2-step Phase-shifting Digital Holographic Optical Encryption and Error Analysis

Seok Hee Jeon

Department of Electronic Engineering, The University of Incheon, Incheon 406-772, Korea

Sang Keun Gil*

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

(Received August 23, 2011 : revised September 6, 2011 : accepted September 6, 2011)

We propose a new 2-step phase-shifting digital holographic optical encryption technique and analyze tolerance error for this cipher system. 2-step phase-shifting digital holograms are acquired by moving the PZT mirror with phase step of 0 or $\pi/2$ in the reference beam path of the Mach-Zehnder type interferometer. Digital hologram with the encrypted information is Fourier transform hologram and is recorded on CCD camera with 256 gray-level quantized intensities. The decryption performance of binary bit data and image data is analyzed by considering error factors. One of the most important errors is quantization error in detecting the digital hologram intensity on CCD. The more 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 to be carried out encryption and decryption with the proposed method and the graph to analyze the tolerance of the quantization error in the system.

Keywords : Optical encryption, Digital holography, Phase-shifting interferometry, Cipher system

OCIS codes : (090.0090) Holography; (090.2880) Holographic interferometry; (070.0070) Fourier optics and optical signal processing; (070.4560) Data processing by optical means; (170.3010) Image reconstruction techniques

I. INTRODUCTION

As communication network such as the internet and the mobile net develops, there is a strong need for information security. However, because the communication network is not secure from information cracking, drains of personnel information and abuses of privacy certificates become serious problems. Recently, various kinds of optical processing have been proposed for cipher and security systems.[1-9] In each case the optical 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 digital networks. However, optical encryption and decryption to record and reconstruct the complex values can easily be performed using a phase-shifting digital holographic technique. The 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 not using holographic

recording media, and it can record the full complex information. [10-19] However, when the encrypted information is transmitted, minimizing the amount of data is important for fast data transmission. Therefore, a 2-step phase-shifting digital holographic technique is more efficient than 4-step or multi-step phase-shifting methods because the 2-step method uses less data than multi-step methods to restore or transmit the encrypted data. [15, 16, 18, 20]

In this paper, we propose a technique for optical encryption of the binary data by using 2-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 an SLM (Spatial Light Modulator) with binary data in the object beam and another random phase pattern displayed on an SLM with a security key code in the reference beam of an optical setup based on Mach-Zehnder type interferometer, and a 256 gray-level quantized digital hologram is obtained by the CCD. The encrypted digital hologram can

*Corresponding author: skgil@suwon.ac.kr

Color versions of one or more of the figures in this paper are available online.

be transmitted over a digital communication network. The decryption can be carried out either digitally or optoelectronically. In section II, the encryption technique with 2-step phase-shifting digital holography and error analysis are described. In section III, computer experiments show results of the reconstructed data and the graph to analyze the quantization error. Finally, conclusions are briefly summarized in section IV.

II. THEORY

2.1. Encryption and Decryption

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 S1 open and after reflecting in a mirror M1, the object beam illuminates the phase-type SLM (SLM1) which displays the binary data to be encrypted. The output beam from SLM1 is multiplied by a random phase mask, resulting in a Fourier transform on the CCD by lens L1. The random phase mask improves the signal by widening the dynamic range of the Fourier transform in the spatial frequency domain on the CCD. With shutter S2 open, the reference beam after being reflected by the PZT mirror illuminates the phase-type SLM (SLM 2), where another random phase pattern with a security key code is displayed, and the beam is Fourier transformed on the CCD by lens L2. This concept is analogous to double-random phase encoding. [4] However, since the proposed encryption system uses phase masks at the spatial plane instead of placing the phase mask at the the spatial frequency plane, it has advantages of requiring less precise alignment and simple setup.

