Journal of the Optical Society of Korea
Vol. 14, No. 2, June 2010, pp. 97-103

DOI: 10.3807/JOSK.2010.14.2.097

QPSK Modulation Based Optical Image Cryptosystem Using Phase-shifting Digital Holography

Seok Hee Jeon

Department of Electronic Engineering, The University of Incheon, Incheon 402-749, Korea

Sang Keun Gil*

Department of Electronic Engineering, The University of Suwon, Suwon 440-600, Korea

(Received April 7, 2010 : revised May 31, 2010 : accepted June 1, 2010)

We propose a new technique for the optical encryption of gray-level optical images digitized into 8-bits binary data by ASCII encoding followed by QPSK modulation. We made an encrypted digital hologram with a security key by using 2-step phase-shifting digital holography, and the encrypted digital hologram is recorded on a CCD camera with 256 gray-level quantized intensities. With these encrypted digital holograms, the phase values are reconstructed by the same security key and are decrypted into the original gray-level optical image by demodulation and decoding. Simulation results show that the proposed method can be used for cryptosystems and security systems.

Keywords : Optical cryptosystem, Digital holography, Phase-shifting interferometry, QPSK modualation
OCIS codes : (090.0090) Holography; (090.2880) Holographic interferometry; (070.0070) Fourier optics and optical signal processing; (070.4560) Optical data processing; (170.3010) Image reconstruction techniques

I. INTRODUCTION

As the digital information network develops rapidly, there has been strong need for information security because personal information is in danger of leakage due to the lack of security provisions. However, most cryptosystems using electronic digital processing have a problem of information cracking. For the purpose of solving this problem, various kinds of optical encryption systems more complicated and rigid against information cracking than electronic digital encryption have been proposed recently.[1-6] In each case the optically encrypted information has complex values, and thus holographic recording may be required. This requirement makes it difficult to store and transmit the encrypted information over a digital network. However, optical encryption and decryption to record and reconstruct the complex values can be easily performed using a phase-shifting digital holographic technique. A phase-shifting digital holographic technique that uses a charge-coupled device(CCD) camera for direct recording of a hologram has an advantage of real time digital information processing without using holographic recording media, and can record the full complex information.[7-18] Phase-shifting digital holography to reconstruct the amplitude and the phase of light is more accurate than off-axis holographic techniques which record digital holograms. The optical encryption and decryption with this phase-shifting digital holographic technique has been well achieved for binary bit data, but is not good for a gray-level optical image. Recently, we proposed an optical encryption of gray-level image using on-axis and 2-f digital holography with 2-step phase-shifting method, in which a gray-level image is changed into binary data by ASCII encoding.[14]

In this paper, we propose a technique for an optical cryptosystem of 256 gray-level optical image by using a quadrature phase shift keying(QPSK) digital modulation method and 2-step phase-shifting digital holography. The basic idea is that we are able to calculate the QPSK modulated phase values from two encrypted digital holograms. A gray-level optical image is digitized into 8-bits binary

*Corresponding author: skgil@suwon.ac.kr
Color versions of one or more of the figures in this paper are available online.

data by ASCII encoding. The 8-bits binary code corresponding to one gray-level value is expressed by four pair of quadrature phase values in a block having 2×2 pixels by QPSK modulation. The converted QPSK phase values and a security key code are displayed on a phase-type SLM(Spatial Light Modulator). The encrypted digital holograms are obtained by interference between an object beam which has the QPSK modulated phase codes and a reference beam which has the security key code, and then 256 gray-level quantized digital holograms are acquired by the CCD. These encrypted digital holograms can be stored by computer and transmitted over a digital network. The QPSK phase values are reconstructed from the encoded digital holograms by the same security key, and the original gray-level optical image is decrypted by ASCII decoding. In section 2, the optical encryption system of the gray-level optical image using QPSK modulation and 2-step phase-shifting digital holography is described. In section 3, we describe computer simulations and results of the encryption and decryption. Finally, conclusions are briefly summarized in section 4.

