Optical scanning cryptography for secure wireless transmission

Ting-Chung Poon, Taegeun Kim, and Kyu Doh

We propose a method for secure wireless transmission of encrypted information. By use of an encryption key, an image or document is optically encrypted by optical heterodyne scanning and hence encryption is performed on the fly. We call this technique optical scanning cryptography. The output of the heterodyne encrypted signal is at radio frequency and can be directly sent through an antenna to a secure site for digital storage to be prepared for decryption. In the secure site, an identical optical scanning system to that used for encryption is used, together with a decryption key, to generate an electrical signal. The electrical signal is then processed and sent to a computer to be used for decryption. Utilizing the stored information received from the encryption stage and the electrical information from the secure site, a digital decryption unit performs a decryption algorithm. If the encryption key and the decryption key are matched, the decryption unit will decrypt the image or document faithfully. The overall cryptosystem can perform the incoherent optical processing counterpart of the well-known coherent double-random phase-encoding technique. We present computer simulations of the idea. © 2003 Optical Society of America

OCIS codes: 110.0110, 090.0090.

1. Introduction

Cryptography is the practice and study of encryption and decryption.[1] The method of quantum cryptography is based on the use of one of the quantum properties of a photon, i.e., polarization, and has the potential to be absolutely unbreakable.[2,3] However, current practical considerations introduce security loopholes, which eavesdroppers can exploit. Indeed, totally secure communications are far from a reality. On the classical front, optical cryptography, which is also based on photons, has a long-standing history. Recent progress in the development of optical components and systems and their increasingly improved technical performance suggest that optical cryptography has significant potential for security applications. Indeed, a plethora of publications in recent years have dealt with secure systems that use optical methods.[4–12]

One of the reasons for using optical encryption is that information, such as images, that needs to be encrypted exists already in the optical domain. Another reason is that optical encryption, as opposed to electronic or digital encryption, can provide many degrees of freedom for securing information. When large volumes of information, such as a three-dimensional (3-D) object, are to be encrypted,[11,13] the use of optical encryption methods is probably the most logical choice. Whereas most optical encryption techniques are optically coherent, an incoherent optical technique for encryption was proposed recently.[12] However, inverse filtering which spoils the signal-to-noise ratio, has been used for decryption. Nevertheless, in general incoherent optical techniques possess many advantages over their coherent counterparts, such as a better signal-to-noise ratio and insensitivity to misalignment of optical elements.[14]

In this paper we propose a novel incoherent optical method for encryption. In particular, we have investigated the optically incoherent implementation of double-random phase encoding. The method is based on optical heterodyne scanning and has many advantages besides being an incoherent technique. Other advantages are as follows: (1). Because it is an optical scanning method, incoherent objects, such

T.-C. Poon (tcpoon@vt.edu) is with the Optical Image Processing Laboratory, Bradley Department of Electrical and Computer Engineering, Virginia Polytechnic Institute and State University, Blacksburg, Virginia 24061. T. Kim is with the Department of Optical Engineering, Sejong University, 98 Kunja-Dong, Kwangjin-Ku, Seoul 143-747, Korea. K. Doh is with the Department of Telecommunication Engineering, Hankuk Aviation University, 200-1 Hwajeon-dong, Goyang-city, Korea.

Received 30 December 2002; revised manuscript received 11 June 2003.

