Available online at www.sciencedirect.com

SCIENCE DIRECT®

Optics Communications xxx (2006) xxx–xxx

OPTICS COMMUNICATIONS

www.elsevier.com/locate/optcom

Space-variant polarization scrambling for image encryption obtained with subwavelength gratings

Gabriel Biener, Avi Niv, Vladimir Kleiner, Erez Hasman *

Optical Engineering Laboratory, Faculty of Mechanical Engineering, Technion-Israel Institute of Technology, Technion City, Haifa 32000, Israel

Received 2 October 2005; received in revised form 28 November 2005; accepted 28 November 2005

Abstract

We present an optical encryption method based on geometrical phase, which is originated from polarization manipulation. The decrypted picture is retrieved by measuring the polarization of the beam emerging from the encrypted element. The encrypted element is achieved by using a computer-generated space-variant subwavelength dielectric grating. Theoretical analyses of the optical concept by use of Jones and Mueller formalisms, as well as experimental results including full optical decryption process are introduced. Digital implementation and the possibility of using watermarking are also discussed.

Keywords: Polarization encoding; Optical encryption; Subwavelength gratings; Geometrical phase; Pancharatnam phase

1. Introduction

Optical encryption and polarization encryption, in particular, have attracted much attention recently [1–18]. The great interest in optical encryption/decryption results from the ability to perform high space-bandwidth product, as well as obtaining real-time encryption, its resistance to unauthorized decryption, and its portability. Moreover, optical encryption has the possibility of using biometrically based approaches [1]. Different optical encryption schemes have been suggested such as double-random phase encryption [2,3,6–8], which was first presented by Refregier and Javidi [2]. This encryption method can be applied either with pure amplitude image encoding [2,6] or with phase-only images encoding [3,5,7]. These methods require coherent and monochromatic source. However, a scheme allowing the use of quasi-monochromatic incoherent light has also been suggested [9].

Several groups have proposed polarization encryption methods, such as using a spatially modulated retardation approach [11–14] or a spatially modulated azimuthal angle procedure [15–18]. Polarization encryption provides additional flexibility in the key encryption design by adding a polarization state manipulation to the phase and amplitude manipulation conventionally used in optical encryption methods [11–18]. This feature is advantageous as it makes the polarization encryption method more secure. The proposed methods were realized by use of liquid crystal modulators. Recently, we demonstrated a method of polarization encryption using computer-generated space-variant subwavelength dielectric gratings (SWG) [17]. We have also shown that space-variant polarization state manipulation inevitably leads to a phase modification of geometrical origin, which is a manifestation of the geometrical Pancharatnam-Berry phase [17–21].

In this paper, we present a comprehensive theoretical analysis along with experimental demonstration of our polarization encryption approach, which is based on SWG. The analysis is done either by Jones calculus or by Mueller formalism. We also describe various decryption processes. In the first decryption method, which is analyzed by Jones calculus, three different intensity measurements are sufficient while in the second method, which is analyzed using Mueller formalism, four different intensity measurements are required. The advantage of the later method is

[*] Corresponding author. Tel.: +972 482 92916; fax: +972 482 95711. *E-mail address:* mehasman@tx.technion.ac.il (E. Hasman).

0030-4018/$ - see front matter © 2005 Elsevier B.V. All rights reserved.
doi:10.1016/j.optcom.2005.11.062

that the values of the birefringent parameters of the encrypted elements are not required for the analysis process, 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 for decrypting the image. A third complete optical decryption method, utilizing a subwavelength grating key element, is also presented. Our encryption method, which is implemented by use of a robust and stable SWG element, can be achieved using a single lithographic process [21,22]. As a result, this method is suitable for chip integration and can be applied to personal security cards, e.g., credit cards or identification cards. Geometrical phase encryption can also be implemented digitally. An important advantage of the digital implementation is the ability to use watermarking.

Section 2 describes the concept of the geometrical phase polarization encryption along with the possibility of using watermarking, when the process is implemented digitally. In this section we analyze the encryption method using both Jones calculus and Stokes–Mueller formalism. Section 3 presents the experimental results, verifying our concept along with a complete optical decryption process using a space-variant subwavelength key element. Finally, Section 4 provides our concluding remarks.

2. Theory

When the period of a grating is smaller than the incident wavelength, only the zeroth order is a propagating order, and the grating behaves as a layer of uniaxial crystal with the optical axes perpendicular and parallel to the grating's grooves [18,21]. Therefore, SWGs are considered to be wave plates with constant retardation and space-varying fast axes, the orientation of which are denoted by $\theta(x, y)$ [21,22].

In order to encrypt a primary image, a SWG that encodes the image intensity added by an arbitrary key function is formed. The SWG, which acts as a space-variant rotating wave plate, imprints the image intensity, in addition to a random key function, in the local orientation of the wave plate's fast axes. Decryption is performed by illuminating the encrypted SWG with a uniformly polarized beam and retrieving the primary image by analyzing the emerging Stokes parameters with the correct key, as shown in Fig. 1(a).

