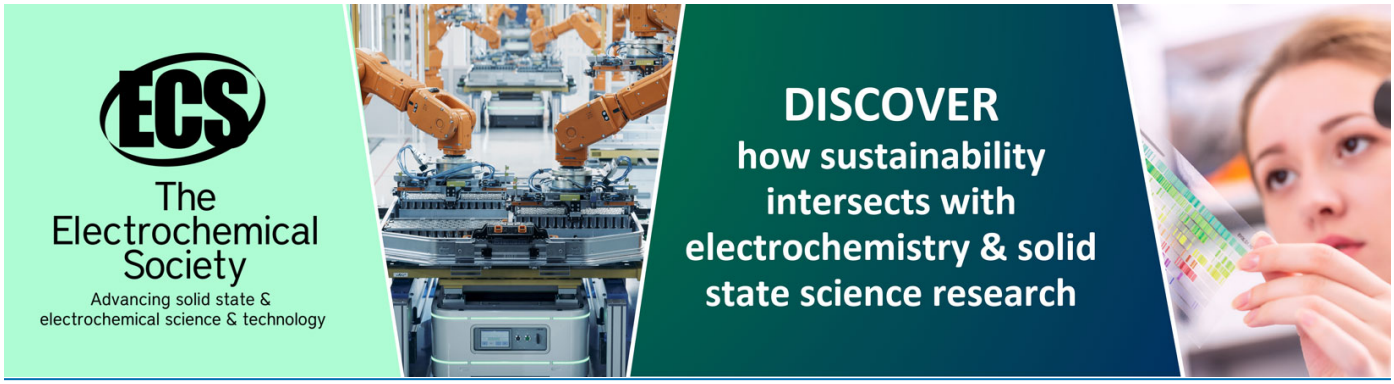
Nonlinear image encryption system using the Gyrator transform and truncation operations



Nonlinear image encryption system using the Gyrator transform and truncation operations

Ronal Perez, Juan M. Vilardy, Carlos J. Jimenez

Grupo GIFES. Faculty of engineering. Universidad de La Guajira, Riohacha (La Guajira), Colombia

E-mail: rperez@uniguajira.edu.co, jmvilardy@uniguajira.edu.co

Abstract. A new nonlinear system for image encryption using the Gyrator transform (GT) and the truncation operations is proposed in this work. The original image is encoded in phase at the beginning of the encryption process. The encryption-decryption system is based on the double random phase encoding (DRPE) in the Gyrator domain (GD). The rotation angle of the Gyrator transform is a new key that increases the security of the encryption system. The amplitude and phase truncation operations are nonlinear and no unitary, these truncation operations allow to select the information of amplitude or phase from a complex-valued image. We apply the truncation operations in the image encryption-decryption system in order to generate two new keys, convert the system in nonlinear and increase the security of the system. To retrieve the original image without error (noise-free) in the decryption system, it is needed all the correct security keys: the two RPMs, the rotation angle of the GT and the two key generated by the amplitude and phase truncation operations. The feasibility of this nonlinear encryption-decryption system is verified and analyzed by numerical simulations.

1. Introduction

The double random phase encoding (DRPE) is a successful method for optical image encryption [1, 2], the DRPE uses two random phase masks (RPMs) with the purpose of encoding the image to encrypt (original image) into a stationary white noise pattern (encrypted image). The optical DRPE can be implemented using a processor 4*f* [3] or a joint transform correlator [4, 5]. One of the main drawbacks of the image encryption systems based on the initial DRPE is that the security of the system is vulnerable to attacks, this weakness is due to the linear property of the DRPE scheme [1, 2, 5]. The DRPE has been further extended from the Fourier domain to the Fresnel domain [6-8], the fractional Fourier domain [9-15], the Gyrator domain (GD) [16-19] and other domains [20-23], with the purpose of adding more keys and increasing the security of the DRPE system.

