Optics Communications 353 (2015) 76–82

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:

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

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/

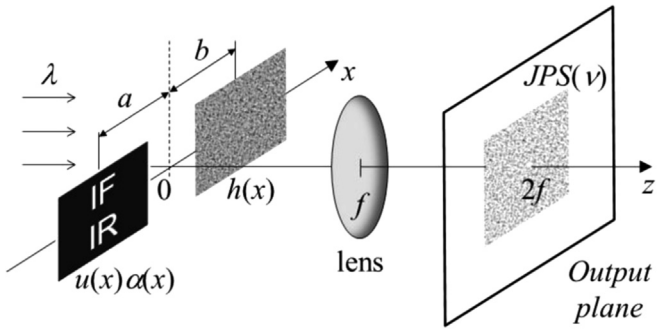

Fig. 1. Optical setup of the JTC used for encryption; where $u(x)$, $\alpha(x)$, $h(x)$, and JPS(ν) are the signal to be encrypted, the RPM, the key code, and the encrypted signal respectively, whereas f is the focal length and λ is the wavelength of the illuminating field.

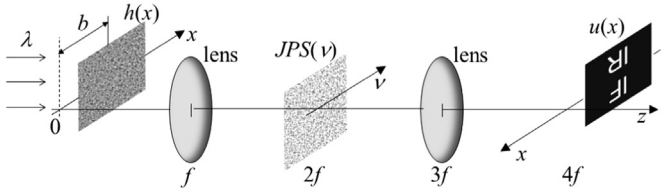

Fig. 2. Optical setup of the JTC used for decryption; where $u(x)$, $h(x)$, and JPS(ν) are the decrypted signal, the key code, and the encrypted signal respectively, whereas f is the focal length and λ is the wavelength of the illuminating field.

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 $\star$ 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 $\int_{-\Delta x_u/2}^{\Delta x_u/2} \mathrm{d}x\,|u(x)|^2 = \int_{-\Delta u_u/2}^{\Delta u_u/2} \mathrm{d}\nu\,|U(\nu)|^2 \approx E$, where Δx_u and $\Delta\nu_u$ are the total spatial and spatial frequency extents of $u(x)$ and $U(\nu)=\mathcal{F}[u(x)]$, 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

