Asian Journal of Physics Vol. 22, No. 2 (2013) 135-152

Experimental double random phase encoding technique under a joint transforms correlator architecture

John Fredy Barrera,[1,*] Myrian Tebaldi[2] and Roberto Torroba[2]
[1]*Grupo de Ópticay Fotónica, Instituto de Física, Universidad de Antioquia, A.A 1226, Medellín, Colombia*
[2]*Centro de Investigaciones Ópticas (CONICET La Plata-CIC) and UID OPTIMO, Facultad de Ingeniería, Universidad Nacional de La Plata, P.O. Box 3 C.P 1897, La Plata, Argentina*

We present a review for updating the last contributions in the field of optical encoding techniques using a joint transform correlator architecture. We focus on the experimental aspects with special reference to both photorefractive and digital based applications. We describe the usual situation involved in developing the experimental set-ups when these techniques are used in multiplexing encrypted data. We address the solution to cross talk and overlapping issues associated with the multiplexing handling.© Anita Publications. All rights reserved.

OCIS codes: 000.0000, 999.9999.

1 Introduction

Researchers carried out extensive studies to employ coherent optical methods in correlation techniques. Among the most popular correlator, we find the classical Joint Transform Correlator (JTC) [1-3]. Many contributions include the use of the JTC as architecture [4, 5]. This optical setup is compact because the object and reference beams share a single 4f optical system consisting of two Fourier-transforming lenses. In the JTC case, the information is stored as intensity distribution in the recording media. Much work was started using the principle of coherent optics filtering for selecting relevant information as frame applications for the JTC scheme. The inherent parallelism of optics provides an appropriate support for information processing techniques. Correlation is conceived as a filtering that aims at extracting the relevant information in order to recognize a pattern in a complex scene. This led to the concept of the classical matched filter (carried out from a single reference) whose purpose is to decide whether a particular object is present in the scene. To obtain a reliable decision about the presence or absence of an object in a given scene, we must correlate the target object, using several correlation filters and taking into account the possible modifications of the target object. Carrying out a part of the processing digitally is a relevant solution to solve this complexity. So far, the use of the JTC architecture in this context has led to a continuous and fruitful development of the field.

The introduction in the field of optical encryption is seen as a new starting point for the JTC architecture [6]. The international economic infrastructure is becoming increasingly dependent on information technology, with computer and communication technology being essential and vital components of government facilities, financial centers, military installations, medical services, to name a few. However, precisely due to the fast development of communication techniques, the world is experiencing a severe increase in unauthorized use and distribution of information, primarily because digital information such as image data delivered over the Internet can be easily hacked. In optical encryption, researchers found means of making communications channels secure.

Technical literature is full of studies on optical information technologies for security and encryption systems. Some data encryption methods use double random phase encoding in a classical 4f optical architecture [7, 8], digital holography [9], virtual digital optics [10], and computer-generated holograms [11]. Information validation has also been possible [12-14]. The 4f solution consists in encoding the input image into two chosen noise functions by using the 4f setup, i.e., convolution between the input image multiplied by the first noise function and the impulse response of the second noise function [7]. These encryption techniques originate in the optical image processing community and continue to set many challenges in several areas. This technique is also used for storing encrypted data and is extended to image encryption in fractional Fourier [15] and Fresnel

Corresponding author :
E-mail: jbarrera@fisica.udea.edu.co (Dr John Fredy Barrera)

domains [16, 17]. In general, the reference beam, the object beam, or both, are encoded optically. However, a holographic configuration of the optical systems is required. It is difficult to make a practical system, because fully complex data is needed for phase encoding.

The properties and versatility of the JTC architecture play then a relevant role as an alternative tool for encrypting purposes. Note that other JTCs were also proposed in the literature [18-20].

As mentioned earlier, the recent progress in data-processing networks and communication systems has considerably increased the facility for information exchange. However, non-authorized people can intercept the transmitted data. This explains why considerable effort is being currently dedicated to data encryption and secure transmission.

To enable efficient and secure information exchange, it is often necessary to develop not only digital or virtual simulations but also experimental approaches are of great importance.

Virtual optics and digital encryption operations are often carried out as two separate research branches, although they are strongly related and can benefit each other.

Intensive research has been directed toward coherent optics, especially combining different strategies to solve the issues associated with encoding, because of the potential for new technological applications in telecommunications. In this review, we study optical information encrypting techniques, in close relationship with their implementation on optical processors. This implementation is in our proposal performed by using the JTC optical setup.

This JTC setup will be the basic concept on which most experimental optical methods described in this review are based. The inherent parallelism of optics provides an appropriate framework for information processing techniques. However, from a practical point of view, it is worth emphasizing that the latter is conditioned largely by the existence of powerful devices.

Our research area advances the frontiers of signal processing and pattern recognition. In this area, a tool like correlation is based on the use of classical matched filtering and is optically implemented by the JTC optical setup.

One key advantage of optics compared with digital-only methods lies in its capability to provide massively parallel operations in a 2D space. Approaches that consist of this kind of processing the data is a topic that has generated great interest from both academic and practical perspectives, as evidenced by the special 'Advances in Optics and Photonics' issue including a tutorial on Optical image compression and encryption methods [21]. As we explain in some detail, in fact these methods become more and more complex to implement optically, especially when we are interested in color images or video sequences, every time the rate of image encryption increases. Carrying out a part of the processing digitally is a relevant solution to solve this complexity while maintaining a high security level.

In this work, we focus on the JTC experimental approach. We distinguish two kinds of solutions. First, there are solutions based on photorefractive crystals [22]. The second type of solution consists in using digital holography as working tool [23].

One major difference between the work presented here and the literature already existing is that we are interested in multiplexing operations and the possibilities they offer for encryption. More specifically, we pay special attention to multiplexing encryption methods that can be realized experimentally. These methods have progressed through the work of many research teams. Space allows us to mention only a sample from well-known groups, from which the interested reader may gain a sense of the scope and power of these ideas. To achieve this goal, photorefractive crystals, and digital holography need to be used.

Photorefractive crystals are used for instance to de-multiplex in real time by tuning a phase conjugation approach using the storing capabilities.

As will be explained, speckle modulation is controlled in the crystal by an external applied voltage, by converting coherent light information from the JTC setup into charge redistribution in the crystal. In the last, one needs a writing light beam containing the modulation information and a reading coherent light beam.

A major advantage of the opto-digital tactic appears in the decryption process. The user can either employ a digital recovering procedure or perform an experimental decryption. The decryption stations are designed to guarantee a straightforward and fast processing while keeping all the security standards. In the area of experimental implementations, we also distinguish single and multiple data approaches under the JTC architecture.

Simple proposals were performed digitally by means of a JTC-based architecture, where the scene is encrypted at a Fresnel plane by means of a random phase reference. The encrypted field and the decrypting key, registered as Fresnel holograms, are obtained by phase-shifting interferometry in the JTC for instance in Ref. [19]. Here, the position of the Fresnel plane is an additional security parameter. Generally, a CCD is used for the registering process. The idea is to gain some simplification, not only in the encrypting step but also in the final user information retrieval procedure. Other contributions pursue methods to eliminate the need of a complex conjugate of the encrypting key. In any case, as expected for these approaches, the digital format of the holographic data can be transmitted to receivers through data communication channels. After the transmission of the encrypted data authorized remote users, who use a correct digital hologram, are able to correctly reconstruct the original data through optical correlation. If one does not have the key hologram, the reconstructed data will be noise-like.

