Occlusion and noise tests on the encrypted image produced by a security system based on a joint transform correlator and the Fresnel transform

IOP Conf. Series: Journal of Physics: Conf. Series **1221** (2019) 012046 doi:10.1088/1742-6596/1221/1/012046

Occlusion and noise tests on the encrypted image produced by a security system based on a joint transform correlator and the Fresnel transform

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

[1]Grupo GIFES. Faculty of Basic and Applied Sciences. Universidad de La Guajira, Riohacha (La Guajira), Colombia

[2]Grupo de Óptica Aplicada y Procesado de Imagen. Universitat Politècnica de Catalunya · BarcelonaTech, Terrassa (Barcelona)–Spain

E-mail: jmvilardy@uniguajira.edu.co

Abstract. In this work, the occlusion and noise test on the encrypted image produced by a joint transform correlator-based encryption system in the Fresnel domain (FrD) are computed and presented, in order to check the performance of this security system with respect to the image quality resulting in the decryption process for the retrieved image. The encryption system based on a joint transform correlator (JTC) in the FrD was proposed by us, with the purpose of using a lensless optical setup. We test the performance of this security system when the encrypted image is affected by common sources of degradation such as noise (additive and multiplicative) or partial occlusion. Finally, we evaluate the performance and robustness of the security system in the FrD by using the metric of the root mean square error (RMSE) between the image to encrypt and the decrypted image when the encrypted image is degraded by noise or modified by occlusion.

1. Introduction

An important technique for optical encryption is the double random phase encoding (DRPE) [1], this technique uses two random phase masks (RPMs) to encode the original image into an encrypted image (stationary white noise pattern). The DRPE has been further extended from the Fourier domain to the Fresnel domain (FrD) [2–6] and the fractional Fourier domain [7–10], in order to increase the number of keys and to improve the security of the encryption-decryption system. The DRPE can be implemented using a holographic system based on the optical processor $4f$ [11]. The physical implementation of the optical processor $4f$ requieres a strict optical alignment, making hard this optical implementation. To alleviate these constraints, Nomura and Javidi have been proposed the use of the joint transform correlator (JTC) architecture for the optical implementation of the DRPE [12]. This JTC architecture for the DRPE [12,13] also was extended from de Fourier domain to the FrD [14–16], the fractional Fourier domain [17–19] and the Gyrator domain [20], with the purpose of improving both the security of the encrypting system and the quality of the decrypted image.

In this paper, we show a nonlinear image encryption-decryption system using two RPMs and a JTC in the FrD to check the performance and robustness of this security system when the encrypted image is degraded by noise or occlusion. For these test, the values of the RPMs

and the physical parameters of the FrT are not modified. The rest of the paper is organized as follows. The definition of the FrT is presented in section 2. The formulation and the numerical simulation of the security system in the FrD are described in section 3. In section 4 are presented the results of the occlusion and noise tests on the encrypted image and the retrieved image at the decryption system. Finally, the main ideas of the paper are summarized in section 5.

2. The Fresnel transform and important properties

The Fresnel transform (FrT) of an object $f(x)$, written in one-dimensional notation for the sake of simplicity, at a propagation distance z when it is illuminated by a plane wave of wavelength λ, can be expressed as [11]

$$f_z(u) = \mathrm{FrT}_{\lambda,z}\{f(x)\} = \int_{-\infty}^{+\infty} f(x) h_{\lambda,z}(u,x)\mathrm{d}x, \tag{1}$$

with

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

where the operator $\mathrm{FrT}_{\lambda,z}$ denotes the FrT at parameters λ and z, $h_{\lambda,z}$ is the kernel of the transformation and $M_{\lambda,z}$ is a constant for a given distance of propagation z. The properties of the FrT that are used in the encryption-decryption system of section 3, are

$$\mathrm{FrT}_{\lambda,z_1}\{\mathrm{FrT}_{\lambda,z_2}[f(x)]\} = \mathrm{FrT}_{\lambda,z_1+z_2}\{f(x)\}, \tag{3}$$

