Experimental multiplexing of encrypted movies using a JTC architecture

John Fredy Barrera,[1,*] Myrian Tebaldi,[2] Carlos Ríos,[1] Edgar Rueda,[1] Néstor Bolognini,[2,3] and Roberto Torroba[2]

[1]*Grupo de Óptica y Fotónica, Instituto de Física, Universidad de Antioquia, A.A. 1226, Medellín, Colombia.*
[2]*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.*
[3]*Facultad de Ciencias Exactas, Universidad Nacional de La Plata, La Plata, Argentina.*
[*]*jbarrera@fisica.udea.edu.co*

Abstract: We present the first experimental technique to encrypt a movie under a joint transform correlator architecture. We also extend the method to multiplex several movies in a single package. We use a Mach-Zehnder interferometer to encrypt experimentally each movie. One arm of the interferometer is the joint transform correlator and the other arm is the reference wave. We include the complete description of the procedure along with experimental results supporting the proposal.

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

References and links

1. F. Mosso, J. F. Barrera, M. Tebaldi, N. Bolognini, and R. Torroba, "All-optical encrypted movie," Opt. Express **19**(6), 5706–5712 (2011), http://www.opticsinfobase.org/spotlight/summary.cfm?uri=oe-19-6-5706.
2. F. Mosso, M. Tebaldi, J. F. Barrera, N. Bolognini, and R. Torroba, "Pure optical dynamical color encryption," Opt. Express **19**(15), 13779–13786 (2011), http://www.opticsinfobase.org/oe/abstract.cfm?URI=oe-19-15-13779.
3. H. E. Hwang, H. T. Chang, and W. N. Lie, "Multiple-image encryption and multiplexing using a modified Gerchberg-Saxton algorithm and phase modulation in Fresnel-transform domain," Opt. Lett. **34**(24), 3917–3919 (2009).
4. H. T. Chang, H. E. Hwang, and C. L. Lee, "Position multiplexing multiple-image encryption using cascaded phase-only masks in Fresnel transform domain," Opt. Commun. **284**(18), 4146–4151 (2011).
5. E. Rueda, C. Ríos, J. F. Barrera, R. Henao, and R. Torroba, "Experimental multiplexing approach via code key rotations under a joint transform correlator scheme," Opt. Commun. **284**(10-11), 2500–2504 (2011).
6. R. Henao, E. Rueda, J. F. Barrera, and R. Torroba, "Noise-free recovery of optodigital encrypted and multiplexed images," Opt. Lett. **35**(3), 333–335 (2010).

1. Introduction

In the frame of the recent field of dynamical encryption, we found solutions to the problems inherent to the multiplexing operation, namely background noise and cross-talk [1, 2]. In those contributions authors developed the concept of an encrypted-decrypted movie to display a time evolving phenomenon. As described in those papers, authors perform a modulation of each encrypted frame to avoid the cross talk that arises when recovering the information after multiplexing. The modulation allows an appropriate selection of non overlapped frames and together to the logical synchronization; a potential receiver is able to finally display the movie. The published approaches were implemented on a 4*f* encrypting architecture. These practical implementations belong to the type of the so called position multiplexing techniques [3, 4].

We are now looking for an extension of the dynamical encryption to a joint transform correlator (JTC) architecture. The JTC encrypting architecture is more compact than the 4f scheme and it is more stable from a holographic point of view. In this scheme, we have to

#155392 - $15.00 USD Received 26 Sep 2011; revised 22 Nov 2011; accepted 23 Nov 2011; published 30 Jan 2012

design a new strategy that allows managing the output frames in a way to avoid superposition. The experimental achievement introduced in Ref [5, 6]. is an adequate instrument to be implemented in the present contribution. The scheme in the references is based on a Mach-Zehnder interferometer, where the JTC is located in one arm and the other arm provides the reference beam. The implementation technique relies on digital holography, where information capture is performed with a CCD camera. The interference equation, or joint power spectrum (JPS), contains four terms, where authors focus their attention in retaining only the term with the encrypted object information [5, 6]. For this purpose, authors separately store the JPS, the background noise corresponding to the zero order terms, and the digital hologram of the Fourier transform (FT) of the encoding key. By digitally subtracting from the JPS the DC terms, and performing a FT it is possible to get two spatially isolated terms carrying the information of the object convolved with the encoding key. Next, one of those terms is removed and at this stage, the remaining term is freely positioned exclusively by digital means. Precisely this freedom in choosing the term position enable us to handle the situation where multiple images are used, and in such case, this possibility is useful to avoid the spatial overlapping of decoded images.

