Improved optical encryption by using tilted lenses

VICENTE MICO,[1,*] IGNACIO MORENO,[2] ZEEV ZALEVSKY,[3] CARLOS FERREIRA[1]

[1]*Departamento de Óptica y de Optometría y Ciencias de la Visión, Facultad de Física, Universitat de Valencia, C/Doctor Moliner 50, Burjassot, 46100, Spain*
[2]*Departamento de Ciencia de Materiales, Óptica y Tecnología Electrónica, Universidad Miguel Hernández, 03202, Elche, Spain*
[2]*School of Engineering, Bar-Ilan University, Ramat-Gan, 52900 Israel*
**Corresponding author: Vicente.Mico@uv.es*

Received XX Month XXXX; revised XX Month, XXXX; accepted XX Month XXXX; posted XX Month XXXX (Doc. ID XXXXX); published XX Month XXXX

A novel concept based on tilted spherical lenses for optical encryption using Lohmann's type I systems is presented. The tilt angle of the spherical lenses is used as encrypted key and the decryption performance is studied both qualitatively (visual image degradation) and quantitatively (MSE analysis) by numerical simulations. The paper presents a general mathematical framework in virtue of the dioptric power matrix formalism and oblique central refraction used in optometry field. Computer simulations show that image information cannot be retrieved after a few degrees of tilt on both spherical lenses in the encryption system. In addition, a preliminary experiment in presented considering a hybrid encryption/decryption process where the image is numerically encrypted but optically decrypted.

OCIS codes: *(070.4550) Correlators; (080.2575) Fractional Fourier transforms; (100.4998) Pattern recognition, optical security and encryption; (200.3050) Information processing.*

http://dx.doi.org/10.1364/AO.99.099999

1. INTRODUCTION

The secure transmission of information among restricted numbers of persons or entities/companies in several and different areas such as industry, business, defense and others is a very appealing research field. Aimed to that, a big amount of methods using different coding processes have been developed in the last years. Among them, optical image encryption systems play an important role due to its inherent capacity to process data in parallel. Most of them are based on the technique proposed by Réfrégier and Javidi in 1995 and known as double random phase encryption (DRPE) [1]. After this pioneer work, Javidi et al. reported on different modifications of that method in order to improve the encryption [2-9]. The common characteristic of these methods is the use of two classical Fourier transformers in cascade with two random phase masks (RPM), one placed at the input plane and the other placed at the Fourier plane of the first Fourier transformer just to get the encrypted image. And the same RPMs act as keys in the decryption process.

Making use of the fractional Fourier systems introduced by Lohmann [10,11] and Mendlovic and Ozaktas [12-14], some years later Unnikrishnan et al. improved the security of this kind of systems by performing the encryption with a pair of fractional Fourier transformers in cascade [15,16]. And nowadays the fractional orders constitute additional keys for the encryption/decryption of information.

After those works using fractional Fourier systems, several methods based on iterative fractional Fourier transform [17,18] as well as encoding in the Fresnel domain [19] have been successfully proposed. And many references have been published since then in the field following these ideas such as, for instance, encryption obtained by combining digital holography and the joint transform correlator architecture [20], or double image encryption combining fractional Fourier domain and pixel scrambling technique [21], or linear blend operation [22].

The extension to anamorphic fractional Fourier transformers in the DRPE is straightforward [23-26]. Those approaches provide the encoding of a 2D image with two different fractional orders in two orthogonal directions by using cylindrical lenses in Lohmann's bulk systems [27]. As a way to improve security far beyond, Kumar et al. reported on the use of anamorphic system in a two Lohmann's type II in cascade configuration where the spherical lenses were replaced by pairs of orthogonally aligned cylindrical lenses [28]. Moreover, they introduced global in-plane rotations at each of the fractional Fourier transformers as extra encryption keys.

In a previous paper inspired on the method reported by Kumar et al, we have proposed the use a pair of two Lohmann's type I systems in cascade where each spherical lens has been replaced by a non-orthogonal cylindrical doublet [29]. The non-orthogonal cylindrical doublet is equivalent to an orthogonal one, rotated with regard to the coordinate axes. Both the rotation angle and the focal lengths of the equivalent doublet are dependent on the original angle between the cylindrical lenses and on the angle of the doublet as a whole with the coordinate axes.

Despite the great number of encryption systems in both revolution symmetry and anamorphic configuration previously mentioned, to the best of our knowledge nobody has considered the possibility of tilting the lenses as an additional key in the Fourier transformers. It is well known that a slightly tilted spherical lens generates a small amount of astigmatism named as astigmatism by oblique incidence. In this generated conoid of Sturm, the principal meridians of the astigmatic wavefront leaving the tilted spherical lens are aligned with the tangential and the sagittal planes of the lens. This behavior can be extended also to the case of sphero-cylindrical lenses in general where two different cases can be identified. On one hand, when the tilt is applied around one of the principal meridian of the sphero-cylindrical lens, the tangential and the sagittal meridians coincide with the principal meridians, and the rays passing through them will stay at those meridians. In this case, the tilt changes the values of the principal focal lengths but does not change the orientation of the cylinder axis. On the other hand, when the tilt is not applied around a principal meridian, both the focal lengths values as well as the orientation of the cylinder axis change with the tilt angle.

The problem of tilted lenses is treated in optometry with the concept of oblique central refraction (OCR) [30,31]. OCR refers to the case produced when the light passes through the central part of a tilted lens. This situation happens, for instance, when a person looks straight ahead through the optical center of a spectacle lens with either a pantoscopic or a faceform tilt. Both angles refer to tilts along the horizontal and the vertical axis, respectively, in order to accommodate the glasses to the head's patient anatomy to maintain the pupillary distance constant for all the vision directions. Keating [30,31] reported on OCR thin lens third order equations to calculate either the effective sphero-cylindrical parameters of the tilted lens or vice versa: which are the compensated lens parameters in such a way that, when the lens is tilted, the effective sphero-cylindrical parameters match the prescription to be compensated. Note that the latter case is of special significance in optometry because there are many practical situations (sunglasses, sport googles, etc.) where it is necessary to apply this correction. Keating made use of the Coddington equations [32,33] to derive the effective horizontal and vertical dioptric power parameters of the tilted lens using the dioptric power matrix (DPM) formalism introduced by Long [34]. Some years later, Blendowske report on a slightly modification of the Keating's proposed equations based on wavefront tracing and analytical derivation of the equations [35]. And finally Harris reported on a generalization of the Blendowske equation by defining a general tilt matrix valid for tilts about any axis and for any type of lens (stigmatic or astigmatic) [36].

In this paper, we propose to study the performance of encryption systems when the encryption/decryption key is produced by tilting the lenses in Lohmann's type I systems. Although the proposed theory is derived for the general framework of sphero-cylindrical lenses, for the sake of simplicity we have included only spherical examples in the numerical simulations as well as in the experimental implementation. Section 2 presents the basic theory using DPM formalism applied to the change in the DPM of a non-orthogonal cylindrical doublet. Note that the DPM corresponding to a spherical lens derives as a particular case of the previous one. Section 3 includes computer simulation results from a qualitative and quantitative point of view and for different variation of the encryption tilt angle. Section 4 presents an experimental validation of a single encryption/decryption case at the lab using spherical lenses. And Section 5 concludes the paper.

2. MATHEMATICAL GENERAL FRAMEWORK

Let us consider an anamorphic fractional Fourier transformer where a non-orthogonal cylindrical doublet is placed between two parallel planes. If we tilt the anamorphic cylindrical doublet and under third order approximation, the dioptric power of the doublet will change and, as consequence, the fractional orders will also change because of the focal lengths variation.

