Wavelength multiplexing encryption using joint transform correlator architecture

Dafne Amaya,[1] Myrian Tebaldi,[1,*] Roberto Torroba,[1] and Néstor Bolognini[2]

[1]Centro de Investigaciones Ópticas (CONICET-CIC) and UID OPTIMO, Facultad Ingeniería, Universidad Nacional de La Plata, P.O. Box 124, La Plata 1900, Argentina.

[2]Centro de Investigaciones Ópticas (CONICET-CIC), Facultad Ingeniería and Ciencias Exactas, Universidad Nacional de La Plata, La Plata 1900, Argentina.

*Corresponding author: myrianc@ciop.unlp.edu.ar

Received 11 December 2008; accepted 20 February 2009;
posted 17 March 2009 (Doc. ID 105243); published 3 April 2009

We show that multiple secure data recording under a wavelength multiplexing technique is possible in a joint transform correlator (JTC) arrangement. We evaluate both the performance of the decrypting procedure and the influence of the input image size when decrypting with a wavelength different from that employed in the encryption step. This analysis reveals that the wavelength is a valid parameter to conduct image multiplexing encoding with the JTC architecture. In addition, we study the influence of the minimum wavelength change that prevents decoding cross talk. Computer simulations confirm the performance of the proposed technique.

OCIS codes: 070.0070, 070.4560.

1. Introduction

Much has been published about security [1–8] and holographic memory systems [9–12]. Optical technologies provide an environment that is resistant to attacks. Typically, encryption is performed by double random-phase encoding in the Fourier domain [2] in which two statistically independent random phase masks, in the input and the Fourier planes, are important components of the method. This technique was extended to the fractional Fourier domain [13] and the Fresnel domain [14,15].

Owing to the adoption of real-valued data for a key code, Nomura and Javidi used the configuration of a joint transform correlator (JTC) where two-dimensional data and a key code can be placed side by side at the input plane [16]. This optical setup is more compact than an ordinary holographic setup because the object and the reference beams share a single optical system that consists of two Fourier-transforming lenses. In contrast, a 4f correlator implies a holographic architecture so that in the decryption step a phase conjugate beam must be generated. A safer working space is generally provided by controlling physical user access and by providing partitions to protect multiply displayed information. In other words, the security of the displayed information is maintained by user authentication and limitation of the viewing information. In this regard, optics has many degrees of freedom (wavelength, polarization, three-dimensional topology, etc.). Some of these parameters are used in several papers to multiplex data [17–21]. In particular, Situ and Zhang proposed a wavelength-multiplexing method for multiple image encryptions [21]. They introduced wavelength multiplexing into a double random-phase encoding system to achieve multiple-image encryption. Each primary image is first encrypted and then superposed to yield the final enciphered image.

We believe that multiple secure data recording by using optical degrees of freedom is also possible by taking advantage of a JTC arrangement. Therefore, we propose the implementation of a wavelength-multiplexing technique with a JTC architecture. In a multiplexing method the limited amount of data

0003-6935/09/112099-06$15.00/0

to be stored depends on the optical parameters employed, the storage medium, and the particular architecture to be considered. Consequently, within this context we study the influence of the minimum wavelength change that avoids cross talk. Another feature to be analyzed is the noise generation that is due to the multiple nondecrypted images over a single decrypted image.

In Section 2 we describe the principle of the proposed system using a JTC configuration. In Section 3 we analyze the increased noise in a decrypted single object when the wavelength shifts with respect to the encryption wavelength (wavelength sensitivity). In Section 4 the multiplexing procedure is presented and we show computer simulations to confirm the performance of the proposed approach, including a discussion of cross-talk prevention. In Section 5 we present the summary and conclusions.

2. Principle of the System

The double random-phase encoding encryption technique [2] uses a phase code key in each of the input and Fourier planes to encrypt the data. The decryption uses the complex conjugate of the Fourier-plane phase code key to recover the data. When using multiplexing procedures under the above-described scheme, we employ sequential encrypting masks or micropositioning devices to arrange the encrypting–decrypting process. In turn, polarizer [18], apertures [19,20], or other alternative devices must be employed to achieve encryption. Alternatively, the basic encrypting correlation procedure and multiplexing can be realized using JTC architecture. We use a JTC to perform the correlation between the convolution of a phase-encoded primary object along a random mask both included in one of the windows and a random phase encoding distribution used as reference in another window. We now discuss the wavelength-multiplexing techniques. These spectral-dependent multiple storing and retrieving techniques reduce the need for masks or other kind of positioning arrangements and allow parallel image handling.

