

Optimized and secure technique for multiplexing QR code images of single characters: application to noiseless messages retrieval

Sorayda Trejos¹, John Fredy Barrera¹ and Roberto Torroba²

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 Óptica (CONICET La Plata-CIC) and UID OPTIMO, Facultad de Ingeniería, Universidad Nacional de La Plata, PO Box 3, C.P 1897, La Plata, Argentina

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

Received 13 February 2015, revised 10 June 2015

Accepted for publication 11 June 2015


Published 31 July 2015



CrossMark

Abstract

We present for the first time an optical encrypting–decrypting protocol for recovering messages without speckle noise. This is a digital holographic technique using a $2f$ scheme to process QR codes entries. In the procedure, letters used to compose eventual messages are individually converted into a QR code, and then each QR code is divided into portions. Through a holographic technique, we store each processed portion. After filtering and repositioning, we add all processed data to create a single pack, thus simplifying the handling and recovery of multiple QR code images, representing the first multiplexing procedure applied to processed QR codes. All QR codes are recovered in a single step and in the same plane, showing neither cross-talk nor noise problems as in other methods. Experiments have been conducted using an interferometric configuration and comparisons between unprocessed and recovered QR codes have been performed, showing differences between them due to the involved processing. Recovered QR codes can be successfully scanned, thanks to their noise tolerance. Finally, the appropriate sequence in the scanning of the recovered QR codes brings a noiseless retrieved message. Additionally, to procure maximum security, the multiplexed pack could be multiplied by a digital diffuser as to encrypt it. The encrypted pack is easily decoded by multiplying the multiplexing with the complex conjugate of the diffuser. As it is a digital operation, no noise is added. Therefore, this technique is threefold robust, involving multiplexing, encryption, and the need of a sequence to retrieve the outcome.

 Online supplementary data available from stacks.iop.org/JOPT/17/085702/mmedia

Keywords: QR codes, optical packaging, image processing, digital holography, multiplexing

1. Introduction

In recent years, optical encryption has shown remarkable development [1–56]. Since the first report on the double random phase encoding (DRPE) technique [1, 2], further remarkable progress was published, including a generalization to 3D keys [3]. Later, an optical DRPE method using a joint transform correlator architecture was proposed and

successfully implemented [4]. In this encrypting architecture, the conjugate of the encrypted key is not required to recover the original information. Overviews show some important advances that illustrate the evolution of the subject [5, 6]. Among new highly developed areas, we can mention QR code optical encryption [7–18], video optical encryption [19–24], structured masks [25–27], asymmetric security systems [28–33], cryptosystems analysis [34–42], and multiplexing

techniques [43–56], to name a few. Specifically, QR codes have driven great attention due to their resistance to noise, among other characteristics, making them highly appropriate to serve as ‘information containers’. Optical encryption and QR coding have been successfully merged to protect information [7, 8]. For security purposes, the information to be protected is encoded into a QR code, and, instead of the original information, this QR code is in turn encrypted. As expected in optical encrypting techniques, the rightly decrypted QR code contains noise. Scanning the noisy decrypted code renders the original data to the final user; he/she receives the pertinent information without the noise arising in the traditional optical encrypting techniques. QR codes offered a practical solution to the noise present over decrypted images, thus releasing a valid actual alternative to solve the problem, besides making more attractive the use of optical encrypting techniques, as QR codes can be scanned by smartphones or tablets with the appropriate program [8, 11, 12].

The insertion of a QR code as an ‘information container’ in optical encryption was introduced for the first time by Barrera *et al* [7]. In this pioneer contribution, the information to be encrypted is transformed into a QR code, and then the QR code is encrypted with a DRPE technique in a $4f$ architecture. The decrypted QR code contains noise due to the optical processing with an optical encrypting arrangement that includes random phase masks. Finally, the decrypted QR code is scanned using a smartphone, rendering the original information free of any kind of noise. This contribution merges QR coding and optical encryption to demonstrate a secure and a noise-free management of information employing widely used technological tools [8].

Nevertheless, to fully profit from the QR code characteristics outside the encryption procedures, we need to further improve the reading capabilities under more severe conditions. Therefore, some ‘cleaning’ methods were developed to get a better reading from polluted QR codes for existing market apps (Android, Apple, etc) available to the common user [9, 10]. The experimental demonstration of the QR optical encryption was performed using a joint transform correlator *JTC* encrypting architecture [9]. As the implementation is not possible in a single step due to the limit of resolution of the optical system, a multiplexing procedure to encrypt QR codes is added. Once the QR code is rightly decrypted and scanned, the original information is recovered free from noise and using the most basic, fast, and free available software [9]. This contribution represents the first experimental demonstration of the QR code optical encryption. Afterward, two techniques to reinforce the QR code optical encryption were presented [10]. First, the inclusion of an experimental scrambling technique in the encrypting protocol adds more protection to the security proposal. Additionally, a nonlinear normalization technique is applied to reduce the noise over the recovered QR codes, besides increasing the security against attacks [51, 52]. The combination of these improvements favored specially the QR codes use as ‘containers’ of the original data.

This novel application revitalized traditional optical encrypting methods; further, it represents an advance in presenting a practical tool, which can be massively used, and solving the drastic issue of the ever-present noise altering the outcome. Motivated by this new approach, several applications came forward, such as multidimensional keys [13], phase retrieval [14, 15], and incoherent superposition [16], to name a few. Also, the QR coding was even adapted for validation purposes [17, 18].

