Optics Communications 284 (2011) 4321–4326

Contents lists available at ScienceDirect

Optics Communications

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

Three-dimensional key in a modified joint transform correlator encryption scheme

E. Rueda [a], M. Tebaldi [b,*], R. Torroba [b], N. Bolognini [b,c]

[a] Grupo de Óptica y Fotónica, Instituto de Física, Universidad de Antioquia, Medellín, Colombia
[b] Centro de Investigaciones Ópticas (CONICET La Plata-CIC) and UID OPTIMO, Facultad de Ingeniería, Universidad Nacional de La Plata, La Plata, Argentina. P.O. Box 3, La Plata (1897), Argentina
[c] Facultad de Ciencias Exactas Universidad Nacional de La Plata, La Plata, Argentina

ARTICLE INFO

Article history:
Received 26 November 2010
Received in revised form 25 February 2011
Accepted 2 May 2011
Available online 18 May 2011

Keywords:
Encryption
JTC architecture
Multiplexing

ABSTRACT

We propose a modified encryption joint transform correlator scheme that introduces an additional random phase mask. The positions of both the conventional and the new mask are crucial for successful recovery of the original data. Although the two random phase masks are 2D, variation of their relative distance constitutes an additional dimension. Consequently by including this notion, both random phase masks act as a 3-dimensional (3D) key code increasing thereby the security with respect to the conventional JTC encryption scheme. We employ this scheme to multiplex encrypted data, displacing the encoding masks. During decryption of the multiplexed information, we only reconstruct the object that matches the correct predetermined 3D key code, i.e. that matches the random masks positions in the encryption step. We present actual experimental results, by using BSO crystal as recording medium, as well as their respective analysis.

1. Introduction

Encryption techniques imply that we cannot recover the original input image without employing the respective encoding mask, which cannot be inferred by unauthorized users. Conventional optical image-encryption methods are based on the 4-*f* correlator architecture that uses two random phase masks [1–3]. In the mentioned scheme, the optical and geometrical parameters must be precisely known in order to successfully recover the input data [4,5]. Consequently, the key code mask without those parameters cannot be used to access the encrypted data. Unsuccessful recovering shows nothing but noise. Experimental version of this setup was implemented with photorefractive crystals as storing medium [6–8].

Optical encoding techniques are not restricted to a 4f scheme. It is well known that the joint transform correlator (JTC) produces a similar but not identical output function to the 4f correlator. In a JTC configuration, 2-dimensional (2D) input data and key code can be placed side by side at the input plane. Many contributions on the random phase encoding technique for security verification show that the JTC can be successfully applied [9–14]. Moreover, the joint power spectrum (JPS) can be eventually recorded in a volume photorefractive intensity sensitive crystal. In the decryption step, after an inverse Fourier transform (FT) of the JPS, which is illuminated by the FT of the key code mask, the input image is correctly recovered. This architecture does not need to generate a conjugate beam, but it is affected from autocorrelation terms that appear in the output plane causing extra noise.

Multiplexing techniques are based on encoding two or more input images and adding them into a single recording medium. Different methods have been proposed to multiplex in a 4f architecture, based on shifting the random phase mask (RPM) [15], the use of a sandwich diffuser in the Fourier plane [16], the use of multiple apertures [17], and the change in the polarization state [7] or the wavelength [18]. A conventional way to reduce cross-talk between multiplexed images in a 4f scheme is to introduce an appropriate shifting in the encoding mask [19]. In the conventional JTC architecture when a plane-recording medium is considered, the JPS is insensitive to in-plane displacements of the RPM. In fact, it means that a constant phase factor is introduced by the displacement and therefore the JPS does not change. In order to introduce in the JTC scheme an approach similar to the in-plane shifting of the 4f Fourier-plane phase mask, the in-plane invariance needs to be broken. To overcome this problem, a modified setup that allows its use under a multiplexing approach was presented [13]. Instead of placing the encrypting mask in contact with the input JTC plane, the actual optical FT of a diffuser is projected over the input plane of the JTC. Once the invariance is resolved, an in-plane shifting of the encrypting mask achieves multiplexing.

The idea behind the last proposal consists in replacing the beam illuminating the conventional JTC double aperture by a structured illumination. In the present contribution, this structured wave front is obtained by introducing an additional RPM in the beam path, instead of a projected image onto the JTC input plane. As the two RPM are 2D, the variation of their relative distance can be considered as an additional dimension, thereby raising the total scheme to a 3D encoding method. This alternative scheme also breaks the mentioned

* Corresponding author. Tel.: +54 221 4840280; fax: +54 221 4712771.
E-mail address: myrianc@ciop.unlp.edu.ar (M. Tebaldi).

