Available online at www.sciencedirect.com
SCIENCE DIRECT®
Optics Communications 248 (2005) 35–40
OPTICS COMMUNICATIONS
www.elsevier.com/locate/optcom

Optical encryption method using toroidal zone plates

John Fredy Barrera [a,*], Rodrigo Henao [a], Roberto Torroba [b]

[a] Instituto de Física, Universidad de Antioquia, Calle 67 53-108, A.A. 1226 Medellín, Colombia
[b] Centro de Investigaciones Opticas (CIOp) and OPTIMO, Facultad de Ingeniería, Universidad Nacional de la Plata, C.C 124, B1902WAB La Plata, Argentina

Received 7 August 2004; received in revised form 23 November 2004; accepted 23 November 2004

Abstract

We present the implementation of an optical encryption method using zone plates. The optical security system is based on a computer generated phase mask. In particular, for this proposal the selected phase mask is a toroidal zone plate. In the encryption process we use an optical processor where this phase mask is placed in the Fourier plane of the object to be encrypted. The original-data recovering is performed by digital reconstruction using the conjugate of the encryption mask. The different phase encoding procedures show that the diffraction efficiency of zone plates is relevant to the decryption process. Computer simulations are presented to demonstrate the validity of the method.

PACS: 42.30.−d; 42.30.Yc
Keywords: Optical data processing; Encryption; Optical security

1. Introduction

Optical information processing entered in an increasing competition to demonstrate it great potentials as a promising tool in security applications [1–6]. Not only all optical [7] and hybrid [8,9] methods are suggested for data encryption and decryption. Non-linear joint transform correlators [10] and computer-generated holograms [11] are considered. Its importance comes not just for encryption but also in hiding information. Optical encoding has the added property that a large amount of data can be stored or retrieved in parallel and at high speed. Encoding techniques include the use of random phase [12], polarization sensitive techniques [13], different kinds of digital techniques [14], etc. All of them represent an opportunity to compete with digital processors for doing the verification. These setups can be considered as the basis for the design of real time optical security devices.

* Corresponding author. Tel.: +5742105630; fax: +5742105666.
E-mail addresses: jbarrera@fisica.udea.edu.co (J.F. Barrera), robertot@ciop.unlp.edu.ar (R. Torroba).

0030-4018/$ - see front matter © 2004 Elsevier B.V. All rights reserved.
doi:10.1016/j.optcom.2004.11.086

Basically, the major purpose of information encryption is that one is able to encode information to be sent in such a way that it is difficult for unauthorized party to decode this information without having a proper key(s). In a security system, the properties of difficult duplication and large tolerance to data loss during the decryption process are of ultimate concern. Random phase masks are easy to produce but difficult to duplicate without the original information. Regarding the use of phase masks, several methods were explored to expand the options in multiple keys methods. Besides, an extensive discussion on the comparative advantages between phase and amplitude encryption can be found in Towghi et al. [15]. It is shown that phase encryption exhibits a better performance with respect to mean-square errors calculations, especially in presence of additive noise. Another benefit of phase masks is that they are energy preserving, in the sense that no absorption is introduced, which is not the case in amplitude-based masks. Additional advantages of phase masks are that they exhibit a better optical efficiency; provide better robustness to variations of the luminance of a scene and a better discrimination capability.

We suggest that phase masks can be catalogued in two categories: random phase masks and structured phase masks. In the first group speckle patterns are classical examples. In the second we can define those masks with a shape given by a specific configuration. In our proposal we are introducing toroidal phase masks as a new alternative. Unlike random phase masks, toroidal masks are easier to position in the decoding step, as they provide their own centering mark (on axis focal ring when illuminated by a parallel beam). In addition, they offer several advantages over previous proposals: they are very difficult to replicate, as they are diffractive optical elements, we can also manipulate the diffraction efficiency depending on the requirements of the optical systems and they have the property of multiple keys in a single mask as extra security parameters.

The optical implementation of the encryption technique is based on an object first optical Fourier transform, superposed on the toroidal zone plate (TZP). A second optical Fourier transform gives rise to the encrypted image. The digital decryption can be done by the Fourier transform of the encrypted image and then multiplying it by the complex conjugate of the toroidal mask. Finally, another Fourier transform yields to the decrypted result.

We stress that the security in our encryption procedure lays in the TZP itself. This TZP acts as a "structured phase encoding mask"; and should not be confused as an additional particular lens to the encoding setup. If unauthorized third parties try to recover the original image with a TZP different from the one used during the encryption, he/she will simply fail. On the other hand, for an authorized receiver, the "lens-like structure" of our encoding mask will help in the right positioning in the decoding setup. This advantage is not present when working with "non-structured phase masks" as in the case of speckle patterns.

