Optical encryption in the axial domain using beams with arbitrary polarization

Artur Carnicer[1], Ignasi Juvells

Universitat de Barcelona (UB), Facultat de Física, Departament de Física Aplicada, Martí i Franquès 1, 08028 Barcelona (Spain)

Bahram Javidi

Electrical and Computer Engineering Department, University of Connecticut, 371 Fairfield Road, Storrs, Connecticut 06269-4157, USA

Rosario Martínez-Herrero

Universidad Complutense de Madrid, Facultad de Ciencias Físicas, Departamento de Óptica, Ciudad Universitaria s/n, 28040 Madrid (Spain)

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.

Keywords: Polarization, Highly focused beams, Optical security

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, 3, 4] and references therein). The Double Random Phase Encoding (DRPE) original approach [5] is based on a $4f$ 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

[1]Corresponding author email: artur.carnicer@ub.edu

demonstrated vulnerabilities in DRPE-based systems [10, 11, 12, 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]:

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

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 Figure 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.:

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

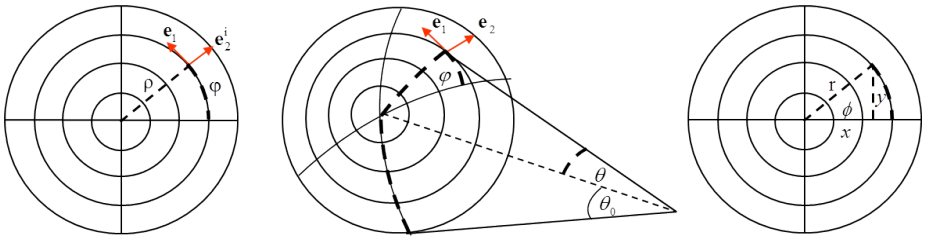


Figure 1: Coordinate systems: left: entrance pupil, center: Gaussian reference sphere, right: focal plane

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 $\mathbf{s}$, $\mathbf{E}_\infty \cdot \mathbf{s} = 0$. Equation (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:

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

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}:

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

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, 25, 26, 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 signal t^{ph} is obtained [19].

It is worth to point out that encryption in the longitudinal domain could be implemented in practice using an optical setup capable to produce focused beams with arbitrary input polarization polarization [28, 29]. A detailed discussion about a system able of producing encrypted fields in the longitudinal domain can be found in [19].

3. Input beam polarization selection

Equation (7) connects E_z with the components of the input field E_{0x} and E_{0y}. However, it is required to determine how E_{0x} and E_{0y} are related. According to Eq. (7) any polarization state of the input beam can by used, but here we demonstrate that the performance of the encryption system is dependent on the design of $\mathbf{E_0}$. We consider circular, spiral and radial polarization. Note that the azimuthal case cannot be taken into account because the focused field is purely transverse and no information can be encoded in the longitudinal domain.

3.1. Relationship between the transverse and the longitudinal components

We first analyze how the transverse components behave when information is encoded in E_z. Because E_z is calculated from the transverse components E_x and E_y using Eq. (8) we provide the formulae for E_x and E_y. It is straightforward to derive them by combining Eqs. (2) and (5):

$$E_{0x}(\sin^2\varphi + \cos^2\varphi\cos\theta) - E_{0y}\sin\varphi\cos\varphi(1-\cos\theta) = \sqrt{\cos\theta}\,\mathrm{FT}^{-1}_{\lambda f}[E_x] \tag{12a}$$

$$E_{0x}\sin\varphi\cos\varphi(\cos\theta - 1) + E_{0y}(\sin^2\varphi\cos\theta + \cos^2\varphi) = \sqrt{\cos\theta}\,\mathrm{FT}^{-1}_{\lambda f}[E_y]. \tag{12b}$$