2.1. Analysis of the encryption method using Jones calculus

It is convenient to describe SWGs by using Jones calculus. In this representation, a uniform wave plate in which

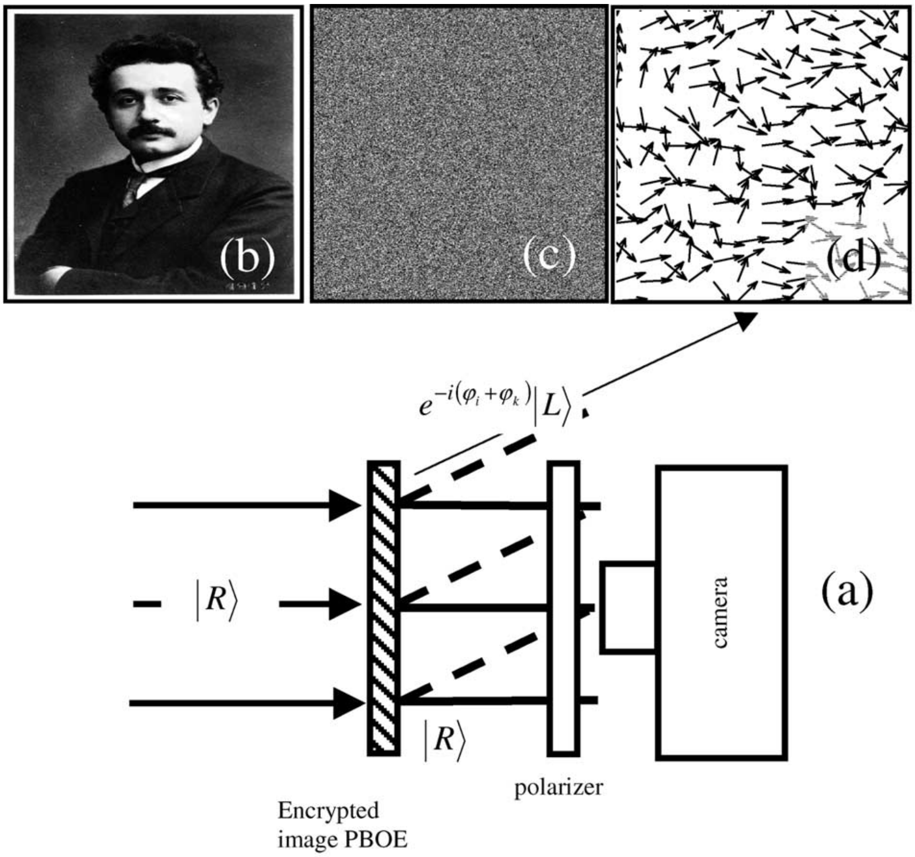

Fig. 1. (a) Schematic representation of the concept of geometrical phase encryption. (b) Primary image intensity to be encrypted. (c) Encrypting SWG wave plate's orientation function, $\theta_i + \theta_k$, in grayscale. (d) Simulated polarization state of the beam emerging from the SWG, taken from a small region near the eyebrow of Einstein, seen in (b).

the fast axis is oriented along the y-axis can be described by the Jones matrix

$$\mathbf{W} = \begin{pmatrix} t_x & 0 \\ 0 & t_y e^{i\phi} \end{pmatrix}, \tag{1}$$

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,$\theta(x, y)$, is space-varying, i.e. different at each location, then the space-variant wave plates can be described by the space-dependent matrix

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

where $\mathbf{R}(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ is a two-dimensional rotation matrix. For convenience we adopt the Dirac braket notation, and convert $\mathbf{T}_C(x, y)$ to the helicity base in which $|\mathbf{R}\rangle = (1 \quad 0)^T$ and $|\mathbf{L}\rangle = (0 \quad 1)^T$ are the two-dimensional unit vectors for right-handed and left-handed circularly polarized light. In this base, the space-variant polarization operator is described by the matrix, $\mathbf{T}(x, y) = \mathbf{U}\mathbf{T}_C\mathbf{U}^{-1}$, where $\mathbf{U} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}$ is a unitary conversion matrix. Explicit calculation of $\mathbf{T}(x, y)$ yields

$$\mathbf{T}(x,y) = \frac{t_x + t_y\exp(i\phi)}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \frac{t_x - t_y\exp(i\phi)}{2} \times \begin{pmatrix} 0 & \exp[i2\theta(x,y)] \\ \exp[-i2\theta(x,y)] & 0 \end{pmatrix}. \tag{3}$$

Thus, for an incident wave with a right-hand circular polarization state and an unknown distributed complex amplitude that follows the paraxial approximation, we find that the resulting field is

$$|\mathbf{E}_{\text{out}}\rangle = \eta_R|\mathbf{R}\rangle + \eta_L\exp[-i2\theta(x,y)]|\mathbf{L}\rangle, \tag{4}$$

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. From Eq. (4) we see that the emerging beam comprises two polarization orders. The first maintains the original polarization state and phase of the incident beam, and the latter is left-handed 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 [17–21].

