Experimental protocol for packaging and encrypting multiple data

IOP PUBLISHING JOURNAL OF OPTICS

J. Opt. **15** (2013) 055406 (6pp) doi:10.1088/2040-8978/15/5/055406

Experimental protocol for packaging and encrypting multiple data

John Fredy Barrera[1], **Sorayda Trejos**[1], **Myrian Tebaldi**[2] **and Roberto Torroba**[2]

[1] Grupo de Óptica y 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, PO Box 3, C.P 1897, La Plata, Argentina

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

Received 23 November 2012, accepted for publication 18 March 2013
Published 11 April 2013
Online at stacks.iop.org/JOpt/15/055406

Abstract

We present a novel single optical packaging and encryption (SOPE) procedure for multiple inputs. This procedure is based on a merging of a 2*f* scheme with a digital holographic technique to achieve efficient handling of multiple data. Through the 2*f* system with a random phase mask attached in its input plane, and the holographic technique, we obtain each processed input. *A posteriori* filtering and repositioning protocol on each hologram followed by an addition of all processed data, allows storing these data to form a single package. The final package is digitally multiplied by a second random phase mask acting as an encryption mask. In this way, the final user receives only one encrypted information unit and a single key, instead of a conventional multiple-image collecting method and several keys. Processing of individual images is cast into an optimization problem. The proposed optimization aims to simplify the handling and recovery of images while packing all of them into a single unit. The decoding process does not have the usual cross-talk or noise problems involved in other methods, as filtering and repositioning precedes the encryption step. All data are recovered in just one step at the same time by applying a simple Fourier transform operation and the decoding key. The proposed protocol takes advantage of optical processing and the versatility of the digital format. Experiments have been conducted using a Mach–Zehnder interferometer. An application is subsequently demonstrated to illustrate the feasibility of the SOPE procedure.

Keywords: optical packaging, encryption, image processing

1. Introduction

Optics-based methods take advantage of processing two-dimensional (2D) data in parallel and have been studied in the context of optical processing. However, in the past decade, optical processing systems, in particular optical encryption techniques, have been evolving into multiple-image encoding, which attracts much attention nowadays owing to economic memory occupation and efficient transmission via a network. Compared with single-image encoding [1], multiple-image encoding encodes several images into a single file [2–7].

On the other hand, in developing these optical procedures, we face some additional problems: image overlap when reconstructing, noise superposition from residual non-decoded images, etc [8–10].

We find an example in wavelength multiplexing in the context of multiple-image encoding [8]. The ultimate processed image was synthesized by superimposing individual encoded images together. This strategy was time consuming and sensitive to the cross-talk effect. Another example is multiple-image encoding based on a key mask shift, proposed to store images in either the Fourier or the fractional Fourier domains. The technique is good at multiple

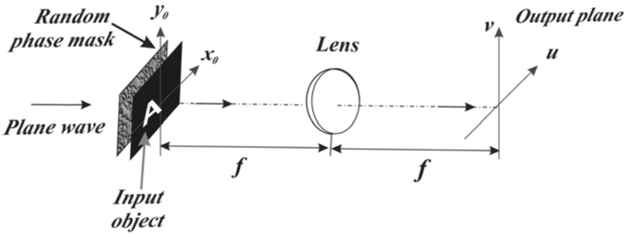

Figure 1. Optical $2fr$ processor (f: focal length of the lens).

images, but high-frequency contents of the images have to be discarded when increasing the number of data to be recorded.

Holography has also become involved in image packing because of the inherent capability of recording images into a hologram. A hologram can preserve the image content in its complex patterns, and the storing procedure can be performed by real optical systems. However, the amount of information contained in a hologram is greater than the information contained in the object itself [11].

However, investigations of packed holograms and encryption methods using our proposed protocol have not, to the best of our knowledge, been explored. In this paper, we believe we present the first work dealing with a single optical packaging and subsequent encryption technique with the SOPE procedure.

