# Nonlinear optical security system based on a joint transform correlator in the Fresnel domain

Juan M. Vilardy,* María S. Millán, and Elisabet Pérez-Cabré

Applied Optics and Image Processing Group, Department of Optics and Optometry, Universitat Politècnica de Catalunya, 08222 Terrassa—Barcelona, Spain

*Corresponding author: juan.manuel.vilardy@estudiant.upc.edu

Received 14 November 2013; revised 29 January 2014; accepted 31 January 2014; posted 5 February 2014 (Doc. ID 201364); published 10 March 2014

A new optical security system for image encryption based on a nonlinear joint transform correlator (JTC) in the Fresnel domain (FrD) is proposed. The proposal of the encryption process is a lensless optical system that produces a real encrypted image and is a simplified version of some previous JTC-based encryption systems. We use a random complex mask as the key in the nonlinear system for the purpose of increasing the security of the encrypted image. In order to retrieve the primary image in the decryption process, a nonlinear operation has to be introduced in the encrypted function. The optical decryption process is implemented through the Fresnel transform and the fractional Fourier transform. The security system proposed in this paper preserves the shift-invariance property of the JTC-based encryption system in the Fourier domain, with respect to the lateral displacement of the key random mask in the decryption process. This system shows an improved resistance to chosen-plaintext and known-plaintext attacks, as they have been proposed in the cryptanalysis of the JTC encrypting system. Numerical simulations show the validity of this new optical security system. 

*OCIS codes:* (050.1970) Diffractive optics; (070.4550) Correlators; (070.4340) Nonlinear optical signal processing; (070.2575) Fractional Fourier transforms; (350.4600) Optical engineering.

http://dx.doi.org/10.1364/AO.53.001674

## 1. Introduction

Information security is an integral part of our lives, which affects most of the transactions among individuals or institutions (public or private). Optical-processing systems have been proposed for information security applications in the last two decades [1] due to their high level of security, parallelism, and ultrafast processing speed.

In 1995, Réfrégier and Javidi proposed an optical encryption scheme named double random phase encoding (DRPE) [2], which has been further extended from the Fourier domain to the Fresnel domain (FrD) [3–10] and the fractional Fourier domain [11], in order to increase the number of keys and hence the security strength of the optical encryption–decryption system. The optical DRPE can be implemented using a classical $4f$-processor [12]. This processor typically requires strict optical alignment, which in practice is difficult to attain. To alleviate this constraint, the optical DRPE can be also performed by means of a joint transform correlator (JTC) architecture that also shows other advantages [13–18]. With the JTC, a CCD camera captures the intensity distribution of the joint power spectrum (JPS) as the encrypted data in the Fourier domain, while the classical DRPE method requires the recording of complex-valued information. An additional advantage of JTC is that the decryption process utilizes the same security key previously used in the encryption process, which eliminates the need pointed out in [2] to produce an exact complex conjugate of the key. However, a practical difficulty arises when trying to reproduce the mathematics of DRPE algorithm as proposed in [2] by means of the JTC architecture: in the input

1559-128X/14/081674-09$15.00/0

plane of the JTC, the image to be encrypted, which is attached to a first random phase mask (RPM), is placed side by side with a "key code" that has to be the inverse Fourier transform of a second RPM [13]. This key code in the input plane of the JTC is a fully complex-valued distribution whose Fourier transform produces a phase-only distribution. The physical reproduction of the key code is not trivial. To optically reproduce this key code in the input plane of a JTC, Nomura and Javidi split the optical entrance of the setup into two beams. This solution is conceptually correct but adds more complexity to the optical setup, which requires finer alignment than a conventional JTC [13]. An alternative solution is given in [18], where the key code is represented by real-valued data. Another solution that involves the nonlinear processing of the JPS is given in [16].

Other optical security applications that use the JTC architecture in the FrD have been proposed in several works [19–22]. These security applications are based on phase-shifting methods, and therefore, the image encryption and the decryption processes differ from the DRPE technique proposed in [2,4,13]. The JTC in the FrD presented in [19,20] was implemented using the Mach–Zehnder interferometer, and hence, the optical entrance of the setup was split into two beams.

Concerning the security of the optical DRPE proposed in [2], it has been proved that the DRPE is vulnerable to chosen-plaintext attack (CPA) [23,24] and known-plaintext attack (KPA) [24,25]. This weakness is due to the linear property of the DRPE scheme [24]. The DRPE implemented by means of a JTC is also vulnerable to CPA [26] and KPA [27]. Finally, the optical DRPE in the FrD proposed in [3–5] is also vulnerable to plaintext attacks [28,29].

Image quality has also been an issue in optical security applications based on JTC architectures. The possibility of applying nonlinear transformations onto the JPS has been explored in order to improve both the security of the encrypted image and the image quality in the retrieval of the decrypted image [16] and in image verification [30].

As mentioned above, the optical DRPE proposed in [2] was extended to the FrD. In this work, we will extend the DRPE implemented with a nonlinear JTC, as proposed in [16], to the FrD in order to increase the security of the encryption scheme and simplify the optical implementation of the encryption–decryption system in comparison with the previous JTC-based encryption systems [13–20]. We introduce a nonlinear operation in the encrypted function that contains the joint Fresnel power distribution (JFPD), for the purpose of retrieving the primary image in the decryption process [31]. The nonlinearity introduced in the FrD becomes essential to retrieve the encrypted image. This makes a significant difference with respect to the JTC-based encryption system in the Fourier domain described in [16], where the nonlinearity applied to the JPS was not essential to decrypt the image but to retrieve it with higher quality and in more secure conditions. The nonlinear JTC-based encryption system in the FrD [31] is mathematically described and further investigated in this paper with the introduction of a general random complex mask (RCM), the use of different probability density functions to generate the random codes, and the evaluation of the system resistance to cryptanalysis. As we will show in the following sections, the nonlinearity introduced in the JFPD and other features of the optical setup, make the system more resistant to CPA [26] and KPA [27]. We also use a RCM as the key of the security system, where both the modulus and phase functions of the RCM are of random magnitudes. This RCM is a general key random mask to be implemented in a JTC-based system and, as we demonstrate, it also increases the security of the encryption compared to the previous algorithm [16].

