Optics Communications 396 (2017) 174–184

Contents lists available at ScienceDirect

Optics Communications

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

Parallel encryption for multi-channel images based on an optical joint transform correlator

Jie Liu[a,b,*], Tingzhu Bai[a], Xueju Shen[b], Shuaifeng Dou[b], Chao Lin[b], Jianjun Cai[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, Mechanical Engineering College, Shijiazhuang 050000, China

ARTICLE INFO

Keywords:
Optical encryption
Multi-channel images
Joint transform correlator

ABSTRACT

We propose an optical encryption method allowing the parallel encryption for multi-channel images based on a joint transform correlator (JTC). Distinguished from the conventional multi-image encryption methods, our proposed cryptosystem can encrypt multi-channel images simultaneously into a single ciphertext, which also can be used to recover arbitrary original images with corresponding keys. This method can achieve the compressed storage of ciphertext. In order to avoid the cross talk between multi-channel images, we restrict the respective joint power spectrum (JPS) into a specific area with optimized phase masks and split the multiple JPS by controlling the position of single JPS using the linear phase shifts. All of these operations are realized by optimizing and designing the phase masks which can be flexibly reconfigured on the spatial light modulator (SLM), leading to a feasible optical implementation with no increase of optical hardware and complexity. Computer simulations provide the validation for it. Experimental implementation is performed in a JTC-based cryptosystem to further verify the feasibility of our proposed method.

1. Introduction

With the rapid development of computer and Internet technology, information security has attracted more and more interests of many researchers. Due to the ultrafast and multidimensional processing, optical information security technique has been popular for a long time.

Some typical optical information-processing methods have been proposed for security applications [1–6]. Especially in the joint transform correlator (JTC) –based image cryptosystem [3,7–10], the decryption utilizes the same key as used in the 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, which is easy to attain in practice.

To increase the encryption efficiency for a large number of images, some researchers proposed lots of methods to implement double-image and multi-image encryption [11–18]. In particular, Situ [11] achieved multiple-image encryption with the technique of wavelength multiplexing into a double random-phase encoding system. Amaya [13] proposed a multichanneling 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. A photorefractive crystal is used to record the different encryption data. Amaya [15] also showed that multiple secure data recording under a wavelength multiplexing technique was possible in a JTC arrangement. Barrera [17] presented the first experimental technique to encrypt a movie under a JTC architecture. They applied a virtual optical implementation to remove unwanted information and then to reposition the encoded image before data multiplexing.

In the application area of multi-image encryption, the data volume of ciphertext, cross talk and cryptosystem complexity should be comprehensively considered. In our previous work [19,20], we found that it was feasible to control the joint power spectrum (JPS) area accurately with optical wedges and SLM. Thus, with further simulation and experiment, we provide the theoretical and experimental validation for the feasibility of our proposed parallel encryption method. In our proposal, without increasing the complexity of cryptosystem based on a JTC scheme, multi-channel images can be encrypted simultaneously and recovered with corresponding decrypted keys without cross talk. This encryption strategy may provide some ideas for the field of multi-image encryption, video encryption and multi-level authorization management.

In Section 2, we analyze the feasibility of the proposed system and describe the adjustment method of JPS, which is crucial for our cryptosystem. In order to verify our proposed system, in Section 3, we describe the computer simulation results and analyze some

* Corresponding author at: Key Laboratory of Photoelectric Imaging Technology and System, Ministry of Education of China, School of Optoelectronics, Beijing Institute of Technology, Beijing 100081, China.
E-mail address: yclj07@163.com (J. Liu).

http://dx.doi.org/10.1016/j.optcom.2017.03.049
Received 24 January 2017; Received in revised form 9 March 2017; Accepted 21 March 2017

