Customized data container for improved performance in optical cryptosystems

Article *in* Journal of optics · November 2016

DOI: 10.1088/2040-8978/18/12/125702

3 authors:

Alejandro Velez Zea
Centro De Investigaciones Opticas Conicet
10 PUBLICATIONS **30** CITATIONS
SEE PROFILE

John Fredy Barrera Ramírez
University of Antioquia
75 PUBLICATIONS **724** CITATIONS
SEE PROFILE

Roberto Torroba
Centro De Investigaciones Opticas (CIOp), La …
136 PUBLICATIONS **1,196** CITATIONS
SEE PROFILE

IOP Publishing Journal of Optics
J. Opt. 18 (2016) 125702 (6pp) doi:10.1088/2040-8978/18/12/125702

Customized data container for improved performance in optical cryptosystems

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

[1] Centro de Investigaciones Ópticas (CONICET La Plata-CIC-UNLP) CC N° 3, 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

E-mail: alejandrov@ciop.unlp.edu.ar

Received 8 September 2016, revised 14 October 2016
Accepted for publication 19 October 2016
Published 16 November 2016

Abstract

Coherent optical encryption procedures introduce speckle noise to the output, limiting many practical applications. Until now the only method available to avoid this noise is to codify the information to be processed into a container that is encrypted instead of the original data. Although the decrypted container presents the noise due to the optical processing, their features remain recognizable enough to allow decoding, bringing the original information free of any kind of degradation. The first adopted containers were the quick response (QR) codes. However, the limitations of optical encryption procedures and the features of QR codes imply that in practice only simple codes containing small amounts of data can be processed without large experimental requirements. In order to overcome this problem, we introduce the first tailor made container to be processed in optical cryptosystems, ensuring larger noise tolerance and the ability to process more information with less experimental requirements. We present both simulations and experimental results to demonstrate the advantages of our proposal.

Keywords: optical encryption, information container, QR codes

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

1. Introduction

Nearly two decades ago, Refregier and Jaividi [1] published their seminal work, in which they described a method for the encryption of information using an optical setup and coherent light. This method, called double random phase encoding (DRPE) revitalized the area of optical security [2]. Authors sought to leverage the many advantages of optical processing (inherent parallelism, light speed processing, properties like beam wavelength, polarization, phase, nonlinear transformations, quantum properties of photons to name a few) in order to find a new approach to encrypt, to validate and to recognize information.

This work was followed by experimental implementations, using the two architectures that would become the main focus of research, named 4 f, which was the one originally proposed by Refriegier and Javidi, and the joint transform correlator encryption (JTC) architecture [3].

Additionally, digital holography [4, 5] and optical multiplexing [6–12] were introduced to combine the capabilities of these optical systems with the flexibility of traditional computer systems, further widening the scope of the possible applications with these hybrid schemes.

However, despite these advances, challenges remained, especially concerning their security and the speckle noise found in every recovered output for all practical DRPE implementations. Regarding security, efforts range from alterations of the basic schemes by introducing nonlinear modifications [13], introducing additional encryption parameters [14], or more recently by use of alternative setups with three-dimensional encryption [15]. Other approaches include: a method using 3D space where each input image is divided into a series of particle-like points distributed in 3D space and all generated particle-like points are simultaneously encoded into a phase-only mask, achieving a higher security for optical multiple-image encryption; [16] and use of single-pixel

correlated imaging, where several random intensity patterns serve as security key ensuring increased security and flexibility, [17]. On the other hand, there have been proposals to reduce or mitigate this noise, by using, for example, the Fresnel transform to simplify the optical setup [18], or modifying the decryption procedure [19], but speckle noise continues to be an issue.