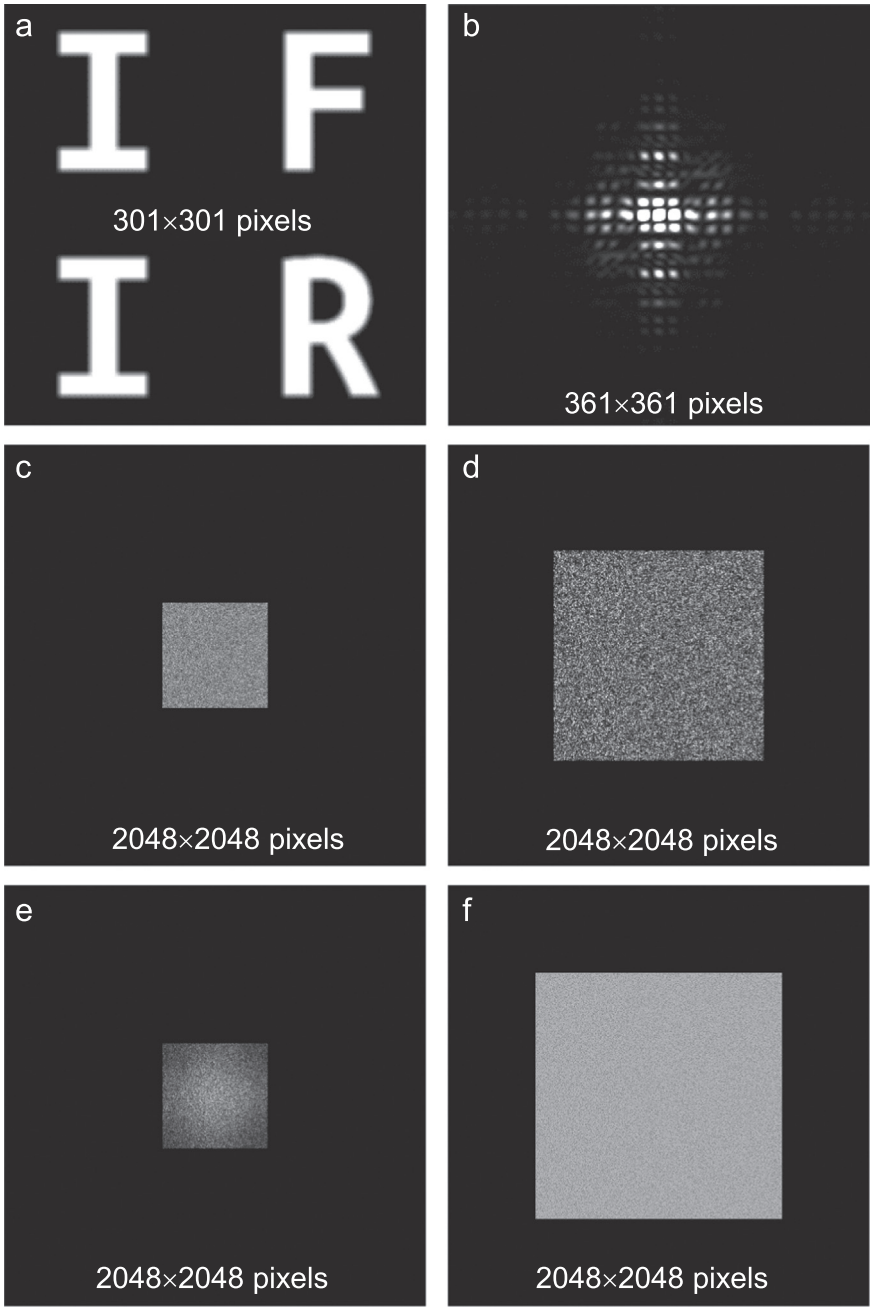

Fig. 3. Input image $u(x)$ and its corresponding spectrum, (a) and (b), respectively (both in intensity). Phase distribution of the RPM $\alpha(x)$ and its corresponding spectrum (in intensity), (c) and (d), respectively. Key code $h(x)$ and its corresponding spectrum (both in intensity), (e) and (f), respectively. The captions specify the size of the subarea shown in each case.

(b). From these figures it can be measured both, the extension of $u(x)$ and its spectral bandwidth, which result in $\Delta x_u = 232$ pixels and $\Delta \nu_u = 160$ pixels, respectively. On the other hand both, the RPM $\alpha(x)$ and the key code $h(x)$, were iteratively designed by following the procedure detailed in Refs. [13] and [14,15], respectively, in order to limit its spatial and spectral extension. In the iterative process used in the design of the RPM, the bandwidth was arbitrarily limited to 1024 pixels. This process is rapidly converging, being the energy of $A(\nu)$, outside the desired range, below 1% after 100 iterations. Fig. 3(c) and (d) shows the final phase distribution of the RPM $\alpha(x)$, as well as its corresponding Fourier transform (in intensity), respectively. From these figures we measured the extension of $\alpha(x)$ and its spectral bandwidth, which result in $\Delta x_\alpha = 512$ pixels and $\Delta \nu_\alpha = 1024$ pixels, respectively, as expected. According to our previous discussion in Section 2, the bandwidth of the key code should fulfill $\Delta \nu_h = \Delta \nu_u + \Delta \nu_\alpha$, i.e. 160 pixels + 1024 pixels = 1184 pixels. Therefore, in the iterative process used in the design of the key code, the bandwidth was limited to a slightly higher value of 1200 pixels. The final intensity distribution of the key code $h(x)$ and its corresponding Fourier transform are shown in Fig. 3(e) and (f), respectively. In this case, after 100 iterations the energy outside the desired range of $H(\nu)$ was below 0.1%. From these figures we measured both, the extension of $h(x)$ and its spectral bandwidth, which result in $\Delta x_h = 512$ pixels and $\Delta \nu_h = 1200$ pixels, respectively. Finally, the JPS, and its corresponding inverse Fourier transform $e(x)$, are shown in Fig. 4(a) and (b), respectively. From these figures we measured a spectral extension $\Delta \nu_{\mathrm{JPS}} = 1200$ pixels, whereas the spatial extension $\Delta x_e = 1763$ pixels. The validity of Eqs. (3) and (4) can be confirmed by replacing with the registered values for the

