Geometrical phase image encryption obtained with space-variant subwavelength gratings

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

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

Received November 15, 2004

An optical encryption method based on a geometrical phase produced by space-variant polarization manipulation is presented. The decrypted picture is retrieved either by a polarization measurement of the beam emerging from the encrypted element or by a single intensity measurement of the beam transmitted through the encrypted element followed by an optical key element. Both elements are realized by use of computer-generated space-variant subwavelength dielectric gratings. Theoretical analyses of the optical concept are presented along with experimental results. © 2005 Optical Society of America

OCIS codes: 050.2770, 260.5430, 999.9999.

In the past few years there has been increased interest in data security and a growing need for improved methods for data encryption. The increasing demand for better and faster security devices is a result of the problems created by unauthorized users and commercial spies gaining access to communication networks. 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 encoding.[1] Other encryption schemes involving phase-only images were explored to improve the decrypted image's visibility.[2] Both methods use double-random phase encryption, a technique first presented by Refregier and Javidi.[1] Since the two methods record the complex field information by interference, they are unstable and cumbersome. Mogensen and Glückstad proposed polarization encryption using spatially modulated retardation,[3] whereas Unnikrishnan *et al.* proposed polarization encryption using a spatially modulated azimuthal angle.[4] 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.

In this Letter we propose an approach for polarization encryption using geometrical phase modification. Geometrical phases originate from polarization state manipulation, as anticipated by Pancharatnam[5] and Berry.[6] Recently, we demonstrated the formation of complex polarization state manipulation by using computer-generated space-variant subwavelength gratings (SWG).[7] We have also shown that such polarization state manipulations inevitably lead to a phase modification of geometrical origin.[8,9] Geometrical phase encryption, which is realized by use of a SWG, results in a robust and stable encryption scheme while applying an element that can be achieved by use of a single lithographic process.[7,8] The method is suitable for chip integration and can be applied to personal security cards, e.g., credit cards or identification cards.[10]

SWGs are considered to be wave plates with constant retardation and space-varying fast axes, the orientation of which is denoted by $\theta(x,y)$.[7,8] The realization procedure of the SWG involves the fabrication of a mask. Figure 1(c) is a magnified illustration of the subwavelength grating mask of the encrypted image. The primary image is shown in Fig. 1(b). To encrypt a primary image, we need to form a SWG that encodes the image intensity while incorporating a random key function. The SWG, which is a space-variant rotating wave plate, imprints the image intensity along with the random key function in the local orientation of the wave plate's fast axes. Decryption is then performed by illuminating the encrypted element with circularly polarized light and retrieving the primary image by analyzing the emerging Stokes parameters using the correct key, as

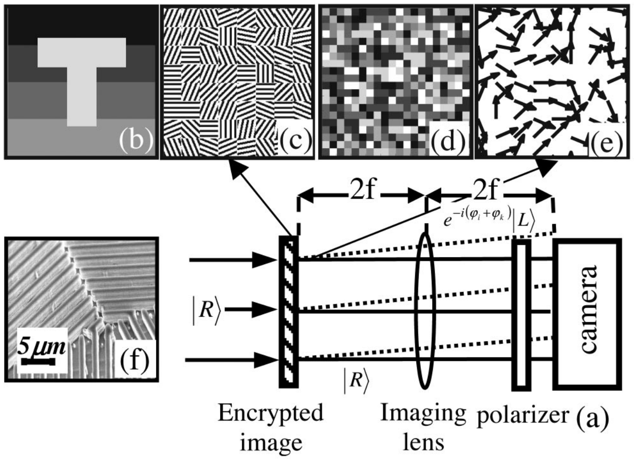

Fig. 1. (a) Schematic representation of the concept of geometrical phase encryption. (b) Primary image intensity to be encrypted. (c) SWG mask of the central region of the SWG. (d) The wave plate's orientation function, θ_k, of the key element is shown in grayscale. (e) Measured polarization state of the beam emerging from the encrypted element taken from the central region. (f) Scanning electron microscope image of the encrypted element taken from a small region in the element.

shown in Fig. 1(a). Alternatively, instead of using the function of the correct key in the analysis, we can insert a SWG into the optical setup to serve as a decryption key. Since this decryption method, which is explained below, involves only a single measurement, the analysis is much simpler.