Let us assume that a SWG with a space-varying wave plate orientation function of $\theta_i(x, y)$ encodes the primary image of young Einstein, as depicted in Fig. 1(b). The relationship between the primary image intensity I and θ_i is chosen to be $\theta_i = aI(x, y)$, where a is a constant. In order to encrypt the encoded primary image information embedded in the SWG, we add a random rotation function, $\theta_k(x, y)$, to the space-varying wave plates' orientation. This rotation factor serves as an encryption/decryption key. The total orientation function of the wave plates, comprising the encrypted SWG, is shown in grayscale in Fig. 1(c). In order to decrypt the primary image, we first illuminate the SWG with $|\mathbf{R}\rangle$ polarized light. The beam emerging from the SWG is a vectorial interference between the two different polarized beams, as can be seen from Eq. (4). The geometrical phase added to the $|\mathbf{L}\rangle$ polarized beam equals $-(\varphi_i(x, y) + \varphi_k(x, y))$, where $\varphi_i(x, y) = 2\theta_i(x, y)$ and $\varphi_k(x, y) = 2\theta_k(x, y)$ denote the geometrical phases added by the encoded primary image intensity and the encoded key, respectively. Fig. 1(d) depicts the space-variant polarization direction emerging from a simulated SWG 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, $\varphi_k(x, y)$, scrambles the space-variant polarization state of the beam and thus spatially randomizes the geometrical phase encoding the primary image, $\varphi_i(x, y)$. In order to retrieve the primary image's geometrical phase, we need to measure the Stokes parameters of the beam emerging from the SWG. The Stokes parameters of a fully polarized light ($S_0 - S_3$) can be calculated using three intensity measurements. These measurements are taken when the transmitted light is passed through a polarizer with its axis oriented at 0° (I_0), 45° (I_{45}) and 90° (I_{90}). A camera is used to capture the intensity pictures. An example of these measurements, taken from the simulated encrypting SWG, is presented in Fig. 2. The relations between the Stokes parameters and the measured intensities are

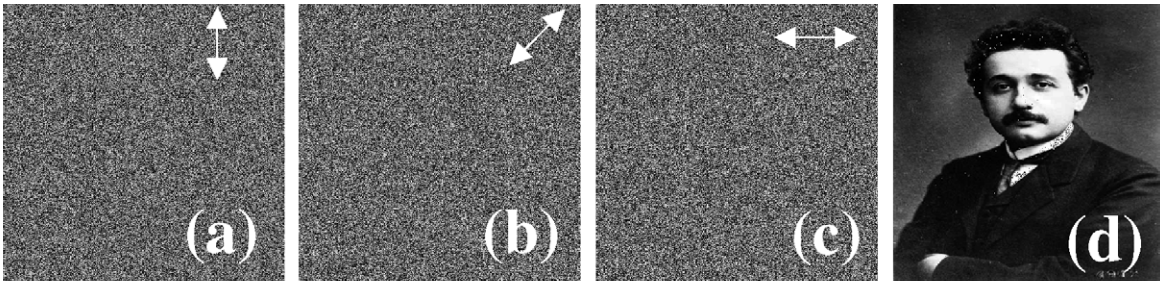

Fig. 2. (a)–(c) Three simulated intensity pictures generated by the decryption process with the polarizer in the different orientations: (a) 0°, (b) 45° and (c) 90°. The arrows indicate the orientation angle of the polarizer. (d) Decrypted image achieved by the decryption process (Jones formalism) using the intensities shown in (a)–(c).

$$S_0 = I_0 + I_{90}, \tag{5a}$$

$$S_1 = I_0 - I_{90}, \tag{5b}$$

$$S_2 = 2I_{45} - S_0, \tag{5c}$$

where $S_0 = |\langle \mathbf{E}_{\text{out}}|\mathbf{R}\rangle|^2 + |\langle \mathbf{E}_{\text{out}}|\mathbf{L}\rangle|^2$, $S_1 = 2\text{Re}\{\langle \mathbf{E}_{\text{out}}|\mathbf{R}\rangle\text{-}\langle \mathbf{L}|\mathbf{E}_{\text{out}}\rangle\}$ and $S_2 = 2\text{Im}\{\langle \mathbf{E}_{\text{out}}|\mathbf{R}\rangle\langle \mathbf{L}|\mathbf{E}_{\text{out}}\rangle\}$, Re{} and Im{} denote the real and imaginary parts of the expression inside the curl brackets, $\langle\alpha|\beta\rangle$ denotes the inner product, and $|\mathbf{E}_{\text{out}}\rangle$ is calculated from Eq. (4). By using the Stokes parameters, that were calculated from Eq. (5), and applying the geometrical phase key, we can retrieve the phase function ($\varphi_{\text{i}}(x, y)$) of the primary image, to give

$$\varphi_{\text{i}}(x,y) = \arctan[S_2(x,y)/S_1(x,y)] - \arg\{\eta_{\text{R}}\eta_{\text{L}}^*\} - \varphi_{\text{k}}(x,y), \tag{6}$$

where arg{} denotes the argument of the expression in the curl brackets, and * denotes the complex conjugate. Fig. 2(d) depicts the decrypted image retrieved from the simulated intensities presented in Fig. 2(a)–(c). Since the emerging beam is fully polarized, the fourth Stokes parameter, S_3, is not required. Note that the complex field coefficients, η_{R} and η_{L}, have no effect on the decryption process as long as they are space-invariant, as indicated by the argument (arg) expression written in Eq. (6). Thus, spatial independence of the subwavelength parameters allows us to ignore the SWG parameters' t_x, t_y, and ϕ values.