0003-6935/03/326496-08$15.00/0

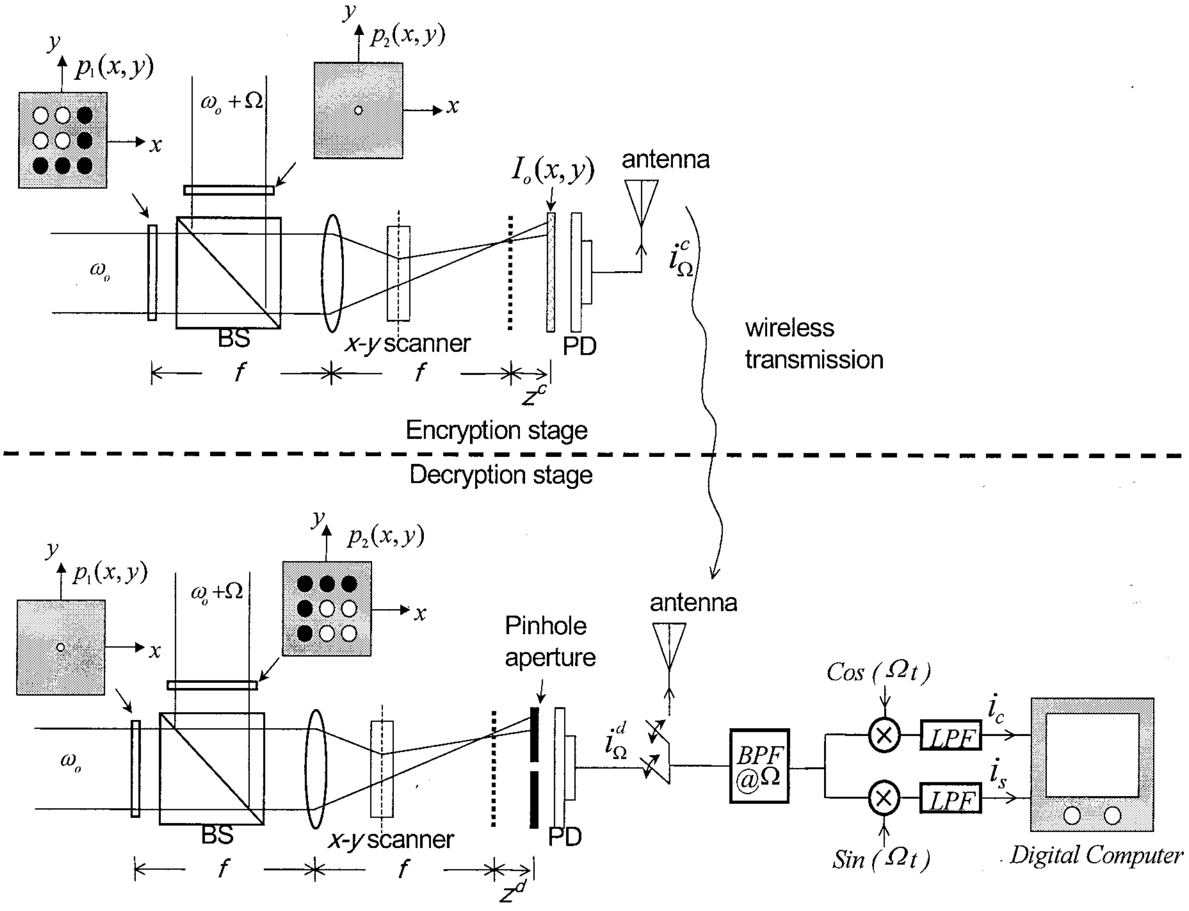

Fig. 1. Optical system for encryption and decryption [$I_0(x, y)$ is the document to be encrypted, $p_1(x, y)$ is the encryption key in the encryption stage, and $p_2(x, y)$ is the decryption key in the decryption stage]: ⊗'s, electronic multipliers; LPFs, low-pass filters; BPF@Ω, bandpass filter tuned at Ω; PDs, photodetectors.

as printed documents, can be directly processed without the need for using spatial light modulators to convert an incoherent image to a coherent image as in the existing coherent techniques cited above. Indeed, the proposed system can perform real-time or on-the-fly encryption. For example, a standard laser scanner, once it is modified according to the proposed technique, can become an on-the-fly optical encryption system. (2). As the output signal is a heterodyne electrical signal and hence the encrypted information is riding on a heterodyne frequency or a carrier frequency as in communications, the signal can be immediately radiated for wireless transmission to a secure site for storage and subsequent encryption. (3). The technique is easily extendible to encryption of 3-D information, as it is based on optical scanning holography.[15] In Section 2 we briefly discuss optical heterodyne scanning, which is the core technique of our proposed cryptosystem. In Sections 3 and 4 we discuss ways in which to perform encryption and decryption, respectively, with the proposed optical scanning technique. In Section 5 we discuss how the proposed encryption system can implement the so-called double-random phase encoding incoherently; i.e., we can work with incoherent objects directly. We provide in Section 6 some computer simulations of the ideas presented. Finally, in Section 7 we give summaries and provide some concluding remarks.

2. Optical Heterodyne Scanning

The cryptosystem includes identical optical systems in the encryption and the decryption stages. We shall therefore describe the optical system in the encryption stage. The optical system is a two-pupil heterodyne scanning system, which has been used extensively for incoherent image processing,[14–17] scanning holographic recording,[15] 3-D microscopy,[18,19] and, more recently, optical recognition of 3-D objects and optical remote sensing.[20–22] Inasmuch as a mathematical description of the two-pupil optical system was recently worked out in detail,[20] we shall briefly describe the system's operation and present some of the results pertinent to the present study.

The encryption stage illustrated in Fig. 1 shows the basic optical heterodyne scanning system. Two pupils, $p_1(x, y)$ and $p_2(x, y)$, located in the front focal planes of the lens, are illuminated by two broad laser beams of temporal frequencies ω_0 and $\omega_0 + \Omega$, respectively. The two beams are then combined by a beam splitter, BS, and used for two-dimensional (2-D) scanning of the object, $I_0(x, y)$, located a distance z^c away from the back focal plane of the lens. The photodetector collects all the light transmitted by the object (or all the scattered light if the object is diffusely reflecting). As the two laser beams are of different temporal frequencies, the photodetector will have a heterodyning current at frequency Ω as one of its outputs (with the other output as a baseband signal). After electronic tuning at Ω, the heterodyne current, $i_\Omega^c(x, y)$, can be isolated and expressed as[20]

$$i_\Omega^c(x, y; z^c) = \mathrm{Re}[i_{\Omega_p}(x, y; z^c)\exp(j\Omega t)], \tag{1}$$

