

Experimental multiplexing protocol to encrypt messages of any length

This article has been downloaded from IOPscience. Please scroll down to see the full text article.

2013 J. Opt. 15 055404

(<http://iopscience.iop.org/2040-8986/15/5/055404>)

View [the table of contents for this issue](#), or go to the [journal homepage](#) for more

Download details:

IP Address: 186.137.32.14

The article was downloaded on 20/03/2013 at 17:29

Please note that [terms and conditions apply](#).

Experimental multiplexing protocol to encrypt messages of any length

John Fredy Barrera¹, Alejandro Vélez¹ and Roberto Torroba²

¹ Grupo de Óptica y Fotónica, Instituto de Física, Universidad de Antioquia, AA 1226, Medellín, Colombia

² Centro de Investigaciones Ópticas (CONICET La Plata-CIC) and UID OPTIMO, Facultad de Ingeniería, Universidad Nacional de La Plata, PO Box 3 CP 1897, La Plata, Argentina

E-mail: jbarrera@fisica.udea.edu.co

Received 31 December 2012, accepted for publication 28 February 2013


Published 20 March 2013

Online at stacks.iop.org/JOpt/15/055404

Abstract

As optical systems are diffraction limited, it is not possible to encrypt in a single step texts containing a large amount of characters. We overcome this situation by separately encrypting several characters, along with a multiplexing procedure to obtain an encrypted keyboard. The experimental application is performed in a joint transform correlator architecture and using digital holography. We combine the different characters into a keyboard encrypted with a single phase mask together with a selection-position key that gives the right sequence to recover safe encrypted messages. The multiplexing operation we suggest is advantageous in the sense that the technique enables processing of messages that otherwise the optical system could not process in a single step. We also employ a repositioning technique to prevent both the natural background noise over recovered characters and the possible cross talk. The lack of any single key avoids the correct message recovery. Experimental results are presented to show the feasibility of our proposal, representing an actual application of the optical encrypting protocols.

Keywords: optical encryption, multiplexing

 Online supplementary data available from stacks.iop.org/JOpt/15/055404/mmedia

(Some figures may appear in colour only in the online journal)

1. Introduction

Encrypting optical systems exhibit useful characteristics. High data handling capacity; several degrees of freedom to data encoding (phase, shifting, wavelength, speckle modulation, etc); the combination of a variety of architectures (4f, joint transform correlators, fractional Fourier transforms, fractional nonconventional joint transform correlators, etc); the use of additional encrypting keys to increase the security level are examples to mention [1–5].

Digital simulations and experimental implementations demonstrate the potentials of the techniques. Experimental results are in fact more significant for verifying and asserting realistic constraints [6–9].

On the other hand, multiplexing is the option when multi-users and/or multi-messages are taken into account. In

this framework, proposals rely in applying a basic encoding scheme to every single frame and then multiplexing the entire set of images into a single package. In this way, we achieve a more compact information-carrying unit. However, we have two serious drawbacks: cross talk and background noise, which limit the amount of recorded images and affect their quality in the decoded results. In a multiplexing procedure, each right set of the encrypting optical parameters is able to decrypt each image at a time. In fact, in decryption procedures, the wavefronts convey the information corresponding to the several encrypted images. Therefore, the remaining non-decrypting information contributes as noise [10]. Several attempts have been done in this direction in the conventional multiplexing approach with the unavoidable mentioned constraint [11–13].

The original 4f double random-phase encoding method requires the recording of complex-valued information [14]. It also requires the complex conjugate of the random-phase code to be used in the decryption process.

Narrowing the scope, we find just a small number of experimental results presented for the joint transform correlator (JTC) configuration [15–18]. An advantage of using the JTC encrypting architecture is that the decryption is performed using the same key code, which eliminates the need to produce an exact complex conjugate of the key or of the encrypted information [19]. The JTC is attractive in the sense that it does not require the accurate optical alignment that the 4f architecture does. The image with an input phase code attached is placed side by side with a key code in the JTC input plane. The joint power spectrum (JPS) is recorded as the encrypted data. That is, the encrypted data are recorded as an intensity basis.

We found an experimental alternative based on a JTC architecture to remove the superposition of noise produced by the non-recovered objects from the recovered object, and additionally introduce a fully controlled way of repositioning the decrypted image in the output plane [20, 21].

In this contribution, we present an experimental alternative based on a JTC architecture using two decoding keys, one corresponding to the JTC optical system, and the other corresponding to the order in which the decrypted data must be selected to recover a letter sequence revealing a given message of any length.