The proposed encryption technique can be applied by means of a lensless optical system that avoids the beam splitting required by other optical JTC implementations [13,19,20]. There is no need to make the optical setup more complicated because a simplified JTC in the FrD suffices for the implementation of the whole process. In addition to this, the amount of information to transmit does not increase with respect to the referred algorithms. Regarding the implementation of the decryption process, we use an optical fractional Fourier transform in the last step of the decryption stage. Finally, the proposed nonlinear JTC-based encryption–decryption system in the FrD preserves the shift-invariance property with respect to lateral displacements of the key random mask in the decryption process [1,17].

The rest of the paper is organized as follows. Section 2 describes the proposed nonlinear JTC-based encryption system in the FrD and presents some numerical experiments to illustrate the proposal. Section 3 specifies the system resistance against CPA [26] and KPA [27]. The results presented and discussed in the paper lead us to outline the conclusions in Section 4.

## 2. Nonlinear JTC-Based Encryption System in the Fresnel Domain

### A. Encryption Stage

The input plane of a JTC is typically composed by two nonoverlapping data distributions, $g(x)$ and $c(x)$, placed side-by-side (Fig. 1) [12–18]. We use one-dimensional notation for the sake of simplicity. Let $f(x)$ be the real image to be encrypted with values in the interval [0, 1], $r(x)$ a RPM, and $h(x)$ a RCM whose mathematical expressions are given by

$$r(x) = \exp\{i2\pi s(x)\}, \quad h(x) = m(x)\exp\{i2\pi n(x)\}, \quad (1)$$

where $s(x)$, $m(x)$, and $n(x)$ are normalized positive functions randomly generated, statistically independent, and distributed in the interval [0, 1]. In the encryption stage, the two functions $g(x)$ and $c(x)$

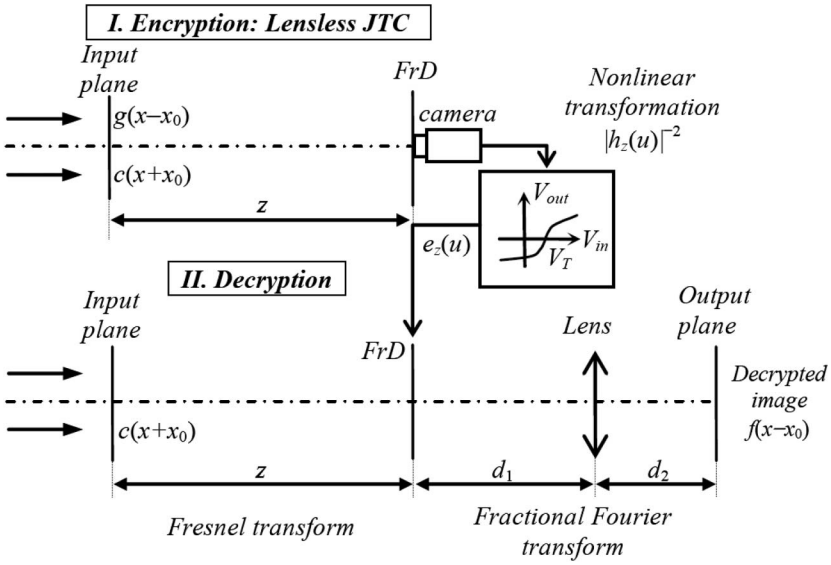


Fig. 1. Scheme of the optical setup composed by an encryption system based on a nonlinear JTC architecture in the FrD and a decryption system based on an optical FrT combined with an optical fractional Fourier transform.

are placed in the input plane of the JTC at coordinates $x = x_0$ and $x = -x_0$, respectively. The function $g(x)$ consists of the real image to be encrypted bonded to the RPM $r(x)$ and modulated by a pure linear phase term

$$g(x) = \exp\left\{\frac{i2\pi v_0(x - v_0)}{\lambda z}\right\} r(x) f(x), \tag{2}$$

where $v_0$ is a real constant. Let the function $c(x)$ be the RCM $h(x)$ modulated by another pure linear phase term

$$c(x) = \exp\left\{\frac{-i2\pi v_0(x + v_0)}{\lambda z}\right\} h(x). \tag{3}$$

Let us denote the Fresnel transform (FrT) at the wavelength $\lambda$ and the propagation distance $z$ of the functions $r(x)f(x)$ and $h(x)$ by

$$\begin{aligned} t_z(u) &= \mathrm{FrT}_{\lambda,z}\{r(x)f(x)\}, \\ h_z(u) &= \mathrm{FrT}_{\lambda,z}\{h(x)\} = |h_z(u)| \exp\{i2\pi\phi_z(u)\}. \end{aligned} \tag{4}$$

We introduce the JFPD at parameters $\lambda$, $z$, and $v_0 = -x_0$ as

$$\mathrm{JFPD}_z(u) = |\mathrm{FrT}_{\lambda,z}\{g(x - x_0) + c(x + x_0)\}|^2. \tag{5}$$

It is worth remarking that the linear phase terms symmetrically introduced in $g(x - x_0)$ [Eq. (2) with $v_0 = -x_0$ and shifted to $x = x_0$] and $c(x + x_0)$ [Eq. (3) with $v_0 = -x_0$ and shifted to $x = -x_0$] are solely intended to ensure that both $\mathrm{FrT}_{\lambda,z}\{g(x - x_0)\}$ and $\mathrm{FrT}_{\lambda,z}\{c(x + x_0)\}$ are centered at the same spatial point of the FrD. We define the encrypted image as the JFPD divided by the nonlinear term $|h_z(u)|^2$, and it is determined by the following equation (see Appendix A):

$$\begin{aligned} e_z(u) = \frac{\mathrm{JFPD}_z(u)}{|h_z(u)|^2} &= \frac{|t_z(u)|^2}{|h_z(u)|^2} + 1 \\ &+ t_z^*(u) \frac{h_z(u)}{|h_z(u)|^2} \exp\left\{\frac{i\pi}{\lambda z}(4x_0)u\right\} \\ &+ t_z(u) \frac{h_z^*(u)}{|h_z(u)|^2} \exp\left\{\frac{-i\pi}{\lambda z}(4x_0)u\right\}. \end{aligned} \tag{6}$$

If $|h_z(u)|^2$ is equal to zero for a particular value of $u$, this intensity value is substituted by a small constant to avoid singularities when computing $e_z(u)$. It is also important to remark that the products $t_z^*(u)h_z(u)$ and $t_z(u)h_z^*(u)$ can be obtained in the FrD due to the pure linear phase modulation introduced in Eqs. (2) and (3). These products in the FrD are essential to convert the primary image in random noise according to the DRPE algorithm implemented with a JTC architecture. The encrypted image consists of a real-valued distribution that can be computed from the intensity distributions of the $\mathrm{JFPD}_z(u)$ and $|h_z(u)|^2$ previously acquired by a conventional power-law device, such as a CCD camera. The nonlinear expression of Eq. (6) is the natural extension to the FrD of the nonlinear expression given in our former work [16] for the JPS in the Fourier domain.

