DOI: 10.1109/WIO.2016.7745605

Effects of using an encrypted image corrupted by noise and occlusion in a security system based on joint transform correlator and Gyrator transform

Juan M. Vilardy O.
Grupo de investigación GIFES
Universidad de La Guajira
Riohacha (La Guajira)–Colombia
E-mail: jmvilardy@uniguajira.edu.co

María S. Millán and Elisabet Pérez–Cabré
Grupo de Óptica Aplicada y Procesado de Imagen
Universitat Politècnica de Catalunya · BarcelonaTech
Terrassa (Barcelona)–Spain
E-mail: millan@oo.upc.edu, elisabet.perez@upc.edu

***Abstract*—Recently, a novel nonlinear encryption system based on joint transform correlator (JTC) in the Gyrator domain (GD) was proposed. The encryption system uses a fully nonlinear non-zero order JTC and Gyrator transform (GT). The decryption system is based on two successive GTs. The proposed system preserves the good quality of the decrypted image while increases the overall security of the complete process. In this work, we analyse the performance of this security system when the encrypted image is affected by common sources of degradation such as noise or occlusion. We test its robustness against additive and multiplicative noise affecting the encrypted function. We also study the effect of data loss due to partial occlusion of the encrypted information. The performance of the encryption-decryption system in the GD is evaluated using the metric of the root mean square error (RMSE) between the original image and the decrypted image when the encrypted image is corrupted by noise or modified by occlusion.**

I. Gyrator transform (GT)

The GT is mathematically defined as a linear canonical integral transform which produces the twisted rotation in position–spatial frequency planes of phase space [1]. 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

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

$$K_\alpha(u,v,x,y) = \frac{e^{i2\pi[(uv+xy)\cot\alpha-(vx+uy)\csc\alpha]}}{|\sin\alpha|}, \tag{2}$$

$$\alpha = \frac{p\pi}{2}, \quad \text{where: } 0 \le \alpha < 2\pi, \text{ and } 0 \le p < 4, \tag{3}$$

where x and y denote the coordinates at the spatial domain, u and v indicate the output coordinates in the Gyrator domain (GD) and K_α is the gyrator kernel. The inverse GT corresponds to the GT at rotation angle $-\alpha$. In addition to linearity, the main properties of the GT that will be used later in the encryption and decryption schemes, are

$$\mathscr{G}^\alpha\{\mathscr{G}^\beta\{f(x,y)\}\} = \mathscr{G}^{\alpha+\beta}\{f(x,y)\}, \tag{4}$$

$$\mathscr{G}^\alpha\{e^{-i2\pi x_0 y\cot\alpha}f(x-x_0,y)\} = e^{-i2\pi x_0 v\csc\alpha}f_\alpha(u,v), \tag{5}$$

where x_0 is a real constant.

II. Encryption and decryption systems based on joint transform correlator (JTC) and GT

The encryption and decryption systems to analyse and test in the next section were proposed in ref. [2]. We briefly describe the security system in this section. Let $f(x,y)$ be the real original image to be encrypted with values in the interval [0, 1]; this original image is encoded in phase $f_{Ph}(x,y) = \exp\{i2\pi f(x,y)\}$. The two random phase masks (RPMs) $r(x,y)$ and $h(x,y)$ are given by

$$r(x,y) = e^{i2\pi s(x,y)}, \quad h(x,y) = e^{i2\pi n(x,y)}, \tag{6}$$

where $s(x,y)$ and $n(x,y)$ are normalized positive functions randomly generated, statistically independent and uniformly distributed in the interval [0, 1]. For the encryption process, we have two non-overlapping data distributions placed side-by-side in the input plane of the JTC. Let us consider the first data distribution 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

$$g(x,y) = e^{-i2\pi x_0 y\cot\alpha}r(x,y)f_{Ph}(x,y), \tag{7}$$

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 of the input plane of the JTC be the RPM $h(x,y)$ modulated by another pure linear phase term

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

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

$$\begin{aligned} t_\alpha(u,v) &= \mathscr{G}^\alpha\{r(x,y)f_{Ph}(x,y)\}, \\ h_\alpha(u,v) &= \mathscr{G}^\alpha\{h(x,y)\}. \end{aligned} \tag{9}$$

