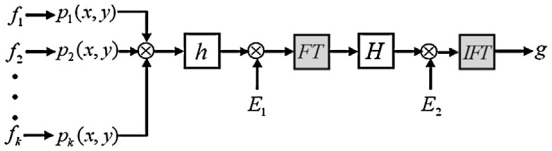

Fig. 1. Flow chart of the encryption process.

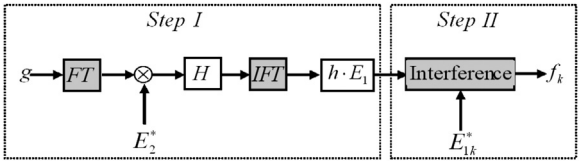

Fig. 2. Flow chart of the decryption process.

accurately recovered based on simple interference rather than the complicated phase-contrast technique that converts a phase image into an intensity pattern [22–24]. Although in our method the fully phase encoding process is also implemented in computer, the computation process is very simple compared with that of the phase retrieval algorithm. In addition, the fully phase-based encryption technique has at least two advantages. One is that fully phase encryption is more secure than amplitude encryption [25]. The other is that the decrypted information obtained from fully phase-based encryption is much more robust to additive noise than that obtained from amplitude-based encryption [26].

2. Method description

The process of the encryption is shown in Fig. 1. Similar to the optical encryption techniques based on fully phase-based encoding [24,25,27,28], in our method all images to be encrypted also are first encoded separately into a phase-only image in computer.

Suppose that N is the number of images to be encrypted, and $f_k(x,y)$, which is normalized in advance to ensure its pixel values are in (0, 1), denotes the kth positive-real image to be encrypted. The fully phase encoding can be realized in computer by the following expression

$$p_k(x,y) = \exp\{i \ \text{arc cos}[\sqrt{f_k(x,y)} - 1]\} \tag{1}$$

where the reason why the normalized $f_k(x, y)$ is nonlinearly transformed before fully phase-based encoding is to ensure that gray-scale image also can be accurately recovered based on interference, which can be seen from the following decryption process. In order to obtain a single encrypted image, all phase-only images are intermodulated into a single phase-only image by multiplication. Thus the single phase-only image can be expressed as

$$h(x,y) = \exp\{i\sum_{k=1}^{N} \text{arc } cos[\sqrt{f_k(x,y)} - 1]\}. \tag{2}$$

Finally, the single phase-only image $h(x, y)$ is used as the input image to be encrypted by the double random phase encoding system [8], which can be expressed by the following two equations

$$H(u,v) = FT[h(x,y) \cdot E_1(x,y)] \tag{3}$$

$$g(x,y) = IFT[H(u,v) \cdot E_2(u,v)], \tag{4}$$

where $FT(\cdot)$ and $IFT(\cdot)$ denote Fourier transform and inverse Fourier transform, respectively. $E_1(x, y)$ and $E_2(u, v)$ are two different random phase functions and used as the two encryption keys. It can be seen from Eqs. (2)–(4) that $g(x, y)$, which is served as the final ciphertext of all plaintexts, contains information of all plaintexts because of intermodulation.

The decryption process, as shown in Fig. 2, can be described as the following two steps. The first step is to recover $h(x,y) \cdot E_1(x,y)$ by using the decryption key $E_2^*(u, v)$ based on the double random phase encoding system [8], which can be described as follows. Firstly, with $E_2^*(u, v)$ as the decryption key, we can obtain $H(u, v)$ by

$$H(u,v) = FT[g(x,y] \cdot E_2^*(u,v), \tag{5}$$

where the superscript * denotes conjugate operation. Then $H(u, v)$ is inverse Fourier transformed to obtain

$$IFT[H(u,v)] = h(x,y) \cdot E_1(x,y) \tag{6}$$

Up to this point, we have recovered $h(x,y) \cdot E_1(x,y)$. Although the single phase-only image $h(x, y)$ can be recovered easily if $E_1^*(x, y)$ is served as another decryption key, the phase-only image $p_k(x, y)$ cannot be recovered because of intermodulation. Moreover, light intensity detectors cannot read the content of the phase-only image $p_k(x, y)$ even if we have recovered it. So we must use other method to reconstruct the original image $f_k(x, y)$, which is just the aim of the second step.

For ease of description, we define $E_{1k}(x, y)$ as

$$E_{1k}(x,y) = \exp\{i\sum_{n \neq k}^{N} \text{arc } cos[\sqrt{f_n(x,y)} - 1]\} \cdot E_1(x,y)$$
$$(n,k) \in [1,N] \tag{7}$$

Thus based on Eq. (7), we can rewrite Eq. (6) as

$$h(x,y) \cdot E_1(x,y) = p_k(x,y) \cdot E_{1k}(x,y) \tag{8}$$

It can be seen from Eq. (8) that in order to reconstruct the original image $f_k(x, y)$, $E_{1k}(x, y)$ in Eq. (8) must be canceled out, and then the phase-only image $p_k(x, y)$ must be converted into the intensity pattern $f_k(x, y)$. Although various techniques, such as phase-contrast technique, have been applied for imaging and visualization of phase objects [22–24], most of them need to pre-fabricate filter and their optical implementation is very complicated. So in this paper we apply the simple interference technique rather than the complicated phase-contrast technique for imaging and visualization of the phase-only image $p_k(x, y)$. Meanwhile, the interference method can also cancel out $E_{1k}(x, y)$ if we use $E_{1k}(x, y)$ as reference wave. In the following section, we will describe the interference method in detail.

The imaging and visualization process based on interference is simply performed by interfering between $h(x,y) \cdot E_1(x,y)$ and a reference wave $E_{1k}(x, y)$, and can be optically realized by a simple Mach–Zehnder interferometer architecture [27–29]. The interference of the two optical path is given by

$$\begin{aligned} I(x,y) &= \left|E_{1k}(x,y) + h(x,y) \cdot E_1(x,y)\right|^2 = \left|E_{1k}(x,y)\right|^2 \left|1 + p_k(x,y)\right|^2 \\ &= \left|1 + \exp\{i \ \text{arc}\, cos[\sqrt{f_k(x,y)} - 1]\}\right|^2 \\ &= \left|2 + 2\sqrt{f_k(x,y)} - 2\right|^2 = 4f_k(x,y). \end{aligned} \tag{9}$$

It can be seen from Eq. (9) that the original image $f_k(x, y)$ can be accurately recovered from the interference intensity distribution $I(x, y)$ if $E_{1k}(x, y)$ is used as the reference wave. Moreover, in our method gray-scale image as well as binary image will not suffer from nonlinear effects introduced by the cosine function because the original image $f_k(x, y)$ is nonlinearly transformed in advance.

It is also can be seen from the whole decryption process that $E_{1k}(x, y)$ and $E_2^*(u, v)$ are essential for reconstructing the original image. So $E_{1k}(x, y)$, which can be pre-generated digitally based on Eq. (7) in the encryption process, and $E_2^*(u, v)$ are served as the decryption keys of this multiple-image encryption system. Based on their different roles in the decryption process, we can refer