With this framework in mind, we propose to extend the procedure to include the case of successive characters that compose a keyboard, leading to its implementation in the JTC architecture. We adopt this experimental protocol to encrypt and to multiplex a set of frames that constitute a message. In our proposal, each input character is displayed as a single frame in a spatial light modulator (SLM). During decryption, the whole data set is simultaneously displayed. To recover the original message of any length, we need the encoding key used to encrypt the keyboard characters and the sequential order in which we choose the characters of the decrypted keyboard. In the following, we describe the encrypting process for a single letter, extending the technique to a message. We also include the theoretical explanation. We present the successful experimental results that include the above potentials besides demonstrating the actual application possibilities.

2. Encryption and decryption using the JTC encrypting architecture and a digital holographic technique

We introduce in this section a practical digital holographic implementation on the JTC architecture [20, 21]. We show the way to filter the unwanted terms, besides repositioning the information contained in the JPS. The steps corresponding to the implementation of the encryption process are successively: (a) storing the JPS of the JTC encrypting architecture input, (b) storing the intensity of the Fourier transform (FT) of the original image multiplied by a random

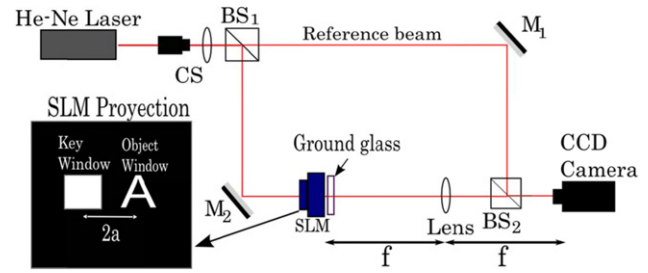


Figure 1. Optical setup (CS: collimation system, BS₁ and BS₂: beam splitters, M₁ and M₂: mirrors, SLM: spatial light modulator, f : focal distance of the lens).

mask, and the intensity of the FT's encrypting key separately to suppress background noise, (c) Fourier transforming, removing the unwanted term and at the same time positioning the desired information in any place in space and back Fourier transforming to get the encrypted information, and (d) the same basic procedure is applied to obtain the information of the decrypting key, but in this case it is necessary to record the hologram of the FT's encrypting key and the intensity of the reference wave. This procedure allows us to separate and identify the different information terms, while enabling us to remove the noise-causing terms and the non-relevant terms. The authorized user recovers the original information employing the encrypted information and the decrypting key [20, 21].

In the JTC encrypting system the input plane contains the information of the object to be encrypted $a_j(x_0, y_0)$ attached to a random-phase mask $r_j(x_0, y_0)$, and another random-phase mask $r(x_0, y_0)$ that acts as the encrypting key. In our experimental implementation, the object and the window that limits the area of the encryption key are projected in a SLM, and the random-phase masks are generated by a ground glass (see figure 1). Therefore, the input plane is obtained when the SLM and the ground glass are in contact,

$$i_0(x_0, y_0) = [a_j(x_0, y_0)r_j(x_0, y_0)] \otimes \delta(x_0 - a, y_0) + r(x_0, y_0) \otimes \delta(x_0 - (-a), y_0) \quad (1)$$

where the symbol \otimes denotes the convolution, $\delta()$ is the Dirac delta function and $2a$ is the distance between the object and the encrypting key.

The experimental setup is a Mach–Zehnder interferometer, where the JTC encrypting system is located in one arm and the other arm provides the reference beam. By blocking the reference beam, the JPS can be registered in the CCD camera,

$$I_j(u, v) = |A_j(u, v)|^2 + A_j^*(u, v)R(u, v)\exp(4\pi iau) + |R(u, v)|^2 + A_j(u, v)R^*(u, v)\exp(-4\pi iau) \quad (2)$$

where $*$ means complex conjugate, $A_j(u, v)$ and $R(u, v)$ are the Fourier transforms of $a_j(x_0, y_0)r_j(x_0, y_0)$ and $r(x_0, y_0)$, respectively. In this case, (x, y) denoted the spatial coordinates, and (u, v) the Fourier domain coordinates. We focus the attention in retaining only the fourth term which

contains the encrypted object information. Therefore, we proceed to cancel the background noise corresponding to the two zero order terms and the filtering of the remaining term. For this purpose, we projected separately in the SLM the object and the window of the encrypting key to register $|R(u, v)|^2$ and $|A_j(u, v)|^2$, respectively. By digitally subtracting from the JPS the DC terms, we get,

$$L_j(u, v) = A_j^*(u, v)R(u, v) \exp(4\pi iau) + A_j(u, v)R^*(u, v) \exp(-4\pi iau). \quad (3)$$