We will center our efforts on the noise problem, with the expectation that an effective method to avoid noise should be applicable to a broad range of DRPE based cryptosystem. Until now the only method available to completely avoid the noise over the recovered data was proposed and demonstrated by Barrera *et al* [20, 21]. Instead of seeking to alter the underlying encryption procedure to reduce or eliminate the speckle noise, their work proposes the use of an 'information container'. The information to be encrypted would first be introduced into this container, which is in turn processed by the DRPE system. The information container would suffer speckle contamination after recovery, like all inputs processed with the DRPE; however, the features of the container remain recognizable enough to ensure that the original data can be extracted. The encryption of the container guarantees the security of the original data, as well as its noise-free recovery. The original proposed container was a QR code, and thanks to the inherent noise tolerance of these codes [22], the decrypted QR code could be still read despite the speckle contamination, thus allowing the noise free recovery of the original data. After the introduction of the container concept, several contributions were developed using the QR codes into optical cryptosystems [23–27]. Although their use seems to be widespreading, the container concept was not explored further.

The QR codes were invented in 1994 by Denso Wave to track vehicles during manufacture [28]. Although the QR codes have been used with cryptosystems based on optical principles, as they were not designed for optical encryption their processing is challenging. As previously discussed, the container is still subject to noise contamination, and the whole method relies on ensuring that the features of the container can be identified despite this noise. QR codes have the advantage of being readable by any smartphone or camera, however, in order to achieve this, they include additional features that have nothing to do with the information contained in them (in particular, the alignment squares and the timing blocks). QR codes incorporate the Solomon–Reed error correction algorithm, in order to ensure that the information is readable even if part of the code is lost. However, noise contamination resulting from optical encryption affects the entire code uniformly. Therefore, this error correction does not increase the noise tolerance of these codes.

Due to these features of the QR code, we could expect that their performance as container in optical cryptosystems will be limited in comparison with a tailor made container that takes into account the particular features of the optical system where it will be processed.

In this work, we set out to design and implement one such container for the JTC cryptosystem as a case study, based in the following criteria: (a) the container should have low spectral bandwidth, to ensure there is little loss due to diffraction, (b) the container should have an easily controlled level of noise tolerance, to ensure optimal reading without being inefficient and (c) the container should be quickly and easily readable.

Figure 1. Proposed information container for a single character 'C'. *X* is the block size and *Y* the block separation.

2. Customized container for optical security (CCOS)

With these basic criteria in mind, we propose the new container, called CCOS as show in figure 1.

The basic CCOS is a binary 3 × 3 square arrangement of nine white square blocks with side *X*, separated a distance *Y* between them. The arrangement is surrounded by a white border that marks the container boundary. Reading is performed as follows: the code area is divided in nine equal squares. Then, the mean intensity of each square is calculated left-to-right and top-to-bottom and compared with the threshold value (in our case, the threshold was 70% the maximum intensity of the input image). A mean intensity above the threshold represents a 1 and one below a 0. In the presented codes, only 8 bits carry data, and the ninth is ignored. The ASCII standard is used to codify traditionally used symbols into 8 bit values to be stored into the codes and to decode the obtained values into symbols after reading. The reading software used was written in MATLAB.

This CCOS satisfies all our basic criteria for an optimal container. First, its spectral content can be deduced from the size and separation between blocks, which in the case when all blocks are 1 and their size equal to their separation will be the same as a 2D Ronchi grating. Secondly, the size of the blocks is directly related to the noise tolerance. The mean intensity of each block region does not vary significantly when block sizes are large compared to the speckle size, allowing easy reading. Only when the speckle size is equal or larger than the block size we expect reading to fail. And finally, the reading of the CCOS is achieved with three simple operations with little computational cost: a division of the code area in nine squares, a calculation of the mean intensity of each square, and a comparison of these mean intensities to a threshold value to determine the value of each bit.