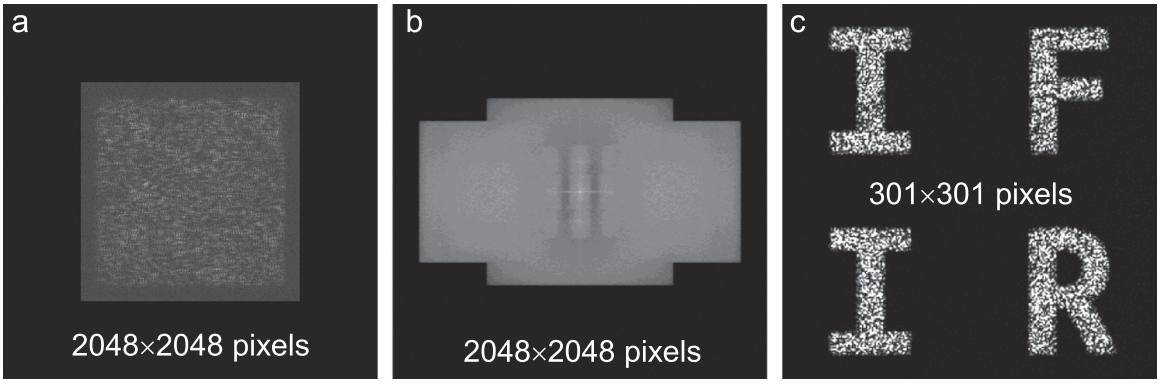

Fig. 4. (a) Joint power spectrum JPS(ν) and (b) its corresponding inverse Fourier transform $e(x)$ (both in intensity), when the bandwidth of the key code is optimally selected. (c) Image finally recovered in the decryption (in intensity).

spatial and spectral extensions. Therefore, we obtain $\Delta\nu_{\mathrm{JPS}}=\max[160$ pixels$+1024$ pixels, 1200 pixel, $\min(160$ pixels$+1024$ pixels, 1200 pixels)$]=1200$ pixels, and $\Delta x_e=2\times[256$ pixels$-(-256$ pixels$)]+232$ pixels$+512$ pixels$=1768$ pixels. In both cases the degree of coincidence is reasonably well for the spatial and spectral extensions; the small differences can be attributed to the impossibility to measure with precision in the spatial and spectral domains, simultaneously. The decrypted image can be observed in Fig. 4(c). This example could be considered the optimum case, in which both the key bandwidths and their extensions are designed to match accordingly to Eqs. (3) and (4). One of the reasons for the noise present in the decrypted image is the non-unitary magnitude in the RPM $\alpha(x)$ and key-code spectrum $H(\nu)$, as a consequence of the iterative process used to limit their bandwidths. Finally, in order to quantify the quality of the image decryption process, we computed the root mean square error *rms* as follows [16]:

$$rms=\sqrt{\frac{1}{NM}\sum_{n=0}^{N-1}\sum_{m=0}^{M-1}\left[|u(n,m)|^2-|u'(n,m)|^2\right]^2} \tag{5}$$

where $u(n, m)$ is the original image, $u'(n, m)$ is the decrypted image, n and m are pixel coordinates, and N and M are image width and height respectively. In this specific case of Fig. 4(c) $rms=53.7$.

