

Optical approach for the efficient data volume handling in experimentally encrypted data

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

2016 J. Opt. 18 065702

(<http://iopscience.iop.org/2040-8986/18/6/065702>)

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

Download details:

IP Address: 129.81.226.78

This content was downloaded on 06/04/2016 at 14:20

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

Optical approach for the efficient data volume handling in experimentally encrypted data

Sorayda Trejos¹, John Fredy Barrera¹, Alejandro Velez²,
Myrian Tebaldi^{2,3} and Roberto Torroba^{2,3}

¹Grupo de Óptica y Fotónica, Instituto de Física, Facultad de Ciencias Exactas y Naturales, Universidad de Antioquia UdeA, Calle 70 No. 52-21, Medellín, Colombia

²Centro de Investigaciones Ópticas (CONICET La Plata-CIC—UNLP) PO Box 3, C.P 1897, La Plata, Argentina

³UIDET OPTIMO, Facultad de Ingeniería, Universidad Nacional de La Plata, La Plata, Argentina

E-mail: sorayda.trejos@udea.edu.co

Received 21 December 2015, revised 19 February 2016

Accepted for publication 7 March 2016

Published 5 April 2016



CrossMark

Abstract

Experimental optical procedures generate a tremendous amount of data, which must be then processed for any practical application. We present a new optical approach in terms of the data volume for the efficient handling of multiple data obtained from an experimental cryptosystem. In order to achieve this goal, we use the combination of optical filtering and optical scaling of the experimentally registered data. The intention is to reduce by optical means the amount of data to be managed. We define a so called ‘efficiency factor’ to describe the effectiveness of the approach. We find that volume reduction depends on this factor and the number of objects to be processed. We achieved substantial data volume reductions up to 94.24%. We introduce the basic concepts as well as experimental results that support both the feasibility and the applicability of our approach.

Keywords: data processing by optical means, pattern recognition, optical security and encryption

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

1. Introduction

Experimental optical encryption has played a significant role in many optics scenarios in recent years. Different optical architectures were presented in the technical literature [1–3]. In practice we can distinguish an encryption step, handling, sending and reception steps, and finally the decryption by the end user. In particular, when many input objects are used, not only an eventual superposition has to be avoided, but efficient handling to convey the information is also important [4, 5]. Precisely, this handling defines the way the encrypted data is organized so as to manage several inputs to conform a single unit to be sent. The optimal handling of holographic data was approached using digital compression techniques [6, 7]. In particular, we found in [6] a proposal based on four digital industry-standard compression techniques and digital lossy

methods like resampling, quantization and discrete Fourier transformation. The results show that digital resampling is not an effective technique for digital interferograms. This is due to the fact that resampling results in an undersampling on the holographic microfringes. These digital compression techniques are digitally based.

Researchers proposed exploring many options to solve this problem. For instance, using the optical field phase only allows the storing requirements to be reduced by half with a minimal optical power loss during reconstruction [8]. Processing in the Fourier domain represents another tactic by filtering non-relevant terms contained in the hologram [9]. Recent examples deal with multiplexing and reconstruction in one step of 3D scenes [10].

The purpose of this contribution is to present an implementation of optical procedures to reduce the data volume

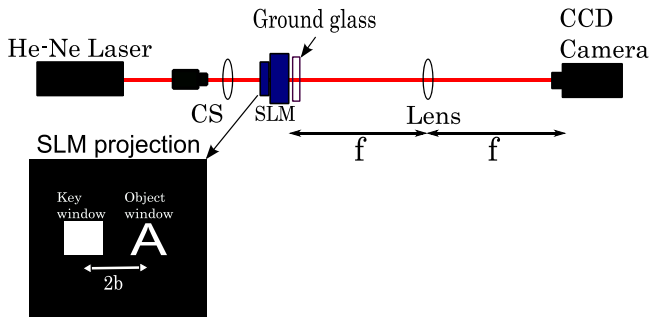


Figure 1. Scheme of the JTC cryptosystem. (CS: collimation system, SLM: spatial light modulator, f : lens focal length).

handling in experimental data obtained by optical means. Certainly, this approach can be complemented with digital compression techniques to further reduce the data. We employed experimental interferometric data and a virtual optical system to perform data volume reduction and reconstruction of the original information.

Among the different optical architectures, we select the joint transform correlator (JTC), which gives rise to the interferometric output we require as explained in the following. Any other interferometrical opto-digital cryptosystem will also equally serve.