Circularly polarized light is the simplest choice for encoding information in the longitudinal component. In this case, $E_{0y} = iE_{0x}$ and therefore, using Eq. (7) the transverse components of the input beam become

$$E_{0x}(E_z) = \exp(-i\varphi)\frac{\sqrt{\cos\theta}}{\sin\theta}\mathrm{FT}^{-1}_{\lambda f}[E_z] \tag{13a}$$

$$E_{0y}(E_z) = i\exp(-i\varphi)\frac{\sqrt{\cos\theta}}{\sin\theta}\mathrm{FT}^{-1}_{\lambda f}[E_z]\,. \tag{13b}$$

A 512x512 pixel image of Lena is used as the plaintext to be encoded in the longitudinal component. Figures 2(a)- 2(d) shows the polarization map, the irradiances $|E_x|^2$ and $|E_y|^2$, and the decoded message from the transverse components of the focused field. As it was expected, Figs. 2(b) and 2(c) are indistinguishable. On top of that, since the components of the focused field are related by means of the Gauss law, the information provided by the irradiance of the transverse components resembles the result of a edge-extraction procedure.

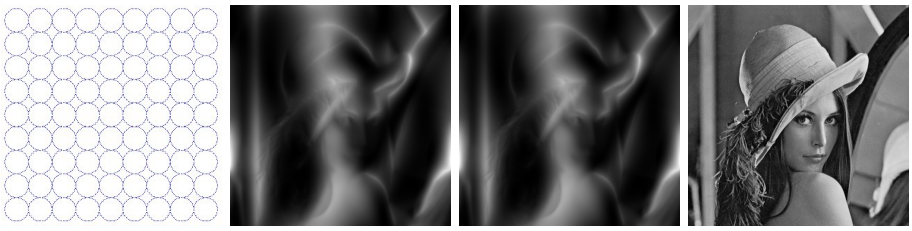
When the input field is linearly polarized according to a spiral law

$$E_{0x} = -E_{0y}\tan(\varphi + \alpha) \tag{14}$$

the components of the input field become

$$E_{0x}(E_z) = \frac{\sqrt{\cos\theta}}{\sin\theta}\frac{1}{\cos\varphi - \sin\varphi\cot(\varphi+\alpha)}\mathrm{FT}^{-1}_{\lambda f}[E_z] \tag{15a}$$

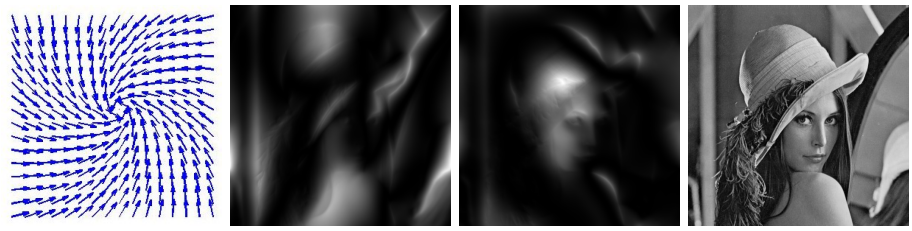
$$E_{0y}(E_z) = \frac{\sqrt{\cos\theta}}{\sin\theta}\frac{1}{\sin\varphi - \cos\varphi\tan(\varphi+\alpha)}\mathrm{FT}^{-1}_{\lambda f}[E_z]. \tag{15b}$$



(a) (b) (c) (d)

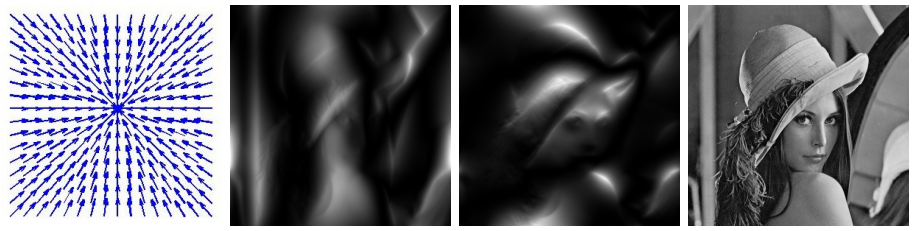
Figure 2: Information encoded in the longitudinal component using circularly polarized light: (a) polarization map, (b) $|E_x|^2$, (c) $|E_y|^2$ and (d) E_z

