DOI: 10.1109/WIO.2016.7745591

Image quality and security through nonlinear joint transform encryption

Juan M. Vilardy
Grupo de investigación GIFES
Universidad de la Guajira
Riohacha (La Guajira), Colombia
jmvilardy@uniguajira.edu.co

Elisabet Pérez-Cabré, María S. Millán
GOAPI, Dept. Òptica i Optometria
Universitat Politècnica de Catalunya (UPC)
Terrassa, Spain
elisabet.perez@upc.edu, millan@oo.upc.edu

Abstract— **Joint-transform correlator (JTC) architecture presents some advantages, such as no requirement of interferometric recording of the phase distribution or complex conjugation of the key phase mask, in order to optically implement the well-known double random phase encryption (DRPE) method. In addition, a practical optical realization was proposed in a way that the whole information (primary image and two random phase masks) was easily introduced in the same input plane of the JTC system. However, poor image quality was obtained in the decryption stage. Cryptanalysis of JTC-based encryption systems demonstrated that they were vulnerable to certain intruder attacks, similarly to the original DRPE method. In this work, we review recent modifications of encryption algorithms based on JTC architecture that permit, on the one hand, to significantly increase the quality of the retrieved image after information decryption, and on the other hand, to achieve a high security level against a variety of system attacks. The modifications, which were firstly introduced in the Fourier-based JTC system, have been also adapted to be used in the Fresnel and Fractional Fourier domains as well as in the Gyrator domain. Nonlinear operations have been also introduced in multifactor encryption-authentication.**

Keywords— ***encryption; nonlinear joint transform correlator; image quality; security; Fresnel domain; Fractional Fourier domain; Gyrator domain; multifactor encryption-authentication***

I. INTRODUCTION

Optical encryption technology is useful for security applications, as is proved by the intense research in the field in the last two decades [1–8]. Significant progress in optoelectronic devices has made optical technologies attractive for security. The security strength of optical cryptography stems from the ability of optics to process the information in a hyperspace of states, where variables such as amplitude, phase, polarization, wavelength, spatial position, and fractional spatial frequency domain can all be used to serve as keys for data encryption or to hide the signal. Moreover, optical processing has the valuable property of inherent parallelism, which allows for fast encryption and decryption of large volumes of complex data, that is, amplitude and phase. High-resolution optical materials can store encoded data in small volumes.

A pioneering optical encryption system, named double random phase encoding (DRPE), was proposed by Réfrégier and Javidi [9]. The optical hardware initially proposed to perform DRPE was the classical 4f-processor.

A preferred implementation of the optical DRPE is the joint transform correlator (JTC) architecture [10], because this JTC permits to alleviate the strict setup alignment requirement of the holographic system used to experimentally carry out the DRPE [9]. 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 [10].

II. NONLINEAR JTC-BASED ENCRYPTION SYSTEM

The initial optical implementation of the DRPE using the JTC architecture [10] has been modified in later contributions [11-13], in order to simplify the experimental setup. In a modified JTC-encryption system, the two RPMs, $r(x)$ and $h(x)$ (we use one-dimensional notation for simplicity), were implemented using a simple diffuser glass (random phase element) at the input plane of the JTC [11-13] (Fig. 1a). The RPM-I $r(x)$ is placed on the real image $f(x)$, and then this pair and the RPM-II $h(x)$ are placed side-by-side in the input plane of the JTC. The encrypted distribution or joint power spectrum (JPS) $e(u)$ is given by

$$\begin{aligned} e(u) &= JPS(u) = \\ &= \left|FT\left[r(x)f(x)*\delta(x-a)+h(x)*\delta(x+a)\right]\right|^2 , \end{aligned} \tag{1}$$