II. THEORY

2.1. Encryption

Fig. 1 shows the optical setup for encryption with phase-shifting digital holography, which is based on Mach-Zehnder type interferometer architecture. Beam splitter BS1 divides collimated light into two plane waves, the reference and the object beams. With shutter S open and after reflecting in a mirror M1, the object beam illuminates the phase-type SLM(SLM1) which then displays QPSK phases to be encrypted. The output beam from SLM1 is multiplied by a random phase mask, resulting in Fourier transform on CCD by lens L1. The random phase mask widens the dynamic range of the Fourier transform in the spatial frequency domain. The reference beam after being reflected by PZT mirror illuminates the phase-type SLM(SLM 2), where another random phase pattern with a security key code information is displayed, and is Fourier transformed on CCD by lens L2. This concept is analogous to a double-random phase encoding method.[4] However, since the proposed encryption system uses phase masks at the spatial plane instead of placing the phase mask at the spatial frequency plane, it has advantages of requiring less precise alignment and a simpler setup. Also, the code information of the random phase mask pattern used in the object beam can be used simultaneously as the same random phase pattern of the security key code in the reference beam when making a digital interference hologram. But if we use a new random phase pattern of the security key code different from the random phase mask pattern in the object beam, the proposed cryptosystem has a higher level of security with two security keys and is more complicated.

Let $f(x, y)$ be a gray-level optical image function to be encrypted. The 256 gray-level optical image is digitized into 8-bits binary bit data by ASCII encoding method. This 8-bits binary code corresponding to one gray-level value is converted into four pairs of quadrature phase values in a block having 2×2 pixels by binding each two bits from MSB(most significant bit) of 8-bits data and modulating it to QPSK phase values. Fig. 2 shows the

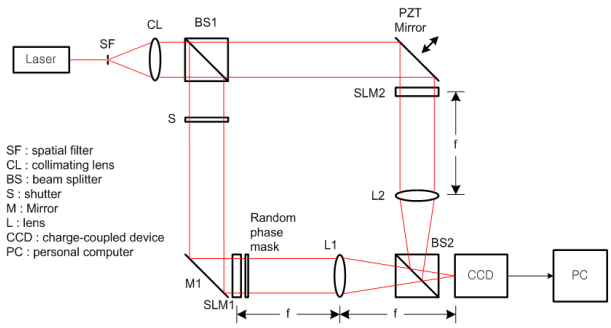


FIG. 1. Optical encryption setup using phase-shifting digital holography.

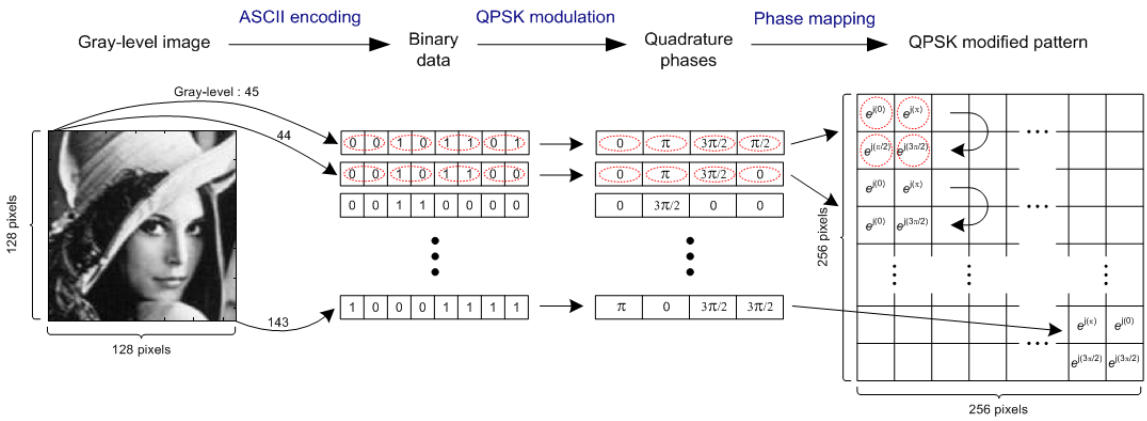


FIG. 2. Procedure of ASCII encoding and QPSK modulation for converting a 256 gray-level optical image into phase values.

converting procedure.

