Nonlinear image encryption using a fully phase nonzero-order joint transform correlator in the Gyrator domain

Juan M. Vilardy[1], María S. Millán[2], and Elisabet Pérez-Cabré[2]

[1]Grupo de Óptica e Informática, Department of Electronic Engineering, Universidad Popular del Cesar, Valledupar (Cesar), Colombia

[2]Applied Optics and Image Processing Group, Department of Optics and Optometry, Universitat Politècnica de Catalunya · BarcelonaTech, Terrassa (Barcelona), Spain

E-mail: vilardy.juan@unicesar.edu.co, elisabet.perez@upc.edu

Abstract. A novel nonlinear image encryption scheme based on a fully phase nonzero-order joint transform correlator architecture (JTC) in the Gyrator domain (GD) is proposed. In this encryption scheme, the two non-overlapping data distributions of the input plane of the JTC are fully encoded in phase and this input plane is transformed using the Gyrator transform (GT); the intensity distribution captured in the GD represents a new definition of the joint Gyrator power distribution (JGPD). The JGPD is modified by two nonlinear operations with the purpose of retrieving the encrypted image, with enhancement of the decrypted signal quality and improvement of the overall security. There are three keys used in the encryption scheme, two random phase masks and the rotation angle of the GT, which are all necessary for a proper decryption. Decryption is highly sensitivity to changes of the rotation angle of the GT as well as to little changes in other parameters or keys. The proposed encryption scheme in the GD still preserves the shift-invariance properties originated in the JTC-based encryption in the Fourier domain. The proposed encryption scheme is more resistant to brute force attacks, chosen-plaintext attacks, known-plaintext attacks, and ciphertext-only attacks, as they have been introduced in the cryptanalysis of the JTC-based encryption system. Numerical results are presented and discussed in order to verify and analyze the feasibility and validity of the novel encryption-decryption scheme.

Keywords: Encryption and decryption systems, Joint transform correlator, Double random phase encoding, Gyrator transform, and Phase retrieval.

1. Introduction

Optical processing techniques have shown great potential in information security applications [1, 2]. A highly successful method for optical image encryption is the double-random phase encoding (DRPE) introduced by Réfrégier and Javidi [3]. The DRPE has been further extended from the Fourier domain to the fractional Fourier domain [4], the Fresnel domain [5, 6] and the Gyrator domain (GD) [7]. Towghi *et al.* proposed a fully phase image encryption technique [8] to further enhance the security and performance of the DRPE in the presence of noise.

A preferred implementation of the optical DRPE is the joint transform correlator (JTC) architecture [9], because this JTC permits to alleviate the strict setup alignment requirement of the holographic system ($4f$-processor [10]) used to experimentally carry out the DRPE [3]; moreover, the encrypted image obtained in the JTC architecture is a real-valued distribution and the random phase mask (RPM) used as key in the encryption process is exactly the same to be used in the decryption process [9].

The initial optical implementation of the DRPE using the JTC architecture [9] has been modified in later contributions [11, 12, 13], in order to simplify the experimental setup. In a modified JTC-encryption system, the two RPMs were implemented using a simple diffuser glass (random phase element) at the input plane of the JTC [11, 12]. As a result of this modification, however, the decrypted signals were affected by a poor image quality. This drawback was overcome in [13] by introducing a nonlinear operation in the encrypted function, obtaining simultaneously an enhancement of the decrypted image quality and an improvement of the system security. The DRPE implemented with a JTC architecture has been extended from the Fourier domain to the Fresnel domain [14, 15], the fractional Fourier domain [16, 17, 18] and the GD [19, 20]. The optical security system presented in [19] is based on phase-shifting interferometry, and therefore, the encrypted image and the decryption process differ from the DRPE presented in [3, 9]. The encryption scheme in the GD proposed in [20] presents the joint Gyrator power spectrum and the joint-extended Gyrator power spectrum, which are complex-valued distributions and consist of just a single term whereas the joint power spectrum (JPS) obtained in [9, 11, 12, 13] has four terms.

The security of the DRPE method is vulnerable to chosen–plaintext attacks (CPA) [21], known–plaintext attacks (KPA) [21], and ciphertext-only attack (COA) [22]. This weakness is due to the linear property of the DRPE method [21]. The DRPE implemented with a JTC is also vulnerable to CPA [23], KPA [24], and COA [25]. These plaintext attacks can be extended to the DRPE systems in the GD, provided the rotation angle of the Gyrator transform (GT) [26] is already known.

The GT is a new tool for manipulation of two-dimensional signals. It belongs to the linear canonical integral transforms as well as the fractional Fourier transform (FrFT) and describes the rotations in the phase space [26]. Rodrigo *et al.* have derived the main properties of the GT [26], designed a setup to optically implement this transform [27] and presented several applications of the GT to image processing [7]. The GT has been

utilized in image encryption with: RPMs generated by chaos [28], Arnold transform [29] and iterative random phase encoding [30, 31, 32], among other works.

In this work, we present a new modified nonlinear JTC in the GD to encrypt images that have been previously encoded in phase. The input plane of the JTC architecture is fully encoded in phase, this feature increases the security of the proposed encryption scheme against CPA, KPA and COA, because the two RPMs used in the proposed encryption scheme become security keys. This new encryption system will extend the DRPE implemented with a nonlinear JTC, as described in [13], to the GD in order to enhance the security of the system, because the rotation angle of the GT can be used as a new key for the encryption scheme. In fact, the rotation angle of the GT strongly affects the decryption process and the decrypted signal is rapidly degraded with small changes of this parameter. We extend the JPS in the Fourier domain presented in [9] to the GD by introducing a new definition of the joint Gyrator power distribution (JGPD). The nonlinear image encryption presented here uses a fully phase nonzero-order JTC [33] extended to the GD. The encrypted function is a real-valued distribution that can be computed from three intensity distributions. The encrypted image is obtained by introducing two nonlinear modifications to the JGPD, these nonlinear modifications will allow us to retrieve the original image in the decryption stage with higher image quality and also to increase the security of the proposed encryption system against several plaintext attacks.