0030-4018/$ – see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.optcom.2011.05.014

JTC invariance. To understand the behavior, we investigate the effect of 3D displacements of the RPMs diffusers. The decrypted images indicate that the quality of the recovered images becomes poorer when displacing the encoding masks. In order to determine the experimental shift tolerance of the decrypted arrangement, we have laterally and axially moved each RPM up to the position where the decoded data disappeared. Accordingly, the diffuser displacement limit is based on the non-retrieval of the image. In this frame, mean square error (MSE) values of reconstructed vs. original data have been evaluated as a function of the RPM´s displacements.

The use of the additional RPM enhances the security of the JTC system. In this sense, an intruder requires additional information on the structure and relative positioning of the space-invariant breaking mask.

If two images are encrypted and multiplexed by using the additional RPM in the same 3D position, the decrypted image shows simultaneously both input data. The additional mask allows avoiding the cross-talk of multiple images at the time of decryption by shifting the encoding RPM in the JTC scheme. We experimentally demonstrate multiple encryptions based on shifting this additional RPM.

2. Description of the method and results

In the conventional JTC scheme, two statistical independent RPMs are placed side by side forming a double aperture in the input plane. One of them is attached to the input object (M_O) and the other serves as encoding mask (M_E). In our proposal, we replace the conventional plane wave illumination by introducing an additional random phase mask (M_A) in the path of a divergent beam. Thus, the JTC double aperture arrangement is illuminated by a structured pattern generated by the additional random diffuser located at a distance Z from the JTC input plane and a distance D from the microscope objective lens. A FT of the double aperture plane, which is the JPS, is stored in an intensity sensitive recording medium. This spectrum can be regarded as the encrypted data because it exhibits a wide sense white noise distributed over the frequency domain. All random phase masks are generated by a white sequence of phase that is uniformly distributed on the interval [0, 2π], have unit amplitude transmittance, and are statistically independent to each other.

Fig. 1 depicts the proposed encryption–decryption optical scheme. Let us study our proposal on an experimental basis. We use as intensity sensitive medium a photorefractive BSO crystal cut in the transverse electro-optic configuration. In accordance with the crystal sensitivity a 100 mW mini YAG laser ($\lambda = 532$ nm) is used. The encrypted JPS is stored into the photorefractive crystal as a volume hologram. The JPS is fringe modulated and the fringes are orthogonal to the line joining the JTC apertures. In this case, we must consider the particular storage-read-out behavior for low frequency modulated patterns [20,21]. The intensity distribution received by the crystal is encoded as the spatial distribution of the resulting electric field strength at each point. This field induces an index grating system through the linear electro-optic effect the crystal exhibits, which represents the JPS.

In the decryption step, a shutter cancels the object aperture in the JTC plane in such a way that the FT of the decoding masks M_E illuminated by M_A is incident onto the photorefractive crystal (see Fig. 1b)). Then, the BSO crystal diffracted light is collected at the back focal plane of the lens L_2. A low power beam must be used to reduce the photorefractive stored gratings erasure and a consequent decrease in the diffraction efficiency. Perfect recovery requires both key masks (M_E and M_A) to strictly coincide with those employed in the encryption step, thus they must be exactly positioned. Moreover, the same encryption read-out wavelength and polarization state must be used to decrypt the data. In the following, we analyze the system behavior in terms of each key mask 2-dimensional displacements that take place in the diffuser planes and those produced along the optical