Put $s(x, y)$ be quadrature phase function after encoding $f(x, y)$ into ASCII codes and QPSK digital modulation. In order to display QPSK phase values on the phase-type SLM1, this QPSK phase function have to be represented as

$$a(x,y) = e^{js(x,y)} = e^{j0} \ or \ e^{j\frac{\pi}{2}} \ or \ e^{j\pi} \ or \ e^{j\frac{3\pi}{2}}, \tag{1}$$

where x and y are transversal coordinates at the spatial plane.

Let $k(x, y)$ with individual values equal to 0 or 1, be a binary bit code that can represent a security key. This security key is changed to a binary phase angle $\theta(x, y)=\pi\{1-k(x, y)\}$, which is converted again into a phase pattern function $b(x, y)$ in order to be displayed on the phase-type SLM2.

$$b(x,y) = e^{j\theta(x,y)} = e^{j\pi} \ or \ e^{j0}, \tag{2}$$

If the binary bit code is random, $b(x, y)$ is also random phase pattern. The multiplication of the QPSK phase function with the security key phase pattern function is represented as

$$o(x,y) = a(x,y)b(x,y) = e^{js(x,y)}e^{j\theta(x,y)} = e^{j\{s(x,y)+\theta(x,y)\}}, \tag{3}$$

Fourier transform of $o(x, y)$ is expressed as

$$O(\alpha,\beta) = F\{o(x,y)\} = |O(\alpha,\beta)|e^{j\phi_O(\alpha,\beta)}, \tag{4}$$

where α and β are transversal coordinates at the spatial frequency plane.

The random phase pattern with unit amplitude can be displayed on the phase-type SLM2 and is expressed as

$$r(x,y) = 1 \cdot e^{j\theta(x,y)}, \tag{5}$$

where unit amplitude is implemented optically by a plane wave in the reference beam. The Fourier transform of $r(x, y)$ is expressed as

$$R(\alpha,\beta) = F\{r(x,y)\} = |R(\alpha,\beta)|e^{j\phi_R(\alpha,\beta)}, \tag{6}$$

The digital holographic intensity pattern recorded by CCD camera at the spatial frequency plane is given by

$$\begin{aligned} I(\alpha,\beta) &= |O(\alpha,\beta) + R(\alpha,\beta)|^2 \\ &= |O(\alpha,\beta)|^2 + |R(\alpha,\beta)|^2 \\ &+ 2\sqrt{|O(\alpha,\beta)||R(\alpha,\beta)|}\cos\Delta\phi, \end{aligned} \tag{7}$$

with the reference beam and the object beam given by Eqs. (4) and (6), where $\Delta\phi = \phi_O - \phi_R$ is the phase difference between the object and the reference beams. The precise phase information can not be acquired by intensity information of Eq. (7) alone. In this paper, we use the phase-shifting digital holography. This technique provides the exact reconstruction of the phase difference between the object and the reference beams and amplitudes of these two beams. Two intensity patterns in the form of a digital hologram are achieved by 2-step phase-shifting holography with the reference beam phase shifted by $\phi_i = 0$ and $\pi/2$ for i=1, 2, respectively. The phase shift with phase step of $\pi/2$ is obtained by properly moving the PZT controlled mirror. Another phase shifting technique, instead of moving the mirror, is to use a phase-type SLM, which is electronically controlled to allow phase shift $\pi/2$ in the reference beam. By rewriting Eq. (7), the phase-shifting digital hologram is expressed as

$$I_i(\alpha,\beta) = |O(\alpha,\beta)|^2 + |R(\alpha,\beta)|^2 + 2\sqrt{O(\alpha,\beta)R(\alpha,\beta)}\cos(\Delta\phi - \phi_i). \tag{8}$$

This 2-step phase-shifting digital holography has the merit of a reduced number of holograms compared to multi-step phase-shifting holography. From Eq. (8), 2-step phase-shifting digital holograms are obtained by

$$\begin{aligned} I_1(\alpha,\beta) &= |O(\alpha,\beta)|^2 + |R(\alpha,\beta)|^2 + 2\sqrt{O(\alpha,\beta)R(\alpha,\beta)}\cos\Delta\phi \\ I_2(\alpha,\beta) &= |O(\alpha,\beta)|^2 + |R(\alpha,\beta)|^2 + 2\sqrt{O(\alpha,\beta)R(\alpha,\beta)}\cos(\Delta\phi - \pi/2). \end{aligned} \tag{9}$$

These two digital holograms are encrypted data, which are stored in a computer and transmitted through the digital communication network.

