Contents lists available at ScienceDirect

Optics Communications

journal homepage: www.elsevier.com/locate/optcom

Joint transform correlator optical encryption system: Extensions of the recorded encrypted signal and its inverse Fourier transform

Gustavo E. Galizzi [a], Christian Cuadrado-Laborde [a,b,*]

[a] Instituto de Física Rosario (CONICET-UNR), Blvr. 27 de Febrero 210bis, S2000EZP Rosario, Santa Fe, Argentina
[b] Pontificia Universidad Católica Argentina, Facultad de Química e Ingeniería, Av. Pellegrini 3314, 2000 Rosario, Santa Fe, Argentina

ARTICLE INFO

Article history:
Received 10 March 2015
Received in revised form
20 April 2015
Accepted 4 May 2015
Available online 6 May 2015

Keywords:
Optical encryption
Optical information processing
Joint transform correlator
Space bandwidth product

ABSTRACT

In this work we study the joint transform correlator setup, finding two analytical expressions for the extensions of the joint power spectrum and its inverse Fourier transform. We found that an optimum efficiency is reached, when the bandwidth of the key code is equal to the sum of the bandwidths of the image plus the random phase mask (RPM). The quality of the decryption is also affected by the ratio between the bandwidths of the RPM and the input image, being better as this ratio increases. In addition, the effect on the decrypted image when the detection area is lower than the encrypted signal extension was analyzed. We illustrate these results through several numerical examples.

1. Introduction

Spatial optical techniques have shown great potential in the field of information security to encode high-security images. The joint transform correlator (JTC) optical encryption setup emerged as an attractive option to previous techniques [1], such as the dual random phase encoding (DRPE) proposed in the 1990s [2]. The main advantage of JTC is that only the intensity of the encrypted signal is necessary for decryption, which relaxes the otherwise restrictive requirements for optical alignment in the system. Further, the decryption is performed using the same key code, which eliminates the need to produce an exact complex conjugate of the key as in the DRPE. Several multiplexed variants were proposed later, in order to increase the system capacity of the JTC [3–8].

The study of the space bandwidth product in different optical systems is of undeniable importance [9]. Hennelly et al. reported important progress in this subject in the context of DRPE [10–11]. In this work, we focus in the study of the extensions of the recorded encrypted signal in the Fourier, as well as direct, domains with the purpose to optimize its space bandwidth product. The theoretical work is supported through several numerical examples.

2. Theory

Fig. 1 shows the JTC optical encryption setup [1]. For the sake of clarity, we used one-dimensional notation. The original image $u(x)$ is bonded to the input random phase mask (RPM) $\alpha(x)$, and both are placed at coordinate $x=a$, whereas the key code $h(x)$ is positioned at coordinate $x=b$. The JTC is illuminated by a plane wave of wavelength λ. The input RPM $\alpha(x)$ has uniform amplitude transmittance and random phase information. The complex-valued key code $h(x)$ is the inverse Fourier transform ($\mathcal{F}^{-1}$) of $H(\nu)$, which in turn purely contains random phase information and unitary amplitude, statistically independent of $\alpha(x)$ [1], where ν is the spatial frequency variable associated to x – additionally a capital letter stands for the Fourier transform ($\mathcal{F}$) of the corresponding function in lower case letter. After transmission through a lens with focal length f, the encrypted signal is obtained at the output plane. In the JTC optical encryption setup the encrypted signal is optically recorded in intensity, for this reason this signal is usually called the joint power spectrum (JPS) [1]. Analytically, the JPS can be expressed through:

$$\begin{aligned}\mathrm{JPS}(\nu) &= |\mathcal{F}[u(x-a)\alpha(x-a) + h(x-b)]|^2\\ &= |U(\nu)*A(\nu)|^2 + |H(\nu)|^2 +\\ &[U(\nu)*A(\nu)]^* H(\nu)\exp^{j2\pi(a-b)\nu} + [U(\nu)*A(\nu)]H^*(\nu)\\ &\exp^{j2\pi(b-a)\nu}\end{aligned} \qquad (1)$$

where $j=\sqrt{-1}$, and the centered asterisk and superscript asterisk denote convolution and complex conjugation, respectively. Let us discuss now the inverse Fourier transform of the JPS, which can be

[*] Corresponding author at: Instituto de Física Rosario (CONICET-UNR), Blvr. 27 de Febrero 210bis, S2000EZP Rosario, Santa Fe, Argentina.
E-mail address: cuadradolaborde@ifir-conicet.gov.ar (C. Cuadrado-Laborde).

http://dx.doi.org/10.1016/j.optcom.2015.05.011
0030-4018/© 2015 Elsevier B.V. All rights reserved.

