Multiplexing of encrypted data using fractal masks

John F. Barrera,[1] Myrian Tebaldi,[2] Dafne Amaya,[2,3] Walter D. Furlan,[4] Juan A. Monsoriu,[5,*] 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*

[4]*Departamento de Óptica, Universitat de València, E-46100 Burjassot, Spain*

[5]*Centro de Tecnologías Físicas, Universitat Politècnica de València, E-46022 Valencia, Spain*

**Corresponding author: jmonsori@fis.upv.es*

Received March 5, 2012; revised April 27, 2012; accepted May 22, 2012; posted May 23, 2012 (Doc. ID 164124); published July 11, 2012

In this Letter, we present to the best of our knowledge a new all-optical technique for multiple-image encryption and multiplexing, based on fractal encrypting masks. The optical architecture is a joint transform correlator. The multiplexed encrypted data are stored in a photorefractive crystal. The fractal parameters of the key can be easily tuned to lead to a multiplexing operation without cross talk effects. Experimental results that support the potential of the method are presented. © 2012 Optical Society of America

OCIS codes: 070.0070, 070.4560.

Double random-phase encoding (DRPE) is the most popular optical encrypting technique. In DRPE, the random-phase mask that represents the security key can be placed either at Fourier [1] or Fresnel planes [2,3] in a 4*f* configuration, or in the input plane in a joint transform correlator (JTC) architecture [4]. However, it has been proven that optical encryption based on DRPE is vulnerable to different types of attacks. To enhance the security optical methods, we recently proposed a novel phase-encoded holographic encryption approach based on fractal zone plate (FZP) security keys [5]. In that contribution, we believe optical cryptography using diffractive optical elements was successfully demonstrated for the first time. The robustness and versatility of the method relies in the process of sending the encrypting mask to the authorized receiver, because it is not necessary to send the key itself as in the case of DRPE; instead, as FZPs are deterministic objects, we only need to send the constructing parameters, which also can be sent independently by multiple public open channels. Moreover, the use of FZP keys allow the employment of spatial light modulators to display them, resulting in easily reconfigurable optical encryption systems.

Optical encryption systems evolved into multiple-image encryption because, for the majority of data communications that take place today, several users must simultaneously share a common channel resource in a controlled, effective way. In general, multiplexing means encoding two or more images into a single one by optical or numerical techniques [6–11]. The usual multiplexed package is synthesized by superimposing individual encrypted images together. Digitally speaking, all the images are superimposed in one composite CCD frame, and each one of them can be independently reconstructed through a digital spatial filtering. This encryption strategy is time-consuming and sensitive to cross talk and noise effects. Optically, it is simple to understand the complexity of the procedure mainly depends on the optical configuration adopted for recording.

Nowadays, we are witnessing an increasing demand for practical multiplexing setups to produce encrypted videos or in smart packaging applications. For example, the first all-optical encrypted movie was presented recently [12]. In this movie, the sequence of encoded frames was multiplexed using theta modulation, and, after an appropriate filtering procedure, a virtual optics decryption procedure was applied to reverse the coding process. However, most of the reported proposals responding to the above mentioned demand present digital simulations to support the main ideas, and only a few provide true experimental evidence [9–11].

In optical multiple image encryption and multiplexing, noise and cross talk are also undesirable, but common, problems. To overcome noise effects, several approaches have been proposed. In particular Henao *et al.* [13] proposed a hybrid optodigital method, in which the position of the recovered object at the exit plane can be fully controlled, avoiding the background noise resulting from superposition of non-decrypted data over the recovered image. In addition, some efforts have been already made to provide techniques to efficiently reduce the amount of transmitted information avoiding cross talk, as required for modern applications.

In this Letter, we propose a multiplexed coding scheme with improved security that is able to perform decoding free from cross talk effects in real time. In our scheme, a JTC encryption system is employed. JTC systems are very suitable due to their simple implementation, robustness, and their easy application to several different images formats (black and white, gray level, or colored images). The highly secure encrypting key we use results from the combination of a random-phase mask with a FZP with variable lacunarity [14].

We demonstrate that this all-optical scheme is easily configurable to avoid cross talk, even for a large amount of multiplexed images. Additionally, since we only need to send a user the constructing parameters, but not the key itself, it is less vulnerable to a hacker attack than DRPE techniques.

Moreover, instead of using a single channel for sending the encoding mask, we can use as the same amount of channels as parameters to construct the fractal mask.

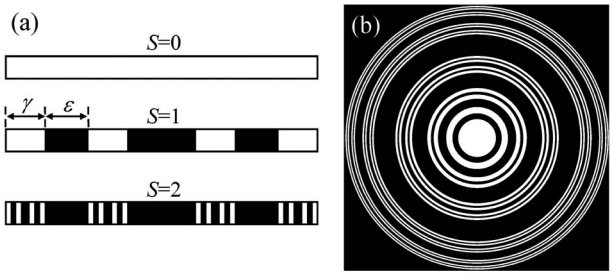

Fig. 1. (a) Fractal Cantor set ($N = 4$) developed up to level $S = 2$, constructed from the *initiator* segment $S = 0$, and the *generator* $S = 1$ [13] and (b) resulting FZP structured mask for $S = 2$.