2.2. Decryption

After receiving the digital holograms and manipulating them, the exact retrieval of the original gray-level optical image has to be done with the same security key. With Eq. (9), let $|O(\alpha,\beta)|^2 + |R(\alpha,\beta)|^2$ meaning the DC-term is $A(\alpha, \beta)$ and $2\sqrt{|O(\alpha,\beta)||R(\alpha,\beta)|}\cos\Delta\phi$ meaning the AC-term is $B(\alpha, \beta)$, then Eq. (9) is rewritten by

$$\begin{aligned} I_1(\alpha,\beta) &= A(\alpha,\beta) + B(\alpha,\beta)\cos\Delta\phi \\ I_2(\alpha,\beta) &= A(\alpha,\beta) + B(\alpha,\beta)\cos(\Delta\phi - \pi/2) \\ &= A(\alpha,\beta) + B(\alpha,\beta)\sin\Delta\phi. \end{aligned} \tag{10}$$

After the DC-term $A(\alpha, \beta)$ is removed in Eq. (10), modified holographic intensities are expressed as

$$\begin{aligned} I_1'(\alpha,\beta) &= I_1(\alpha,\beta) - A(\alpha,\beta) = B(\alpha,\beta)\cos\Delta\phi, \\ I_2'(\alpha,\beta) &= I_2(\alpha,\beta) - A(\alpha,\beta) = B(\alpha,\beta)\sin\Delta\phi. \end{aligned} \tag{11}$$

From Eq. (11), the phase difference of the object beam and reference beam is calculated as follows.

$$\frac{I_1'}{I_2'} = \frac{\sin\Delta\phi}{\cos\Delta\phi} = \tan\Delta\phi \quad , \tag{12}$$

$$\Delta\phi = \Delta\phi_O - \Delta\phi_R = \tan^{-1}\left(\frac{I_1'}{I_2'}\right). \tag{13}$$

The DC-term removal is effective for calculating the phase difference easily. Using Eqs. (12) and (13), the magnitude of the AC-term is calculated as follows.

$$A_{OR} = |O(\alpha,\beta)||R(\alpha,\beta)| = \frac{1}{4}\left\{(I_1')^2 + (I_2')^2\right\}. \tag{14}$$

From Eqs. (13) and (14), the complex hologram with encryption information is expressed as

$$H(\alpha,\beta) = A_{OR}\, e^{j\Delta\phi}. \tag{15}$$

In order to get the complex distribution $O(\alpha, \beta)$ and decrypt the original 256 gray-level image, we need the complex distribution $R(\alpha, \beta)$ of the key code phase pattern. Note that it is possible to get $R(\alpha, \beta)$ with knowledge of the phase pattern because the phase pattern is made by the known binary key code. To reconstruct $O(\alpha, \beta)$, we also need the intensity distribution $|R(\alpha,\beta)|$ of the key code phase pattern. The intensity pattern recorded by the CCD camera gives $|R(\alpha,\beta)|^2$ by removing the object beam in Mach-Zehnder interferometer shown in fig. 1, which is done by closing shutter S. Using the complex hologram and the security key code information, the reconstructed complex distribution is obtained by

$$\begin{aligned} G(\alpha,\beta) &= \frac{H(\alpha,\beta)R(\alpha,\beta)}{|R(\alpha,\beta)|^2} = \frac{|O(\alpha,\beta)||R(\alpha,\beta)|e^{j(\phi_O-\phi_R)}|R(\alpha,\beta)|e^{j\phi_R}}{|R(\alpha,\beta)|^2} \\ &= O(\alpha,\beta)e^{j\phi_O}. \end{aligned} \tag{16}$$

