Experimental scrambling and noise reduction applied to the optical encryption of QR codes

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

[1]*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*

[2]*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*

**john.barrera@udea.edu.co*

Abstract: In this contribution, we implement two techniques to reinforce optical encryption, which we restrict in particular to the QR codes, but could be applied in a general encoding situation. To our knowledge, we present the first experimental-positional optical scrambling merged with an optical encryption procedure. The inclusion of an experimental scrambling technique in an optical encryption protocol, in particular dealing with a QR code "container", adds more protection to the encoding proposal. Additionally, a nonlinear normalization technique is applied to reduce the noise over the recovered images besides increasing the security against attacks. The opto-digital techniques employ an interferometric arrangement and a joint transform correlator encrypting architecture. The experimental results demonstrate the capability of the methods to accomplish the task.

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

References and links

1. P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. **20**(7), 767–769 (1995).
2. T. Nomura and B. Javidi, "Optical encryption using a joint transform correlator architecture," Opt. Eng. **39**(8), 2031–2035 (2000).
3. G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption system that uses phase conjugation in a photorefractive crystal," Appl. Opt. **37**(35), 8181–8186 (1998).
4. N. K. Nishchal and T. J. Naughton, "Flexible optical encryption with multiple users and multiple security levels," Opt. Commun. **284**(3), 735–739 (2011).
5. A. Alfalou and C. Brosseau, "Optical image compression and encryption methods," Adv. Opt. Photon. **1**(3), 589–636 (2009).
6. B. Hennelly and J. T. Sheridan, "Optical image encryption by random shifting in fractional Fourier domains," Opt. Lett. **28**(4), 269–271 (2003).
7. S. Liu and J. T. Sheridan, "Optical encryption by combining image scrambling techniques in fractional Fourier domains," Opt. Commun. **287**, 73–80 (2013).
8. J. F. Barrera, E. Rueda, C. Rios, M. Tebaldi, N. Bolognini, and R. Torroba, "Experimental opto-digital synthesis of encrypted sub-samples of an image to improve its decoded quality," Opt. Commun. **284**(19), 4350–4355 (2011).
9. J. F. Barrera, A. Mira, and R. Torroba, "Optical encryption and QR codes: Secure and noise-free information retrieval," Opt. Express **21**(5), 5373–5378 (2013).
10. J. F. Barrera, A. Mira-Agudelo, and R. Torroba, "Experimental QR code optical encryption: noise-free data recovering," Opt. Lett. **39**(10), 3074–3077 (2014).
11. Z. Ren, P. Su, J. Ma, and G. Jin, "Secure and noise-free holographic encryption with a quick-response code," Chin. Opt. Lett. **12**(1), 010601–010604 (2014).
12. A. Alfalou, M. Elbouz, A. Mansour, and G. Keryer, "New spectral image compression method based on an optimal phase coding and the RMS duration principle," J. Opt. **12**(11), 115403 (2010).
13. A. Alfalou, A. Mansour, M. Elbouz, and C. Brosseau, "Optical compression scheme to multiplex and simultaneously encode images," in *Optical and Digital Image Processing Fundamentals and Applications*, G. Cristobal, P. Schelkens, and H. Thienpont, eds. (Wiley, 2011).
14. J. M. Vilardy, M. S. Millán, and E. Perez-Cabre, "Improved decryption quality and security of a joint transform correlator-based encryption system," J. Opt. **15**(2), 025401 (2013).

#210067 - $15.00 USD Received 16 Apr 2014; revised 25 Jul 2014; accepted 29 Jul 2014; published 14 Aug 2014

15. O. Graydon, "Cryptography: Quick response codes," Nat. Photonics **7**(5), 343 (2013).
16. ISO, IEC 18004: 2006, "Information technology - Automatic identification and data capture techniques – QR Code 2005 bar code symbology specification," International Organization for Standardization, Geneva, Switzerland (2006).

1. Introduction

Transforming the original input into stationary white-noise data is the major achievement for optical encryption methods protecting stored information. The potentials were readily proved in security schemes [1–11]. The most used scheme is the double random phase mask, by means of two statistical independent pure random phase masks. The simplest double random phase mask scheme implies to position one mask in the input plane and the other one in the Fourier plane [1]. Other possibilities that increase the security of the system were successfully explored [4–7]. Also, subsampling and multiplexing techniques [8] and compression methods [12, 13] have been implemented to improve the global performance of the encrypting systems. In encryption procedures, input data must be encoded in such a way that only the use of the correct key in the decryption step reveals the original data.

