Optics Letters

Three-dimensional joint transform correlator cryptosystem

Alejandro Velez Zea,[1,*] John Fredy Barrera Ramirez,[2] and Roberto Torroba[1,3]

[1]Centro de Investigaciones Ópticas (CONICET La Plata-CIC) C.P 1897, La Plata, Argentina
[2]Grupo de Óptica y Fotónica, Instituto de Física, Facultad de Ciencias Exactas y Naturales, Universidad de Antioquia UdeA, Calle 70 No. 52-21, Medellín, Colombia
[3]UIDET OPTIMO, Facultad de Ingeniería, Universidad Nacional de La Plata, La Plata, Argentina
*Corresponding author: alejandrov@ciop.unlp.edu.ar

Received 7 October 2015; revised 20 December 2015; accepted 21 December 2015; posted 21 December 2015 (Doc. ID 251222); published 29 January 2016

We introduce for the first time, to the best of our knowledge, a three-dimensional experimental joint transform correlator (JTC) cryptosystem allowing the encryption of information for any 3D object, and as an additional novel feature, a second 3D object plays the role of the encoding key. While the JTC architecture is normally used to process 2D data, in this work, we envisage a technique that allows the use of this architecture to protect 3D data. The encrypted object information is contained in the joint power spectrum. We register the key object as a digital off-axis Fourier hologram. The encryption procedure is done optically, while the decryption is carried out by means of a virtual optical system, allowing for flexible implementation of the proposal. We present experimental results to demonstrate the validity and feasibility of the method.

OCIS codes: (060.4785) Optical security and encryption; (070.4560) Data processing by optical means; (100.4998) Pattern recognition, optical security and encryption.

http://dx.doi.org/10.1364/OL.41.000599

The modern subject of 3D imaging evolved from traditional optical holography [1,2]. Customarily, a hologram results from recording the interference pattern acquired from the superposition of a reference beam and an object beam. The phase of the object beam holds the 3D information about the object. According to the basis of interferometry, this information is present in the intensity of the hologram.

Digital recording methods stepped forward, helping to improve the analog procedures and thus avoiding instances of time consuming developing, repositioning techniques, and other such previously used courses of action.

The advantages of digital holography are not only the above mentioned; for instance, the digital era provided both a great chance for real-time analysis and for a lot of techniques difficult to implement with analog optics [3,4]. Because digital holograms are directly available in digital form, they can readily be processed.

Nevertheless, the actual size of the pixels in digital cameras sets a limit on the spatial frequency of the interference pattern and, therefore, prevents the use of large angles between the object and the reference beams [5]. This restriction makes it necessary in practice to use an in-line recording configuration, in which the reference beam is parallel to the object.

But now, the increased availability of high-resolution and low-cost digital cameras allows new techniques for the manipulation of holographic data, including fast digital filtering and multiplexing, besides extending the practical use of off-axis recording setups [6].

On the other hand, associated with any digital holography process, we find speckle noise, becoming visible in numerical as well as optical reconstruction. Obviously, it worsens the information for the object wavefront. In particular, a hologram encoding strategy has been introduced that allows direct synthesis of the contribution of multiple acquisitions into a single complex wavefront, thus improving both the numerical and optical reconstructions and showing remarkable noise suppression with respect to processing of a single hologram [7].

Among the interesting applications of digital holography, we find optical encryption, as security and information safety, has become increasingly important [8–11].

We also have to note that in a closely related subject in the frame of optical processing, researchers carried out extensive studies to employ coherent optical methods in correlation techniques. Among the most popular correlators is the classical joint transform correlator (JTC) [12]. Correlation is conceived as a filtering that aims to extract the relevant information in order to recognize a pattern in a complex scene. Many contributions include the use of the JTC as architecture. In the JTC case, the information is stored as an intensity distribution in the recording media. Much work has been started using the principle of coherent optics filtering for selecting relevant information as frame applications for the JTC scheme [13], both for 2D and 3D scenes [14]. The inherent parallelism of the optics provides an appropriate support for information processing techniques. So far, the use of the JTC architecture in this context has led to the continuous and fruitful development of the field.

We also find recent contributions in the use of the JTC architecture in optical encryption [15–17]. The handling and processing of 2D information is conveniently accomplished under this scheme.

However, we live in a 3D world, and 3D objects provide several degrees of freedom to perform imaging and optical information processing. Three-dimensional imaging is an important topic because it allows the construction of natural views.