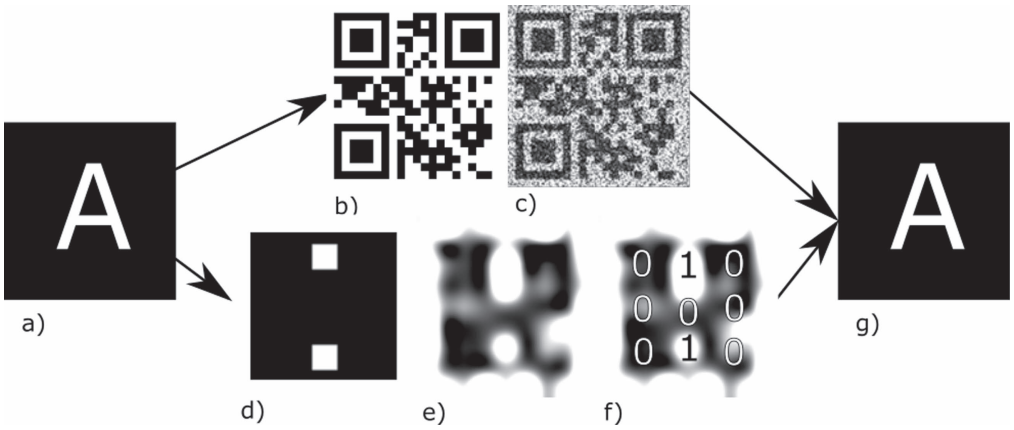

Figure 2. (a) Input data, (b) QR code of the input data, (c) QR code shown in (b) after encryption–decryption with object window of 150 × 150 pixels, (d) original CCOS of input data, and (e) code shown in (d) after encryption–decryption with window size 9 × 9 pixels, (f) lecture of the CCOS, and (g) recovered data from (c) and (e).

3. Test cryptosystem description

In order to test the effectiveness of our proposal, we now present several tests, both simulated and in a laboratory environment, where we will compare the performance of a QR code as a container versus that of the CCOS, when both are processed by the same JTC cryptosystem.

In the JTC cryptosystem, two windows separated a distance $2a$ are placed in the focal plane of a convergent lens, in contact with a random phase mask (in a laboratory setup this phase mask is provided by a ground glass). In the conjugate plane of the lens, there is an intensity recording medium.

One of the windows on the input plane is empty, thus letting light go through to be modified by the phase mask. This will be the encryption key. The object to be processed is placed in the other window.

Thus, our intensity recording medium registers the intensity of the interference between the Fourier transform (FT) of both windows, called the joint power spectrum, given by

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

where * means complex conjugate; $C(u, v)$ is the FT of $o(x_0, y_0)r_1(x_0, y_0)$, with $o(x_0, y_0)$ the object to be encrypted, $r_1(x_0, y_0)$ is a random phase function representing a phase mask, and $R_2(u, v)$ is the FT of the encoding key $r_2(x_0, y_0)$, which is another random phase mask.

By performing the FT of equation (1), we can isolate its fourth term, and discard the rest, and by performing the inverse Fourier transform (IFT), we obtain the encrypted object [25].

$$E(u, v) = C(u, v)R_2{}^*(u, v). \tag{2}$$

Attempting to recover the original data by performing the IFT will result in a convolution between $o(x_0, y_0)r_1(x_0, y_0)$ and $r_2(x_0, y_0)$, and since $r_2(x_0, y_0)$ is a random function, this convolution will appear as white noise. In order to recover the original data, it is necessary to perform the product between equation (2) and $R_2(u, v)$, and then apply the IFT.

4. Numerical results of QR code and CCOS performance comparison

Using the described cryptosystem, we codified the letter 'A' (figure 2(a)) into a QR (figure 2(b)) code and a CCOS (figure 2(d)) using a simulated JTC cryptosystem, and sought the minimal size necessary to recover a legible container after decryption.

As we demonstrate in figure 2(c), the minimal window size needed for recovery of a readable QR code after decryption is 150 × 150 pixels, while for a CCOS is only 9 × 9 (figure 2(e)). Although this decrypted CCOS seems to be severely degraded, lecture (figure 2(f)) yields the data corresponding to the correct message without noise (figure 2(g)). The small number of pixels needed to process a CCOS compared with a QR code allows for processing the same input in a more compact optical setup.

We also note that data sets larger than 9 bits can be codified by performing arrangements of several CCOSs. To show this, we codify the same 144-character message (figure 3(a)) into an arrangement of CCOS (figure 3(b)) and a QR code (figure 3(e)), and process them with our JTC cryptosystem.

