Optical encryption in the longitudinal domain of focused fields

Artur Carnicer,[1,*] Ignasi Juvells,[1] Bahram Javidi,[2] and Rosario Martínez-Herrero[3]

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

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

[3]*Departamento de Óptica, Facultad de Ciencias Físicas, Universidad Complutense de Madrid, Ciudad Universitaria, 28040 Madrid, Spain*

[*]*artur.carnicer@ub.edu*

Abstract: We develop a method for encoding information in the longitudinal component of a focused field. Focused beams display a non-zero contribution of the electric field in the direction of propagation. However, the associated irradiance is very weak and difficult to isolate from the transverse part of the beam. For these reasons, the longitudinal component of a focused field could be a good choice for encoding and securing information. Using the Richards and Wolf formalism we show how to encrypt information in the longitudinal domain of the focal area. In addition, we use quantum imaging techniques to enhance the security and to prevent unauthorized access to the information. To the best of our knowledge, this is the first report on using the longitudinal component of the focused fields in optical security.

OCIS codes: (100.4998) Pattern recognition, optical security and encryption; (260.5430) Polarization; (030.5260) Photon counting.

References and links

1. R. Dorn, S. Quabis, and G. Leuchs, "Sharper focus for a radially polarized light beam," Phys. Rev. Lett. **91**(23), 233901 (2003).
2. N. Davidson and N. Bokor, "High-numerical-aperture focusing of radially polarized doughnut beams with a parabolic mirror and a flat diffractive lens," Opt. Lett. **29**(12), 1318–1320 (2004).
3. M. Leutenegger, R. Rao, R. A. Leitgeb, and T. Lasser, "Fast focus field calculations," Opt. Express **14**(23), 11277–11291 (2006).
4. Y. Kozawa and S. Sato, "Sharper focal spot formed by higher-order radially polarized laser beams," J. Opt. Soc. Am. A **24**(6), 1793–1798 (2007).
5. H. Wang, L. Shi, B. Lukyanchuk, C. Sheppard, and C. T. Chong, "Creation of a needle of longitudinally polarized light in vacuum using binary optics," Nat. Photonics **2**(8), 501–505 (2008).
6. G. M. Lerman and U. Levy, "Effect of radial polarization and apodization on spot size under tight focusing conditions," Opt. Express **16**(7), 4567–4581 (2008).
7. X. Hao, C. Kuang, T. Wang, and X. Liu, "Phase encoding for sharper focus of the azimuthally polarized beam," Opt. Lett. **35**(23), 3928–3930 (2010).
8. S. N. Khonina and S. G. Volotovsky, "Controlling the contribution of the electric field components to the focus of a high-aperture lens using binary phase structures," J. Opt. Soc. Am. A **27**(10), 2188–2197 (2010).
9. Q. Zhan, "Cylindrical vector beams: from mathematical concepts to applications," Adv. Opt. Photonics **1**(1), 1–57 (2009).
10. R. Martínez-Herrero, I. Juvells, and A. Carnicer, "On the physical realizability of highly focused electromagnetic field distributions," Opt. Lett. **38**(12), 2065–2067 (2013).
11. O. Matoba, T. Nomura, E. Pérez-Cabré, M. S. Millan, and B. Javidi, "Optical Techniques for Information Security," Proc. IEEE **97**(6), 1128–1148 (2009).
12. B. Javidi and A. Carnicer, "Roadmap in optical encryption and security," J. Opt. (accepted for publication).
13. W. Chen, B. Javidi, and X. Chen, "Advances in optical security systems," Adv. Opt. Photonics **6**(2), 120–155 (2014).
14. B. Richards and E. Wolf, "Electromagnetic diffraction in optical systems. II. Structure of the image field in an aplanatic system," P. Royal Soc. London A Mater. **253**(1274), 358–379 (1959).
15. P. Réfrégier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. **20**(7), 767–769 (1995).

#255568 Received 10 Dec 2015; revised 16 Mar 2016; accepted 17 Mar 2016; published 21 Mar 2016

