Optics and Lasers in Engineering 112 (2019) 119–127

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

# Improved decryption quality with a random reference beam cryptosystem

Alexis Jaramillo Osorio [a,*], John Fredy Barrera Ramírez [a], Santiago Montoya [a], Alejandro Mira-Agudelo [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
Fourier transform
Fresnel transform
Decryption quality
Multiplexing

ABSTRACT

The secure managing of sensible data is one of the main challenges nowadays. During the last years several advances have demonstrated the ability of optical encrypting systems to protect information. In spite of these developments, there are some evident issues to be solved. One of the main concerns is the limitation of the experimental cryptosystems in the size of the inputs that can be properly protected and recovered by the encrypting system. In the case of the experimental joint transform correlator (JTC) cryptosystem, the data to be encoded and the key are placed side by side in the input plane. Therefore, the size of the object to be encrypted is limited by the size of the encryption key and the separation between the input and the key. This limitation leads to degradation on the recovered data according the size and the spatial frequencies content of the object for a given recording media. In this work we experimentally implement an interferometric cryptosystem in which the encryption key is a ground glass diffuser (GGD) located in the reference arm. In the object arm, the information to be encoded is displayed in a spatial light modulator (SLM) and placed in contact with another GGD. This system allows the projection of the input object in the whole SLM area. The encryption process results from the interference between the reference beam and the Fourier transform of the input object plane. We experimentally analyze the quality of the decrypted object in relation with the size of the input original object. Then, we compare the performance of this system with the JTC cryptosystem. Finally, we implement a protocol for a multi-user environment under the rotation of the key. Experimental results show the viability, versatility and applicability of the proposal.

## 1. Introduction

Information security is the practice of protecting information while still providing access to authorized users. This field has advanced significantly in recent years. Despite of the advances, the attacks on information systems are growing in prominence every day, demonstrating that more research is imperative to deny unauthorized access to critical data. Information security offers many areas for specialization, including securing networks, securing applications and databases, security testing and optical security.

In the area of optical security, the systems dedicated to protect information using light are widely known as optical encrypting systems [1,2]. These systems have evolved from a first proposal supported by computational simulations [3] to experimental systems capable of implementing optical security processes at nano [4] and micro scale [5], protecting color [6] and grayscale information [7]; also setups to experimentally demonstrate the vulnerability of a determined optical encrypting technique [8], the successful multiplexing of encrypted movies [9], the optical voice encryption based on digital holography [10], and an experimental optical processors that assure a high degree of protection and noise-free recovering [11], among others. Additionally, recent interesting works in optical security supported by computational simulations include the use of computer-generated hologram in optical watermarking [12] and verification [13], structured [14] and deterministic masks [15] in optical encryption.

According to the important advances in optical encryption, especially during the last decade, challenges in this area have become evident. Some of these challenges are: the analysis and improvement of the optical encrypting architectures to increase the flexibility and expand the potential applications of the cryptosystems, the cryptanalysis of the experimental systems to prove the resistance to attacks, and the improvement of the dynamic encryption of video sequences, to mention some of them.

As mentioned above, one of the main challenges is related with the optical encrypting architectures. The first proposal used a simulated 4f system along with two random phase masks to introduce the

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

https://doi.org/10.1016/j.optlaseng.2018.09.006
Received 11 June 2018; Received in revised form 29 August 2018; Accepted 7 September 2018

concept of data encryption in the optical domain [3]. The encrypted data is obtained by random-phase encoding in both the input and the Fourier planes. This technique is known as double random phase encoding (DRPE) and allows encoding data into a stationary white noise. The random phase mask placed in the Fourier plane is known as security key because it is the element that allows both encryption and decryption. The original information can be recovered when an authorized user has access to the encoded information and the security key. In the experimental demonstration, the original data is encoded using a random phase mask with a limited number of pixels [16]. The encrypted information was recorded on a Kodak holographic film as a hologram. During decryption the complex conjugate of the security key is used as the decrypting key. The decrypted data is finally registered in a CCD camera. These experimental results demonstrated the validity of the proposal.

This first proposal and its experimental demonstration generated a great interest in the optics and photonics community. Unnikrishnan et al. implemented an experimental optical encryption system based on DRPE in a 4f system using a photorefractive crystal. In this contribution the information is decrypted by generating a conjugate of the encrypted data through phase conjugation in a photorefractive crystal. Additionally, the security key that is used during encryption can also be used for recovering the data, thereby alleviating the need for generating and positioning the conjugate of the key [17]. Later on, an encrypted memory system using the DRPE technique in the Fresnel domain was presented. The two random phase masks and their positions form three-dimensional keys. The encryption and decryption processes were performed using angular multiplexing in a photorefractive crystal [18].

