Optics and Lasers in Engineering 89 (2017) 145–149

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

journal homepage: www.elsevier.com/locate/optlaseng

Optical encryption in the axial domain using beams with arbitrary polarization

Artur Carnicer [a,*], Ignasi Juvells [a], Bahram Javidi [b], Rosario Martínez-Herrero [c]

[a] Universitat de Barcelona (UB), Facultat de Física, Departament de Física Aplicada, Martí i Franquès 1, 08028 Barcelona, Spain
[b] Electrical and Computer Engineering Department, University of Connecticut, 371 Fairfield Road, Storrs, CT 06269-4157, USA
[c] Universidad Complutense de Madrid, Facultad de Ciencias Físicas, Departamento de Óptica, Ciudad Universitaria s/n, 28040 Madrid, Spain

ARTICLE INFO

Article history:
Received 27 January 2016
Received in revised form
22 June 2016
Accepted 30 June 2016
Available online 16 July 2016

Keywords:
Polarization
Highly focused beams
Optical security

ABSTRACT

Recently, a cryptosystem based on the analysis of light in the focal area of a high numerical aperture system has been proposed. A key element in the design of this device is the selection of the polarization of the input beam. In this paper we analyze how polarization influences the performance of the encoded message. In order to avoid attacks and enhance security, the system is assumed to work in photon-counting illumination conditions.

1. Introduction

The study of optical systems for security purposes attracts great interest. In 1994, Javidi and Horner published their seminal paper on optical security [1]. Since then, the number of papers in the area has been growing year after year (see, for instance, [2,**?**,4] and references therein). The Double Random Phase Encoding (DRPE) original approach [5] is based on a 4*f* system within the framework of the scalar propagation theory. Later, the use of polarized light became widespread as more degrees of freedom are added to the cryptosystem [6,7]. Moreover, the combined use of polarimetric techniques with pattern recognition methods entitle to address complex problems in security, including classification or counterfeiting validation [8,9]. Several authors have demonstrated vulnerabilities in DRPE-based systems [10–13] but actually, solutions to avoid weakness and possible attacks have been proposed [14,15]. In particular, those systems operating in low light conditions have been demonstrated very efficient and difficult to broke [16,17]. They are particularly appropriate in validation applications.

Recently, we proposed a cryptosystem based on the use of highly focused fields [18]. Despite the fact the optical setup can be complex and difficult to carry out, focused beams present some advantages that justify their use in cryptography. Note that fields in the focal area display a non negligible amount of energy in the direction of propagation of the wave. This component is very weak and it is completely embedded by the transverse part of the wave. In [19] we discussed how to encode and encrypt information in the longitudinal component of the beam. Moreover, if the transverse part of the wave is recorded, the information encoded can be accessed by means of the Gauss law.

A key element in the design of an optical encryption system based on highly focused fields is the selection of the polarization of the input beam. The objective of this paper is to analyze how polarization influences the performance of these systems. The paper is organized as follows: in Section 2 we review basic concepts in the theory of propagation of light in the focal area and how information can be encoded and encrypted in the longitudinal component of a highly focused beam. In Section 3 we study how input polarization (circular, spiral, radial) affects the transverse and the longitudinal parts of the field. These results are used to analyze the performance of the encrypted signal. In order to avoid attacks, it is assumed the systems works in photon-counting illumination conditions. Finally, the conclusions are presented in Section 4.

2. Background: encoding information in the longitudinal domain

The Richards and Wolf equation provides the framework to describe the vector behaviour of an electromagnetic field $\mathbf{E} = (E_x, E_y, E_z)$ in the focal area [20]:

* Corresponding author.
E-mail address: artur.carnicer@ub.edu (A. Carnicer).