Let $r(x, y)$ be a binary code that can represent a security key code. This key code is multiplied by π (radian) to become a binary phase $\theta_r(x, y) = \pi r(x, y)$ if $r(x, y)$ is 1 or 0, where x and y are transversal coordinates at the spatial plane. As a result, a phase function $\exp[j\theta_r(x, y)]$ represents a key code phase pattern. If the binary key code is random, $\exp[j\theta_r(x, y)]$ is also a random phase pattern. This random

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

$$r(x, y) = 1 \cdot e^{j\theta_r(x, y)}, \quad (1)$$

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

$$R(\alpha, \beta) = F[r(x, y)] = |R(\alpha, \beta)| e^{j\phi_r(\alpha, \beta)}, \quad (2)$$

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

Let $|s(x, y)|$ be a binary data to be encrypted and $\exp[j\theta_s(x, y)]$ be a random phase mask, where x and y are transversal coordinates at the input spatial plane. The multiplication of the two is represented as

$$s(x, y) = |s(x, y)| e^{j\theta_s(x, y)}. \quad (3)$$

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

$$S(\alpha, \beta) = |S(\alpha, \beta)| e^{j\phi_s(\alpha, \beta)}. \quad (4)$$

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

$$\begin{aligned} I(\alpha, \beta) &= |S(\alpha, \beta) + R(\alpha, \beta)|^2 \\ &= |S(\alpha, \beta)|^2 + |R(\alpha, \beta)|^2 + 2|S(\alpha, \beta)||R(\alpha, \beta)|\cos\Delta\phi, \end{aligned} \quad (5)$$

with the reference beam and the object beam given by Eqs. (2) and (4), where $\Delta\phi = \phi_s - \phi_r$ is the phase difference between the object and the reference beams. The phase-shifting interferometry method gives the exact reconstruction of the phase difference between the object and the reference beams and amplitude of these two beams. Two intensity patterns in the form of digital holograms are achieved by 2-step phase-shifting digital holography with the reference beam phase shifted by ϕ_i and $\pi/2$ for $i = 1, 2$, respectively. The PZT mirror can allow phase shift with phase steps of $\pi/2$ by moving the mirror. This 2-step phase-shifting digital holography has a merit of the reduced number of holograms compared to multi-step phase-shifting holography. By rewriting Eq. (5), 2-step phase-shifting digital holograms are represented as

$$\begin{aligned} I_1(\alpha, \beta) &= |S(\alpha, \beta)|^2 + |R(\alpha, \beta)|^2 + 2|S(\alpha, \beta)||R(\alpha, \beta)|\cos\Delta\phi \\ I_2(\alpha, \beta) &= |S(\alpha, \beta)|^2 + |R(\alpha, \beta)|^2 + 2|S(\alpha, \beta)||R(\alpha, \beta)|\cos(\Delta\phi - \pi/2). \end{aligned} \quad (6)$$

These two digital holograms are encrypted data, which is

FIG.1. 2-step phase-shifting digital holographic system for Fourier transform encryption of the binary data.

stored in a computer and transmitted through the digital communication network.

With Eq.(6), Let $|S(\alpha, \beta)|^2 + |R(\alpha, \beta)|^2$ meaning DC-term is $A(\alpha, \beta)$, and $2|S(\alpha, \beta)||R(\alpha, \beta)|\cos\Delta\phi$ meaning AC-term is $B(\alpha, \beta)\cos\Delta\phi$, then Eq. (6) is rewritten by

$$\begin{aligned} I_1(\alpha, \beta) &= A(\alpha, \beta) + B(\alpha, \beta)\cos\Delta\phi \\ I_2(\alpha, \beta) &= A(\alpha, \beta) + B(\alpha, \beta)\cos(\Delta\phi - \pi/2) = A(\alpha, \beta) + B(\alpha, \beta)\sin\Delta\phi. \end{aligned} \quad (7)$$

The only object beam intensity recorded on the CCD camera gives $|S(\alpha, \beta)|^2$ by opening the shutter S1 and closing the shutter S2 in the proposed optical setup shown in Fig. 1. Similarly, the only reference beam intensity recorded on the CCD camera gives $|R(\alpha, \beta)|^2$ by opening the shutter S2 and closing the shutter S1 in the optical setup. Then, we can get the DC-term $A(\alpha, \beta)$ by adding these two intensities. These two auxiliary intensities are also transmitted and used for a DC-term removal process. After the DC-term $A(\alpha, \beta)$ is removed in Eq. (7), modified holographic intensities are expressed as

$$\begin{aligned} I_1'(\alpha, \beta) &= I_1(\alpha, \beta) - A(\alpha, \beta) = B(\alpha, \beta)\cos\Delta\phi \\ I_2'(\alpha, \beta) &= I_2(\alpha, \beta) - A(\alpha, \beta) = B(\alpha, \beta)\sin\Delta\phi. \end{aligned} \quad (8)$$

From Eq. (8), the phase difference of the object beam and the reference beam is calculated as follows.

