Available online at www.sciencedirect.com

SCIENCE @ DIRECT®

ELSEVIER

Optics Communications 260 (2006) 109–112

OPTICS COMMUNICATIONS

www.elsevier.com/locate/optcom

Multiplexing encrypted data by using polarized light

John Fredy Barrera [a], Rodrigo Henao [a], Myrian Tebaldi [b,*], Roberto Torroba [b], Néstor Bolognini [c]

[a] *Grupo de Óptica y Fotónica, Instituto de Física, Universidad de Antioquia A.A. 1226 Medellín, Colombia*

[b] *Centro de Investigaciones Ópticas (CONICET-CIC) and UID OPTIMO, Facultad de Ingeniería, Universidad Nacional de La Plata, Camino Centenario entre 505 y 508, P.O. Box 124, Gonnet, La Plata 1900, Argentina*

[c] *Centro de Investigaciones Ópticas (CONICET-CIC), UID OPTIMO, Facultad de Ingeniería and Facultad de Ciencias Exactas, Universidad Nacional de La Plata, P.O. Box 124, La Plata 1900, Argentina*

Received 23 September 2005; received in revised form 21 October 2005; accepted 24 October 2005

Abstract

We investigate the feasibility of multiplexing, employing polarized light, a set of security encrypted data. The encryption approach is based on the double random pure-phase enciphering method. Phase conjugation operation is conducted in the reconstruction stage with the aid of a photorefractive crystal which stores the encrypted information. When storing each encrypted image, a polarization change is introduced in the system. This induces decorrelation on the speckle patterns inside the storing medium. We apply this approach for multiple image encryption. We show experimental results that confirm our approach.
© 2005 Elsevier B.V. All rights reserved.

PACS: 42.30.Va; 42.25.Ja

1. Introduction

In the optical field there has been constant efforts on both multiplexed [1] and security encrypted [2] data storage. Securing data in high-capacity storage systems is one of the challenging tasks in order to meet user-requirements in data storage.

Optical data storage presents great advantages over traditional non-optical storage systems with the potentiality of low cost, high storage capacity, high transfer rate, and hardware-based data encryption. To overcome the difficulties concerning the storage means for recording photorefractive crystals have been used.

There are many methods for multiplexing holograms, e.g., wavelength-, shift-, angle-, and phase-coded multiplexing.

Several efforts were performed thanks to the advent of the liquid crystal spatial light modulator (LC-SLM). It has opened up the possibility for dynamic control of amplitude, phase or polarization state of light. The use of LC-SLMs for the spatial control of the state of polarization has already been described and experimentally demonstrated [3].

Several optical systems based on the encryption of information using phase components of wave front have been experimentally demonstrated [4–6]. Polarization has been used for the visualization of the decoded information. Two dimensional encoding of the polarization state of light using a parallel aligned liquid crystal SLM has recently been demonstrated [7]. Unnikrishnan et al. [8] experimentally demonstrated an optical encryption system based on polarization encoding to encrypt binary images. The encryption is done by XOR operation between the image and a random code (key to the encrypted image). The XOR operation is done in the polarization domain of coherent light by using two ferroelectric liquid crystal spatial light modulators. The

[*] Corresponding author. Tel.: +54 221 4840280; fax: +54 221 4712771. *E-mail address:* myrianc@ciop.unlp.edu.ar (M. Tebaldi).

0030-4018/$ - see front matter © 2005 Elsevier B.V. All rights reserved.
doi:10.1016/j.optcom.2005.10.053

information encoded as polarization states of coherent light is converted to intensity variations by using a polarizer. The decryption of the encrypted data are done by a second XOR operation between the encrypted image and the key. Mogensen et al. [9] have proposed an optical encryption and decryption system based on XOR operations using high frame rate ferroelectric liquid crystal spatial light modulators. Tan et al. [10] have proposed a secure holographic memory system with polarization encoding. The polarization state at each pixel is scrambled by a mask (SLM) that changes the polarization state into a random state. Eriksen et al. [11] have proposed a method for spatially encoding the state of polarization in a 2-D wave front with elliptically polarized light controlling both the ellipticity and rotation angle of the major axis of the ellipses. A technique was has also been developed, based on polarization-encoding using digital speckle pattern correlation [12]. In that method, security is twofold by the speckle and polarization characteristics of the procedure. Both encoding and decoding keys are stored digitally.

