# Experimental QR code optical encryption: noise-free data recovering

**John Fredy Barrera,[1,]* Alejandro Mira-Agudelo,[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*
**Corresponding author: john.barrera@udea.edu.co*

Received February 21, 2014; revised March 28, 2014; accepted April 10, 2014;
posted April 14, 2014 (Doc. ID 206958); published May 15, 2014

We report, to our knowledge for the first time, the experimental implementation of a quick response (QR) code as a "container" in an optical encryption system. A joint transform correlator architecture in an interferometric configuration is chosen as the experimental scheme. As the implementation is not possible in a single step, a multiplexing procedure to encrypt the QR code of the original information is applied. Once the QR code is correctly decrypted, the speckle noise present in the recovered QR code is eliminated by a simple digital procedure. Finally, the original information is retrieved completely free of any kind of degradation after reading the QR code. Additionally, we propose and implement a new protocol in which the reception of the encrypted QR code and its decryption, the digital block processing, and the reading of the decrypted QR code are performed employing only one device (smartphone, tablet, or computer). The overall method probes to produce an outcome far more attractive to make the adoption of the technique a plausible option. Experimental results are presented to demonstrate the practicality of the proposed security system.

*OCIS codes:* (060.4785) Optical security and encryption; (100.4998) Pattern recognition, optical security and encryption; (070.4560) Data processing by optical means.
http://dx.doi.org/10.1364/OL.39.003074

Optical security techniques are attractive alternatives with applications in encoding, encryption, recognition, secure identification, watermarking, and/or verification. After the successful report of Réfrégier and Javidi in optical encrypting techniques [1], much effort has been made by the researchers to develop new options [2–4]. Optical encryption probed its robustness, applicability, potentiality, and flexibility. Another promising extension is called the multiplexing alternative [5–7], employing the techniques ahead of intended attacks. We can also mention the development of an encrypted movie in theta modulation [8] and the encryption of messages of any length [9]. A different and interesting approach to optical encryption is developed in the frame of the optical asymmetric-key cryptography [10,11]. This new tactic, through a nonlinear operation, brings robustness against existing attacks. From the perspective of cryptology, asymmetric cryptography is of the same significance as a symmetric scheme. Summarizing, optics brings recognized capabilities of protecting information as alternatives to previous well-established methodologies.

However, a major concern is claimed against the decoded results when obtained using actual experimental optical arrangements, as although highly protected there is a lack of the original quality due to the speckle noise [2–4,9,12]. Although some techniques allow reducing the speckle noise, none of them completely remove it [13,14]. In this regard, potential users are unwilling to accept the optical protocols in view of the somehow deteriorated original inputs.

In a previous contribution, we introduced, to our knowledge for the first time, the concept of an information "container" before a standard optical encrypting procedure [15]. The proposal was demonstrated by means of a $4f$ encrypting system implemented as a virtual optical system. The "container" selected is a quick response (QR) code that offers the main advantage of being tolerant of pollutant speckle noise. In addition, smartphones or tablets, both with the appropriate application [16,17], can read the QR code. Moreover, QR codes include another secure step to add to the encrypting benefits the optical methods provide. The QR codes are generated by means of software available worldwide. This software allows raw text to be transformed into a bidimensional code matrix. The concept development probes that speckle noise polluting the outcomes of normal optical encrypting procedures can be avoided, thus making more attractive the adoption of these techniques.

This novel contribution attracts a remarkable interest over the specialized scientific community [18]. This success is mainly due to two reasons: first, our technique represents an advance in presenting a practical tool to solve the drastic issue of the ever-present speckle noise altering the recovered information, and second, it employs an informatics tool at hand for everybody. These two elements constitute real progress toward offering a secure and practical alternative to protect data with an actual optical processor.

We are now looking for an application using a joint transform correlator (JTC) encrypting architecture, as it is more compact than the $4f$ scheme and it is more stable from a holographic point of view in an experimental scheme.

The practical implementation of our proposal in a single step is not feasible due to the natural resolution limit of the actual optical systems; therefore, we recall the results of [12]. There we find the development of an experimental protocol to visualize decrypted images that otherwise would have been barely recognizable, while keeping the standard security levels. This experimental achievement is the adequate instrument to be implemented in the present contribution.

Summarizing, we introduce in this contribution a combination of improvements. In the first place, we use the concept of information "container" by converting the original message into a QR code [15]. Second, the QR code is divided into subsamples; then they are individually encrypted and multiplexed, proving the advantage used in [12] of obtaining a frequency enhancement. Finally, a block processing applied to the decrypted QR code recovers a completely noise-free version of the QR code, bringing back, after reading, the original undistorted information. For practical purposes, each subsample is displayed in a spatial light modulator (SLM). The experimental setup employed for the optical processing is an interferometric arrangement, where the JTC encrypting architecture is located in one arm and the other arm supplies the reference beam (see Fig. 1).

