BISTUA
Revista de la Facultad de Ciencias Básicas
ISSN: 0120-4211

Cryptogram steganography method using a JFT optical architecture

Método de estenografía de criptogramas usando una arquitectura óptica de transformada de Fourier conjunta

María-Alejandra Guerrero V; Jorge-Enrique Rueda-P
Grupo Óptica Moderna; Departamento de Física y Geología,
Universidad de Pamplona, Colombia
Contacto: guerrerovanegasmarialejandra@gmail.com

Recibido: Febrero 10, 2020. Aceptado: Junio 8, 2020

https://doi.org/10.24054/bistua.v18i1.210

Resumen

En los métodos ópticos para encriptación de imágenes, los criptogramas guardan el mismo patrón de las máscaras de encriptación y esto facilita su detección. Nosotros presentamos un método de encriptación que simultáneamente produce un criptograma estenograma. En las múltiples pruebas de validación de la técnica, incluso para la misma imagen secreta, nosotros obtuvimos estenogramas totalmente diferentes.

Palabras clave: Encriptación óptica; Esteganografía, Transformada de Fourier.

Abstract

In known optical methods for secret image encryption, cryptograms retain the same pattern of encryption masks and this facilitates its detection. We present an encryption method that simultaneously produces a cryptogram steganogram. In the multiple validation tests of the technique, even for the same input secret image, we obtained completely different steganograms.

***Keywords*:** Optical encryption; Steganography; Fourier Transform

1 Introduction

The need to maintain private communications and to transmit information safely and reliably remains a problem with an incomplete solution. Currently we can find that an important number of results of image encryption techniques in the domain of physical optics have been reported to solve the security problem of private information. Different methods of secret image encryption using optical techniques have been reported [1-9], where the method of double random phase has been the most used, however, most of them methods have in common that they only generate the cryptogram.

We asked ourselves if it would be possible to produce cryptogram patterns, different from each other, in their spatial structure, with the purpose that this situation becomes a subjective security parameter, in terms of preventing cryptogram detection. We find the answer in the combination of optical encryption and steganography.

Optical steganography and combination of steganography and optical encryption has been implemented in many works [10-15]. An important number of that works are focused on to do digital steganography and optical encryption of steganogram. We propose a fully optics technique to do steganography of cipher images.

In this work, a methodology was developed that in a single process, the secret image was encrypted and simultaneously a steganogram of the cryptogram was generated. The methodology developed consists of a Joint Fourier Transform (JFT) optical architecture, where we use an only-phase key, two amplitude masks that works how encryption keys and cover image of steganogram, and a non-linear filtering. Under this situation, an intruder, even knowing the architecture of the cryptosystem, requires detecting the steganogram and determining the masks used in the encryption.

2 Encryption-decryption method

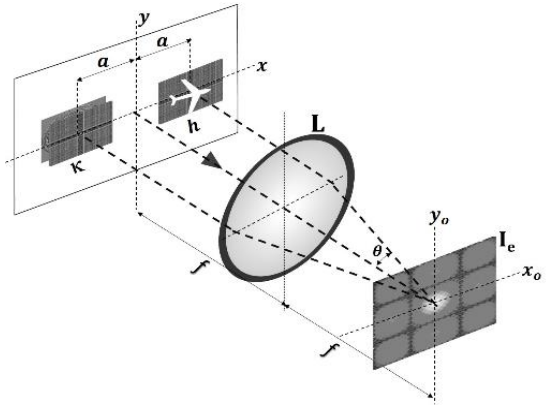
Figure 1 (a) is a JFT optical architecture, which simultaneously produces the cryptogram and steganogram of the secret image. The JFT is illuminated with a monochromatic plane wave, of wavelength λ. The input plane (x,y) contains the secret image $f(x\text{-}a,y)$ and the masks $\kappa(x+a,y)$ and $\kappa_m(x-a,y)$. Then the transmittance of the plane (x, y) is of the next form:

$$t(x,y) = h(x-a,y) + \kappa(x+a,y), \qquad (1)$$

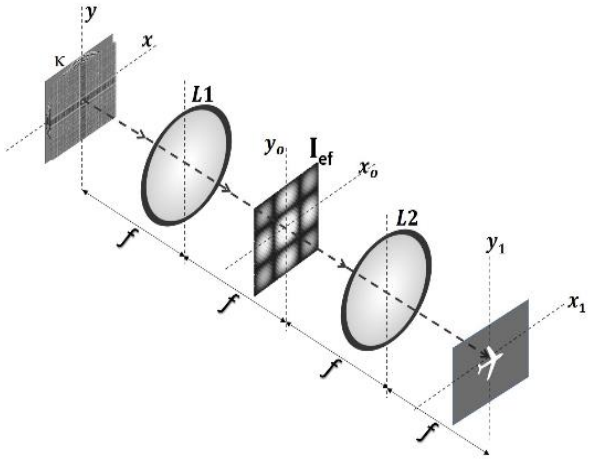
© The authors; licensee Universidad de Pamplona.