By using an inverse Fourier transformation, the information of the object beam is reconstructed and the reconstructed data represents the function $o(x, y)$, which is the multiplication of the original QPSK phase function and the original security key phase pattern function.

$$g(x,y) = F^{-1}\{G(\alpha,\beta\} = F^{-1}\{O(\alpha,\beta)\} = o(x,y) = a(x,y)b(x,y). \tag{17}$$

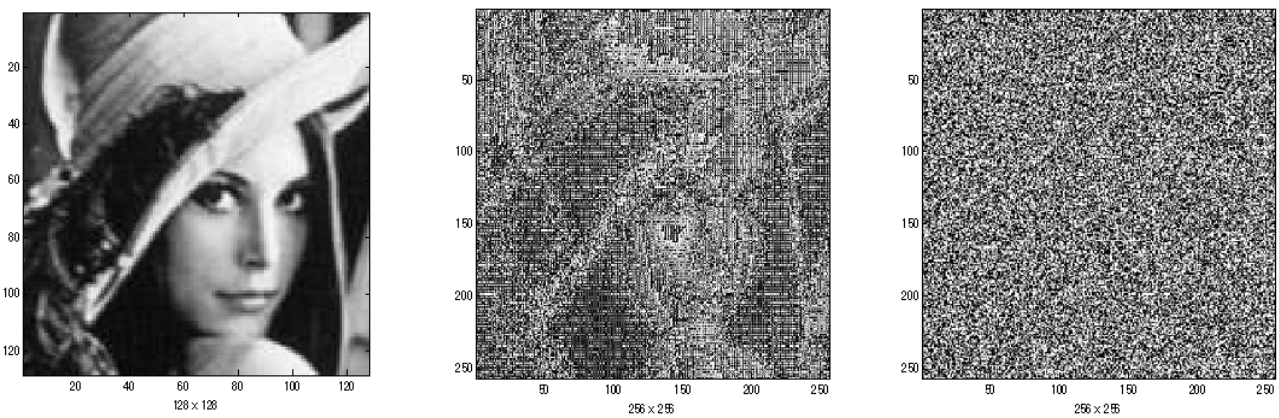
This reconstructed information expressed as Eq. (17) is processed again using the same security key for the purpose of acquiring the original QPSK modulated phase function as follows.

$$p(x,y) = g(x,y)b^*(x,y) = a(x,y). \tag{18}$$

where * means complex conjugate. Therefore, the original 256 gray-level optical image of $f(x, y)$ can be decrypted by ASCII decoding from Eq. (18).

