(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 January 2006 (05.01.2006)

PCT

(10) International Publication Number
WO 2006/001012 A2

(51) International Patent Classification:
G06F 17/10 (2006.01)

(21) International Application Number:
PCT/IL2005/000675

(22) International Filing Date: 23 June 2005 (23.06.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/582,439 25 June 2004 (25.06.2004) US

(71) Applicant *(for all designated States except US)*: **TECHNION RESEARCH AND DEVELOPMENT FOUNDATION LTD.** [IL/IL]; Senatae Building, Technion City, 32000 Haifa (IL).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **HASMAN, Erez** [IL/IL]; 6/2 Haeshed street, 38493 Hadera (IL). **BINNER, Gabriel** [IL/IL]; 1 Sitvanit street, 71401 Lod (IL). **NIV, Avi** [IL/IL]; Kibbutz Kfar Bloom, 12150 M.P. Upper Galilee (IL).

(74) Agent: **MILLER - SIERADZKI, ADVOCATES & PATENT ATTORNEYS**; P.O.B. 6145, 31061 Haifa (IL).

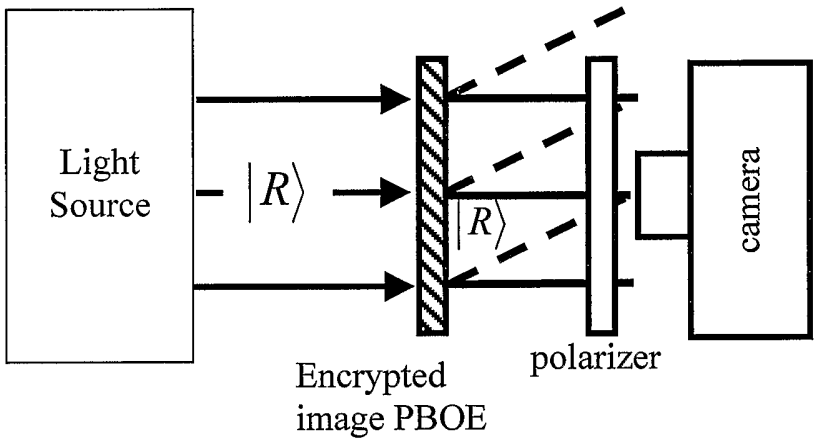
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: GEOMETRICAL PHASE DATA ENCRYPTION AND DECRYPTION



(57) Abstract: A method and device for encryption and decryption of an input data. The encryption method comprises producing carrier for the data in the form of a space-variant subwavelength grating element, with local gratings having angles of orientation corresponding to the data.

WO 2006/001012 A2

GEOMETRICAL PHASE DATA ENCRYPTION AND DECRYPTION

FIELD OF THE INVENTION

The present invention relates to encryption. More particularly it relates to optical encryption method and device based on geometrical phase, which is originated from polarization manipulation. A space-variant subwavelength grating element is used as a carrier of the encrypted information.

BACKGROUND OF THE INVENTION

In the past few years there has been increased interest in data security and a need for improved methods for encrypting data. The increasing demands for better and faster security devices are results of the enormous interest in communication through the net, especially of unauthorized users and commercial spies. One of the processes that has been extensively investigated is the optical encryption technique. Several advantages of optical encryption over conventional digital encryption include real time encryption, high space-bandwidth product, difficulty in unauthorized decryption, portability and the possibility of using biometrics. Different optical encryption schemes have been suggested, for example schemes involving pure amplitude image encryption (see P. Refregier and B. Javidi, Opt. Lett. **20**, 767 (1995)). Other encryption schemes involving phase-only images were explored to improve the decrypted image's visibility (see N. Towghi, B. Javidi and Z. Luo, J. Opt. Soc. Am. A **16**, 1915 (1999)). Both methods use double-random phase encryption, first presented by Refregier and Javidi. The two methods record the complex field information by interference, and thus are unstable and cumbersome. Mogensen and Gluckstad proposed polarization encryption using spatially modulated retardation (P. C. Mogensen and J. Gluckstad, Opt. Commun. **173**, 177 (2000)), while Unnikrishnan et al., proposed polarization encryption using spatially modulated azimuthal angle (G. Unnikrishnan, M. Pohit and K. Singh, Opt. Commun. **185**, 25 (2000)). Polarization encryption provides additional flexibility in the key encryption design by adding a polarization state manipulation to the conventional phase and amplitude manipulation used in the former methods. This feature is advantageous as it makes the polarization encryption method more secure.