With this framework in mind, we propose to extend the procedure to include the case of successive images that compose a dynamical event, leading to its implementation in the JTC architecture. We adopt this experimental protocol to encrypt and to multiplex a set of frames that constitute a movie. In our proposal, the dynamical input is displayed as a set of still frames in a spatial light modulator (SLM). Unlike previous contributions, during decryption the whole data set is simultaneously displayed. Moreover, this procedure is extended to include different movies in a multi-user environment. Any dynamical situation comprises the possibility of single or multi-users, implying even the use of more than one encrypting key. In the following sections, we describe the encrypting process for a single frame, extending the technique to a movie. We also include a brief theoretical explanation. We present the successful experimental results that include the above potentials besides demonstrating the actual application possibilities.

2. Description of the encrypting process

The first step in the encrypting process is performed employing the experimental setup shown in Fig. 1. The optical setup consists in a Mach–Zehnder interferometer with a JTC encrypting system in one arm and a reference wave in the other. In the JTC encrypting scheme, the input is

$$\begin{aligned} u_0(x_0,y_0) = &\left[f_l(x_0,y_0)\, m_l(x_0,y_0) \right] \otimes \delta\left(x_0-(-a),y_0\right) \\ &+ k(x_0,y_0) \otimes \delta(x_0-a,y_0) \end{aligned} \tag{1}$$

where $m_l(x_0,y_0)$ and $k(x_0,y_0)$ are random phase masks, $f_l(x_0,y_0)$ is the object to be encrypted, $\otimes$ means convolution, $k(x_0,y_0)$ represents the security key of the system, and $2a$ is the distance between the object and the key.

By blocking the reference arm, the joint power spectrum $JPS(u,v)$ at plane E is:

$$\begin{aligned} JPS(u,v) = &\left|F_l(u,v)\right|^2 + \left|K(u,v)\right|^2 + F_l^*(u,v)\,K(u,v)\exp(-4\pi i a u) \\ &+ F_l(u,v)\,K^*(u,v)\exp(4\pi i a u) \end{aligned} \tag{2}$$

where * means complex conjugate, $F_l(u,v)$ and $K(u,v)$ are the Fourier transforms of $f_l(x_0,y_0)m_l(x_0,y_0)$ and $k(x_0,y_0)$, respectively. The encrypted information is obtained after filtering to retain and then to position the last term of Eq. (2) (see Ref [5].),

#155392 - $15.00 USD Received 26 Sep 2011; revised 22 Nov 2011; accepted 23 Nov 2011; published 30 Jan 2012

$$E_l(u,v) = F_l(u,v)K^*(u,v)\exp\left[4\pi i\left(x_l u + y_l v\right)\right] \tag{3}$$

The position at coordinates (x_l, y_l) allow locating the decrypted data in any desired position in the recovering plane, which is essential in the case of encrypting a movie, as this positioning avoids any frame overlapping at the output plane.

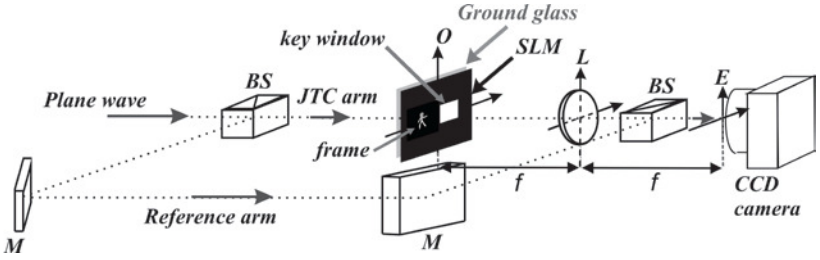


Fig. 1. Optical setup for the encrypting procedure (*BS*: cubic beam splitter, *SLM*: spatial light modulator, *O*: input plane, *M*: mirror, *L*: lens of focal distance *f*, *E*: CCD camera plane).