Regardless the input to a given optical system, we always face the problem of image resolution. Besides determining if we are using coherent light sources, we have the intrusion of the speckle phenomenon and both produce corresponding image deterioration. A practical partial solution to this problem is found in the contribution of Barrera *et al* [53]. It is an experimental protocol to visualize images that otherwise would have been barely recognizable due to the above-mentioned issues. This protocol is based on an optical image synthesis with digital holography using enlarged sub-samples of an entire image together with a multiplexing technique. As a result, they get smaller speckle patterns on the final assembled image and a spatial frequency enhancement with respect to the input image obtained with the conventional procedures. This enhancement allows us to implement a protocol to process, in a secure manner, messages of any length employing a *JTC* encrypting processor [54]. The correct retrieving of the message requires the individual encryption of several characters, a multiplexing procedure to obtain an encrypted keyboard, and a selection-position key that gives the right sequence. The experimental results show the feasibility of the proposal, representing an actual application of the optical encrypting protocols. Although optical encryption has achieved huge popularity due to its great range of possible applications, some protocols, procedures, and even the optical encrypting processors must be improved to represent an actual tool with a real potential for commercial purposes. In order to further reduce the optical architecture normally involved in optical processing, in particular in the above-mentioned technique, an optical packaging and encrypting (SOPE) procedure [55] is employed. Although intended for encryption purposes, its use can be extended to other practical image-handling approaches. An interferometric architecture with a simple $2f$ optical processor in one arm and a corresponding reference beam in the other allows recording several processed data; then, after digital processing, the data are filtered, repositioned, and multiplexed. During recovery, all processed information is displayed in the same plane employing a friendly retrieving procedure. This procedure allows the packaging of multiple entries in a single unit without introducing image superposition or cross-talk. This protocol can also be performed using a theta modulation procedure over each part of processed data before multiplexing, assuring the recovering of all data without superposition [56].

The constant improvement of optical components and the advances in optical processing has made the achievement of a new style of optical information handling possible, by using digital holographic techniques together with the packaging of

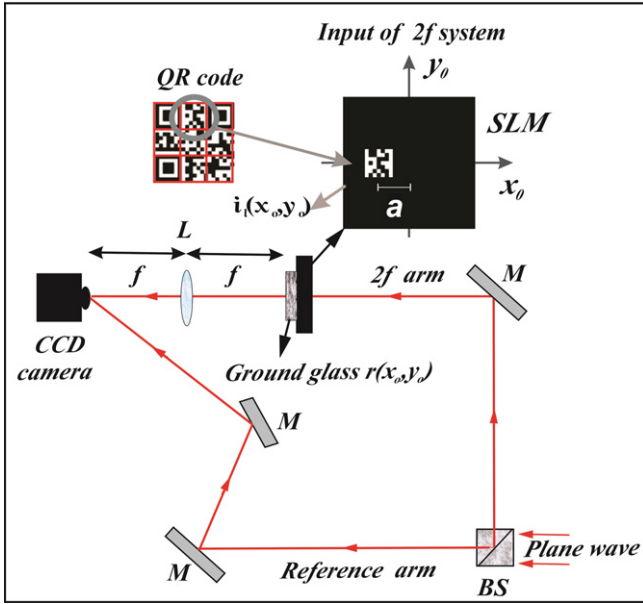


Figure 1. Interferometric setup to register the holograms of the processed QR code sections (BS: beam splitter, M: mirror, SLM: spatial light modulator, L: Lens of focal length f).

multi-images and its final encryption. This type of optical information handling is used and implemented in this paper in an actual application with great potential, namely a panel made with QR codes for each letter. In the present approach, each letter is transformed into a QR code and then, to avoid any optical resolution problem, we subdivide the QR codes into portions. Afterward, portions are displayed in a spatial light modulator (SLM) covered by a diffuser. A hologram is obtained and digitally stored for each portion. Posteriori filtering, repositioning, and adding operations compose the multiplexing. This procedure represents the first reported multiplexing of encrypted QR codes. To offer another strengthening step, we digitally multiply the pack by a random phase mask, thus making a simple encrypting mechanism. The pack and decryption random mask are sent once to the user, while the sequence ordering the codes can be changed according to the delivered message. Once the QR codes are recovered, then by the most basic, fast, and free available software on the Internet, the message is obtained without the noise associated with optodigital processing. This technique represents end-user benefits whenever there is an efficient combination of the optical security methods and the digital procedures.

2. Basic processing for every QR code

This section describes and illustrates the process performed for a single QR code. As the optical processing of a QR code is not possible in a single step, due to the limit of resolution of the optical system [9, 53], the code is divided into nine equal-size portions, where each one is located in the entrance plane of a $2f$ setup. For the experimental realization, each QR code section is attached to a random phase mask. An

interferometric setup allows us to record the hologram of the optically processed data, as depicted in figure 1. The input plane of the $2f$ optical processor is described by

$$q_I(x_0, y_0) = [i_I(x_0, y_0)r(x_0, y_0)] \otimes \delta(x_0 - (-a), y_0) \quad (1)$$

where $i_I(x_0, y_0)$ is the QR section projected in a SLM, the ground glass placed behind the SLM is represented by the random phase mask $r(x_0, y_0)$, \otimes means convolution, $\delta()$ is the Dirac delta function, and $|a|$ is the distance between the QR section and the optical axis in the input plane. We illuminate this input with a monochromatic plane wave, and we get at the output plane the processed QR code section:

$$Q_I(u, v) = FT \left\{ [i_I(x_0, y_0)r(x_0, y_0)] \otimes \delta(x_0 - (-a), y_0) \right\} \quad (2)$$

The expression $FT \{ \}$ denotes the Fourier transform (FT) operation. At this step, we can deduce from equation (2) that the object spectrum will be spread in a wider area in the output plane.

