Optical encryption and QR codes: Secure and noise-free information retrieval

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

[1]*Grupo de Óptica y Fotónica, Instituto de Física, Universidad de Antioquia, A.A 1226, 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*
**jbarrera@fisica.udea.edu.co*

Abstract: We introduce for the first time the concept of an information "container" before a standard optical encrypting procedure. The "container" selected is a QR code which offers the main advantage of being tolerant to pollutant speckle noise. Besides, the QR code can be read by smartphones, a massively used device. Additionally, QR code includes another secure step to the encrypting benefits the optical methods provide. The QR is generated by means of worldwide free available software. The concept development probes that speckle noise polluting the outcomes of normal optical encrypting procedures can be avoided, then making more attractive the adoption of these techniques. Actual smartphone collected results are shown to validate our proposal.

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. O. Matoba and B. Javidi, "Optical retrieval of encrypted digital holograms for secure real-time display," Opt. Lett. **27**(5), 321–323 (2002).
3. T. Nomura and B. Javidi, "Optical encryption using a joint transform correlator architecture," Opt. Eng. **39**(8), 2031–2035 (2000).
4. G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain," Opt. Lett. **25**(12), 887–889 (2000).
5. G. Situ and J. Zhang, "Double random-phase encoding in the Fresnel domain," Opt. Lett. **29**(14), 1584–1586 (2004).
6. 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).
7. X. Tan, O. Matoba, Y. Okada-Shudo, M. Ide, T. Shimura, and K. Kuroda, "Secure optical memory system with polarization encryption," Appl. Opt. **40**(14), 2310–2315 (2001).
8. R. Henao, E. Rueda, J. F. Barrera, and R. Torroba, "Noise-free recovery of optodigital encrypted and multiplexed images," Opt. Lett. **35**(3), 333–335 (2010).
9. G. Situ and J. Zhang, "Multiple-image encryption by wavelength multiplexing," Opt. Lett. **30**(11), 1306–1308 (2005).
10. N. K. Nishchal and T. J. Naughton, "Flexible optical encryption with multiple users and multiple security levels," Opt. Commun. **284**(3), 735–739 (2011).
11. C. Lin, X. Shen, R. Tang, and X. Zou, "Multiple images encryption based on Fourier transform hologram," Opt. Commun. **285**(6), 1023–1028 (2012).
12. A. Alfalou and C. Brosseau, "Optical image compression and encryption methods," Adv. Opt. Photon. **1**(3), 589–636 (2009).
13. F. Mosso, J. F. Barrera, M. Tebaldi, N. Bolognini, and R. Torroba, "All-optical encrypted movie," Opt. Express **19**(6), 5706–5712 (2011).
14. J. F. Barrera, M. Tebaldi, C. Ríos, E. Rueda, N. Bolognini, and R. Torroba, "Experimental multiplexing of encrypted movies using a JTC architecture," Opt. Express **20**(4), 3388–3393 (2012).
15. F. Liu, Q. K. Fu, and L. M. Cheng, "Wave-atoms-based multipurpose scheme via perceptual image hashing and watermarking," Appl. Opt. **51**(27), 6561–6570 (2012).
16. H. Wang, W. Zhang, and A. Dong, "Modeling and validation of photometric characteristics of space targets oriented to space-based observation," Appl. Opt. **51**(32), 7810–7819 (2012).

#182072 - $15.00 USD
(C) 2013 OSA

Received 19 Dec 2012; accepted 9 Jan 2013; published 25 Feb 2013

17. A. Carnicer, M. Montes-Usategui, S. Arcos, and I. Juvells, “Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys,” Opt. Lett. **30**(13), 1644–1646 (2005).
18. X. Peng, P. Zhang, H. Wei, and B. Yu, “Known-plaintext attack on optical encryption based on double random phase keys,” Opt. Lett. **31**(8), 1044–1046 (2006).
19. J. F. Barrera, C. Vargas, M. Tebaldi, R. Torroba, and N. Bolognini, “Known-plaintext attack on a joint transform correlator encrypting system,” Opt. Lett. **35**(21), 3553–3555 (2010).
20. 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).
21. S. Dey, “SD-EQR: A new technique to use QR codesTM in cryptography: use of QR CodesTM in data hiding and securing,” in Proceedings of International Conference on Emerging Trends of Computers and Information Technology, Vol 3 of 2012 WINBIS, (Open Learning Society, 2012), pp. 11–21.
22. E. Ohbuchi, H. Hanaizumi, and L. A. Hock, “Barcode readers using the camera device in mobile phones,” in *Proceedings of IEEE 2004 International Conference on Cyberworlds* (IEEE, 2004), pp. 260 – 265.
23. K. C. Liao and W. H. Lee, “A novel user authentication scheme based on QR-Code,” J. Netw. **5**, 937–941 (2010).

