Experimental analysis of a joint free space cryptosystem

Article *in* Optics and Lasers in Engineering · August 2016

DOI: 10.1016/j.optlaseng.2016.03.010

4 authors:

Alejandro Velez Zea
Centro De Investigaciones Opticas Conicet
10 PUBLICATIONS **30** CITATIONS
SEE PROFILE

Alexis Jaramillo
University of Antioquia
1 PUBLICATION **1** CITATION
SEE PROFILE

John Fredy Barrera Ramírez
University of Antioquia
75 PUBLICATIONS **724** CITATIONS
SEE PROFILE

Roberto Torroba
Centro De Investigaciones Opticas (CIOp), La …
136 PUBLICATIONS **1,196** CITATIONS
SEE PROFILE

Optics and Lasers in Engineering 83 (2016) 126–130

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

Experimental analysis of a joint free space cryptosystem

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

[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), PO Box 3, C.P 1897, La Plata, Argentina
[c] UID OPTIMO, Facultad de Ingenieria, Universidad Nacional de La Plata, La Plata, Argentina

ARTICLE INFO

Article history:
Received 7 August 2015
Received in revised form
12 February 2016
Accepted 8 March 2016

Keywords:
Optical security
Encryption
Fresnel transform
Optical data processing

ABSTRACT

In this paper, we analyze a joint free space cryptosystem scheme implemented in an actual laboratory environment. In this encrypting architecture, the object to be encoded and the security key are placed side by side in the input plane without optical elements between the input and the output planes. In order to get the encrypted information, the joint Fresnel power distribution JFPD coming from the input plane is registered in a CMOS camera. The information of the encrypting key is registered with an off axis Fresnel holographic setup. The data registered with the experimental setup is digitally filtered to obtain the encrypted object and the encryption key. In addition, we explore the performance of the experimental system as a function of the object-camera and key-camera distances, which are two new parameters of interest. These parameters become available as a result of developing this encrypting scheme. The theoretical and experimental analysis shows the validity and applicability of the cryptosystem.

1. Introduction

Optical image encryption opened a new route in information security to protect data from counterfeiting and unauthorized access. We are able to meet this challenge from the nanoworld [1] to the use of QR codes as "information containers" [2–5]. The voyage started with the contribution of Refregier and Javidi [6], introducing the concept and the first implementation on the so called 4f encrypting architecture. The optical encryption scheme is called double random phase encoding, because involves two random phase masks, one in the input plane and a second in the Fourier domain. It can be shown that if the phases in these masks can be described as statistically independent, then the resulting encrypted image is a white-noise distribution. Alternatively, other encrypting schemes were developed under the joint transform correlator (JTC) architecture [7–9]. This optical setup is more compact than the conventional 4f holographic scheme, because the object and reference beams share a single optical system consisting of one Fourier-transforming lens. The JTC encrypting architecture also offers two major advantages: the encrypted information is stored as an intensity distribution in a recording media and the decryption process is performed using the encoding key, not its complex conjugate. These advantages decrease the requirements for an experimental implementation in a laboratory environment, thus becoming the favored architecture for most practical applications [5,10,11]. Digital holographic setups were developed to implement the JTC cryptosystem [12,13], bringing new exciting possibilities to optical encryption. On the other hand, several techniques have been proposed in the literature to optically encrypt images using the gyrator transform [14,15] and the fractional Fourier transform (FFRT) [16–24].

An alternative optical security system for image encryption based on a nonlinear JTC in the Fresnel domain (FrD) was proposed [25]. In the suggested scheme, the encryption process is performed by a lensless optical system that encrypts the desired data into an intensity pattern called joint Fresnel power distribution (JFPD). Like in the traditional JTC cryptosystem, the key is a random complex mask. To further reduce the speckle contamination of the decrypted object and enhance security, a nonlinear modification is performed. The decryption protocol is performed through a Fresnel transform, allowing to control the reconstruction plane and magnification of the decrypted image. We will refer this system as a joint free space cryptosystem (JFSC), because the encryption is achieved by the joint interference of the freely propagated key and object waves.