3. Encrypting a movie

In our case, the multiplexing of all encrypted frames $V(u,v)$ composes an encrypted movie. According to Eq. (3), for *n* frames we have

$$V(u,v) = \sum_{l=1}^{n} F_l(u,v)K^*(u,v)\exp\left[4\pi i\left(x_l u + y_l v\right)\right] \tag{4}$$

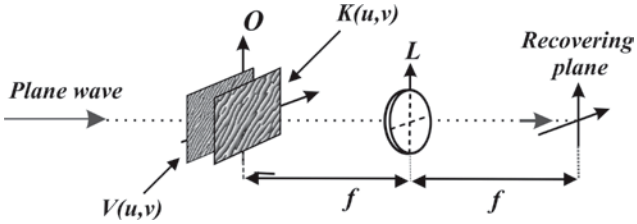


Fig. 2. System to decrypt all frames ($V(u,v)$: encrypted movie; $K(u,v)$: hologram of the FT of the key).

On the other hand, in order to record the hologram of the FT of security key, we proceed to block the object window and simultaneously to unblock the reference arm [5]. Therefore, we have four terms and proceeding as in the previous section, we can filter the DC terms, eliminating one of the diffracted terms and the remaining one is positioned at coordinates $(0,0)$, resulting in,

$$G(u,v) = K(u,v) \tag{5}$$

Recovering is performed by multiplying the encrypted movie (Eq. (4)) with the result of Eq. (5). By using a 2*f* system (see Fig. 2), we simultaneously recover all frames in the same plane without superposing, as described by

$$D(x,y) = \sum_{l=1}^{n} f_l(x_0,y_0)m_l(x_0,y_0) \otimes \delta(x - x_l, y - y_l) \tag{6}$$

It is important to remark that we record the intensity $\left|D(x,y)\right|^2$, thus recovering the information $\left|f_l(x_0,y_0)\right|^2$ alone. The final step is to select and to synchronize in a timely fashion the decrypted information to compose the movie.

#155392 - $15.00 USD Received 26 Sep 2011; revised 22 Nov 2011; accepted 23 Nov 2011; published 30 Jan 2012

4. Experimental results

In the experimental setup, we use a lens of 200 mm focal length, a He-Ne laser, and a PULNIX TM6703 CCD camera with 640 x 480 pixels and 9 μm × 9 μm pixel area. The key window and each frame window are projected in a Holoeye LC2002 SLM. We use a translucent SLM with the following characteristics: 800 x 600 pixels, pixel pitch 32 μm and fill factor 55%. A ground glass placed behind the SLM generates the two masks needed for the JTC architecture. The frame window size is 1.92 mm × 1.92 mm, the area of the key window is 1.92 mm x 1.92 mm, and the distance between windows is 2.6 mm. The actual size for each frame is 150 × 150 pixels, while the sizes for $K(u,v)$ and $V(u,v)$ depend on the number of frames. In our experiments, for one movie, their sizes were 1800 x 1800 pixels while for three movies 2800 × 2800 pixels. In Fig. 3(a) we show one frame from the movie while in Fig. 3(b) we show the right simultaneously decrypted frames and in Fig. 3(c) the same sequence wrongly decrypted. To implement the decryption step to finally obtain a movie the receiver must get the encrypted movie, the FT of the encrypting key, the spatial order and the time interval between frames. The receiver multiplies the encrypted movie by the FT of the encrypting key and proceeds to FT this result (see Fig. 3(b)). Now the receiver crops the decrypted frames and then using the spatial order and the time interval data, the receiver can properly recover the movie.

Fig. 3. (a) One of the actual input frames as projected in the SLM, (b) all decrypted frames with the right security key and (c) all recovered frames using a wrong key.

It results evident that the use of different encoding keys for every frame will increase the security level of the method, but on the other hand this introduces additional steps in the decoding process. We have to recall that the phase the translucent SLM could introduce is kept constant along the whole process. Then, it does not affect the decryption procedure. In Fig. 4(a), we show the full successfully decrypted movie (Media 1) and in Fig. 4(b) an attempt to decrypt the same movie but using an invalid key (Media 2). We display 36 frames at a speed of 8 frames per second.

