A Public-key-based Optical Image Cryptosystem with Data Embedding Techniques

Guo-Shiang Lin[1], Hsuan T. Chang[2], Wen-Nung Lie[1], and Cheng-Hung Chuang[1]

[1]Department of Electrical Engineering

National Chung Cheng University, Taiwan, ROC.

E-mail : wnlie@ee.ccu.edu.tw

[2]Department of Electrical Engineering

National Yunlin University of Science and Technology, Taiwan, ROC.

Email : htchang@pine.yuntech.edu.tw

ABSTRACT

In this paper, a public-key-based optical image cryptosystem is proposed for practical secure communications. Conventional encryption algorithms that use the same key in the transmitter and receiver, i.e., a symmetric algorithm, are limited in real applications. The proposed system is based on a hybrid architecture in which the symmetric double random-phase algorithm is used to cipher an image and an asymmetric algorithm is exploited for ciphering the session keys. In addition, the ciphered key is embedded into the quantized amplitude of the complex encrypted data and then transmitted to a receiver for resolving the problem of key delivery. To find a covert channel, we analyze the double random-phase algorithm and obtain two results: the efficacy of the phase mask in the frequency domain is more than the other one in the spatial domain and the amplitude part of the ciphered image is insensitive to little distortion. The experimental results show that the amplitude part in the frequency domain is more suitable than that in the spatial domain to convey secret messages and the reconstructed images with high visual quality can be obtained.

I. INTRODUCTION

Recently, multimedia have accelerated the development of networked systems and introduced many advanced services such as video streaming, tele-conferencing, video on demand, electronic commerce, etc. Due to the real-time requirements, optical devices that have the properties of data storage and retrieval at high speed have been used to practical applications progressively. However, the Internet is perceived as being an unsecured network. Thus information protection has become important and necessary. The security of optical information processing and communication is currently an important issue.

Basically, the encryption algorithms are categorized into the symmetric and asymmetric types [14]. In most of the symmetric algorithms, the encryption key is the same as that used in decryption. Many symmetric algorithms had proposed, e.g., Data Encryption Standard (DES), RC5, and International Data Encryption Algorithm (IDEA) [14]. In brief, encryption and decryption of a symmetric algorithm can be denoted as

$$E(M, K_s) = C,\ D(C, K_s) = M\ , \tag{1}$$

where M, C, $E(\cdot)$, $D(\cdot)$, and K_s denote the plaintext, ciphertext, encryption function, decryption function, and the secret key, respectively. As we can see in Eq. (1), the receiver should have the same key K_s used in encryption to decipher the ciphertext. Thus the secret key must be safely distributed in a secure channel for communication. Therefore, the key delivery between senders and receivers is an important issue in symmetric cryptosystem. On the other hand, the encryption key differs from the key used in decryption in the asymmetric algorithms. A public key K_u is used to encrypt a plaintext in the transmitter and a private key K_p is used to decrypt the ciphertext for reconstructing the plaintext. That is, a sender can use the public key to encrypt messages, but only a receiver who has the corresponding private key

can recover messages. Some asymmetric algorithms were also proposed, e.g., Rivest-Shamire-Adelman (RSA) and ElGamal [14]. In an asymmetric algorithm, encryption and decryption can be denoted as

$$E(M, K_u) = C\ ,\ D(C, K_p) = M\ , \tag{2}$$

where K_u and K_p denote the public and private keys, respectively. As shown in Eq. (2), because the public key is not distributed and the receiver owns the private key, the problem of key delivery need not be considered in an asymmetric algorithm.

Although the asymmetric algorithms are adequately applied to real applications, there are two reasons so that they are not used in place of symmetric algorithms [14]. First, asymmetric algorithms are slower than symmetric ones. Specifically, the speed of software implementation in asymmetric algorithm is far slower than that of symmetric ones. Next, asymmetric cryptosystems are vulnerable to chosen-plaintext attacks. In contrast to an asymmetric algorithm, symmetric ones are not vulnerable to this attack because attackers cannot achieve test cryptosystems with an unknown key. Therefore, a hybrid cryptosystem in which an asymmetric algorithm is used to secure and distribute the session key and a symmetric algorithm with the session key is exploited to cipher/decipher images is designed for most practical implementations. After receiving the ciphered key, a receiver with a corresponding private key can obtain the session key for decryption. Besides, the session keys just used for one communication session will be discarded such that the security of the proposed system increases.

Many optical encryption techniques proposed for security applications [2-3,6-7] use symmetric algorithms to cipher/decipher an image. An optical image encryption method [6] that ciphers and deciphers an image by using the exclusive-OR (XOR) operator had been proposed. First, a graylevel image is converted to eight bit planes. Then the optical XOR

operations between bit planes and random patterns are performed by the polarization encoding method. On the other hand, several optical image encryption methods are based on the double random phase encryption algorithm [3]. Figure 1 illustrates the 4-*f* optical architecture of the double random phase encryption algorithm. These dashed line arrows denote that the light propagates from the left-hand side to the right-hand side in ciphering process. Two random phase masks, one in the input plane (spatial domain) and the other in the Fourier plane (frequency domain), are used to transform an image to complex-value stationary noise in the output plane. That is, the input image is multiplied with a random-phase mask in the spatial domain and then processed with the other one in the frequency domain again to obtain an encrypted image. In decryption as shown in Fig. 1(b), the reconstructed image can be obtained after the encrypted data is processed with the conjugate phase function of the double random phase masks in encryption.