In this regard, a practical digital holographic implementation of the JTC architecture uses the basic JTC setup in one arm of a Mach-Zehnder interferometric arrangement and a reference wave in the other arm.

In the multiplexing options, we show the main drawback in recovering decoded results: the superposition or cross-talk or even background noise. Therefore, it is important to recover results with noise elimination or at least reduction. We described several successful attempts in this direction, like moving the reference wave, key rotations, digital repositioning, object sub-sampling, etc.

In this contribution, we have presented several recent studies concerning optical encryption applications. The focus of this work is on using the JTC methods. Originally, the JTC based methods have been used to find an object in a target scene, but they are not confined to this specific application. They can be used to modify the spectral distribution of given information (for encryption). It is worth mentioning again that the significance of these optical methods lies in their ability to perform encryption in the spectral domain.

The first part of this presentation is devoted to the introduction of several optical methods employing photorefractive crystals. Satisfactory results can be obtained by these methods. Indeed, they have been developed for some specific applications, e.g., the multiplexing domain. Other methods have attempted to implement optical encryption methods, but they encountered a serious problem due to the complexity of the setup required for implementing them optically, especially regarding phase conjugation.

In the second part of this review, several optical encryption methods based on digital holography are described. These methods have received special interest because of the simplicity of their principles.

Several studies have been developed to improve the encryption rate, specifically to achieve encrypted movies. This led to an increase of the implementation complexity, but we present a practical solution, which is explained in detail.

Although we hope to have provided a sample of some of the techniques and ideas of encryption methods in this review, our strategy has been to give only a few examples. For readers more interested in encryption techniques, we recommend [24]. For a deeper understanding and further applications of these ideas, the interested reader is invited to consult the cited literature, which is a selection of what we found particularly useful. In closing, we can notice that the methods of encryption using photorefractive crystals and digital holography have been developed separately, knowing that they are linked and influence each other. We strongly believe that mixed methods will be developed in the future to meet the needs of information technology. In addition, we feel that hybrid methods (optical-digital) need to be further developed for two reasons. On the one hand, they let us simplify problems associated with optical implementation, such as the need to use several SLMs, and the problem of alignment. On the other hand, they can increase encryption rates, specifically for dynamical situations.

This work survey is structured as follows. In Section 2, we present a brief yet detailed summary related to the JTC architecture. Section 3 presents three applications of encryption multiplexing techniques carried out in photorefractive crystals, studying the dependence with wavelength, additional security keys and a multi-channeling option. Finally, in section 4 we show examples of experimental digital holography applications of optical encryption, exhibiting the potentials for prospective uses. Indeed, this section will enable us to help the reader appreciate optical encoding techniques based on the most recent advances in this regards.

2 Encryption by using JTC architecture

The conventional JTC encryption architecture contains two apertures, one with the input image information bonded to a random phase mask, while the other aperture contains the random phase key code. We denote $r_i(x_0, y_0)$ as the object random-phase mask, $o_i(x_0, y_0)$ as the object to be encrypted and $k_i(x_0, y_0)$ the key code, which are positioned at coordinates $(-a, 0)$, $(-a, 0)\,(-a,0)$ and $(a, 0)$, respectively. The input plane of the JTC is,

$$i(x_0, y_0) = u_i(x_0, y_0) \otimes \delta(x_0 - (-a), y_0) \; + k_i(x_0, y_0) \otimes \delta(x_0 - a, y_0) \qquad ...(1)$$

where $u_i(x_0, y_0) = o_i(x_0, y_0)\, r_i(x_0, y_0)$. The joint power spectrum (JPS) (encrypted power spectrum) corresponding to the signal encryption is given by,

$$\begin{aligned} JPS(u, \nu) = {} & \left|U_i(u, \nu)\right|^2 + \left|K_i(u, \nu)\right|^2 \\ & + [U_i(u, \nu)]^* \cdot K_i(u, \nu) \cdot \exp(-i4\pi au) \\ & + [U_i(u, \nu)] \cdot K_i^*(u, \nu) \cdot \exp(i4\pi au) \end{aligned} \qquad ...(2)$$

where $U_i(u, v)$, $K_i(u, v)$ represent the Fourier transforms (FT) of $u_i(k_0, y_0)$ and $k_i(k_0, y_0)$, respectively; and the symbol * denotes the complex conjugate. When $K_i(u, v)$ have phase-only information so $|K_i(u, v)|^2 = 1$, which is required for perfect recovery of the decrypted image.

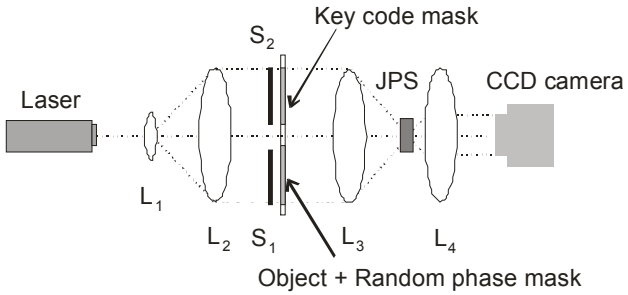


Fig. 1. Encryption scheme by using JTC architecture (L_1, L_2, L_3 and L_4: lenses; S_1 and S_2: shutters; JPS: joint power spectrum).

In the decryption process, the key code mask $k_i(k_0, y_0)$ is returned to the input plane to decode the encrypted JPS and then retrieve the input image. When the key code is placed at $(a, 0)$, the encrypted power spectrum is illuminated by $K(u, v)$. $\exp[-2\pi iau]$. We obtain

$$\begin{aligned} M(u, \nu) = {} & JPS(u, \nu) \cdot K_i(u, \nu) \cdot \exp\left(-2\pi iau\right) \\ = {} & \left|U_i(u, \nu)\right|^2 \cdot K_i(u, \nu) \cdot \exp\left(-2\pi iau\right) \\ & + \left|K_i(u, \nu)\right|^2 \cdot K_i(u, \nu) \cdot \exp\left(-2\pi iau\right) \\ & + \left[U_i(u, \nu)\right]^* \cdot K_i(u, \nu) \cdot K_i(u, \nu) \cdot \exp\left(-6\pi iau\right) \\ & + U_i(u, \nu) \cdot \exp\left(2\pi iau\right) \end{aligned} \qquad ...(3)$$

By inverse Fourier-transforming $M(u, v)$, we obtain

$$\begin{aligned} m(x,y) = & k_i(x,y) \otimes \left[u_i(x,y)\right] \cdot \left[u_i(x,y)\right] \otimes \delta\left(x-a\right) \\ & + k_i(x,y) \otimes \delta\left(x-a\right) \\ & + k_i(x,y) \otimes k_i(x,y) \cdot \left[u_i(x,y)\right] \otimes \delta\left(x-3a\right) \\ & + u_i(x,y) \otimes \delta\left(x-\left(-a\right)\right) \end{aligned} \tag{4}$$

The intensity of the fourth term of this equation produces the input image. The undesired terms are spatially separated from the recovered image.

