Subsampling technique to enhance the decoded output of JTC encrypting system

John Fredy Barrera[a,*], Edgar Rueda[a], Carlos Ríos[a], Myrian Tebladi[b], Nestor Bolognini[b,c], Roberto Torroba[b]

[a] *Grupo de Óptica y Fotónica, Instituto de Física, Universidad de Antioquia, A.A 1226, Medellín, Colombia.*
[b] *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*
[c] *Facultad de Ciencias Exactas, Universidad Nacional de La Plata*

ABSTRACT

Optical systems have physical restrictions that impose limits in the finest spatial feature that can be processed. In this work we combine a subsampling procedure with a multiplexing technique to overtake the limit on the information that is processed in a JTC encryption system. In the process the object is divided in subsamples and each subsample is encrypted separately. Then the encrypted subsamples are multiplexed. The encryption of the subsamples is performed in a real optical JTC encrypting system. The multiplexing and the decryption process are carried out by means of a virtual optical system. Experimental results are presented to show the validity of the proposal.

Keywords: optical processing; encryption; multiplexing; subsampling.

1. INTRODUCTION

Optical systems are limited by diffraction, which imposes some restrictions in the information that can be processed by the system. There are some techniques that allows overtake the limitations and expand the capacities of the optical processors, but involving modifications and/or additions over the optical setup [1-5]. W. Lukosz proposed some methods to extend the bandwidth of the transferred spatial frequencies transmitted by a given optical system [1]. Its proposals included the reduction of the object area, to extend the bandwidth in one direction or transmitting the information using one state of polarization only. In the literature, we find other methods, an architecture based on a beamsplitter and linearly translating mirror is presented in [2]. An approach described in [3] uses a beamsplitter and a rotating mirror, and an interesting approach that allows improving the resolution of the reconstructed image effectively is proposed and implemented in [4]. Additionally, it was demonstrated that an increase in the resolution is possible through phase correction and superposition of two reconstructed object waves [5].

On the other hand, during the last decades optical processors had shown their great ability to process data in an efficient and secure way [6-8]. For this reason, a large amount of research has been developed in the area of optical information processing. In particular, in the last two decades the encryption techniques using optical systems focused the attention of many researchers [9]. Among the encrypting methods, the most common optical system is based on the double random phase encoding, using indistinctly 4f or JTC architectures [10-11]. The JTC encrypting architecture is inherently holographic, compact and with less alignment requirements than the 4f architecture [12-13]. Therefore in this work, the method that allows encrypting data using the JTC encrypting architecture is preferred.

22nd Congress of the International Commission for Optics: Light for the Development of the World,
edited by Ramón Rodríguez-Vera, Rufino Díaz-Uribe, Proc. of SPIE Vol. 8011, 80117C
2011 SPIE · CCC code: 0277-786X/11/$18 · doi: 10.1117/12.902195

A limitation of the experimental optical encryption system is the frequency content that can be processed by the system. We propose a method that combines a subsampling technique with a multiplexing operation to overcome this limitation. In the implementation of the procedure, it is not necessary to introduce additional elements or to change the position of the existing elements in the optical setup.

2. THEORETICAL DESCRIPTION OF THE METHOD

In the encryption process the object $o(x,y)$ (Figure 1(a)) is divided into mth subsamples $o_m(x,y)$ of equal size as shown in Figure 1(b). The number of subsamples will depend on the object and the maximum resolution expected.

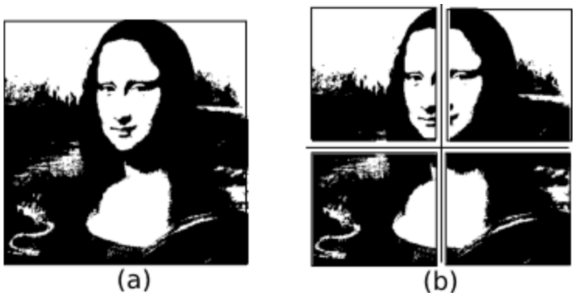

Figure 1. (a) Original object and (b) original object divided into four subsamples.