As described above, most of the proposed methods use the same key for encryption and decryption. However, senders still confronts how they securely deliver the secret key to receivers. The security of modern cryptosystems depends on the key used for encryption and is not inherent in knowledge of the algorithm. That is, anyone can decrypt and reach for secret messages when the key is divulged. This is why the key delivery is so significant in cryptograpgy. In contrast to a symmetric encryption algorithm, an asymmetric encryption algorithm that overcomes the problem of key delivery is suitably used in practical applications. Here we propose a hybrid optical cryptosystem in which an image is ciphered/deciphered by using a symmetrical algorithm with a session key that is encrypted/decrypted by using an asymmetric algorithm with public and private keys. Besides, the session key can be transmitted to a receiver through a secret channel. A receiver with a corresponding private key can decipher the transmitted data with the extracted session key.

The organization for the remainder of this paper is as follows. The review of data embedding methods is given in Section II. Section III analyzes that which part of a ciphered image is suitable to convey secret messages and depicts the details of the architecture in the proposed cryptosystem. The simulation results are provided in Section IV. Finally, Section V concludes this paper.

II. EXISTING METHODS OF DATA EMBEDDING

Recently, the data embedding has been a popular research issue. It concerns mainly about embedding a special signal, called an embedded signal, into a transmitted signal, called a cover signal, to create a composite signal, called a stego-signal, without serious degradation to its cover signal. The embedded signal may be some secret data, signatures or copyright marks; the cover signals are distributed in digital formats for images, audio, or video. The attractive applications of data embedding can often be found in two main fields: one is the digital watermarking which provides protection of intellectual property rights and the other is steganography that sets up a covert channel between two parties such that its existence is difficult to be detected by the third party, especially the eavesdroppers and attackers. The major differences between the watermarking and steganography are the robustness and capacity requirements. The capacity of steganographic methods is higher than that of the watermarking, but the robustness of the watermarking schemes is much more than that of steganography for resisting the possible attacks.

Common approaches for image hiding or watermarking can be categorized into the spatial or transform (e.g., Discrete Fourier Transform, Discrete Cosine Transform (DCT), and wavelets) domain methods. The earliest watermarking method [8] that embedded data into the least significant bits (LSBs) of image pixels is a simple scheme with high capacity. But the embedded data are easily removed by simple image processing such as the smoothing and

compression. A statistical approach, Patchwork [9], randomly chooses two distinct areas in an image and lightens or darkens them, respectively, to indicate the presence or absence of a mark. This method shows high resistance to most non-geometric image modifications. In addition, coefficients of transformed cover-signals can be manipulated for hiding message in transform domain [10]-[13]. To be invisible, high frequency components are chosen, while for robustness, low frequency components are preferable. Middle-band components [10], however, make a tradeoff between these two considerations. To reduce visual degradation of the watermarked image, spread spectrum techniques that use a pseudo-random noise sequence for watermark pre-modulation had applied before embedding it into the DCT domain [11]. Lie *et. al*. [12] proposed a public watermarking scheme, which embeds copyright data by altering DCT coefficients with a differential mode in the middle band and retrieves them without the original image. Ogihara *et al*. [13] also proposed a DCT-based steganographic method that controlled the modified amount for each DCT coefficient by using a threshold table and a quality factor.

From the viewpoint of extraction algorithm without/with the original image, the data hiding methods can be categorized into the blind [8-9], [12-13] and the non-blind [10-11] methods, respectively. The external information required for data extraction puts a heavy restriction on practical applications because it is impossible to maintain a very large database that associate the modified images with the corresponding original ones and special parameters. The data hiding technique is also applied to other applications. For example, a data embedding algorithm [17] had proposed to improve performance of error resilience in the H.263 coding standard. It is expected that the picture header or motion vectors could be incorrect for transmitting compressed videos through a highly noisy channel. The decoder cannot correctly work with the wrong header or motion vectors in reconstructing the

transmitted video bit stream. Thus the parity checking bits of the picture header and motion vectors are embedded into half-pixel motion vectors to solve the random errors. Thus, it is also interesting to find and create a secret and suitable channel for key delivery. That is, a covert channel built in the encrypted image can be used to transmit the session key for resolving the problem of key delivery. To set up a covert channel, data-embedding techniques are exploited in the proposed algorithm.

III. A PUBLIC-KEY-BASED OPTICAL IMAGE CRYPTOSYSTEM

To resolve the problem of key delivery, the basic idea is to build a covert channel in the ciphered image for transmitting the session key to receivers. After receiving the ciphered image, the receiver with the corresponding private key can acquire the session key hidden in the received image. The proposed public-key-based optical image cryptosystem is illustrated in Fig. 2. The proposed cryptosystem uses a hybrid architecture that contains three parts: a double random-phase encryption algorithm, an asymmetric encryption algorithm, and a data embedding algorithm. The double random phase encryption algorithm is used to cipher/decipher the input image and the session key is ciphered/deciphered by the use of an asymmetric encryption algorithm for secure key delivery. After the session key is ciphered and embedded into the encrypted image, it is expected that the caused disturbances will lead to degradation of the visual quality in the deciphered image. On the other hand, the little distortion between the original image and the modified one is hardly observed because human eyes are not sensitive enough. The requirement that the decrypted image should be equal to the original one can be also released in an image cryptosystem. However, it is still important to maintain the reconstructed image with a good visual quality.