In this specification, we propose an approach for polarization encryption using geometrical phase modification. Geometrical phases originate from polarization state manipulation, as anticipated by Pancharatnam (1956) and Berry (1984). Recently, we demonstrated the formation of complex polarization state manipulation by using computer-generated space-variant subwavelength dielectric gratings (A. Niv, G. Biener, V. Kleiner and E. Hasman, Opt. Lett. **29**, 238 (2004)). We have also shown that such polarization state manipulations inevitably lead to a phase modification of geometrical origin, which is a manifestation of the geometrical Pancharatnam-Berry phase (E. Hasman, V. Kleiner, G. Biener and A. Niv, Appl. Phys. Lett. **82**, 328 (2003)). Optical elements which use this effect to form a desired phase front are called Pancharatnam-Berry phase optical elements (PBOEs).

BRIEF DESCRIPTION OF THE INVENTION

There is thus provided, in accordance with some preferred embodiments of the present invention, a method for encryption of an input data, the method comprising: producing carrier for the data in the form of a space-variant subwavelength grating element, with local gratings having angles of orientation corresponding to the data.

Furthermore, in accordance with some preferred embodiments of the present invention, the method further comprises:

illuminating the carrier by a polarized incident beam;

polarizing an emerging beam by a polarizer to obtain at least three images of the emerging beam acquired under different polarizer orientations;

analyzing said at least three images to obtain a geometrical phase corresponding to the data.

Furthermore, in accordance with some preferred embodiments of the present invention, the method further comprises applying a key function on the input data to obtain the data to be carried by the carrier, and after analyzing the images based on knowledge of the key function retrieving the input data.

Furthermore, in accordance with some preferred embodiments of the present invention, the different polarizer orientations comprise two orthogonal orientations and one intermediate orientation.

Furthermore, in accordance with some preferred embodiments of the present invention, the method further comprises applying a key function on the input data to obtain the data to be carried by the carrier.

Furthermore, in accordance with some preferred embodiments of the present invention, the method further comprises:

illuminating the carrier by an incident beam;

polarizing an emerging beam by a polarizer to obtain at least three images of the emerging beam acquired under different polarizer orientations; and

using said at least three images as carriers of the data.

Furthermore, in accordance with some preferred embodiments of the present invention, the method further comprises:

simulating illumination of the carrier by an incident beam and simulating polarization of an emerging beam to obtain at least three images of the emerging beam acquired under different polarization orientations; and

using said at least three images as carriers of the data data.

Furthermore, in accordance with some preferred embodiments of the present invention, said at least three images are watermarked.

Furthermore, in accordance with some preferred embodiments of the present invention, the method further comprises:

illuminating the carrier by a polarized incident beam;

polarizing an emerging beam by a polarizer to obtain two pairs of images of the emerging beam, each pair acquired using different polarization states of the incident beam, and each image of the pairs acquired under different orientations of the polarizer; and

analyzing said two pairs of images to obtain a geometrical phase corresponding to the encrypted data.

Furthermore, in accordance with some preferred embodiments of the present invention, there is provided a device for carrying encrypted data, the device comprising a space-variant subwavelength grating element, with local gratings having angles of orientation corresponding to the encrypted data.

Furthermore, in accordance with some preferred embodiments of the present invention, the element is reflective.

Furthermore, in accordance with some preferred embodiments of the present invention, the element is transmissive.

Furthermore, in accordance with some preferred embodiments of the present invention, the gratings are made of dielectric material.

Furthermore, in accordance with some preferred embodiments of the present invention, the gratings are made of metallic material.

Furthermore, in accordance with some preferred embodiments of the present invention, there is provided a decrypting apparatus for decrypting encrypted data carried by a space-variant subwavelength grating element, with local gratings having angles of orientation corresponding to the encrypted data, the apparatus comprising:

a light source for providing a light beam to illuminate the grating element;

at least one polarizer for polarzing an emerging beam from the grating element in at different polarizer orientations;

an imaging device for acquiring images acquired under different polarizer orientations of the emerging beam.