Now we present a novel information encryption method for digital images based on joint transform correlator (JTC) encoding methods and scrambling techniques. This is an opto-digital procedure applied to a complex object, previously piecewise divided to avoid the natural resolution limit imposed by any diffraction limited optical system. The use of the nonlinear modification during the decoding step allows a remarkable noise reduction. An additional security level is also introduced with the scrambling method, requiring an extra decoding key to correctly recover the original input object. The scrambling technique is used to rearrange the sections of the encrypted image by using a specified scrambling rule.

To meet the challenges arising from a variety of applications, robust encryption of digital information is extremely necessary. Therefore, using our procedure a higher security is achieved. Furthermore, the encrypted image is robust against noise and distortion. The flexibility of this method is demonstrated both theoretically and experimentally. Scrambling is performed by dividing a given input and applying limited steps of primary matrix transformations, causing the pieces to be displaced [6, 7]. One could not obtain any information about the original image from the scrambled image, but the original image can be retrieved by repositioning the disturbed image according to a special order. Image scrambling techniques are important image encoding methods applied to digital image processing, information hiding, and digital watermarking to enhance information security [6, 7]. Because successful image reconstruction needs the correct scrambling path parameters, the scrambling techniques can be protected by the secret parameters. Although the methods perform well, external keys are needed for the image reconstruction, and some distortion may be found in reconstructed images.

A common element of the optical encrypting techniques based on double random phase encoding is the random noise presented in the decrypted images [9, 10]. Independently of the encrypted object (a character, a code, an image, etc), it is a challenge to reduce the random noise presented in an actual optical encrypting system. In order to achieve a noise reduction over the decrypted images, Vilardy *et al* [14] analyzed some reported methods that optically implement the double random phase encoding (DRPE) in a JTC. They concluded that it is possible to significantly improve the quality of the decrypted image by introducing a simple nonlinear operation in the encrypted function that contains the joint power spectrum (JPS). This nonlinearity consists in dividing the JPS by the squared magnitude of the Fourier transform of the security key. With this nonlinearity, the encryption JTC system approaches better the implementation of DRPE as it was proposed originally by Nomura and Javidi [2]. There is no need to make the optical setup more complicated because a conventional JTC is adequate for the implementation of the whole process. Besides, the nonlinear operation allows an enhancement in the security of the encrypted image, enabling the encrypted image to be robust against chosen-plaintext attacks [14]. The proposed nonlinear-modified encryption

#210067 - $15.00 USD Received 16 Apr 2014; revised 25 Jul 2014; accepted 29 Jul 2014; published 14 Aug 2014

method still benefits from the easier optical implementation of contributions [7, 8]. In addition to this, it keeps the same amount of information to be transmitted since the resulting encrypted function has the same size as its original counterpart and only requires one key for decryption.

There are two questions concerning optical encryption: 1) would it be possible to keep the protecting properties the optical methods bring without getting speckle-contaminated results due to the optical processing?, and 2) would it be possible to reach a wider public with an instrument readily at hand of almost everyone, then making the decoded result widely available without the need of accessing a computer?. We find the answers in a proposal that allows taking advantage of the security capabilities of optical systems and at the same time alleviates the effects of the inherent speckle noise introduced by the optical processing [9–11]. In this method, the information to be encrypted is codified in an information "container", and then this "container" is encrypted with one of the usual optical protocols. The appropriate "container" is a quick response (QR) code [15], both noise resistant and available to almost anyone. Smartphones or tablets with the appropriate application can read QR codes. Inherently, QR codes are tolerant to speckle noise. As expected, after a right recovering procedure the speckle noise will affect the decrypted QR code. But due to the inherent tolerance to noise of the QR codes, the speckle introduced by the optical processing in the encrypting and decrypting procedures does not affect the ability to read the information stored in the decrypted QR code. Therefore, if we can two-fold protect the container using a scrambling technique, and also reducing the speckle noise over the decrypted QR code, we are still offering a practical and safe solution with a far better performance, and enhancing the security level.