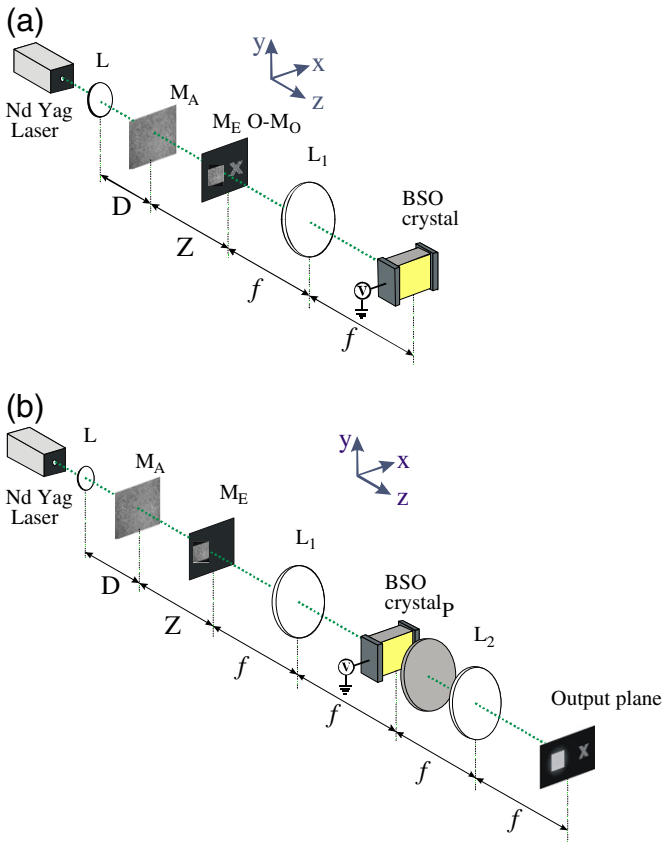

Fig. 1. Experimental modified JTC setup. a) Encryption step and b) decryption step (L: microscope objective lens that generates the divergent beam, M_A: additional random phase mask, O: input object, M_E: JTC encryption mask, M_O: random mask attached to the input object; L_1 and L_2: Fourier transform lens with focal length *f*; P: polarizer; D: distance between L and M_A; Z: distance between M_A and JTC double aperture plane).

axis direction. In order to determine the experimental shift tolerance of the decryption mask we have laterally and axially moved each RPM up to the position where the decoded data disappeared. It means that the diffuser displacement limit (threshold) is based on the non-retrieval of the image.

Let us consider a point source represented by a divergent laser beam positioned a distance D from M_A. The incident beam onto M_A generates a spot of radius R. The light forward scattered from this diffuser impinges onto the JTC plane where both apertures are located.

In order to analyze the proposed scheme, the MSE between the input data and the decrypted data under diffuser displacements is evaluated. Both RPMs must be used to retrieve the stored images; which are regarded as the key codes. Each diffuser is placed on a micro-translation stage. During the decryption process, we displace M_E and M_A and observe the decrypted data with a CCD camera. As usual the positions of the RPM are kept fixed before encrypting the inputs. At this point we want to introduce a comment about the sign of the displacement along the three axes. In our experiments, we always move mask M_A towards the JTC input plane. Obviously the inverse displacement does not produce the same decrypting behavior because of the divergent illuminating beam. On the other hand, in-plane displacements of diffuser M_A are symmetric with respect to the optical axis. This symmetry is confirmed throughout our experimental results. Therefore, it is irrelevant to address the sign of the X and Y displacement. The reconstructed decrypted outputs are used to determine the experimental MSE curves. We will analyze separately the effect of the RPMs displacements over three different directions (in-plane and axial) on the final decryption results.

The MSE curves of Fig. 2a) and b) correspond to an X-direction displacement of M_A and M_E, respectively. In this case, a divergent beam generated by a 16 mm focal length objective microscope is employed. The decrypted image behavior under RPM shifting is evaluated for different distances between M_E and M_A (Z = 28.5 cm, Z = 21 cm and Z = 16 cm where Z is the distance between M_A and the JTC double aperture plane) while the laser source is kept fixed. The experimental results of Fig. 2 indicate that when the diffuser M_E is displaced in X-direction by an amount of ± 15 μm corresponding to MSE = 0.8, the reconstructed beam is unable to decode the encrypted data stored in the crystal as can be confirmed by observing Fig. 3(b). This figure shows the decrypted image obtained with a 15 μm X-direction displacement of the diffuser M_A while the M_E matches the encrypted key position. This result corresponds to Z = 16 cm and the same write-in parameters as Fig. 2. The same system sensitivity is also observed by in-plane displacing the diffuser M_A in X-direction. Therefore, for 16 mm focal length objective microscope, the results of Fig. 2a) and b) show that no matter which mask is laterally displaced the system is unable to decrypt the image.