Recently, an approach for polarization encryption using geometrical phase modification has been proposed. Geometrical phases originate from polarization state manipulation, by using computer-generated space-variant subwavelength gratings (SWG) [13].

In [14], an optical encryption arrangement based on polarization is implemented by using a bacteriorhodopsin film as a polarization sensitive holographic memory. In this case, a single polarization modulation is used to encrypt the data. Reference [15] is an extension of the above paper introducing a double-random polarization encryption that uses two random polarization-modulation masks.

Although several optical encryption arrangements codified the input data in polarization, there have been no working implementations for data multiplexing encryption in the form of polarization encoding. In this paper, we describe a system for optical two-dimensional (2D) multiplexing encoding using the polarization state of light. The proposed technique simultaneously combines double random phase encryption method and polarized behaviour of the encrypted beam. Most of the above mentioned articles use one or two associated SLM, which implies the calibration of such instruments, aside of the additional cost in equipment. In our proposal, we directly used retardation plates, which facilitate the process and lower the costs of the experience.

Our multiplexing proposal has a practical application in optical encryption, increasing the total number of combination possibilities yet improving the robustness of the encryption system.

Another feature to be stressed is precisely the polarization sensitivity. This attribute can be used as a secondary key code to ensure the encryption in case of possible message interception.

Experimental results that confirm our proposal are presented.

2. Description of the method

Fig. 1 shows the basic optical system architecture employed. In this case, multiple encrypted data are stored within a photorefractive holographic memory using the double random phase encoding technique. This technique involves the use of a random pure-phase mask in the input plane R_1 and another R_2 in the spatial frequency plane, thus resulting in the formation of stationary white noise. Generally speaking, the second random pure-phase mask can be located at the Fresnel domain. In our arrangement, besides the two masks, a retardation plate WP_1 is employed to encode the input amplitude data O. Lens L_2 images the encrypted information on a 10 mm × 10 mm × 10 mm photorefractive BSO crystal. The experimental arrangement is illuminated by Nd-YAG laser operating at wavelength 532 nm with 50 mW output power. The encrypted information is holographically recorded by a reference plane wave. The interference between the encrypted data and the reference beam is obtained inside the crystal volume. The intensity patterns redistribute the photoinduced charges, resulting in an electric field strength at each point, which induces, through the linear electro-optic effect that the crystal exhibits, a corresponding spatial variation of the refractive index. In this way, the input pattern is encoded in terms of the refractive index variation generating index gratings. The angle between the recording beams is 8°.

There is an obvious dependence of the speckle pattern distribution with the polarization of the light source that has been extensively studied by several authors [16–18].

Based on this concept, we introduce a change in the polarization state of the object beam in order to achieve multiplexing. Therefore, for every polarization change the speckle pattern is somehow altered in the same way as a phase change is introduced.