As encryption methods evolved, additional parameters were included to reinforce the security level and to allow for the multiplexing of data, ensuring that the object can be recovered only when using the right combination of those optical parameters. In the literature, we find contributions where the wavelength [26,27], the

* Corresponding author.
E-mail address: john.barrera@udea.edu.co (J.F.B. Ramírez).

http://dx.doi.org/10.1016/j.optlaseng.2016.03.010
0143-8166/

polarization [28], in-plane shifting [29], rotation [30], modulation [31], axial shift [32], and other parameters were proposed and demonstrated as valid encrypting parameters. In particular, studies regarding the valid range of each of these parameters are crucial to establish the adequate working conditions under which these parameters are useful.

Although these studies are indicatives of the validity of the proposed parameters, we still find that practical implementations are bonded to restrictions arising from practical laboratory conditions. A careful experimental study would reveal the actual behavior in a laboratory environment. In particular, we find that the behavior of the system cannot be explained by a single factor when the propagation length is changed. Besides, a comprehensive study of the real effects of this parameter requires an experimental implementation in order to take into account for all possible factors.

Additionally, during the implementation of the experimental setup, we explore the performance of the system as a function of the object-camera and key-camera distances. We show that in the JFSC scheme there is a gradual degradation of the recovered object as the object-camera distance increases, resulting in a practical limitation on the operational range of the system. Besides, the system tolerance to axial displacements of the encryption key is significant. Both features must be taken into account in any future implementation of this system, either simulated or experimental.

2. Description of the architecture and the encryption–decryption process

In the proposed JFSC architecture, we project in the input plane of the optical system both the object to be encrypted and a blank key window. This window determines the size of the encryption key. We use a spatial light modulator (SLM) to display the object and the key window in our physical setup, which limits their maximum size and the details of the object due to its display resolution and pixel size. We attach to the SLM a ground glass diffuser covering both the object and the key window (Fig. 1), which will provide both random phase masks.

As in the JFSC architecture, there is no lens that performs an optical Fourier transform of the input plane, the pattern registered by the CMOS camera corresponds to the free space propagation of the input plane, which is described mathematically by a Fresnel transform (FRT) [33]. Considering $c(x,y)=o(x,y)r(x,y)$ with $o(x,y)$ the object to be encrypted, $r(x,y)$ and $l(x,y)$ random phase masks, the last representing the encrypting key, the JFPD is then

$$I(v,w)=|C_z(v,w)|^2+|L_z(v,w)|^2+C_z(v,w)L_z^*(v,w)e^{-4\pi iav}+C_z^*(v,w)L_z(v,w)e^{4\pi iav} \quad (1)$$

where $C_z(v,w)$ and $L_z(v,w)$ are the Fresnel transforms of $c(x,y)$ and $l(x,y)$ at propagation distance z, $v=x/\lambda z$ and $w=y/\lambda z$ are the coordinates in the Fresnel plane, and λ is the wavelength. The exponential expressions will result in interference fringes in the JFPD whose frequency will depend on the separation $2a$ between key and object. Due to the limited pixel size of the recording medium, this separation cannot be made arbitrarily large. In the proposed JFSC, the maximum separation between key window and object is given by [34]

$$a=z\tan\left(\arcsin\left(\frac{\lambda}{4\Delta x}\right)\right) \quad (2)$$

where Δx is the pixel size of the CMOS camera. The intensity of the FRT of object and key windows can be registered separately and then subtracted from Eq. (1), resulting in

$$I(v,w)=C_z(v,w)L_z^*(v,w)e^{-4\pi iav}+C_z^*(v,w)L_z(v,w)e^{4\pi iav} \quad (3)$$

These two terms can be isolated by performing the Fourier transform (FT) of Eq. (3), obtaining

$$i(\xi,\eta)=FT\{C_z(v,w)L_z^*v,w)\}\otimes\delta(\xi+2a,\eta)+FT\{C_z^*(v,w)L_z(v,w)\}\otimes\delta(\xi-2a,\eta) \quad (4)$$

where $FT\{\}$ represents the FT operation, the symbol $\otimes$ denotes the convolution, and $\delta()$ is the delta Dirac function. The spatial separation caused by the convolution with the delta functions allows to select one of these two terms and to discard the other. The selected term is digitally positioned in any desired spatial coordinate (x',y'), and then performing the inverse Fourier transform (IFT), we obtain

$$E_z(v,w)=C_z(v,w)L_z^*(v,w)e^{2\pi i(vx'+wy')} \quad (5)$$

In Eq. (5), we find the filtered encrypted object along a phase factor with the object coordinates after decryption. In order to recover the encrypted object, we must first multiply Eq. (5) by the FRT of the encrypting key and then we perform the adequate inverse Fresnel transform (IFRT). Attempting to decrypt without multiplying by the correct key will result in a speckle pattern instead of the original object.