In order to achieve an efficient SOPE, we utilize a Mach–Zehnder architecture with an optical $2f$ processor in one arm and the other as a corresponding reference beam to record each processed image, then after recording we introduce the digital protocol to filter and reposition the data. Once data is arranged in a single unit, the encryption is achieved by digitally multiplying the unit with a random phase mask. We want to emphasize that the new scheme is neither a $2f$ nor a JTC architecture, although it uses two phase masks to complete the encryption process.

The development of a new generation of optical components and the constant progress in optical processing has made the realization of a new type of optical information transport possible, by basing it on the concept of digital holography in coordination with the packaging of multi-images and encryption. In this paper, such a new type of optical information transport and handling is presented, analyzed and implemented. In the following sections we will show its potential and their level of applicability. The new concept confronts the challenge of growing network capacity while cutting costs and allowing an efficient combination of digital optical and single-packaging integration benefits.

2. Description of the process for a single input

In figure 1, we depict the optical scheme we use to introduce the novel procedure presented in the paper. A simple optical processor, we name a $2fr$ system, is used. The term $2fr$ denotes a single lens of focal length f and a random phase mask r attached to every input object. It represents an inexpensive compact system (a lens and a mask). The lens provides the Fourier spectrum of the input object. The Fourier spectrum of an object facilitates its optical processing. The mask serves to spread the information in the output plane of the lens, which is essential to our purpose.

This $2fr$ optical system will be used to process multiple data. We now implement a procedure to record the optical field at the output plane for each input, then process this information and finally add all of them in a single package. The package is digitally encrypted by multiplying it with another random phase mask, resulting in an encrypted unit ready to be transmitted and received via Internet or an Internal Network.

As commented above, we need a holographic setup [12, 13], for this reason we introduce the optical processor in the Mach–Zehnder architecture shown in figure 2.

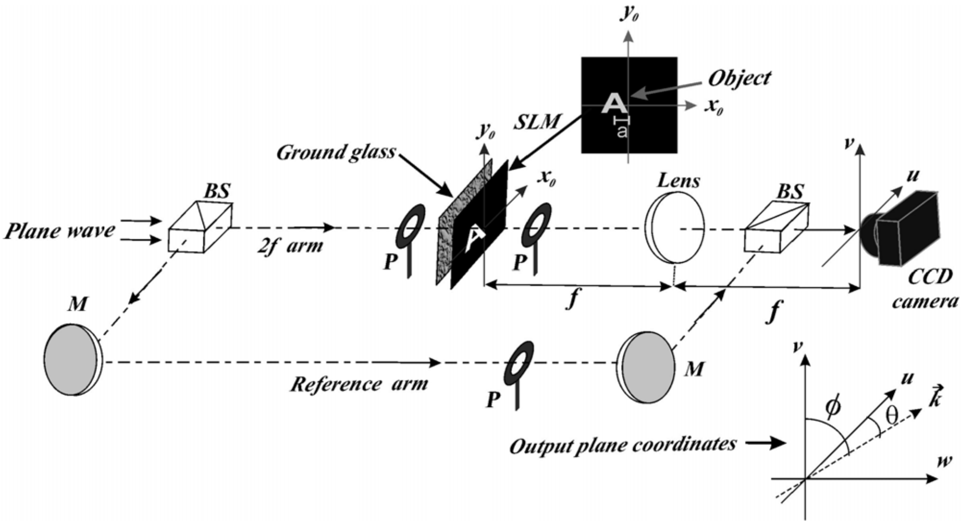

Figure 2. Mach–Zehnder interferometer for the optical processing (*BS*: beam splitter, *M*: mirror, *SLM*: spatial light modulator, $\vec{k}$: propagation vector, *P*: polarizer).

Accordingly, for the experimental realization, each input object is optically processed by employing the $2fr$ optical system. Then, the Mach–Zehnder interferometer allows recording of the hologram of the optically processed data (see figure 2) by providing the reference beam.

