Multi-user multiplexed scheme for decoding modulated-encoded sequential information

Fabian Mosso[a], Myrian Tebaldi[a,*], John Fredy Barrera[c], Néstor Bolognini[a,b] and Roberto Torroba[a]

[a]Centro de Investigaciones Ópticas (CONICET La Plata-CIC) and UID OPTIMO, Facultad de Ingeniería, Universidad Nacional de La Plata, P.O. Box 3 C.P 1897, La Plata, Argentina
[b]Facultad de Ciencias Exactas, Universidad Nacional de La Plata
[c]Grupo de Óptica y Fotónica, Instituto de Física, Universidad de Antioquia, A.A 1226 Medellín, Colombia.

ABSTRACT

Encrypting procedures with multiplexed operations exhibit an inherent noise. We presented options to avoid background noise arising from the non-decoded images. We have a coding mask corresponding to each single input object, thus resulting in a static decrypting mechanism. Besides, if we manage the spatial destination of each decoded output, then we avoid the noise superposition. In those schemes, the displaying output order was irrelevant. However, when we face a sequence of events including multi-users, we need to develop another strategy. We present a multi-user encrypting scheme with a single encoding mask that removes the background noise, also showing the decrypted data in a prescribed sequence. The multiplexing scheme is based on the 4f double random phase encryption architecture and a theta modulation method, which consists in superposing each encrypted information with a determined sinusoidal grating. Afterwards we proceed to the completely encoded data multiplexing. In a multi-user scheme, we employ different encrypting masks in the 4f optical setup for each user, and the same mask is employed for the user sequence. We store the encrypted data in the single medium. After a Fourier transform operation and an appropriate filtering procedure, we reach the sequence of isolated encrypted spots corresponding to the right user. With the aid of the pertaining decoding mask, the user can decrypt the sequence. We avoid the noise by the appropriate choice of the modulating gratings pitch as to elude the overlapping of spots at the Fourier plane, which is the cause of information degradation.

Keywords: Optical encryption, optical security, multiplexing, speckle

1. INTRODUCTION

Optical encryption is a way to transform original information to an unreadable format. The input information is converted into white noise via, for instance, a double random phase encryption protocol. The information transformed via the encoding process is called an optical encrypted image. The original image is reconstructed from the encoded result using a reversing or decryption process. The mentioned double random phase encryption is based on the 4*f* architecture [1, 2]. In this scheme, the encrypted image and the encoding mask play the main role in order to retrieve the input information. Note that, it is necessary to known exactly the optical parameters (polarization, wavelengths, pupil aperture, etc) to correctly decrypt the data. In fact, these parameters act as extra encoding keys [3-5].

It has been demonstrated that the system is insecure under some attack protocols [6, 7]. Then, researches have devoted efforts to find new alternatives to increment the security level [8]. Nevertheless, most of these schemes proposed to maintain their linearity properties still making them insecure. Trying to avoid the weakness it has been introduced the encryption multiplexing operation. There exist reports of different alternatives to achieve a multiplexing process: shifting the random pure-phase mask [9], changing the polarized state [3], and changing the pupil aperture between exposures [10], among others [11-12]. In addition, a multichannel puzzle-like encryption method consists in decomposing the input information and then encrypting them separately [13]. Another proposal exploits the relationship between both, amplitude and phase of an object, encrypting them in separate channels [14].

The importance of the multiplexing approach relays in the multiple data recording in a single medium. In the decryption procedure, the recovered wave front carries information associated to all encrypted data. The parameter employed as the

22nd Congress of the International Commission for Optics: Light for the Development of the World, edited by Ramón Rodríguez-Vera, Rufino Díaz-Uribe, Proc. of SPIE Vol. 8011, 801173
2011 SPIE · CCC code: 0277-786X/11/$18 · doi: 10.1117/12.902124

multiplexing key selects each input information by setting it in a determined state. Then the decrypting procedure reveals the right recovered data and the unavoidable background noise due to non-decrypted images. In principle, by using non-correlated key code masks, the number of images to be multiplexed could be very high. Nevertheless, the mentioned noise severely reduces the number of inputs to be encoded and multiplexed. Note that the optical parameters have a useful range to be utilized. Then, this range imposes a limit on how many images can be handled so that the remaining non-decoded ones do not pollute each decoded image.