where we have adopted the convention for phasor ψ_p as $\psi(x, y, t) = \mathrm{Re}[\psi_p(x, y, t)\exp(j\Omega t)]$, and Re[ ] denotes the real part of the bracketed quantity. $i_{\Omega_p}(x, y; z^c)$ is the output phasor, which contains the amplitude and the phase information on the heterodyne current and constitutes the scanned and processed version of the object $I_0(x, y)$. It has been shown that the spectrum of i_{Ω_p} is related to the spectrum of $I_0(x, y)$ as follows[20]:

$$\mathcal{F}\{i_{\Omega_p}(x, y; z^c)\} = \mathcal{F}\{I_0(x, y; z^c)\}\mathrm{OTF}_\Omega(k_x, k_y; z^c), \tag{2}$$

where $\mathcal{F}$ denotes the 2-D Fourier-transform operation and is defined as $\mathcal{F}\{u(x, y)\} = \iint u(x, y)\exp(jk_x x + jk_y y)\mathrm{d}x\mathrm{d}y = U(k_x, k_y)$, k_x and k_y denote the spatial frequencies, and uppercase function U denotes the transform of lowercase function u. $\mathrm{OTF}_\Omega(k_x, k_y; z^c)$ is the optical transfer function (OTF) of the heterodyne scanning system and can be expressed in terms of the two processing pupils as[20]

$$\begin{aligned}\mathrm{OTF}_\Omega(k_x, k_y; z^c) = {} & \exp\left[j\,\frac{z^c}{2k_0}\,({k_x}^2 + {k_y}^2)\right] \\ & \times \iint p_1{}^*(x', y')p_2\left[x' + \frac{f}{k_0}\,k_x, y' + \frac{f}{k_0}\,k_y\right] \\ & \times \exp\left[j\,\frac{z^c}{f}(x'k_x + y'k_y)\right]\mathrm{d}x'\mathrm{d}y',\end{aligned} \tag{3}$$

where k_0 is the wave number of the laser and f is the focal length of the lens. Finally, in writing Eq. (2) we deliberately inserted z^c into the argument of I_0 as a parameter to emphasize that the input and output relationship in Eq. (2) refers to a single plane, $z = z^c$. Using Eq. (2) transforms Eq. (1) into

$$\begin{aligned}i_\Omega^c(x, y; z^c) &= \mathrm{Re}[i_{\Omega_p}(x, y; z^c)\exp(j\Omega t)] \\ &= \mathrm{Re}[\mathcal{F}^{-1}\{\mathcal{F}\{I_0(x, y; z^c)\} \\ &\quad \times \mathrm{OTF}_\Omega(k_x, k_y; z^c)\}\exp(j\Omega t)],\end{aligned} \tag{4}$$

where $\mathcal{F}^{-1}$ denotes an inverse 2-D Fourier transform. In Section 3 below, we use Eq. (4), together with Eq. (3), to discuss encryption and decryption concepts. Equation (4) is a general equation that describes the output heterodyne current of the two-pupil optical scanning system. The output current is the scanned and processed version of the scanned input $I_0(x, y; z^c)$. The processing elements are the two pupil functions, $p_1(x, y)$ and $p_2(x, y)$. In other words, by modifying the pupils we will have different processed outputs.

Inspecting Eq. (4), we can see that the processed information is carried by a temporal carrier at frequency Ω, and, if Ω is chosen to be in the radio-frequency domain (which can be done easily through the use of acousto-optic modulators[23]), the processed information can be readily radiated to a secure site for further processing, as shown in Fig. 1. After the secure site receives the processed information from an antenna, the information is further processed electronically as shown in Fig. 1; i.e., the incoming signal is multiplied by $\cos(\Omega t)$ and $\sin(\Omega t)$ and low-pass filtered, yielding two signals, i_c and i_s, respectively, as given by[20]

$$i_c(x, y; z^c) = \mathrm{Re}[\mathcal{F}^{-1}\{\mathcal{F}\{I_0(x, y; z^c)\} \times \mathrm{OTF}_\Omega\}], \tag{5a}$$

$$i_s(x, y; z^c) = \mathrm{Im}[\mathcal{F}^{-1}\{\mathcal{F}\{I_0(x, y; z^c)\} \times \mathrm{OTF}_\Omega\}], \tag{5b}$$

where Im[ ] denotes the imaginary part of the bracketed quantity. If we now add the expression given by Eqs. (5) in the following fashion: $i(x, y; z^c) = i_c(x, y; z^c) + ji_s(x, y; z^c)$, we have a complex expression from which the full amplitude and phase are available:

$$i(x, y; z^c) = \mathcal{F}^{-1}\{\mathcal{F}\{I_0(x, y; z^c)\} \times \mathrm{OTF}_\Omega\}. \tag{6}$$

In passing, it is interesting to point out that the results described above can be used to process intensity images with complex point-spread functions,[17] as the OTF in the expression can be made complex in general.

