Image encryption using the Gyrator transform and random phase masks generated by using chaos

Juan M. Vilardy, Carlos J. Jimenez, and Ronal Perez
Grupo GIFES. Faculty of engineering. Universidad de La Guajira, Riohacha (La Guajira), Colombia
E-mail: jmvilardy@uniguajira.edu.co

Abstract. The Gyrator transform (GT), chaotic random phase masks (CRPMs) and a random permutation of the Jigsaw transform (JT) are utilized to design an images encryption-decryption system. The encryption-decryption system is based on the double random phase encoding (DRPE) in the Gyrator domain (GD), this technique uses two random phase masks (RPMs) to encode the image to encrypt (original image) into a random noise. The RPMs are generated by using chaos, these masks are CRPMs. The parameters of the chaotic function have the control of the generation of the CRPMs. We apply a random permutation to the resulting image of the DRPE technique, with the purpose of obtaining an encrypted image with a higher randomness. In order to successfully retrieve the original image (without errors or noise-free) at the output of the decryption system is necessary to have all the proper keys, which are: the rotation angles of the GTs, the parameters of the chaotic function utilized to generate the two CRPMs and the random permutation of the JT. We check and analyze the validity of the image encryption and decryption systems by means of computing simulations.

1. Introduction
The image encryption is different from traditional cryptology because the spatial, frequency and redundancy features of the image to encrypt are analysed and processed by the image encryption system [1]. The double random phase encoding (DRPE) is a successful method for optical image encryption [1–3], 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). 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 [1–3]. The DRPE has been further extended from the Fourier domain to the Fresnel domain [4–6], the fractional Fourier domain [7–12], the Gyrator domain (GD) [13–16] and other domains [17–20], 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 [21]. The GT has been used in optics [22], signal processing [13] and image encryption [13–16].

In this paper, we propose a nonlinear image encryption-decryption system based on the DRPE, the GT, the chaotic random phase masks (CRPMs) and the Jigsaw transform (JT), in order to overcome the security vulnerabilities of the initial DRPE proposed in Ref. [2]. We use the GT to improve the security of the original DRPE by adding a new key for the encryption system (the
rotation angle of the GT). It has been demonstrated that the nonlinearities introduced in the initial DRPE leading to an improvement in security [3, 5, 11, 14]. The generation of the RPMs by using a chaotic map allows to obtain the chaotic RPMs or CRPMs with a higher security. We use the Logistic map in order to generate the random codes of the CRPMs [23]. The values of the generated random codes are highly sensitive to the values of the parameters that control the iterations of the Logistic map [23]. This high sensitivity on the parameters of the Logistic map is used to obtain keys with a high security. The generation of the CRPMs by using the Logistic map is a nonlinear process. Finally, we use the JT in order to convert the encrypted image more random and to make the encryption/decryption system becomes nonlinear.

The outline of the paper is as follows: the definition and properties of the GT are introduced in section 2. The process to generate the random code of the CRPM by using a chaotic map is presented in section 3. The JT is introduced in section 4. In section 5, the nonlinear encryption and decryption systems are described. Simulation results for the encryption and decryption systems are provided in section 6. Finally, conclusions are summarized in section 7.

2. The Gyrator transform

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

\[
f_o(x_o, y_o) = \mathcal{G}^{\alpha}\{f_i(x_i, y_i)\} = \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} f_i(x_i, y_i) K_\alpha(x_i, x_o, y_i, y_o) dx_i dy_i,
\]

with

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

where \( K_\alpha \) 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 [21]. 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 \( 2\pi \) 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. [21]. The optical GT can be implemented using the optoelectronic setup described in ref. [22]. The digital GT will be computed using the fast algorithm of discrete GT based on convolution operation [24] for the nonlinear image encryption-decryption system that it will be described in section 5.