The Gyrator transform (GT) is a mathematical tool for analysis and processing of two-dimensional signals [24]. The GT has been used in optics [25], signal processing [16] and image encryption [16-19]. In this paper, we propose a nonlinear image encryption-decryption system based on the DRPE in the GD and truncation operations. We use the GT to improve the security of the original DRPE by adding a new key for the encryption system, which is the rotation angle of the GT; the value of this rotation angle is a new key and it is set by the user of the encryption system. The amplitude and phase truncations operations are nonlinear [26] and we use them in order to convert the proposed security system in nonlinear, generate two new security keys and improve the security of the encrypted image.

The outline of the paper is as follows: the definition and properties of the GT are introduced in section 2. The amplitude and phase truncation operations are presented in section 3. The mathematical description of the encryption and decryption systems are described in section 4. In section 5 are presented the computer simulations of the encryption and decryption systems. Finally, the main ideas of the paper are summarized in section 6.

2. The Gyrator transform

The Gyrator transform (GT) at parameter α, called further as a rotation angle, of a two-dimensional function $f_i(x_i, y_i)$ is defined as

$$f_o(x_o, y_o) = \mathsf{G}^{\alpha}\{f_i(x_i, y_i)\}(x_o, y_o) = \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} f_i(x_i, y_i) K_{\alpha}(x_i, x_o, y_i, y_o)\mathrm{d}x_i\mathrm{d}y_i, \tag{1}$$

with

$$K_{\alpha}(x_i, x_o, y_i, y_o) = \frac{1}{|\sin(\alpha)|}\exp\left[i2\pi\frac{(x_o y_o + x_i y_i)\cos(\alpha) - (x_i y_o \quad x_o y_i)}{\sin(\alpha)}\right], \quad -\pi < \alpha \quad \pi, \tag{2}$$

where K_{α} is the kernel function of GT. The GT is mathematically defined as a linear canonical integral transform which produces the rotation in position–spatial frequency planes (x, q_y) and (y, q_x) of phase space [24]. For $\alpha = 0$, it corresponds to the identity transform. For $\alpha = \pm\pi/2$ it reduces to the direct/inverse Fourier transform with rotation of the coordinates at $\pi/2$. For $\alpha = \pm\pi$ the reverse transform described by the kernel $\delta(x_i \pm x_o, y_i \pm y_o)$ is obtained. The GT is periodic and additive with respect to rotation angle: the period is 2π and $\mathcal{G}^{\alpha}\mathcal{G}^{\beta} = \mathcal{G}^{\alpha+\beta}$, respectively. The inverse GT corresponds to the GT at angle $-\alpha$.

The main theorems such as scaling, shift, modulation, etc. for the GT have been formulated in ref. [24]. The optical GT can be implemented using the optoelectronic setup described in ref. [25]. The digital GT will be computed using the fast algorithm of discrete GT based on convolution operation [27] for the nonlinear image encryption-decryption system that it will be described in section 4.

3. Amplitude and phase truncation operations

The truncation operations are nonlinear mathematical tools that can be applied to a complex-valued image [26]. Let $f(x, y) = a(x, y)\exp\{i2\pi\varphi(x, y)\}$ be a complex-valued function, where $a(x, y)$ and $\varphi(x, y)$ represent the amplitude and the phase of the function $f(x, y)$, respectively. The amplitude $a(x, y)$ is a positive real-valued function and the phase $\varphi(x, y)$ is a real-valued function with positive and/or negative values.

The amplitude truncation (AT) allows to select the phase function $\varphi(x, y)$ from the complex-valued function $f(x, y)$. Therefore, the result of the AT when is applied to the complex-valued function $f(x, y)$ is

$$AT\{f(x,y)\} = AT\{a(x,y)\exp\{i2\pi\phi(x,y)\}\} = \phi(x,y). \tag{3}$$

The phase truncation (PT) allows to select the amplitude function $a(x, y)$ from the complex-valued function $f(x, y)$. When the PT is applied to the complex-valued function $f(x, y)$, we obtain

$$PT\{f(x,y)\} = PT\{a(x,y)\exp\{i2\pi\phi(x,y)\}\} = a(x,y). \tag{4}$$

4. Nonlinear image encryption and decryption systems

Let $f(x, y)$ be the real-valued image to encrypt (original image) with values in the interval [0, 1], and let $r(x, y)$ and $h(u, v)$ be two random phase masks (RPMs) given by