Each subsample is encrypted by using the double random phase encryption technique in the joint transform correlator (JTC) optical setup shown in Figure 2 [12-13].

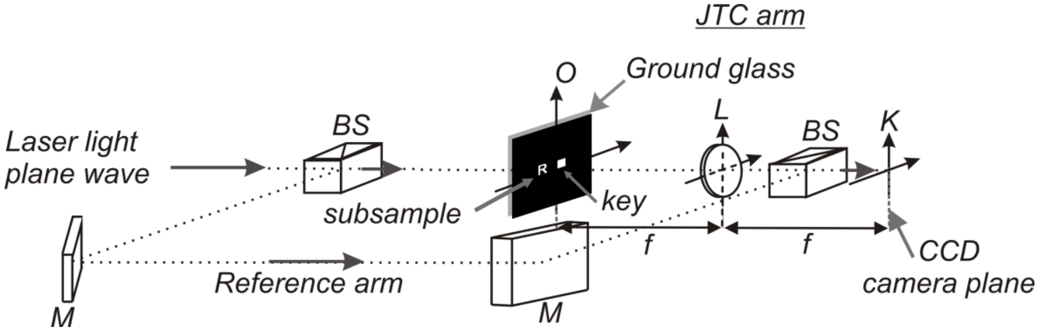

Figure 2. Joint transform correlator optical setup in a Mach-Zehnder scheme for the encryption of each subsample. *BS*: cubic beam splitter, *M*: mirror, *L*: lens of focal distance *f*, *O*: input plane, *K*: CCD camera plane.

In the input plane of the JTC, the subsample $o_m(x,y)$ is placed in a window in contact with a random phase mask $g(x,y)=\exp\left(i2\pi b(x,y)\right)$ and at a distance $2a$ from the encrypting random phase key $h(x,y)=\exp\left(i2\pi c(x,y)\right)$, where $b(x,y)$ and $h(x,y)$ are random functions in the range $[0,1]$. Thus, in the input plane the transmittance is

$$e_m(x,y)=f_m(x,y)\otimes\delta(x+a,y)+h(x,y)\otimes\delta(x-a,y), \tag{1}$$

where $\otimes$ means convolution operation, $f_m(x,y)=o_m(x,y)g(x,y)$ and $\delta(\cdot)$ is the Dirac delta function. The first step in the encryption process corresponds to the recording of input plane's joint power spectrum (JPS). Therefore, the reference beam is blocked to obtain:

$$E_m(u,v)=|F_m(u,v)|^2+|H(u,v)|^2+F_m^*(u,v)H(u,v)\exp[-2\pi iua]+F_m(u,v)H^*(u,v)\exp[-2\pi iu(-a)] \tag{2}$$

In this case some constant terms are omitted [13]. $F_m(u,v)$ and $H(u,v)$ are the Fourier transform (FT) of $f_m(x,y)$ and $h(x,y)$ respectively, (u,v) are the transforming coordinates of (x,y), and $|\cdot|^2$ and $*$ are the square module and the complex conjugate of a function, respectively. The JPS is stored using a CCD camera at plane K (see Figure 2). Only the 4th term in equation 2 is necessary, the third one is redundant information and the first one and the second one correspond to noise. Thus, intensity terms $|F_m(u,v)|^2$ and $|H(u,v)|^2$ are recorded separately, blocking the key the object intensity is recorded and then blocking the object is possible to register the key intensity. Subtracting these intensities from the JPS Eq. (2) yields

$$E'_m(u,v) = F_m^*(u,v)H(u,v)\exp[-2\pi iu(2a)] + F_m(u,v)H^*(u,v)\exp[-2\pi iu(-2a)] \tag{3}$$