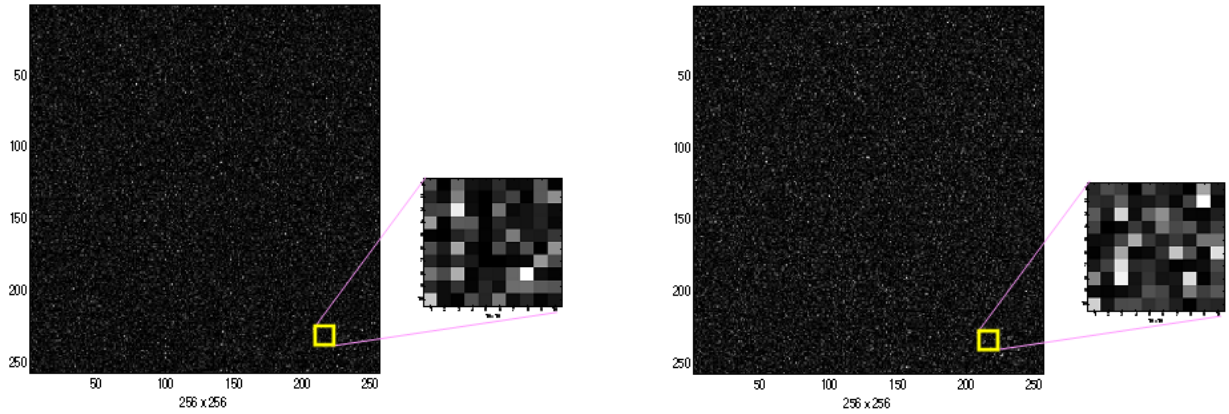
III. COMPUTER SIMULATIONS

We show the performance of the proposed cryptosystem by using computer simulations. The Lena image 128×128 pixels in size with 256 gray levels shown in Fig. 3 (a) is used as the optical image to be encrypted. Fig. 3 (b) represents the converted phase values of the QPSK modulated function. We use an ASCII encoding technique for changing the 256 gray-level Lena image into binary bit data. The 8-bits binary data corresponding to one gray-level value is mapped to four pairs of quadrature phase values and is arranged in a block having 2×2 pixels in a clockwise sequence by QPSK modulation, and the converted data expands to 256×256 pixels in size. Fig. 2 shows the proposed encoding and QPSK digital modulation technique. Fig. 3 (c) shows a random generated security key code for encryption and decryption and has also 256×256 pixels in



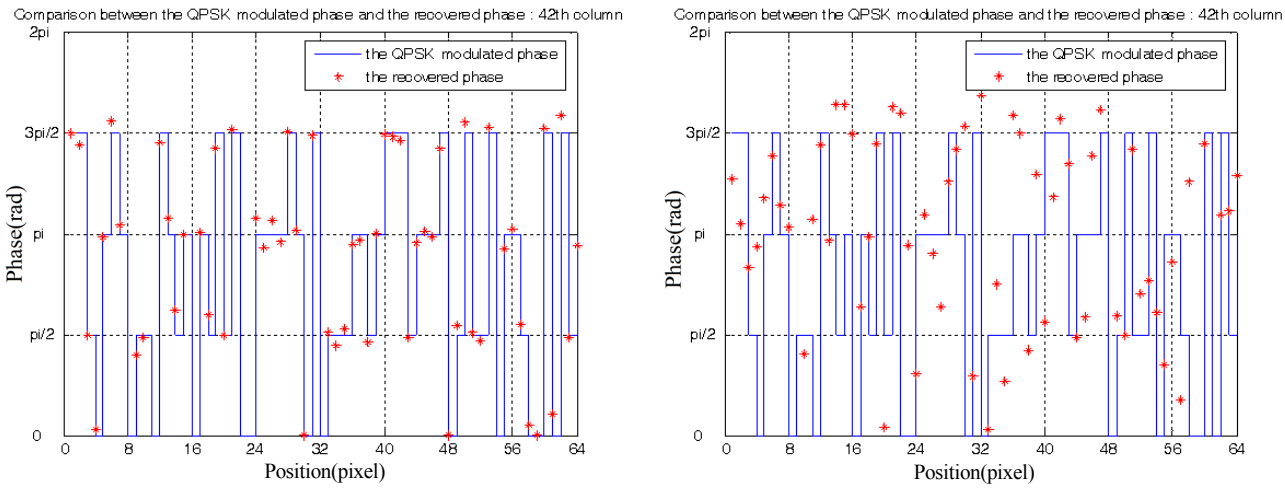
(a) (b) (c)

FIG. 3. Data for computer simulations: (a) a 256 gray-level Lena image to be encrypted(128 × 128 pixels), (b) the converted phase values by using QPSK modulation and ASCII encoding(256 × 256 pixels), (c) a random generated binary key(256 × 256 pixels).



(a) (b)

FIG. 4. Two encrypted digital holograms(256 × 256 pixels) obtained by using 2-step phase-shifting digital holography: (a) intensity pattern of the digital hologram for phase step $\phi_i = 0$, (b) $\phi_i = \pi/2$.