Figure 1 shows the basic implementation for a single encrypted record as well as the mathematical expressions that represent the approach. For the sake of brevity, we limited ourselves to a one-dimensional notation. Let $r(x)$, $g(x)$, and $h(x)$ represent the image random-phase mask, the image to be encrypted, and the reference key code mask, respectively. Both random-phase masks have uniform amplitude transmittance. The complex-valued key code, $h(x)$, is the inverse Fourier transform of a random-phase mask $H(\nu)$, where ν is the spatial frequency. As mentioned above, the phase mask $H(\nu)$ is purely random-phase information, which is statistically independent of $r(x)$. During the encryption process, the image random-phase mask $r(x)$ covers image $g(x)$, which implies a product operation between them. In the input plane the JTC apertures contain at coordinate $x = a$ the distribution $r(x)g(x)$ and another aperture

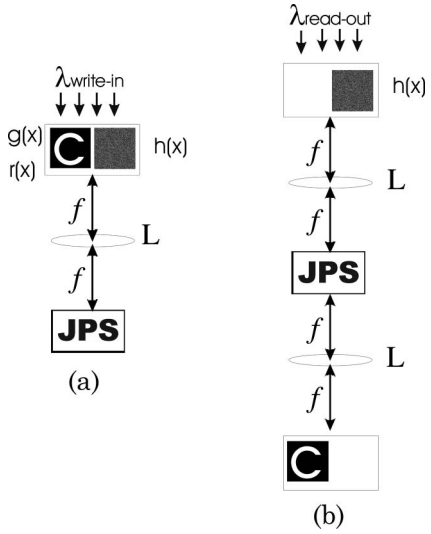


Fig. 1. JTC scheme used in the proposal: (a) write-in step and (b) read-out step, where L is a lens, f is the focal length ($f = 5$ cm), and $g(x)$ and $r(x)$ are random-phase masks.

at $x = b$ contains random reference key code $h(x)$. A plane wave illuminates the arrangement and, after transmission through a lens, the joint power spectrum (JPS) is obtained at its focal plane. The JPS results are

$$\begin{aligned}\mathrm{JPS}(\nu) &= |F[r(x-a)g(x-a) + h(x-b)]|^2 \\ &= |R(\nu) \otimes G(\nu)|^2 + 1 \\ &\quad + [R(\nu) \otimes G(\nu)]^* H(\nu) \exp[-2i\pi(b-a)\nu] \\ &\quad + [R(\nu) \otimes G(\nu)] H^*(\nu) \exp[-2i\pi(a-b)\nu], \quad (1)\end{aligned}$$

where $F[], R(\nu)$, and $G(\nu)$ represent the Fourier transform operation and the Fourier transforms of $r(x)$ and $g(x)$, respectively. In our case, $H(\nu)$ only has phase information so we set $|H(\nu)|^2 = 1$. The symbol $\otimes$ and the superscript asterisk $*$ represent convolution and complex conjugation, respectively. The $\mathrm{JPS}(\nu)$ is the encrypted data or the encrypted power spectrum. If the storage medium transmittance behaves as an intensity linear register, in the decryption step after plane-wave illumination and inverse Fourier transformation, the stored $\mathrm{JPS}(\nu)$ yields

$$\begin{aligned}\mathrm{JPS}(x) &= [r(x)g(x)] \bullet [r(x)g(x)] \\ &\quad + \delta(x) + h(x) \bullet [r(x)g(x)] \otimes \delta(x-b+a) \\ &\quad + [r(x)g(x)] \bullet h(x) \otimes \delta(x-a+b), \quad (2)\end{aligned}$$

where the $\bullet$ and $\delta(x)$ denote the correlation operation and the Dirac delta function, respectively. At the output at coordinates $x = a - b$ and $x = b - a$, we obtain the cross correlations of $r(x)$, $g(x)$, and $h(x)$. These terms represent noiselike images. We cannot recover image $g(x)$ without knowledge of $h(x)$. The autocorrelation of $r(x) \cdot g(x)$ is obtained at coordinate $x = 0$, which is also a noiselike image. We cannot recover image $g(x)$ from this autocorrelation signal without