The security keys needed for decryption are the RCM $h(x)$, the wavelength $\lambda$, and the distance of propagation $z$. The RPM $r(x)$ is used to spread the information content of the original image $f(x)$ onto the encrypted distribution $e_z(u)$. Compared to previous JTC-based encryption systems [13–18], this encryption system is a lensless setup that minimizes the optical hardware requirements and is easier to

implement. Figure 1 shows the optical encryption scheme based on a nonlinear JTC architecture in the FrD.

### B. Decryption Stage

The initial step of the decryption process is to perform the product between the encrypted distribution and the FrT at parameters $\lambda$ and $z$ of $c(x+x_0)$ with $v_0=-x_0$, and this can be expressed (see Appendix A) by

$$\begin{aligned} d_z(u) &= e_z(u)\mathrm{FrT}_{\lambda,z}\{c(x+x_0)\} \\ &= \exp\left\{\frac{i\pi}{\lambda z}(2x_0u-x_0^2)\right\}\frac{h_z(u)}{|h_z(u)|^2}|t_z(u)|^2 \\ &\quad+\exp\left\{\frac{i\pi}{\lambda z}(2x_0u-x_0^2)\right\}h_z(u) \\ &\quad+\exp\left\{\frac{i\pi}{\lambda z}(6x_0u-x_0^2)\right\}t_z^*(u)\frac{h_z^2(u)}{|h_z(u)|^2} \\ &\quad+\exp\left\{\frac{-i\pi}{\lambda z}(2x_0u+x_0^2)\right\}t_z(u)\frac{h_z^*(u)h_z(u)}{|h_z(u)|^2}. \end{aligned} \tag{7}$$

The fourth term of Eq. (7) is the most interesting since it retains the information to be decrypted [16]. Therefore, when the FrT at parameters $\lambda$ and $-z$ is applied to the simplified fourth term of Eq. (7) and the absolute value is taken, we obtain the decrypted image at coordinate $x=x_0$ given by

$$\tilde{f}(x-x_0)=\left|\mathrm{FrT}_{\lambda,-z}\left\{\exp\left[\frac{-i\pi}{\lambda z}(2x_0u+x_0^2)\right]t_z(u)\right\}\right|. \tag{8}$$

Note that if we use $c(x)$ shifted to the position of coordinate $x=-x_1$ with $v_0=-x_1$ for the decryption process, the decrypted image can be recovered at coordinate $x=2x_0-x_1$

$$\begin{aligned} &\tilde{f}(x-2x_0+x_1) \\ &=\left|\mathrm{FrT}_{\lambda,-z}\left\{\exp\left[\frac{-i\pi}{\lambda z}(2(2x_0-x_1)u+x_1^2)\right]t_z(u)\right\}\right|. \end{aligned} \tag{9}$$

The previous equation demonstrates that the encryption–decryption system based on a nonlinear JTC in the FrD preserves the shift-invariance property of the complex key mask $c(x)$ for decryption, in the same way as the Fourier domain-JTC encryption system does. This shift-invariant property of the proposed encryption–decryption system is a consequence of the definition of the JFPD given in Eq. (5). We remark that it will not be possible to retrieve the original image in the decryption stage unless the nonlinear operation is introduced as described in Eq. (6). This result differs from the previous proposal [16] where the applied nonlinearity helped to improve the quality of the retrieved image, but it was not such an essential operation. The reason for this is that all the transformations are performed in the FrD and the key mask of the encryption–decryption system is a fully complex-valued random distribution in the input plane of the JTC.

Since the FrT at parameters $\lambda$ and $-z$ cannot be implemented optically [4] and the complex conjugation of the real-valued encrypted distribution $e_z(u)$ is not useful in the decrypting procedure, we use the relationship between the FrT and the fractional Fourier transform (Appendix B) for the purpose of simulating an optical inverse FrT. The FrT at parameters $\lambda$ and $z$ is related to a fractional Fourier transform at fractional order $\alpha$ [5,32,33]. Therefore, we applied an optical fractional Fourier transform at fractional order $\pi-\alpha$ to the simplified fourth term of Eq. (7) and then we take the absolute value in order to retrieve an inverted version of the primary image $\tilde{f}(-x)$ at coordinate $x=-x_0$. Figure 1 also shows the optical decryption scheme based on an optical FrT combined with an optical fractional Fourier transform (the distances $d_1$, $d_2$, and the focal length of the lens define the value of the fractional order $\pi-\alpha$ [32]).

### C. Computer Simulations

Numerical simulations are carried out to analyze the performance of the proposed encryption and decryption procedures. The original image to be encrypted is $256\times256$ pixel size [Fig. 2(a)], the distance between pixels (pixel pitch) is 8 μm. The random distribution code $s(x)$, corresponding to the RPM $r(x)$, and its histogram are shown in Figs. 2(b) and 2(c), respectively. Similar noisy distributions are considered for $m(x)$ and $n(x)$ of the RCM $h(x)$. Figure 2(c) reveals the relative uniformity of the probability density function of the random distribution code $s(x)$. The distance $x_0$ used in the input plane of the JTC, is set to 4.096 mm (512 pixels). The encrypted function obtained by using the keys $\lambda=532$ nm and $z=70$ mm is depicted in Fig. 2(d).