The ideal method should enable to multiplex several encrypted data and selectively recover each one free of noise. Recently, we have proposed a new encryption multiplexing technique, which avoids the noise due to non-decrypted images [15]. Our procedure combines the theta modulation technique [16] and the conventional 4f architecture [1]. As it is well known, several techniques for image storing and subsequent retrieval have been proposed based upon the modulation of the input signal through a spatial frequency carrier. Furthermore, in several proposals, the carrier frequency is derived from an intensity speckle pattern, the advantage of which is to spread out the information in the Fourier plane. In this way, the signal spectrum can occupy an adequate dimension that allows processing it more easily. The introduction of a spatial frequency carrier through the modulation technique has been applied to optical information processing and metrology [17-20]. Our proposal consists in modulating each encrypted data with a different grating. Then a filtering procedure during decoding allows retrieving specific information and in turn eliminates the noise contribution of non-decrypted data. This technique brings the possibility to encrypt dynamic phenomena. Additionally, we have the advantage to extend the method to a multi-user encoding-decoding multiplexing scheme by including the possibility of using different multiplexed independent phenomena with different encoding keys. In order to recover the assigned phenomenon, the user must employ the assigned encoding key.

2. PROCEDURE

We propose a multi-user encoding-decoding multiplexed scheme for dynamic information storage. Each user is allowed to decode a different dynamic scene. The experimental encryption-decryption set-up is schematized in Figure 1 and Figure 2. The whole method can be segmented in four procedures: encryption step, the theta modulation-multiplexing and phase conjugation operation, filtering-synchronization and the decryption step.

The encryption of each frame F_i is carried out using the conventional 4*f* double random phase masks encoding architecture [1]. This operation must be sequentially carried out n times in order to decrypt all movie frames. The amplitude A_i for each input frame is given by:

$$A_i = F_i\, R \tag{1}$$

where F_i is the corresponding i^{th} frame amplitude and R is the first random phase mask. We use different encoding masks R'_a, R'_b and R'_c to encrypt the different dynamic event corresponding to each user. By multiplying the Fourier transform (FT) of each frame by the corresponding key code mask R'_a, R'_b and R'_c results in:

$$\Im[F_i\, R]\cdot R'_a \qquad \text{(where } i = 1\ldots10 \text{ and } F_i \text{ belongs to the first user`s sequence)} \tag{2}$$

$$\Im[F_i\, R]\cdot R'_b \qquad \text{(where } i = 11\ldots20 \text{ and } F_i \text{ belongs to the second user`s sequence)} \tag{3}$$

$$\Im[F_i\, R]\cdot R'_c \qquad \text{(where } i = 21\ldots30 \text{ and } F_i \text{ belongs to the third user`s sequence)} \tag{4}$$

Note that the mask R is used for every frame. However, R'_a, R'_b and R'_c are used to encrypt the first, second and third user`s sequence respectively. Each encrypted frame for the first user in the 4 *f* encrypting architecture is:

$$E_i = F_i\, R \otimes \Im[R'_a] \tag{5}$$

where $i = 1\ldots10$, $\otimes$ represents the convolution operation. An equivalent equation as Eq. (5) holds for the other users.
At this point, we modulate each encrypted frame E_i with a sinusoidal amplitude grating G_i which has a pitch d_i and a determined orientation. This grating pitch d_i fulfills $d_i << S_t$ where t S_t is the transversal average speckle size which in turn is inversely proportional to the output pupil size of the system. At this point the entire input frames belonging to each user are conveniently encrypted. Then, we proceed with the overall multiplexing and phase conjugation operation and we obtain:

$$M^* = \left(\sum_{i=1}^{30} E_i^* \, G_i \right) \tag{6}$$

Each user receives the complex conjugate encoding of the total multiplexed data set, together with the assigned encoding key. This procedure can be experimentally accomplished by storing each individual term of the above equation into a photorefractive crystal, or alternatively by adding into a single frame each captured term of Eq. (6).