Then, performing a FT operation we get two spatially isolated terms carrying the information of the object convolved with the encoding key,

$$l_j(x', y') = a_j^*(x', y')r_j^*(x', y') \otimes r(-x', -y') \otimes \delta(x' - 2a, y') + a_j(-x', -y')r_j(-x', -y') \otimes r^*(x', y') \otimes \delta(x' + 2a, y'). \quad (4)$$

Next, the first term is removed and the second term is freely positioned in a selected coordinate (x_j, y_j) ,

$$e_j(x', y') = a_j(-x, -y)r_j(-x, -y) \otimes r^*(x, y) \otimes \delta(x - x_j, y - y_j). \quad (5)$$

Finally, a FT allows getting the encrypted information

$$E_j(u, v) = A_j(u, v)R^*(u, v) \exp[2\pi i(x_ju + y_jv)]. \quad (6)$$

Precisely this freedom in choosing the term position enables us to handle the situation where multiple objects are used, and in such a case, this possibility is useful to avoid the spatial overlapping of decoded images.

The next step in the encrypting process is recording the information of the decrypting key. The hologram of the FT of the encrypting key is stored when projecting only the window of the key,

$$Q(u, v) = |W(u, v)|^2 + W^*(u, v)R(u, v) \exp[2\pi iua] + W(u, v)R^*(u, v) \exp[-2\pi iua] + |R(u, v)|^2 \quad (7)$$

here $W(u, v)$ represents the reference plane wave. Again, we want to retain only the relevant information, this time represented by the second term of the hologram. Now we follow a similar procedure as that performed from equation (2) to obtain equation (6). Therefore, $|W(u, v)|^2$ and $|R(u, v)|^2$ are registered and then subtracted from equation (7). Then, a FT operation is performed on the remaining two terms, eliminating one of the diffracted terms and the remaining one is positioned at coordinates $(x', y') = (0, 0)$. Finally, a FT gives the decrypting key,

$$F(u, v) = R(u, v). \quad (8)$$

In this context, the decrypting key is the FT of the encrypting key. At this point, we are able to recover the original information. Multiplying the encrypted information (equation (6)) by the decrypting key (equation (8)), and after an inverse FT operation we get,

$$kb(x, y) = a_j(x, y)r_j(x, y) \otimes \delta(x - x_j, y - y_j). \quad (9)$$

3. Multiplexing of the encrypted characters

Optical systems, due to their physical dimensions and characteristics, impose a limit, not allowing processing any type of input information. Certainly, we could improve this limit, for example, by enlarging the optical components using our super-resolution techniques, but in any case a limit always exists. In the case of text encryption, as the number of characters rise, so does the number of frequencies the system should process, reaching a value difficult to handle adequately. Besides, we also have to add the noise of the inherent speckle patterns. If we intend to encrypt a complete book dividing the information into portions that the optical system can process, we have a huge amount of information to send, including the spending of energy and the consumption of storing space. When thinking of the simplest approach to accomplish a writing task, the first solution is to have a keyboard. In this way, we have every single character of a given language, plus additional characters.

Multiplexing is the practical tool to process a whole text neither altering the optical setup nor introducing other elements, becoming a realistic solution to this problem. Therefore, to obtain the encrypted keyboard, the n characters that constitute the keyboard are separately encrypted following the procedure describe in section 2. Then, the encrypted characters are finally multiplexed,

$$N(u, v) = \sum_{j=1}^n A_j(u, v)R^*(u, v) \exp[2\pi i(x_ju + y_jv)]. \quad (10)$$

Equation (10) represents the encrypted keyboard. At this point, it is important to highlight that in case an unauthorized person intercepts the encrypted keyboard without accessing the security key, it is impossible for him to recover the keyboard.

In the recovering process, the multiplexing (equation (10)) is multiplied by the decrypting key (equation (8)). Afterwards, performing a FT, the n characters of the keyboard are recovered in the same plane without superposing,

$$n(x, y) = \sum_{j=1}^n a_j(x, y)r_j(x, y) \otimes \delta(x - x_j, y - y_j). \quad (11)$$

In this way, the position of each decrypted character in the recovered keyboard is imposed during the encryption process, and therefore the keyboard configuration can be controlled. We want to remark that the message needs two keys to be revealed: the right optical key decodes the keyboard and the selection-position key shows the message itself. The selection-position key provides the information about the order to adequately select the keyboard data, and the way to position them to disclose the final text. Therefore, the use of two validating keys reinforces the entire process security.