knowledge of $r(x)$. In the decryption step, a plane wave illuminates the reference key code mask $h(x)$ placed at coordinate $x = b$ and after Fourier transformation gives $H(\nu)\exp[-2\pi i b\nu]$. Then, the encrypted power spectrum JPS(ν) at the focal plane of the lens is illuminated by the detailed Fourier transform and results as follows:

$$\begin{aligned} M(\nu) &= \mathrm{JPS}(\nu)H(\nu)\exp[-2\pi i b\nu] \\ &= |R(\nu) \otimes G(\nu)|^2 H(\nu)\exp[-2\pi i b\nu] + H(\nu) \\ &\quad \times \exp[-2\pi i b\nu] + [R(\nu) \otimes G(\nu)]^* H(\nu)H(\nu) \\ &\quad \times \exp[-2\pi i(2b-a)\nu] + R(\nu) \otimes G(\nu) \\ &\quad \times \exp[-2\pi i a\nu]. \end{aligned} \tag{3}$$

By inverse Fourier transformation of $M(\nu)$, we obtain

$$\begin{aligned} m(x) &= h(x) \otimes [r(x)g(x)] \bullet [r(x)g(x)] \otimes \delta(x-b) \\ &\quad + h(x) \otimes \delta(x-b) + h(x) \otimes h(x)[r(x)g(x)] \\ &\quad \otimes \delta(x-2b-a) + r(x)g(x) \otimes \delta(x-a). \end{aligned} \tag{4}$$

The intensity of the fourth term on the right-hand side of Eq. (4) produces the original image, provided that $g(x)$ is positive and an intensity-sensitive device removes phase function $r(x)$. The image is obtained at coordinate $x = a$. The undesired terms obtained at coordinates $x = b$ and $x = 2b - a$ are spatially separated from the recovered image.

Bear in mind that the original double random-phase encoding method requires the complex conjugate of the Fourier phase key to decrypt the image. The two step JTC architecture is inherently holographic. In the decryption step, an exact complex conjugate of the key code does not need to be used, just plane-wave illumination is necessary to implement the decryption procedure. As expected, if the illumination wavelength changes maintaining the reference random-phase key code, the encrypted spectrum changes as well. To proceed with the multiplexing, each input object encrypted with a different wavelength, is recorded one by one at the output plane. Each JPS associated with each channel is stored in the same medium, thereby generating the multiplexed joint power spectra.

In the above image encryption system, we encrypted the information independently in several channels and the iterative encryption method increases the number of keys. The keys in all these channels should be correct for decryption, otherwise we could not correctly recover the information.

3. Wavelength Sensitivity and Noise Influence

In this analysis we assume that the phase key code $h(x)$ is correct. If adequate wavelength λ is used for decryption, the image is correctly decrypted. Otherwise, the random noise introduced by $h(x)$ cannot be removed and might affect the information recovery of the system. Let us assume that the decryption wavelength differs in $\Delta\lambda$ from the encryption wavelength. In this case, the impulse response (IR) of the decryption system becomes, in single coordinate notation [14],

$$\begin{aligned} \mathrm{IR}(x, x_0, f, \lambda+\Delta\lambda) &= \frac{\exp[2\pi i f/(\lambda+\Delta\lambda)]}{i(\lambda+\Delta\lambda)f} \\ &\quad \times \exp\left\{\frac{i\pi}{(\lambda+\Delta\lambda)f}[x-x_0]^2\right\}, \end{aligned} \tag{5}$$

where f represents the focal length of lens L and x and x_0 are spatial variables. It is possible to show that

$$\frac{1}{\lambda+\Delta\lambda} = \frac{1}{\lambda} - \frac{\Delta\lambda}{\lambda^2}. \tag{6}$$

Using Eq. (6), the first phase factor of Eq. (5) can be expressed as $\exp[2\pi i f/\lambda]\exp[-2\pi i f\Delta\lambda/\lambda^2]$. That is, the effect of $\Delta\lambda$ is to add a phase to the phase distribution in the transform plane. By a similar analysis, we can show that the second phase factor affects the distribution in the transform. Thus, application of the correct phase code cannot remove the phase introduced by $\Delta\lambda$. This phase adds up to the random original structure mapping it in the decryption step in another random distribution that does not coincide with the original one. Therefore the propagation fails to decrypt the information correctly.