This multichanneling option adds to the method's global security. Additionally, our proposal employs a photorefractive BTO crystal that allows fine dynamic data storage in a volume hologram and real-time readout. Our proposed technique could be useful to optimize the transmission of coded information between a recording head and a display unit in separate locations.

A FZP is a zone plate with a fractal structure constructed from a specific polyadic Cantor set [13]. As shown in Fig. 1, there are several parameters that can be varied in the FZP construction. The parameters that define a particular element of a given Cantor set are: the number (N) of copies of the *initiator* (a segment of unit length) into the *generator*, the scaling factor γ, the lacunarity ε (spacing between the copies of the scaled *initiator*), and the level of the set S [Fig. 1(a)].

The resulting FZP is a radially symmetric two-dimensional (2D) structure, composed of rings that are distributed following a given one-dimensional (1D) fractal structure along the square of the radial coordinate [Fig. 1(b)]. Note that there is an infinite number of possible combinations of the above parameters for the construction of a particular FZP. In this Letter, we describe how this feature can be profited in an experimental setup to construct different keys in a multiplexing encryption setup.

Figure 2(a) schematically depicts the architecture based on a JTC. At the input plane a spatial-light modulator (SLM) simultaneously displays a compound random-phase fractal key (located in the right window), and the input object attached to another random-phase mask (located in the left window). A BTO crystal (thickness: 8 mm, cut in the transverse electro-optic configuration) is placed at the joint power spectrum (JPS) plane. The distance between windows is 12 mm, and each window size is 6 mm × 6 mm.

This configuration generates a fringe pitch of approximately 10 μm at the crystal volume. Then, the JPSs corresponding to different objects and the corresponding keys are stored sequentially in the photorefractive crystal. The encrypted information is encoded in the crystal as a spatial distribution of electric field strength. To decode each entry, a shutter sequentially cancels the object aperture in such a way that the BTO crystal is illuminated only by the Fourier transform of the combined key. Then, the stack of reconstructed images are registered by a CCD camera at the back focal plane of the lens (L_2). In the experiment, a three-exposure

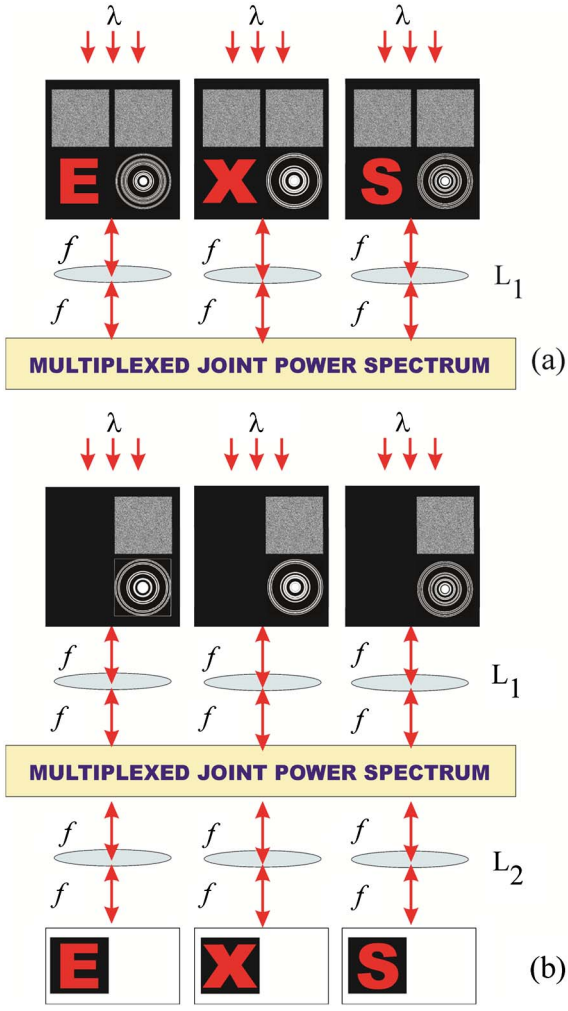

Fig. 2. (Color online) Experimental arrangement: (a) write-in step and (b) read-out step (He–Ne laser, $\lambda = 632.8$ nm), L_1 and L_2: lenses with focal lengths of 100 and 50 mm, respectively). The multiplexed joint power spectrum is stored in a BTO crystal.

multiplexing operation is implemented. A record–erase cycle is performed to optimize the read-out diffraction efficiency of all decrypted inputs.