Among the techniques suggested in the literature for multiplexing making it possible to increase the amount of encoding inputs significantly, we focus on the approaches proposed in [22–24] for comparison purposes. In [22] the authors call the attention to several multiplexing methods. However, although these approaches are elegant, in some of

them there are overlapping among the recovered information and the non-decrypted data, or include restrictions regarding the complexity of the optical setup or accurate positioning to name a few.

Particularly, the method reported in [23] shows a contribution specifically designed for correlation studies in which the stored reference image is phase encrypted prior to applying the JTC. The encryption disperses all the trivial correlation peaks in the correlator output. Unlike our proposal designed for multiplexing encrypted images, the number of simultaneous correlations is proportional to the SLM size and limited by the correlation energy in the correlation output. They present computer simulations and propose an experimental setup with two SLM devices, instead of one, as in our case.

In [24] a method of wavelength multiplexing, based on a modified Gerchberg–Saxton algorithm and a cascaded phase modulation scheme in the Fresnel transform domain to reduce the cross talk in the multiple-image-encryption framework, is presented. Actually it is a digital implementation, where the maximum limit of multiplexing the encrypted images is dependent on the acceptable maximum cross talk or the required minimum correlation coefficient in real applications. In our case, our performed experiments show that cross talk is totally eliminated without any length restrictions.

4. Experimental results

We use a He–Ne laser, a lens of 200 mm focal length, and a PULNIX TM6703 CCD camera with 640×480 pixels and $9 \mu\text{m} \times 9 \mu\text{m}$ pixel area. The key window and each object window are projected in a Holoeye LC2002 SLM. A ground glass placed behind the SLM generates the two random masks needed for the JTC architecture. The object window size is $3.2 \text{ mm} \times 3.2 \text{ mm}$, the area of the key window is $1.3 \text{ mm} \times 1.3 \text{ mm}$, and the distance between windows is 3.84 mm (see figure 1).

As mentioned earlier, the optical system imposes limitations to the availability of frequency content in the input plane due to the SLM display and to the pixel size of the CCD, to name a few. Therefore, in order to fully process the keyboard ensuring the proper characters recognition, we encrypt each character separately. In this way, under our particular experimental conditions we are not able to unambiguously recover more than one character at a time.

In figure 2(a) we present the decoded keyboard where the characters do not necessarily follow any classical distribution (for example qwerty). The text assembling needs the right selection-position key (see figure 2(b) and media 1 available at stacks.iop.org/JOpt/15/055404/mmedia). Precisely this key determines the final length for the text. In our case, we show a movie with the sequential reconstruction of a complete sentence to demonstrate the feasibility of our opto-digital protocol. We remark through this example the importance of reconstructing with fidelity each character of the keyboard otherwise any blurry or undefined character will affect the text understanding.

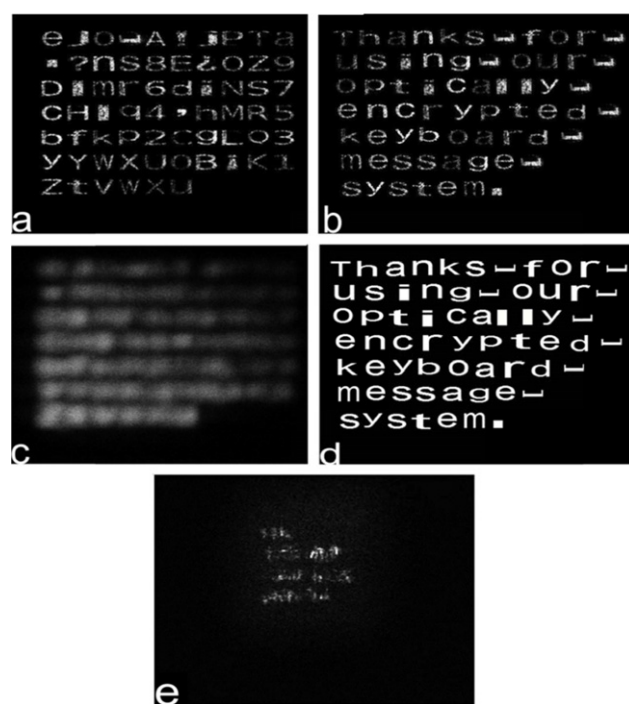


Figure 2. (a) Decryption of the keyboard using the right optical key, (b) actual reconstruction of the text using the selection-position key (see media 1 available at stacks.iop.org/JOpt/15/055404/mmedia), (c) decryption of the key board with a different key. The projected and processed message in a single step, and the corresponding decrypted message using the right decrypting key are shown in (d) and (e) respectively.