Since Eq. (14) depends on the parameter α, azimuthal ($\alpha = 0$) and radial ($\alpha = \pi/2$) polarizations can be considered special cases of spiral polarization. Moreover, note that $E_z = 0$ when $\alpha = 0$ (see Eq. (15a) and (15b)). The polarization map for $\alpha = \pi/3$ is depicted in Fig. 3(a). The irradiances of the $x-$ and $y-$ components are shown in Fig. 3(b) and 3(c) and the decoded message E_z is displayed in 3(d). The results for the radial polarization case $\alpha = \pi/2$ are presented in Figs. 4(a)-4(d).



(a) (b) (c) (d)

Figure 3: Information encoded in the longitudinal component using spirally polarized light: (a) polarization map, (b) $|E_x|^2$, (c) $|E_y|^2$ and (d) E_z.



(a) (b) (c) (d)

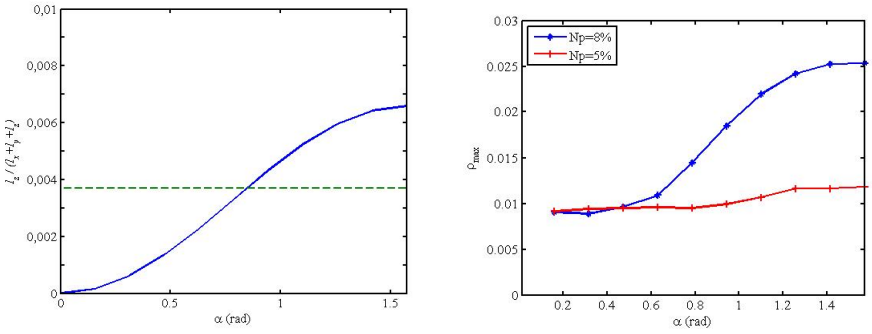
Figure 4: Information encoded in the longitudinal component using radially polarized light: (a) polarization map, (b) $|E_x|^2$, (c) $|E_y|^2$ and (d) E_z

3.2. Energy of the longitudinal component and photon-counting encryption

The integrated irradiance of the components of the focused field is defined as

$$I_j = \int |E_j|^2 \, dxdy \quad \text{with } j = x, y, z. \tag{16}$$

Figure 5a displays the ratio $I_z/(I_x + I_y + I_Z)$ as a function of α. The green dashed line represents the value corresponding to the circular polarization. The longitudinal irradiance I_z is always very small but radially polarized beams produce focused fields with the strongest longitudinal component [30, 31].



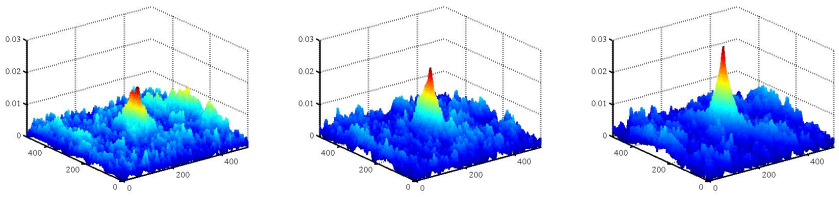
(a) (b)

Figure 5: (a) Ratio $I_z/(I_x + I_y + I_z)$ as a function of α; (b) Coefficient $\rho_{\max}$ as a function of α.