(a) (b)

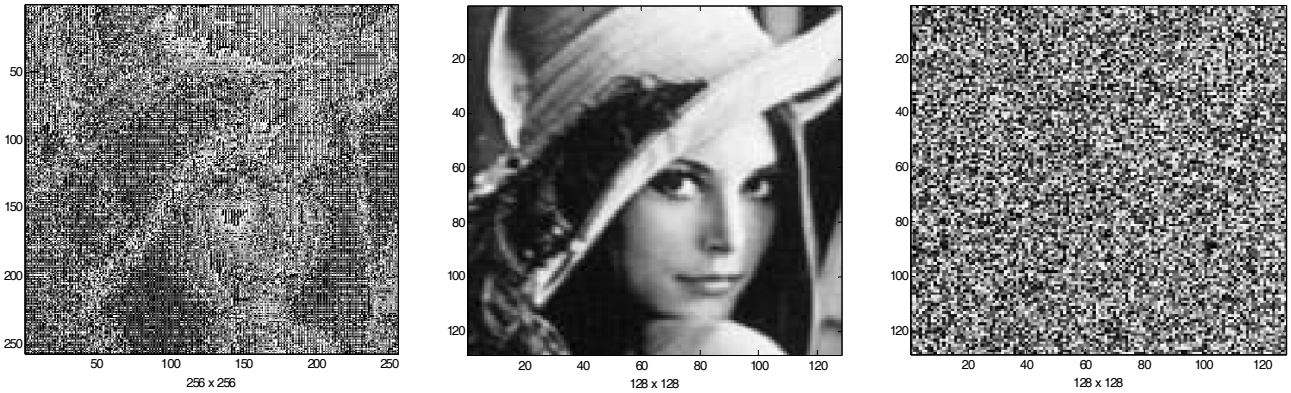
FIG. 5. The encrypted phase generated from gray-level image by QPSK digital modulation and the recovered phase values by the proposed cryptography technique: (a) when the correct security key is used, (b) when the incorrect security key is used.

size, where white areas have value of 1 and black area is 0 numerically. The security key code pattern was generated from a random generator in MATLAB Program.

Fig. 4 shows two encrypted digital holograms using phase-shifting digital holography. Each hologram is quantized with 256 gray levels. From the complex hologram calculated by the encrypted phase and amplitude, reconstruction and decryption of the encrypted phase information are carried out successfully by the same encrypting security key.

Fig. 5 shows the phase difference between the encrypted phases generated from a gray-level image by QPSK digital modulation and the recovered phase values by the proposed cryptosystem. Fig. 5 (a) shows an approximate value of the recovered phase when the correct security key is used, and the exact original quadrature phase value can be reconstructed from the recovered phase value by proper estimation and decision method. Fig. 5 (b) shows an approximate value of the recovered phase when the incorrect security key is used, and some recovered phases are far from the original quadrature phase values.

Fig. 6 shows results of reconstruction and decryption. Fig. 6 (a) is the reconstructed phase values of the image when the correct security key is used, where the exact original quadrature phase values can be obtained from the recovered phase values by proper estimation and decision algorithms. We notice DC-term removal is essential to reconstruct the original phase data for 2-step phase-shifting digital holography. If the incorrect key is used for reconstruction, the original phase values will not be



(a) (b) (c)

FIG. 6. Result of reconstruction and decryption: (a) the reconstructed phase values of the image when the correct security key is used (256 × 256 pixels), (b) the decrypted Lena image after QPSK demodulation and ASCII decoding(128 × 128 pixels), (c) the reconstructed and decrypted image when the incorrect security key is used(128 × 128 pixels).

reconstructed and these phase data will not be decoded into the original Lena image.

IV. CONCLUSION

We propose a new optical cryptosystem of gray-level optical image using QPSK digital modulation method and digital holographic technique with 2-step phase-shifting method. A gray-level optical image is digitized into 8-bits binary bit data by ASCII encoding method and these binary bit data are expressed by four pairs of quadrature phase values in a block having 2×2 pixels by QPSK digital modulation. After ASCII encoding and QPSK modulation, the size of data to be encrypted expands to two times more than the original size of the gray-level optical image. The modified information data with corresponding phase values is displayed on a phase-type spatial light modulator and is encrypted with a security key by using optical digital holography. The security key is expressed with random binary phase. Two-step phase-shifting is implemented by controlling the PZT mirror with phase steps of 0 or $\pi/2$. The proposed system is based on Mach-Zehnder type phase-shifting digital holography, which has advantages of compactness, easy configuration of the optical system, and security improvement. The digital hologram in this method is a Fourier transform hologram and is recorded on a CCD camera with 256 gray-level quantized intensities. For encryption, we use a random phase pattern to enlarge the dynamic range of the Fourier transform hologram in the spatial frequency plane. The random phase that is masking the QPSK modulated phase data with image information and the random phase pattern displayed on the phase-type SLM with the security key code are statistically independent. DC-term removal of the phase-shift digital hologram is performed, which is essential to reconstruct the original phase data in 2-step phase-shifting digital holography. The method using 2-step phase-shifting digital holography is more efficient than the multi-step phase-shifting method because 2-step phase-shifting method produces less data to be transmitted than the multi-step method does. The simulation result demonstrates that the proposed technique is good for encryption and decryption of gray-level optical images and can be used for cryptosystems and security applications systems.