Consequently, to accomplish the decryption process, we need the information of the encrypting key. Since this information has both phase and amplitude components, we use the off-axis digital holography setup shown in Fig. 2.

In order to register the information of the encryption key $L_z(v,w)$, we only project the key window on the SLM and register the resulting hologram

$$H(v,w)=|P(v,w)|^2+|L_z(v,w)|^2+P(v,w)L_z^*(v,w)+P^*(v,w)L_z(v,w) \quad (6)$$

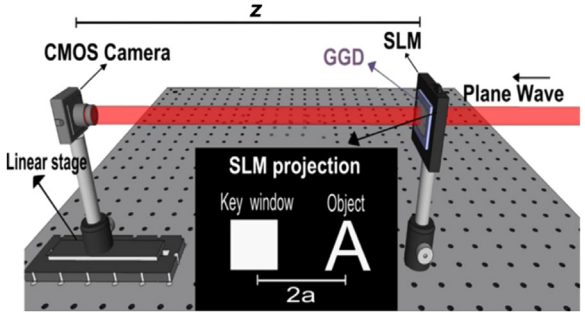

Fig. 1. Basic JFSC scheme. SLM spatial light modulator, GGD ground glass diffuser, and z propagation distance.

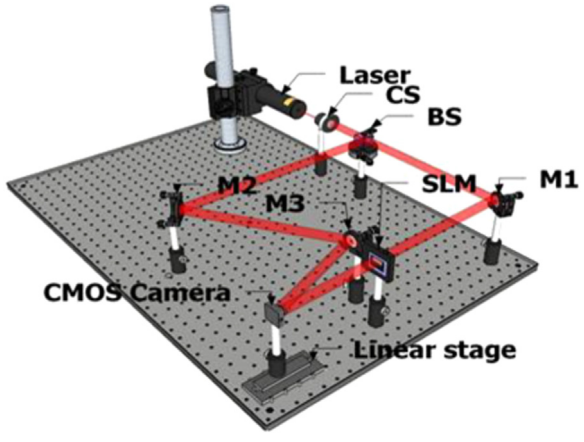

Fig. 2. Experimental setup to record the hologram of the encrypting key, CS collimation system, BS beam splitter, M mirror, and SLM spatial light modulator.

here $P(v,w)$ is the reference plane wave that can be described as

$$P(v,w) = A\exp(-i2\pi z(v\cos\alpha + w\cos\beta)) \tag{7}$$

where A is the uniform amplitude of the reference wave, and α and β are its tilt angles. Subtracting the central order terms $|L_z(v,w)|^2$ and $|P(v,w)|^2$ from Eq. (6), and performing an FT we get

$$H(\xi,\eta) = l_z(\xi,\eta) \otimes \delta(\xi + z\cos\alpha, \eta + z\cos\beta) + l_z^*(\xi,\eta) \otimes \delta(\xi - z\cos\alpha, \eta - z\cos\beta) \tag{8}$$

These remaining terms contain the information of the FRT of the encrypting key and its complex conjugate. As we can see from Eq. (8), the separation of these terms depends on the tilt of the reference plane wave and the object-camera distance z. Therefore, due to the limited pixel size of the recording medium, the tilt of the reference plane wave must be carefully selected to ensure an adequate recording of the key hologram, yet large enough to avoid crosstalk between these terms. Finally, the second term is discarded and the first term is centered. Then, by performing the inverse Fourier transform, we get $L_z(v,w)$.