Keating described the dioptric power variation using DPM formalism from the Coddington equations [30,31]. DPM formalism was introduced by Long [34] and it is a very useful formalism in optometry and physiological optics for a wide variety of calculations such as lens decentration problems and prismatic effects [34], multivariate analysis and changes in refractive status [37,38], intraocular lens power estimations [39] and lateral magnification calculations [40], just to cite a few. Power matrices generalize the dioptric power of any astigmatic surface and become the natural mathematical representation of dioptric power in general [41]. And since we are only to consider changes in the dioptric power, we will describe the tilt effects in the lenses by using the 2X2 DPM formalism [34]. Considering the general case of an astigmatic lens represented by its classical sphero-cylindrical notation of ($S, C \times \theta$), its DPM becomes in:

$$P = \begin{pmatrix} S + C\sin^2\theta & -C\sin\theta\cos\theta \\ -C\sin\theta\cos\theta & S + C\cos^2\theta \end{pmatrix} \quad \textbf{(1)}$$

and the sphere and cylinder values are computed as $S = P_x$ and $C = P_y - P_x$, where P_x and P_y are the dioptric powers along the x- and y-axes, respectively. Finally, the θ-angle represents the angle between the S-meridian and the x-axis.

Equation (1) is the Long's matrix formalism of the dioptric power [34] and the diagonal elements of that matrix are the powers of the lens in the x- and y-axis, respectively. When $S = 0$ and $\theta \neq 0$, Eq. (1) simplifies to the DPM of an in-plane rotated cylindrical lens:

$$P_{cyl} = \begin{pmatrix} C\sin^2\theta & -C\sin\theta\cos\theta \\ -C\sin\theta\cos\theta & C\cos^2\theta \end{pmatrix} \quad \textbf{(2)}$$

Let us consider now a cylindrical doublet composed of two cylindrical lenses being θ_1 and θ_2 the angles of the respective cylinder axes with the x-axis. Note that this is our case in Lohmann's type I systems where θ_2 is not necessarily equal to $\theta_2 = \theta_1 + 90°$. Then, the DPM of the equivalent lens results as the addition of two power matrices according to Eq. (2), that is:

$$P_{cyl} = \begin{pmatrix} C_1\sin^2\theta_1 + C_2\sin^2\theta_2 & \\ -C_1\sin\theta_1\cos\theta_1 - C_2\sin\theta_2\cos\theta_2 & \\ & -C_1\sin\theta_1\cos\theta_1 - C_2\sin\theta_2\cos\theta_2 \\ & C_1\cos^2\theta_1 + C_2\cos^2\theta_2 \end{pmatrix} \quad \textbf{(3)}$$

For determining the parameters of the equivalent lens, one solution is to diagonalize the matrix. From a physical point of view, the eigenvalues λ_1 and λ_2 are the principal powers of the equivalent lens:

$$\begin{pmatrix} S & 0 \\ 0 & S + C \end{pmatrix} = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} \quad \textbf{(4)}$$

Diagonalization process yields in the following characteristic equation:

$$\lambda^2 - \lambda\left(C_1 + C_2\right) + C_1C_2\left(\sin\theta_1\cos\theta_2 - \cos\theta_1\sin\theta_2\right)^2 = 0 \quad \textbf{(5)}$$

and if we call $\theta = \theta_1 - \theta_2$, the solution of Eq. (5) is:

$$\lambda = \frac{\left(C_1 + C_2\right) \pm \left(C_1^2 + C_2^2 + 2C_1C_2\cos 2\theta\right)^{1/2}}{2} \quad \textbf{(6)}$$

The eigenvalues λ_1 and λ_2 are the powers of the virtual orthogonal doublet equivalent to the pair of non-orthogonal cylindrical lenses. And this virtual orthogonal doublet will be rotated an angle φ with respect to the x-axis. Let us call

$$C = \pm\left(C_1^2 + C_2^2 + 2C_1C_2\cos 2\theta\right)^{1/2} \quad \textbf{(7)}$$

If we now take the minus sign, the corresponding eigenvalue is given by:

$$\lambda = \frac{C_1 + C_2 - C}{2}. \quad \textbf{(8)}$$

Taking into account that the corresponding eigenvector can be written as $\begin{pmatrix}\cos\varphi \\ \sin\varphi\end{pmatrix}$, we have:

$$\begin{aligned}&\left(C_1 \sin^2\theta_1 + C_2 \sin^2\theta_2\right)\cos\varphi \\ &-\left(C_1 \sin\theta_1\cos\theta_1 + C_2 \sin\theta_2\cos\theta_2\right)\sin\varphi \\ &= \frac{1}{2}\left(C_1 + C_2 - C\right)\cos\varphi\end{aligned} \quad \textbf{(9)}$$

Finally, the rotation angle of the virtual doublet is

$$\tan\varphi_{(\theta_1\neq 0)} = \frac{C - C_1\cos\left(2\theta_1\right) - C_2\cos\left(2\theta_2\right)}{C_1\sin\left(2\theta_1\right) + C_2\sin\left(2\theta_2\right)} \quad \textbf{(10)}$$

When $\theta_1 = 0$, Eq. (10) reduces to

$$\tan\varphi_{(\theta_1=0)} = \frac{C - C_1 - C_2\cos\left(2\theta_2\right)}{C_2\sin\left(2\theta_2\right)} \quad \textbf{(11)}$$

This is another version of the one obtained by Macukow and Arsenault using ray matrix theory [42].

Another way to determine the resulting orthogonal lens parameters from Eq. (3) is by using the trace (represented by t) and the determinant (represented by d) of the DPM [43]. It can be demonstrated from Eq. (1) that the trace is $t(P) = 2S+C$, that is, is independent of the coordinate system in which is expressed the DPM. Similarly, the determinant becomes $d(P) = S(S+C)$. From these values, it is possible to retrieve the resulting lens in sphero-cylindrical notation as [43]:

$$C = \pm\sqrt{t^2 - 4d} \quad \textbf{(12)}$$

$$S = \frac{t \mp \sqrt{t^2 - 4d}}{2} \quad \textbf{(13)}$$

$$\theta = \arctan\left(\frac{S - a_{11}}{a_{12}}\right) \quad \textbf{(14)}$$

where $a_{11} = S+C\sin^2\theta$ and $a_{12} = -C\sin\theta\cos\theta$.

For the cylindrical doublet represented by Eq. (3), the trace becomes in $t(P_{cyl}) = C_1+C_2$ and the determinant in $d(P_{cyl}) = C_1 C_2 \sin^2\theta$. Thus, we finally get:

$$C = \pm\sqrt{C_1^2 + C_2^2 + 2C_1C_2\cos\left(2\theta\right)} \quad \textbf{(15)}$$

$$S = \frac{\left(C_1 + C_2\right) \mp \sqrt{C_1^2 + C_2^2 + 2C_1C_2\cos\left(2\theta\right)}}{2} \quad \textbf{(16)}$$

Let us consider now that the doublet is titled an angle ζ either faceform or pantoscopic. For a faceform tilt and distant object, we can use the Coddington equations [32, 33] to find the effective horizontal and vertical dioptric powers E_x, E_y of the tilted lens by knowing the lens powers P_x, P_y before the tilt [30,31]:

$$E_x = P_x T_c \quad \textbf{(17)}$$

$$E_y = P_y S_c \quad \textbf{(18)}$$

where:

$$S_c = 1 + \frac{\sin^2\zeta}{2n} = h\left(\zeta\right) \quad \textbf{(19)}$$

$$T_c = \frac{2n + \sin^2\zeta}{2n\cos^2\zeta} = \frac{h\left(\zeta\right)}{\cos^2\zeta} \quad \textbf{(20)}$$

being n the refractive index of the lens. Equations (17-20) are third order approximated equation, so they begin to lose accuracy for high tilt angles ($\zeta \geq 30°$ according to Refs. [30,31]).