3. Random phase masks (RPMs) generated by using chaos

The RPMs for the encryption and decryption systems are generated by using a chaotic map. We use the Logistic map in order to generate the random codes of the CRPMs. The Logistic map is a one-dimensional chaotic map defined as

\[
x_{n+1} = \lambda x_n (1 - x_n),
\]

where \( \lambda \in (0, 4) \), \( x_n \in [0, 1] \) and \( n = 0, 1, 2, 3, \ldots \) [23]. The Logistic map given by the Eq. (3) is a recursive relation that it uses one initial value for \( x_n \), which is \( x_0 \), and one value for \( \lambda \). When the values \( x_0 \in [0, 1] \) and \( \lambda \in [3.6, 4) \), the sequence \( x_n \) is chaotic [23].
Figure 1. (a) Random code generated by using the Logistic map, and (b) Histogram of the random code generated in (a).

The random codes of the CRPMs are random real-valued images of $M \times N$ pixels. In order to generate a random code of $M \times N$ pixels, we set the values of $x_0 \in [0, 1]$ and $\lambda \in [3.6, 4]$, and the Eq. (3) is iterated $n$ times. The value of $x_{n+1}$ will be the first value of the random code. Then, the Logistic map given by the Eq. (3) is iterated $MN - 1$ times. The generated values between $x_{n+1}$ and $x_{n+MN}$ represent the values of the random code when these generated values are reshaped into a two-dimensional array of $M \times N$ pixels. All the generated pixels have their values in the interval $[0, 1]$. Therefore, we need three parameters ($n$, $x_0$ and $\lambda$) with the purpose of generating a random code of $M \times N$ pixels by using the Logistic map.

A generated random code of $512 \times 512$ pixels for the parameters $n = 121$, $x_0 = 0.712745$ and $\lambda = 3.89945$ is shown in figure 1(a). The histogram of the generated random code is presented in figure 1(b). The pixel values of the generated random code by using the Logistic map follow the values of an uniform distribution, this type of random distribution is commonly used in the optical encryption systems based on the DRPE [1, 2].

The generation of the random code by using the Logistic map or other chaotic map is more convenient to distribute or to store the RPMs keys of an encryption system, because it is not necessary to distribute or to store all the $M \times N$ pixels of the random code. We just need to provide three parameters in order to generate a random code of $M \times N$ pixels by using the Logistic map.

4. The Jigsaw transform

The Jigsaw transform (JT) is defined as a juxtaposition of different sections of an image [25]. A simple two-dimensional case is shown in figure 2(a). The effect of this transform on an image (figure 2(b)) is shown in figure 2(c).

In this case the image was broken up into 64 subsections of $8 \times 8$ pixels size, which were repositioned relative to each other according to some permutation. The permutation used is random. The JT is unitary, energy being conserved through the transform and it also has an inverse. In the case shown in figure 2(c), there are $64!$ possible permutations for the JT. Each particular JT is denoted by some index e.g. $J_b\{\}$ and its inverse is denoted by $J_{-b}\{\}$.

5. Nonlinear image encryption and decryption systems

In this section, we describe all the processes about the encryption and decryption systems. The image to encrypt (original image) $f(x, y)$ is a real-valued distribution and their pixel values are
The CRPMs $r(x, y)$ and $h(u, v)$ are given by

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

where $(x, y)$ and $(u, v)$ represent the coordinates for the spatial domain and the GD determined by the result of the GT at parameter $\alpha$, respectively, $s(x, y)$ and $n(u, v)$ are random codes generated by using the Logistic map and the generation process described in section 3. All the pixel values of $s(x, y)$ and $n(u, v)$ are in the interval $[0, 1]$. To generate the random code $s(x, y)$, we use three parameters $(n^{(1)}, x_0^{(1)}, \lambda^{(1)})$ and for the random code $n(u, v)$, we utilize $(n^{(2)}, x_0^{(2)}, \lambda^{(2)})$.