Then, the optically processed QR code section is holographically recorded using the interferometrical arrangement of figure 1. The interferogram registered in the CCD camera is mathematically represented by

$$\begin{aligned} I_I(u, v) &= |Q_I(u, v)|^2 + |P(u, v)|^2 \\ &+ Q_I^*(u, v)P(u, v) \exp(-2\pi i \alpha u) \\ &+ Q_I(u, v)P^*(u, v) \exp(2\pi i \alpha u) \end{aligned} \quad (3)$$

where $*$ means complex conjugate, $P(u, v) = \exp[2\pi i(\alpha u f + \beta v f)]$ represents the reference plane wave written in frequency coordinates $u = x_0/\lambda f$ and $v = y_0/\lambda f$ where $\alpha = \cos \theta/\lambda$ and $\beta = \cos \phi/\lambda$, and $\cos \phi$ are the directional cosines, and λ is the wavelength. Then, we filtered the terms of no interest in equation (3). For this purpose, we register separately the terms $|P(u, v)|^2$ and $|Q_I(u, v)|^2$ by blocking the $2f$ arm and the reference arm, respectively. The procedure up to this point is experimentally developed, and from now on, we perform digital operations. Subtracting these last two terms from equation (3) we obtain

$$\begin{aligned} S_I(u, v) &= Q_I^*(u, v)P(u, v) \exp(-2\pi i \alpha u) \\ &+ Q_I(u, v)P^*(u, v) \exp(2\pi i \alpha u) \end{aligned} \quad (4)$$

From equation (4), we want to only retain one term. Then, we proceed to perform the FT of equation (4) to get two spatially separated terms:

$$\begin{aligned} t_I(x', y') &= q_I^*(x', y') \otimes \delta(x' + \alpha \lambda f, y' + \beta \lambda f) \otimes \delta(x' + a, y') \\ &+ q_I(x', y') \otimes \delta(x' - \alpha \lambda f, y' - \beta \lambda f) \otimes \delta(x' - a, y') \end{aligned} \quad (5)$$

The separation between the terms in equation (5) is proportional to $|a|$, which is controlled during the projection of the QR code section on the SLM. The value of $|a|$ is carefully selected to prevent any kind of superposition between these two terms.