In figure 3(d) we see that the decrypted CCOS can be recognized easily, ensuring successful reading (figure 3(f)). The QR code containing the same message suffers significant degradation when processed with the same window size (figure 3(e)), and its reading fails. These results demonstrate that the same optical setup can process messages coded as CCOS that could not be successfully processed as QR codes.

Next we measure the resistance to data loss of both the QR codes and CCOS. In order to do this, we encrypt both a CCOS and a QR code from figures 2(a) and (c) with the same window size, and proceed to introduce an increasing percentage of random data loss to the encrypted codes. We then measure the normalized mean square error (NMSE)

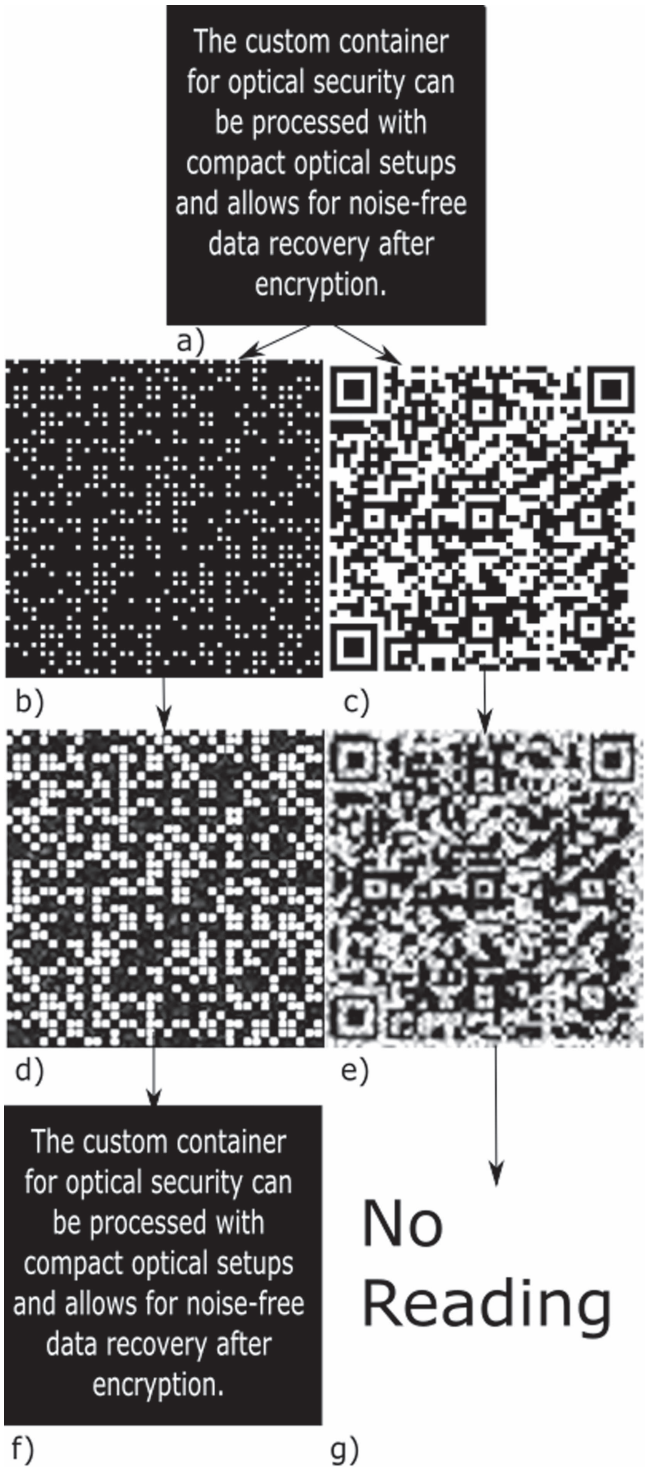

Figure 3. (a) Input message, (b) input codified into a CCOS, (c) input codified into a QR code, (d) decrypted from (b) with a window size of 72 × 72 pixels, (e) decrypted from (c) with a window size of 72 × 72 pixels, and (f) reading of (d), and (g) failed reading of (e).