$$\frac{I_1'}{I_2'} = \frac{\sin\Delta\phi}{\cos\Delta\phi} = \tan\Delta\phi, \quad (9)$$

$$\Delta\phi = \Delta\phi_s - \Delta\phi_R = \tan^{-1}\left(\frac{I_1'}{I_2'}\right). \quad (10)$$

DC-term removal is effective for calculating the phase difference easily. Using Eq. (7) and (8), the magnitude of the AC-term is calculated as follows.

$$|S(\alpha, \beta)||R(\alpha, \beta)| = \frac{1}{2}\sqrt{(I_1')^2 + (I_2')^2}. \quad (11)$$

From Eqs. (10) and (11), the complex hologram with encryption information is expressed as

$$H(\alpha, \beta) = |S(\alpha, \beta)||R(\alpha, \beta)|e^{j\Delta\phi}. \quad (12)$$

In order to get the complex distribution $S(\alpha, \beta)$ and decrypt the original binary data, 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. We also need the intensity distribution

FIG. 2. Block diagram of the encryption/decryption procedure: (a) encryption process, (b) decryption process.

$|R(\alpha, \beta)|^2$ of the key code phase pattern in order to reconstruct $S(\alpha, \beta)$. This intensity $|R(\alpha, \beta)|^2$ is acquired when we get the DC-term information by removing the object beam in the optical setup shown in Fig. 1, which is done by closing the shutter S2 and opening the shutter S1. Using the complex hologram and the security key, the reconstructed complex distribution is obtained by

$$\begin{aligned} D(\alpha, \beta) &= \frac{H(\alpha, \beta)R(\alpha, \beta)}{|R(\alpha, \beta)|^2} = \frac{|S(\alpha, \beta)||R(\alpha, \beta)|e^{j(\Delta\phi_s - \Delta\phi_R)}|R(\alpha, \beta)|e^{j\Delta\phi_R}}{|R(\alpha, \beta)|^2} \\ &= S(\alpha, \beta)e^{j\Delta\phi_s}. \end{aligned} \quad (13)$$

By using an inverse Fourier transformation, the data information of the object beam is reconstructed and the original binary data is decrypted after carrying out the proper threshold.

$$d(x, y) = F^{-1}[D(\alpha, \beta)] = F^{-1}[S(\alpha, \beta)] = s(x, y). \quad (14)$$

Fig. 2 shows block diagram of encryption and decryption procedures.

2.2. Error Analysis

A digital hologram recorded on the 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. This error is defined as quantization error, which can cause reconstructed data to have wrong bits with respect to the original data. First, the complex hologram which has the error due to gray-level variation (Δ_g) can be represented as

$$H_1(\alpha, \beta) = |S_g(\alpha, \beta)||R_g(\alpha, \beta)|e^{j\Delta\phi_g}, \quad (15)$$

where $|S_g(\alpha, \beta)||R_g(\alpha, \beta)| = |S(\alpha, \beta)||R(\alpha, \beta)| + A_e$, $\Delta\phi_g =$

$(\phi_s - \phi_R) + \phi_e + \phi_e$. A_e and ϕ_e stand for the errors in amplitude and phase. The reconstructed complex distribution can be obtained by

$$D(\alpha, \beta) = \frac{H_1 \cdot R(\alpha, \beta)}{|R(\alpha, \beta)|^2} = \frac{|S_s(\alpha, \beta)| |R_s(\alpha, \beta)| e^{j\Delta\phi_s} \cdot |R(\alpha, \beta)| e^{j\phi_e}}{|R(\alpha, \beta)|^2} \quad (16)$$

$$= S(\alpha, \beta) e^{j(\phi_s + \phi_e)} + E_1(\alpha, \beta),$$

where $E_1(\alpha, \beta)$ which generates the error is expressed as $\frac{A_e e^{j(\phi_s + \phi_e)}}{|R(\alpha, \beta)|}$. By an inverse Fourier transform of Eq. (16), the original data is decrypted as follows.

$$F^{-1}[D(\alpha, \beta)] = F^{-1}[S(\alpha, \beta) e^{j(\phi_s + \phi_e)}] + F^{-1}[E_1(\alpha, \beta)]. \quad (17)$$

If $\phi_e = 0$, $A_e = 0$ in Eq. (18), the original data is exactly decrypted. But if $\phi_e \neq 0$ or $A_e \neq 0$, the decrypted data is $d(x, y) = s(x, y) + e(x, y)$, so the data has errors.

