Optics & Laser Technology 51 (2013) 5–10

Contents lists available at SciVerse ScienceDirect

Optics & Laser Technology

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

Optical encryption in a JTC encrypting architecture without the use of an external reference wave

Yi Qin*, Qiong Gong

College of Physics and Electronic Engineering, Nanyang Normal University, Nanyang 473061, China

ARTICLE INFO

Article history:
Received 3 December 2012
Received in revised form
25 February 2013
Accepted 16 March 2013
Available online 11 April 2013

Keywords:
Optical encryption
Joint transform correlator
External reference wave

ABSTRACT

In practical optodigital encrypting architectures, the use of a reference wave is always necessary. In this paper, we present a protocol for image encryption and decryption by the use of a JTC architecture without the need of an external reference wave. We describe the practical implementation of this architecture, along with computer simulation results that support the proposal. We also find that image retrieved by our approach owns a better quality compared with that by the conventional method. Besides, some other advantages of the proposed protocol are discussed.

1. Introduction

Optical information-processing methods have been widely explored for information security applications [1–6]. An original work by Refregier and Javidi known as double random phase encoding (DRPE) employs two random phase keys in both of the input and Fourier planes to encrypt the data [7]. This approach, that enables one to encode a primary image into a stationary white noise, was later extended to the fractional Fourier domain [8] and the Fresnel domain [9]. However, The DRPE method requires accurate optical alignment, since the optical system is a holographic system. By contrast, a joint transform correlator (JTC) has some advantages when compared to DRPE. For instance, alignment and resolution requirements are relaxed, and spatial filter synthesis is unnecessary [10]. Afterward, Barrera et al. experimentally multiplexed several movies in a single package under the JTC architecture[11]. Recently, more methods have been further developed. Chen et al. proposed a new method, using coherent diffractive imaging for optical color-image encryption and synthesis in the Fresnel domain [12]. Chen et al. described a novel approach for optical image encryption in three-dimensional (3D) space. The 2D plaintext is considered as a series of particles distributed in 3D space, and an iterative phase retrieval algorithm is developed based on a modified Gerchberg–Saxton algorithm to encrypt the series of particles into phase-only mask [13].

More recently, Rueda et al. proposed a digital holographic configuration in a JTC architecture for encryption purposes [14]. With the aid of the reference wave introduced in the JTC architecture, it is possible to record the hologram of the key code and also to store and transmit via an ordinary communication link, avoiding the delivery of complex key code directly. However, it should be emphasized that any interferometric scheme requires stability and solid alignment conditions. Meanwhile, the optical architecture accompanies with supplementary optical elements and a larger working space. Due to these issues, it is attractive to develop other effective schemes where the interferometric architecture could be austerely employed or even avoided. For this reason, Rueda et al. presented an alternative to avoid the reference wave during the encrypting procedure in a JTC architecture by introducing a master key [15]. The concept of the master key, which has been reported in some previous contributions [16,17], plays an important role in the cryptosystem. In Rueda's proposal, although the reference wave is prevented from the encryption process, it is still inevitable in order to manufacture the master key. In this regard, we present here, to our best knowledge, a novel optical construction–reconstruction encrypting protocol by the use of a JTC architecture that completely free from the reference wave. We shall show in this paper that the intrinsic holographic character of the JTC scheme provided us a simple way for recording and reproducing the complex encoding key with two intensity images. Therefore, the encryption of the original plaintext to intensity images could be performed in a more simple and robust way with no need of the external reference wave. In addition, we also find this approach more advantageous in the sense that it retrieves images with better quality compared with the conventional method and requires a smaller number of images to complete encryption.

This paper is organized as follows. The encryption and decryption protocol are presented in Section 2. The simulation results together with discussions are given in Section 3 and a brief conclusion is included in Section 4.

* Corresponding author. Tel.: +86 135 692 230 36.
E-mail address: 641858757@qq.com (Y. Qin).

0030-3992/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.optlastec.2013.03.009

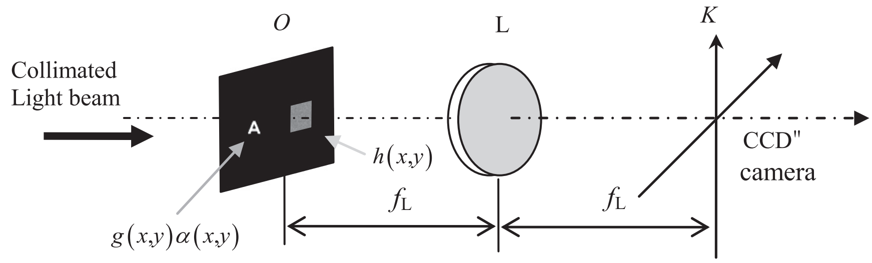

Fig. 1. Optical encryption using a joint transform correlator architecture. O: input plane; L: lens; f_L: focal length of L; K: output plane where the CCD camera is placed.