between the decrypted code with and without data loss. The NMSE between the recovered code without noise $I(m, n)$, and with a percentage p of data loss $I_p(m, n)$ is defined as

$$\mathrm{NMSE} = \frac{\sum_{m,n}^{N,M} |I(m, n) - I_p(m, n)|^2}{\sum_{m,n}^{N,M} |I(m, n) - I_w(m, n)|^2}, \quad (3)$$

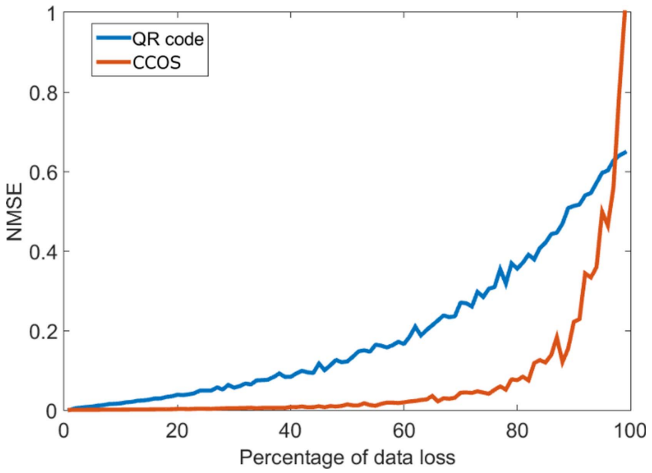

Figure 4. NMSE between the decrypted codes of the letter A with and without data loss and the same window size.

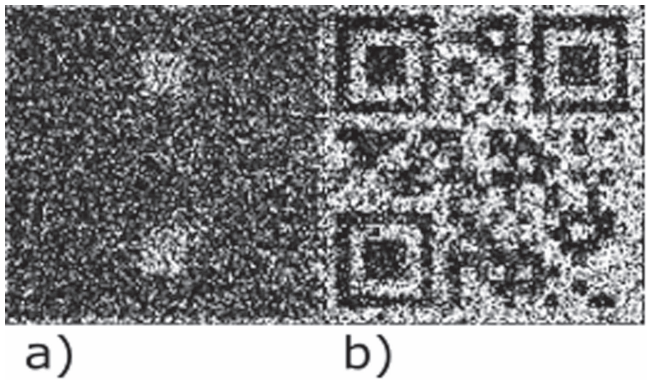

Figure 5. (a) Worst readable CM with 92% data loss and (b) worst readable QR code with 60% data loss.

where (m, n) are the pixel coordinates, $M \times N$ is the number of pixels of the recovered code, and $I_w(m, n)$ is the worst expected case.

In figure 4 the resulting NMSE is shown. For the same percentage of data loss, the CCOS presents lower error than the QR code. Additionally, when testing readability, the CCOS remains readable up to 92% of data loss, against 60% for the QR code, as show in figure 5. These results show using the same optical setup, CCOS allow for processing more data or processing the same data as a QR code with higher data loss tolerance.

5. Experimental results

Now we proceed to test the performance of the two codes in an actual laboratory environment, using the scheme of figure 6. All experimental results in this paper were carried out using a CMOS EO-10012C camera, with a pixel size of 1.67 × 1.67 μm and 3480 × 2748 pixels resolution. The object and the key windows were projected using a spatial light modulator HOLOEYE LC2000, with a pixel size of 32 × 32 μm. The lens focal length was 200 mm.

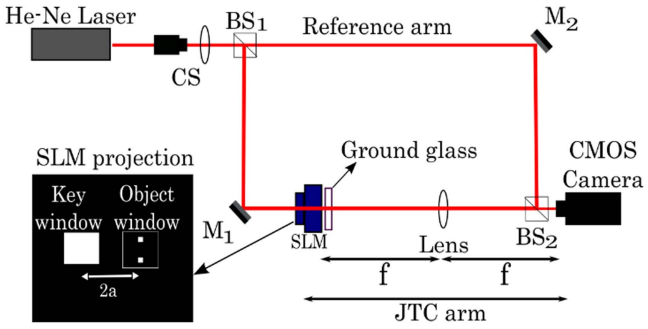

Figure 6. Scheme of the laboratory setup. BS: beam splitter, M: mirror, SLM: spatial light modulator, f: lens focal length, CS: collimation system.