16. B. Javidi and J. L. Horner, "Optical pattern recognition for validation and security verification," Opt. Eng. **33**(6), 1752–1756 (1994).
17. O. Matoba and B. Javidi, "Encrypted optical memory system using three-dimensional keys in the Fresnel domain," Opt. Lett. **24**(11), 762–764 (1999).
18. G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain," Opt. Lett. **25**(12), 887–889 (2000).
19. X. Tan, O. Matoba, Y. Okada-Shudo, M. Ide, T. Shimura, and K. Kuroda, "Secure optical memory system with polarization encryption," Appl. Opt. **40**(14), 2310–2315 (2001).
20. O. Matoba and B. Javidi, "Secure holographic memory by double-random polarization encryption," Appl. Opt. **43**(14), 2915–2919 (2004).
21. J. F. Barrera, R. Henao, M. Tebaldi, R. Torroba, and N. Bolognini, "Multiplexing encrypted data by using polarized light," Opt. Commun. **260**(1), 109–112 (2006).
22. W. Chen, X. Chen, and C. J. R. Sheppard, "Optical image encryption based on diffractive imaging," Opt. Lett. **35**(22), 3817–3819 (2010).
23. A. Carnicer, M. Montes-Usategui, S. Arcos, and I. Juvells, "Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys," Opt. Lett. **30**(13), 1644–1646 (2005).
24. X. Peng, P. Zhang, H. Wei, and B. Yu, "Known-plaintext attack on optical encryption based on double random phase keys," Opt. Lett. **31**(8), 1044–1046 (2006).
25. Y. Frauel, A. Castro, T. J. Naughton, and B. Javidi, "Resistance of the double random phase encryption against various attacks," Opt. Express **15**(16), 10253–10265 (2007).
26. H. Tashima, M. Takeda, H. Suzuki, T. Obi, M. Yamaguchi, and 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), 13772–13781 (2010).
27. K. Nakano, M. Takeda, H. Suzuki, and M. Yamaguchi, "Evaluations of phase-only double random phase encoding based on key-space analysis," Appl. Opt. **52**(6), 1276–1283 (2013).
28. P. Kumar, A. Kumar, J. Joseph, and K. Singh, "Impulse attack free double-random-phase encryption scheme with randomized lens-phase functions," Opt. Lett. **34**(3), 331–333 (2009).
29. T. J. Naughton, B. M. Hennelly, and T. Dowling, "Introducing secure modes of operation for optical encryption," J. Opt. Soc. Am. A **25**(10), 2608–2617 (2008).
30. K. Nakano, M. Takeda, H. Suzuki, and M. Yamaguchi, "Security analysis of phase-only DRPE based on known-plaintext attack using multiple known plaintext-ciphertext pairs," Appl. Opt. **53**(28), 6435–6443 (2014).
31. E. Pérez-Cabré, M. Cho, and B. Javidi, "Information authentication using photon-counting double-random-phase encrypted images," Opt. Lett. **36**(1), 22–24 (2011).
32. M. Cho and B. Javidi, "Three-dimensional photon counting double-random-phase encryption," Opt. Lett. **38**(17), 3198–3201 (2013).
33. D. Maluenda, A. Carnicer, R. Martínez-Herrero, I. Juvells, and B. Javidi, "Optical encryption using photon-counting polarimetric imaging," Opt. Express **23**(2), 655–666 (2015).
34. L. Novotni and B. Hecht, *Principles of Nano-Optics* (Cambridge University, 2012)
35. A. Carnicer, I. Juvells, D. Maluenda, R. Martínez-Herrero, and P. M. Mejías, "On the longitudinal component of paraxial fields," Eur. J. Phys. **33**(5), 1235–1247 (2012).
36. J. W. Goodman, *Statistical Optics* (John Wiley & Sons, 1985)
37. V. Arrizón, L. A. González, R. Ponce, and A. Serrano-Heredia, "Computer-generated holograms with optimum bandwidths obtained with twisted-nematic liquid-crystal displays," Appl. Opt. **44**(9), 1625–1634 (2005).
38. D. Maluenda, R. Martínez-Herrero, I. Juvells, and A. Carnicer, "Synthesis of highly focused fields with circular polarization at any transverse plane," Opt. Express **22**(6), 6859–6867 (2014).
39. D. Maluenda, I. Juvells, R. Martínez-Herrero, and A. Carnicer, "Reconfigurable beams with arbitrary polarization and shape distributions at a given plane," Opt. Express **21**(5), 5432–5439 (2013).

1. Introduction

Nowadays, highly focused beams are present in numerous research areas and technical applications [1–10]. However, to the best of our knowledge no research has been reported in the field of optical security [11–13], using focused fields. It is well known that the electric field associated to a plane wave is transverse to the direction of propagation. However, in general this is not true for converging beams since a non-zero contribution of the electric field in the direction of propagation appears. This fact is a consequence of the Maxwell's Equations. Nevertheless, the irradiance of this longitudinal component is small compared to the energy associated to the transverse components, even when the beam is focused with a high numerical aperture objective lens. In fact, the transverse part of the field completely embeds the longitudinal irradiance. Furthermore, it is not possible to isolate the irradiance of the longitudinal component by using holographic techniques or by means of polarizers. Taking focused fields into account, it seems appropriate to hide and/or secure information in the longitudinal component. Thus, focused fields can be used for optical security provided an authorized user is able to access the encoded message. Despite the fact that the longitudinal

#255568 Received 10 Dec 2015; revised 16 Mar 2016; accepted 17 Mar 2016; published 21 Mar 2016

component of the field cannot be easily accessed, the Gauss law provides a mean to numerically access the encoded information by using the transverse field distribution. This encoding procedure can be used in combination with a variety of optical encryption techniques, and providing an extra layer of security.