2. General procedure behind encrypting and recovering processes

The interferometric arrangement is shown in Fig. 1, where one of its arms is a JTC encrypting setup and the other carries a plane reference wave. The input of the JTC encryption arm contains two apertures as illustrated by Fig. 1, one with the input object information (Object window) attached to a random phase mask, while the other aperture (Key window) contains the second random phase mask or key code mask. In order to realize experimentally the input procedure, we place a ground glass completely covering the input plane, therefore generating the input of the JTC encrypting architecture.

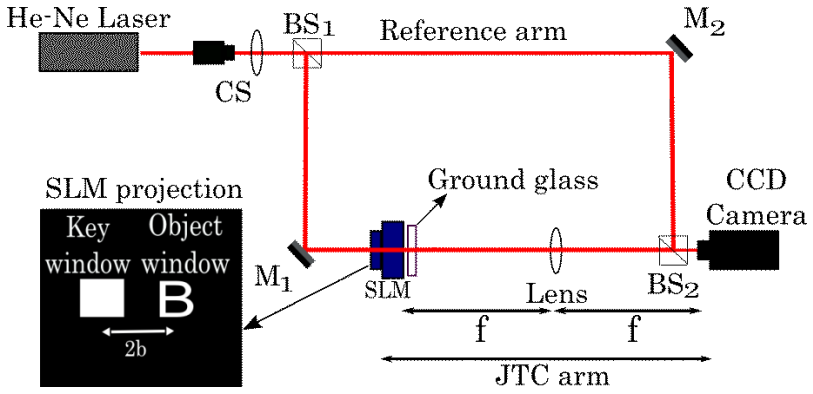

Fig. 1. Experimental setup (CS: collimation system, BS_1 and BS_2: beam splitters, M_1 and M_2: mirrors, SLM: spatial light modulator, f: focal distance of the lens).

According to the scheme depicted in Fig. 1 a lens performs the Fourier transform (FT) of a given input object on the CCD camera. The result is the recording of the JPS of this input [8],

#210067 - $15.00 USD Received 16 Apr 2014; revised 25 Jul 2014; accepted 29 Jul 2014; published 14 Aug 2014

$$JPS(u,v)=\left|C(u,v)\right|^2+\left|R_2(u,v)\right|^2+C^*(u,v)R_2(u,v)\exp(-4\pi ibu)+C(u,v)R_2^*(u,v)\exp(4\pi ibu) \quad (1)$$

where $2b$ is the separation between the object and the key, * means complex conjugate; $C(u,v)$ is the FT of $o(x_0,y_0)r_1(x_0,y_0)$, with $o(x_0,y_0)$ the single entry to be encrypted, $r_1(x_0,y_0)$ is a random function representing a phase mask, and $R_2(u,v)$ is the FT of the encoding key $r_2(x_0,y_0)$. The first two terms in Eq. (1) are filtered by subtracting the intensities of the FT of the key and the FT of the product between the input object and the random phase mask $r_1(x_0,y_0)$. Afterwards, the third term is filtered and after positioning the fourth term (x',y') the encrypted object is obtained [8],

$$E(u,v)=C(u,v)R_2^*(u,v)\exp\left[2\pi i(x'u+y'v)\right] \quad (2)$$

The decryption process requires the FT of security key $R_2(u,v)$, we proceed to block the object window and simultaneously to unblock the reference arm. Therefore, we have four terms and proceeding as above, we can filter the DC terms, eliminating one of the diffracted terms and the remaining one is positioned at coordinates $(0,0)$, resulting in [8],

$$L(u,v)=R_2(u,v) \quad (3)$$

This last equation represents the decoding key. We digitally multiply Eq. (2) and Eq. (3) resulting, after performing an inverse FT, in the recovering of the object

$$d(x,y)=o(x,y)r_1(x,y)\otimes\left[r_2^*(-x,-y)\otimes r_2(x,y)\right]\otimes\delta(x-x',y-y') \quad (4)$$

where adopting the approximation $r_2^*(-x,-y)\otimes r_2(x,y)\approx\delta(x,y)$ (see Ref [3].),

$$i(x,y)=o(x,y)r_1(x,y)\otimes\delta(x-x',y-y') \quad (5)$$

At this point, it is worth to mention that each (x',y') position belonging to the decrypted information is controlled during the encoding procedure.