As mentioned above, the decoding step involves two processes, the filtering-synchronization, and the decryption step. The filtering-synchronization procedure involves a FT of the multiplexed and phase conjugated encoded data. Then, after another FT (see the decryption set-up depicted in Fig. 2) it results:

$$\Im\left(M^*\right) = \Im\left(\sum_{i=1}^{30} E_i^* G_i^* \right) = \sum_{i=1}^{30} \left[\Im\left(E_i^*\right) \otimes \Im\left(G_i^*\right) \right] \tag{7}$$

As it is well known, the FT of the sinusoidal grating G_i gives rise to three terms one centered in the optical axis and the other two symmetrically located around the centered term. The location of these spots depends both on the grating orientation and on pitch, and the size depends on the parameters of the optical system. In our proposal, due to the theta modulation operation, the FT reveals paired spots belonging to each encrypted frame. We have to recall that we are storing 30 frames; therefore we are obtaining several diffracted spots as can be seen in the second image from the right in the scheme of Fig. 2 a). The spots pairs corresponding to different frames are located at non-common spatial positions. In the filtering process, the user filters out all but a given spot, in order to obtain, after a new FT, a single encrypted frame. By adequately selecting the filter position, we obtain from the i^{th} term of Eq. (7) only one diffracted spot associated to $\Im\left(E_i^*\right)$, extracted from the two corresponding spots symmetrically located around the center. In this way, the filtering process isolates each encrypted frame from the remaining encrypted information, thus avoiding noise. The filtering operation involves a synchronizing operation. Then, an inverse FT operation allows obtaining each conjugated encrypted frame E_i^*. Finally, we proceed for each encrypted pattern with the classical decrypting step for the 4*f* decrypting architecture. As described in Fig. 2 b), the decoding process requires another 4*f* scheme. At this step, for the first user, the conventional decrypting procedure allows recovering the frame F_i by Fourier transforming E_i^* and then multiplying by the first user key code mask R'_a:

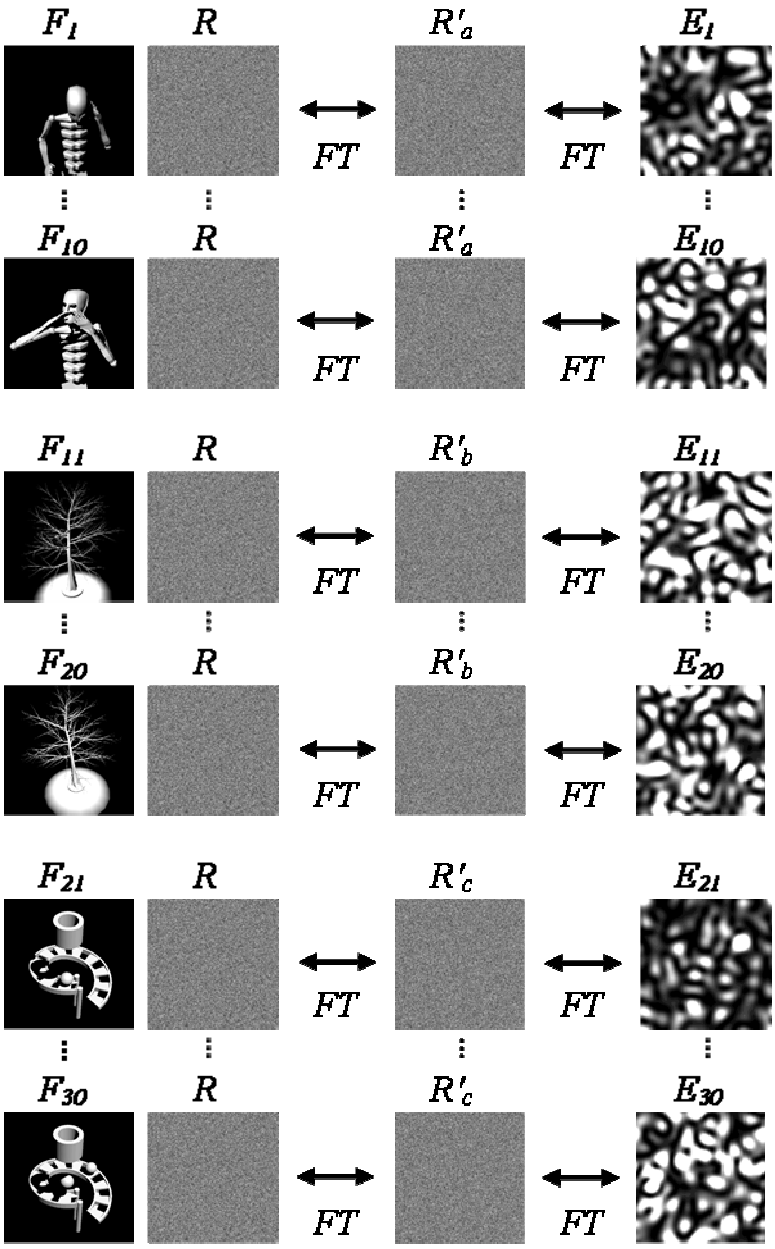
$$\Im\left(E^*_i\right) R'_a = \Im\left(F_i^* \, R^*\right) \left[R'^*_a \, R'_a \right] \tag{8}$$