First, each QR code subsample is processed using the JTC encrypting architecture. In the experimental JTC scheme the input plane contains both the object window and the key window projected in a SLM, which is in contact with a ground glass. The key window limits the area of the encrypting key, while the subsample is rescaled so as to occupy the whole object window (Fig. 1). Therefore, the input is

$$u_l(x_0,y_0) = o_l(x_0,y_0) \otimes \delta(x_0 - b, y_0) + k(x_0,y_0) \otimes \delta(x_0 - (-b), y_0), \tag{1}$$

where $o_l(x_0,y_0) = s_l(x_0,y_0) r(x_0,y_0)$ and $r(x_0,y_0)$ is a random phase mask, $2b$ is the distance between the QR code subsample $s_l(x_0,y_0)$ and the encrypting key $k(x_0,y_0)$, $\otimes$ means convolution, and $\delta()$ is the delta Dirac function. It is worth mentioning that the security of the system relies on the physical random phase mask (ground glass), which acts as an encoding key.

The reference arm is blocked to store the joint power spectrum (JPS) of the input plane in the CCD camera,

$$\mathrm{JPS}_l(u,v) = |O_l(u,v)|^2 + O_l^*(u,v)K(u,v)\exp(4\pi ibu) + |K(u,v)|^2 + O_l(u,v)K^*(u,v)\exp(-4\pi ibu), \tag{2}$$

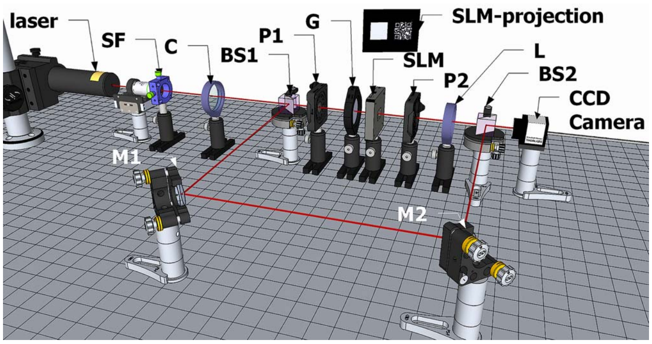

Fig. 1. Experimental setup for the encryption procedure (SF, spatial filter; C, collimating lens; BS1 and BS2, beam splitters; P1 and P2, polarizers; G, ground glass; SLM, spatial light modulator; L, lens; M1 and M2, mirrors).

where $(x,y)$ denoted the spatial coordinates and $(u,v)$ the Fourier domain coordinates, $*$ means complex conjugate, $O_l(u,v)$ and $K(u,v)$ are the Fourier transforms of $o_l(x_0,y_0)$ and $k(x_0,y_0)$, respectively.

The JPS contains four terms, where attention is focused on retaining only the relevant term with the encrypted QR code subsample information. For this purpose, $|O_l(u,v)|^2$ and $|K(u,v)|^2$ are registered and then subtracted from the JPS. After performing a Fourier transform (FT) it is possible to get two spatially isolated terms carrying the information of the object convolved with the encoding key. Next, one of those terms is removed and the remaining term is freely positioned; finally, a FT allows getting the encrypted subsample [12],

$$E_l(u,v) = O_l(u,v)K^*(u,v)\exp[2\pi i(x_l u + y_l v)]. \tag{3}$$

Each QR code subsample is processed following the same procedure described above but with different coordinates $(x_l, y_l)$. The coordinates $(x_l, y_l)$ are carefully chosen to avoid the spatial overlapping of the subsamples during decryption [12]. Finally, the multiplexing of encrypted subsamples represents the encrypted QR code,

$$E_{\mathrm{QR}}(u,v) = \sum_{l=1}^{m} O_l(u,v)K^*(u,v)\exp[2\pi i(x_l u + y_l v)]. \tag{4}$$

The multiplexing reduces the amount of information to be sent and received as we are sending the encrypted QR code instead of sending all encrypted QR code subsamples as individual data, and at the same time it contains the information of each subsample relative position.

By blocking the window object, the digital hologram of the FT of the encoding key is registered. From this hologram the FT of the encrypting key $(K(u,v))$ is obtained [12].

During retrieval, the authorized user receives the multiplexing of encrypted subsamples [Eq. (4)] and the recovering key $(K(u,v))$. Multiplying this information and after a FT operation, the complete QR code is decrypted (see Fig. 2):

$$D_{\mathrm{QR}}(x,y) = \sum_{l=1}^{m} s_l(x,y)r(x,y) \otimes \delta(x - x_l, y - y_l). \tag{5}$$

It is important to observe that we record the square modulus of Eq. (5); therefore, it should be noted that the decrypted QR code is read on an intensity base. Consequently, as $r(x,y)$ in Eq. (5) is a pure phase mask common to all subsamples, it simply does not contribute to the final result.