To reduce the degradation on the decrypted image, the problems are that where the ciphered session key is embedded and how much degradation the embedded key affects the

visual quality of the decrypted image. First, we briefly review the double random phase algorithm. We consider the case of the double phase algorithm whose optical setup is shown in Fig. 1. The encrypted image in the output plane can be described as follows:

$$I^C(x,y) = F^{-1}\{F\{I^O(x,y)\cdot\exp[i2\pi P_s(x,y)]\}\cdot\exp[i2\pi P_f(u,v)]\}, \quad (3)$$

where $I^O(x,y)$ and $I^C(x,y)$ denote the input image and the ciphered one, respectively. $P_s(x,y)$ and $P_f(u,v)$ represent independent phase-only masks, both phases are uniformly distributed in (0,1), and are used in the spatial and frequency domains, respectively. (u,v) and (x,y) are denoted as the spectral and spatial indices, respectively. $F(\cdot)$ and $F^{-1}(\cdot)$ represent the Fourier and inverse Fourier transform, respectively. To reconstruct the deciphered image, the ciphered image is multiplied only with the conjugate function of the random phase masks in the frequency and spatial domains. Because the spatial mask is a phase-only filter, the deciphered image is also obtained by using an image sensor such as a charge-coupled device (CCD) camera. The decrypted image in the output plane can be described as follows:

$$I^D(x,y) = F^{-1}\{F\{I^C(x,y)\}\cdot\exp[i2\pi P_f^*(x,y)]\}\cdot\exp[i2\pi P_s^*(u,v)], \quad (4)$$

where $I^D(x,y)$ represent the decrypted image and $(\cdot)^*$ denotes the conjugate function.

Subsequently, we discuss the effect of each phase mask on ciphering an image in the double random phase algorithm. Figure 3(a) shows an original image. The results of individually using a phase-only mask in the spatial and Fourier domains to cipher an image are shown in Fig. 3(b) and (c), respectively. Compared with Fig. 3(c), Fig. 3(b) shows that only one random phase mask used in the input plane cannot make the image invisible. Because the random phase modification can be removed by using a light intensity detector such as a CCD camera in the output plane. On the contrary, the effect of the random phase mask in the Fourier plane cannot be eliminated. Due to the chaotic phase drifts by using a

random phase in the Fourier plane, it is expected that a random output will be obtained. It means that the phase mask in the Fourier plane plays a major role for image encryption. Compared with Fig. 3(c), Fig. 3(d) shows the output image by using the double random phase algorithm, that is a complex-value stationary noise in the output plane. It is well known that the Fourier transform performs energy compaction on low spectral coefficients for highly correlated data. Because a random phase mask used in the Fourier plane alters the phase relation of each Fourier coefficient, a noise-like output shown in Fig. 3(c) is obtained.

We also analyze the effects of only modifying the phases in the low and high frequency bands in the frequency domain. Here the DC component (i.e., the zero frequency term) is in the center of the Fourier plane: figure 4 depicts the low and high frequency bands. The results obtained by multiplying random phase masks in the low and high frequency bands are shown in Fig. 5(a) and 5(b), respectively. Fig. 5(a) shows that most information of an image is invisible by modifying the phases in the low band and only little information in the middle and high band (e.g., edges) is revealed. As shown in Fig. 5(b), the image is well maintained while whose phase relation the phases in the high frequency band is altered. Thus, the phase relation in the low band is important than that in other bands and can be easily modified to obtain a ciphered image. The phase modification in the high frequency band of the original image only yields little distortion that is insensitive to human eyes.

Ref. 15 shows that the phase information of the encrypted data can recover most content of the image while the amplitude part cannot. Thus, the phase information is more important than the amplitude part in reconstructing the original image. Here we analyze the tolerance of the different forms of the ciphered image for building an appropriate channel to transmit the session key. On the other hand, the fidelity of the modified image is evaluated by the peak-to-signal-noise-ratio (PSNR) which is defined as

$$\mathrm{PSNR} = 10\log_{10}(PW_{cover} / PW_{noise}),$$

where PW_{cover} and PW_{noise} represent signal powers of the cover image and the systematic noise, respectively. The systematic noise is caused from the methodological errors and the embedded messages. The methodological errors and the embedded messages depend on the embedding algorithm and the amount of the hidden secret data, respectively. Thus, the total error causing the degradation of visual quality in a cover image increases while the amount of the embedded data is raised. In other words, the embedded messages should be restrained and spread to obtain a stego-image with good visual quality and avoid the disturbances observed by eavesdroppers.

Because the session key can be embedded into the Fourier and output planes, the schematic diagrams of our proposed system are illustrated in Fig. 6. In this section, we then discuss the effects on the visual quality of the reconstructed image by means of a uniform quantizer applied to the Fourier and spatial planes.

A. The frequency domain

The Fourier coefficients of a ciphered image are complex values and can also be expressed in terms of real and imaginary parts as follows:

$$I^C(u,v) = I_R^C(u,v) + jI_I^C(u,v), \tag{5}$$

where $I_R^C(u,v)$ and $I_I^C(u,v)$ denote the real part and the imaginary part, respectively. In addition, they can also be expressed by using the polar form as follows:

$$I^C(u,v) = \Psi^C(u,v)\angle\psi^C(u,v), \tag{6}$$

where $\Psi^C(u,v)$ and $\psi^C(u,v)$ represent the amplitude part and the phase part, respectively. Due to the manufacturing technologies, the available phase levels in optical devices such as

the diffraction elements are finite in practical implementation and applications. Thus a uniform quantizer is applied to each part of the Fourier coefficients of the ciphered image for evaluating their degradation of visual quality. The results are listed in Table I. It is expected that the PSNRs increase when the quantizarion level increases. Because the quantization step decreases after the quantization level increases, the quantization errors will be diminished to obtain a good visual quality image. It shows that a deciphered image with good quality (>30dB) can be obtained regardless of what part in the frequency domain when the quantization level is larger than 32. The PSNRs of the deciphered image for quantizing amplitude information with different levels are higher than others in Table I. It means that the quantization error introduced in the amplitude part of the Fourier coefficients leads to little disturbance. Thus, a covert channel can be set up in each part of the Fourier coefficients while the quantization level is more than 32 and suitably built in the amplitude part while the quantization level is down to 16, especially.

