Pure optical dynamical color encryption

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

[1]*Centro de Investigaciones Ópticas (CONICET La Plata-CIC) and UID OPTIMO, Facultad de Ingenieria, 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, 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 a way to encrypt-decrypt a color dynamical phenomenon using a pure optical alternative. We split the three basic chromatic channels composing the input, and then each channel is processed through a 4f encoding method and a theta modulation applied to the each encrypted frame in every channel. All frames for a single channel are multiplexed. The same phase mask is used to encode all the information. Unlike the usual procedure we do not multiplex the three chromatic channels into a single encoding media, because we want to decrypt the information in real time. Then, we send to the decoding station the phase mask and the three packages each one containing the multiplexing of a single channel. The end user synchronizes and decodes the information contained in the separate channels. Finally, the decoding information is conveyed together to bring the decoded dynamical color phenomenon in real-time. We present material that supports our concepts.

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

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).
2. P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. **20**(7), 767–769 (1995).
3. J. 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).
4. J. Fredybarrera, 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).
5. J. Barrera, R. Henao, M. Tebaldi, R. Torroba, and N. Bolognini, "Multiplexing encrypted data by using polarized light," Opt. Commun. **260**(1), 109–112 (2006).
6. D. Amaya, M. Tebaldi, R. Torroba, and N. Bolognini, "Multichanneled puzzle-like encryption," Opt. Commun. **281**(13), 3434–3439 (2008).
7. L. Chen and D. Zhao, "Optical color image encryption by wavelength multiplexing and lensless Fresnel transform holograms," Opt. Express **14**(19), 8552–8560 (2006).
8. L. Chen and D. Zhao, "Color information processing (coding and synthesis) with fractional Fourier transforms and digital holography," Opt. Express **15**(24), 16080–16089 (2007).
9. M. Joshi, Chandrashakher, and K. Singh, "Color image encryption and decryption using fractional Fourier transform," Opt. Commun. **279**(1), 35–42 (2007).
10. D. Amaya, M. Tebaldi, R. Torroba, and N. Bolognini, "Digital color encryption using a multi-wavelength approach and a joint transform correlator," J. Opt. A, Pure Appl. Opt. **10**(10), 104031 (2008).
11. D. Amaya, M. Tebaldi, R. Torroba, and N. Bolognini, "Wavelength multiplexing encryption using joint transform correlator architecture," Appl. Opt. **48**(11), 2099–2104 (2009).
12. M. Tebaldi, S. Horrillo, E. E. Pérez-Cabré, M. S. Millán, D. Amaya, R. Torroba, and N. Bolognini, "Experimental color encryption in a joint transform correlator architecture," J. Phys.: Conf. Ser. **274**, 012054 (2011).
13. A. Carnicer, M. Montes-Usategui, S. Arcos, and I. Juvells, "Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys," Opt. Lett. **30**(13), 1644–1646 (2005).

#145481 - $15.00 USD Received 6 Apr 2011; revised 3 Jun 2011; accepted 20 Jun 2011; published 5 Jul 2011

14. X. Peng, P. Zhang, H. Wei, and B. Yu, "Known-plaintext attack on optical encryption based on double random phase keys," Opt. Lett. **31**(8), 1044–1046 (2006).

1. Introduction

Optical encryption is one of the techniques used to safely handling and protecting an image. In Optical encryption, an image is converted into white noise via a double random phase encryption protocol and reconstructed from the encoded result using a reversing process. In particular, encrypted images created by an analogical and/or virtual optical system are called all optical encrypted images.

In a previous contribution in this area, we have reported a successful creation of a monochromatic movie reproduced in real-time [1]. We must synchronize the output to reconstruct an encrypted movie using all optical encrypted images. The synchronization is crucial to display the information at a right speed and in real-time.

The usefulness of this method also offers new perspectives in encryption. Possible extensions include the use of unitary transformations other than the Fourier transform, incorporation of watermarks, an additional level of encryption due to appropriate choice of non-uniform theta-modulation angles, a systematic study of the stability of the encryption-decryption procedure with respect to noise, the incorporation of phase-retrieval concepts into the analysis, and an investigation of the role of partial coherence.

On the other hand, some applications demand the use of polychromatic processes and therefore a natural extension of our proposal leads to encompass full color scenes.