3. Scrambling

An interesting application to this procedure is found in connection with problems involving image resolution. Our proposal allows a trade-off between optical and digital processing complexity, and it can be used in applications where more conventional imaging approaches have difficulty meeting resolution requirements [8]. If we were restricted to take a single record of the original input of Fig. 2(a), using the setup of Fig. 1, we get after processing the result depicted in Fig. 2(b), showing little resemblance with the original. The reason is mainly due the limited resolution in the optical setup. However, if the object was divided into 36 sections as schemed in Fig. 2(c), we can test the practical advantages of dividing the object in pieces in comparison with using the whole object as input, following the procedure of this section. We present the results in Fig. 2(f), with a remarkable difference compared to Fig. 2(b). Therefore, we adequately recover the input data, thus avoiding a major resolution restriction imposed by the optical system. To cope with the limit of resolution shown in Fig. 2(b), we divide the input object $o(x_0,y_0)$ into $N=36$ sections $o_m(x_0,y_0)$ as in Fig. 2(c). Every part is encrypted in the same way as in the object as a whole (Eq. (1) and Eq. (2)) getting each encrypted part as

$$E_m(u,v)=C_m(u,v)R_2^*(u,v)\exp\left[2\pi i(x_mu+y_mv)\right] \quad (6)$$

#210067 - $15.00 USD Received 16 Apr 2014; revised 25 Jul 2014; accepted 29 Jul 2014; published 14 Aug 2014

with $m = 1, 2, 3, ..., N$ and $C_m(u,v)$ the FT of $o_m(x,y) r_1(x,y)$. If an authorized user is in possession of the encrypted sections and the security key (Eq. (3)), by following

$$i_m(x,y) = o_m(x,y) r_1(x,y) \otimes \delta(x - x_m, y - y_m) \tag{7}$$

where each part is obtained in the same output plane spatial position given by coordinates (x_m, y_m).

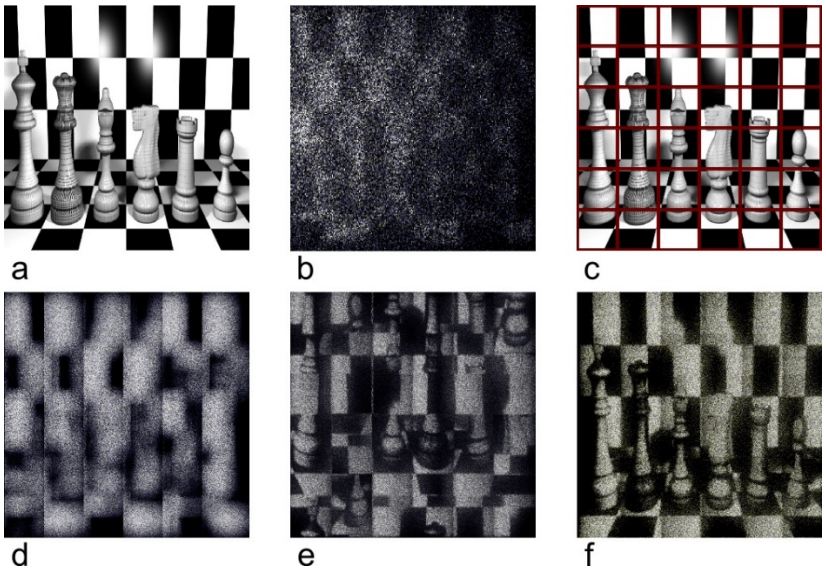

Fig. 2. (a) Original input (image taken from Txemi Jendrix inspiriens, http://www.txemijendrix.com), (b) input recovered without subdivision, (c) input divided into 36 pieces, (d) output with the wrong optical key, (e) result using the right optical key, but not having the scrambling key, and (f) input recovered with the optical and the scrambling keys.

We now proceed to add an additional security measure, known as scrambling. Scrambling is performed by dividing the original image into several sections and displacing the position of the sections according to a pre-defined random or pseudo-random rule, in such a way that the original information be undistinguishable if the reversing process is unknown. Object recovery is achievable only by having the rule that gives the proper positions or the seed used to randomize the coordinates.