3 Experimental encryption by using photorefractive crystals as recording medium

In the following, we will describe a first experimental approach to optical encryption using photorefractive crystals. In Ref. [18] an optical data storage system for encrypting by using a JTC architecture is demonstrated experimentally. Actually, in this original work the optical set-up is not an exact JTC setup (see Fig. 2). Accordingly, the encrypted information is stored as intensity distribution. In such a case, photorefractive crystals represent an adequate storing medium. Nomura et al.[19] use a $LiNbO_3$ ferroelectric photorefractive crystal doped with iron ions ~0.05 mol to store the JPS. In the crystal, the refractive index change is proportional to the fringe modulation depth. This property makes the crystal a suitable device to record an encrypted power spectrum. In the decryption step, the JPS is illuminated by the FT of the key code mask. After Fourier transforming with lens L_4, a CCD camera captures the decrypted image. The crystal operates as a volume hologram. In the decryption process, when we use the correct key code, its meets the Bragg condition.

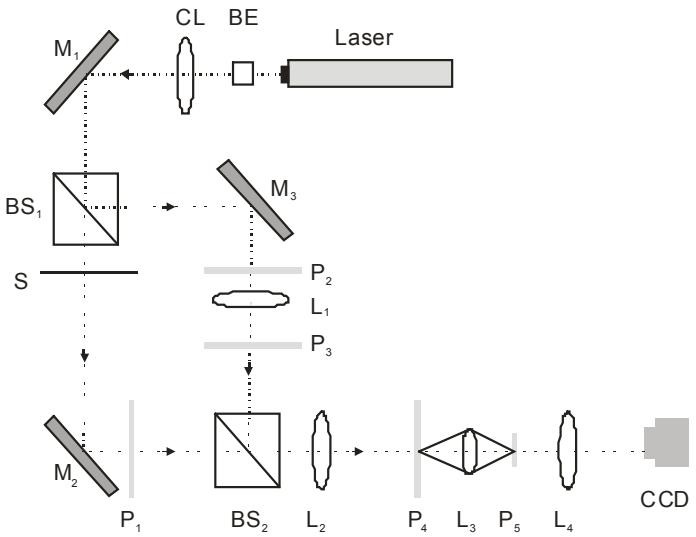


Fig. 2. Photorefractive optical arrangement employed to demonstrate the double random phase encryption using a JTC architecture (BE: beam expander, M_1; M_2 and M_3: mirrors; L_1, L_2, L_3 and L_4: lenses; BS_1 and BS_2: beam splitters, S: shutter).

3.1 Multiple encryption by using photorefractive crystals

Photorefractive holographic memories are attractive due to their high-density storage capacity [25], which can be advantageously extended to perform multiple image encryption [26]. In general, the main idea of multi-encryption methods consists in encoding several input objects and storing them into a single medium (in our case, a photorefractive crystal) [27-29]. It should be pointed out that the multiplexing schemes exhibits

better security because an intruder, which intercepts the encrypted multiplexed data, could not determine by simple observation, the number of objects included in the storing medium.

Different methods have been proposed to multiplex encrypted data. However, the techniques may present overlapping (cross-talk) between decrypted images. The conventional way to store multiple data in a volume-recording medium is by introducing different recording angles to store data (angular multiplexing). In fact, the first multiplexing proposal based on the JTC architecture is implemented by angular multiplexing [19]. In this work, a 10 mm x 12 mm x 2 mm $LiNbO_3$ crystal doped with 0.03 mol % iron is used as a volume storing medium. The basic experimental set-up is depicted in Fig. 1. During the encrypting process, the collimated Nd YAG laser beam (532 nm) illuminates both the object to be encrypted and the key code, which are placed side-by-side at input plane. In addition, a random phase mask is bonded to the object. This input is Fourier transformed and the JPS is recorded into a photorefractive crystal. In the decryption process, the JPS is illuminated by the Fourier transform of the key code. The recovered image after Fourier transforming is obtained at CCD camera plane (see Fig. 1). In this case, the decrypted image quality diminishes due to the non uniformity of the Fourier amplitude distribution of the key code.

Also, in Ref. [19] it is experimentally verified that it is possible to implement multiplexing procedures by changing the key code. If a new statistical independent random phase mask replaces the original key code mask, the encrypted pattern (that is the joint power spectrum) changes as well. Then, several objects encrypted with statistical independent key code masks and multiplexed in a single recording medium, can be decrypted without cross-talk.

In the JTC architecture, the encrypted pattern depends on the key code mask characteristics, optical parameters (illumination wavelengths, polarization, etc) and/or geometrical parameters. Then, the mentioned optical parameters, like the wavelength for instance, represent valid alternatives to implement multiple secure data recording. In order to apply the multiplexing procedure, it is necessary to evaluate the recovering performance when decrypting with a wavelength different from that employed in the encryption step. As mentioned, a problem associated with multiplexing operations is the possible cross-talk between the recovered images that would distort the final outputs. In Ref. [30], it is theoretically determined the minimum wavelength change that prevents the decrypting cross-talk.

This analysis is confirmed by the experimental implementation presented in Ref. [31]. Multiplexing is achieved by keeping the same optical scheme and same random phase masks in each encrypting step, and only changing the illuminating wavelength. As expected, if the illumination wavelength changes though maintaining the other parameters, the encrypted spectrum changes as well. The spectral-dependent JPS, allows multiple encryptions, avoiding the need of different key code masks, while keeping parallel image handling.

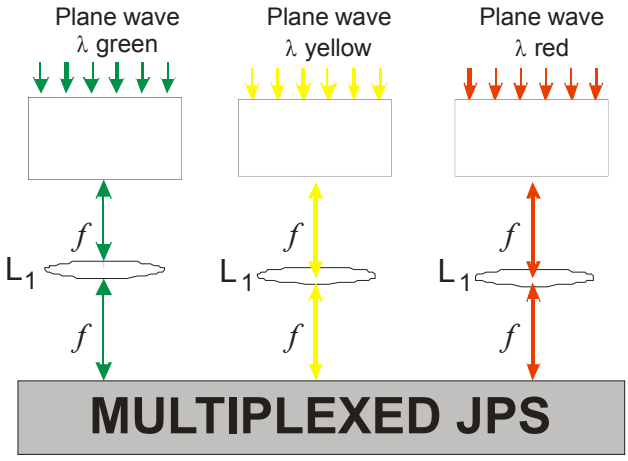
In the experimental set-up, the different wavelength components are obtained by using a tunable Ar-Kr laser. Photorefractive BTO silenite crystal represents an interesting option to implement experimentally in real time the mentioned optical encryption scheme by storing the JPS. In order to understand the result, it is necessary to consider the storage-read-out behavior in these crystals for low frequency modulated patterns that is JPS [32, 33]. The intensity distribution received by this crystal creates photocharges. In the JTC scheme, the charges drift due to the external electric field. The intensity distribution received by the crystal is encoded as the spatial distribution of the resulting electric field strength at each point. This field induces, through the linear electro-optic effect the crystal exhibits, the corresponding spatial variation of the refractive index. Therefore, the JPS in each exposure is stored as an index grating systemFor multiplexing, each input object, independently encrypted with a different wavelength, is sequentially recorded and multiplexed in a single photorefractive crystal. This operation yields the final single multiplexed encrypted data. In the experimental verification, three input objects are multiplexed in a BTO crystal by using the wavelengths 647 nm, 556nm and 520nm. Among the available Ar-Kr tunable laser lines, the selection of

wavelengths is based on the power of each line and the highest diffraction efficiency. In the case of a BTO crystal, the blue lines absorption coefficient is very high. Therefore, the diffraction efficiency of those lines is severely decreased and consequently disregarded.

