All-optical encrypted movie

Fabian Mosso,[1] John Fredy Barrera,[3] Myrian Tebaldi,[1,*] Néstor Bolognini,[1,2] and Roberto Torroba[1]

[1]*Centro de Investigaciones Ópticas (CONICET La Plata-CIC) and UID OPTIMO, Facultad de Ciencias Exactas, Universidad Nacional de La Plata, P.O. Box 3 C.P 1897, La Plata, Argentina*
[2]*Facultad de Ciencias Exactas, Universidad Nacional de La Plata, P.O. Box 3 C.P 1897, La Plata, Argentina*
[3]*Grupo de Óptica y Fotónica, Instituto de Física, Universidad de Antioquia, A.A 1226 Medellín, Colombia*
**myrianc@ciop.unlp.edu.ar*

Abstract: We introduce for the first time the concept of an all-optical encrypted movie. This movie joints several encrypted frames corresponding to a time evolving situation employing the same encoding mask. Thanks to a multiplexing operation we compact the encrypted movie information into a single package. But the decryption of this single package implies the existence of cross-talk if we do not adequately pre-process the encoded information before multiplexing. In this regard, we introduce a grating modulation to each encoded image, and then we proceed to multiplexing. After appropriate filtering and synchronizing procedures applied to the multiplexing, we are able to decrypt and to reproduce the movie. This movie is only properly decoded when in possession of the right decoding key. The concept development is carried-out in virtual optical systems, both for the encrypting and the filtering-decrypting stages. Experimental results are shown to confirm our approach.

OCIS codes: (060.4785) Optical security and encryption; (070.4560) Data processing by optical means; (200.4740) Optical processing; (030.6140) Speckle.

References and links

1. G. Situ and J. Zhang, "Multiple-image encryption by wavelength multiplexing," Opt. Lett. **30**(11), 1306–1308 (2005).
2. J. F. Barrera, R. Henao, M. Tebaldi, R. Torroba, and N. Bolognini, "Multiplexing encryption-decryption via lateral shifting of a random phase mask," Opt. Commun. **259**(2), 532–536 (2006).
3. J. F. Barrera, R. Henao, M. Tebaldi, R. Torroba, and N. Bolognini, "Multiplexing encrypted data by using polarized light," Opt. Commun. **260**(1), 109–112 (2006).
4. J. F. Barrera, R. Henao, M. Tebaldi, R. Torroba, and N. Bolognini, "Multiple image encryption using an aperture modulated optical system," Opt. Commun. **261**(1), 29–33 (2006).
5. J. F. Barrera, R. Henao, M. Tebaldi, R. Torroba, and N. Bolognini, "Code retrieval via undercover multiplexing," Optik (Jena) **119**, 139–142 (2008).
6. P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. **20**(7), 767–769 (1995).
7. J. Ojeda-Castañeda and E. E. Sicre, "Theta-modulation decoder based on the Lau effect," Opt. Commun. **59**(2), 87–91 (1986).
8. J. W. Goodman, *Introduction to Fourier Optics* (Roberts & Company Publishers, 2004), pp. 80–81.

1. Introduction

Since optical techniques appear as practical tools in securing and validating information, researchers adopted significant efforts to investigate these techniques under the insight of cryptoanalysis. Researchers cast doubts on the efficiency in the sense if the techniques were able to endure attacks from cryptoanalysis. There are some common criteria for evaluating the effectiveness of these methods in practice: the key functions should be difficult to find by chance, the images delivered openly should be intensity patterns for use in Internet communication, and decryption should be relatively easy for receivers with the keys. One

#139612 - $15.00 USD Received 3 Jan 2011; revised 3 Mar 2011; accepted 5 Mar 2011; published 11 Mar 2011

important feature that reinforces optical encryption is the multiplexing concept. This procedure brings the chance for storing multiple messages in a single recording medium. In this regard, multiplexing proposals have a practical application in optical encryption, increasing the total number of possible combinations yet improving the robustness of the encrypting system. In multiplexing arrangements, the encryption of an input image is associated to a determined status of the encrypting parameters. There exist a biunivocal relation between each input image and its encrypted version. The multiplexing basic principle consists on encrypting several images into a single package in order to not only to bring the change for multiple users, but also to increase data security. Several multiplexing encryption methods were proposed, for instance, wavelength multiplexing [1], multiplexing by random-phase mask shifting [2], modifying the polarization state [3], or using multiple apertures that change between exposures [4,5].