Where $h(x-a,y) = f(x-a,y)\kappa_m(x-a,y)$, and

$$\kappa(x+a,y) = \kappa_n(x+a,y)\kappa_{ch}(x+a,y). \quad (2)$$



(a) JFT optical architecture.



(b) 4 *f* optical architecture.

Figure 1. L, L1 and L2 are positive focal length lenses *f*. Source: authors

Assuming paraxial approximation, then $a = f\sin(\theta)$. Thus, κ_n (x + a, y) and $\kappa_m(x-a,y)$ are periodic spatial distribution amplitude masks, and $\kappa_{ch}(x+a,y)$ is a phase mask in circular harmonics with pseudo-random phase distribution proposed by the ref [9]. The combination of the mask κ_{ch} and the masks κ_m and κ_n encrypts the secret image and generate the steganogram of the cryptogram.

$$U_e(f_x,f_y) = \frac{1}{\lambda f}H(f_x,f_y)\exp(-i2\pi f\sin(\theta)f_x) + \\ +\frac{1}{\lambda f}K(f_x,f_y)\exp(i2\pi f\sin(\theta)f_x), \quad (3)$$

With, $f_x = \frac{x_0}{\lambda f}$, $f_y = \frac{y_0}{\lambda f}$,

$$K(f_x,f_y) = K_n(f_x,f_y) \circledast K_{ch}(f_x,f_y), \quad (4)$$

$$H(f_x,f_y) = f(f_x,f_y) \circledast K_m(f_x,f_y) \quad (5)$$

The symbol $\circledast$ denotes convolution operator. Then the Joint Spectral Density $I_e = |U_1(f_x,f_y)|^2$ is the steganogram of the cryptogram of the secret image, that is:

$$I_e(f_x,f_y) = \frac{1}{(\lambda f)^2}\Big[|H(f_x,f_y)|^2 + |K(f_x,f_y)|^2 + \\ +H^*(f_x,f_y)K(f_x,f_y)\exp(i4\pi f\sin(\theta)f_x) + \\ +H(f_x,f_y)K^*(f_x,f_y)\exp(-i4\pi f\sin(\theta)f_x)\Big]. \quad (6)$$

The first two terms of the equation (6) are not necessary to decrypt the image, otherwise they decrease the signal / noise ratio of the decrypted image. On the other hand, only the third or fourth term is enough to decrypt the image. The above is solved by a bandpass filtering. Therefore, first we proceed by means of a Fourier transform of equation (6), and we obtain,

$$U_2(x',y') \approx [\, h\odot h + \kappa\odot k + \\ +h\odot\kappa \circledast \delta(x'+2a,y') + \\ +h\odot k \circledast \delta(x'-2a,y')]. \quad (7)$$

The symbol $\odot$ denotes correlation operator. To the result equation (7), we must multiply it by a bandpass filter, of width equal to the width of one of the higher orders of equation (7), centred in the desired order. Of the geometrical dimensions of each term in equation (7), and assuming that W_x is the width, in the *x* direction, of the input plane (*x*, *y*), and that the dimensions (L_x,L_y) of the secret image and of the masks are equal, then we can establish the following criteria, for an optimal pass-band filtering:

$$\frac{(W_x-2L_x)}{4} \geq a \quad ; \quad f_p > \frac{L_x}{\lambda f}, \quad (8)$$

where f_p is the carrier frequency of the encryption plane. Then, if we consider removing the first, second and third terms from the steganogram (equation (6)), then the appropriate bandpass filter should be of the form,

$$\mathrm{Rect}(x'-2a,y') = \begin{cases} 1 & si \quad 2a-L_x \leq x' \leq 2a+L_x \\ & \quad -L_y \leq y' \leq L_y \\ 0 & Fuera \end{cases} \quad (9)$$

Once this filter (9) is applied, we apply to this result a translation to the origin of the coordinates, and in this position a Fourier inverse transform. On the other hand, even the filtered steganogram contains noise that decreases the quality of the decrypted secret image. The problem is solved by means of the inverse filter [16] $\frac{1}{|K(f_x,f_y)|^2}$, that multiplying it by the previous result the final steganogram is obtained:

$$I_{ef}(f_x,f_y) \approx \frac{F(f_x,f_y)\circledast K_m(f_x,f_y)}{K(f_x,f_y)}. \quad (10)$$

Now this steganogram allows obtaining a decrypted secret image with a high signal/noise ratio. For the results presented in this paper, we consider $\kappa_m = \kappa_n$.