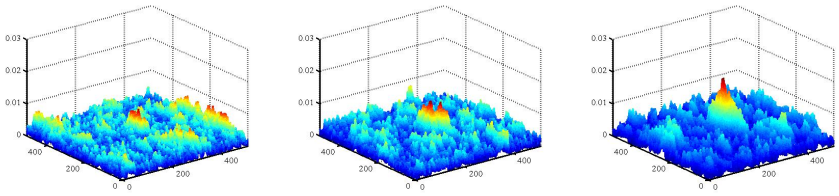
The image of Lena is encoded and encrypted on the longitudinal component [Eq. (9)] and then, the transverse components are recorded in photon counting conditions [Eq. (10)-(11)]. Figure 5b show the maximum value of the normalized correlation $\rho_{\max}$ between t and t^{ph} as function of α for $N_p = 5\%$ and $N_p = 8\%$ of the total number of pixels in the scene. It is apparent that the best results are obtained when the input beam is radially polarized ($\alpha = \pi/2$) because less photons are required to obtain the same correlation values. For completeness, correlation for some selected cases are presented in Fig. 6.

4. Concluding remarks

In this paper we analysed the dependence of the encoded signal with the polarization state of the input beam that illuminates an optical system able to generate highly focused beams for encryption purposes. When the system works using quantum image techniques it becomes stronger against attacks. In this case, the capability to perform successful validation depends on the number of photon counts. The message is encrypted in the longitudinal component of the focused field and thus this information is embedded by the transverse part of the field. For this reason, the use of radially polarized beams is advisable because



(a) $\rho_{\max}$=0.0099 (b) $\rho_{\max}$=0.013 (c) $\rho_{\max}$=0.0195



(d) $\rho_{\max}$=0.0172 (e) $\rho_{\max}$=0.023 (f) $\rho_{\max}$=0.0264

Figure 6: Photon-counting encryption correlation coefficient, $N_p = 8\%$: (a) circular polarization, (b) spiral polarization, (c) radial polarization. $N_p = 5\%$: (d) circular polarization, (e) spiral polarization, (f) radial polarization.

such beams produce more intense longitudinal signals. Consequently, validation can be performed successfully with less photons that other input polarizations.

Acknowledgments

This research is funded by Ministerio de Economía y Competitividad (Spain), projects FIS2013-46475.

References

[1] B. Javidi, J. L. Horner, Optical pattern recognition for validation and security verification, Opt. Eng. 33 (6) (1994) 1752–1756.

[2] O. Matoba, T. Nomura, E. Pérez-Cabré, M. S. Millán, B. Javidi, Optical techniques for information security, Proc. of the IEEE 97 (6) (2009) 1128–1148.

[3] A. Alfalou, C. Brosseau, Optical image compression and encryption methods, Adv. Opt. Photonics 1 (3) (2009) 589–636.

[4] W. Chen, B. Javidi, X. Chen, Advances in optical security systems, Adv. Opt. Photonics 6 (2) (2014) 120–155.

[5] P. Refregier, B. Javidi, Optical image encryption based on input plane and fourier plane random encoding, Opt. Letters 20 (7) (1995) 767–769.

[6] X. Tan, O. Matoba, Y. Okada-Shudo, M. Ide, T. Shimura, K. Kuroda, Secure optical memory system with polarization encryption, Appl. Opt. 40 (14) (2001) 2310–2315.

[7] O. Matoba, B. Javidi, Secure holographic memory by double-random polarization encryption, Appl. Opt. 43 (14) (2004) 2915–2919.

[8] A. Carnicer, A. Hassanfiroozi, P. Latorre-Carmona, Y.-P. Huang, B. Javidi, Security authentication using phase-encoded nanoparticle structures and polarized light, Opt. Lett. 40 (2) (2015) 135–138.

[9] A. Carnicer, O. Arteaga, E. Pascual, A. Canillas, S. Vallmitjana, B. Javidi, E. Bertran, Optical security verification by synthesizing thin films with unique polarimetric signatures, Opt. Lett. 40 (22) (2015) 5399–5402.

[10] A. Carnicer, M. Montes-Usategui, S. Arcos, I. Juvells, Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys, Opt. Lett. 30 (13) (2005) 1644–1646.

