Journal of the Optical Society of Korea, Vol. 10, No. 3, September 2006, pp. 118-123

Error Analysis for Optical Security by means of 4-Step Phase-Shifting Digital Holography

Hyun Jin Lee and Sang Keun Gil*

Department of Electronics Engineering, The University of Suwon, Hwaseong, Gyenggi, 445-743, Korea

(Received September 11, 2006 : revised September 20, 2006)

We present an optical security method for binary data information by using 4-step phase-shifting digital holography and we analyze tolerance error for the decrypted data. 4-step phase-shifting digital holograms are acquired by moving the PZT mirror with equidistant phase steps of $\pi/2$ in the Mach-Zender type interferometer. The digital hologram in this method is a Fourier transform hologram and is quantized with 256 gray level. The decryption performance of the binary data information is analyzed. One of the most important errors is the quantization error in detecting the hologram intensity on CCD. The greater the number of quantization error pixels and the variation of gray level increase, the more the number of error bits increases for decryption. Computer experiments show the results for encryption and decryption with the proposed method and show the graph to analyze the tolerance of the quantization error in the system.

OCIS codes : 070.2580, 070.4560, 090.2880

I. INTRODUCTION

In communication networks such as the Internet and with the rapid spread of mobile terminals shown in fig. 1, there have been strong demands for remote access without intrusions. However, due to the openness and lack of security provisions, a significant private information data such as ID and password for verification and authentication are in danger of leakage. Recently, various kinds of optical processing technology have been proposed for encryption and information security systems [1,2], and authentication and verification [3]. One approach among these technologies is a method to encode an image using a double-random phase mask in the input and Fourier planes [4]. In each case the encrypted information is fully complex, and thus holographic recording may be required. However, this requirement makes it difficult to transmit the encrypted information over communication lines. Digital holographic techniques that use a CCD (Charge Coupled Device) camera for direct capture of a hologram have become available owing to advances in imaging technology [5-7], and it is possible by use of phase-shifting digital interferometry to record the complete complex information [8,13].

In this paper, we introduce a technique for optical encryption of the binary data by use of 4-step phase-shifting digital holography, and we analyze tolerance error for the decryption procedure. The encrypted Fourier transform hologram is obtained by use of one random phase mask attached to input in the object beam and another random phase pattern displayed on a SLM (Spatial Light Modulator) with a key code in the reference beam of an optical setup based on a Mach-Zehnder interferometer. The encrypted digital hologram can be transmitted over a digital communication network. The decryption can be carried out either digitally or optoelectronically.

In section II encryption/decryption with phase-shifting digital holography is described. In section III we analyze the decryption error which can be generated in the proposed system. In section IV computer experiments

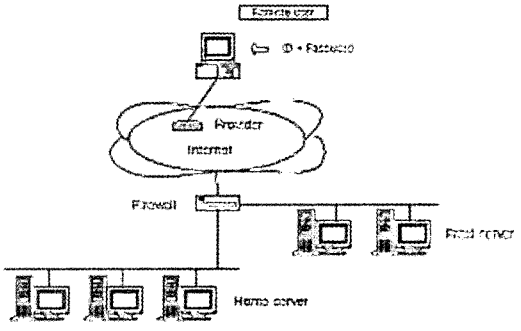


FIG. 1. Computer network system.

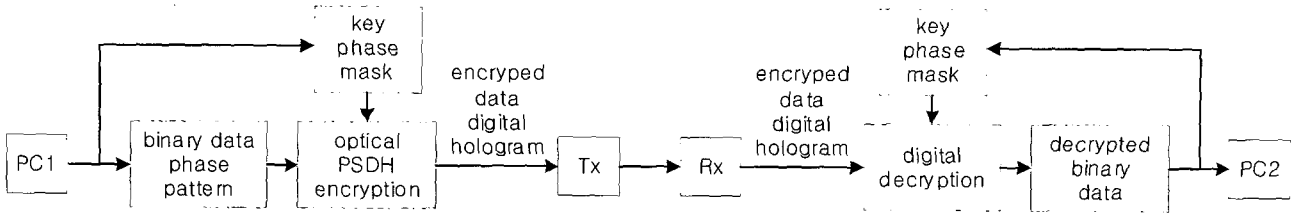


FIG. 2. A schematic for encryption and decryption.

show results of the reconstructed data and the graph to analyze the quantization error. Finally, conclusions are briefly summarized in section V.