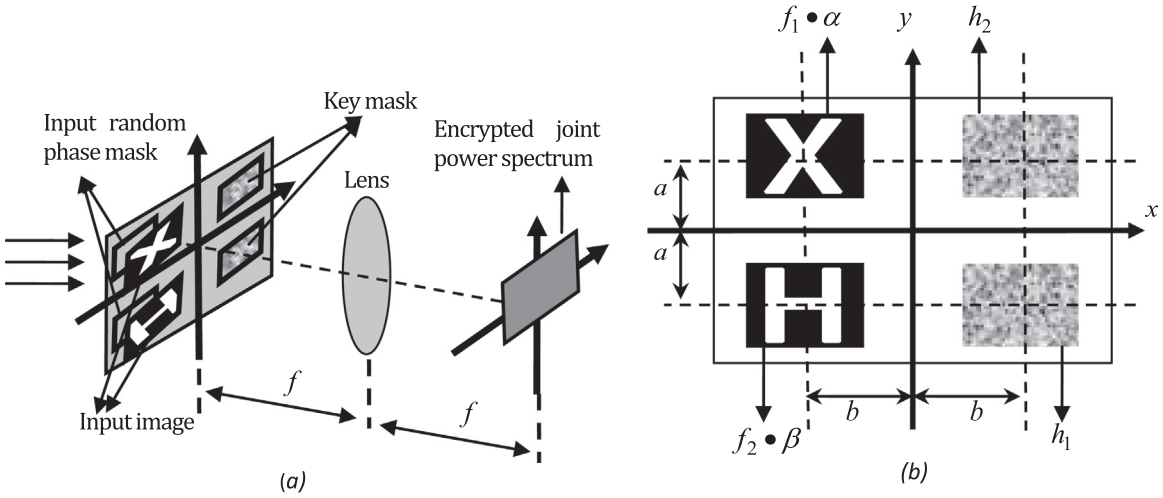

Fig. 1. Encryption scheme. (a) Encryption step and (b) the arrangement of input plane ($f_1 \bullet \alpha$: input images f_1 with a RPM α; $f_2 \bullet \beta$: input images f_2 with a RPM).

particular methods for avoiding cross talk. In Section 4, the initial experiment system is constructed to further validate the feasibility of our proposed parallel encryption system.

2. Principle of parallel encryption for multi-channel images in a JTC

2.1. Feasibility analysis on this method

In the conventional JTC encryption architecture, the input image with a random phase mask (RPM) attached is placed side by side with a key mask in the JTC input plane. In our proposal, multi-channel input images and key masks are arranged in the input plane. Referring to Fig. 1, we describe the initial design of the proposed encryption system based on JTC. Fig. 1(a) shows the encryption scheme. We use two channel images for simplicity. Two key masks and two input images attached with random phase masks are positioned in the same plane. Fig. 1(b) depicts the arrangement of them. a is the distance between input aperture and x axis in vertical direction, and b is the distance between input aperture image and y axis in horizontal direction. In this proposed scheme, the input image $f_1(x, y)$ and key mask $h_1(x, y)$ are placed diagonally and constitute a group for JTC. $f_2(x, y)$ and $h_2(x, y)$ constitute another group. $\alpha(x, y)$ and $\beta(x, y)$ denote the input RPMs bonded with $f_1(x, y)$ and $f_2(x, y)$, respectively. This arrangement is illuminated by a plane wave and the joint power spectrum (JPS) at the focal plane is given by

$$\begin{aligned} JPS(\upsilon_x, \upsilon_y) &= |\Im[\alpha(x+a, y-b)f_1(x+a, y-b) + h_1(x-a, y+b) \\ &\quad + \beta(x+a, y+b)f_2(x+a, y+b) + h_2(x-a, y-b)]\ |^2 \\ &= |A^*F_1|^2 + [A^*F_1]H_1^* \times \exp[-j4\pi(a\upsilon_x + b\upsilon_y)] \\ &\quad + [A^*F_1][B^*F_2]^* \times \exp[-j4\pi b\upsilon_y] + [A^*F_1]H_2^* \times \exp[j4\pi a\upsilon_x] \\ &\quad + H_1[A^*F_1]^* \times \exp[-j4\pi(a\upsilon_x - b\upsilon_y)] + 1 \\ &\quad + H_1[B^*F_2]^* \times \exp[-j4\pi a\upsilon_x] + H_1H_2^* \times \exp[j4\pi b\upsilon_y] \\ &\quad + [B^*F_2][A^*F_1]^* \times \exp[j4\pi b\upsilon_y] + [B^*F_2]H_1^* \times \exp[j4\pi a\upsilon_x] \\ &\quad + |B^*F_2|^2 + [B^*F_2]H_2^* \times \exp[j4\pi(a\upsilon_x + b\upsilon_y)] \\ &\quad + H_2[A^*F_1]^* \times \exp[-j4\pi a\upsilon_x] + H_2H_1^* \times \exp[-j4\pi b\upsilon_y] \\ &\quad + H_2[B^*F_2]^* \times \exp[-j4\pi(a\upsilon_x + b\upsilon_y)] + 1 \end{aligned} \quad (1)$$