The theoretical analysis of the encryption method described here is accompanied by a computer simulation. This simulation can be regarded as the digital implementation of our method. The optical implementation will be experimentally described in the next chapter. When using digital implementation, the encryption process ends after the formation of the three intensity pictures achieved by the simulated analyzer. 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

$$I_0^{\text{WM}} = I_0 + I_{\text{WMP}}, \tag{7a}$$

$$I_{45}^{\text{WM}} = I_{45} + I_{\text{WMP}}, \tag{7b}$$

$$I_{90}^{\text{WM}} = I_{90} + I_{\text{WMP}}, \tag{7c}$$

where I_{WMP} symbolizes the watermark picture and I_0^{WM}, I_{45}^{WM} and I_{90}^{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. Fig. 3(a)–(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.

2.2. Analysis of the decryption process by using Mueller formalism

Another method for describing a SWG is the Stokes–Mueller fomalism approach. In this representation, a uniform wave plate in which the fast axis is oriented along the y-axis can be described by a 4 × 4 matrix known as the Mueller matrix,

$$\mathbf{W} = \frac{1}{2}\begin{pmatrix} t_x^2 + t_y^2 & t_x^2 - t_y^2 & 0 & 0 \\ t_x^2 - t_y^2 & t_x^2 + t_y^2 & 0 & 0 \\ 0 & 0 & 2t_xt_y\cos\phi & -2t_xt_y\sin\phi \\ 0 & 0 & 2t_xt_y\sin\phi & 2t_xt_y\cos\phi \end{pmatrix}, \tag{8}$$

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

$$\mathbf{M}(x,y) = \mathbf{R}(\theta(x,y))\mathbf{W}\mathbf{R}^{-1}(\theta(x,y)), \tag{9}$$

where

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

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

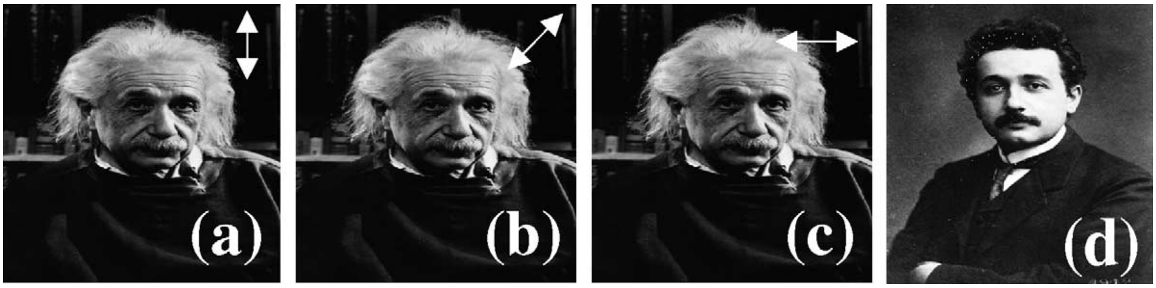

Fig. 3. (a)–(c) Three simulated watermarked pictures with the polarizer oriented at (a) 0°, (b) 45° and (c) 90°. The arrows indicate the orientation angle of the polarizer. (d) Decrypted image achieved by using the three watermarked pictures and the correct key.

$$\mathbf{M}(\theta(x,y)) = \begin{pmatrix} |A|^2+|B|^2 & 2\mathrm{Re}\{AB^*\}\cos 2\theta & 2\mathrm{Re}\{AB^*\}\sin 2\theta & 0 \\ 2\mathrm{Re}\{AB^*\}\cos 2\theta & |A|^2+|B|^2\cos 4\theta & |B|^2\sin 4\theta & 2\mathrm{Im}\{AB^*\}\sin 2\theta \\ 2\mathrm{Re}\{AB^*\}\cos 2\theta & |B|^2\sin 4\theta & |A|^2-|B|^2\cos 4\theta & -2\mathrm{Re}\{AB^*\}\cos 2\theta \\ 0 & -2\mathrm{Im}\{AB^*\}\sin 2\theta & 2\mathrm{Im}\{AB^*\}\cos 2\theta & |A|^2-|B|^2 \end{pmatrix}, \tag{10}$$

where $A = [t_x + t_y \exp(\mathrm{i}\phi)]/2$ and $B = [t_x - t_y \exp(\mathrm{i}\phi)]/2$ 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, $\theta_\mathrm{i} + \theta_\mathrm{k}$. As can be seen from Eq. (10) the groove orientation is found by dividing the SWG Mueller matrix members $-m_{42}$ by m_{43}, which results in

$$\frac{-m_{42}}{m_{43}} = \frac{\mathrm{Im}\{AB^*\}\sin 2\theta}{\mathrm{Im}\{AB^*\}\cos 2\theta} = \tan 2\theta. \tag{11}$$