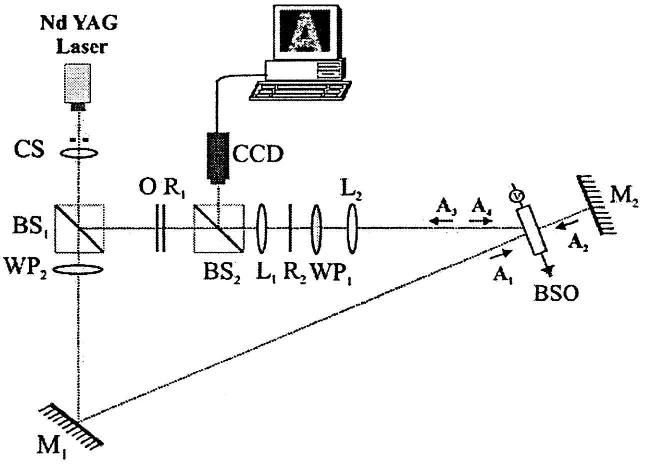

Fig. 1. Optical system architecture to multiple polarization encryption procedure (O: input data; R_1 and R_2: random pure-phase masks; WP_1 and WP_2: retardation plates; BS_1 and BS_2: beam splitters; L_1 and L_2: lenses; CS: collimation system; and M_1 and M_2: mirrors).

Phase conjugation of the reference beam is introduced in the decryption process to read out the data stored in the crystal. Let us denote A_1 and A_4 the amplitudes of the interfering beams. In our set-up, beam A_2 is the transmitted part of beam A_1 retroreflected by mirror M_2. After beam A_2 passes through the crystal, beam A_3 is generated which is proportional to the conjugate of the image bearing beam A_4. Exact cancellation of the phase change introduced in the encryption process is necessary to decrypt the input. Data recovering is observed by a CCD camera according to Fig. 1.

Note that the encrypted information stored in the crystal is essentially a speckle pattern. Each speckle interferes with the reference wave; therefore the speckle pattern is modulated by fringe systems existing in its whole volume. Then, the resulting pattern gives rise to a micro hologram inside each speckle.

It should be emphasized that the registered index gratings are random in phase according to the incident distribution. Each of these gratings interact with the counterpropagating pump beam thus producing a local phase conjugated beam inside each speckle, with a random phase that recognizes the original local speckle phase. The total contribution to the phase conjugation reflectivity is thus produced by each speckle. Therefore, the reconstructed beam A_3 is a phase conjugate beam which is, in turn, a pattern governed by the same statistical behaviour as the input beam.

The recording medium is intensity sensitive and it is not affected by polarization changes. However, in our case the polarization changes modify the intensity distribution of the encrypted pattern which interferes with the reference beam altering thereby the fringe systems and the resulting index grating. In order to maintain the fringe contrast the polarization state of the recording beams must remain unchanged.

Fig. 2 shows the experimental results demonstrating the polarization sensitive of the double random phase encryption arrangement: (a) object to be encrypted, (b) decryption using the right polarization direction, and (c) decryption with a wrong angle of the polarization direction. In this case, the polarization change is introduced by a half wave retardation plate.

Fig. 3(a)–(c) shows the same sequence as described in Fig. 2 but using a quarter wave retardation plate. It should be mentioned that in this case, a 1° rotation of the quarter wave retardation plate is enough to a complete detuning of the right decrypted image. In the half wave retardation plate is necessary a 5° rotation in order to avoid a right decryption. This analysis is useful to assess a correct multiplexing schedule avoiding any cross talk.

A procedure of multiple encryption by using the polarization as a key implies to govern the polarization state of the appropriate device in the successive inputs to be encrypted. The data of the *i*th stored image can be reconstructed not only if the phase conjugated beam travels through the retardation plate in the adequate orientation, but if it also travels through the second random pure-phase mask R_2 used in the encryption process.

Fig. 4 shows the encryption-decryption procedure for multiple input objects. O_1 and O_2 correspond to the input images, E_1 and E_2: the encrypted images, each one encrypted by using a determined polarization state. The polarization key is a quarter wave retardation plate. As it was established in the experience of Fig. 3, in order to avoid cross talk a 1° retardation plate rotation is introduced. D_1 and D_2: multiple decrypted images by using the correct polarization key.