In order to take advantage of digital registering and manipulation methods, an information security method that uses a digital holographic technique was presented by Javidi and Nomura. In this technique the encoded data and the decryption key were stored as a digital hologram [19]. The original information can be decrypted by means of a virtual optical system. This security technique provides secure storage, and data transmission and reception via Internet or an Internal Network. In this direction, a digital phase-shifting interferometry was employed for recording of phase and amplitude information with a CCD array [20]. The encryption is performed by use of the DRPE technique with one random phase mask in the object plane and another in the Fresnel domain. This technique was adapted to protect information using either the Fraunhofer or the Fresnel diffraction pattern of the input. These contributions motivated the emergence of new experimental encrypting systems based on the DRPE technique and different optical architectures [21–23]. Some of these proposals include encrypting systems using the joint transform correlator JTC architecture [21], in the fractional Fourier domain [22] and in the Fresnel Domain [23].

One of most developed and studied architectures in recent years is the JTC encrypting architecture [21,24–41]. In this encrypting system, the joint power spectrum (JPS) between the information to be encrypted in contact with a random phase mask and the key contain the encrypted data. Unlike the case with classical DRPE technique, the encrypted data is an intensity pattern and the same key code is used to both encrypt and decrypt the data, and the conjugate key is not required. These advantages decrease the requirements for an experimental implementation in a laboratory environment. The first implementation of the JTC encrypting system was performed using a photorefractive crystal as recording media [21]. Afterwards, a JTC cryptosystem with a binary key projected in a SLM was proposed. The cryptosystem based on a photorefractive crystal as a registering media was employed to perform shift-invariant encryption and decryption [24]. Also, the multiplexing capabilities of this system were experimentally demonstrated by recording multiple two-dimensional data in the same crystal by angular multiplexing and/or key code multiplexing [25]. A posterior experimental demonstration of a multichanneling encryption method by using multiple random-phase mask apertures in the input plane based on a joint transform correlation scheme was presented. In this case, two encrypted objects are stored in a photorefractive crystal and then independently recovered [26].

Taking advantage of the benefits of the JTC cryptosystem and the flexibility of the opto-digital implementation, a JTC encrypting system where the encrypted data and the decrypting key are obtained by phase-shifting interferometry was proposed and experimentally demonstrated [27]. The experimental implementation was performed with a CCD camera as recording media and a programmable liquid-crystal TV display used to represent the input data and to introduce the phase shifts. The decryption process was achieved by digital and optical means.

Motivated by the advances mentioned above, during the last decade the research on experimental cryptosystems based on JTC encrypting architecture with the DRPE technique has shown an important upgrowth [28–33]. We find opto-digital implementations of the JTC, where the JPS was registered with a digital camera and then filtered it to remove the non-relevant information [28]. This filtering procedure allows extracting the encrypted data from the JPS, thus reducing the amount of handled information, making the whole process more efficient and also increasing the system resistance against some attacks [29]. Additionally, several schemes using the JTC encrypting architecture along with a digital holography technique showed that it is possible to encrypt: multiple videos [9], messages of any length [30], multi-images [31,32], three-dimensional information [33] and grayscale data [7]. In addition, the JTC encrypting architecture has been successfully implemented in the fractional [34–38] and in the Fresnel domains [39–41].

On the other hand, some interesting optical cryptosystems that employ a random phase mask in the reference arm have been proposed [42–47]. An encryption system to protect three-dimensional (3D) information was experimental implemented [42]. In this contribution, a phase-shifting interferometer records the phase and amplitude information generated by a 3D object at a plane located in the Fresnel diffraction region. The encryption process was performed with the Fresnel diffraction pattern generated by a random phase mask located in the reference arm. Also, a holographic memory setup based on random phase-encoded multiplexing in a photorefractive crystal was presented [43]. A rotating diffuser placed as a random phase modulator in the reference beam allows increasing the holographic storage capabilities of the crystal. The technique was successfully applied to a triple phase-encoded optical security system that takes advantage of the high angular selectivity of the scheme. Later on, a secure system with signal and reference waves dually encrypted was proposed [44]. The images were encrypted using the DRPE technique and a reference beam encoded with another random phase mask. This system provides the potential to dually encrypt signal and reference waves in a digital holographic system. Then, a numerical technique for simulating the recording and readout of two-wave encryption to determine the degree of security was implemented [45]. The retrieval characteristics by the proposed simulator and estimated the necessary key correlation for decrypting-encrypted data were analyzed. In another approach, a method for spatial-identification image encryption to improve the encryption degree was demonstrated [46]. The technique employs a random phase mask displayed on a spatial light modulator (SLM) in the reference arm and a four-step phase-shifting method. The original data is encrypted by subareas using a reference beam with a different random phase for each subarea. The computer simulations shown the effectiveness of the proposal to process grayscale data. In another two-wave encryption method [47], the output intensity for unauthorized memory access is reduced. The computer simulations show that the robustness can be improved by increasing the key length. According to the experimental results, the use of a compatible key reproduces a clear original image, but unauthorized key-based reproduction reduced output strength significantly.

Another important aspect to be considered is the managing of multiple data in a secure and efficient manner; with this purpose multiplexing techniques have been incorporated in the optical encrypting protocols. These protocols have progressed through the work of many research teams [9,25,26,30–32,48–53]. In general, the main idea of multi-