Remembering that the transversal speckle average dimensions onto the JTC plane are [22]:

$$\langle S_x \rangle = \langle S_y \rangle \approx \frac{\lambda Z}{R} \tag{1}$$

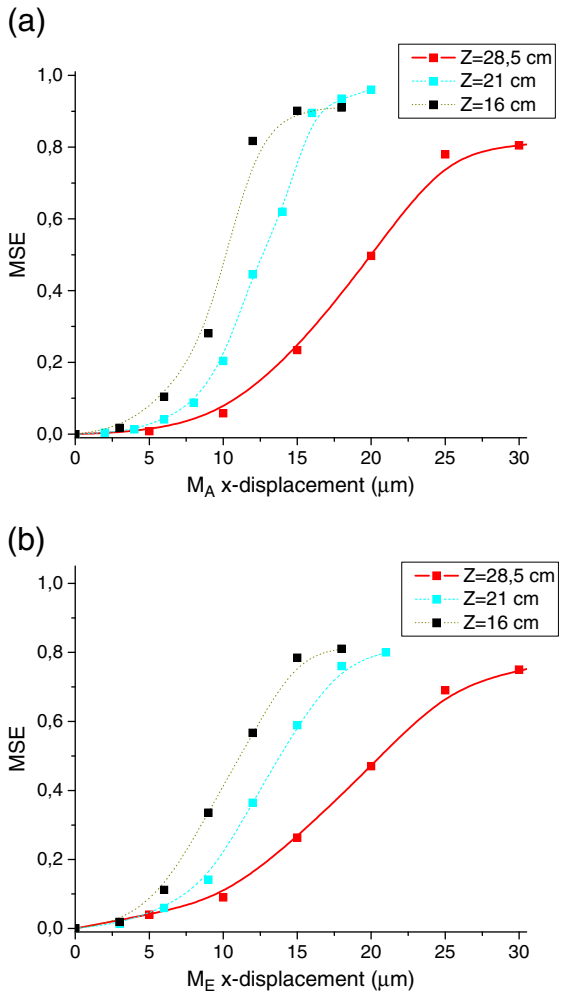

Fig. 2. MSE in terms of the x-direction displacement of: (a) the diffuser M_A and (b) the diffuser M_E, respectively. The write-in wavelength is 532 nm, the diffuser roughness is 30 μm and the microscope objective focal length is 16 mm.

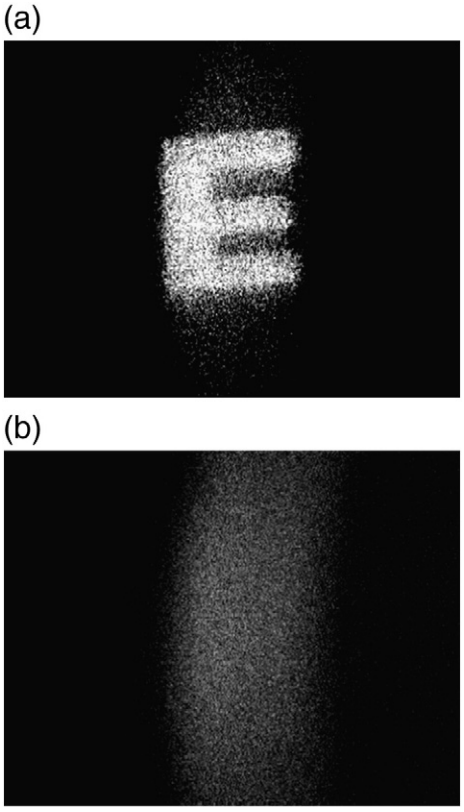

Fig. 3. Decrypted images obtained with: (a) both diffusers matching the corresponding encrypted keys positions (b) results from a 15 μm X-direction displacement of the diffuser M_A and the M_E matching the encrypted key position. The write-in wavelength is 532 nm, the diffuser roughness is 30 μm and the microscope objective focal length is 16 mm and Z = 16 mm.

and the longitudinal speckle average dimension is [22]:

$$\langle S_z \rangle \approx \lambda \left(\frac{Z}{R}\right)^2 \tag{2}$$

Note that the average transversal speckle size (Eq. (1)) in the JTC plane can be rewrite as:

$$\langle S_x \rangle \approx \frac{\lambda}{tg(\alpha)}\left(\frac{Z}{D}\right) = \frac{\lambda}{tg(\alpha)}\left(\frac{Z}{cte - Z}\right) \tag{3}$$

where α indicates the beam divergence, and in our experimental condition is imposed by Z + D = *constant*. It is evident that as Z decreases and R increases the average values diminish.

Note that when Z decreases, Z/D decreases as well, and therefore the situation where Z = 16 cm is more sensitive to decryption failures under diffusers shifting in comparison with Z = 28.5 cm and Z = 21 cm, respectively. This behavior agrees with the results displayed in Fig. 2.