2. Methodology for volume reduction

The proposal is based on the processing of the joint power spectrum (JPS) captured by using a CCD camera in the JTC cryptosystem, as show in figure 1.

In the JTC encrypting system the input plane contains the information of the object to be encrypted $o(x_0, y_0)$ attached to a random-phase mask $r_1(x_0, y_0)$, and another random-phase mask $r_2(x_0, y_0)$ 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 spatial light modulator (SLM), and the random-phase masks are generated by a ground glass. Therefore, the input plane is obtained when the SLM and the ground glass are placed in contact.

According to the scheme depicted in figure 1 a lens performs the Fourier transform (FT) of the input on the CCD camera. The result is the recording of the JPS of this input [11],

$$\begin{aligned} \text{JPS}(u, v) = & |C(u, v)|^2 + |R_2(u, v)|^2 \\ & + C^*(u, v)R_2(u, v)\exp(-4\pi i b u) \\ & + C(u, v)R_2^*(u, v)\exp(4\pi i b u) \end{aligned} \quad (1)$$

where $2b$ is the separation between the object and the key, $*$ means complex conjugate; $C(u, v)$ is the FT of $o(x_0, y_0)r_1(x_0, y_0)$, and $R_2(u, v)$ is the FT of the encoding key $r_2(x_0, y_0)$. Equation (1) arises from the interference between the light from both windows at the SLM plane.

In general, we take as data volume the amount of data in a file or database. In our case, the data volume of the JPS is $X_c * Y_c * B_c$, where X_c and Y_c are the horizontal and vertical

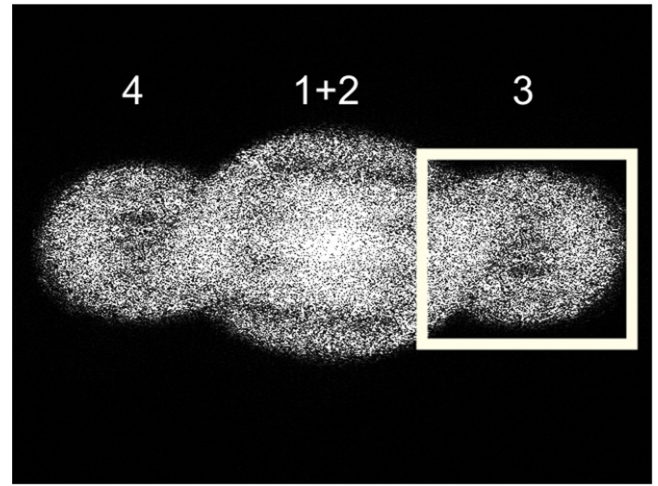


Figure 2. Intensity of the FT of equations (1); 1 + 2 central order corresponding to the FT of the object and key intensity, 3 and 4 are the FT of the third and fourth terms respectively.

resolutions respectively, and B_c the bit depth of the acquisition device. As we require a minimum volume for efficient handling, we focus our attention in retaining the third term of the JPS which contains the encrypted object information.

We perform the FT of the intensity represented by equation (1), obtaining the corresponding intensity distribution shown in figure 2, thanks to the interference fringes. We see a dc term corresponding to the FT of the key and object intensities and two orders, corresponding to the FT of the third and fourth term.

As shown in figure 2, we can select the third term which is smaller in size than the original JPS, and contains the information required to perform an adequate recovery of the original object [12]. In general, the size of the FT of the desired term is related to the physical dimensions of the object and the camera technical specifications. In this case, the filter window size is 177×198 . It is worth mentioning that increasing the filter widow size does not affect the quality of the final output and further reduction may cause both intensity and information loss. According to the previous definition, the data volume of the filtered object is $2 * X_o * Y_o * B_c$ where factor 2 is because the FT of the JPS contains both phase and amplitude information.

We define the 'efficiency factor' (E) as the ratio between the initial and final data volume after the different procedures applied over the data. As our technique encompasses two steps, each step will contribute to the final efficiency factor. Therefore in the following we analyze each contribution separately. The efficiency factor E_f achieved with filtering is given by

$$E_f = \frac{V_{\text{jps}}}{V_{\text{ft}}} = \frac{X_c * Y_c * B_c}{2 * X_o * Y_o * B_c} \quad (2)$$

where V_{jps} is the volume of the JPS registered by the CCD camera, and V_{ft} is the volume of the data after filtering. The filtered region in our JTC cryptosystem is equal to or less than one third of the total JPS region, thus guaranteeing that $V_{\text{ft}} < V_{\text{jps}}$. In this way the efficiency factor due to filtering is

