Data Steganography for Optical Color Image Cryptosystems

Cheng-Hung Chuang chchuang@asia.edu.tw
Department of Computer Science and Information Engineering
Asia University
Taichung County, 41354, Taiwan

Guo-Shiang Lin khlin@mail.dyu.edu.tw
Department of Computer Science and Information Engineering
Da-Yeh University
Changhua County, 51591, Taiwan

Abstract

In this paper, an optical color image cryptosystem with a data hiding scheme is proposed. In the proposed optical cryptosystem, a confidential color image is embedded into the host image of the same size. Then the stego-image is encrypted by using the double random phase encoding algorithm. The seeds to generate random phase data are hidden in the encrypted stego-image by a content-dependent and low distortion data embedding technique. The confidential image and secret data delivery is accomplished by hiding the image into the host image and embedding the data into the encrypted stego-image. Experimental results show that the proposed data steganographic cryptosystem provides large data hiding capacity and high reconstructed image quality.

Keywords: Data embedding, Data hiding, Image encryption, Optical security, Double random phase.

1. INTRODUCTION

With the fast development of communication and network technology, it is convenient to acquire various multimedia data through Internet. Unfortunately, the problem of illegal data access occurred frequently and popularly. Hence, it is important to protect the content and the authorized use of multimedia data against the pirates. Data encryption is a strategy to make the data unreadable, invisible or incomprehensible during transmission by scrambling the content of data [1]. In an image cryptosystem, it uses some reliable encryption algorithms or secret keys to transform or encrypt secret images into ciphered images. Only the authorized users can decrypt secret images from the ciphered images. The ciphered images are meaningless and non-recognizable for any unauthorized users who grab them without knowing the decryption algorithms or the secret keys.

Dissimilarly, data hiding or steganographic techniques refer to methods of embedding secret data into some host data in such a way that people can not discern the existence of the hidden data. For example, the well-known watermarking which usually hides copyright marks in multimedia data is a kind of data hiding technique [2]. Common methods for data hiding can be categorized into spatial and transform domain methods. The earliest method, which is simple and has high embedding capacity, embedded data into least significant bits (LSBs) of image pixels (i.e. spatial domain). Contrarily, in the transform domain, e.g., discrete cosine transform (DCT), Fourier transform, or wavelets, transformed coefficients of host signals can be manipulated to hide

messages. The image steganographic methods (or called virtual image cryptosystems) [3-6] are proposed to hide the secret images into readable but non-critical host images. They are designed to reduce the notice of illegal users.

For high speed application, image encryption methods based on optical systems have been developed. Many optical image encryption algorithms have been proposed for transmission security [7-11]. The double random phase encoding [7] is a famous and widely used algorithm which employs two random phase masks in the input plane and the Fourier plane to encrypt images into stationary white noise. In [8], an optical image cryptosystem based on the double random phase encryption and a public-key type of data embedded technique is proposed. In [9], a new image cryptosystem with an adaptive steganographic method is proposed to improve the security and visual quality. However, the input image is limited to grayscale in those cryptosystems. In [10], the encryption method using wavelength multiplexing and lensless Fresnel transform hologram is proposed for color image application. In [11], the optical color image encryption scheme is performed in the fractional Fourier transform domain.

In this paper, we propose a data steganographic scheme within an optical color image cryptosystem. A confidential color image is embedded into the phase term of the host image to become the stego-image. Then it is encrypted by using the double random phase algorithm, that is, it is multiplied by two random phase masks. The seeds to generate random phase data are embedded into the LSBs of the encrypted stego-image, in which a zero-LSB sorting technique is applied to find the hiding sequence. Simulations and experiments regarding the hiding method (in comparison with the traditional scheme [8]) are performed. Experimental results show that the proposed color image cryptosystem has a good performance in secure data embedding, large hiding capacity, and high visual quality.

In Section 2, the conventional data embedding technique and the optical cryptosystem are reviewed. Section 3 introduces the proposed steganographic optical color image cryptosystem. Section 4 shows some experimental results to demonstrate the performance of the proposed scheme and a comparison with the previous method [8]. Finally, Section 5 gives conclusion and future work.