In this paper, we describe how to encode information in the longitudinal component of a focused field within the framework of the Richardson and Wolf vector propagation theory [14]. We demonstrate that the signal can be encrypted to be equivalent to the cypher-text obtained using classical Double Random Phase Encryption (DRPE) [15]. Consequently, additional improvements with optical security techniques [16–22] could be adapted to be used with focused beams. To avoid conventional attacks against the information encrypted in the longitudinal component [23–30], the use of quantum imaging techniques is suggested [31–33].

The paper is organized as follows: in section 2 we summarize basic concepts in vector diffraction theory, and in section 3 we introduce a method for encoding information in the longitudinal component of a focused field. In section 4, we present how the codification technique is adapted for obtaining encrypted signals in the longitudinal domain. Finally, the conclusions are presented in section 5.

2. Review on highly focused beams

The electric field **E** at the focal area of a high numerical aperture (NA) microscope lens following the sine condition is described by the so-called Richards-Wolf integral [14]:

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

where A is a proportionality constant, k is the wavenumber, r and ϕ are the polar coordinates at the focal plane, θ and φ are the polar and azimuthal angles at the exit pupil and θ_0 is the semi-aperture angle, i.e. NA = sin θ_0. See Fig. 1 for details. $\mathbf{E}_\infty$ is the field at the Gaussian sphere of reference, described as:

$$\mathbf{E}_\infty(\theta,\phi) = P(\theta)\left(a\mathbf{e_1}(\phi) + b\mathbf{e_2}(\phi,\theta)\right). \quad (2)$$

This field can also be understood as the vector angular spectrum of plane waves. In Eq. (2), $P(\theta)$ is the so-called apodization function; in particular, for isoplanatic optical systems following the sine condition $P(\theta) = \sqrt{\cos\theta}$; $\mathbf{e_1}$ and $\mathbf{e}^{\mathbf{i}}_{\mathbf{2}}$ are unit vectors in the radial and azimuthal directions, and $\mathbf{e_2}$ is the projection of $\mathbf{e}^{\mathbf{i}}_{\mathbf{2}}$ on the convergent wave-front surface:

$$\begin{aligned}
\mathbf{e_1}(\phi) &= (-\sin\phi, \cos\phi, 0)\\
\mathbf{e}^{\mathbf{i}}_{\mathbf{2}}(\phi) &= (\cos\phi, \sin\phi, 0)\\
\mathbf{e_2}(\phi,\theta) &= (\cos\theta\cos\phi, \cos\theta\sin\phi, \sin\theta).
\end{aligned} \quad (3)$$

The wave-front vector **s** is defined as:

$$\mathbf{s} = (\alpha,\beta,\gamma) = \left(\sin\theta\cos\phi, \sin\theta\sin\phi, -\cos\theta\right). \quad (4)$$

Here, $\mathbf{e_1}$, $\mathbf{e_2}$ and **s** form a triad of a mutually orthogonal right-handed system of unit vectors. Note that $\mathbf{E}_\infty$ is normal to the wavefront vector **s**, that is $\mathbf{s}\cdot\mathbf{E}_\infty = 0$. Distributions a and b are the azimuthal and radial parts of input field $\mathbf{E_0}$ assumed transverse $\mathbf{E_0} = (E_{0x}, E_{0y}, 0)$:

$$\begin{aligned}
a &= \mathbf{E_0}\cdot\mathbf{e_1} = -E_{0x}\sin\phi + E_{0y}\cos\phi\\
b &= \mathbf{E_0}\cdot\mathbf{e}^{\mathbf{i}}_{\mathbf{2}} = E_{0x}\cos\phi + E_{0y}\sin\phi.
\end{aligned} \quad (5)$$

The Richards-Wolf integral can be rewritten in a more compact way by using Fourier transforms. The first exponential term in Eq. (1) is developed as follows:

#255568 Received 10 Dec 2015; revised 16 Mar 2016; accepted 17 Mar 2016; published 21 Mar 2016

$$\exp\left(ikr\sin\theta\cos\left(\varphi-\phi\right)\right)=\exp\left(i\frac{2\pi}{\lambda}\left(\alpha x+\beta y\right)\right) \tag{6}$$

where $x = r\cos\varphi$ and $y = r\sin\varphi$ are the rectangular coordinates at the focal plane, and λ is the wavelength of the illumination source. Let $(x_\infty, y_\infty, z_\infty)$ be the coordinates of a point on the Gaussian sphere of reference. According to Fig. 1, $x_\infty = f\alpha$ and $y_\infty = f\beta$, and $\exp\left(i\frac{2\pi}{\lambda}\left(\alpha x+\beta y\right)\right)=\exp\left(i\frac{2\pi}{\lambda f}\left(x_\infty x+y_\infty y\right)\right)$, where f is the focal length of the objective lens. In addition, surface differentials are related by $\sin\theta d\theta d\phi=\frac{1}{f^2\cos\theta}dx_\infty dy_\infty$ (see chapter 3 of reference [34] for details). Equation (1) at z = 0 becomes:

$$\mathbf{E}(x,y,0)=\mathrm{FT}_{\lambda f}\left[\frac{\mathbf{E}_\infty}{\cos\theta}\right]=\mathrm{FT}_{\lambda f}\left[\frac{\left(\left(\mathbf{E}_0\cdot\mathbf{e}_1\right)\mathbf{e}_1+\left(\mathbf{E}_0\cdot\mathbf{e}_2^{\iota}\right)\mathbf{e}_2\right)}{\sqrt{\cos\theta}}\right], \tag{7}$$

where operator $\mathrm{FT}_{\lambda f}[]$ stands for the λf–scaled Fourier transform.

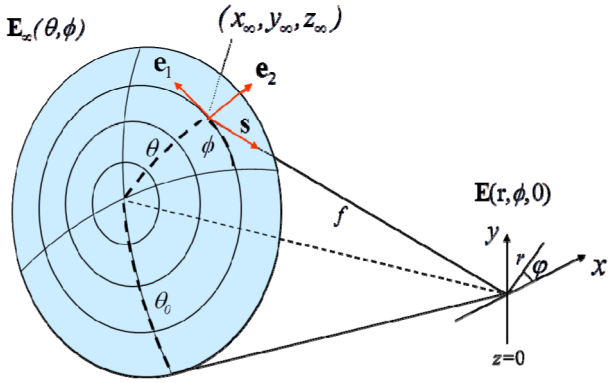

Fig. 1. Notation and coordinate systems at the Gaussian reference sphere and at the focal plane.

It is worth to point out that even though the incident beam $\mathbf{E_0}$ is assumed to be purely transverse, the electric field at the focal plane $\mathbf{E}(x,y,0)$ shows a non-negligible longitudinal component E_z . Thus, the polarization has to be described as a 3D phenomenon. The radial part of $\mathbf{E}_\infty$ generates the longitudinal component of the focused field since vector $\mathbf{e_2}$ is not transverse. On the other hand, an azimuthal beam with $b = 0$ produces a purely transverse focused field, i.e. with a longitudinal component $E_z = 0$.

3. Information encoding

A remarkable property of focused fields is the irradiance associated to the longitudinal component I_z

$$I_z=\int\left|E_z\right|^2 dxdy. \tag{8}$$

This longitudinal component is very small compared with the irradiance of the total field **E**:

$$I_T=I_x+I_y+I_z=\int\left(\left|E_x\right|^2+\left|E_y\right|^2+\left|E_z\right|^2\right)dxdy. \tag{9}$$

For instance, for a circularly polarized input beam used in combination with an objective lens NA = 0.9, $I_z \approx 0.003 I_T$ [35]. The z-component of the focal electric field cannot be separated

#255568 Received 10 Dec 2015; revised 16 Mar 2016; accepted 17 Mar 2016; published 21 Mar 2016

from the other two components using linear polarizers and/or holographic recording. Thus, it cannot be accessed by direct observation using conventional optical equipment. For this reason, the use of highly focused fields in optical security enables the possibility to securely encode information in the longitudinal component E_z. Since the energy associated with the longitudinal component is very weak, the information is embedded by the transverse part of the focused field. This encoding approach can be understood as a way of implementing steganography using the physical properties of focused light beams.

According to Eqs. (2) and (3), the longitudinal component of the vector angular spectrum reads:

$$E_{\infty z} = \sqrt{\cos\theta} b \sin\theta = \sqrt{\cos\theta}\left(\mathbf{E_0}\cdot\mathbf{e}_2^{\mathbf{i}}\right)\sin\theta = \sqrt{\cos\theta}\left(E_{0x}\cos\phi + E_{0y}\sin\phi\right)\sin\theta.. \quad (10)$$

The longitudinal or z-component of the focused field is obtained using Eq. (7):

$$E_z(x,y,0) = \mathrm{FT}_{\lambda f}\left[\frac{E_{\infty z}}{\cos\theta}\right] = \mathrm{FT}_{\lambda f}\left[\left(E_{0x}\cos\phi + E_{0y}\sin\phi\right)\frac{\sin\theta}{\sqrt{\cos\theta}}\right]. \quad (11)$$

This equation provides a simple relationship between the longitudinal component of the focused field E_z and the input beam $\mathbf{E_0}$. Equivalently,

$$E_{0x}\cos\phi + E_{0y}\sin\phi = \frac{\sqrt{\cos\theta}}{\sin\theta}\mathrm{FT}_{\lambda f}^{-1}\left[E_z(x,y,0)\right]. \quad (12)$$