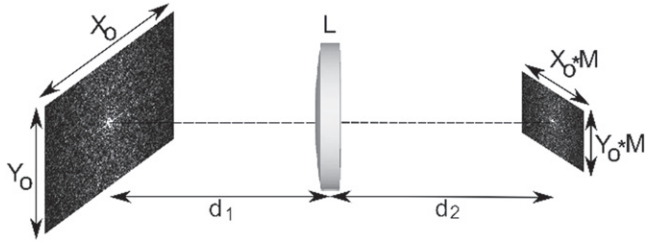


Figure 3. Virtual optical system used for scaling the filtered data: d_1 object distance, L convergent lens, d_2 image distance, X_0 filtered object width, Y_0 filtered object height, M magnification.

always greater than 1, meaning that we can reduce the data volume to be processed later simply with the filtering process.

In order to further increase the efficiency in data handling, we introduce an optical scaling procedure, to be applied over the filtered data. This procedure employs a virtual optical setup composed of a convergent lens used to scale the filtered data (see figure 3). Therefore, the efficiency factor for optical scaling E_M is given by

$$E_M = \frac{V_{ft}}{V_M} = \frac{2 * X_o * Y_o * B_c}{2 * X_o * Y_o * B_c * M^2} = \frac{1}{M^2} \quad (3)$$

where V_M is the volume of the data after scaling and M is the magnification of the virtual optical setup. It is important to take into account that the filtered data no longer contain the interferometrical fringes. A demagnification ($M < 1$) is mandatory in order to achieve $E_M > 1$ (equation (3)).

Therefore, an optical scaling over the filtered data does not involve the undersampling on the holographic microfringes present in digital resampling. Then, after performing both filtering and optical scaling, we achieve an efficiency factor of

$$E = \frac{V_{jps}}{V_M} = \frac{X_c * Y_c * B_c}{2 * X_o * Y_o * B_c * M^2}. \quad (4)$$

According to equations (2), (3) and (4), we can see that the efficiency factor of our proposal is the product of the efficiency factors of the filtering and optical scaling procedures $E = E_f E_M$.

This efficiency factor holds for a single encrypted object; however, we are interested in handling large amounts of encrypted objects. In order to take advantage of the inherent parallelism of optics, we can place all filtered data in a square matrix arrangement [12]. Then by performing the optical scaling over this arrangement, we process simultaneously all objects, instead of applying the procedure separately to each filtered data. In the following analysis, we assume that all objects share the same size and are registered in the same experimental setup; however, the procedure can be extended to the handling of data with different sizes from different setups.

The efficiency factor for N encrypted objects after filtering and scaling becomes

$$E_N = \frac{N * V_{jps}}{V_{NM}} = \frac{N * X_c * Y_c * B_c}{2 * N * X_o * Y_o * B_c * M^2} \quad (5)$$

defining V_{NM} as the data volume of N filtered objects after scaling. We can conclude, from equations (4) and (5), that the efficiency factor of the filtering and scaling does not depend on the number of encrypted objects $E_N = E$.

The parameter to quantify the efficiency of our proposal in terms of the data volume is the difference between the initial and the final volume,

$$\Delta V = N * (V_{jps} - V_M). \quad (6)$$

Using equation (4) we explicitly obtain

$$\Delta V = N * V_{jps} \left(1 - \frac{1}{E} \right). \quad (7)$$

As we expected, ΔV depends on the number of encrypted objects and the efficiency factor achieved with filtering and scaling processes. As $E_f > 1$ and $E_M > 1$ we achieve an efficiency factor $E > 1$, assuring a data volume reduction. We look for a data volume reduction as a result of our efficient procedure; therefore, we present an example to quantify the reduction achieved in an actual experimental case.

3. Results

In the next experimental example, we use 16 input objects, where the JPS corresponding to each object is individually recorded using the scheme of figure 1. The JPS of each encrypted object is recorded using a PULNIX TM6703 CCD camera with 640×480 pixels and a pixel pitch of $9 \mu\text{m}$. Consequently, each recorded JPS has a volume of 300.00 kB. For our 16 objects we have an initial data volume of 4.69 MB.