Next, another error is generated when the original data is decrypted even though an incorrect security key is used. Assume that $r_f(x, y)$ is a false security key with some incorrect pixel values. $R_f(\alpha, \beta)$ is the Fourier transform of $r_f(x, y)$.

$$R_f(\alpha, \beta) = R(\alpha, \beta) + R_e(\alpha, \beta), \quad (18)$$

where $R(\alpha, \beta)$ is the correct security key distribution and $R_e(\alpha, \beta)$ is the complex distribution generating errors. The reconstructed complex distribution can be obtained by

$$D(\alpha, \beta) = \frac{H_1 \cdot R_f(\alpha, \beta)}{|R(\alpha, \beta)|^2} = \frac{|S(\alpha, \beta)| |R(\alpha, \beta)| e^{j\Delta\phi} \cdot R_f(\alpha, \beta)}{|R(\alpha, \beta)|^2} \quad (19)$$

$$= S(\alpha, \beta) e^{j\phi_s} + E_2(\alpha, \beta),$$

where $E_2(\alpha, \beta)$ which generates the error is expressed as

$\frac{|S(\alpha, \beta)| |R(\alpha, \beta)| e^{j\Delta\phi} \cdot R_e(\alpha, \beta)}{|R(\alpha, \beta)|^2}$. By an inverse Fourier transform of Eq. (19), the original data is decrypted as follows.

$$F^{-1}[D(\alpha, \beta)] = F^{-1}[S(\alpha, \beta) e^{j\phi_s}] + F^{-1}[E_2(\alpha, \beta)]. \quad (20)$$

If $R_e(\alpha, \beta)$ in Eq. (18), the original data is exactly decrypted. But if $R_e(\alpha, \beta) \neq 0$, the decrypted data has errors.

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

$$N_E = \sum_{x=1}^{N_X} \sum_{y=1}^{N_Y} |d(x, y) - s(x, y)|^2, \quad (21)$$

where N_X , N_Y are the entire pixel number. Dividing Eq. (21) by N_X and N_Y , MSE (Mean Square Error) formula is as follows.

$$MSE = \frac{1}{N_X} \frac{1}{N_Y} \sum_{x=1}^{N_X} \sum_{y=1}^{N_Y} |d(x, y) - s(x, y)|^2. \quad (22)$$

III. COMPUTER SIMULATIONS

We show the performance of the proposed encryption method by computer simulations. The binary bit and image data of size 128×128 pixels shown in Fig. 3(a) and (b) are used as input data to be encrypted, and Fig. 3(c) shows a phase map of a random generated phase mask pattern for encryption and decryption. We use a random generated binary bit data as general input data because any analog data can be encoded into binary bit data which shows some randomness.

Fig. 4 shows an example of two encrypted digital holograms of the encrypted data shown in Fig. 3(a) or (b) using 2-step phase-shifting digital holography. Each hologram is

FIG. 3. A binary bit or image data to be encrypted and a security key for computer simulations (128×128 pixels): (a) a random generated binary bit data, (b) a binary image data, (c) a phase map of a random generated phase mask pattern, (d) a random generated binary code.

FIG. 4. Example of two encrypted digital holograms(128×128 pixels) with 256 gray levels obtained by using 2-step phase-shifting digital holography: (a) the intensity pattern of the digital hologram for phase step $\phi_i = 0$, (b) $\phi_i = \pi/2$.

FIG. 5. Result of decryption for the binary bit data shown in FIG. 3 (a) when incorrect security key is used(128×128 pixels): (a) a reconstructed data pattern by decryption process, (b) a graph showing the signal bits of the 64th row of the reconstructed data in Fig. 5(a), (c) a graph showing the noise bits of the 64th row of the reconstructed data in Fig. 5(a), (d) a decrypted binary bit data after binarization with the proper threshold value.

FIG. 6. Result of decryption for the binary bit data shown in FIG. 3 (a) when correct security key is used(128×128 pixels): (a) a reconstructed data pattern by decryption process, (b) a graph showing the signal bits of the 64th row of the reconstructed data in Fig. 6(a), (c) a graph showing the noise bits of the 64th row of the reconstructed data in Fig. 6(a), (d) a decrypted binary bit data after binarization with the proper threshold value.

quantized with 256 gray levels. From the complex hologram calculated by the encrypted phase and amplitude and the same encrypting key, reconstruction and decryption of the encrypted data are carried out successfully.

