Optical-data storage-readout technique based on fractal encrypting masks

Myrian Tebaldi,[1,2] Walter D. Furlan,[3,*] Roberto Torroba,[1,2] and Néstor Bolognini[1,2,4]

[1]*Centro de Investigaciones Ópticas (CONICET-CIC), P.O. Box 124, La Plata (1900), Argentina*
[2]*UID OPTIMO, Facultad Ingeniería, Universidad Nacional de La Plata, 1900 La Plata, Argentina*
[3]*Departamento de Óptica, Universitat de València, E-46100 Burjassot, Spain*
[4]*Facultad Ciencias Exactas, Universidad Nacional de La Plata, 1900 La Plata, Argentina*
**Corresponding author: walter.furlan@uv.es*

Received September 8, 2008; revised December 1, 2008; accepted December 8, 2008;
posted December 16, 2008 (Doc. ID 101343); published January 27, 2009

We propose the use of fractal structured diffractive masks as keys in secure storage-readout systems. A joint transform correlator based on a photorefractive crystal in the Fourier domain is implemented to perform encryption and decryption. We discuss the advantages of encrypting information using this kind of deterministic keys in comparison to conventional random phase masks. Preliminary experimental results are presented to demonstrate the effectiveness of the proposed system. © 2009 Optical Society of America

OCIS codes: 070.0070, 210.1635.

Several authors have proposed different methods for encrypting 2D information with linear optical systems. Optical security techniques involve tasks such as encryption, recognition, secure identification, and/or verification. The bases of optical security technology are complex processes, where the signals are hidden to human perception to keep them secret during the information sending. Traditional methods relay on the double-random-phase encoding system under a classical 4*f* optical architecture [1–3]. The idea is to encode a primary image into a white-noise-like distribution employing a random phase key (RPK) in the input plane and another one in the Fourier plane. The encryption and decryption stages can both be implemented either optically or electronically. Nevertheless, it has been proved that optical encryption based on double RPK is vulnerable to different types of attacks [4,5], compromising the security of these optical encryption techniques. As an alternative to RPKs, structured phase keys, i.e., keys with a shape given by a specific configuration, were proposed, and their performance was numerically validated [6].

An encoding technique using the Joint Transform Correlator architecture (JTC) was first proposed by Nomura and Javidi [7]. The optical implementation of the JTC architecture is simple in comparison with double-random-phase encoding, because it is an inherent two-step holographic setup avoiding the use of complex conjugate waves, and thus it is especially suitable for real-time applications. Moreover, multiple secure data recording is also possible in a JTC scheme [8].

To further improve the optical encrypting methods, in this Letter we merge the two main features highlighted above by the use of a novel kind of structured masks, acting as key codes in a JTC optical architecture. This approach is used to present, which are, to the best of our knowledge, the first experimental results of optical cryptography using diffractive optical elements. In addition, the diffractive element we propose for this application is a fractal zone plate (FrZP) [9]. FrZPs have several degrees of freedom for their design that are profited in our proposal to give extra security parameters. In this way, with our approach, there will be no need for sending the mask itself (the main reason of the vulnerability of RPKs) but a simple set of numerical parameters to reconstruct it, thus reducing the chance for losses in the transmission stage. Therefore FrZPs, with their robustness and simplicity, fulfill the encrypting mask requirements for high security and easiness respectively.

The construction of a general FrZP is shown in Fig. 1. The first step consists in the design of the corresponding Cantor fractal set. It starts by defining a straight-line segment of unit length called *initiator* (stage $S=0$). Next, at stage $S=1$, the *generator* of the set is constructed by N nonoverlapping copies of the initiator ($N=4$ in the figure), each one with a scale $\gamma<1$. At the following stages ($S=2,3,\ldots$), the generation process is repeated over and over again for each segment in the previous stage. To characterize the resulting Cantor set it is necessary to specify the distribution of the N copies into the unit length segment. Two copies are fixed at the ends of the generator, while the position of the others is given by the width of outermost gap in the first stage, ε (see Fig. 1). This parameter specifies the lacunarity of the resulting structure. Thus there exists a relationship among N, γ, and the value of ε [10]. For $N=4$, the extension of the central gap varies between zero (for $2\varepsilon=1-4\gamma$) and $1-4\gamma$ (for $\varepsilon=0$). Any fractal structure can be constructed in this way, and the result can be used to define a binary 1D compact supported function $q(\varsigma)$, as represented in Fig. 2(a). The next step in

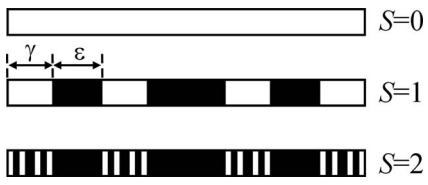


Fig. 1. Construction of a 1D fractal binary structure binary function with the following parameters: $N=4$, $S=2$. γ is the scale factor and ε is the lacunarity.