We now analyze the situation when the key code $h(x)$ has an spectral bandwidth $\Delta\nu_h$ above the optimum, given by $\Delta\nu_u+\Delta\nu_\alpha$. In this case, we selected $\Delta\nu_h=1600$ pixels. The JPS, and its corresponding inverse Fourier transform $e(x)$, are shown in Fig. 5(a) and (b), respectively. From these figures we measured a spectral extension $\Delta\nu_{\mathrm{JPS}}=1600$ pixels, whereas the spatial extension $\Delta x_e=1763$ pixels. The validity of Eqs. (3) and (4) can be confirmed one more time, by replacing with the measured values for the spatial and spectral extensions. Therefore, we obtain $\Delta\nu_{\mathrm{JPS}}=\max[160$ pixels$+1024$ pixels, 1600 pixels, $\min(160$ pixels$+1024$ pixels, 1600 pixels$)]=1600$ pixels, and $\Delta x_e=2\times[256$ pixels$-(-256$ pixels$)]+232$ pixels$+512$ pixels$=1768$ pixels. In both cases the degree of coincidence is reasonably well. The decrypted image can be observed in Fig. 5(c) ($rms=54.2$). In this case the quality of decryption should be practically unaffected, as it can be observed by comparing Figs. 4(c) and 5(c); which is further confirmed by the similarity in the obtained RMS error values. Finally, we analyze the situation when the key code $h(x)$ has an spectral bandwidth $\Delta\nu_h$ bellow the optimum, given by $\Delta\nu_f+\Delta\nu_\alpha$. In this case, we selected $\Delta\nu_h=512$ pixels. The JPS, and its corresponding inverse Fourier transform $e(x)$, are shown in Fig. 6(a) and (b), respectively. From these figures we measured a spectral extension $\Delta\nu_{\mathrm{JPS}}=1200$ pixels, whereas the spatial extension $\Delta x_e=1763$ pixels. The validity of Eqs. (3) and (4) is confirmed, by replacing with the registered values for the spatial and spectral extensions. Therefore, we obtain $\Delta\nu_{\mathrm{JPS}}=\max[160$ pixels$+1024$ pixels, 512 pixels, $\min(160$ pixels$+1024$ pixels, 512 pixels$)]=1184$ pixels, and $\Delta x_e=2\times[256$ pixels$-(-256$ pixels$)]+232$ pixels$+512$ pixels$=1768$ pixels. In both cases the degree of coincidence is reasonably well. The decrypted image can be observed in Fig. 6(c) ($rms=75.95$). In this case the quality of decryption was indeed affected, as it can be observed by comparing Figs. 4(c) and 6(c), as a consequence of a partial encryption of the image. This is confirmed also by the increment in the RMS error from $rms=53.7$ in Fig. 4(c) to the actual value of 75.95.

Eq. (3) can be used to match the encrypted signal extension at the output plane with the transversal length of the optical available recording medium. When one, or both, the RPM or the key code bandwidth are un-limited, the encrypted signal extension increases without control, see Eq. (3). In this case, an intensity

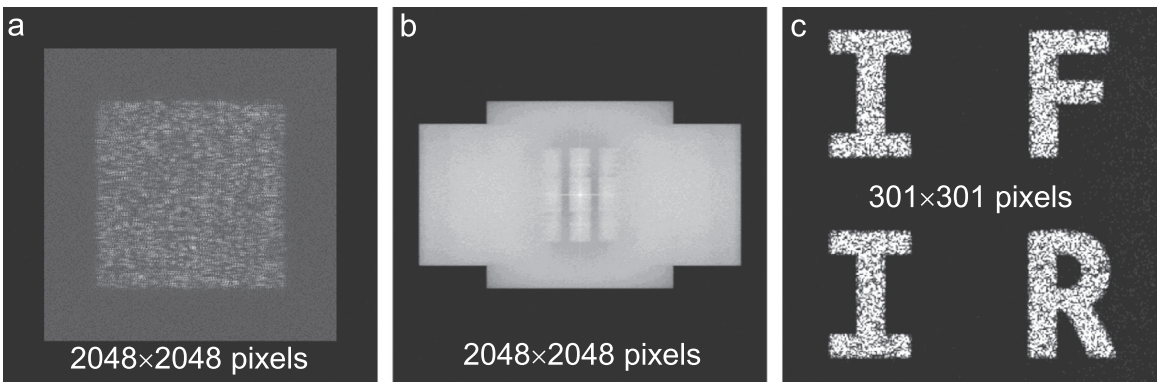

Fig. 5. (a) Joint power spectrum JPS(ν) and (b) its corresponding inverse Fourier transform $e(x)$ (both in intensity), when the bandwidth of the key code exceeds the optimum value. (c) Image finally recovered in the decryption (in intensity).