Fig. 5 shows the reconstructed binary data when the incorrect security key is used for decryption, which has a

different phase pattern compared to the one used for encryption. We investigated the distribution of the pixel magnitude of the reconstructed data pattern. One of the cross sections in the reconstructed data is shown in Fig. 5(b) and (c). Since the magnitude of the noise bits (zero value in the original bit data) of some pixels are bigger than the magnitude of

signal bits(one value in the original data), the threshold value cannot be defined. Therefore, the reconstructed data cannot be decrypted into the original bit data.

Fig. 6 shows the reconstructed data when the correct security key is used. The magnitude of signal bits is about 1 in Fig. 6(b), but the magnitude of the noise bits is below about 0.1 for the decryption in Fig. 6(c). Fig.6(d) is the decrypted binary bit data after binarization with the proper threshold value. We notice DC-term removal is

essential to reconstruct the original binary data for our 2-step phase-shifting digital holography.

In a similar way, Fig. 7 and Fig. 8 show the results of decryption for the binary image data shown in FIG. 3 (b) when incorrect or correct security key is used, and show the reconstructed image patterns by decryption process and one of the cross sections in the reconstructed image data.

Fig. 9 shows the results of decryption for the binary image shown in FIG. 3 (b) when the variation of gray-level

FIG. 7. Result of decryption for the binary image data shown in FIG. 3 (b) when incorrect security key is used(128×128 pixels): (a) a reconstructed image pattern by decryption process, (b) a graph showing the signal bits of the 67th row of the reconstructed image in Fig.7(a), (c) a graph showing the noise bits of the 67th row of the reconstructed image in Fig.7(a), (d) a decrypted binary image data after binarization with the proper threshold value.

FIG. 8. Result of decryption for the binary image data shown in FIG. 3 (b) when correct security key is used(128×128 pixels): (a) a reconstructed image pattern by decryption process, (b) a graph showing the signal bits of the 67th row of the reconstructed image in Fig. 8(a), (c) a graph showing the noise bits of the 67th row of the reconstructed image in Fig. 8(a), (d) a decrypted binary image data after binarization with the proper threshold value.

FIG. 9. Result of decryption for the binary image shown in FIG. 3 (b) when the variation of gray-level in CCD quantization is (a) $\Delta_g = \pm 1$, (b) $\Delta_g = \pm 3$, (c) $\Delta_g = \pm 5$, (d) $\Delta_g = \pm 7$.

FIG. 10. Error graphs of the decrypted data according to the number of CCD camera pixels generating error: (a) MSE when $\Delta_g = \pm 1$ (b) the number of error pixels when $\Delta_g = \pm 1$, (c) the number of error pixels when $\Delta_g = \pm 1, \pm 2, \pm 3$.

FIG. 11. An error graph of the decrypted data according to the number of key pixels generating error.

in CCD quantization happens. From the figure, we know that the original binary image cannot be reconstructed as CCD quantization error increases.

Fig. 10 shows MSE and the number of error pixels of the decrypted data versus an increase of CCD camera pixels which have gray level errors for a binary bit data encryption case. The random generated data and the encryption key shown in Fig. 3(a) and (d) are used. All graphs are an average value which is plotted by 100 random evaluations. Fig. 10(b) shows the simulation result when the gray level variation (Δ_g) is ± 1 , and Fig. 10(c) shows the result when Δ_g is $\pm 1, \pm 2, \pm 3$, respectively. As shown in Fig. 10 (b) and (c), when $\Delta_g = \pm 1$, the decrypted data begins to have errors from about 3,500 pixels, and when $\Delta_g = \pm 2, \pm 3$, the decrypted data begins to have errors from about 600 pixels and 150 pixels. In other words the original data is not decrypted. The more the number of quantization error pixels and the variation of gray level Δ_g increase, the more the number of error bits increases for decryption. In our system, $\Delta_g = \pm 1$ is very robust for the quantization error in this encryption system.

