The Optical Image Cryptosystem with a Position-selected Data Embedding Technique

Cheng-Hung Chuang
Dept. of CSIE, Asia University
chchuang@asia.edu.tw

Guo-Shiang Lin
Dept. of CSIE, Da-Yeh University
khlin@mail.dyu.edu.tw

ABSTRACT

In this paper, an optical cryptosystem with a position-selected data embedding technique is proposed for practical secure communications. The optical cryptosystem employs a two-random-phase encryption algorithm to cipher images and a position-selected data embedding technique to hide the secret keys into ciphered images. The secret keys are extracted and used to decipher images in the receiver side. Experimental results show that the newly proposed system has a higher visual quality of reconstructed images than the conventional one.

Keywords: data embedding, data hiding, data encryption, image cryptosystem, optical security.

1. INTRODUCTION

Due to the advanced multimedia and communication technologies in these years, it is very convenient to acquire multimedia applications and services such as video streaming, Internet access, video on demand, tele-conferencing, etc. Unfortunately, the unauthorized use of multimedia data appears rapidly and popularly as the convenience of accessing multimedia data raises. Therefore, it is important to authenticate the use of multimedia data, protect copyright or ownership of multimedia data, transmit multimedia data securely, and defend the communication security. A lot of data hiding, data embedding, and data encryption techniques have been developed to accomplish these goals [1–12].

Data hiding techniques [1–3] refer to methods of hiding or embedding secret information into multimedia data. This multimedia data is often called host signals or cover signals. The main purpose is to create data embedded signals without degenerating host signals seriously. Most importantly, any unauthorized users will not be aware of the existence of the hidden or embedded data in the data embedded signals. The virtual image cryptosystem or image steganographic methods [4, 5] are proposed to hide the secret images into cover images which are readable but non-critical. This image steganography is designed to reduce the notice of illegal users. However, the distortion of decrypted secret images is allowed due to the difficulty of encrypting a large amount of image data.

Common methods for data hiding can be categorized into spatial and transform domain methods. The earliest data hiding method, which is simple and has high embedding capacity, embedded data into least significant bitplanes (LSB) of image pixels (i.e. spatial domain). There are some LSB-based data hiding algorithms proposed in literature [6, 7] to reduce embedding distortion of host signals. Additionally, in the transform domain, e.g. discrete Fourier transform, discrete cosine transform (DCT), or wavelets, transformed coefficients of host signals can be manipulated to hide data.

Contrarily, data encryption techniques use some reliable algorithms or secret keys to transform or encrypt secret data into ciphered data [8, 9]. The ciphered data is usually unreadable, invisible, or incomprehensible during transmission [8]. Only the authorized users can decrypt the secret data from the ciphered data. Any illegal users, who grab the ciphered data without knowing the decryption algorithms or the secret keys, will obtain meaningless and non-recognizable data. One important issue of data encryption techniques is that the decrypted data must be identical to the original secret data.

On the other hand, due to the requirement of real time applications, optical devices that have the properties of data storage and retrieval at a high speed have been developed. Many optical encryption techniques had been proposed for security applications [9–12]. In [11], an optical image encryption method that ciphers and deciphers images by using the XOR operator was proposed. After an input image is converted to eight bit planes, the optical XOR operations between bit planes and random patterns are performed by polarization encoding method. In [12], the two-phase encryption method was proposed to apply two random phase masks, one is in the spatial domain and the other is in the Fourier domain, to cipher images.

In [9], a public-key-based optical image cryptosystem based on data embedding techniques was proposed. In this optical image cryptosystem, a two-random-phase encoding algorithm is applied to cipher and decipher images with secret keys. Moreover, a public-key type of secret data is employed based on a LSB data embedding technique for secure communication. However, in this conventional system, data is successively embedded into a fixed area. In this study, we propose a more adaptive embedding method to hide the secret data. The embedding positions are selected through a feature discriminant. This method increases not only the visual quality of reconstructed images but also the security. In the experiment, the results of proposed method have a higher image visual quality than those of the conventional method.

2. BACKGROUND

The purpose of the optical image cryptosystem proposed in [9] is to construct a speedy and secure multimedia transmission system with a high image visual quality for real time application. In this system, the secret keys are used to generate two random phase masks for ciphering and deciphering images. These secret keys are encrypted with public keys by a public-key type encryption (asymmetric) algorithm. Then the encrypted (secret) data is embedded into the ciphered image signals. These signals are delivered to the receiver side and extracted to get the hidden data. Authorized users can utilize their private keys of the asymmetric algorithm to decrypt the hidden data and obtain the secret keys. Then these secret keys are applied to decipher images. Thus authorized users can observe the multimedia signals. The $4f$ (f is the focal length of lens) optical architecture is shown in Fig. 1.