Then, the tilted lens has an effective matrix for faceform tilt equal to:

$$E = \begin{pmatrix} E_x & E_t \\ E_t & E_y \end{pmatrix} = \begin{pmatrix} P_x T_c & P_t H_c \\ P_t H_c & P_y S_c \end{pmatrix} \quad \textbf{(21)}$$

where:

$$H_c = \frac{T_c + S_c}{2} = \frac{\left(2n + \sin^2\zeta\right)\left(1 + \cos^2\zeta\right)}{4n\cos^2\zeta} \quad \textbf{(22)}$$

From Eqs. (19), (20) and (22), S_c, T_c, and H_c do not depend on the dioptric power and can be tabulated for n and ζ [30,31]. However and according to Blendowske [35], the off-diagonal elements of the matrix in Eq. (21) should be slightly modified because the value of H_c must be calculated as the geometric mean of S_c and T_c instead of the arithmetic mean, i.e.:

$$H_c = \sqrt{T_c S_c} = \frac{h\left(\zeta\right)}{\cos\zeta} \quad \textbf{(23)}$$

Nevertheless, the numerical difference between both factors for angles up to 30° is so small that is negligible for practical purposes. Accepting the Blendowske modification, the tilted power matrix becomes in:

$$E\left(\zeta\right) = \begin{pmatrix} P_x T_c & P_t H_c \\ P_t H_c & P_y S_c \end{pmatrix} = h\left(\zeta\right)\begin{pmatrix} \dfrac{P_x}{\cos^2\zeta} & \dfrac{P_t}{\cos\zeta} \\ \dfrac{P_t}{\cos\zeta} & P_y \end{pmatrix} \quad \textbf{(24)}$$

Blendowske defined the faceform tilt matrix as:

$$M\left(\zeta\right) = \sqrt{h\left(\zeta\right)}\begin{pmatrix} \sec\zeta & 0 \\ 0 & 1 \end{pmatrix} \quad \textbf{(25)}$$

and the tilted power matrix becomes in:

$$E\left(\zeta\right) = M\left(\zeta\right)P\left(\theta\right)M\left(\zeta\right) \quad \textbf{(26)}$$

Considering that the trace and the determinant of this new matrix are $t(P_{tilt}) = T_C P_x + S_C P_y$ and $d(P_{tilt}) = T_C S_C P_x P_y - (H_C P_t)^2$, respectively, the values resulting from Eqs. (12-14) are:

$$C = \pm\sqrt{T_c P_x + S_c P_y - 4\left(T_c S_c P_x P_y - H_c^2 P_t^2\right)} \quad \textbf{(27)}$$

$$S = \frac{\left(T_c P_x + S_c P_y\right) \mp \sqrt{T_c P_x + S_c P_y - 4\left(T_c S_c P_x P_y - H_c^2 P_t^2\right)}}{2} \quad (28)$$

$$\theta = \tan^{-1}\left(\frac{S - T_c P_x}{H_c P_t}\right) \quad \textbf{(29)}$$

Let us consider an example just to fix some ideas. Suppose a cylindrical doublet composed of one cylindrical lens equal to (0.00, 4.00x0°) combined with another equal to (0.00, 6.00x50°). The resulting power matrix according to Eq. (3) is:

$$P_{cyl} = \begin{pmatrix} P_x & P_t \\ P_t & P_y \end{pmatrix} = \begin{pmatrix} 3.52 & -2.95 \\ -2.95 & 6.48 \end{pmatrix} D \quad \textbf{(30)}$$

being D = diopters. The trace and the determinant are $t(P_{cyl}) = 10D$ and $d(P_{cyl}) = 14.09D^2$. Following Eqs. (27-29): $C = \pm 6.61D$, $S = 1.70D$ or $S = 8.30D$ (depending on the C sign) and $\theta = 31.67°$. Now, we perform a faceform tilt of $\zeta = 24°$. Supposing a refractive index value of the lenses

of $n = 1.5$, we get $T_c = 1.264$, $S_c = 1.055$ and $H_c = 1.155$. From Eq. (24), the effective matrix representing the tilted lens is:

$$E(\zeta = 24^{\circ}) = \begin{pmatrix} 4.45 & -3.41 \\ -3.41 & 6.84 \end{pmatrix} D \qquad \textbf{(31)}$$

Coming back to the sphero-cylindrical notation, the new trace and determinant are $t(E) = 11.29D$ and $d(E) = 18.81D^2$, and the new parameters of the doublet are $C_E = \pm 7.18D$, $S_E = 2.06D$ or $S_E = 9.24D$ (depending on the C_E sign), and $\theta_E = 35.03°$. Notice that, as a result of the faceform tilt, the principal powers of the equivalent lens as well as the cylinder axis have changed from (S, C x θ) = (8.3D, -6.6D x 31.7°) to (S, C x θ) = (9.25D, -7.2D x 35°). This is a significant change caused by the tilt and we need to know the proper key, that is, the new parameters of the tilted lens used in the encryption, for the decryption process. Otherwise we will get a wrong decryption and, consequently, information lost.

A similar procedure can be considered for the pantoscopic tilt. According to Blendowske [35], the pantoscopic tilt matrix is:

$$N(\zeta) = \sqrt{h(\zeta)} \begin{pmatrix} 1 & 0 \\ 0 & \sec\zeta \end{pmatrix} \qquad \textbf{(32)}$$

meaning that the corresponding tilted power matrix can be computed as:

$$E(\zeta) = N(\zeta) P(\theta) N(\zeta) \qquad \textbf{(33)}$$

Both faceform and pantoscopic tilt matrices are particular cases of a general tilt matrix developed by Harris some months later the Blendowske's work [36]. This general tilt matrix $N'(\zeta)$ can be computed as:

$$N'(\zeta, \psi) = \sqrt{h(\zeta)} \left[I + (\sec\zeta - 1) \begin{pmatrix} \sin^2\psi & -\sin\psi\cos\psi \\ -\sin\psi\cos\psi & \cos^2\psi \end{pmatrix} \right] \qquad (34)$$

being I the identity matrix, ζ the tilt angle, and ψ is the angle of the axis where the tilt is performed. For a general description about how this matrix is obtained, the reader can consult Ref. [36]. As it can be easily seen from Eq. (34), $\psi = 90°$ and $\psi = 0°$ retrieve the faceform and the pantoscopic tilt matrices of Eqs. (25) and (32) , respectively.

3. NUMERICAL SIMULATIONS

The performance of tilted lenses as additional key to improve security in encryption/decryption system is analyzed by numerical simulations using Matlab platform. We propose an encryption system based on two Lohmann's type I systems in cascade including spherical lenses as it is depicted through Fig. 1. The use of spherical lenses instead of anamorphic doublets does not restricts the applicability of the proposed approach but it simplifies their use. For this reason, we have performed simulations considering spherical lenses.

The classical encrypted branch can be seen through Fig. 1(a) where the first lens L1 provides a first fractional Fourier transformer plane (FrFTP) of the input object which multiplied at the input plane (IP) by a first random mask (RM1). From IP to FrFTP we apply a numerical propagation algorithm based on angular spectrum approach in a double stage: first a propagation distance of d_1 until L1, multiplication of the complex amplitude distribution by the L1 lens complex transmittance, and d_1 numerical second propagation. The complex amplitude distribution at FrFTP is then multiplied by the second random mask (RM2) and a similar double stage numerical propagation process using a difference distance d_2 and a new lens L2 is applied until the output plane (OP). We are using $d_1 = 150$mm and $d_2 = 200$ as propagation distances, and $f_1 = 300$mm and $f_2 = 500$mm as focal lengths of the lenses L1 and L2, respectively.