Let us consider the wavelength selectivity when one has the correct phase key to decrypt data. One-dimensional notation is used for simplicity. We therefore write the reconstruction of the fourth term of Eq. (1) with an incorrect wave field $H(\eta\nu)\exp[-2\pi i b\eta\nu]$ as follows:

$$W(\nu) = K(\nu)\exp[-2\pi i(\Phi(\eta\nu) - \Phi(\nu))], \tag{7}$$

with $K(\nu) = R(\nu) \otimes G(\nu)$, and its inverse Fourier transform yields to

$$w(x) = r(x)g(x) \otimes F[\exp[-2\pi i(\Phi(\eta\nu) - \Phi(\nu))]], \tag{8}$$

where $\eta = \lambda/(\lambda+\Delta\lambda)$ is the wavelength ratio between the recording and the readout beams, and random phase functions $\Phi(\eta\nu)$ and $\Phi(\nu)$ are statistically independent and are uniformly distributed in the interval $[0, 2\pi]$. This fact prevents the correct reconstruction of the encrypted object. Actually, because of the finite correlation length of the mask, there will be a partial overlap between $\Phi(\eta\nu)$ and $\Phi(\eta\nu)$ as a function of the correlation length and the scale change. The result shown in Eq. (8) reveals that it is impossible to faithfully reconstruct the encoded information.

We performed an encryption procedure to codify the inputs by using a 640 nm wavelength. Let us evaluate the influence of the input data pixel amount when decrypting with a shifted wavelength with respect to that employed in the encryption step. To implement the evaluation, the same input image

with different sizes is employed. In Fig. 2, the first, second, and third column display the decrypted images when the input image sizes are 400×400, 300×300, and 200×200 pixels, respectively. The first row in Fig 2 shows the decrypted images when the decryption wavelength is also 640 nm. In the successive rows the decrypted images were obtained with a decryption wavelength that differs in steps of 4 nm with respect to that employed in the encryption procedure (640 nm wavelength).

A parameter to obtain a more quantitative evaluation is the mean-square error (MSE). Figure 3 shows the MSE curves calculated between the original data correctly decrypted and the decrypted data when a shifted wavelength is employed in a single encryption procedure. The data employed in calculating the curves belong to the cases considered in Fig. 2. Each curve shows the wavelength shifting sensitivity behavior of the system. The 400×400 pixel encrypted image curve shows that, when the wavelength difference is 4 nm, the mean error between decrypted and original data is 0.9. For the same wavelength difference, in the 200×200 pixel encrypted image, the mean error is 0.5. These results also illustrate that the wavelength sensitivity of the encrypted data depends on the amount of encrypted information. This fact suggests that, if a certain degree of fidelity recovering is required, as the input data amount increases a shorter wavelength shifting decryption is allowed. This analysis can be utilized in a multiplexing procedure to decrypt each input without cross talk.

