Available online at www.sciencedirect.com

ScienceDirect

Optik 119 (2008) 139–142

Optik Optics

www.elsevier.de/ijleo

Code retrieval via undercover multiplexing

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, Medellín, Colombia
[b]Centro de Investigaciones Ópticas (CONICET-CIC) and UID OPTIMO, Facultad Ingeniería, Universidad Nacional de La Plata, P.O. Box 124, 1900 Gonnet La Plata, Prov. Buenos Aires, Argentina
[c]Centro de Investigaciones Ópticas (CONICET-CIC), UID OPTIMO, Facultad Ingeniería and Facultad Ciencias Exactas, Universidad Nacional de La Plata, La Plata, Argentina

Received 11 May 2006; accepted 4 July 2006

Abstract

The purpose of this research is to develop an undercover multiplexing technique to give additional protection for optical information encryption. We employ the double random phase mask as our basic optical encryption system. The holographic storage medium of choice is a photorefractive crystal. To achieve the multiplexing we use the aperture size of the pupil in the optical system, as it governs the speckle size. We introduce such variation in order to produce a decorrelation between two consecutively stored speckle patterns. Each stored speckle pattern is associated to an input encrypted image, thus producing a multiplexing of the encrypted information. We implement this operation without altering the setup architecture and the random phase masks. This multiplexing is our undercover operation to encipher a true code behind a fake code. Under this approach, the user can only recover the bulk information stored in the volume hologram. However, he cannot recover the true code without the additional information on the pupil size key, even if accessed in position of the original decoding mask.

Keywords: Security; Optical encryption; Volume holography

1. Introduction

As it is well known, speckle patterns are obtained either by using an imaging formation system or by free propagation, usually defined as subjective or objective speckles, respectively [1,2]. The size, shape, intensity and phase of speckles depend on several parameters. Note that the subjective speckle features depend not only on the diffuser structure, but also on the architecture of the optical scheme that originates them. Besides, this dependence extends to the wavelength and the polarization characteristics of the illumination source. In particular, the speckle pattern depends on the size and shape of the optical system pupil apertures. A classical example is the method proposed by Kopf [3] where the aperture of the lens is a slit and the image is composed of speckles oriented perpendicularly to the wider side of the slit. In that case, the spectrum of the registered image shows, after processing, diffracted light at large angles in the direction perpendicular to the oriented speckles.

---

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

0030-4026/$ - see front matter © 2006 Elsevier GmbH. All rights reserved.
doi:10.1016/j.ijleo.2006.07.008

This method allows to overlap photographs recorded with the slit apertures in different azimuthal positions and to separate them later by spatial filtering.

Besides, the control of the optical systems pupil apertures is of particular interest in several applications regarding metrology [4,5] and optical information processing under coherent light. Image encryption is a recent application [6].

The most used encryption method is based on protecting the stored information by transforming the original data into stationary white-noise data. The double random phase-mask technique leads to this objective [7]. Precisely, these random phase masks generate speckle patterns.

For succeeding in this encryption method, it is essential to get in the decoding step the phase-conjugated version of either the encoding random phase mask, or the whole wave front encrypted information. In order to fulfill properly the last condition, we need a suitable recording medium that simultaneously makes possible the phase conjugation operation. Precisely, photorefractive materials are the option, with the additional advantage of operating in real time. In this context, optical encryption systems by using phase conjugation with photorefractive crystals were developed [8–10].

Photorefractive materials are volume media that present a high storage capability, for instance suitable to multiplexing procedures. In the literature, we find proposals that take advantage of this feature. There are extensions of multiplexing techniques to encryption methods. Recently, we proposed a multiplexing double random phase-mask-based cryptosystem by using an optical scheme where we use spatially disjoint pupil apertures between exposures [6]. In that reference, we also experimentally analyzed the arrangement and we showed that, by an adequate selection of the pupil sequence, it is possible to store multiple encrypted information without cross-talk.

We take advantage of the above-mentioned research with the objective of designing an approach to undercover a true message within a fake code, provided by a multiplexing procedure using photorefractive materials. To implement this approach, we introduce the possibility of handling the speckle size used during the encryption process. In the present proposal, we control the speckle size by only varying the pupil aperture diameter of the optical system between exposures. We present experimental and computer-simulated results to validate our approach.

Our specific aim is to provide an optical undercover multiplexing that represents a securing option to protect encrypted data.

2. Description of the method

Our proposed technique provides the chance to store in a photorefractive medium a set of images (multiplexing) based on the decorrelation of speckle patterns. We induce these decorrelations via a pupil aperture-size variation. When using the full aperture we simultaneously recover these images, building up a single code. However, only the authorized user can find the true hidden code after using the correct aperture size.

We first discuss the way to encrypt and to produce multiplexing and thereafter we will describe the characteristics of the recording material.

In Fig. 1, we show the concept of the encryption technique. We use two random phase masks to generate a white-noise encoding. The input image data pass through the masks R_1 and R_2, thus encrypting the data [7]. We focus the attention of the reader to the fact that, under the present optical architecture, the encrypted information takes the form of a speckle pattern. The final speckle pattern represents the encrypted data stored in the recording material.

We now recall the expressions to show the way the speckles can be conveniently modified. We remember that the speckle average diameter is $\langle S_X \rangle \approx \lambda \cdot (Z_C/D)^2$ and the average depth is $\langle S_Z \rangle \approx \lambda \cdot (Z_C/D)$, where Z_C is the distance between the lens and the crystal, λ the wavelength, and D the limiting aperture of the optical system. From these expressions, we see that when the magnitudes λ and Z_C are fixed only the parameter D determines the speckle size.

In our setup, we introduce an iris diaphragm D as limiting entrance to the system (See Fig. 1). Consequently, we store in the recording medium different speckle patterns depending on the diaphragm diameter. The medium is placed at the image plane of the optical system. We stress that each speckle pattern codifies each input image. Therefore, each imaged speckle intensity distribution carries different input data without altering any random phase masks in the setup.

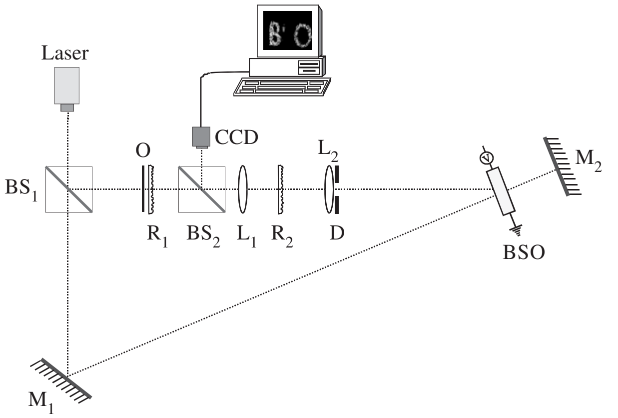

Fig. 1. Experimental setup: BS_1 and BS_2: beam splitters, O: input object; R_1 and R_2: pure random phase masks; L_1 and L_2: lenses; D: iris diaphragm; M_1 and M_2: mirrors; CCD: camera; BSO: photorefractive crystal.