It is convenient to describe SWGs by using Jones calculus. We find the space-dependent transmission matrix for the SWG, $\mathbf{T}_C$, 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

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

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-handed circular polarization and unknown distributed complex amplitude that follows the paraxial approximation, we find that the resulting field is

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

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 $|\mathbf{R}\rangle=(1\ 0)^T$ and $|\mathbf{L}\rangle=(0\ 1)^T$ represent the right- and left-handed circularly polarized components in the helical basis, respectively. From Eq. (2) we see that the emerging beam from a SWG 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.[5–9]

Let us assume that a SWG with a space-varying wave plate orientation function of $\theta_i(x,y)$ encodes the primary image depicted in Fig. 1(b). 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. To further 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 plate's orientation. This random rotation factor serves as an encryption–decryption key. The orientation function of the wave plates, which serves as the encrypting key, $\theta_k(x,y)$, is shown in grayscale in Fig. 1(d). To decrypt the primary image, we first illuminate the encrypted SWG with $|\mathbf{R}\rangle$ polarized light. The beam emerging from the encrypted element 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 $\varphi_i=2\theta_i(x,y)$ and $\varphi_k=2\theta_k(x,y)$ denote the phases of the encoded primary image intensity and the encoded key, respectively.

To retrieve the primary image's geometrical phase we need to measure the Stokes parameters of the beam emerging from the encrypted element. 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), 45° (I_{45}), and 90° (I_{90}). A camera is used to capture the intensity pictures. The relations between the Stokes parameters and the measured intensities are $S_0=I_0+I_{90}$, $S_1=I_0-I_{90}$, and $S_2=2I_{45}-S_0$, where

$$S_0 = |\langle\mathbf{E}_{\text{out}}|\mathbf{R}\rangle|^2 + |\langle\mathbf{E}_{\text{out}}|\mathbf{L}\rangle|^2,$$

$$S_1 = 2\,\text{Re}\{\langle\mathbf{E}_{\text{out}}|\mathbf{R}\rangle\langle\mathbf{L}|\mathbf{E}_{\text{out}}\rangle\},$$

$$S_2 = 2\,\text{Im}\{\langle\mathbf{E}_{\text{out}}|\mathbf{R}\rangle\langle\mathbf{L}|\mathbf{E}_{\text{out}}\rangle\},$$

where Re{ } and Im{ } denote the real and imaginary parts of the expression inside the braces and $\langle\boldsymbol{\alpha}|\boldsymbol{\beta}\rangle$ 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

$$\varphi_i = \arctan(S_2/S_1) - \arg\{\eta_R\eta_L^*\} - \varphi_k, \quad (3)$$

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

To test the concept we formed an encrypted element, encrypting the primary image intensity depicted in Fig. 1(b) by use of an advanced photolithographic process.[7] The encrypted element comprised 20×20 pixels, each pixel having dimensions of $500\ \mu\text{m}\times 500\ \mu\text{m}$. The SWG, which was designed for the 10.6-μm wavelength, was fabricated on a 500-μm-thick GaAs wafer to a nominal grating depth of 2.5 μm, with a 2-μm subwavelength period. This resulted in measured retardation values of $\phi=0.4\pi$ and amplitude transmission coefficients of $t_x=0.88$ and $t_y=0.77$, close to the theoretical predictions achieved by rigorous coupled-wave analysis utilizing the measured profiles of the gratings. A scanning electron microscope image of a small region of the encrypted SWG is shown in Fig. 1(f).

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 three different orientations (0°, 45°, and 90°). Figures 2(a)–2(c) show the three intensity pictures obtained by setting the polarizer at the three different orientations. The decrypted image shown in Fig. 2(d) was attained by calculating the Stokes parameters when applying the intensities, and by using Eq. (3) when applying the correct geometrical phase key, φ_k. When the wrong key is used, as for the one with the geometrical phase depicted in Fig. 3(a), the resulting decrypted image would show only white noise as can be seen in Fig. 3(b), with no possibility of reconstructing the original image.

Figure 1(e) shows the measured space-variant polarization directions emerging from the encrypted SWG. As can be seen, the orientation of the arrows is completely random. The emerging field, which is a result of the vectorial self-interference given in Eq. (2), is a space-varying polarized field. The geometrical phase key, φ_k, scrambles the space-variant polarization state of the beam and thus randomizes the geometrical phase, thereby encoding the primary image, φ_i.

We also propose an alternative method for decryption by using the optical setup illustrated in Fig. 4. This method involves two SWGs, one to encode the encrypted image, with the transmission matrix $\mathbf{T}_e$, and the other to encode the key, having the transmission matrix $\mathbf{T}_k$. Both elements were fabricated upon a 500-μm GaAs wafer with a 2-μm subwavelength period. Using this method, to decrypt the image we illuminated the encrypted element with CO_2 laser radiation at the wavelength of 10.6-μm having right-handed circular polarization. The beam was then transmitted through a 4-f system followed by the key element. The beam emerging from the key element was then passed through a circular polarizer to omit the right-handed circularly polarized portion of the beam and finally imaged onto a Pyrocam III camera. The transmitted portion of the beam can be written as a projection of the beam emerging from the key element on a left-handed circularly polarized state, i.e., $|\mathbf{E}_{\text{out}}\rangle = [\langle \mathbf{L}|\mathbf{T}_k\mathbf{T}_e|\mathbf{R}\rangle]|\mathbf{L}\rangle$, where $\mathbf{T}_k = \mathbf{T}[2\theta_k(x,y)]$, $\mathbf{T}_e = \mathbf{T}\{2[\theta_i(x,y)+\theta_k(x,y)]\}$, and $\mathbf{T}$ is the transmission matrix for a SWG given by Eq. (1). Explicitly, the calculation yields $|\mathbf{E}_{\text{out}}\rangle = 2\eta_R\eta_L \exp[i(\varphi_i+2\varphi_k)/2] \times\cos(\varphi_i/2)|\mathbf{L}\rangle$. The experimental result is shown in the inset of Fig. 4, 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.