In case of using a single encoding mask, the problem for the end user will be the cross talk among the overlapping of decoded images. To avoid this cross-talk, a classical solution involves setting the encrypting optical parameters in a way to define separately the encoded images or to modify the encrypting machine. So far, multiplexing methods were performed such that the encrypted images are completely uncorrelated. In this case, the main issue is the superposition of the decrypted information over the non-decrypted data, this last acting as noise.

These protocols refer to the idea of multiple users sharing common multiplexed pieces of information and in possession of an authorized decoding key to get a single piece. Each piece of information represents a static image. We can extend the idea to a single user with the capability of decoding a whole sequence of individually encrypted but associated events. The new concept thus involves the idea of encoding a dynamic situation. Besides, to retrieve the complete dynamic input information, it is necessary not only to properly decrypt the images but also to compose them.

As we intend to use a single encrypting mask, we have to solve the crosstalk problem arising from the spatial superposition of the multiplexed images. We suggest the use of an inner spatial modulation of the speckles contained in each encrypted image before multiplexing. Thanks to this modulation, we are able to introduce a later filtering procedure to overcome the cross-talk issue.

If all input data correspond to a sequence of images representing successive frames of a moving scene, then we are encrypting and multiplexing a movie. It only remains to synchronize the recovering procedure to adequately display the decoded movie.

In this contribution, we propose and implement the first reported technique to obtain an all-optical encrypted movie carried out with only virtual optical systems. The frames that compose the movie are encrypted and fringe modulated separately before multiplexing. The encryption of each frame is performed using the same coding key and without changing the encrypting virtual optical system. Before sending the multiplexing results, we perform its phase conjugation. During recovering, each phase conjugated encrypted frame is obtained from the multiplexing by means of a filtering process. Finally, using the right coding key during decryption, each frame is recovered. This process along with the synchronization in the filtering steps results in the adequate reconstruction of the movie.

2. Description of the method

We select as encrypting protocol the classical 4*f* double random phase encoding architecture [6]. The goal of our proposal is to encrypt–decrypt a synchronized sequence of frames that compose a dynamic scene constituting a movie. Referring to Fig. 1, in the first step we show in each row a single frame encrypting procedure using the same encoding mask R´ and without modifications of the encrypting virtual optical system for every frame. But a multiplexing at this step by considering a single encoding mask leads, after decoding, to severe image degradation due to cross-talk. This degradation is caused by the simultaneous

#139612 - $15.00 USD Received 3 Jan 2011; revised 3 Mar 2011; accepted 5 Mar 2011; published 11 Mar 2011

spatial overlapping of the decoded frames. Therefore we have to design strategies to overcome this issue. We now recall the well known theta modulation method applied to speckle patterns with gratings to primarily store different images into a single record [7]. This approach leads us to recover each frame without the influence of the remaining ones. We will use this approach to introduce an external tool that allows one to spatially separate the different frames F_i. For this reason in step 2 of Fig. 1, we introduce a physical grating G_i in contact with each encrypted frame E_i, and we rotate the grating for the different frames. In this way, we assign different spatial "labels" for each frame. Once this procedure is accomplished we proceed to multiplex all frames. The multiplexing operation results from the addition of the modulated encrypted information obtained by the grating attaching procedure above described for each encrypted input frame. In general, this procedure will be extended to not only the grating rotation but also to a simultaneous pitch variation in a way to expand the possibilities to increase the number of "labeled" frames.