BRIEF DESCRIPTION OF THE DRAWINGS

In order to better understand the present invention, and appreciate its practical applications, the following Figures are provided and referenced hereafter. It should be noted that the Figures are given as examples only and in no way limit the scope of the invention. Like components are denoted by like reference numerals.

Figure 1a is an exemplary decryption arrangement, in accordance with a preferred embodiment of the present invention.

Figure 1b is an example of an input data, in the form of an image to be encrypted.

Figure 1 c illustrates the representation of the image of Fig. 1b after it was subjected to a secured key funcition.

Figure 1d depicts an example of a space-variant subwavelength grating element, made according to a preferred embodiment of the present invention, based on the encrypted input information of the image shown Fig. 1c.

Figure 1e depicts the space-variant polarization direction emerging from a space-variant subwavelength grating element.

Figures 2a, 2b and 2c show three intensity pictures obtained by three different orientations of a polarizer used in a computerized simulation of the method of the present invention.

Figures 3a, 3b and 3c show watermarked intensity pictures for three polarization orientations 0°, 45° and 90° respectively.

Figure 3d shows a properly decrypted image when using the watermarked images in the decryption process with the correct geometrical phase key.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

Geometrical phase encryption can be optically realized by using a PBOE, which results in a robust and stable element that can be achieved using a single lithographic process. Therefore, this method is suitable for chip integration and can also be applied to personal security cards, e.g., credit cards or identification cards, without limiting other possible uses. Geometrical phase encryption can also be implemented digitally, by computerized simulation. An important advantage of the digital implementation is the ability to use watermarking. The watermarking process is discussed later in this specification.

In order to encrypt a primary input data, for example an image, we propose forming a PBOE that encodes the image intensity subjected to a secured key function. The PBOE, which is a space-variant rotating wave plate, imprints the image intensity plus the key function in the local orientations of the wave plate's fast axes. The result is a space-variant subwavelength grating element (PBOE), with local gratings having angles of orientation corresponding to the encrypted data. Consider Fig. 1c, which depicts an example of a space-variant subwavelength grating element, whose grating orientations (shown in Fig. 1d) represent the encrypted information on the element.

It is noted that although the example discussed in this specification is an image, other forms of input data can be also subjected to the encryption method suggested herein. The input data can be a matrix of any number dimensions, a string,

or other form of information arrangement. The information may be discrete or continuous.

The secured key function itself may be any key function that is acceptable by the user of the encryption method suggested herein, and in fact the present invention may also be implemented without using a secured key function. In the latter case it must be understood that the carrier (the PBOE) will be carrying information that can be recognized immediately in the decryption process, without having to be subjected to the corresponding secured key decryption. This means that the encryption of the input information is only subjected to medium change by way of transforming into geometrical phases on the PBOE, and once the geometrical phases of the PBOE are retrieved the in the decryption process the holder of this retrieved information will have the input data at his disposal.

The PBOE may be reflective, so that incident light illuminated on it emerges on the same side of the incident light source, or it may be transmissive, so that incident light illuminated on it emerges from the other side of the element.

Decryption is performed by illuminating the encrypted PBOE with a circularly polarized light from a light source and retrieving the primary image by analyzing the emerging Stokes parameters with the correct key, as shown in Fig 1(a).

PBOEs are considered to be wave plates with constant retardation and space varying fast axes, the orientation of which is denoted by $\theta(x,y)$. It is convenient to describe PBOEs by using Jones calculus. We find the space-dependent transmission matrix for the PBOE, $\mathbf{T}_C$, by applying the optical rotator matrix, $\mathbf{R}(\theta(x,y))$, to the Jones matrix of a wave plate, $\mathbf{W}$, i.e., $\mathbf{T}_C=\mathbf{R}^{-1}[\theta(x,y)]\mathbf{W}\mathbf{R}[\theta(x,y)]$. By transforming the space-dependent transmission matrix to the helical bases using the helical transformation matrix $\mathbf{U}$, in which $\mathbf{T}=\mathbf{U}^{-1}\mathbf{T}_C\mathbf{U}$, we obtain the expression