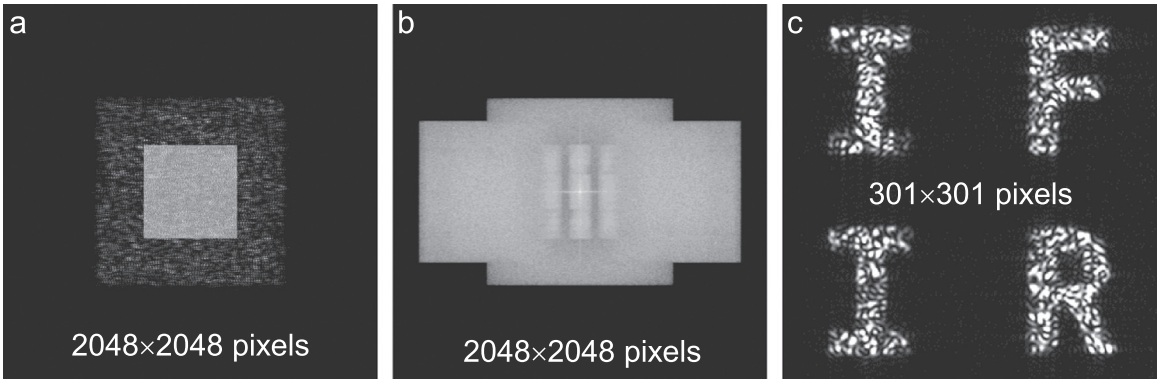

Fig. 6. (a) Joint power spectrum JPS(ν) and (b) its corresponding inverse Fourier transform $e(x)$ (both in intensity), when the bandwidth of the key code falls behind the optimum value. (c) Image finally recovered in the decryption (in intensity).

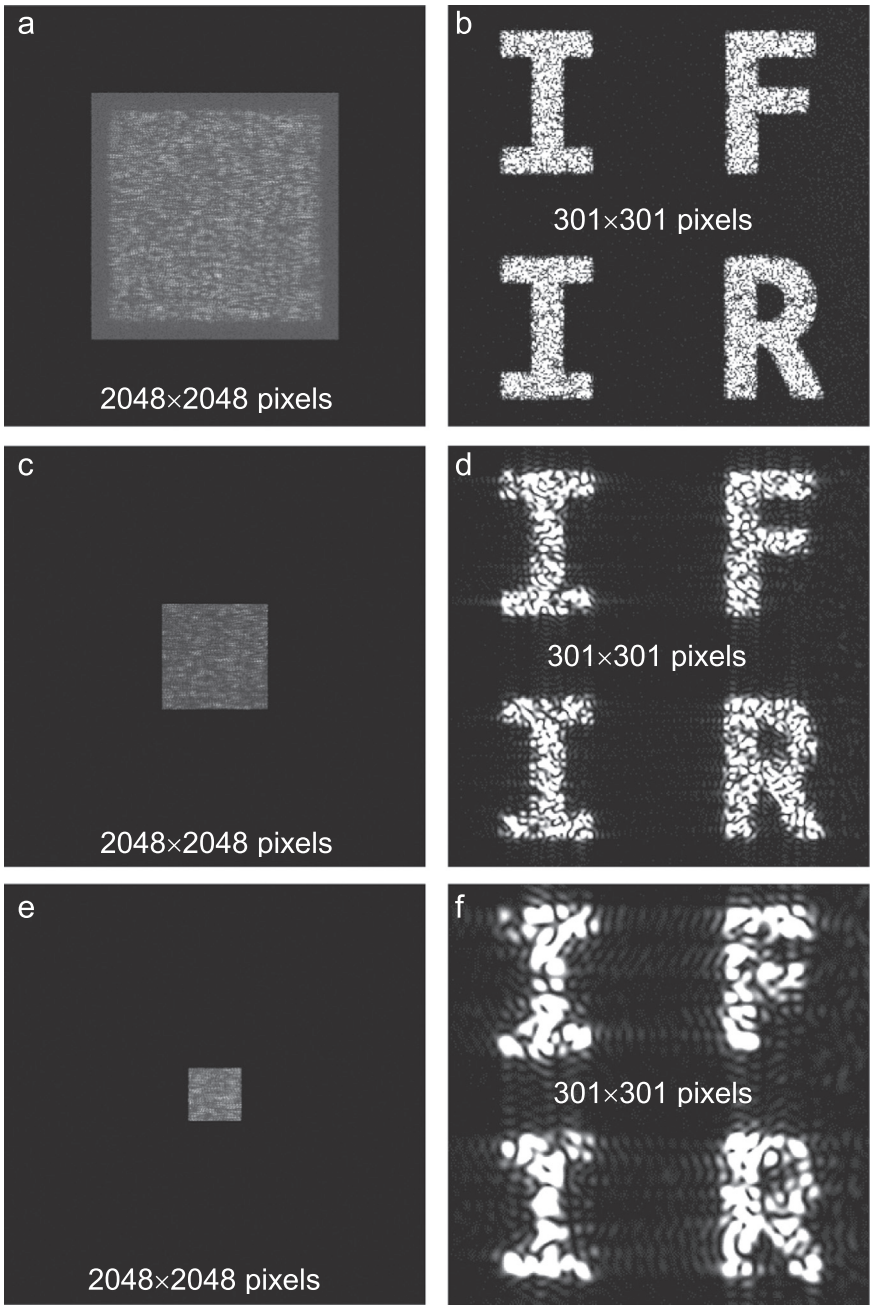

Fig. 7. Joint power spectrum and its corresponding decrypted image (both in intensity), when the extension of the JPS and the detection area exactly match (a) and (b), the detection area is lower than the extension of the JPS with a 57% mismatch (c) and (d), and a 79% mismatch (e) and (f), respectively.

