Optics Communications 426 (2018) 497–505

Contents lists available at ScienceDirect

Optics Communications

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

# Parallel encryption and hierarchical retrieval for multi-channel images using an optical joint Fresnel transform correlator

Jie Liu [a,b,*], Tingzhu Bai [a], Xueju Shen [b], Shuaifeng Dou [b], Chao Lin [c], Qi Chen [b], Jiaju Ying [b]

[a] Key Laboratory of Photoelectric Imaging Technology and System, Ministry of Education of China, School of Optoelectronics, Beijing Institute of Technology, Beijing 100081, China

[b] Department of Opto-Electronics Engineering, Shijiazhuang Campus, AEU, Shijiazhuang 050000, China

[c] Department of Control Engineering, Yantai Aviation University, Yantai 264001, China

ARTICLE INFO

*Keywords:*
Optical encryption
Multi-channel images
Joint Fresnel transform correlator
Hierarchical retrieval

ABSTRACT

We propose an optical encryption method allowing the parallel encryption and hierarchical retrieval for multi-channel images based on a joint Fresnel transform correlator. In our designed scheme, the linear phase shift operation for the phase masks is utilized to achieve the aim of ensuring that the center of the complex amplitude distributions from the same group can overlap with each other in Fresnel domain, and the phase retrieval algorithm for designing the phase masks is used to avoid the cross talk between multi-channel images. The optimized phase masks can be flexibly reconfigured on the spatial light modulator without increasing the additional optical hardware and system complexity. Our designed scheme can encrypt multi-channel images simultaneously into a single cipher-text, which can also be used to recover arbitrary original images with corresponding keys. Thus, this method can achieve the aim of the hierarchical retrieval of encrypted images from a single cipher-text. Moreover, because the encryption process does not require any transformative lenses and accurate alignment of optical elements, the encryption scheme is easy to be optically implemented. Furthermore, compared with the previous JTC-based cryptosystems, the Fresnel diffraction distance and the position of the key masks in our proposed scheme can both be utilized as the additional encryption keys, which can enhance the security effectively. The theoretical analysis and numeric simulation results both validate the feasibility and effectiveness of the designed scheme.

## 1. Introduction

The optical image encryption technique has become more and more attractive since Refregier and Javidi proposed an image encryption method based on double random phase encoding in 1995 [1]. Benefitting from the inherent nature of light waves, information security with optics can achieve ultrafast processing and multiple degrees of freedom encoding capability. Some typical optical information-processing methods have been proposed for security applications [2–13]. Especially in the joint transform correlator (JTC)-based image cryptosystem [3,14–16], the decryption utilizes the same key used in encryption stage, which eliminates the need to generate a complex conjugate of the key. And moreover, the JTC-based cryptosystem can be implemented without accurate optical alignment.

In recent years, multiple-image encryption (MIE) technique [17–29] has caught increasing attention due to its high encryption efficiency. Situ proposed the technique of wavelength multiplexing [17] and position multiplexing [18] to realize the multiple-image encryption. Barrera et al. [19] designed a polarization encoded encryption system based on a double random pure phase mask technique and retardation plate. Amaya [20] proposed a multi-channel encryption method by using multiple random-phase mask apertures in the input plane based on a JTC scheme. Aperture keys with precise distance and geometric parameters are used to access the system. H.T. Chang et al. [23] proposed a position multiplexing method based on the modified Gerchberg–Saxton algorithm and a cascaded phase modulation scheme in the Fresnel transform domain. Rueda et al. [24] proposed an experimental procedure to multiplex optical information by using the JTC architecture. The rotation of the input plane encoding mask admits the multiplexing capability. J. Wu et al. [27] proposed an optical multiple-image encryption scheme based on computational ghost imaging with the position multiplexing. In the encryption process, each image is encrypted into an intensity vector by using the computational ghost imaging with a different diffraction distance.

* Corresponding author at: Department of Opto-Electronics Engineering, Shijiazhuang Campus, AEU, Shijiazhuang 050000, China.
*E-mail address:* yclj07@163.com (J. Liu).

https://doi.org/10.1016/j.optcom.2018.06.005
Received 12 April 2018; Received in revised form 16 May 2018; Accepted 1 June 2018

In our previous work [30], we proposed the parallel encryption method based on a JTC architecture and validated the feasibility by means of numerical simulation and optical experiment. In order to further simplify the optical hardware and enhance the security, we design a parallel encryption scheme based on a joint Fresnel transform correlator(JFTC). The remaining sections of this paper are organized as follows: Section 2 introduces the methods of linear phase shift and phase retrieval in detail, and then analyzes the parallel encryption process and hierarchical retrieval process by means of the theoretical derivation. Section 3 presents the numerical simulation results to demonstrate the performance of the scheme. Section 4 states the conclusions.