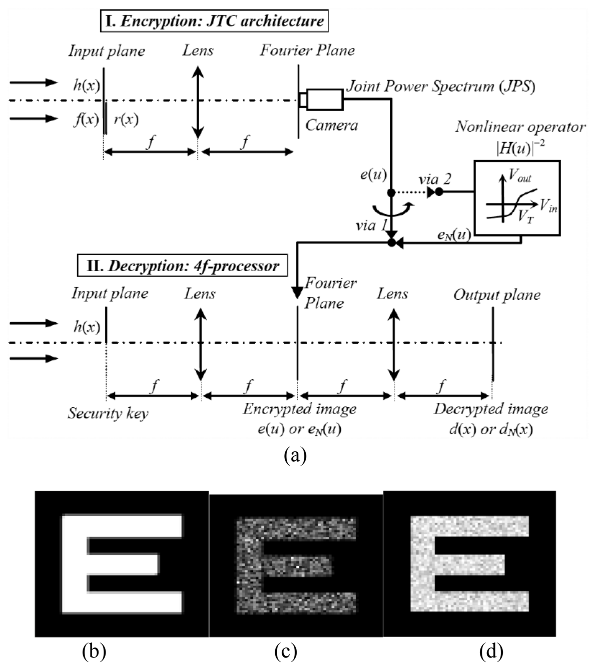
where FT indicates Fourier transform and the symbol * the convolution operation. As a result of such modification in the input plane, however, the decrypted images were affected by poor quality. This drawback was overcome in [13] by introducing a nonlinear operation in the encrypted function. This nonlinearity consists of dividing the JPS by the squared magnitude of the Fourier transform of the RPM-II

$$e_N(u) = \frac{JPS(u)}{\left|FT\left\{h(x)\right\}\right|^2} . \tag{2}$$

The nonlinear JTC encryption system simultaneously increases the decrypted image quality and improves its overall security (Fig. 1(c)-(d)). With this nonlinearity the encryption JTC system approaches better the implementation of DRPE as

This research was partly funded by the Spanish Ministerio de Economía y competitividad and Fondos FEDER (Project DPI2013-43220-R).

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



(a)

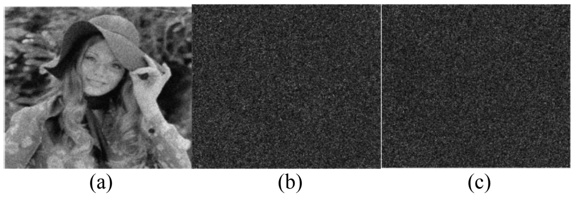
(b) (c) (d)

Fig. 1. (a) Optical setup. (b) Original image $f(x)$. Decrypted images for (c) linear JTC (via 1 in (a)); and (d) nonlinear JTC (via 2 in (a)).

it was originally proposed in [9]. Moreover, the introduction of this nonlinearity does not require to complicate the optical setup, therefore a conventional JTC suffices to implement the whole process. This nonlinearity also makes the system more resistant to chosen plaintext attacks (CPAs). We additionally explored the system resistance against this type of attack when a variety of probability density functions are used to generate the two RPMs of the encryption–decryption process [13]. The encryption system is asymmetric with respect to the random distributions used for the two RPMs, and the secret of the encrypted image is better protected when a non-uniform random distribution is used in the generation of RPM-II.

III. Extended Nonlinear Joint Transform Processor

The DRPE implemented with a JTC architecture has been extended from the Fourier domain to the Fresnel domain [14], the fractional Fourier domain [15-16] and the Gyrator domain [17-19]. In the nonlinear approaches [14,16,19], the nonlinear operations introduced in the JTC have become essential to correctly decrypt the input signal with satisfactory quality. Moreover, the extension to other domains has increased the security of the overall encryption-decryption system by introducing new parameters that must be adjusted prior to obtaining the hidden information.



(a) (b) (c)

Fig. 2. Decrypted images with the nonlinear Fresnel processor: (a) when the correct keys λ, z and the RPM $h(x)$ are used; (b) when the nonlinearity $\left|h_z(u)\right|^2$ is not introduced in the encrypted function and all the correct keys are used for decryption; and (d) using just an incorrect distance of propagation z=73mm, but the rest of keys are correct.