In the case of Fig. 2, due to the large focal length of the microscope objective, the divergence angle α is very small (approximately 1 degree). The transversal X-direction displacement of M_A produces an equivalent transversal displacement of the speckle distribution formed at the JTC input plane. Therefore, when M_E is transversally displaced and M_A is kept fixed, the situation is similar to that obtained when M_A is displaced and M_E is fixed. Note that this result would have been obtained in the case where a plane wave would have been employed to illuminate M_A.

The MSE curves of Fig. 4a) and b) correspond to the case when a 4 mm focal length objective microscope generates the incident

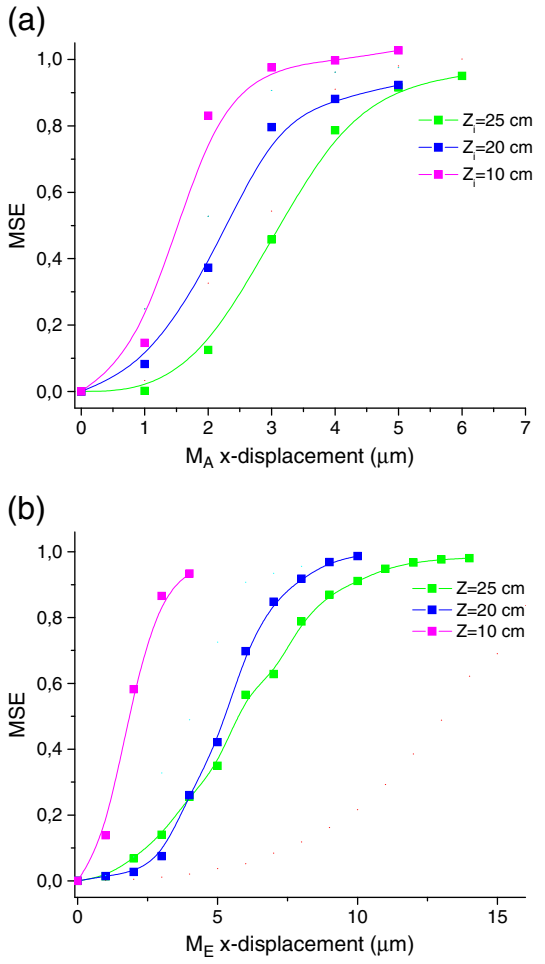

Fig. 4. MSE in terms of the X-direction displacement of: (a) the diffuser M_A and (b) the diffuser M_E, respectively. The write-in wavelength is 532 nm, the diffuser roughness is 30 μm, and the microscope objective focal length is 4 mm.

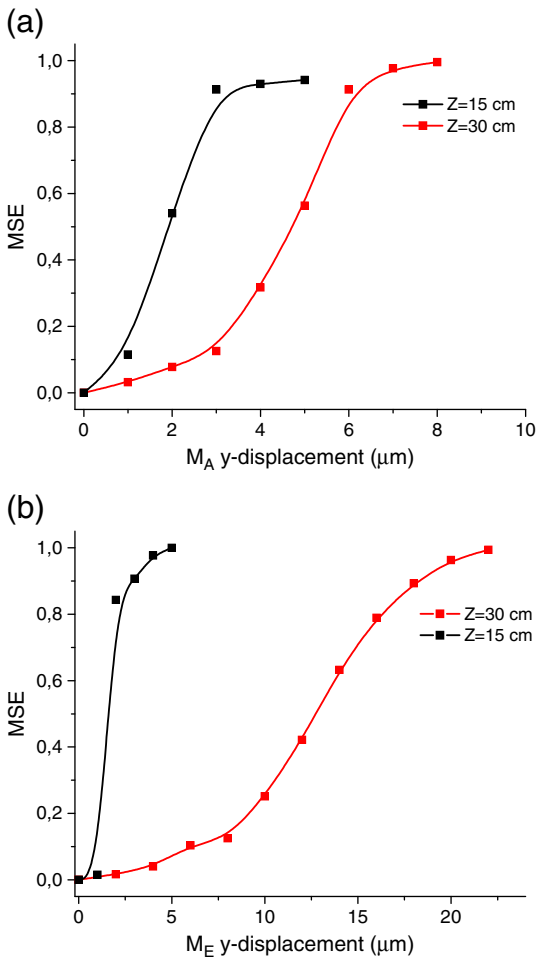

Fig. 5. MSE in terms of the Y-direction displacement of: (a) the diffuser M_A and (b) the diffuser M_E, respectively. The write-in wavelength is 532 nm, the diffuser roughness is 30 μm and the microscope objective focal length is 4 mm.