In the decryption step, the crystal is illuminated only by the FT of the key code mask and one recording wavelength. The diffracted light is collected at the back focal plane of L_2, reconstructing thereby the input object according to the selected wavelength. As expected, the user should receive the encrypted information, the key code mask, and the wavelength information to retrieve the input data. The wavelength information can be sent to each authorized users via a separate channel other than the one used to send the key mask. The experimental results of Fig. 3 shows the feasibility of multiple image encryptions by spectral multiplexing in the JTC configuration.

In the 4f encryption architecture, a way to multiplex images is to introduce an appropriate shifting in the encoding mask [26, 34]. However, in the conventional JTC architecture the encoding mask shifting does not represent a valid alternative to multiplex information. The JTC-based encrypting system is invariance to in-plane shifts of the key masks in the decryption process. In this scheme, the JTC input is illuminated by a plane wave and a constant phase factor is introduced by the random phase mask displacement and therefore the JPS do not change. However, it is possible to implement a non invariant alternative scheme as can be demonstrated in Ref. [35]. In order to introduce in the JTC scheme an approach similar to the in-plane shifting of the 4f scheme, the mentioned in-plane invariance needs to be broken. This proposal consists in replacing the plane wave illuminating beam of the conventional JTC scheme by a structured illumination. This structured wave front is obtained by introducing an additional random phase mask in the beam path (see the diagram depicted in Fig. 4). In Ref. [35], authors investigated the effect of 3D displacements of each of the involved random phase masks. As the two random phase masks are 2D, the variation of their relative distance can be considered as an additional dimension, thereby raising the total scheme to a 3D encrypting method.

In the proposed modified JTC architecture, the introduction of an additional mask, which acts as an extra encrypting key in addition to the conventional key mask, reinforces the system security. Therefore, in the decryption step when any of the masks is located at an incorrect position, the input data cannot be recovered and only noise appears at the output plane. In this case, an intruder requires additional information on the structure and relative positioning of the space-invariant breaking mask. In addition, both random masks have an equivalent security hierarchical level.



(a)

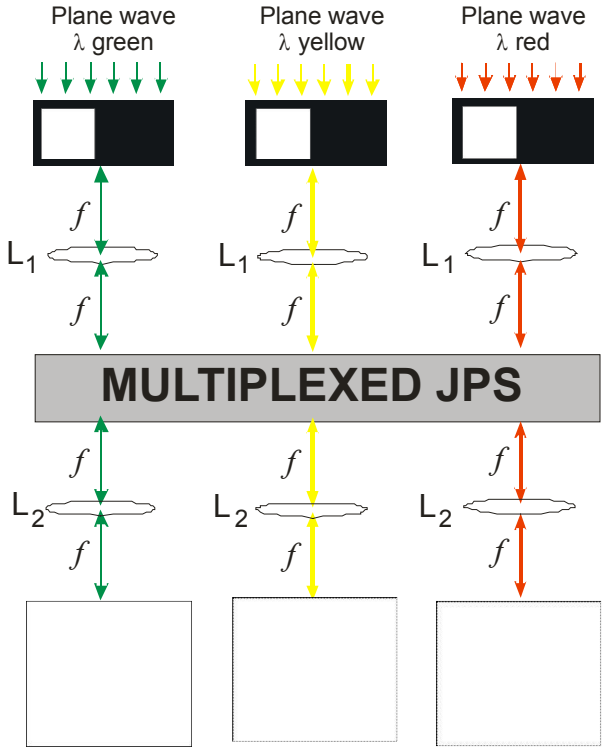
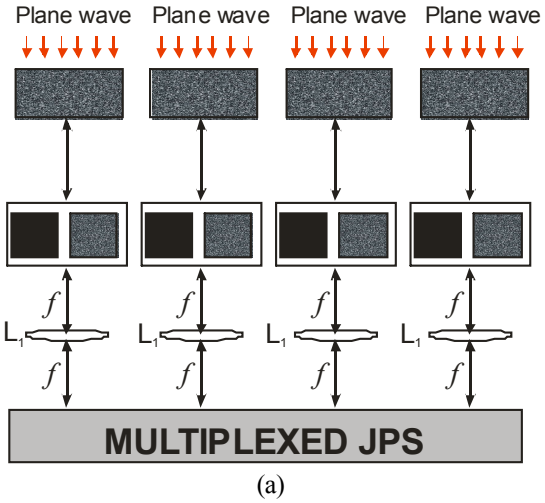
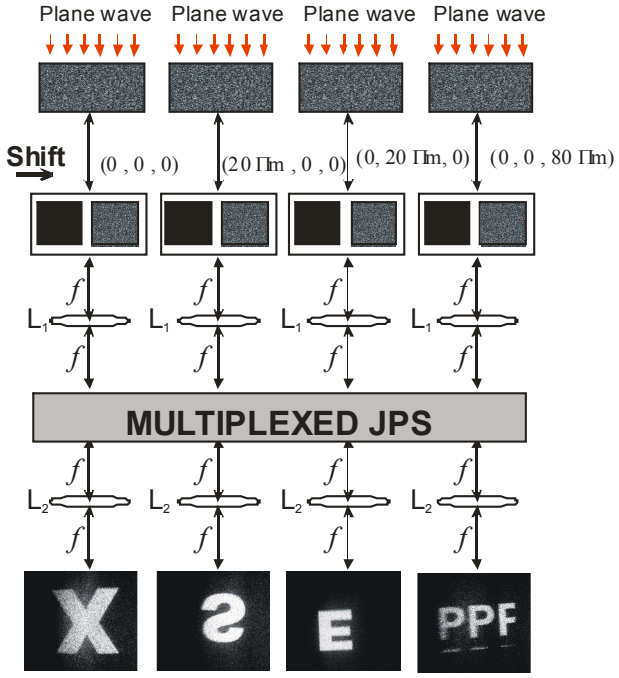


Fig. 3. Wavelength multiplexing encryption scheme (a) Encryption step diagram (b) Decryption step diagram (L_1 and L_2: lenses and f: focal length).

Once the invariance is broken, an in plane shifting of the encrypting mask allows multiplexing data in the same recording media and recovering without cross-talk. We experimentally demonstrate multiple encryptions based on shifting the additional random phase mask (see the results shown in the diagram of Fig. 4).

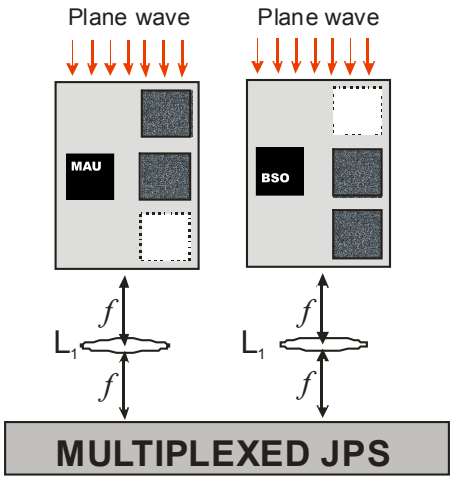




(b)

Fig. 4. Extra encrypting key in the JTC double random phase encryption architecture. (a) Encryption step diagram (b) Decryption step diagram (L_1 and L_2: lenses and f: focal length).

Another interesting alternative in the encryption procedure is to use multiple random-phase masks as windows, all in the JTC input plane. This new approach provides different access levels [36]. Considering a double exposure scheme, a multiplexing operation is performed when the sequential encryption of input objects is implemented by using multiple random phase masks that change between exposures (see the scheme of Fig. 5). During the decryption step, the appropriate use of the random-phase mask can ensure the retrieval of different non-mixed information. In summary, the random phase mask delivered to the user determines the information accessibility.