II. ENCRYPTION/DECRYPTION METHOD

Fig. 2 shows a transmission schematic for encryption/decryption using 4-step phase-shifting digital holography. Four different encrypted interferograms or holograms are transmitted to the other side terminal. After a reconstruction process with these four encrypted holograms is carried out digitally, the original binary data information is decrypted [9].

Fig. 3 shows the optical setup for the phase-shifting digital holographic system based on Mach-Zehnder interferometer architecture. BS1 divides the collimated light into two plane waves as the object and the reference beams. With shutter S open and after reflecting in a mirror M, the object beam illuminates the input to be encrypted. The binary input information data is expressed on SLM1 and multiplied by a random phase mask. The diffraction pattern through lens L1 is a Fourier transform pattern and is recorded on the CCD camera. At this time a random phase mask improves the dynamic range of the Fourier transform in the spatial frequency plane. Let $a(x,y)$ be an input data to be encrypted, which contains binary bit information, and a function $\exp[j\theta_a(x,y)]$ be a random phase mask, where x and y are transverse coordinates at the input spatial plane. The input function is represented as

$$o(x,y) = a(x,y)\, e^{j\theta_a(x,y)}. \tag{1}$$

Fourier transform of $o(x,y)$ by lens L1 is expressed as

$$O(\xi,\eta) = \mathrm{F}\{o(x,y)\} = |O(\xi,\eta)|\, e^{j\phi_o(\xi,\eta)}, \tag{2}$$

where ξ and η are transverse coordinates at the spatial frequency plane.

The reference beam illuminates SLM2, where a random phase pattern with encryption key information is displayed, after being reflected by the PZT mirror, and is Fourier transformed by lens L2 and is recorded on the CCD camera. Let $b(x,y)$ be a binary key code that can represent a common key or a secret key,

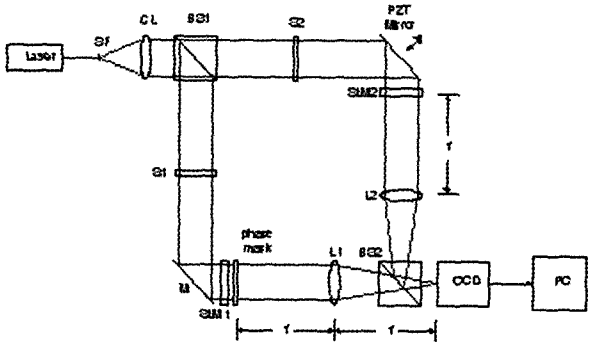


FIG. 3. Optical schematic for encryption; SF, spatial filter; CL, collimating lens; BSs, beam splitter; S, shutter; M, mirror; Ls, lenses; PC, personal computer.

which is multiplied by π (radian) to become a binary phase pattern $\theta_b(x,y) - \pi \cdot b(x,y)$ with $b(x,y)$ equal to 1 or 0. As a result, a phase function $\exp[j\theta_b(x,y)]$ represents the key code phase pattern. If the binary key code is random, $\exp[j\theta_b(x,y)]$ is also a random phase pattern. This random phase pattern with unit amplitude can be displayed on the phase-type SLM and is expressed by

$$r(x,y) = 1 \cdot e^{j\theta_b(x,y)}, \tag{3}$$

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

$$R(\xi,\eta) = F\{r(x,y)\} = |R(\xi,\eta)|\, e^{j\phi_R(\xi,\eta)}. \tag{4}$$

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

$$I(\xi,\eta) = |O(\xi,\eta) + R(\xi,\eta)|^2, \tag{5}$$

with the object beam and the reference beams given by Eqs. (2) and (4), respectively. The phase-shifting holography technique provides the exact reconstruction of the phase difference between the object and the reference beams and the amplitude of these two beams. Four intensity patterns in the form of digital holograms are achieved by 4-step phase-shifting holography with

the reference beam phase shifted by $\phi_i = 0,\ \pi/2,\ \pi$, and $3\pi/2$ for $i = 1,2,3,4$, respectively. The PZT mirror allows phase shifts with equidistant phase steps of $\pi/2$ by moving the mirror. Denoting the phase difference between the object and the reference beams with $\Delta\phi_{OR} = \phi_0 - \phi_R$ and the Fourier transformed reference beam with $R_i(\xi,\eta) = |R_i(\xi,\eta)|e^{j\{\phi_R(\xi,\eta)+\phi_R\}}$, Eq. (5) can be rewritten by

$$I_i(\xi,\eta) = |O(\xi,\eta)|^2 + |R(\xi,\eta)|^2 + 2\sqrt{O(\xi,\eta)\,R(\xi,\eta)}\cos(\Delta\phi_{OR}+\phi_i). \tag{6}$$

