Journal of the Optical Society of Korea
Vol. 17, No. 5, October 2013, pp. 362-370
DOI: http://dx.doi.org/10.3807/JOSK.2013.17.5.362

Optical Implementation of Triple DES Algorithm Based on Dual XOR Logic Operations

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

[1]*Department of Electronic Engineering, Incheon National University, Incheon 406-772, Korea*
[2]*Department of Electronic Engineering, The University of Suwon, Whasung 440-600, Korea*

(Received July 15, 2013 : revised August 20, 2013 : accepted August 20, 2013)

In this paper, we propose a novel optical implementation of a 3DES algorithm based on dual XOR logic operations for a cryptographic system. In the schematic architecture, the optical 3DES system consists of dual XOR logic operations, where XOR logic operation is implemented by using a free-space interconnected optical logic gate method. The main point in the proposed 3DES method is to make a higher secure cryptosystem, which is acquired by encrypting an individual private key separately, and this encrypted private key is used to decrypt the plain text from the cipher text. Schematically, the proposed optical configuration of this cryptosystem can be used for the decryption process as well. The major advantage of this optical method is that vast 2-D data can be processed in parallel very quickly regardless of data size. The proposed scheme can be applied to watermark authentication and can also be applied to the OTP encryption if every different private key is created and used for encryption only once. When a security key has data of 512×256 pixels in size, our proposed method performs 2,048 DES blocks or 1,024 3DES blocks cipher in this paper. Besides, because the key length is equal to 512×256 bits, $2^{512\times256}$ attempts are required to find the correct key. Numerical simulations show the results to be carried out encryption and decryption successfully with the proposed 3DES algorithm.

Keywords : Optical encryption, Cryptosystem, XOR logic, Free-space parallel processing, DES
OCIS codes : (070.4560) Data processing by optical means; (200.2610) Free-space digital optics; (200.3760) Logic-based optical processing; (200.4660) Optical logic; (200.4960) Parallel processing

I. INTRODUCTION

As the public communication network expands rapidly, there have been strong demands for secure personal communication. However, significant personal information is threatened to leak because of weaknesses of security systems. For this reason, information security of the public network has become a great issue. In an attempt to protect information from hacking or cracking, a number of electronic or optical cryptosystems have been proposed. One of the simple methods to ensure security is to consider all data as binary strings and to encrypt them using encryption algorithms such as DES (Data Encryption Standard) or AES(Advanced Encryption Standard) [1]. Encryption is the process of transforming a plain text to a cipher text with a security key. In order for an authorized user to decrypt the cipher text, the same correct security key has to be known to the authorized user. In conventional symmetric key cryptography, a public key is constructed previously and opened to all the users as a common key. Therefore, this type of algorithm has a weak point against data interception by an unauthorized user. Since the security key is the core of most data cryptosystems, the protection of the security key is also very important. An advanced algorithm such as 3DES or asymmetric key cryptography uses double key encryption to enhance security strength, but the sharing of the private key is needed. In general, the conventional electronic encryption methods treat binary data. However, these methods involve large amounts of computation and are not fast enough for massive-volume data [2]. On the contrary an optical processing system has the advantage of fast processing 2-D data in parallel, which makes optical systems suitable for massive data encryption. In recent years, there has been increasing interest in the use of optical encryption

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

methods for security systems because optical systems have the merits of parallel processing and fast operation [3-12]. In each case the encrypted data is fully complex, and thus holographic recording may be required. This requirement makes it difficult to store and transmit the cipher data over digital communication networks. In order to solve this problem, optical encryption and decryption to record and reconstruct the complex values has been performed using a phase-shifting digital holographic technique [13-19]. Optoelectronic methods using digital logics are adequate for encryption. Some researchers reported XOR-based optical encryptions [20, 21].

In this paper, we propose a new optical implementation of a 3DES algorithm based on dual XOR logic operations for a cryptographic system, and show the performance of the proposed cryptosystem. The decryption can be carried out optically by using the same optical schematic. Section II is organized as four parts. In the first part, the conventional DES algorithm is overviewed. The second part explains the 3DES algorithm, and double encryption using two keys is described using XOR logic operation, in particular double encryption using private key exchanging is proposed and described. In the third part, a free-space interconnected optical logic gate method is introduced to implement the optical XOR logic operation. In the fourth part, we propose an optical architecture of 3DES and explain the encryption/decryption procedure in the proposed architecture. Computer experiments show results of the encryption and the decryption with the proposed method in Section III. Finally, conclusions are briefly summarized in Section IV.

II. THEORY

2.1. DES Algorithm

The Data Encryption Standard (DES) which is also known as the Data Encryption Algorithm (DEA) was the first symmetric block cipher chosen and was first issued as a standard in 1977 by the American National Standard Institute (ANSI), and the National Institute of Standards and Technology(NIST) believes that DES provides adequate security for its intended unclassified information applications [1]. The algorithm specified in the DES is very complex. It encrypts plain text data in 64-bit blocks by using a 56-bit secret key. DES has been one of the most successful and widely used secret key cryptographic systems. However, some cryptographers have been arguing that its 56-bit key would not be sufficient to provide enough security strength ever since the DES was used for public cryptosystem. Therefore the DES algorithm and the key length have been controversial issues.