To remove the first term in this equation a FT is performed,

$$e'_m(x,y) = f_m^*(x,y) \otimes h(-x,-y) \otimes \delta(x+2a,y) + f_m(-x,-y) \otimes h^*(x,y) \otimes \delta(x-2a,y) \tag{4}$$

this FT separates the two terms, the redundant term is removed and the remaining term is repositioned into a desire position (x_m, y_m). This reposition allows recovering each subsample, in the decryption step, in its respective relative original position, avoiding mismatching of any kind. Therefore Eq. (4) results

$$e''_m(x,y) = f_m(-x,-y) \otimes h^*(x,y) \otimes \delta(x-x_m, y-y_m), \tag{5}$$

and by performing an inverse Fourier transform (IFT), the encrypted subsample is:

$$E''_m(u,v) = F_m(u,v)H^*(u,v)\exp[2\pi i(x_m u + y_m v)] \tag{6}$$

All encrypted subsamples are obtained with the procedure detailed above and using the same encrypting key $h(x,y)$. Next, the reference beam is unblocked, the object in the input plane is blocked, and the hologram of the FT of the encrypting key is recorded to be sent to the end user for the decryption procedure,

$$G(u,v) = |P(u,v)|^2 + |H(u,v)|^2 + P^*(u,v)H(u,v)\exp[-2\pi iua] + P(u,v)H^*(u,v)\exp[-2\pi iu(-a)] \tag{7}$$

$P(u,v)$ is a plane wave that represents the reference beam; some constant terms were omitted. The hologram is stored using a CCD camera at plane K. Again, only the third term is necessary, thus, the intensity terms $|P(u,v)|^2$ and $|H(u,v)|^2$ are recorded separately and subtracted from the hologram in Eq. (7) yielding

$$G'(u,v) = P^*(u,v)H(u,v)\exp[-2\pi iua] + P(u,v)H^*(u,v)\exp[-2\pi iu(-a)] \tag{8}$$

Then next step is to remove the second term of this last equation, to achieve this is necessary to perform a FT,

$$g'(x,y) = p^*(x,y) \otimes h(-x,-y) \otimes \delta(x+2a,y) + p(-x,-y) \otimes h^*(x,y) \otimes \delta(x-2a,y), \tag{9}$$

The last operation allows to separate the two related terms, the redundant term is removed and the surviving is repositioned at the center of the coordinate system. Therefore Eq. (9) will transform into

$$g''(x,y) = h(-x,-y) \otimes \delta(x,y), \tag{10}$$

where $p(x,y)$ is the FT of a plane wave, i.e., a Dirac delta function. By performing an IFT, the recorded FT of the key is:

$$G''(u,v) = H(u,v) \tag{11}$$

To recover the entire original object $o(x,y)$, during the decrypting procedure the FT of the key is send to the end user along with the encrypted and filtered information of all the subsamples. A multiplexing procedure for the N encrypted subsamples is performed (Figure 3) to get,

$$M(u,v) = \textstyle\sum_{m=1}^{N} F_m(u,v)H^*(u,v)\exp[2\pi i(x_m u + y_m v)] \tag{12}$$