B. The spatial domain

In the same manner, the ciphered image obtained in the output plane of encryption can be expressed in terms of real and imaginary parts as follows:

$$I^C(x,y) = I_R^C(x,y) + jI_I^C(x,y), \tag{7}$$

where $I_R^C(x,y)$ and $I_I^C(x,y)$ are denoted as the real part and the imaginary part, respectively. In addition, it can be also expressed by using the polar form as follows:

$$I^C(x,y) = \Psi^C(x,y)\angle\psi^C(x,y), \tag{8}$$

where $\Psi^C(x,y)$ and $\psi^C(x,y)$ denote the amplitude part and the phase part, respectively. Here a uniform quantization is applied to each part of the ciphered image in the spatial domain for evaluating the visual quality. As shown in Table II, a deciphered image with good

quality can be obtained regardless of what part in the spatial domain when the quantization level is larger than 32. The PSNRs of the deciphered image for quantizing phase information with different levels are lower than those of the other parts in Table II. That is, the phase part is sensitive to the quantization error in reconstructing an image. Table II also shows that the PSNRs in the amplitude part are higher than those in the other parts. That is, the quantization error introduced in the amplitude part of the Fourier coefficients leads to the lesser disturbance. The PSNRs are higher even than 30 dB when the quantization level is down to 16. This result is similar to that in the Fourier plane. Thus, a covert channel set up in the amplitude part of a ciphered image is more suitable than the other ones.

Although the amplitude parts of a ciphered image in the frequency and spatial domains are more suitable than the other ones to convey the transmitted messages, the fidelity of the ciphered image should be also maintained after the secret messages are hidden. Another considered problem is where is used to convey the secret messages as the reconstructed image with a good visual quality. That is, the position for embedding the secret messages must be carefully chosen (especially for the case in the Fourier plane). On the other hand, a data embedding algorithm with blind recovery is necessary to retrieve the hidden messages in practical circumstances. To allow the blind recovery of the embedded data, we always embed them into the specific places. In the Fourier plane, the gray region depicted in Fig. 5 is used to hide secret messages and denoted as Ω_H. In the spatial domain, secret data are randomly embedded in a ciphered image. To reduce the degradation caused by the embedded data, the ciphered messages are embedded into the LSBs of the quantized amplitude part in the frequency and spatial domains.

Since secret messages can be embedded into the frequency or spatial domain, the steps of the encryption in our system are described as follows.

1. The session keys K_s and K_f are used to generate two random phase masks $P_s(x)$ and $P_f(x)$ to cipher an image by using Eq. (3).

2. The amplitude part is quantized with *L* levels.

$$\left|\Psi_Q^C(p,q)\right| = \mathbf{Q}_L(\left|\Psi^C(p,q)\right|), \tag{7}$$

where $\mathbf{Q}_L(\cdot)$ denotes a quantizer with *L* levels and $\left|\Psi_Q^C(p,q)\right|$ represents the quantized amplitude part in the frequency or spatial domain.

3. The session keys K_s and K_f are ciphered by an asymmetric method with the public key K_u. To increase the efficiency of a public key encryption, we concatenate the values of two session keys to form a larger one before ciphering and the ciphering function can be described as

$$E_{K_u}([K_s \mid K_f]) = m, \tag{8}$$

where $E_{K_d}(\cdot)$ represents an asymmetric encryption function, "|" is a concatenation operator, and *m* represents the result of the asymmetric encryption function.

4. In general, *m* is a large value with possibly hundreds of digits and can be represented as a binary bit stream $\{b_1, b_2, ..., b_n\}$. This stream is embedded, bit by bit, into the quantized amplitude part in the frequency or spatial domain. The embedding rule that modifies the LSBs of the quantized amplitude part to embed the binary bit stream is expressed by

$$\left|\Psi_Q^{C,H}(p,q)\right| = \begin{cases} \left|\Psi_Q^C(p,q)\right| - \mathrm{sgn}(\left|\Psi_Q^C(p,q)\right|), & \text{if } b_i = 1 \text{ and } \left|\Psi_Q^C(p,q)\right| \%2 = 0 \\ \left|\Psi_Q^C(p,q)\right| - \mathrm{sgn}(\left|\Psi_Q^C(p,q)\right|), & \text{if } b_i = 0 \text{ and } \left|\Psi_Q^C(p,q)\right| \%2 = 1 \\ \left|\Psi_Q^C(p,q)\right|, & \text{otherwise} \end{cases}, \left|\Psi_Q^{C,H}(p,q)\right| \in \Omega, \; i=1,..,n.$$

where $\left|\Psi_Q^{C,H}(p,q)\right|$ represents the quantized amplitude part of the input data after hiding the session keys, sgn(·) and % denote the signum function and modular operator, respectively. The symbol Ω is defined as the embedding area for hiding secret messages. In the frequency domain, the secret data are hidden into the high frequency band Ω_H, that is, $\Omega = \Omega_H$. If we embed the secret data in the spatial domain, the Ω is denoted as the randomly-chosen specific position.

5. The ciphered image obtained in the output plane can be described by the following equations (9) and (10) for embedding the encrypted result *m* into the spatial and Fourier planes, respectively.

$$I^{C,H}(x,y) = \mathbf{Q}^{-1}(\left|\Psi_Q^{C,H}(p,q)\right|)\angle\psi(p,q), \tag{9}$$

$$I^{C,H}(x,y) = F^{-1}\{\mathbf{Q}^{-1}(\left|\Psi_Q^{C,H}(p,q)\right|)\angle\psi(p,q)\}, \tag{10}$$

where $\mathbf{Q}_L^{-1}(\cdot)$ denotes a de-quantizer with *L* levels and $I^{C,H}(x,y)$ represents a ciphered image in the output of the encryption after ciphering and hiding.