Depending on how the system is illuminated, $E_{\infty z}$ is described differently. For instance, if the input beam is circularly polarized $\mathbf{E}_0 = (E_0, iE_0, 0)$, then $E_{\infty z} = E_0\sqrt{\cos\theta}\sin\theta\exp(i\phi)$ and

$$E_0 = \exp(-i\phi)\frac{\sqrt{\cos\theta}}{\sin\theta}\mathrm{FT}_{\lambda f}^{-1}\left[E_z\right],\ E_z = \mathrm{FT}_{\lambda f}\left[\exp(i\phi)E_0\frac{\sin\theta}{\sqrt{\cos\theta}}\right]. \quad (13)$$

Alternatively, if the system is illuminated with a radially polarized beam, then $\mathbf{E}_0 = (E_0\cos\phi, E_0\sin\phi, 0)$ then $E_{\infty z} = E_0\sqrt{\cos\theta}\sin\theta$. In this case

$$E_0 = \frac{\sqrt{\cos\theta}}{\sin\theta}\mathrm{FT}_{\lambda f}^{-1}\left[E_z\right],\ E_z = \mathrm{FT}_{\lambda f}\left[E_0\frac{\sin\theta}{\sqrt{\cos\theta}}\right]. \quad (14)$$

Interestingly, azimuthally polarized beams, that is $\mathbf{E}_0 = (-E_0\sin\phi, E_0\cos\phi, 0)$, produce purely transverse distributions of light at the focal plane, i.e. $E_{\infty z} = 0$. This means that this polarization cannot be used since no longitudinal component is generated.

Despite the fact that I_z is very weak compared with the total irradiance of the focused field and E_z cannot be isolated from the transverse part of the beam, the longitudinal component can be accessed using the condition $\mathbf{s}\cdot\mathbf{E}_\infty = 0$, or $\alpha E_{\infty x} + \beta E_{\infty y} + \gamma E_{\infty z} = 0$ with $\gamma = -\sqrt{1-\alpha^2-\beta^2}$. Then, the longitudinal component E_z can be deduced from:

$$E_z = \mathrm{FT}_{\lambda f}\left[\frac{\alpha\mathrm{FT}_{\lambda f}^{-1}\left[E_x\right] + \beta\mathrm{FT}_{\lambda f}^{-1}\left[E_y\right]}{\sqrt{1-\alpha^2-\beta^2}}\right]. \quad (15)$$

Because the transverse components of the focused field E_x and E_y can be determined experimentally (see section 4), Eq. (15) indicates a practical way to estimate the component E_z.

#255568 Received 10 Dec 2015; revised 16 Mar 2016; accepted 17 Mar 2016; published 21 Mar 2016

4. Encryption and validation

In the previous section, we have demonstrated a method for encoding information in the longitudinal field of a highly focused beam. Among the different possibilities for encrypting information in the longitudinal component E_z using the present approach, we have selected the simplest one. Let M_1 and M_2 random phase masks (keys), and t the plain-text to be encoded [Fig. 2]. Using circularly polarized light [Eq. (13)], the encrypted components of the input beam E'_{0x} and E'_{0y} are:

$$E'_{0x} = \exp(-i\phi)\frac{\sqrt{\cos\theta}}{\sin\theta} M_2 \mathrm{FT}_{\lambda f}\left[M_1 t\right],\ E'_{0y} = iE'_{0x}. \tag{16}$$

Interestingly, in this case the generated cypher-text E'_z is identical to the one obtained with the classical double random phase encryption procedure (DRPE) [15,16]:

$$E'_z = \mathrm{FT}_{\lambda f}\left[\exp(i\phi)E'_{0x}\frac{\sin\theta}{\sqrt{\cos\theta}}\right] = \mathrm{FT}_{\lambda f}\left[M_2 \mathrm{FT}_{\lambda f}\left[M_1 t\right]\right]. \tag{17}$$

As indicated in Eq. (15) and (16), t can be determined from the information contained in the focused encoded components E'_x and E'_y, provided M_2 is known.

$$t = \left|\mathrm{FT}^{-1}_{\lambda f}\left[M_2^{-1}\frac{\alpha \mathrm{FT}^{-1}_{\lambda f}\left[E'_x\right] + \beta \mathrm{FT}^{-1}_{\lambda f}\left[E'_y\right]}{\sqrt{1-\alpha^2-\beta^2}}\right]\right|. \tag{18}$$

Note that the present encoding system shares the same weakness of the DRPE method. Despite the fact that a plurality of attacks have been designed to break DRPE systems [23–30], different approaches were suggested to improved security in DRPE. For instance, it has been demonstrated that quantum encryption systems that works with few photons are very secure [31,32]. In this case, the encrypted signal is no longer accessible but it can be authenticated. Moreover, note that other non-linear encryption procedures can be implemented in the longitudinal domain as well.