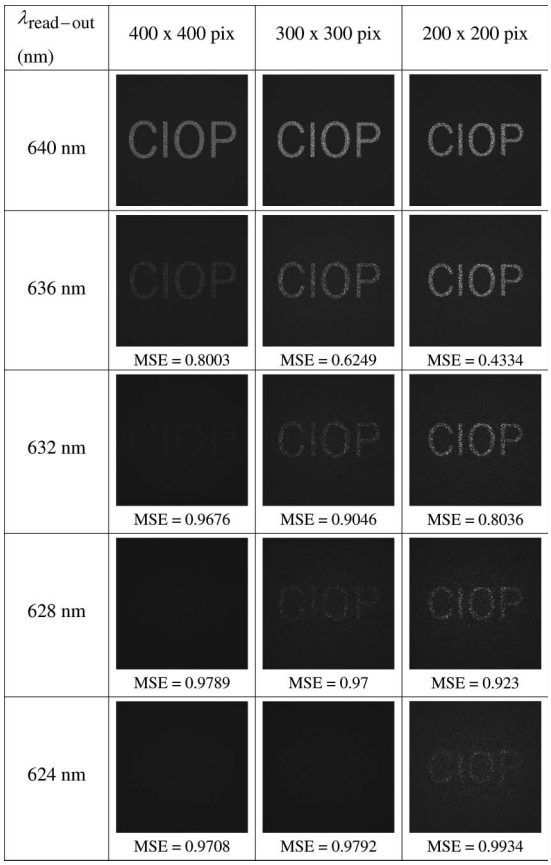


Fig. 2. Results showing the reconstruction of the encrypted input data, the word CIOP, for different input pixel size and for a read-out wavelength shifted with respect to that used in the write-in step. The MSE value is listed for the shifted wavelength reconstruction cases.

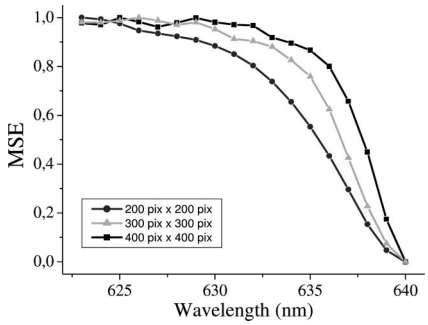


Fig. 3. MSE in terms of the read-out wavelengths. Note that the write-in wavelength is 640 nm.

4. Wavelength Multiplexing

We now analyze a multiplexing procedure to encrypt and decrypt input images. The proposed approach is to combine several encrypted images. The encryption parameter in this case is the wavelength and each input is encrypted with a different wavelength. It is apparent that the performance of a multiple image security system will improve if cross talk is diminished. Let us consider as an example a four input image encryption of four different characters. Each encrypted image is decrypted with the same wavelength as employed in its encryption procedure. The decrypted images are shown in Fig. 4. The decryption outputs that belong to the same input character are displayed along each column. For the decrypted output placed at row m, column i, the encryption wavelength is $\lambda_{mi} = \lambda_0 + (i-1)\Delta\lambda_{0m}$,

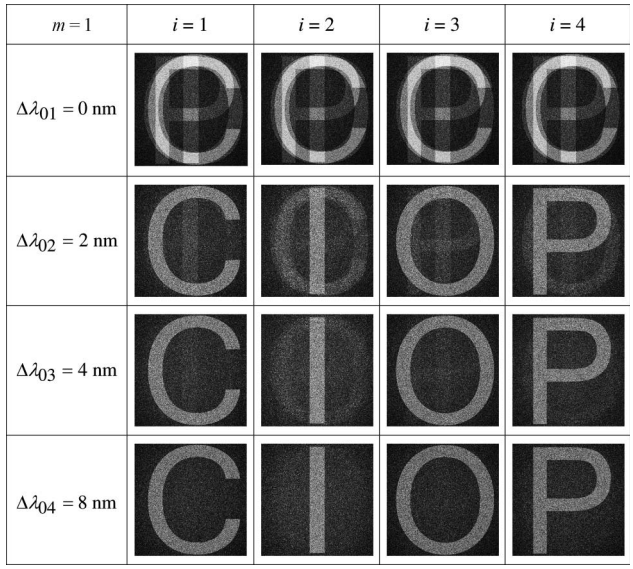
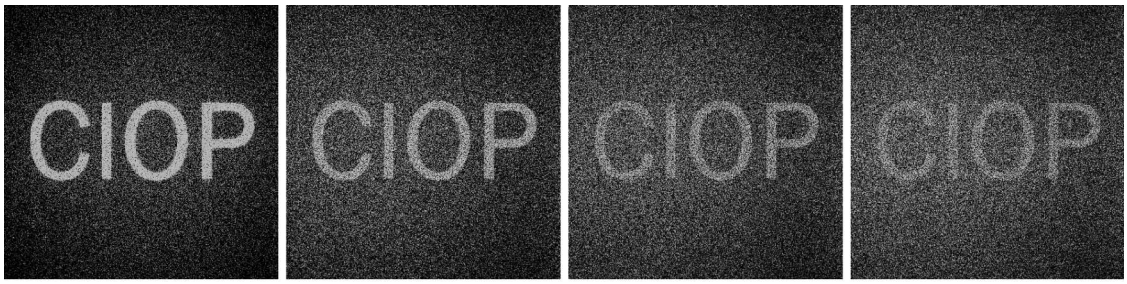


Fig. 4. Multiplexing decrypted images, each one reading out with the wavelength as they were encrypted.



