Optics and Lasers in Engineering 102 (2018) 119–125

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

Fractional optical cryptographic protocol for data containers in a noise-free multiuser environment

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

[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) CC N° 3, C.P 1897, La Plata, Argentina*
[c] *Facultad de Ciencias Exactas, Universidad Nacional de La Plata, La Plata, Argentina*
[d] *UIDET OPTIMO, Facultad de Ingeniería, Universidad Nacional de La Plata, La Plata, Argentina*

ARTICLE INFO

Keywords:
Encryption
Fractional fourier transform
Multiplexing
QR codes

ABSTRACT

Optical encryption systems have great potential for flexible and high-performance data protection, making them an area of rapid development. However, most approaches present two main issues, namely, the presence of speckle noise, and the degree of security they offer. Here we introduce an experimental implementation of an optical encrypting protocol that tackles these issues by taking advantage of recent developments in the field. These developments include the introduction of information containers for noise free information retrieval, the use of multiplexing to allow for a multiple user environment and an architecture based on the Joint fractional Fourier transform that allows increased degrees of freedom and simplifies the experimental requirements. Thus, data handling via QR code containers involving multiple users processed in a fractional joint transform correlator produce coded information with increased security and ease of use. In this way, we can guarantee that only the user with the correct combination of encryption key and security parameters can achieve noise free information after deciphering. We analyze the performance of the system when the order of the fractional Fourier transform is changed during decryption. We show experimental results that confirm the validity of our proposal.

© 2017 Elsevier Ltd. All rights reserved.

1. Introduction

Information security is an important subject, especially as the growing interchange of data increases its vulnerability to attacks, and interception by unauthorized users presents a substantial increment. Optical cryptosystems have been proposed as an alternative solution with great potential, offering many degrees of freedom that can be employed to reinforce the security of the information [1,2].

The pioneer cryptosystem was proposed and demonstrated by Refrieger and Javidi [3]. Their proposal was a 4f system with a double random phase encoding (DRPE) technique. In this system, one random phase mask is placed in the input plane, while the second phase mask is located in the Fourier domain of a first lens. This second phase mask is the encryption key. A second lens produces the encrypted data, resulting in a white noise distribution from which the original information cannot be extracted without the information of the encryption key. After the implementation of the 4f system, several encryption architectures were proposed, amongst which we find the joint transform correlator (JTC) cryptosystem [4,5]. The JTC architecture presents several advantages over the 4f system. The encrypted data is codified into an intensity distribution; the decryption procedure is carried with the encryption key without needing the complex conjugate of the encrypting key, and presents less stringent alignment requirements for the experimental implementation. These properties make the JTC system a flexible alternative for further developments [6–9]. In this frame, the JTC cryptosystem has been object of continued research, both to determine and to improve its security against attackers [10–12] and to reduce the noise in the decrypted data [13,14].

Alternative optical securities schemes are still under active research, for example, an optical-digital encryption process was combined with a fingerprint authentication technique to increase the security of the optical system [15]. Another technique for improving the security in the encryption process is steganography, where the information to be protected is embedded into a carrier signal, containing non-secret information which obfuscates the protected data [16,17].

The JTC cryptosystem has also been modified with implementations in the Fresnel domain [18,19]. This implementation has the advantage of not requiring a lens, enabling the use of the free space propagation distance between the input and output planes as a new security parameter. The Fresnel JTC encrypting architecture inherits all security properties of JTC system. In this case the information is stored as an intensity distribution called joint Fresnel power distribution (JFPD). Other alternative to classic DRPE and JTC techniques is optical encryption using Hartley transforms. The Hartley transform is performed through two

[*] Corresponding author.
E-mail address: jhonalexis.jaramillo@udea.edu.co (A. Jaramillo).

https://doi.org/10.1016/j.optlaseng.2017.10.008
Received 13 July 2017; Received in revised form 12 September 2017; Accepted 14 October 2017
0143-8166/© 2017 Elsevier Ltd. All rights reserved.

Fourier transforms in combination with a Michelson interferometer, and like in the JTC cryptosystem the encoded information is a pure random intensity mask [20].

A further generalization of a DRPE system with improved security was developed in the fractional Fourier domain, first digitally implemented and thereafter experimentally tested [21,22]. This last implementation opened the way to new applications for a digital cryptosystem in the fractional Fourier domain [23–29]. Two experimental approaches of the JTC cryptosystem in the fractional Fourier domain were proposed in [30,31]. These experimental implementations showed the viability of these security systems. Afterwards, the JTC cryptosystem in the fractional Fourier domain was digitally analyzed [32]. Additional to the security parameters due to the encrypting architecture, other parameters like the wavelength [33,34], the polarization [35], key rotation [36] and in-plane shifting [37] can be associated with the security of the fractional JTC (FrJTC) encrypting system.

On the other hand, it is evident the optical encrypting systems had demonstrated its security, versatility and applicability. But from the practical point of view, the information recovered using the optical cryptosystems must be free of any kind of degradation. The users not only ask for security but also for fidelity in the retrieved information. As the decrypted information in optical cryptosystems contains degradation due to the optical processing, reducing or eliminating the noise was a remaining challenge. Several methods that allowed to reduce the degradation over the recovered information, were presented, but none of them allows completely noise-free retrieving [14,38,39].

In order to overcome this issue, the concept of "information container" in optical data processing was introduced by Barrera et al [40]. The security process based on this concept consists in introducing the original information in a container. Afterwards, this container is encrypted using the optical cryptosystem in the same way as any other data. In the recovering process, the right decryption brings the container with the noise and/or degradation due to the optical processing. Therefore, the container must be selected to be tolerant to noise and degradation. Finally, after reading/scanning the decrypted container the original information can be recovered with any kind of degradation [40–42].