Afterwards, each JPS is filtered and, as discussed above, each filtered data is arranged within a square matrix as shown in figure 4(a). The input for the scaling process is the arrangement of filtered data (figure 4(a)). The area of the matrix arrangement will be equal to the area of the filtered JPS of each object multiplied by the number of objects to be multiplexed. In this example the filtered area is 177×198 pixels, with a data volume of 68.45 kB and the matrix arrangement has an area of 708×792 pixels, with a data volume of 1.07 MB. In figure 4(b) we show the outcome after data recovery [12]. Therefore, the initial data volume is 4.69 MB, and after filtering we achieve a volume of 1.07 MB. Finally, this arrangement is optically scaled using the setup of figure 3, and after recovery we obtain the result shown in figure 4(c).

When using a magnification of 0.5, we achieve a final data volume of 0.27 MB. The entire process has an efficiency factor of 17.53, and the final volume difference ΔV is

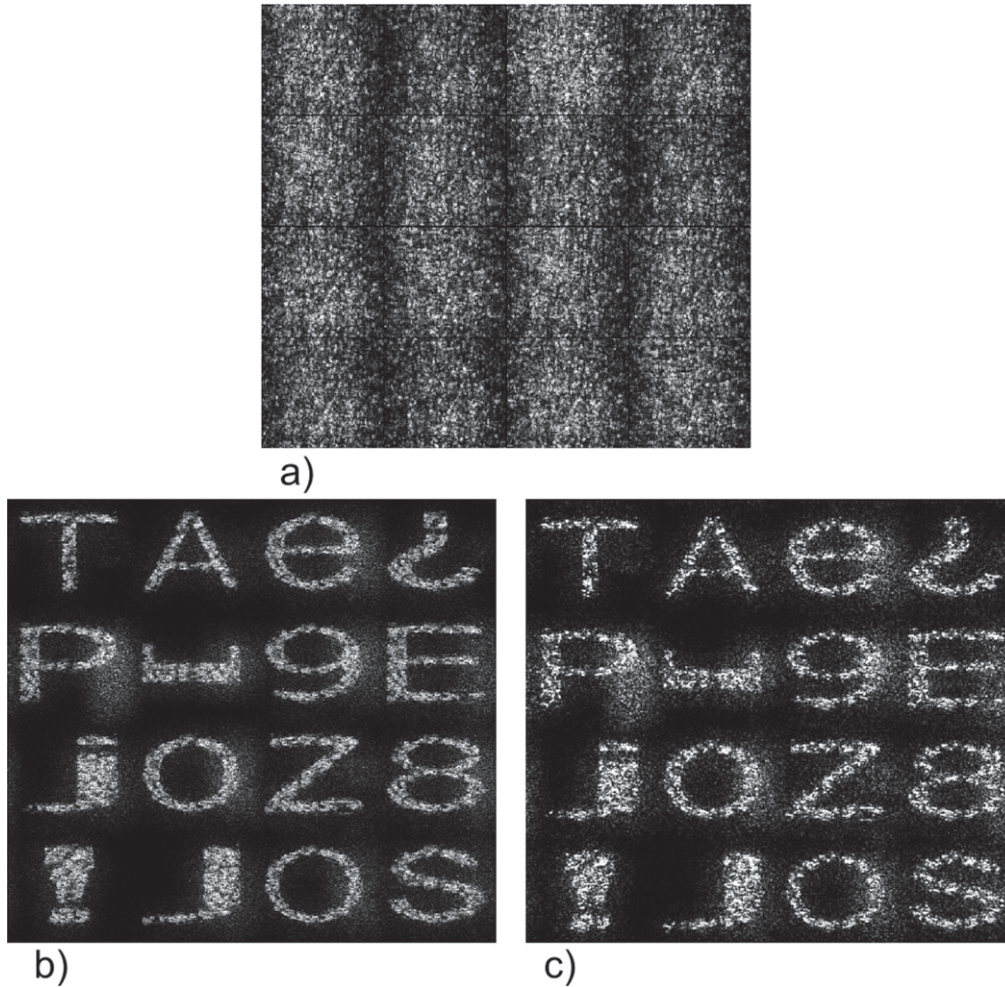


Figure 4. (a) Arrangement of 16 filtered objects in a square matrix, recovered objects from (a): (b) without optical scaling and (c) with scaling ($M = 0.5$).

4.42 MB. This means a percentage volume reduction of 94.24%.

In order to measure the error caused by the magnification procedure, we calculate the normalized mean square error (NMSE) between the data recovered from different magnifications of the matrix arrangement of figure 4(a) and the data recovered without magnification. If the recovery from the magnified matrix is $m(p, q)$ and the reference recovered from the non-magnified is $m_r(p, q)$, the NMSE is given by

$$NMSE = \frac{\sum_{p,q}^{N,M} |m(p, q) - m_r(p, q)|^2}{\sum_{p,q}^{N,M} |m(p, q) - m_w(p, q)|^2} \quad (8)$$

where (p, q) are the pixels coordinates, N and M are the number of horizontal and vertical pixels of the recovered data, and $m_w(p, q)$ is the case with minimal magnification.