The input plane of the optical processor is

$$d_l(x_0, y_0) = [o_l(x_0, y_0)r(x_0, y_0)] \otimes \delta(x_0 - (-a), y_0) \quad (1)$$

where $o_l(x_0, y_0)$ is the object to be optically processed, $r(x_0, y_0)$ is the random phase mask, $\otimes$ means convolution, and $|a|$ is the distance between the object and the optical axis in the input plane. Here, the object is not centered on the optical axis, as it will allow the filtering of unwanted terms. If we illuminate this input with a monochromatic plane wave, we get at the output plane the processed data,

$$D_l(u, v) = \mathrm{FT}\{[o_l(x_0, y_0)r(x_0, y_0)] \otimes \delta(x_0 - (-a), y_0)\}. \quad (2)$$

FT{ } means the Fourier transform (FT) operation. In the experimental setup, the input object $o_l(x_0, y_0)$ is projected in a spatial light modulator (SLM) and a ground glass placed behind the SLM represents the random phase mask $r(x_0, y_0)$. The SLM and the random mask are placed in contact to generate the input plane. At this step, we can see from (2) that the product of the object with the random phase mask will produce after a FT, a convolution, thus resulting in the distribution of the FT of the object in a wider area in the output plane.

On the other hand, through the beam splitter a reference plane wave arrives at the same output plane. Then, the interferogram recorded by the CCD camera is

$$I_l(u, v) = |D_l(u, v)|^2 + |P(u, v)|^2 + D_l^*(u, v)P(u, v) \times \exp(-2\pi \mathrm{i} au) + D_l(u, v)P^*(u, v)\exp(2\pi \mathrm{i} au) \quad (3)$$

where * means complex conjugate, $P(u, v) = \exp[-2\pi \mathrm{i}(\alpha u + \beta v)]$ represents the reference plane wave with $\alpha = \cos\theta/\lambda$ and $\beta = \cos\phi/\lambda$, $\cos\theta$ and $\cos\phi$ are the directional cosines, and λ is the wavelength (see figure 2).

We want to retain only the relevant information contained in the interferogram. Therefore, we register separately the terms $|P(u, v)|^2$ and $|D_l(u, v)|^2$ by blocking the $2f$ arm and the reference arm, respectively. The procedure up to this point is experimentally developed, and from now on we perform digital operations. Subtracting these two last terms from (3) we obtain

$$Q_l(u, v) = D_l^*(u, v)P(u, v)\exp(-2\pi \mathrm{i} au) + D_l(u, v)P^*(u, v)\exp(2\pi \mathrm{i} au). \quad (4)$$

From (4) we want to retain only one term. Then, we proceed to perform the FT of (4) to get two spatially separated terms

$$n_l(x', y') = d_l^*(x', y') \otimes \delta(x' + \alpha\lambda f, y' + \beta\lambda f) \otimes \delta(x' + a, y') + d_l(x', y') \otimes \delta(x' - \alpha\lambda f, y' - \beta\lambda f) \otimes \delta(x' - a, y'). \quad (5)$$

The separation between terms is proportional to $|a|$, which in turn is controlled during the projection of the input objects on the SLM. It is important to mention that the value of $|a|$ must be carefully selected to prevent any kind of superposition between these two terms. Although it may also depend on the orientation of the reference wave, we kept it constant throughout the process.

Then, the first term of (5) is removed by filtering and the remaining term is repositioned around a desired coordinate point (x_l, y_l).

$$g_l(x, y) = d_l(x, y) \otimes \delta(x - x_l, y - y_l). \quad (6)$$

We have to remember that we need to obtain the FT of the input plane information $d_l(x_0, y_0)$ (see (1)), therefore we apply an inverse FT to (6),

$$F_l(u, v) = D_l(u, v)\exp[2\pi \mathrm{i}(x_l u + y_l v)]. \quad (7)$$

This last equation represents the opto-digital processed data. Although hologram data are not only complex but also occupy much more memory than does the original image, as shown by (3), by retaining the term of (7) we are saving storage capabilities while retaining the pertinent information. The positioning at coordinates (x_l, y_l) allows the recovered data to be located in any desired position in the output plane, as we want to process multiple data and to recover it without superposition in the output plane.