If a system works in low light illumination conditions, irradiance is recorded according to the photon-counting model. It is assumed that, in these conditions the image is statistically modeled by the Poisson distribution [36]. The photon-counting binary version $|E'_x|^{ph}$ of $|E'_x|$ is obtained according to:

$$\left|E'_x\right|^{ph}(x,y) = \begin{cases} 0, \text{ if } \mathrm{rand}(x,y) \le \exp\left(-n_p(x,y)\right) \\ 1, \text{otherwise} \end{cases} \tag{19}$$

where rand(x, y) is a uniformly distributed random number within the range [0,1], N_P is the predetermined number of photon counts in the entire scene, NxM is the total number of pixels and $n_p(x,y)$ is the normalized irradiance at pixel (x, y):

$$n_p(x,y) = \frac{N_p\left|E'_x(x,y)\right|^2}{\sum_{n,m=1}^{N,M}\left|E'_x(n,m)\right|^2} \tag{20}$$

m and n are the summation indices and $|E'_y|^{ph}$ is generated using the same approach. The encrypted signal uses the photon-counting version of E'_x and E'_y but the phase remains the same:

$$E'^{ph}_x = \left|E'_x\right|^{ph}\frac{E'_x}{\left|E'_x\right|} \text{ and } E'^{ph}_y = \left|E'_y\right|^{ph}\frac{E'_y}{\left|E_y\right|}. \tag{21}$$

#255568 Received 10 Dec 2015; revised 16 Mar 2016; accepted 17 Mar 2016; published 21 Mar 2016

Finally, t^{ph} is estimated by means of Eq. (18). To determine whether t^{ph} contains information related with t or not, the correlation coefficient ρ calculated at pixel (x,y) is:

$$\rho(x,y)=\frac{\sum_{n,m=1}^{N,M}\left[t^{ph}(m+x,n+y)-\left\langle t^{ph}\right\rangle\right]\left[t(m,n)-\langle t\rangle\right]}{\sqrt{\sum_{n,m=1}^{N,M}\left[t^{ph}(m,n)-\left\langle t^{ph}\right\rangle\right]^2\sum_{n,m=1}^{N,M}\left[t(m,n)-\langle t\rangle\right]^2}}, \tag{22}$$

where $\left\langle t^{ph}\right\rangle$ and $\langle t\rangle$ are respectively the mean values of t^{ph} and t.

The presented encryption procedure could be implemented in practice using an optical setup able to generate highly focused fields using only conventional components. To provide more insight, we suggest a possible design for a practical implementation. This system is sketched in Fig. 2(a). First, image t is phase-encoded using a random code such as a diffuser (mask M_1) and illuminated by a circularly polarized coherent source. The set $M_1 t$ is located in the front focal plane of lens L_1. This distribution is optically Fourier transformed using lens L_1. A transmission type modulator is placed in the back focal plane of L_1. Half-wave plate HWP and quarter-wave plate QWP are used to set up a twisted nematic modulator in order to achieve a phase-mostly configuration. Using Arrizon's cell-oriented codification method [37], it is possible to achieve full complex modulation: a certain value in the complex plane can be accessed as a combination of two points that belong to the modulation curve. A detailed explanation of the implementation of this procedure can be found in references [38,39]. This device displays hologram H containing the following information

$$H=\exp(-i\phi)\frac{\sqrt{\cos\theta}}{\sin\theta}M_2. \tag{23}$$

The SLM plane is imaged on the entrance pupil plane of the microscope objective using lenses L_A and L_B in a *4f* configuration. The spatial filter in the back focal plane of lens L_A is required to remove non-desired high order terms produced during the codification. Interestingly, the informative part of the beam is propagated on axis. Then, the field E'_x is focused by means of an objective lens and the transverse part of field is recorded by a CCD camera. In order to preserve the phase of the encrypted field, the interference between the field E'_x and a reference beam is recorded. E'_y is accessed in a similar way, by rotating 90° polarizer LP. Using encrypted components E'_x, and E'_y, and the correct mask M_2, plain-text t can be numerically accessed with the help of Eq. (18).

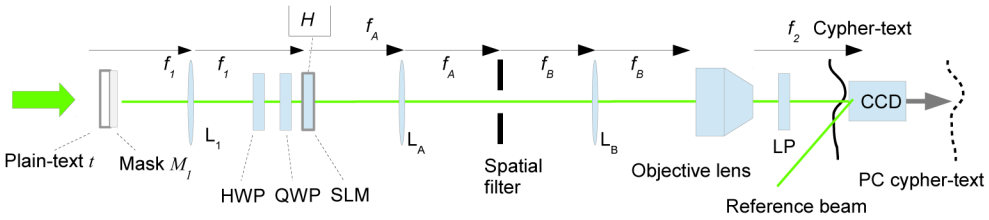

Fig. 2. (a) Optical setup to implement for the proposed encryption procedure: L_1: Fourier lens; L_A and L_B: relay optics lenses; f_1, f_A, f_B and f_2 are the focal lengths of lenses L_1, L_A, L_B and the microscope objective respectively; SLM: spatial light modulator; HWP and QWP: half and quarter wave plates; LP: linear polarizer; CCD: camera.