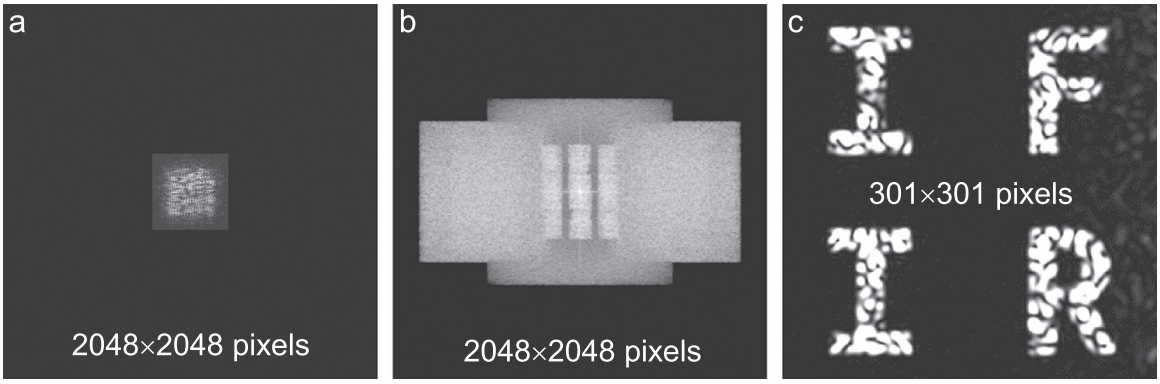

Fig. 8. (a) Joint power spectrum JPS(ν) and (b) its corresponding inverse Fourier transform $e(x)$ (both in intensity), when the bandwidth of the RPM decreases up to 256 pixels. (c) Image finally recovered in the decryption (in intensity).

detector only can record a fraction of the encrypted signal, being the subsequent loss of information the responsible of a low quality decryption. In the following, we illustrate the consequences of a mismatch between the encrypted signal extension at the output plane $\Delta\nu_{JPS}$ and the area of detection $\Delta\nu_d$. This effect was numerically simulated by multiplying the JPS obtained in the example shown in Fig. 4, with an amplitude-only matrix filled with ones within the area of detection, and zeros otherwise. In Fig. 7 (a) and (b), the JPS and its corresponding decrypted signal are shown ($rms=53.85$), respectively, when the extension of the JPS and the area of detection exactly match, i.e. $\Delta\nu_{\mathrm{JPS}}=\Delta\nu_d=1200$ pixels. As expected, the decryption is unaffected by this restriction, when compared to Fig. 5(c), where this restriction does not apply. Fig. 7(c) and (d) shows the JPS and the decrypted signal ($rms=61.72$), respectively, when the area of detection is further reduced to $\Delta\nu_d=512$ pixels, i.e. a mismatch of 57%. In this case the decryption can be performed, although the noise content clearly increases; being this further corroborated by the increment in the RMS error from $rms=53.85$ in the preceding case up to $rms=61.72$ in this case. Finally, Fig. 7(e) and (f) shows the JPS and decrypted signal ($rms=63.15$), respectively, when the area of detection is finally reduced to $\Delta\nu_d=256$ pixels, i.e. a mismatch of 79%. As a consequence of the strong mismatch between the extensions of the JPS and detector, the loss of information has severely increased. Despite this, the decryption can still be performed, although the noise content in the decrypted image is evidently higher, as compared to our previous results.