$$\mathrm{FrT}_{\lambda,z}\left\{\exp\left(\frac{i2\pi v_0 x}{\lambda z}\right) f(x-x_0)\right\} = \exp\left\{\frac{i\pi}{\lambda z}\left(2uv_0 - v_0^2\right)\right\} f_z(u-x_0-v_0), \tag{4}$$

where x_0 and v_0 are real constants. If we choose $v_0 = -x_0$, the Eq. (4) is reduced to [14]

$$\mathrm{FrT}_{\lambda,z}\left\{\exp\left(\frac{-i2\pi x_0 x}{\lambda z}\right) f(x-x_0)\right\} = \exp\left\{\frac{-i\pi}{\lambda z}\left(2ux_0 + x_0^2\right)\right\} f_z(u). \tag{5}$$

3. Nonlinear JTC-based encryption system in the Fresnel domain

The encryption and decryption systems to test and check in the next section were proposed in ref. [14] and it is described in this section. Let $f(x)$ be the real original image to encrypt with values in the interval [0, 1]. The two random phase masks (RPMs) $r(x)$ and $h(x)$ are given by

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

where $s(x)$ and $n(x)$ are normalized positive functions randomly generated, statistically independent and uniformly distributed in the interval [0, 1]. In the encryption process, we have two non-overlapping data distributions placed side-by-side in the input plane of the JTC. The first data distribution is the original image $f(x)$ placed against the RPM $r(x)$ and modulated by a pure linear phase term

$$g(x) = \exp\left\{\frac{-i2\pi x_0(x+x_0)}{\lambda z}\right\} r(x) f(x), \tag{7}$$

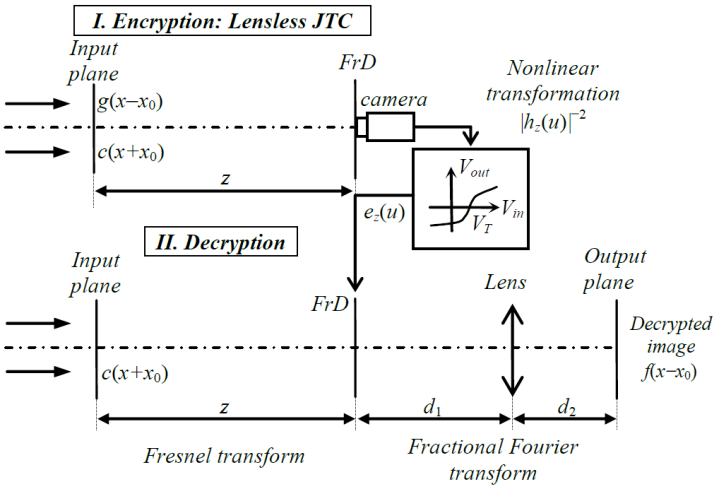


Figure 1. Schematic representation of the optical setup. The encryption scheme (Part I) is based on a nonlinear JTC in the FrD and the decryption scheme (Part II) is composed by an optical FrT and an optical fractional Fourier transform.

where x_0 is a real constant. The second data distribution of the input plane of the JTC is the RPM $h(x)$ modulated by another pure linear phase term

$$c(x) = \exp\left\{\frac{i2\pi x_0(x-x_0)}{\lambda z}\right\}h(x). \tag{8}$$

The FrT at the wavelength λ and the propagation distance z of $r(x)f(x)$ and $h(x)$ are

$$t_z(u) = \mathrm{FrT}_{\lambda,z}\{r(x)f(x)\}, \qquad h_z(u) = \mathrm{FrT}_{\lambda,z}\{h(x)\} = \left|h_z(u)\right|\exp\{i2\pi\phi_z(u)\}. \tag{9}$$

The joint Fresnel power distribution (JFPD) introduced in ref. [14] at parameters λ and z, is

$$\mathrm{JFPD}_z(u) = \left|\mathrm{FrT}_{\lambda,z}\left\{g(x-x_0)+c(x+x_0)\right\}\right|^2. \tag{10}$$