In comparison to previous proposals, the amount of information to transmit does not increase since the resulting encrypted function has the same size as the original version [13, 14, 17]. The proposed encryption scheme can be implemented using a simplified nonzero-order JTC in the GD that avoids the beam splitting required by other optical JTC implementations [9, 19, 20]. Finally, the proposed nonlinear JTC-based encryption-decryption scheme in the GD preserves the shift-invariance property of previous JTC-based proposals [1, 14, 17].

The paper is organized as follows: in section 2, the GT and some important properties are introduced. In section 3, the encryption and decryption schemes are presented. Simulation results for the encryption and decryption schemes are provided in section 4. Cryptanalysis of the scheme is presented in section 5. Finally, conclusions are summarized in section 6.

2. Gyrator transform

The Gyrator transform (GT) is mathematically defined as a linear canonical integral transform which produces the twisted rotation in position–spatial frequency planes of phase space [26]. The GT at parameter α, which is the rotation angle, of a two-dimensional function $f(x, y)$ can be written in the following form

$$f_\alpha(u, v) = \mathcal{G}^\alpha\{f(x, y)\} = \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} f(x, y)K_\alpha(u, v, x, y)\mathrm{d}x\mathrm{d}y, \tag{1}$$

$$K_\alpha(u,v,x,y) = \frac{1}{|\sin\alpha|}\exp\left\{\frac{i2\pi}{\sin\alpha}\Big[(uv+xy)\cos\alpha-(vx+uy)\Big]\right\}, \qquad (2)$$

where $0 \le \alpha < 2\pi$, x and y denote the input coordinates at the spatial domain, u and v indicate the output coordinates in the GD and K_α is the Gyrator kernel. For $\alpha = 0$, it corresponds to the identity transform. For $\alpha = \pi/2$, it becomes the direct Fourier transform with rotation of the coordinate at $\pi/2$. For $\alpha = \pi$, the reverse transform is obtained. For $\alpha = 3\pi/2$, it corresponds to the inverse Fourier transform with rotation of the coordinate at $\pi/2$. The inverse GT corresponds to the GT at rotation angle $-\alpha$. There are certain similarities in the properties of the GT and the FrFT although these transforms are basically different. Thus, the kernel of the GT is a product of the hyperbolic and plane waves, whereas the kernel of the FrFT is the product of the spherical and the plane waves.

In addition to linearity, the main properties of the GT that will be used later in the encryption and decryption schemes, are

$$\mathcal{G}^\alpha\{\mathcal{G}^\beta\{f(x,y)\}\} = \mathcal{G}^{\alpha+\beta}\{f(x,y)\}, \qquad (3)$$

$$\mathcal{G}^\alpha\{\exp\{-i2\pi x_0 y\cot\alpha\}f(x-x_0,y)\} = \exp\{-i2\pi x_0 v\csc\alpha\}f_\alpha(u,v). \qquad (4)$$

where x_0 is a real constant.

3. Encryption and decryption schemes

In order to explain our proposal, we describe the encryption and decryption schemes with the aid of the well-known equation of the JTC architecture [1, 9, 10]. First, let us define the functions to use in the encryption and decryption schemes. The original image to be encrypted is represented by the real-valued function $f(x,y)$ with values in the interval [0, 1]; this original image is encoded in phase

$$f_{Ph}(x,y) = \exp\{i2\pi f(x,y)\}, \qquad (5)$$

and the RPMs $r(x,y)$ and $h(x,y)$ are given by the following equation

$$r(x,y) = \exp\{i2\pi s(x,y)\}, \quad h(x,y) = \exp\{i2\pi n(x,y)\}, \qquad (6)$$

where $s(x,y)$ and $n(x,y)$ are normalized positive functions randomly generated, statistically independent and uniformly distributed in the interval [0, 1]. The functions $f(x,y)$, $s(x,y)$ and $n(x,y)$ are images with $M \times N$ pixel size.

The input plane of a JTC is typically composed by two non-overlapping data distributions, $g(x,y)$ and $c(x,y)$, placed side-by-side [1, 9, 10]. Let us consider the first data distribution $g(x,y)$ be the original image encoded in phase $f_{Ph}(x,y)$ placed against the RPM $r(x,y)$ and modulated by a pure linear phase term

$$g(x,y) = \exp\{-i2\pi x_0 y\cot\alpha\}r(x,y)f_{Ph}(x,y). \qquad (7)$$

where x_0 is a real constant and α is the rotation angle to be used in the GT. Let us consider the second data distribution $c(x, y)$ of the input plane of the JTC be the RPM $h(x, y)$ modulated by a symmetrical (with respect to axis z) pure linear phase term

$$c(x, y) = \exp\{i2\pi x_0 y \cot\alpha\} h(x, y). \tag{8}$$

The GTs at parameter α of the functions $r(x, y) f_{Ph}(x, y)$ and $h(x, y)$ are given by

$$t_\alpha(u, v) = \mathcal{G}^\alpha\{r(x, y) f_{Ph}(x, y)\}, \quad h_\alpha(u, v) = \mathcal{G}^\alpha\{h(x, y)\}. \tag{9}$$

3.1. Encryption scheme

The input plane of the JTC-based encryption scheme is defined using the two phase-only images $g(x, y)$ and $c(x, y)$ placed side-by-side at coordinates $(x, y) = (x_0, 0)$ and $(x, y) = (-x_0, 0)$, respectively

$$m(x, y) = g(x - x_0, y) + c(x + x_0, y). \tag{10}$$

Figure 1 shows a representation for the input plane of the JTC-based encryption scheme. With $x_0 = M/2$ pixels, the spatial region of the input plane is fully covered by the input functions with no blank space.