To correctly obtain the reconstructed image, the hidden session keys should be retrieved before decryption. After data extraction and deciphering to acquire the session keys used in the encryption, we can reconstruct the output image by using the double random-phase decryption with the retrieved keys. Steps of the decryption algorithm are reverse to those in our encryption algorithm and described as follows:

1. The amplitude part of the received image in the frequency or spatial domain is quantized with *L* levels.

$$\left|\Psi_Q^{C,H}(p,q)\right| = \mathbf{Q}_L(\left|\Psi^{C,H}(p,q)\right|), \tag{11}$$

2. Extracting the embedded bit stream $\{b_1, b_2, ..., b_n\}$ from the received image by using the rule,

$$\{b_1, b_2, ..., b_n\} = \begin{cases} b_i = 1, & \text{if } \left|\Psi_Q^{C,H}(p,q)\right| \%2 = 1 \\ b_i = 0, & \text{if } \left|\Psi_Q^{C,H}(p,q)\right| \%2 = 0 \end{cases}, \ \left|\Psi_Q^{C,H}(p,q)\right| \in \Omega_H, \ i=1,\ldots,n.$$

3. Deciphering *m* by using an asymmetric method with the private key K_d via

$$D_{K_d}(m) = [K_s \mid K_f], \tag{12}$$

where $D_{K_d}(\cdot)$ represents an asymmetric decryption function.

4. The extracted keys K_s and K_f are used to decipher and obtain an output image in the double random phase encryption algorithm by using Eq. (4).

IV. COMPUTER SIMULATION

A. Experimental Results

To evaluate the performance of the proposed cryptosystem, two 256×256 images, Lena and Jetplane, with 8-bit grayscale resolution are used in our experiments. To cipher the session keys used in the double random-phase algorithm, the well-known asymmetric encryption algorithm, RSA [14], is used. To evaluate the visual quality, the PSNR is used to measure the difference between the original and the reconstructed images. Figures 7 and 8 show the results of our proposed algorithm by embedding secret messages into the frequency and spatial domains, respectively. Figure 7(b)~7(d) demonstrate the experimental results for the Lena image shown in Fig. 7(a). As shown in Fig. 7(b), the input image is well transformed to a white noise pattern. To embed the message *m* whose size is 676 bits, the ciphered images with different quantization levels (L=16 and 64) are shown in the Fig. 7(c) and 7(d), respectively. Although the secret messages are hidden into the Fourier coefficients of the ciphered image, Fig. 7(c) shows that a good visual quality (32.76dB) is maintained between

the reconstructed image and original one. While the quantization level is up to 64, the PSNR of the ciphered image shown in Fig. 7(d) is higher than 44dB.

Figure 8 demonstrates the simulation for the Jetplane image. Fig. 8(a) and 8(b) show the original image and the ciphered one whose amplitude part in the spatial domain is used to convey the secret data, respectively. Fig. 8(b) shows the processed image is well ciphered because no information is revealed. To hide the message m whose size is 2209 bits, the ciphered images with different quantization levels (L=16 and 64) are shown in Fig. 8(c) and 8(d), respectively. The reconstructed image with acceptable quality (29.67dB) is shown in Fig. 8(c). A good quality (40.95dB) is obtained in Fig. 8(d) while the quantization level is 64.

To enhance the security capability of the proposed cryptosystem against attacks, the length of the session keys should be enlarged, i.e., the number of the embedded bits should be increased. After embedding different bits of secret data and quantizing the embedded data with different levels in the frequency and spatial domains, the results of visual quality are shown in Table III and IV, respectively. As we can see, the PSNRs raise while the quantization level increase, too. Good visual quality (>30dB) can be achieved regardless of in the spatial or frequency domain while the quantization level is more than 32. Compared with Table I, the PSNRs in the Table III are less than those in the Table I when the 676 bits are embedded. The similar results are also shown in the spatial domain by comparing Tables II and IV. Considering the ‘Lena’ image, the differences of PSNRs between Table I and III introduced by data embedding are less than 0.45dB. In the same manner, the differences of PSNRs between Table II and IV are less than 1.2 dB. If the bits of the embedded messages are raised from 676 to 2209 in the same quantization level, the differences of visual quality for each test image are less than 2.13dB and 2.2 dB in the frequency and spatial domains, respectively. Therefore, it is obvious that the degradation in the frequency domain is generally

less than that in the spatial domain when 676 bits are embedded. When a number of bits are hidden, it is expected that the degradation in the frequency and spatial domains increases.

B. Security Analysis

To decrypt a scrambled image, several types of attacks can be used to break the crypto-system. The first one is the ciphertext-only attack [14], [16]. In this type of attack, the illegal users are assumed to have only an encrypted image and do not have the session keys. Because illegal users cannot obtain the session keys K_s and K_f, they cannot reconstruct the original image faithfully. Supposing that the illegal users try to conjecture the session key K_f by using brute force search. It is time-consuming to find the true one K_f. Supposing that illegal users try to obtain the session keys K_s and K_f by factoring large numbers in an asymmetric encryption algorithm, it is impossible to achieve this purpose with a fast computer within a reasonable time interval [14]. The difficulty of factoring a large number is proportional to its number of bits. Thus the number of bits can be increased to withstand this attack for improving the security.

The known-plaintext and chosen-plaintext attacks are more powerful and common than the ciphertext-only attack [14],[16]. For these two attacks, illegal users are assumed to have not only the encrypted image but also several original ones. In these cases, illegal users can analyze the encrypted image to infer the session keys (i.e., K_s and K_f) and decrypt the next image correctly if the provider still encrypts image with the same session keys. The session keys are produced when secure communication happens and destroyed when they are not no longer needed. Thus it is hard to deduce the session keys from the whole image by known-plaintext or chosen- plaintext attack.

Because we set up a covert channel in the ciphered image to transmit the secret messages, it is expected that a meaningless and noise-like output will be obtained after the eavesdropper attack the ciphered image by using some processing such as smoothing to destroy the secret channel. The eavesdropper cannot still obtain the original image. On the other hand, if the attackers want to extract the hidden messages to break our proposed cryptosystem after they illegally obtain the exact position used for data embedding, they also face to break the RSA algorithm for thieving the transmitted image. If not, it is similar to the ciphertext-only attack that is time-consuming and very arduous.

