Current Optics and Photonics
Vol. 3, No. 2, April 2019, pp. 119-127

ISSN: 2508-7266(Print) / ISSN: 2508-7274(Online)
DOI: https://doi.org/10.3807/COPP.2019.3.2.119

Secret-key-sharing Cryptosystem Using Optical Phase-shifting Digital Holography

Seok Hee Jeon[1] and Sang Keun Gil[2]*

[1]*Department of Electronic Engineering, Incheon National University, Incheon 22012, Korea*
[2]*Department of Electronic Engineering, The University of Suwon, Whasung 18323, Korea*

(Received February 4, 2019 : revised March 31, 2019 : accepted April 3, 2019)

A new secret-key-sharing cryptosystem using optical phase-shifting digital holography is proposed. The proposed secret-key-sharing algorithm is based on the Diffie-Hellman key-exchange protocol, which is modified to an optical cipher system implemented by a two-step quadrature phase-shifting digital holographic encryption method using orthogonal polarization. Two unknown users' private keys are encrypted by two-step phase-shifting digital holography and are changed into three digital-hologram ciphers, which are stored by computer and are opened to a public communication network for secret-key-sharing. Two-step phase-shifting digital holograms are acquired by applying a phase step of 0 or $\pi/2$ in the reference beam's path. The encrypted digital hologram in the optical setup is a Fourier-transform hologram, and is recorded on CCDs with 256 quantized gray-level intensities. The digital hologram shows an analog-type noise-like randomized cipher with a two-dimensional array, which has a stronger security level than conventional electronic cryptography, due to the complexity of optical encryption, and protects against the possibility of a replay attack. Decryption with three encrypted digital holograms generates the same shared secret key for each user. Schematically, the proposed optical configuration has the advantage of producing a kind of double-key encryption, which can enhance security strength compared to the conventional Diffie-Hellman key-exchange protocol. Another advantage of the proposed secret-key-sharing cryptosystem is that it is free to change each user's private key in generating the public keys at any time. The proposed method is very effective cryptography when applied to a secret-key-exchange cryptosystem with high security strength.

Keywords : Optical encryption, Phase-shifting digital holography, Cryptography, Secret key sharing, Secret key exchange
OCIS codes : (060.4785) Optical security and encryption; (090.1995) Digital holography; (090.2880) Holographic interferometry; (070.0070) Fourier optics and optical signal processing; (070.4560) Data processing by optical means

I. INTRODUCTION

Recently, information security of the public network has become a much more important issue, as public networks develop. However, digital information on the public network tends to be insecure against unauthorized attack, because of the fast development of computers. To maintain information security in a communication network, various kinds of encryption algorithms have been introduced for cryptosystems. In general, an electronic encryption system requires much time to compute the encryption procedure, if the encryption key is long and the message is large. On the contrary, an optical encryption system has the advantages of fast computation and vast data handling, owing to the inherent two-dimensional (2-D) parallel signal-processing capability. Another advantage of the optical encryption system is that a large key length can be made easily with the 2-D format, rendering brute-force attacks almost impossible. For these reasons, various cryptosystems using optical methodology have been increasingly studied in recent years. Since an optical encryption method using double-random-phase encoding (DRPE) was proposed [1], a variety of encryption systems based on DRPE have been developed

*Corresponding author: skgil@suwon.ac.kr, ORCID 0000-0002-3828-0939
Color versions of one or more of the figures in this paper are available online.

over the past two decades by applying it to the fractional Fourier transform [2], discrete cosine transform [3], Fresnel domain [4], gyrator transform domain [5], and photon counting [6] to enhance cryptosystem security. In addition, optical encryption with coherent diffractive imaging [7], 3-D phase-retrieval [8], and phase-truncated strategy [9] for optical encryption have been established. Multiple-image encryption [10] is also a new optical encryption method. Another example of progress in optical security systems is the combination of optical and digital encrypting techniques that are based on joint transform correlators (JTC) [11], digital holography [12, 13], or optical XOR logic-operation techniques [14-16]. Moreover, polarization encryption [17, 20] has been reported as an optical encryption method.

For the purpose of establishing a secure encryption system, the most important thing is that the encryption key must not be known to unauthorized persons, and must be hard to break by attacks. A symmetric private-key algorithm such as DES (Data Encryption Standard) carries the risk that attackers may cryptanalyze the symmetric key, because this type of cryptosystem has only one key. To solve this problem, asymmetric cryptography such as the Diffie-Hellman (D-H) secret-key-sharing algorithm was introduced [18]. In this protocol, two users who are unknown to each other can open a public key for their asymmetric key-exchange cryptosystem and share a secret key together. However, this shared secret key can be revealed by a "meet in the middle" attack, because this shared secret key is used to encrypt messages by applying symmetric cryptography. Therefore, to realize a higher level of security, an advanced algorithm using a double-key encryption technique must be introduced as a method of solving this problem.

In our recent studies of optical encryption systems, modified D-H secret-key-exchange algorithms using Boolean-logic-based optical operations were reported [15, 16]. In this paper, an application to an optical secret-key-sharing cryptosystem using phase-shifting digital holography and its optical implementation are proposed. The objective of this paper is to present and verify the feasibility and effectiveness of the proposed optical system for secret-key-exchange cryptography. Section II describes the proposed secret-key-sharing cryptography algorithm based on the D-H secret-key-sharing protocol, and the optical implementation of the proposed cryptosystem. In Section III, the feasibility of the proposed optical system and the performance of applying it to a secret-key-sharing cryptosystem are proven by computer simulations. Finally, the conclusions are briefly summarized in Section IV.