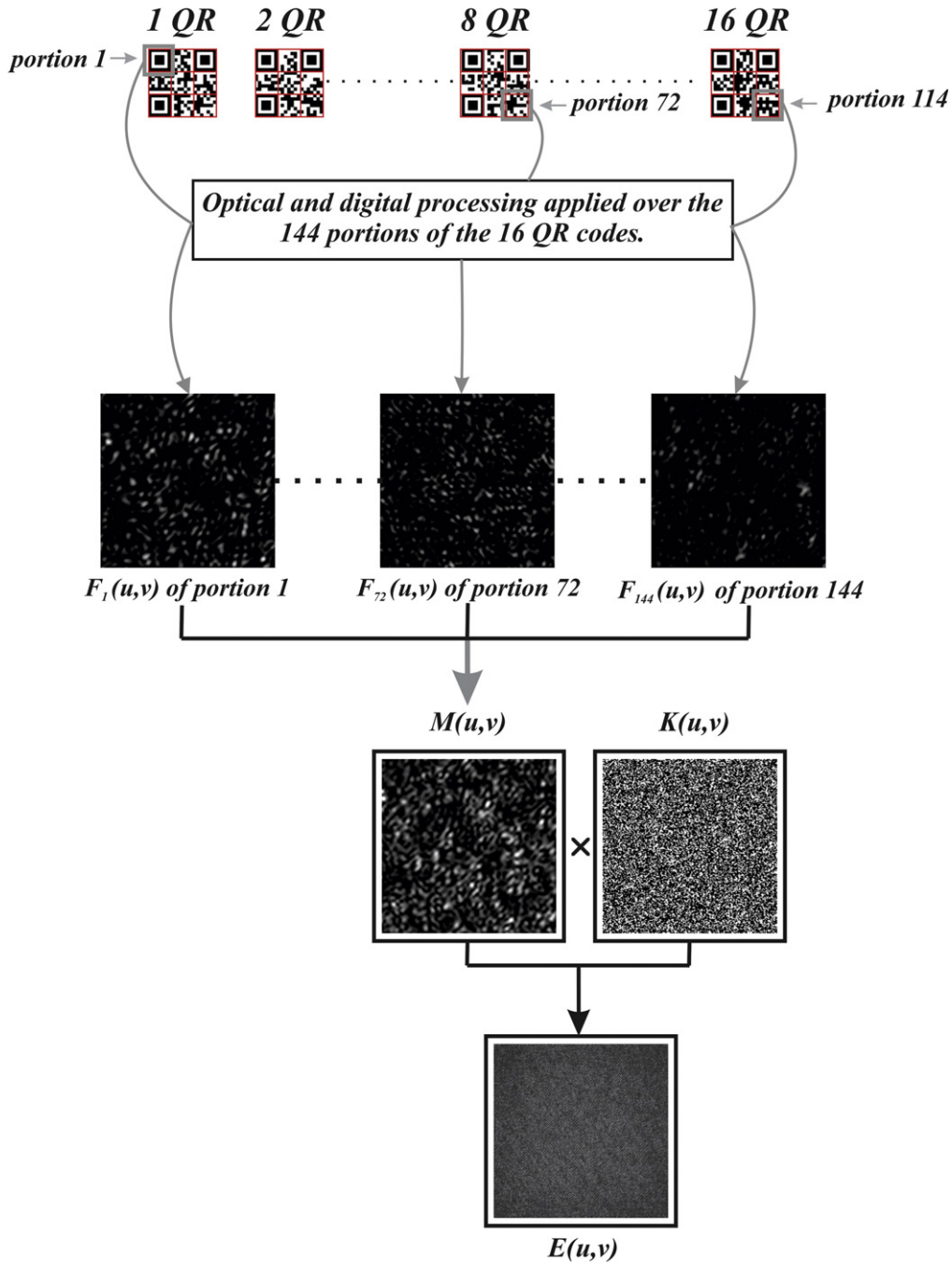


Figure 2. Processing, multiplexing, and encrypting of 144 QR codes portions.

Then, the first term of equation (5) is removed by filtering and the remaining term is repositioned around a desired coordinate (x_l, y_l) , then we apply an inverse FT to complete the filtering process [55]:

$$F_l(u, v) = Q_l(u, v) \exp[2\pi i(x_l u + y_l v)] \quad (6)$$

This last equation represents the optodigital processed QR portion (see figure 2). The positioning at coordinates (x_l, y_l) allow us to locate the recovered data in any desired position in the output plane, as we want to process multiple QR codes and recover them without superposition.

3. Multiple data processing and encryption

In this case, 16 QR codes are processed. As each QR code is divided in nine portions, 144 QR portions are processed individually by the optical system, filtered, and positioned digitally, as discussed in section (2), getting so for every single portion its respective function $F_l(u, v)$.

The multiplexing is a practical tool to manage multiple data without altering the optical setup or introducing other elements, becoming a practical solution for processing QR codes. Therefore, once all data is optodigital processed, a multiplexing operation is applied to generate

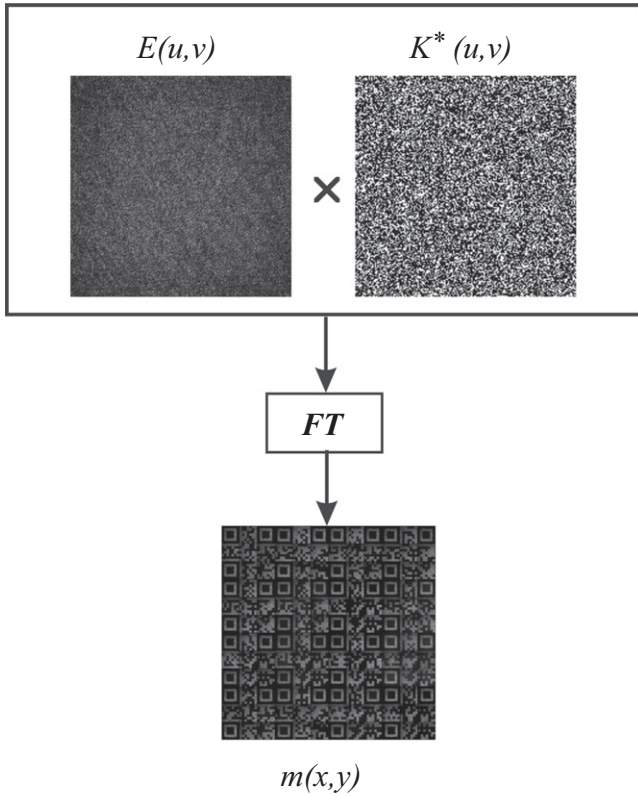


Figure 3. Scheme for decrypting, recovering, and displaying the package of QR codes.

a single information unit $M(u, v)$. As we process 144 sections (equation (6)), the optical package is expressed as:

$$M(u, v) = \sum_{l=1}^{144} F_l(u, v) = \sum_{l=1}^{144} Q_l(u, v) \exp[2\pi i(x_l u + y_l v)] \quad (7)$$

Multiplexing allows the easily handling of the sent information, as instead of separately sending each processed data, we send a single package containing all processed data. During processing of each portion, the coordinates (x_l, y_l) are carefully chosen to assure a correct reassembly when retrieving all portions. As a final step, we protect the package using one random digital phase mask $K(u, v)$ (see figure 2), which acts as the encrypting key. Accordingly, by a digital multiplication of $M(u, v)$ and $K(u, v)$, we get the encrypted package:

$$E(u, v) = M(u, v)K(u, v) \quad (8)$$

This result and the complex conjugate of the key $K^*(u, v)$ are sent separately to users in remote locations. The end user performs a multiplication between the encrypted data and the complex conjugate of the key, and with a subsequent FT operation, the hidden codes are recovered in the imposed positions. The recovering of all processed QR codes is

represented as:

$$m(x, y) = \sum_{l=1}^{144} q_l(x, y)k(x, y) \otimes \delta(x - x_l, y - y_l) \quad (9)$$

The QR codes are displayed in one step, in the same plane, and at the same time. As $K(u, v)$ is a random phase mask, it vanishes when we record the intensity of $m(x, y)$ to get the intensity of the recovered portions $|q_l(x, y)|^2$. Note that our experimental technique does not imply setup alterations. We want to emphasize that the new scheme is neither a $4f$ nor a JTC architecture, although it uses two phase masks to protect the information. In this contribution, we use a $2f$ architecture (only one lens), where the masks are placed at the input plane and at the Fourier plane of the lens. Meanwhile, the $4f$ system consists of two lenses of focal length f , therefore the distance between input and output planes is $4f$ [1]. The first encoding mask is positioned at the input plane and the remaining mask at the first Fourier plane (at a distance f from the first lens). Regarding the JTC encrypting architecture, it uses one lens in order to encrypt the information, but the object and the two encrypting masks are placed at the input plane [4].