In the conventional digital cryptography for block encryption systems, the Electronic Codebook (ECB) mode is the simplest mode which transforms 64 bits of input to 64 bits of output. In this mode, blocks are encrypted sequentially,

$$C_i = E_k(P_i), \quad 1 \le i \le m, \tag{1}$$

where E_k (•) denotes some encryption method with some key k in the case of encryption, P_i denotes the i-th plain text, and C_i denotes the corresponding cipher text, where m is the total number of plain text being encrypted. Decryption is given by

$$P_i = D_k(C_i), \quad 1 \le i \le m, \tag{2}$$

where D_k (•) denotes the corresponding decryption method with the key k in the case of encryption.

The DES algorithm can be used in ECB mode, where the encryption and decryption schemes can be simply implemented by an exclusive-OR (XOR) logic function. Therefore, the operation of the encryption system is mathematically described by the XOR logic operation, that is, modulo two addition. Specifically, XOR-only encryption schemes will be perfectly secure if and only if the key data is perfectly random and never reused. The XOR-based encryption method can only be applied to binary data or images consisting of black and white pixels, and this method means independent encryption of each pixel separately. When we apply the XOR-based encryption method to the above DES algorithm in the ECB mode, Eqs. (1) and (2) can be expressed as follows.

Let P be a plain text to be encrypted, and K is a security key. Then a cipher text C can be obtained by encrypting the plain text P with the security key K.

$$C = P \oplus K, \tag{3}$$

where symbol $\oplus$ represents the bitwise XOR operation.

To retrieve the original plain text from the cipher text, C is decrypted with the same key K.

$$D = C \oplus K = (P \oplus K) \oplus K = P. \tag{4}$$

Unfortunately, this method for DES does not give us much algorithm strength in the security system. 3DES is a kind of security enhancement method to strengthen DES by doubling the DES algorithm and increasing key length without diminishing encryption speed.

2.2. Triple DES Algorithm

Ever since DES was released for public security, however, a lot of cryptographers have argued that the security of DES would be endangered in present days due to its short key length. In order to overcome this problem, many efforts were made to expand key size. Some of them are entire redesigning of DES to have more key bits, and some others are using the DES algorithm multiple times. Another method to increase key length is chaining two DES in parallel instead of serial application of DES.

However, the security of DES is threatened by attackers in present days because of rapid processor speed, and some possible attacking methods are suggested. Recently, Triple DES (3DES) has been adopted as a temporary standard and is incorporated in several international standards. 3DES is known as Encrypt-Decrypt-Encrypt (EDE) and Triple DEA (3DEA). 3DES is the name now most often given one popular form of multiple DES applications. Most 3DES implementations use two security keys. If the total length of the two keys has 112 bits, then cryptanalysis requires triple computational efforts compared to DES with 56-bit key length. The resultant 3DES cipher text is much harder to break.

2.2.1. Double Encryption using Two Keys

A reasonable approach to lengthen the security key bit is to use two keys in succession. Let P be a plain text to be encrypted, and K_1 and K_2 are two different security keys, respectively. First, an intermediate cipher text C_1 can be obtained by encrypting the plain text P with the K_1. Second, a final cipher text C_2 can be obtained by encrypting the cipher text C_1 with the key K_2.

$$C_1 = P \oplus K_1, \tag{5}$$

$$C_2 = C_1 \oplus K_2 = (P \oplus K_1) \oplus K_2. \tag{6}$$

To retrieve the original plain text from the cipher text C_2, C_2 is decrypted with the key K_2 to get C_1 and it is decrypted with the key K_1 again to have back the plain text P.

$$D_1 = C_2 \oplus K_2 = (P \oplus K_1 \oplus K_2) \oplus K_2 = P \oplus K_1, \tag{7}$$

$$D_2 = D_1 \oplus K_1 = (P \oplus K_1) \oplus K_1 = P. \tag{8}$$

However, this method has a disadvantage that we must know both of two security keys for decryption.

2.2.2. Double Encryption using Private Key Exchanging : A Proposed Method

In order to avoid the key sharing of the double encryption with two keys, we suggest a triple encryption using two keys in special way. Let K_1 and K_2 be two different security keys, respectively. The keys K_1 and K_2 could be called as a public key and a private key for convenience. In this method, an intermediate encrypted key K can be obtained by encrypting the private key K_2 with the public key K_1, and a cipher text C can be obtained by encrypting a plain text P with the private key K_2.

$$K = K_2 \oplus K_1, \tag{9}$$

$$C = P \oplus K_2. \tag{10}$$

To retrieve the original plain text from the cipher text C, the encrypted key K is decrypted with the public key K_1 to reconstruct the private key K_2. Generally, the public key is opened to users as a common key. Then the cipher text is decrypted with the retrieved private key K_2 to have back the plain text P.