$$\mathbf{T}(x,y)=\frac{t_x+t_y\exp(i\phi)}{2}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}+\frac{t_x-t_y\exp(i\phi)}{2}\begin{pmatrix}0 & \exp[i2\theta(x,y)]\\ \exp[-i2\theta(x,y)] & 0\end{pmatrix}, \quad (1)$$

where $\mathbf{T}$ is the space-variant transmission matrix in the helical bases, t_x and t_y are the real amplitude transmission coefficients for the light polarized perpendicular and parallel to the optical axes, respectively, and ϕ is the retardation of the wave plate. Thus, for an incident wave with right hand circular polarization and unknown

distributed complex amplitude, that follows the paraxial approximation, we find that the resulting field is

$$|\mathbf{E}_{out}\rangle = \eta_R|\mathbf{R}\rangle + \eta_L \exp[-i2\theta(x,y)]|\mathbf{L}\rangle, \qquad (2)$$

where $\eta_R = [t_x + t_y \exp(i\phi)]/2$ and $\eta_L = [t_x - t_y \exp(i\phi)]/2$ are the complex field coefficients, and $|\mathbf{R}\rangle = (1 \quad 0)^T$ and $|\mathbf{L}\rangle = (0 \quad 1)^T$ represent the right and left hand circularly polarized components in the helical basis respectively. From Eq. (2) we see that the emerging beam from a PBOE comprises two polarization orders. The first maintains the original polarization state and phase of the incident beam, and the latter is left hand circularly polarized and has the phase modification of $-2\theta(x,y)$. The phase modification of the $|\mathbf{L}\rangle$ polarization order originates solely from the local changes in the polarization state of the emerging beam, and is therefore, geometrical in nature. [5-8]

Let us assume that a PBOE with a space-varying wave plate orientation function of $\theta_i(x,y)$ encodes the primary image of young Einstein, depicted in Fig. 1b. The relationship between the primary image intensity I and θ_i is assumed to be $\theta_i = aI(x,y)$, where a is a constant. In order to further encrypt the encoded primary image information embedded in the PBOE, we add a random rotation function, $\theta_k(x,y)$, to the space-varying wave plates' orientation. This random rotation factor serves as an encryption/decryption key. The total orientation function of the wave plates, comprising the encrypted PBOE, is shown in grayscale in Fig. 1c. In order to decrypt the primary image, we first illuminate the PBOE with $|\mathbf{R}\rangle$ polarized light. The beam emerging from the PBOE is a vectorial interference between two different polarized beams, as can be seen from Eq. (2). The geometrical phase added to the $|\mathbf{L}\rangle$ polarized beam equals $-(\varphi_i + \varphi_k)$, where $\varphi_i = 2\theta_i$ and $\varphi_k = 2\theta_k$ denote the geometrical phase added by the encoded primary image intensity and the encoded key respectively. Figure 1e depicts the space-variant polarization direction emerging from a PBOE with optical parameters of $t_x = t_y = 1$ and $\phi = \pi/2$. The emerging field, which is a result of the vectorial self-interference, is a space varying polarized field. As can be seen, the orientation of the arrows is random. The geometrical phase key, φ_k,

scrambles the space-variant polarization state of the beam and thus randomizes the geometrical phase encoding the primary image, φ_i. In order to retrieve the primary image's geometrical phase we need to measure the Stokes parameters of the beam emerging from the PBOE. The Stokes parameters of a fully polarized light (S_0-S_3) are calculated from three intensity measurements. These measurements are taken when the transmitted light is passed through a polarizer with its axis oriented at 0° ($I_{0,0}$), 45° ($I_{45,0}$) and 90° ($I_{90,0}$). A camera is used to capture the intensity pictures. The relations between the Stokes parameters and the measured intensities are, $S_0 = I_{0,0} + I_{90,0}$;

$S_1 = I_{0,0} - I_{90,0}$; $S_2 = 2I_{45,0} - S_0$, where $S_0 = \left|\langle \mathbf{E}_{out} | \mathbf{R} \rangle\right|^2 + \left|\langle \mathbf{E}_{out} | \mathbf{L} \rangle\right|^2$,