In our proposal a scrambling procedure can be implemented, assigning randomly the coordinates during the filtering step. As explained above, each encrypted part of the QR code has an exponential term that contains the coordinates (x_m, y_m) (Eq. (6)). Then, the spatial position of each decrypted part is given by these coordinates (Eq. (7)). In the conventional procedure, the coordinates (x_m, y_m) for each encrypted part are chosen to recover the decrypted parts $o_m(x,y)$ in the spatial positions that allow recombining the original QR code. In our scrambling procedure, the coordinates (x_m, y_m) corresponding to each encrypted QR part are permutated using a random number generator. This permutation represents the scrambling key. Therefore, it is not possible to reassemble the original object even in possession of the right decoding key.

The recovering step consists in using the decoding key to obtain the decrypted QR sections. The final step is reassembling the object from these decrypted sections. We need the scrambling key to accomplish this task, which links the original positions of the sections with

#210067 - $15.00 USD Received 16 Apr 2014; revised 25 Jul 2014; accepted 29 Jul 2014; published 14 Aug 2014

the scrambled positions (x_m, y_m). Each decrypted part $o_m(x, y)$ is redirected as to recombine the original object. Without the right security key, even in possession of the correct scrambling key, we obtain the object shown in Fig. 2(d), while in the inverse case we get the result of Fig. 2(e). Only in possession of both keys we recover the object of Fig. 2(f). We highlight that the decryption and reassembling processes for each part can be carried out in a virtual optical system, after introducing the optical and scrambling keys.

In general, the degree of the object recognition depends on the number of pieces in which the object is divided. Increasing the number of pieces induces a corresponding increase in the security, although at the same time increases the complexity of the method. Nevertheless, the procedure to solve the low-resolution issue, allowed us to implement naturally the object division and repositioning, and in turn leading to the scrambling technique.

As introduced in a previous publication [9], the great advantage of encrypting QR codes, used as information "containers", is obtaining noise-free information from the reading of a noisy QR decrypted code. If we also add as an extra feature the scrambling procedure, we are reinforcing the counterfeit measurements, as QR codes do not admit the minimum scrambling of their sections. When trying to read a scrambled QR code, nothing is retrieved. For the scrambling, we perform a random permutation of the pieces assigned to each matrix element. If the scrambling process is unknown, the decryption reveals an image of the same size as the original, but the information remains hidden due to the disordering of the pieces. We illustrate through the sequential images of Fig. 3 the scrambling technique over the decrypted QR code, in a way that it is not possible to read the information therein contained. A scrambling process applied to a QR code previously divided in few pieces does not allow its reading. Moreover, as the information contained in the QR code increases, the more increases the complexity of its structure, making it difficult to detect the original form.

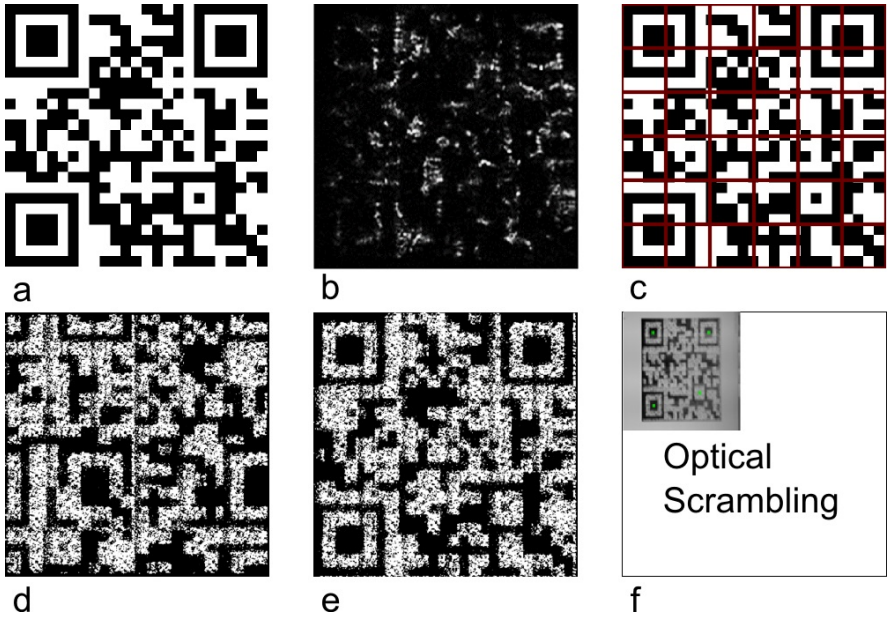

Fig. 3. (a) original QR code containing the message "Optical scrambling", (b) QR code processed in a single step, (c) QR code (a) divided into a matrix of 6x6 elements, (d) QR code recovered with the optical key, but not having the scrambling key, (e) QR code recovered with the appropriate keys and (f) result from reading (e) using a smartphone.