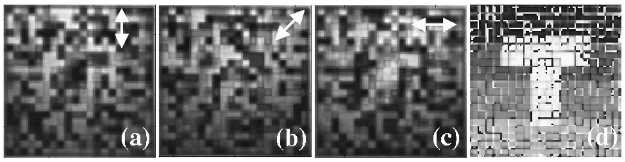

Fig. 2. (a)–(c) Three pictures of the measured intensity obtained by the decryption process with the polarizer in varying orientations: (a) 0°, (b) 45°, and (c) 90°. The white arrows indicate the orientation angle of the polarizer. (d) Decrypted image achieved by the decryption process using the intensities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

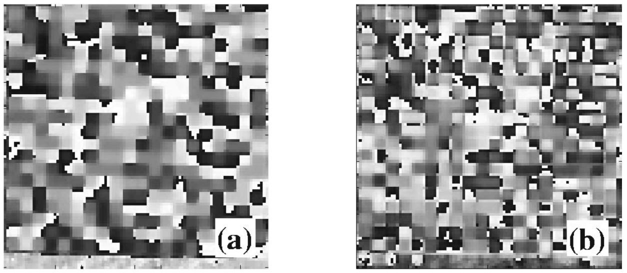

Fig. 3. (a) Wrong geometrical phase key. (b) White noise decrypted image that resulted from using the key depicted in (a).

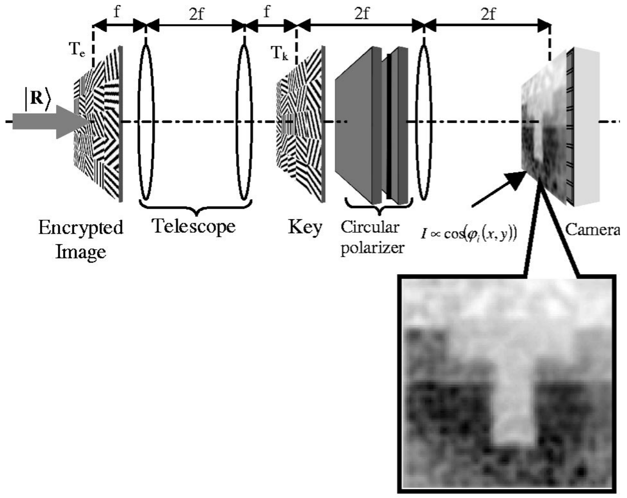

Fig. 4. Optical decryption setup comprising the encrypted and key elements. The telescope between the two elements is used to image the complex amplitude of the beam emerging from the encrypted element onto the key element. The beam emerging from the key is transmitted through a circular polarizer and then imaged onto a camera. The inset represents the experimental result of the optical decryption.

E. Hasman's e-mail address is mehasman @tx.technion.ac.il.

References

1. P. Refregier and B. Javidi, Opt. Lett. **20**, 767 (1995).
2. N. Towghi, B. Javidi, and Z. Luo, J. Opt. Soc. Am. A **16**, 1915 (1999).
3. P. C. Mogensen and J. Glückstad, Opt. Commun. **173**, 177 (2000).
4. G. Unnikrishnan, M. Pohit, and K. Singh, Opt. Commun. **185**, 25 (2000).
5. S. Pancharatnam, Proc. Indian Acad. Sci. Sect. A **44**, 247 (1956).
6. M. V. Berry, Proc. R. Soc. London Ser. A **392**, 45 (1984).
7. A. Niv, G. Biener, V. Kleiner, and E. Hasman, Opt. Lett. **29**, 238 (2004).
8. E. Hasman, V. Kleiner, G. Biener, and A. Niv, Appl. Phys. Lett. **82**, 328 (2003).
9. E. Hasman, G. Biener, A. Niv, and V. Kleiner, *Progress in Optics*, E. Wolf, ed. (Elsevier, Amsterdam, to be published), Vol. 47.
10. B. Javidi and J. L. Horner, Opt. Eng. **33**, 1752 (1994).