Note that misalignment is a very serious problem that can jeopardize the encryption procedure. Since the matching procedure can be a laborious task, instead of using lens L_1 to produce the Fourier transform of the input signal, distribution H FT[$M1$ t] can be displayed directly on the SLM, being lens L_1 no longer necessary.

#255568 Received 10 Dec 2015; revised 16 Mar 2016; accepted 17 Mar 2016; published 21 Mar 2016

5. Numerical tests

Some calculations were carried out to demonstrate how the system works. A 512x512 pixels image of Lena is used as the plaintext t to be encoded in the longitudinal domain E_z. Figure 3 displays $|E'_x|^2$ and $|E'_z|^2$. Note that $|E'_x|^2 = |E'_y|^2$ whereas $|E'_z|^2$ is a random distribution.

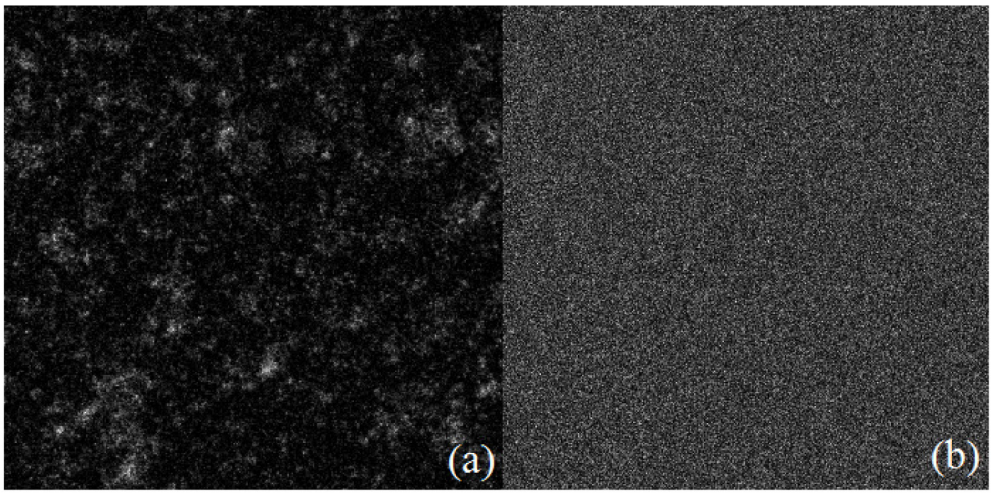

Fig. 3. Encrypted components: (a) $|E'_x|^2$ and (b) $|E'_z|^2$.

Figure 4 shows photon counting versions of $|E'_x|^{ph}$, $|E'_y|^{ph}$. N_P is set to 10% of the pixels of the image.

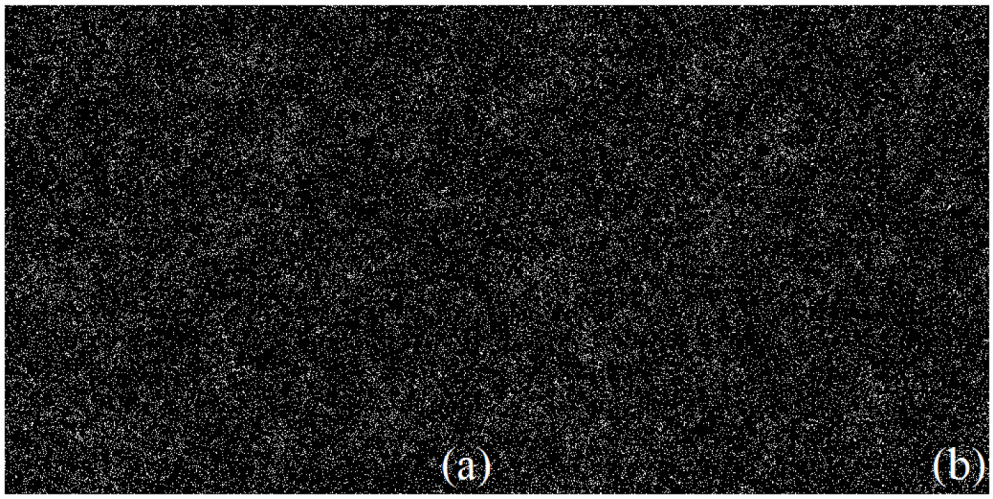

Fig. 4. Photon counting encrypted components: (a) $|E'_x|^{ph}$, (b) $|E'_y|^{ph}$.