N = 1 (a) N = 10 (b) N = 20 (c) N = 30 (d)

Fig. 5. One channel recovered image sequences that correspond to encrypted N input images. The input image size is 400 × 400 pixels.

where $m,i = 1, 2, 3, 4$, and $\Delta\lambda_{01} = 0$ nm, $\Delta\lambda_{02} = 2$ nm, $\Delta\lambda_{03} = 4$ nm, and $\Delta\lambda_{04} = 8$ nm. Therefore, the decryption outputs shown in the first row ($m = 1$) correspond to the case when all the input characters are encrypted by the same wavelength, that is, $\lambda_0 = 640$ nm. These outputs show that the correct information is revealed, although it suffers from severe cross talk because each decrypted character is displayed simultaneously with the remaining characters and all have the same fidelity.

In the second row, $\Delta\lambda_{02} = 2$ nm and each decrypted character also suffers from cross talk although it is clearly attenuated in comparison with the situation in the first row. In the third row, $\Delta\lambda_{03} = 4$ nm and the residual cross talk is further attenuated. As mentioned, the decrypted images in all cases are read out with the same wavelength with which they were encrypted. In addition, the decryption outputs are displayed along each column belonging to the same input character; along each row one can observe that the cross-talk strength of the remaining characters is not uniform. For example, the character I adds cross talk to the outputs in the second row, columns 1, 3, and 4. But its strength is higher in columns 1 and 3 than in column 4. Clearly, its residual appearance depends on wavelength shifting. The decryption procedure reveals cross-talk attenuation when $\Delta\lambda$ increases. Finally, in the fourth row, with a wavelength separation of 8 nm, cross talk disappears and each character suffers only random noise. Therefore, in general, in a multiple decryption procedure when reading out with λ_i, the ith decrypted image can be expressed as

$$\hat{g}_i(x) = g_i(x) + n(x), \tag{9}$$

where

$$n(x) = \sum_{j=1}^{N} w_j(x, \lambda_i + \Delta\lambda_{ij}), \qquad i = 1N, \tag{10}$$

with $w_j(x, \lambda_i + \Delta\lambda_{ij})$ is defined in Eq. (8), $\Delta\lambda_{ij} = \lambda_j - \lambda_i$, and N represents the number of multiplexed images.

The least separation $\Delta\lambda_{\min}$ between the two operating wavelengths should take the value that makes cross talk $n(x)$ become random noise. From this point of view, the cross talk is specified by the impulse response of each stage of the system or the system's structure parameters. In our case, $\Delta\lambda_{\min}$ is 8 nm. As is shown in Ref. [20], by recording more than N encrypted images in the same file, the mth user can recover his secret image in a form that contains cross-talk noise that is greater in strength than that in Eq. (9). Moreover, its strength increases along with the total number N of encrypted images.

Figure 5 shows the decryption results when the same input is multiplexed N times with $N = 10$, 20, and 30 and $\Delta\lambda$ is 8 nm. It is observed that the noise increases when N increases. Although this noise is diffuse, the signal of interest is immersed in it when the cross-talk strength is large enough. Therefore, it will always be necessary to determine the maximum number, $N_{\max}$, that the recovered authorized signal can tolerate. In addition, the criterion ought to be the error between the recovered image and the corresponding input image.

5. Conclusions

Multiple secure data recording has been demonstrated in a joint transform correlator scheme that requires neither phase conjugation nor accurate optical alignment as with the conventional *4f* architecture. In our proposal, the random phase mask and wavelength are essential encoding keys. The multiplexing procedure implemented uses the wavelength as the encryption parameter. Each new input is encrypted with a wavelength that is shifted with respect to the wavelength used to encrypt previous inputs. An important result becomes obvious when one considers that the input image size or, equivalently, the amount of information stored affects the decryption information. In this sense, we proved that a minor change in the decoding wavelength reconstruction affects the fidelity of data recovery, which in turn depends on the input image size. We have to note that, in a multiplexing procedure, we are unable to distinguish whether the JPS is constituted by a single or several joint

power spectra. This feature is a consequence of the nature of the JPS data and also reinforces the security that we pursue in our approach. Our multiplexing scheme is immune to known attack procedures that rely on the existence of an input-encryption image pair. In this sense multiplexing increases the protection against attacks. Since the additive cross talk created by mutual disturbances results in evident deterioration of the quality of multiple extractions, this multiplexing technique is limited. The quality of the final decrypted image depends on the object bandwidth imposed by multiplexing for any given optical architecture. These constraints imply an upper limit to the number of multiplexed images in a rather complex way.