http://dx.doi.org/10.1016/j.optlaseng.2016.06.027
0143-8166/

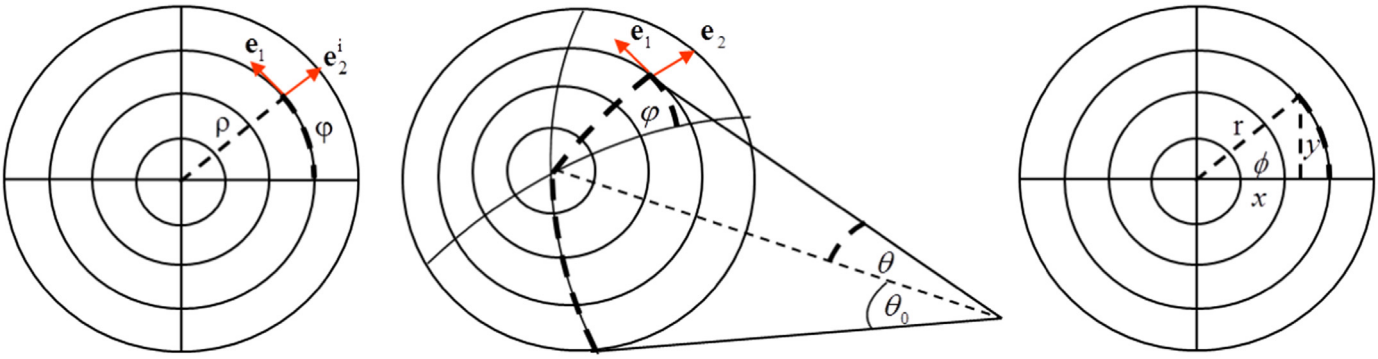

Fig. 1. Coordinate systems: left: entrance pupil, center: Gaussian reference sphere, right: focal plane.

$$\mathbf{E}(r,\phi,0) = A\int_0^{\theta_0}\int_0^{2\pi}\mathbf{E}_\infty(\theta,\varphi)\exp(ikr\sin\theta\cos(\phi-\varphi))\sin\theta d\theta d\varphi, \tag{1}$$

where $\mathbf{E}_\infty$ is electromagnetic field at the Gaussian sphere of reference, θ_0 is the semi-aperture angle, k is the wavenumber and A is a constant; θ and φ, and r and ϕ are the coordinates at the Gaussian sphere and at the focal plane respectively. See Fig. 1 for details.

$\mathbf{E}_\infty$ is described as the combination of projections $\mathbf{E}_0\cdot\mathbf{e}_1$ and $\mathbf{E}_0\cdot\mathbf{e}_2^i$ of the input field $\mathbf{E}_0$ on the radial ($\mathbf{e}_1$) and the azimuthal directions ($\mathbf{e}_2$), i.e.:

$$\mathbf{E}_\infty = \sqrt{\cos\theta}\left(\mathbf{E}_0\cdot\mathbf{e}_1\,\mathbf{e}_1 + \mathbf{E}_0\cdot\mathbf{e}_2^i\,\mathbf{e}_2\right), \tag{2}$$

where vectors $\mathbf{e}_1$, $\mathbf{e}_2$ and $\mathbf{e}_2^i$ are described by:

$$\mathbf{e}_1(\varphi) = (-\sin\varphi, \cos\varphi, 0) \tag{3a}$$

$$\mathbf{e}_2^i(\varphi) = (\cos\varphi, \sin\varphi, 0) \tag{3b}$$

$$\mathbf{e}_2(\varphi,\theta) = (\cos\theta\cos\varphi, \cos\theta\sin\varphi, \sin\theta), \tag{3c}$$

and the wave-front vector $\mathbf{s}$ is defined as:

$$\mathbf{s} = (\alpha,\beta,\gamma) = (\sin\theta\cos\varphi, \sin\theta\sin\varphi, -\cos\theta). \tag{4}$$

Notice that $\mathbf{e}_1$, $\mathbf{e}_2$ and $\mathbf{s}$ form a triad of mutually orthogonal right-handed system of unit vectors. In particular, $\mathbf{E}_\infty$ is normal to the wave-front vector $\mathbf{s}$, $\mathbf{E}_\infty\cdot\mathbf{s} = 0$. Eq. (1) can be rewritten in a more compact way using Fourier transforms. After some algebra, Eq. (1) takes the form (see [21] for details):

$$\mathbf{E}(x,y,0) = \mathrm{FT}_{\lambda f}\left[\frac{\mathbf{E}_\infty}{\cos\theta}\right] \tag{5}$$

where f is the focal length of the microscope objective used to focus the beam, λ is the wavelength and FT stands for the Fourier transform operator. The subindex λf indicates that spatial frequencies are scaled accordingly. Developing Eq. (2), the longitudinal component $E_{\infty z}$ reads:

$$E_{\infty z} = \sqrt{\cos\theta}\left(E_{0x}\cos\varphi + E_{0y}\sin\varphi\right)\sin\theta. \tag{6}$$