First, we describe all the steps of the encryption system. The original image $f(x, y)$ is encoded in phase $f_{ph}(x, y) = \exp\{i2\pi f(x, y)\}$ [9, 14]. The image $f_{ph}(x, y)$ is bonded to the CRPM $r(x, y)$ and then, the GT at parameter $\alpha$ is performed

$$g_\alpha(u, v) = \mathcal{F}^\alpha \{r(x, y) f_{ph}(x, y)\}.$$  

The complex-valued distribution $g_\alpha(u, v)$ is multiplied by the CRPM $h(u, v)$ and this product is transformed using the GT at parameter $\beta$. Finally, we apply the JT with an index $b$ to the result of the last GT, in order to obtain the complex-valued encrypted image

$$e(p, q) = J_b\{\mathcal{F}^{\beta} \{h(u, v) g_\alpha(u, v)\}\} = e_a(p, q) \exp\{i2\pi c_{ph}(p, q)\},$$

where $(p, q)$ are the coordinates for the GD given by the result of the GT at parameter $\alpha + \beta$, the index $b$ of the JT denotes a specific random permutation of $T$ elements, the real-valued images $e_a(p, q)$ and $c_{ph}(p, q)$ are the amplitude and phase distribution of the complex-valued encrypted image $e(p, q)$. The CRPMs $r(x, y)$ and $h(u, v)$ are used to spread the information content of the original image $f_{ph}(x, y)$ onto the encrypted distribution $e(p, q)$ and to make this encrypted distribution a stationary white noise pattern [1, 2]. The JT provides a higher randomness to the encrypted image. The nine security keys of the encryption system are given by the two rotation angle $\alpha$ and $\beta$ of the GTs, the six parameters $(n^{(1)}, x_0^{(1)}, \lambda^{(1)})$ and $(n^{(2)}, x_0^{(2)}, \lambda^{(2)})$ used to generate the random code $s(x, y)$ of the CRPM $r(x, y)$ and the random code $n(u, v)$ of the CRPM $h(u, v)$, respectively, and the random permutation of $T$ elements used in the JT.

The decryption process is the same encryption process applied in the inverse sense on the complex-valued encrypted image $e(p, q)$ with the index $-b$ of the JT, the complex conjugate of the CRPMs $r(x, y)$ and $h(u, v)$ and the negatives rotation angles $(-\alpha$ and $-\beta$) for the GTs. Using the additivity property of the GT and the inverse of the JT, we obtain

$$d(x, y) = \arg\{r^*(x, y) \mathcal{F}^{-\alpha} \{h^*(u, v) \mathcal{F}^{-\beta} \{J_{-b}\{e(p, q)\}\}\}\} = 2\pi f(x, y),$$

where the function $\arg\{\cdot\}$ is used for extracting the argument of the resulting phase. The original image $f(x, y)$ can be correctly recovered without errors at the output of the decryption system whenever the values of the nine security keys used in the encryption and decryption systems are the same.
Figure 3. (a) Original image to encrypt $f(x,y)$. Complex-valued encrypted image for the rotation angles $\alpha = 1.77\pi$ and $\beta = 0.41\pi$ of the GTs and the other seven security keys: (b) Amplitude image $e_a(p,q)$, and (c) Phase image $e_{ph}(p,q)$. (d) Decrypted image $d(x,y)$ using the right values of the nine security keys. Decrypted images for the following wrong security keys: (e) the rotation angle $\alpha = 1.770001\pi$, (f) the parameter $x_0^{(2)} = 0.245775001$, and (g) the random permutation used in the JT.

6. Computer simulations

The results of the computer simulations of the encryption and decryption systems following the steps described in section 5 are shown in figure 3. All image used in the encryption and decryption systems have $512 \times 512$ pixels in grayscale. The image to be encrypted (original image) is presented in figure 3(a). The random code $s(x,y)$ of the CRPM $r(x,y)$ generated by using the process described in section 3 with the parameters $n^{(1)} = 121$, $x_0^{(1)} = 0.712745$ and $\lambda^{(1)} = 3.89945$, it was depicted in figure 1(a). The random code $n(u,v)$ of the CRPM $h(u,v)$ was generated by using the Logistic map with the parameters $n^{(2)} = 577$, $x_0^{(2)} = 0.245775$ and $\lambda^{(2)} = 3.93217$. The random code $n(u,v)$ of the CRPM $h(u,v)$ has different values but similar appearance to the image presented in figure 1(a).