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. (11). This result indicates that the extracted space-variant subwavelength orientation function does not depend on the subwavelength grating's parameter values. Thus, the decryption method is insensitive to spatial fabrication non-uniformities. Another 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 are process-dependent parameters, θ is very accurate and does not depend on either the process or on the illumination. Therefore, by extracting θ without the influence of t_x, t_y and ϕ, the decryption process is simplified and made more accurate.

By extracting $\theta_\mathrm{i} + \theta_\mathrm{k}$ and applying the correct key, we can retrieve the primary image, thus

$$\theta_\mathrm{i} = \frac{1}{2}\arctan\left(\frac{-m_{42}}{m_{43}}\right) - \theta_\mathrm{k}. \tag{12}$$

The measurement of the Mueller matrix members, m_{42} and m_{43} is carried out 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 quarter wave plate (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 $I_{45}^{\alpha}(I_{-45}^{\alpha})$, where 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

$$\begin{aligned} m_{42} &= I_{-45}^{0} - I_{45}^{0}, \\ m_{43} &= I_{45}^{45} - I_{-45}^{45}. \end{aligned} \tag{13}$$

3. Realization and experimental results

We formed binary chrome masks of the encrypted image to encrypt the primary image intensity, as depicted in Fig. 4(a). The amplitude transmission, $t(x, y)$, of the masks is derived from

$$t(x,y) = U_\mathrm{s}\left[\cos\left(\frac{2\pi}{\Lambda}(x\cos\theta(x,y) + y\sin\theta(x,y))\right) - \cos(\pi q)\right], \tag{14}$$

where Λ and q are the period and fill factor of the subwavelength grating, respectively, $\theta(x, y)$ is the groove orientation function of the encrypted image, and U_s is the unit step function defined by

$$U_\mathrm{s}(\xi) = \begin{cases} 1, & \xi \geqslant 0 \\ 0, & \xi < 0 \end{cases}. \tag{15}$$

The mask was comprised of 20 × 20 pixels, each pixel having dimensions of 500 μm × 500 μm. A subwavelength period of $\Lambda = 2$ μm was selected together with a fill factor

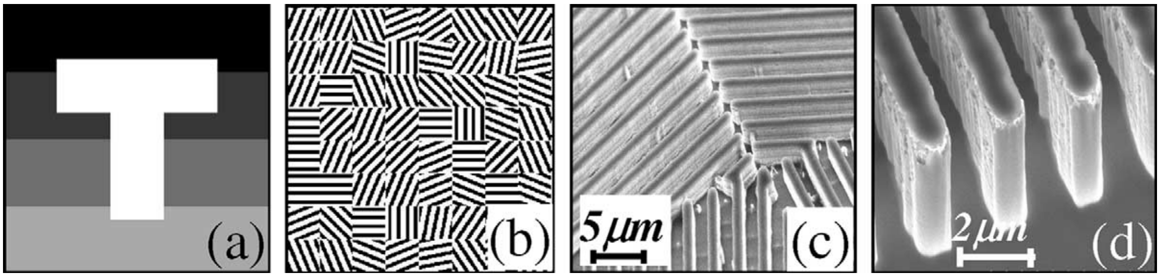

Fig. 4. (a) Primary image intensity to be experimentally encrypted. (b) Subwavelength grating mask of the encrypted element. (c) Scanning electron microscope (SEM) image of an area on the SWG. (d) SEM image of the subwavelength grating's grooves.

$q = 0.5$ for use with CO_2 laser radiation with a 10.6 μm wavelength. Fig. 4(b) shows a magnified geometry of the mask. The mask was transferred by contact lithography to 500 μm thick GaAs wafers onto which had been deposited a 2000 Å-thick layer of SiN_x. The SiN_x deposition was achieved by enhanced chemical vapor deposition (PECVD) at 900 mTorr and 300 °C. At this stage, a 700 Å Ni adhesion layer was used for the lift-off process. Next, the SiN_x layer was etched through the Ni strips, which served as a mask. The etching was performed by reactive ion etching (RIE) for 30 s at room temperature with CF_4 and O_2 at gas flow rates of 35 and 14 sccm, respectively, and at a pressure of 80 mTorr. The GaAs was etched by electron cyclone resonance (ECR) for about 4 min, with the etched SiN_x layer serving as a mask. The ECR conditions were: 20 sccm of Cl_2, 5 sccm of Ar, 75 W RF power and 600 W microwave power, at 100 °C. The remaining SiN_x was removed using HF acid resulting in a grating with a nominal depth of 2.5 μm. At this stage, an anti-reflection coating was deposited on the backside of the element to finish the fabrication of the desired SWG. Fig. 4(c) shows a scanning electron microscope (SEM) image of the central part of the element. Fig. 4(d) shows a SEM image of the subwavelength grooves. Note the rectangular shape of the grooves. The encrypted element resulted in a measured retardation value of $\phi = 0.4\pi$ and amplitude transmission coefficients of $t_x = 0.88$ and $t_y = 0.77$; these values are close to the theoretical predictions achieved by rigorous coupled-wave analysis utilizing the measured profiles of the gratings.