3. Encryption

To perform encryption on input $I_0(x, y; z^c)$ located a distance z^c away from the back focal plane of the lens at the encryption stage, in general we can manipulate the two pupils, $p_1(x, y)$ and $p_2(x, y)$. As a simple example, we let $p_2(x, y) = \delta(x, y)$, a pinhole, and keep $p_1(x, y)$ as is. We call $p_1(x, y)$ an encryption key and z^c a coding distance. Under these conditions the OTF of the system becomes, according to Eq. (3),

$$\begin{aligned}\mathrm{OTF}_\Omega(k_x, k_y; z^c) = {} & \exp\left[-j\,\frac{z^c}{2k_0}\,({k_x}^2 + {k_y}^2)\right] \\ & \times p_1{}^*\left(\frac{-f}{k_0}\,k_x, \frac{-f}{k_0}\,k_y\right),\end{aligned} \tag{7}$$

and Eq. (6) then becomes

$$\begin{aligned}i(x, y; z^c) = {} & \mathcal{F}^{-1}\left\{\mathcal{F}\{I_0(x, y; z^c)\}\exp\left[-j\,\frac{z^c}{2k_0}\right.\right. \\ & \left.\left.\times ({k_x}^2 + {k_y}^2)\right]p_1{}^*\left(\frac{-f}{k_0}\,k_x, \frac{-f}{k_0}\,k_y\right)\right\},\end{aligned} \tag{8}$$

where $i(x, y; z^c)$ is the coded or encrypted image and can be stored by the digital computer. Note that the spectrum of $I_0(x, y; z^c)$ is multiplied by two terms. As the product of the object's spectrum with the term $\exp[-j(z^c/2k_0)(k_x^2 + k_y^2)]$ translates to holographic recording of the object located z^c away from the lens,[20] we can interpret Eq. (8) as holographic information of the object (or a hologram of the object) encrypted or coded by p_1. This idea of coding holographic information was investigated by Schilling and Poon in the context of optical scanning holography.[24] Now, if we group the object's spectrum with p_1 first, we can interpret it as the object's being encrypted or coded by p_1 and then the encrypted information holographically recorded; i.e., we obtain a hologram of the encrypted document.

4. Decryption

After the object has been coded or encrypted, we need to decode or decrypt it. To do this we turn to the optical system at the secure site. Again, note that the optical system is the same, except in the choice of pupils, and the laser beams now scan a pinhole as an object, i.e., $I_0(x, y; z^d) = \delta(x, y; z^d)$, located a distance z^d away from the back focal plane of the lens at the decryption stage. We call z^d a decoding distance. This time, though, the switch, as shown in Fig. 1, is on the output of the optical system at the secure site. Results in Eq. (6) can be applied again, but with z^c replaced by z^d. Now we choose, for example, $p_1(x, y) = \delta(x, y)$, a pinhole, and keep $p_2(x, y)$ as is. We call $p_2(x, y)$ a decryption key. This choice of pupils gives the following OTF, according to Eq. (3):

$$\mathrm{OTF}_\Omega(k_x, k_y; z^d) = \exp\left[j\,\frac{z^d}{2k_0}\,(k_x^{\,2} + k_y^{\,2})\right] \times p_2\!\left(\frac{f}{k_0}\,k_x, \frac{f}{k_0}\,k_y\right). \tag{9}$$

Using Eq. (6) and the fact that $\mathscr{F}\{I_0(x, y; z^d)\} = 1$, we have

$$i(x, y; z^d) = \mathscr{F}^{-1}\left\{\exp\left[j\,\frac{z^d}{2k_0}\,(k_x^{\,2} + k_y^{\,2})\right] \times p_2\!\left(\frac{f}{k_0}\,k_x, \frac{f}{k_0}\,k_y\right)\right\}. \tag{10}$$

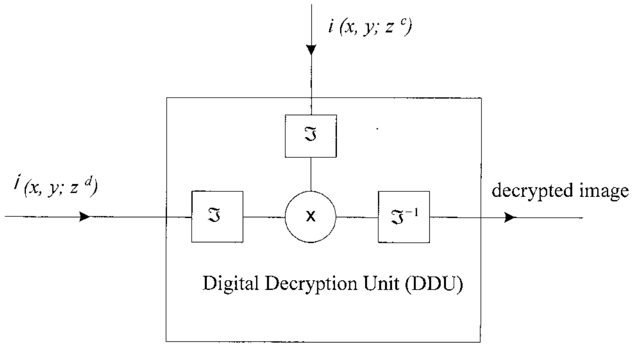

Fig. 2. DDU: $i(x, y; z^c)$, encrypted information with encryption key $p_1(x, y) = \exp[j2\pi M(x, y)]$ inserted into the encryption stage, which is sent from the encryption site by wireless transmission; $i(x, y; z^d)$, signal generated at the decryption stage where decryption key $p_2(x, y) = \exp[j2\pi M(-x, -y)]$ is inserted into the scanning stage to scan a pinhole aperture.