An authorized user can access the original information after getting the encrypted data and the information of the encrypting key. In order to recover the encrypted object, we multiply Eq. (5) by $L_z(v,w)$, obtaining

$$E_z(v,w) = C_z(v,w)L_z(v,w)L_z^*(v,w)e^{2\pi i(x'v+y'w)} \tag{9}$$

As $L_z(v,w)$ is taken to be approximately a phase only function [35], the product of $L_z(v,w)$ with its complex conjugate is then equal to 1. After using this approximation, we obtain

$$E_z(v,w) = C_z(v,w)e^{2\pi i(x'v+y'w)} \tag{10}$$

And performing the IFRT, we finally obtain

$$e(x,y) = c(x,y) \otimes \delta(x-x', y-y') \tag{11}$$

which represents the decrypted object positioned at the desired coordinates (x', y'). As the previous discussion shows, in this architecture, the decryption process requires not only the encrypted data and the encryption key, but also the value of the propagation distance z, in order to perform the adequate IFRT required for the recovery of the original information.

3. Experimental results

The experimental results shown in this paper were obtained with the setup of Fig. 2. All objects were registered using an EO-10012M CMOS camera with pixel size 1.67 × 1.67 μm and resolution of 3840 ×2748 pixels. The illumination source was a DPSS laser with a wavelength of 532 nm. The object and key windows have a size of 3.2 mm × 3.2 mm with 3.87 mm of separation and are projected on a Holoeye 2002 SLM with a resolution of 800 × 600 pixels and a pixel size of 32 μm × 32 μm. In order to perform the axial shift tests, a 50 cm linear stage was used.

We test the basic capabilities of the experimental JFSC by employing the letter A as object (Fig. 3(a)). Fig. 3 shows the experimental results using the procedure described in Section 2. In this case, the distance between the input and output planes is $z = 350$ mm, and we register the JFPD using a CMOS camera (Fig. 3(b)). When using the correct key, the original information is retrieved (Fig. 3(c)), with a level of speckle noise comparable to other optical cryptosystems. As expected, it is not possible to recover the object when decrypting with an incorrect key (Fig. 3(d)).

Additionally, we test the decryption results of objects registered with different object-camera distances, as shown in Fig. 4.

If we maintain the laser intensity and the camera gain both equal when registering the JFPD and the key hologram at different distances, we can appreciate a qualitative degradation of the recovered object. Notice the gradual loss of intensity and the increase in speckle size of the decrypted image shown in Fig. 4 as we increase the distance object-camera. In order to measure the degradation of the image quality as a function of the propagation distance, we calculate the normalized mean square error (NMSE) between the decrypted object from a JFPD registered with different object-camera distances $m_z(p,q)$ and the original object $m(p,q)$. Then, the NMSE is defined by

$$\mathrm{NMSE} = \frac{\sum_{p,q}^{N,M} |m(p,q) - m_z(p,q)|^2}{\sum_{p,q}^{N,M} |m(p,q) - m_w(p,q)|^2} \tag{12}$$

where (p,q) are the pixels coordinates, N and M are the number of horizontal and vertical pixels of the recovered message, respectively, and $m_w(p,q)$ is the worst expected case.