Following the fabrication, the encrypted element was illuminated with a right-handed circularly polarized light at 10.6 μm wavelength. The beam emerging from the encrypted element was then transmitted through a polarizer oriented in the three different orientations (0°, 45° and 90°). Fig. 5(a) and (b) show the two Stokes parameters, S_1 and S_2, which were calculated from the three intensities measured using Eq. (5). The decrypted image shown in Fig. 5(c) was attained by applying the Stokes parameters and by using Eq. (6) with the correct geometrical phase key, φ_k. The primary image is clearly observed, thus demonstrating the successful decryption of the coded image. Fig. 5(d) shows the measured space-variant polarization directions emerging from the encrypted SWG. As can be seen, the orientation of the arrows is completely random

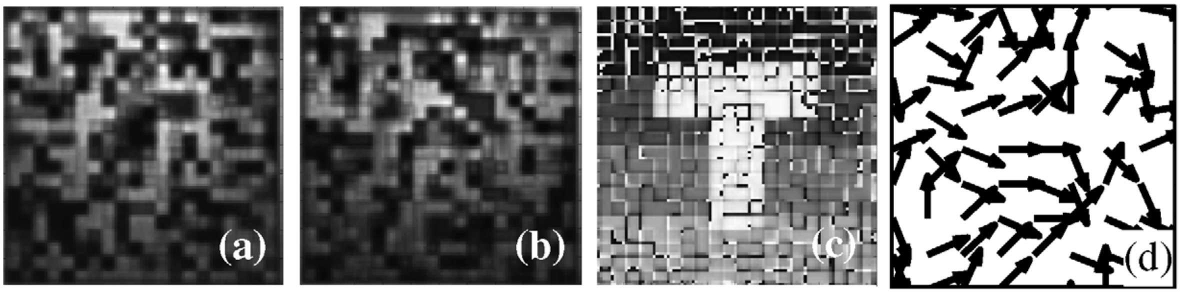

Fig. 5. (a) and (b) represent the calculated Stokes parameters S_1 and S_2 , respectively. The calculation of the relevant Stokes parameters were achieved using the three intensity measurements. (c) Decrypted image obtained by using S_1 and S_2 depicted in (a) and (b) along with the correct key (Jones formalism). (d) Measured polarization state of the beam emerging from the SWG.

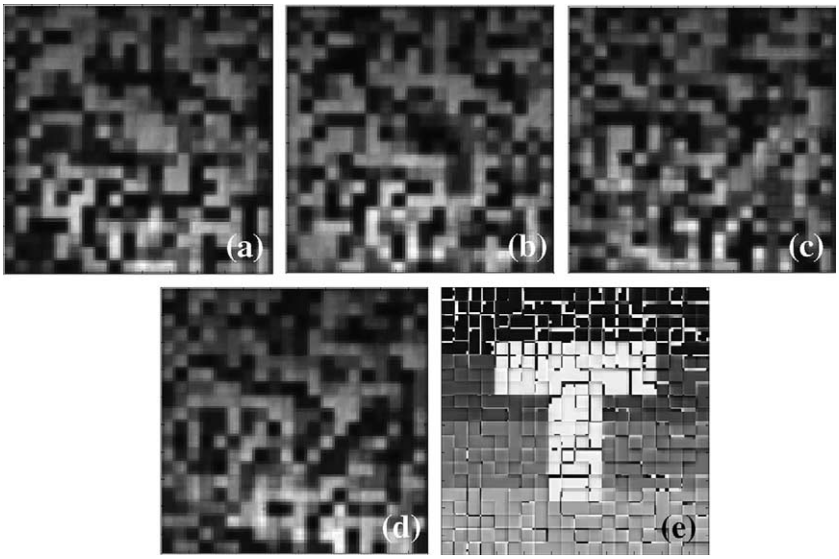

Fig. 6. (a) and (b) Two measured intensity pictures generated by the decryption process (Mueller formalism) for the horizontal linearly polarized illumination analyzed by a circular analyzer (QWP oriented at 0° and the polarizer oriented at (a) 45° and (b) −45°). (c) and (d) Same as (a) and (b) with a 45° linearly polarized illumination. (e) Decrypted image achieved by the decryption process using the intensities shown in (a)–(d).

as expected (see also Fig. 1(d)). A second approach of using Mueller formalism was also tested. Fig. 6(a)–(d) show the four intensity measurements, I^{0}_{45}, I^{0}_{-45}, I^{45}_{45} and I^{45}_{-45}, and Fig. 6(e) is the decrypted image achieved using the four intensity pictures together with the correct key. Again, the image was successfully decrypted. If the wrong key were to be used, such as the one seen in Fig. 7(a), the resulting decrypted image would show only stationary white noise, as shown in the experimental result of Fig. 7(b), and it would be impossible to reconstruct the original image.