$$D_1 = K \oplus K_1 = (K_2 \oplus K_1) \oplus K_1 = K_2, \tag{11}$$

$$D_2 = C \oplus D_1 = (P \oplus K_2) \oplus K_2 = P. \tag{12}$$

It is interesting that we can apply this algorithm to watermark verification. If we substitute a private key K_2 with a watermark of the one user A, then Eq. (9) expresses the encrypted form of the watermark. This ciphered watermark is transmitted to the other user B and is decrypted with the key K_1 by Eq. (11) to show the watermark of user A. The reconstructed watermark is verified by user B and is used for decrypting the cipher text P by Eq. (12). Furthermore, this algorithm can be applied to One Time Pad(OTP) encryption if we use a different private key only once whenever we create cipher text. One of the advantages of this proposed method is that it is a more advanced cryptosystem to transmit the encrypted private key and the encrypted cipher text at the same time. Another advantage of this method is that it is convenient to exchange the private key in the form of the encryption and to decrypt the plain text without knowing the other user's private key directly. This means this method has the property that users can change private keys at their own discretion. Of course, this method is also an improved cryptosystem over double encryption of DES.

Figure 1 shows the block diagram of the proposed 3DES

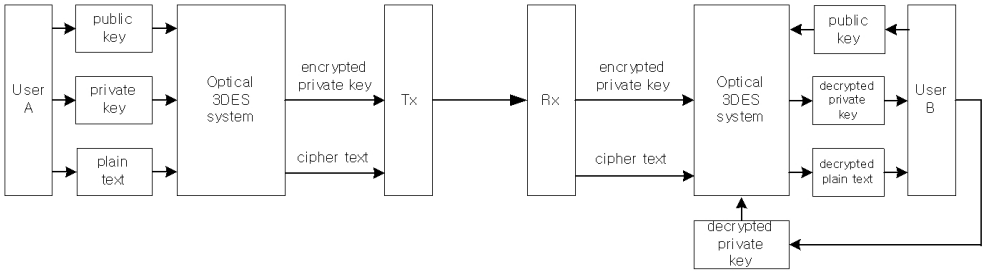

FIG. 1. Block diagram of 3DES encryption/decryption procedure.

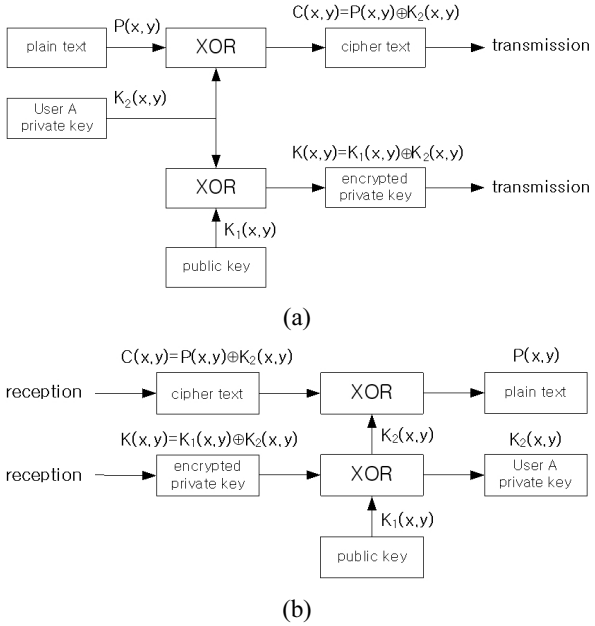

FIG. 2. Flow chart for 3DES; (a) encryption, (b) decryption.

encryption/decryption procedure. We can modify this procedure to simultaneous watermark verification and data encryption by changing the private key with the watermark in this Fig. 1.

Figure 2 shows the flow chart of the encryption and decryption for the proposed 3DES. The box XOR in the figure means the exclusive-OR logic operation.

2.3. Optical XOR Operation using a Free-space Interconnected Optical Logic Gate Method

An optical logic gate processing concept can be regarded as a free-space interconnected gate with logic. The free-space optical interconnection is important not only in communication systems but also in massive digital optical computing because of its various advantages, such as its efficiency to implement logic functions and the complexity of the implementation system. In this paper, we apply a free-space interconnected optical logic gate method in order to implement an XOR logic operation in an optical way. The free-space interconnected optical logic gate method is probably a good breakthrough to solve the difficulties of input-output pattern match. In the type of data encoding, a bit of information is represented by the position of a bright spot rather than by its intensity or polarization. The advantage of the free-space interconnected optical logic gate method is that no cell coding-decoding process is required and the output has the same format as the input. In the optical configuration of a logic gate, binary input variables are spatially encoded by using two's complement.