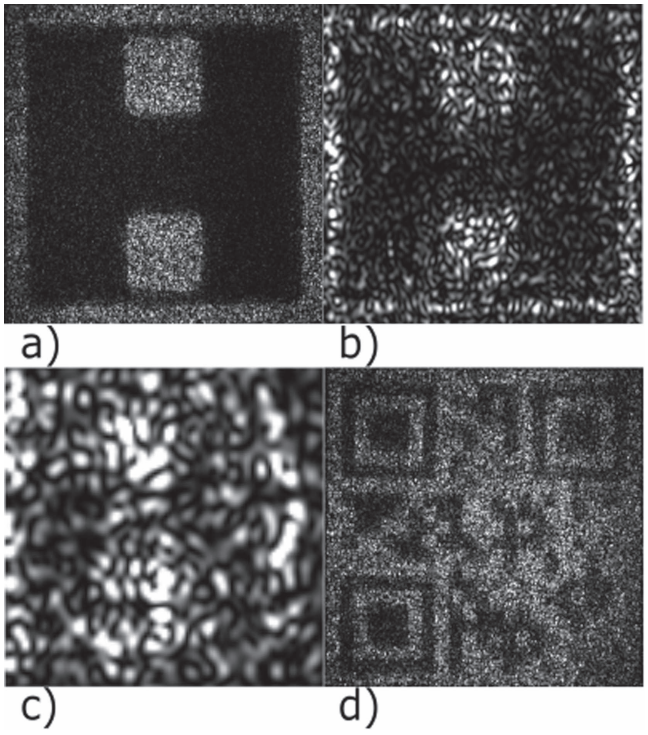

Figure 7. Experimental encryption–decryption results of letter A: (a) CCOS with size 6.4 × 6.4 mm^2, (b) CCOS with size 1.6 × 1.6 mm^2, (c) CCOS with size 0.64 × 0.64 mm^2, and (d) QR code with size 6.4 × 6.4 mm^2.

The interferometric scheme of figure 6 is necessary in order to record the key window data as a hologram. Now we proceed to encrypt both the CCOS and the QR code, using increasingly smaller window sizes, in order to find the minimum size that can be processed and still be readable.

In figure 7 we show experimental results of the encryption–decryption processes of both the CCOS and the QR code of letter A. Using the maximum available area in our experimental setup, the CCOS can be easily read (figure 7(a)) while the QR code cannot (figure 7(d)). In general, QR codes are difficult to process in actual laboratory conditions, and thus many contributions limit themselves to simulations, including post processing algorithms or even processing them into multiple pieces [29]. When the area of the CCOS is reduced to a fourth of the maximum possible size it remains readable (figure 7(b)). The minimal area required by the CCOS after encryption–decryption with our setup was found to be 0.64 × 0.64 mm^2 (figure 7(c)). Although at this size the CCOS is severely degraded, the difference in block mean intensity is enough to ensure reading. This result further highlights the increased effectiveness of the CCOS over QR codes as an information container for our test setup.

6. Conclusions

The customized container for optical security allows for a large enhancement in noise tolerance, increasing the amount of information to be protected with an optical cryptosystem and then recovered free of any kind of degradation. Also, this proposal ensures an important reduction in the setup requirements to process a specific data set and a high data loss tolerance, while maintaining all the advantages of the underlying optical cryptosystem unaltered. It is evident that a tailor made information container offers great potential for optical security techniques that were considered of limited application due to presence of noise and the restriction in the amount of data that could be processed simultaneously. It can be concluded that customized containers will allow for the design of high performance optical security systems. We believe that additional work is needed in order to explore the concept of information container and the relationship between the input characteristics and the output quality in optical security systems like the JTC.

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), MINCyT-COLCIENCIAS CO/13/05, CONICET Nos. 0849/16 and 0549/12 (Argentina), and Facultad de Ingeniería, Universidad Nacional de La Plata No. 11/I215 (Argentina). John Fredy Barrera Ramirez acknowledges support from The International Centre for Theoretical Physics ICTP Associateship Scheme.