We also propose an alternative method for decryption by using the optical setup illustrated in Fig. 8. This method involves two SWGs in which one encodes the encrypted image with the transmission matrix

$$\mathbf{T}_{\mathrm{e}} = \eta_{\mathrm{R}}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \eta_{\mathrm{L}}\begin{pmatrix} 0 & \exp[\mathrm{i}2\theta_{\mathrm{e}}(x,y)] \\ \exp[-\mathrm{i}2\theta_{\mathrm{e}}(x,y)] & 0 \end{pmatrix}, \tag{16}$$

where $\theta_{\mathrm{e}} = \theta_{\mathrm{i}} + \theta_{\mathrm{k}}$, and the other encodes the key, having the transmission matrix

$$\mathbf{T}_{\mathrm{k}} = \eta_{\mathrm{R}}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \eta_{\mathrm{L}}\begin{pmatrix} 0 & \exp[\mathrm{i}2\theta_{\mathrm{k}}(x,y)] \\ \exp[-\mathrm{i}2\theta_{\mathrm{k}}(x,y)] & 0 \end{pmatrix}. \tag{17}$$

The space-variant subwavelength key element was fabricated upon a 500 μm – thick GaAs wafer with a 2 μm subwavelength period, employing the same process used to form the encrypted element. In order to decrypt the image, we illuminated the encrypted element with a right-handed, circularly polarized CO_2 laser radiation at a wavelength of 10.6 μm. The beam was then transmitted through a 4-f system followed by the key element. The beam emerging from the key element has the form of

$$\begin{aligned} |\mathbf{E}_{\mathrm{d}}\rangle &= \mathbf{T}_{\mathrm{k}}\mathbf{T}_{\mathrm{e}}|\mathbf{R}\rangle \\ &= \lfloor \eta_{\mathrm{R}}^2 + \eta_{\mathrm{L}}^2 \exp(\mathrm{i}\varphi_{\mathrm{i}}) \rfloor |\mathbf{R}\rangle + 2\eta_{\mathrm{R}}\eta_{\mathrm{L}} \exp[-\mathrm{i}(\varphi_{\mathrm{i}} \\ &\quad + 2\varphi_{\mathrm{k}})/2] \cos(\varphi_{\mathrm{i}}/2)|\mathbf{L}\rangle, \end{aligned} \tag{18}$$

where φ_{i} encodes the primary image. The emerging beam was then passed through a circular polarizer to block the right-handed circularly polarized portion of the beam leaving only

$$|\mathbf{E}_{\mathrm{out}}\rangle = 2\eta_{\mathrm{R}}\eta_{\mathrm{L}} \exp[-\mathrm{i}(\varphi_{\mathrm{i}} + 2\varphi_{\mathrm{k}})/2] \cos(\varphi_{\mathrm{i}}/2)|\mathbf{L}\rangle. \tag{19}$$

Finally, the filtered portion of the beam was imaged onto a Pyrocam III camera. The experimental result is shown in the inset of Fig. 8, indicating good agreement with our prediction. As can be seen from the last result, the intensity of the decrypted image captured by the camera is proportional to cos φ_{i}. In order to identically reproduce the primary image's intensity without further analysis, we need to encode the primary image's intensity using the relationship $\theta_{\mathrm{i}} = a\cos^{-1}(I)$ instead of the linear relationship used above.

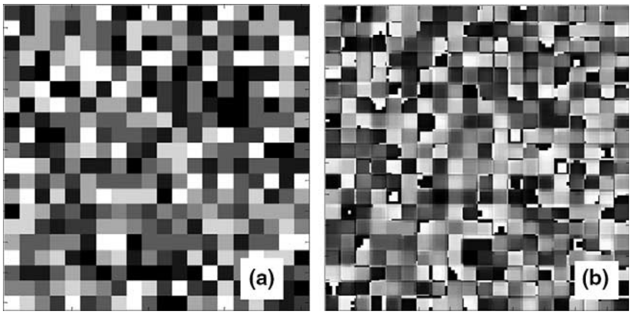

Fig. 7. (a) Wrong geometrical phase key. (b) "White noise" decrypted image resulting from using the key depicted in (a), along with the measured intensities shown in Fig. 6(a)–(d).