divergent beam. The decrypted image behavior when the random mask moves, in X-direction, is evaluated for different distances between M_E and M_A (Z = 25 cm, Z = 20 cm and Z = 10 cm) while the laser source is fixed. The angle α (~7°) is higher in this case than in the case of Fig. 2. Therefore, a transversal displacement of M_A changes the speckle distribution that impinges on the JTC plane faster than with α = 1°, and the decorrelation increases as well. In this situation, moving M_E while M_A remains fixed is not equivalent to msove M_A while M_E is fixed. In Fig. 4b) the speckle distribution incident on the M_E diffuser does not change significantly and the correlation is kept along a larger distance.

As it is expected, the transversal displacement along the Y-axis shows an equivalent behavior to that obtained by the X-direction displacement, and this result is experimentally confirmed. Fig. 5a) and b) corresponds to the MSE curves when we introduce a transversal Y-direction displacement of M_A and M_E, respectively. In this case, a divergent beam generated by a 4 mm focal length objective microscope is employed. The decrypted output behavior when the mask moves is evaluated for different distances between M_A and M_E (Z = 30 cm and Z = 15 cm), while the laser source is fixed.

Finally, as it is shown in Figs. 6 and 7 the system is tested when displacing along Z-axis. Practical limitations of the involved mechanical parts in the optical setup did not allow implementing the same Z-displacements for the M_A and M_E. This situation is observed in Figs. 6 and 7. Note that the longitudinal speckle average dimensions are longer than the speckle average transversal dimensions (see Eqs. (1) and (2)). As it is expected, a greater mask displacement along Z-axis is tolerated in comparison with X-axis and Y-axis displacements, in order to decrypt the information. This behavior is revealed when comparing the curves for Z = 15 cm of Fig. 5a) and Fig. 6.

A correct input recovering depends on the sharpness correlation degree between both speckle distributions. Therefore, it seems appropriate to use a speckle correlation-length analysis to determine

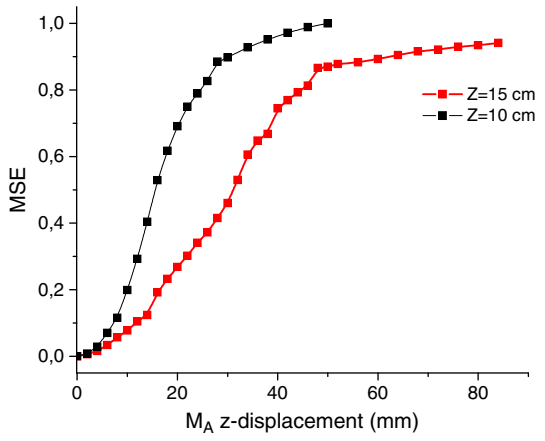

Fig. 6. MSE in terms of the Z-direction displacement of the diffuser M_A. The write-in wavelength is 532 nm, the diffuser roughness is 30 μm and the microscope objective focal length is 4 mm.

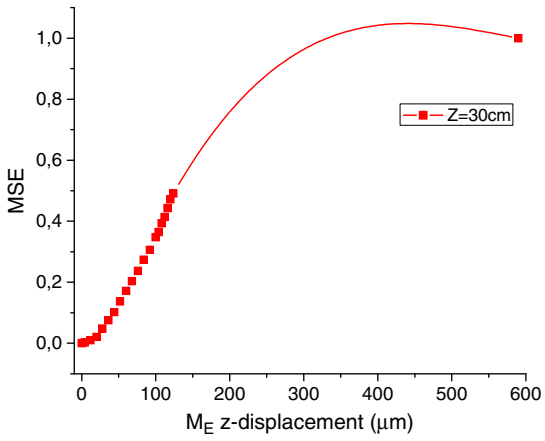

Fig. 7. MSE in terms of the Z-direction displacement of the diffuser M_E. The write-in wavelength is 532 nm, the diffuser roughness is 30 μm and the microscope objective focal length is 4 mm.

the system sensitivity in terms of the displacement of both masks. We show that the behavior observed in the MSE curves coincide with that shown in the correlation curves and therefore only the MSE curves are presented.