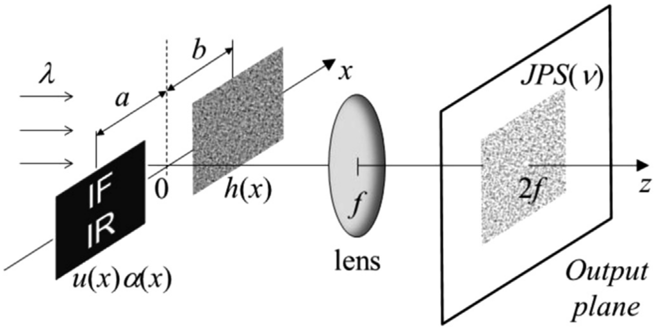

Fig. 1. Optical setup of the JTC used for encryption; where $u(x)$, $\alpha(x)$, $h(x)$, and JPS(ν) are the signal to be encrypted, the RPM, the key code, and the encrypted signal respectively, whereas f is the focal length and λ is the wavelength of the illuminating field.

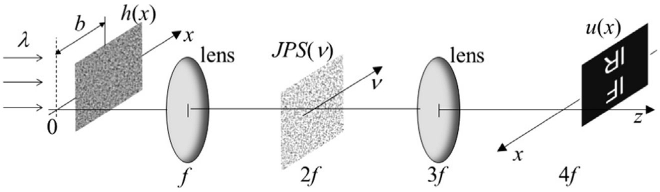

Fig. 2. Optical setup of the JTC used for decryption; where $u(x)$, $h(x)$, and JPS(ν) are the decrypted signal, the key code, and the encrypted signal respectively, whereas f is the focal length and λ is the wavelength of the illuminating field.

obtained by inverse Fourier transforming each term in Eq. (1):

$$e(x) = \mathcal{F}^{-1}[\mathrm{JPS}(\nu)] = [\alpha(x)u(x)]\star[\alpha(x)u(x)] + h(x)\star h(x)$$
$$+ h(x)\star[\alpha(x)u(x)]^{*}\delta(x-b+a) + h(x)\star[\alpha(x)u(x)]^{*}\delta(x-a+b) \quad (2)$$

where ★ stands for the cross-correlation operation. Briefly, see Fig. 2, in the decryption process, the key code $h(x)$ is positioned at coordinate $x=b$ of the input plane of a $4f$ setup. In the Fourier plane, i.e. at $z=2f$, the JPS is located on axis; being illuminated by the Fourier transform of $h(x-b)$, i.e., $H(\nu)\times\exp(-j2\pi\nu b)$. After another optical Fourier transform, the original signal $u(x)$ is obtained at $x=a$, and $z=4f$; provided $u(x)$ is positive, and the RPM is removed by an intensity sensitive device.

Let us now discuss the spatial and frequency extents of the encrypted signal recorded, i.e. the JPS. In what follows we assume that signals – e.g. $u(x)$ – are bounded within some finite region in the spatial and spatial frequency space, where the optical power of the signal itself, as well as its spectrum, is significantly a non-zero function [9–11]. This is, if E represents the total function energy, then $\int_{-\Delta x_u/2}^{\Delta x_u/2} \mathrm{d}x\,|u(x)|^2 = \int_{-\Delta \nu_u/2}^{\Delta \nu_u/2} \mathrm{d}\nu\,|U(\nu)|^2 \approx E$, where Δx_u and $\Delta\nu_u$ are the total spatial and spatial frequency extents of $u(x)$ and $U(\nu)=\mathscr{F}[u(x)]$, respectively. The same digression applies for all the other signals present through the encryption process. Let us now analyze the JPS bandwidth, see Eq. (1). The JPS signal bandwidth will be as high as the highest bandwidth of any of the four signals present in its composition, see Eq. (1). The spectral bandwidth of the first term, i.e. $|U(\nu)*A(\nu)|^2$, is given by the sum of the individual bandwidths, because of the convolution operation, i.e. $\Delta\nu_u + \Delta\nu_\alpha$. The second term has a spectral bandwidth simply given by $\Delta\nu_h$. The third and fourth terms has the same spectral bandwidth, because the complex conjugation does not affect this parameter. As a consequence of the multiplication present in these terms, the bandwidth can be obtained from the minimum between the bandwidths of $U(\nu)*A(\nu)$ and $H^*(\nu)$, i.e. $\min(\Delta\nu_u + \Delta\nu_\alpha, \Delta\nu_h)$. The final result for the JPS bandwidth can be expressed as follows:

$$\Delta\nu_{\mathrm{JPS}} = \max\left[\Delta\nu_u + \Delta\nu_\alpha,\ \Delta\nu_h,\ \min(\Delta\nu_u + \Delta\nu_\alpha,\ \Delta\nu_h)\right] \quad (3)$$