Certainly, as the applications of 3D imaging systems increase, we expect a corresponding need for holographic data security.

Among the proposals for securing 3D object data, we find a technique that uses a diffuser to provide a speckle reference beam, which interferes with the light from the object to form a hologram containing the encrypted data. This ensures that an adequate reconstruction of the object from the hologram can only be accomplished with knowledge of the specific speckle reference beam. Therefore, this diffuser behaves as the security key for the object data contained in the hologram [18].

Although the JTC architecture has been proposed for the processing of 2D data, we find that there are no restrictions to extending this application to 3D, as the fundamental behavior of the system allows processing not only the intensity but also the phase information. Therefore, data can also be encrypted and recovered with the advantages of 3D imaging, and additionally, we can assume the encrypting key is an arbitrarily diffusing object. We now propose a method that allows the encryption of any diffuse 3D object using another 3D object as the key, carefully addressing the experimental feasibility of this approach.

The proposal is based in double random phase mask optical encryption with a joint transform correlator architecture, as shown in Fig. 1. The random phase masks are provided by the natural diffusing properties of the surfaces of the key object and the input object [19].

As can be seen in Fig. 1, the system is an interferometer, where one beam provides illumination to the key and input objects, and the other provides a reference plane wave. The key and input objects are placed side by side on a platform with a separation $2a$. In order to perform the encryption procedure, the reference wave is obstructed. A lens with focal length f performs the joint Fourier transform (FT) of the light reflected by the key and input objects. The camera then registers the joint power spectrum (JPS), given by

$$J(v,w) = |O_k(v,w)|^2 + |O_p(v,w)|^2 + O_k(v,w)O_p^*(v,w)e^{-4\pi iav} + O_k^*(v,w)O_p(v,w)e^{4\pi iav}. \quad (1)$$

$O_k(v,w)$ and $O_p(v,w)$ are the FT of the key object $o_k(x,y)$ and the input object $o_p(x,y)$, respectively; $v = x/\lambda f$ and $w = y/\lambda f$ are the coordinates in the Fourier plane. The first two terms correspond to the intensity of the FT of the object key and the input object, and the exponential terms will result in fringes that will depend on the separation $2a$ between both objects. The maximal value of this separation is given by the pixel size of the CMOS camera.

Both the third and fourth terms of the JPS contain the encrypted data, so one can be selected and the remainder terms discarded. This is achieved by performing the FT of the JPS, obtaining

$$j(x,y) = \mathrm{FT}\{|O_p(v,w)|^2\} + \mathrm{FT}\{|O_k(v,w)|^2\} + \mathrm{FT}\{O_p(v,w)O_k^*(v,w)\} \otimes \delta(x+2a,y) + \mathrm{FT}\{O_p^*(v,w)O_k(v,w)\} \otimes \delta(x-2a,y). \quad (2)$$

The Dirac delta functions arise from the exponential factors of Eq. (1) and result in a spatial separation between the intensity terms and the terms containing the encrypted data, as can be seen in Fig. 2.

Due to this spatial separation, we can isolate the third term in Eq. (1). Then, we place this term in any desired coordinates (x', y'). By performing the inverse Fourier transform (IFT), we finally obtain the encrypted object

$$E(v,w) = O_p(v,w)O_k^*(v,w)\exp[2\pi(vx' + wy')]. \quad (3)$$

Equation (3) contains the information for both the key object and the input object, but attempting to reconstruct the input object by performing the FT of Eq. (3) results in

$$e(x,y) = o_p(x,y) \otimes o_k^*(x,y) \otimes \delta(x-x', y-y'). \quad (4)$$

The convolution between $o_p(x,y)$ and $o_k(x,y)$, due to the phase irregularities of any diffuse surface, results in a random speckle pattern, making it impossible to recover the phase and amplitude data of the input object.

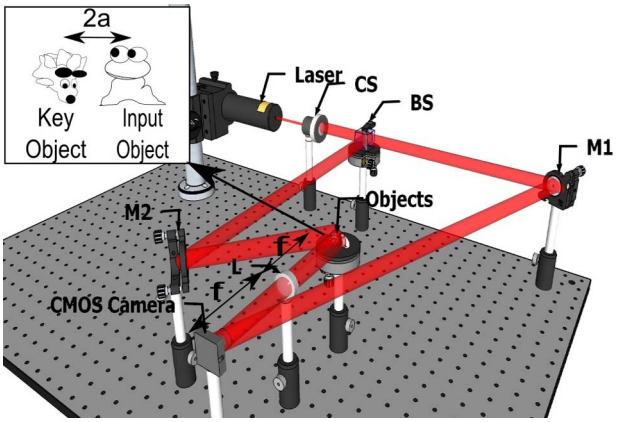

Fig. 1. Scheme of the proposed experimental 3D cryptosystem: CS, collimation system; BS, beam splitter; M, mirror; L, lens; f, lens focal length.