$$r(x,y) = \exp\{i2\pi s(x,y)\}, \quad h(u,v) = \exp\{i2\pi n(u,v)\}, \tag{5}$$

where (x, y) and (u, v) represent the coordinates for the spatial domain and the GD, respectively, $s(x, y)$ and $n(u, v)$ are normalized positive functions randomly generated, statistically independent and uniformly distributed in the interval [0, 1]. For the initial step of the encryption system, the original image $f(x, y)$ is encoded in phase $f_{ph}(x, y) = \exp\{i2\pi f(x, y)\}$ [11, 17]. Then, the image $f_{ph}(x, y)$ is multiplied by the RPM $r(x, y)$ and this product is transformed using the GT at parameter α

$$g_\alpha(u,v) = \mathsf{G}^\alpha\{r(x,y) f_{ph}(x,y)\} = q_\alpha(u,v)\exp\{i2\pi\phi_\alpha(u,v)\}, \tag{6}$$

where the functions $q_\alpha(u, v)$ and $\varphi_\alpha(u, v)$ represent the amplitude and the phase of the complex-valued image $g_\alpha(u, v)$, respectively. The real values of the functions $q_\alpha(u, v)$ and $\varphi_\alpha(u, v)$ are dependent on the values of the RPM $r(x, y)$ and the image $f_{ph}(x, y)$. We apply the amplitude and phase truncation operations over the image $g_\alpha(u, v)$ in order to obtain the following real-valued images

$$q_\alpha(u,v) = PT\{g_\alpha(u,v)\}, \quad \phi_\alpha(u,v) = AT\{g_\alpha(u,v)\}. \tag{7}$$

The amplitude image $q_\alpha(u, v)$ is multiplied by the RPM $h(u, v)$ and this product is transformed using the GT at parameter $-\alpha$

$$t(x,y) = \mathsf{G}^{-\alpha}\{q_\alpha(u,v)h(u,v)\} = e(x,y)\exp\{i2\pi\theta(x,y)\}, \tag{8}$$

where the functions $e(x, y)$ and $\theta(x, y)$ denote the amplitude and the phase of the complex-valued image $t(x, y)$, respectively. Finally, the amplitude and phase truncation operations are applied to the image $t(x, y)$

$$e(x,y) = PT\{t(x,y)\}, \quad \theta(x,y) = AT\{t(x,y)\}. \tag{9}$$

The encrypted image is given by the real-valued data distribution $e(x,y)$ and the five security keys of the encryption system are represented by the rotation angle α of the GT, the two RPMs $r(x, y)$ and $h(u, v)$ and the two pseudorandom images $\varphi_\alpha(u,v)$ and $\theta(x,y)$.

The decryption system uses the same process as the encryption system applied in the inverse sense. The inputs of the decryption system are the encrypted image $e(x, y)$ and the five security keys used in the encryption system. The output image of the decryption system is the decrypted image $d(x, y)$. When the security keys used in the encryption and decryption systems are the same, the decrypted image $d(x, y)$ is a replica of the original image $f(x, y)$.

The original image $f(x, y)$ can be retrieved at the output of the decryption system from the encrypted image $e(x, y)$ using the five correct security keys. The decrypted image $d(x, y)$ can be obtained using the following equations

$$q_\alpha(u,v) = h^*(u,v)\mathsf{G}^\alpha\{e(x,y)\exp\{i2\pi\theta(x,y)\}\}, \tag{10}$$

$$f_{ph}(x,y) = r^*(x,y)\mathsf{G}^{-\alpha}\{q_\alpha(u,v)\exp\{i2\pi\phi_\alpha(u,v)\}\}, \tag{11}$$

$$d(x,y) = AT\left\{f_{ph}(x,y)\right\} = f(x,y). \tag{12}$$

The original image $f(x, y)$ can be correctly recovered at the output of the decryption system whenever the values of the security keys (the rotation angle α of the GT, the two RPMs $r(x, y)$ and $h(u, v)$ and the two pseudorandom images $\varphi_\alpha(u, v)$ and $\theta(x, y)$) used in the encryption and decryption systems are the same.