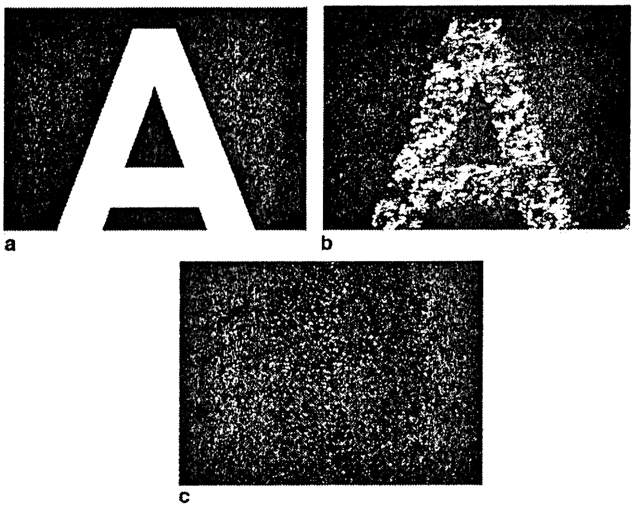

Fig. 2. Experimental results shows (a) object to be encrypted; (b) decryption when the polarization device (half wave retardation plate) is set at the correct polarization state (as in the encrypted procedure); and (c) decryption with a wrong polarization state.

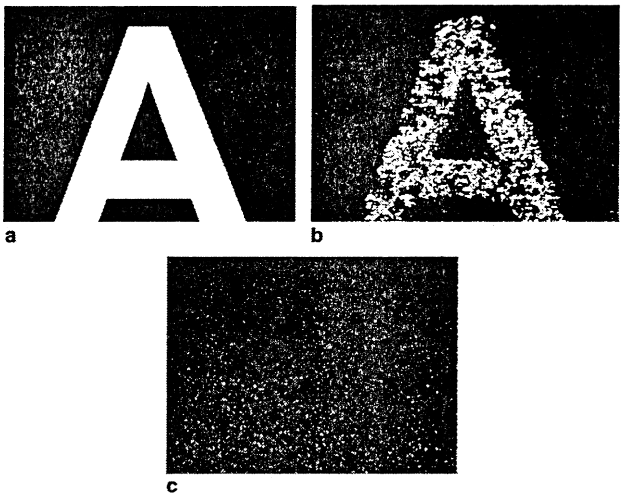

Fig. 3. Experimental results shows (a) object to be encrypted; (b) decryption when the polarization device (quarter wave retardation plate) is set at the correct polarization state (as in the encrypted procedure); and (c) decryption with a wrong polarization state.