In this method, the phase difference can be obtained by

$$\Delta\phi_{OR} = \phi_o - \phi_R = \tan^{-1}\frac{I_2 - I_4}{I_1 - I_3} \tag{7}$$

and the amplitude can also be obtained by

$$A_{OR} = |O(\xi,\eta) \parallel R(\xi,\eta)| = \frac{1}{4}\sqrt{(I_1 - I_3)^2 + (I_2 - I_4)^2}. \tag{8}$$

From Eqs. (7) and (8), the complex hologram can be represented as

$$H(\xi,\eta) = A_{OR}\,e^{J\Delta\phi_{OR}}. \tag{9}$$

In order to obtain the complex distribution $O(\xi,\eta)$ and to decrypt the input data, we need the complex distribution $R(\xi,\eta)$ of the key code phase pattern. Note that it is possible to get $R(\xi,\eta)$ with knowledge of the phase pattern because the phase pattern is made by the known binary key code. The encryption process is performed by using the object beam with a random phase mask and the reference beam with another random phase pattern. The random phase pattern in the reference beam is displayed on the phase-type SLM. This is similar to a double-random phase encoding method. However, since the proposed encryption system uses only one phase mask at the spatial plane in the object beam without placing the phase mask at the spatial frequency plane, it has advantages of a smaller number of phase masks and less precise alignment requirements. To recover $O(\xi,\eta)$, we also need the intensity distribution $|R(\xi,\eta)|^2$ of the key code phase pattern. The intensity pattern recorded by the CCD camera gives $|R(\xi,\eta)|^2$ by removing the object beam in the Mach-Zehnder interferometer, which is done by closing shutter S. The reconstructed complex distribution is obtained by

$$D(\xi,\eta) = \frac{H(\xi,\eta)\,R(\xi,\eta)}{|R(\xi,\eta)|^2} = |O(\xi,\eta)|e^{j\phi_O}. \tag{10}$$

By an inverse Fourier transform, the original input data is decrypted as follows:

$$F^{-1}\{D(\xi,\eta)\} = o(x,y). \tag{11}$$

III. ERROR ANALYSIS

A digital hologram recorded on CCD is quantized with 256 gray levels. So, a gray level error on CCD camera pixels can be generated due to a small intensity variation [10,11]. This error is defined as quantization error, which results in the reconstructed data having wrong bits with respect to the original data [12]. First, the complex hologram which has the error due to gray level variation (Δ) can be represented as

$$H_1(\xi,\eta) = |O_g(\xi,\eta) \parallel R_g(\xi,\eta)|e^{j\Delta\phi_R}, \tag{12}$$

Where $|O_g(\xi,\eta) \parallel R_g(\xi,\eta)| = |O(\xi,\eta) \parallel R(\xi,\eta)| + A_e$, $\Delta\phi_g = (\phi_O - \phi_R) + \phi_e$. A_e and ϕ_e each stand for the errors in amplitude and phase. The reconstructed complex distribution can be obtained by

$$\begin{aligned} D(\xi,\eta) &= \frac{H_1(\xi,\eta)\,R(\xi,\eta)}{|R(\xi,\eta)|^2} \\ &= \frac{|O_g(\xi,\eta) \parallel R_g(\xi,\eta)|e^{j\Delta\phi_R} \cdot |R(\xi,\eta)|e^{j\phi_R}}{|R(\xi,\eta)|^2}, \\ &= O(\xi,\eta)e^{j(\phi_O+\phi_e)} + \frac{A_e e^{j(\phi_O+\phi_e)}}{|R(\xi,\eta)|} \end{aligned} \tag{13}$$

where $\dfrac{A_e e^{j(\phi_O+\phi_e)}}{|R(\xi,\eta)|}$ which generates the error is expressed as $E(\xi,\eta)$. By an inverse Fourier transform of Eq. (13), the original input data is decrypted as follows:

$$\begin{aligned} &F^{-1}\{D(\xi,\eta)\} \\ &= F^{-1}\left\{|O(\xi,\eta)|e^{j(\phi_o+\phi_e)}\right\} + F^{-1}\{E(\xi,\eta)\}. \end{aligned} \tag{14}$$

If $\phi_e = 0$, $A_e = 0$ in Eq. (14), the original input data is exactly decrypted. But if $\phi_e \neq 0$, $A_e \neq 0$, the decrypted data is $d(x,y) = o(x,y) + e(x,y)$, so the data has errors.