In this optical image cryptosystem, the secret data is embedded into the LSBs of the quantized coefficients in the Fourier transform (frequency) domain or the spatial domain (the output plane of the two-random-phase encryption). In this paper, the processing will be focused on the Fourier domain. In Fourier domain, three frequency components are analyzed, i.e. low, middle, and high frequency bands shown in Fig. 2. The high frequency band is chosen for imperceptibility, while the low frequency band is picked for robustness. Besides, the middle frequency band represents a compromise between them. In [9], the secret data is always hidden in a fixed area of the high frequency band, e.g., the gray region Ω_H in Fig. 2. However, the way of fixed embedding area decreases the security; moreover, the image visual quality is not good enough when the quantization level of

transformed coefficients is low.

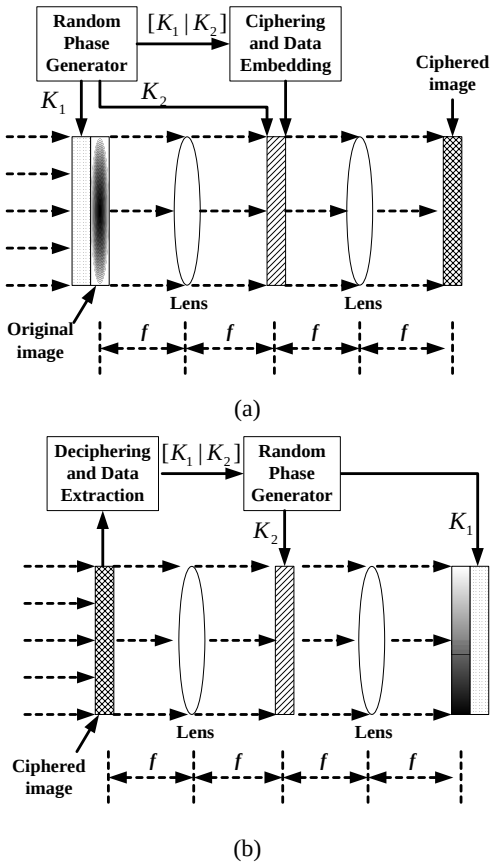

Fig. 1 The 4*f* optical architecture. (a) Encoding (transmitter) side and (b) Decoding (receiver) side.

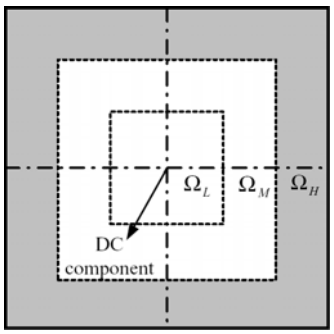

Fig. 2 Bands of the low (Ω_L), middle (Ω_M), and high (Ω_H) frequency in the Fourier domain.

3. METHOD

To improve the deciphered image visual quality of the optical cryptosystem, a position-selected data embedding technique is proposed to hide the secret data. In the Fourier domain of the image cryptosystem, all coefficients are complex numbers, in which the real and imaginary parts can be used to hide secret data. The complex number forms can be defined as

$$I_f = \alpha + i\beta, \qquad (1)$$

where I_f is the image Fourier domain, α and β are values of real and imaginary parts in the Fourier domain. Then secret messages are embedded into LSBs of the quantized values. The issue is how to select the regions or positions that result in low distortion in the reconstructed images when their LSBs are modified. In this paper, we will focus on the real part of coefficients in the Fourier domain.

In the newly proposed method, the embedding positions with smaller absolute values are preferable since they have small energy and small quantization step size. Moreover, they should be different among different images to enhance security. Furthermore, it is necessary to keep the embedding and extracting sequences invariant. Therefore, in our strategy, a feature discriminant is proposed to select the embedding positions. The feature discriminant is described as

$$D = \delta \cdot \max(\alpha), \quad \delta < 1 \qquad (2)$$

where D is the discriminant, δ is an adjustment parameter, max(.) is the maximal value function, and α is values of real parts in the Fourier domain. When the value α of a position is smaller than D, this position is selected to hide data. Otherwise, it is not embedded. That is, D is a threshold value to determine whether the position is embedded data or not. Since each value that is larger than D will not be modified, the value $\max(\alpha)$ in both transmitter and receiver sides will be identical. The parameter δ is adjustable. When δ is small, the D value is also small and it will result in a better performance. However, it

may lead to the lack of embedding positions when δ is too small. The sequence of frequency bands for hiding data is high, middle, and low bands (i.e., Ω_H, Ω_M, and Ω_L in Fig. 2).

Figure 3 shows the illustration of the embedding position maps of the newly proposed method and the conventional one. There are total 52 bits to hide in 52 positions. The black dots mean the positions where data is embedded while the white dots denote those positions where data is NOT embedded. That is, the feature values in these white dots are not smaller than *D*. The embedding positions in the left map are selective according to the discriminant *D*. However, the embedding positions in the right map are successive and fixed.

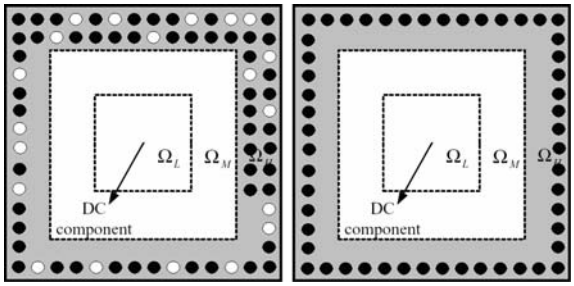

Fig. 3 The illustration of the embedding position maps of the newly proposed method (left) and the conventional one (right).