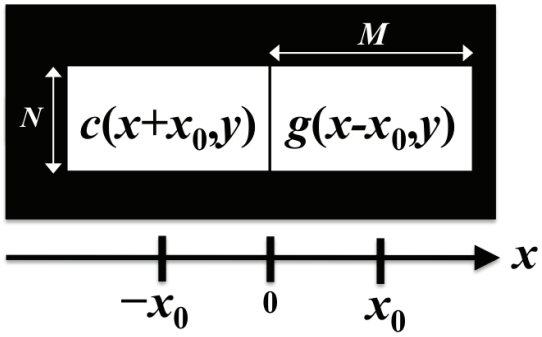

Figure 1. Representation of the input plane of the JTC-based encryption scheme.

We introduce the JGPD at parameter α as

$$\begin{aligned} \mathrm{JGPD}_\alpha(u, v) &= |\mathcal{G}^\alpha\{m(x, y)\}|^2 = |\mathcal{G}^\alpha\{g(x - x_0, y) + c(x + x_0, y)\}|^2 \\ &= |t_\alpha(u, v)|^2 + |h_\alpha(u, v)|^2 \\ &\quad + t^*_\alpha(u, v) h_\alpha(u, v) \exp\{i2\pi(2x_0) v \csc\alpha\} \\ &\quad + t_\alpha(u, v) h^*_\alpha(u, v) \exp\{-i2\pi(2x_0) v \csc\alpha\}. \end{aligned} \tag{11}$$

Note that in the definition of JGPD (Eq. (11)), the transforms $\mathcal{G}^\alpha\{g(x - x_0, y)\}$ and $\mathcal{G}^\alpha\{c(x + x_0, y)\}$ are centered at the same spatial point of the GD due to the pure linear phase terms ($\exp\{\pm i2\pi x_0 y \cot\alpha\}$) symmetrically introduced in $g(x - x_0, y)$ (Eq. (7) shifted to $(x, y) = (x_0, 0)$) and $c(x + x_0, y)$ (Eq. (8) shifted to $(x, y) = (-x_0, 0)$). The JGPD is a positive real-valued distribution.

The JGPD described by Eq. (11) is an extension to the GD of the joint power spectrum (JPS) in the Fourier domain but different from other definitions introduced in related papers [20].

In the next step of the encryption scheme, we use the nonzero-order joint transform correlator [33] extended to the GD. We eliminate the central orders ($|t_\alpha(u,v)|^2$ and $|h_\alpha(u,v)|^2$) of the JGPD. This modified JGPD is then divided by the nonlinear term $|h_\alpha(u,v)|^2$ in order to obtain the encrypted image [13, 17, 18]

$$\begin{aligned} e_\alpha(u,v) &= \frac{\mathrm{JGPD}_\alpha(u,v) - |t_\alpha(u,v)|^2 - |h_\alpha(u,v)|^2}{|h_\alpha(u,v)|^2} \\ &= t_\alpha^*(u,v)\frac{h_\alpha(u,v)}{|h_\alpha(u,v)|^2}\exp\{i2\pi(2x_0)v\csc\alpha\} \\ &\quad + t_\alpha(u,v)\frac{h_\alpha^*(u,v)}{|h_\alpha(u,v)|^2}\exp\{-i2\pi(2x_0)v\csc\alpha\}. \end{aligned} \tag{12}$$

If $|h_\alpha(u,v)|^2$ is equal to zero for a particular value of the coordinate (u,v), this intensity value is substituted by a small constant to avoid singularities when computing $e_\alpha(u,v)$. The encrypted image $e_\alpha(u,v)$ is a real-valued distribution that can be computed from the $\mathrm{JGPD}_\alpha(u,v)$, $|t_\alpha(u,v)|^2$ and $|h_\alpha(u,v)|^2$. Figure 2 depicts the optical encryption scheme (Part I) based on a fully phase nonzero-order JTC architecture and the optical decryption scheme (Part II) based on two successive GTs. The security keys needed for decryption are the two RPMs $r(x,y)$ and $h(x,y)$, and the rotation angle α of the GT. The RPM $r(x,y)$ is used to spread the information content of the original image $f(x,y)$ encoded in phase onto the encrypted distribution $e_\alpha(u,v)$. The nonlinear expression of Eq. (12) represents an extension to the GD of the nonlinear expression given in our previous work [13] for the nonzero-order JPS in the Fourier domain.

The two-step nonzero-order JTC [33, 34, 35] in the GD can be used to optically implement the encrypted distribution given by Eq. (12). In the first step, the intensity functions $|t_\alpha(u,v)|^2$ and $|h_\alpha(u,v)|^2$ are sequentially captured by a CCD camera placed in the output plane of the encryption scheme when the functions $g(x-x_0,y)$ and $c(x+x_0,y)$ are sequentially displayed on the input plane of the setup, respectively, and the optical GT is performed (Fig. 2, Part I). In the second step, the $\mathrm{JGPD}_\alpha(u,v)$ of Eq. (11) is captured [36]; for this step, the phase-only functions $c(x+x_0,y)$ and $g(x-x_0,y)$ are simultaneously placed at the input plane of the JTC. Subsequently, the intensity distributions $|t_\alpha(u,v)|^2$ and $|h_\alpha(u,v)|^2$ are digitally subtracted from the JGPD, and then, this result is divided by $|h_\alpha(u,v)|^2$; as a result, we obtain the encrypted image represented by Eq. (12).