In the proposed system the number of error pixels between the original data and the decrypted data is defined as

$$N_e = \sum_{x=1}^{P_X}\sum_{y=1}^{P_Y} |d(x,y) - o(x,y)|^2, \tag{15}$$

where P_X and P_Y are the entire pixel number. Dividing Eq. (15) by P_X and, P_Y MSE (Mean Square Error) fomula is as follows:

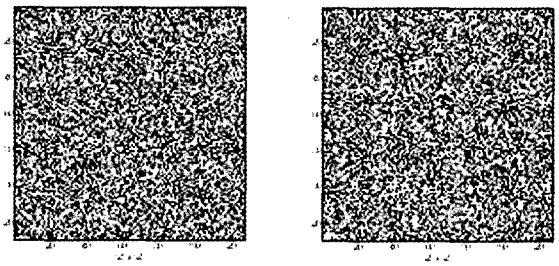
$$MSE = \frac{1}{P_X}\frac{1}{P_Y}\sum_{x=1}^{P_X}\sum_{y=1}^{P_y} |d(x,y) - o(x,y)|^2. \tag{16}$$

IV. COMPUTER EXPERIMENTS

By computer experiments, we show the performance of the proposed encryption system. The binary data of size 128×128 pixels shown in fig. 4 (a) are used as input to be encrypted, and fig. 4 (b) shows a key for encryption and decryption. The binary data and the key code were randomly generated.

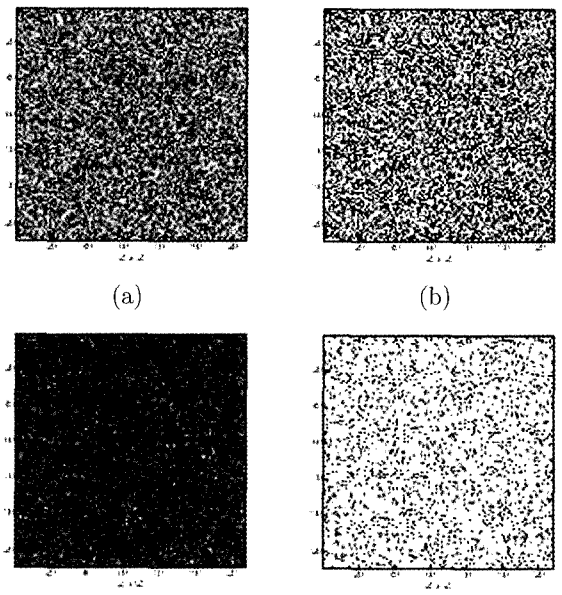
Fig. 5 shows the simulation results. Fig. 5 (a) shows the reconstructed data obtained when the correct key is used for decryption. Fig. 5 (b) shows the decrypted binary data after binarization with the proper threshold, which is exactly the same binary data as the original input data. Fig. 5 (c) shows the reconstructed data obtained when the incorrect key, which has a different phase pattern compared to the one used for encryption, is used for decryption. As shown in fig. 5 (d), the decryption is impossible even if threshold isused.

Fig. 6 and 7 show MSE and the number of error pixels of the decrypted data versus an increment of CCD camera pixels which have a error. The random generated input data and the encryption key shown in fig. 4 are used. All graphs are an average value which is plotted by 100 random evaluations.



(a) (b)

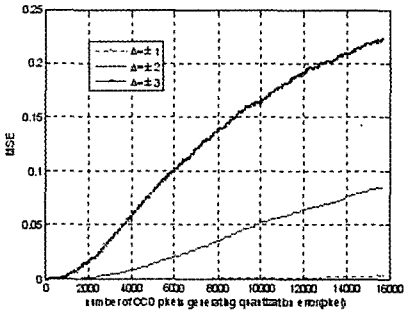
FIG. 4. Original input data to be encrypted and an encryption key for computer simulation (128×128 pixels): (a) a random generated binary bit data, (b) a random generated encryption key.