Figure 3 shows the optical schemes for bitwise logic operations using the free-space interconnected optical logic gate method, that is, the corresponding optical configurations

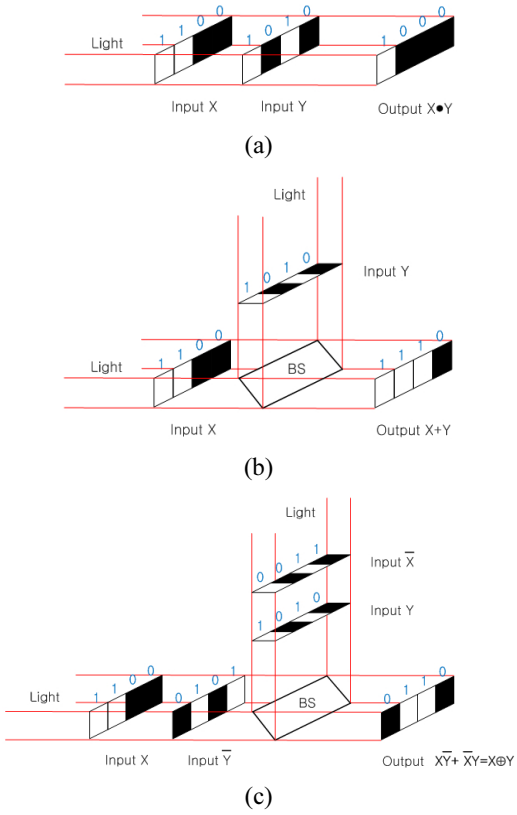

FIG. 3. Bitwise logic operations using the free-space interconnected optical logic gate method; (a) AND logic, (b) OR logic, (c) XOR logic.

for AND logic, OR logic, and XOR logic, respectively. Consider input variables X and Y divided into 4×1 pixel quadrants to apply the free-space interconnected optical logic gate method. The two inputs X and Y are segmented into four equal pixel quadrants, and each of the four quadrants is represented by a transparent(logic '1') or opaque (logic '0') coding characteristic. Logic AND operation is obtained by inner production pixel by pixel. The two spatially assigned binary inputs X and Y are placed in series. Logic OR operation is obtained from adding two inputs X and Y placed in parallel. Figure 3(a) and (b) show these logic operations. The architecture of XOR logic operation can be made by combining the logic AND scheme with the logic OR scheme. In this architecture shown in Fig. 3(c), the encoding principle of the input data format is that one input variable X is placed in one path of light, while the complement of X, i.e., $\overline{X}$, is placed in the other path of light. The other input variable Y is spatially located in a similar manner, but input variable Y is placed with input variable $\overline{X}$ in series and the complement of Y, i.e., $\overline{Y}$, is placed with input variable X in series. In order to gather these two outputs into one position, a beam combining element such as a beam splitter is employed. The basic principle of XOR logic can be described in terms of the combination of two logic ANDs and one logic OR. In Fig. 3(c), the two output lights passed

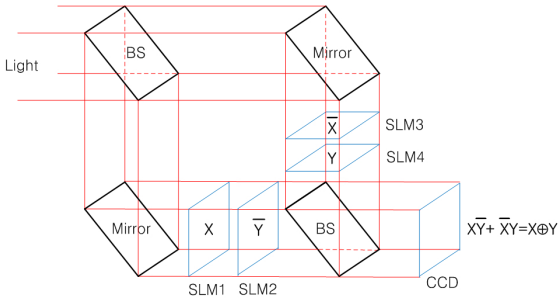

FIG. 4. Page-oriented XOR logic operation using the free-space interconnected optical logic gate method.

from input variables X, $\overline{Y}$ and $\overline{X}$, Y operate AND logics due to cascaded alignment. These two lights are overlapped to one output light by a beam splitter, which performs OR logic. Finally, the resultant output intensity distribution is equivalent to XOR logic of inputs X and Y. The input functions are now expressed by

$$f(x,y) = X(x,y) \bullet \overline{Y}(x,y), \tag{13}$$

$$g(x,y) = \overline{X}(x,y) \bullet Y(x,y), \tag{14}$$

where symbol • represents AND logic operation. After inner production and addition are carried out pixel by pixel, the logic function on this scheme is given by

$$\begin{aligned} f(x,y) + g(x,y) &= X(x,y) \bullet \overline{Y}(x,y) \\ &+ \overline{X}(x,y) \bullet Y(x,y) = X(x,y) \oplus Y(x,y), \end{aligned} \tag{15}$$

where symbols + and $\oplus$ represent OR and XOR logic operations, respectively.