In the following, we describe how the use of the double random phase encryption architecture in combination with the theta modulation technique allows implementing color dynamical encryption procedures.

As it is well known, in 4*f* encrypting architectures, input information is encoded into white noise with two random diffusers, which are located both at the input plane and at the Fourier transforming plane [2, 3]. It should be pointed out that not only the key code mask must be known in the decryption step, but also the optical parameters (polarization, wavelength, etc) act as extra encoding keys in the same way as the mentioned key mask. The key code mask positions [4] or some optical parameters [5] could be use to encrypt multiple data in the same medium. In a multiplexing procedure, each right set of the mentioned elements is able to decrypt each image at a time. In fact, in decryption procedures, the wave fronts convey the information corresponding to the several encrypted images. Therefore, the remaining non-decrypted information contributes as noise. Several attempts have been done in this direction in the conventional multiplexing approach with the unavoidable mentioned constrain. In Ref [4–6]. new encryption keys were introduced, like polarization state and random phase mask positions.

To overcome this problem, in Ref [1] an adequate conjunction of a multiplexing technique with a the theta modulation approach in an encryption scheme permits to remove the cumbersome inherent noise appearing due to the cross talk produced by the non-decrypted information. With this issue resolved, we were able to encrypt in the same medium a dynamical scene.

In optical encryption-decryption procedures, when a monochromatic light is used to illuminate a color image during the encryption step, color information is lost. It is evident that a color image provides more information than just a gray level image. In recent years, the encryption scheme of color images [7–9] has been analyzed based on different methods. To encrypt a color image, the three color components (red, green and blue) must be considered. We implemented an approach to color image encryption based on a JTC architecture [10–12].

Our new proposed strategy consists on using the three basic chromatic channels, but separately encrypting each one of them.

In some experimental cases, optoelectronic systems are necessary to combine the chromatic channels in a practical way. This last implies that the all optical implementation is

#145481 - $15.00 USD Received 6 Apr 2011; revised 3 Jun 2011; accepted 20 Jun 2011; published 5 Jul 2011

no longer possible in real-time. The underlying problem is to adjust the phase mask magnifications to compensate the different chromatic channels. It is important to remark that in our approach we think in using only one encrypting mask to save resources. Therefore, the chromatic magnification issue is solved by using the three channels separately with the same phase mask replica in every single channel. Indirectly we avoid the multiplexing of the chromatic channel into a single medium. The reason to avoid this multiplexing is the impossibility to recombine the whole picture in real-time as the multiplexing force to sequentially decoded every single channel and not in parallel thus breaking the decoding possibility in real-time.

In other optical set ups, the focal lengths of the lenses and the distances from input planes to the lenses should be carefully chosen in each color channel. In this way, we make sure that the three components of the color image are recovered at the same plane and with the same size. We see that algorithm solutions either to image rescaling or to fix pixel mismatching do not represent valid alternatives in the concept of an all optical procedure, because they do not show the physical limitation arising from the actual speckle patterns, diffraction, etc.

Other implementations as phase shifting techniques are not appropriate to be used in dynamical color encryption procedures. Note that any phase shifting technique is wavelength-dependent; therefore the implementation would alter the real-time decrypting operation. It is important to remark once again that the dynamic procedure is practically implemented thanks to the theta modulation technique. We recall that this technique is applied on the encrypted image without altering the encrypting procedure in any of their steps.

Summarizing, in this contribution we extent the concept of all optical encrypted movie to encrypt a dynamical phenomenon in color with the reconstruction in real-time. As a way to analyze the practical implementation, we select to describe the influence of the pupil aperture on the movie extent and the consequent limitation on the frequency content on the input information. We present examples to confirm the validity of the approach.

2. Procedure description

We first briefly describe the basic approach employed in Ref [1]. We use the conventional 4*f* double random phase encoding architecture [6], besides synchronizing the frames sequence that compose a dynamic scene constituting a movie. We use the same encoding mask and a virtual optical system to encrypt every frame. At the same time we introduce the tetha modulation technique to modulate every encrypted frame with gratings of different pitches and orientations before multiplexing the sequence. In this way, during decryption the theta modulation technique will help in spatially separating the different frames avoiding overlapping. We 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. A Fourier transform (FT) of the encrypted input reveals the existence of paired spots belonging to each frame located at a different spatial position. 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, thus avoiding cross talk. Finally, we proceed with the classical decoding of each single frame for the 4*f* decrypting architecture. The entire procedure leads to clearly visualize each single frame without the influence of the others.