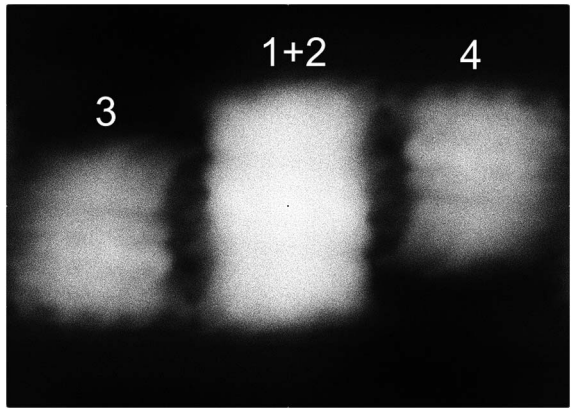

Fig. 2. Intensity of Eq. (1): 1 + 2) first two terms, 3) third term, and 4) fourth term.

In order to recover the input object information, we must register the phase and amplitude data of the key object. Using the system of Fig. 1, we remove the input object and, therefore, the light reflected by the key object interferes with the reference plane wave. Then, we register with the CMOS camera an off-axis Fourier hologram of the key object (Fig. 3), given by

$$H(v,w) = |P(v,w)|^2 + |O_k(v,w)|^2 + P(v,w)O_k^*(v,w) + P^*(v,w)O_k(v,w). \quad (5)$$

$P(v,w)$ is the tilted reference plane wave, described as

$$P(v,w) = A\,\exp(-i2\pi f(v\cos\alpha + w\cos\beta)), \quad (6)$$

where A is the uniform amplitude of the reference wave, and α and β are the tilt angles.

The first two terms of Eq. (5) can be eliminated by subtracting the intensity of the FT of $O_k(v,w)$ and $P(v,w)$, which can be registered separately by obstructing the corresponding beam in the experimental setup. Performing the FT of the remaining terms, we obtain

$$h(x,y) = o_k(x,y) \otimes \delta(x + f\cos\alpha, y + f\cos\beta) + o_k^*(x,y) \otimes \delta(x - f\cos\alpha, y - f\cos\beta). \quad (7)$$

The terms of Eq. (7) are the key object and the corresponding complex conjugate separated by Dirac delta functions. These functions will depend on the tilt angles of the plane reference wave. Isolating the first term and performing the IFT we can obtain $O_k(v,w)$.

Now, in order to recover the input object, we multiply Eq. (3) by $O_k(v,w)$, obtaining

$$E(v,w) = O_p(v,w)O_k^*(v,w)O_k(v,w)\exp[2\pi(vx' + wy')]. \quad (8)$$

If $O_k(v,w)$ is taken to be approximately a phase-only function, the product of $O_k(v,w)$ with its complex conjugate is then equal to 1 [20]. Applying this approximation and performing the IFT of Eq. (8), we obtain

$$e(x,y) = o_p(x,y) \otimes \delta(x - x', y - y'), \quad (9)$$

which is finally the input object recovered in coordinates (x', y').

Using Fig. 4, we can examine the experimental results of the 3D cryptosystem. When using a wrong key object during the decryption process, we are unable to recognize the input object [Fig. 4(b)]; however, when using the right key, we are able to recognize the input object despite the speckle pollution [Fig. 4(c)]. In Fig. 4(d), we show the object reconstructed from an off-axis Fourier hologram, taken with the same optical setup employed in the encryption process but removing the key object. This means that Fig. 4(d) presents the object reconstructed from an off-axis hologram without involving the encryption process. Comparing this image with Fig. 4(c), we note that the encryption and decryption procedures introduce a contrast loss and additional speckle noise over the reconstructed object, as expected in a JTC-based cryptosystem. In order to quantify the degradation caused by the encryption and decryption over the reconstructed object, we measured the normalized mean square error (NMSE) between the object recovered from an off-axis hologram $m'(p,q)$ [Fig. 4(d)] and the retrieved object after encryption, applying an increasing percentage of random noise over the encrypted data and, finally, the decryption. If we assume $m(p,q)$ is the decrypted data when random noise is introduced over the encrypted object, and $m_w(p,q)$ is the case with maximum noise, the NMSE is given by