As expected in the implemented optical encrypting protocol, the recovering of the keyboard is possible when the right encrypting key is employed. Therefore, the use of another key produces a noise result (figure 2(c)). The applicability and potential of our proposed protocol is evident from the result presented in figures 2(d) and (e), where the entire message is projected in the SLM (figure 2(d)) and then processed (figure 2(e)) as described in section 2. As mentioned above, the limitations in the resolution of our optical system does not allow the right recovering of the entire message.

We can mention several advantages present in our proposal. When encrypting separately each letter, instead of encoding the whole keyboard, we are ensuring the clear resolving of each character (figure 2(b)), a situation not guaranteed when the whole keyboard is presented as unique input in the SLM display (figure (e)). We can safely handle a text of unlimited length, with double key security. We can affirm that multiplexing allows the encoding system flexible and practical, in a way that it is possible to encrypt from a simple code to a length text. Security is increased because we are using an optical key and a selection-position key. Once we send the multiplexed keyboard and the optical key we are saving in data transfer operation, as for new text we only need to send the corresponding selection-position key. The advantages of an opto-digital procedure (optical processing, physical key, versatility) allow the user to have the security of an optical system without needing laboratory equipment. The

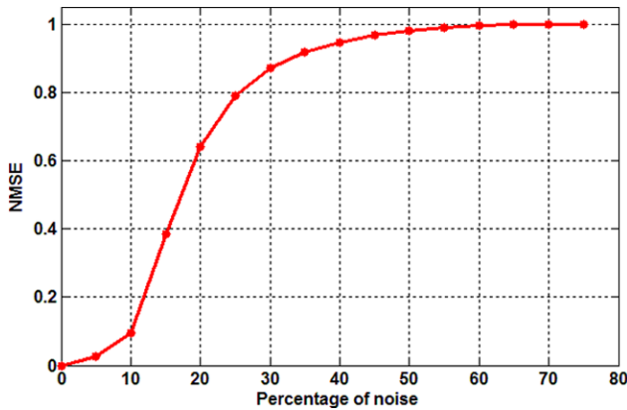


Figure 3. Curve shows the influence of noise over multiplexing through the NMSE.

encrypted keyboard and the optical key can be purchased from a technical laboratory, and then be employed in a computer. Moreover, this procedure can be extended to include different messages in a multi-user environment.

In order to evaluate the performance of the proposed scheme, we calculate the normalized mean square error (NMSE) for the case when adding random 8 bit noise to the multiplexing of the encrypted characters (equation (10)). The NMSE between the recovered message $m(p, q)$ (figure 2(b)) (without adding the noise to the multiplexing) and the retrieved message $m'(p, q)$ (when there are different percentages of noise over the multiplexing) can be defined as,

$$\text{NMSE} = \frac{\sum_{p,q}^N |m(p, q) - m'(p, q)|^2}{\sum_{p,q}^N |m(p, q) - m_w(p, q)|^2} \quad (12)$$

where (p, q) are the pixels coordinates, $N \times N$ is the number of pixels of the recovered message, and $m_w(p, q)$ is the worst expected case.

Figure 3 shows the comparison between the retrieved message and the successive recovered messages when noise is added. Taking into account the behaviour of the NMSE curve (figure 3), as we increase the noise it results evident the degradation in the pertinent information as expected. If the noise affects less than the 50% of the encrypted image, we can still reasonably recognize the message. When this range is extended from 55% up to 60%, image recovery diminishes notably. Increasing over 65% we are not able to recover the message.

5. Conclusions

We have proposed a new JTC encrypting protocol to be used with text of unlimited length. Basically it is a multiplexing procedure leading to encrypt a keyboard, thus allowing its use as a typewriter machine. This is an experimental technique using a JTC architecture as scheme and digital holography as the working tool. The message is arranged thanks to a selection-position key, also acting as a security reinforcing key. A SLM serves as input information display. A convenient repositioning method helps in avoiding the cross

talk and noise superposition, common to the multiplexing technologies.

This new technique leads to the possibility of conveying a large amount of information relative to several single texts sequentially sent. In this sense we are reducing the size with a single database (keyboard). Because of the advantages of an easily handled multiplexing technique and a compact experimental configuration, it will be attractive for applications in many fields, especially in massive data transmitting systems. The experiments are performed with consistent results.