3. Packaging, encrypting and recovering the processed data

In general, when implementing an experimental technique one finds several constraints related to technical procedures. Among these limitations we have the resolution of the optical system, the limited size and resolution of the SLM display, the recording media, mechanical instruments, etc. All these constraints should be taken into account when applying any experimental procedure. In our protocol, we propose a solution to multiple data handling, when all data cannot simultaneously be displayed on the SLM. In addition, the optical system does not necessarily resolve all the set, but rather single inputs. Moreover, the CCD device can properly record each processed input.

Accordingly, when processing multiple objects, instead of processing all the data in one step, we propose to separately process each object. When applying the procedure explained in section 2 on each object, a set of individually processed objects is obtained. Then, a packaging operation is applied to generate a single information unit. If n represents the number of processed objects (7), then the package is

$$U(u, v) = \sum_{l=1}^{n} D_l(u, v)\exp[2\pi \mathrm{i}(x_l u + y_l v)]. \quad (8)$$

Note that, during the processing of each data, the coordinates (x_l, y_l) are chosen so as to get recovered objects in separate locations in the exit plane. The final step is to encrypt the package using another random phase mask $R_1(u, v)$, which acts as the encryption key. Accordingly, by a digital multiplication of $U(u, v)$ and $R_1(u, v)$ we get

$$E(u, v) = \left\{\sum_{l=1}^{n} D_l(u, v)\exp[2\pi \mathrm{i}(x_l u + y_l v)]\right\} R_1(u, v). \quad (9)$$

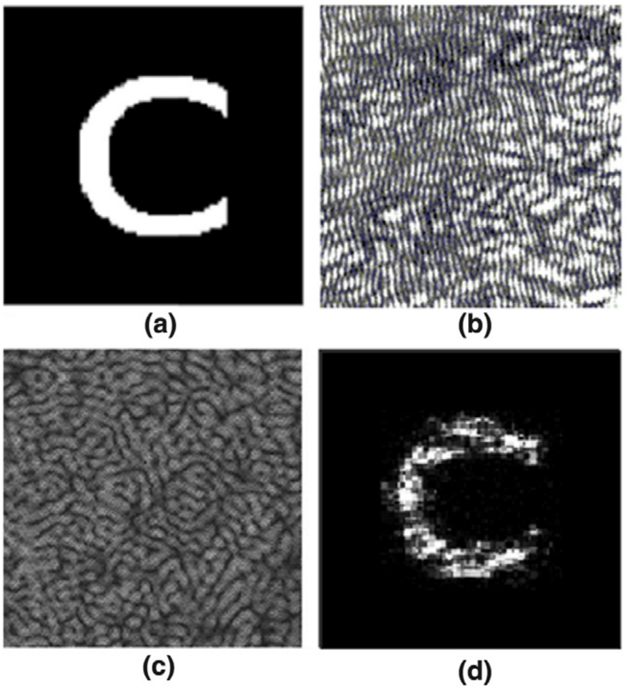

Figure 3. (a) Input object, (b) hologram of the optically processed object, (c) final-processed data (before encryption), and (d) recovered object (with the correct key).

This encrypted package and the complex conjugate of the digital encoding key can be sent to users in remote locations. The end user performs only a multiplication by the conjugate of the encryption mask and a subsequent FT operation in recovering the hidden data in the corresponding chosen positions. These positions were fixed when constructing the package,

$$u(x, y) = \sum_{l=1}^{n} o_l(x, y) r(x, y) \otimes \delta(x - x_l, y - y_l). \qquad (10)$$

The data are displayed in one step, in the same plane, and at the same time. As $r(x, y)$ is a random phase mask, we record the intensity of $u(x, y)$ to get the intensity of the input objects $|o_l(x, y)|^2$. Note that our experimental technique does not imply setup alterations.

4. Experimental results

In the experimental arrangement, we use a solid-state laser operating at wavelength 532 nm with 50 mW output power, a lens of 200 mm focal length, and a CCD camera with 640 × 480 pixels and 9.9 μm × 9.9 μm pixel area. A ground glass placed behind the SLM provides the random mask. The objects are projected in a Holoeye LC2002 SLM working in amplitude mode [14–17], the projected object size is 3.2 mm× 3.2 mm and the distance between the object and optical axis in the input plane $|a|$ is 1.4 mm.