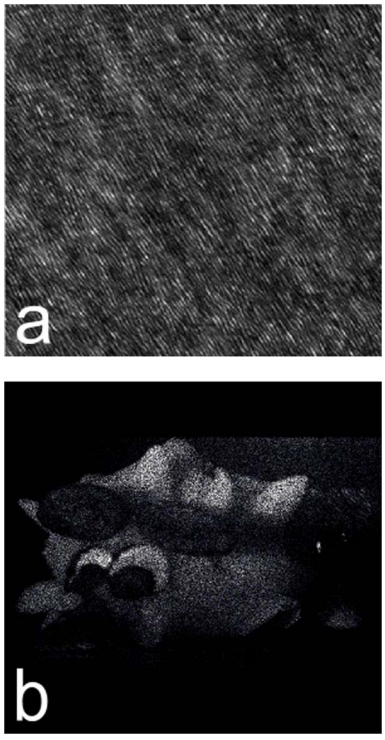

Fig. 3. (a) Fourier hologram of the key object and (b) intensity of the key object reconstructed from the filtered hologram $O_k(v,w)$.

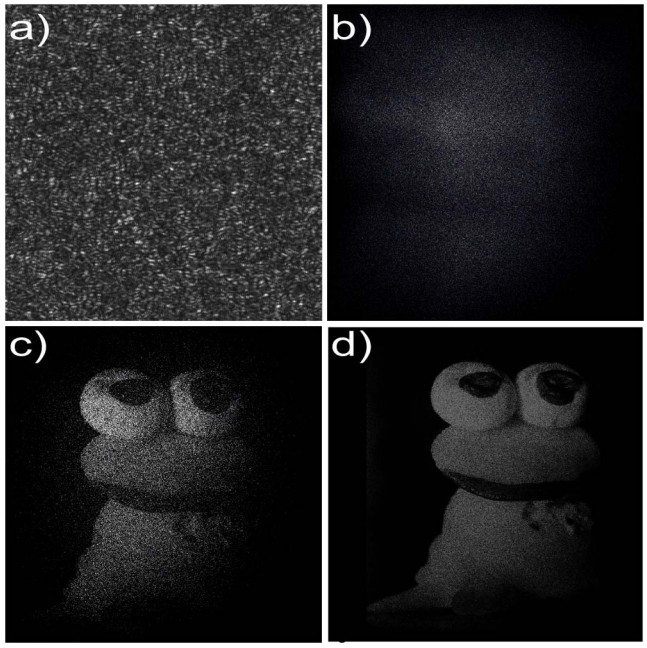

Fig. 4. (a) Encrypted object; (b) decrypted object using the wrong key object; (c) decrypted object using the right key object; and (d) reconstructed object from an off-axis hologram.

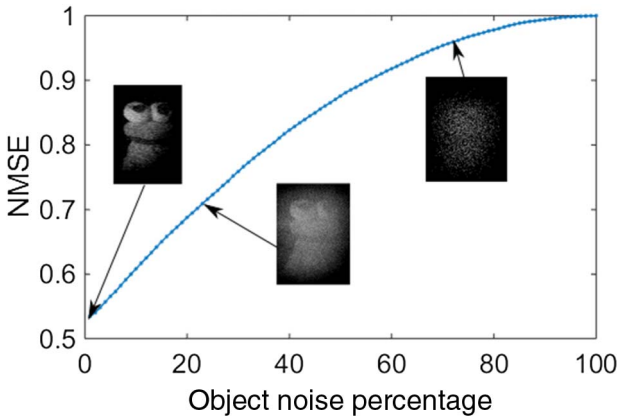

Fig. 5. NMSE between the decrypted object with random noise added over the encrypted data and the object reconstructed from an off-axis hologram without applying the encrypting process.

$$\mathrm{NMSE} = \frac{\sum_{p,q}^{N} |m(p,q) - m'(p,q)|^2}{\sum_{p,q}^{N} |m(p,q) - m_w(p,q)|^2}, \tag{10}$$

where (p, q) are the pixel coordinates, and $N \times N$ is the number of pixels.