This encryption process can be perfectly decrypted and the information about the input object completely retrieved by using the decrypted brand included in Fig. 1(c) and by knowing the previously introduced parameters in the encryption branch. Note that the propagation starts from the OP in reverse sense (negative propagation distances) and the decryption considers complex conjugate functions of the encoding elements (L1, L2, RM1 and RM2). However, a tilt in the lenses L1 and L2 is applied as additional key for encryption (see Fig. 1b) meaning that, even in the case that one knows the encrypted parameters, the decryption process will not properly work due to the tilted angle using in the encryption.

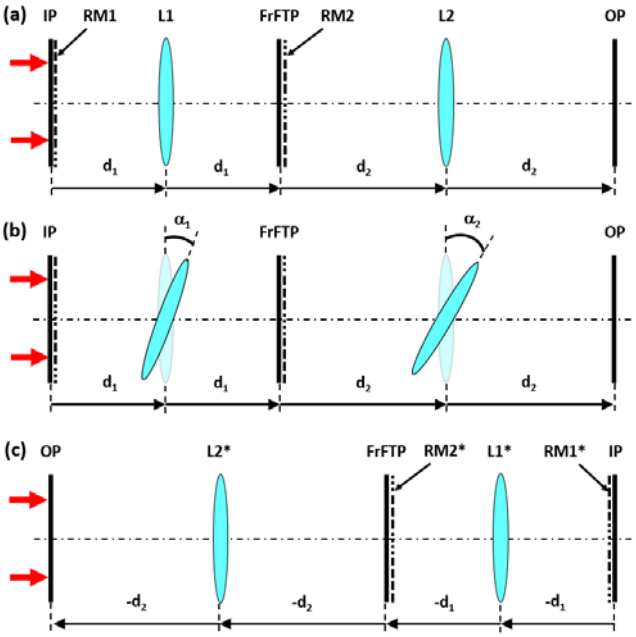


Fig. 1. Scheme of the proposed encryption/decryption process using spherical tilted lenses: (a) is the encryption system with two Lohmann's type I systems in cascade, (b) depicts our proposed implementation where the lenses (L1 and L2) can be tilted α_1 and α_2, respectively, .and (c) the decryption branch without tilted lenses. The rest of the symbols mean: IP (Input Plane), RM1 (Random Mask 1), FrFTP (Fractional Fourier Transform Plane), RM2 (Random Mask 2), OP (Output Plane), and d_1, d_2 are the propagation distances. Red arrows indicate the light path.

Figure 2 includes some numerical results to illustrate the process. As input object (Fig. 2a) we have used a homemade image including a QR code in decreasing size as in a resolution test target. The input object is encrypted by two random masks as the one included in Fig. 2b. The spherical profile of one of the lenses is included in Fig. 2c while a cross-section along the horizontal and vertical black lines is plotted in Fig. 2d. There is no difference in curvature because it is a spherical lens. But applying a faceform tilt of 30°, the phase profile of the lens changes. The new tilted lens becomes in a sphero-cylindrical lens represented in Fig. 2e and in Fig. 2f where now the two cross-sections have different curvature as corresponds to a sphero-cylindrical lens.

To check the performance of the proposed method, we have divided the numerical simulations into three different cases. The first one relates with tilting only the first L1 lens while remaining untilted the second one L2. The encryption is done for 4 different angles (2.5°, 5°, 7.5° and 10°) and, for each encryption angle, the decryption is done

separately for each lens by continuously varying the decoding angle from -15° to 15°. The second case involves a similar procedure than the previous one but for the second lens L2. And the third case is defined by encrypting with the two lenses L1 and L2 simultaneously tilted the same angle (2.5°, 5°, 7.5° and 10°). On all the cases, we present two outputs for analyzing the results: i) the retrieved decrypted images of the input object to qualitatively show how image becomes degraded and information lost for certain interesting points on each configuration, and ii) the decryption sensitivity with respect to the perfect decrypted image which is usually measured by the mean squared error (MSE) between the decrypted and the original images. The MSE is given by:

$$MSE = \frac{1}{MxN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left|I_0(i,j) - I_d(i,j)\right|^2 \qquad (35)$$

where $I_0(i, j)$ denotes the original image, $I_d(i, j)$ the decrypted one, and M and N are the number of pixels along the x- and y-axes, respectively.

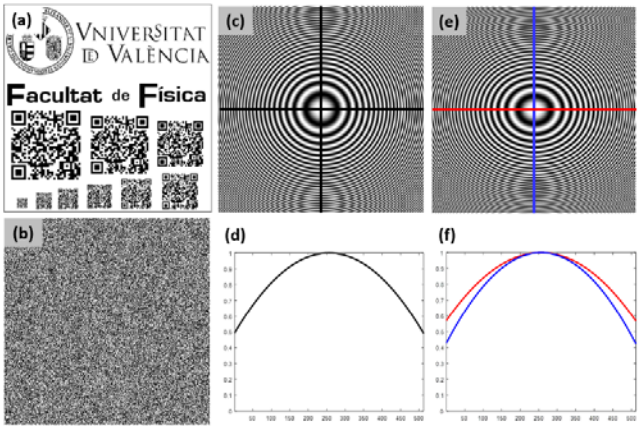


Fig. 2. Some interesting images used in the numerical simulations: (a) the input object, (b) a random mask for the encryption/decryption process, (c) the phase profile of a spherical lens and (d) the plots along its vertical and horizontal meridians (solid black lines), (e) the same lens after a faceform tilt of 30° and (f) the plots along its vertical (solid blue line) and horizontal (solid red line) meridians.

A. Encryption with tilted lens L1

Figure 3 includes the numerical simulation results obtained when the first lens L1 is tilted from 0° to 10° at 2.5° steps. Figure 3a presents the MSE results through two plots for the 5 previously identified tilted cases. The two plots are the normalized MSE profiles when the decryption is performed by varying the decrypted tilted angle of L1 from -15° to +15° (solid black line) and the same but for L2 lens (dashed black line). We can see that a perfect image (MSE = 0) is recovered when the tilted angle of the lens L1 in the decryption process equals the one used for that lens in the encryption (points targeted with × green marks). For those points, the recovered image is exactly the input object (Fig. 2a). Obviously, this is not the case when the angular variation is introduced in the second L2 lens leaving the first L1 lens at 0°.

But what it is interesting to see is which image is recovered when the decryption is performed without tilt the lenses. That is, the encryption is performed with tilted angles and the decryption is performed without knowledge of such encryption key. Those cases are targeted with the × red marks identified by 4 points in Fig. 3a and the decrypted results are presented in the images depicted from Fig. 3b to Fig. 3e. Obviously and as we can see from the first graph in Fig. 3a, when the encryption is performed with 0°/0° at L1/L2, the decryption retrieves a perfect image (MSE = 0). But as the tilted angle of L1 is increased (2.5°/0°, 5°/0°, 7.5°/0° and 10°/0° at L1/L2), the result becomes to be noisier and, for the latest case (10°/0° at L1/L2), only the letters can be read from the retrieved image. Note that although the graphs indicate a value up to 95% of MSE for 5°/0°, 7.5°/0° and 10°/0° at L1/L2, it is a normalized value for each encryption/decryption case and does not mean full information lost. For this reason, the output must be read taking both results (plots and images) into account.