References

[1] Refregier P and Javidi B 1995 Optical image encryption based on input plane and Fourier plane random encoding *Opt. Lett.* **20** 767
[2] Javidi B *et al* 2016 Roadmap on optical security *J. Opt.* **18** 083001
[3] Nomura T and Javidi B 2000 Optical encryption using a joint transform correlator architecture *Opt. Eng.* **39** 2031
[4] 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] Rueda E, Barrera J F, Henao R and Torroba R 2009 Optical encryption with a reference wave in a joint transform correlator architecture *Opt. Commun.* **282** 3243

[6] Amaya D, Tebaldi M, Torroba R and Bolognini N 2009 Wavelength multiplexing encryption using joint transform correlator architecture *Appl. Opt.* **48** 2099
[7] Situ G and Zhang J 2005 Multiple-image encryption by wavelength multiplexing *Opt. Lett.* **30** 1306
[8] Barrera J F, Henao R, Tebaldi M, Bolognini N and Torroba R 2006 Multiplexing encrypted data by using polarized light *Opt. Commun.* **260** 109
[9] 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
[10] Rueda E, Rios 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
[11] Barrera J F, Henao R, Tebaldi M, Torroba R and Bolognini N 2006 Multiple image encryption using an aperture modulated optical system *Opt. Commun.* **261** 29
[12] Guohai S and Jingjuan Z 2006 Position multiplexing for multiple-image encryption *J. Opt. A: Pure Appl. Opt.* **8** 391
[13] Vilardy J M, Millán M S and Perez-Cabré E 2013 Improved decryption quality and security of a joint transform correlator-based encryption system *J. Opt.* **15** 025401
[14] Vilardy J M, Torres Y, Millan M S and Perez-Cabre E 2014 Generalized formulation of an encryption system based on a joint transform correlator and fractional Fourier transform *J. Opt.* **16** 125405
[15] Velez A, Barrera J F and Torroba R 2016 Three-dimensional joint transform correlator cryptosystem *Opt. Lett.* **41** 599
[16] Chen W 2016 Optical multiple-image encryption using three-dimensional space *IEEE Photonics J.* **8** 6900608
[17] Chen W 2016 Optical data security system using phase extraction scheme via single-pixel detection *IEEE Photonics J.* **8** 7801507
[18] Barrera J F, Jaramillo A, Velez A and Torroba R 2016 Experimental analysis of a joint free space cryptosystem *Opt. Laser Eng.* **83** 126
[19] Barrera J F, Velez A and Torroba R 2014 Experimental scrambling and noise reduction applied to the optical encryption of QR codes *Opt. Express* **22** 20268
[20] Barrera J F, Mira A and Torroba R 2013 Optical encryption and QR codes: secure and noise- free information retrieval *Opt. Express* **21** 5373
[21] Graydon O 2013 Cryptography: quick response codes *Nat. Photon.* **7** 343
[22] Barrera J F, Mira A and Torroba R 2014 Experimental QR code optical encryption: noise-free data recovering *Opt. Lett.* **39** 3074
[23] Deng X 2015 Optical image encryption based on real-valued coding and subtracting with the help of QR code *Opt. Commun.* **349** 48
[24] Qin Y, Wang H, Wang Z, Gong Q and Wang D 2016 Encryption of QR code and grayscale image in interference-based scheme with high quality retrieval and silhouette problem removal *Opt. Lasers Eng.* **84** 62
[25] Qin Y and Gong Q 2014 Optical information encryption based on incoherent superposition with the help of the QR code *Opt. Commun.* **310** 69
[26] Wang X, Chen W and Chen X 2015 Optical information authentication using compressed double-random-phase-encoded images and quick-response codes *Opt. Express* **23** 6239
[27] 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
[28] ISO/IEC 18004: 2006. *Information Technology. Automatic Identification and Data Capture Techniques. QR Code* 2005
[29] Barrera J F, Rueda E, Rios 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