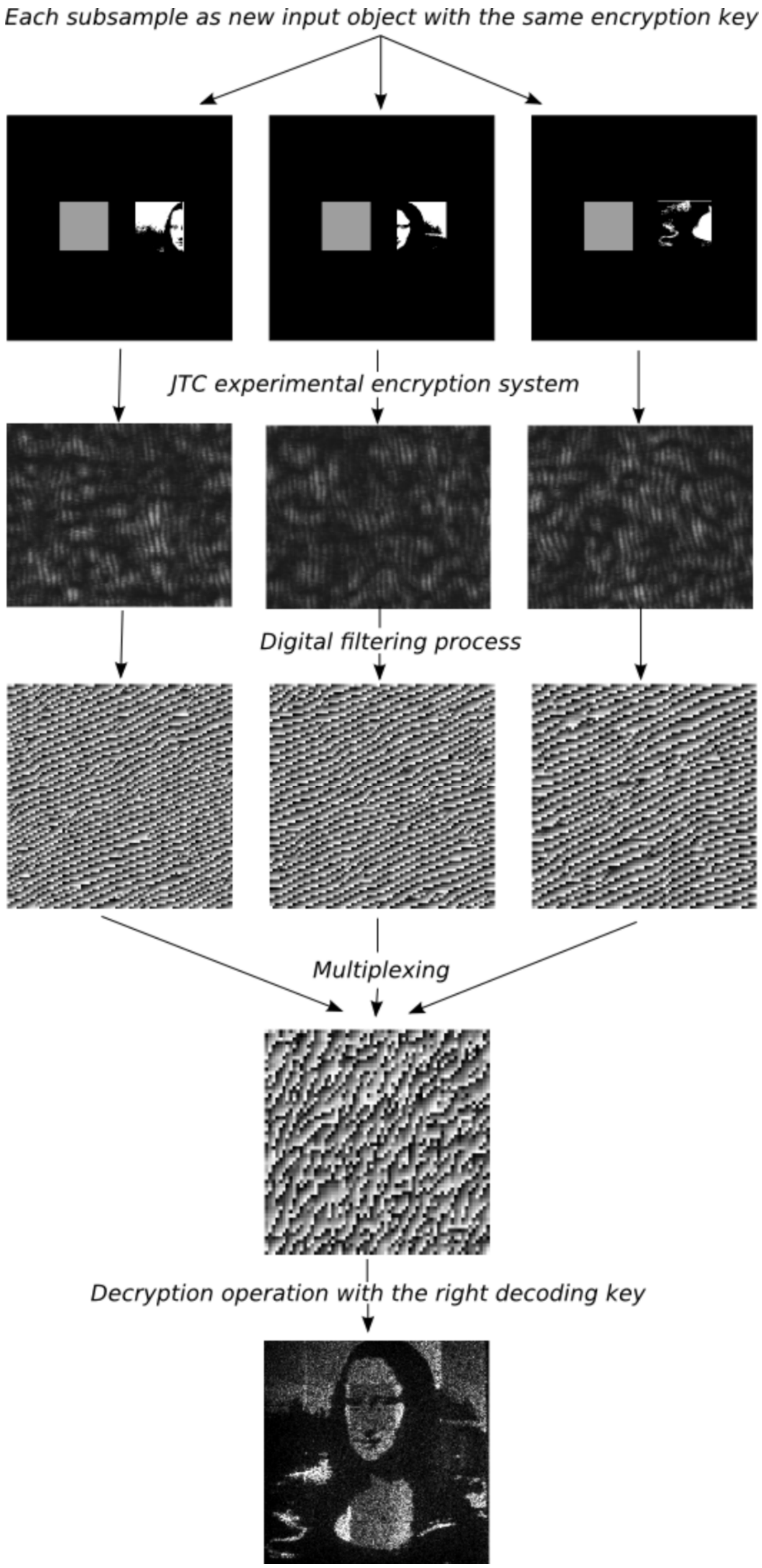
Each subsample as new input object with the same encryption key
JTC experimental encryption system
Digital filtering process
Multiplexing
Decryption operation with the right decoding key

Figure 3. Block diagram of the entire procedure.

In the recovering process, the authorized users multiply the FT of the encrypting key (Eq. (11)) and the information of all the encrypted subsamples (Eq. (12)),

$$D(u,v) = \sum_{m=1}^{N} F_m(u,v)H^*(u,v)H(u,v)\exp[2\pi i(x_m u + y_m v)]. \tag{13}$$

and performing an IFT,

$$d(x,y) = \sum_{m=1}^{N} f_m(x,y)\otimes[h^*(-x,-y)\otimes \mathrm{h}(x,y)]\otimes\delta(x - x_m, y - y_m), \tag{14}$$

where $h^*(-x,-y)\otimes \mathrm{h}(x,y) \approx \delta(x,y)$ [1]. Thus Eq. (14) can be simplify,

$$d(x,y) = \sum_{m=1}^{N} f_m(x,y)\otimes\delta(x - x_m, y - y_m). \tag{15}$$

Eq. (15) corresponds to an augmented version of the original object.