An additional interesting comment is that it is equivalent to perform the tilts at positive than at negative angles. This sentence is extracted by looking at the normalized MSE plot of the first lens L1 and realizing that a perfect reconstruction is retrieved at both sides of the 0° case since there are two symmetrical points of MSE = 0 at the solid black line. This fact makes sense since a spherical lens tilt at positive faceform angle produces the same Sturm interval of astigmatism by oblique incidence than the same tilt on the opposite angular direction.

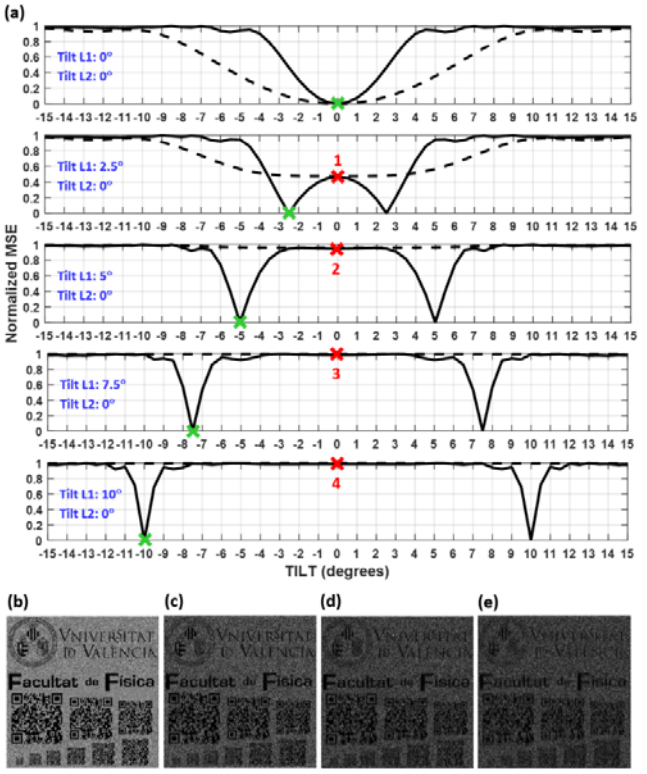


Fig. 3. Numerical results when encrypting in L1 lens. (a) Normalized MSE output when the encryption is at 2.5° steps until 10° and the decryption is separately performed for the lenses L1 (solid black line) and L2 (dashed black line) with a continuous variation from -15° to +15°. (b)-(e) are the retrieved images corresponding with the 1 to 4 red points at the graphs, respectively.

B. Encryption with tilted lens L2

The second case proposes the same procedure previously presented but for the case of tilting the second lens L2 in the system. Results can be seen through Fig. 4 in a parallel manner to Fig. 3. Once again, perfect outputs are retrieved when the tilted angle of L2 equals in modulus the one used in the encryption. Note that by modulus we are referring to the fact (last comment on previous section) regarding the symmetry in the tilts for producing the same Strum interval of astigmatism by oblique incidence. Those cases are identified by ×

green marks at the dashed black line (the normalized MSE plot for the lens L2 in the decryption).

And the resulting images provided when no tilt is considered during the decryption and corresponding with the × red marks are presented through the images included at Figs. 4b-e. Now, we can see that, again, the result becomes to be noisier as the tilted angle of L2 is increased (2.5°/0°, 5°/0°, 7.5°/0° and 10°/0° at L1/L2). And finally the input object information is completely lost: no object structure can be identified from Fig. 3d (0°/7.5° at L1/L2). This case corresponds with a normalized MSE value of 70%.

Regarding the previous results, 70% of normalized MSE in the second lens case destroys much more the spatial object information than 100% of normalized MSE for the same tilted angle but in the first lens L1. This fact means that the encryption system is more sensitive to tilts in the second lens than in the first one.

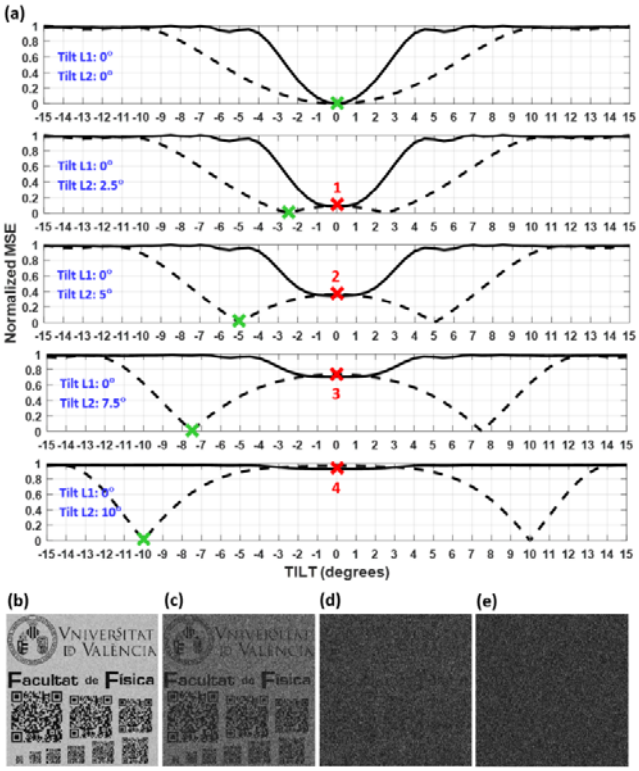


Fig. 4. Numerical results when encrypting in L2 lens. (a) Normalized MSE output when the encryption is at 2.5° steps until 10° and the decryption is separately performed for the lenses L1 (solid black line) and L2 (dashed black line) with a continuous variation from -15° to +15°. (b)-(e) are the retrieved images corresponding with the 1 to 4 red points at the graphs, respectively.

C. Encryption with tilted both lenses L1 and L2

To complete our numerical investigation, Fig. 5 presents here the results provided by the system in which both spherical lenses are tilted the same angle from 0° to 10° at 2.5° steps, that is: 2.5°/2.5°, 5°/5°, 7.5°/7.5° and 10°/10° at L1/L2 according to our nomenclature. Globally, a similar behavior to the first case (encryption with tilted lens L1) is obtained but with even more sensitivity to the encodings since full object information is completely lost at lower tilted angles.

From Fig. 5a we can see as a perfect image (MSE = 0) is no longer recovered at any green mark because, although the tilted angle of the first lens L1 will be known, the tilted angle of the second lens L2 will always destroy the recovered image quality. This fact can be seen through the images included in Figs. 5b-e. Note that these images are exactly the same images included in Figs. 4b-e because we are supposing to decrypt with perfect key for lens L1 (no error in tilted lens L1 or equivalently 0° of tilt) while no information is accessible for the lens L2.

Finally, the retrieved decrypted images in the case where no information about the tilted keys are available are included in Figs. 5f-i. We can see as the spatial information of the input object is complete lost above 5°/5° at L1/L2. This value suggests that tilted lenses as encryption key are useful since small angles do not increase the amount of aberrations in the system while the encrypted information cannot be retrieved.