As can be seen in figure 5, the error increases as the magnification decreases. Besides, there is an evident connection between image magnification and image quality as straightforwardly noted from the graphic of figure 5. This behavior can be explained by the gradual loss of spatial frequencies of the input in the optical scaling procedure as the magnification decreases. Depending on the specific frequency content of the particular input, we can expect the degradation

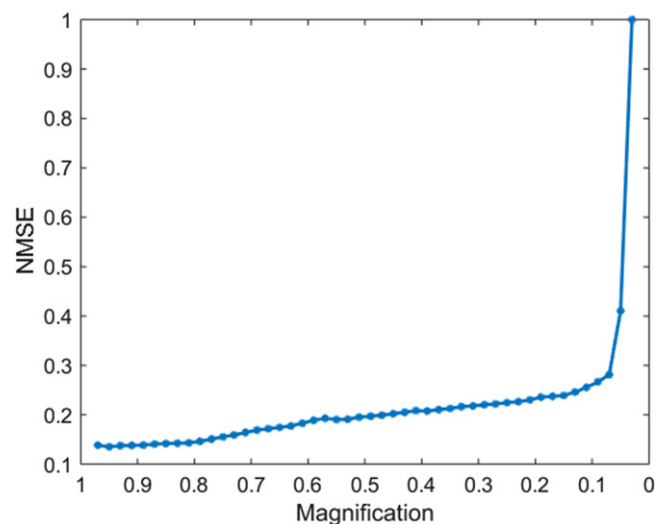


Figure 5. NMSE between the recovered data from the arrangement of figure 4(a) before and after magnification.

of quality to happen on a lower or higher magnification. In this sense there is not a general minimal achievable magnification, because it will strongly depend on the input and the parameters involved in the whole procedure.

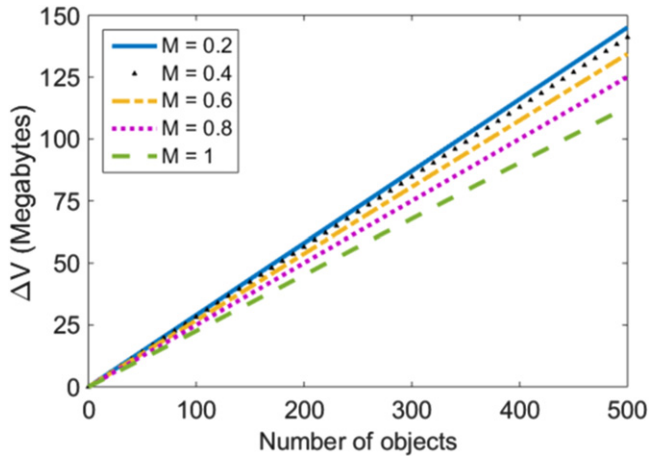


Figure 6. Dependence of ΔV on the number of objects for five M values.

We observe in figure 6 that the slope of ΔV as a function of the object number depends on the magnification. In this case, each object has the same properties as those shown in figure 4. The line corresponding to $M = 1$ shows the difference of volume when considering only the filtering process. Also, we see that the slope rate change diminishes as magnification reduces. Note that the volume reduction increases as the number of objects increases and the magnification reduces.

From figure 7, we stress that the filtering procedure sets a starting baseline of 77.18% to the volume reduction percentage. Magnification adds a further reduction from this baseline. The reduction shown in this plot is an indication of the potentials of filtering and optical scaling.

4. Conclusions

With this new optical approach, we present a strategy that improves the handling of a large volume of data. The combination of optical filtering and optical scaling steps allows formalizing the experimental technique. In order to measure the effectiveness of our method, we define the efficiency factor in terms of the parameters involved in each step. The resulting efficiency of the entire process is the product of the efficiency associated to each step. The final volume difference is a figure of merit that shows the final achievement. We would also like to emphasize that, in our demonstrations, we use experimental information and that the image reconstruction was solely based on previously known decoding techniques.

Any input can be processed as long as the experimental setup allows a proper encoding-decoding. Experimental results highlight the great potential of the method in impressively reducing the amount of data volume to be stored and transmitted. Although we introduced the experimental technique with a JTC encrypting architecture, any other optical encoding scheme can be successfully adapted to these ideas.