II. THEORY

The secret-key-sharing algorithm introduced by Diffie and Hellman in 1976 [18] is a kind of public-key cryptographic method for two users to exchange their encrypted private keys by generating a shared secret key over a public communication network, without any prior secrets between them. As a result, plain messages can be encrypted into cipher messages by using this symmetric shared secret key. In this protocol, two users agree upon and make public two numbers g and p, where g is called a generator and p is a prime number. Both generate public keys by modulo-arithmetic computing with a generator g, a prime number p, and their own private keys. With this public key, two users generate a shared secret key by modulo-arithmetic computing. Figure 1(a) shows the Diffie-Hellman key-exchange algorithm. However, the D-H secret-key-sharing algorithm may have two problems in implementation with optical techniques. The first is how to implement modulo arithmetic in the D-H secret-key-sharing algorithm by optical methods. The second is to the difficulty of representing a prime number properly with an optical device. Despite these problems, an optical secret-key-sharing cryptosystem is proposed by modifying the conventional D-H secret-key-sharing algorithm [21]. In the proposed cryptosystem, the first problem can be solved by replacing the mathematical modulo-arithmetic encryption with an optical phase-shifting digital holographic encryption process, and the second problem can be solved by using random-number encryption instead of prime-number encryption. Therefore, an optically realizable secret-key-sharing cryptosystem is implemented by the phase-shifting digital holographic encryption method, which is regarded as a kind of block encryption. Specifically, this encryption concept is perfectly secure if and only if the key data are perfectly random and never reused.

In the conventional D-H secret-key-sharing cryptosystem, the main drawback of this algorithm is that it suffers from the "meet in the middle" attack problem. This implies that the authenticity of private keys is essential. If we turn the private-key information into double-encrypted information by pre-encrypting the private key with a shared random number, then enhanced security strength will be acquired, although attackers may know the encrypted private-key information and the common key opened to the public. In this paper, a new optical secret-key-sharing cryptosystem combined with pre-encryption and phase-shifting holographic encryption is proposed with this idea. The pre-encryption to enact double encryption is carried out by applying the optical XOR logic operation before the phase-shifting digital holographic encryption. The proposed secret-key-sharing cryptographic algorithm can be described as follows.

Two users share a common key number k and a generator g, where k and g are generated randomly, instead of being prime numbers. Note that these numbers are open to the public; anyone can access them.

One user A chooses a random number p_A as a private key, where this private key number is kept secret in public network. The private key should be chosen at random for security purposes. User A computes $g \oplus p_A$ by Boolean XOR logic. Next, user A computes public-key ciphers by digital holographic encryption $E(g \oplus p_A)$ using the common key k, and sends them to another user B.

$$c_A = E(g \oplus p_A) \text{ by common key } k. \quad (1)$$

Similarly, user B chooses a random number p_B as a private key, where this private key number is kept secret in public network. This private key, too, should be chosen at random for security purposes. User B computes $g \oplus p_B$ by Boolean XOR logic. Next, user B computes public-key ciphers by digital holographic encryption $E(g \oplus p_B)$ using the common key k, and sends them to user A.

$$c_B = E(g \oplus p_B) \text{ by common key } k. \quad (2)$$

User A decrypts user B's private-key information of $g \oplus p_B$ with the same common key k by computing the holographic reconstruction $D(c_B)$.

$$g \oplus p_B = D(c_B) \text{ by common key } k. \quad (3)$$

Similarly, user B decrypts user A's private-key information of $g \oplus p_A$ with the same common key k by computing the holographic reconstruction $D(c_A)$.

$$g \oplus p_A = D(c_A) \text{ by common key } k. \quad (4)$$

User A computes a shared secret key by Boolean XOR logic with user A's own private key p_A.

$$s_{BA} = \{g \oplus p_B\} \oplus p_A. \quad (5)$$

Similarly, user B computes a shared secret key by Boolean XOR logic with user B's own private key p_B.

$$s_{AB} = \{g \oplus p_A\} \oplus p_B. \quad (6)$$

Now both users have the same shared secret key, namely s.

$$s = s_{BA} = s_{AB} = g \oplus p_A \oplus p_B. \quad (7)$$

Figure 1(b) shows the proposed secret-key-sharing cryptosystem algorithm, and Fig. 2 shows the flow charts of the procedure for the proposed secret-key-sharing method. As shown in Figs. 1 and 2, the first step is pre-encryption of the user's private key with generator g.

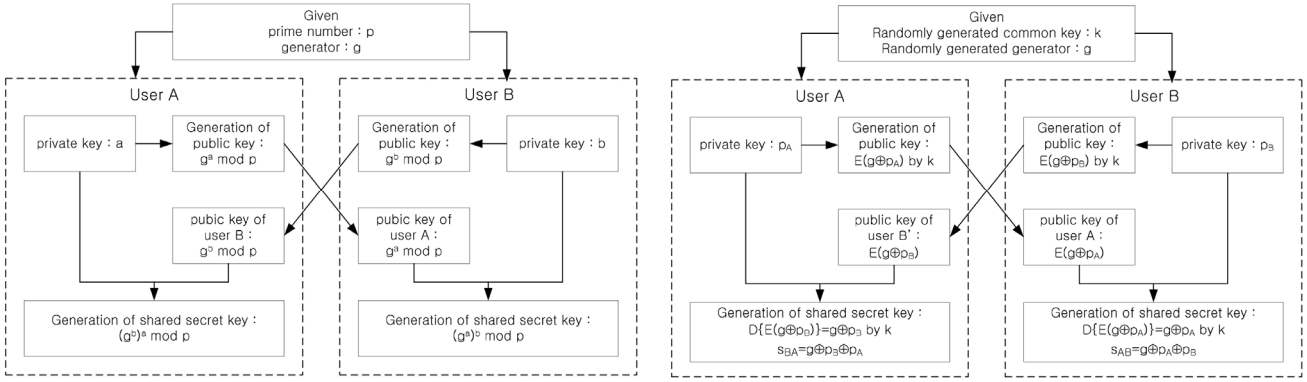

FIG. 1. (a) Diffie-Hellman secret-key-sharing algorithm. (b) The proposed secret-key-sharing algorithm, modifying the D-H algorithm.