We now want to show the experimental approach to encrypt several movies in a single package. In doing so, it is necessary to obtain each encrypted movie (Eq. (4)) and then generate the multiplexing of *q* movies of *n* frames each:

$$M(u,v)=\sum_{j=1}^{q}\sum_{l=1}^{n}F_{l,j}(u,v)K_j^{*}(u,v)\exp\left[4\pi i\left(x_{l,j}u+y_{l,j}v\right)\right] \qquad (7)$$

where the term $F_{l,j}(u,v)K_j^{*}(u,v)\exp\left[4\pi i\left(x_{l,j}u+y_{l,j}v\right)\right]$ represents in general the encrypted information of the frame *l* with the key *j*. To decrypt each encrypted and multiplexed movie, it is also necessary to get the hologram of the FT of each security key $G_j(u,v)=K_j(u,v)$ where j = 1, 2, 3,…, k,….q. Equation (7) reveals the case for a multiplexing procedure,

#155392 - $15.00 USD Received 26 Sep 2011; revised 22 Nov 2011; accepted 23 Nov 2011; published 30 Jan 2012

including the storing of multiple movies where each single movie is associated to a single recovering key.

To recover movie number k, the authorized user gets the multiplexed information $M(u,v)$ and the corresponding key $K_k(u,v)$ to obtain, after processing

$$D_k(x,y)=\sum_{l=1}^{n} f_{l,k}(x,y)\, m_l(x_0,y_0)\otimes\delta(x-x_{l,k},y-y_{l,k}) \tag{8}$$

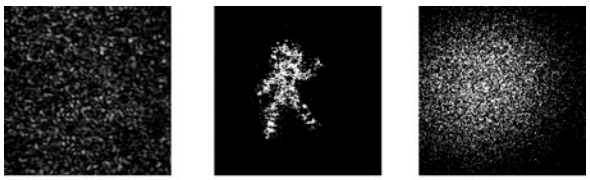


Fig. 4. (a) Encrypted movie, (b) fully decrypted optical movie with the right security key (Media 1) and (c) non-decrypted optical movie with a wrong key (Media 2).

We recall that positions $(x_{l,k},y_{l,k})$ are chosen as to guarantee no superposition of any frame. In practice each frame in each encrypted video, according to our procedure, will have at the output a determined position, therefore at the moment of generating the single package it is irrelevant the order in which we store the encrypted frames for every video.

The use of this approach could be to provide multiple movies to different users or several movies to a single user. To illustrate this example we include the results shown in Fig. 5. We packed three movies in sequential order, the first and the last shearing the same key. In Fig. 5(a) we find three sampled recovered frames taken from the decoding procedure using the key for the first and the last movies. Note that the non-decrypted movie is observed as noise at the middle of the sequence (Media 3). In Fig. 5(b) we show the inverse case (Media 4).