This information is now stored in the digital computer to be used to decrypt the information coming from the encryption site by means of wireless transmission. To decrypt the image from Eq. (8) we propose the use of the digital decryption unit (DDU) shown in Fig. (2). Again, $i(x, y; z^c)$ is the wireless transmitted encrypted information from the encryption stage and $i(x, y; z^d)$ is the information generated at the decryption site. We can see that, at the output of the unit, we have, using Eqs. (8) and (10),

$$\begin{aligned}\text{output of DDU} \propto\ & \mathscr{F}^{-1}\left\{\mathscr{F}\{I_0(x, y; z^c)\}\exp\left[-j\,\frac{z^c}{2k_0}\right.\right.\\ & \left.\left.\times\ (k_x^{\,2} + k_y^{\,2})\right]p_1{}^*\!\left(\frac{-f}{k_0}\,k_x, \frac{-f}{k_0}\,k_y\right)\right\}\\ & \times \exp\left[j\,\frac{z^d}{2k_0}\,(k_x^{\,2} + k_y^{\,2})\right]\\ & \times p_2\!\left(\frac{f}{k_0}\,k_x, \frac{f}{k_0}\,k_y\right)\\ =\ & I_0(x, y; z^c)\end{aligned} \tag{11}$$

if the following conditions are met: (1) $z^d = z^c$ (i.e., the coding distance in the encryption stage and the decoding distance in the decryption stage are the same) and (2) $p_1{}^*(-x, -y)p_2(x, y) = 1$. Condition (1) simply means that the holographic reconstruction is in focus. For any values of $z^d \neq z^c$, we have defocused image reconstruction. Condition (2) allows us choose the functional form of the encryption key, $p_1(x, y)$, in the encryption stage and of the decryption key, $p_2(x, y)$, in the decryption site.

5. Double-Random Phase Encoding

We showed above that encryption of incoherent objects such as printed documents can be performed on the fly by use of optical heterodyne scanning. The encrypted information can be delivered to a secure site by wireless transmission. At the secure site, a digital device can be used for decryption. For the overall cryptosystem to function properly, one of the important conditions, namely, that $p_1{}^*(-x, -y)p_2(x, y) = 1$ as discussed in Section 4, needs to be satisfied, where p_1 is the encryption key and p_2 is the decryption key. It is clear that the choice of phase keys presents a simple and efficient way to satisfy the condition. However, with p_1 chosen as an encryption phase key, the encrypted information in the frequency domain presented in Eq. (8) is basically based on multiplying the Fourier transform of the incoherent image by a pure phase function, namely, $\exp[-j(z^c/2k_0)(k_x{}^2 + k_y{}^2)]p_1{}^*[(-f/k_0)k_x, (-f/k_0)k_y]$. Because the phase of the Fourier transform can be retrieved by phase-retrieval techniques, the system proposed so far is vulnerable to eavesdropping. To overcome this drawback we explore the so-called double-random phase encoding in the context of optical scanning to make the encryption much more secure.

The technique of double-random phase encoding was investigated by Réfrégier and Javidi[25] and by Goudail *et al.*[26] The idea is as follows: The coherent image $f(x, y)$ to be encrypted is multiplied by a random phase mask $\exp[j2\pi r(x, y)]$, and the result is then convolved by a function, which has a phase-only Fourier transform of the form $\exp[j2\pi s(k_x, k_y)]$, to become an encrypted image $\psi(x, y) = f(x, y)\exp[j2\pi r(x, y)] \otimes \mathscr{F}^{-1}\{\exp[j2\pi s(k_x, k_y)]\}$, where $\otimes$ denotes 2-D convolution. As $r(x, y)$ and $s(k_x, k_y)$ are chosen as two independent random functions, one cannot use phase-retrieval techniques to recover the original image just by knowing the encrypted information only. In this section we describe ways in which such double-random phase encoding can be implemented with the present proposed cryptosystem with a simple revision.

Inspecting Eq. (8) we can rewrite the encrypted image in terms of convolution as

$$i(x, y; z^c) = I_0(x, y; z^c) \otimes \mathscr{F}^{-1}\left\{\exp\left[-j\,\frac{z^c}{2k_0}\,(k_x{}^2 + k_y{}^2)\right]\right\} \otimes \mathscr{F}^{-1}\left\{p_1{}^*\left(\frac{-f}{k_0}\,k_x, \frac{-f}{k_0}\,k_y\right)\right\}. \tag{12}$$

We can implement double-random phase encoding if we have the original image $I_0(x, y; z^c)$ multiplied by a random phase mask and then let encryption key $p_1(x, y)$ become a random phase function. We can multiply the original image by a random phase mask simply by directly putting a phase mask $\exp[j2\pi r(x, y)]$ immediately in front of the original image before scanning in the encryption system. Hence the double-random phase-encoding version of the proposed scanning system has an encrypted image of the form

$$\begin{aligned} i(x, y; z^c) = I_0(x, y; z^c)&\exp[j2\pi r(x, y)] \\ &\otimes \mathscr{F}^{-1}\left\{\exp\left[-j\,\frac{z^c}{2k_0}\,(k_x{}^2 + k_y{}^2)\right]\right\} \\ &\otimes \mathscr{F}^{-1}\left\{p_1{}^*\left(\frac{-f}{k_0}\,k_x, \frac{-f}{k_0}\,k_y\right)\right\}. \end{aligned} \tag{13}$$

Note that this encryption is even more secure than the originally proposed double-random phase-encoding idea, as there is an additional parameter, namely, decoding distance z^c, which is still needed for successful decryption, as we demonstrate in Section 6.