The absolute value of the output plane after the decryption procedure with the correct keys $\lambda$, $z$, and the RCM $h(x)$ is shown in Fig. 3(a). The decrypted image is presented in Fig. 3(b), which depicts the magnified region of interest of the output plane [Fig. 3(a)]. The ideal decrypted image has been obtained by calculating just the right term of Eq. (8) and it is displayed in Fig. 3(c). To evaluate the quality of the decrypted image, we use the root mean square error (RMSE) defined by [34]

$$\mathrm{RMSE}=\left(\frac{\sum_{x=1}^{M}[f(x)-\tilde{f}(x)]^2}{\sum_{x=1}^{M}[f(x)]^2}\right)^{\frac{1}{2}}, \tag{10}$$

where $f(x)$ and $\tilde{f}(x)$ denote the original image and the decrypted image, respectively. The RMSE between the original image of Fig. 2(a) and the decrypted image of Fig. 3(b) is 0.114, whereas it is only $4.44\times10^{-15}$ if the original image of Fig. 2(a) is compared with the ideal decrypted image of Fig. 3(c). The

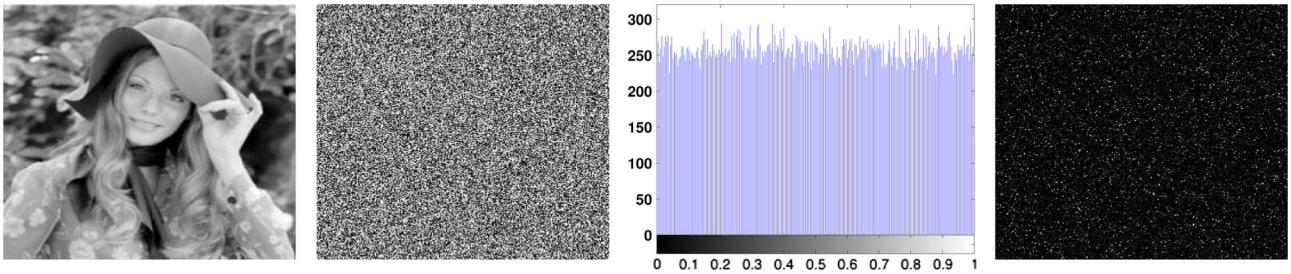


Fig. 2. (a) Original image to be encrypted $f(x)$. (b) Random distribution code $s(x)$ of the RPM $r(x)$. (c) Histogram of $s(x)$ (uniform random distribution). (d) Encrypted image $e_z(u)$ for the keys $\lambda = 532$ nm and $z = 70$ mm.

two previous decrypted images have been simulated using the FrT with parameters $\lambda = 532$ nm and $z = -70$ mm in the last step of the decryption process. When this inverse FrT is replaced by a fractional Fourier transform of fractional order $\pi - \alpha$, with $\alpha = 0.35\pi$, the decrypted images obtained are similar to those presented in Figs. 3(b) and 3(c).

We test the role of the introduced nonlinearity in the proposed encryption system. When the nonlinearity $|h_z(u)|^2$ of Eq. (6) is not applied in the encryption algorithm, the decrypted output obtained with the correct keys is shown in Fig. 3(d). In such a case, the resulting image has still a noisy-like appearance and thus the original image can not be retrieved. The RMSE between the original image of Fig. 2(a) and the decrypted image of Fig. 3(d) is 0.783. The result shown in Fig. 3(d) proves that the nonlinearity $|h_z(u)|^2$ introduced in the encrypted function is essential to the decryption process in order to retrieve the original image.

We also tested the influence of the security keys on the decrypted image. The retrieved image with an incorrect distance of propagation $z$ and the others correct keys [the wavelength $\lambda$ and the RCM $h(x)$] is shown in Fig. 3(e). The resulting decrypted image has a noisy pattern without any relevant information from the original image. The RMSE between the original image of Fig. 2(a) and the decrypted image of Fig. 3(e) is 0.794. When an incorrect wavelength $\lambda$ or an incorrect random code images of the RCM $h(x)$ [either the modulus $m(x)$ or the phase $n(x)$, or both at the same time] are used in the decryption process, the decrypted images obtained are noisy patterns similar to Fig. 3(e). These results prove that all the keys are required in the decryption stage for the correct retrieval of the original image.

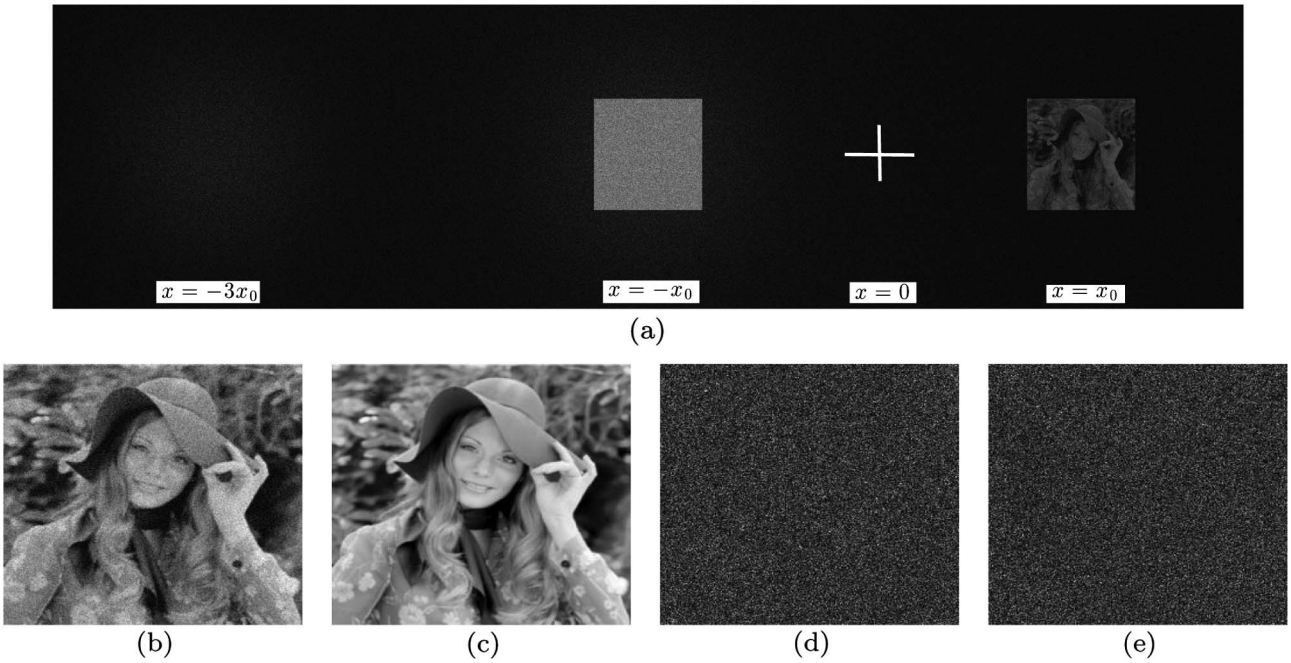


Fig. 3. (a) Absolute value of the output plane after the decryption procedure with the correct keys $\lambda$, $z$, and the RCM $h(x)$. (b) Magnified region of interest of (a) corresponding to the decrypted image. (c) Ideal decrypted image obtained by calculating just the right term of Eq. (8). Decrypted images from Fig. 2(d): (d) when the nonlinearity $|h_z(u)|^2$ of Eq. (6) is not introduced in the encrypted function and all the correct keys are used for decryption and (e) using just an incorrect distance of propagation $z = 73$ mm, but the rest of keys [$\lambda$ and the RCM $h(x)$] are correct.