In the encryption system, $g(x,y)$ and $c(x,y)$ are placed side by side on the input plane of the JTC at coordinates

978-1-5090-2163-5/16/$31.00 ©2016 IEEE

$(x,y)=(x_0,0)$ and $(x,y)=(-x_0,0)$, respectively. The joint Gyrator power distribution (JGPD) at parameter α is [2]

$$\text{JGPD}_\alpha(u,v)=\left|\mathscr{G}^\alpha\left\{g(x-x_0,y)+c(x+x_0,y)\right\}\right|^2. \quad (10)$$

To generate the encrypted image [2], we substract the central orders ($|t_\alpha(u,v)|^2$ and $|h_\alpha(u,v)|^2$) from the JGPD and divide by the nonlinear term $|h_\alpha(u,v)|^2$, thus obtaining the expression

$$\begin{aligned} e_\alpha(u,v) &= \frac{\text{JGPD}_\alpha(u,v)-|t_\alpha(u,v)|^2-|h_\alpha(u,v)|^2}{|h_\alpha(u,v)|^2} \\ &= t^*_\alpha(u,v)\frac{h_\alpha(u,v)}{|h_\alpha(u,v)|^2}e^{i2\pi(2x_0)v\csc\alpha} \\ &\quad + t_\alpha(u,v)\frac{h^*_\alpha(u,v)}{|h_\alpha(u,v)|^2}e^{-i2\pi(2x_0)v\csc\alpha}, \end{aligned} \quad (11)$$

where Eq. (5) has been used to obtain the complete expression of the encrypted image. 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 $\text{JGPD}_\alpha(u,v)$, $|t_\alpha(u,v)|^2$ and $|h_\alpha(u,v)|^2$. 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. Figure 1 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.

In the decryption system, the 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

$$\begin{aligned} d_\alpha(u,v) &= e_\alpha(u,v)\mathscr{G}^\alpha\left\{c(x+x_0,y)\right\} \\ &= t^*_\alpha(u,v)\frac{h^2_\alpha(u,v)}{|h_\alpha(u,v)|^2}e^{i2\pi(3x_0)v\csc\alpha} \\ &\quad + t_\alpha(u,v)\frac{h^*_\alpha(u,v)h_\alpha(u,v)}{|h_\alpha(u,v)|^2}e^{-i2\pi x_0 v\csc\alpha}. \end{aligned} \quad (12)$$

By Gyrator transforming at parameter $-\alpha$ the second term of Eq. (12) and then, subtracting the phase shift $(-i2\pi x_0 y\cot\alpha)$,

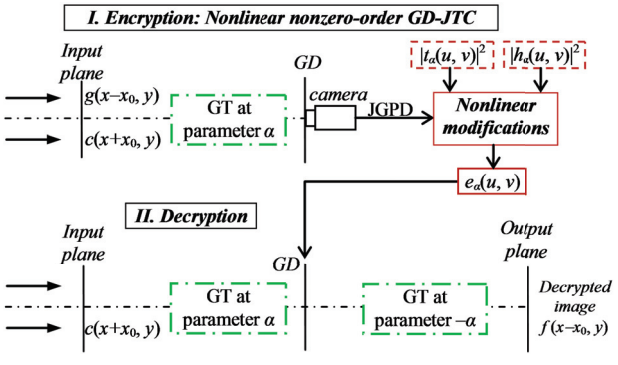


Fig. 1. Schematic representation of the optical setup. The encryption scheme (Part I) is based on a fully phase nonzero-order JTC in the GD and the decryption scheme (Part II) is composed by two successive GTs.