Figure 4 shows the proposed optical schematic architecture for implementing a page-oriented optical XOR operation by using the basic concept of Fig. 3. In Fig. 4, the last beam splitter is used for combining two lights passed through SLMs. Two input operands X and $\overline{Y}$ are displayed on SLM1 and SLM2 in the one path of light. Also, the compliments of these two inputs, i.e., $\overline{X}$ and Y are displayed on SLM3 and SLM4 in the other path of light. All input data have the form of page-oriented functions which can consist of n×m binary bits. The output intensity on charge coupled device(CCD) results in the XOR logic operation and can be expressed as follows simply.

$$X \oplus Y = X\overline{Y} + \overline{X}Y, \tag{16}$$

2.4. Optical Implementation of Triple DES

The security of a symmetric cryptosystem is a function of the length of the key. The longer the key, the more resistant the security strength is. For this reason, the key length is chosen as the first parameter for specifying cryptographic algorithms. Assuming there is no better way to break the cryptosystem, other than to try every possible key with a brute force attack, the longer the key, the longer it will take to make the number of attacks necessary to find the correct key. In fact, every extra key bit generally doubles the number of possible keys and therefore increases the effort required for a successful brute force attack against most symmetric key algorithms. Generally, a key length of N bits means that 2^N attempts are required. For example, there are 2^{56} possible keys for the conventional DES and 2^{112} possible keys for the conventional 3DES. Even though two-key algorithm has more enhanced security strength, they require longer processing time of encryption or decryption when compared to one-key algorithm. Since the transmission technology advances, we need faster cryptosystems to catch up with the transmission speed.

In order to meet these requirements, in this paper we are going to propose a security enhancement method to strengthen 3DES algorithm. Basically, the optical system has an inherent advantage of two dimensional image data processing and fast parallel information processing time. The main idea of the proposed method is that the 3DES algorithm is implemented in an optical way and the key length is increased by expanding the key to a 2-D array. This 2-D expansion does not diminish encryption speed. With these properties, we suggest an optical implementation of XOR-based 3DES system which has 2-D page-typed plain text and security key input formats, resulting in the same 2-D cipher text output. If the 2-D key data consists of N×M pixels, then $2^{N\times M}$ attempts are required to find the correct key. However, the encryption speed using this XOR operation method is not affected by the data size because of parallel XOR operational processing. The symmetric encryption algorithm such as DES can be implemented optically with a bitwise XOR logical operator. Han et al. suggested optical image encryption based on XOR operation [20]. A two-input XOR gate was implemented very simply using two polarizers and two liquid crystal displays. This method can be used to implement a simple DES algorithm, but cannot be applied to the double encryption such as 3DES because of difficulty in implementing sequential optical XOR logic operations. However, our proposed method will solve the sequential XOR operations by using the free-space interconnected optical logic technique in implementing the XOR logic optically.

The main idea in the proposed optical 3DES method is to make a more secure cryptographic system, which is accomplished by encrypting and transmitting the individual private key and the plain text, and this encrypted private key is used to decrypt the original plain text. Referring to the block diagram of 3DES encryption and decryption procedure shown in Fig. 1, the optical 3DES system can be designed with optical components such as mirrors, beam splitters, lenses, and spatial light modulators (SLMs). Figure 5 shows the proposed optical implementation setup

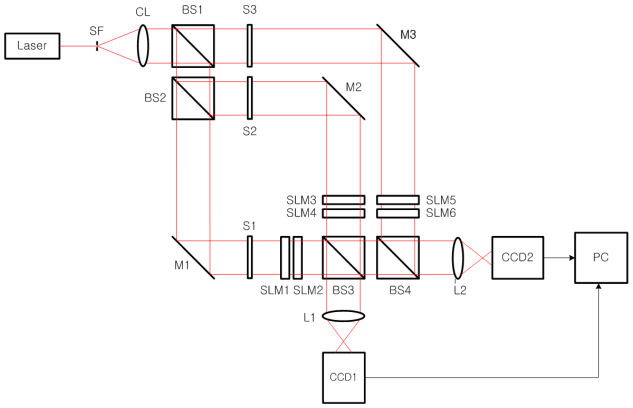

FIG. 5. Proposed optical implementation setup for Triple DES based on dual free-space interconnected XOR logic operations.

for 3DES using dual XOR logic operations, which is based on the free-space interconnected XOR logic operation architecture for binary data. Schematically, the optical setup contains two Mach-Zehnder type interferometers. Beam splitters BS1 and BS2 divide a collimated light into three plane waves and BS3 and BS4 combine these divided lights into two lights, resulting in records on CCDs. Also, this system is composed of six SLMs which are used for data input devices.

In order to investigate operating principles of 3DES, the flow charts shown in Fig. 2 are considered. First, let us consider the encryption procedure shown in Fig. 2(a). One plain text and two security keys are displayed on SLMs as free-space interconnected optical logic gates. Shutters S1, S2, and S3 are placed in the path of light to control encryption operations. In Fig. 5, with shutters S1, S2 open and S3 closed, the inner interferometer is used for encrypting the private key of the one user with the public(or common) key. The collimating light after being reflected by the mirror M1 illuminates the SLM1 which displays the binary private key (K_2), and continuously passes the SLM2 which displays the complement of the binary public key ($\overline{K_1}$). The other collimating light reflected by the mirror M2 illuminates the SLM3 which displays the complement of the private key ($\overline{K_2}$), and continuously passes the SLM4 which displays the public key (K_1). Then, the combined output light from BS3 which means the XOR encrypted private key (K) is recorded on CCD1 by the lens L1, where the imaging lens L1 plays a role of pixel matching between image and CCD pixel array. Next, we can encrypt the plain text with the private key in a similar way. With shutters S1, S3 open and S2 closed, the outer interferometer is used for encrypting the plain text such as binary data or image with the private key. In this case, the collimating light reflected by the mirror M3 illuminates the SLM5 which displays the complement of the private key ($\overline{K_2}$), and the passing output light is multiplied by the plain text (P) which is displayed on the SLM6. At this time, the input data of the SLM2 is changed to the