In Section 2 we demonstrated that a maximum efficiency is obtained when the bandwidth of the key code $h(x)$ and the sum of the bandwidths of the RPM $\alpha(x)$ plus the image $u(x)$. In this case, the bandwidth of the JPS $\Delta\nu_{\mathrm{JPS}}$ is either $\Delta\nu_h$ or $\Delta\nu_u + \Delta\nu_\alpha$. This raises the following question: how much tight the JPS could be for a given input image while simultaneously preserving an acceptable decryption? To address this topic is a relevant subject, since the area of the detector relates directly to its price. The answer is given by the ratio between the bandwidths of the RPM and the image. In the example shown in Fig. 4, this ratio was $\Delta\nu_\alpha/\Delta\nu_u=1024$ pixels/ 160 pixels$=6.4$. In the new example shown in Fig. 8, we reduce the RPM bandwidth to $\Delta\nu_\alpha=256$ pixels – while preserving all lengths and separations identical to the example shown in Fig. 4. Therefore, the ratio $\Delta\nu_\alpha/\Delta\nu_u$ reduces now to 256 pixels/160 pixels$=1.6$. A fair comparison should contemplate simultaneously a key code bandwidth reduction up to the optimum value, since we are interested in a reduction of the JPS extension. Thus, the new key code bandwidth was given by $\Delta\nu_h=\Delta\nu_u+\Delta\nu_\alpha=160$ pixels$+256$ pixels$=416$ pixels. Therefore, the expected extensions in the JPS and its corresponding inverse Fourier transform should be $\Delta\nu_{\mathrm{JPS}}=416$ pixels and $\Delta x_e=1768$ pixels, according to Eqs. (3) and (4), respectively. The JPS and its corresponding inverse Fourier transform $e(x)$ are shown in Fig. 8(a) and (b), respectively. From these figures we measured the spectral extension $\Delta\nu_{\mathrm{JPS}}=420$ pixels, whereas the spatial extension $\Delta x_e=1763$ pixels, which reasonably agree with the expected values. The decrypted image is depicted in Fig. 8(c) ($rms=53.43$). In this figure, it can be observed that, as a consequence of a reduction in the RPM bandwidth, the decrypted image has decreased its quality. Finally, we reduced further the RPM bandwidth up to 80 pixels – while preserving all lengths and separations identical to the example shown in Fig. 4. The ratio $\Delta\nu_\alpha/\Delta\nu_u$ reduces to 80 pixels/ 160 pixels$=0.5$. Again, in order to make a fair comparison, the key code bandwidth should be adequately reduced to the optimum value, given now by $\Delta\nu_h = \Delta\nu_u + \Delta\nu_\alpha = 160$ pixels$+80$ pixels$=240$ pixels. According to Eqs. (3) and (4), the expected extensions in the JPS and its corresponding inverse Fourier transform should be $\Delta\nu_{\mathrm{JPS}}=240$ pixels

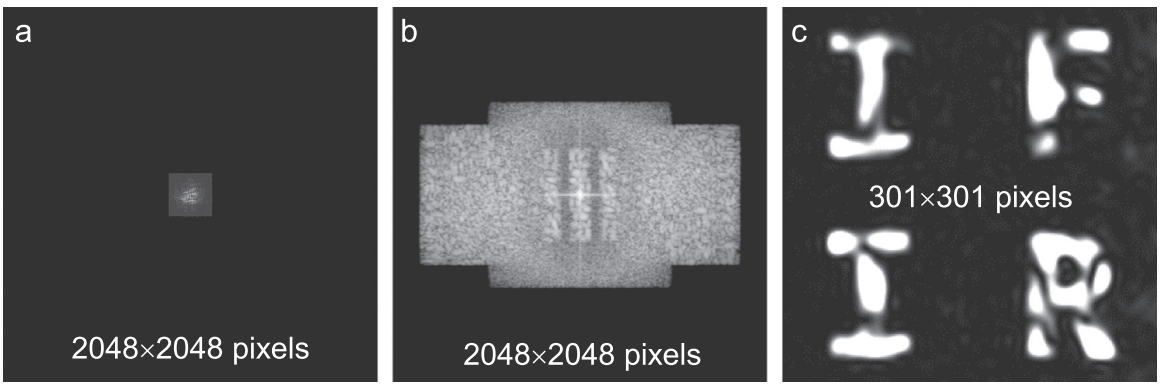

Fig. 9. (a) Joint power spectrum JPS(ν) and (b) its corresponding inverse Fourier transform $e(x)$ (both in intensity), when the bandwidth of the RPM decreases up to 80 pixels. (c) Image finally recovered in the decryption (in intensity).

and $\Delta x_e = 1768$ pixels, respectively. The JPS and its corresponding inverse Fourier transform $e(x)$ are shown in Figs. 9(a) and (b), respectively. From these figures we measured the spectral extension $\Delta \nu_{JPS} = 240$ pixels, whereas the spatial extension $\Delta x_e = 1763$ pixels, which reasonably agree with the expected values. The decrypted image can be observed in Fig. 9(c) ($rms = 53.19$). In the present case of strong RPM bandwidth reduction, the decrypted image shows broader speckle grains than in the preceding cases. Despite this, the RMS error does not significantly increases because the JTC parameters were optimally set.