2. REVIEW OF OPTICAL IMAGE CRYPTOSYSTEM

In optical image cryptosystems, the double random phase algorithm [7] is a very common encryption and decryption method. In the double-random-phase encoding, an image I is multiplied by a random phase mask P_1 in the input spatial plane and Fourier transformed to frequency domain. It is multiplied by another random phase mask P_2 in the Fourier plane. Then it is inverse Fourier transformed to obtain its ciphered image I_E in the output spatial plane. In the decoding process, the ciphered image I_E is Fourier transformed and then multiplied by the conjugate function of mask P_2 and inverse Fourier transformed to spatial domain. It is multiplied by the conjugate function of mask P_1 to obtain its deciphered image I_D in the output spatial plane. The equations are expressed as follows.

$$I_E = F^{-1}\left[F\left(I \times P_1\right) \times P_2\right] \tag{1}$$

$$I_D = F^{-1}\left[F\left(I_E\right) \times P_2^*\right] \times P_1^* \tag{2}$$

where $P_1 = \exp(i2\pi p_1)$ and $P_2 = \exp(i2\pi p_2)$, p_1 and p_2 are random numbers of the image size between [0, 1], F and F^{-1} define the Fourier and inverse Fourier transforms, and * denotes the conjugate operation. The optical 4f architecture, where f is the focal length of the lens, is shown in Figure 1.

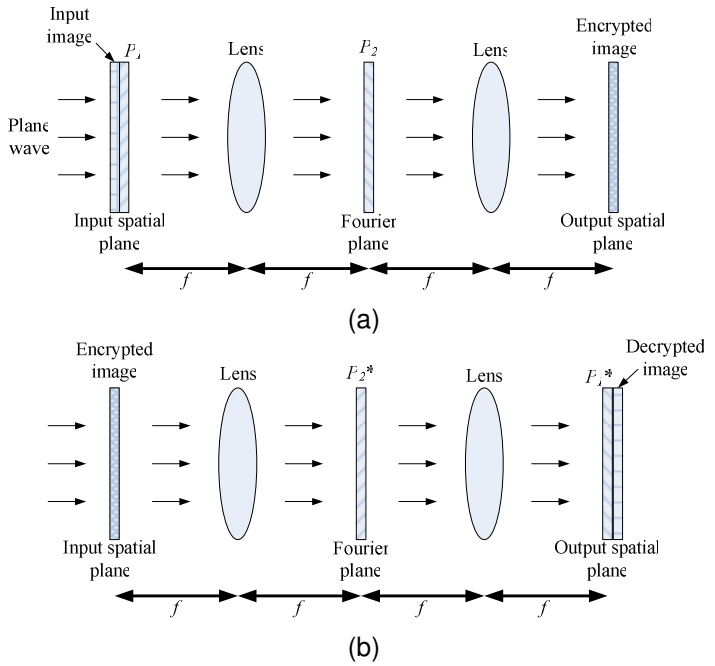

FIGURE 1: Optical 4*f* Architecture of the image cryptosystem. (a) Encryption (b) Decryption.

The data hiding scheme for the optical image cryptosystem proposed in [8] always embeds data in a fixed area of the encrypted image. Although it is a simple and fast way to complete the data embedding and extracting framework, the visual quality of the decrypted images is lower when the hidden data size is large. Therefore, in [9], a new image cryptosystem with an adaptive steganographic method is proposed to improve the visual quality of the reconstructed images. In this paper, the adaptive data hiding method is applied to the proposed optical color image cryptosystem for embedding the seeds which are used to generate double random phase. Besides, confidential or secret images can be embedded into the host images in the proposed cryptosystem.

3. THE PROPOSED METHOD

The proposed optical color image cryptosystem is based on the double random phase encryption theorem [7]. Before encoding, the confidential image I_c is embedded into the phase term of the host image I_h. Then the stego-image I_s is multiplied by a random phase mask P_1 in the input domain and transformed to Fourier plane. It is multiplied by another random phase mask P_2 and converted to the spatial domain for obtaining the encrypted stego-image I_e. The equations are defined as follows.

$$I_s = I_h \exp(i\frac{\pi}{2} I_c) \tag{3}$$

$$I_e = F^{-1}\left[F\left(I_s \times P_1\right) \times P_2\right] \tag{4}$$

where $P_1 = \exp(i2\pi p_1)$ and $P_2 = \exp(i2\pi p_2)$, p_1 and p_2 are random numbers of the image size between [0, 1], and F and F^{-1} define the Fourier and inverse Fourier transforms.