$S_1 = 2\,\mathrm{Re}\left\{\langle \mathbf{E}_{out} | \mathbf{R} \rangle \langle \mathbf{L} | \mathbf{E}_{out} \rangle\right\}$ and $S_2 = 2\,\mathrm{Im}\left\{\langle \mathbf{E}_{out} | \mathbf{R} \rangle \langle \mathbf{L} | \mathbf{E}_{out} \rangle\right\}$, Re{} and Im{} denote the real and imaginary parts of the expression inside the curl brackets and $\langle \alpha | \beta \rangle$ denotes the inner product. By using the Stokes parameters calculated above and by applying the geometrical phase key, we can retrieve the phase function (φ_i) of the primary image, such that

$$\varphi_i = \arctan(S_2/S_1) - \arg\left\{\eta_E \eta_L^*\right\} - \varphi_k, \qquad (3)$$

where arg{} denotes the argument of the expression in the curl brackets, and * denotes the complex conjugate. Since the emerging beam is fully polarized, the fourth Stokes parameter, S_3, is not required.

For the realization of the optical concept, we can implement a method, recently demonstrated for space variant polarization–state manipulations using computer-generated subwavelength structures.[7,8] When the period of a subwavelength periodic structure is smaller than the incident wavelength, only the zeroth order is a propagating order, and all other orders are evanescent. The subwavelength grating behaves as a uniaxial crystal with the optical axes parallel and perpendicular to the subwavelength grooves. Therefore, by fabricating locally periodic subwavelength structures for which the orientation of the subwavelength grooves is space varying, we achieve spatially rotating wave plates. The realization procedure of the PBOE involves the fabrication of a computer-generated space-variant subwavelength-grating mask. Figure 1(d) is a magnified illustration of the subwavelength grating mask of the encrypted element.

In order to test the concept, we used a computer simulation. For the encryption process we simulated a PBOE, encrypting the primary image intensity depicted in Fig. 1(b). The PBOE used has the birefringent parameters of $t_x=t_y=1$ and $\phi=\pi/2$. In order to decrypt the primary image, we illuminated the simulated encrypted element with a right circularly polarized light. Afterwards, we calculated the intensity pictures behind a simulated polarizer in the three orientations (0°, 45° and 90°). Figures 2(a)-2(c) show the three intensity pictures obtained by the three different orientations of the simulated polarizer. The three intensity pictures can be achieved optically using the realized PBOE, a polarizer and a CCD (see Fig. 1(a)). The decrypted image shown in Fig. 2(d) is attained by calculating the Stokes parameters when applying the simulated intensities, and by using Eq. (3), when applying the correct geometrical phase key, φ_k. A case in which the wrong key is used the decrypted image would result in white noise, without the possibility of reconstructing the original image.

An alternative method for geometrical phase encryption makes use of digital implementation. In order to encrypt the information using this method, we need to calculate the three intensity pictures achieved by transmitting the beam, emerging from the digital PBOE through a digital polarizer, oriented in three different angles. These three intensity pictures are then sent via an optical communication net to an authorized receiver possessing the correct key. The authorized receiver is able to decrypt the primary image by calculating the Stokes parameters from the three intensity pictures and inserting these values into Eq. (3), along with the correct key.

A great advantage of the digital implementation approach is the possibility of using watermarking. The watermarking procedure is achieved by adding a false image (as a deception) to the intensity pictures generated by the encryption process, such that $I_{0,0}^{WM}=I_{0,0}+I_{WMP}$, $I_{45,0}^{WM}=I_{45,0}+I_{WMP}$ and $I_{90,0}^{WM}=I_{90,0}+I_{WMP}$, where I_{WMP} symbolizes the watermark picture and $I_{0,0}^{WM}$, $I_{45,0}^{WM}$ and $I_{90,0}^{WM}$ symbolize the watermarked intensity pictures. Although the watermark picture has little effect on the decryption process, it can be used to mislead unauthorized receivers. Figures 3(a)-3(c) show the watermarked intensity pictures for the three polarization orientations 0°, 45° and 90° respectively, while Fig. 3(d) shows the properly decrypted image when

using the watermarked intensities in the decryption process with the correct geometrical phase key.