In Fig. 5, we show the NMSE as random noise is added to the encrypted data in 1% steps. There is a baseline error due to the encryption procedure, and the decrypted object shows a gradual degradation as the percentage of noise increases, as is usual in JTC-based cryptosystems. Beyond a certain threshold (25% in this case), the image reconstruction quality becomes compromised.

The experimental results in this Letter were obtained with the setup of Fig. 1. We used a CMOS EO-10012M camera, with a pixel size of 1.67 μm × 1.67 μm and 3480 pixel × 2748 pixel resolution. A Laserglow Technologies diode pumped solid state (DPSS) laser operating at a wavelength of 542 nm and an output power of 50 mW was employed. The objects had maximum dimensions of 18 mm × 24 mm × 16 mm, and the separation $2a$ was 35 mm. The focal length of the lens was 200 mm.

The 3D information is encrypted using the joint transform correlator optical architecture and a 3D object as an encrypting key. Since this system is, in essence, an off-axis Fourier holography setup, the maximum axial length that the objects should have, to be fully recorded, will depend on the focal depth of the lens used during encryption. Obviously, the performance of the system will be affected by several factors, amongst these are the diffusing characteristics of the key and input objects, the separation between objects, and their spatial bandwidth, since these factors will directly influence the size of the speckle and the interference fringes on the JPS.

We expect this proposal inherits most of the characteristics of 2D JTC cryptosystems, and therefore many of the applications developed for them can be extended to 3D objects under the presented scheme. Additional research is necessary to optimize the performance of the system, in order to show the limitations and to take advantage of the additional flexibility of 3D object processing.

Funding. COLCIENCIAS; Comité para el Desarrollo de la Investigación (CODI); CONICET (0863/09, 0549/12); Estrategia de Sostenibilidad 2014–2015; Facultad de Ingeniería, Universidad Nacional de La Plata (11/I168); MINCyT-COLCIENCIAS (CO/13/05).

Acknowledgment. John Fredy Barrera Ramirez acknowledges support from The International Centre for Theoretical Physics ICTP Associateship Scheme.

REFERENCES

1. D. Gabor, Nature **161**, 777 (1948).
2. U. Schnars and W. P. O. Jüptner, Meas. Sci. Technol. **13**, R85 (2002).
3. M. A. Kronrod, N. S. Merzlyakoz, and L. P. Yaroslavskii, Sov. Phys. Tech. Phys. **17**, 333 (1972).
4. U. Schnars and W. Jüptner, Appl. Opt. **33**, 179 (1994).
5. E. N. Leith and J. Upatnieks, J. Opt. Soc. Am. **52**, 1123 (1962).
6. A. Velez, J. F. Barrera, and R. Torroba, Opt. Laser Technol. **75**, 146 (2015).
7. P. Memmolo, V. Bianco, M. Paturzo, B. Javidi, P. Netti, and P. Ferraro, Opt. Express **22**, 25768 (2014).
8. H. Di, K. Zheng, X. Zhang, E. Y. Lam, T. Kim, Y. S. Kim, T. Poon, and C. Zhou, Appl. Opt. **51**, 1000 (2012).
9. W. Chen, B. Javidi, and X. Chen, Adv. Opt. Photon. **6**, 120 (2014).
10. Q. Gao, Y. Wang, T. Li, and Y. Shi, Appl. Opt. **53**, 4700 (2014).
11. M. T. Shiu, Y. K. Chew, H. T. Chan, X. Y. Wong, and C. C. Chang, Appl. Opt. **54**, A84 (2015).
12. J. Goodman and C. Weaver, Appl. Opt. **5**, 1248 (1966).
13. M. S. Millán, J. Opt. **14**, 103001 (2012).
14. J. Rosen, Appl. Opt. **37**, 7538 (1998).
15. T. Nomura and B. Javidi, Opt. Eng. **39**, 2439 (2000).
16. J. F. Barrera, M. Tebaldi, C. Ríos, E. Rueda, N. Bolognini, and R. Torroba, Opt. Express **20**, 3388 (2012).
17. J. F. Barrera, A. Mira, and R. Torroba, Opt. Express **21**, 5373 (2013).
18. E. Tajahuerce and B. Javidi, Appl. Opt. **39**, 6595 (2000).
19. J. W. Goodman and J. C. Dainty, eds., *Laser Speckle and Related Phenomena* (Spring-Verlag, 1984).
20. G. Unnikrishnan, J. Joseph, and K. Singh, Appl. Opt. **37**, 8181 (1998).