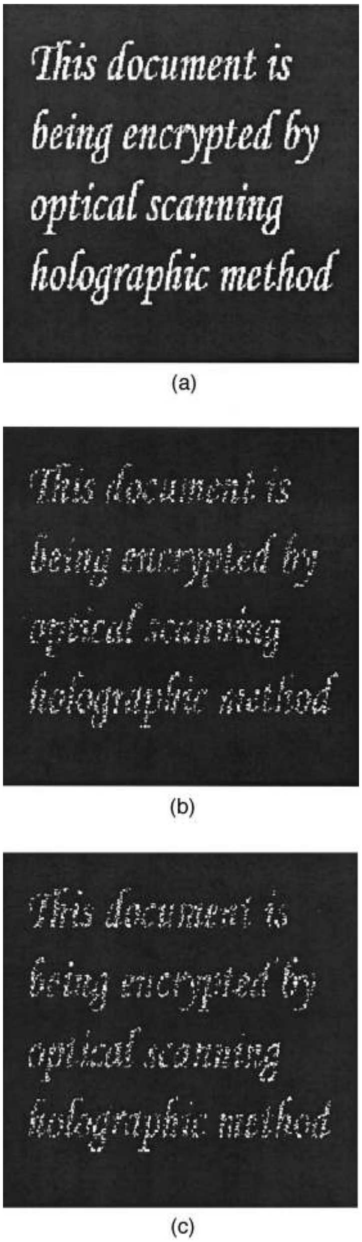

Fig. 3. (a) Original incoherent image; (b) real part of the original document multiplied by a random phase mask $\exp[j2\pi r(x, y)]$ placed immediately in front of the document, not shown in Fig. 1; (c) imaginary part of the original document multiplied by a random phase mask.

6. Simulation Results

As a simple example of manipulating the pupil functions for encryption, we let $p_1(x, y) = \exp[j2\pi M(x, y)]$, where $M(x, y)$ is a function of random numbers chosen from a uniform distribution on the interval (0.0, 1.0). $p_2(x, y) = \delta(x, y)$, a pinhole, in the encryption

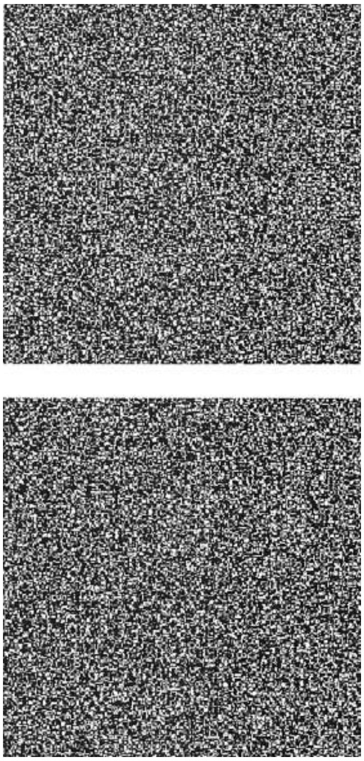

Fig. 4. Top, real and, bottom, imaginary parts of the encryption key, $p_1(x, y) = \exp[j2\pi M(x, y)]$.

stage. For this choice of pupil, according to Eq. (13) we have the encrypted image:

$$i(x, y; z^c) = I_0(x, y; z^c)\exp[j2\pi r(x, y)] \otimes \mathcal{F}^{-1}\left\{\exp\left[-j\,\frac{z^c}{2k_0}\,(k_x{}^2 + k_y{}^2)\right]\right\} \otimes \mathcal{F}^{-1}\left\{\exp\left[-j2\pi M\left(\frac{-fk_x}{k_0}, \frac{-fk_y}{k_0}\right)\right]\right\}, \tag{14}$$

where we have assumed that $r(x, y)$ in Eq. (14) is another function of random numbers, independently of $M(x, y)$ statistically. Figure 3(a) shows the original of the image–document $I_0(x, y; z^c)$ of dimensions 20 mm × 20 mm to be encrypted. Figures 3(b) and 3(c) show the real and the imaginary parts of $I_0(x, y; z^c)\exp[j2\pi r(x, y)]$, respectively. Figure 4 shows the real and the imaginary parts of the random-phase encryption key, $p_1(x, y) = \exp[j2\pi M(x, y)]$, of dimensions 0.8 mm × 0.8 mm, placed in the front focal plane of the lens in the encryption stage. Figure 5 shows the intensity of the encrypted document according to Eq. (14) under the following realistically chosen conditions: focal length f, 10 cm; wavelength of light used λ, 0.6 μm; and finally, $z^c = 30$ cm.

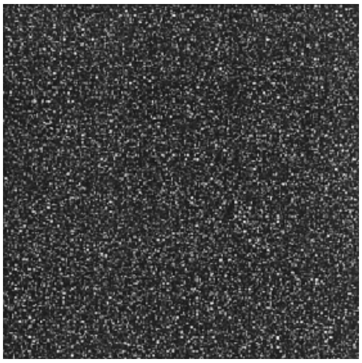

Fig. 5. Intensity of the encrypted document.