Acknowledgments

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

References

- [1] Millán M S and Pérez-Cabré E 2011 Optical data encryption *Optical and Digital Image Processing: Fundamentals and Applications* ed G Cristóbal, P Schelkens and H Thienpont (Weinheim: Wiley-VCH Verlag) pp 739–67
- [2] Situ G and Zhang J 2004 Double random-phase encoding in the Fresnel domain *Opt. Lett.* **29** 1584–6
- [3] Unnikrishnan G, Joseph J and Singh K 2000 Optical encryption by double-random phase encoding in the fractional Fourier domain *Opt. Lett.* **25** 887–9
- [4] Amaya D, Tebaldi M, Torroba R and Bolognini N 2009 Wavelength multiplexing encryption using joint transform correlator architecture *Appl. Opt.* **48** 2099–104
- [5] Rajput S K and Nishchal N K 2012 Image encryption and authentication verification using fractional nonconventional joint transform correlator *Opt. Lasers Eng.* **50** 1474–83
- [6] Matoba O and Javidi B 2004 Secure holographic memory by double-random polarization encryption *Appl. Opt.* **43** 2915–9
- [7] Barrera J F, Henao R, Tebaldi M, Bolognini N and Torroba R 2006 Multiplexing encryption–decryption via lateral shifting of a random phase mask *Opt. Commun.* **259** 532–6
- [8] La Mela C and Iemmi C 2006 Optical encryption using phase-shifting interferometry in a joint transform correlator *Opt. Lett.* **31** 2562–4
- [9] Singh M, Kumar A and Singh K 2008 Secure optical system that uses fully phase-based encryption and lithium niobate crystal as phase contrast filter for decryption *Opt. Laser Technol.* **40** 619–24
- [10] Situ G and Zhang J 2005 Multiple-image encryption by wavelength multiplexing *Opt. Lett.* **30** 1306–8
- [11] Barrera J F, Henao R, Tebaldi M, Bolognini N and Torroba R 2006 Multiplexing encrypted data by using polarized light *Opt. Commun.* **260** 109–12
- [12] Nishchal N K and Naughton T J 2011 Flexible optical encryption with multiple users and multiple security levels *Opt. Commun.* **284** 735–9
- [13] Zhao H, Liu J, Jia J, Zhu N, Xie J and Wang Y 2013 Multiple-image encryption based on position multiplexing of Fresnel phase *Opt. Commun.* **286** 85–90

- [14] Javidi B, Zhang G and Li J 1996 Experimental demonstration of the random phase encoding technique for image encryption and security verification *Opt. Eng.* **35** 2506–12
- [15] Nomura T and Javidi B 2000 Optical encryption system with a binary key code *Appl. Opt.* **39** 4783–7
- [16] Nomura T, Mikan S, Morimoto Y and Javidi B 2003 Secure optical data storage with random phase key codes by use of a configuration of a joint transform correlator *Appl. Opt.* **42** 1508–14
- [17] Barrera J F, Tebaldi M, Amaya D, Furlan W D, Monsoriu J, Bolognini N and Torroba R 2012 Multiplexing of encrypted data using fractal masks *Opt. Lett.* **37** 2895–7
- [18] Amaya D, Tebaldi M, Torroba R and Bolognini N 2008 Multichanneled encryption via a joint transform correlator architecture *Appl. Opt.* **47** 5903–7
- [19] Nomura T and Javidi B 2000 Optical encryption using a joint transform correlator architecture *Opt. Eng.* **39** 2031–45
- [20] Rueda E, Ríos C, Barrera J F, Henao R and Torroba R 2011 Experimental multiplexing approach via key code rotations under a joint transform correlator scheme *Opt. Commun.* **284** 2500–4
- [21] Rueda E, Ríos C, Barrera J F and Torroba R 2012 Master key generation to avoid the use of an external reference wave in an experimental JTC encrypting architecture *Appl. Opt.* **51** 1822–7
- [22] Alfalou A and Brosseau C 2009 Optical image compression and encryption methods *Adv. Opt. Photon.* **1** 589–636
- [23] Alsamman A 2010 Spatially efficient reference phase-encrypted joint transform correlator *Appl. Opt.* **49** B104–10
- [24] Chang H T, Hwang H E, Lee C L and Lee M T 2011 Wavelength multiplexing multiple-image encryption using cascaded phase-only masks in the Fresnel transform domain *Appl. Opt.* **50** 710–6