Contrasting other methods, where all data are first encrypted and then multiplexed [24, 32, 46, 50], in our proposal we start by processing multiple data, then multiplex and finally encrypt them in a single step by a multiplication with the second key.

4. Experimental results

In the experimental arrangement, we use a solid-state laser operating at a wavelength of 632 nm. A diffusing glass is placed in contact in the SLM to provide the random phase mask. The size of the projected object into the SLM is 6.4×6.4 mm. The SLM is a Holoeye LC2002, whose pixel size is $32 \mu\text{m}$. The distance $|a|$ between the object and the optical axis in the input plane is 5.6 mm.

The SLM is placed at a distance f of a positive lens L of focal length $f=200$ mm and the CCD camera is placed so that the distance between the lens and the sensor is equal to f (see figure 1). The camera size is 3840×2748 pixels and the pixel size is $1.67 \times 1.67 \mu\text{m}$.

For the experimental realization, 144 portions were handled (16 QR codes), where each portion was optodigitally processed according to the description of section (2) and (3). After the experimental and digital steps, we obtain the processed QR codes ready to be encrypted with the encoding mask as described previously. It is important to remark that the multiplexing contains the information of all managed QR codes. In order to recover the original QR codes, it is necessary to cancel the effect of the encrypting key and perform a FT operation (see figure 3). From the last operation, we get the QR codes, which are not free of speckle. From a practical point of view in a security system, one of its main requirements is that the recovering process should be friendly

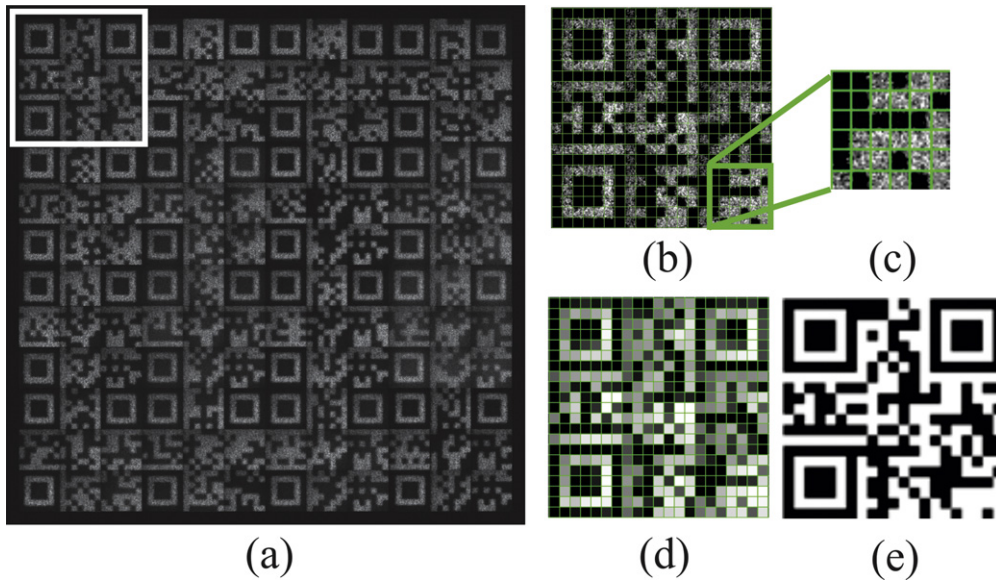


Figure 4. (a) Panel containing all recovered QR codes after using the appropriate recovering procedure, (b) one QR code of the panel corresponding to the white square in (a), (c) magnified inset box of a section of (b), (d) average value of each block in (c) (between 0 and 255), and (e) decrypted QR code after the process of binarization.

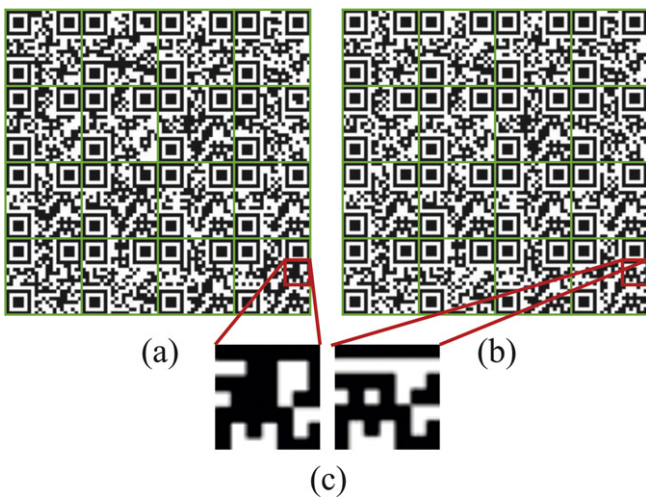


Figure 5. Panel with (a) the processed and binarized QR codes and (b) the original QR codes, and (c) the zooming of one portion of a QR code in (a) and the zooming of its corresponding section in (b).

to the final user. Although the processing of the QR codes involves several optical and digital operations, the retrieving of the QR codes implies only two operations to display all QR codes on the same plane, at the same time, without any kind of overlap, and using informatics tools freely available for everybody.