and by Fourier transforming again its results:

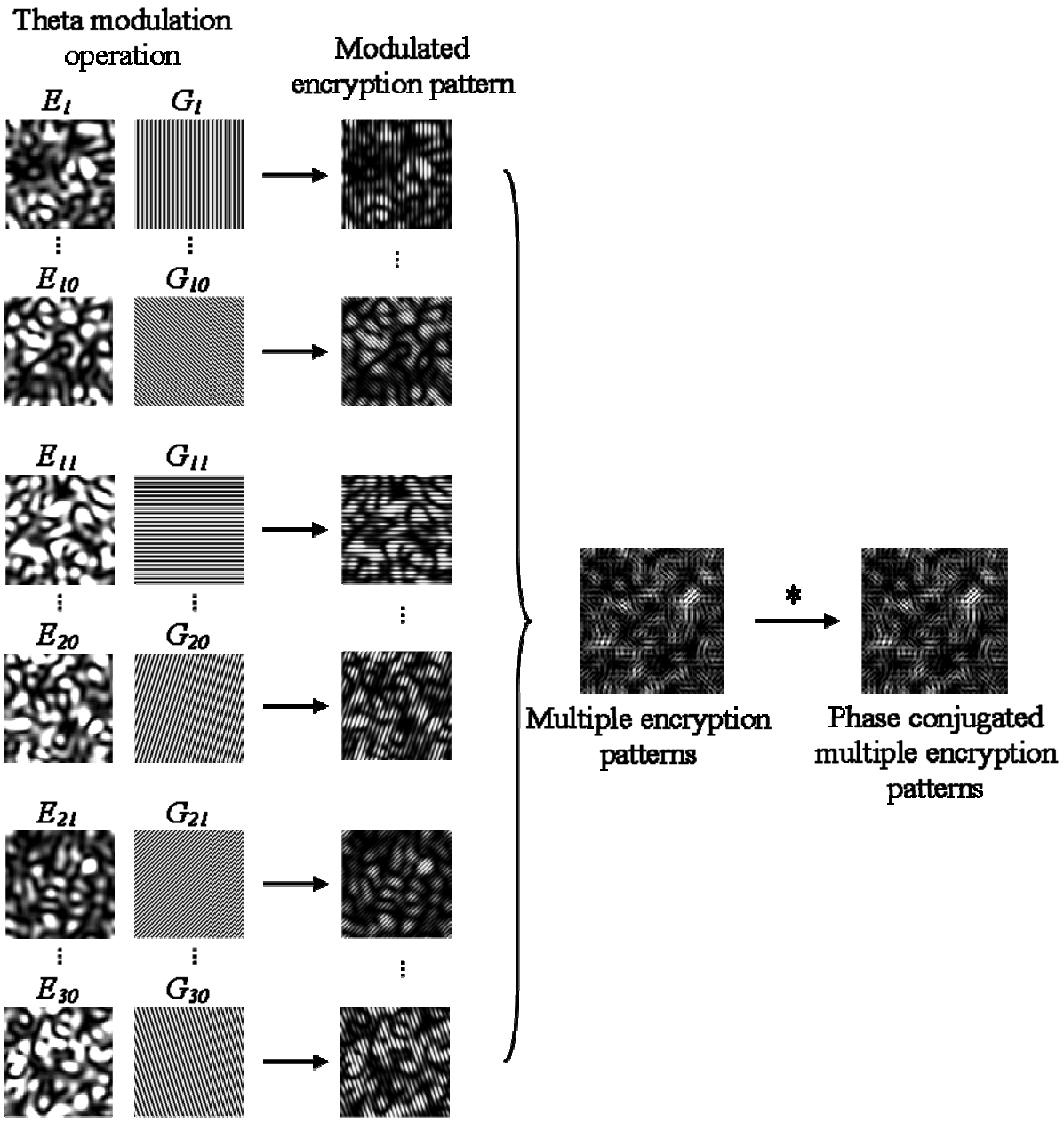
$$\Im\left[\Im\left(E^*_i\right) R'_a \right] = F_i^* \, R^* \tag{9}$$