(a)

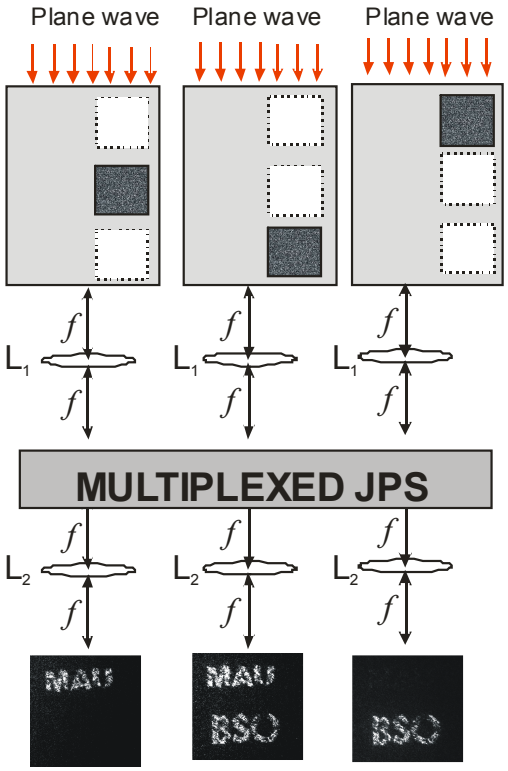


Fig. 5. Multiple random phase masks encryption scheme (a) Encryption step diagram (b) Decryption step diagram (L_1 and L_2: lenses and f: focal length).

In the following, the encryption of a single signal is described. We denote $r_i(x_0, y_0)$ as the image random-phase mask, $o_A(x_0, y_0)$ as the object to be encrypted and $k_{Ai}(x_0, y_0)$ and $k_i(x_0, y_0)$ as the key codes, which are positioned at coordinates $(-a, 0)$; $(-a, 0)$; $(a, 0)$ and (a, b), respectively. In this case, the JPS corresponding to one encryption data is given by,

$$\begin{aligned} JPS(u,v) = {} & \left|U_i(u,v)\right|^2 + 1 + 1 \\ & + \left[U_i(u,v)\right]^* \cdot K_i(u,v) \cdot \exp\left(-i4\pi au\right) \\ & + \left[U_i(u,v)\right] \cdot K^*{}_i(u,v) \cdot \exp\left(i4\pi au\right) \\ & + \left[U_i(u,v)\right]^* . K_{Ai}(u,v) \cdot \exp\left[-2i\pi(2au + bv)\right] \\ & + \left[U_i(u,v)\right] \cdot K_{Ai}{}^*(u,v) \cdot \exp\left[2i\pi(2au + bv)\right] \\ & + K^*{}_i(u,v) \cdot K_{Ai}(u,v) \cdot \exp\left(-2i\pi bv\right) \\ & + K_i(u,v) \cdot K_{Ai}{}^*(u,v) \cdot \exp\left(2i\pi bv\right) \end{aligned} \quad \ldots(5)$$

where $U_i(u, v)$, $K_i(u, v)$, $U_{Ai}(u, v)$ represent the FTs of $u_i(x_0, y_0)$, $k_i(x_0, y_0)$ and $k_{Ai}(x_0, y_0)$. In the decryption process, the key mask $k_{Ai}(x_0, y_0)$ and/or $k_i(x_0, y_0)$ is returned to the input plane to decode the encrypted JPS and then retrieve the input image. Thus, we obtain the decrypted image in the output plane. We cannot recover the input object $o_A(x_0, y_0)$ without the knowledge of $k_i(x_0, y_0)$ and/or $k_{Ai}(x_0, y_0)$. For instance, when the key code is placed at the encrypted power spectrum is illuminated by . After inverse-Fourier-transforming we recover the input object, given that is positive and an intensity-sensitive device removes

the phase function . Clearly, if the other key code is employed in the decryption step, the same input information is obtained at the output plane.

The multiplexing procedure is operated by changing the input objects and the multiple key code mask between the two exposures as seen in the block diagram schematized in Fig. 5. We show the aperture random phase masks arrangement employed to encrypt and decrypt each input data. It is evident by comparing the JTC input in each exposure that we have a common and a non-common random phase mask aperture in both exposures. In accordance with the random phase mask employed in decryption step, we can recover one object with no traces of the other input objects; or we can observe both objects simultaneously. In consequence, the random phase masks behave as separate information channels.

In every exposure, each point in the crystal receives three contributions, one from each aperture. Then, the resulting pattern appears as the interference of the mentioned distributions. These patterns are fringe modulated and the fringes are orthogonal to the line joining the aperture centers. Then, three low frequency fringe systems are produced: vertical, diagonal and horizontal. As analyzed in Ref. [37, 38] the index grating diffraction efficiency strongly depends on the direction of the fringes that modulate the speckle pattern. This anisotropic behavior must be taken into account in the modified JTC processor because it influences with different weights each term of the JPS.

4 Experimental JTC double random phase encoding using digital storage

Nowadays the employing opto-digital techniques to handle information has undisputed advantages. In particular, the storing of the optical processed information in the digital format offers important benefits; among them, we can mention: (a) the information can be transmitted and received via Internet and (b) the stored data can be processed optically or digitally. In the specific case of the optical encryption, the encrypted data and the security key(s) can be sent to the authorized user(s) via Internet [23, 39-45]. Another advantage of the opto-digital approach relies on the decryption process, where an authorized user can either apply a digital recovering procedure or perform an experimental decryption. The decryption stations are designed to assure a simple and a fast processing while keeping all the security standards.

According to the above mentioned, the advantages and characteristics of the JTC encrypting architecture along with the benefits of the opto-digital protocols provide the appropriate environment for developing a secure and flexible encrypting system. These characteristics lead to useful experimental protocol with applications in process for a single users [39, 40] or/and strategies that involve multiple users [23, 41-45].

4.1 Encrypting a single input object

In one of the first implementation of the opto-digital JTC encrypting technique, the encrypted object and the recovering key are obtained employing a three-step phase-shifting interferometric technique [39]. A programmable liquid-crystal TV display allows projecting the phase input data and producing the phase shifts. The encrypted information and the decrypted key are registered as Fresnel holograms; as a result the position of the Fresnel plane represents an extra security parameter. The objects are optically encrypted using the double random phase encoding technique and the processed data is stored in a CCD camera, then the recovering process of the original information can be performed digitally or optically. One advantage of the method is the optical encryption and decryption procedures are performed employing the same compact opto-digital experimental setup.

Afterwards, it was proposed and implemented another opto-digital JTC encrypting configuration (see Fig. 6). In this proposal, the experimental set up is a Mach–Zehnder interferometer with a JTC encrypting system in one arm and a reference wave in the other [40]. The encrypting step is carried out in an optical set up meanwhile the decrypting process is done digitally [23, 39-45]. In this contribution, the intensity saturation was recognized as a source of additional noise. The filtering of the non-relevant terms reduces the amount of handled information, making the whole process more efficient [40]. The basic experimental setup employed to encrypt the input data is shown in Fig. 6.