According to the described proposal, a panel containing several QR codes is displayed after performing the correct retrieving protocol. As each code contains the information of a single character, the final step is scanning the panel using the appropriate sequence to reveal the hidden message. The scanning process can be performed using a QR scanning program from a smartphone, a computer, or a tablet [7, 8, 10–12]. Other option is employing the most basic, fast, and free

available software on the Internet. This software works only for binary QR codes. An original QR code consists of black and white blocks arranged in a square grid, while decrypted QR codes are not binary (figure 4(b)). We want to take advantage of this software to make the scanning process simpler and faster. Therefore, we proceed to binarize individually each QR code contained in the panel. For doing so, first we divide each decrypted QR code in blocks, where each block contains several pixels of the code. A threshold value is chosen such that gray values above the threshold become white, while for gray values lower than the threshold become black, thus generating a QR code binarized as shown in the figure 4(e).

Figure 5(a) presents the binarized panel with the retrieved QR codes, while figure 5(b) shows a panel containing the original QR codes. From a simple visual comparison between figures 5(a) and (b), it is not easy to deduce the differences between the original and the processed and binarized QR codes. We expect some differences between the original and binarized QR codes due to the changes suffered by the QR codes during the application of the protocol. In order to make evident these differences, we zoomed in on one section of a binarized QR code and the corresponding sections taken from its original version. Figure 5(c) clearly shows dissimilarities among the processed and original QR codes. Despite these differences, the processed QR codes using our proposed technique can be successfully scanned.

If we now add a predetermined sequence over the final QR panel (figure 5(a)), we are able to recover a noiseless hiding message, as shown in figure 6(a) (see media 1). The phrase ‘PACKAGING AND CODING’ is reconstructed without traces of degradation. In the standard procedures [1–6, 51–56], we observe that the final outcomes are recovered with a speckle noise generated by the optodigital processing

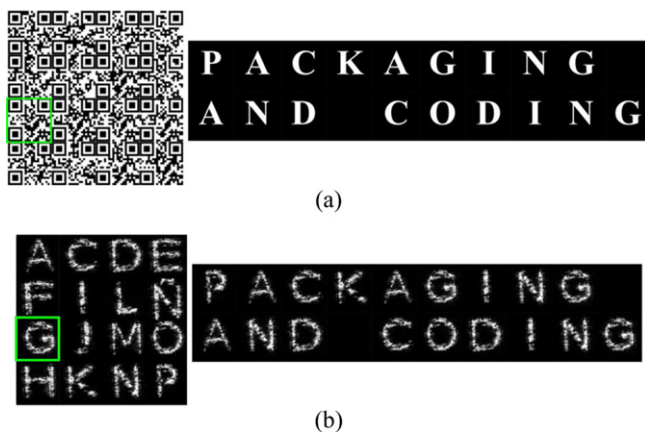


Figure 6. (a) Recovered message with the proposed protocol (media 1) and (b) message retrieved with the classical procedure.

(see figure 6(b)). This noise is because each character is directly processed by the optical system, while in our proposal, each character is first converted into a QR code and then the QR code is processed instead. Processing noise affects the recovered multiplexing of the processed QR codes, but when binarizing and reading each code, the finally decoded message is noise-free (see figure 6(a)).

The important advance represented by the new implementation is evident from figure 6 and media 1. The new security protocol allows recovering secret messages with no noise, while in classical optical security protocols, the retrieved message contains the noise arising from the processing. Also, once we get the panel with the recovered QR codes, we only need a new scanning sequence to reveal a new message, thus saving resources.

Although 16 QR codes are used to illustrate the procedure (figure 4(a)), the scheme is not altered if the number of QR codes changes. Our protocol can be extended for the general case where the authorized user can recover a panel containing a complete keyboard whose keys are contained in the QR codes. Using this panel and recovery sequence, it is possible to obtain a message of any length and any content. In the general case, the maximum number of multiplexed QR codes corresponds to the amount of letters, symbols, and numbers that a keyboard may contain.

Under the proposed protocol, the user gets in one occasion the multiplexed and encrypted information and the corresponding decode key. After performing the correct recovering procedure, the retrieved panel of QR codes allows us to recover the protected message using the reading sequence (see media 1). In the general case, where the panel contains a complete keyboard constituted by the corresponding QR codes of its characters, different messages with a variety of content and extent are recovered when applying the reading sequences over the panel. It is important to remark that once the panel is obtained, to recover any new message, it is only necessary to access its corresponding reading sequence. Note that the spatial location of the QR codes in the panel should not necessarily follow that of a regular QWERTY keyboard.