In Fig. 3(a) we present the QR code of the message "Optical Scrambling", made with a software freely available on the Internet. The retrieved image of Fig. 3(b) shows the result of

#210067 - $15.00 USD Received 16 Apr 2014; revised 25 Jul 2014; accepted 29 Jul 2014; published 14 Aug 2014

a single step process, without scrambling. Although the QR code is noise resistant, any attempt to read this result fails to reconstruct the message. On the other hand, by performing the QR code division and proceeding with our proposed protocol including scrambling, using the right optical key, but not introducing the scrambling key, we get the image depicted in Fig. 3(d). Due to the properties of the QR coding, a scrambled QR code cannot be read [16]. Therefore, the information contained in the decrypted QR code of Fig. 3(d) is not retrieved. If the scrambling key remains unknown, the information contained in the decrypted and scrambled QR code cannot be recovered. Thus, the scrambling key represents an additional requirement in the recovering process increasing the global security of the method.

Finally, if besides the right optical decoding key, also the proper descrambling key is used, we get the image of Fig. 3(e), which in spite of the visible speckle noise arising from the QR code encryption; the reading brings back the message contained in the decrypted QR code, as seen in Fig. 3(f). The experiments confirmed our theoretical predictions and allowed comparisons to the single step approach, showing that a better resolution capability can have a dramatic impact on the overall procedure. Besides we increase the security level by scrambling, profiting from the possibility of repositioning separately each decrypted piece.

4. Noise reduction

Basic optical encrypting systems provide a trustful approach for protecting data. Yet we observe that the decoded outputs present speckle noise, thus somehow degrading the original input condition. Even though QR codes are noise resistant, there is certain degree of noise that affects their reading. Taking into account this fact, and considering that QR codes become more structured when containing more information, it is important to adopt an additional noise reduction technique to get recovered QR codes with better quality. Let us then analyze the cause of such noise. During the decryption step, we perform the multiplication of the encoding mask with its complex conjugate; the encoding mask is represented by a complex function, with an amplitude part that remains after multiplying, and contributing to increase the noise in the decrypted image.

In [14], Vilardy *et al* propose a nonlinear modification to overcome the above-mentioned drawback. Instead of sending the encrypted object Eq. (2), we send it but divided by the intensity of the FT of the key,

$$N(u,v) = \frac{E(u,v)}{\left|R_2(u,v)\right|^2} \cdot R_2(u,v) \tag{8}$$

Singularities in the points where the intensity of the key is zero are avoided by substituting them with a small constant [14]. In this way, the major noise contribution caused by the real part of the key is reduced, thus improving the quality of the result. Then, after a FT we directly get,

$$i(x,y) = o(x,y) r_1(x,y) \tag{9}$$

It is interesting to note that in this case we do not adopt the approximation mentioned before Eq. (5). Additional comments on this feature: 1) this is the first time this method is experimentally implemented; 2) noise reduction is accomplished by a simple division operation besides increasing the resistance against attacks as already demonstrated [14], and 3) easy implementation as we do not require any additional experimental data because we already have $\left|R_2(u,v)\right|^2$.

In Fig. 4 we compare the case where images Fig. 4(a) and Fig. 4(b) present the object decrypted under the usual technique, and Fig. 4(c) and Fig. 4(d) the result applying the nonlinear correction. A simple visual comparison reveals the improvement. With this result, we prove that the suggested method helps in reducing the speckle noise without increasing the complexity of the decoding operation.

