Optics and Lasers in Engineering 102 (2018) 119–125

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

journal homepage: www.elsevier.com/locate/optlaseng

# Fractional optical cryptographic protocol for data containers in a noise-free multiuser environment

Alexis Jaramillo[a,*], John Fredy Barrera[a], Alejandro Vélez Zea[b,c], Roberto Torroba[b,d]

[a] 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
[b] Centro de Investigaciones Ópticas (CONICET La Plata-CIC-UNLP) CC N° 3, C.P 1897, La Plata, Argentina
[c] Facultad de Ciencias Exactas, Universidad Nacional de La Plata, La Plata, Argentina
[d] UIDET OPTIMO, Facultad de Ingeniería, Universidad Nacional de La Plata, La Plata, Argentina

ARTICLE INFO

*Keywords:*
Encryption
Fractional fourier transform
Multiplexing
QR codes

ABSTRACT

Optical encryption systems have great potential for flexible and high-performance data protection, making them an area of rapid development. However, most approaches present two main issues, namely, the presence of speckle noise, and the degree of security they offer. Here we introduce an experimental implementation of an optical encrypting protocol that tackles these issues by taking advantage of recent developments in the field. These developments include the introduction of information containers for noise free information retrieval, the use of multiplexing to allow for a multiple user environment and an architecture based on the Joint fractional Fourier transform that allows increased degrees of freedom and simplifies the experimental requirements. Thus, data handling via QR code containers involving multiple users processed in a fractional joint transform correlator produce coded information with increased security and ease of use. In this way, we can guarantee that only the user with the correct combination of encryption key and security parameters can achieve noise free information after deciphering. We analyze the performance of the system when the order of the fractional Fourier transform is changed during decryption. We show experimental results that confirm the validity of our proposal.



## 1. Introduction

Information security is an important subject, especially as the growing interchange of data increases its vulnerability to attacks, and interception by unauthorized users presents a substantial increment. Optical cryptosystems have been proposed as an alternative solution with great potential, offering many degrees of freedom that can be employed to reinforce the security of the information [1,2].

The pioneer cryptosystem was proposed and demonstrated by Refrieger and Javidi [3]. Their proposal was a 4f system with a double random phase encoding (DRPE) technique. In this system, one random phase mask is placed in the input plane, while the second phase mask is located in the Fourier domain of a first lens. This second phase mask is the encryption key. A second lens produces the encrypted data, resulting in a white noise distribution from which the original information cannot be extracted without the information of the encryption key. After the implementation of the 4f system, several encryption architectures were proposed, amongst which we find the joint transform correlator (JTC) cryptosystem [4,5]. The JTC architecture presents several advantages over the 4f system. The encrypted data is codified into an intensity distribution; the decryption procedure is carried with the encryption key without needing the complex conjugate of the encrypting key, and presents less stringent alignment requirements for the experimental implementation. These properties make the JTC system a flexible alternative for further developments [6–9]. In this frame, the JTC cryptosystem has been object of continued research, both to determine and to improve its security against attackers [10–12] and to reduce the noise in the decrypted data [13,14].

Alternative optical securities schemes are still under active research, for example, an optical-digital encryption process was combined with a fingerprint authentication technique to increase the security of the optical system [15]. Another technique for improving the security in the encryption process is steganography, where the information to be protected is embedded into a carrier signal, containing non-secret information which obfuscates the protected data [16,17].

The JTC cryptosystem has also been modified with implementations in the Fresnel domain [18,19]. This implementation has the advantage of not requiring a lens, enabling the use of the free space propagation distance between the input and output planes as a new security parameter. The Fresnel JTC encrypting architecture inherits all security properties of JTC system. In this case the information is stored as an intensity distribution called joint Fresnel power distribution (JFPD). Other alternative to classic DRPE and JTC techniques is optical encryption using Hartley transforms. The Hartley transform is performed through two

* Corresponding author.
*E-mail address:* jhonalexis.jaramillo@udea.edu.co (A. Jaramillo).

https://doi.org/10.1016/j.optlaseng.2017.10.008
Received 13 July 2017; Received in revised form 12 September 2017; Accepted 14 October 2017
0143-8166/

Fourier transforms in combination with a Michelson interferometer, and like in the JTC cryptosystem the encoded information is a pure random intensity mask [20].

A further generalization of a DRPE system with improved security was developed in the fractional Fourier domain, first digitally implemented and thereafter experimentally tested [21,22]. This last implementation opened the way to new applications for a digital cryptosystem in the fractional Fourier domain [23–29]. Two experimental approaches of the JTC cryptosystem in the fractional Fourier domain were proposed in [30,31]. These experimental implementations showed the viability of these security systems. Afterwards, the JTC cryptosystem in the fractional Fourier domain was digitally analyzed [32]. Additional to the security parameters due to the encrypting architecture, other parameters like the wavelength [33,34], the polarization [35], key rotation [36] and in-plane shifting [37] can be associated with the security of the fractional JTC (FrJTC) encrypting system.

On the other hand, it is evident the optical encrypting systems had demonstrated its security, versatility and applicability. But from the practical point of view, the information recovered using the optical cryptosystems must be free of any kind of degradation. The users not only ask for security but also for fidelity in the retrieved information. As the decrypted information in optical cryptosystems contains degradation due to the optical processing, reducing or eliminating the noise was a remaining challenge. Several methods that allowed to reduce the degradation over the recovered information, were presented, but none of them allows completely noise-free retrieving [14,38,39].

In order to overcome this issue, the concept of “information container” in optical data processing was introduced by Barrera et al [40]. The security process based on this concept consists in introducing the original information in a container. Afterwards, this container is encrypted using the optical cryptosystem in the same way as any other data. In the recovering process, the right decryption brings the container with the noise and/or degradation due to the optical processing. Therefore, the container must be selected to be tolerant to noise and degradation. Finally, after reading/scanning the decrypted container the original information can be recovered with any kind of degradation [40–42].