In the decoding step, the encrypted stego-image I_e is transformed to the Fourier plane, multiplied by the conjugate of mask P_2, converted to spatial domain, and multiplied by the conjugate of mask P_1 to obtain its decrypted image I_d. Ideally, the decrypted image I_d is equal to the stego-

image I_s in a lossless manner. The host image can be obtained by computing the complex modulus of the decrypted image I_d. Also the secret image can be retrieved by calculating the complex argument of the decrypted image I_d. The equations are described as follows.

$$I_d = F^{-1}\left[F(I_e)\times P_2^*\right]\times P_1^* \tag{5}$$

$$I_h = \left|I_d\right| \tag{6}$$

$$I_c = \frac{\arg(I_d)}{\pi/2} \tag{7}$$

where P_1^* and P_2^* indicate the conjugate masks of P_1 and P_2, and $\arg(\cdot)$ takes the complex argument.

For color images, they are first separated into three channels: red, green, and blue. Each channel is processed from Equations (3) to (7). However, the three channels can be coded by different random phase masks, i.e. multiplied by random phase masks P_{1R}, P_{1G}, P_{1B} and P_{2R}, P_{2G}, P_{2B}. The seeds to generate random phase data are embedded into the encrypted stego-image I_e. In the receiver side, the first thing is to decode the embedded seeds from the encrypted stego-image I_e. The decoded seeds are used to re-generate the same random numbers which are applied to produce the conjugate random phase masks P_{1R}^*, P_{1G}^*, P_{1B}^* and P_{2R}^*, P_{2G}^*, P_{2B}^*. Thus one can decode the encrypted stego-image I_e to get the decrypted image I_d using the hidden seed data extracted from the encrypted stego-image itself. Figure 2 shows the schema of the proposed optical color image cryptosystem.

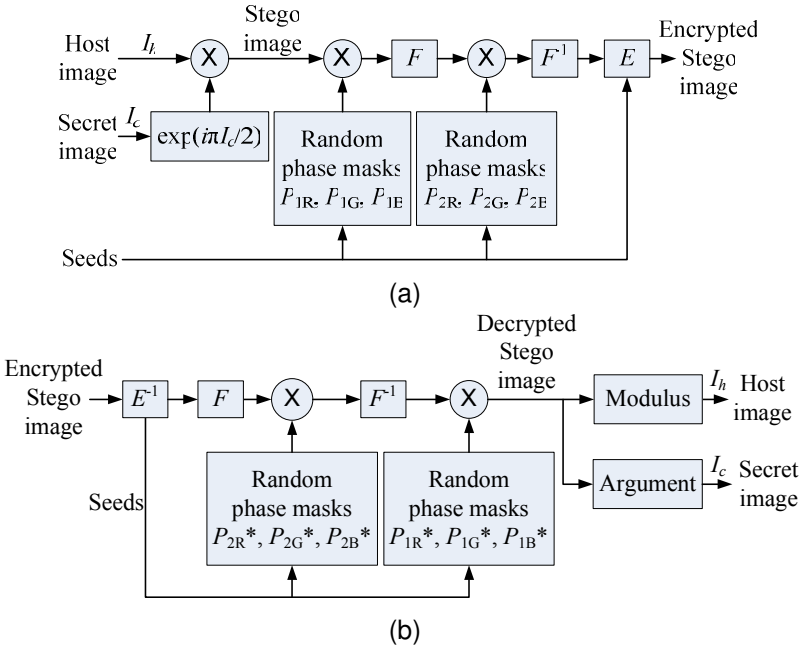

FIGURE 2: Schema of the proposed color image cryptosystem. (a) Encryption, (b) Decryption (X: multiplication, E and E^{-1}: the data embedding and extracting functions, F and F^{-1}: the Fourier and inverse Fourier transforms).

Since the signal values in the optical system are complex number format, there are real and imaginary parts that can be used to embed data. In this paper, we choose the real parts of complex numbers to be the hidden site. That is, the seeds for generating random phase data are embedded into LSBs of the quantized real parts of the encrypted stego-image bit by bit. However,

the quantization and embedding procedure will cause the loss of visual quality in the decrypted host and confidential images. The important issue is how to select the hidden positions that result in low distortion of the decrypted images. It is a simple way to hide the data within a fixed region in the encrypted stego-image [8]. Nevertheless, due to the different image content, the fixed hidden positions are not always suitable for hiding data. To improve the visual quality of the decrypted image and more safely convey the secret seed data, a low distortion, adaptive, and content-dependent data hiding technique [9] is applied to hide the secret data. In our strategy, the positions with smaller absolute values are preferable since they have smaller energy and quantization step size. To keep the embedding and decoding sequences invariant, the LSBs are set to zero and a sorting technique is employed. The detailed data hiding and extraction procedures are described as follows.