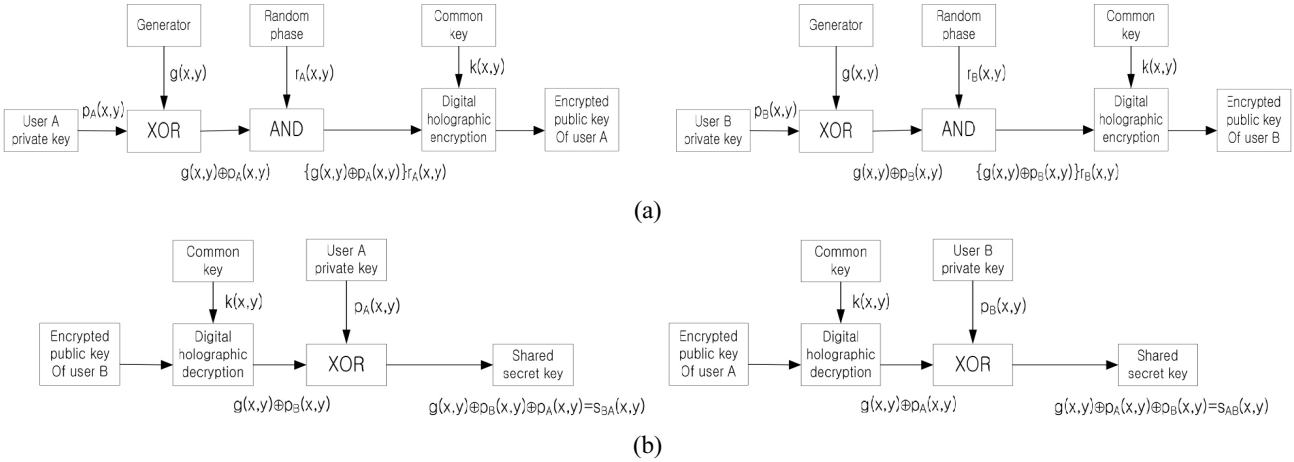

FIG. 2. Flow charts for the proposed secret-key-sharing cryptography: (a) encryption, (b) decryption.

The second step is about the encryption process with the common encryption key k by phase-shifting digital holography, as in Eqs. (1) and (2). In Fig. 2, the pre-encrypted private key is multiplied by a random phase, which enables the encrypted digital hologram to be a random pattern. The third step is reconstruction of the pre-encrypted private key with the same common key k from the received public-key ciphers, in compliance with Eqs. (3) and (4). Eqs. (3) and (4) imply that attackers cannot infer the private information, due to the noise-like cipher pattern, even if they know the public keys. The last step is the generation of the shared secret key, which is computed by XOR operation with each private key, according to Eqs. (5) and (6).

The optical information processing deals with a 2-D data array, and has the advantage of fast parallel computation. This implies that an optical encryption system can have a very long key to enhance security strength, and can process massive amounts of data quickly. Moreover, if an encryption system has a key length of a 2-D array with M × N bits, it means that $2^{M\times N}$ brute-force attacks are required to discover the correct key. The principal idea in this paper is that optical phase-shifting digital holography can be applied to a secret-key-sharing cryptosystem by modifying the conventional D-H secret-key-sharing algorithm. The mathematical modulo-arithmetic encryption in the D-H secret-key-sharing is replaced with a digital holographic method. The encryption of a private key is carried out using two-step quadrature phase-shifting digital holography based on orthogonal polarization to generate ciphers, and these ciphers are used to generate a shared secret key by the corresponding decryption process.

Referring to the proposed secret-key-sharing cryptosystem algorithm shown in Figs. 1 and 2, Fig. 3 shows the optical schematic for the proposed secret-key-sharing cryptosystem using two-step quadrature phase-shifting digital holography. In this configuration, the optical setup contains two Mach-Zehnder-interferometer paths and consists of a spatial filter (SF), a collimating lens (CL), two shutters (S), three linear polarizers (P), four beam splitters (BS), two mirrors (M), a λ/4-plate, two convex lenses (L), a random phase mask (RPM), five spatial light modulators (SLM), and two charge-coupled devices (CCD). This scheme makes it possible to acquire two-step quadrature phase-shifting digital holograms with π/2 phase shift between s-polarization and p-polarization on the CCDs. The encryption and decryption principles of the optical cryptosystem using two-step quadrature phase-shifting digital holography and its error analysis were described in references [19] and [20].

In the beginning, the pre-encryption of user A's private key is achieved by optical XOR operation in the inner Mach-Zehnder-interferometer setup. As for user A, two random numbers $g(x, y)$ and $p_A(x, y)$ yield a signal message $|s(x, y)|$ by optical XOR operation, where x and y are transverse coordinates in the spatial domain.

$$|s(x,y)| = g(x,y) \oplus p_A(x,y). \tag{8}$$

The two-step phase-shifting digital holographic encryption process is accomplished by the outer Mach-Zehnder-interferometer. Let $s(x, y)$ be the signal-message function to be encrypted. Assume that a random-phase-mask function $\exp[j\theta_s(x, y)]$ consists of a randomly generated number that represents 1 or 0 randomly in a 2-D array, which enables the encrypted digital hologram to be like a random pattern. The multiplication of the signal message and random phase mask is represented as

$$s(x,y) = |s(x,y)| e^{j\theta_s(x,y)}. \tag{9}$$

Let $|k(x, y)|$ be an encryption common-key function, which is assumed to be another random number. This key is multiplied by π (radians) to become a binary phase π $|k(x, y)|$, where $|k(x, y)|$ is 1 or 0 in a 2-D array. Then the