The next step to extend this application to encrypt a color movie is to define the procedure for every single color frame. Basically, the color information on every frame can be separated into its RGB (red R, green G and blue B) components. Afterwards, we can identify these components as single channels where we can operate by following the technique above described.

The final user receives therefore the three separate color channels encrypted information and a single key code mask employed for all frames and all channels. The success of the procedure relays on the automatic synchronization which is produced independently at the

#145481 - $15.00 USD Received 6 Apr 2011; revised 3 Jun 2011; accepted 20 Jun 2011; published 5 Jul 2011

decryption machine for each channel. The adequate synchronization allows the convenient color movie reconstruction in real time.

We introduce in Fig. 1 the encryption procedure along with the mathematical expressions that represent the different steps involved in the method. Each color encrypted data E_i is multiplied by a sinusoidal grating G_i of pitch d_i which fulfills $d_i \ll S_t$ (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 M implies to encrypt *n* frames in the same medium. In Fig. 2 we include the filtering, synchronization and decryption steps that allow obtaining the final composed decrypted movie. In the same way the mathematical formulations associated to each one of these steps are included. In this way, we introduce for the first time a color crypto movie based on a whole optical approach.

During decryption step, for a determined color channel to recover the original information a phase conjugate operation must be carried out. Then, after this phase conjugation operation and another Fourier transform for instance, for the red channel it results,

$$\Im\left(M_R^*\right) = \Im\left(\sum_{i=1}^{n} E_{i_R}^* G_i^*\right) = \sum_{i=1}^{n}\left[\Im\left(E_{i_R}^*\right) \otimes \Im\left(G_i^*\right)\right] \qquad (1)$$

The Fourier transform 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 on the grating orientation and pitch and the size depends on the parameters of the optical system. We are storing *n* frames; therefore we are obtaining several diffracted spots. The filtering procedure F is performed on the Fourier plane, 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. (1) only one diffracted spot associated to $\Im\left(E_{i_R}^*\right)$ from the corresponding two symmetrically spots located around the center. Then, an inverse Fourier transform operation allows obtaining each conjugated encrypted frame $E_{i_R}^*$. As described in Fig. 2, the decoding process requires of another 4*f* scheme. At this step, the conventional decrypting procedure allows recovering the frame F_{i_R}. This operation must be sequentially carried out *n* times in order to decrypt all movie frames for each color channel.

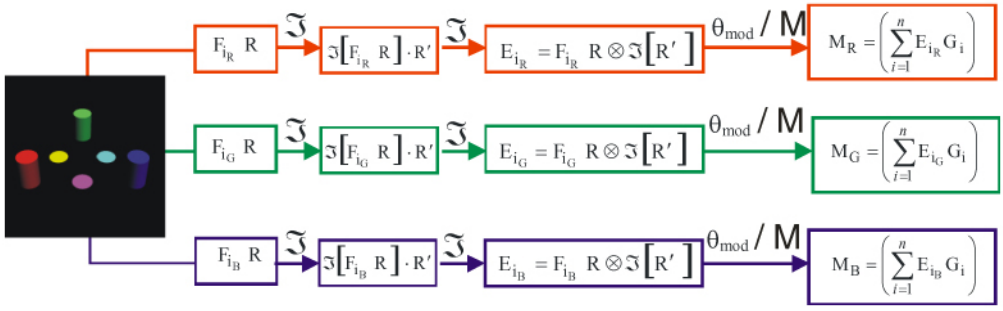


Fig. 1. Encryption, multiplexing and theta modulation processes ($\Im$: Fourier Transform operation; θ_{mod}: Theta modulation operation; M: multiplexing operation; $\otimes$ convolution operation, R: random phase mask, F_{iR}, F_{iG} and F_{iB}: i-th red, green and blue frames respectively; R´: random phase encoding mask, E_{iR}, E_{iG} and E_{iB}: i-th encrypted red, green and blue frames, respectively, G_i: i-th amplitude grating; M_R, M_G and M_B: multiplexed frames for the red, green and blue channels, respectively).