We consider that the encrypted image is free of noise and not affected by partial occlusion. Such interesting issues are out of the scope of this paper and deserve further study, as we have done elsewhere [17]. The encrypted image is the only information to transmit. It is worth remarking that, when comparing with other related algorithms [13, 14, 15, 17], this encryption scheme does not increase the amount of data to be sent prior the decryption scheme. The optical GT can be performed by

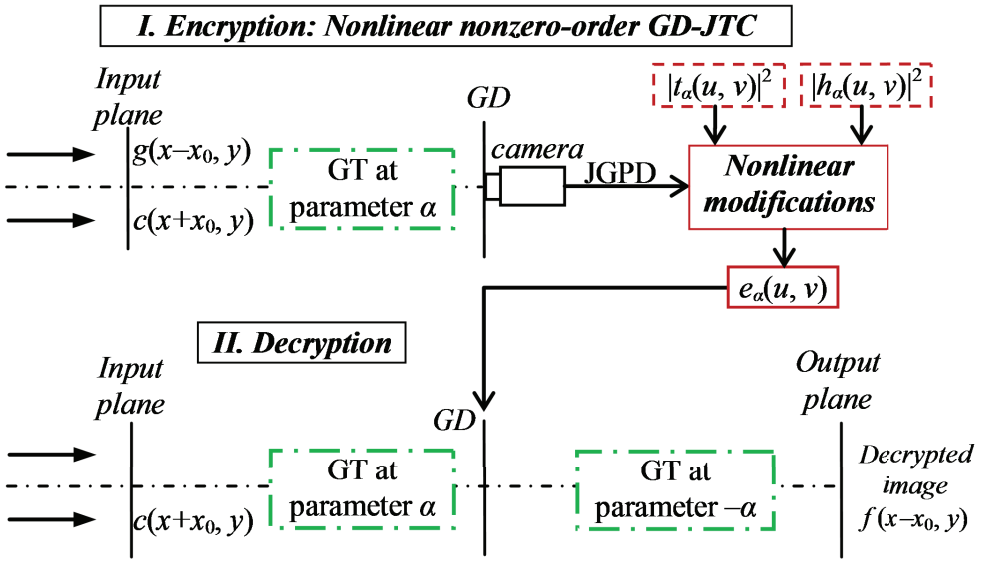

Figure 2. Schematic representation of the optical setup. The encryption scheme (Part I) is based on a fully phase nonzero-order JTC in the GD and the decryption scheme (Part II) is composed by two successive GTs.

means of the optoelectronic setup developed in [27], using a system composed of six thin cylinder lenses.

The linear phase terms symmetrically introduced in the two non-overlapping data distributions, $g(x, y)$ and $c(x, y)$, of the input plane of the JTC (see Eqs. (7) and (8), respectively) can be implemented using an optical biprism or a phase-only spatial light modulator (SLM). The RPMs $r(x, y)$ and $h(x, y)$ can be implemented using a simple diffuser glass [11, 13, 14]. In fact, these linear phase terms as well as the RPMs $r(x, y)$ and $h(x, y)$ can be displayed all together by means of a phase-only SLM.

3.2. Decryption scheme

For the decryption process (Fig. 2, Part II), the second data distribution $c(x, y)$ is placed at coordinate $(x, y) = (-x_0, 0)$ and is Gyrator transformed with rotation angle α; the result of this transformation is then multipled by the encrypted image $e_\alpha(u, v)$ to obtain

$$\begin{aligned} d_\alpha(u, v) &= e_\alpha(u, v)\mathcal{G}^\alpha\{c(x + x_0, y)\} \\ &= t^*_\alpha(u, v)\frac{h^2_\alpha(u, v)}{|h_\alpha(u, v)|^2}\exp\{i2\pi(3x_0)v\csc\alpha\} \\ &\quad + t_\alpha(u, v)\frac{h^*_\alpha(u, v)h_\alpha(u, v)}{|h_\alpha(u, v)|^2}\exp\{-i2\pi x_0 v\csc\alpha\}. \end{aligned} \tag{13}$$

In the optical implementation, the two terms of Eq. (13) would separate angularly from each other. By Gyrator transforming at parameter $-\alpha$ the second term of Eq. (13) and then, subtracting the phase shift $(-i2\pi x_0 y\cot\alpha)$, multiplying by the complex conjugate of $r(x - x_0, y)$ and finally, extracting the argument of the resulting phase

(function $\arg\{\cdot\}$), we obtain a version of the decrypted image $\tilde{f}(x,y)$ at coordinate $(x,y)=(x_0,0)$ given by

$$2\pi\tilde{f}(x-x_0,y)=\arg\{\mathcal{G}^{-\alpha}\{\exp\{-i2\pi x_0 v\csc\alpha\}t_\alpha(u,v)\}\times\exp\{i2\pi x_0 y\cot\alpha\}r^*(x-x_0,y)\}. \tag{14}$$

Additionally, if we use $c(x,y)$ at coordinate $(x,y)=(-x_1,0)$ and assuming that x_0 is replaced by x_1 in Eq. (8), the decrypted image can still be obtained at coordinate $(x,y)=(2x_0-x_1,0)$

$$2\pi\tilde{f}(x-2x_0+x_1,y)=\arg\{\mathcal{G}^{-\alpha}\{\exp\{-i2\pi(2x_0-x_1)v\csc\alpha\}t_\alpha(u,v)\}\times\exp\{i2\pi(2x_0-x_1)y\cot\alpha\}\times r^*(x-2x_0+x_1,y)\}. \tag{15}$$

Eq. (15) proves that the encryption-decryption method based on a nonlinear JTC in the GD preserves the shift-invariance property of the JTC-based encryption scheme in the Fourier domain, with respect to $c(x,y)$ (this distribution contains one key given by the RPM $h(x,y)$) and the recovered image in the decryption method.