The amplitude and phase images of the complex-valued encrypted image for the rotation angles $\alpha = 1.77\pi$ and $\beta = 0.41\pi$ of the GTs, the previous generated CRPMs $r(x,y)$ and $h(u,v)$ and a random permutation of 1024 elements of the JT, are shown in figures 3(b) and 3(c), respectively. When the JT is applied over an image, this image is divided in blocks of $32 \times 32$ pixels and each block is repositioned by using the same random permutation of 1024 elements and the JT. The decrypted image $d(x,y)$ obtained from the complex-valued encrypted image $e(x,y)$ and the right values of the nine security keys is shown in figure 3(d).

To evaluate the quality of the decrypted images, we use the root mean square error (RMSE) between the decrypted images $d(x,y)$ and the original image $f(x,y)$ [3]

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

(8)
The values of the RMSE metric for evaluating image quality 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 at the output of the decryption system whereas the values of the RMSE close or equal to 1 represent a worse quality image. The RMSE between the original image of figure 3(a) and the decrypted image of figure 3(d) is $4.4 \times 10^{-32}$. Therefore, the decrypted image of figure 3(d) is a perfect replica of the original image $f(x, y)$.

The random pattern images presented in figures 3(e), 3(f) and 3(g) correspond to the obtained decrypted images from the encrypted image $e(p, q)$ using a wrong value for the rotation angle $\alpha$, the parameter $x_0^{(2)}$ or an incorrect random permutation used in the JT, respectively. The RMSEs between the original image of figure 3(a) and the decrypted images of figures 3(e), 3(f) and 3(g) are 0.81, 0.72 and 0.87, respectively. When the other six security keys ($\beta$, $n^{(1)}$, $x_0^{(1)}$, $\lambda^{(1)}$, $n^{(2)}$, and $\lambda^{(2)}$) used in the decryption process are not equal to the values used in the encryption process, the decrypted image is a noisy pattern very similar to the figures 3(e), 3(f) and 3(g). Therefore, all the nine security keys with their correct values are needed in the decryption system for the correct retrieval of the original image.

The key space analysis for the proposed nonlinear encryption system consists of every possible combination of the values of the nine security keys: the two rotation angles $\alpha$ and $\beta$ of the GTs, the six parameters $(n^{(1)}, x_0^{(1)}, \lambda^{(1)})$ and $(n^{(2)}, x_0^{(2)}, \lambda^{(2)})$ used to generate the random code $s(x, y)$ of the CRPM $r(x, y)$ and the random code $n(u, v)$ of the CRPM $h(u, v)$, respectively, and the random permutation of 1024 elements used in the JT.

The GT has a period equal $2\pi$ with respect to the rotation angle $\alpha$ or $\beta$. From computational experiments it was found that the rotation angles $\alpha$ or $\beta$ are sensitive to a variation of $1 \times 10^{-7}$. This sensitivity of the rotation angle of the GT was calculated using the values of the RMSE between the original image and the decrypted images for different rotation angles, including the right and wrong values of $\alpha$ and $\beta$. Therefore, the key space for the two rotation angles of the GTs is $4\pi^2 \times 10^{14}$.

The parameter $n$ used in the generation of the random codes of the CRPMs is limited to the maximum value of $1 \times 10^6$, this value depends on the computing power used to generate the random code. The possibles values for $n^{(1)}$ and $n^{(2)}$ are $1 \times 10^{12}$. From computational experiments it was found that the parameters $x_0$ and $\lambda$ are sensitive to a variation of $1 \times 10^{-16}$ and $1 \times 10^{-15}$, respectively. The parameters $x_0 \in [0, 1]$ and $\lambda \in [3.6, 4)$. Therefore, the possibles values for $x_0^{(1)}$ and $x_0^{(2)}$ are $1 \times 10^{32}$, and the possibles values for $\lambda^{(1)}$ and $\lambda^{(2)}$ are $1.6 \times 10^{29}$.

The random permutation of the JT has 1024 elements. Thus, there are 1024! possible permutations for the JT.