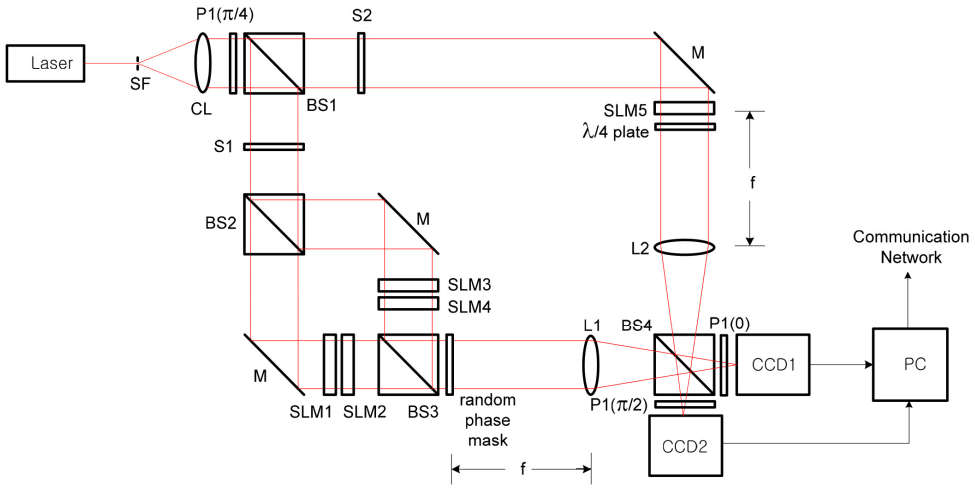

FIG. 3. Optical schematic for the proposed secret-key-sharing cryptosystem using two-step quadrature phase-shifting digital holography.

random phase pattern of the encryption common-key function $k(x, y)$ with unit amplitude is expressed by

$$k(x,y) = 1 \cdot e^{j\pi|k(x,y)|}. \tag{10}$$

The Fourier-transformed functions of Eqs. (9) and (10) are taken to be $S(\alpha, \beta)$ and $K(\alpha, \beta)$ respectively, where α and β are transverse coordinates in the spatial-frequency domain:

$$S(\alpha,\beta) = F\{s(x,y)\} = |S(\alpha,\beta)|e^{j\phi_S(\alpha,\beta)}, \tag{11}$$

$$K(\alpha,\beta) = F\{k(x,y)\} = |K(\alpha,\beta)|e^{j\phi_K(\alpha,\beta)}. \tag{12}$$

Then the two-step quadrature phase-shifting digital holographic method gives two intensity patterns recorded on the CCDs in the form of a digital hologram:

$$\begin{aligned} I_1(\alpha,\beta) = {} & |S(\alpha,\beta)|^2 + |K(\alpha,\beta)|^2 \\ & + 2|S(\alpha,\beta)||K(\alpha,\beta)|\cos\triangle\phi_{SK} \end{aligned}, \tag{13}$$

$$\begin{aligned} I_2(\alpha,\beta) = {} & |S(\alpha,\beta)|^2 + |K(\alpha,\beta)|^2 + \\ & 2|S(\alpha,\beta)||K(\alpha,\beta)|\sin\triangle\phi_{SK} \end{aligned}. \tag{14}$$

where $\triangle\phi_{SK} = \phi_S - \phi_K$ is the phase difference between the object and reference beams. These two digital holograms are recorded on CCD1 and CCD2 respectively. Each hologram is assumed to be quantized with 256 gray levels on the CCD. These two digital holograms contain the encrypted information of the signal message. Meanwhile, only the object beam's intensity distribution $I_S = |S(\alpha, \beta)|^2$ is acquired on CCD1, by blocking the reference beam with shutter S2 in the optical setup shown in Fig. 3. Similarly, only the reference beam's intensity $I_K = |K(\alpha, \beta)|^2 = C_3$ is acquired on CCD1 by blocking the object beam with shutter S1, and it is used for decryption as a ciphered public key C_3. Applying the DC-term-removal technique to Eqs. (13) and (14) gives two ciphered public keys C_1 and C_2:

$$\begin{aligned} \tilde{I}_1(\alpha,\beta) = {} & I_1 - I_S - I_K = I_1 - |S(\alpha,\beta)|^2 - |K(\alpha,\beta)|^2 \\ & = 2|S(\alpha,\beta)||K(\alpha,\beta)|\cos\triangle\phi_{SK} = C_1 \end{aligned}, \tag{15}$$

$$\begin{aligned} \tilde{I}_2(\alpha,\beta) = {} & I_2 - I_S - I_K = I_2 - |S(\alpha,\beta)|^2 - |K(\alpha,\beta)|^2 \\ & = 2|S(\alpha,\beta)||K(\alpha,\beta)|\sin\triangle\phi_{SK} = C_2 \end{aligned}. \tag{16}$$

Thereby, three ciphers $\{C_1, C_2, C_3\} = \{\tilde{I}_1, \tilde{I}_2, I_K\}$ as one group are acquired, stored in a computer, and transmitted through the communication network as a cipher group of open public keys.

After receiving the open public keys of these ciphers, the decryption process is accomplished as follows. The phase difference $\triangle\phi_{SK}$ between the object and reference beams and the amplitude component A_{SK} are calculated as

$$\triangle\phi_{SK} = \phi_S - \phi_K = \tan^{-1}\left(\frac{\tilde{I}_2}{\tilde{I}_1}\right) = \tan^{-1}\left(\frac{C_2}{C_1}\right), \tag{17}$$

$$\begin{aligned} A_{SK} = {} & |S(\alpha,\beta)||K(\alpha,\beta)| \\ & = \frac{1}{2}\sqrt{(\tilde{I}_1)^2 + (\tilde{I}_2)^2} = \frac{1}{2}\sqrt{(C_1)^2 + (C_2)^2} \end{aligned}. \tag{18}$$

From Eqs. (17) and (18), the complex hologram with encryption information is expressed as

$$H(\alpha,\beta) = A_{SK}e^{j\triangle\phi_{SK}} = |S(\alpha,\beta)||K(\alpha,\beta)|e^{j(\phi_S - \phi_K)}. \tag{19}$$

By using this complex hologram $H(\alpha, \beta)$ and the same encryption common-key information of Eq. (12), the complex distribution of the object wave is reconstructed, and the original signal message function is restored.