Intensive work in the research line of optical information processing using optical containers have been performed [43–52]. The original proposal was applied in several optical encrypting architectures [14,43–47], for optical verification [48–50], integral imaging [51,52] and recently in incoherent optical cryptosystems [53].

As another important aspect, multiplexing methods have been widely used in optical security. These methods are employed to store multiple encrypted information in a single package. Usually the encrypted package is obtained using the same cryptosystem but modifying one of the parameters involved in the process [33,35–37,54–63].

Particularly, the optical encryption of movies has been possible thanks to the multiplexing techniques. The concept of an encrypted movie was introduced for the first time by Mosso et al [64]. The movie joins several encrypted frames corresponding to a time evolving situation employing the same encrypting key. Thanks to a multiplexing operation, the encrypted movie is compacted into a single package. Each frame of the movie is modulated during encryption to avoid the superposition of the frames during decryption. Later, the encryption on time evolving situations was extended to color scenes [65], multiple videos [8] and recently the encryption of a video using chaotic masks was presented [66].

Taking into account the advantages and the flexibilities achieved by recent advances in multiplexing and information containers, we present a protocol based in a fractional optical cryptographic approach [21,22]. Our protocol aims to secure data in a multiuser environment without the detrimental effects of noise. Fractional Fourier transform setups show great flexibility thanks to the many different configurations in which the fractional transform can be achieved [23–32], while also introducing a new security parameter, namely the fractional order of the transform.

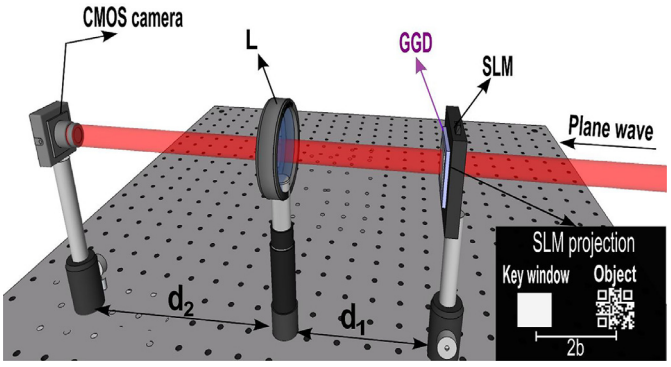



**Fig. 1.** Basic FrJTC cryptosystem scheme. L lens, GGD ground glass diffuser, SLM spatial light modulator, $d_1$ input plane-lens distance, $d_2$ lens-output plane distance.

These benefits make the fractional Fourier cryptosystems of special interest in experimental implementations.

In the following sections, we first demonstrate an experimental implementation of a FrJTC cryptosystem. In this system, the processed information is stored as an intensity distribution named joint fractional Fourier power distribution (JFrPD). We demonstrate the robustness of our proposal by analyzing the performance of these cryptosystems as a function of the fractional order. We then test the capability of the system for processing of QR codes as information containers to perform a noise-free information recovering. Finally, we experimentally demonstrate the ability of the FrJTC cryptosystem to manage multiple encrypted data with different fractional orders.

## 2. Description of the architecture, encryption and decryption processes

In the input plane of the FrJTC encrypting system an object to be encrypted and the key window are projected in a spatial light modulator (SLM) (Fig. 1). The key window is an empty square that determines the size of the encryption key. We attach to the SLM a ground glass diffuser to provide the two random phase masks required by the encrypting architecture. The area of the diffuser in contact with the object provides one of the masks, while the area in contact with the key window will be the encrypting key.

We can represent mathematically the input plane as $e(x,y) = \tau_{b,\alpha}\{c(x,y)\} + \tau_{-b,\alpha}\{l(x,y)\}$. Where $c(x,y) = o(x,y)r(x,y)$ with $o(x,y)$ the object to be encrypted, $r(x,y)$ is a random phase mask and $l(x,y)$ the random phase mask that represents the encryption key, $2b$ is the separation between the object and key window in the input plane, $\tau_{b,\alpha}\{\}$ is the translation fractional Fourier operator and $\alpha$ is the fractional order [67,68]. The combination of the free space propagation between the input plane and the lens, the lens phase, and the free space propagation from the lens to the output plane determines a fractional Fourier transform with a specific fractional order $\alpha$. When $\alpha = \pi/2$ we have the traditional JTC encrypting system [68]. We can express the fractional order as [21,69],

$$\alpha = arcos\left(\frac{\sqrt{(d_1 - f)(d_2 - f)}}{f}\right) \tag{1}$$

where $d_1$ is the input plane-lens distance, $d_2$ is the lens-output plane distance and $f$ is the lens focal length (Fig. 1).

Then, in the CMOS camera we register the JFrPD,

$$I_\alpha(u,w) = |c_\alpha(u,w)|^2 + |l_\alpha(u,w)|^2 + c_\alpha(u,w)l^*{}_\alpha(u,w)\exp[4\pi ibu\csc(\alpha)] + c_\alpha{}^*(u,w)l_\alpha(u,w)\exp[-4\pi ibu\csc(\alpha)] \tag{2}$$

Here $c_\alpha(u,w)$ and $l_\alpha(u,w)$ are the fractional Fourier transform (FrFT) with order $\alpha$ of $c(x,y)$ and $l(x,y)$ respectively, $^*$ means the complex conjugate, csc() is the cosecant trigonometric function and $i = \sqrt{-1}$ is