As it is well known for the conventional JTC architecture, when we consider a plane-recording medium, the encrypted data are invariant under in-plane translations of the encoding mask due to the FT properties. On the other hand, if a volume-recording medium is employed, when the mask translates the invariance property does not hold. However, it is necessary to introduce a larger random mask displacement to observe this effect in the conventional JTC encryption scheme. In our proposal, the introduction of an additional mask M_A turns the system space variant under very small diffuser translations. Therefore, when a photorefractive volume crystal is used as storage medium, these random mask translations influence on the encryption–decryption procedure. Nevertheless, the influence produced by the structured illumination is more important than the effect introduced by the volume medium. Therefore, we focus the attention in the former case.

As verified above, the introduction of the additional key code mask in the JTC architecture makes the system variant under small translations of either M_E or M_A. As it is expected by considering the speckle dimensions, this modified scheme tolerates, in the decryption procedure, a greater mask displacement along Z-axis in comparison with X-axis and Y-axis displacements without affecting the image decryption. This analysis allows encrypting–decrypting multiplexed images without cross-talk, and the experimental results reveal the feasibility of the proposed system.

This idea is useful in a multiplexing scheme to encrypt several input data, providing that different random phase mask positions be introduced. In the proposed scheme, the cross-talk problem may arise from the encrypting masks position range as pointed out in the above discussion. Obviously, if two images are encrypted by using the random masks in the same positions and then multiplexing both data on the same medium, the decrypted image shows simultaneously both inputs. By changing the position of M_E or M_A between successive recordings, it allows multiplexing the encrypted images and decrypting them separately. This means that the position mask threshold must be kept between the successive encrypting data.

Summarizing, the proposed technique allows one to implement a multiplexing operation. The introduction of the key code mask M_A in the JTC architecture makes the system space variant under lateral and axial translation of either M_E or M_A. This feature is used to store multiple data.

In the experimental conditions we have, if any of the masks is displaced along X-axis or Y-axis by 15 μm from its original position, the recovered image completely disappears.

The photorefractive-material stores the multiple JPS generated by shifting M_E or M_A. The experimental procedure we present consists in four exposures where the random mask position is modified between exposures. The multiplexing technique has been investigated by using binary characters as input images. In each exposure, the key mask is shifted in X-axis, Y-axis and Z-axis direction with a precision translation stage. It is interesting to remark that we need only to translate 20 μm along X and Y directions, but to get the next multiplexed image in Z-direction we need to translate 80 μm. To achieve diffraction efficiencies comparable in the different exposures, we take into account the recording-erasure response of the crystal. Then, the time is changed in each exposure in order to obtain efficiencies comparable in all decrypted data. The results are displayed in Fig. 8.

We have to highlight that the threshold values for the masks 3D position depend on the masks and on the setup geometrical parameters. The findings in the present contribution were obtained for a particular random phase masks employed during our experimental analysis. As a rule, one has to analyze the MSE curve for each particular case.

3. Conclusions

In the proposed modified JTC architecture, the introduction of another mask, which acts as an encoding key in addition to the JTC usual mask, reinforces the system security. In this JTC arrangement, both random masks have an equivalent security hierarchical level. Therefore, in the decryption step when any of the masks is located at an incorrect position, the input data cannot be recovered and only noise appears at the JTC output plane. In this case, not only the phase information but also the positions of the masks must be known. We stress that both RPM are 2D, but we consider the variation of their relative distance as an additional dimension and this leads to what we call a 3D encrypting key.

The mentioned encoding key can be use to multiplex encrypted data. The use of this additional random mask allows the multiplexing capability and increase the security of the system. It should be pointed out that the masks position, the distance between masks, and the laser divergence can be adjusted to optimize the amount of information to be multiplexed.

As already recognized, the use of a diffuser provides high security because diffusers are extremely difficult to be replicated. Consequently, the use of two mask diffusers increases even more the eavesdropper task.

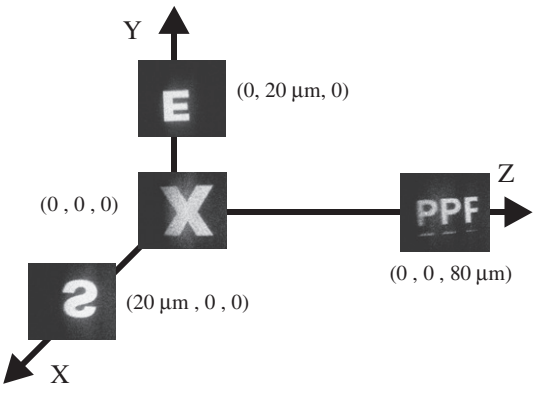

Fig. 8. Decrypted multiplexed images. The image "X" is obtained with the diffuser M_E and M_A matching the corresponding encrypted keys position defining the position (0 μm, 0 μm, 0 μm). Accordingly, the image "S" is obtained by displacing the diffuser M_A (20 μm, 0 μm, 0 μm), the image "E" is obtained by displacing the diffuser M_A (0 μm, 20 μm, 0 μm) while the image "PPF" is obtained by displacing the diffuser M_A (0 μm, 0 μm, 80 μm). The write-in wavelength is 532 nm, the diffuser roughness is 30 μm and the microscope objective focal length is 4 mm.

