Optics and Lasers in Engineering 83 (2016) 126–130

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

Experimental analysis of a joint free space cryptosystem

John Fredy Barrera Ramírez [a,*], Alexis Jaramillo Osorio [a], Alejandro Vélez Zea [b], Roberto Torroba [b,c]

[a] Grupo de Óptica y Fotónica, Instituto de Física, Facultad de Ciencias Exactas y Naturales, Universidad de Antioquia UdeA, Calle 70 No. 52-21, Medellín, Colombia
[b] Centro de Investigaciones Ópticas (CONICET La Plata – CIC - UNLP), PO Box 3, C.P 1897, La Plata, Argentina
[c] UID OPTIMO, Facultad de Ingenieria, Universidad Nacional de La Plata, La Plata, Argentina

ARTICLE INFO

Article history:
Received 7 August 2015
Received in revised form
12 February 2016
Accepted 8 March 2016
Available online 28 March 2016

Keywords:
Optical security
Encryption
Fresnel transform
Optical data processing

ABSTRACT

In this paper, we analyze a joint free space cryptosystem scheme implemented in an actual laboratory environment. In this encrypting architecture, the object to be encoded and the security key are placed side by side in the input plane without optical elements between the input and the output planes. In order to get the encrypted information, the joint Fresnel power distribution JFPD coming from the input plane is registered in a CMOS camera. The information of the encrypting key is registered with an off axis Fresnel holographic setup. The data registered with the experimental setup is digitally filtered to obtain the encrypted object and the encryption key. In addition, we explore the performance of the experimental system as a function of the object-camera and key-camera distances, which are two new parameters of interest. These parameters become available as a result of developing this encrypting scheme. The theoretical and experimental analysis shows the validity and applicability of the cryptosystem.

1. Introduction

Optical image encryption opened a new route in information security to protect data from counterfeiting and unauthorized access. We are able to meet this challenge from the nanoworld [1] to the use of QR codes as “information containers” [2–5]. The voyage started with the contribution of Refregier and Javidi [6], introducing the concept and the first implementation on the so called 4f encrypting architecture. The optical encryption scheme is called double random phase encoding, because involves two random phase masks, one in the input plane and a second in the Fourier domain. It can be shown that if the phases in these masks can be described as statistically independent, then the resulting encrypted image is a white-noise distribution. Alternatively, other encrypting schemes were developed under the joint transform correlator (JTC) architecture [7–9]. This optical setup is more compact than the conventional 4f holographic scheme, because the object and reference beams share a single optical system consisting of one Fourier-transforming lens. The JTC encrypting architecture also offers two major advantages: the encrypted information is stored as an intensity distribution in a recording media and the decryption process is performed using the encoding key, not its complex conjugate. These advantages decrease the requirements for an experimental implementation in a laboratory environment, thus becoming the favored architecture for most practical applications [5,10,11]. Digital holographic setups were developed to implement the JTC cryptosystem [12,13], bringing new exciting possibilities to optical encryption. On the other hand, several techniques have been proposed in the literature to optically encrypt images using the gyrator transform [14,15] and the fractional Fourier transform (FFRT) [16–24].

An alternative optical security system for image encryption based on a nonlinear JTC in the Fresnel domain (FrD) was proposed [25]. In the suggested scheme, the encryption process is performed by a lensless optical system that encrypts the desired data into an intensity pattern called joint Fresnel power distribution (JFPD). Like in the traditional JTC cryptosystem, the key is a random complex mask. To further reduce the speckle contamination of the decrypted object and enhance security, a nonlinear modification is performed. The decryption protocol is performed through a Fresnel transform, allowing to control the reconstruction plane and magnification of the decrypted image. We will refer this system as a joint free space cryptosystem (JFSC), because the encryption is achieved by the joint interference of the freely propagated key and object waves.

As encryption methods evolved, additional parameters were included to reinforce the security level and to allow for the multiplexing of data, ensuring that the object can be recovered only when using the right combination of those optical parameters. In the literature, we find contributions where the wavelength [26,27], the

* Corresponding author.
E-mail address: john.barrera@udea.edu.co (J.F.B. Ramírez).

http://dx.doi.org/10.1016/j.optlaseng.2016.03.010
0143-8166/

polarization [28], in-plane shifting [29], rotation [30], modulation [31], axial shift [32], and other parameters were proposed and demonstrated as valid encrypting parameters. In particular, studies regarding the valid range of each of these parameters are crucial to establish the adequate working conditions under which these parameters are useful.

Although these studies are indicatives of the validity of the proposed parameters, we still find that practical implementations are bonded to restrictions arising from practical laboratory conditions. A careful experimental study would reveal the actual behavior in a laboratory environment. In particular, we find that the behavior of the system cannot be explained by a single factor when the propagation length is changed. Besides, a comprehensive study of the real effects of this parameter requires an experimental implementation in order to take into account for all possible factors.

Additionally, during the implementation of the experimental setup, we explore the performance of the system as a function of the object-camera and key-camera distances. We show that in the JFSC scheme there is a gradual degradation of the recovered object as the object-camera distance increases, resulting in a practical limitation on the operational range of the system. Besides, the system tolerance to axial displacements of the encryption key is significant. Both features must be taken into account in any future implementation of this system, either simulated or experimental.