This research was performed under grants CONICET 5995, ANCYT PICT 1167 (Argentina), and Facultad Ingeniería, Universidad Nacional de La Plata, Argentina.

References

1. H.-Y. S. Li, Y. Qiao, and D. Psaltis, "Optical network for real-time face recognition," Appl. Opt. **32**, 5026–5035 (1993).
2. P. Refregier and B. Javidi, "Optical image encryption using input and Fourier plane random phase encoding," Opt. Lett. **20**, 767–769 (1995).
3. B. Javidi and T. Nomura, "Securing information by use of digital holography," Opt. Lett. **25**, 28–30 (2000).
4. T. Nomura and B. Javidi, "Optical encryption system with a binary key code," Appl. Opt. **39**, 4783–4787 (2000).
5. E. Tajahuerce, O. Matoba, S. C. Verrall, and B. Javidi, "Optoelectronic information encryption with phase-shifting interferometry," Appl. Opt. **39**, 2313–2320 (2000).
6. E. Tajahuerce and B. Javidi, "Encrypting three-dimensional information with digital holography," Appl. Opt. **39**, 6595–6601 (2000).
7. G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain," Opt. Lett. **25**, 887–889 (2000).
8. B. Wang, C. Sun, W. Su, and A. E. T. Chiou, "Shift tolerance of a double random phase encryption system," Appl. Opt. **39**, 4788–4793 (2000).
9. J. F. Heanue, M. C. Bashaw, and L. Hesselink, "Encrypted holographic data storage based on orthogonal-phase-code multiplexing," Appl. Opt. **34**, 6012–6015 (1995).
10. F. H. Mok, "Angle-multiplexed storage of 5000 holograms in lithium niobate," Opt. Lett. **18**, 915–917 (1993).
11. O. Matoba and B. Javidi, "Encrypted optical storage with wavelength-key and random phase codes," Appl. Opt. **38**, 6785–6790 (1999).
12. X. Tan, O. Matoba, T. Shimura, K. Kuroda, and B. Javidi, "Secure optical storage that uses fully phase encryption," Appl. Opt. **39**, 6689–6694 (2000).
13. B. M. Hennelly and J. B. Sheridan, "Image encryption and the fractional Fourier transform," Optik (Jena) **114**, 251–265 (2003).
14. G. Situ and J. Zhang, "Double random-phase encoding in the Fresnel domain," Opt. Lett. **29**, 1584–1586 (2004).
15. B. M. Hennelly and J. T. Sheridan, "Random phase and jigsaw encryption in the Fresnel domain," Opt. Eng. **43**, 2239–2249 (2004).
16. T. Nomura and B. Javidi, "Optical encryption using a joint transform correlator architecture," Opt. Eng. **39**, 2031–2035 (2000).
17. J. F. Barrera, R. Henao, M. Tebaldi, N. Bolognini, and R. Torroba, "Multiplexing encryption-decryption via lateral shifting of a random phase mask," Opt. Commun. **259**, 532–536 (2006).
18. J. F. Barrera, R. Henao, M. Tebaldi, N. Bolognini, and R. Torroba, "Multiplexing encrypted data by using polarized light," Opt. Commun. **260**, 109–112 (2006).
19. J. F. Barrera, R. Henao, M. Tebaldi, N. Bolognini, and R. Torroba, "Multiple image encryption using an aperture-modulated optical system," Opt. Commun. **261**, 29–33 (2006).
20. J. F. Barrera, R. Henao, M. Tebaldi, R. Torroba, and N. Bolognini, "Code retrieval via undercover multiplexing," Optik (Jena) **119**, 139–142 (2008).
21. G. Situ and J. Zhang, "Multiple-image encryption by wavelength multiplexing," Opt. Lett. **30**, 1306–1308 (2005).