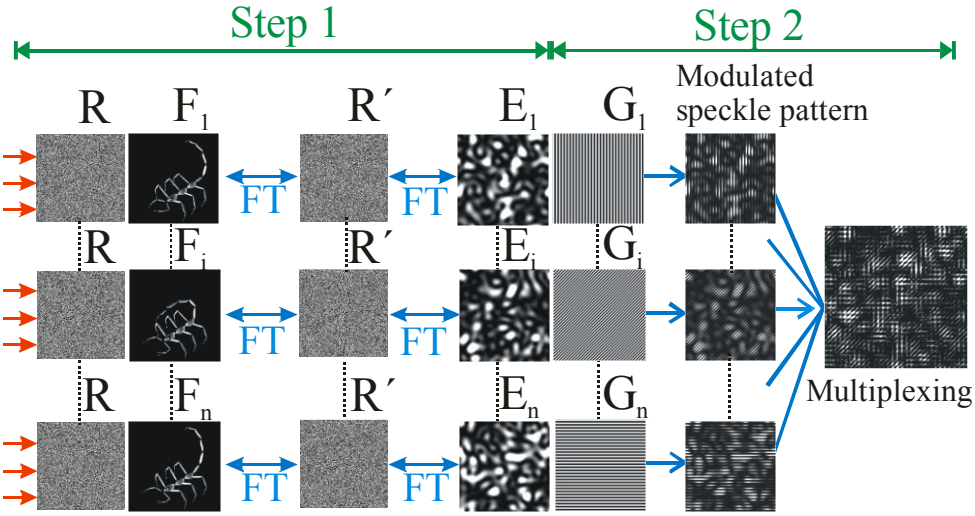


Fig. 1. Step 1: encryption process (R: random phase mask, F_i: i-th frame; R´: key mask, E_i: i-th encrypted frame, FT: Fourier transform); step 2: theta speckle modulation and multiplexing (G_i: i-th amplitude grating). All shown speckle patterns correspond to enlarged version of the actual patterns.

Figure 2 shows an enlarged region of an encrypted frame modulated by the grating. We can see the different speckles covered with horizontal lines corresponding to that grating orientation. We recall that the exit pupil of the encoding 4f architecture controls the average speckle size. It is important to note that the grating does not affect this speckle size distribution.

Fig. 2. Enlarged version of an encrypted grating modulated frame.

#139612 - $15.00 USD Received 3 Jan 2011; revised 3 Mar 2011; accepted 5 Mar 2011; published 11 Mar 2011

We now send to the user the complex conjugate of the multiplexing together with a copy of the original encoding key. The recovering procedure performed by the user consists on filtering and decrypting steps. Although we show for clarity these steps in two separate figures, they are performed into a single decoding unit which consists in a virtual optical system.

We now analyze in Fig. 3 the filtering process. A Fourier transform (FT) of the input reveals the existence of paired spots belonging to each "labeled" frames located a different spatial positions. We have to remember that these positions depend on the pitch and orientation of the "labeling" grating.

To speed up data collection to arrange the movie, we prefer to display the "labeled" pair information in concentric circles expanding their radius as we increase the number of stored frames. The experimental conception previous to the filtering process, bearing in mind the final synchronization procedure, lead us to choose the initial step by using a grating with their lines vertically oriented. Then we start to sequentially change the input frame as we start a 180 degree rotation of the grating. Therefore, we achieve the inner most "labeled" circle to be observed at the filtering plane. In order to define the next outer circle, we reduce the grating pitch and proceed in the same way as before. As a consequence the first grating defines the largest pitch involved. For reconstruction, the order established above before multiplexing, should be maintained to retrieve the motion in its natural sequence.

We filter out all but a given spot, in order to obtain, after a new FT, a single encrypted frame. In this way, we isolate each encrypted frame from the information of the remaining encrypted frames. Consequently, we are avoiding the existence of possible cross talking during the next decoding step. We keep only one spot as the display of the paired spots will introduce a polluting grating structure on the filtered image.

The minimum pitch selection should be as to detect at least two fringes in each speckle. In this point, we want to highlight that the final number of frames to be processed is limited by several aspects: a) the minimum resolved speckle modulation spacing; b) as the parameters of the encrypting optical procedure define the area of each spot associated to each frame at the filtering plane we have a limited number of spots provided that overlapping is avoided, c) the number of spots that fall on the available area within the filtering plane. The detailed discussion of the influence this limitation imposes on the number of frames as well as on cross-talk reduction will be addressed in a future contribution.

Accordingly in Fig. 4 we proceed with the classical decoding of each single frame for the 4*f* decrypting architecture. Finally, the entire procedure leads to clearly visualize each single frame without the influence of the others.

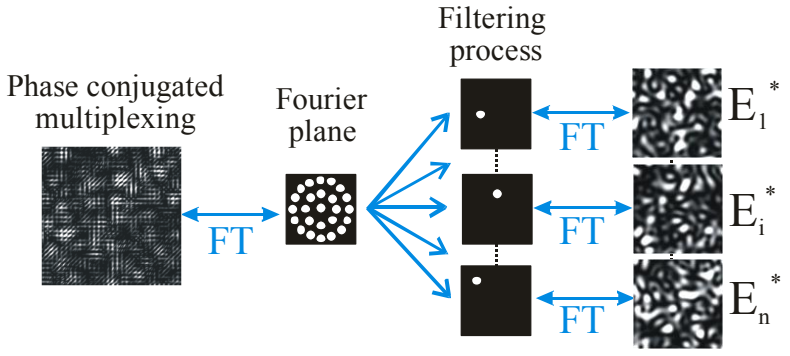


Fig. 3. Filtering process.