We remark that the nonlinear operation introduced in Eq. (12) given by the term $|h_\alpha(u,v)|^2$ in the denominator, permits the retrieval of the original image in Eq. (14) [14, 15, 17, 18]. The decryption scheme presented in Fig. 2 (Part II) is based on two successive GTs and a phase retrieval function. These operations in the decryption scheme can be carried out by either optoelectronics [27] or digital [37] implementations.

4. Simulation results

Figure 3 shows an example to illustrate the simulation results obtained when using the encryption and decryption schemes presented in subsections 3.1 and 3.2. We apply the whole process to a picture of a natural scene, which contains fine structures and details. The original image to encrypt $f(x,y)$ and the random distribution code $s(x,y)$ of the RPM $r(x,y)$ are displayed in Figs. 3(a) and 3(b), respectively. The random distribution code $n(x,y)$ of RPM $h(x,y)$ has different values but similar appearance to the image presented in Fig. 3(b). The images $f(x,y)$, $s(x,y)$ and $n(x,y)$ are 512×512 pixel size ($M=N=512$). The encrypted image $e_\alpha(u,v)$ for the rotation angle $\alpha=0.885\pi$ in the GT is depicted in Fig. 3(c); the digital GT was implemented using the fast algorithm of discrete GT based on convolution operation [37]. The final distributions in phase for the output plane of the decryption scheme with the correct values keys, the rotation angle α of GT, and the RPMs $r(x,y)$ and $h(x,y)$, are shown in Fig. 3(d). The decrypted image $\tilde{f}(x,y)$ presented in Fig. 3(e) is the magnified region of interest, centered at position $(x,y)=(x_0,0)$, of Fig. 3(d).

Unlike proposals based on nonlinear correlation [38], we use the root mean square error (RMSE) [39] to quantitatively evaluate the quality of the decrypted images. The RMSE for the decrypted image $\tilde{f}(x,y)$ with respect to the original image $f(x,y)$ is

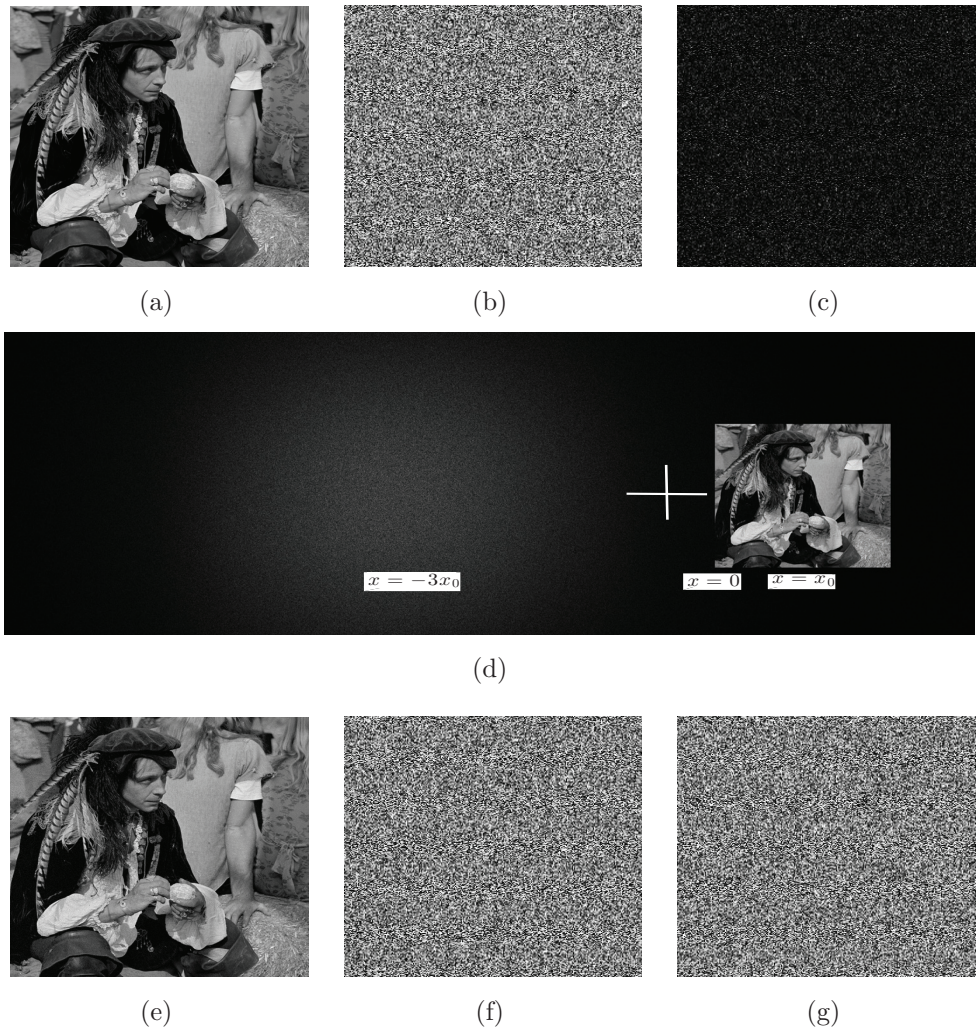

Figure 3. (a) Original image to encrypt $f(x, y)$. (b) Random distribution code $s(x, y)$ of the RPM $r(x, y)$. (c) Encrypted image $e_\alpha(u, v)$ for the rotation angle $\alpha = 0.885\pi$. (d) Final distributions in phase for the output plane of the decryption scheme with the correct parameters, rotation angle α of GT and keys RPMs $r(x, y)$ and $h(x, y)$. (e) Magnified region of interest of the output plane (d) with the image correctly decrypted. Unsuccessful decryptions: (f) when the denominator $|h_\alpha(u, v)|^2$ is not introduced in the encrypted function (Eq. (12)), (g) when just one of the keys (RPM $r(x, y)$) fails.