$$\begin{aligned} D(\alpha,\beta) &= \frac{H(\alpha,\beta)K(\alpha,\beta)}{C_3} \\ &= \frac{|S(\alpha,\beta)||K(\alpha,\beta)|e^{j(\phi_S - \phi_K)}|K(\alpha,\beta)|e^{j\phi_K}}{|K(\alpha,\beta)|^2}, \\ &= |S(\alpha,\beta)|e^{j\phi_S} = S(\alpha,\beta) \end{aligned} \tag{20}$$

$$\begin{aligned} d(x,y) &= |F^{-1}\{D(\alpha,\beta)\}| = |F^{-1}\{S(\alpha,\beta)\}| \\ &= |s(x,y)| = g(x,y) \oplus p_A(x,y) \end{aligned}. \tag{21}$$

In the last process, XOR logic is carried out between the restored function $d(x, y)$ and user B's private key p_B for shared secret key generation.

$$\begin{aligned} s_{AB}(x,y) &= d(x,y) \oplus p_B(x,y) \\ &= g(x,y) \oplus p_A(x,y) \oplus p_B(x,y) \end{aligned}. \tag{22}$$

Similarly, user B's shared secret key is achieved by the same encryption and decryption process, which generates the same result as user A's shared secret key of Eq. (22).

$$\begin{aligned} s_{BA}(x,y) &= d(x,y) \oplus p_A(x,y) \\ &= g(x,y) \oplus p_B(x,y) \oplus p_A(x,y) \end{aligned}. \tag{23}$$

Encryption and decryption flow charts for the two-step phase-shifting digital holographic cryptosystem are shown in Fig. 4.

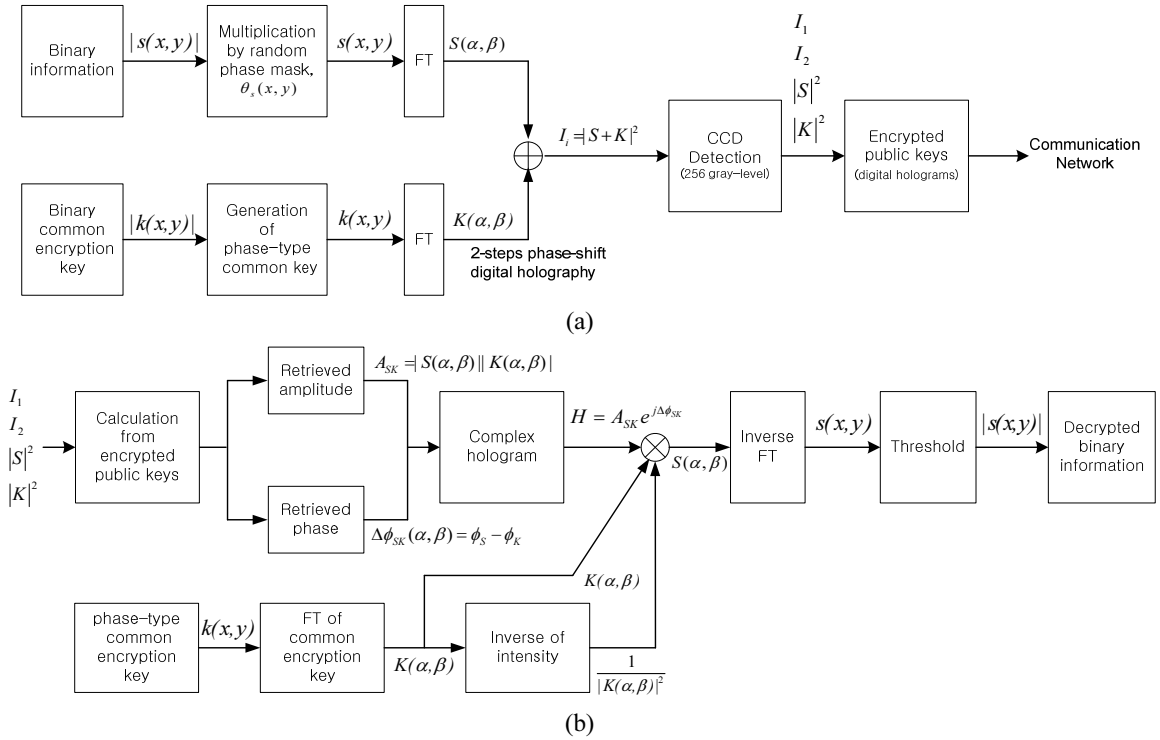

FIG. 4. Flow charts for the two-step phase-shifting digital holographic cryptosystem: (a) encryption, (b) decryption.

III. SIMULATIONS AND RESULTS

Computer simulations using the MATLAB program are presented to prove the performance of the proposed cryptosystem. In this method, 2-D arrays of binary data, or images, of size 256 × 256 pixels are used for simulation convenience. Schematically in the optical system, the number of 2-D array data can be expanded to larger array depending on the SLM specification. A larger array provides stronger security strength, due to the larger encryption-key length. Figures 5(a)~5(d) show the binary data and images to be used in the secret-key-sharing cryptosystem. Figures 5(a) and 5(b) show randomly generated binary data images as generator g and encryption common key k, and Figs. 5(c) and 5(d) show binary images as user A's private key p_A and user B's private key p_B, respectively. In general, these private keys are also expressed as randomly generated binary data, which enable cryptographers to present a stronger and more complicated cryptosystem, owing to the randomness. However, a binary image is used as a private key for visual convenience in this paper. Figure 6 shows the pre-encrypted private-key data images for each user, before the phase-shifting digital holographic encryption is carried out. Figure 6(a) shows user A's pre-encrypted private-key data image $p_A \oplus g$ by XOR operation of p_A and g, and Fig. 6(b) shows user B's pre-encrypted private-key data image