A. Fresnel domain

The nonlinear JTC-based encryption system in the Fresnel domain (FrD) can be applied by means of a lensless optical system [14], which minimizes the optical hardware requirements and is easier to implement. To do this, the input distributions described above are now modulated by two pure phase linear terms:

$$\begin{aligned} g(x) &= \exp\left\{\frac{i2\pi v_0\left(x - v_0\right)}{\lambda z}\right\} r(x) f(x) \\ c(x) &= \exp\left\{\frac{-i2\pi v_0\left(x + v_0\right)}{\lambda z}\right\} h(x) \end{aligned} \quad . \qquad (3)$$

The linear phase terms are symmetrically introduced to ensure the complete overlapping of both Fresnel spectra at a distance of propagation z where the joint Fresnel power distribution (JFPD$_z(u)$) is recorded. The encrypted function is now defined as the JFPD$_z(u)$ divided by the nonlinear term $\left|h_z(u)\right|^2$ which is the Fresnel transform at the wavelength λ and the distance z. Both parameters have to be properly set for a satisfactory decryption (see Fig. 2a). Results shown in Figs. 2(b,c) prove that the introduced nonlinearity is essential to decrypt and retrieve the original image. When the nonlinearity is properly introduced, the other parameters (wavelength λ and propagation distance z) need to be correctly adjusted to avoid just noisy failed outputs (Figs. 2(b,c)). The cryptanalysis of the proposed system has proved that vulnerability to different attacks (CPA and known-plaintext attacks or KPA) of the JTC-based encryption system in the Fourier domain has been overcome by the proposed nonlinear scheme.

B. Fractional Fourier domain

A generalized formulation of the nonlinear JTC-based encryption systems using the fractional Fourier transform and its combination with a nonzero-order JTC were introduced with the purpose of improving the quality of the decrypted images and increasing the security of the processor [16]. The fractional order of the fractional Fourier transform, α, provides and additional parameter to further control the encryption and decryption stages. Robustness of the proposed encryption system to certain amount of degradation in the encrypted function has been tested with the presence of noise or partial occlusion of the encrypted distribution.

C. Gyrator domain

A fully-phase nonzero-order JTC architecture in the Gyrator domain has been designed with an improved resistance to brute force attacks, CPA, KPA and cyphertext-only attacks [19]. In this case the combination of two nonlinearities along with the rotation angle of the Gyrator transform improve the security of the encryption scheme.

IV. Photon-Counting Multifactor Optical Encryption-Authentication (MOEA)

Simultaneous encryption-authentication of multiple factors is a highly secure optical encryption method for demanding security systems (Fig. 3) [20]. Recent research in this field has demonstrated the potential of MOEA combined with nonlinear operations such as photon-counting imaging techniques for the secure surveillance of different items, with simultaneous verification of multiple factors, thus allowing a significant data compression with proved resistance against unauthorized attacks [21,1].

V. Conclusions

Nonlinear modifications have been introduced in JTC-based encryption systems. As a result, the security of the encrypted image has improved and the system becomes more resistant to attacks without deleterious effects on the quality of the decrypted image. The extension to the Fresnel, fractional Fourier and Gyrator domains adds new parameters that require to be accurately set for satisfactory information decryption. The retrieval of the original image with extremely low level of noise in the decryption stage is possible thanks to the proposed nonlinear modification introduced in the joint power distribution. The recovered image shows higher quality than in other related systems that keep their joint power distribution unchanged. The nonlinear modifications do not increase the amount of data to transmit. In the case of photon-counting multifactor optical encryption-authentication, it even permits to significantly compress the information to transmit. All the described encryption-decryption systems are suitable for optoelectronic and/or digital implementation. Cryptanalysis shows the high resistance of the proposed encryption schemes against several types of attacks.

References

[1] B. Javidi, et al. “Roadmap on optical security,” J. Opt., 2016 (in press).

[2] W. Chen, B. Javidi, and X. Chen, “Advances in optical security systems,” Adv. Opt. Photonics, vol. 6, pp. 120–155, 2014.

[3] S. Liu, C. Guo, and J. T. Sheridan, “A review of optical image encryption techniques,” Opt. Laser Technol., vol. 57, pp. 327–342, Apr. 2014.

[4] 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. 2011, pp. 739–767.

