Available online at www.sciencedirect.com
ScienceDirect
Optik 120 (2009) 351–355
Optik Optics
www.elsevier.de/ijleo

Multiplexing encryption technique by combining random amplitude and phase masks

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

Received 20 July 2007; accepted 7 October 2007

Abstract

We propose and demonstrate an encryption-selectable undercover multiplexing. We encrypt and multiplex images for storage by means of a random phase mask common to every image, covered with random amplitude masks different for each image. In order to get a correct decryption of the encoded information, we have to use the appropriate random amplitude mask; otherwise fake information is recovered. We employ a phase conjugation scheme to generate the recovering wavefronts. We analyze and compare the different alternatives and degrees of complexity this combination of masks brings to enhance the security of optical encrypting techniques. We also include an analysis on the advantages and disadvantages this undercover multiplexing protocol offers. We present digital simulations to demonstrate the soundness of the proposal.

Keywords: Security; Optical encryption; Multiplexing

1. Introduction

It is becoming increasingly simple to reproduce input data in security system. Therefore, data protection has become necessary. The most preferred optical method is that of double random phase encryption [1]. In the encryption process, input data (positive real-valued image) are multiplied by a random phase function, and then Fourier transformed and finally multiplied by a second random phase function. We can obtain a decrypted image by first multiplying by the complex conjugate of the second encoding phase function and taking a Fourier transform. Many related contributions were generated, including the use of a joint-transform correlator (JTC) [2] or optical arrangements using photorefractive crystals [3–6].

Since optical techniques appear as practical tools in securing and validating information, researchers adopted significant efforts to investigate these techniques under the insight of cryptoanalysis. Researchers cast doubts on the efficiency in the sense if the techniques were able to endure attacks from cryptoanalysis.

We generally present vulnerability in the following ways:

(1) We can apply a key decryption algorithm either to the encryption machine (the most vulnerable) or to

*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 © 2007 Elsevier GmbH. All rights reserved.
doi:10.1016/j.ijleo.2007.10.001

the decryption machine. In effect, if we ask the system to encrypt a centered Dirac delta function, it will produce, at the output, the Fourier transform of the second encryption key. The holographic recording captures this Fourier transform, and the second key is then readily obtained by inverse transformation and conjugation of the result.

If only the decryption machine is accessible, the system will still be at risk, although from a more sophisticated attack by repeatedly probing the machine with a set of ciphertexts skillfully designed to skip this problem. (The reader can find a detailed description in Ref. [7].)

(2) The optical encryption scheme based on double random phase keys is also vulnerable to another kind of attack, where an opponent can access random phase keys in both the signal domain and the spatial frequency domain.

It is worthwhile to point out that all calculations in the encryption and decryption procedures in the double-random phase encoding obey a linear relationship. From an optics point of view, the output plane is conjugate to the input plane, so the linearity between the encrypted image and object is obvious even though the encrypted image has become stationary white noise. Ref. [8] shows that this linearity will lead to a security flaw in an optical encryption scheme based on double random phase keys.

One important feature that reinforces optical encryption is the multiplexing concept. This procedure brings the chance for storing multiple messages in a single recording medium. Note that multiplexing allows the strengthening against attacks [9]. So far multiplexing was conducted using phase masks only [10]. We center our proposal on the idea of supplementing the phase mask using the concept of multiplexing with amplitude mask. In this way, we introduce an amplitude mask in contact with the second phase mask in a conventional double phase masks encoding architecture when encrypting a first image. Immediately after introducing a second image, we modify or change the first amplitude mask by another amplitude mask. Therefore, two images are sequentially stored with the same phase masks arrangement, but different amplitude masks. The unauthorized user, even capturing the second speckle mask or attempting the described ciphertexts attacks, retrieves the addition of the two encrypted objects; therefore, he retrieves a "fake ciphertext". Here we introduce the concept of "fake ciphertext", because the intruder reveals not a single fake image but a fake superposed message. To secure the information data from unauthorized users, we add some trivial images to those that will appear as information to unauthorized receivers. In this way, the publicly delivered content images will look just like ordinary pictures, although some random noise will be present as background. Only knowing the right amplitude masks will allow the appropriate retrieval of the true encoded information separately.

In the section to follow, we explain in detail the procedure, along with simple examples in order to understand the principle of the technique. Finally, the potential of the technique is shown. Evidently, by introducing amplitude masks, we run the risk of losing some frequency information besides the logical intensity decrease. Therefore, we include a discussion on the advantages and disadvantages we find in operating with the proposed technique.

2. Discussion of the method

We use in all of our examples a $4f$ architecture to perform the encryption, like the one shown in Fig. 1. The two random phase masks PM_1 and PM_2, one in the object plane and the other in the Fourier plane, satisfy the phase condition of independent white noise distributed in the region $[0, 2\pi]$. Propagation distances along all planes coincide with the focal lengths.

When we practice the conventional process with this scheme, we encrypt a single image. Multiplexing requires an extra feature, like an arrangement of pupils [4,10], random phase mask translation either in its own plane [5] or in the optical axis direction [11], polarization changes between exposures [6], etc.

We introduce complementary binary amplitude masks to explore the multiplexing possibilities beyond the above-described examples by including the non-overlapping mask concept. The use of non-overlapping binary amplitude elements cooperates in the enhancement of security multiplexing capabilities.

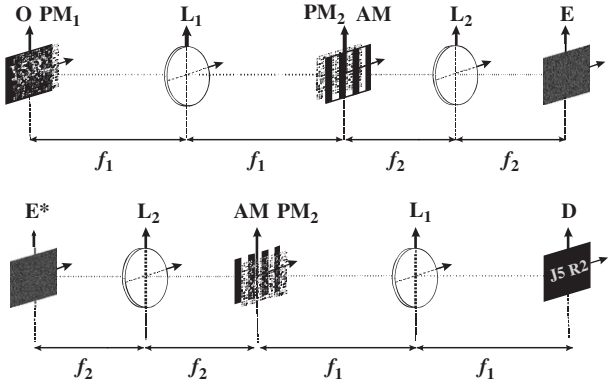

Fig. 1. Encryption–decryption setup. O: object; PM_1 and PM_2: random phase masks; AM: amplitude mask; L_1 and L_2: lenses with focal length f_1 and f_2, respectively; E: encrypted information; E*: phase-conjugated encrypted information; D: decrypted object.