It is interesting to remark that we display the movie in intensity form; therefore this intensity operation removes the phase mask R. Then, equivalent equations as (8) and (9) hold for the second and the third users.

The entire procedure leads to visualize each decrypted frame without the influence of the others. Thus, the dynamic scene is reconstructed. The encoding key for each user allows decrypting only the assigned information. The use of a determined key code mask and filtering-synchronizing procedure, allows recovering the information of the assigned dynamic sequence.

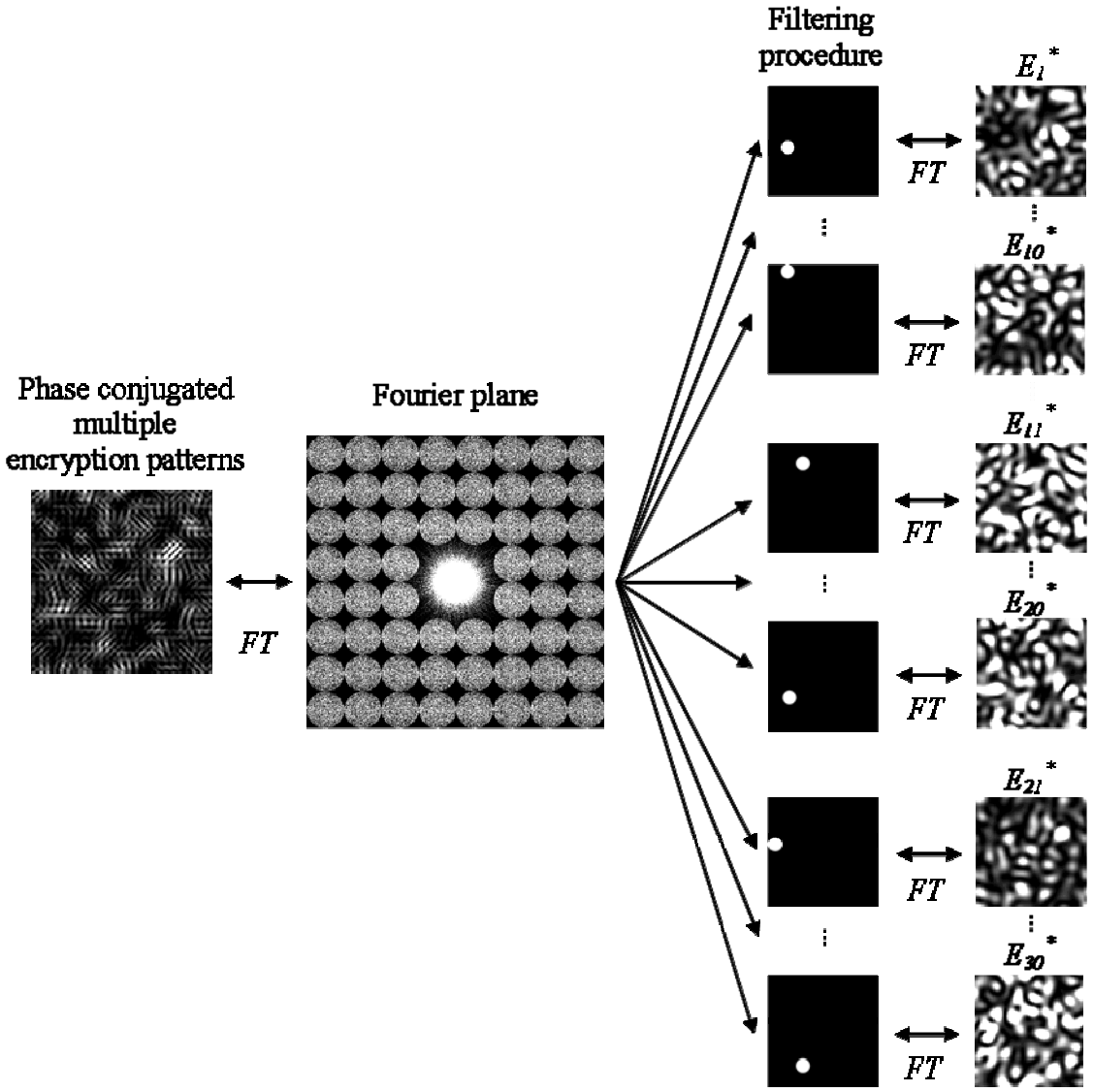