We further propose an alternative decryption variation of the present invention, which is analyzed using Mueller formalism, where four different intensity measurements are required. The advantage of the later method is that the birefringent parameters of the encrypted elements are not required, thus the method is insensitive to spatial fabrication errors and can be used with incoherent, polychromatic and, unpolarized illumination. These two methods use digital key when decrypting an image.

An other approach for discribing a subwavelength grating is the Stokes-Mueller fomalism approach. In this representation, a uniform wave plate where the fast axis is oriented along the y-axis can be described by a 4*x*4 matrix known as the Mueller matrix,

$$\mathbf{W}=\frac{1}{2}\begin{pmatrix} t_x^2+t_y^2 & t_x^2-t_y^2 & 0 & 0 \\ t_x^2-t_y^2 & t_x^2+t_y^2 & 0 & 0 \\ 0 & 0 & 2t_xt_y\cos\phi & -2t_xt_y\sin\phi \\ 0 & 0 & 2t_xt_y\sin\phi & 2t_xt_y\cos\phi \end{pmatrix}, \tag{1}$$

where t_x, t_y are the real amplitude transmission coefficients for light polarized perpendicular and parallel to the optical axes and ϕ is the retardation of the wave plate. If the orientation of the wave plate is space-varying, i.e. different at each location, then the space-variant wave plates can be described by the space-dependent matrix,

$$\mathbf{M}(x,y)=\mathbf{R}(\theta(x,y))\mathbf{W}\mathbf{R}^{-1}(\theta(x,y)), \tag{2}$$

$$\mathbf{R}(\theta)=\begin{pmatrix}1 & 0 & 0 & 0\\ 0 & \cos 2\theta & \sin 2\theta & 0\\ 0 & -\sin 2\theta & \cos 2\theta & 0\\ 0 & 0 & 0 & 1\end{pmatrix},$$

is the Mueller rotation matrix. Explicit calculation of $\mathbf{M}(x,y)$ yields,

$$\mathbf{M}(\theta)=\begin{pmatrix}|A|^2+|B|^2 & 2\mathrm{Re}\{AB^*\}\cos 2\theta & 2\mathrm{Re}\{AB^*\}\sin 2\theta & 0\\ 2\mathrm{Re}\{AB^*\}\cos 2\theta & |A|^2+|B|^2\cos 4\theta & |B|^2\sin 4\theta & 2\mathrm{Im}\{AB^*\}\sin 2\theta\\ 2\mathrm{Re}\{AB^*\}\cos 2\theta & |B|^2\sin 4\theta & |A|^2-|B|^2\cos 4\theta & -2\mathrm{Re}\{AB^*\}\cos 2\theta\\ 0 & -2\mathrm{Im}\{AB^*\}\sin 2\theta & 2\mathrm{Im}\{AB^*\}\cos 2\theta & |A|^2-|B|^2\end{pmatrix}, \quad (3)$$

where $A=(t_x+t_y exp\phi)/2$ and $B=(t_x-t_y exp\phi)/2$ and Re{} and Im{} denote the real and imaginary parts of the expression inside the curl brackets.

In order to decrypt the primary image, we need to measure the space-variant subwavelength groove orientation, $\theta_i+\theta_k$. As can be seen from Eq. (3) the groove orientation is found by dividing the SWG Mueller matrix members $-m_{42}$ by m_{43}, which result in,

$$\frac{-m_{42}}{m_{43}}=\frac{\mathrm{Im}\{AB^*\}\sin 2\theta}{\mathrm{Im}\{AB^*\}\cos 2\theta}=\tan 2\theta. \quad (4)$$

We note that the imaginary parts written within the two matrix members are canceled when dividing these two members, as can be seen in Eq. (4). This result indicates that the extracted space-variant subwavelength orientation function does not depend on the subwavelength grating parameter values. Thus, the decryption method is insensitive to spatial fabrication non-uniformities. An other conclusion results from the cancellation of the subwavelength grating parameter values is that the decryption process can be implemented in an incoherent, quasi-monochromatic, and unpolarized source. While t_x, t_y and ϕ is process dependent θ is very accurate and does not depend on the process

nor on the illumination, and thus, by extracting θ without the influence of t_x, t_y and ϕ, makes the decryption process more simple and accurate.