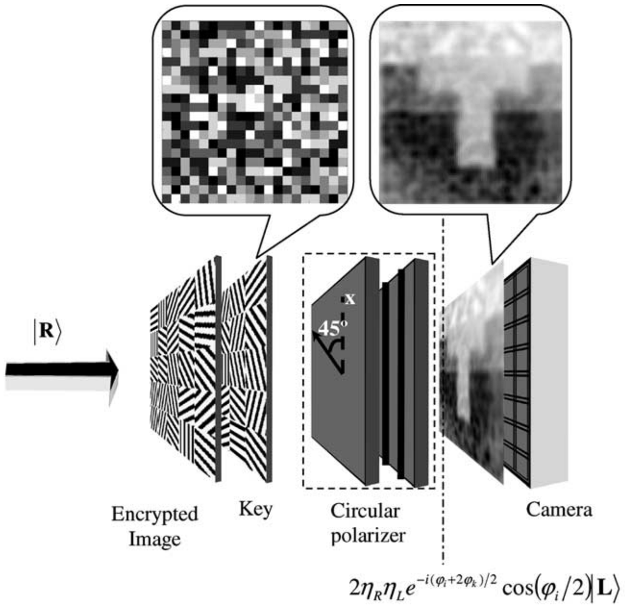
|R⟩
x
45°
Encrypted Image
Key
Circular polarizer
Camera
$2\eta_R\eta_L e^{-i(\varphi_i+2\varphi_k)/2}\cos(\varphi_i/2)|\mathbf{L}\rangle$

Fig. 8. Optical decryption concept comprising the encrypted and key elements. A telescope (not shown) between the two elements is used in the experiment to image the complex amplitude of the beam emerging from the encrypted element onto the key element. The wave plate's orientation function, $\theta_{\mathrm{k}}(x, y)$, is shown in grayscale in the above left inset. The beam emerging from the key is transmitted through a circular polarizer and then imaged onto a camera. The upper right inset represents the experimental result of the optical decryption.

4. Conclusions

We have introduced an approach for geometrical phase encryption using spatial polarization state manipulation. This paper presented a theoretical analysis using Jones calculus and Mueller formalism along with experimental results. The decryption method which was analyzed using Mueller formalism is insensitive to spatial manufacturing errors and can be applied to incoherent, polychromatic, and unpolarized light. A full optical decryption method was also demonstrated. While full optical decryption has the advantage of using only a single measurement, the method requires coherent, monochromatic, and polarized illumination and high quality fabricated elements. Our method can be realized using space-variant subwavelength dielectric gratings, thereby making it suitable for personal security cards. It can also be implemented solely in a digital environment thus enabling the additional security feature of watermarking.

References

[1] E.G. Johnson, J.D. Brasher, D. Gregory, P. Erbach, M. Duignan, G. Behrman, S.H. Lee, W. Dashner, P. Long, Opt. Eng. 37 (1998) 18.

[2] P. Refregier, B. Javidi, Opt. Lett. 20 (1995) 767.

[3] N. Towghi, B. Javidi, Z. Luo, J. Opt. Soc. Am. A 16 (1999) 1915.

[4] P.C. Mogensen, J. Glückstad, Opt. Lett. 25 (2000) 566.

[5] G. Situ, J. Zhang, Opt. Commun. 232 (2004) 115.

[6] G. Unnikrishnan, J. Joseph, K. Singh, Opt. Lett. 25 (2000) 887.

[7] G. Unnikrishnan, K. Singh, Opt. Eng. 39 (2000) 2853.

[8] E. Tajahuerce, O. Matoba, S.C. Verrall, B. Javidi, Appl. Opt. 39 (2000) 2313.

[9] E. Tajahuerce, J. Lancis, B. Javidi, P. Andrés, Opt. Lett. 26 (2001) 678.

[10] D.H. Seo, S.J. Kim, Opt. Lett. 28 (2003) 304.

[11] P.C. Mogensen, J. Glückstad, Opt. Commun. 173 (2000) 177.

[12] X. Tan, O. Matoba, Y. Okada-Shudo, M. Ide, T. Shimura, K. Kuroda, Appl. Opt. 40 (2001) 2310.

[13] O. Matoba, B. Javidi, Appl. Opt. 43 (2004) 2915.

[14] H.Y. Tu, C.J. Cheng, M.L. Chen, J. Opt. A: Pure Appl. Opt. 6 (2004) 524.

[15] G. Unnikrishnan, M. Pohit, K. Singh, Opt. Commun. 185 (2000) 25.

[16] B. Javidi, T. Nomura, Opt. Eng. 39 (2000) 2439.

[17] G. Biener, A. Niv, V. Kleiner, E. Hasman, Opt. Lett. 30 (2005) 1096.

[18] E. Hasman, G. Biener, A. Niv, V. Kleiner, in: E. Wolf (Ed.), Progress in Optics, vol. 47, Elsevier, Amsterdam, 2005.

[19] S. Pancharatnam, Proc. Ind. Acad. Sci. A 44 (1956) 247.

[20] M.V. Berry, Proc. R. Soc. Lon. Ser. A 392 (1984) 45.

[21] E. Hasman, V. Kleiner, G. Biener, A. Niv, Appl. Phys. Lett. 82 (2003) 328.

[22] A. Niv, G. Biener, V. Kleiner, E. Hasman, Opt. Lett. 29 (2004) 238.