defined by

$$\mathrm{RMSE} = \left(\frac{\sum_{x=1}^{M} \sum_{y=1}^{N} [f(x, y) - \tilde{f}(x, y)]^2}{\sum_{x=1}^{M} \sum_{y=1}^{N} [f(x, y)]^2} \right)^{\frac{1}{2}}, \tag{16}$$

The RMSE between the original image (Fig. 3(a)) and the correctly decrypted image (Fig. 3(e)) is 15×10^{-3}. The image quality for the decrypted image (Fig. 3(e)) is higher because the central orders ($|t_\alpha(u, v)|^2$ and $|h_\alpha(u, v)|^2$) were removed from the JGPD and the nonlinear operation given by the term $|h_\alpha(u, v)|^2$ was introduced in the denominator of the encrypted function, see Eq. (12) [13, 14, 17].

Figure 3(f) shows an unsuccessful decryption produced when the nonlinear operation (Eq. (12)) is not properly applied. More specifically, when the term in the denominator of Eq. (12) is not introduced in the encrypted function, even though the correct values keys are used in the decryption scheme. The resulting image is noisy and does not disclose the original image. The RMSE between the original image of Fig. 3(a) and the distribution of Fig. 3(f) is 0.774. The result of Fig. 3(f) evidences that the nonlinearity $|h_\alpha(u,v)|^2$ introduced in the denominator of the encrypted function is essential to retrieve the original image in the decryption scheme [14, 15].

The noisy distribution of Fig. 3(g), corresponds to the result obtained when the key of the RPM $r(x,y)$ is wrong although the rest of the decryption process is correct. The RMSE between the original image from Fig. 3(a) and the distribution of Fig. 3(g) is 0.821. When a wrong RPM $h(x,y)$ or an incorrect value of the rotation angle α are used in the decryption scheme, the results after the decryption process are noisy distributions similar to Fig. 3(g). Therefore, the provided results prove that the all correct parameters and keys (the rotation angle α, and the RPMs $r(x,y)$ and $h(x,y)$) are required in the decryption scheme for a correct retrieval of the original image.

On the basis of the RMSE metric, the decrypted image of Fig. 3(e), with RMSE $= 15 \times 10^{-3}$, is of the same order quality as the decrypted image obtained after applying an encryption-decryption process based on JTC and FrFT with analogous nonlinear modification of the encrypted fractional power spectrum (RMSE $= 12 \times 10^{-3}$ obtained for the decrypted image of another natural scene; see reference [17] for details). As a matter of fact, the results obtained in the referred work [17] represent a larger series of numerical experiments since we considered a generalized formulation of the DRPE-encryption systems that covered a wide variety of JTC architectures defined by the fractional order and fractional Fourier operators (including the conventional Fourier domain JTC as a particular case).

From all these results, we estimate that the encryption system in the GD does not significantly affect the image quality of the decrypted image, but preserves the good quality already achieved by the encryption systems with generalized JTC architectures. The advantages of using fully-phase encoding and GD are then more related to the security of the system and its resistance to attacks, as we will see in the next section.

5. Cryptanalysis

5.1. Key space

The available key space of the proposed encryption scheme is analyzed in this section. For this purpose, every possible combination of the keys, i.e. the RPMs $r(x,y)$ and $h(x,y)$, and the rotation angle α of the GT, is considered.

Both RPMs $r(x,y)$ and $h(x,y)$ have a size of $M \times N$ pixels and each pixel has L possible values. The number of attempts required to retrieve both RPMs is of the order of L^{2MN}. For $L = 256$ gray levels and $M = N = 512$, then the number of RPMs to try

would be 256^{524288}. Therefore, the brute force attacks are intractable just considering every possibility of the two RPMs [21].

The GT has a period equal 2π with respect to the rotation angle α. The rotation angle can be expressed as $\alpha = p\pi/2$, where p has a period equal 4. The sensitivity on the rotation angle p of the GT for the decrypted images is examined by introducing a small error in this, and then by calculating the RMSE (Eq. (16)), between the original image $f(x, y)$ and the decrypted image $\tilde{f}(x, y)$ to measure the level of protection of the encrypted image $e_\alpha(u, v)$. Figure 4 shows the RMSE versus the relative error of p for the image retrieval and it was found that is sensitive to a variation of 10^{-7} in p. This sensitivity -and thus, system security- is much higher, more specifically, three orders of magnitude higher than the sensitivity shown by the encryption systems that use generalized JTC to variations in the fractional order [17]. The space key for the rotation angle of the GT is 4×10^7.