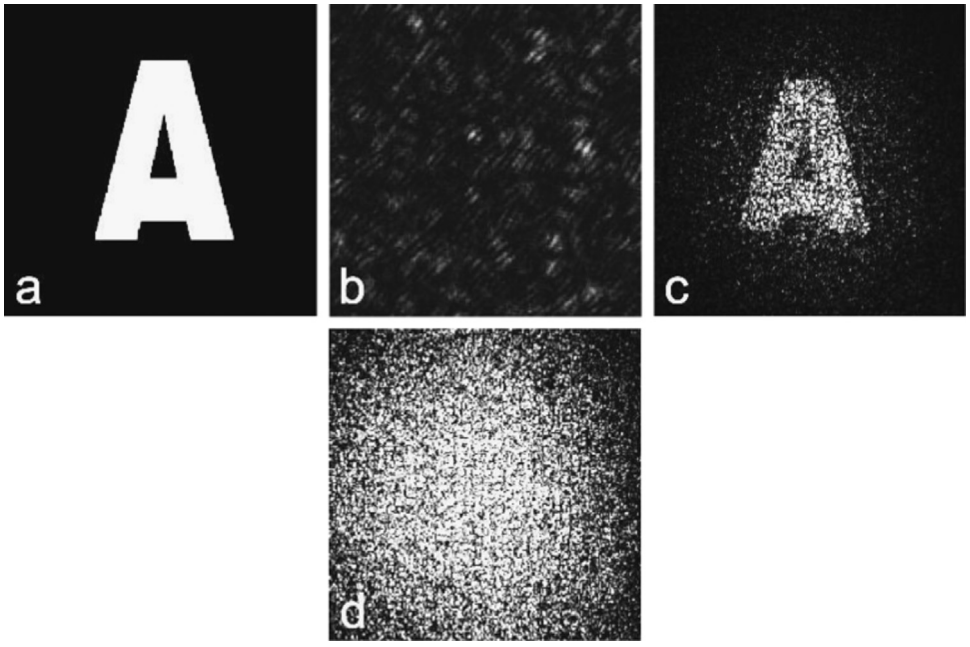

Fig. 3. (a) Original object. (b) JFPD of (a). (c) Decrypted object with the correct key. (d) Decrypted object with the incorrect key.

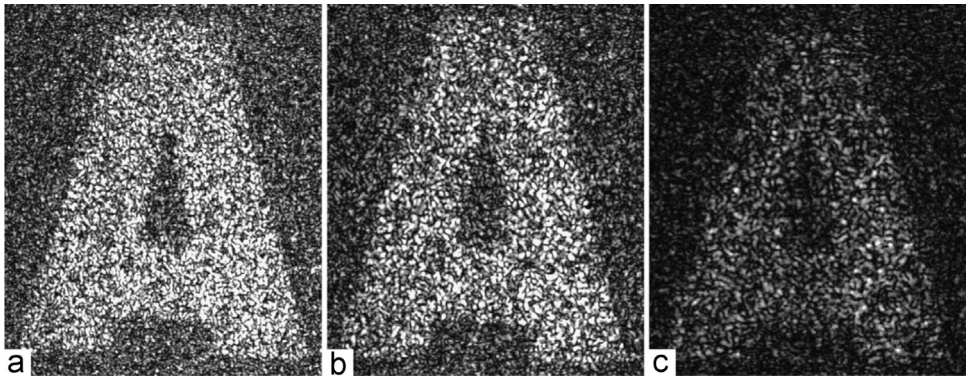

Fig. 4. Right decryption of an encrypted object registered at (a) 250 mm, (b) 300 mm and (c) 350 mm.

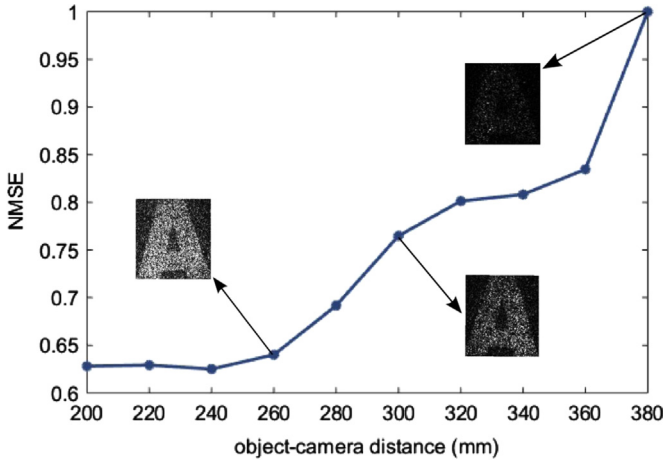

Fig. 5. NMSE curve for the retrieved objects using JFPD registered at different object-camera distances, compared to the original object.

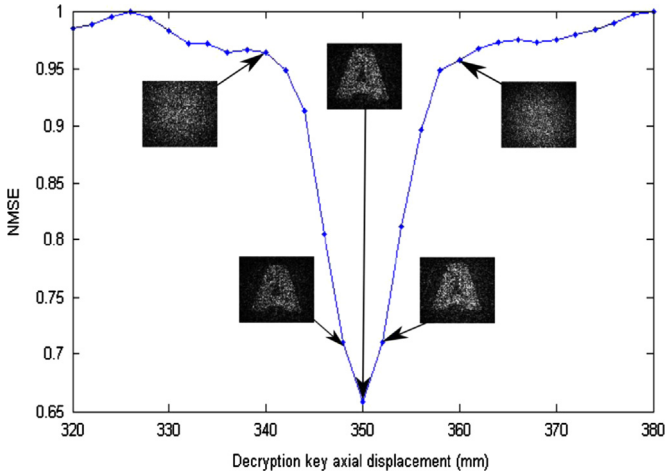

Fig. 6. NMSE curve for the retrieved objects using decrypting keys registered at different key-camera distances, compared to the original object (see Media 1).