2. Description of the architecture and the encryption–decryption process

In the proposed JFSC architecture, we project in the input plane of the optical system both the object to be encrypted and a blank key window. This window determines the size of the encryption key. We use a spatial light modulator (SLM) to display the object and the key window in our physical setup, which limits their maximum size and the details of the object due to its display resolution and pixel size. We attach to the SLM a ground glass diffuser covering both the object and the key window (Fig. 1), which will provide both random phase masks.

As in the JFSC architecture, there is no lens that performs an optical Fourier transform of the input plane, the pattern registered by the CMOS camera corresponds to the free space propagation of the input plane, which is described mathematically by a Fresnel transform (FRT) [33]. Considering $c(x,y)=o(x,y)r(x,y)$ with $o(x,y)$ the object to be encrypted, $r(x,y)$ and $l(x,y)$ random phase masks, the last representing the encrypting key, the JFPD is then

$$I(v,w)=|C_z(v,w)|^2+|L_z(v,w)|^2+C_z(v,w)L_z^*(v,w)e^{-4\pi iav}+C_z^*(v,w)L_z(v,w)e^{4\pi iav} \quad (1)$$

where $C_z(v,w)$ and $L_z(v,w)$ are the Fresnel transforms of $c(x,y)$ and $l(x,y)$ at propagation distance z, $v=x/\lambda z$ and $w=y/\lambda z$ are the coordinates in the Fresnel plane, and λ is the wavelength. The exponential expressions will result in interference fringes in the JFPD whose frequency will depend on the separation $2a$ between key and object. Due to the limited pixel size of the recording medium, this separation cannot be made arbitrarily large. In the proposed JFSC, the maximum separation between key window and object is given by [34]

$$a=z\tan\left(\arcsin\left(\frac{\lambda}{4\Delta x}\right)\right) \quad (2)$$

where Δx is the pixel size of the CMOS camera. The intensity of the FRT of object and key windows can be registered separately and then subtracted from Eq. (1), resulting in

$$I(v,w)=C_z(v,w)L_z^*(v,w)e^{-4\pi iav}+C_z^*(v,w)L_z(v,w)e^{4\pi iav} \quad (3)$$

These two terms can be isolated by performing the Fourier transform (FT) of Eq. (3), obtaining

$$i(\xi,\eta)=FT\{C_z(v,w)L_z^*v,w)\}\otimes\delta(\xi+2a,\eta)+FT\{C_z^*(v,w)L_z(v,w)\}\otimes\delta(\xi-2a,\eta) \quad (4)$$

where $FT\{\}$ represents the FT operation, the symbol $\otimes$ denotes the convolution, and $\delta()$ is the delta Dirac function. The spatial separation caused by the convolution with the delta functions allows to select one of these two terms and to discard the other. The selected term is digitally positioned in any desired spatial coordinate (x',y'), and then performing the inverse Fourier transform (IFT), we obtain

$$E_z(v,w)=C_z(v,w)L_z^*(v,w)e^{2\pi i(vx'+wy')} \quad (5)$$

In Eq. (5), we find the filtered encrypted object along a phase factor with the object coordinates after decryption. In order to recover the encrypted object, we must first multiply Eq. (5) by the FRT of the encrypting key and then we perform the adequate inverse Fresnel transform (IFRT). Attempting to decrypt without multiplying by the correct key will result in a speckle pattern instead of the original object.

Consequently, to accomplish the decryption process, we need the information of the encrypting key. Since this information has both phase and amplitude components, we use the off-axis digital holography setup shown in Fig. 2.

In order to register the information of the encryption key $L_z(v,w)$, we only project the key window on the SLM and register the resulting hologram

$$H(v,w)=|P(v,w)|^2+|L_z(v,w)|^2+P(v,w)L_z^*(v,w)+P^*(v,w)L_z(v,w) \quad (6)$$

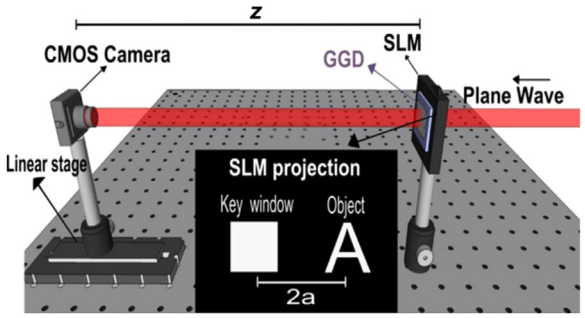

Fig. 1. Basic JFSC scheme. SLM spatial light modulator, GGD ground glass diffuser, and z propagation distance.

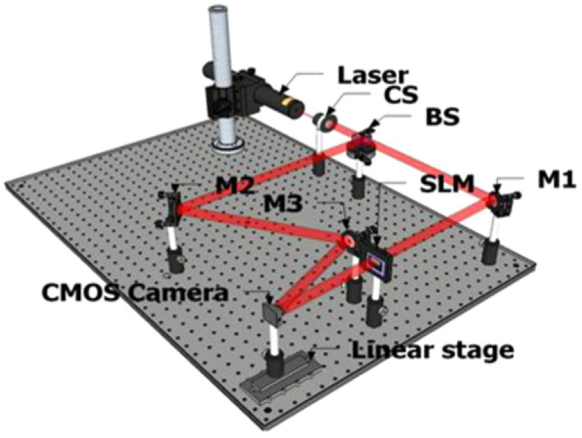

Fig. 2. Experimental setup to record the hologram of the encrypting key, CS collimation system, BS beam splitter, M mirror, and SLM spatial light modulator.