V. CONCLUSIONS

A public-key-based optical image cryptosystem is proposed for practical secure communications in this paper. Conventional optical encryption algorithms that use the same key in the transmitter and receiver (i.e., symmetric architecture) are not suitable in practical circumstance. They confront an important problem that the secret key should be securely transmitted to the receiver in practical applications. In order to overcome the key delivery problem, we first analyze the effect of each phase mask on ciphering an image in the double random-phase algorithm. The result that the effectiveness of the phase mask processed in the frequency domain is more than that in the spatial domain is observed. Besides, another result that the amplitude parts of the ciphered image in Fourier and spatial domains are insensitive to little distortion is obtained. It means that the amplitude parts of the ciphered image are suitable to set up a covert channel. Thus, a public-key-based cryptosystem with hybrid architecture is adopted. Our system utilizes the double random-phase algorithm and an asymmetric one to cipher an image and the session keys, respectively. In addition, the ciphered session keys are embedded into the quantized amplitude part in the frequency or spatial domain and transmitted to the receiver for resolving the problem of key delivery. The

experimental results show that the reconstructed images with high visual quality can be obtained.

ACKNOWLEDGEMENTS

This work was supported in part by the National Science Council, ROC., under contract number 90-2213-E-224-030.

REFERENCES

[1] J.W. Goodman, *Introduction to Fourier Optics*, Second Edition, Singapore, McGraw-Hill, 1996.

[2] L.E.M. Brackenbury and K.M. Bell, "Optical encryption of digital data," *Applied Optics*, vol. 39, no. 29, pp. 5374-5379, October 2000.

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

[4] F. Goudail, F. Bollaro, B. Javidi, and P. Refregier, "Influence of a perturbation in a double phase-encoding system," *Journal of Optical Society of America*, vol. 15, no. 10, pp. 2629-2638, October, 1998.

[5] J.-W. Han, S.-H. Lee, and E.-S. Kim, "Optical key bit stream generator," *Optical Engineering*, vol. 38, no. 1, pp. 33-38, Jan 1999.

[6] J.-W. Han, C.-S. Park, D.-H. Ryu, and E.-S. Kim, "Optical image encryption based on XOR operations," *Optical Engineering*, vol. 38, no.1, pp. 47-54, Jan. 1999.

[7] B. Jadivi, A. Sergent, G. Zhang, and L. Guilbert, "Fault tolerance properties of a double-phase encoding encryption technique," *Optical Engineering*, vol. 36, no. 4, pp. 992-998, 1997.

[8] R. G. Van Schyndel, A. Z. Trikel, and C. F. Osborne, "A Digital Watermark," *Proc. Of*

IEEE Int'l Conf. On Image Processing, pp. 86-90, 1994.

[9] W. Bender, D. Gruhl, N. Morimot, and A. Lu, "Techniques for Data Hiding," *IBM Syst. J.*, Vol. 35, No. 3/4, pp. 313-336, 1996.

[10] Chiou Ting Hsu and Ja Ling Wu, "Hidden Digital Watermarks in Images," *IEEE Transactions on Image Processing*, Vol. 8, No. 1, pp. 58-68, January 1999.

[11] I. J. Cox, Joe Kilian, F. Thomson Leighton, and Talal Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," *IEEE Transactions on Image Processing*, Vol. 6, No. 12, pp. 1673-1687, Dec. 1997.

[12] Wen-Nung Lie, Guo-Shiang Lin, and Chih-Liang Wu, "Robust Image Watermarking on the DCT Domain," *IEEE International Symposium on Circuits and Systems*, May 2000.

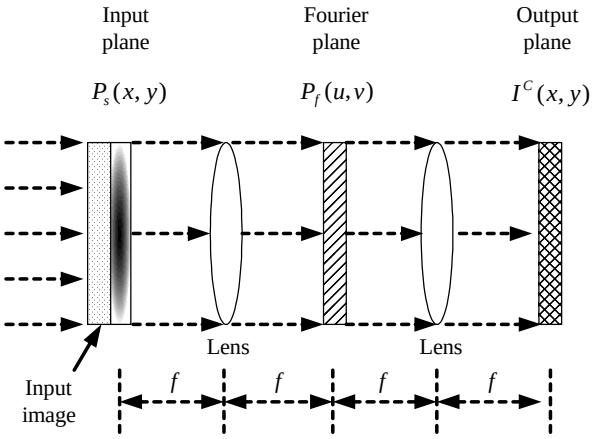
[13] T. Ogihara, D. Nakamura and N. Yokoya, "Data Embedding into Pictorial with Less Distortion Using Discrete Cosine Transform," *Proc. of ICPR '96*, pp. 675-679, 1996.

[14] B. Schneier, *Applied Cryptography, Second Edition, Protocols, Algorithms and Source Codes in C*, John Wiley & Sons, Inc., 1996.

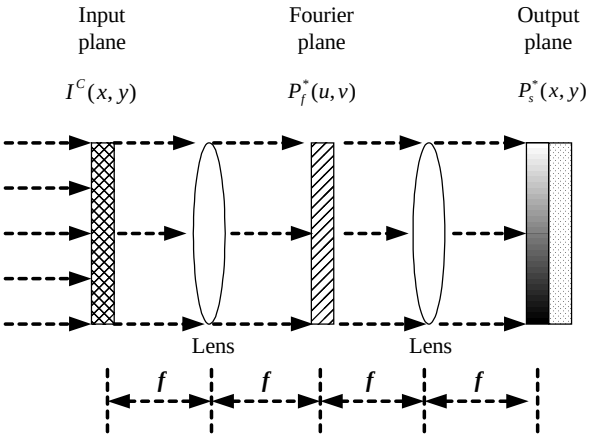
[15] B. Javidi, A. Sergent, and E. Ahouzi, "Performance of double phase encoding encryption technique using binarized encrypted images," *Optical Engineering*, vol. 37, no. 2, pp. 565-569, 1998.