[11] X. Peng, P. Zhang, H. Wei, B. Yu, Known-plaintext attack on optical encryption based on double random phase keys, Opt. Lett. 31 (8) (2006) 1044–1046.

[12] Y. Frauel, A. Castro, T. J. Naughton, B. Javidi, Resistance of the double random phase encryption against various attacks, Opt. Express 15 (16) (2007) 10253–10265.

[13] H. Tashima, M. Takeda, H. Suzuki, T. Obi, M. Yamaguchi, N. Ohyama, Known plaintext attack on double random phase encoding using fingerprint as key and a method for avoiding the attack, Opt. Express 18 (13) (2010) 13772–13781.

[14] P. Kumar, A. Kumar, J. Joseph, K. Singh, Impulse attack free double-random-phase encryption scheme with randomized lens-phase functions, Opt. Lett. 34 (3) (2009) 331–333.

[15] T. J. Naughton, B. M. Hennelly, T. Dowling, Introducing secure modes of operation for optical encryption, J. Opt. Soc. Am. A 25 (10) (2008) 2608–2617.

[16] E. Pérez-Cabré, M. Cho, B. Javidi, Information authentication using photon-counting double-random-phase encrypted images, Opt. Lett. 36 (1) (2011) 22–24.

[17] D. Maluenda, A. Carnicer, R. Martínez-Herrero, I. Juvells, B. Javidi, Optical encryption using photon-counting polarimetric imaging, Opt. Express 23 (2) (2015) 655–666.

[18] B. Javidi, A. Carnicer, Roadmap on optical security, J. Optics (accepted, 2016).

[19] A. Carnicer, I. Juvells, B. Javidi, R. Martínez-Herrero, Optical encryption in the longitudinal domain of focused fields, Opt. Express 24 (7) (2016) 6793–6801.

[20] B. Richards, E. Wolf, Electromagnetic diffraction in optical systems. ii. structure of the image field in an aplanatic system, P. Rot. Soc Lond. A Mat. 253 (1274) (1959) 358–379.

[21] L. Novotny, B. Hecht, Principles of nano-optics, Cambridge University Press, 2012.

[22] A. Carnicer, I. Juvells, D. Maluenda, R. Martínez-Herrero, P. M. Mejías, On the longitudinal component of paraxial fields, Eur. J. Phys. 33 (5) (2012) 1235.

[23] J. W. Goodman, R. L. Haupt, Statistical Optics, John Wiley & Sons, 2015.

[24] S. Yeom, B. Javidi, E. Watson, Photon counting passive 3d image sensing for automatic target recognition, Optics express 13 (23) (2005) 9310–9330.

[25] B. Tavakoli, B. Javidi, E. Watson, Three dimensional visualization by photon counting computational integral imaging, Optics Express 16 (7) (2008) 4426–4436.

[26] A. Stern, D. Aloni, B. Javidi, Experiments with three-dimensional integral imaging under low light levels, IEEE Photonics Journal 4 (4) (2012) 1188–1195.

[27] A. Carnicer, B. Javidi, Polarimetric 3d integral imaging in photon-starved conditions, Optics express 23 (5) (2015) 6408–6417.

[28] D. Maluenda, I. Juvells, R. Martínez-Herrero, A. Carnicer, Reconfigurable beams with arbitrary polarization and shape distributions at a given plane, Opt. Express 21 (5) (2013) 5432–5439.

[29] D. Maluenda, R. Martínez-Herrero, I. Juvells, A. Carnicer, Synthesis of highly focused fields with circular polarization at any transverse plane, Opt. Express 22 (6) (2014) 6859–6867.

[30] R. Dorn, S. Quabis, G. Leuchs, Sharper focus for a radially polarized light beam, Phys. Rev. Lett. 91 (23) (2003) 233901.

[31] R. Martínez-Herrero, I. Juvells, A. Carnicer, On the physical realizability of highly focused electromagnetic field distributions, Opt. Letters 38 (12) (2013) 2065–2067.