5. Computer simulations

In this section, we present the results of numerical simulations to examine the validity and robustness of our proposed encryption-decryption system. All image used in the encryption and decryption systems have 512×512 pixels in grayscale. The original image $f(x, y)$ and the random distribution code $s(x, y)$ of the RPM $r(x, y)$ are presented in figures 1(a) and 1(b), respectively. The rotation angle of the

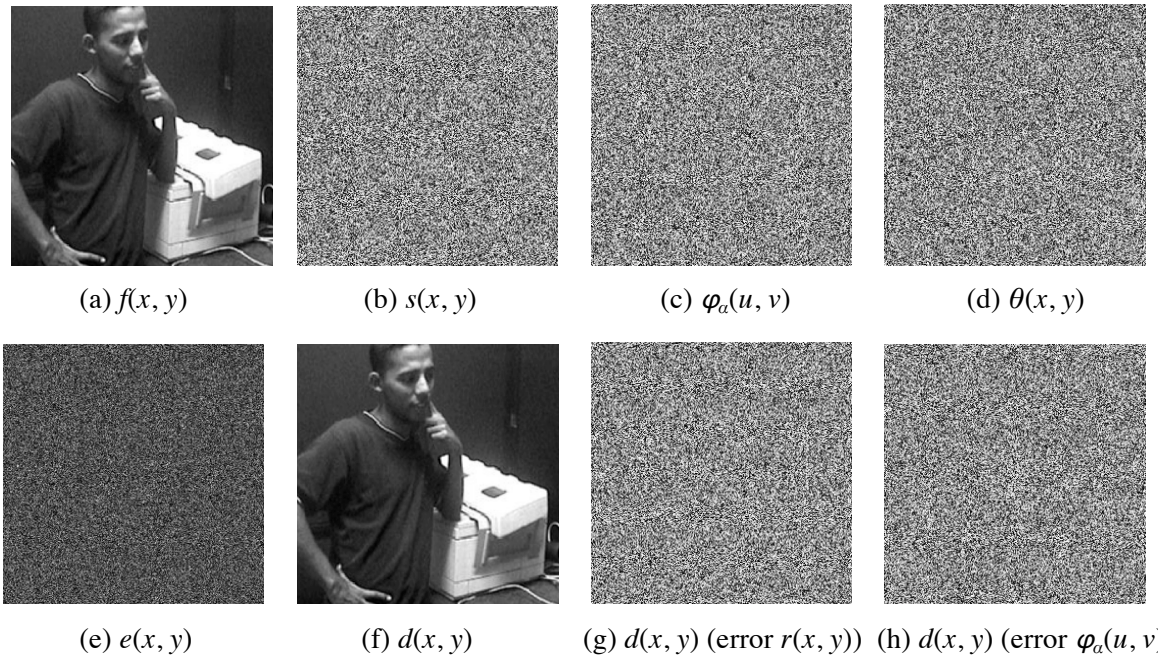
GT used in the encryption system is equal to $\alpha = 0.3547\pi$. The two obtained pseudorandom images $\varphi_\alpha(u, v)$ and $\theta(x, y)$ in the encryption process, are depicted in figures 1(c) and 1(d), respectively. These images have a noisy appearance very similar to the random code $s(x, y)$ of figure 1(b), but the two images $\varphi_\alpha(u, v)$ and $\theta(x, y)$ are pseudorandom data distributions because these images are dependent on the values of the image $f_{ph}(x, y)$, the rotation angle α of the GT and the RPMs $r(x, y)$ and $h(u, v)$.

The real-valued encrypted image $e(x, y)$ for the rotation angle $\alpha = 0.3547\pi$ of the GT is shown in figure 1(e). This encrypted image is a noisy data distribution which does not disclose any information of the original image $f(x, y)$. When the decryption process is done with the encrypted image $e(x, y)$ and the correct security keys (the rotation angle α of the GT, the two RPMs $r(x,y)$ and $h(u,v)$ and the two pseudorandom images $\varphi_\alpha(u, v)$ and $\theta(x, y)$), the original image $f(x, y)$ is recovered at the output of the decryption system with loses not visible to the human eye. The decrypted image $d(x, y)$ obtained from the encrypted image $e(x, y)$ and the correct security keys is shown in figure 1(f).