To generate the encrypted image [14], the JFPD is divide by the nonlinear term $|h_z(u)|^2$, thus obtaining the expression

$$\begin{aligned} e_z(u) = \frac{\mathrm{JFPD}_z(u)}{\left|h_z(u)\right|^2} = \frac{\left|t_z(u)\right|^2}{\left|h_z(u)\right|^2} + 1 + t_z^*(u)\frac{h_z(u)}{\left|h_z(u)\right|^2}\exp\left\{\frac{i\pi}{\lambda z}(4x_0)u\right\} \\ + t_z(u)\frac{h_z^*(u)}{\left|h_z(u)\right|^2}\exp\left\{\frac{-i\pi}{\lambda z}(4x_0)u\right\}, \end{aligned} \tag{11}$$

where Eq. (5) has been used to obtain the complete expression of the encrypted image. If $|h_z(u)|^2$ is equal to zero for a particular value of the coordinate u, this intensity value is substituted by a small constant to avoid singularities when computing $e_z(u)$. The encrypted image $e_z(u)$ is a real-valued distribution that can be computed from the $\mathrm{JFPD}_z(u)$ and $|h_z(u)|^2$. The security keys needed for decryption are the RPM $h(x)$, the wavelength λ and the distance of propagation z. Figure 1 (part I) shows the optical encrypting scheme based on a nonlinear JTC architecture in the FrD.

In the decryption system (Figure 1, part II), the data distribution $c(x)$ is placed at coordinate $x = -x_0$ and is Fresnel transformed at parameters λ and z; the result of this transformation is then multiplied by the encrypted image $e_z(u)$ to obtain

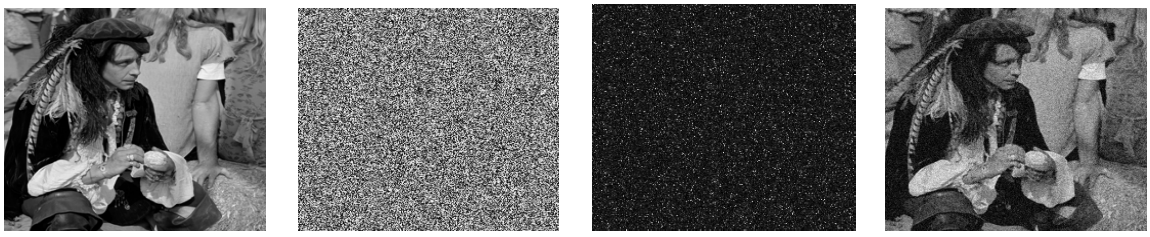
$$\begin{aligned} d_z(u) &= e_z(u)\mathrm{FrT}_{\lambda,z}\left\{c(x+x_0)\right\} \\ &= \exp\left\{\frac{i\pi}{\lambda z}\left(2x_0u - x_0^2\right)\right\}\frac{h_z(u)}{\left|h_z(u)\right|^2}\left|t_z(u)\right|^2 + \exp\left\{\frac{i\pi}{\lambda z}\left(2x_0u - x_0^2\right)\right\}h_z(u) \\ &\quad + \exp\left\{\frac{i\pi}{\lambda z}\left(6x_0u - x_0^2\right)\right\}t_z^*(u)\frac{h_z^2(u)}{\left|h_z(u)\right|^2} + \exp\left\{\frac{-i\pi}{\lambda z}\left(2x_0u + x_0^2\right)\right\}t_z(u)\frac{h_z^*(u)h_z(u)}{\left|h_z(u)\right|^2}. \end{aligned} \tag{12}$$

By Fresnel transforming at parameter λ and $-z$ the fourth term of Eq. (12) and taking the absolute value, we obtain a version of the decrypted image $\tilde{f}(x)$ at coordinate $x = x_0$ given by

$$\tilde{f}(x - x_0) = \left|\mathrm{FrT}_{\lambda,-z}\left\{\exp\left[\frac{-i\pi}{\lambda z}\left(2x_0u + x_0^2\right)\right]t_z(u)\right\}\right|. \tag{13}$$