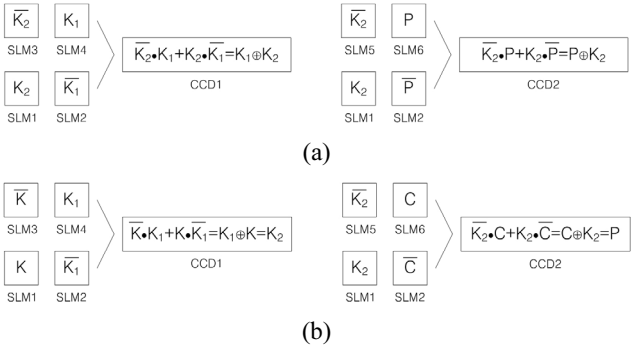

FIG. 6. Representations of input SLMs' data and output CCDs' data; (a) encryption, (b) decryption.

complement of the plain text ($\overline{P}$), while the private key (K_2) is stayed to the SLM1. The combined output from BS4 is recorded on CCD2 by the imaging lens L2, resulting in the XOR cipher text (C). Figure 6(a) shows representations of input SLMs' data and output CCD data for encryption. Finally, these two recorded lights on CCD1 and CCD2 are the encrypted data, which are stored in a computer and transmitted through the digital communication network.

Second, the decryption procedure shown in Fig. 2(b) is explained as follows. In our proposed cryptographic system, the decryption can be accomplished by using the same optical 3DES system as shown in the Fig. 5. The decrypting technique is that the encrypted private key data, which is transmitted to and received by the other user, is used for decrypting the original private key of the one user. Again, this decrypted private key is used for decrypting the original plain text from the received cipher text. In Fig. 5, with shutters S1, S2 open and S3 closed, the inner interferometer is used for decrypting the private key of the one user with the known public key (K_1). In the decryption mode of the optical 3DES system, the encrypted and received private key data (K) is displayed on SLM1 and the complement of this received data ($\overline{K}$) is also displayed on SLM3. Meanwhile, SLM2 and SLM4 display the complement of the public key ($\overline{K_1}$) and the public key (K_1), respectively. The collimating lights reflected by mirrors M1 and M2 pass through these SLMs and are combined to CCD1 by BS3. Then, the recorded light is the result of the XOR operation between the encrypted private key (K) and the public key (K_1), resulting in the retrieval of the original private key (K_2). Next, with shutters S1, S3 open and S2 closed, the outer interferometer is used for decrypting the original plain text with the reconstructed private key. In this case, the retrieved and decrypted private key (K_2) is displayed on SLM1 and the complement of this retrieved data ($\overline{K_2}$) is displayed on SLM5, while the received cipher text data (C) is displayed on SLM6 and the complement of this cipher text data ($\overline{C}$) is displayed on SLM2. As a result, the recorded light on CCD2 via BS4 comes out the XOR operation between the

cipher text (C) and the private key (K_2), resulting in the decryption of the original plain text (P). Figure 6(b) shows representations of input SLMs' data and output CCD data for decryption.

III. COMPUTER EXPERIMENTS

We show the performance of the proposed optical 3DES cryptographic method based on dual XOR logic operations by numerical simulations. In our method, input data to be encrypted must be binary bit data or a binary image. Therefore, a gray-level optical image to be encrypted must be converted to binary data in our proposed cryptosystem. In the previous papers [16-17], we use analog-to-digital ASCII encoding technique for converting a 256 gray-level image into the digitized 8-bits binary data. The 8-bits binary data corresponding to one gray-level value is arranged in a block having 4×2 pixels by block coding, and the converted data expands to 512×256 pixels in size by block mapping. Figure 7 shows the procedure of the proposed ASCII encoding and block mapping method for converting

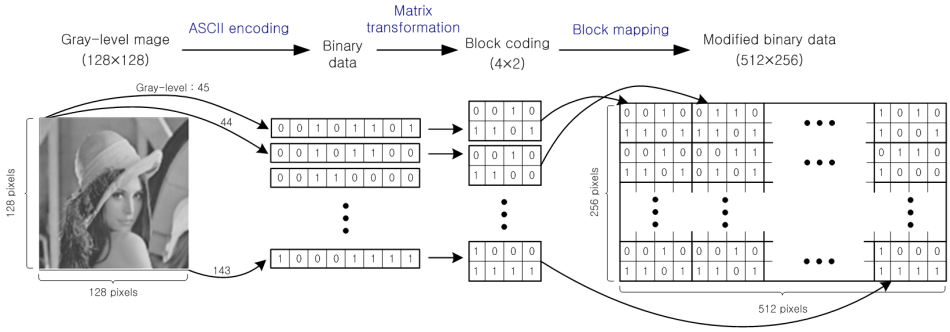

FIG. 7. Procedure of ASCII encoding and block mapping for converting a 256 gray-level optical image into binary data.