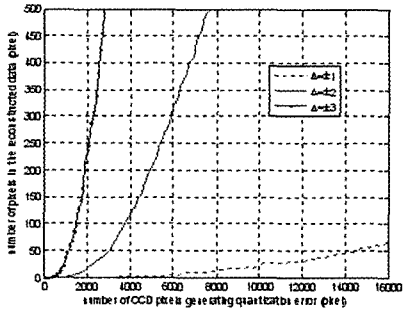
(a) (b)

(c) (d)

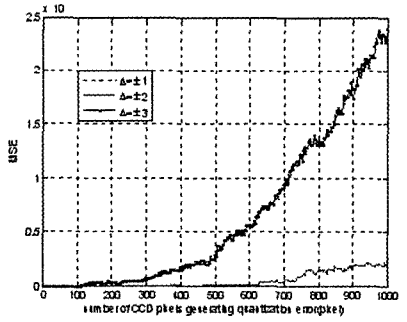
FIG. 5. Simulation results of decryption of the input data (128×128 pixels): (a) reconstructed data with correct key, (b) decrypted data after binarization with proper threshold value, (c) reconstructed data with incorrect key, (d) decrypted data after binarization with threshold value same as (b).



(a)



(b)



(c)

FIG. 6. An error graph of the decrypted data according to the number of CCD camera pixels generating error, when $\Delta = \pm 1, \pm 2, \pm 3$ on 256 gray level CCD camera; average value is plotted by 100 random evaluations: (a) MSE, (b) the number of error pixels, (c) a detailed graph.

Fig. 6 shows the simulation result when the gray level variation ($\triangle$) is ± 1, ± 2, ± 3. As show in (c), when $\triangle = \pm 2, \pm 3$, the decrypted data begins to have errors from about 360 pixels and 100 pixels. In other words the original input data isn't decrypted. When $\triangle = \pm 1$, the error is generated from about 1,600 pixels. $\triangle = \pm 1$ is very robust for the quantization error in this encryption system.

Fig. 7 shows MSE and the number of error pixels about the quantization error when $\triangle = \pm 4, \pm 5, \pm 6$. Fig. 7 (a) shows MSE versus percentage of CCD camera pixels generating the quantiztion error and fig. 7 (b) shows the number of error pixel versus number of CCD camera pixels generating error. As shown in fig. 7 (c), when the gray level variation $\triangle = \pm 4, \pm 5$, the decrypted data begins to have errors each from about 27 pixels and 17 pixels. When $\triangle = \pm 6$, the quantization error is generated since the number of CCD camera pixels generating quantization error is about 11 pixels. This result means that decryption is well performed even though CCD camera pixels generating error have 20 pixels.

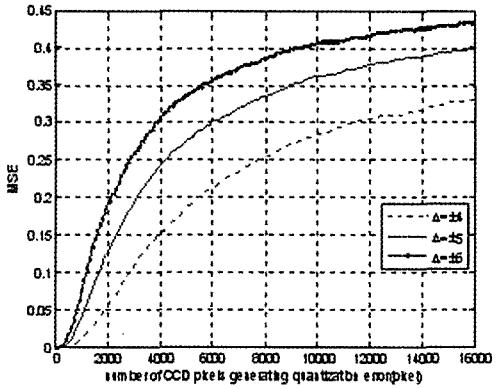
V. CONCLUSIONS

We have proposed an encryption and decryption technique based on 4-step phase-shifting digital holography for a security system. 4-step phase-shifting is implemented by moving the PZT mirror with equidistant phase steps of $\pi/2$. Also, other phase-shifting methods can be used to optically encrypt information. Mach-Zehnder type phase-shifting digital holography and Fourier transform holography have advantages of compactness, easy configuration of the optical system, and security improvement. The digital hologram from this method is a Fourier transform hologram and quantized with 256 gray level. The encrypted data in the form of a digital hologram can be transmitted through communication channels and reconstructed and decrypted digitally. The random phase code that is masking input binary data and the random phase pattern that is displayed on a SLM with the key code are statistically independent. Computer experiments confirmed that the proposed technique is useful for encryption, transmission, and decryption for security applications. The algorithm is suitable for both digital and optical implementation. For $\triangle = \pm 1$ the quantization error begins to be generated since the number of CCD camera pixels generating quantization error is about 1,600 pixels. In other words $\triangle = \pm 1$ is robust for the quantization error in the proposed encryption system. When $\triangle = \pm 6$, the quantization error is generated since the number of CCD camera pixels generating quantization error is about 11 pixels. This result means that the original input data is decrypted even though CCD camera pixels generating error have 11 pixels.