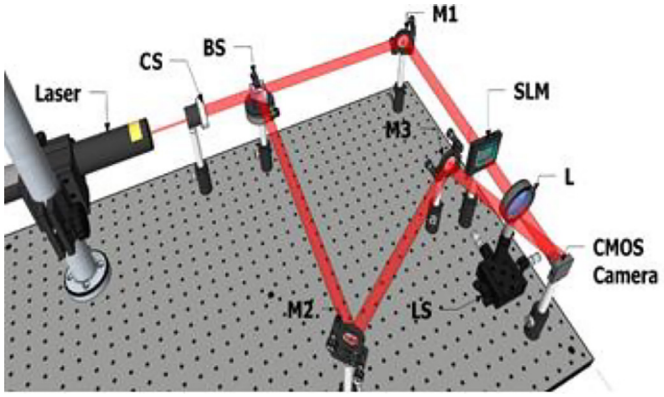



**Fig. 2.** Experimental setup to record the hologram of the encrypting key. CS collimation system, BS beam splitter, LS linear stage, M mirrors and SLM spatial light modulator.

the imaginary number. We can consider a JFrPD as the interference pattern of two subjective speckle patterns on the CMOS camera plane. At least 3 pixels in each dimension are needed to adequately register each modulated speckle of the JFrPD. In this sense, the relationship between the object dimensions and the pixel size of the CMOS camera is $D = 2.4\lambda u/(3\Delta x)$ where $D$ is the system pupil, $u$ is the lens-camera distance, $\lambda$ the wavelength and $\Delta x$ the camera pixel size [70]. In this equation, we have assumed that the lens pupil is larger than the object, so $D$ is the object dimension.

We can register the intensity of $c_\alpha(u, w)$ and $l_\alpha(u, w)$ separately and subtract them from Eq. (2), and then we perform the Fourier transform (FT) of the result, obtaining

$$i_\alpha(\xi,\eta) = \Im\{c_\alpha(u,w){l^*}_\alpha(u,w)\} \otimes \delta(\xi - 2b\csc\alpha,\eta) + \Im\{{c^*}_\alpha(u,w) l_\alpha(u,w)\} \otimes \delta(\xi + 2b\csc\alpha,\eta) \quad (3)$$

Here $\Im$ represents the Fourier transform operator, $\otimes$ denotes the convolution operation, and $\delta()$ is the delta Dirac function. These two terms are the FT of the encrypted data and its complex conjugate. Their spatial separation depends on the distance between the object and the key window in the input plane and the order $\alpha$. We then digitally filter the second term and retain the first and after performing the inverse Fourier transform (IFT), we obtain

$$E_\alpha(u,w) = c_\alpha(u,w){l_\alpha}^*(u,w) \quad (4)$$

Eq. (4) represents the encrypted object. In order to achieve decryption, the knowledge of the key $l_\alpha(u, w)$ is required, however, this function is complex valued. This means that we require a holographic setup to register the key experimentally with a digital camera. For this reason, we implemented the off-axis digital holography setup shown in Fig. 2.

The setup of Fig. 2 is an interferometer, where one arm contains the encrypting setup of Fig. 1 and the other provides the reference plane wave $P(v, w)$, described by,

$$P(u,w) = \exp[2\pi i\lambda(u\sin\theta + w\sin\beta)] \quad (5)$$

where $\lambda$ is the wavelength and $\theta$, $\beta$ are the incidence angles of the reference plane wave on the camera plane. In this plane, the light coming from the encrypting setup interferes with the reference beam, allowing the holographic recording.

In order to obtain the information of the encryption key $l_\alpha(u, w)$, we first project only the key window on the SLM and we register the resulting hologram,

$$H_\alpha(u,w) = |l_\alpha(u,w)|^2 + 1 + l_\alpha(u,w)\exp[-2\pi i\lambda(u\sin\theta + w\sin\beta)] + {l_\alpha}^*(u,w)\exp[2\pi i\lambda(u\sin\theta + w\sin\beta)] \quad (6)$$

If we now perform the FT of Eq. (6) we will obtain a central order related to the autocorrelation of the FT of $l_\alpha(u, w)$, the FT of the encryption key $l_\alpha(u, w)$ and its complex conjugate, with a spatial separation

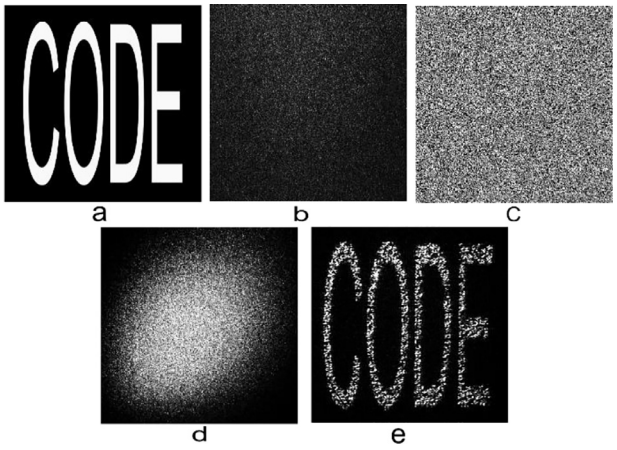



**Fig. 3.** (a) Original object, (b) JFrPD of (a), (c) encrypted data, (d) decrypted data with an incorrect key, and (e) properly decoded data.

that will depend on the incidence angles $\theta$ and $\beta$. Thanks to this separation, we can select the term corresponding to the FT of $l_\alpha(u, w)$ and discard the remaining data. Afterwards, and IFT results in $l_\alpha(u, w)$.

To successfully achieve decryption with the FrJTC system, the encrypted data (Eq. (4)) must be multiplied by the encryption key $l_\alpha(u, w)$, obtaining

$$D_\alpha(u,w) = c_\alpha(u,w){l_\alpha}^*(u,w)l_\alpha(u,w) \quad (7)$$

If we consider the encryption key $l_\alpha(u, w)$ as phase only function, then $l^*_\alpha(u,w)l_\alpha(u,w) = 1$ [71]. With this consideration, after performing an inverse FrFT of order $\alpha$ to Eq. (7), we obtain the decrypted data

$$d(x,y) = c(x,y) \quad (8)$$

The right recovering requires not only having the information of the encryption key and the encrypted data, but also the correct fractional Fourier order. This means that the fractional order represents an extra security key.