Additionally to the examples just provided, the interested reader is referred to other papers [3–5,9,11,29] that report similar effects obtained after introducing small errors in the various keys (such as the lateral distances $z$, $d_1$, and $d_2$, and the wavelength $\lambda$) of related DRPE encryption systems in the FrD.

As another test, the random distribution codes $m(x)$ and $n(x)$ of the RCM $h(x)$ presented in Figs. 4(a) and 4(b), respectively, were generated using the nonuniform random distributions Weibull and chi-square, respectively. Figures 4(c) and 4(d) show the histograms of $m(x)$ and $n(x)$, respectively, which reveal the nonuniformity of the probability density functions of these codes. Considering such RCM $h(x)$ and the original image shown in Fig. 2(a), the encrypted image for the keys $\lambda = 532$ nm and $z = 70$ mm is depicted in Fig. 4(e). Even though the RCM $h(x)$ is obtained by using nonuniform distributions, the final encrypted image of Fig. 4(e) has a noisy-like appearance very similar to the result of Fig. 2(d). The decrypted image using all the correct keys is shown in Fig. 4(f). Thus, in accordance to the analysis carried out in [16], we recommend using nonuniform random distributions for $m(x)$ or $n(x)$ in the encryption system, for the purpose of improving the security of the encrypted image.

### D. Feasibility of Experimental Optical Setup

The former optical implementation of the DRPE using the JTC architecture [13] has been modified in several works [14–16]. Initially, the complex-valued key code in the input plane of the JTC was directly replaced by a RPM [14,15]. Although this did not exactly reproduce the DRPE as proposed in [2], this modified JTC-based encryption system became easier to implement with the help of a simple diffuser glass (random phase element) placed in the input plane to fully cover its aperture. On the one side of the JTC input plane, a zone of the diffuser (first RPM) was against the image to be encrypted and, on the other side, another zone of the diffuser was used for the second RPM. The latter RPM constituted the security key used in both the encryption and the decryption stages. Thus, whereas the second RPM acted in the Fourier domain for the original DRPE, it acted in the spatial domain for the modified DRPE [16]. The decrypted images obtained in [14,15] presented low quality, due to this modification. As we showed in [16], it is possible to significantly improve the quality of the decrypted image in the security system described in [14,15] by introducing a simple nonlinear operation in the encrypted function that contains the JPS.

The nonlinear JTC-based encryption system proposed in this work can be implemented using the optoelectronic setup of Fig. 1 (JTC part) by following the procedure proposed in [35–37] extended to the FrD. The encrypted image given by Eq. (6) can be optically implemented by a two-step JTC [35,36] in the FrD. In the first step, the intensity function $|h_z(u)|^2$ is captured, which is equal to $|\mathrm{FrT}_{\lambda,z}\{c(x+x_0)\}|^2$ with $v_0 = -x_0$. Then, the JFPD represented by Eq. (5) is captured in the second step [37]. Finally, the JFPD is digitally divided by $|h_z(u)|^2$, and thus, the encrypted image of Eq. (6) is computed. This encrypted distribution is the only information to transmit. Therefore, this method does not increment the amount of data to send prior the decryption stage [16].

The pure linear phase terms introduced to the distributions $g(x)$ and $c(x)$ in the input plane of the JTC can be implemented using an optical biprism or a phase-only SLM. The RCM can be displayed by

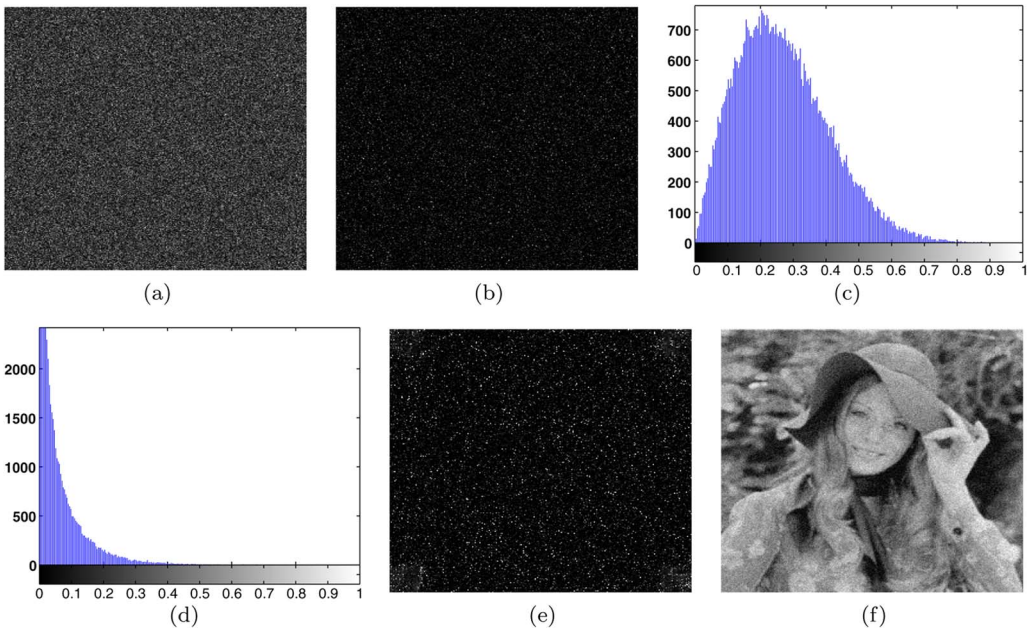


Fig. 4. Nonuniform random distributions: (a) Weibull for $m(x)$ and (b) Chi-square for $n(x)$. Histograms of (c) $m(x)$ and (d) $n(x)$. (e) Encrypted image $e_z(u)$ and (f) Decrypted image using all the correct keys.