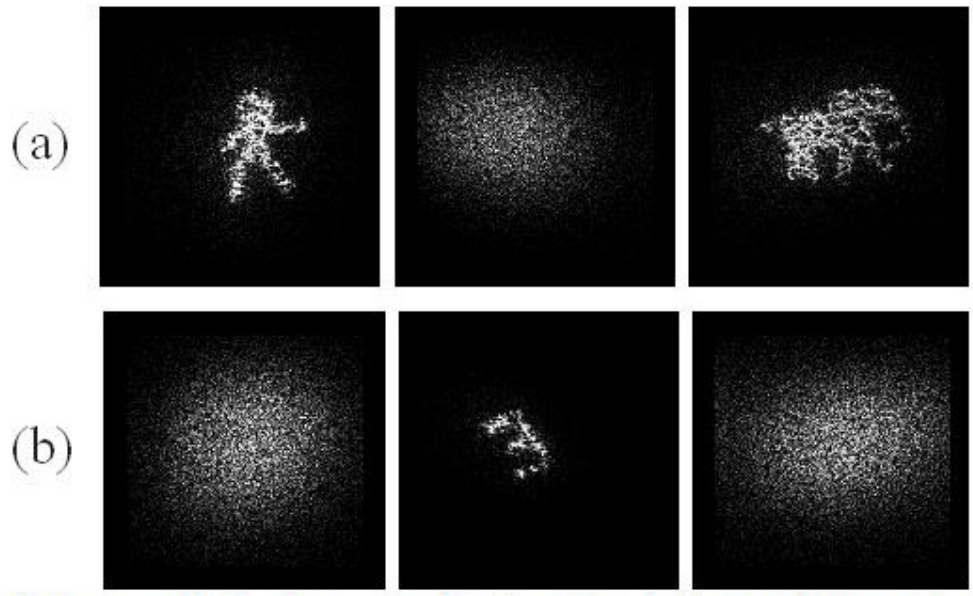
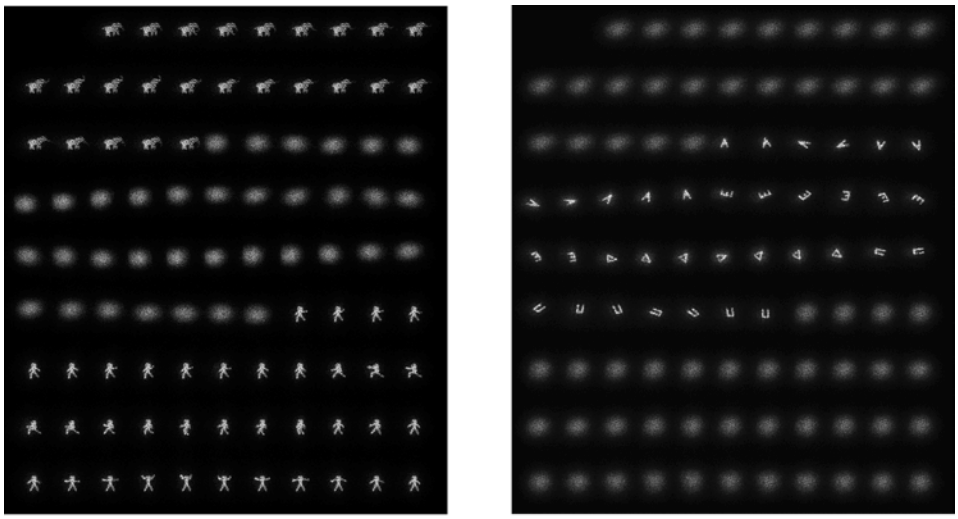


Fig. 5. Experimental multiplexing results for three encrypted movies with two different keys. (a) Decryption using the first key showing two different movies and the non-decrypted movie (Media 3). (b) Decryption of the remaining movie with the second key and the two non-decrypted movies (Media 4).

#155392 - $15.00 USD Received 26 Sep 2011; revised 22 Nov 2011; accepted 23 Nov 2011; published 30 Jan 2012

Figures 6(a) and 6(b) show the output planes from a single package simultaneously displaying the frames that compose the movies corresponding to Media 3 and Media 4. We can observe that the frames are shown in the sequential order in which they will appear in the respective movie.



(a) (b)

Fig. 6. (a) Output plane for Media 3 and (b) output plane for Media 4.

6. Conclusions

In further developing the implementation of encrypting movies, we introduce the first experimental result for a JTC architecture. We use a technique to filtering and to repositioning the information to achieve at the end the decoded frames without spatial superposition. One characteristic of our proposal is the simultaneous display of the decrypted results without needing a separate decryption for each frame, thus saving decrypting time. The quality of the results is highly dependent of the experimental handling of the displaying device. Nevertheless, we are able to show three different movies in the same package successfully. The encrypted movies in a single package and their corresponding decoding keys can be transmitted to remote users through normal communication channels. Another advantage of the proposed opto-digital approach relies on the decryption step, where the end user applies a digital recovering procedure without an experimental station. Both multi- and single users are favored with this technique in recovering one or several movies independently. The decryption task is simple in the sense that it does not represent inconvenient involving cumbersome procedures while keeping all the security standards. In all this development, we have to keep in mind that these are actual experimental results and this is the main reason why we found the inherent speckle noise in all recovered movies. We hope that future developments in the field will help in reducing the speckle noise, thus improving the quality of the results.

Acknowledgments

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

#155392 - $15.00 USD Received 26 Sep 2011; revised 22 Nov 2011; accepted 23 Nov 2011; published 30 Jan 2012