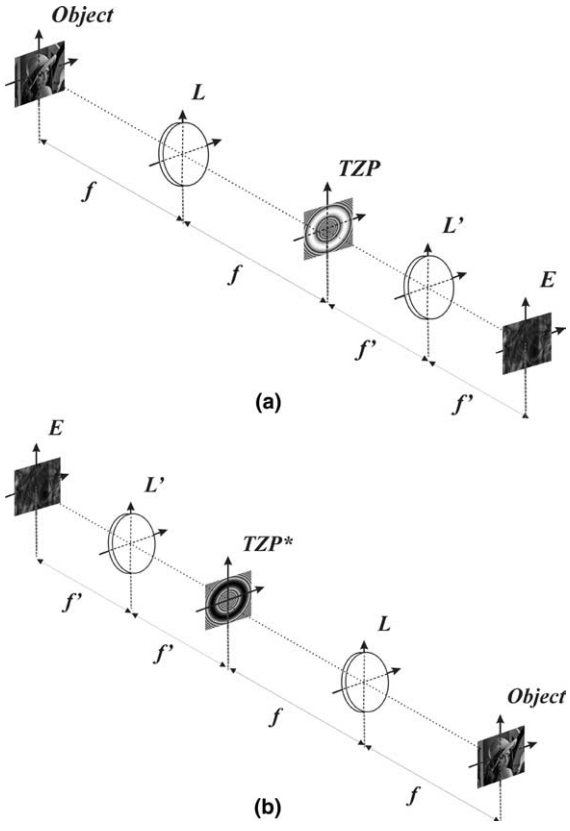

Fig. 1. (a) The optical setup used for image encryption, lenses L and L′ have focal lengths f and f', respectively, TZP represents the toroidal zone plate, and E is the resulting encrypted image. (b) The decryption stage, where L, L′ and E are the same as above, and TZP∗ means the complex conjugate of TZP.

In the present contribution, we will show the theoretical background of toroidal lenses, the principle of our method and the computer simulations that support our proposal. Finally, a discussion on the influence of the diffraction efficiency in the decryption process is addressed.

2. Theoretical background and principle of the method

The complex amplitude distribution produced on a plane $z = 0$ by a converging toroidal wave front can be written as

$$U(r) = \exp\left(\frac{-ik}{2f_T}(r - r_o)^2\right), \quad (1)$$

where the optical axis is assumed to be coincident with the direction z, $k = 2\pi/\lambda$, λ being the wavelength, and f_T and r_o are positive real constants. For convenience, other amplitude factors have been set constant and equal to 1. It is easy to show that if such a wavefront propagates in a homogeneous medium, then it gives rise to a ring focus of radius r_o located at the plane $z = f_T$ [16].

We now recall the scheme in Fig. 1(a). A monochromatic plane wave illuminates the original image (Object) positioned at the back focal plane