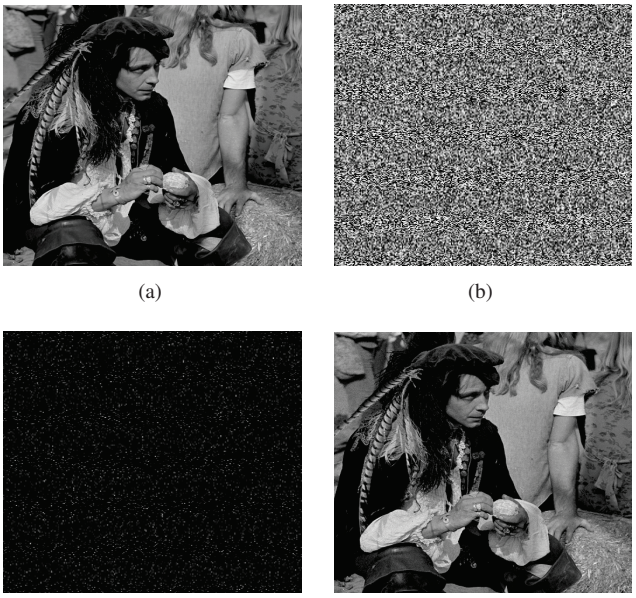


Fig. 2. (a) Original image to encrypt $f(x,y)$. (b) Random distribution code $s(x,y)$ of the RPM $r(x,y)$. (c) Encrypted image $e_\alpha(u,v)$ for the rotation angle $\alpha=0.885\pi$. (d) The image correctly decrypted with the correct parameters, rotation angle α of GT and keys RPMs $r(x,y)$ and $h(x,y)$.

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

$$\begin{aligned} 2\pi\tilde{f}(x-x_0,y) = \arg\{&\mathscr{G}^{-\alpha}\{e^{-i2\pi x_0 v\csc\alpha}t_\alpha(u,v)\} \\ &\times e^{i2\pi x_0 y\cot\alpha}r^*(x-x_0,y)\}. \end{aligned} \quad (13)$$

The encryption and decryption processes, following the steps described in this section, are illustrated with an example in Fig. 2. The original image to encrypt $f(x,y)$ and the random distribution code $s(x,y)$ of the RPM $r(x,y)$ are depicted in Figs. 2(a) and 2(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. 2(b). The images $f(x,y)$, $s(x,y)$ and $n(x,y)$ are 512×512 pixel size ($M\times N=512\times512$). The encrypted image $e_\alpha(u,v)$ for the rotation angle $\alpha=0.885\pi$ in the GT is depicted in Fig. 2(c). The decrypted image, in phase, $\tilde{f}(x,y)$ presented in Fig. 2(d) is obtained centered at position $(x,y)=(x_0,0)$ of the output plane of the decryption system, when the correct values keys ($r(x,y)$, $h(x,y)$ and α) are used.

To evaluate the quality of the decrypted image, we use the root mean square error (RMSE) defined by [3]

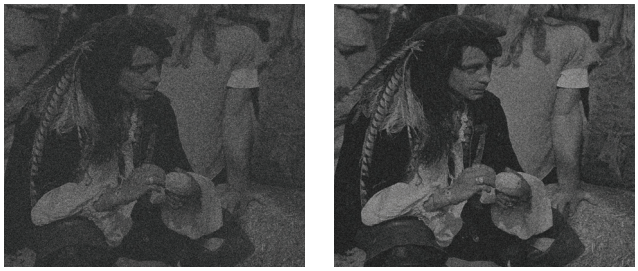
$$\text{RMSE}=\left(\frac{\sum_{x=1}^{M}\sum_{y=1}^{N}[f(x,y)-\tilde{f}(x,y)]^2}{\sum_{x=1}^{M}\sum_{y=1}^{N}[f(x,y)]^2}\right)^{\frac{1}{2}}, \quad (14)$$

where $f(x,y)$ and $\tilde{f}(x,y)$ denote the original image and the decrypted image, respectively. The RMSE between the original image of Fig. 2(a) and the correctly decrypted image

of Fig. 2(d) is 15×10^{-3}. A high image quality for the decrypted image (Fig. 2(d)) is retrieved, 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. (11) [2].

III. Encrypted image corrupted by noise or modified by occlusion

We evaluate the performance of the encryption-decryption system described in the previous section, when the encrypted image is corrupted by noise or modified by occlusion. The quality of the decrypted image is computed using the RMSE metric. Figure 3 depicts the retrieved images when the encrypted function shown in Fig. 2(c) is corrupted by noise. Applied noise consists of Gaussian white noise with zero mean and variance of $\sigma^2 = 0.2$. Figure 3(a) presents the decrypted image when additive noise is considered and Fig. 3(b) corresponds to multiplicative noise. In both cases, decryption has been performed with the correct key values ($r(x,y)$, $h(x,y)$ and α). The RMSEs between the original image (Fig. 2(a)) and the decrypted images (Figs. 3(a) and 3(b)) are 0.3761 and 0.2925, respectively.