Finally, the total key space of the proposed nonlinear encryption process is of the order of $(4\pi^2 \times 10^{14})(1 \times 10^{12})(1 \times 10^{32})(1.6 \times 10^{29}) \cdot (1024!) = (6.3 \times 10^{88}) \cdot (1024!)$, this number represents a very larger key space. Hence, the brute force attacks are intractable just considering every possibility of the nine security keys.

7. Conclusions

A new nonlinear method for images encryption and decryption has been proposed involving the use of the double random phase encoding technique, the Gyrator transform (GT), the generation of random phase masks (RPMs) by using a chaotic map and the Jigsaw transform (JT). The nine security keys allow to obtain a very larger key space for the proposed security system. Therefore, the secret of the encrypted image is very-well protected against security attacks. The GT increases the security on the encrypted image due to the addition of a new key, given by the rotation angle. The generation of the chaotic RPMs or CRPMs by using the Logistic map is more suitable to distribute or to storage these security keys, because it is much easier to generate a random code of $M \times N$ pixels using a chaotic iterative map with three parameters.
instead of distributing or storing all the $M \times N$ pixels of the random code. The generation of the CRPMs is very sensitive with respect to the values of the three parameters used in the Logistic map. Apart from this, the random permutation used in the nonlinear JT increases much more the security for any cryptanalyst who tries to decrypt the digital image without authorization. The encrypted image is more protected due to the result of the JT and the all possible random permutations that can be used in the JT. Finally, the simulation results have shown that the encryption-decryption systems are more secure because the decrypted images are very sensitive to the change on the right values of the nine 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] Vilardy J, Millán M S and Pérez-Cabré E 2013 *J. Opt.* 15 025401
[4] Situ G and Zhang J 2004 *Opt. Lett.* 29 1584–6
[5] Vilardy J, Millán M S and Pérez-Cabré E 2014 *Appl. Opt.* 53, 1674–82
[6] Vilardy J, Millán M S and Pérez-Cabré E 2013 *Proc. of SPIE* 8785, 87853J
[7] Unnikrishnan G, Joseph J and Singh K 2000 *Opt. Lett.* 25 887–9
[8] Vilardy J, Torres C and Mattos L 2008 *AIP Conf. Proc.* 992 1067–72
[9] Vilardy J, Torres C and Mattos L 2008 *Revista Colombiana de Física* 40 143–6
[10] Vilardy J, Torres C and Mattos L 2011 *Revista Colombiana de Física* 43 523–7
[11] Vilardy J, Torres Y, Millán M S and Pérez-Cabré E 2014 *J. Opt.* 16 125405
[12] Vilardy J, Millán M S and Pérez-Cabré E 2014 *Opt. Para y Apl.* 47 35–41
[13] Rodrigo J A, Alieva T and Calvo M L 2007 *Opt. Commun.* 278 279–84
[14] 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)
[15] Vilardy J, Torres C and Mattos L 2013 *Proc. of SPIE* 8785 87851Q
[16] 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 Publishing) pp 1–6
[17] Morales Y, Díaz L and Torres C 2015 *J. Phys.: Conf. Series* 582 012063
[18] Vilardy J, Torres C and Jimenez C 2013 *Proc. of SPIE* 8785 87851R
[19] Vilardy J, Torres C, Useche J and Mattos L 2011 *J. Phys.: Conf. Series* 274 012047
[20] Vilardy J, Torres C, Useche J and Mattos L 2011 *Revista Colombiana de Física* 43 170–4
[21] Rodrigo J A, Alieva T and Calvo M L 2007 *Opt. Express* 15 2190–203
[22] Rodrigo J A, Alieva T and Calvo M L 2007 *J. Opt. Soc. Am. A* 24 3135–9
[23] Artur M 2002 *Chaos, Soliton & Fractals* 14 1749–56
[24] Liu Z, Chen D, Ma J, Wei S, Zhang Y, Dai J and Liu S 2011 *Optik* 122 864–7
[25] Hennelly B and Sheridan J 2003 *Opt. Lett.* 28 269–71