#210067 - $15.00 USD Received 16 Apr 2014; revised 25 Jul 2014; accepted 29 Jul 2014; published 14 Aug 2014

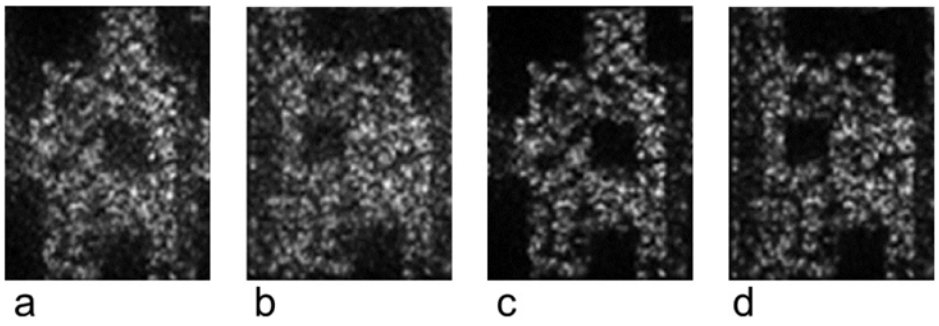

Fig. 4. Recovering images: (a) and (b) with both appropriate optical and scrambling keys, (c) and (d) including the nonlinear method.

Figure 5 describes the example of a QR code made for letter "B", where in (a) we find the QR reconstruction after encrypting and scrambling, using the right keys. As noted, speckle noise covers most part of the image. In Fig. 5(b) we perform the nonlinear noise reduction technique. After reading the QR code of Fig. 5(b) with a standard smartphone, we get Fig. 5(c). As a QR code consists of black and white blocks arranged in a square grid, the noise reduction allows a better block discrimination. Letter "B" is clearly seen without any kind of distortions. Note that images of Figs. 4(a) and 4(b) correspond to sections of Fig. 5(a); while Figs. 4(c) and 4(d) correspond to sections of Fig. 5(b).

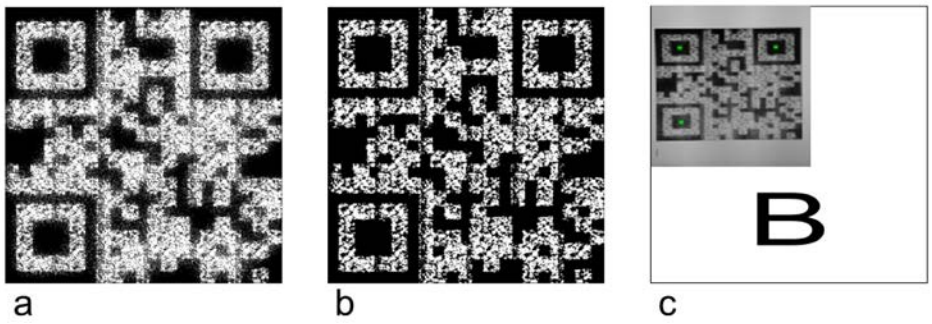

Fig. 5. Protocol applied to a QR code with the letter "B"; (a) result recovered with both correct keys, (b) result retrieved adding the nonlinear noise reduction technique, and (c) smartphone reading from (b).

In order to evaluate the performance of the nonlinear method, we calculate the normalized mean square error (NMSE) for the right recovering of the QR code corresponding to the letter "B" (Fig. 5(a) and Fig. 5(b)). The NMSE between the original QR code of Letter "B" $I(m,n)$, and the retrieved QR code $I'(m,n)$ is defined as

$$NMSE = \frac{\sum_{m,n}^{M,N} \left| I(m,n) - I'(m,n) \right|^2}{\sum_{m,n}^{M,N} \left| I(m,n) - I_w(m,n) \right|^2} \tag{10}$$

where (m,n) are the pixels coordinates, $M \times N$ is the number of pixels of the recovered QR code, and $I_w(m,n)$ is the decrypted QR code using the conventional procedure. As expected from the normalization, the NMSE of the decrypted QR code using the conventional method is 1.00 (Fig. 5(a)) while the NMSE in the nonlinear case is 0.97 (Fig. 5(b)). These

#210067 - $15.00 USD Received 16 Apr 2014; revised 25 Jul 2014; accepted 29 Jul 2014; published 14 Aug 2014

NMSE values demonstrate the noise reduction achieved when implementing the nonlinear method.

Additionally, we compare the noise resistance during transmission both in the nonlinear and the conventional methods. We calculate the NMSE for the case when adding random 8 bit noise to the encrypted sections of the QR code of the message "Optical Scrambling". In this case, $I(m,n)$ is the original QR code of the message "Optical Scrambling", $I'(m,n)$ is the retrieved QR code when there are different percentages of noise over the encrypted sections and $I_w(m,n)$ is the worst expected case.