The decryption procedure requires the use of a 4*f* optical architecture (Fig 1 (b)). In the input plane of the 4*f*, the encryption mask κ (x, y) is located, and in the spectral plane (x_o,y_o) the steganogram I_{ef} is located, in this way, in the spectral plane, the product is obtained between the Fourier transform of κ (x, y) and the steganogram I_{ef}. Then in the focal plane of the lens *L2* the convolution between $\kappa(x_1, y_1)$ and the transform of I_{ef} is obtained. Finally, this result must be multiplied by the inverse of the mask κ_m, and thus the image decrypted in the plane (x_1,y_1) is obtained.

3 Results and discussion

The method was implemented in MatLab programming language. We developed the Graphical User Interface (GUI) shown in Fig. 2. The input plane (x,y) was designed of size 1024×768 pixels, and in this matrix were embedded the matrix of the encryption masks $\kappa\,(x+a,y)$ and the secret image -$f(x-a,y)$ –, each matrix of size 170×170 pixels.

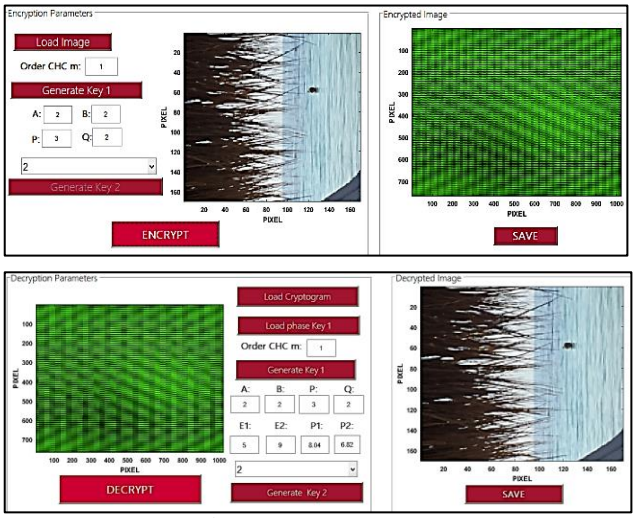


Figure 2. GUI of the method implemented. Source: Authors

Table 1: Parameters of the computational simulations

Wavelength	$\lambda = 532\ nm$
Focal length of the lens	$f = 30\ cm$
Pixel size	$19\ \mu m$
Input plane width	W_x=19.456 mm (1024 pixels)
Width of the scenes	L_x=3.23 mm (170 pixels)
Separation between $f(x-a,y)$ and $\kappa(x+a,y)$	a =3.249 mm (171 pixels)
Carrier frequency	f_p =20.357 ln/mm

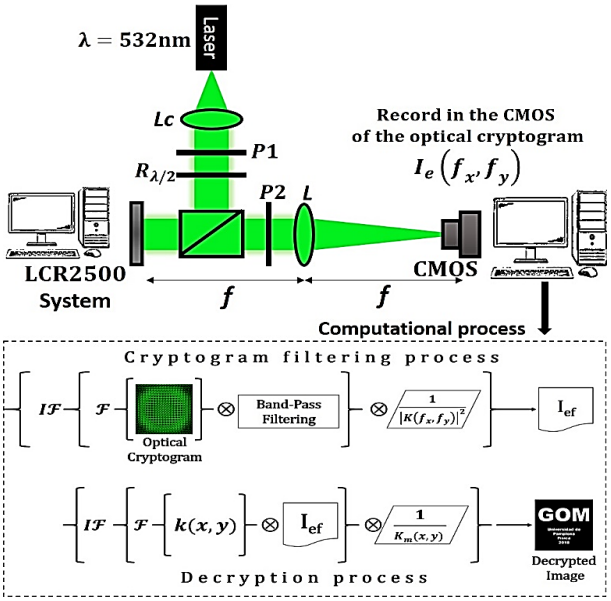
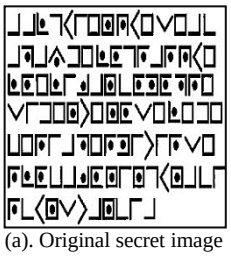
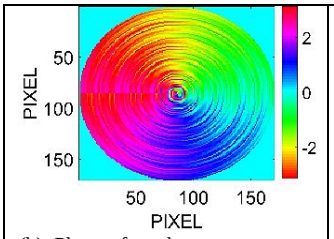