The procedure is explained in the block diagram of Figure 3, in the encrypting stage the object is divided in subsamples, each subsample is encrypted and filtered separately, and then the encrypted subsamples are multiplexed. Finally, the object is decrypted when the right key and the multiplexed of the encrypted subsamples are employed.

3. EXPERIMENTAL RESULTS

In the experimental setup, we used a 200 mm focal length lens, a He-Ne laser, and a PULNIX TM6703 CCD camera with 640x480 pixels and 9 µm pixel size. The empty window and each subsample window were projected in a Holoeye LC2002 spatial light modulator (SLM) (see Figure 2). A ground glass placed behind the empty window generates the encrypting key. The subsample window size is 1.92 mm x 1.92 mm, the area of the empty window is 1.6 mm x 1.6 mm, and the distance between windows is 2.6 mm.

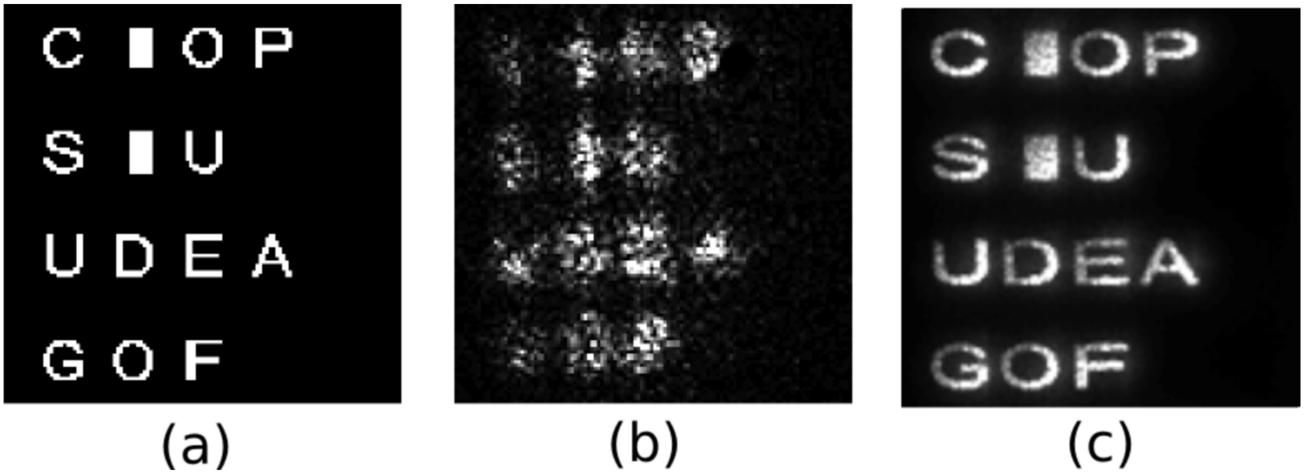

Figure 4. (a) Original object projected in the SLM, experimental decrypted objects employing: (b) the entire object as the unique sample and (c) the proposed subsampling method.

The experimental results are obtained using the arrangement shown in Figure 2. In Figure 4(a) the object to be processed is displayed; this object without subsampling is inserted in the optical setup and encrypted-decrypted using the right encrypting key. Finally, the recovered information is presented in Figure 1(b). It is evident that due to the limitations of the optical systems in fully handling the frequency information content of the original object, it is not possible to display the whole object details. To overcome this issue the object is divided into subsamples, where each subsample corresponds to one of the letters that compound the original object.

If the subsamples are encrypted and filtered separately, and then multiplexed, a right decryption procedure allows recovering the original data shown in Figure 4(c). In this sense, our approach allows processing information in a secure way surpassing the natural limitations of the optical systems by means of the subsampling, filtering and multiplexing processes.