(a)

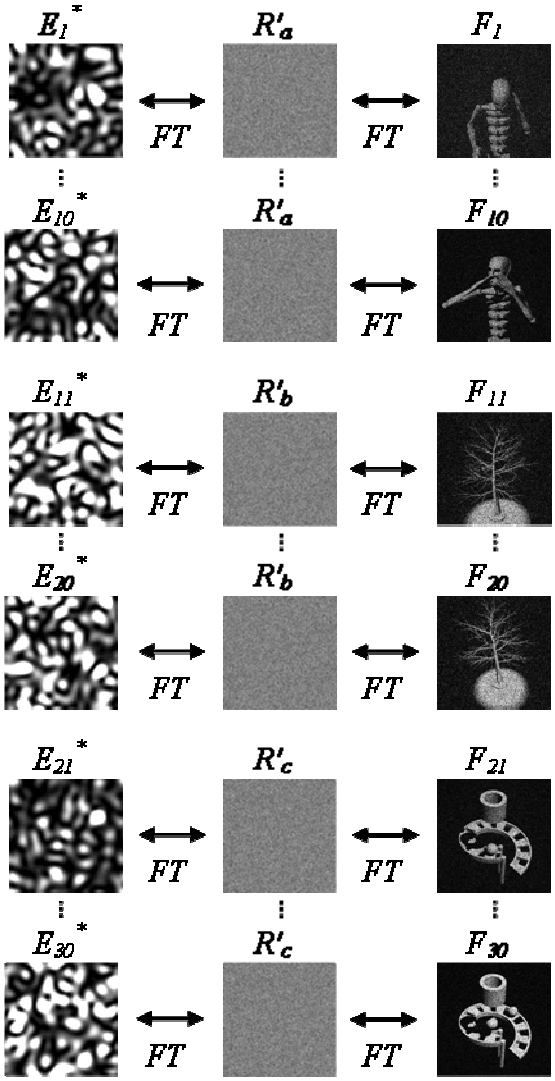


(b)

Figure 1 (a) 4f encryption procedure. F_i: ith frame of the dynamic scene, E_i: ith encrypted frame of the dynamic scene, FT: Fourier transform, R: input random phase mask, R'_a: random phase key employed to encrypt the first movie, R'_b: random phase key employed to encrypt the second movie and R'_c: random phase key employed to encrypt the third movie, (b) theta modulation, multiplexing and phase conjugation operation. G_i: ith amplitude modulation grating, *: phase conjugate operation.



(a)

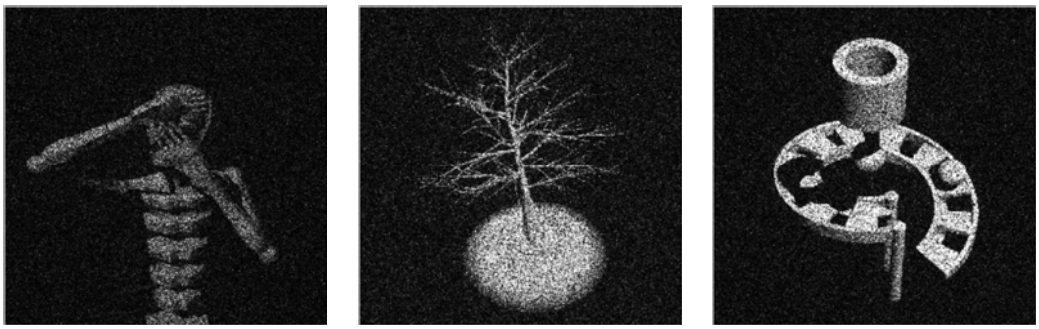


(b)