To evaluate the quality of the decrypted images, we use the root mean square error (RMSE) and the signal-to-noise ratio (SNR) between the decrypted images $d(x, y)$ and the original image $f(x, y)$ [5]

$$\mathrm{RMSE} = \left(\frac{\sum_{x=1}^{M}\sum_{y=1}^{N}[f(x,y)-d(x,y)]^2}{\sum_{x=1}^{M}\sum_{y=1}^{N}[f(x,y)]^2} \right)^{\frac{1}{2}}, \qquad \mathrm{SNR} = 10\log_{10}\left[\frac{\sum_{x=1}^{M}\sum_{y=1}^{N}[f(x,y)]^2}{\sum_{x=1}^{M}\sum_{y=1}^{N}[f(x,y)-d(x,y)]^2} \right]. \quad (13)$$

The values of the RMSE metric are between 0 and 1; when the value of the RMSE is close or equal to 0, this metric indicates an excellent quality image for the retrieval of the decrypted image whereas the values of the RMSE close or equal to 1 represent a worse quality image. The SNR is inversely proportional to RMSE and it is given in decibel (dB). The RMSE and the SNR between the original image of figure 1(a) and the decrypted image of figure 1(f) are 4.7×10^{-10} and 186.5 dB, respectively.



(a) $f(x, y)$ (b) $s(x, y)$ (c) $\varphi_\alpha(u, v)$ (d) $\theta(x, y)$

(e) $e(x, y)$ (f) $d(x, y)$ (g) $d(x, y)$ (error $r(x, y)$) (h) $d(x, y)$ (error $\varphi_\alpha(u, v)$)

Figure 1. (a) Original image to encrypt $f(x, y)$. (b) Random distribution code $s(x, y)$ of the RPM $r(x, y)$. Pseudorandom images for the rotation angle $\alpha = 0.3547\pi$: (c) $\varphi_\alpha(u, v)$, and (d) $\theta(x, y)$. (e) Encrypted image $e(x, y)$ for the rotation angle $\alpha = 0.3547\pi$ of the GT. (f) Decrypted image $d(x, y)$ using the five correct security keys (α, $r(x, y)$, $h_\alpha(u, v)$, $\varphi_\alpha(u, v)$, and $\theta(x, y)$). Decrypted images for the following wrong security keys: (g) the RPM $r(x, y)$, and (h) the pseudorandom image $\varphi_\alpha(u, v)$.

The obtained low RMSE and high SNR values between the original image of figure 1(a) and the decrypted image of figure 1(f) correspond to a good quality and excellent retrieval of the original image at the output of the decryption system. The obtained decrypted images from the encrypted image of figure 1(e) using a wrong RPM $r(x, y)$ or an incorrect pseudorandom image $\varphi_\alpha(u, v)$, are displayed in figures 1(g) and 1(h), respectively. The RMSEs and the SNRs between the original image of figure 1(a) and the decrypted images of figures 1(g) and 1(h) are 0.87 and 0.91, 1.2 dB and 0.82 dB, respectively. If the values of the rotation angle α of the GT, the RPM $h(u, v)$ and the pseudorandom image $\theta(x, y)$ used in the decryption method are not equal to the values used in the encryption method, the decrypted image will be a noisy pattern. Therefore, all the five security keys whit their correct values are needed in the decryption system for the correct retrieval of the original image.

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. We evaluate the sensitivity on the rotation angle p of the GT by introducing small errors in this and leaving fixed the other four security keys in the decryption system. The RMSE is used to measure the level of protection on the encrypted image. For this deviation test of the rotation angle p on the correct values for the decryption process, it is introduced a small error that varies between -1×10^{-6} and 1×10^{-6}, then for each variation is calculated the RMSE, the results for p is presented in figure 2. From computational experiments it was found that rotation angle is sensitive to a variation of 1×10^{-7}.