This method represents a solution to the problem of a single user with a single decoding mask trying to visualize a set of encrypted images. Without the external grating "labeling" to each encrypted frame and their subsequent filtering process, the visualization of each separate

#139612 - $15.00 USD Received 3 Jan 2011; revised 3 Mar 2011; accepted 5 Mar 2011; published 11 Mar 2011

frame will be hindered. Additionally, we are reconstructing each decoded frame with the same visual quality. The quality was checked by comparing each input frame with their corresponding decoded outputs by the well known normalized mean root square error (NMSE) metric, giving the almost flat response depicted in Fig. 5. In fact, this curve indicates a uniform quality along the process for the complete movie. This technique leads to the idea that each frame could be associated to a time evolving phenomenon. If we display these consecutive frames in a time sequential order, we can reconstruct a movie of this phenomenon. Then, we are developing the first idea of an all-optical encrypted-decrypted movie. The user in possession of not only the right decoding mask but also the right time sequence could see the movie.

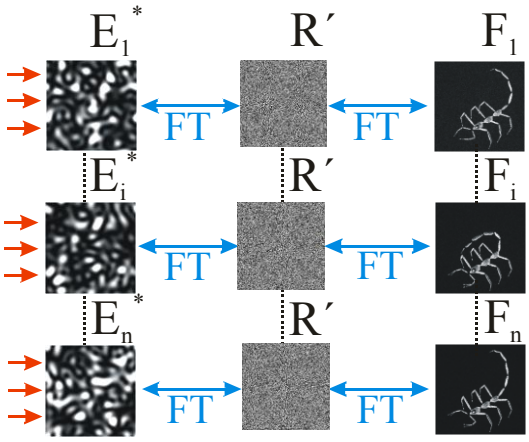


Fig. 4. Decryption process (E_i*: i-th complex conjugated encryption frame).

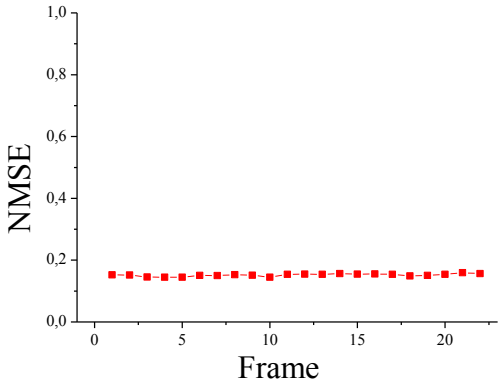


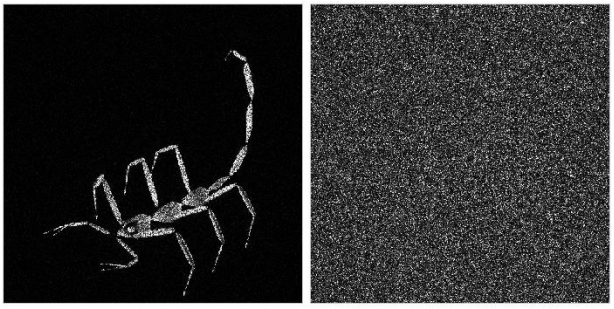
Fig. 5. Normalized NMSE for all frames in the movie.

3. Experimental results

In our experiment we take 22 frames of an original movie and submitted to the procedure above described. After decryption we synchronize the display to 10 frames per second to get a 2.2 seconds movie, shown in Fig. 6(a) (Media 1). We clearly see the fluid movement of the movie subject. If we intend to reproduce the movie without placing the right decoding key R´ we get the boiling speckled movie of Fig. 6(b) (Media 2). We want to emphasize that the speckle is ever present in the entire process as we are performing operations with virtual optical systems. The object size is 5.7 x 5.7 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

#139612 - $15.00 USD Received 3 Jan 2011; revised 3 Mar 2011; accepted 5 Mar 2011; published 11 Mar 2011

wavelength is 632.8 nm. The area of the filtering plane is 45 x 45 mm^2. The spot diameter and the separation between adjacent spots at the filtering plane are both 6.5 mm.