Intensive work in the research line of optical information processing using optical containers have been performed [43–52]. The original proposal was applied in several optical encrypting architectures [14,43–47], for optical verification [48–50], integral imaging [51,52] and recently in incoherent optical cryptosystems [53].

As another important aspect, multiplexing methods have been widely used in optical security. These methods are employed to store multiple encrypted information in a single package. Usually the encrypted package is obtained using the same cryptosystem but modifying one of the parameters involved in the process [33,35–37,54–63].

Particularly, the optical encryption of movies has been possible thanks to the multiplexing techniques. The concept of an encrypted movie was introduced for the first time by Mosso et al [64]. The movie joins several encrypted frames corresponding to a time evolving situation employing the same encrypting key. Thanks to a multiplexing operation, the encrypted movie is compacted into a single package. Each frame of the movie is modulated during encryption to avoid the superposition of the frames during decryption. Later, the encryption on time evolving situations was extended to color scenes [65], multiple videos [8] and recently the encryption of a video using chaotic masks was presented [66].

Taking into account the advantages and the flexibilities achieved by recent advances in multiplexing and information containers, we present a protocol based in a fractional optical cryptographic approach [21,22]. Our protocol aims to secure data in a multiuser environment without the detrimental effects of noise. Fractional Fourier transform setups show great flexibility thanks to the many different configurations in which the fractional transform can be achieved [23–32], while also introducing a new security parameter, namely the fractional order of the transform.

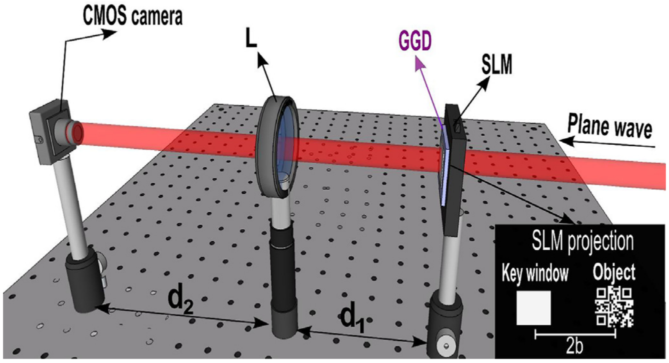

Fig. 1. Basic FrJTC cryptosystem scheme. L lens, GGD ground glass diffuser, SLM spatial light modulator, d_1 input plane-lens distance, d_2 lens-output plane distance.

These benefits make the fractional Fourier cryptosystems of special interest in experimental implementations.

In the following sections, we first demonstrate an experimental implementation of a FrJTC cryptosystem. In this system, the processed information is stored as an intensity distribution named joint fractional Fourier power distribution (JFrPD). We demonstrate the robustness of our proposal by analyzing the performance of these cryptosystems as a function of the fractional order. We then test the capability of the system for processing of QR codes as information containers to perform a noise-free information recovering. Finally, we experimentally demonstrate the ability of the FrJTC cryptosystem to manage multiple encrypted data with different fractional orders.

2. Description of the architecture, encryption and decryption processes

In the input plane of the FrJTC encrypting system an object to be encrypted and the key window are projected in a spatial light modulator (SLM) (Fig. 1). The key window is an empty square that determines the size of the encryption key. We attach to the SLM a ground glass diffuser to provide the two random phase masks required by the encrypting architecture. The area of the diffuser in contact with the object provides one of the masks, while the area in contact with the key window will be the encrypting key.

We can represent mathematically the input plane as $e(x,y) = \tau_{b,\alpha}\{c(x,y)\} + \tau_{-b,\alpha}\{l(x,y)\}$. Where $c(x,y) = o(x,y)r(x,y)$ with $o(x, y)$ the object to be encrypted, $r(x, y)$ is a random phase mask and $l(x, y)$ the random phase mask that represents the encryption key, $2b$ is the separation between the object and key window in the input plane, $\tau_{b,\ \alpha}\{\}$ is the translation fractional Fourier operator and α is the fractional order [67,68]. The combination of the free space propagation between the input plane and the lens, the lens phase, and the free space propagation from the lens to the output plane determines a fractional Fourier transform with a specific fractional order α. When $\alpha = \pi/2$ we have the traditional JTC encrypting system [68]. We can express the fractional order as [21,69],

$$\alpha = arcos\left(\frac{\sqrt{(d_1 - f)(d_2 - f)}}{f}\right) \tag{1}$$

where d_1 is the input plane-lens distance, d_2 is the lens-output plane distance and f is the lens focal length (Fig. 1).

Then, in the CMOS camera we register the JFrPD,

$$\begin{aligned} I_\alpha(u,w) = {}& |c_\alpha(u,w)|^2 + |l_\alpha(u,w)|^2 + c_\alpha(u,w) l^*{}_\alpha(u,w)\exp[4\pi i b u \csc(\alpha)] \\ & + c_\alpha{}^*(u,w) l_\alpha(u,w)\exp[-4\pi i b u \csc(\alpha)] \end{aligned} \tag{2}$$

Here $c_\alpha(u, w)$ and $l_\alpha(u, w)$ are the fractional Fourier transform (FrFT) with order α of $c(x, y)$ and $l(x, y)$ respectively, * means the complex conjugate, csc() is the cosecant trigonometric function and $i = \sqrt{-1}$ is

Download English Version:

https://daneshyari.com/en/article/7131973

Download Persian Version:

https://daneshyari.com/article/7131973

Daneshyari.com