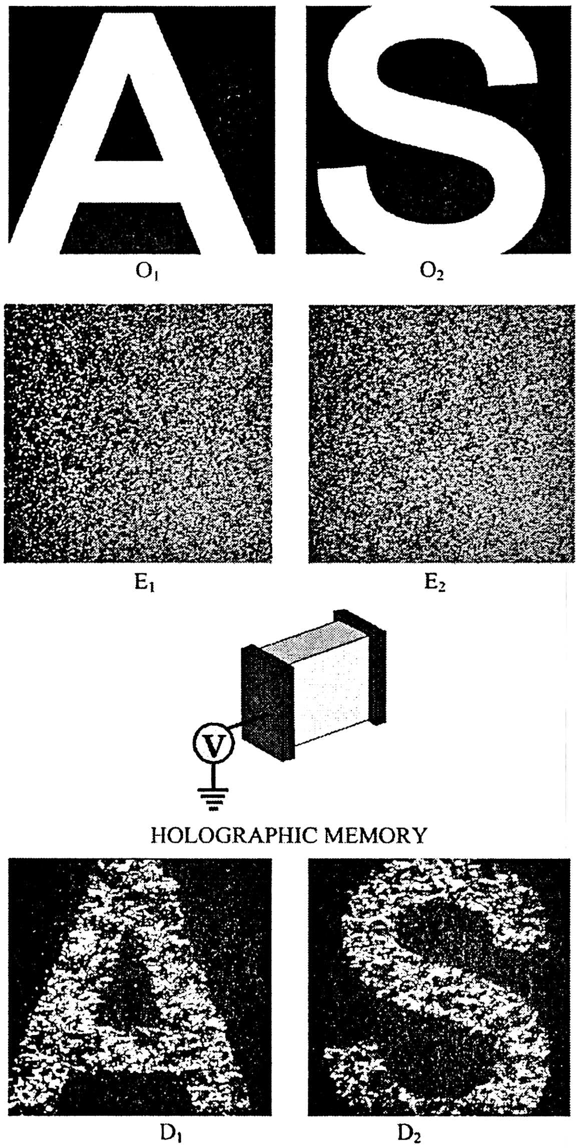

Fig. 4. Multiplexing polarization encryption-decryption procedure (O$_1$ and O$_2$: input objects; E$_1$ and E$_2$: encrypted images; and D$_1$ and D$_2$: decrypted images).

The experiments detailed above clearly confirm that the polarization can be used as unique key to encryption-decryption procedure.

3. Conclusions

In our paper, we propose and demonstrate a polarization encoded encryption system based on a double random pure phase mask technique and retardation plate.

In addition to the exact repositioning required for the random phase mask, for a successful recovering it is essential that a precise retardation plate orientation should be achieved.

It should be emphasized the simplicity and lower costs of the proposed experience in comparison with other polarization arrangements. Our set-up increases the security of the encryption through the introduction of the polarization as an alternative multiplexing encryption key.

To our knowledge this security polarization key is introduced for the first time in a multiple encryption image scheme. Parallel channelling operations are now an open possibility to security optics.

It remains to extensively analyze the sensitivity characteristics of the different polarization schemes.

Summarizing, we settle a new point of view to a multiplexing storing mechanism that expands the possible combinations of encrypted objects with a given optical architecture.

Acknowledgments

This Research was performed under the Auspicious of Colciencias (Colombia), Conicet PIP 2417 (Argentina), Cicpba (Argentina), ANPCYT PICT 12564 (Argentina) and Facultad Ingeniería, Universidad Nacional de la Plata (Argentina).

References

[1] Y. Taketomi, J.E. Ford, H. Sasaki, J. Ma, Y. Fairirnan, S.H. Lee, Opt. Lett. 16 (1991) 1774.
[2] C. Denz, T. Deliwig, J. Lembcke, T. Tschudi, Opt. Lett. 21 (1996) 278.
[3] M. Stalder, M. Schadt, Opt. Lett. 21 (1996) 1948.
[4] P.C. Mogenson, J. Gluckstad, Opt. Commun. 173 (2000) 177.
[5] P.C. Mogenson, J. Gluckstad, Opt. Lett. 25 (2000) 566.
[6] R. Torroba, R. Henao, R. Arizaga, Opt. Commun. 221 (2003) 43.
[7] J.A. Davis, D.E. McNamara, D.M. Cottrell, T. Sonehara, Appl. Opt. 39 (2000) 1549.
[8] G. Unnikrishnan, M. Pohit, K. Singh, Opt. Commun. 185 (2000) 25.
[9] P.C. Mogensen, R.L. Eriksen, J. Gluckstad, J. Opt. A 3 (2001) 10.
[10] X. Tan, O. Matoba, Y. Okada-Shudo, M. Ide, T. Shimura, K. Kuroda, Appl. Opt. 40 (2001) 2310.
[11] R.L. Eriksen, P.C. Mogensen, J. Gluckstad, Opt. Commun. 187 (2001) 325.
[12] R. Arizaga, R. Torroba, Optik 113 (2002) 333.
[13] G. Biener, A. Niv, V. Kleiner, E. Hasman, Opt. Lett. 30 (2005) 1096.
[14] X. Tan, O. Matoba, T. Shimura, K. Kuroda, B. Javidi, Appl. Opt. 39 (2000) 6689.
[15] O. Matoba, B. Javidi, Appl. Opt. 43 (2004) 2915.
[16] J.C. Dainty (Ed.), Laser Speckle and Related Phenomena, Springer, New York, 1975.
[17] J.W. Goodman, Statistical Optics, Wiley, New York, 1978.
[18] J.K. Boger, Opt. Lett. 24 (1999) 611.