For decryption, again, we need to gather information by scanning a pinhole object located z^d away from the back focal plane of the lens when the pupils are $p_1(x, y) = \delta(x, y)$, a pinhole, and $p_2(x, y) = \exp[j2\pi M(-x, -y)]$, satisfying Condition (2) as discussed in Section 5. According to Eq. (10), the scanned output to be stored in the digital computer becomes

$$i(x, y; z^d) = \mathcal{F}^{-1}\left\{\exp\left[j\,\frac{z^d}{2k_0}\,(k_x{}^2 + k_y{}^2)\right] \times \exp\left[j2\pi M\left(\frac{-fk_x}{k_0}, \frac{-fk_y}{k_0}\right)\right]\right\}. \tag{15}$$

When the information from Eqs. (14) and (15) is the input to the DDU, its output, according to Fig. 2, is as follows:

$$\begin{aligned}\text{output of DDU} \propto \mathcal{F}^{-1}\Bigg\{&\mathcal{F}\{I_0(x, y; z^c)\exp[j2\pi r(x, y)]\} \\ &\times \exp\left[-j\,\frac{z^c}{2k_0}\,(k_x{}^2 + k_y{}^2)\right] \\ &\times \exp\left[-j2\pi M\left(\frac{-fk_x}{k_0}, \frac{-fk_y}{k_0}\right)\right] \\ &\times \exp\left[j\,\frac{z^d}{2k_0}\,(k_x{}^2 + k_y{}^2)\right] \\ &\times \exp\left[j2\pi M\left(\frac{-fk_x}{k_0}, \frac{-fk_y}{k_0}\right)\right]\Bigg\} \\ = {}& I_0(x, y; z^c)\exp[j2\pi r(x, y)],\end{aligned} \tag{16}$$

when $z^d = 30$ cm $= z^c$. The decrypted output intensity is shown in Fig. 6(a). If decoding distance z^d is guessed or chosen incorrectly, say, $z^d = 20$ cm, the DDU output is as shown in Fig. 6(b). We can see that the introduction of z^d gives an extra security measure for double-random phase encoding. Finally, in Fig. 7 we use an incorrect random-phase decryption key but with the correct decoding distance for decryption. The key's random phase is statistically independent of the encryption key. It is obvious that it does not work.

7. Concluding Remarks

In summary, we have proposed a method for performing optical scanning cryptography. The image–

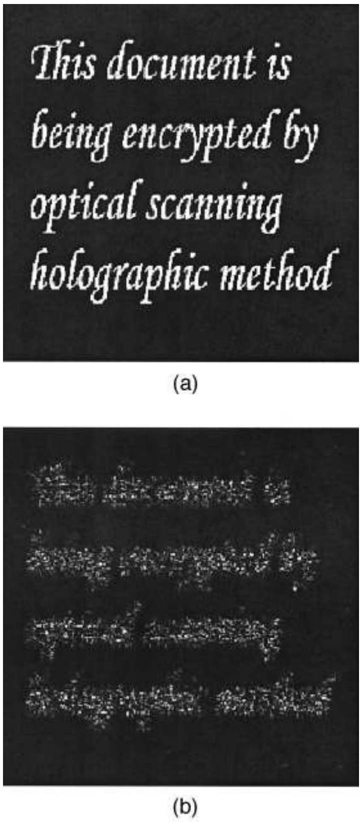

Fig. 6. (a) Intensity of a decrypted document when the decryption key is matched to the encryption key and the decoding distance is the same as the coding distance and (b) when the decoding distance is not the same as the coding distance.

Fig. 7. Intensity of decrypted document when the decryption key is not the same as the encryption key but the decoding distance is matched to the coding distance.

document to be encrypted is scanned optically. Encryption is performed on the fly by a two-pupil optical system based on optical heterodyne scanning, and we have shown that double-random phase encoding can be implemented incoherently with the proposed scanning system. Because the encrypted signal is in the radio-frequency range, the signal can be directly sent to an antenna for wireless transmission to a secure site for decryption. In the encryption stage, one of the pupils is a pinhole and the other is the encryption key of the form of a random phase function, $\exp[j2\pi M(x, y)]$. In the decryption site an identical two-pupil optical system is used, but this time it is scanning a pinhole instead. Again, one of the pupils is a pinhole and the other pupil is the decryption key of the form $\exp[j2\pi M(-x, -y)]$. It is important to point out that the encryption key and the decryption key are of the same functional form and hence are actually the same key. As we can see, once we have the encryption key, we can change it to a decryption key by simply flipping it upon the x axis and then upon the y axis. Therefore, in the present paper we have discussed symmetric key cryptography (SKC); i.e., we are using the same key (the secret key) to encrypt and decrypt a message. In asymmetric key cryptography (AKC), however, the encryption key and the decryption key are not identical.[27] AKC is more efficient and reliable, and it is popularly used in today's security applications. In light of this, it is important that our current proposed method can be extended to work for AKC. So far, we have used a single pupil as an encryption key in the encryption stage and also one pupil as a decryption key in the decryption stage in the proposed two-pupil system. The other pupil in the two stages is just a pinhole. It may be possible to find some suitable pupils other than those pinholes used in the scanning system in such a way that the encryption key and the decryption key are different. Instead of the condition that $p_1{}^*(-x, -y)p_2(x, y) = 1$ be required for decryption in our current SKC scheme, we might come up with other conditions such that AKC can be implemented with the proposed optical system. It is worthwhile looking into this possibility.