By extracting $\theta_i + \theta_k$ and applying the correct key we can retrieve the primary image, thus,

$$\theta_i = \frac{1}{2}\arctan\left(\frac{-m_{42}}{m_{43}}\right) - \theta_k . \tag{5}$$

The measurement of the Mueller matrix members m_{42} and m_{43} is done by illuminating the SWG with two differently polarized beams, for m_{42} we will illuminate with horizontally linear polarized beam and for m_{43} we will illuminate the SWG with 45° oriented linearly polarized beam. In both cases the intensities are measured using a circular analyzer, which is composed of a QWP oriented at 0° and a polarizer oriented at 45° and –45°, for the transmitted $|\mathbf{R}\rangle$ and $|\mathbf{L}\rangle$ polarization state, respectively. The intensities resulting from the circular analyzer with a polarizer oriented at 45°(-45°) are denoted by $I_{45}^{\alpha}(I_{-45}^{\alpha})$, were α equals 0° or 45° for horizontally or 45° oriented linear polarized illumination respectively. Explicitly the connection between the measured intensities and the relevant Mueller matrix elements is given by,

$$\begin{aligned} m_{42} &= I_{-45}^{0} - I_{45}^{0} \\ m_{43} &= I_{45}^{45} - I_{-45}^{45} \end{aligned} \tag{6}$$

To conclude, we have introduced an approach for geometrical phase encryption using spatial polarization state manipulation. Our method can be realized using space-variant subwavelength gratings, thereby making it suitable for personal security cards, or implemented solely in a digital environment thus enabling the additional feature of watermarking. Alternatively, the present invention may be realized in computerized simulation.

It should be clear that the description of the embodiments and attached Figures set forth in this specification serves only for a better understanding of the invention, without limiting its scope.

It should also be clear that a person skilled in the art, after reading the present specification could make adjustments or amendments to the attached Figures and above described embodiments that would still be covered by the present invention.

CLAIMS

1. A method for encryption of an input data, the method comprising:
producing carrier for the data in the form of a space-variant subwavelength grating element, with local gratings having angles of orientation corresponding to the data.

2. The method of claim 1, further comprising:
illuminating the carrier by a polarized incident beam;
polarizing an emerging beam by a polarizer to obtain at least three images of the emerging beam acquired under different polarizer orientations;
analyzing said at least three images to obtain a geometrical phase corresponding to the data.

3. The method of claim 2, further comprising applying a key function on the input data to obtain the data to be carried by the carrier, and after analyzing the images based on knowledge of the key function retrieving the input data.

4. The method of claim 2, wherein the different polarizer orientations comprise two orthogonal orientations and one intermediate orientation.

5. The method of claim 1, further comprising applying a key function on the input data to obtain the data to be carried by the carrier.

6. The method of claim 1, further comprising:
illuminating the carrier by an incident beam;
polarizing an emerging beam by a polarizer to obtain at least three images of the emerging beam acquired under different polarizer orientations; and
using said at least three images as carriers of the data.

7. The method of claim 6, wherein the different polarization orientations comprise two orthogonal orientations and one intermediate orientation.

8. The method of claim 1, further comprising:
simulating illumination of the carrier by an incident beam and simulating polarization of an emerging beam to obtain at least three images of the emerging beam acquired under different polarization orientations; and
using said at least three images as carriers of the data data.

9. The method of claim 8, wherein the different polarization orientations comprise two orthogonal orientations and one intermediate orientation.

10. The method of claim 9, wherein said at least three images are watermarked.

11. The method of claim 1, further comprising:

illuminating the carrier by a polarized incident beam;

polarizing an emerging beam by a polarizer to obtain two pairs of images of the emerging beam, each pair acquired using different polarization states of the incident beam, and each image of the pairs acquired under different orientations of the polarizer; and

analyzing said two pairs of images to obtain a geometrical phase corresponding to the encrypted data.

12. The method of claim 11, further comprising applying a key function on the input data to obtain the data to be carried by the carrier, and after analyzing the images based on knowledge of the key function retrieving the input data.; and based on knowledge of the key function retrieving the input data.

13. A device for carrying encrypted data, the device comprising a space-variant subwavelength grating element, with local gratings having angles of orientation corresponding to the encrypted data.