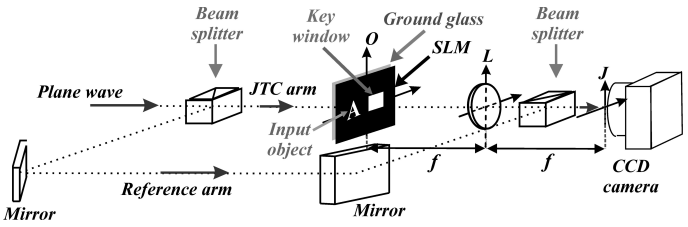


Fig. 6. Optical setup for the encrypting procedure (*SLM*: spatial light modulator, *O*: input plane, *L*: lens of focal distance *f*, *J*: CCD camera plane).

Under this scheme, the process of encrypting a single data can be described employing some elements described in the Refs. [23, 40-45]. The first step of the process is obtaining the joint power spectrum $JPS(u, v)$ at plane J (Eq. (2)). The second step is removing the contribution of the non-relevant information. The intensity terms $|U_i(u, v)|^2$ and $|K_i(u, v)|^2$ are separately recording in the CCD camera, and then subtracting them from the $JPS(u, v)$ (Eq. (2)):

$$I_i(u,v) = \left[U_i(u,v)\right]^* \cdot K_i(u,v) \cdot \exp\left(-i4\pi au\right) + \left[U_i(u,v)\right] \cdot K_i^*(u,v) \cdot \exp\left(i4\pi au\right) \quad ...(6)$$

Then, the encrypted object is obtained after removing the first term of Eq. (6) [41],

$$E(u,v) = \left[U_i(u,v)\right] \cdot K_i^*(u,v) \cdot \exp\left(i4\pi au\right) \quad ...(7)$$

The second stage of the encrypting process is getting the decryption key. Therefore, the hologram of the FT of security key is recorded by blocking the object window and simultaneously to unblock the reference arm. Then, after eliminating the non-relevant terms the hologram of the FT of security key is [41]

$$G_i(u,v) = K_i(u,v) \exp\left(-2\pi iau\right) \quad ...(8)$$

In order to recover the original object, the encrypted information (Eq. (7)) and the decrypting key (Eq. (8)) are sent to the authorized user. The recovering of the input object is performed by using the virtual optical system shown in Fig. 7. The encrypted data and the decrypting key are multiplied and after a FT operation the original data is recovered in the out plane (Fig. 7),

$$D_i(x,y) = \sum_{i=1}^{n} o_i(-x,-y)\, r_i(-x,-y) \otimes \delta(x-a,y) \quad ...(9)$$

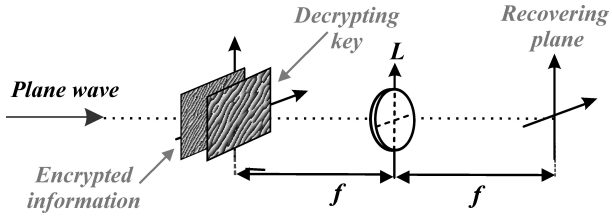


Fig. 7. Virtual optical system to decrypt the input object (Decrypting key: hologram of the FT of the encrypting key).

Finally, the intensity of the decrypted information $|D_i(x, y)|^2$ allows recovering the information of the amplitude input object $|o_i(x, y)|^2$.

4.2 Opto-digital encryption of multiple data

Once the encrypting opto-digital protocol described in section 4.1 is presented, the efforts in this area are focused in protocols to encrypt multiple data [23, 41-45]. To achieve this task, the multiplexing

techniques are the appropriate tools. In the first contribution related with the multiplexing of encrypted objects, a setup modification of the input plane of the JTC is applied. In this case, instead of placing the encrypting key in contact with the input JTC plane, the optical FT of a diffuser is projected over the entrance plane of the JTC [41]. Therefore, the optical FT of the diffuser acts as encrypting key in the input plane of the JTC encrypting architecture. The multiplexing is performed applying a controlled lateral shifts over this diffuser. The key of the protocol is that each time the diffuser is properly shifted, is equivalent to introduce a new encryption mask in the classical JTC encrypting architecture. In the implementation of the multiplexing operation, each input object is sequentially and separately encrypted with the same diffuser but placed at different lateral positions. The information of each encrypted object is obtained using the procedure described in Section 4.1. Then, encrypted objects are digitally multiplexed. According to Eq. (7), the multiplexing of n encrypted objects is,

$$M(u,v)=\sum_{i=1}^{n}\left[U_i(u,v)\right]\cdot K_i^{*}(u,v)\cdot\exp\left(i4\pi au\right) \qquad ...(10)$$

where $i = 1, 2, 3, ..., j....n$. Each authorized user has access to the multiplexing (Eq. (10)) and their respective decrypting key $G_i(u, v)$ (Eq. (8)). Note that, each key $K_i(u, v)$ corresponds to a specific lateral position of the diffuser that projects its optical FT over the entrance plane of the JTC. In order to recover the input object $o_j(x_0, y_0)$ the multiplexing is multiply by the decrypting key $G_J(u, v)$, and then a FT operation is performed to get

$$\begin{aligned}D_j(x,y)&=o_j(-x,-y)\,r_j(-x,-y)\otimes\delta(x-a,y)\\&+\sum_{i\neq j}^{n}o_i(-x,-y)\,r_i(-x,-y)\otimes\left[k_i^{*}(-x,-y)\otimes k_j(x,y)\right]\otimes\delta(x-a,y)\end{aligned} \qquad ...(11)$$

The first term of the recovered information contains the information of the input object $o_j(x_0,y_0)$, while the second term is noise produced by the non-decrypted input objects. The overlapping of these terms affects the retrieved object. As the number of object involved in the multiplexing increases, the noise increases as well. This fact represented a limit on the amount of data to be securely process [30].

In order to remove the noise caused by the non-decrypted data, the use of different reference wave angles during the encryption of each data was proposed and experimentally demonstrated [23]. The position of the recovered object in the exit plane can be fully controlled by the angle of the reference wave. Therefore, each decrypted object is decrypted in a desire position of the recovering plane avoiding any kind of superposition.

In this contribution, 24 objects are experimentally encrypted, multiplexed, and then recovered at the same plane and at the same plane in the same plane without overlapping [23]. The multiplexing of n encrypted objects under this protocol is represented by

$$M'(u,v)=\sum_{i=1}^{n}\left[U_i(u,v)\right]K_i^{*}(u,v)\exp\left[4\pi i\left(x_l u+y_l v\right)\right] \qquad ...(12)$$

where the position coordinates (x_l, y_l) are controlled with the inclination of the reference wave. When, an authorized user can recover the input object $o_j(x_0, y_0)$ multiplies the multiplexing (Eq.(12)) is multiply by the decrypting key $G_j(u, v)$. Afterwards, a simply FT operation allows recovering the input object without superposing,

$$\begin{aligned}D'_j(x,y)&=o_j(-x,-y)\,r_j(-x,-y)\otimes\delta\left(x-x_j,y-y_j\right)\\&+\sum_{i\neq j}^{n}o_i(-x,-y)\,r_i(-x,-y)\otimes\left[k_i^{*}(-x,-y)\otimes k_j(x,y)\right]\otimes\delta\left(x-x_i,y-y_i\right)\end{aligned} \qquad ...(13)$$

The position coordinates (x_l, y_l) are carefully chosen to avoid the overlapping between the decrypted information (first term of Eq. (13)) and the noise caused by the non-recovered objects (second term of Eq. (13)). Through the described technique is possible to increase significantly the amount of data to be processed in a multiplexing scheme.