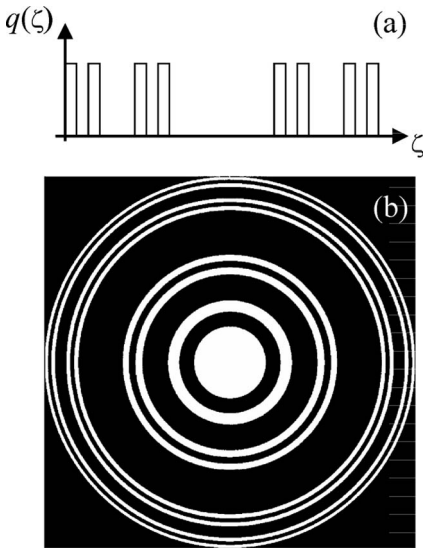


Fig. 2. Encryption-key mask-generation procedure based on a 1D fractal. FrZP is built by using the methods detailed in the main text: (a) compact-supported fractal function, (b) resulting FrZP structured mask.

the construction of a FrZP is to perform the change of variables $\varsigma=(r/a)^2$ to obtain a new function that represents the radial distribution of the zones in a 2D zone plate of radius a, r being the radial variable. The final result is the FrZP represented in Fig. 2(b). Summarizing, the number of stages S, the generation number N, the lacunarity ε, and the scale γ are the independent parameters in the construction of a given FrZP (see [10] for further details).

The optical setup we used to perform secure data storage-readout experiment is depicted in Fig. 3. It represents a JTC correlator in which the recording medium is a photorefractive silenite BaTiO (BTO) crystal. A BTO crystal, cut in the transverse electro-optic configuration, is employed. The directions $(1\bar{1}0)$, (001), and (110) of the crystal coincide with the

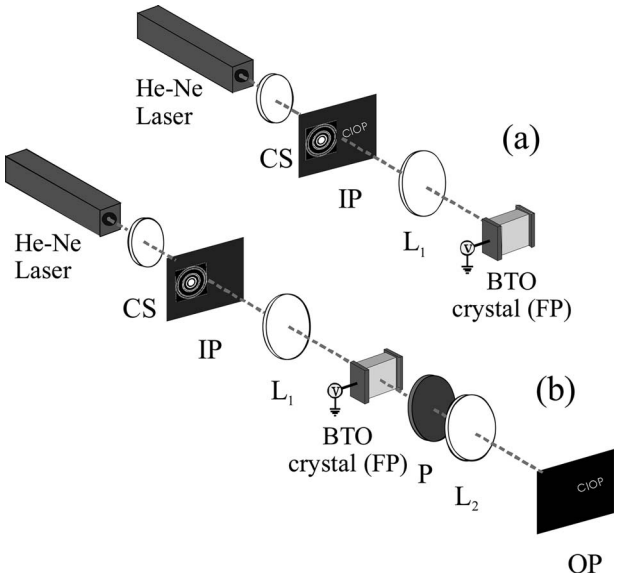
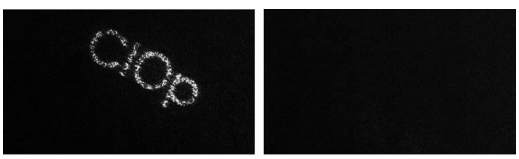


Fig. 3. JTC scheme used in the experiment: (a) write-in step, (b) read-out step. CS, collimation system; IP, input plane; L_1 and L_2, lenses; P, polarizer; FP, Fourier frequency plane; OP, output plane.

XYZ axes, and the linear dimensions are $L_X=L_Y=L_Z=8$ mm. As presented in Fig. 3(a), at the input plane (IP)—illuminated with a collimated coherent light beam—the key FrZP mask, $k(x,y)$, and the object to be encrypted, $t(x,y)$, were displayed separated by a distance $2a=12$ mm. The FrZP used for the key was constructed by using the following parameters: $S=3$, $N=2$, $\gamma=1/3$, and $\varepsilon=1/3$. In our experiment the object was an amplitude mask with the word "CIOp" multiplied by a random-phase mask. The 10 mm focal length lens L_1 Fourier transforms the IP information at the Fourier frequency plane (FP), giving the joint power spectrum (JPS) $|\Im\{k(x+a,y)+t(x-a,y)\}|^2$, which is recorded in the BTO crystal as a volumetric modulation of its refractive index. In our proposal, as the period fringes involved are 10 μm on average, the diffusion transport mechanism is negligible, and drift dominates. Then, a voltage of 7 kV was applied between the $(1\bar{1}0)$ crystal faces.

To reconstruct the input data, only the window containing the key mask is employed [see Fig. 3(b)], and the stored JPS is placed at the focal plane of lens L_1. The wavefront propagating through the crystal is Fourier transformed by the lens L_2 (10 mm focal length) to give the noise-free recovered image of $t(x,y)$, placed at a distance a from the coordinate center at the output plane (OP) plane. Figure 4(a) is the decrypted image that shows the successfully recovered input data. Figure 4(b) displays the reconstructed image when a wrong key (a conventional Fresnel zone plate) is employed in decryption step. In this case, the reconstruction fails to recover the original input object.