The recording time is varied in each exposure to obtain comparable efficiencies in all recovered data. The first recording time is 6 min to ensure a steady-state diffraction efficiency. The storing times for the second and third multiplexed data are 2.5 min and 1 min, respectively. As the BTO crystal is a volume-recording medium, it is necessary to consider a three-dimensional (3D) correlation-length analysis to determine the system's sensitivity to the fractal mask change.

Figure 3 shows the three different fractal masks employed in the experiment and the corresponding decrypted objects. Note that these masks correspond to the same Cantor family ($N = 4$, $S = 2$, and $\gamma = 1/7$) but they differ only on the lacunarity. Despite only the lacunarity being the single free parameter, the results are free from the effects of cross talk. These experimental results demonstrate the feasibility of our proposal.

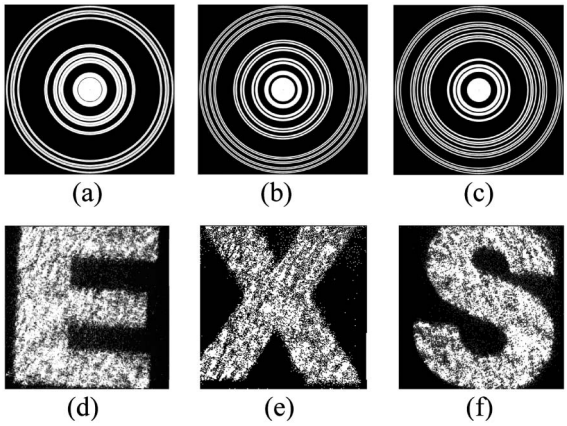

Fig. 3. Upper row shows the fractal masks with parameters $N = 4$, $S = 2$, $\gamma = 1/7$, and lacunarity (a) $\varepsilon = 0.01$, (b) $\varepsilon = 0.07$, and (c) $\varepsilon = 0.19$. Bottom row, (d), (e), (f), corresponding decrypted objects.

This result allows other possibilities to be explored to improve the performance of the process, as, for example, the maximum data to be securely handled with a single parameter variation. In fact, as we demonstrated, the restriction of fixing all parameters except one for all the keys needed in a particular application seems to be a real handicap of the method. Moreover, the reported experimental technique is a simply way to manage the FZP parameters, which avoids any possible image superposition during demultiplexing. For instance, instead of using the lacunarity as the parameter to be tuned in our multiplexing experiment, it is possible to select several values for γ. This feature is a key point that underscores the versatility of the method.

This research was performed under grants TWAS-UNESCO Associateship Scheme at Centres of Excellence in the South, CONICET No. 0863 (Argentina), ANCYT PICT 1167 (Argentina), and Facultad de Ingeniería, Universidad Nacional de La Plata No. 11/I125 (Argentina), Sostenibilidad 2011-2012, and CODI (Universidad de Antioquia-Colombia). W. D. Furlan and J. A. Monsoriua acknowledge financial support from Ministerio de Economía y Competitividad (grant FIS2011-23175), Generalitat Valenciana (grant PROMETEO2009-077), and Universitat Politècnica de Valencia (grants PAID-05-11 and PAID-02-11), Spain.

References

1. P. Refregier and B. Javidi, Opt. Lett. **20**, 767 (1995).
2. O. Matoba and B. Javidi, Opt. Lett. **24**, 762 (1999).
3. G. Unnikrishnan, J. Joseph, and K. Singh, Opt. Lett. **25**, 887 (2000).
4. T. Nomura and B. Javidi, Opt. Eng. **39**, 2031 (2000).
5. M. Tebaldi, W. D. Furlan, R. Torroba, and N. Bolognini, Opt. Lett. **34**, 316 (2009).
6. G. Situ and J. Zhang, Opt. Lett. **30**, 1306 (2005).
7. Z. Liu and S. Liu, Opt. Commun. **275**, 324 (2007).
8. H. E. Hwang, H. T. Chang, and W. N. Lie, Opt. Lett. **34**, 3917 (2009).
9. O. Matoba and B. Javidi, Appl. Opt. **38**, 7288 (1999).
10. J. F. Barrera, R. Henao, M. Tebaldi, R. Torroba, and N. Bolognini, Opt. Commun. **259**, 532 (2006).
11. R. Henao, E. Rueda, J. F. Barrera, and R. Torroba, Opt. Lett. **35**, 333 (2010).
12. J. F. Barrera, R. Henao, M. Tebaldi, R. Torroba, and N. Bolognini, Opt. Commun. **261**, 29 (2006).
13. F. Mosso, J. F. Barrera, M. Tebaldi, N. Bolognini, and R. Torroba, Opt. Express **19**, 5706 (2011).
14. J. A. Monsoriu, W. D. Furlan, and G. Saavedra, Opt. Express **12**, 4227 (2004).