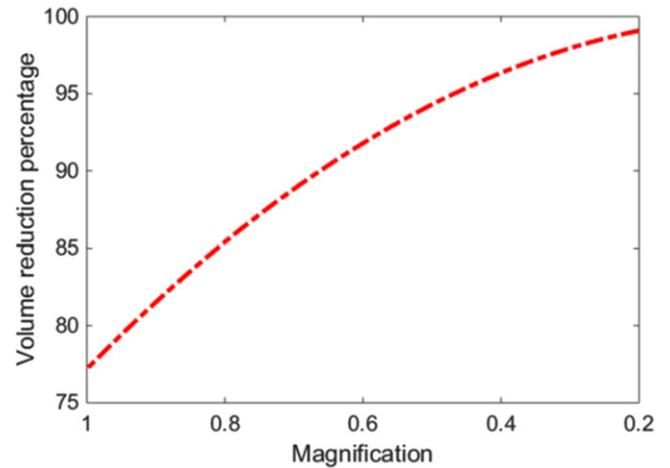


Figure 7. Percentage of volume reduction as a function of the magnification.

Handling optically encrypted images with data volume reduction techniques involving simple procedures, like the ones presented here, opens avenues for saving space in information conveying actions. This ability to form a single encrypted information unit with reduced space in managing multiplexed data opens new possibilities related to image techniques. The results obtained with a virtual optical system mean that it should be possible to implement the proposed optical protocol in an experimental optical setup, with all the advantages associated with optical processors.

This procedure can be extended to the handling of 2D and 3D multiple data in optical information processing. Even these concepts can be extended to the digital domain. Finally, we can mention that our optical techniques can be accompanied by digital techniques presented in the literature to improve data volume reduction. In this contribution, we only intend to introduce the concept, thus deferring the logical optimizations of the whole procedure to future contributions.

Acknowledgments

This research was performed under grants from Estrategia de Sostenibilidad 2014–2015 and Comité para el Desarrollo de la Investigación -CODI- (Universidad de Antioquia-Colombia), COLCIENCIAS (Colombia), MINCYT-COLCIENCIAS CO/13/05, CONICET No. 0549/12 (Argentina), and Facultad de Ingeniería, Universidad Nacional de La Plata No. 11/1168 (Argentina). John Fredy Barrera Ramírez acknowledges the support from The International Centre for Theoretical Physics (ICTP) Associateship Scheme.

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

- [2] Tajahuerce E, Matoba O, Verrall S C and Javidi B 2010 Optoelectronic information encryption with phase-shifting interferometry *Appl. Opt.* **39** 2313
- [3] Barrera J F, Mira-Agudelo A and Torroba R 2014 Experimental QR code optical encryption: noise-free data recovering *Opt. Lett.* **39** 3074
- [4] Barrera J F, Tebaldi M, Ríos C, Rueda E, Bolognini N and Torroba R 2012 Experimental multiplexing of encrypted movies using a JTC architecture *Opt. Express* **20** 3388
- [5] Trejos S, Barrera J F and Torroba R 2015 Optimized and secure technique for multiplexing QR code images of single characters: application to noiseless messages retrieval *J. Opt.* **17** 085702
- [6] Naughton T J, Frauel Y, Javidi B and Tajahuerce E 2002 Compression of digital holograms for three-dimensional object reconstruction and recognition *Appl. Opt.* **41** 4124
- [7] Darakis E and Soraghan J J 2007 Reconstruction domain compression of phase-shifting digital holograms *Appl. Opt.* **46** 351
- [8] Matoba O, Naughton T J, Frauel Y, Bertaux N and Bahram J 2002 Real-time three-dimensional object reconstruction by use of a phase-encoded digital hologram *Appl. Opt.* **41** 6187
- [9] Cucho E, Marquet P and Depeursinge C 2000 Spatial filtering for zero-order and twin-image elimination in digital off-axis holography *Appl. Opt.* **39** 4070
- [10] Velez A, Barrera J F and Torroba R 2015 One-step reconstruction of digitally assembled 3D extended holographic scenes *Opt. Laser Technol.* **75** 146
- [11] Nomura T and Javidi B 2000 Optical encryption using a joint transform correlator architecture *Opt. Eng.* **39** 2031
- [12] Barrera J F, Velez A and Torroba R 2013 Experimental multiplexing protocol to encrypt messages of any length *J. Opt.* **15** 055404