## 3. Experimental results

The experimental results were obtained with the setup shown in Fig. 2. The registering medium was a CMOS camera EO-10012M with pixel size 1.6 μm × 1.6 μm and a resolution of 3840 × 2848 pixels. For our CMOS camera, this gives us an upper limit on the object size of approximately 5.3 cm. This is more than twice the size of our SLM, so any object that can be projected on the SLM can be registered with our camera.

A linear stage is employed for changing the input plane-lens and lens-output plane distances (Fig. 2). The illumination source was a JDS UNIPHASE 1135 laser with a wavelength of 632 nm and an input power of 20 mW. A Holoeye 2002 SLM with a pixel size of 32 μm × 32 μm and a resolution of 800 × 600 pixels displays the object and the key window, therefore the displaying area of SLM is 25.6 mm × 19.2 mm. As the size of the input plane of the FrJTC encrypting system must be less or equal than the displaying area of the SLM, in our experiment the size of the input plane (seee SLM projection in Fig. 1) was 11.2 mm × 9.6 mm. In this case, the object has a size of 9.6 mm × 9.6 mm, the key size was 3.2 mm × 3.2 mm, and the separation between the object and key windows in the SLM was $2b = 4.8$ mm. The lens has a focal length of $f = 200$ mm. The distances input plane-lens and lens-output plane were $d_1 = 180$ mm and $d_2 = 250$ mm respectively. Therefore, in this case the fractional order is $\alpha = 1.57 - 0.14i$.

The word CODE was used as test object of our experimental setup (Fig. 3a). Fig. 3(b) shows the JFrPD registered with the CMOS camera. The encrypted data represented by Eq. (4) is shown in Fig. 3(c). When decrypting with the incorrect key the retrieved information is a noise

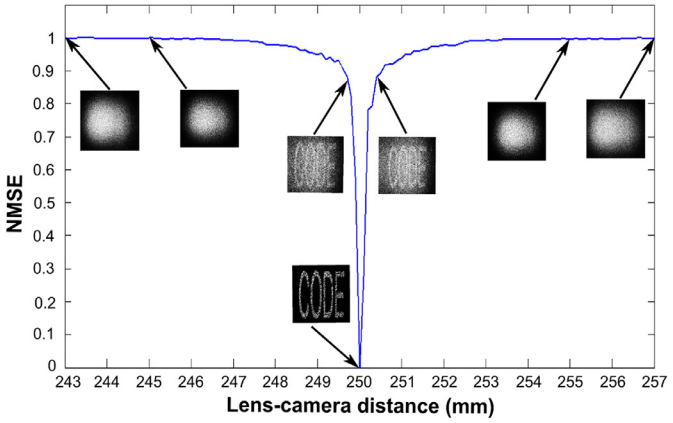



**Fig. 4.** NMSE experimental curve for the retrieved object at different lens-camera distance.

pattern (Fig. 3(d)). On the contrary, when we use both the correct key and the right fractional order it is possible to access to the original information (Fig. 3(e)).

Since the fractional order can be considered a security parameter of the FrJTC system, it is useful to test the tolerance of the decryption procedure when the key and encrypted data are registered with different fractional orders. For this test, we measured the degradation in the quality of the retrieved object as a function of the lens-output plane distance $d_2$ of the FrJTC cryptosystem (see Eq. (1)). We calculate the normalized mean square error (NMSE) between the object decrypted with the encryption key registered in the same lens-output plane distance used during encryption $m(p, q)$ and the decrypted objects $n(p, q)$ for different output plane distances. This variation in $d_2$ is related to a variation of the fractional order as given by Eq. (1). In this case, the NMSE is defined by,

$$NMSE = \frac{\sum_{p,q}^{N,M} |m(p,q) - n(p,q)|^2}{\sum_{p,q}^{N,M} |m(p,q) - n_w(p,q)|^2} \tag{9}$$

Here $p, q$ are the pixels coordinates, $N \times M$ is the number of pixels of the recovered message, and $n_w(p, q)$ was the worst decrypted result.

We can appreciate a gradual quality degradation in the recovered object when the lens-output plane distance changes from the distance employed during encryption (Fig. 4). The inset images pointing at 245 mm and 255 mm lens-camera distances correspond to the decryption after a change of 5 mm. In this case, the object cannot be recovered. Further displacement from this point does not allow any recovery as seen in the inset images at 243 mm and 257 mm. Since a change in the lens-output plane distance results in a change of the fractional order, this result shows that although the fractional order can be considered as an extra security key, it is not a strong security parameter by itself. The tolerance of decryption with a wrong fractional order must be considered when performing multiplexing of an encrypted package in a multi-user environment

## 4. Noise-free recovering

After the experimental demonstration of the security capabilities provided by the FrJTC cryptosystem, we proceed to test the capability of information containers to realize a secure and noise-free recovering procedure in this system. In this work, we use QR codes as containers due to their proven effectiveness for noise-free data recovery after processing by optical cryptosystems like the conventional JTC systems [40,41].

This test consists in introducing our object, the word CODE, in a QR code (Fig. 5(a)). The information container is displayed in the SLM, and then it is encrypted and decrypted following the procedure described in Section 2. The recovered QR code is shown in Fig. 5(b). As expected

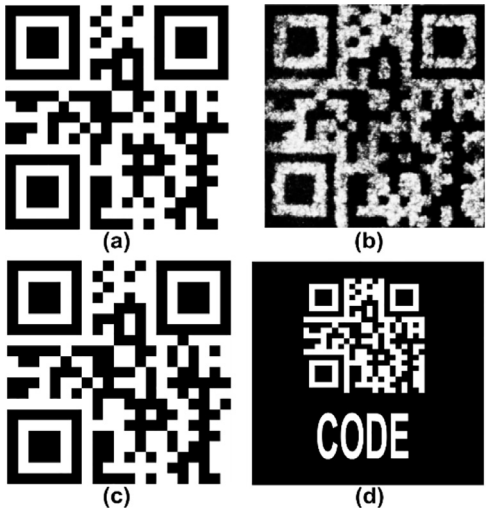



**Fig. 5.** (a) Original QR code of the word CODE, (b) decrypted data, (c) binarization of (b), and (d) noise-free information recovering obtained after scanning (c).