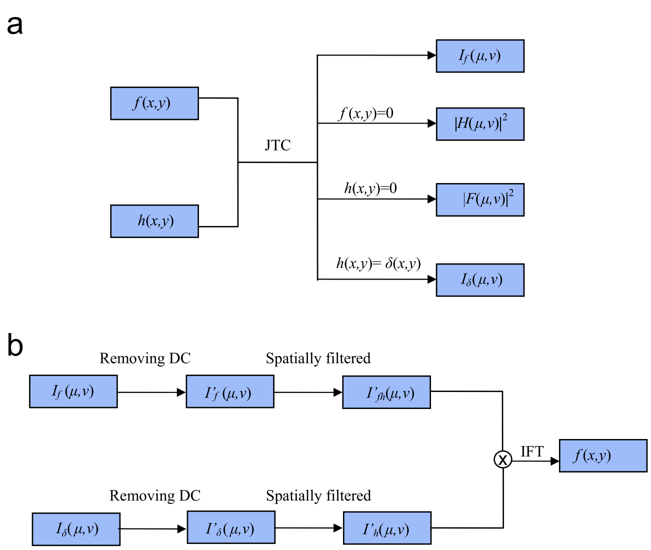

Fig. 2. Flow charts of the encryption process (a) and decryption process (b).

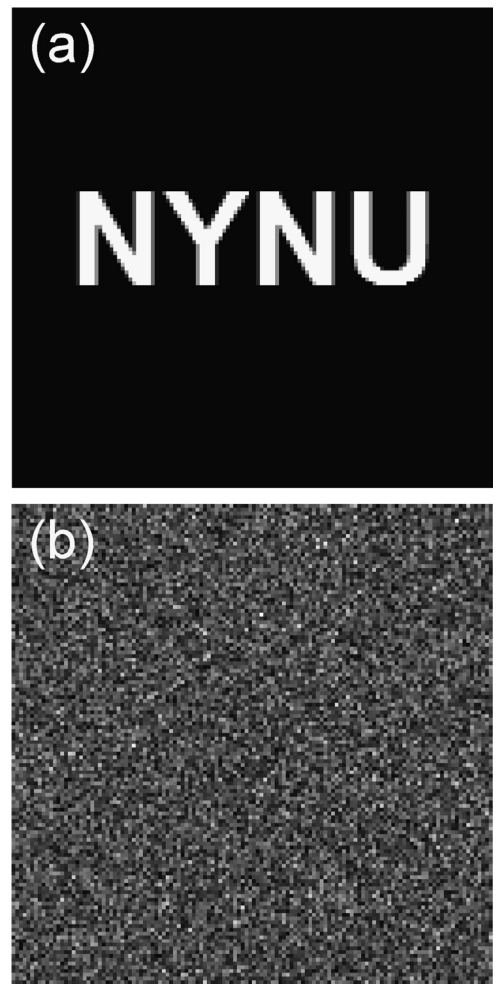

Fig. 3. The plaintext (a) and the encrypting key code (b).

2. Encryption and decryption process

2.1. Recording of the encryption key

As it can be learned from references [14,15], the introduction of a reference wave or a master key in the JTC architecture is essentially the recording of the complex value encryption key. In this regard, it is worthwhile to recall the fact that the JTC scheme possesses naturally the holographic property. Therefore, we could record the encryption key in a more simple way by taking advantages of this character. To accomplish this advantage, let us first briefly review the implementation of encryption procedures of the cryptosystem in the JTC architecture.

As depicted in Fig. 1, one of the JTC apertures contains the input image information $g(x,y)$ bonded to a random phase mask $\alpha(x,y)$, while the other JTC aperture contains the reference random key code $h(x,y)$. The complex valued key code, $h(x,y)$, is the inverse Fourier transform of a random phase mask $H(\mu,\nu)$. Both random phase masks are statistically independent and have uniform amplitude transmittance. In the encryption process, $f(x,y)=\alpha(x,y)g(x,y)$ and $h(x,y)$ are placed side by side on the input plane O and positioned at coordinates $x=-a$ and $x=a$, respectively. The double aperture input arrangement is illuminated by a plane wave.

Under such conditions, the transmittance $u(x,y)$ at the input plane is

$$u(x,y)=f(x,y)\otimes\delta(x-(-a),y)+h(x,y)\otimes\delta(x-a,y) \qquad (1)$$

the symbol $\otimes$ denotes convolution. The joint power spectrum(JPS) at the output plane K of the encrypting system is given by

$$I_f(\mu,\nu)=|F(\mu,\nu)|^2+|H(\mu,\nu)|^2 +[F(\mu,\nu)]^*H(\mu,\nu)\exp[-j2\pi(2a)\mu] +[F(\mu,\nu)]H(\mu,\nu)^*\exp[-j2\pi(-2a)\mu] \qquad (2)$$

Where * represents the complex conjugate, $||^2$ is the square module. $F(\mu,\nu)$ and $H(\mu,\nu)$ are the Fourier transforms of $f(x,y)$ and $h(x,y)$, respectively. Here (x,y) represents the spatial coordinates and (μ,ν) denotes the coordinates in the Fourier domain.

In the following, we discuss the recording of the encryption key. By replacing the plaintext in the object aperture with a Dirac delta function and retaining the encode key, the transmittance