means of the optical implementation presented in [17]. This optical implementation requires a more precise optical alignment, because it is necessary to employ two SLMs in order to modulate the amplitude and phase in a separate way. The requirements of the optical implementation for the proposed nonlinear encryption–decryption system can be relaxed when the RCM $h(x)$ is reduced to a RPM, making $m(x)$ equal to 1 in Eq. (1). In this case, the RPMs $r(x)$ and $h(x)$ can be implemented using a diffusor glass as mentioned in this section. Another practical optical implementation could be by displaying the pure linear phase terms and the RPMs $r(x)$ and $h(x)$ of the input plane of the JTC by means of a phase-only SLM. The optical fractional Fourier transform that is used in the decryption process, can be performed by means of the optoelectronic setup developed in [38].

## 3. Cryptanalysis

The security of the proposed nonlinear JTC-based encryption system in the FrD is further evaluated in this section. We test the resistance of the nonlinear encryption system against CPA [26] and KPA [27] that proved the vulnerability of the JTC-based encryption system in the Fourier domain.

### A. Chosen-Plaintext Attack

The CPA defined in [26] was applied to a JTC-based encryption system in the Fourier domain, which has a RPM as key. The encryption process proposed in this paper is based on a JTC in the FrD ($\lambda$ and $z$ represent additional keys) and has a RCM $h(x)$ as key. The CPA presented in [26] does not directly apply to our encryption method. However, if we consider that $\lambda$ and $z$ are known, the CPA defined in [26] can be still applied to the encryption system proposed in this paper. The CPA introduces a couple of chosen plaintexts in the encryption system, in order to obtain the information related to $h(x)$ [26]. The first chosen plaintext introduced in the encryption system is a null image $f_1(x) = 0$, and thus, the encryption distribution according to Eq. (6) would be

$$e_z(u) = 1. \tag{11}$$

The previous result shows that, unlike the traditional JTC in the Fourier domain, it is not possible to obtain any information about either $h(x)$ or $h_z(u)$ when a null image is introduced in the proposed encryption system. The second chosen plaintext presents a Dirac delta function for the image to be encrypted $f_2(x) = \delta(x)$. The corresponding encrypted image, using Eq. (6), would then be

$$e_z(u) = \frac{1}{\lambda z |h_z(u)|^2} + 1 + \frac{2}{\sqrt{\lambda z}|h_z(u)|} \times \cos\left(2\pi\left[\phi_z(u) - \frac{u}{2\lambda z}(u - 4x_0) - s(0) - \frac{z}{\lambda} + \frac{1}{8}\right]\right), \tag{12}$$

where both the modulus $|h_z(u)|$ and phase $\phi_z(u)$ functions of $h_z(u)$ are unknown and cannot be obtained separately. Therefore, the proposed nonlinear JTC-based encryption system in the FrD is resistant to the CPA defined in [26], because the information about $h(x)$ or $h_z(u)$ cannot be disclosed.

### B. Known-Plaintext Attack

The KPA implemented in [27] also was designed to be applied to a JTC-based encryption system in the Fourier domain. The KPA tries to find the RPM key of the encryption system. This KPA is an iterative process that is based on a heuristic hybrid algorithm [39,40] and the Gerchberg–Saxton (GS) algorithm [41]. The heuristic hybrid algorithm produces a first key based on an initial guess of the RPM key and a plaintext with its corresponding ciphertext (encrypted image). The first key along with the plaintext and its corresponding ciphertext are introduced in the GS algorithm adapted to the JTC architecture [27], in order to obtain the final RPM key. Once again, the KPA defined in [27] does not directly apply to the encryption system proposed in this paper, because the nonlinear encryption system described in Section 2.A is based on a JTC in the FrD and has a RCM $h(x)$ key. However, if we consider that $\lambda$ and $z$ are known, the KPA defined in [27] requires extending the GS algorithm to the FrD [42] in order to find a final RPM key. Even if such extension of the GS algorithm was done, the KPA developed in [27] would only be able to find a RPM key (phase-only function), but the nonlinear encryption system proposed in this paper has a RCM key $h(x)$ (with both modulus and phase function being random magnitudes). We remark that it is very important to use the correct random code image of the RCM $h(x)$ [modulus $m(x)$ and phase $n(x)$] to retrieve the original image in the decryption system, as mentioned previously in Section 2.C.

On the other hand, the GS algorithm in [27] was adapted only for the JPS in the Fourier domain, and we have shown in Section 2.A that the encrypted image is currently represented by a nonlinear modification of the JFPD. Therefore, the convergency of the GS algorithm in [27] extended to the FrD [42] would be affected by the introduction of the nonlinear modification in the JFPD.

Since the RPM key obtained in [27] depends on the probability density function selected at the beginning of the attack, we propose to increase the security of the RCM $h(x)$ used in our work by considering different probability density functions (not only uniform) for the random code distributions corresponding to the RCM $h(x)$. For all these reasons, we can say that the proposed nonlinear JTC-based encryption system in the FrD is resistant to the KPA implemented in [27].

## 4. Conclusion

A new optical information system has been proposed for image encryption–decryption involving the use of

a nonlinear JTC architecture in the FrD. The proposed encryption system is a lensless optical system, which makes the difference with respect to the previous DRPE implemented with a JTC architecture. The nonlinear modification introduced in the FrD has allowed the retrieval of the primary image in the decryption process. Additionally, the nonlinear term introduced into the JFPD and the RCM used in the input plane of the JTC has improved the security of the encrypted image. We have tested the security of the proposed encryption system against CPA and KPA and proved its resistance to these attacks. The nonlinear modification of the JFPD, applied just before the generation of the encrypted image, does not increase the amount of data to transmit. The security system proposed in this paper preserves the shift-invariance property of the complex key mask for decryption in the same way as the Fourier domain-JTC encryption system does. Finally, the nonlinear encryption and decryption systems are suitable for optoelectronic implementation. A two-step JTC in the FrD can be used for the encryption stage and an optical FrT combined with an optical fractional Fourier transform for the decryption stage.