[16] Tung-Shou Chen, Chin-Chen Chang; Min-Shiang Hwang, "A virtual image cryptosystem based upon vector quantization" *IEEE Transactions on Image Processing*, pp. 1485 – 1488, Vol. 7, Oct. 1998.

[17] Jie Song Liu and K. J. R., "A data embedding scheme for H.263 compatible video coding," *ISCAS '99*, vol.4, pp. 390 – 393, 1999.



(a)



(b)

Fig. 1 Optical setup of the double phase encryption algorithm. (a) Encryption and (b) Decryption.

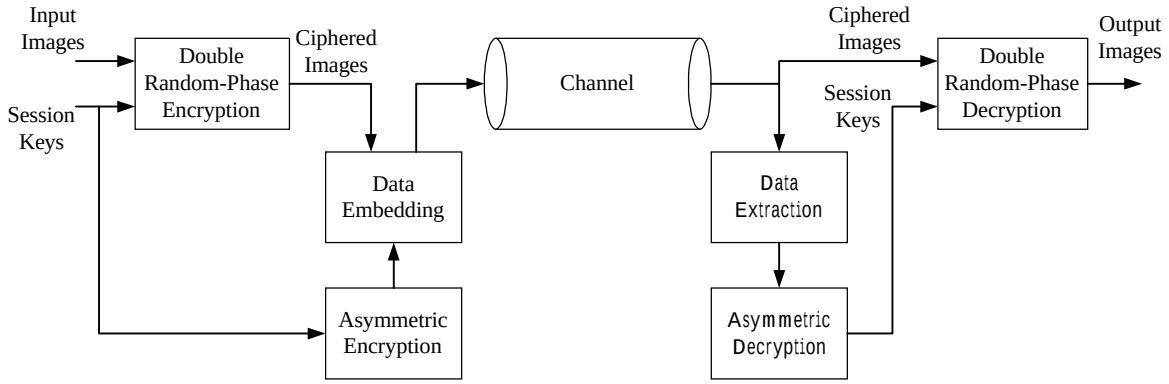
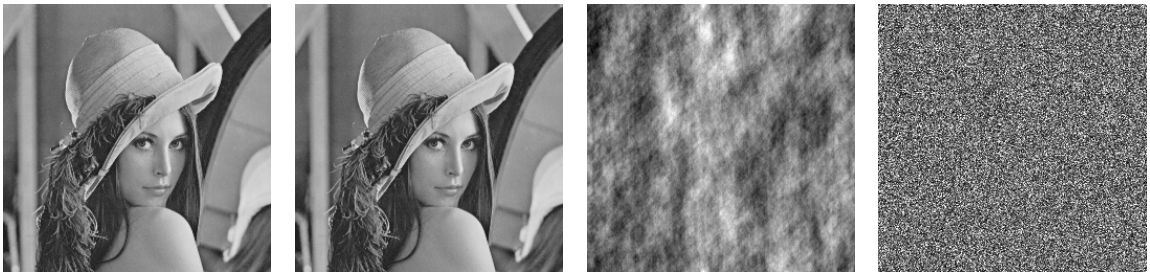


Fig. 2 The flowchart of our proposed optical cryptosystem.



(a) (b) (c) (d)

Fig. 3 (a) original image, the ciphered images by only using a random phase (b) in the input plane, (c) in the Fourier plane, and (d) another ciphered image by using the double random phase algorithm [3].

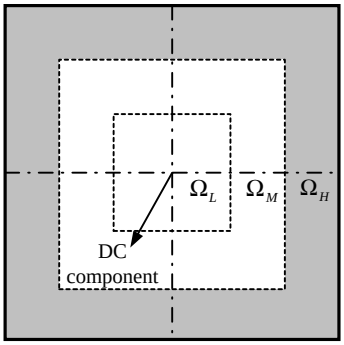
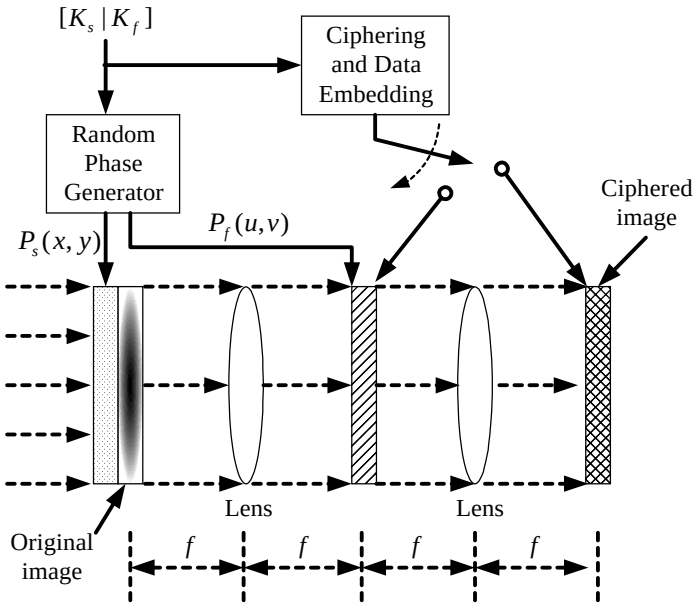