Figs. 5(a) and 5(b) show the recovered signals t and t^{ph}. Correlation ρ when the correct key mask M_2 and an incorrect key mask M_2 are used are presented in Figs. 5(c) and 5(d). As expected, t^{ph} does not provide any visual information of the plain-text image, but correlation ρ between t^{ph} and t shows a clear peak when the proper key mask is used. Figures 5(e) and 5(f) display correlation ρ with the true and false phase masks but using a higher number of photons (N_P = 0.15 photons/pixel).

#255568 Received 10 Dec 2015; revised 16 Mar 2016; accepted 17 Mar 2016; published 21 Mar 2016

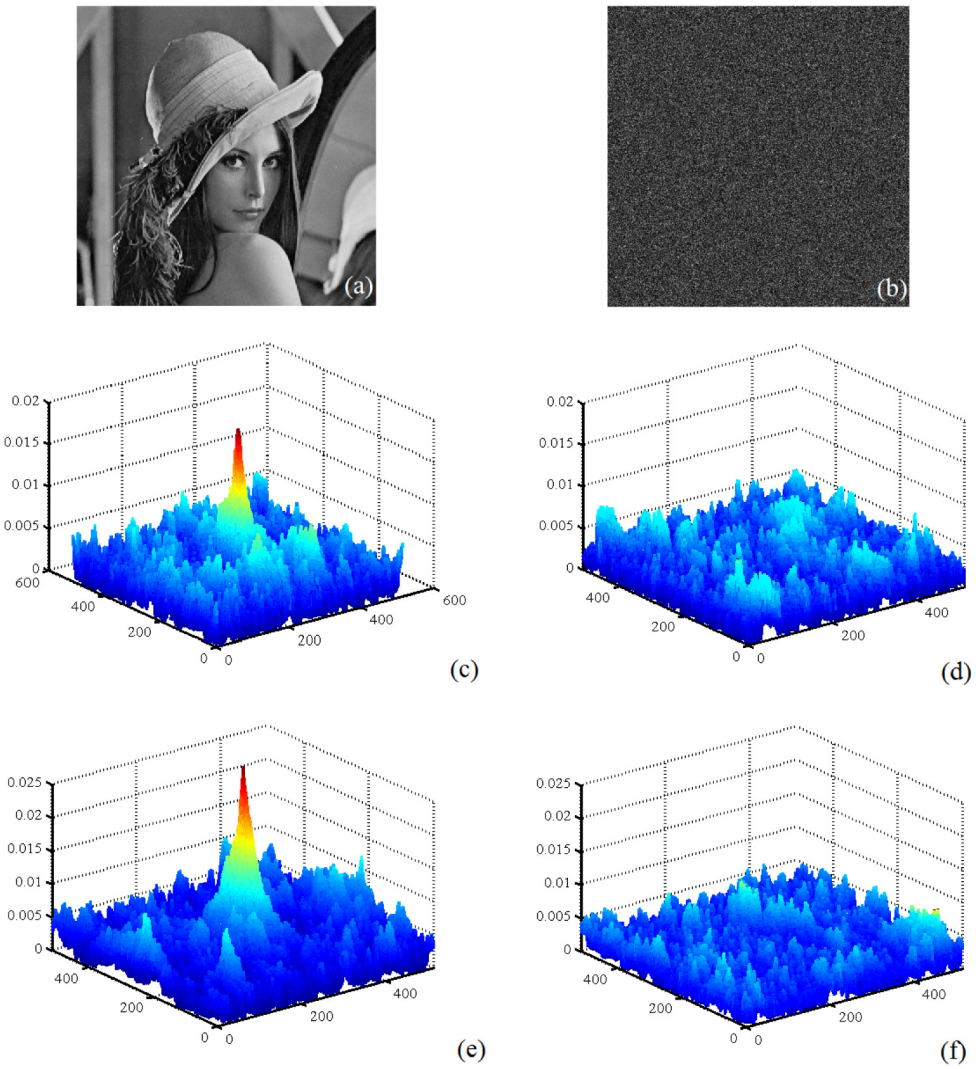

Fig. 5. Recovered signals using the correct key M2: (a) decrypted plaintext t (b) photon-counting decrypted plaintext t^{ph}, (c) correlation signal ρ using the correct key M_2 and N_P = 0.1 photons/pixel, (d) ρ using an incorrect key M_2 and N_P = 0.1 photons/pixel, (e) correlation signal ρ using the correct key M_2 and N_P = 0.15 photons/pixel, (f) ρ using an incorrect key M_2 and N_P = 0.15 photons/pixel.

#255568 Received 10 Dec 2015; revised 16 Mar 2016; accepted 17 Mar 2016; published 21 Mar 2016