Figure 2: (a) Filtering procedure. E_i^*: ith phase conjugated encrypted frame, F_i: ith retrieved frame, (b) 4f decryption procedure. E_i^*: ith phase conjugated encrypted frame, R'_a: decoding key of the first movie, R'_b: decoding key of the second movie and R'_c: decoding key of the third movie.

3. RESULTS

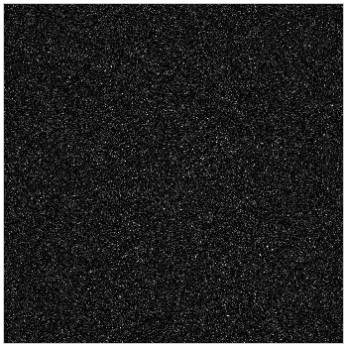
In order to demonstrate the validity of our multi-user encoding proposal, we consider a case of three valid users. The procedure described in the previous section is utilized to encrypt and multiplex three movies in the same medium. Each movie is codified by using different encryption mask, R'_a, R'_b and R'_c, in order to generate independent access channels. Each movie contains 10 frames meaning 1.67 seconds. The user receives the multiple encrypted patterns and the corresponding encrypting mask in order to retrieve after decryption the assigned movie. In Figure 3 the movie decrypted by each user is shown.



(a) (b) (c)

Figure 3. Decrypted movies. (a) Video 1. Dynamic scene watched by the user #1. http://dx.doi.org/doi.number.goes.here. (b) Video 2. Dynamic scene watched by the user #2. http://dx.doi.org/doi.number.goes.here. (c) Video 3. Dynamic scene watched by the user #3. http://dx.doi.org/doi.number.goes.here

Note that each frame is associated to a single sinusoidal grating and therefore we get a single pair of diffracted orders at the filtering plane. Then, there exist a unique relation between each frame and each pair of diffracted orders. A movie implies a temporal sequence of frames, which must be preserved during decoding. Therefore, in theta modulating, we must select the appropriate pitches and orientations of gratings to assign the diffracted orders position associated to the encoded movie frames that build the dynamic scene transmitted to each user. To decode a given movie, the user must have not only the right key but also the right synchronization to retrieve each frame in a correct time sequence. If a user wishes to update a subscription from the same multiplexed material, he/she must apply for new mask and synchronization options. On a regular basis of subscription, a user can be slotted in the same filtering-synchronization scheme for different multiplexed material, thus only needing a mask update for accessing the authorized information. In any case, if a mask different to the authorized encoding masks is employed, noise will be recovered in all the movie during decryption, as seen from Video 4.



Video 4. Decrypted movie obtained with a wrong key. http://dx.doi.org/doi.number.goes.here

Let us detail the optical parameters of the virtual optical system. The object size is 6.14 mm^2.The lenses involved in the FTs in the different steps of the virtual optical system have identical focal length of 100 mm. The wavelength is 632.8 nm. The area of the filtering plane is 42.2 mm^2. The spot diameter and the separation between adjacent spots at the filtering plane are both 5.27 mm, respectively. We want to emphasize that the speckle is always present in the decryption step as we are performing operations with virtual optical systems.

4. CONCLUSIONS

We present a multi-user encryption-decryption arrangement based on the conventional 4f architecture, multiplexing operation and the theta modulation approach. The proposal allows to free noise decode each input image. The theta modulation approach precludes polluting the recovered image with the noise associated to the remaining multiple information. We take advantage of this fact to encrypt several movies. Note that a movie implies a temporal sequence that in our proposal is mapped to a spatial sequence in the filtering plane. Then, the adequate filtering procedure allows recovering the movie in the correct sequence.