(a) (b)

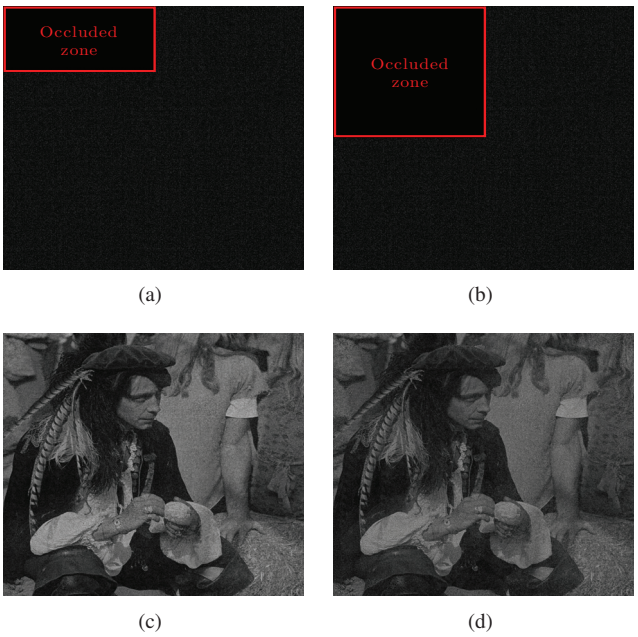
Fig. 3. Decrypted images when the encrypted image of Fig. 2(c) is corrupted by a Gaussian white noise with zero mean and variance of $\sigma^2 = 0.2$: (a) additive noise and (b) multiplicative noise.

If the encrypted image of Fig. 2(c) is occluded by 12.5% (Fig. 4(a)) and 25% (Fig. 4(b)) of its area (the values of occluded pixels are replaced with zero values), we obtain the decrypted images depicted in Figs. 4(c) and 4(d), respectively, when the correct keys values ($r(x,y)$, $h(x,y)$ and α) are used. The RMSEs between the original image (Fig. 2(a)) and the decrypted images (Figs. 4(c) and 4(d)) are 0.1815 and 0.2545, respectively.

Despite the loss of quality that affects the decrypted images shown in Figs. 3(a), 3(b), 4(c), and 4(d), the presence of the original image (Fig. 2(a)) can be recognized in all the evaluated cases. These examples show the robustness of the encryption-decryption system to certain amount of degradation (noise or occlusion) in the encrypted image.

IV. Conclusion

In this paper we have described an encryption system based on a nonlinear joint transform correlator and the Gyrator transform. We have shown and tested the performance of the nonlinear JTC-based encryption-decryption system in the Gyrator domain, when the encrypted image is affected by the degradation of noise or occlusion and we evaluate the quality of the resulting decrypted image using the RMSE metric. The security system shows a slightly better response when the encrypted image is corrupted by multiplicative noise in comparison to additive noise. As it was expected, the quality of the decrypted image decreases when the occluded part of the encrypted image is increased. However, the quality of the resulting decrypted images is still acceptable when the encrypted image is occluded up to a quarter of its area.



(a) (b)

(c) (d)

Fig. 4. Occluded encrypted images from Fig. 2(c) with the following percentage occlusion of its area: (a) 12.5% and (b) 25%. Decrypted images corresponding to the occluded encrypted images of: (c) Fig. 4(a) and (d) Fig. 4(b).

Acknowledgment

This research has been funded by the Universidad de La Guajira from Riohacha (La Guajira), Colombia, and the Spanish Ministerio de Ciencia e Innovación and Fondos FEDER (Project DPI2013-43220-R).

References

[1] J. A. Rodrigo, T. Alieva, and M. L. Calvo, "Gyrator transform: properties and applications," Opt. Express **15**, 2190–2203 (2007).

[2] J. M. Vilardy, M. S. Millán and E. Pérez–Cabré, "Nonlinear image encryption using a fully phase nonzero-order joint transform correlator in the Gyrator domain," Opt. and Lasers in Eng. (2016), http://dx.doi.org/10.1016/j.optlaseng.2016.02.013.

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