T.-C. Poon, T. Kim, and K. Doh express their gratitude for financial support by the National Science Foundation (ECS-9810158), by the Ministry of Information & Communication of the Republic of Korea (C1-2002-072-0-4), and by the Regional Research Center of Korea Science and Engineering Foundation (R12-2001-051-00007-0), respectively. We also thank the reviewers for helpful comments and suggestions.

References

1. S. Singh, *The Code Book* (Random House, New York, 1999).
2. S. Wiesner, "Conjugate coding," SIGACT News **15**(78), 78–88 (1983); original manuscript written and circulated in 1970.
3. C. H. Beneett, C. Brassard, and A. Ekert, "Quantum cryptography," Sci. Am. **269**(10), 26–33 (1992).
4. S. Lai and M. A. Neifeld, "Digital wavefront reconstruction and its applications to image encryption," Opt. Commun. **178,** 283–289 (2000).
5. B. Wang, C.-C. Sun, W.-C. Su, and A. Chiou, "Shift-tolerance property of an optical double-random phase-encoding encryption system," Appl. Opt. **39,** 4788–4793 (2000).
6. B. Zhu, S. Liu, and Q. Ran, "Optical image encryption based on multifractional Fourier transforms," Opt. Lett. **25,** 1159–1161 (2000).
7. P. C. Magensen and J. Gluckstad, "Phase-only optical decryption of a fixed mask," Appl. Opt. **8,** 1226–1235 (2001).
8. H. T. Chang, "Image encryption using separable amplitude-based virtual image and iteratively retrieved phase information," Opt. Eng. **40,** 2165–2171 (2001).

9. T. Nomura and B. Javidi, “Optical encryption system with a binary key code,” Appl. Opt. **39,** 4783–4787 (2000).
10. O. Matoba and B. Javidi, “Secure ultrafast communication using spatial–temporal converters,” Appl. Opt. **39,** 2975–2981 (2000).
11. E. Tajahuerce and B. Javidi, “Encrypting three-dimensional information with digital holography,” Appl. Opt. **39,** 6595–6601 (2000).
12. E. Tajahuerce, J. Lancis, B. Javidi, and P. Andres, “Optical security and encryption with totally incoherent light,” Opt. Lett. **26,** 678–680 (2001).
13. T. Naughton, Y. Frauel, E. Tajahuerce, and B. Javidi, “Compression of digital holograms for three-dimensional object reconstruction and recognition,” Appl. Opt. **41,** 4124–4132 (2002).
14. G. Indebetouw and T.-C. Poon, “Novel approaches of incoherent image processing with emphasis on scanning methods,” Opt. Eng. **31,** 2159–2167 (1992).
15. T.-C. Poon, M. Wu, K. Shinoda, and Y. Suzuki, “Optical scanning holography,” Proc. IEEE **84,** 753–764 (1996).
16. A. W. Lohmann and W. T. Rhodes, “Two-pupil synthesis of optical transfer functions,” Appl. Opt. **17,** 1145–1151 (1978).
17. J. Mait, “Pupil-function design for complex incoherent spatial filtering,” J. Opt. Soc. Am. A **4,** 1185–1193 (1987).
18. T.-C. Poon, “Three-dimensional fluorescence microscopy by optical scanning holography,” Opt. Photon. News **8**(12), 22–23 (1997).
19. J. Swoger, M. Martinez-Corral, J. Huisken, and E. H. K. Stelzer, “Optical scanning holography as a technique for high-resolution three-dimensional biological microscopy,” J. Opt. Soc. Am. A **19,** 1910–1918 (2002).
20. T.-C. Poon and T. Kim, “Optical image recognition of three-dimensional objects,” Appl. Opt. **38,** 370–381 (1999).
21. T. Kim, T.-C. Poon, and G. Indebetouw, “Depth detection and image recovery in remote sensing by optical scanning holography,” Opt. Eng. **41,** 1331–1338 (2002).
22. B. W. Schilling and G. C. Templeton, “Three-dimensional remote sensing by optical scanning holography,” Appl. Opt. **40,** 5474–5481 (2001).
23. A. Korpel, “Acousto-optics,” in *Applied Solid State Science*, R. Wolfe, ed. (Academic, New York, 1972), Vol. 3, pp. 71–75.
24. B. Schilling and T.-C. Poon, “Real-time pre-processing of holographic information,” Opt. Eng. **34,** 3174–3180 (1995).
25. P. Réfrégier and B. Javidi, “Optical image encryption using input and Fourier plane random phase encoding,” Opt. Lett. **20,** 767–769 (1995).
26. F. Goudail, F. Bollaro, B. Javidi, and P. Réfrégier, “Influence of a perturbation in a double phase-encoding system,” J. Opt. Soc. Am. A **15,** 2629–2638 (1998).
27. W. Diffe and M. Hellman, “New directions in cryptography,” IEEE Trans. Inf. Theory **IT-22,** 644–654 (1976).