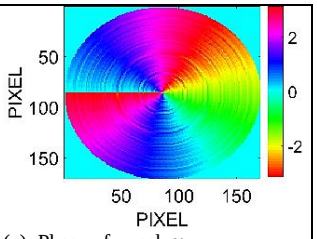
Figure 3: Optical-Digital encryption-decryption system. P1 and P2 are linear polarizers, $R_{\lambda/2}$ half retarder used to tune the modulation type in the LCR250 (1024×768 pixels). ⊗ is the multiplication arithmetic operator, F{..} is the Fourier transform operator, and IF{..} is the inverse Fourier transform operator. Source: Authors



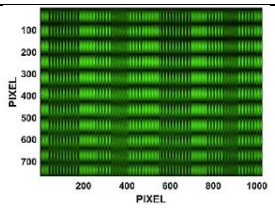
(a). Original secret image



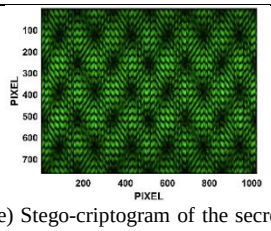
(b). Phase of mask κ_{ch1}; order **m = 1.1**



(c). Phase of mask κ_{ch2}; order **m =1.5**



(d) Stego-criptogram of the secret image (a), using (b) mask κ_{ch1} and mask κ_{m1}.



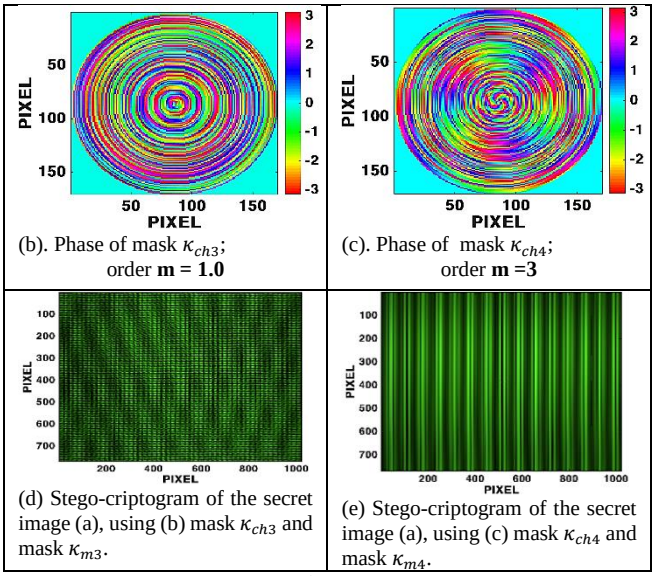
(e) Stego-criptogram of the secret image (a), using (c) mask κ_{ch2} and mask κ_{m2}.

Figure 4. Results encryption of image (a). In this results $\kappa_m = \kappa_n$
Parameters of the Mask κ_m for Stego-criptogram:
(d) κ_{m1}: function{| 4 | 3 | 3 | 4 | 9 | 9 | 0.71 | 2.81 | 1 |}.
Parameters of the Mask κ_m for Stego-criptogram:
(e) κ_{m2}: function{| | 1 | 2 | 2 | 2 | 4 | 3 | 0.57 | 0.97 | 1 | }. Source: Authors

Table 1 contains the relation of values of the parameters used in the algorithm of the Encryption-Decryption system shown in Fig. 3. The parameters in Table 1 were thought so to the possibility of an optical-digital implementation, in which a spatial liquid crystal modulator (type LCR2500) could be used as the input plane of the optical arrangement of the Fig. 1 (a), and the decryption step of Fig.1.(b) is realizing using the developed GUI.



(a). Original secret image



(b). Phase of mask κ_{ch3}; order **m = 1.0**

(c). Phase of mask κ_{ch4}; order **m =3**

(d) Stego-criptogram of the secret image (a), using (b) mask κ_{ch3} and mask κ_{m3}.

(e) Stego-criptogram of the secret image (a), using (c) mask κ_{ch4} and mask κ_{m4}.