The experimental results of Figs. 4 and 5 show that there is a loss of spatial frequencies due to the limited sensor size of the CMOS camera. The exact ranges for optimal operation of the JFSC will depend on several factors like: object size and complexity, key window size, camera sensor size, resolution and properties of the diffusor. Therefore, the optimal operation range is not arbitrarily large in any experimental implementation.

The presented system works by allowing the free propagation of the light coming from both key and object, in order to produce the JFPD. This free propagation distance is the new main parameter that becomes available when using this architecture. We now proceed to study the tolerance of the decryption to an axial displacement of the key. In order to perform this test, an object is encrypted with an object-camera distance z of 350 mm and then decrypted using decryption keys registered in different planes. The quality of the decrypted objects with the shifted keys is then measured using the NMSE metric with the original object as reference. The NMSE between the decrypted object using decrypting keys registered at different key-camera distances $m_z(p,q)$ and the original object $m(p,q)$ is shown in Fig. 6.

Supplementary material related to this article can be found online at: doi:10.1016/j.optlaseng.2016.03.010.

Fig. 6 shows that the decrypted object can be recognized within a range of 1 cm. When the decryption key is displaced outside this range, the right decryption is no longer achieved. This range demonstrates the existence of a decoding tolerance thus breaking the desired behavior of the cryptosystem to adequately protect the encoded data for any decryption outside the right distance. Therefore, any scheme involving the propagation length as an additional security measure or as part of a protocol leading to data multiplexing, to mention two examples, would have to take into account this tolerance. In Media 1, we can see the effect of the key displacement, where each frame represents 2 mm of axial displacement. Similar to the range of optimal operation of the JFSC, an exact tolerance value will depend on several factors. However, any intent to optimize the system behavior would acknowledge the fact that this tolerance range cannot be made arbitrarily small.

Due to the nature of the Fresnel transform, if an unauthorized user acquires the actual encryption key but has no knowledge of the right object-key distance, he can easily find it by successive propagations.

4. Conclusions

In this contribution, the experimental implementation and the corresponding theoretical analysis of a joint free space cryptosystem is presented. The experimental results demonstrate the ability of the encrypting system to protect data. As usual, the user can recover the original information when accessing the encrypted data and the right decoding key. The decrypting protocol is simple in the sense that it does not involve cumbersome procedures while keeping all the security standards, and the decrypted results present the same characteristics of any encrypting architecture. Additionally, an experimental analysis of the object-camera and key-camera distances was performed. Although these parameters can be used as additional security measures, the system exhibits a tolerance to changes in these parameters large enough to warrant a careful consideration of their use in any practical application. On the other side, from an experimental point of view, we remark that this alternative optical

architecture is simpler than others as it does not require lenses; thus, the associated aberrations, focal length restrictions and alignment issues are removed.

Acknowledgment

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). John Fredy Barrera Ramírez acknowledges support from The International Centre for Theoretical Physics ICTP Associateship Scheme.