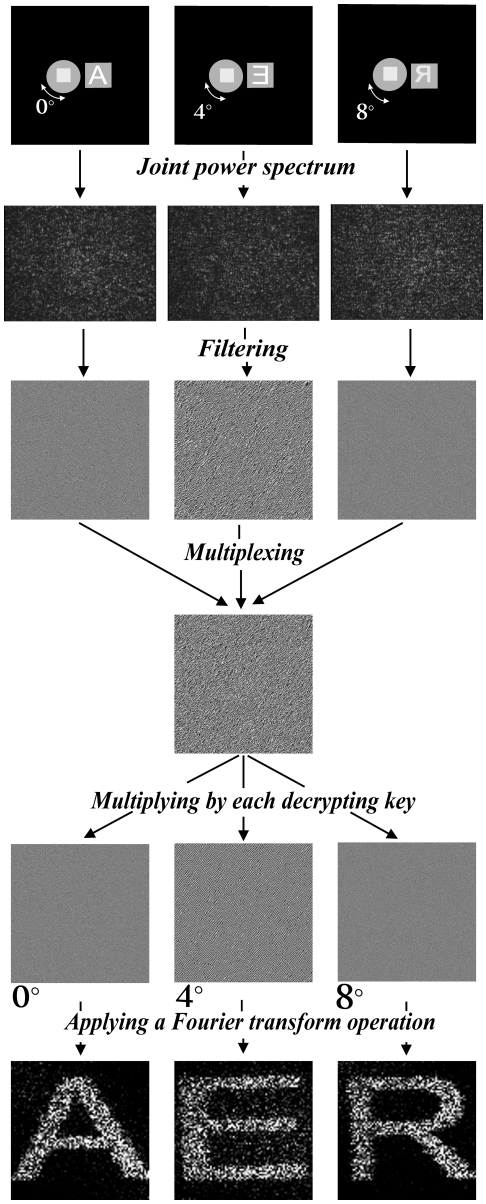


Fig. 8. Block diagram for the experimental multiplexing approach via code key rotations.

The above described procedure motivates a series of contributions that involve the securely handling of multiple data in an efficient way [42-45].

Introducing lateral shifts over a random phase mask is an alternative to perform a multiplexing procedure [26, 41]. It is possible under a 4f encrypting architecture [26] or when the random phase mask is

placed at the back Fourier plane of a JTC arrangement [41]. Applying in-plane translations over the encrypting key in a JTC classical encrypting architecture is not an alternative to carry out a multiplexing operation, as it results in invariance under the in-plane translations. Accordingly, a new strategy is designed on a different approach, namely, in-plane rotations. Accordingly, a novel experimental protocol has been proposed by using the classical JTC encrypting architecture to multiplex information, namely, in-plane rotations [42]. In this application, the rotation of the input plane encoding mask admits the multiplexing capability.

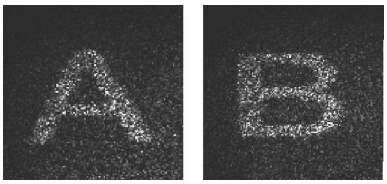
We employ the procedure described above to separately encrypt each single object and then obtain the multiplexing (Eq. (12)). Thus, removing the non-relevant terms and avoid the overlapping among the recovered object and the non-decrypted data. Each object is encrypted using a different in-plane angular position of a single diffuser. The angular position of diffuser is carefully chosen to avoid any kind of cross-talk. In order to retrieve the objects, the multiplexing (Eq. (12)) and the hologram of the FT of a security key (Eq. (8)) are multiplied and after a FT operation, the corresponding input object is recovered. It is important to remark that the different decrypting keys $G_i(u, v)$ are generated with the same random phase mask but placed in different in-plane angular positions. In Fig. 8 is shown the diagram of the entire process for three input objects.

Afterwards, an experimental opto-digital synthesis of encrypted sub-samples of an image to improve its decoded quality is presented [43]. The implementation of the proposed method allows experimentally the recovering of better decoded images without losing the security level of the process, or making difficult the recording and processing systems. In particular, the technique allows visualizing decrypted objects that otherwise would have been barely recognizable. The image deterioration is partly due to the speckle noise as well as the practical limitations of the optical setup.

The proposal leads us to consider an input object as a sample and each equally subdivided part as a sub-sample. Then, instead of encrypting the whole object, the subsamples are separately encrypted with the same key and then multiplexed. Using the methodology described above, after a right choice of the position coordinates (x_l, y_l) during the encryption of each sub-sample, the entire sample can be recovered in a single step.

The demonstrated versatility of the multiplexing protocol leads to other interesting developments [44, 45]. One important applications of the multiplexing under a JTC encrypting protocol is presented as the first experimental technique to encrypt a movie. Additionally, the method is extended to multiplex several movies in a single package. In this case, instead of encrypting an object or a sub-sample of an object, each single frame of a movie is separately and sequentially encrypted, and then all the encrypted frames are multiplexed to obtain the encrypted movie [44]. Three movies are experimentally encrypted in a single package employing three different security keys. The encrypted movies and their corresponding encrypting keys enable the recovering of the videos, as described above. In order to recover a movie, it is necessary to guarantee that every decoded frame follows a specific spatial order with the right time interval between them.

In Ref. [45], a master key generation, a concept which has not been employed so far in the context of the experimental optical encryption, is proposed and experimentally demonstrated to avoid the use of an external reference wave. The technique is successfully applied for several input objects.



(a) (b)

Fig. 9. Experimental results: (a) and (b) are the decrypted objects employing the same master key and their respective encoding keys.

In the first step of the protocol, the hologram of the FT of the master key is stored and processed using an interferometric arrangement and the digital holographic technique described above. The second step consists in obtaining the encrypted object with the usual procedure. For the third step, the JPS between the master key and the encrypting key is stored and processed. The user can recover the original information by means of the information processed in these three steps. The method allows carrying out of an optical encrypting process using the interferometric setup only for getting the information of the master key.

In case of handling multiple data, each input object is encrypted with different keys and the encrypted objects are multiplexed (Eq. (12)). Then, the JPS between each key and the master key is recorded and processed.

Fig. 9 represents the experimental demonstration of the applicability of the master key concept in case of securely handling of two objects [45]. We recall that the introduction of the master key in the optical encrypting protocol presents two main advantages: (a) the application of the external reference wave is reduced to only once during the experimental procedure in a JTC encrypting architecture and (b) the security of the double random phase mask encoding technique is reinforced, as the encoding key and the master key are needed to recover each of the involved objects.

Acknowledgments: This research was performed under grants TWAS-UNESCO Associateship Scheme at Centres of Excellence in the South, CONICET No. 0863/09 and No. 0549/12 (Argentina), and Facultad de Ingeniería, Universidad Nacional de La Plata No. 11/I168 (Argentina), Sostenibilidad 2011-2012 and CODI (Universidad de Antioquia-Colombia).