1. Introduction

Optical security technology is based on complex information processes where the signals are hidden from human perception (to keep them secret). Besides, images should be extremely difficult to be reproduced with the same properties (to avoid counterfeiting). Optical security techniques involve tasks such as encoding, encryption, recognition, secure identification, watermarking and/or verification. Since the first successful application in optical encrypting techniques [1], much effort was developed by the community in the field to develop new alternatives. Different architectures were used [2,3], and several domains were examined to get satisfactory results [4,5]. Optical encryption probed its robustness, applicability, potentiality, and flexibility. Diverse recording media were inspected trying to find better storing capabilities [6–8]. Either one or more input objects were analyzed developing what is called multiplexing alternatives [9–12]. Even the developing of an encrypted movie was addressed in theta modulation [13] or another alternative [14]. Validation and watermarking were also branches derived from the encrypting proposals [15,16]. Besides, the resistance to hacker attacks was analyzed to look for weaknesses and to reinforce the encrypting strength [17–19]. Common to these proposals are the recognized capabilities of protecting information the optics brings, as alternatives to previous well established methodologies.

Underlying to the encoding procedures is the speckle field involved in the encrypting key. The unique key properties guarantee the inviolability of the techniques, besides the additional geometrical or optical properties that eventually were used to enhance the security.

However, a major concern is claimed against the decoded results, although protected, there is a lack of the original quality precisely due to the same protecting factor: the inherent speckle noise that pollutes the outcomes. In this regard, potentials user are reluctant to accept the optical protocols in view of the somehow deteriorated originals inputs.

The question is; would it be possible to keep the protecting properties the optical methods bring without getting polluted results? On the other hand, 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?

In pursuing these objectives, we think in two steps: a first step is the transforming of the input information into a “container”, and then the following step is the encrypting of the “container” with one of the usual optical protocols. Therefore, the speckle noise will affect the decoded “container”. If there is a suitable “container” that allows recovering the original information without any kind of alteration no matter it is affected by the speckle, then the goal is accomplished. We find such “container” in the Quick Response (QR) code [20,21], both noise resistant and available to almost anyone. QR codes can be read by smartphones or tablets with the appropriate application [22,23].

In the following we will show how the QR code works, the way it could be successfully used as a first coding step or “container”, the application of an optical encrypting technique to

Received 19 Dec 2012; accepted 9 Jan 2013; published 25 Feb 2013

the QR code, the corresponding decrypting operation, and finally the original information retrieval without quality loss, as QR codes are tolerant to speckle noise. The analysis will show the obvious advantages found in connection with our new proposal, as the final user is satisfied by clearly distinguishing the original input. In either case, we believe we offered a practical solution to the speckle noise over decrypted images, thus releasing a valid actual alternative to solve the problem, besides making more attractive the use of optical encrypting techniques.

2. Optical encryption

The encryption protocol we preferred is the usual double random phase encoding (DRPE) realized in a 4f architecture, due to its common knowledge among the researchers in the field. This most popular encryption method is based on protecting the stored information by transforming the original data into stationary white-noise data.