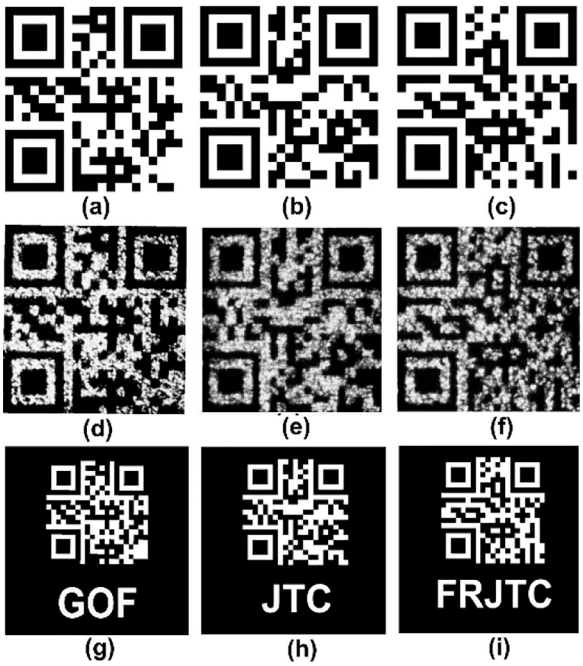



**Fig. 6.** Experimental results of the multiplexing protocol: (a), (b) and (c) original QR codes; (d), (e) and (f) decrypted QR codes with the correct key and the right fractional orders; (g), (h) and (i) noise-free information after binarizing and reading the respective QR codes.

the decrypted code presents a degradation due to the noise produced by optical processing with random masks making direct reading of the code impossible. Since QR codes are always a binary array of blocks, we can apply a binarization procedure to the decrypted QR code to eliminate most of the unwanted noise [41], guaranteeing proper reading by any kind of scanning device (Fig. 5(c)). Finally, the scanning of the decrypted and binarized QR code allows retrieval of the original information, free of any kind of noise (Fig. 5(d)). These last results show experimental confirmation that combining the FrJTC cryptosystem with information containers allows data protection with noise-free retrieval.

## 5. Multi-user encryption with noise-free recovering

As mentioned before, multiplexing is an appropriate technique to store in a single package several encrypted objects. It may be desirable

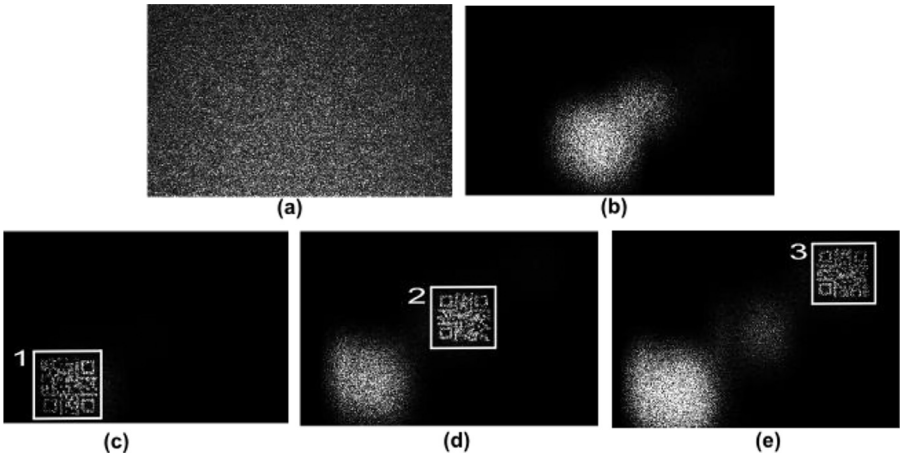



**Fig. 7.** Multiplexing of the encrypted QR codes of Fig. 6. (a) Multiplexed package, (b) decryption attempt with a wrong key, (c) QR code of the expression GOF decrypted with correct key and fractional order $\alpha = 1.42$ (inset window 1), (d) QR code of the expression JTC decrypted with correct key and fractional order $\alpha = 1.57$ (inset window 2), and (e) QR code of the expression FRJTC decrypted with correct key and fractional order $\alpha = 1.57 - 0.14i$ (inset window 3).

to send a single encrypted package to several users, multiplexed in such a way that each user can only access a specific data. With the FrJTC cytosystem, this can be easily achieved by giving to each authorized user a fractional order and its corresponding decryption key. These fractional orders associated to each user must be different enough to ensure no overlapping according to the tolerance ranges demonstrated in Fig. 4. Thus, our multiuser encryption protocol for noise-free recovery can be summarized as follows:

1. A fractional order is assigned to each user.
2. The data to be encrypted and sent to each user is codified into different QR codes.
3. Each QR code is encrypted with the fractional order corresponding to the receiver.
4. All encrypted QR codes are multiplexed into a single package.
5. All users receive the package of the multiplexed encrypted QR codes and the decryption key, while each user receive the assigned fractional order.
6. The user decrypts with its corresponding fractional order
7. The retrieved QR code is read and the original information is recovered free of noise.

We multiplexed three encrypted QR codes with different fractional Fourier orders. The axial position of the transforming lens is changed during the encryption of each QR code, preserving the distance between the input and output planes and the same ground glass diffuser.