Interestingly, this expression provides a constrain between the input field components $\mathbf{E}_0 = (E_{0x}, E_{0y}, 0)$, and $E_{\infty z}$. Using Eqs. (2) and (5), the longitudinal component E_z of the focused field is written in terms of E_{0x} and E_{0y}:

$$E_{0x}\cos\varphi + E_{0y}\sin\varphi = \frac{\sqrt{\cos\theta}}{\sin\theta}\mathrm{FT}_{\lambda f}^{-1}[E_z]. \tag{7}$$

This formula shows how the z-component of a focused field is related to the transverse field distribution of the illuminating beam. We use this equation to encode information in the longitudinal component E_z. This equation is a necessary condition that has to be fulfilled, but the relationship between E_{0x} and E_{0y} is not set.

Since the longitudinal component cannot be easily isolated by optical means, E_z can be an appropriate container for encoding information. On the other hand, E_z can be accessed numerically using the Gauss law, $\nabla\mathbf{E} = 0$, which is equivalent to the condition $\mathbf{E}_\infty\cdot s = 0$. Because $|\mathbf{s}| = 1$, E_z can be determined by using the following equation [22]:

$$E_z = \mathrm{FT}_{\lambda f}\left[\frac{\alpha\mathrm{FT}_{\lambda f}^{-1}[E_x] + \beta\mathrm{FT}_{\lambda f}^{-1}[E_y]}{\sqrt{1-\alpha^2-\beta^2}}\right]. \tag{8}$$

Encryption is performed as follows. Let t be the message to be encrypted and M_1 and M_2 two random phase masks. If the signal encoded in the longitudinal component is equivalent to the obtained using DRPE, then $E_z = \mathrm{FT}_{\lambda f}\left[M_2\mathrm{FT}_{\lambda f}[M_1 t]\right]$. Note that other encoding methods can be used. The components of the encoded input field $(E_{0x}^e, E_{0y}^e, 0)$ are related by means of Eq. (7):

$$E_{0x}^e\cos\varphi + E_{0y}^e\sin\varphi = \frac{\sqrt{\cos\theta}}{\sin\theta}M_2\mathrm{FT}_{\lambda f}[M_1 t]. \tag{9}$$

In order to prevent attacks, the system emulates low light conditions. The transverse components of the encrypted focused field E_x^e and E_y^e are binarized using the photon counting model [16]. A description of imaging system working in low light conditions [23] can be found elsewhere [16,24–27]. Using the Poisson law, the binary version of the encrypted x-component reads:

$$E_x^{e\,\mathrm{ph}}(x,y) = \begin{cases} 0 & \text{if } \mathrm{rand}(x,y) \le \exp\left(-N_p\dfrac{|E_x^e(x,y)|^2}{I_x^e}\right) \\ \dfrac{E_x^e(x,y)}{|E_x^e(x,y)|} & \text{otherwise} \end{cases} \tag{10}$$

where N_p is the predetermined number of photon counts in the entire scene and I_x^e is the total irradiance of the encrypted component x (see Eq. (16)). Component $E_y^{e\,\mathrm{ph}}$ is obtained using the same approach:

$$E_y^{e\,\mathrm{ph}}(x,y) = \begin{cases} 0 & \text{if } \mathrm{rand}(x,y) \le \exp\left(-N_p\dfrac{|E_y^e(x,y)|^2}{I_y^e}\right) \\ \dfrac{E_y^e(x,y)}{|E_y^e(x,y)|} & \text{otherwise} \end{cases} \tag{11}$$

Using the correct key M_2 and the Gauss law [8], the decrypted photon-counting signal t^{ph} is obtained [19].

It is worth to point out that encryption in the longitudinal