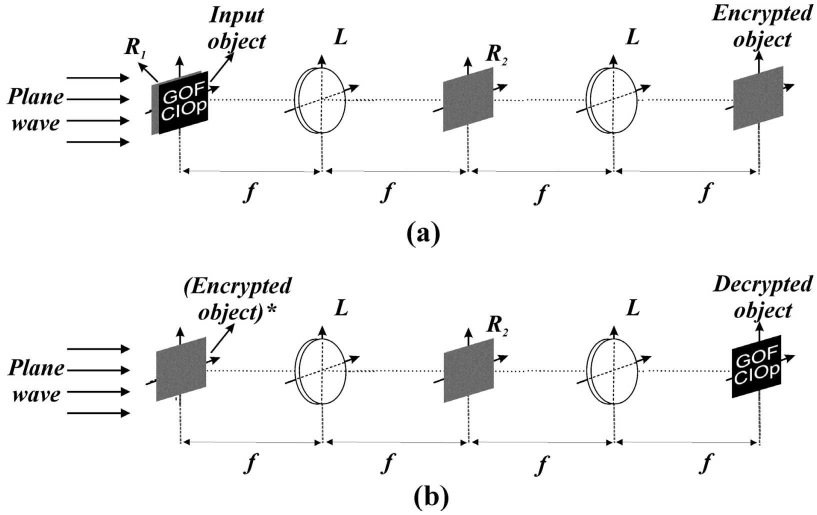

Fig. 1. (a) Encrypting and (b) decrypting systems (f : focal length of the lens L , R_1 and R_2 : random phase masks).

Figure 1 depicts the basic optical encrypting and decrypting arrangements. The method uses two random phase key codes on each of the input and Fourier planes and it can be implemented either optically or electronically in both the encryption and the decryption stages. Figure 1(b) shows the decrypting architecture, where the user inserts a complex conjugate of the encrypted information, and the corresponding encrypting key R_2 as depicted.

At the output plane of the decrypting scheme, we visualize the decoded image. In Fig. 2, we sequentially show (a) the input object, (b) the encrypted object, (c) the result of decrypting but using an invalid key, and (d) the correct recovered object observing the inherent speckle noise all over the image. Obviously, the speckle noise is unavoidable when employing optical encryption with DRPE under any architecture, domain, or protocol [1–19].

Received 19 Dec 2012; accepted 9 Jan 2013; published 25 Feb 2013

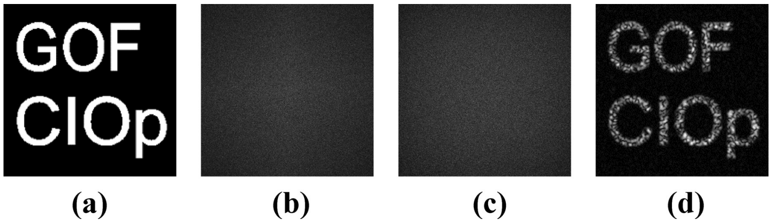

Fig. 2. (a) Input object, (b) encrypted object, (c) decrypted object with a wrong key, and (d) recovered object with the original key.

3. What is a QR code?

On the other hand, QR Code (from Quick Response Code) is the trademark for a two-dimensional code first designed for vehicle industry. More recently, the system has become popular outside the industry due to its fast readability and large storage capacity compared to standard UPC barcodes. The code consists of black modules (square dots) arranged in a square pattern on a white background. The information encoded can be made up of four standardized kinds ("modes") of data (numeric, alphanumeric, byte/binary, etc.), or through supported extensions, virtually any kind of data [20,23]. The QR Code was invented in Japan by the Toyota subsidiary Denso Wave in 1994 to track vehicles during the manufacturing process, and was originally designed to allow components to be scanned at high speed. It has since become one of the most popular types of two-dimensional barcodes.

Unlike the older one-dimensional barcode that was designed to be mechanically scanned by a narrow beam of light, the QR code is detected as a 2-dimensional digital image by a semiconductor image sensor and is then digitally analyzed by a programmed processor. The processor locates the three distinctive squares at the corners of the image, and uses a smaller square near the fourth corner to normalize the image for size, orientation, and angle of viewing. The small dots are then converted to binary numbers and validity checked with an error-correcting code. We show in Fig. 3(a) a QR image, describing the main QR features, and if read with a smartphone it appears "GOF CIOp" as in Fig. 3(b).