References

[1] Grosges T, Barchiesi D. Toward nanoworld-based secure encryption for enduring data storage. Opt Lett 2010;35:2421–3.
[2] Barrera JF, Mira A, Torroba R. Optical encryption and QR codes: Secure and noise-free information retrieval. Opt Express 2013;21:5373–8.
[3] Graydon O. Cryptography: Quick response codes. Nat Photonics 2013;7:343.
[4] Barrera JF, Vélez A, Torroba R. Experimental scrambling and noise reduction applied to the optical encryption of QR codes. Opt Express 2014;22:20268–77.
[5] Barrera JF, Mira A, Torroba R. Experimental QR code optical encryption: Noise-free data recovering. Opt Lett 2014;39:3074–7.
[6] Refregier P, Javidi B. Optical image encryption based on input plane and Fourier plane random encoding. Opt Lett 1995;20:767–9.
[7] Nomura T, Javidi B. Optical encryption using a joint transform correlator architecture. Opt Eng 2000;39:2031–5.
[8] 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.
[9] Mehra I, Rajput SK, Nishchal NK. Cryptoanalysis of an image encryption scheme based on joint transform correlator with amplitude- and phase-truncation approach. Opt Lasers Eng 2014;52:167–73.
[10] Barrera JF, Vélez A, Torroba R. Experimental multiplexing protocol to encrypt messages of any length. J Opt 2013;15:055404.
[11] Barrera JF, 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.
[12] Javidi B, Nomura T. Securing information by use of digital holography. Opt Lett 2000;25:28–30.
[13] Rueda E, Barrera JF, Henao R, Torroba R. Optical encryption with a reference wave in a joint transform correlator architecture. Opt Commun 2009;282:3243–9.
[14] Chen J-X, Zhu Z-L, Fu C, Zhang L-B, Yu H. Analysis and improvement of a double-image encryption scheme using pixel scrambling technique in gyrator domains. Opt Lasers Eng 2015;66:1–9.
[15] Singh H, Yadav AK, Vashisth S, Singh K. Double phase-image encryption using gyrator transform and structured phase mask in the frequency plane. Opt Lasers Eng 2015;67:145–56.
[16] Unnikrishnan G, Joseph J, Singh K. Optical encryption by double-random phase encoding in the fractional Fourier domain. Opt Lett 2000;25:887–9.
[17] Liu S, Yu L, Zhu B. Optical image encryption by cascaded fractional Fourier transform with random phase filtering. Opt Commun 2001;187:57–63.
[18] Zhang Y, Zheng C, Tanno N. Optical encryption based on iterative fractional Fourier transform. Opt Commun 2002;202:277–85.
[19] Zhu B, Liu S. Optical image encryption based on the generalized fractional convolution operation. Opt Commun 2001;195:371–81.
[20] Liu S, Mi Q, Zhu B. Optical image encryption with multistage and multichannel fractional Fourier-domain filtering. Opt Lett 2001;26:1242–4.
[21] Zhu B, Liu S, Ran Q. Optical image encryption based on multifractional Fourier transforms. Opt Lett 2000;25:1159–61.
[22] Li X-W, Lee I-K. Modified computational integral imaging-based double image encryption using fractional Fourier transform. Opt Lasers Eng 2015;66:112–21.
[23] Li Y, Zhang F, Li Y, Tao R. Asymmetric multiple-image encryption based on the cascaded fractional Fourier transform. Opt Lasers Eng 2015;72:18–25.
[24] Rajput SK, Nishchal NK. Image encryption and authentication verification using fractional nonconventional joint transform correlator. Opt Laser Eng 2012;50:1474–83.
[25] Vilardy JM, Millán MS, Pérez-Cabré E. Nonlinear optical security system based on a joint transform correlator in the Fresnel domain. Appl Opt 2014;53:1674–82.
[26] Amaya D, Tebaldi M, Torroba R, Bolognini N. Wavelength multiplexing encryption using joint transform correlator architecture. Appl Opt 2009;48:2099–104.
[27] Situ G, Zhang J. Multiple-image encryption by wavelength multiplexing. Opt Lett 2005;30:1306–8.
[28] Barrera JF, Henao R, Tebaldi M, Bolognini N, Torroba R. Multiplexing encrypted data by using polarized light. Opt Commun 2006;260:109–12.
[29] Barrera JF, 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.
[30] Rueda E, Rios C, Barrera JF, Henao R, Torroba R. Experimental multiplexing approach via key code rotations under a joint transform correlator scheme. Opt Commun 2011;284:2500–4.
[31] Barrera JF, Henao R, Tebaldi M, Torroba R, Bolognini N. Multiple image encryption using an aperture modulated optical system. Opt Commun 2006;261:29–33.
[32] Guohai S, Jingjuan Z. Position multiplexing for multiple-image encryption. J Opt A: Pure Appl Opt 2006;8:391–7.
[33] Schnars U, Jüptner W. Digital holography: Digital hologram recording, numerical reconstruction, and related techniques. 1st ed. Berlin: Springer-Verlag GmbH; 2005.
[34] Ostrovsky I Y, Butosov MM, Ostrovskaja GV. Interferometry by holography. 1st ed. Berlin: Springer-Verlag GmbH; 1980.
[35] Unnikrishnan G, Joseph J, Singh K. Optical encryption system that uses phase conjugation in a photorefractive crystal. Appl Opt 1998;37:8181–6.