In our experimental scheme, we use a He–Ne laser, a lens of 200 mm focal length, and a PULNIX TM6703 CCD with 640 × 480 pixels provided with a 9 μm × 9 μm pixel area. The key window and each object window are projected in a Holoeye LC2002 SLM. A ground glass placed behind the SLM generates the two random masks for the JTC architecture [3]. Both the key and the object windows have the same size 1.92 mm × 1.92 mm. The distance between windows is 3.84 mm.

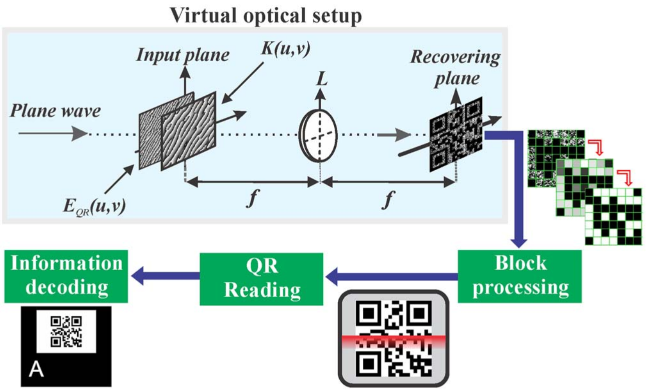

Fig. 2. Virtual processing scheme. The multiplexed package is correctly decrypted yielding to the QR code. Afterward, a binarization procedure follows to get a noiseless QR code for an optimized reading.

In the experimental demonstration, the letter "A" is converted into a QR code [Fig 3(a)]. If the complete QR code is projected as a single input, we find the result of Fig. 3(b). The limited resolution of the optical setup does not bring an adequate recovering [12]. To overcome this difficulty, the QR code is divided into 16 subsamples [Fig. 3(a)]. Afterward, each subsample is encrypted and processed to obtain the encrypted QR code [Eq. (4)]. Subsequently, whether a correct decrypting is carried out, the result is the recovering of the QR code [Fig. 3(c)]. As this method is based on a technique intended to enhance the spatial frequency content of a finally processed image, we obtain a frequency improvement in the decoded QR code [12].

It is important to emphasize that the only image involved in the procedure is that of the QR code, which is essentially binary according to the way it is created.

On the other hand, the most basic, fast, and free available software for reading QR codes is able to read only QR codes completely free of noise. We want to employ this software to make simpler and faster the reading process of the QR code. For this purpose, before the reading of the decrypted QR, we implement a digital block processing that permits eliminating the speckle noise (see Fig. 2). A QR code consists of black and white blocks arranged in a square grid. We scan each block of the decrypted QR code to find out the mean pixel value to represent each block. Therefore, we get a QR code whose blocks are not yet black and white [see Fig. 3(d)]. Then, a binarization process over each block is carried out to obtain a noise-free QR code. It is important to remark that the recovering procedure is friendly for the end user not only because it is performed using one device (smartphone, tablet, or computer), but also because the QR code is decrypted in one step (see Fig. 2).

The decrypted QR code and its corresponding QR code free of noise are shown in Figs. 3(c) and 3(e), respectively. It is important to take into account that when using an actual optical security setup based on random phase mask, although a digital processing is applied on the decrypted data, there is always dissimilarity between the original object and the digitally processed decrypted object. In this proposal, thanks to the tolerance of QR reading, after reading the decrypted and digitally processed QR code, the original object can be retrieved without any kind of degradation (Fig. 2).

In Fig. 4 we present an example to reinforce the validity and applicability of this proposal. As expected, due to the speckle noise present in the decrypted QR code, the original QR code is different from the digital processed code, as shown in Figs. 4(b) and 4(e). The results shown in Fig. 4 demonstrate the great benefit of including QR codes as containers in an optical encryption procedure.