In Fig. 6 we see experimental results of encryption decryption of the QR codes corresponding to the expressions GOF, JTC and FRJTC. The encrypting process of each QR code is the same described in Section 2. These codes are encrypted with the fractional orders $\alpha = 1.42$, $\alpha = 1.57$ and $\alpha = 1.57 - 0.14i$ respectively.

Before multiplexing the encrypted codes of Fig. 6 into a single package, during the filtering process we reposition the encrypted information to avoid crosstalk after recovery (Fig. 7(c), (d) and (e)) [7,42,44]. Then, the encrypted and repositioned information is multiplexed.

In general, multiplexing of the encrypted data with different fractional orders can be expressed as [55],

$$M(u,w) = \sum_{j=1}^{N} c_{\alpha_j}(u,w) l^{*}_{\alpha_j}(u,w) \exp[2\pi i(x_j u + y_j w)\csc(\alpha_j)] \tag{10}$$

Here $j = 1, 2 \ldots N$, and $x_j$, $y_j$ are the new coordinates where each data is positioned during filtering. Each key $l_{\alpha_j}(u,w)$ is registered for a specific position of the lens between the input and output planes. These positions correspond to different fractional orders $\alpha_j$. The user with the information of the jth key can only access to the information corresponding to the jth data. The information of the non-decrypted data will appear as white noise. This noise is not superposed with the recovered information thanks to the positioning process carried out over the encrypted data before multiplexing.

The results in Fig. 7 demonstrate the experimental validity of the proposed protocol applied to the QR codes of Fig. 6(a), the right decryption of the QR code requires both the correct fractional order and the correct key (Fig. 7(c), (d) and (e)). An attempt to access to the information contained in the multiplexed package without the correct key, results in a random noise distribution (Fig. 7(b)). The decrypted QR codes are then binarized and scanned to obtain the original information free of any kind of degradation (Fig. 6(g), (h) and (i)). Note that the fractional order $\alpha = 1.57$ corresponds to a JTC cryptosystem. As the input plane-lens distance increases, more energy is lost due to light that falls outside the lens pupils after propagation. As a consequence, each recovered data in Fig. 7(c), (d) and (e) are reconstructed with different intensities. This limits the practical range of operation of the system for a given lens size.

## 6. Conclusions

In this contribution, we demonstrate that the experimental FrJTC encrypting system is capable of information security with noise-free recovery as well as useful in a multi-user environment. An authorized user requires not only the correct key, but also the adequate fractional Fourier order to access to the encrypted information. The experimental results show that the fractional Fourier order can be considered as an extra security key. QR codes used as “information containers” in optical cryptosystems allow for noise-free information recovery. We show that these containers can be successfully processed with the FrJTC cryptosystem.

Encrypted information containers are combined with multiplexing to manage in multiple data in a secure way along with noise-free recovery, thus stablishing a multi-user protocol for optical encryption in a FrJTC cryptosystem. This novel protocol can be considered as a way of addressing real-world use cases of optical cryptosystems. The theoretical description and the experimental results included in this contribution, not only demonstrate the applicability, versatility and potential of the FrJTC encrypting system, but also can encourage new research to explore novel security protocols based in this optical security system.

## Acknowledgment

This research was performed under grants from Comité para el Desarrollo de la Investigación -CODI (Universidad de Antioquia-Colombia), CONICET Nos. 0849/16 and 0549/12 (Argentina), and Facultad de Ingeniería, Universidad Nacional de La Plata No. 11/I215 (Argentina). John

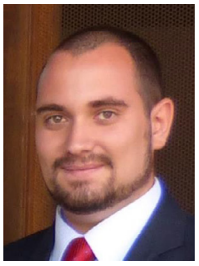
Fredy Barrera Ramírez acknowledges the support from the International Centre for Theoretical Physics ICTP Associateship Scheme.