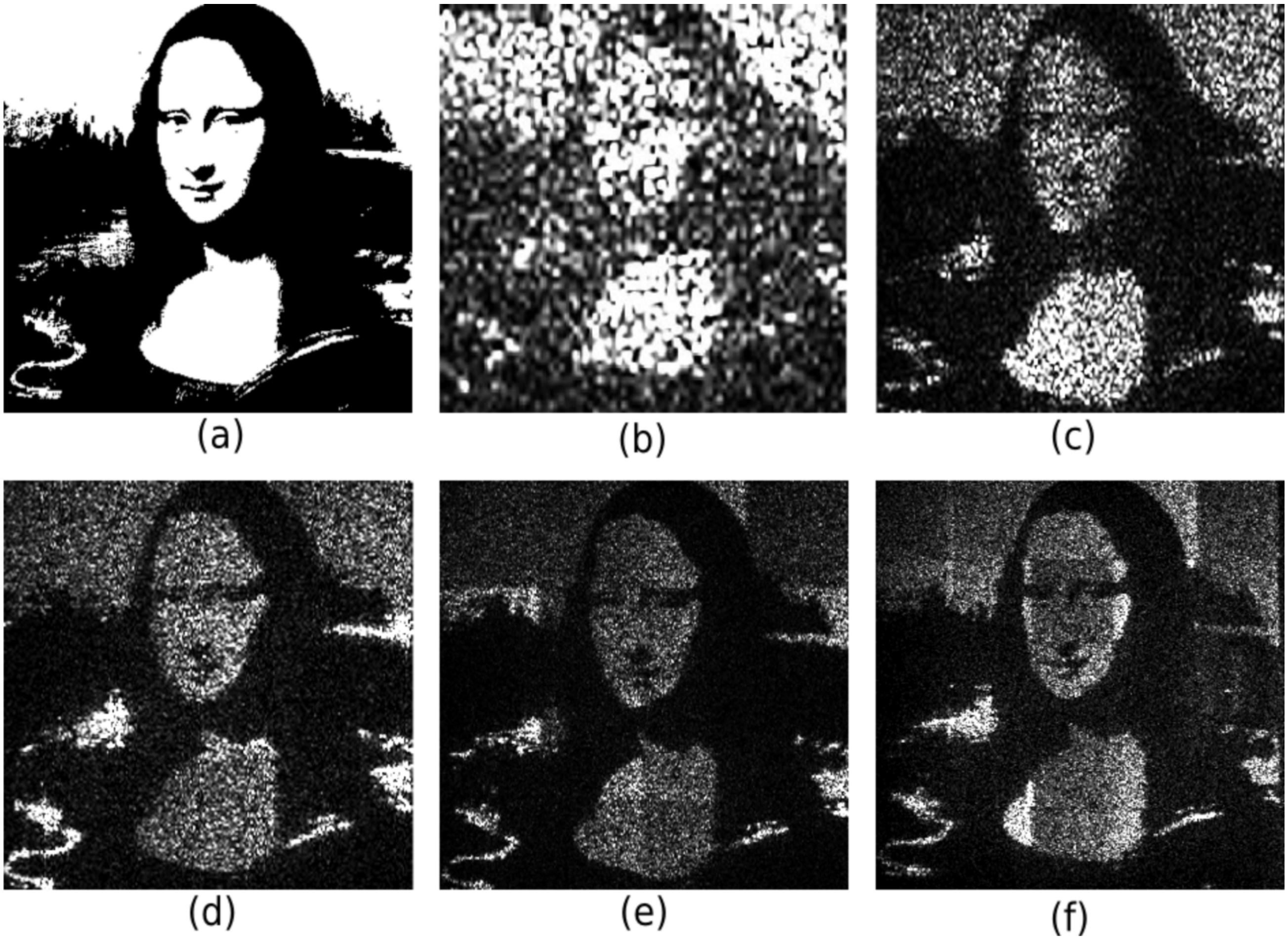

Figure 5. (a) Original object and (b) the decrypted version without subsampling. Decrypted object employing: (c) 4, (d) 9, (e) 16, and (f) 25 subsamples.