The entire protocol for one object is presented in figure 3. The experimental station of the protocol consists in projecting at the SLM the input object (figure 3(a)) and registering the hologram of the optically processed object in the CCD camera (figure 3(b)). The digital step consists of filtering the unwanted terms and positioning the desired information (figure 3(c)). After the experimental and the digital steps, we obtain the processed object ready to be encrypted with the encoding mask, as described above. In order to recover the original object, it is necessary to cancel the effect of the encryption key and perform a FT operation (figure 3(d)).

Figure 4(a) shows 100 characters used as the input data of the optical processor. The input data is processed as a single object, following the procedure described above. In this experimental demonstration, the input data is projected on the available area of the SLM (480 × 480 pixels) and the recorded data has 640 × 480 pixels. After the correct encryption and decryption stages, the recovered data (figure 4(b)) does not have a good resemblance to the original input (figure 4(a)). We should mention that increasing the number of individual objects in the single input frame will result in a greater loss and degradation of information. The explanation for this issue is not the proposed protocol, but rather the optical resolution of the setup. We have to remember that optical resolution

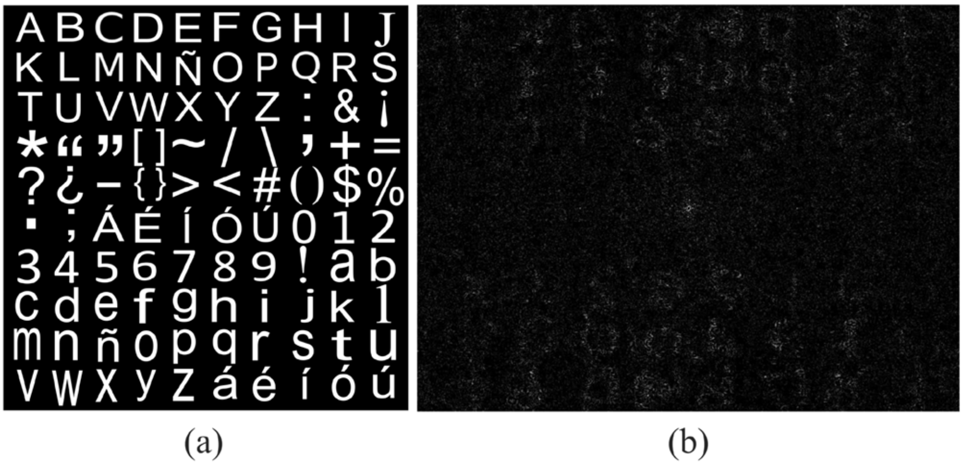

Figure 4. (a) Input data and (b) recovered data after processing.

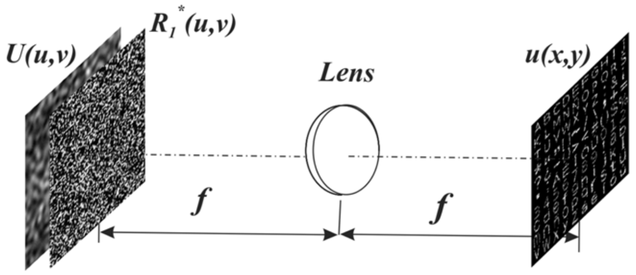

Figure 5. System for decrypting the package.

describes the ability of an imaging system to resolve details in the object that is being imaged. An imaging system may have many individual components, including lenses and recording and display components. Each of these contributes to the optical resolution of the system, as will the environment in which the imaging is done. In this contribution we intend to propose and to implement a procedure that allows the correct processing of all the characters of the input data by means of a multiplexing technique.

A major point to recall when handling an image containing multiple data is that it cannot be displayed and/or processed as a single input, mainly due to practical resolution issues imposed by the optical system. If the image has to be subdivided and introduced piecewise, or we have several input images that need to be introduced one by one to overcome the resolution problem, our protocol represents a practical solution regarding the packaging and posterior encryption of multiple data.