The maximum efficiency is obtained when the bandwidth of the key code $h(x)$ on the one hand, and the sum of the bandwidths of the RPM $\alpha(x)$ plus the image $u(x)$, on the other, are equal, i.e., $\Delta\nu_h = \Delta\nu_u + \Delta\nu_\alpha$. In this case the bandwidth of the JPS becomes $\Delta\nu_{\mathrm{JPS}} = \Delta\nu_h = \Delta\nu_u + \Delta\nu_\alpha$. This physically implies that both, the Fourier transform of the key code $h(x)$, as well as the Fourier transform of the tandem RPM plus image $\alpha(x)u(x)$ fill the same area in the intensity detector that records the JPS, maximizing the efficiency. On the contrary, when $\Delta\nu_h \ll \Delta\nu_u + \Delta\nu_\alpha$, the image is only partially encrypted, because a fraction of the Fourier transform of the tandem RPM plus image $\alpha(x)u(x)$ is not fully covered by the Fourier transform of the key code $h(x)$. In this case a low quality decryption is expected, without mentioning an increment in the vulnerability of the (partially) encrypted signal. Finally, when $\Delta\nu_h \gg \Delta\nu_u + \Delta\nu_\alpha$, i.e., when the key code bandwidth largely exceeds the bandwidth of $\alpha(x)u(x)$, the encryption–decryption is performed inefficiently. This is because a large fraction of the key code spectrum $H(\nu)$ is not used in the encryption process. On the contrary, the quality of decryption is unaffected.

On the other hand, the calculus of the spatial extent of $e(x)$ differs from the calculus of the bandwidth analyzed above; essentially because of the presence of two off-centered terms, see the Dirac deltas in Eq. (2). We start by analyzing the first term; because of the cross-correlation, its spatial extent is twice the spatial extent of $\alpha(x)u(x)$ – which in turn we can consider equal to Δx_u – In this way the spatial extent of the first term of $e(x)$ is given by $2\Delta x_u$, being centered at $x=0$. The second term of $e(x)$ has an spatial extent simply given by $2\Delta x_h$, being also centered at $x=0$. The third term has a spatial extension given by $\Delta x_h + \Delta x_{\alpha u} = \Delta x_h + \Delta x_u$, centered at $x=a-b$. Finally, the fourth term has identical spatial extent as the third term, but centered at $x=b-a$. Therefore, the spatial extent of $e(x)$ can be written as follows:

$$\Delta x_e = 2(b-a) + \Delta x_u + \Delta x_h \quad (4)$$

Generally, images, RPMs, and key codes have equal extensions and are placed side by side, i.e. $b=-a$, and $\Delta x_u = \Delta x_h = \Delta x_\alpha = 2b$; in this case $\Delta x_e = 4\Delta x_u$.

Finally, it should be taken into account that although we refer to the extension of JPS as a bandwidth, in an experiment its extension is measured in units of length. Reciprocally, $e(x)$ could be considered as a spectrum, with its extension given by Eq. (4), as a bandwidth. In both cases, the parameter λf – with λ as the optical wavelength and f as the focal length – must be used to solve this difference between the mathematical predictions and the experimental measurements. It is worth to mention also that in this work we focus on the extensions of the already registered encrypted signal, which is recorded in intensity. As opposed to Ref. [12] where the analysis was done on the optical fields by using the Wigner distribution function.

3. Results

In this section we numerically prove the validity of the analytical results obtained, by using several computer simulated examples. Without loss of generality, our signals in the input plane will be measured in units of pixels, as well as in the Fourier plane. However, if it is necessary to work in the usual units of length, the pixel size should be known. In the Fourier plane the usual units of frequency will be obtained by simple dividing the pixel size with λf. The key code $h(x)$ was located at $x=b=256$ pixels, whereas the RPM $\alpha(x)$ was attached to the image $u(x)$ and located at $x=a=-256$ pixels. As original image $u(x)$, we used the acronym of our host institution "IFIR", which is shown together with its corresponding Fourier transform $U(\nu)$ (in intensity), see Fig. 3(a) and