The decrypted images in Figure 4 demonstrate the potentiality and applicability of the proposed protocol. To expand the range of applications of the method, an object with a wide band of spatial frequencies is experimentally processed. The original object and its recovered data using the optical setup without the subsampling operation are presented in Figures 5(a) and (b) respectively. The decoding results when the original object is divided and processed in 4, 9, 16, and 25 subsamples are presented in Figures 5(c), 5(d), 5(e) and 5(f) respectively. These last results evidence the advantage of the proposal when a wide bandwidth objects want to be manipulated in a secure way.

4. CONCLUSIONS

We proposed and experimentally implemented a technique to solve the limitations in the finest spatial feature that can be processed for an optical encryption setup. The technique is a combination of subsampling and multiplexing procedures. The experimental arrangement is a Mach-Zehnder interferometer with a JTC encrypting architecture in one arm. The encrypted sections of a sampled object are filtered and multiplexed. To recover the original data, the encrypting key along with the multiplexed information is sent to the authorized user. The whole procedure is performed without carrying out modifications on the optical setup. The experimental results showed the effectiveness and great potential of the method to be applied in practical implementations. The procedure can be used in dynamical encryption or multi-user secure systems. It is important to take into account that this approach can be used not only in encrypting systems but in particular in those areas that involve optical processing setups.

Acknowledgments

This research was performed under grants COLCIENCIAS, CODI -Universidad de Antioquia (Colombia), TWAS-UNESCO Associateship Scheme at Centres of Excellence in the South, CONICET No. 0863, ANCyT PICT 1167 and Facultad de Ingeniería, Universidad Nacional de La Plata No. 11/I125 (Argentina)

REFERENCES

[1] Lukosz, W., "Optical Systems with Resolving Powers Exceeding the Classical Limit," J. Opt. Soc. Am. 56(11) 1463-1472 (1966).
[2] Marcia, R.F., Kim, C., Eldeniz, C., Kim, J., Brady, D.J. and Willett, R.M., "Superimposed video disambiguation for increased field of view," Opt. Express 16(21) 16352-16363 (2008).
[3] Uttam, S., Goodman, N.A., Neifeld, M.A., Kim, C., John, R., Kim, J. and Brady, D. "Optically multiplexed imaging with superposition space tracking," Opt. Express 17(3) 1691-1713 (2009).
[4] Martínez-León, L. and Javidi, B., "Synthetic aperture single-exposure on-axis digital holography," Opt. Express 16(1) 161-169 (2008).
[5] Zhao, J., Yan, X., Sun, W. and Di, J., "Resolution improvement of digital holographic images based on angular multiplexing with incoherent beams in orthogonal polarization states," Opt. Lett. 35(20) 3519-3521 (2010).
[6] Marschall, L. and Kra, G., "The power processing of light," OPN March 38-42 (2002).
[7] Li, G., "Recent advances in coherent optical communication," Advances in Optics and Photonics 1(2) 279-307 (2009).
[8] Matoba, O. and Javidi, B., "Secure Ultrafast Data Communication and Processing," OPN May 70-73 (2002).
[9] Matoba, O. and Nomura, T., Pérez-Cabré, E., Millán, M.S. and Javidi. B., "Optical Techniques for Information Security,"
Proceedings of the IEEE 97(6) 1128-1148 (2009).
[10] Refregier, P. and Javidi, B., "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. 20(7) 767-769 (1995).
[11] Nomura, T. and Javidi, B., "Optical encryption using a joint transform correlator architecture," Opt. Eng. 39(8) 2031-2035 (2000).
[12] Rueda, E., Barrera, J.F., Henao, R. and Torroba, R., "Optical encryption with a reference wave in a joint transform correlator architecture," Opt. Commun. 282(16) 3243-3249 (2009).
[13] Henao, R., Rueda, E., Barrera, J.F. and Torroba, R., "Noise-free recovery of optodigital encrypted and multiplexed images," Opt. Lett. 35(3) 333-335 (2010).