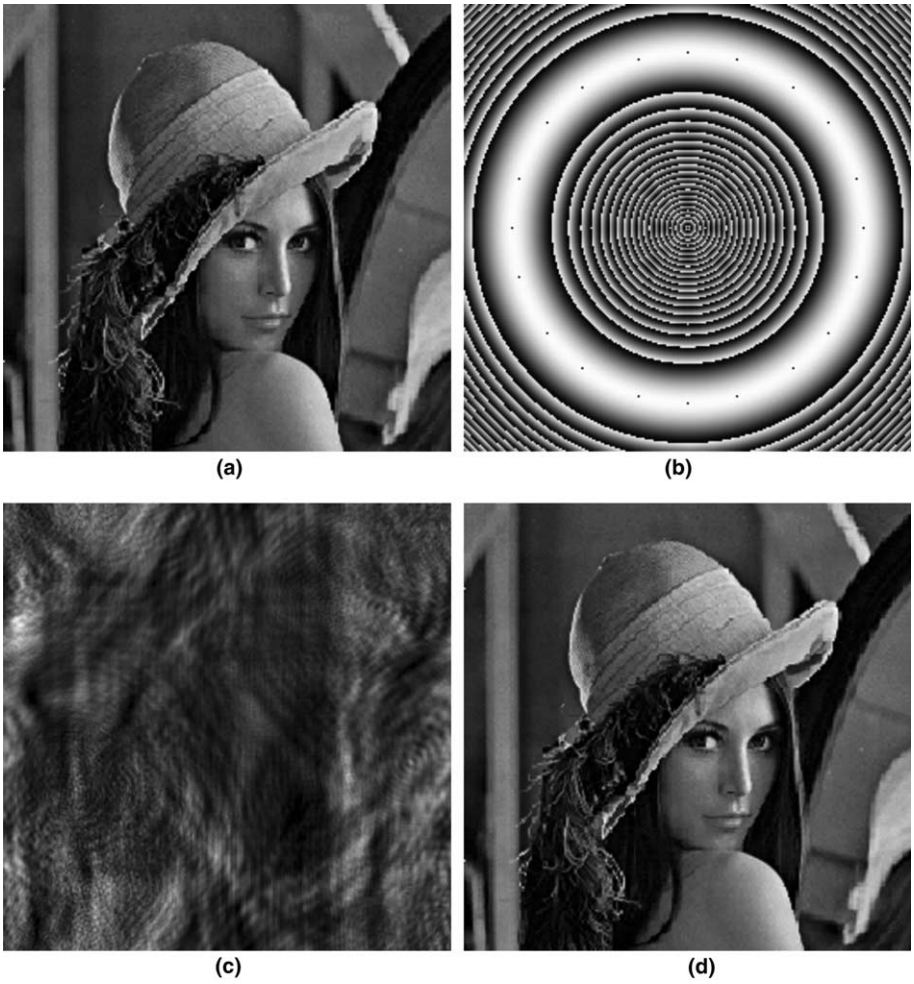

Fig. 2. Results of computer simulation: (a) original image, (b) toroidal zone plate used for the encryption- right key ($f = 4$ cm), (c) encrypted image, and (d) retrieved image by the right decoding key.

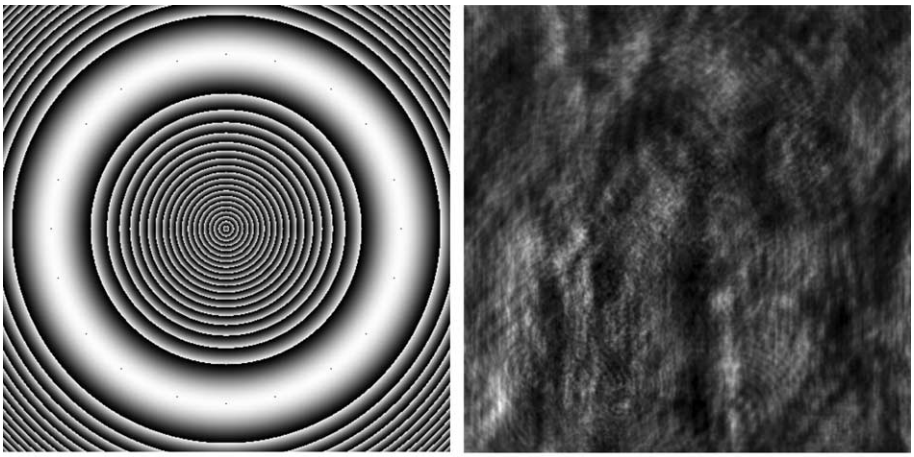

Fig. 3. Result obtained using a zone plate different from the original encoding key: (a) wrong key and (b) retrieved image using the wrong key of (a).

of lens L. To avoid mathematical difficulties in this paper, we ignore an input phase mask [12]. At the Fourier plane a toroidal phase plate is placed. Another lens L′ performs a second Fourier transform to give rise to the encrypted image E. The digital decryption process is represented by the optical scheme of Fig. 1(b). The Fourier transform of the encrypted image E is performed by the lens L′. At the Fourier plane the complex conjugate of the toroidal mask used in the encryption process TZP* (the right key) is placed, and finally the lens L performs the final recovering Fourier transform. Besides, there are no relations among the focal lengths of L, L′ and TZP. We stress that this procedure, although optically represented, is performed digitally.

Let x and y denoted the spatial coordinates, and let μ and η denote the Fourier domain coordinates. If we represent by $I(\mu,\eta)$ the Fourier transform of object intensity $i(x,y)$ and $T(\mu,\eta)$ represents the amplitude of the toroidal phase mask placed at the Fourier plane, the field emerging from the Fourier domain is expressed by

$$H(\mu,\eta) = (I(\mu,\eta)\cdot T(\mu,\eta)). \tag{2}$$

After performing the second transform we get

$$K(x,y) = (i(x,y) * t(x,y)), \tag{3}$$

where $K(x,y)$ and $t(x,y)$ are the Fourier transforms of $H(\mu,\eta)$ and $T(\mu,\eta)$, respectively; and $*$ means the convolution operation.