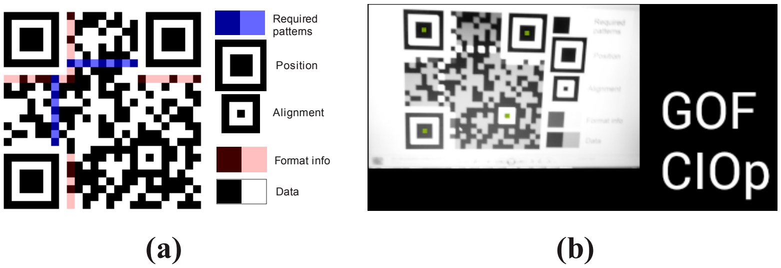

Fig. 3. (a) QR code of the text "GOF CIOp" and (b) the outcome when reading the QR code with a smartphone.

One of the best features QR codes exhibit is a level of error correction which directly depend on the storage capacity. Thanks to these levels of correction contained in the generating algorithm, information can be correctly scanned even though localized damage and/or contamination affect the QR code.

Formerly only for industrial uses, it has in recent years become common in consumer advertising and packaging, due to the large availability of smartphones and tablets. As a result, the QR Code has become a focus of advertising strategy, since it provides quick and effortless access to the brand's website. QR Codes are now used over a much wider range of applications, including commercial tracking, entertainment and transport ticketing, product/loyalty marketing, and in-store product labeling.

Individuals can generate and print their own QR Codes for others to scan and use by visiting one of several pay or free QR Code-generating sites or apps for scanning QR Codes can be found on nearly all smartphone and tablets devices.

QR Codes storing addresses and Uniform Resource Locators (URLs) may appear in magazines, on signs, on buses, on business cards, or on almost any object about which users might need information. Users with a smartphone or a tablet equipped with the correct reader application can scan the image of the QR Code to display text, contact information, connect to a wireless network, or open a web page in the telephone's browser.

The use of QR Codes is free of any license. The QR Code is clearly defined and published as an ISO standard [20]. Denso Wave owns the patent rights on QR Codes, but has chosen not to exercise them. The word QR Code itself is a registered trademark of Denso Wave Incorporated.

4. Transforming the QR into an encrypted container

Our proposal is combining the optical DRPE encrypting technique with the QR coding to eliminate the noise in the recovered information. Once we discussed the properties and uses of the QR codes, we can proceed to employ it to "contain" a given input. Again, we want to point out that the QR procedure itself provides a safe environment for the coded input. There exists a number of software to create the QR codes depending on the device intended to use during reading. In Fig. 4(a) we present the input message to be typed in the software and in Fig. 4(b) the corresponding QR code. Therefore, we created an information "container" which we intend to use for the next step.