## 2. Principle of multi-channel parallel encryption using JFTC

### 2.1. Parallel encryption process

Key phase masks and multi-channel input images are arranged in the input plane, which is shown in Fig. 1(a). The input image $f_1$ is attached with random phase mask (RPM) $\alpha_0$. In order to realize hierarchical retrieval, the key phase mask $h_{10}$ is placed side by side with $f_1 \bullet \alpha_0$ and they constitute a group for JFTC. Also, the input image $f_2$ attached with RPM $\beta_0$ and key phase mask $h_{20}$ constitute the second group. The input image $f_3$ attached with RPM $\gamma_0$ and key phase mask $h_{30}$ constitute the last group. As shown in Fig. 1(a), $a$ is the distance between the centers of all input apertures and $y$ axis in the horizontal direction, and $b$ is the distance between the centers of all input apertures and $x$ axis in the vertical direction. As shown in Fig. 1(b), under the illumination of a monochromatic plane wave with wavelength $\lambda$, the joint Fresnel power distribution (JFPD) can be captured in the output plane with a distance $d$ away from the input plane. Fig. 1(c) shows the optical configuration of the encryption scheme. The intensity of the laser can be changed by the attenuator. The input images are uploaded to SLM1, which is the amplitude-only spatial light modulator (SLM) and used for amplitude modulation. All the phase masks are uploaded to SLM2, which is the phase-only reflective SLM and used for phase modulation. After the reflection of SLM2 and light splitter, the JFPD can be recorded by a CCD on the recording plane with a distance $d$ away from the SLM2 and transmitted as the cipher-text. In Fig. 1(c), $d$ is the sum of the distance $d_1$ and $d_2$. Whereas, due to the space-variant characteristics of the JFTC scheme [31], the center of the two beams that propagate through the object window and key window cannot overlap with each other in the output plane. Therefore, the key masks and phase masks boned with the input images should be modified to solve this problem. Shen et al. [31] utilized double optical wedges to achieve that the complex amplitude distribution of both input windows can spatially overlap with each other. Certainly, superposing the linear phase on the phase masks with SLM also can be utilized to solve this problem. After this modulation operation, all the phase masks in Fig. 1 can be expressed as

$$\alpha_0'(x_1 - a, y_1 + b) = \alpha_0(x_1 - a, y_1 + b) \bullet p_1(x_1) \tag{1}$$

$$h_{10}'(x_1 + a, y_1 + b) = h_{10}(x_1 + a, y_1 + b) \bullet p_1'(x_1) \tag{2}$$

$$\beta_0'(x_1 - a, y_1) = \beta_0(x_1 - a, y_1) \bullet p_2(x_1) \tag{3}$$

$$h_{20}'(x_1 + a, y_1) = h_{20}(x_1 + a, y_1) \bullet p_2'(x_1) \tag{4}$$

$$\gamma_0'(x_1 - a, y_1 - b) = \gamma_0(x_1 - a, y_1 - b) \bullet p_3(x_1) \tag{5}$$

$$h_{30}'(x_1 + a, y_1 - b) = h_{30}(x_1 + a, y_1 - b) \bullet p_3'(x_1) \tag{6}$$

where, $\alpha_0'$, $h_{10}'$, $\beta_0'$, $h_{20}'$, $\gamma_0'$ and $h_{30}'$ denote the modulation results of $\alpha_0, h_{10}, \beta_0, h_{20}, \gamma_0$ and $h_{30}$, which are superposed with the respective linear phase $p_1(x_1), p_1'(x_1)$, $p_2(x_1)$, $p_2'(x_1)$, $p_3(x_1)$ and $p_3'(x_1)$. Then, the complex amplitude distribution in the output plane can be written as

$$E(x_2, y_2) = \mathrm{FrT}_{\lambda,z}\{\alpha_0' f_1 + h_{10}' + \beta_0' f_2 + h_{20}' + r_0' f_3 + h_{30}'\} \tag{7}$$

where, FrT denotes the Fresnel transform operator. $\lambda$ is the wavelength of the incident plane wave. $z$ represents the distance between the input plane $(x_1, y_1)$ and output plane $(x_2, y_2)$. However, because of the utilization of RPMs, the JFPDs from different groups will overlap partially with each other in the output plane and this causes cross talk, which is the primary problem in multi-channel encryption.