### Appendix A: Fresnel Transform

The Fresnel transform (FrT) of an object $f(x)$ at a propagation distance $z$ when it is illuminated by a plane wave of wavelength $\lambda$ can be expressed as [12]

$$f_z(u) = \mathrm{FrT}_{\lambda,z}\{f(x)\} = \int_{-\infty}^{+\infty} f(x) h_{\lambda,z}(u,x)\mathrm{d}x, \quad \text{(A1)}$$

with

$$h_{\lambda,z}(u,x) = M_{\lambda,z}\ \exp\left\{\frac{i\pi}{\lambda z}(u-x)^2\right\}, \quad \text{and}$$
$$M_{\lambda,z} = \frac{1}{\sqrt{i\lambda z}}\ \exp\left\{i\frac{2\pi z}{\lambda}\right\}, \quad \text{(A2)}$$

where the operator $\mathrm{FrT}_{\lambda,z}$ denotes the FrT at parameters $\lambda$ and $z$, $h_{\lambda,z}$ is the kernel of the transformation, and $M_{\lambda,z}$ is a constant for a given distance of propagation $z$. The properties of the FrT that are used in the encryption–decryption method of Section 2 are

$$\mathrm{FrT}_{\lambda,z_1}\{\mathrm{FrT}_{\lambda,z_2}[f(x)]\} = \mathrm{FrT}_{\lambda,z_1+z_2}\{f(x)\}, \quad \text{(A3)}$$

$$\mathrm{FrT}_{\lambda,z}\left\{\exp\left(\frac{i2\pi v_0 x}{\lambda z}\right) f(x-x_0)\right\}$$
$$= \exp\left\{\frac{i\pi}{\lambda z}(2uv_0 - v_0^2)\right\} f_z(u-x_0-v_0), \quad \text{(A4)}$$

where $x_0$ and $v_0$ are real constants. If we choose $v_0 = -x_0$, the Eq. (A4) is reduced to

$$\mathrm{FrT}_{\lambda,z}\left\{\exp\left(\frac{-i2\pi x_0 x}{\lambda z}\right) f(x-x_0)\right\}$$
$$= \exp\left\{\frac{-i\pi}{\lambda z}(2ux_0 + x_0^2)\right\} f_z(u). \quad \text{(A5)}$$

### Appendix B: Relationship between the Fractional Fourier Transform and the Fresnel Transform

The fractional Fourier transform of order $\alpha$ is a linear integral operator that maps a given function $f(\rho)$ onto function $f_\alpha(\sigma)$ by [32]

$$f_\alpha(\sigma) = \mathcal{F}^\alpha\{f(\rho)\} = \int_{-\infty}^{+\infty} f(\rho) K_\alpha(\sigma,\rho)\mathrm{d}\rho \quad \text{(B1)}$$

with

$$K_\alpha(\sigma,\rho) = C_\alpha\ \exp\{i\pi[(\sigma^2+\rho^2)\cot\alpha - 2\sigma\rho\ \csc\alpha]\},$$
$$C_\alpha = \frac{\exp\left\{-i\left(\frac{\pi}{4}\mathrm{sgn}(\alpha) - \frac{\alpha}{2}\right)\right\}}{\sqrt{|\sin\alpha|}}, \quad -\pi < \alpha \le \pi, \quad \text{(B2)}$$

where $K_\alpha$ is the fractional Fourier kernel and sgn is the sign function. For $\alpha = 0$, it corresponds to the identity transform. For $\alpha = \pi/2$, it reduces to the direct Fourier transform. For $\alpha = \pi$, the reverse transform is obtained. For $\alpha = -\pi/2$, it corresponds to the inverse Fourier transform. The inverse fractional Fourier transform corresponds to the fractional Fourier transform at fractional order $-\alpha$. The fractional Fourier operator is additive with respect to the fractional order $\mathcal{F}^\alpha\mathcal{F}^\beta = \mathcal{F}^{\alpha+\beta}$.

The FrT represented by Eq. (A1) can be related to the fractional Fourier transform denoted by Eq. (B1) using the following relationship [33]:

$$f_z\left(\sqrt{\lambda z}\frac{\sigma}{L}\right) = \frac{\sqrt{\lambda z}}{K} M_{\lambda,z} C_\alpha^{-1}\ \exp\{i\pi\sigma^2\ \tan\alpha\}$$
$$\times\ \mathcal{F}^\alpha\left\{f\left(\sqrt{\lambda z}\frac{\rho}{K}\right)\right\}, \quad \text{(B3)}$$

where

$$\rho = (1/\lambda z)^{\frac{1}{2}} Kx, \qquad \sigma = (1/\lambda z)^{\frac{1}{2}} Lu, \qquad K^2 = \tan\alpha,$$
$$L^2 = \sin\alpha\cos\alpha, \qquad 0 \le \alpha \le \pi/2. \quad \text{(B4)}$$

This research has been partly funded by the Spanish Ministerio de Ciencia e Innovación and Fondos FEDER (Project DPI2009-08879). The first author also wishes to thank the Departamento Administrativo de Ciencia, Tecnología e Innovación from Colombia, COLCIENCIAS, for a doctoral scholarship.