We also studied the evolution of the crystal efficiency during write-in and read-out (encryption–decryption steps). In the write-in step it is important to get the saturation level in the index grating depth, which can be monitored by the diffraction efficiency evolution. In our experiment, the saturation value was reached after approximately 1000 s by using an incident power of 40 μW. We observed that after 1 h of continuous readout, the diffraction efficiency drops to about 15% of the saturation diffraction efficiency in this medium. In our case, we used a BTO silenite crystal owing to its high sensitivity, allowing thereby the use of very low input power. A BTO crystal permits the use of a He–Ne laser as light source because of its wide spectral sensitivity range. BTO crystals also allow fast storage procedures, although the stored information degrades with time. However, if



(a) (b)

Fig. 4. (a) Experimental result showing the right reconstruction of the encrypted input data: the word "CIOp." (b) System output when the correct decrypting parameters are mismatched.

we decline to use low power, we can store the JPS in a LiNbO3:Fe crystal in which the temporal degradation is reduced. Moreover, to get a nearly permanent storing of the JPS, a high-temperature fixing procedure could be done (as demonstrated in [11]). On the other hand, the crystals of the silenite family have low diffraction efficiency in comparison with LiNbO3. However, it should be emphasized that the barium silicate, $Be_{12}GeO_{12}$, and BTO crystals considerably improve the signal-to-noise ratio in the reconstructed output owing to their polarization properties, representing an advantageous recording media in encryption–decryption arrangement [12].

It should be noted that, for the purposes of the experimental demonstration, we used binary amplitude key FrZP masks, although we are in fact not limited to this case. Actually, the encryption technique we present could also be applied to systems in which multiple amplitude and phase levels can be used for the masks.

Summarizing, in this contribution optical cryptography using diffractive optical elements has been successfully demonstrated for the first time, to our knowledge. In our experiment we also introduced a novel phase-encoded holographic encryption approach based on FrZP. In a general comparison between the encryption holographic methods using either a conventional RPK or a deterministic FrZP, we emphasize that, if a FrZP is used as a key to control the phase encoding, the system becomes more robust. The reason can be found in the process of sending the encrypting mask to the authorized receiver. Employing a conventional RPK the complex key itself needs to be transmitted in a single step by a single channel, risking to be lost, broken, or polluted by noise. Alternatively, by using a FrZP we can prevent these failures, because we do not need to send the key itself; instead we only need to send the constructing parameters (the fractal order, the lacunarity, the dimension, etc.) that can also be sent independently by multiple public open channels. In this sense conventional RPKs are more vulnerable than FrZPs. With regard to versatility, although the key itself has almost the same degree of security of a RPK, in the sense that it is a complex 2D object, it is conceptually different, and its deterministic feature provides an extra degree of versatility. For example, the use of FrZP keys allow the employment of spatial light modulators to display them, resulting in easily reconfigurable optical encryption systems.

As a concluding remark, we stress that every encrypting method presents security flaws, depending mainly on the previous knowledge that the cryptanalyst has about the encrypting machinery and encoding scheme. Therefore, the development of alternative nonusual approaches always results in an improvement in comparison with the previous encrypting schemes. We are aware that the FrZP architecture could not be immune to a future attacking strategy, but its versatility and robustness against pollution, breakage, and losses renders it as a promising alternative.

This research was performed under the grants CONICET 5995, ANCYT PICT 1167, and Facultad Ingeniería, Universidad Nacional de La Plata (Argentina). W. D. Furlan acknowledges financial support from Plan Nacional I + D + I, Ministerio de Ciencia y Tecnología, Spain (grants DPI 2006-8309 and DPI 2008-02953).

References

1. P. Refregier and B. Javidi, Opt. Lett. **20**, 767 (1995).
2. G. Unnikrishnan, J. Joseph, and K. Singh, Opt. Lett. **25**, 887 (2000).
3. J. F. Barrera, R. Henao, M. Tebaldi, R. Torroba, and N. Bolognini, Opt. Commun. **276**, 231 (2007).
4. A. Carnicer, M. Montes-Usategui, S. Arcos, and I. Juvells, Opt. Lett. **30**, 1644 (2005).
5. X. Peng, P. Zhang, H. Wei, and B. Yu, Opt. Lett. **31**, 1044 (2006).
6. J. F. Barrera, R. Henao, and R. Torroba, Opt. Commun. **248**, 35 (2005).
7. T. Nomura and B. Javidi, Appl. Opt. **39**, 4783 (2000).
8. D. Amaya, M. Tebaldi, R. Torroba, and N. Bolognini, J. Opt. A **10**, 104031 (2008).
9. G. Saavedra, W. D. Furlan, and J. A. Monsoriu, Opt. Lett. **28**, 971 (2003).
10. J. A. Monsoriu, G. Saavedra, and W. D. Furlan, Opt. Express **12**, 4227 (2004).
11. E. M. De Miguel-Sanz, M. Tebaldi, S. Granieri, N. Bolognini, and L. Arizmendi, Appl. Phys. B **70**, 379 (2000).
12. M. Tebaldi, M. C. Lasprilla, and N. Bolognini, Optik (Jena) **110**, 127 (1999).