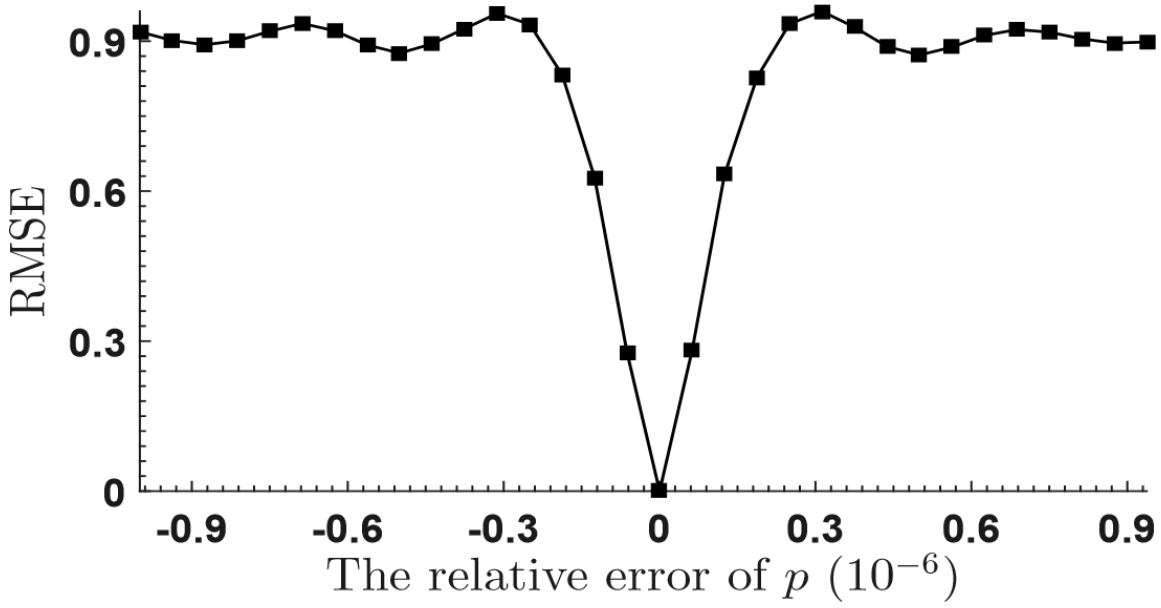


Figure 2. Deviation test of the rotation angle p on the correct values for the decryption process.

For the key space analysis of the proposed encryption system, it is considered every possible combination of keys: the rotation angle p of the GT, the two RPMs $r(x, y)$ and $h(u, v)$, and the two pseudorandom images $\varphi_\alpha(u, v)$ and $\theta(x, y)$. Using the obtained sensitivity of the rotation angle p, the key space for the rotation angle p of the GT is 4×10^7. The two RPMs $r(x, y)$ and $h(x, y)$, and the two pseudorandom images $\varphi_\alpha(u, v)$ and $\theta(x, y)$ have a size of 512×512 pixels and each pixel has L possible values. The number of attempts required to retrieve both RPMs and pseudorandom images is of the order of $L^{4(512)^2}$. For $L = 256$ gray levels, then the number of RPMs and pseudorandom images to try would be $256^{1048576}$. Therefore, the brute force attacks are intractable just considering every possibility of the two RPMs and the two pseudorandom images [17]. The total key space of the nonlinear

encryption process proposed in this paper is: $(4\times10^7)\cdot256^{1048576}$, this number represents a very larger key space.

6. Conclusions

A new nonlinear security system has been proposed for image encryption-decryption involving the use of the Gyrator transform and the amplitude and phase truncation operations. The Gyrator transform increases the security on the encrypted image due to the addition of a new key, given by the rotation angle α. The simulation results show that the retrieval of the original image in the decryption scheme is very sensitive to the changes on the security key of the rotation angle. Apart from this, the two obtained pseudorandom images by the amplitude truncation increase much more the security for any cryptanalyst who tries to decrypt the digital image without authorization. The keys of the proposed nonlinear encryption-decryption system are represented by one rotation angle of the GT, two RPMs and two pseudorandom images. These five key allow to obtain a very larger key space for the proposed security system. The simulation results have shown that the encryption-decryption systems are more secure because the decrypted images are very sensitive to the changes on the five security keys.