We stress that unlike the other methods, the preset protocol solves the drastic issue of the ever-present speckle noise over the final recovered information. It is important to mention an interesting feature arising when comparing the original and the recovered and processed QR codes in Fig. 4. As the message complexity increases, the recovered and processed QR code structure details differ from the original [Figs. 4(b) and 4(e)]; however, the quality of the final decoded information

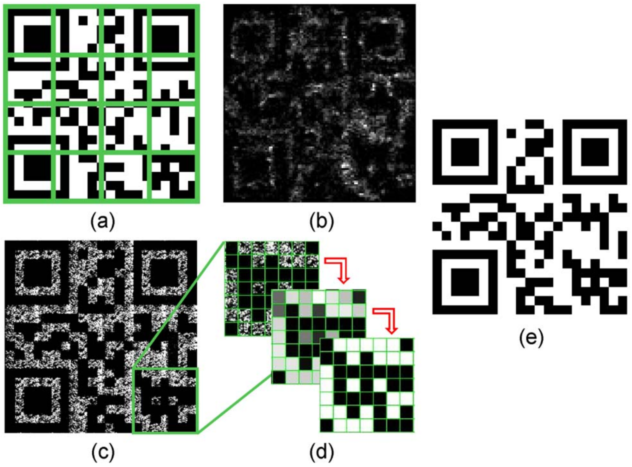

Fig. 3. (a) Original QR code of letter "A," (b) decrypted QR code when (a) is used as a single input, (c) decrypted QR code using subsampling and multiplexing, (d) magnified inset box showing the digital block processing, and (e) decrypted QR code after the block processing.

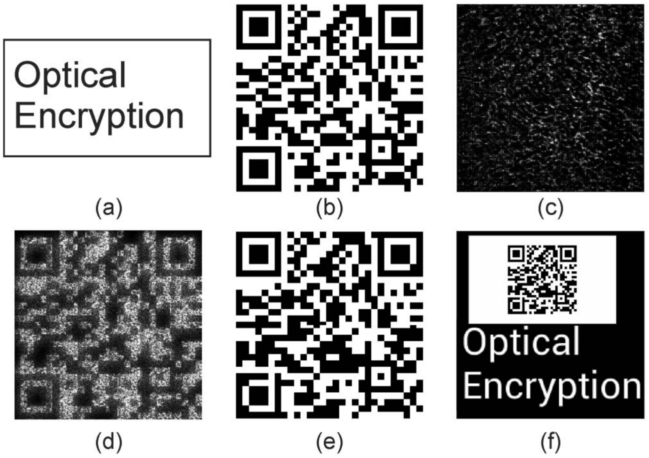

Fig. 4. (a) Input message and (b) its respective QR code, (c) encrypted QR code, (d) decrypted QR code, (e) decrypted QR code after block processing, and (f) recovered information after reading (e).

remains the same thanks to the remarkable noise resistance of the QR codes [Fig. 4(f)].

The proposed and implemented system preserves the security of the actual optical processors based on physical random mask (ground glass), and at the same time allows recovering the original data completely free of any kind of noise or degradation. In this proposal during the recovering station, it is not necessary to print or to project the QR code before the reading. We stress that an important advantage of the method relies in using only one recovering device (smartphone, tablet, or computer).

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

## References

1. P. Réfrégier and B. Javidi, Opt. Lett. **20**, 767 (1995).
2. O. Matoba and B. Javidi, Opt. Lett. **27**, 321 (2002).
3. T. Nomura and B. Javidi, Opt. Eng. **39**, 2031 (2000).
4. G. Unnikrishnan, J. Joseph, and K. Singh, Opt. Lett. **25**, 887 (2000).
5. G. Situ and J. Zhang, Opt. Lett. **30**, 1306 (2005).
6. N. K. Nishchal and T. J. Naughton, Opt. Commun. **284**, 735 (2011).
7. A. Alfalou and C. Brosseau, Adv. Opt. Photon. **1**, 589 (2009).
8. F. Mosso, J. F. Barrera, M. Tebaldi, N. Bolognini, and R. Torroba, Opt. Express **19**, 5706 (2011).
9. J. F. Barrera, A. Vélez, and R. Torroba, J. Opt. **15**, 055404 (2013) (IOPselect article).
10. W. Qin and X. Peng, Opt. Lett. **35**, 118 (2010).
11. W. Qin, X. Peng, B. Gao, and X. Meng, Opt. Eng. **50**, 080501 (2011).
12. J. F. Barrera, E. Rueda, C. Ríos, M. Tebaldi, N. Bolognini, and R. Torroba, Opt. Commun. **284**, 4350 (2011).
13. J. M. Vilardy, M. S. Millan, and E. Perez-Cabre, J. Opt. **15**, 025401 (2013).
14. B. Javidi, N. Towghi, N. Maghzi, and S. C. Verrall, Appl. Opt. **39**, 4117 (2000).
15. J. F. Barrera, A. Mira, and R. Torroba, Opt. Express **21**, 5373 (2013).
16. E. Ohbuchi, H. Hanaizumi, and L. A. Hock, in *Proceedings of IEEE 2004 International Conference on Cyberworlds* (IEEE, 2004), pp. 260–265.
17. K. C. Liao and W. H. Lee, J. Netw. **5**, 937 (2010).
18. O. Graydon, Nat. Photonics **7**, 343 (2013).