4. Conclusions

In this work we analyzed the extensions in the recorded JPS in both, spatial and Fourier domains. The expressions were further corroborated through several numerical examples under different situations. An optimum efficiency is reached, when the bandwidth of the key code on the one hand, and the sum of the bandwidths of the image plus the random phase mask, on the other, are equal. 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. The effects on the decrypted image, when the detection area is lower than the encrypted signal extension, were analyzed also.

Acknowledgments

G.E. Galizzi would like to thank financial support from project PIP 11220110100971 (CONICET, Argentina).

References

[1] T. Nomura, B. Javidi, Optical encryption using a joint transform correlator architecture, Opt. Eng. 39 (2000) 2031–2035.
[2] P. Réfrégier, B. Javidi, Optical image encryption based on input plane and Fourier plane random encoding, Opt. Lett. 20 (1995) 767–769.
[3] D. Amaya, M. Tebaldi, R. Torroba, N. Bolognini, Multichanneled encryption via a joint transform correlator architecture, Appl. Opt. 47 (2008) 5903–5907.
[4] D. Amaya, M. Tebaldi, R. Torroba, N. Bolognini, Wavelength multiplexing encryption using joint transform correlator architecture, Appl. Opt. 48 (2009) 2099–2104.
[5] J.F. Barrera, M. Tebaldi, C. Ríos, E. Rueda, N. Bolognini, R. Torroba, Experimental multiplexing of encrypted movies using a JTC architecture, Opt. Express 20 (2012) 3388–3393.
[6] M. Tebaldi, S. Horrillo, E. Pérez-Cabré, M.S. Millán, D. Amaya, R. Torroba, N. Bolognini, Experimental color encryption in a joint transform correlator architecture, J. Phys.: Conf. Ser. 274 (2011) 012054.
[7] E. Rueda, J.F. Barrera, R. Henao, R. Torroba, Lateral shift multiplexing with a modified random mask in a joint transform correlator encrypting architecture, Opt. Eng. 48 (2009) 027006.
[8] D. Amaya, M. Tebaldi, R. Torroba, N. Bolognini, Digital color encryption using a multi-wavelength approach and a joint transform correlator, J. Opt. A: Pure Appl. Opt. 10 (2008) 104031.
[9] A. Lohmann, R. Dorsch, D. Mendlovic, C. Ferreira, Z. Zalevsky, Space-bandwidth product of optical signals and systems, J. Opt. Soc. Am. A 13 (1996) 470–473.
[10] B.M. Hennelly, J.T. Sheridan, Optical encryption and the space bandwidth product, Opt. Commun. 247 (2005) 291–305.
[11] B. Hennelly, T. Naughton, J. McDonald, J. Sheridan, G. Unnikrishnan, D. Kelly, B. Javidi, Spread-space spread-spectrum technique for secure multiplexing, Opt. Lett. 32 (2007) 1060–1062.
[12] C. Cuadrado-Laborde, J. Lancis, The space-bandwidth product in the joint transform correlator, Opt. Commun. 284 (2011) 4316–4320.
[13] T. Nomura, E. Nitanai, T. Numata, B. Javidi, Design of input phase mask for the space bandwidth of the optical encryption system, Opt. Eng. 45 (2006) 017006-1–017006-5.
[14] C. Chen, L. Lin, C. Cheng, Design and implementation of an optical joint transform encryption system using complex-encoded key mask, Opt. Eng. 47 (2008) 068201-1–068201-8.
[15] T. Nomura, S. Mikan, Y. Morimoto, B. Javidi, Secure optical data storage with random phase key codes by use of a configuration of a joint transform correlator, Appl. Opt. 42 (2003) 1508–1514.
[16] J.A. Muñoz-Rodríguez, R. Rodríguez-Vera, Image encryption based on a grating generated by a reflection intensity map, J. Mod. Opt. 52 (2005) 1385–1395.