The original image recovering process follows Fig. 1(b), where we perform the inverse Fourier transform, then we multiply by the complex conjugate of the original toroidal phase plate, and finally another Fourier transform is applied

$$I(\mu,\eta)T(\mu,\eta)T^{*}(\mu,\eta) \rightarrow I(\mu,\eta) \Rightarrow FT^{-1}[I(\mu,\eta)] = i(x,y). \tag{4}$$

In Fig. 2, we show a computer simulation. The intensity of the original image 2(a) and the structured phase mask (a toroidal phase plate) 2(b) are shown. The encrypted image 2(c) and the results using the right decoding key 2(d) are also displayed.

In Fig. 3(a), toroidal phase plate different from the one used in the encryption step, and Fig. 3(b) the corresponding result revealing a wrongly decrypted image.

3. Analysis on the influence of diffraction efficiency in the decryption process

Actual diffractive optical elements are normally produced under two different methods. One uses amplitude-only diffractive elements and the other phase-only diffractive elements. Regarding this last

Fig. 4. Retrieved images using the same type of toroidal zone plate but constructed with different codifications: (a) the right binary amplitude decoding key, (b) binary phase, (c) four phase levels, (d) eight phase levels, (e) 16 phase levels, and (f) ideal case.

class of elements, they can be built using several phase levels. Obviously, image quality formation when using these phase elements is of great importance. And this parameter is strongly conditioned by the diffraction efficiency, which in turn depends on the phase levels used in the construction procedure. The more the levels, the better the diffraction efficiency [17].

In Fig. 4, we analyze the decryption process by using the same toroidal zone plate, considering different phase levels in its construction, besides comparing them with the same zone plate but binary amplitude. It is worth mention that in all cases the reconstruction key is the same; we only change its codification. In Fig. 4(a), we show the retrieved image when decoding using the binary amplitude zone plate. Fig. 4(b) exhibits the reconstructed image by using a binary phase zone plate to decrypt. Fig. 4(c) depicts the image obtained with a four-levels phase plate. Fig. 4(d) and (e) shows the decoding cases for eight and 16 phase levels, respectively. Finally, Fig. 4(f) illustrates the simulation of the ideal case.

4. Conclusions

We presented an alternative method for encryption of optical information by using a toroidal phase plate. Major advantages of this encryption technique are the energy preservation, the multiple keys in a single phase mask, difficult to reproduce and easy to align. In addition, we analyzed the influence of the diffraction efficiency on the decryption process, showing that this is also a decoding key to be considered.

Acknowledgements

The grants from CONICET (PICT Nr. 008/98), from Universidad Nacional de La Plata and CODI-Universidad de Antioquia are gratefully acknowledged. John Fredy Barrera acknowledges the financial support form COLCIENCIAS – Colombia. Rodrigo Henao gratefully recognizes the financial assistance of the Multipurpose Optical Network (ICTP, Trieste, Italy).

References

[1] B. Javidi, J.L. Horner, Opt. Eng. 33 (1994) 1752.
[2] B. Javidi, E. Ahouzi, Appl. Opt. 37 (1998) 6247.
[3] O. Matoba, B. Javidi, Appl. Opt. 38 (1999) 7288.
[4] X. Tan, O. Matoba, T. Shimura, K. Kuroda, B. Javidi, Appl. Opt. 39 (2000) 6689.
[5] S. Lai, M. Neifield, Opt. Commun. 178 (2000) 283.
[6] O. Matoba, B. Javidi, Opt. Lett. 27 (2002) 321.
[7] J. Horner, B. Javidi, Opt. Eng. 38 (1999) 8.
[8] B. Javidi, T. Nomura, Opt. Lett. 25 (2000) 28.
[9] B. Javidi, E. Tajahuerce, Opt. Lett. 25 (2000) 610.
[10] D. Weber, J. Trolinger, Opt. Eng. 38 (1999) 62.
[11] N. Yoshikawa, M. Itoh, T. Yatagai, Opt. Lett. 20 (1995) 752.
[12] P. Réfrégier, B. Javidi, Opt. Lett. 20 (1995) 767.
[13] R. Arizaga, R. Torroba, Opt. Commun. 215 (2003) 31.
[14] R. Torroba, R. Henao, R. Arizaga, Opt. Commun. 221 (2003) 43.
[15] N. Towghi, B. Javidi, Z. Luo, J. Opt. Soc. Am. A 16 (1999) 1915.
[16] Lj Janicijevic, T. Tufekcieva, M. Jonoska, Pure Appl. Opt. 7 (1998) 685.
[17] O. Bryngdahl, F. Wyrowski, in: E. Wolf (Ed.), Progress in Optics, vol. 28, North-Holland, Amsterdam, 1990.