where, $\Im[]$, $A(\upsilon_x, \upsilon_y)$, $F_1(\upsilon_x, \upsilon_y)$, $B(\upsilon_x, \upsilon_y)$, $F_2(\upsilon_x, \upsilon_y)$, $H_1(\upsilon_x, \upsilon_y)$ and .. denote the Fourier transformation and the Fourier transforms of $\alpha(x, y)$, $f_1(x, y)$, $\beta(x, y)$, $f_2(x, y)$, $h_1(x, y)$ and $h_2(x, y)$, respectively. * and $[]^*$ denote the convolution operation and complex conjugation, respectively. JPS is recorded as the encryption data and can be utilized in the decryption step.

As shown in Fig. 2, the key mask h_2 is returned to the input plane and illuminated in the decryption scheme. For the recovery of the corresponding original image f_2, JPS is illuminated by $H_2\exp[-j2\pi(a\upsilon_x + b\upsilon_y)]$ at the first lens' focal plane. $D(\upsilon_x, \upsilon_y)$ is given by

$$\begin{aligned} D(\upsilon_x, \upsilon_y) &= JPS(\upsilon_x, \upsilon_y)H_2 \times \exp[-j2\pi(a\upsilon_x + b\upsilon_y)] \\ &= |A^*F_1|^2H_2 \times \exp[-j2\pi(a\upsilon_x + b\upsilon_y)] + [A^*F_1]H_1^*H_2 \\ &\quad \times \exp[-j2\pi(3a\upsilon_x + 3b\upsilon_y)] + [A^*F_1][B^*F_2]^*H_2 \\ &\quad \times \exp[-j2\pi(a\upsilon_x + 3b\upsilon_y)] + [A^*F_1] \times \exp[j2\pi(a\upsilon_x - b\upsilon_y)] \\ &\quad + H_1[A^*F_1]^*H_2 \times \exp[-j2\pi(3a\upsilon_x - b\upsilon_y)] \\ &\quad + H_2 \times \exp[-j2\pi(a\upsilon_x + b\upsilon_y)] + H_1[B^*F_2]^*H_2 \\ &\quad \times \exp[-j2\pi(3a\upsilon_x + b\upsilon_y)] + H_1 \times \exp[-j2\pi(a\upsilon_x - b\upsilon_y)] \\ &\quad + [B^*F_2][A^*F_1]^*H_2 \times \exp[-j2\pi(a\upsilon_x - b\upsilon_y)] \\ &\quad + [B^*F_2]H_1^*H_2 \times \exp[j2\pi(a\upsilon_x - b\upsilon_y)] + |B^*F_2|^2H_2 \\ &\quad \times \exp[-j2\pi(a\upsilon_x + b\upsilon_y)] + [B^*F_2] \times \exp[j2\pi(a\upsilon_x + b\upsilon_y)] \\ &\quad + H_2[A^*F_1]^*H_2 \times \exp[-j2\pi(3a\upsilon_x + b\upsilon_y)] \\ &\quad + H_2H_1^*H_2 \times \exp[-j2\pi(a\upsilon_x + 3b\upsilon_y)] + H_2[B^*F_2]^*H_2 \\ &\quad \times \exp[-j2\pi(3a\upsilon_x + 3b\upsilon_y)] + H_2 \times \exp[-j2\pi(a\upsilon_x + b\upsilon_y)] \end{aligned} \quad (2)$$

After inverse-Fourier-transforming, the decryption image $d(x, y)$ at

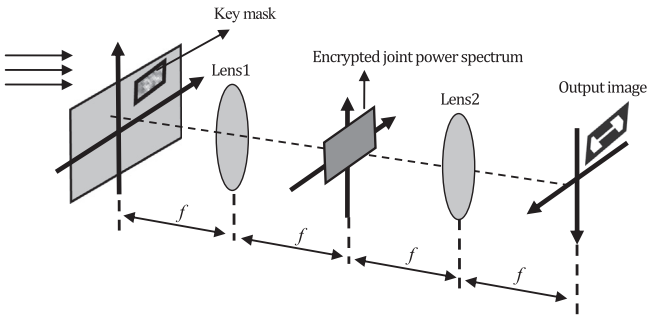

Fig. 2. Decryption scheme.