Acknowledgments

This research was performed under grants COLCIENCIAS, CODI -Universidad de Antioquia (Colombia), TWAS-UNESCO Associateship Scheme at Centres of Excellence in the South, CONICET No. 0863, ANCyT PICT 1167 and Facultad de Ingeniería, Universidad Nacional de La Plata No. 11/I125 (Argentina), bilateral project CO/08/16 between MINCyT (Argentina) and COLCIENCIAS (Colombia).

REFERENCES

[1] Refregier, P., Javidi, B., "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. 20(7), 767–769 (1995)
[2] Unnikrishnan, G., Joseph, J., Singh, K., "Optical encryption system that uses phase conjugation in a photorefractive crystal," Appl. Opt. 37(35), 8181-8186 (1998).
[3] Barrera, J.F., Henao, R., Tebaldi, M., Torroba, R., Bolognini, N., "Multiplexing encrypted data by using polarized light," Opt. Commun. 260(1), 109-112 (2006).
[4] Matoba, O., Javidi., B., "Encrypted optical storage with wavelength-key and random phase codes," Appl. Opt. 38(32): 6785-6790 (1999).
[5] Barrera, J.F., Henao, R., Tebaldi, M., Torroba, R., Bolognini, N., "Multiple image encryption using an aperture-modulated optical system," Opt. Commun. 261(1), 29-33 (2006).
[6] Carnicer, A., Montes-Usategui, M., Arcos, S., Juvells, I., "Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys," Opt. Lett. 30(13) 1644-1646 (2005).
[7] Barrera, J.F., Vargas, C., Tebaldi, M., Torroba, R., Bolognini, N., "Known-plaintext attack on a joint transform correlator encrypting system," Opt. Lett. Vol. 35(21), 3553-3555 (2010).
[8] Kumar, P., Kumar, A., Joby; J., Singh, K., "Impulse attack free double-random-phase encryption scheme with randomized lens-phase functions," Opt. Lett. 34(3), 331-333 (2009).
[9] Barrera, J.F., Henao, R., Tebaldi, M., Torroba, R., Bolognini, N., "Multiplexing encryption-decryption via lateral shifting of a random phase mask," Opt. Commun. 259(2), 532-536 (2006).
[10] Barrera, J.F., Henao, R., Tebaldi, M., Torroba, R., Bolognini, N., "Code retrieval via undercover multiplexing," Optik 119 (3), 139-142 (2008).
[11] Barrera, J.F., Henao, R., Tebaldi, M., Torroba, R., Bolognini, N., "Digital encryption with undercover multiplexing by scaling the encoding mask," Optik 120(7), 342-346 (2009).
[12] Mosso, F., Tebaldi, M., Torroba, R., Bolognini, N., "Double random phase encoding method using a key code generated by affine transformation," Optik 122(6), 529-534 (2011).
[13] Amaya, D., Tebaldi, M., Torroba, R., Bolognini, N., "Multichanneled puzzle-like encryption," Opt. Commun. 281(13) 3434–3439 (2008).
[14] Barrera, J.F., Torroba, R., "Efficient encrypting procedure using amplitude and phase as independent channels to display decoy objects," Appl. Opt. 48(17) 3120-3128 (2009).
[15] Mosso, F., Barrera, J.F., Tebaldi, M., Bolognini, N., Torroba, R., "All-optical encrypted movie," Opt. Exp. 19(6) 5706-5712 (2011).
[16] Rabal, H.J., Bolognini, N., Sicre, E., Garavaglia, M., "Optical image subtraction through speckle modulated by young fringes," Opt. Commun. 34(1) 7-10 (1980).

[17] Tebaldi, M., Angel, L., Lasprilla, M.C., Bolognini, N., "Image multiplexing by speckle in BSO," Opt. Commun. 155(4-6) 342-350 (1998).
[18] Angel, L., Tebaldi, M., Trivi, M., Bolognini, N., "Optical operations based on speckle modulation by using a photorefractive crystal," Opt. Commun. 168(1-4) 55-64 (1999).
[19] Tebaldi, M., Angel, L., Trivi, M., Bolognini, N., "New multiple aperture arrangements for speckle photography," Opt. Commun. 182(1-3) 95-105 (2000).
[20] Angel, L., Tebaldi, M., Bolognini, N., "Multiple rotation assessment through isothetic fringes in speckle photography," Appl. Opt. 46(14) 2676-2682 (2007).