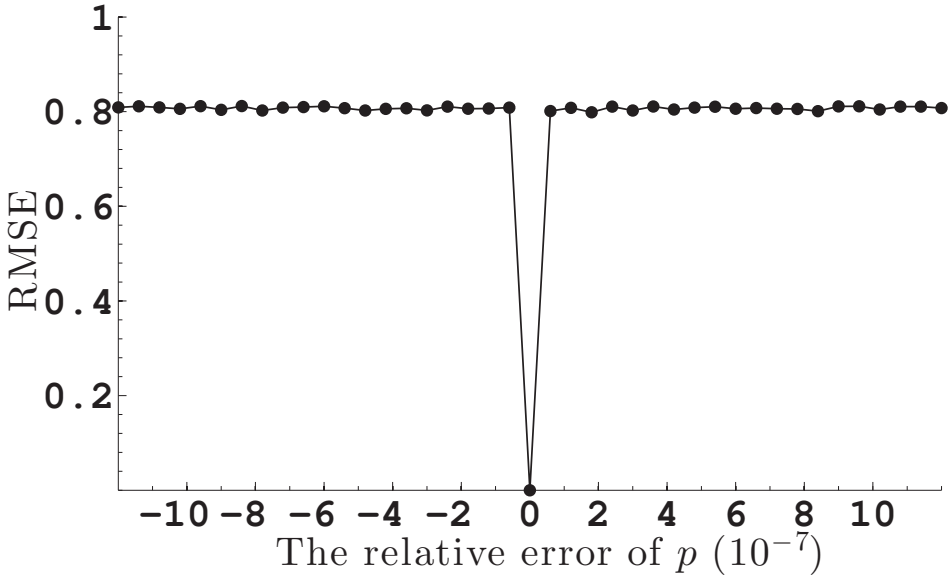

Figure 4. Variations of the RMSE versus the relative error of p for the decryption scheme.

5.2. Chosen–plaintext, known–plaintext and ciphertext–only attacks

The chosen-plaintext attack (CPA) [23], the known-plaintext attack (KPA) [24] and the ciphertext-only attack (COA) [25] have proven that the JTC-based encryption systems proposed in the references [9, 11, 12] are vulnerable to several attacks.

The encryption systems of references [9, 11, 12] were described in the Fourier domain with a RPM as a key. These security systems encode the original image in amplitude. When the original image is encoded in amplitude, only one of the two RPMs of the JTC-based encryption system is a key of the security system. If the original image

is encoded in phase, however, both RPMs become keys for the JTC-based encryption system.

The CPA and KPA presented in references [23] and [24], respectively, try to find the key represented by the RPM $h(x, y)$, using the complete knowledge of the security system, chosen plaintexts (images to encrypt) with its corresponding ciphertexts (encrypted images) and iterative phase retrieval algorithms. The CPA and KPA were specifically designed for the JPS in the Fourier domain and these attacks only were able to find one RPM key [23, 24]. The encryption scheme proposed in this paper is based on a nonlinear fully phase nonzero-order JTC in the GD, which has two RPMs as key. The CPA described in [23] does not break the security of our encryption scheme, because the nonlinear operations introduced in the JGPD (Eq. (12)) improve the security of the encryption scheme, as was demonstrated in references [13, 14], and the CPA is not able to find the RPM key represented by $r(x, y)$. We remark that it is very important to use the correct values of all keys in the decryption scheme, in order to retrieve the original image. The KPA described in [24] does not break the security of our encryption scheme either, because the convergency of the iterative phase retrieval algorithm extended to the GD and its use for this KPA would be affected by the introduction of the nonlinear operations in the JGPD [14, 17], and the KPA also is not able to find the RPM key given by $r(x, y)$. With the purpose of further improving the resistance of the JTC-based encryption in the GD against KPA, we recommend to use different probability density functions (uniform and nonuniform distributions) for the random code functions $s(x, y)$ and $n(x, y)$ corresponding to the RPMs $r(x, y)$ and $h(x, y)$, respectively, and replace the RPM $h(x, y)$ by a random complex mask (RCM) [14].

The COA implemented in [25] uses an iterative phase retrieval algorithm for retrieving an arbitrary plaintext by using only a ciphertext, whenever the plaintext was encoded in amplitude at the input plane of the JTC-based encryption scheme. The COA described in [25] fails when is applied to the encryption scheme proposed in this paper, because the plaintext is encoded in phase at the input plane of the JTC architecture. The difficulty to obtain any success by attacking our encryption system has been significantly increased due to the hardness of retrieving the phase information (the plaintext encoded in phase) from a single intensity (ciphertext) for the phase retrieval algorithm [22, 25, 40]. The COA is not able to retrieve the correct values of the RPMs $r(x, y)$ and $h(x, y)$ either [25].

For all these reasons, we can say that the proposed nonlinear fully phase nonzero-order JTC-based encryption system in the GD is resistant to the CPA, KPA and COA described in [23], [24] and [25], respectively.

6. Conclusion

In summary, we have introduced two nonlinear modifications in the JTC architecture to carry out fully phase image encryption in the GD. These modifications consist of the phase encoding of the image to encrypt and the nonlinear operations introduced in

the JGPD. As a result, the security of the encrypted image is improved and the system becomes more resistant to attacks, without deleterious effects on the quality of the decrypted image. The extension to the Gyrator domain adds the rotation angle as a new parameter that requires to be accurately set for satisfactory information decryption. The rotation angle of the GT also improves the security of the encryption scheme with respect to the JTC-based encryption systems in the fractional Fourier domain. The input plane of the JTC is efficiently used since it can be fully covered by the input functions with no need of leaving blank spaces between them. The retrieval of the original image with extremely low level of noise in the decryption process is possible due to the nonlinear modifications introduced in the JGPD. The recovered original image in the decryption scheme has higher image quality than other related systems that keep their joint power distribution unchanged. The nonlinear modifications of the JGPD, applied just before the generation of the encrypted image, do not increase the amount of data to transmit. The new encryption-decryption system proposed in this paper preserves the shift-invariance property of the RPM $h(x, y)$ for the decryption system and the retrieval of the original image. The encryption and decryption scheme is suitable for optoelectronics and/or digital implementation. The promising rapid development of optoelectronic devices will improve the experimental realization of the GT. The simulation results show that the retrieval of the original image in the decryption scheme is very sensitive to the changes in the keys (the two RPMs and the rotation angle of GT). We have analysed the high resistance of the proposed encryption scheme against brute force attacks, CPA, KPA and COA.

Acknowledgments

This research has been partly funded by the Spanish Ministerio de Ciencia e Innovación and Fondos FEDER (Project DPI2013-43220-R).