Acknowledgments

This research has been funded by the Universidad de La Guajira.

References

[1] Millán M S and Pérez-Cabré E 2011 *Optical and Digital Image Processing: Fundamentals and Applications* ed G Cristóbal, P Schelkens and H Thienpont (Weinheim: Wiley) chapter 33 pp 739–67
[2] Réfrégier P and Javidi B 1995 *Opt. Lett.* **20** 767–9
[3] Goodman J W 1996 *Introduction to Fourier Optics* (Columbus: McGraw-Hill)
[4] Nomura T and Javidi B 2000 *Opt. Eng.* **39** 2031–5
[5] Vilardy J, Millán M S and Pérez-Cabré E 2013 *J. Opt.* **15** 025401
[6] Situ G and Zhang J 2004 *Opt. Lett.* **29** 1584–6
[7] Vilardy J, Millán M S and Pérez-Cabré E 2014 *Appl. Opt.* **53**, 1674–82
[8] Vilardy J, Millán M S and Pérez-Cabré E 2013 *Proc. of SPIE* **8785**, 87853J
[9] Unnikrishnan G, Joseph J and Singh K 2000 *Opt. Lett.* **25** 887–9
[10] Vilardy J, Torres C and Mattos L 2008 *AIP Conf. Proc.* **992** 1067–72
[11] Vilardy J, Torres C and Mattos L 2008 *Revista Colombiana de Física* **40** 143–6
[12] Vilardy J, Torres C and Mattos L 2011 *Revista Colombiana de Física* **43** 523–7
[13] Vilardy J, Torres Y, Millán M S and Pérez-Cabré E 2014 *J. Opt.* **16** 125405
[14] Vilardy J, Millán M S and Pérez-Cabré E 2014 *Opt. Pura y Apl.* **47** 35–41
[15] Ozaktas H M, Zalevsky Z and Kutay M A 2001 *The Fractional Fourier Transform: with Applications in Optics and Signal Processing* (Weinheim: Wiley)
[16] Rodrigo J A, Alieva T and Calvo M L 2007 *Opt. Commun.* **278** 279–84
[17] Vilardy J, Millán M S and Pérez-Cabré E 2016 Nonlinear image encryption using a fully phase nonzero-order joint transform correlator in the Gyrator domain *Opt. Laser Eng.* (*Preprint* http://dx.doi.org/10.1016/j.optlaseng.2016.02.013)
[18] Vilardy J, Torres C and Mattos L 2013 *Proc. of SPIE* **8785** 87851Q
[19] Vilardy J, Millán M S and Pérez-Cabré E 2015 *Proc. 20th Symposium on Signal Processing, Images and Computer Vision (STSIVA)* (*Bogotá*) vol 1 (Washington: IEEE) pp 1–6
[20] Morales Y, Díaz L and Torres C 2015 *J. Phys.: Conf. Series* **582** 012063
[21] Vilardy J, Torres C and Jimenez C 2013 *Proc. of SPIE* **8785** 87851R
[22] Vilardy J, Torres C, Useche J and Mattos L 2011 *J. Phys.: Conf. Series* **274** 012047
[23] Vilardy J, Torres C, Useche J and Mattos L 2011 *Revista Colombiana de Física* **43** 170–4
[24] Rodrigo J A, Alieva T and Calvo M L 2007 *Opt. Express* **15** 2190–203

[25] Rodrigo J A, Alieva T and Calvo M L 2007 *J. Opt. Soc. Am.* A **24** 3135–9
[26] Qin W and Peng X 2010 *Opt. Lett.* **35** 118–20
[27] Liu Z, Chen D, Ma J, Wei S, Zhang Y, Dai J and Liu S 2011 *Optik* **122** 864–7