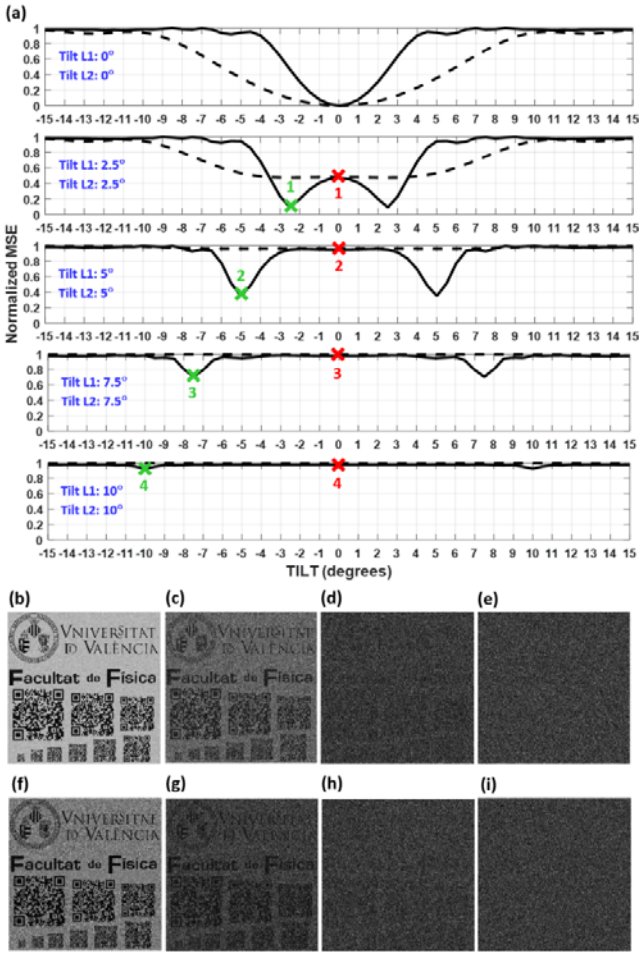


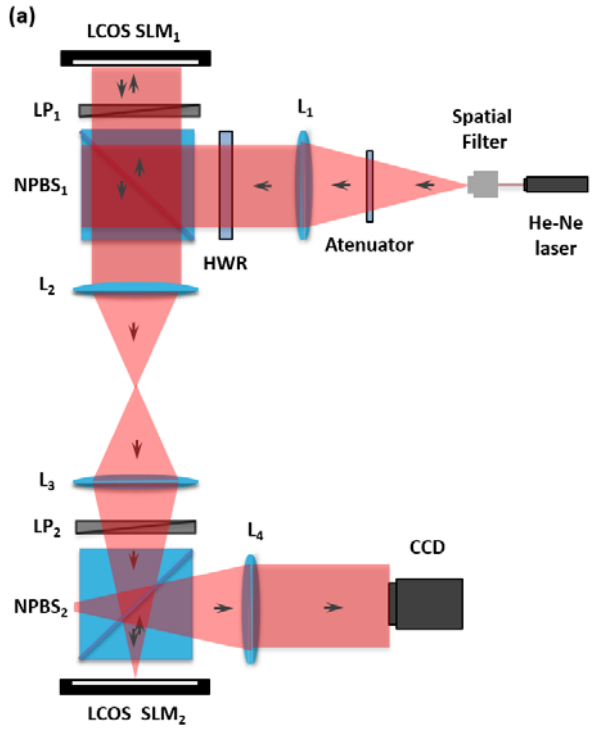
Fig. 5. Numerical results when encrypting in both L!/L2 lenses. (a) Normalized MSE output when the encryption is at 2.5° steps until 10° and the decryption is separately performed for the lenses L1 (solid black line) and L2 (dashed black line) with a continuous variation from -15° to +15°. (b)-(e) and (f)-(i) are the retrieved images corresponding with the 1 to 4 green and red points at the graphs, respectively.

4. EXPERIMENTAL VALIDATION

A preliminary experimental validation of hybrid encryption/decryption process based on tilted lenses is presented in this section. By hybrid we mean that we are providing numerical encryption using tilted lens angles as encryption keys but the decryption process is implemented with an optical experiment at the

lab. However and for the sake of simplicity at the lab, the hybrid experimental validation is implemented using a Fourier transformer scheme instead of the FrFT configuration used in previous section.

For the encryption, we have used an adapted numerical simulator from the previous FrFT script, adapted in the sense of providing image encryption using Fourier transformers. This numerical encrypter employs several approximations that allow a realization of such a complicated experiment: 1) We consider only a Fourier transform system; 2) We use two liquid-crystal displays to introduce the encrypted image and the decryption mask, but we use them as phase-only modulators. Therefore, only the phase of the numerically calculated diffractive elements is useful for the experiment, while the modulus information is discarded. The reason for that drastic approximation is that liquid-crystal displays can operate easily as phase-only spatial light modulators (by aligning the input linear polarization with the liquid crystal director), but they can not display complex valued directly.



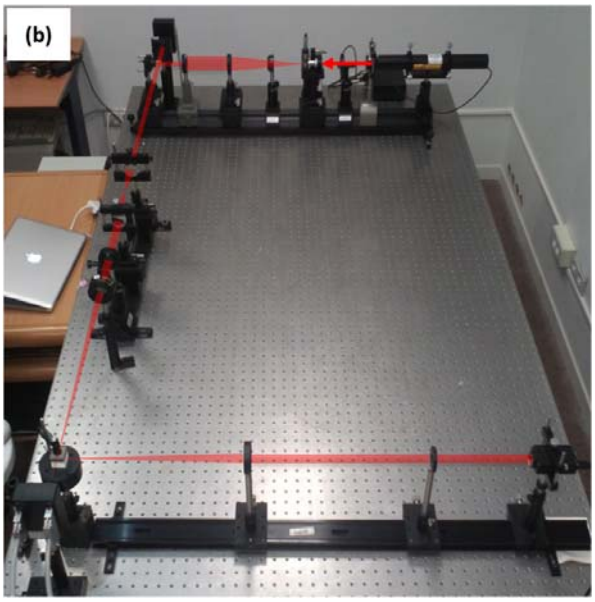


Fig. 6. Experimental demonstrator for decryption of images encrypted by using tilted spherical lenses: (a) scheme of the layout and (b) picture of the experimental layout assembled at the lab (same perspective than the scheme).

Figure 6 shows both a scheme and a picture of the optical system built at the laboratory for decryption. Note that the encryption is done numerically with the same system but in reverse sense. Figure 6 shows a He-Ne laser with a wavelength of 632.8 nm which is spatially filtered and the beam is collimated using a first spherical lens (L_1 at Fig. 6a). We used two liquid crystal on silicon (LCOS) spatial light modulators (SLM) to display two different phase masks: the first one (SLM_1) corresponding to the IP/RM1 plane, and a second one (SLM_2) to display RM2. These are two displays from Hamamatsu, parallel aligned PAL-LCOS-SLM model X10468-01, with 792×600 pixels, 20×20 μm^2 pixel size and video-rate operation (60 Hz). The liquid crystal director is oriented horizontal with respect to the laboratory frame. The devices are programmable linear retarders, where the extraordinary axis is oriented horizontally, therefore producing a phase-only modulation for linearly polarized light oriented in this direction. A half-wave retarder (HWR) is mounted onto a rotatable mount and introduced to control the orientation of the linear polarization of the input light beam. This way we orient the polarization to be parallel to the liquid crystal director of the displays. But, since the beam-splitters may introduce some modification in the state of polarization, two linear polarizers (LP_1 and LP_2) are introduced in order to ensure perfect linearly polarized light impinging the SLMs. The two SLMs produce a phase retardation variation that exceeds 2π radians for the operating wavelength of 633 nm.

Because the SLMs are reflective devices, two non-polarizing beam splitters (NPBS) are included in the optical architecture. The optical Fourier transform relation from SLM_1 to SLM_2 is performed with a combination of two convergent spherical lenses (L_2 and L_3 at Fig. 6a) having the same focal length (100 mm) and separated 215 mm. The distance between SLM_1-L_2 and L_3-SLM_2 is the same and equal to 747 mm. This is very relevant since the success of the decryption process critically depends on the correct matching between the scale of the optical Fourier transform implemented in the system and the digital Fourier transform used to calculate the mask in SLM2. Adjusting the distance between lenses L_2 and L_3 allows varying the focal length of their combination, and therefore changing the scale of the optical

Fourier transform. Finally, another spherical lens L_4 performs another Fourier transform and produces an image of the SLM_1 plane onto the final CCD camera.