#145481 - $15.00 USD Received 6 Apr 2011; revised 3 Jun 2011; accepted 20 Jun 2011; published 5 Jul 2011

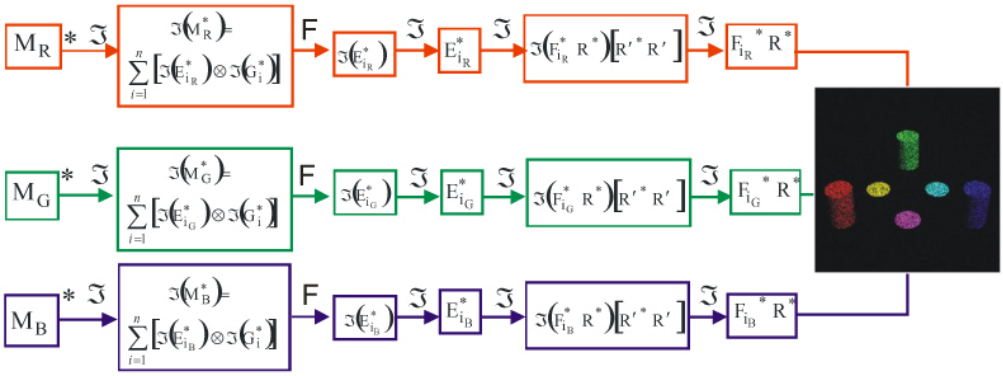


Fig. 2. Phase Conjugation, filtering and decoding processes (* phase conjugation operation, $\Im$: Fourier Transform operation; F: filtering operation). The remaining symbols are defined in Fig. 1.

Figure 3 shows two examples (a) moving cylinders and (c) a balancing bird correctly decrypted while in (b) and (d) we include the uncorrected decoded outputs. If we intend to reproduce the movie without placing the right decoding key R´ we get a boiling speckled movie. We display 10 frames per second to get a 3 seconds movie (Media 1—Media 4). Note that the speckle is ever present in the entire process as we are performing operations with virtual optical systems. Although there are several parameters that control the crypto movie reconstruction, we focus on the parameters governing the movie extent. We test for the two different color movies depicted in Fig. 3 the effect of the movie extent on its visualization.

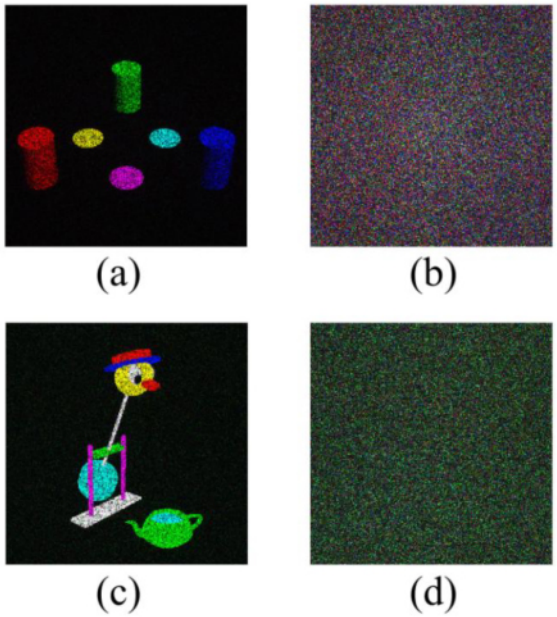


Fig. 3. (a) Right decrypted cylinder movie (Media 1); (b) Wrong decrypted cylinder movie (Media 2) (c) Right decrypted balancing bird movie (Media 3) and (b) Wrong decrypted balancing bird movie (Media 4).

In the encryption procedure, the theta modulation approach have been implemented, whose main advantage is the capability to concentrate the information of each frame in different frequency regions of the filtering plane. The spectral content of each movie frame is gathered into the diffraction spots associated with the respective frame. The pupil of the

#145481 - $15.00 USD Received 6 Apr 2011; revised 3 Jun 2011; accepted 20 Jun 2011; published 5 Jul 2011

optical encryption system limits the spectral content of each encoded frame at the filtering plane. The grating frequency and the pupil system parameters are selected so that the spectral components of the input frame are not overlapped with the other frames. The use of different pupil sizes allows controlling the optical movie extent. The number of spots is directly related to the number of frames to be stored along the process, in this sense we refer to the movie extent. As it is well known, the pupil size determines the cut off frequency for the input image content. Consequently, when we are thinking about the extent of a given movie we have to balance the frequency content on any given input frame versus the number of frames contained in the movie. This is evaluated in the following example where we selected two different objects. For the first case, as the input object is simpler, we can manage a larger number of frames than in the second case without further degrading the image. In either case, as pupil size decreases speckle size increases and in a certain way contributes to the degradation. However, the pupil cut off frequency itself imposes another constrain, thus limiting a larger extent without a serious image degradation. From the experimental results we can compare in Fig. 4 the influence of the pupil size on the final output for the selected input movies.