5. Conclusions

In the present contribution, we proposed and implemented for the first time an optodigital protocol to securely manage messages, besides assuring their recovery was free of any kind of noise or degradation. We employ a simple $2f$ system and an interferometrical arrangement for the optical processing. A QR coding of the original information elements (letters) along with a filtering, positioning, multiplexing, and encryption completed the process to obtain an encrypted package with the QR processed codes. The multiplexing procedure not only represents the first multiplexing of optodigital processed QR codes, but also allows us to include in a single unit of information all processed QR codes, thus simplifying the handling and recovery of multiple QR codes. The proposed protocol is friendly to the final user because the recovery stage includes only two operations to bring the display of all QR codes in the same plane, at the same time, and without any kind of overlap. Then, by binarizing the recovered QR codes and acceding to the right scanning sequence, it is possible to recover the clean message. The protocol involves informatics tools available for free. Once the user gets the recovered and binarized panel of the QR codes, the retrieving of new messages only requires the knowledge of the scanning sequence. This protocol can be implemented for a multi-user environment. In this case, all authorized users receive the encrypted package and the encrypting mask by separate channels, and then each user gets the corresponding sequence in order to recover a particular message.

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 nos. 0863/09 and 0549/12 (Argentina), and Facultad de Ingeniería, Universidad Nacional de La Plata no. 11/I168 (Argentina). J F Barrera Ramírez acknowledges the support from The International Centre for Theoretical Physics ICTP Associateship Scheme and The World Academy of Sciences TWAS.

References

- [1] Refregier P and Javidi B 1995 Optical image encryption based on input plane fourier plane random encoding *Opt. Lett.* **20** 767–9
- [2] Javidi B and Horner J L 1994 Optical pattern recognition for validation and security verification *Opt. Eng.* **33** 1752–6
- [3] Matoba O and Javidi B 1999 Encrypted optical memory system using three-dimensional keys in the Fresnel domain *Opt. Lett.* **24** 762–4
- [4] Nomura T and Javidi B 2000 Optical encryption using a joint transform correlator architecture *Opt. Eng.* **39** 2031–5