References

[1] M. S. Millán and E. Pérez-Cabré, "Optical data encryption," in *Optical and Digital Image Processing: Fundamentals and Applications*, G. Cristóbal, P. Schelkens, and H. Thienpont, eds. (Wiley, 2011), pp. 739–767.

[2] W. Chen, B. Javidi, and X. Chen, "Advances in optical security systems," Adv. Opt. Photon. **6**, 120–155 (2014).

[3] P. Réfrégier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. **20**, 767–769 (1995).

[4] 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).

[5] O. Matoba and B. Javidi, "Encrypted optical memory system using three-dimensional keys in the Fresnel domain," Opt. Lett. **24**, 762–764 (1999).

[6] G. Situ and J. Zhang, "Double random-phase encoding in the Fresnel domain," Opt. Lett. **29**, 1584–1586 (2004).

[7] J. A. Rodrigo, T. Alieva, and M. L. Calvo, "Applications of gyrator transform for image processing," Opt. Commun. **278**, 279–284 (2007).

[8] N. Towghi, B. Javidi, and Z. Luo, "Fully phase encrypted image processor," J. Opt. Soc. Am. A **16**, 1915–1927 (1999).
[9] T. Nomura and B. Javidi, "Optical encryption using a joint transform correlator architecture," Opt. Eng. **39**, 2031–2035 (2000).
[10] J. W. Goodman, *Introduction to Fourier Optics* (McGraw-Hill, 1996).
[11] 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).
[12] 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).
[13] J. M. 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).
[14] J. M. Vilardy, M. S. Millán, and E. Pérez-Cabré, "Nonlinear optical security system based on a joint transform correlator in the Fresnel domain," Appl. Opt. **53**, 1674–1682 (2014).
[15] J. M. Vilardy, M. S. Millán, and E. Pérez-Cabré, "Joint transform correlator-based encryption system using the Fresnel transform and nonlinear filtering," Proc. of SPIE **8785**, 87853J (2013).
[16] D. Lu and W. Jin, "Color image encryption based on joint fractional Fourier transform correlator," Opt. Eng. **50**, 068201 (2011).
[17] J. M. Vilardy, Y. Torres, M. S. Millán, and E. Pérez-Cabré, "Generalized formulation of an encryption system based on a joint transform correlator and fractional Fourier transform," J. Opt. **16**, 125405 (2014).
[18] J. M. Vilardy, M. S. Millán, and E. Pérez-Cabré, "Images encryption system based on a fractional joint transform correlator and nonlinear filtering," Opt. Pura y Appl. **47**, 35–41 (2014).
[19] H. Li, "Image encryption based on gyrator transform and two-step phase-shifting interferometry," Opt. and Lasers in Eng. **47**, 45–50 (2009).
[20] M. R. Abuturab, "Noise-free recovery of color information using a joint-extended gyrator transform correlator," Opt. Lasers and Eng. **51**, 230–239 (2013).
[21] 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).
[22] C. Guo, S. Liu, and J. T. Sheridan, "Iterative phase retrieval algorithms. Part II: Attacking optical encryption systems," Appl. Opt. **54**, 4709–4719 (2015).
[23] 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).
[24] 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).
[25] C. Zhang, M. Liao, W. He, and X. Peng, "Ciphertext-only attack on a joint transform correlator encryption system," Opt. Express **21**, 28523–28530 (2013).
[26] J. A. Rodrigo, T. Alieva, and M. L. Calvo, "Gyrator transform: properties and applications," Opt. Express **15**, 2190–2203 (2007).
[27] J. A. Rodrigo, T. Alieva, and M. L. Calvo, "Experimental implementation of the gyrator transform," J. Opt. Soc. Am. A **24**, 3135–3139 (2007).
[28] N. Singh and A. Sinha, "Gyrator transform-based optical image encryption, using chaos," Opt. and Lasers in Eng. **47**, 539-546 (2009).
[29] M. R. Abuturab, "Securing color information using Arnold transform in gyrator transform domain," Opt. and Lasers in Eng. **50**, 772-779 (2012).
[30] Z. Liu, Q. Guo, L. Xu, M. A. Ahmad, and S. Liu, "Double image encryption by using iterative random binary encoding in gyrator domains," Opt. Express **18**, 12033-12043 (2010).
[31] Z. Liu, L. Xu, C. Lin, J. Dai, and S. Liu, "Image encryption scheme by using iterative random phase encoding in gyrator transform domains," Opt. and Lasers in Eng. **49**, 542-546 (2011).
[32] H. Li and Y. Wang, "Double-image encryption based on iterative gyrator transform," Opt. Commun. **281**, 5745-5749 (2008).
[33] C-T. Li, S. Yin, and F. T. S. Yu, "Nonzero-order joint transform correlator," Opt. Eng. **37**, 58–65

(1998).

[34] 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).

[35] 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).

[36] 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. Physics: Conf. Ser. **274**, 012054 (2011).

[37] Z. Liu, D. Chen, J. Ma, S. Wei, Y. Zhang, J. Dai, and S. Liu, "Fast algorithm of discrete gyrator transform based on convolution operation," Optik **122**, 864–867 (2011).

[38] W. Chen, and X. Chen, "Optical authentication via photon-synthesized ghost imaging using optical nonlinear correlation," Opt. and Lasers in Eng. **73**, 123–127 (2015).

[39] R. C. Gonzalez, R. E. Woods, and S. L. Eddins, *Digital Image Processing Using Matlab,* 2nd ed. (Gatesmark Publishing, 2009).

[40] J. R. Fienup, "Phase retrieval algorithms: a comparison," Appl. Opt. **21**, 2758-2769 (1982).