## References


[1] Javidi B, Carnicier A, Chen W, Chen X, Pérez-Cabré E, Millán M, et al. Roadmap in optical security. J Opt 2016;19:013001.
[2] Liu S, Guo C, Sheridan JT. A review of optical image encryption techniques. Opt Laser Technol 2014;57:327–42.
[3] Refregier P, Javidi B. Optical image encryption based on input plane and Fourier plane random encoding. Opt Lett 1995;20:767–9.
[4] Nomura T, Javidi B. Optical encryption using a joint transform correlator architecture. Opt Eng 2000;39:2031–5.
[5] Mehra I, Rajput S, Nishchal N. Cryptoanalysis of an image encryption scheme based on joint transform correlator with amplitude- and phase- truncation approach. Opt Lasers Eng 2014;52:167–73.
[6] Nomura T, Mikan S, Morimoto Y, Javidi B. Secure optical data storage with random phase key codes by use of a configuration of a joint transform correlator. Appl Opt 2003;42:1508–14.
[7] Barrera J, Vélez A, Torroba R. Experimental multiplexing protocol to encrypt messages of any length. J Opt 2013;15:055404.
[8] Barrera J, Tebaldi M, Ríos C, Rueda E, Bolognini N, Torroba R. Experimental multiplexing of encrypted movies using a JTC architecture. Opt Express 2012;20:3388–93.
[9] Rueda E, Barrera J, Henao R, Torroba R. Optical encryption with a reference wave in a joint transform correlator architecture. Opt Commun 2009;282:3243–9.
[10] Barrera J, Vargas C, Tebaldi M, Torroba R. Chosen-plaintext attack on a joint transform correlator encrypting system. Opt Commun 2010;283:3917–21.
[11] Barrera J, Vargas C, Tebaldi M, Torroba R, Bolognini N. Known-plaintext attack on a joint transform correlator encrypting system. Opt Lett 2010;35:3553–5.
[12] Zhang C, Liao M, He W, Peng X. Ciphertext-only attack on a joint transform correlator encryption system. Opt Express 2013;21:28523–30.
[13] Vilardy J, Millán M, Pérez-Cabré E. Improved decryption quality and security of a joint transform correlator-based encryption system. J Opt 2012;15:025401.
[14] Vélez A, Barrera J, Torroba R. Innovative speckle noise reduction procedure in optical encryption. J Opt 2017;19:055704.
[15] Yan A, Poon TC, Hu Z, Zhang J. Optical image encryption using optical scanning and fingerprint keys. J. Mod. Opt. 2016;63:38–43.
[16] Liao X, Qin Z, Ding L. Data embedding in digital images using critical functions. Signal Processing: Image 2017;58:146–56.
[17] Liao X, Shu C. Reversible data hiding in encrypted images based on absolute mean difference of multiple neighboring pixels. J Vis Commun Image Represent 2015;28:21–7.
[18] Vilardy J, Millán M, Pérez-Cabré E. Nonlinear optical security system based on a joint transform correlator in the Fresnel domain. Appl Opt 2014;53:1674–82.
[19] Barrera J, Jaramillo A, Vélez A, Torroba R. Experimental analysis of a joint free space cryptosystem. Opt Laser Eng 2016;83:126–30.
[20] Chen L, Zhao D. Optical image encryption with Hartley transforms. Opt Lett 2006;31:3438–40.
[21] Unnikrishnan G, Singh K. Double random fractional Fourier-domain encoding for optical security. Opt Eng 2000;39:2853–9.
[22] Unnikrishnan G, Joseph J, Singh K. Optical encryption by double-random phase encoding in the fractional Fourier domain. Opt Lett 2000;25:887–9.
[23] Banghe Z, Shutian L. Optical image encryption based on the generalized fractional convolution operation. Opt Commun 2001;195:371–81.
[24] Zhang Y, Zheng CH, Tanno N. Optical encryption based on iterative fractional Fourier transform. Opt Commun 2002;202:277–85.
[25] Hennelly B, Sheridan J. Image encryption and the fractional Fourier transform. Optik 2013;114:251–65.
[26] Shutian L, Li Y, Banghe Z. Optical image encryption by cascaded fractional Fourier transform with randon phase filtering. Opt Commun 2001;187:57–63.
[27] Banghe Z, Shutian L, Qiwen R. Optical image encryption based on multifractional Fourier transforms. Opt Lett 2000;25:1159–61.
[28] Shutian L, Quanlin M, Banghe Z. Optical image encryption with multistage and multichannel fractional Fourier-domain filtering. Opt Lett 2001;26:1242–4.
[29] Hennelly B, Sheridan J. Optical image encryption by random shifting in fractional Fourier domains. Opt Lett 2003;28:269–71.
[30] Lu D, Jin W. Color image encryption based on joint fractional Fourier transform correlator. Opt Eng 2011;50:068201.
[31] Wang Q, Guo Q, Lei L, Zhou J. Optical image encryption based on joint fractional transform correlator architecture and digital holography. Opt Eng 2013;52:048201.
[32] Villardy J, Torres Y, Millan M, Pérez-Cabré E. Generalized formulation of an encryption system based on a joint transform correlator and fractional Fourier transform. J Opt 2014;16:125405–13.
[33] Situ G, Zhang J. Multiple-image encryption by wavelength multiplexing. Opt Lett 2005;30:1306–8.
[34] Amaya D, Tebaldi M, Torroba R, Bolognini N. Wavelength multiplexing encryption using joint transform correlator architecture. Appl Opt 2009;48:2099–104.
[35] Barrera J, Henao R, Tebaldi M, Bolognini N, Torroba R. Multiplexing encrypted data by using polarized light. Opt Commun 2006;260:109–12.
[36] Rueda E, Rios C, Barrera J, Henao R, Torroba R. Experimental multiplexing approach via key code rotations under a joint transform correlator scheme. Opt Commun 2011;284:2500–4.
[37] Barrera J, Henao R, Tebaldi M, Bolognini N, Torroba R. Multiplexing encryption–decryption via lateral shifting of a random phase mask. Opt Commun 2006;259:532–6.
[38] Javidi B, Towghi N, Maghzi N, Verrall S. Error-reduction techniques and error analysis for fully phase- and amplitude-based encryption. Appl Opt 2000;39:4117–30.
[39] Javidi B, Sergent A, Ahouzi E. Performance of double phase encoding encryption technique using binarized encrypted images. Opt Eng 1998;37:565–9.
[40] Barrera J, Mira A, Torroba R. Optical encryption and QR codes: Secure and noise-free information retrieval. Opt Express 2013;21:5373–8.
[41] Barrera J, Mira A, Torroba R. Experimental QR code optical encryption: noise-free data recovering. Opt Lett 2014;39:3074–7.
[42] Barrera J, Vélez A, Torroba R. Experimental scrambling and noise reduction applied to the optical encryption of QR codes. Opt Express 2014;22:20268–77.
[43] Qin Y, Wang H, Wang Z, Gong Q, Wang D. Encryption of QR code and grayscale image in interference-based scheme with high quality retrieval and silhouette problem removal. Opt Laser Eng 2016;84:62.
[44] Trejos S, Barrera J, Torroba R. Optimized and secure technique for multiplexing QR code images of single characters: Application to noiseless messages retrieval. J Opt 2015;17:085702.
[45] Qin Y, Zhang Y. Information encryption in ghost imaging with customized data container and XOR operation. IEEE Photonics J 2017;9:7802208.
[46] Vélez A, Barrera J, Torroba R. Customized data container for improved performance in optical cryptosystems. J Opt 2016;18:125702.
[47] Jiao S, Zou W, Li X. QR code based noise-free optical encryption and decryption of a gray scale image. Opt Commun 2017;387:235.
[48] Carnicer A, Hassanfiroozi A, Latorre-Carmona P, Huang Y, Javidi B. Security authentication using phase-encoded nanoparticle structures and polarized light. Opt Lett 2015;40:135–8.
[49] Markman A, Javidi B, Tehranipoor M. Photon-counting security tagging and verification using optically encoded QR codes. IEEE Photonics J 2014;6:1–9.
[50] Li W, Shen Y, Chen Z, Cui Q, Li S, Chen L. Demonstration of patterned polymer-stabilized cholesteric liquid crystal textures for anti-counterfeiting two-dimensional barcodes. Appl Opt 2017;56:601–6.
[51] Markman A, Wang J, Javidi B. Three-dimensional integral imaging displays using a quick-response encoded elemental image array. Optica 2014;1:332–5.
[52] Xing Y, Wang Q, Xiong Z, Deng H. Encrypting three-dimensional information system based on integral imaging and multiple chaotic maps. Opt Eng 2016;55:023107.
[53] Cheremkhin P, Krasnov V, Rodin V, Starikov R. QR code optical encryption using spatially incoherent illumination. Laser Phys Lett 2017;14:026202.
[54] Barrera J, Henao R, Tebaldi M, Torroba R, Bolognini N. Multiple-encoding retrieval for optical security. Opt Commun 2007;276:231–6.
[55] Barrera J, Rueda E, Ríos C, Tebaldi M, Bolognini N, Torroba R. Experimental opto-digital synthesis of encrypted sub-samples of an image to improve its decoded quality. Opt Commun 2011;284:4350–5.
[56] Wang X, Zhao D. Multiple-image encryption based on nonlinear amplitude-truncation and phase-truncation in Fourier domain. Opt Commun 2011;284:148–52.
[57] Jain A, Ahmad M, Khare V. A ridgelet based symmetric multiple image encryption in wavelet domain using chaotic key image. Eco-friendly comput commun syst 2012;1:135–44.
[58] Kim DH, Jeon S, Park NC, Park YP. Crosstalk analysis for multiple-image encryption and image-quality equalization technology. Microsys Technol 2015;21:2717–25.
[59] Deng P, Diao M, Shan M, Zhong Z, Zhang Y. Multiple-image encryption using spectral cropping and spatial multiplexing. Opt Commun 2016;359:234–9.
[60] Singh N, Sinha A. Chaos based multiple image encryption using multiple canonical transforms. Opt Laser Technol 2010;42:724–31.
[61] Fan D, Meng X, Wang Y, Yang X, Pan X, Peng X, et al. Multiple-image authentication with a cascaded multilevel architecture based on amplitude field random sampling and phase information multiplexing. Appl Opt 2015;54:3204–15.
[62] Qin Y, Gong Q. Multiple-image encryption in an interference-based scheme by lateral shift multiplexing. Opt Commun 2014;315:220–5.
[63] Lin C, Shen X, Tang R, Zou X. Multiple images encryption based on Fourier transform hologram. Opt Commun 2012;285:1023–8.
[64] Mosso F, Barrera J, Tebaldi M, Bolognini N, Torroba R. All-optical encrypted movie. Opt Express 2011;19:5706–12.
[65] Mosso F, Tebaldi M, Barrera J, Bolognini N, Torroba R. Pure optical dynamical color encryption. Opt Express 2011;19:13779–86.
[66] Saini N, Sinha A. Video encryption using chaotic masks in joint transform correlator. J Opt 2015;17:035701.
[67] Torres R, Pellat-Finet P, Torres Y. Fractional convolution, fractional correlation and their translation invariance properties. Signal Process 2010;90:1976–84.
[68] Lohmann A, Mendlovic D. Fractional joint transform correlator. Appl Opt 1997;36:7402–7.
[69] Unnikrishnan G, Singh K. Optical encryption using quadratic phase systems. Opt Commun 2001;193:51–67.
[70] Dainty JC. Laser speckle and related phenomena. Spring-Verlag; 1984.
[71] Unnikrishnan G, Joseph J, Singh K. Optical encryption system that uses phase conjugation in a photorefractive crystal. Appl Opt 1998;37:8181–6.