[5] O. Matoba, T. Nomura, E. Pérez-Cabré, M. S. Millán, and B. Javidi, “Optical Techniques for Information Security,” Proc. IEEE, vol. 97, no. 6, pp. 1128–1148, Jun. 2009.

[6] A. Alfalou and C. Brosseau, “Optical image compression and encryption methods,” Adv. Opt. Photonics, vol. 1, no. 3, p. 589, Oct. 2009.

[7] B. Javidi, “Securing Information with Optical Technologies,” Phys. Today, vol. 50, no. 3, p. 27, 1997.

[8] B. Javidi and J. L. Horner, “Optical pattern recognition for validation and security verification,” in Opt. Eng., vol. 2237, pp. 1752–1756, 1994.

[9] P. Réfrégier and B. Javidi, “Optical image encryption based on input plane and Fourier plane random encoding,” Opt. Lett., vol. 20, no. 7, pp. 767–9, Apr. 1995.

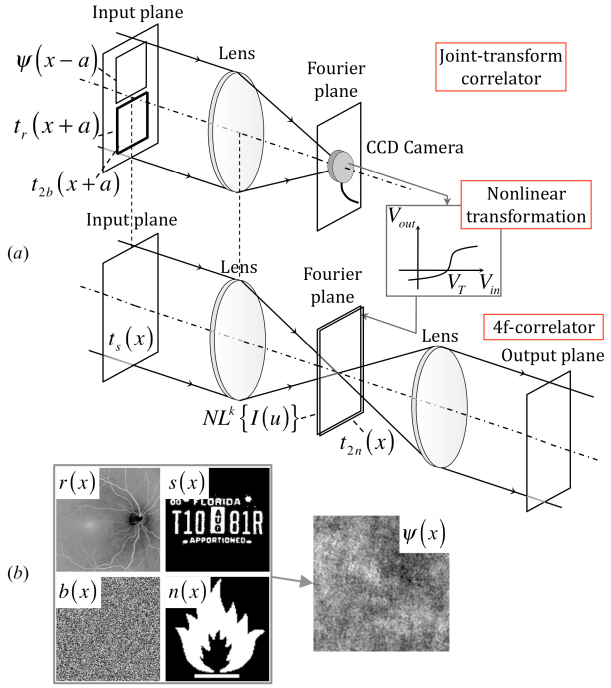


Fig. 3. (a) MOEA setup; (b) Four factors of different nature and MOEA complex-valued encrypted function.

[10] T. Nomura and B. Javidi, “Optical encryption using a joint transform correlator architecture,” Opt. Eng., vol. 39, no. 8, pp. 2031–2035, 2000.

[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., vol. 282, no. 16, pp. 3243–3249, Aug. 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, vol. 20, no. 4, pp. 3388–93, Feb. 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., vol. 15, no. 2, p. 025401, Feb. 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., vol. 53, no. 8, pp. 1674–82, Mar. 2014.

[15] D. Lu and W. Jin, “Color image encryption based on joint fractional Fourier transform correlator,” Opt. Eng., vol. 50, no. 6, p. 068201, 2011.

[16] 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., vol. 16, no. 12, p. 125405, Dec. 2014.

[17] H. Li, “Image encryption based on gyrator transform and two-step phase-shifting interferometry,” Opt. Lasers Eng., vol. 47, pp. 45–50, 2009.

[18] M. R. Abuturab, “Noise-free recovery of color information using a joint-extended gyrator transform correlator,” Opt. Lasers Eng., vol. 51, no. 3, pp. 230–239, 2013.

[19] 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. Lasers Eng. (2016). http://dx.doi.org/10.1016/j.optlaseng.2016.02.013i.

[20] M. S. Millán, E.Pérez-Cabré, B. Javidi, “Multifactor authentication reinforces optical security,” Opt. Lett., vol. 31, no. 6, pp.721-723, 2006.

[21] E. Pérez-Cabré, E. Mohammed, M. S. Millán, and H. L. Saadon, “Photon-counting multifactor optical encryption and authentication,” J. Opt., vol. 17, no. 2, p. 025706, 2015.