ACKNOWLEDGMENT

This work was supported by University of Incheon Research Grant in 2008.

REFERENCES

1. N. Yoshikawa, M. Itoh, and T. Yatagai, "Binary computer-generated holograms for security applications from a synthetic double-exposure method by electron-beam lithography," Opt. Lett. **23**, 1483-1485 (1990).
2. B. Javidi and J. L. Horner, "Optical pattern recognition for validation and security verification," Opt. Eng. **33**, 1752-1756 (1994).
3. J. F. Heanue, M. C. Bashaw, and L. Hesselink, "Encrypted holographic data storage based on orthogonal-phase-code multiplexing," Appl. Opt. **34**, 6012-6015 (1995).
4. P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. **20**, 767-769 (1995).
5. D. Weber and J. Trolinger, "Novel implementation of nonlinear joint transform correlators in optical security and validation," Opt. Eng. **38**, 62-68 (1999).
6. G.-S. Lin, H. T. Chang, W.-N. Lie, and C.-H. Chuang, "Public-key-based optical image cryptosystem based on data embedding techniques," Opt. Eng. **42**, 2331-2339 (2003).
7. I. Yamaguchi and T. Zhang, "Phase-shifting digital holo-

graphy," Opt. Lett. **22**, 610-612 (1998).
8. E. Cuche, F. Bevilacqua, and C. Depeursinge, "Digital holography for quantitative phase-contrast imaging," Opt. Lett. **24**, 291-293 (1999).
9. E. Tajahuerce, O. Matoba, S. C. Verrall, and B. Javidi, "Optoelectronic information encryption with phase-shifting interferometry," Appl. Opt. **39**, 2313-2320 (2000).
10. G. Unnikrishnan and K. Singh, "Double random fractional Fourier domain encoding for optical security," Opt. Eng. **39**, 2853-2859 (2000).
11. F. Zhang, J. D. R. Valera, and I. Yamaguchi, "Vibration analysis by phase shifting digital holography," Opt. Rev. **11**, 297-299 (2004).
12. S. K. Gil, S. H. Jeon, N. Kim, and J. R. Jeong, "Successive encryption and transmission with phase-shifting digital holography," Proc. SPIE **6136**, 339-346 (2006).
13. S. K. Gil, H. J. Byun, H. J. Lee, S. H. Jeon, and J. R. Jeong, "Optical encryption of binary data information with 2-step phase-shifting digital holography," Proc. SPIE **6488**, 648812 (2007).
14. S. H. Jeon, Y. G. Hwang, and S. K. Gil, "Optical encryption of gray-level image using on-axis and 2-f digital holography with two-step phase-shifting method," Opt. Rev. **15**, 181-186 (2008).
15. P. Hariharan, "Digital phase-shifting interferometry : a simple error compensating phase calculation algorithm," Appl. Opt. **26**, 2504-2505 (1987).
16. P. Hariharan, "Error analysis for optical security by means of 4-step phase-shifting digital hologaphy," J. Opt. Soc. Korea **10**, 118-123 (2006).
17. M.-O. Jeong, N. Kim, and J.-H. Park, "Elemental image synthesis for integral imaging using phase-shifting digital holography," J. Opt. Soc. Korea **12**, 275-280 (2008).
18. D. Kim and Y. J. Cho, "3-D surface profile measurement using an acousto-optic tunable filter based on spectral phase shifting technique," J. Opt. Soc. Korea **12**, 281-287 (2008).