Fig. 11 shows the number of error pixels of the decrypted data versus an increase of error pixels of the security key for the case of a binary bit data encryption. The graph is also plotted by an average value which is obtained by 100 random evaluations. As show in Fig. 11, even though about 6 error pixels exist in the key compared to the correct key, the original bit data is decrypted completely. However, this error is very minor because the portion of 6 pixels error is only about 0.04% of the total key size of 128×128 pixels. When 10 error pixels exist in the key, the decrypted data has errors in about 9 pixels. This means that about 99.94% of the original data size of 128×128 pixels is reconstructed when the key has 0.06% error.

IV. CONCLUSION

We propose a new optical encryption method based on 2-step phase-shifting digital holography for a security system. 2-step phase-shifting is implemented by controlling the PZT mirror with phase steps of 0 or $\pi/2$. Fourier transform holography and Mach-Zehnder type phase-shifting digital holography have advantages of compactness and easy configuration of the optical system. The digital hologram from this method is a Fourier transform hologram, quantized with 256 gray-level. The random phase pattern that is masking the binary data/image and another random phase pattern that is displayed on a SLM with the security key code are statistically independent. We remove the DC-term of the phase-shift digital holograms. DC-term removal is essential to reconstruct the original binary data in 2-step phase-shifting digital holography. The magnitude of signal bits is about 1, but the magnitude of the noise bits is below about 0.1 for the binary bit data. The decryption performance of the proposed technique is analyzed in case that errors generate in recording digital holograms on CCD. The more the number of quantization error pixels and the variation of gray level increase, the more the number of error bits increases for decryption. The error pixels of the

reconstructed data are generated when the number of error pixels is over 3,500 and the variation of gray-level is ± 1 in CCD quantization. In case of decryption using an incorrect security key, the error pixels of the reconstructed data are generated when the incorrect key differs from the original key by more than 6 pixels. The method using 2-step phase-shifting digital holography is more efficient than 4-step phase-shifting digital holography system, because 2-step phase-shifting digital holography system requires less data than 4-step phase-shifting digital holography system for data transmission. Computer experiments verify that the proposed method is good for encryption and decryption for security applications. The algorithm is suitable for digital, optical implementation and communication systems.

ACKNOWLEDGMENT

This work was supported by University of Incheon Research Grant in 2009.

REFERENCES

1. B. Javidi and J. L. Horner, "Optical pattern recognition for validation and security verification," *Opt. Eng.* **33**, 1752-1756 (1994).
2. 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).
3. P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Opt. Lett.* **20**, 767-769 (1995).
4. B. Javidi, A. Sergent, and E. Ahouzi, "Performance of double phase encoding encryption technique using binarized encrypted images," *Opt. Eng.* **37**, 565-569 (1998).
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. E. Cucho, F. Bevilacqua, and C. Depeursinge, "Digital holography for quantitative phase-contrast imaging," *Opt. Lett.* **24**, 291-293 (1999).
7. B. Javidi and T. Nomura, "Securing information by means of digital holography," *Opt. Lett.* **25**, 28-30 (2000).
8. G. Unnikrishnan and K. Singh, "Double random fractional Fourier domain encoding for optical security," *Opt. Eng.* **39**, 2853-2859 (2000).
9. 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).
10. U. Schnars and W. Jueptner, "Direct recording of holograms by a CCD target and numerical reconstruction," *Appl. Opt.* **33**, 179-181 (1994).
11. P. Hariharan, "Digital phase-shifting interferometry : a simple error compensating phase calculation algorithm," *Appl. Opt.* **26**, 2504-0505 (1987).
12. I. Yamaguchi and T. Zhang, "Phase-shifting digital holography," *Opt. Lett.* **22**, 610-612 (1998).
13. H. J. Lee and S. G. Gil, "Error analysis for optical security by means of 4-step phase-shifting digital holography," *J. Opt. Soc. Korea* **10**, 118-123 (2006).
14. 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).
15. 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).
16. J.-P. Liu, T.-C. Poon, G.-S. Jhou, and P.-J. Chen, "Comparison of two-, three, and four-exposure quadrature phase-shifting holography," *Appl. Opt.* **50**, 2443-2450 (2011).
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. 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).
19. S. H. Jeon and S. K. Gil, "Measurement of a mirror surface topography using 2-frame phase-shifting digital interferometry," *J. Opt. Soc. Korea* **13**, 245-250 (2009).
20. S. H. Jeon and S. K. Gil, "QPSK modulation based optical image cryptosystem using phase-shifting digital holography," *J. Opt. Soc. Korea* **14**, 97-103 (2010).