We remark that the nonlinear operation introduced in Eq. (11) permits the retrieval of the original image in the decryption system. The decryption scheme (Part II) is shown in Fig. 1 and it is based on an optical FrT and an optical fractional Fourier transform. Since the FrT at parameter $-z$ cannot be obtained optically, and the complex conjugation of the encrypted image $e_z(u)$ is not useful (due to the fact that this distribution is a real-valued function), we use the relationship between the FrT and the fractional Fourier transform [10]. The fractional Fourier transform of fractional order α can be related to a FrT of parameters λ and z. Thus, we apply an optical fractional Fourier transform at fractional order $\pi - \alpha$ to the term of interest in Eq. (12). Then, we take the absolute value to retrieve an inverted version of the primary image $\tilde{f}(-x)$ at coordinate $x = -x_0$.

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 $f(x)$ and the random distribution code $n(x)$ of the RPM $h(x)$ are depicted in Figs. 2(a) and 2(b), respectively. The random distribution code $s(x)$ of RPM $r(x)$ has different values but similar appearance to the image presented in Fig. 2(b). The images $f(x)$, $s(x)$ and $n(x)$ are 512×512 pixel size ($M \times N = 512 \times 512$). The encrypted image $e_z(u)$ for the keys $\lambda = 543$ nm and $z = 50$ mm is depicted in Fig. 2(c). The decrypted image $\tilde{f}(x)$ presented in Fig. 2(d) is obtained centered at position $x = x_0$ of the output plane of the decryption system, when the correct values keys ($h(x)$,



(a) (b) (c) (d)

Figure 2. (a) Original image to encrypt $f(x)$. (b) Random distribution code $n(x)$ of the RPM $h(x)$. (c) Encrypted image $e_z(u)$ for the keys $\lambda = 543$ nm and $z = 50$ mm. (d) The image correctly decrypted with the correct keys: the RPM $h(x)$, λ and z.

λ and z) are used. To evaluate the quality of the decrypted image, we use the root mean square error (RMSE) defined by [14]

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

where $f(x)$ and $\tilde{f}(x)$ denote the original image and the decrypted image, respectively. The RMSE between the original image of Fig. 2(a) and the correctly decrypted image of Fig. 2(d) is 0.102. A high image quality for the decrypted image (Fig. 2(d)) is retrieved, because the nonlinear operation given by the term $|h_z(u)|^2$ was introduced in the denominator of the encrypted function, see Eq. (11) [13, 14].

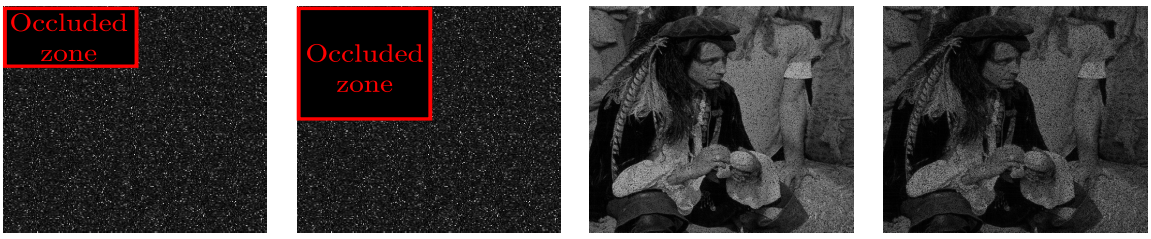
4. Occlusion and noise tests on the encrypted image

In this section, the encrypted image of the encryption system described in the previous section is modified by occlusion or noise and we evaluate the performance of the decryption system when the retrieved image of this system is compared to the original image that it was encrypted.

If the encrypted image of Fig. 2(c) is occluded by 12.5% (Fig. 3(a)) and 25% (Fig. 3(b)) of its area (the values of occluded pixels are replaced with zero values), we obtain the decrypted images depicted in Figs. 3(c) and 3(d), respectively, when the correct keys values ($h(x)$, λ and z) are used. The quality of the decrypted image is computed using the RMSE metric. The RMSEs between the original image (Fig. 2(a)) and the decrypted images (Figs. 3(c) and 3(d)) are 0.1747 and 0.2434, respectively. The more the encrypted image is occluded in its area, the more the retrieved image at the output of the decryption system is degraded, as it was expected.