### References

1. M. S. Millán and E. Pérez-Cabré, "Optical data encryption," *Optical and Digital Image Processing: Fundamentals and*

*Applications*, G. Cristóbal, P. Schelkens, and H. Thienpont, eds. (Wiley, 2011), pp. 739–767.
2. P. Réfrégier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. **20**, 767–769 (1995).
3. O. Matoba and B. Javidi, "Encrypted optical memory system using three-dimensional keys in the Fresnel domain," Opt. Lett. **24**, 762–764 (1999).
4. G. Situ and J. Zhang, "Double random-phase encoding in the Fresnel domain," Opt. Lett. **29**, 1584–1586 (2004).
5. B. M. Hennelly and J. T. Sheridan, "Random phase and jigsaw encryption in the Fresnel domain," Opt. Eng. **43**, 2239–2249 (2004).
6. G. Situ and J. Zhang, "Multiple-image encryption by wavelength multiplexing," Opt. Lett. **30**, 1306–1308 (2005).
7. G. Situ and J. Zhang, "Position multiplexing for multiple-image encryption," J. Opt. A **8**, 391–397 (2006).
8. X. F. Meng, L. Z. Cai, Y. R. Wang, X. L. Yang, X. F. Xu, G. Y. Dong, X. X. Shen, H. Zhang, and X. C. Cheng, "Hierarchical image encryption based on cascaded iterative phase retrieval algorithm in the Fresnel domain," J. Opt. A **9**, 1070–1075 (2007).
9. P. Kumar, J. Joseph, and K. Singh, "Holographic encryption system in the Fresnel domain with convergent random illumination," Opt. Eng. **49**, 095803 (2010).
10. L. Chen and D. Zhao, "Optical color image encryption by wavelength multiplexing and lensless Fresnel transform holograms," Opt. Express **14**, 8552–8560 (2006).
11. G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain," Opt. Lett. **25**, 887–889 (2000).
12. J. W. Goodman, *Introduction to Fourier Optics* (McGraw-Hill, 1996).
13. T. Nomura and B. Javidi, "Optical encryption using a joint transform correlator architecture," Opt. Eng. **39**, 2031–2035 (2000).
14. E. Rueda, J. F. Barrera, R. Henao, and R. Torroba, "Optical encryption with a reference wave in a joint transform correlator architecture," Opt. Commun. **282**, 3243–3249 (2009).
15. 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**, 3388–3393 (2012).
16. J. Vilardy, M. S. Millán, and E. Pérez-Cabré, "Improved decryption quality and security of a joint transform correlator-based encryption system," J. Opt. **15**, 025401 (2013).
17. C.-L. Chen, L.-C. Lin, and C.-J. Cheng, "Design and implementation of an optical joint transform encryption system using complex-encoded key mask," Opt. Eng. **47**, 068201 (2008).
18. T. Nomura, S. Mikan, Y. Morimoto, and B. Javidi, "Secure optical data storage with random phase key codes by use of a configuration of a joint transform correlator," Appl. Opt. **42**, 1508–1514 (2003).
19. E. Tajahuerce, O. Matoba, S. C. Verrall, and B. Javidi, "Optoelectronic information encryption with phase-shifting interferometry," Appl. Opt. **39**, 2313–2320 (2000).
20. X. Shi, D. Zhao, and Y. Huang, "Double images hiding by using joint transform correlator architecture adopting two-step phase-shifting digital holography," Opt. Commun. **297**, 32–37 (2013).
21. C. La Mela and C. Iemmi, "Optical encryption using phase-shifting interferometry in a joint transform correlator," Opt. Lett. **31**, 2562–2564 (2006).
22. J. Li, T. Zheng, Q.-z. Liu, and R. Li, "Double-image encryption on joint transform correlator using two-step-only quadrature phase-shifting digital holography," Opt. Commun. **285**, 1704–1709 (2012).
23. 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**, 1644–1646 (2005).
24. Y. Frauel, A. Castro, T. J. Naughton, and B. Javidi, "Resistance of the double random phase encryption against various attacks," Opt. Express **15**, 10253–10265 (2007).
25. X. Peng, P. Zhang, H. Wei, and B. Yu, "Known-plaintext attack on optical encryption based on double random phase keys," Opt. Lett. **31**, 1044–1046 (2006).
26. J. F. Barrera, C. Vargas, M. Tebaldi, and R. Torroba, "Chosen-plaintext attack on a joint transform correlator encrypting system," Opt. Commun. **283**, 3917–3921 (2010).
27. 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**, 3553–3555 (2010).
28. X. Peng, H. Wei, and P. Zhang, "Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain," Opt. Lett. **31**, 3261–3263 (2006).
29. G. Situ, G. Pedrini, and W. Osten, "Strategy for cryptanalysis of optical encryption in the Fresnel domain," Appl. Opt. **49**, 457–462 (2010).
30. H. T. Chang and C.-C. Chen, "Fully phase asymmetric image verification system based on joint transform correlator," Opt. Express **14**, 1458–1467 (2006).
31. J. M. Vilardy, M. S. Millán, and E. Pérez-Cabré, "Joint transform correlator-based encryption system using the Fresnel transform and nonlinear filtering," Proc. SPIE **8785**, 87853J (2013).
32. H. M. Ozaktas, Z. Zalevsky, and M. A. Kutay, *The Fractional Fourier Transform: with Applications in Optics and Signal Processing* (Wiley, 2001).
33. P. Pellat-Finet, "Fresnel diffraction and the fractional-order Fourier transform," Opt. Lett. **19**, 1388–1390 (1994).
34. R. C. Gonzalez, R. E. Woods, and S. L. Eddins, *Digital Image Processing Using Matlab*, 2nd ed. (Gatesmark, 2009).
35. E. Pérez, K. Chałasińska-Macukow, K. Styczyński, R. Kotyński, and M. S. Millán, "Dual nonlinear correlator based on computer controlled joint transform processor: digital analysis and optical results," J. Mod. Opt. **44**, 1535–1552 (1997).
36. E. Pérez, M. S. Millán, and K. Chałasińska-Macukow, "Optical pattern recognition with adjustable sensitivity to shape and texture," Opt. Commun. **202**, 239–255 (2002).
37. M. Tebaldi, S. Horrillo, E. Pérez-Cabré, M. S. Millán, D. Amaya, R. Torroba, and N. Bolognini, "Experimental color encryption in a joint transform correlator architecture," J. Phys. Conf. Ser. **274**, 012054 (2011).
38. J. A. Rodrigo, T. Alieva, and M. L. Calvo, "Programmable two-dimensional optical fractional Fourier processor," Opt. Express **17**, 4976–4983 (2009).
39. W. Liu, G. Yang, and H. Xie, "A hybrid heuristic algorithm to improve known-plaintext attack on Fourier plane encryption," Opt. Express **17**, 13928–13938 (2009).
40. M. Nieto-Vesperinas, R. Navarro, and F. J. Fuentes, "Performance of a simulated-annealing algorithm for phase retrieval," J. Opt. Soc. Am. A **5**, 30–38 (1988).
41. R. W. Gerchberg and O. Saxton, "A practical algorithm for the determination of the phase from image and diffraction plane pictures," Optik **35**, 237–246 (1972).
42. Z. Zalevsky, D. Mendlovic, and R. G. Dorsch, "Gerchberg–Saxton algorithm applied in the fractional Fourier or the Fresnel domain," Opt. Lett. **21**, 842–844 (1996).