Therefore, instead of processing all the characters as a single input, each character is separately processed optically and digitally. Then, all the processed characters are multiplexed to obtain the package. Finally, in the last step, the package is encrypted. As example, we process 100 characters. Applying the recovery procedure, we obtain all the characters as a single recovered data in the output plane depicted in figure 5, where we show the scheme the final user applies to decode and recover the characters without any kind of superposition. In figure 6(a) we show the actual image presenting 100 reconstructed characters, while figure 6(b) shows the result using an incorrect decryption mask. It is important to highlight that the procedure is efficient for the final user in the sense that we only need to multiply the encrypted data and the recovery mask, followed by a single FT operation.

From equation (5), we distinguish two terms, whose information is contained in a 640 × 480-pixel matrix. Precisely, this size corresponds to the CCD sensor. According to the procedure detailed above, we seek a non-overlapping situation among the reconstructed objects. Therefore, the chosen positioning coordinate by the remaining term (equation (6)), and subsequently the size of the containing matrix, will depend on the number of input objects and their respective sizes. In our experimental example the input objects are 100 × 100 pixels in size on the SLM, and accordingly the recovery plane (figure 6(a)) has 1000 × 1000 pixels. Therefore, under our protocol, as the number of input objects increases, the dimension of the recovery plane increases as well, unless a scaling is applied. When comparing the protocol using a single input containing all characters (figure 4(b)) with our packing protocol (figure 6(a)), it is evident that our proposal allows the processing of several input data in a secure way ensuring an accurate recovery.

Also, the benefits are clear when comparing our proposed protocol with the 4f and JTC encryption proposals. In the first place, in our protocol we first pack the data, then we encrypt the package in a single step, unlike previous implementations where each input was separately encrypted and thereafter the multiplexing was generated. There the total procedure presented several restrictions. In comparison with the 4f architecture, we avoid the use of two lenses, thus making our setup more compact, both for the multiplexing and the

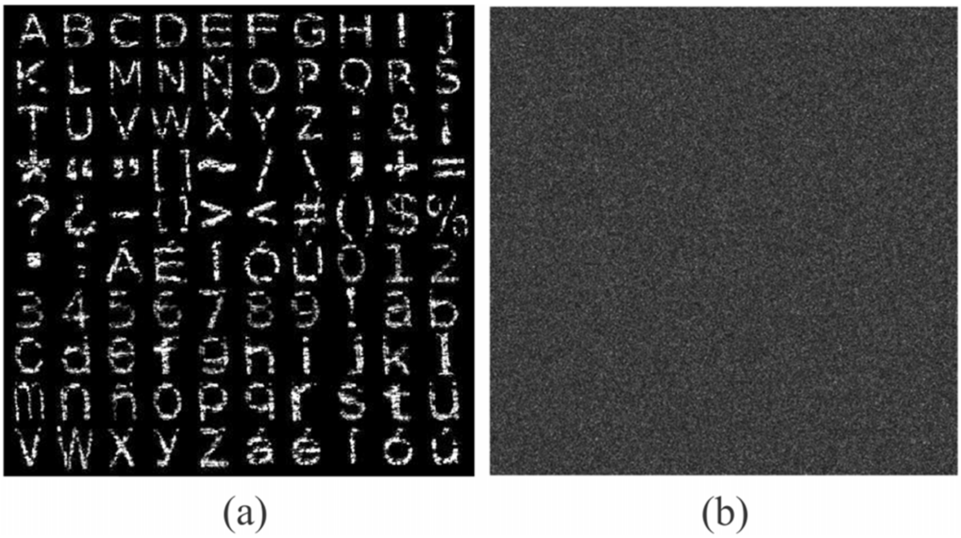

Figure 6. One hundred recovered objects using (a) the correct encryption key, and (b) an incorrect decryption key.

encryption as well as for data recovery. Regarding the JTC scheme, the input plane in our case contains only the object, implying simpler data collection, avoiding recording of the encryption key hologram, and also avoiding recording the joint power spectra between the key and each input object. Also we have no restrictions arising from the resolution limit imposed by windows separation in the JTC arrangement. Therefore, from these comparisons we say our protocol is more compact and more flexible.