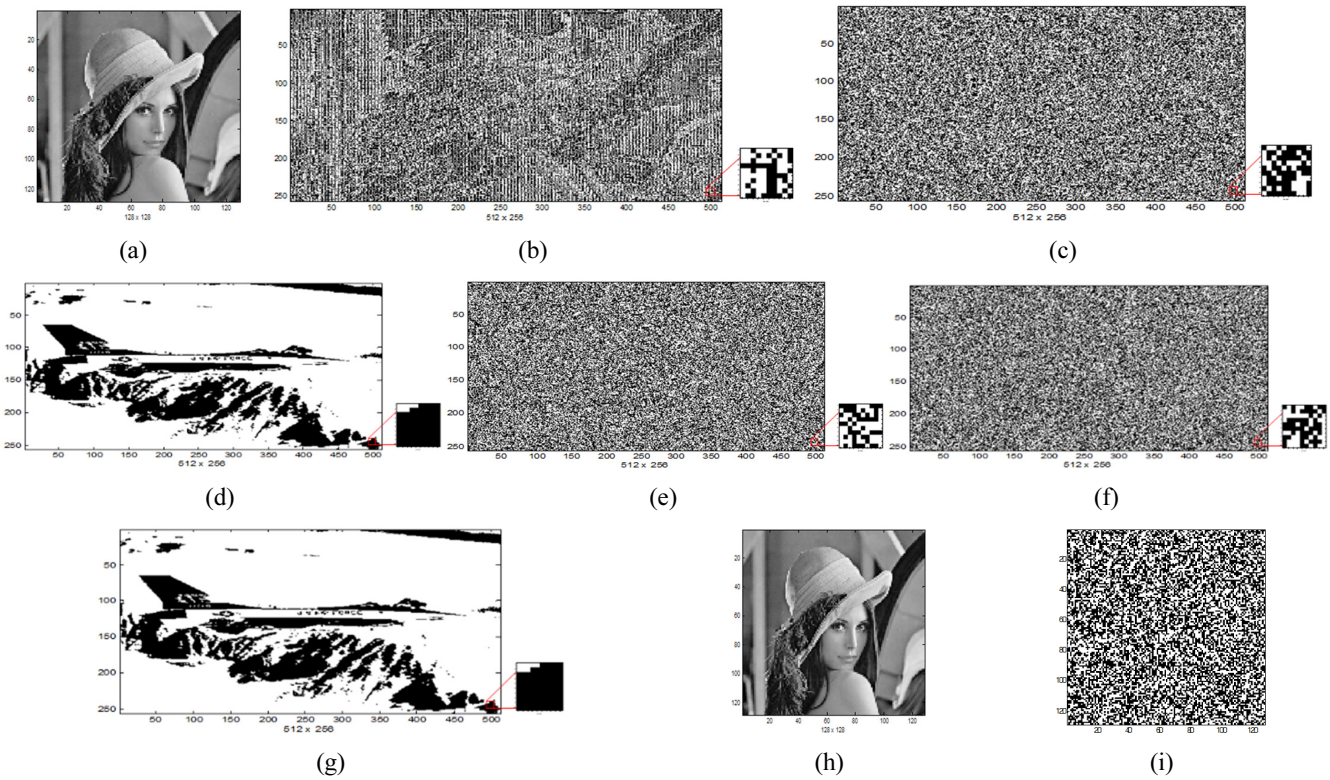

FIG. 8. Numerical simulations; (a) a 256 gray-level Lena image to be encrypted(128×128 pixels), (b) the converted binary data of Lena image (plain text, 512×256 pixels), (c) a random generated binary bit code as a public key (512×256 pixels), (d) a binary plane image as a private key (or watermark) of user (512×256 pixels), (e) the encrypted private key by the public key (512×256 pixels), (f) the encrypted binary data of Lena image by the private key (cipher text, 512×256 pixels), (g) the decrypted private key by the correct public key (512×256 pixels), (h) the decrypted Lena image by the correctly decrypted private key and ASCII decoding (128×128 pixels), (i) the decrypted false image by an incorrect private key (128×128 pixels).

the 256 gray-level image into binary data.