Figure 4 consist in six thumbnails showing the reconstruction of two movies with different extent. In the first line the input object are moving color cylinders. The three shown cases present an extent of 3 seconds, 4.8 seconds and 12.6 seconds. In going from left to right as extent increases we appreciate greater speckles. Besides, although the pupil size decreases there is not a significant lost in the image frequency.

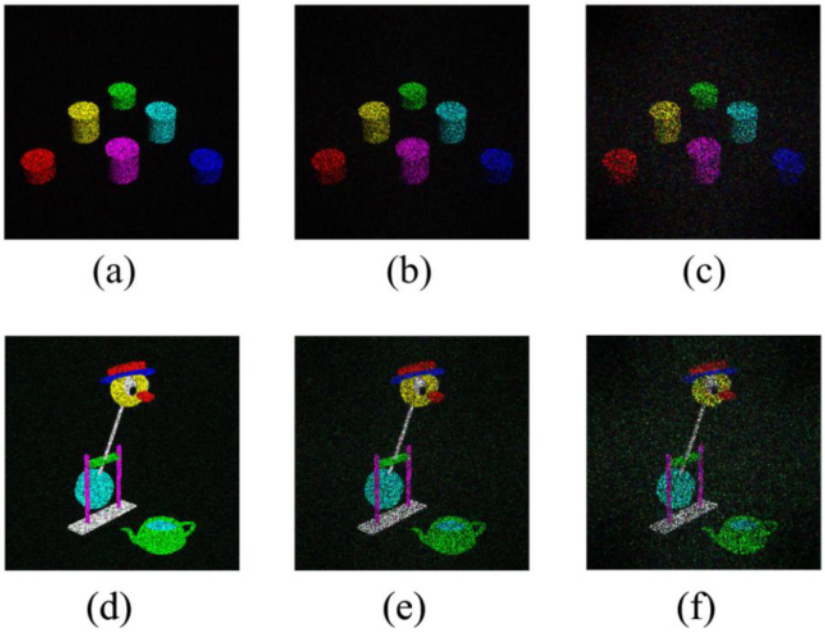
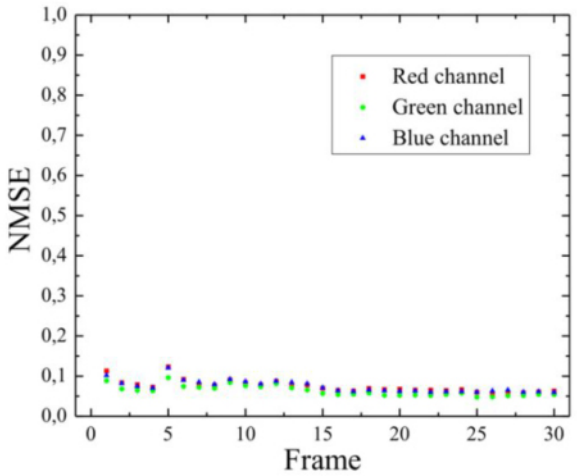


Fig. 4. Full decrypted movies for different extensions: (a) and (d) 3 seconds (Media 5 and Media 8, respectively) (b) and (e) 4.8 seconds (Media 6 and Media 9, respectively), (c) and (f) 12.6 seconds (Media 7 and Media 10, respectively).