- [5] Matoba O, Nomura T, Perez-Cabre E, Millá M S and Javidi B 2009 Optical techniques for information security *Proc. IEEE* **97** 1128–48
- [6] Chen W, Javidi B and Chen X 2014 Advances in optical security systems *Adv. Opt. Photon* **6** 120–55
- [7] Barrera J F, Mira A and Torroba R 2013 Optical encryption and QR codes: secure and noise-free information retrieval *Opt. Express* **21** 5373–8
- [8] Graydon O 2013 Quick response codes *Nat. Photonics* **7** 343
- [9] Barrera J F, Mira A and Torroba R 2014 Experimental QR code optical encryption: noise-free data recovering *Opt. Lett.* **39** 3074–7
- [10] Barrera J F, Vélez A and Torroba R 2014 Experimental scrambling and noise reduction applied to the optical encryption of QR codes *Opt. Express* **22** 20268–77
- [11] Ohbuchi E, Hanaizumi H and Hock L A 2004 Barcode readers using the camera device in mobile phones in *Proc. of IEEE 2004 Int. Conf. Cyberworlds (IEEE, 2004)* pp 260–5
- [12] Liao K C and Lee W H 2010 A novel user authentication scheme based on QR-Code *J. Netw* **5** 937–41
- [13] Lin C, Shen X and Li B 2014 Four-dimensional key design in amplitude, phase, polarization and distance for optical encryption based on polarization digital holography and QR code *Opt. Express* **22** 20727–39
- [14] Wang Z, Zhang S, Liu H and Qin Y 2014 Single-intensity-recording optical encryption technique based on phase retrieval algorithm and QR code *Commun.* **332** 36–41
- [15] Fan D, Meng X, Wang Y, Yang X, Peng X, He W, Dong G and Chen H 2013 Optical identity authentication scheme based on elliptic curve digital signature algorithm and phase retrieval algorithm *Appl. Opt.* **52** 5645–52
- [16] Qin Y and Gong Q 2014 Optical information encryption based on incoherent superposition with the help of the QR code *Opt. Commun.* **310** 69–74
- [17] Markman A, Javidi B and Tehramipour M 2014 Photon-counting security tagging and verification using optically encoded QR codes *IEEE Photon. J.* **6** 6800609
- [18] Carnicer A, Hassanfiroozi A, Latorre-Carmona P, Huang Y P and Javidi B 2015 Security authentication using phase-encoded nanoparticle structures and polarized light *Opt. Lett.* **40** 135–8
- [19] Mosso F, Barrera J F, Tebaldi M, Bolognini N and Torroba R 2011 All-optical encrypted movie *Opt. Express* **19** 5706–12
- [20] Mosso F, Tebaldi M, Barrera J F, Bolognini N and Torroba R 2011 Pure optical dynamical color encryption *Opt. Express* **19** 13779–86
- [21] 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** 3388–93
- [22] Zhong Z, Yu Zhang, Shan M, Wang Y, Zhang Y and Xie H 2014 Optical movie encryption based on a discrete multiple-parameter fractional Fourier transform *J. Opt.* **16** 125404
- [23] Aldossari M, Alfalou A and Brosseau C 2014 Simultaneous compression and encryption of closely resembling images: application to video sequences and polarimetric images *Opt. Express* **22** 22349–68
- [24] Saini N and Sinha A 2015 Video encryption using chaotic masks in joint transform correlator *J. Opt.* **17** 035701
- [25] Barrera J F, Tebaldi M, Amaya D, Furlan W D, Monsoriu J, Bolognini N and Torroba R 2012 Multiplexing of encrypted data using fractal masks *Opt. Lett.* **37** 2895–97
- [26] Abuturab M R 2012 Color image security system using double random-structured phase encoding in gyrator transform domain *Appl. Opt.* **51** 3006–16
- [27] Singh H, Yadav A K, Vashisth S and Singh K 2015 Double phase-image encryption using gyrator transforms, and structured phase mask in the frequency plane *Opt. Laser Eng.* **67** 145–56
- [28] Chen W and Chen X 2011 Optical asymmetric cryptography using a three-dimensional space-based model *J. Opt.* **13** 075404
- [29] Rajput S K and Nishchal N K 2012 Asymmetric color cryptosystem using polarization selective diffractive optical element and structured phase mask *Appl. Opt.* **51** 5377–86
- [30] Wenqi H, Meng X and Peng X 2013 Asymmetric cryptosystem using random binary phase modulation based on mixture retrieval type of Yang-Gu algorithm: comment *Opt. Lett.* **38** 4044
- [31] Mehra I and Nishchal N K 2014 Asymmetric cryptosystem for securing multiple images using two beam interference phenomenon *Opt. Laser Technol.* **60** 1–7
- [32] Liu W, Xie Z, Liu Z, Zhang Y and Liu S 2015 Multiple-image encryption based on optical asymmetric key cryptosystem *Opt. Commun.* **335** 205–11
- [33] Sui L, Duan K, Liang J and Hei X 2014 Asymmetric double-image encryption based on cascaded discrete fractional random transform and logistic maps *Opt. Express* **22** 10605–21
- [34] Barrera J F, Vargas C, Tebaldi M, Torroba R and Bolognini N 2010 Known-plaintext attack on a joint transform correlator encrypting system *Opt. Lett.* **35** 3553–5
- [35] Barrera J F, Vargas C, Tebaldi M and Torroba R 2010 Chosen-plaintext attack on a joint transform correlator encrypting system *Opt. Commun.* **283** 3917–21
- [36] Qin W, Peng X and Meng X 2011 Cryptanalysis of optical encryption schemes based on joint transform correlator architecture *Opt. Eng.* **50** 028201
- [37] Wang X and Zhao D 2012 Double images encryption method with resistance against the specific attack based on an asymmetric algorithm *Opt. Express* **20** 11994–2003
- [38] Kumar P, Joseph J and Singh K 2012 Known-plaintext attack-free double random phase-amplitude optical encryption: vulnerability to impulse function attack *J. Opt.* **14** 045401
- [39] Wang X and Zhao D 2012 A special attack on the asymmetric cryptosystem based on phase-truncated Fourier transforms *Opt. Commun.* **285** 1078–81
- [40] Liao M, He W, Peng X, Liu X and Meng X 2013 Cryptanalysis of optical encryption with a reference wave in a joint transform correlator architecture *Opt. Laser Technol.* **45** 763–7
- [41] Rajput S K and Nishchal N K 2013 Known-plaintext attack-based optical cryptosystem using phase-truncated Fresnel transform *Appl. Opt.* **52** 871–8
- [42] Zhang C, Liao M, He W and Peng X 2013 Ciphertext-only attack on a joint transform correlator encryption system *Opt. Express* **21** 28523–30
- [43] Wang X and Zhao D 2011 Multiple-image encryption based on nonlinear amplitude-truncation and phase-truncation in Fourier domain *Opt. Commun.* **284** 148–52
- [44] Liu Z, Zhanga Y, Zhao H, Ahmad M A and Liu S 2011 Optical multi-image encryption based on frequency shift *Optik* **122** 1010–3
- [45] Lin C, Shen X, Tang R and Zou X 2012 Multiple images encryption based on Fourier transform hologram *Opt. Commun.* **285** 1023–8
- [46] Shen X, Lin C and Kong D 2012 Fresnel-transform holographic encryption based on angular multiplexing and random-amplitude mask *Opt. Eng.* **51** 068201
- [47] Yin S and Tao S 2013 Compression and storage of multiple images with modulating blazed gratings *J. Opt.* **15** 075406
- [48] Zhao H, Liu J, Jia J, Zhu N, Xie J and Wang Y 2013 Multiple-image encryption based on position multiplexing of Fresnel phase *Opt. Commun.* **286** 85–90
- [49] Alfalou A, Brosseau C, Abdallah N and Jridi M 2013 Assessing the performance of a method of simultaneous compression and encryption of multiple images and its resistance against various attacks *Opt. Express* **21** 8025–43

- [50] Wang Y, Quan C and Tay C J 2014 Nonlinear multiple-image encryption based on mixture retrieval algorithm in Fresnel domain *Opt. Commun.* **330** 91–8
- [51] Vilarity J M, Millán M S and Perez-Cabre E 2013 Improved decryption quality and security of a joint transform correlator-based encryption system *J. Opt.* **15** 025401
- [52] Vilarity J M, Millán M S and Perez-Cabre E 2014 Nonlinear optical security system based on a joint transform correlator in the Fresnel domain *Appl. Opt.* **53** 1674–82
- [53] 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** 4350–5
- [54] Barrera J F, Vélez A and Torroba R 2013 Experimental multiplexing protocol to encrypt messages of any length *J. Opt.* **15** 055404
- [55] Barrera J F, Trejos S, Tebaldi M and Torroba R 2013 Experimental protocol for packaging and encrypting multiple data *J. Opt.* **15** 055406
- [56] Trejos S, Barrera J F, Tebaldi M and Torroba R 2014 Experimental optodigital processing of multiple data via modulation, packaging and encryption *J. Opt.* **16** 055402