As mentioned before, we use this system to experimentally validate a hybrid encryption/decryption process. Regarding this fact, one important aspect to consider is that the SLMs operate as phase-only modulators. Therefore, only the phase content of the encrypted image is displayed (the amplitude distribution is discarded, made it equal to one in all pixels). We selected this option instead of using an additional SLM to implement the amplitude distribution in order to keep the optical system simpler. Nevertheless, the fact that we introduce a random phase pattern (RM1) on the input image reproduces the classical technique employed in computer-generated holography used reduce the impact of the phase-only operation in Fourier transform holograms [44]. However, this introduces an additional complication in the decryption process, especially because adds speckle noise in the reconstructed image.

Thus, the digital process to encode the encrypted image for this experiment consists in the following process which must be read in reverse sense to the layout included at Fig. 6: 1) the initial regular amplitude image (IP) is combined with a random phase pattern (RM1); 2) a numerical propagation until the lens L_4 is digitally performed; 3) the complex field is multiplied by a titled lens L_4; 4) an additional numerical propagation until the SLM_2 plane is performed (note that the IP and the SLM_2 planes are related by a Fourier transform but we have used two numerical propagations to consider the tilt at the lens L_4 for the encryption); 5) the amplitude at the SLM_2 plane is discarded, keeping only the phase distribution; 6) a second random key (RM2) is added to this phase distribution; 7) finally, another digital Fourier transform is performed and the phase distribution of the resulting pattern becomes the encrypted pattern to be displayed on SLM_1 for the decryption process. Thus, only one tilted lens is considered in this hybrid experimental validation of the proposed concept. Note in addition that, as we previously stated, encryption is performed considering the conjugate spatial distributions of the optical elements used in the decryption.

Finally, another practical aspect to consider is related to the fringing effect that affects SLMs [45]. This electronic effect prevents the correct display of phase values when rapid spatial variations are present in the image. In order to minimize this effect, we selected the random phase key RM2 made of macro-pixels, where random phase values were selected in squares of 8x8 pixels filling the complete image.

And then, the decryption process is performed optically. The system in Fig. 6 performs an optical Fourier transform from SLM_1 plane to SLM_2 plane. Thus, SLM_2 is used to display the opposite random key RM2. The final optical Fourier transform produces the retrieved image on the CCD plane. Figure 7 includes the outputs of the optical decryption experiment where the input object is an A letter. We selected this simpler object in comparison with the complex images presented at previous sections due to the difficulty in the experiment. Figure 7a shows the retrieved image when no tilt is used at lens L_4 in the encryption branch. This is the ideal result and we can see as it contains a lot of speckle noise. The speckle noise is generated due to the coherence of the illumination laser light when passing through the optical elements of the layout, and because of the phase-only operation required to display the encrypted image on the SLM_1. Despite the speckle noise, the contour of an A letter can be identified in the reconstruction.

However, no information is available when the encrypted image is numerically generated by considering a tilt of 10° at the lens L4 of the experimental layout. The resulting image is included in Fig. 7b showing as no trace of the A letter is retrieved.

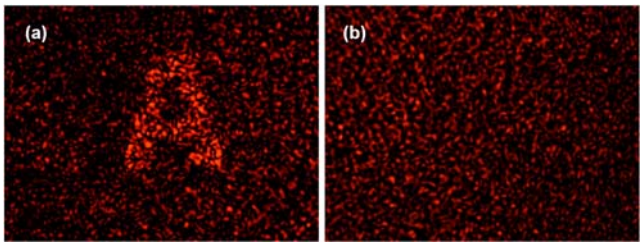


Fig. 7. Experimental results obtained when using numerical encryption with tilted lenses and optical decryption with untilted lenses: (a) the output when no tilt is considered in the encryption process and (b) the output when the encryption is performed with 10° of tilt at L4.

Finally, an additional experiment is performed in order to improve image quality in our approach. We have considered different realizations of the same experiment but changing not the tilted angle key but the encoding masks. Thus, since speckle is mainly generated by those masks, incoherent addition of several reconstruction reduces speckle noise in the retrieved image. Figure 8 includes the experimental results for (a) single realization (same output than in Fig. 7a), (b) 3 realizations, (c) 5 realizations and (d) 10 realizations. The 10 realizations (temporal sequence) are also included in a video movie (Visualization1.mov). It is visible how, as expected, as the number of different realizations that are integrated increases the noise gets significantly reduced and allows a better reproduction of the decrypted image.

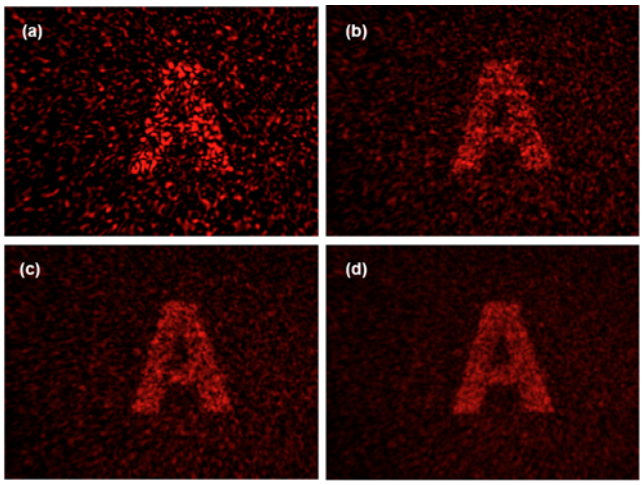


Fig. 8. Experimental images obtained by (a) a single experiment, and when considering the incoherent averaging of (b) 3, (c) 5 and (d) 10 realizations. (Visualization1.avi, 1.1MB).

5. CONCLUSIONS

In this paper we have reported on a novel concept for optical encryption/decryption of object information. The concept is based on the tilt produced in the lenses used in the encryption process. When a lens is tilted, the principal powers and meridians usually change due to the generation of astigmatism by oblique incidence. This fact provides an additional key to perform encoding/decoding and improve security in encryption systems.

The proposed approach is theoretically described using two Lohmann's type I systems in cascade. This mathematical description presents the general frame including any type of sphero-cylindrical lenses and considering how the tilted angle modifies the principal

dioptric powers and meridians. The theory involving these calculations is presented in virtue of the dioptric power matrix formalism and oblique central refraction used in optometry field.

After that, simulation results validate the proposed approach from both qualitative and quantitative points of view. Numerical simulations are presented considering the same two Lohmann's type I systems in cascade but using spherical lenses for the sake of simplicity. These numerical results outcome that almost spatial information of the encrypted object is completely lost with tilts around 5°/5°. This is a modest tilt which highlight a strong sensitivity of the system to the new encryption key.

And finally, a laboratory experiment where decryption is optically performed has also included in the manuscript. The experiment proposes a hybrid method in which the image is encrypted numerically and decrypted optically. For the experimental implementation, we have selected a Fourier transformer configuration to simplify the experimental layout. The experiment shows how decryption is not possible with only 10° of tilt in one of the system lenses. Nevertheless, the process is fully dominated by speckle and the retrieved image contains a strong speckle noise. Such speckle noise can be appreciably reduced by averaging some decryptions, as it has also been demonstrated.

Funding Information. The Spanish Ministerio de Economía y Competitividad and the Fondo Europeo de Desarrollo Regional (FIS2013-47548-P and FIS2015-66328-C3-3-R).