Figure 5. Results encryption of image (a). In this results $\kappa_m = \kappa_n$, Parameters of the Mask κ_m for Stego-criptogram: (d) κ_{m3} : function {| 2 | 1 | 1 | 2 | 5 | 4 | 1 | 4.98 | 1 |} Parameters of the Mask κ_m for Stego-criptogram: (e) κ_{m4} : function { | 5 | 2 | 2 | 5 | 2 | 4 | 10 | 6.39 | 3 |}. Source: Authors

Figures 4 and 5 show two results of the technique implemented. We founded that the quality of the decrypted images is high. We determined an average PSNR of 172 dB for binary images and 180 dB for RGB images. We used κ_m=κ_n masks of periodic spatial structure, such that their structure changes by manipulation of the parameters function {| A | B | P | Q | E1 | E2 | P1 | P2 |#Key2}, where m, A, B, P, Q, E1, E2, P1, P2 are positive real numbers.

An additional parameter to take account is the image-compression algorithm used to storage the stego-criptogram. The system proposed by us requires algorithms whit none or low compression for recovered the images with high quality.

4. Conclusions

In sumary, in the multiple tests that we were realizing, it was always possible to obtain different steganograms for each secret image. For different steganograms, we perform tests to break the steganogram by means of multiple combinations of masks different from those of encryption. None of these tests was successful in the sense of relieving the information carried by the steganogram. In Fig. 4 and Fig. 5, it is evident that the four steganograms are different. We consider that the technique has a high degree of security, because, the architecture includes a non-linear filtering and additionally the intruder should intercept the phase key κ_{ch}, the steganogram and the parameters {|m| A | B | P | Q | E1 | E2 | P1 | P2 |#Key2|}. The results obtained maintain the principle of different steganogram in each encryption process, even for the same input image.

Referencias

[1] Refregier P., Javidi B., Optical image encryption based on input plane and fourier plane encoding, Optics Letters, vol. 20, nº 7, pp. 767-769, 1995.

[2] Nomura T., Javidi B., Optical encryption using a joint transform correlator architecture, Optical Engineering, vol. 39, nº 8, 2000.

[3] Xiong Y., Du J.Q.C., Optical encryption and authentication scherme based on phase-shifting interferometry in a joint transform correlator, Optics and Laser Technology, vol. 126, 2020.

[4] Liu X., Meng X., Wang Y., Huazheng W., Yang X., He W., Chen H., Optical multilevel authentication based on singular value decomposition ghost imaging and secret sharing cryptography., Optics and Lasers in Engineering, vol. 137, 2021.

[5] Chen H., Liu Z., Tanougast C., Liu F., Blondel W., Optical cryptosystem scheme for hyperspectral image based on random spiral transform in gyrator domains, Optics and Lasers in Engineering, vol. 137, 2021.

[6] Yi K., Leihong Z., Hualong Y., Mantong Z., Kanwai S., Dawei C., Camouflaged optical encryption based on comprenssive ghost imaging, Optics and Lasers in Engineering, vol. 134, 2020.

[7] Caia J., Shena X., Fanb C., Zhou B., Security-enhanced optical encryption based on JTC architecture, Optik-International Journal for Light and Electron Optics, vol. 206, 2020.

[8] Liu S., Guo C., Sheridan J.T., A review of optical image encryption techniques, Optics and Laser Technology, 2014.

[9] Rueda J.E., Encryption using circular harmonic key, Dyna, vol. 82, nº 190, pp. 70-73, 2015.

[10] Jiao S., Zhou Y., Li X., Review on optical image hiding and watermarking techniques, Optics ans Laser Technology, vol. 109, pp. 370-380, 2019.

[11] Miri A., Faez K., Adaptative image steganography based on transform domain via genetic algorithm, Optik, vol. 145, pp. 158-168, 2017.

[12] Wang C., Wang H., Ji Y., Multi-bit wavelength coding phase-shift-keying optical steganography based on amplifies spontaneus emission noise, Optics Communications, vol. 407, pp. 1-8, 2018.

[13] Liu H.C., Chen W., Optical ghost cryptography and steganography, Optics and Laser in Engineering , vol. 130, 2020.

[14] Zhang J., Lu W., Yin X., Liu W., Yeung Y., Binary image steganography based on joint distortion measurement, J. Vis. Commun. Image R, vol. 58, pp. 600-605, 2019.

[15] Rosen J., Steganography and encryption systems based on spatial correlators with meaningful output images, de Optical and Digital Techniques for information Security, pp. 59-94.

[16] Vilardy J., Millan M.S., Pérez-Cabré E., Experimental optical encryption scheme for the double random phase enconding using a nonlinear joint transform correlator, Optik, vol. 217, 2020.