**John Alexis Jaramillo Osorio** received his BSc degree in physics from Antioquia University (Medellin, Colombia) in 2016. He is now MSc student at the Optics and Photonic's Group from Antioquia University and teacher assistant in the faculty of engineering from the same university. He has published 1 peer reviewed papers in international journals. His research is centered in areas in the field of encryption and validation, optical processing and digital holography.

**John Fredy Barrera Ramírez** received his BSc, MSc, and PhD degrees in physics from Antioquia University (Medellín, Colombia) in 2001, 2003, and 2007, respectively. Since 2006 he has been with Antioquia University, where he is Professor in the Physics Institute and coordinator of the Optics and Photonic's Group. He is "Junior Associate" of the International Centre for Theoretical Physics and "Young Affiliate" of the World Academy of Sciences, "Senior Member" of the Optical Society and member of the International Society for Optics and Photonics. He has authored 50 peer-reviewed international papers, one invention patent, 18 publications in international conference proceedings and 18 publications in national peer-reviewed journals with more than one thousand citations.



**Alejandro Velez Zea** received his BSc degree in physics from Antioquia University (Medellin, Colombia) in 2014. He is now a PhD student at the Center for Optical Research of La Plata (CIOp), Argentina and teacher assistant in the School of Engineering at the National University of La Plata in Argentina. He has published 10 peer reviewed papers in international journals, with research centered around optical encryption, digital holography and optical data compression.

**Professor Roberto Torroba**, published over 120 papers in peer reviewed journals, and a number of contributions in Congresses around the world. He serves as reviewer in international journals, supervised several doctoral thesis, and much of his work was highlighted and distinguished in prestigious journals. Presently he is Member of the Argentinean research council as Superior Researcher, full Professor at the School of Engineering at the University of La Plata in Argentina and Director of the Unit of Research and Development "OPTIMO". His areas of interest are in the field of optical processing, encryption and validation, digital holography and virtual optics.