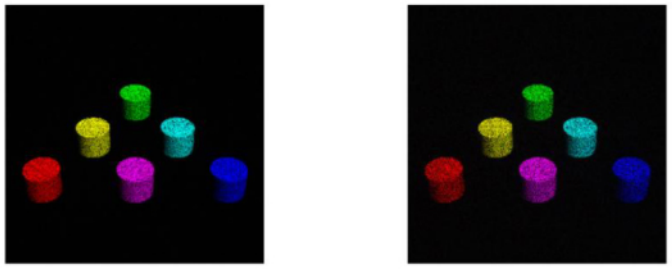
In the lower row, the speckle behavior is the same as a function of the pupil size, but additionally we perceive image degradation. The difference between these two cases relays in their original frequency content. As the cylinders exhibits less frequency content then the image degradation is less apparent. Regarding the quality check of the decrypted outputs, we perform an analysis based on a NRMS metric comparing every single decrypted frame with the corresponding output for a normal 4*f* single encrypting-decrypting procedure. In this way,

#145481 - $15.00 USD Received 6 Apr 2011; revised 3 Jun 2011; accepted 20 Jun 2011; published 5 Jul 2011

we observe the behavior depicted in Fig. 5 a) where we plot the NRMS for the three wavelengths thus obtaining values between 0.05 and 0.1, showing that there is no appreciable difference between the corresponding outputs. In Figs. 5 b) an c), we include the image of frame number 25th extracted from the multiplexing operation and the corresponding single decrypted frame for simple visual comparison. It is important to remark the ever present noise aspect on all decrypted images where a speckle phase mask is used as encoding key.



(a)



(b) (c)

Fig. 5. a) Normalized NMSE for all frames in the cylinder movie; b) decryption without multiplexing by using the conventional 4*f* architecture, c) decryption with multiplexing by using the proposed scheme.

On the other hand, it is important to mention the issue related to the risk of an attack from an intruder. We have to mention that if a system becomes vulnerable to certain attack, it does not imply that the proposed method does not work; it means that it must generate a new process to eliminate this vulnerability. In cryptanalysis, it is implicit that intruders already know the encryption algorithm and other resources, for example, an object–encrypted information pair. Using this information, they try to deduce the encryption key. In Optics, the equivalent to the encryption algorithm is the optical architecture together with the corresponding procedure. As leading examples, Carnicer et al. [13] and Peng et al. [14] retrieved exact solutions to the decryption key for chosen- and known- plaintext attacks on a 4f optical encrypting platform.

In the chosen-plaintext attack, the intruder launches an adequately designed input in the encryption-decryption machine in order to determine the key. In this case, the encryption

#145481 - $15.00 USD Received 6 Apr 2011; revised 3 Jun 2011; accepted 20 Jun 2011; published 5 Jul 2011

system will be at risk by repeatedly probing the machine with a set of chosen plaintexts proficiently designed to skip this problem.

In a known-plaintext attack, the intruder knows a single plaintext (input data)–ciphertext (encrypted data) pair besides the encryption method. In this attack, an intruder can access keys in the signal domain and the spatial frequency domain by using a phase retrieval algorithm.

However, multiplexing operations and the introduction of hiding parameters represent an alternative to enhance the security of a 4*f* encrypting procedure. Multiplexing encryption arrangements are immune to known attack procedures (chosen plain text, known plain text, brute force, blind) that rely on the existence of an input-encrypted image pair. In this sense, multiplexing actions increase the protection against intruders.

In our case, if a hacker gets one of the possible movie frame, he/she needs to find the corresponding encrypted order and the corresponding magnification and the involved geometrical parameters in order to conduct an attack. Therefore, as in other multiplexing options, the amount of combinations, which increases with the number of encoded frames, make it impossible to obtain the encoding mask. Besides, the intruder has to known the synchronization order to properly reconstruct the encoded material.

3. Conclusions

We presented an extension of a dynamical optical encrypting technique to color time evolving phenomena. We rely on the basic approach by theta modulating each chromatic channel for a given color input using the same encoding mask for all channels and all frames.

Unlike other color methods, we do not multiplex the chromatic channels into a single record because we want to keep the possibility of real-time decoding. We synchronize in parallel all chromatic channels at the same time during filtering and decoding, thus allowing the real-time decryption. We also tested, as an introductory extension to the many possible analysis of the technique, the movie extent as a function of the pupil aperture size. This parameter directly governs the number of spots at the decoding station. This limiting pupil also governs the cut-off frequency content; therefore this is a consequence to be balanced when producing the dynamical encrypting technique. Certainly, we envisage other alternatives that combined will influence on the movie quality, but so far this comprehensive analysis will be the subject of future contributions.

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).

#145481 - $15.00 USD Received 6 Apr 2011; revised 3 Jun 2011; accepted 20 Jun 2011; published 5 Jul 2011