References

1. P. Réfrégier and B. Javidi, "Optical image encryption based on input plane Fourier plane random encoding", Opt. Lett. 20, 767-769 (1995).
2. N. Towghi, B. Javidi, and Z. Luo, "Fully phase encrypted image processor", J. Opt. Soc. Am. A 16, 1915-1927 (1999).
3. E. Tajahuerce, O. Matoba, S. C. Verrall, and B. Javidi, "Optoelectronic information encryption with phase-shifting interferometry", Appl. Opt. 39, 2313-2320 (2000).
4. T. Nomura and B. Javidi, "Optical encryption system with a binary key code", Appl. Opt. 39, 4783-4787 (2000).
5. O. Matoba and B. Javidi, "Encrypted optical storage with wavelength-key and random phase codes", Appl. Opt. 38, 6785-6790 (1999).
6. O. Matoba and B. Javidi, "Encrypted optical storage with angular multiplexing", Appl. Opt. 38, 7289-7293 (1999).
7. X. Tan, O. Matoba, T. Shimura, K. Kuroda, and B. Javidi, "Secure optical storage that uses fully phase encryption", Appl. Opt. 39, 6689-6694 (2000).
8. E. Tajahuerce and B. Javidi, "Encrypting three-dimensional information with digital holography", Appl. Opt. 39, 6595-6601 (2000).
9. T. Nomura and B. Javidi, "Optical encryption using a joint transform correlator architecture", Opt. Eng. 39, 2031-2045 (2000).
10. A. W. Lohmann, "Image rotation, Wigner rotation, and the fractional Fourier transform", J. Opt. Soc. Am. A 10, 2181-2186 (1993).
11. A. W. Lohmann, "A fake zoom lens for fractional Fourier experiments", Opt. Commun. 115, 437-443 (1995).
12. D. Mendlovic and H. M. Ozaktas, "Fractional Fourier transforms and their optical implementation: I", J. Opt. Soc. Am. A 10, 1875-1881 (1993).
13. H. M. Ozaktas and D. Mendlovic, "Fractional Fourier transforms and their optical implementation: II", J. Opt. Soc. Am. A 10, 2522-2531 (1993).
14. H. M. Ozaktas and D. Mendlovic, "Fourier transforms of fractional order and their optical implementation", Opt. Commun. 101, 163-169 (1993).
15. G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption by double random phase encoding in the fractional Fourier domain", Opt. Lett. 25, 887-889 (2000).
16. G. Unnikrishnan and K. Singh, "Double random fractional Fourier-domain encoding for optical security", Opt. Eng. 39, 2853-2859 (2000).
17. Y. Zhang, C-H. Zheng, N. Tanno, "Optical encryption based on iterative fractional Fourier transform", Opt. Commun. 202, 277-285 (2002).
18. Z. Liu and S. Liu, "Double image encryption based on iterative fractional Fourier transform", Opt. Commun. 275, 324-329 (2007).
19. G. Situ and J. Zhang, "Double random-phase encoding in the Fresnel domain", Opt. Lett. 29, 1584-1586 (2004).
20. Q. Wang, Q. Guo, L. Lei, and J. Zhou, "Optical image encryption based on joint fractional transform correlator architecture and digital holography", Opt. Eng. 52¸048201.1-7 (2013)
21. Z. Zhong, J. Chang, M. Shan, and B. Hao, "Fractional Fourier-domain random encoding and pixel scrambling technique for double image encryption", Opt. Commun. 285, 18-23 (2012).
22. Q. Wang, Q. Guo and J Zhou, "Double image encryption based on linear blend operation and random phase encoding in fractional Fourier domain", Opt. Commun. 285, 4317-4323 (2012).
23. D. Mendlovic, Y. Bitran, R. Dorsch, C. Ferreira, J. García, and H. M. Ozaktas, "Anamorphic fractional Fourier transform: optical implementation and applications", Appl. Opt. 34, 7451-7456 (1995).
24. A. Sahin, H. M. Ozaktas, and D. Mendlovic, "Optical implementation of the two-dimensional fractional Fourier transform with different orders in two dimensions", Opt. Commun. 120, 134-138 (1995).
25. J. García, D. Mendlovic, Z. Zalevsky, and A. W. Lohmann, "Space-variant simultaneous detection of several objects by the use of multiple anamorphic fractional Fourier transform filters", Appl. Opt. 35, 3945-3952 (1996).
26. I. Moreno, C. Ferreira, and M. M. Sánchez-López, "Ray matrix analysis of anamorphic fractional Fourier systems", J. Opt.: Pure Appl. Opt. 8, 427-435 (2006).
27. G. Unnikrishnan, J. Joseph, and K. Singh, "Fractional Fourier domain encrypted holographic memory by use of an anamorphic optical system" Appl. Opt. 40, 299-306 (2001).
28. P. Kumar, J. Joseph, and K. Singh, "Double random phase encryption with in-plane rotation of a modified Lohmann's second-type system in the anamorphic fractional Fourier domain", Opt. Eng. 47, 117001.1 –7 (2008).
29. C. Ferreira, V. Micó, P. García-Martínez, I. Moreno, J. García, and Z. Zalevsky, "Anamorphic Lohmann's first type system with a non-orthogonal cylindrical doublet. Application to optical encryption", Asian J. Phys. 24, 1679-1702 (2015).
30. M. P. Keating, "Oblique central refraction in spherocylindrical lenses tilted around an off-axis meridian", Optom. Vis. Science 70, 785-791 (1993).
31. M. P. Keating, "Oblique central refraction in spherocylindrical corrections with both faceform and pantoscopic tilt," Optom. Vis. Science 72, 258-265 (1995).
32. F. A. Jenkins and H. E. White, Fundamental of Optics, McGraw-Hill, New York (1950).
33. R. Kingslake, "Who discovered Coddington's equations?", Opt. Photon. News 5, 20-23 (1994).
34. W. T. Long, "A matrix formalism for decentration problems", Am. J. Optom. Physiol. Opt., 53, 27-33 (1976).
35. R. Blendowske, "Oblique central refraction in tilted sphero-cylindrical lenses", Optom. Vis. Sci. 79, 68-73 (2002).
36. W. F. Harris, "Tilted power of thin lenses", Optom. Vis. Sci. 79, 512-515 (2002).
37. W. F. Harris and O. J. Malan, "Trajectories of changing refractive status", Optom. Vis. Sci. 69, 959-965 (1992)
38. S. B. Kaye and W. F. Harris, "Analyzing refractive data", Cataract. Refract. Surg. 28, 2109-2116,(2002)

39. G. E. MacKenzie and W. F. Harris, “Determining the power of a thin toric intraocular lens in an astigmatic eye”, Optom. Vis. Sci. 79, 667–671 (2002)
40. M. Espinos and V. Mico, “Lateral magnification matrix from the dioptric power matrix formalism in the paraxial case”, Ophthalmic Physiol. Opt. 33, 467-481 (2013).
41. W. F. Harris, “Dioptric power: its nature and its representation in three and four- dimensional space”, Optom. Vis. Sci. 74, 349-366 (1997)
42. B. Macukow and H. H. Arsenault, “Matrix decompositions for nonsysmmetrical optical systems”, J. Opt. Soc. Am. 73, 1360-1366 (1983).
43. M. P. Keating, “An easier method to obtain the sphere, cylinder, and axis from an off-axis dioptric power matrix,” Am J. Optom. Physiol. Opt. 57, 734-737 (1980).
44. J. A. Davis, S. W. Flowers, D. M. Cottrell and R. A. Lilly, “Smoothing of the edge-enhanced impulse response from binary phase-only filters using random binary patterns,” Appl. Opt. 28, 2987–2988 (1989).
45. C. Lingel, T. Haist, and W. Osten, “Optimizing the diffraction efficiency of SLM-based holography with respect to the fringing field effect,” Appl. Opt. 52, 6877–6883 (2013).