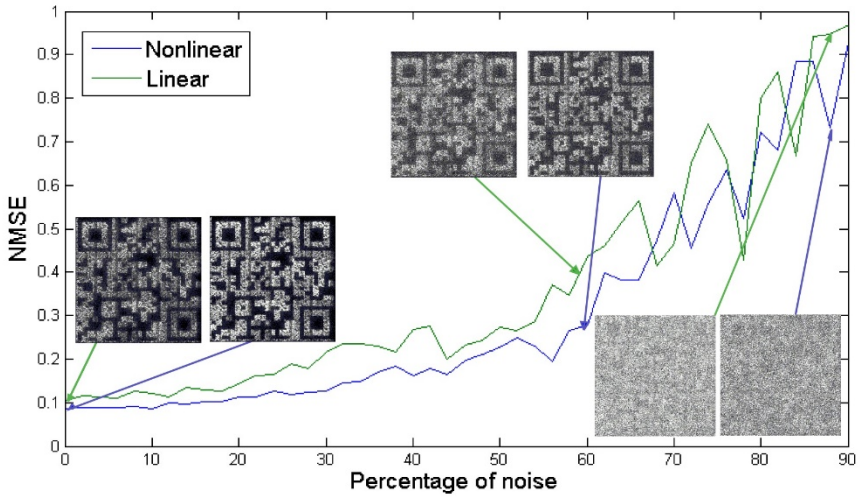

Fig. 6. NMSE curves as a function of the percentage of random noise affecting the encrypted sections of the QR code of the message "Optical scrambling".

The curves of Fig. 6 are a quantitative proof of the noise reduction attained using the nonlinear approach. The recovered QR codes corresponding to 0%, 60% and 86% of noise for the conventional and nonlinear methods are included in Fig. 6. The values of the NMSE in the conventional case for 0%, 60% and 86% of noise are 0.1048, 0.3476 and 0.9457, respectively. While in the nonlinear method the corresponding values are 0.0849, 0.2657 and 0.7324. It should be noted, however, that over a NMSE of 70%, large fluctuations in the curves are appreciated. A natural consequence of this comparison shows that noise tolerance of the nonlinear method is similar to the conventional method while the nonlinear method keeps a lower NMSE due to noise reduction. This behaviour remains in the region where the random noise over the decrypted QR is not dominant, that is in the region where the noise is lower than 70%. The indented images are the visual evidence of the decrease in the noise when using the nonlinear method.

All experimental results in this paper were carried out in the scheme of Fig. 1. We use a CMOS EO-10012M camera, with a pixel size of 1.67x1.67 μm and 3480x2748 pixels resolution. The object and the key windows were projected using a spatial light modulator HOLOEYE LC2000, with a pixel size of 32x32 μm. Both object and key windows have the same size 3.2 mm x 3.2 mm and the distance between both windows is 3.84 mm.

5. Conclusions

Summarizing, we present two techniques to improve optical encryption-decryption using an experimental JTC architecture in a holographic digital scheme. First, a piecewise division of the input object allows not only alleviating the system resolution limits, but also implementing a scrambling method as an extra security layer requiring a key to complete the

#210067 - $15.00 USD Received 16 Apr 2014; revised 25 Jul 2014; accepted 29 Jul 2014; published 14 Aug 2014

object assembling. Second, we use a nonlinear technique to reduce the natural speckle noise. With this last feature, we also add an extra security measure against eavesdropping. The combination of these improvements favored specially the QR codes use as "containers" of the original message. We are delivering the optimal outcome, even under worst circumstances of high speckle noise acting on the QR code. Besides, scrambling allows an additional security level, without increasing the complexity of the method. The experiments demonstrated the potentials and effectiveness of the procedure, thus supporting the proposal.

Acknowledgments

This research was performed under grants of CODI (Universidad de Antioquia-Colombia), COLCIENCIAS (Colombia), the International Centre for Theoretical Physics ICTP Associateship Scheme, CONICET No. 0863/09 and No. 0549/12 (Argentina), and Facultad de Ingeniería, Universidad Nacional de La Plata No. 11/I168 (Argentina).

#210067 - $15.00 USD Received 16 Apr 2014; revised 25 Jul 2014; accepted 29 Jul 2014; published 14 Aug 2014