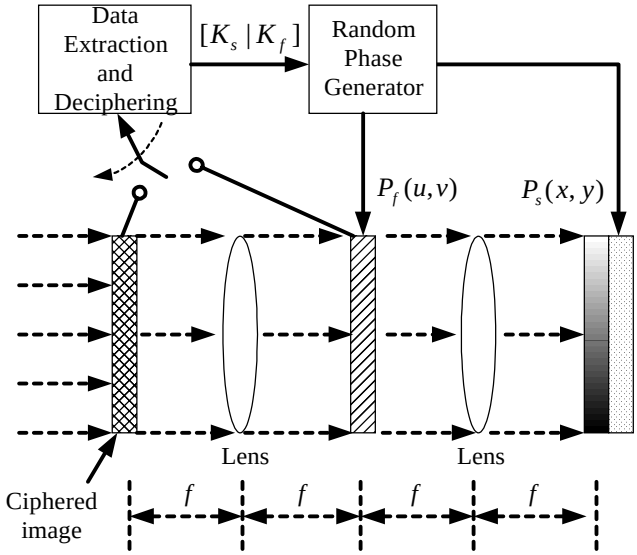
Fig. 4 Positions of the low, middle, and high bands in the frequency domain.

(a) (b)

Fig. 5 The images ciphered by only modifying the phases (a) in the low frequency band and (b) in the high frequency band.

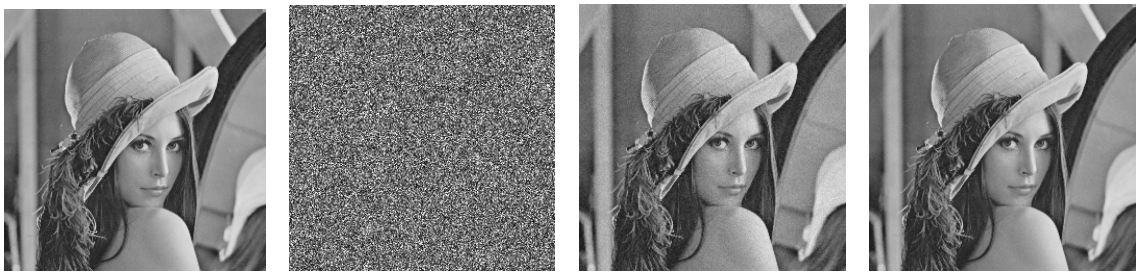


(a)



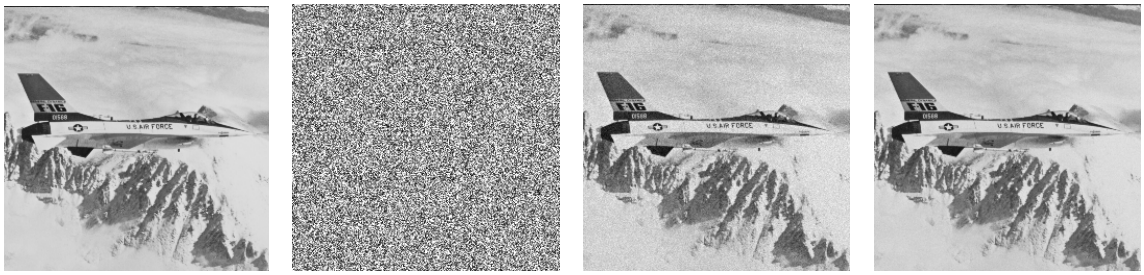
(b)

Fig. 6 Schematic diagrams of a public-key-based optical image cryptosystem. (a) Encryption and (b) Decryption.



(a) (b) (c) (d)

Fig. 7 (a) Original image ‘Lena’, (b) the ciphered image, (c) the reconstructed image (L=16), and (d) another reconstructed one (L=64).



(a) (b) (c) (d)

Fig. 8 (a) Input image ‘Jetplane’, (b) the ciphered image, (c) the reconstructed image (L=16), and (d) another reconstructed one (L=64).

Table I The results of different parts of the reconstructed images after quantization with different levels in the Fourier plane.

Quantization Levels	Lena PSNR (dB)				Jetplane PSNR (dB)			
	Real	Imaginary	Amplitude	Phase	Real	Imaginary	Amplitude	Phase
8	23.03	22.08	27.48	21.76	19.36	18.90	24.17	18.84
16	28.20	27.54	33.10	27.65	25.32	25.08	30.04	24.72
32	33.34	34.26	39.44	33.61	31.49	31.13	36.84	30.74
64	40.07	40.78	44.99	39.69	35.97	36.91	41.97	36.77

Table II The results of different parts of the decrypted images after quantization with different levels in the output plane.

Quantization Levels	Lena PSNR (dB)				Jetplane PSNR (dB)			
	Real	Imaginary	Amplitude	Phase	Real	Imaginary	Amplitude	Phase
8	21.73	22.23	27.12	21.83	18.97	19.12	23.90	18.88
16	27.56	27.97	33.15	27.61	24.77	24.90	30.50	24.75
32	33.68	34.45	39.42	33.61	30.97	31.06	36.19	30.76
64	40.00	39.78	45.09	39.68	37.49	37.55	42.41	36.73

Table III The visual quality of the reconstructed image for different embedded bits and quantization levels in the frequency domain.

Quantization Levels	Lena PSNR (dB)		Jetplane PSNR (dB)	
	676 bits	2209 bits	676 bits	2209 bits
8	27.12	26.79	23.99	23.41
16	32.76	31.07	29.83	29.31
32	39.14	37.58	36.22	35.22
64	44.05	44.09	41.64	41.41

Table IV The visual quality of the reconstructed image for different embedded bits and quantization levels in the spatial domain.

Quantization Levels	Lena PSNR (dB)		Jetplane PSNR (dB)	
	676 bits	2209 bits	676 bits	2209 bits
8	26.85	26.34	23.28	21.85
16	32.10	32.01	29.86	29.67
32	38.29	38.09	35.62	34.47
64	44.61	42.99	41.46	40.95