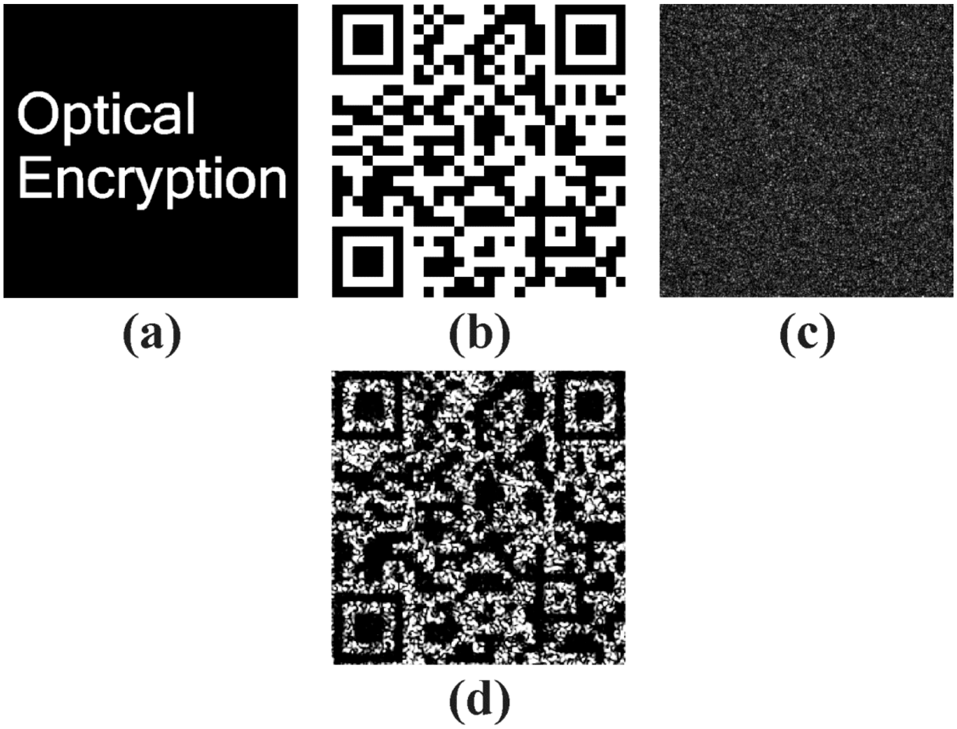

Fig. 4. (a) Representation of the input message and (b) its respective QR code. (c) Optically encrypted and (d) decrypted QR code.

Figure 4(c) shows the encrypted output when the QR code of Fig. 4(b) is used as input of the 4f encrypting architecture, which is our encrypted "container". As expected, we are not able to recognize a single trace of the QR code, satisfying its conversion into stationary white-noise data.

The encrypted information now can be sent to a user, together with the encoding key R_2. Obviously, the retrieved QR Code (Fig. 4(d)) presents the natural speckle noise due to the optical processing with random phase mask.

5. Decoded results, comparison to previous methods, and potentials

Precisely the speckle noise generates a reduction in the original quality of the object, thus inducing the potential clients of the method to be reluctant to widely accepting it for their operations.

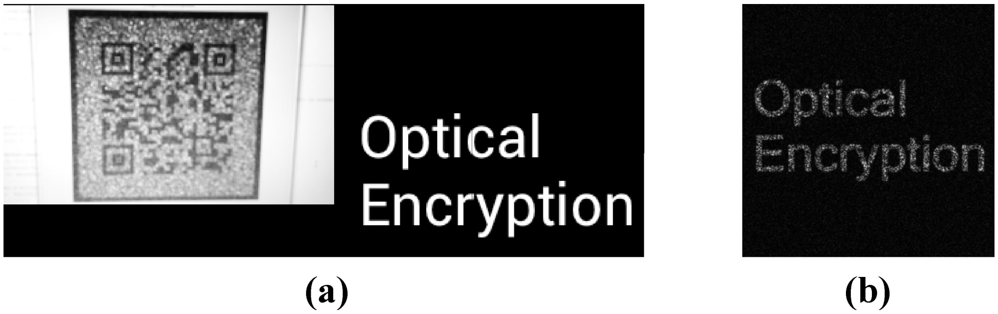

Fig. 5. (a) Reading of the decrypted QR Code revealing the noise-free message and (b) recovering of the message using only optical encryption.

Nevertheless, and thanks to the error correction levels, the direct scan of Fig. 4(d) reveals the result of Fig. 5(a), that is a recovered input with total resemblance with the original information, and totally noise-free. Figure 5(b) presents the noisy decrypted image with the traditional DRPE optical encryption technique. Figure 5(a) actually is the demonstration of a noise-free recovered message when employing optical encryption and QR coding together, thus proving the great potential of this contribution.

In this contribution, we only intend to introduce the concept, thus deferring the logical optimization of the whole procedure to future contributions.

Extensions can be envisaged as to comprise multiplexing options, involving the practical solutions already found in this context as to avoid cross talk and residual noise. Even dynamical approaches could be intended, supported in future developments dealing with QR synchronization in collecting the individual frames to launch a movie.

In this sense, we believe this novel application merging the QR code to the optical encryption revitalizes the traditional optical encrypting methods. According to our criterion, our technique represents an advance in presenting a practical tool, which can be massively used, and solving the drastically issue of the ever present speckle noise altering the outcome.

Acknowledgments

This research was performed under grants TWAS-UNESCO Associateship Scheme at Centres of Excellence in the South, CONICET No. 0863/09 and No. 0549/12 (Argentina), Facultad de Ingeniería, Universidad Nacional de La Plata No. 11/I168 (Argentina), Estrategia de Sostenibilidad 2011-2012 and CODI (Universidad de Antioquia-Colombia).