5. Conclusions

We present a novel opto-digital procedure named SOPE. The procedure is based on an optical architecture defined as $2fr$, for a single lens of focal length f and a random phase mask r at the input object plane, together with digital filtering, positioning and encryption. This procedure allows the packaging of multiple entries in a single unit without introducing image superposition or cross-talk. Moreover, we use a simple encryption operation, namely digital multiplication of the package by a random phase mask. The main tools are digital holography and numerical manipulation to locate appropriately each processed object in a single package. The final user decodes the entire set at the same time and in a simple way.

It is worth mentioning three distinct advantages: (a) the $2fr$ optical processor is compact, in the sense that it employs a lens and a phase mask; (b) the use of a digital phase mask during encryption facilitates access to its conjugate; and (c) the SOPE procedure does not involve mechanical movements or setup alterations.

As usual in the different architectures and protocols employed to encrypt single or multiple data, we hope that in future contributions the degrees of freedom that optical processing offers may act as extra keys to reinforce the security of our proposal.

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] Matoba O, Nomura T, Pérez-Cabré E, Millán M S and Javidi B 2009 Optical techniques for information security *Proc. IEEE* **97** 1128–48

[2] Matoba O and Javidi B 1999 Encrypted optical memory system using three-dimensional keys in the Fresnel domain *Opt. Lett.* **24** 762–4

[3] Matoba O and Javidi B 1999 Encrypted optical storage with angular multiplexing *Appl. Opt.* **38** 7288–93

[4] 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

[5] Alfalou A and Brosseau C 2009 Optical image compression and encryption methods *Adv. Opt. Photon.* **1** 589–636

[6] Singh M, Kumar A and Singh K 2009 Securing multiplexed information by in-plane rotation of random phase diffusers constituting a sandwich diffuser placed in the Fourier plane *Opt. Laser Technol.* **41** 32–41

[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] Situ G and Zhang J 2005 Multiple-image encryption by wavelength multiplexing *Opt. Lett.* **30** 1306–8

[9] Amaya D, Tebaldi M, Torroba R and Bolognini N 2008 Multichanneled puzzle-like encryption *Opt. Commun.* **281** 3434–9

[10] Henao R, Rueda E, Barrera J F and Torroba R 2010 Noise-free recovery of optodigital encrypted and multiplexed images *Opt. Lett.* **35** 333–5

[11] Di H, Zheng K, Zhang X, Lam E Y, Kim T, Seok Y, Poon T C and Zhou C 2012 Multiple-image encryption by compressive holography *Appl. Opt.* **51** 1000–9

[12] Barrera J F, Rueda E, Ríos C, Tebaldi M, Bolognini N and Torroba R 2011 Experimental opto-digital synthesis of encrypted sub-samples of an image to improve its decoded quality *Opt. Commun.* **284** 4350–5

[13] Rueda E, Ríos C, Barrera J F, Henao R and Torroba R 2011 Experimental multiplexing approach via code key rotations under a joint transform correlator scheme *Opt. Commun.* **284** 2500–4

[14] Soutar C and Lu K 1994 Determination of the physical properties of an arbitrary twisted-nematic liquid crystal cell *Opt. Eng.* **33** 2704–12

[15] Davis J, Allison D, D'Nelly K, Wilson M and Moreno I 1999 Ambiguities in measuring the physical parameters for twisted-nematic liquid crystal spatial light modulators *Opt. Eng.* **38** 705–9

[16] Marquez A, Iemmi C, Moreno I, Davis J, Campos J and Izuel M 2001 Quantitative prediction of the modulation behavior of twisted nematic liquid crystal displays based on a simple physical model *Opt. Eng.* **40** 2558–64

[17] Kim H and Lee Y 2005 Unique measurement of the parameters of a twisted-nematic liquid-crystal display *Appl. Opt.* **44** 1642–9