(a) (b)

Fig. 6. (a) Full decrypted optical movie (Media 1) and (b) full non-decrypted optical movie (Media 2).

4. Conclusions

In the present contribution we developed the concept of an encrypted-decrypted movie to display a time evolving phenomenon. As described in the paper, we perform a "labeling" of each encrypted frame to avoid the cross talk that arises when recovering the information after multiplexing. The "labeling" allows an appropriate selection of non overlapped frames and together to the logical synchronization; we are able to finally display the movie. We want to stress that the application is intended for a single user in a friendly environment, as the user requires a single synchronizing-decrypting unit that performs the final displaying task.

The experimental results illustrate the feasibility of the proposal. As we only intend to introduce the concept, we defer the logical optimization of the whole procedure to future contributions.

Appendix

Let us mathematically describe the encryption-decryption set-up (see Fig. 1, Fig. 3, and Fig. 4). The whole procedure can be expressed as follows. The amplitude A_i for each input frame is given by: $A_i = F_i R$ where F_i is the corresponding i-th frame amplitude and R is the input random phase mask. By multiplying its Fourier transform by the key code mask R´ results in: $\Im[F_i R]\cdot R'$. Note that R and R´ are used for every frame. Then, each encrypted frame for the $4f$ encrypting architecture is:

$$E_i = F_i R \otimes \Im[R'] \tag{1}$$

where $\otimes$ represents the convolution operation. By considering the second step of the encryption procedure (see Fig. 1), the encrypted output E_i is multiplied by a sinusoidal grating G_i whose expression follows the traditional definition in optics (see Ref [8]. page 80). This grating has a pitch d_i which fulfills $d_i << S_t$ (where S_t is the transversal average speckle size) and S_t is inversely proportional to the output pupil size of the system. The multiplexing procedure implied to encrypt n frames. We have to stress that the whole stored encrypted information M is expressed as:

$$M = \left(\sum_{i=1}^{n} E_i G_i \right) \tag{2}$$

#139612 - $15.00 USD Received 3 Jan 2011; revised 3 Mar 2011; accepted 5 Mar 2011; published 11 Mar 2011

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. (2).

As usual, in order to recover the original information a phase conjugate operation must be carried out. At this point we have to perform this phase conjugation operation, which can be realized for instance by illuminating the photorefractive crystal with a phase conjugated reference beam or by digitally changing the sign of the phase in the stored multiplexed pattern. Then, after this phase conjugation operation and another Fourier transform (see Fig. 3) it results

$$\Im\left(M^{*}\right)=\Im\left(\sum_{i=1}^{n} E_{i}^{*} G_{i}^{*}\right)=\sum_{i=1}^{n}\left[\Im\left(E_{i}^{*}\right)\otimes\Im\left(G_{i}^{*}\right)\right] \tag{3}$$

As it is well known, the Fourier transform of the sinusoidal grating 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 on the grating orientation and pitch and the size depends on the parameters of the optical system (see Ref [8]. page 81). We have to recall that we are storing n frames; therefore we are obtaining several diffracted spots as can be seen in the second image from the right in Fig. 3. The filtering procedure is performed on the plane where these spots are displayed, by adequately positioning a circle of unitary transmittance scaled to the size of the diffracted order while assigning zero transmittance to the rest. By adequately selecting the filter position, we retain from the i-th term of Eq. (3) only one diffracted spot associated to $\Im\left(E_{i}^{*}\right)$ from the corresponding two symmetrically spots located around the center. In Fig. 3 this procedure is displayed in the two last columns for three cases. Then, an inverse Fourier transform operation allows obtaining each conjugated encrypted frame E_{i}^{*}. As described in Fig. 4, the decoding process requires of another 4f scheme. At this step, the conventional decrypting procedure allows recovering the frame F_i by the operation

$$\Im\left(E_{i}^{*}\right)R'=\Im\left(F_{i}^{*}\,R^{*}\right)\left[R'^{*}\,R'\right] \tag{4}$$

and finally another Fourier transform gives

$$\Im\left[\Im\left(E_{i}^{*}\right)R'\right]=F_{i}^{*}\,R^{*} \tag{5}$$

This operation must be sequentially carried out n times in order to decrypt all movie frames. It is interesting to remark that we display the movie in intensity form, therefore this intensity operation removes the phase mask information R*.

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).

#139612 - $15.00 USD Received 3 Jan 2011; revised 3 Mar 2011; accepted 5 Mar 2011; published 11 Mar 2011