Figure 4 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 4(a) presents the decrypted image when additive noise is considered and Fig. 4(b) corresponds to multiplicative noise. In both cases, decryption has been performed with the correct key values ($h(x)$, λ and z). The RMSEs between the original image (Fig. 2(a)) and the decrypted images (Figs. 4(a) and 4(b)) are 0.316 and 0.3137, respectively. For this noise test, the obtained decrypted images have the same quality of image.

Despite the loss of quality that affects the decrypted images shown in Figs. 3(c), 3(d), 4(a) and 4(b), 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.



(a) (b) (c) (d)

Figure 3. 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. 3(a) and (d) Fig. 3(b).

(a) (b)

Figure 4. Decrypted images when the encrypted image of Fig. 2(c) is degraded by a Gaussian white noise with zero mean and variance of $\sigma^2 = 0.2$: (a) additive noise and (b) multiplicative noise.

5. Conclusions

We have presented the results of occlusion and noise tests for a nonlinear JTC-based encryption-decryption system in the Fresnel domain, when the encrypted image is modified by the perturbations of noise or occlusion and we evaluate the quality of the resulting decrypted image using the RMSE metric. As it was expected, the quality of the decrypted image decreases when the occluded part of the encrypted image is increased. The quality of the resulting decrypted images is still acceptable when the encrypted image is occluded up to a quarter of its area. Finally, the decryption system shows the same response when the encrypted image is degraded by additive or multiplicative noise.

Acknowledgments

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

References

[1] Réfrégier P and Javidi B 1995 *Opt. Lett.* **20** 767–9
[2] Millán M S and Pérez-Cabré E. 2011 *Optical and Digital Image Processing: Fundamentals and Applications* ed Cristóbal G, Schelkens P and Thienpont H (Wiley-VCH Verlag GmbH & Co.) chapter 33 pp. 739–67.
[3] Matoba O and Javidi B 1999 *Opt. Lett.* **24** 762–4
[4] Situ G and Zhang J 2004 *Opt. Lett.* **29** 1584–6
[5] Chen W, Javidi B and Chen X 2014 *Adv. Opt. Photonics* **6** 120-55
[6] Javidi B, Carnicer A, Yamaguchi M, Nomura T, Pérez-Cabré E, Millán M, Nishchal N, and Torroba R, Barrera J, He W and others 2016 *J. Opt.* **18** 083001
[7] Unnikrishnan G, Joseph J and Singh K 2000 *Opt. Lett.* **25** 887–9
[8] Hennelly B and Sheridan J T 2003 *Opt. Lett.* **28** 269–71
[9] Hennelly B and Sheridan J T 2003 *Optik* **114** 251–265
[10] Ozaktas H M, Zalevsky Z and Kutay M A 2001 *The Fractional Fourier Transform: with Applications in Optics and Signal Processing* (Weinheim: Wiley)
[11] Goodman J W 1996 *Introduction to Fourier Optics* (Columbus: McGraw-Hill)
[12] Nomura T and Javidi B 2000 *Opt. Eng.* **39** 2031–5
[13] Vilardy J, Millán M S and Pérez-Cabré E 2013 *J. Opt.* **15** 025401
[14] Vilardy J, Millán M S and Pérez-Cabré E 2014 *Appl. Opt.* **53**, 1674–82
[15] Vilardy J, Millán M S and Pérez-Cabré E 2013 *Proc. of SPIE* **8785**, 87853J
[16] Barrera J, Jaramillo A, Vélez A and Torroba R 2016 *Opt. Laser Eng.* **83** 126–30.
[17] Vilardy J, Torres Y, Millán M S and Pérez-Cabré E 2014 *J. Opt.* **16** 125405
[18] Vilardy J, Millán M S and Pérez-Cabré E 2014 *Opt. Pura y Apl.* **47** 35–41
[19] Lu D and Jin W 2011 *Opt. Eng.* **50** 068201
[20] Vilardy J, Millán M S and Pérez-Cabré E 2017 *Opt. Laser Eng.* **89** 88-94