4. EXPERIMENT

In this experiment, the peak-to-signal-noise-ratio (PSNR) is used to evaluate the visual quality of the reconstructed images. The conventional method [9], where data is hided in the high-frequency band in Fourier domain, is performed for comparison. There are one hundred various 512×512 (8-bit grayscale) images used for experiment. The size of embedded data is 9216 bits. The adjustment parameter δ is set to 0.0625. Figure 4 plots PSNRs of the reconstructed images of the one hundred images, where the upper line stands for results of the new method and the lower line represents those of the conventional one. The mean PSNRs are 34.8716 dB and 29.7856 dB for the new method and the conventional one, respectively. The PSNR promotes about 5 dB for each image. Figure 5 shows some sample reconstructed images. The images in left column are results of the new method while the images in right column are those of the conventional one. The PSNRs of them are shown in Table 1. In Fig. 5(d), the image distortion is obvious in the plain regions; however, a better visual quality is obtained in Fig. 5(c).

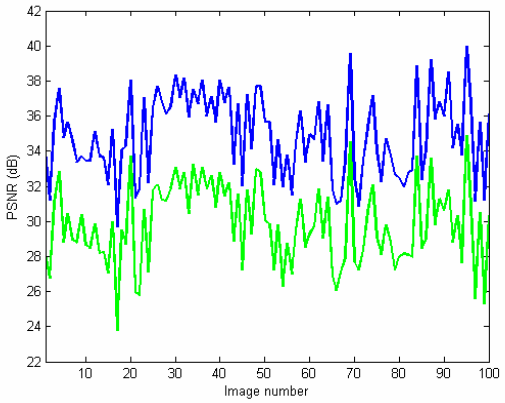

Fig. 4 The PSNR plot of the reconstructed images using the new method (upper) and the conventional one (lower).

5. CONCLUSIONS

The optical image cryptosystem based on the position-selected data embedding technique is presented in this paper. The secret key delivery is accomplished by using this data embedding technique. In this technique, a feature discriminant is used to find the superior embedding positions. Thus the LSB based data embedding method can provide the image cryptosystem with the advantage of low embedding distortion and high security. The experiment shows a higher image visual quality of the new system than that of the conventional one. Furthermore, the position-selected data embedding technique can serve as a dynamic embedding system when a dynamic parameter δ is applied.

Fig. 5 The sample reconstructed images. (Left column: results of new method; Right column: results of conventional method.)

Table 1 PSNRs of Fig. 5

Figure name	PSNR (dB)
Fig. 5(a) / Fig. 5(b)	34.0873 / 29.0327
Fig. 5(c) / Fig. 5(d)	31.8612 / 25.7789
Fig. 5(e) / Fig. 5(f)	33.4606 / 28.6441
Fig. 5(g) / Fig. 5(h)	34.2922 / 28.6882
Fig. 5(i) / Fig. 5(j)	35.8304 / 29.8040
Fig. 5(k) / Fig. 5(l)	37.0473 / 30.6960

ACKNOWLEDGMENTS

This research was supported by the National Science Council, Taiwan, under the grant of NSC96-2218-E-468-003.

REFERENCES

[1] M. Wu and B. Liu, “Data hiding in images and videos: Part I—Fundamental issues and solutions,” IEEE Trans. Image Processing, vol. 12, pp. 685–695, 2003.

[2] M. Wu, H. Yu, and B. Liu, “Data hiding in images and videos: Part II—Designs and applications,” IEEE Trans. Image Processing, vol. 12, pp. 696–705, 2003.

[3] T.-H. Lan and A.H. Tewfik, “A novel high-capacity data-embedding system,” IEEE Trans. Image Processing, vol. 15, pp. 2431–2440, 2006.

[4] Y.-C. Hu, “High-capacity image hiding scheme based on vector quantization,” *Pattern Recognition*, vol. 39, no. 9, pp. 1715–1724, 2006.

[5] C.-C. Chang, C.-Y. Lin, and Y.-Z. Wang, “New image steganographic methods using run-length approach,” *Information Sciences*, vol. 176, no. 22, pp. 3393–3408, 2006.

[6] C.-C. Chang, J.-Y. Hsiao, and C.-S. Chan, “Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy,” *Pattern Recognition*, vol. 36, no. 7, pp. 1583–1595, 2003.

[7] C.-K. Chan and L.M. Cheng, “Hiding data in images by simple LSB substitution,” *Pattern Recognition*, vol. 37, no. 3, pp. 469–474, 2004.

[8] M. Yang, N. Bourbakis, and Li Shujun, “Data-image-video encryption,” *IEEE Potentials*, vol. 23, no. 3, pp. 28–34, 2004.

[9] G.-S. Lin, H. T. Chang, W.-N. Lie, and C.-H. Chuang, “A public-key-based optical image cryptosystem based on data embedding techniques”, *Optical Engineering*, vol. 42, no. 8, pp. 2331–2339, 2003.

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

[11] 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.

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