In order to solve the cross talk problem, we utilize the phase retrieval algorithm to redesign all the phase masks and restrict the size of their corresponding complex amplitude distribution. Ref. [32] proposed an iteration method to design the input phase mask in a JTC architecture. The Fourier spectrum can be set in a specified domain, which can match to the space bandwidth of the optical system. Based on this iteration method [32], we propose a phase retrieval algorithm to solve the cross talk problem in Fresnel domain. The proposed algorithm as shown in Fig. 2 starts with the initial random phase mask $m_0(x_1, y_1)$. After the Fresnel transform operation, the complex amplitude distribution can be expressed as $M_N(x_2, y_2)$. C{} denotes the extracted operation in the output plane. In the extracted area, the complex amplitude distribution will be retained. Otherwise, it will be set to 0 value. After this operation, the complex amplitude distribution can be expressed as $M_N'(x_2, y_2)$. The power transmittance ratio (PTR) of the extracted area is utilized as the criterion [32] and defined by

$$PTR = \frac{\sum_{(x_2,y_2)\in\Omega} |M|^2}{\sum_{(x_2,y_2)} |M|^2} \tag{8}$$

where, $M$ and $\Omega$ denote the complex amplitude distribution and the extracted area, respectively. The processing cycle will be iterated until the PTR can get our expected value. Otherwise, $M_N'(x_2, y_2)$ will be inverse Fresnel-transformed and a new phase mask can be given by $m_N'(x_1, y_1)$. F{} denotes the operation of setting the amplitude to unity. At last, we can get the input phase mask $m_{N+1}(x_1, y_1)$, which will be sent into the next cycle. Once the PTR gets the expected value, we will get the input phase mask we wanted.

Using the designed phase masks superposed with the respective linear phases $p_1, p_1'$, $p_2$, $p_2'$, $p_3$ and $p_3'$, the JFPD from the different groups will be set into the respective area and the cross talk problem can be solved. Thus, the JFPD in the output plane can be expressed as

$$\begin{aligned} JFPD(x_2, y_2) = &\left|\mathrm{FrT}_{\lambda,z}\{\alpha' f_1 p_1 + h_1' p_1'\}\right|^2 + \left|\mathrm{FrT}_{\lambda,z}\{\beta' f_2 p_2 + h_2' p_2'\}\right|^2 \\ &+ \left|\mathrm{FrT}_{\lambda,z}\{r' f_3 p_3 + h_3' p_3'\}\right|^2 \end{aligned} \tag{9}$$

where, $\alpha'$, $h_1'$, $\beta'$, $h_2'$, $\gamma'$ and $h_3'$ denote the iterated phase masks. For simplicity, the second term of Eq. (9) will be analyzed and its complex amplitude distribution can be expressed as

$$\begin{aligned} E_2(x_2, y_2) = &\ \mathrm{FrT}_{\lambda,z}\{\beta'(x_1 - a, y_1) f_2(x_1 - a, y_1) \exp(j\frac{2\pi\theta_1}{\lambda} x_1)\} \\ &+ \mathrm{FrT}_{\lambda,z}\{h_2'(x_1 + a, y_1) \exp(j\frac{2\pi\theta_2}{\lambda} x_1)\} \end{aligned} \tag{10}$$

where, $\theta_1$ and $\theta_2$ denote the deflection angle in the linear phase $p_2$ and $p_2'$, respectively.

After setting $x_1' = x_1 - a$, the first term of Eq. (10) can be rewritten as

$$\begin{aligned} E_{21}(x_2, y_2) = &\ \exp[-j\frac{\pi}{\lambda z}(2ax_2 - a^2 - 2z\theta_1 a)]\mathrm{FrT}_{\lambda,z}\{\beta'(x_1', y_1) \\ &\times f_2(x_1', y_1)\}(x_2 - a - z\theta_1, y_2). \end{aligned} \tag{11}$$

After setting $x_1'' = x_1 + a$, the second term of Eq. (10) can be rewritten as

$$\begin{aligned} E_{22}(x_2, y_2) = &\ \exp[j\frac{\pi}{\lambda z}(2ax_2 + a^2 - 2z\theta_2 a)] \\ &\times \mathrm{FrT}_{\lambda,z}\{h_2'(x_1'', y_1)\}(x_2 + a - z\theta_2, y_2). \end{aligned} \tag{12}$$

From Eqs. (11) and (12), let $a + z\theta_1 = -a + z\theta_2$, that is

$$z(\theta_2 - \theta_1) = 2a. \tag{13}$$

Then, the center of the two beams that propagate through the object window and key window can overlap with each other in the output plane. In addition, when Eq. (13) can be satisfied, we can change the