In this paper, a 256 gray-level Lena image of size 128×128 pixels shown in Fig. 8(a) is used as an input image to be encrypted. Figure 8(b) represents the converted binary data of the Lena image as the plain text to be encrypted, size of which is expanded to 512×256 pixels, where white areas have value of 1 and black areas are 0 numerically. Figure 8(c) shows a random generated binary bit code of size 512×256 pixels as a public key used for encryption and decryption, and a binary plane image of size 512×256 pixels shown in Fig. 8(d) is used as a user's private key (or watermark) to be encrypted for key encryption. The data with 512×256 pixels in size is equivalent to (64×8)×(64×4) pixels, i.e., 64×2048 bits or 128×1024 bits. This means that our configuration has 2,048 DES blocks of data and each block uses its own random generated key to cipher block data. Because the 2-D optical system has a property of parallel processing, there is an effect that 2,048 DES blocks or 1,024 3DES blocks are encrypted simultaneously compared to similar DES operations in digital electronics. Note that this private key can be interpreted as user's own watermark image for authentication application. Figure 8(e) and (f) show the encrypted private key by the public key and the encrypted binary data as the cipher text by the private key, respectively. These encrypted data which are recorded on CCDs have a form of randomness, and are transmitted to the other user. From the proposed optical 3DES cryptographic system, the decryption of the original private key is carried out by the correct public key and the original Lena image is decrypted by the correct decrypted private key and ASCII decoding successfully. Figure 8(g) and (h) show the exactly decrypted private key and Lena image. Figure 8(g) shows the exactly decrypted private key (or watermark) when the correct public key is used for the private key decryption, and Fig. 8(h) shows the exactly decrypted Lena image by the correctly decrypted private key. On the other hand, when we don't know the private key information, we cannot decrypt the original Lena image. Figure 8(i) shows the decrypted false image by an incorrect private key.

IV. CONCLUSION

We propose a novel optical implementation method of a triple DES algorithm based on dual XOR logic operations for a cryptographic system. The optical 3DES system is realized by dual XOR logic operations, where XOR logic operation is implemented by using a free-space interconnected optical logic gate method. The optical schematic of the proposed method has two Mach-Zehnder type interferometers simultaneously. The inner interferometer is used for encrypting a private key with a public key, while the outer interferometer is used for encrypting a plain text with the same private key. The suggested optical setup of the cryptosystem can also be used for the decryption process. The major merit of this optical implemented cryptography is that a vast amount of data can be processed in parallel very quickly and the encryption/decryption processing time is much faster than electronic methods. Also, the encryption/decryption processing time does not diminish in spite of data expansion owing to the parallel processing property. The proposed system is convenient for exchanging the different private keys in the form of cipher and for decrypting the plain text only by the corresponding private key. This fact implies that our scheme can be applied to the OTP encryption if users create different private keys each time at their own discretion. Of course, the proposed dual XOR optical encryption method provides higher security strength to use double key encryption, and has an advantage of simple optical setup configuration. Our proposed method seems to perform 2,048 DES blocks or 1,024 3DES blocks cipher. Besides, because the key length is equal to 512×256 bits, $2^{512\times256}$ attempts are required to find the correct key. Computer experiments verified that the proposed method is perfect and suitable for cryptographic applications and secure communication system.

ACKNOWLEDGMENT

This work was supported by the Incheon National University (International Cooperative) Research Grant in 2011.

REFERENCES

1. B. Schneier, *Applied Cryptography*, 2nd ed. (John Wiley, New York, USA, 1994).
2. C. Li, S. Li, M. Asim, J. Nunez, G. Alvarez, and G. Chen, "On the security defects of an image encryption scheme," Image and Vision Computing **27**, 1371-1381 (2009).
3. B. Javidi and J. L. Horner, "Optical pattern recognition for validation and security verification," Opt. Eng. **33**, 1752-1756 (1994).
4. 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).
5. P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. **20**, 767-769 (1995).
6. B. Javidi, A. Sergent, and E. Ahouzi, "Performance of double phase encoding encryption technique using binarized encrypted images," Opt. Eng. **37**, 565-569 (1998).
7. D. Weber and J. Trolinger, "Novel implementation of nonlinear joint transform correlators in optical security and validation," Opt. Eng. **38**, 62-68 (1999).
8. E. Cuche, F. Bevilacqua, and C. Depeursinge, "Digital holography for quantitative phase-contrast imaging," Opt. Lett. **24**, 291-293 (1999).
9. B. Javidi and T. Nomura, "Securing information by means of digital holography," Opt. Lett. **25**, 28-30 (2000).

10. G. Unnikrishnan and K. Singh, "Double random fractional Fourier domain encoding for optical security," Opt. Eng. **39**, 2853-2859 (2000).
11. 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).
12. T. Nomura, A. Okazaki, M. Kameda, and Y. Morimoto, "Image reconstruction from compressed encrypted digital hologram," Opt. Eng. **44**, 2313-2320 (2005).
13. P. Hariharan, "Digital phase-shifting interferometry: a simple error compensating phase calculation algorithm," Appl. Opt. **26**, 2504-0505 (1987).
14. I. Yamaguchi and T. Zhang, "Phase-shifting digital holography," Opt. Lett. **22**, 610-612 (1998).
15. 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).
16. 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).
17. 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).
18. 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).
19. S. H. Jeon and S. K. Gil, "Dual optical encryption for binary data and secret key using phase-shifting digital holography," J. Opt. Soc. Korea **16**, 263-269 (2012).
20. 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).
21. C.-M. Shin and S.-J. Kim, "Image encryption using modified exclusive-OR rules and phase-wrapping technique," Opt. Commun. **254**, 67-75 (2005).