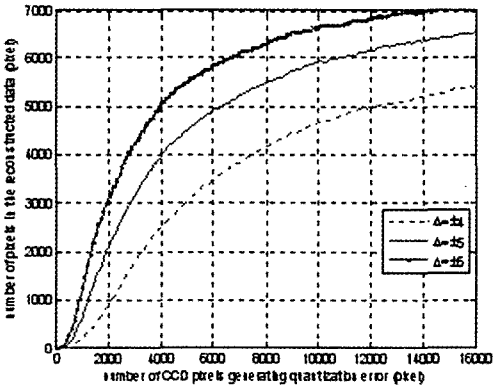
ACKNOWLEDGMENT

This research was supported by grant No. R01-2003-000-10528-0 (2005) from KOSEF.

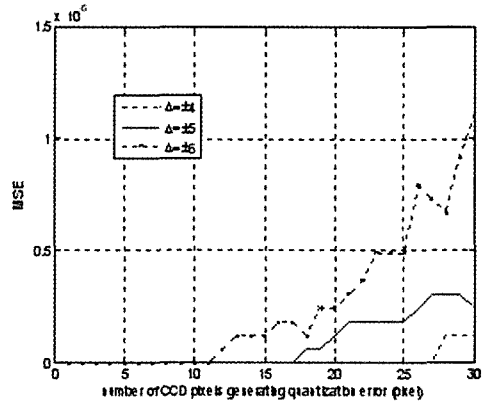
*Corresponding author : skgil@suwon.ac.kr



(a)



(b)



(c)

FIG. 7. An error graph of the decrypted data according to the number of CCD camera pixels generating error, when $\triangle = \pm 4, \pm 5, \pm 6$ on 256 gray level CCD camera; average value is plotted by 100 random evaluations: (a) MSE, (b) the number of error pixels, (c) a detailed graph.

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.*, vol. 23, pp. 1483-1485, 1990.

[2] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding", *Opt. Lett.*, vol. 20, pp. 767-769, 1995.

[3] B. Javidi and J. L. Horner, "Optical pattern recognition for validation and security verification", *Opt. Eng.*, vol. 33, pp. 1752-1756, 1994.

[4] G. Unnikrishnan and K. Singh, "Double random fractional Fourier domain encoding for optical security", *Opt. Eng.*, vol. 39, pp. 2853-2859, 2000.

[5] E. Cuche, F. Bevilacqua, and C. Depeursinge, "Digital holography for quantitative phase-contrast imaging", *Opt. Lett.*, vol. 24, pp. 291-293, 1999.

[6] B. Javidi and T. Nomura, "Securing information by means of digital holography", *Opt. Lett.*, vol. 25, pp. 28-30, 2000.

[7] E. Tajahuerce and B. Javidi, "Encrypting three-dimensional information with digital holography", *Appl. Opt.*, vol. 39, pp. 6595-6601, 2000.

[8] I. Yamaguchi and T. Zhang, "Phase-shifting digital holography", *Opt. Lett.*, vol. 22, pp. 610-612, 1998.

[9] S. K. Gil and S. H. Jeon, "Successive encryption and transmission with phase-shifting", *Proc. of SPIE*, vol. 6136, pp. 22-23, 2006.

[10] S. G. Kim, "Phase error analysis in polarization phase-shifting technique using a wollaston prsim and wave plates", *J. Opt. Soc. Kor.*, vol. 9, pp. 145-150, 2005.

[11] H. L. Sin and H. O. Kim, "The phase sensitivity of the coincidence detection in one output port of a Mach-Zehnder interferometer", *J. Opt. Soc. Kor.*, vol. 9, pp. 169-172, 2005.

[12] H. J. Lee and S. K. Gil, "Error analysis on encryption system with 4-step phase-shifting digital interferometry", *COOC 2006*, 2006.

[13] U. Schnars and W. Jűeptner, *Digital Holography* (Springer, Berlin, Germany, 2005), pp. 37-61.