In summary, the advantages of the proposed optical security system include:

a) The security level is increased since more than one key is employed.
b) Multiplexing encryption capability is introduced with the generation of multiple keys, by simply modifying the structured illumination incident on the input plane mask.

In the classical 4f encryption method, the restriction in image decryption is imposed by the precise random phase mask repositioning. On the other hand, the conventional JTC encryption scheme is invariant under in-plane translation of the random phase mask. In our proposal, we break the detailed invariance giving another security step to the encrypting scheme. In this way, this weakness in the JTC architecture is strengthened. Nevertheless the same restriction regarding phase mask repositioning still remains as in the classical 4f encoding scheme.

Acknowledgments

This research was performed under grants COLCIENCIAS (Colombia), CODI—Universidad de Antioquia (Colombia), CONICET No. 112-200801-00863 (Argentina), ANCYT PICT1167 (Argentina), bilateral project CO/08/16 between MINCYT (Argentina) and COLCIENCIAS (Colombia), and Facultad de Ingeniería, Universidad Nacional de La Plata No. 11/I125 (Argentina).

References

[1] P. Réfrégier, B. Javidi, Opt. Lett. 20 (1995) 767.
[2] D. Amaya, M. Tebaldi, R. Torroba, N. Bolognini, Opt. Commun. 281 (2008) 3434.
[3] G. Unnikrishnan, J. Joseph, K. Singh, Opt. Lett. 25 (2000) 887.
[4] Sun Ching-Cherng, Su Wei-Chia, Wang Bor, A.E.T. Chiou, Opt. Commun. 191 (2001) 209.
[5] O. Matoba, B. Javidi, Appl. Opt. 38 (1999) 6785.
[6] J.F. Barrera, R. Henao, M. Tebaldi, R. Torroba, N. Bolognini, Optik 119 (2008) 139.
[7] J.F. Barrera, R. Henao, M. Tebaldi, N. Bolognini, R. Torroba, Opt. Commun. 260 (2006) 109.
[8] G. Unnikrishnan, J. Joseph, K. Singh, Appl. Opt. 37 (1998) 8181.
[9] T. Nomura, B. Javidi, Opt. Eng. 39 (2000) 2031.
[10] M. Tebaldi, W.D. Furlan, R. Torroba, N. Bolognini, Opt. Lett. 34 (2009) 316.
[11] D. Amaya, M. Tebaldi, R. Torroba, N. Bolognini, Appl. Opt. 48 (2009) 2099.
[12] E. Rueda, J.F. Barrera, R. Henao, R. Torroba, Opt. Commun. 282 (2009) 3243.
[13] E. Rueda, J.F. Barrera, R. Henao, R. Torroba, Opt. Eng. 48 (2009) 027006.
[14] D. Amaya, M. Tebaldi, R. Torroba, N. Bolognini, Appl. Opt. 47 (2008) 5903.
[15] W.-C. Su, C.-H. Lin, Opt. Commun. 241 (2004) 29.
[16] M. Singh, A. Kumar, K. Singh, Optics & Laser Technology 41 (2009) 32.
[17] J.F. Barrera, R. Henao, M. Tebaldi, N. Bolognini, R. Torroba, Opt. Commun. 261 (2006) 29.
[18] G. Situ, J. Zhang, Opt. Lett. 30 (2005) 1306.
[19] J.F. Barrera, R. Henao, M. Tebaldi, N. Bolognini, R. Torroba, Opt. Commun. 259 (2006) 532.
[20] M. Tebaldi, L. Angel Toro, M.C. Lasprilla, N. Bolognini, Opt. Commun. 155 (1998) 342.
[21] M. Tebaldi, A. Lencina, N. Bolognini, Opt. Commun. 202 (2002) 257.
[22] J.M. Goodman, Statistical properties of laser speckle pattern, in: J.C. Dainty (Ed.), Laser Speckle and Related Phenomena, Springer-Verlag, New York, 1975.