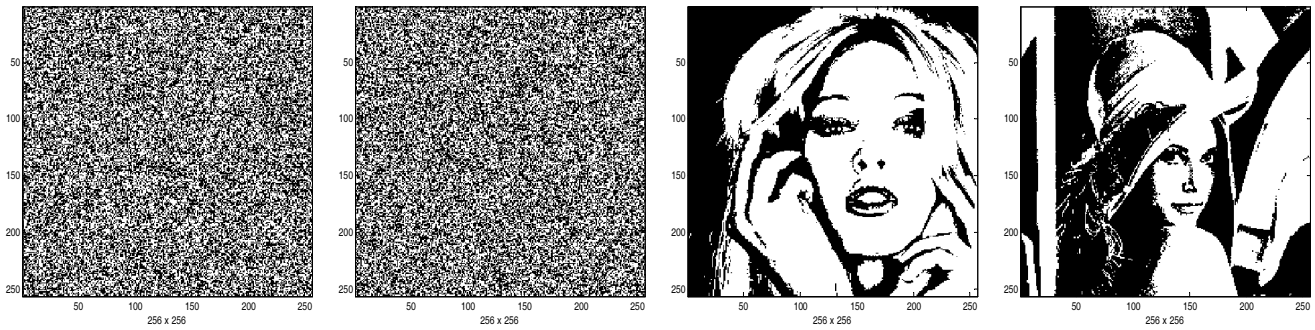

FIG. 5. Binary data and images to be used for the secret-key-sharing cryptosystem (256 × 256 pixels): (a) a randomly generated binary data image as the generator g, (b) a randomly binary data image as the encryption common key k, (c) a binary image as user A's private key p_A, and (d) a binary image as user B's private key p_B.

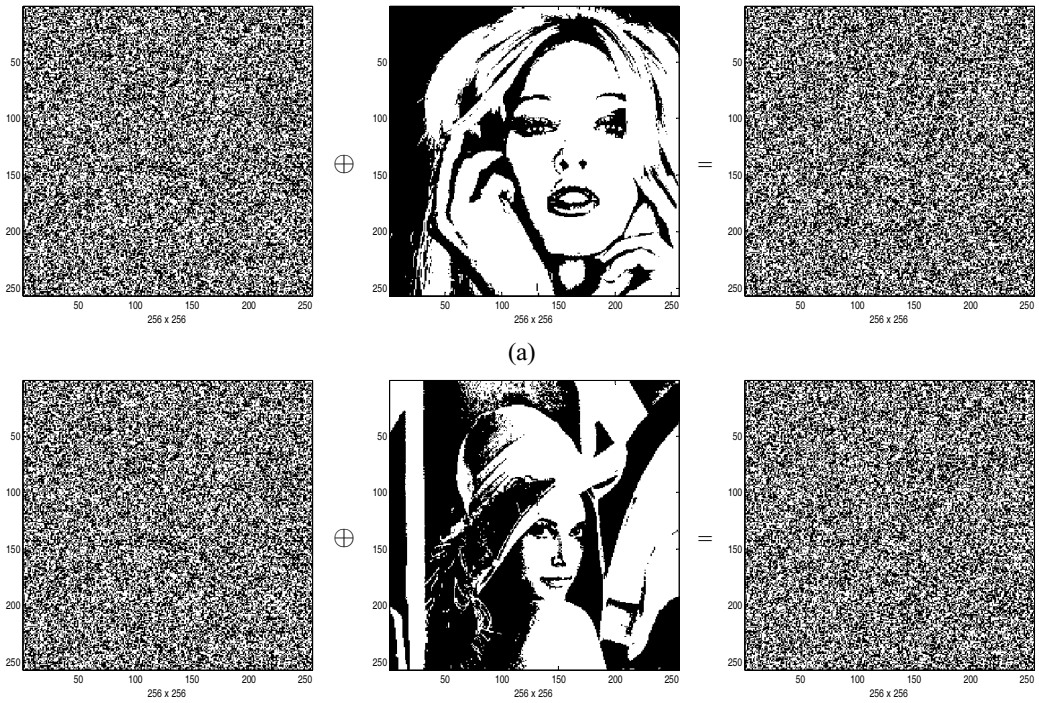

FIG. 6. Pre-encrypted private-key data images before the phase-shifting digital holographic encryption: (a) user A's pre-encrypted data $p_A \oplus g$ by XOR operation of p_A and g, and (b) user B's pre-encrypted data $p_B \oplus g$ by XOR operation of p_B and g.