References

1. Weaver C S, Goodman J W, A technique for optically convolving two Functions, *Appl Opt*, 5(1966)1248-1249.
2. Yu F T S, Lu X J, A real-time programmable joint transform correlator, *Opt Commun*, 52(1984)10-16.
3. Yu F T S, Jutamulia S, Lin T, Gregory D A, Adaptive real-time pattern recognition using a liquid crystal TV based joint transform correlator, *Appl Opt*, 26 (1987)1370-1372
4. Lu G, Zhang Z, Wu S, Yu F T S, Implementation of a non-zero-order joint-transform correlator by use of phase-shifting techniques, *Appl Opt*, 36(1997)470–483.
5. Li C, Yin S, Yu F T S, Nonzero-order joint transform correlators, *Opt Eng*, 37(1998)58-65.
6. Abookasis D, Arazi O, Rosen J, Javidi B, Security optical systems based on a joint transform correlator with significant output images, *Opt Eng*, 40(2001)1584-1589.
7. Refregier P, Javidi B, Optical image encryption based on input plane Fourier plane random encoding, *Opt Lett*, 20(1995)767-769.
8. Matoba O, Javidi B, Encrypted optical memory system using three-dimensional keys in the Fresnel domain, *Opt Lett*, 24(1999)762-764.
9. Tajahuerce E, Javidi B, Encrypting three dimensional information with digital holography, *Appl Opt*, 39(2000) 6595-6601.
10. Arizaga R, Henao R, Torroba R, Fully digital encryption technique, *Opt Commun*, 221(2003)43-47.
11. Guo Y, Huang Q, Du J, Zhang Y, Decomposition storage of information based on computer-generated hologram interference and its application in optical image encryption, *Appl Opt*, 40(2001)2860-2863.
12. Takai N, Mifune Y, Digital watermarking by a holographic technique, *Appl Opt*, 41(2002)865-873.
13. Arizaga R, Torroba R, Validation through a binary key code and a polarization sensitive digital technique, *Opt Commun*, 215(2003)31-36.
14. Kim H, Lee Y, Optimal watermarking of digital hologram of 3D object, *Opt Expr*, 13(2005)2881-2886.
15. B. Hennelly and J. Sheridan, "Image encryption and the fractional fourier transform, *Optik,* 114(2003)251-265.
16. Situ G, Zhang J, Double random-phase encryption in the Fresnel domain, *Opt Lett*, 29(2004)1584–1586.
17. Hennelly B, Sheridan J, Random phase and jigsaw encryption in the Fresnel domain, *Opt Eng*, 43(2004)2239-2249.

18. Nomura T, Javidi B, Optical encryption using a joint transform correlator architecture, *Opt Eng*, 39(2000) 2031-2035.
19. Nomura T, Mikan S, Morimoto Y, Javidi B, Secure optical data storage with random phase key codes by use of a configuration of a joint transform correlator, *Appl Opt*, 42(2003)1508-1514.
20. Amaya D, Tebaldi M, Torroba R, Bolognini N, Digital color encryption using a multi-wavelength approach and a joint transform correlator, *J Opt A Pure Appl Opt*, 10(2008104031-104035. **Pl check the name of Journal.**
21. Alfalou A, Brosseau C, Optical image compression and encryption methods, *Adv Opt Photon*, 1(2009)589-636.
22. Tebaldi M, Furlan W, Torroba R, Bolognini N, Optical-data storage-readout technique based on fractal encrypting masks, *Opt Lett*, 34(2009)316-318.
23. Henao R, Rueda E, Barrera J, Torroba R, Noise-free recovering of optodigital encrypted and multiplexed images, *Opt Lett,* 35(2010)333-335.
24. Matoba O, Nomura T, Perez-Cabre E, Millan M S, Javidi B, Optical techniques for information security, *Proc IEEE*, 97 (2009)1128-1148.
25. Mok F H, Angle-multiplexed storage of 5000 holograms in lithium niobate, *Opt Lett*, 18(1993)915-917.
26. Barrera J F, Hena R, Tebaldi, Torroba R, Bolognini N, Multiplexing encryption-decryption via lateral shifting of a random phase mask, *Opt Commun*, 259(2006) 532-536.
27. Unnikrishnan G, Joseph J, Singh K, Optical encryption system that uses phase conjugation in a photorefractive crystal, Appl. Opt, 37(1998)8181-8186.
28. Barrera J F, Henao R, Tebaldi M, Bolognini N, Torroba R, Multiple image encryption using an aperture modulated optical system, Opt Commun, 261(2006)29-33.
29. Barrera J F, Henao R, Tebaldi M, Bolognini N, Torroba R, Multiplexing encrypted data by using polarized light, *Opt Commun*, 260(2006)109-112.
30. Amaya D, Tebaldi M, Torroba R, Bolognini N, Wavelength multiplexing encryption using JTC architecture, *Appl Opt*, 48(2009)2099-2104.
31. Tebaldi M, Horrillo S, Pérez-Cabré E, Millán M S, Amaya D, Torroba R, Bolognini N, Experimental color encryption in a joint transform correlator architecture, *Journal of Physics*: Conf Series, 274(2011)012054 (doi:10.1088/1742-6596/274/1/012054).
32. Tebaldi M, Lencina A, Bolognini N, Analysis and applications of the speckle patterns registered in a photorefractive BTO crystal, *Opt Commun*, 202(2002)257-270.
33. Tebaldi M, Toro L A, Trivi M, Bolognini N, Optical processing by fringed speckles registered in a BSO crystal, *Opt Eng*, 39(2000)3232-3238.
34. Wang B, Sun C, Su W, Chiou A E T, Shift tolerance of a double random phase encryption system, *Appl Opt*, 39 (2000)4788-4793.
35. Rueda E, Tebaldi M, Torroba R, Bolognini N, Three-dimensional key in a modified joint transform correlator encryption scheme, *Opt Commun*, 284(2011)4321- 4326.
36. Amaya D, Tebaldi M, Torroba R, Bolognini N, Multichanneled encryption via a modified Joint Transform correlator architecture, *Appl Opt,* 47(2008)5903-5907.
37. Tebaldi M, Toro L A, Lasprilla M C, Bolognini N, Image multiplexing by speckle in BSO, *Opt Commun*, 155(1998) 342- 350.
38. Tebaldi M, Lencina V, Bolognini N, Analysis and applications of the speckle patterns registered in a photorefractive BTO crystal, *Opt Commun*, 202(2002)257-270.
39. Mela C La, Iemmi C, Optical encryption using phase-shifting interferometry in a joint transform correlator,*Opt Lett*, 31 (2006)2562-2564.
40. Rueda E, Barrera J F, Henao R, Torroba R, Optical encryption with a reference wave in a joint transform correlator architecture, *Opt Commun*, 282(2009)3243-3249.
41. Rueda E, Barrera J F, Henao R, Torroba R, Lateral shift multiplexing with a modified random mask in a JTC encrypting architecture, *Opt Eng*, 48(2009)027006.

42. Rueda E, Ríos C, Barrera J F, Henao R, Torroba R, Experimental multiplexing approach via code key rotations under a joint transform correlator scheme, *Opt Commun*, 284(2011) 2500-2504.
43. Barrera J F, Rueda E, Ríos C, Tebaldi M, Bolognini N, Torroba R, Experimental opto-digital synthesis of encrypted sub-samples of an image to improve its decoded quality, *Opt Commun*, 284(2011)4350-4355.
44. Barrera J F, Tebaldi M, Ríos C, Rueda E, Bolognini N, Torroba R, Experimental multiplexing of encrypted movies using a JTC architecture, *Opt Expr*, 20(2012)3388-3393.
45. Rueda E, Ríos C, Barrera J F, Torroba R, Master key generation to avoid the use of an external reference wave in an experimental JTC encrypting architecture, *Appl Opt*, 51(2012)822-1827.

[*Received*: 1.03.2013; *accepted*: 20.05.2013]