14. The device of claim 13, wherein the element is reflective.

15. The device of claim 13, wherein the element is transmissive.

16. The device of claim 13, wherein the gratings are made of dielectric material.

17. The device of claim 13, wherein the gratings are made of metallic material.

18. A decrypting apparatus for decrypting encrypted data carried by a space-variant subwavelength grating element, with local gratings having angles of orientation corresponding to the encrypted data, the apparatus comprising:

a light source for providing a light beam to illuminate the grating element;

at least one polarizer for polarzing an emerging beam from the grating element in at different polarizer orientations;

an imaging device for acquiring images acquired under different polarizer orientations of the emerging beam.

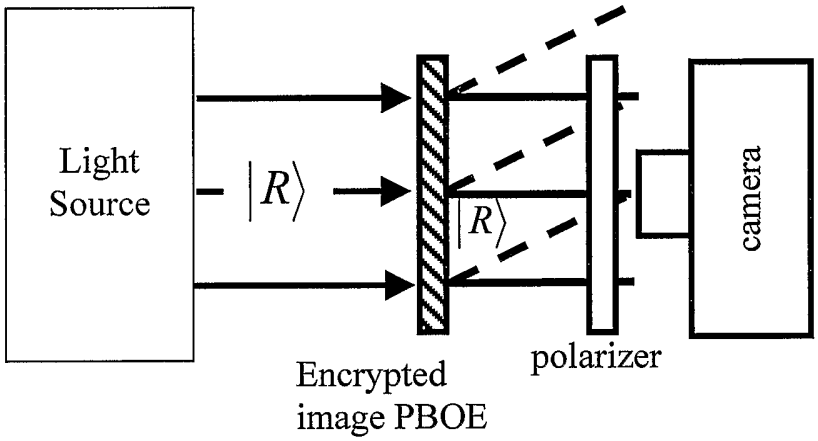


Fig. 1a

Fig. 1b

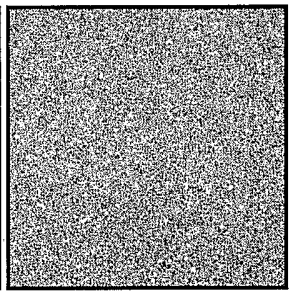


Fig. 1c

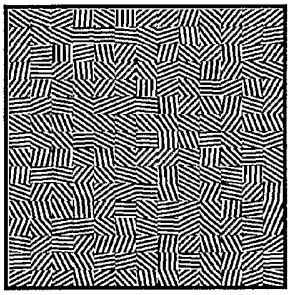


Fig. 1d

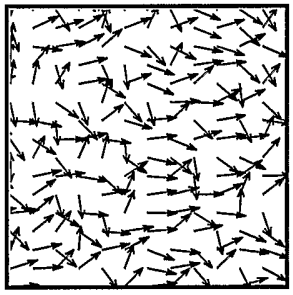


Fig. 1e

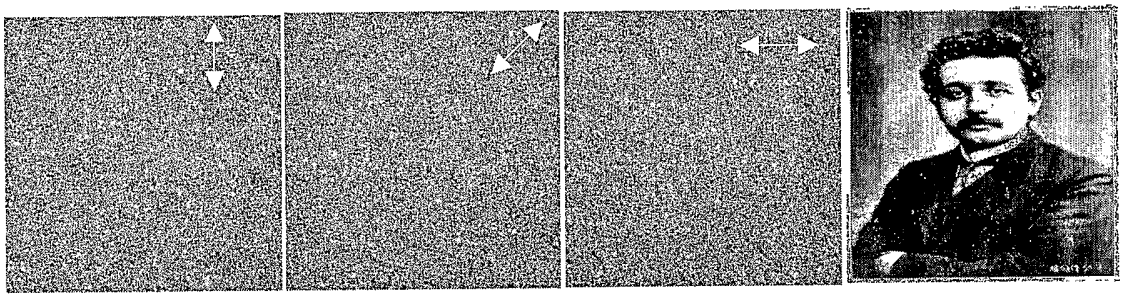


Fig. 2a Fig. 2b Fig. 2c Fig. 2d

Fig. 3a Fig. 3b Fig. 3c Fig. 3d