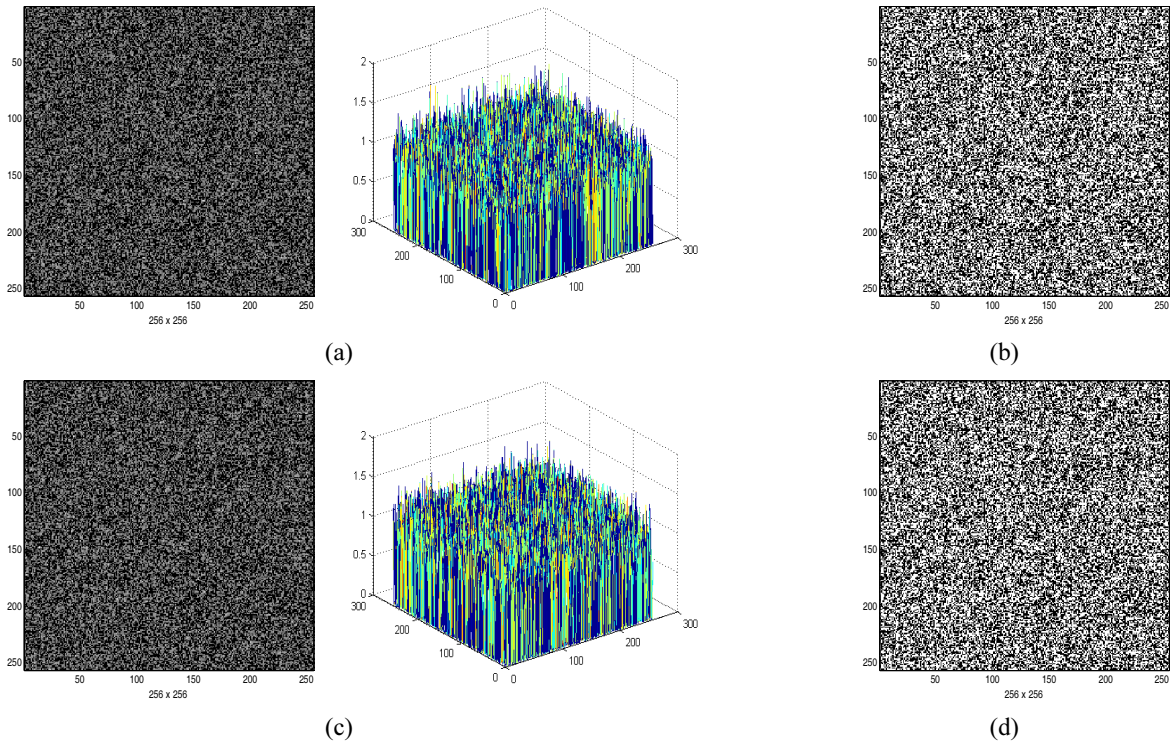

FIG. 7. Results of reconstruction for the encrypted private-key data images: (a) the reconstructed image pattern obtained from the complex hologram H_B and its intensity histogram; (b) user A's correctly decrypted binary data image $p_A \oplus g$, applying the proper threshold value of 0.4 to the reconstructed image; (c) the reconstructed image pattern obtained from the complex hologram H_A and its intensity histogram; and (d) user B's correctly decrypted binary data image $p_B \oplus g$, applying the proper threshold value of 0.4 to the reconstructed image.

$p_B \oplus g$ by XOR operation of p_B and g. As shown in Fig. 6, the resultant pre-encrypted private-key data show a randomly distributed binary pattern owing to the randomly generated binary pattern of the generator g. Figure 7 shows the results of reconstruction for the encrypted private-key data images after decryption using the same encryption common key k that was used for encryption in the phase-shifting digital holography. Figure 7(a) is the reconstructed image pattern obtained from the complex hologram H_B for user B and the same encryption common key k, and shows its intensity histogram. Figure 7(b) shows user A's correctly decrypted binary data image $p_A \oplus g$, applying the proper threshold value of 0.4 to the reconstructed image. Similarly, Fig. 7(c) is the reconstructed image pattern obtained from the complex hologram H_A for user A and the same encryption common key k, and shows its intensity histogram. Figure 7(d) shows user B's correctly decrypted binary data image $p_B \oplus g$, applying the proper threshold value of 0.4 to the reconstructed image. As shown in Figs. 7(b) and 7(d), the retrieved binary data image of $p_A \oplus g$ is exactly the same as user A's pre-encrypted private-key data image $p_A \oplus g$ in Fig. 6(a), and the retrieved binary data image of $p_B \oplus g$ is exactly the same as user B's pre-encrypted private-key data image $p_B \oplus g$ in Fig. 6(b). Figure 8 shows the results of post-decryption for the shared secret-key generation. Figure 8(a) is user A's shared secret key $s_{BA} = (p_B \oplus g) \oplus p_A$ by XOR operation between the retrieved binary data image $p_B \oplus g$ and user A's private key p_A, and Fig. 8(b) is user B's shared secret key $s_{AB} = (p_A \oplus g) \oplus p_B$ by XOR operation between the retrieved binary data image $p_A \oplus g$ and user B's private key p_B. As shown in Fig. 8, these two binary bit patterns have the same data as a shared secret key. This shared secret key will be used as a secret key only between users A and B in their message information encryption.

IV. CONCLUSION

An optical phase-shifting digital holographic encryption technique is applied to a secret-key-sharing cryptosystem. The proposed secret-key-sharing algorithm is optically implemented by a pre-encryption technique with XOR operation and a two-step quadrature phase-shifting digital holographic encryption technique using orthogonal polarization. Encrypted digital holograms in the optical holographic encryption system are Fourier-transform holograms, and are recorded on CCDs with 256 gray levels of quantized intensity. These ciphered digital holograms show an analog-type noise-like randomized pattern with a 2-D array, which has a stronger security level than conventional electronic cryptography due to the complexity of optical encryption, and protects against the possibility of a replay attack. Three digital-hologram ciphers with each private key's information are opened to the public network for secret-key exchange, and are decrypted into the same secret key by the proposed algorithm. The optical encryption system has

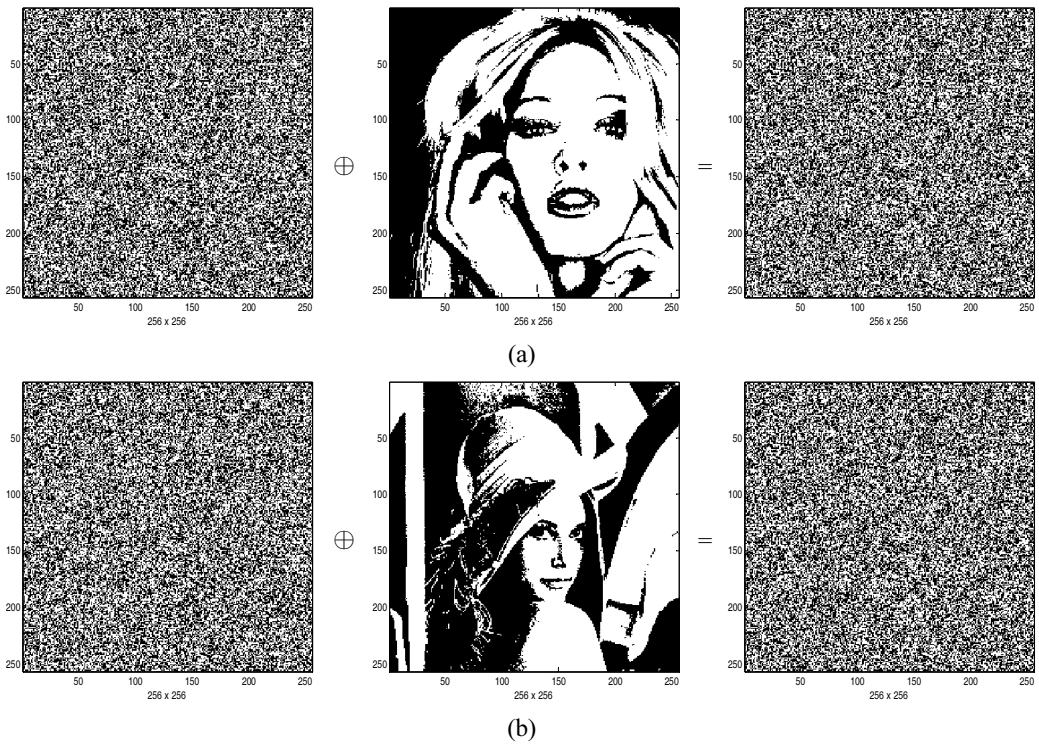

FIG. 8. Results of post-decryption for the shared-secret-key generation: (a) user A's shared secret key $s_{BA} = (p_B \oplus g) \oplus p_A$, (b) user B's shared secret key $s_{AB} = (p_A \oplus g) \oplus p_B$.

the advantage of increasing key length easily. The optical encryption setup can provide longer 2-D key length, resulting in a higher-security cryptosystem than a conventional system with one-dimensional key length. Schematically, the proposed optical secret-key-sharing method uses pre-encryption of the user's private key in combination with randomly generated binary data (called a generator) before digital holographic encryption, which provides a kind of layered security system with a double key and enhances security strength, compared to the conventional Diffie-Hellman key-exchange protocol. Another advantage of the proposed secret-key-sharing cryptosystem is that it is free to change each user's private key in generating the public keys at any time. This alteration enables the cryptosystem to protect the secret key against reuse attack. Computer simulations present results verifying that the proposed method is feasible for application in secret-key-sharing cryptography.

ACKNOWLEDGMENT

This work was supported by the Incheon National University (International Cooperative) Research Grant in 2016.

REFERENCES

1. P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. **20**, 767-769 (1995).
2. G. Unnikrishnan and K. Singh, "Double random fractional Fourier domain encoding for optical security," Opt. Eng. **39**, 2853-2859 (2000).
3. Z. Liu, L. Xu, T. Liu, H. Chen, P. Li, C. Lin, and S. Liu, "Color image encryption by using Arnold transform and color-blend operation in discrete cosine transform domains," Opt. Commun. **284**, 123-128 (2011).
4. O. Matoba and B. Javidi, "Encrypted optical memory system using three-dimensional keys in the Fresnel domain," Opt. Lett. **24**, 762-764 (1999).
5. Z. Liu, L. Xu, C. Lin, and S. Liu, "Image encryption by encoding with a nonuniform optical beam in gyrator transform domains," Appl. Opt. **49**, 5632-5637 (2010).
6. M. Cho and B. Javidi, "Three-dimensional photon counting double-random phase encryption," Opt. Lett. **38**, 3198-3201 (2013).
7. W. Chen, X. Chen, and C. J. R. Sheppard, "Optical image encryption based on diffractive imaging," Opt. Lett. **35**, 3817-3819 (2010).
8. X. F. Meng, L. Z. Cai, Y. R. Wang, X. L. Yang, X. F. Xu, G. Y. Dong, X. X. Shen, H. Zhang, and X. C. Cheng, "Hierarchical image encryption based on cascaded iterative phase retrieval algorithm in the Fresnel domain," J. Opt. A: Pure Appl. Opt. **9**, 1070-1075 (2007).
9. W. Qin and X. Peng, "Asymmetric cryptosystem based on phase-truncated Fourier transforms," Opt. Lett. **35**, 118-120 (2010).
10. G. Situ and J. Zhang, "Multiple-image encryption by wavelength multiplexing," Opt. Lett. **30**, 1306-1308 (2005).
11. D. Weber and J. Trolinger, "Novel implementation of nonlinear joint transform correlators in optical security and validation," Opt. Eng. **38**, 62-68 (1999).
12. B. Javidi and T. Nomura, "Securing information by means of digital holography," Opt. Lett. **25**, 28-30 (2000).
13. X. Wang, D. Zhao, F. Jing, and X. Wei, "Information synthesis (complex amplitude addition and subtraction) and encryption with digital holography and virtual optics," Opt. Exp. **14**, 1476-1486 (2006).
14. J.-W. Han, C.-S. Park, D.-H. Ryu, and E.-S. Kim, "Optical image encryption based on XOR operations," Opt. Eng. **38**, 47-54 (1999).
15. S. H. Jeon and S. K. Gil, "Optical secret key sharing method based on Diffie-Hellman key exchange algorithm," J. Opt. Soc. Korea **18**, 477-484 (2014).
16. S. H. Jeon and S. K. Gil, "Optical implementation of asymmetric cryptosystem combined with D-H secret key sharing and triple DES," J. Opt. Soc. Korea **19**, 592-603 (2015).
17. B. Javidi and T. Nomura, "Polarization encoding for optical security systems," Opt. Eng. **39**, 2439-2443 (2000).
18. W. Diffie and M. Hellman, "New directions in cryptography," IEEE Trans. Inf. Theory **22**, 644-654 (1976).
19. S. H. Jeon and S. K. Gil, "2-step phase-shifting digital holographic optical encryption and error analysis," J. Opt. Soc. Korea 15, 244-251 (2011).
20. S. K. Gil, "2-step quadrature phase-shifting digital holographic optical encryption using orthogonal polarization and error analysis," J. Opt. Soc. Korea **16**, 354-364 (2012).
21. S. K. Gil, S. H. Jeon, and J. R. Jung, "Application to optical secret key sharing cryptography using phase-shifting digital holography," Proc. SPIE **10558**, 10558W (2018).