3.1 Data Hiding Procedure

Step 1: Assume that there are N bits in the secret data $B=\{b_1,b_2,...,b_N\}$. The values of real parts in the encrypted stego-image I_e are sorted in ascending order with their absolute values. The sorted set of the first N+2 numbers except the maximum and the minimum is chosen and defined as $\Lambda=\{\alpha_1,\alpha_2,\mathrm{K},\alpha_N\}$, where $|\alpha_i|\le|\alpha_{i+1}|$, α_i and $\alpha_{i+1}\in\Lambda$. Note that the maximum and minimum in the first N+2 numbers are not used to be quantized and hidden data because the quantization step size is computed from them.

Step 2: The sorted set Λ is quantized to become $\Lambda_Q=Q_L(\Lambda)=\{\alpha_{q1},\alpha_{q2},...,\alpha_{qN}\}$, where $Q_L(.)$ denotes a quantizer with L levels.

Step 3: The zero-LSB set $\Lambda_{QZ}=\{\alpha_{qz1},\alpha_{qz2},...,\alpha_{qzN}\}$ is obtained by setting all LSBs of Λ_Q to be zero. The elements in Λ_{QZ} are sorted in ascending order with their absolute values to get $\Lambda_{QZS}=\{\alpha_{qzs_1},\alpha_{qzs_2},...,\alpha_{qzs_N}\}$, where $|\alpha_{qzs_i}|\le|\alpha_{qzs_{i+1}}|$, α_{qzs_i} and $\alpha_{qzs_{i+1}}\in\Lambda_{QZS}$.

Step 4: The sequence $S=\{s_1,s_2,...,s_N\}$, where $s_i\in\{1,2,...,N\}$ and $i=1,2,...,N$, generated by the set Λ_{QZS}, is used to be the data hiding index. That is, the secret data is successively embedded into the LSBs of the set Λ_Q according to the sequence S, i.e. $\Lambda_{QS}=\{\alpha_{qs_1},\alpha_{qs_2},...,\alpha_{qs_N}\}$, where $\alpha_{qs_i}\in\Lambda_Q$.

Step 5: The hiding rule is defined as

$$\Lambda_{QS}^E=\Lambda_{QS}+\mathrm{sgn}(B-\mathrm{mod}(\Lambda_{QS},2)) \tag{8}$$

where $\mathrm{sgn}(\cdot)\in\{-1,0,1\}$ is the signum function and $B=\{b_1,b_2,...,b_N\}$ is the secret data. The set with hidden data is $\Lambda_{QS}^E=\{\alpha_{qs_1}^e,\alpha_{qs_2}^e,...,\alpha_{qs_N}^e\}$.

Step 6: Finally, the set Λ_{QS}^E is de-quantized to obtain $\Lambda_S^E=Q_L^{-1}(\Lambda_{QS}^E)=\{\alpha_{s_1}^e,\alpha_{s_2}^e,...,\alpha_{s_N}^e\}$, where $Q_L^{-1}(\cdot)$ is the de-quantizer with L levels.

3.2 Data Extraction Procedure

Step 1: This step is the same as the first step in data hiding procedure to find the sorted set. The set is defined as $\Lambda^E=\{\alpha_1^e,\alpha_2^e,...,\alpha_N^e\}$, where $|\alpha_i^e|\le|\alpha_{i+1}^e|$, α_i^e and $\alpha_{i+1}^e\in\Lambda^E$. The sequence in the sorted set Λ^E is different from that in the sorted set Λ.

Step 2: The sorted set Λ^E is quantized with L levels to be $\Lambda_Q^E=Q_L(\Lambda^E)=\{\alpha_{q1}^e,\alpha_{q2}^e,...,\alpha_{qN}^e\}$.

Step 3: All LSBs of Λ_Q^E are set to zero to obtain the zero-LSB set $\Lambda_{QZ}^E=\{\alpha_{qz1}^e,\alpha_{qz2}^e,...,\alpha_{qzN}^e\}$. The elements in Λ_{QZ}^E are sorted in ascending order with their absolute values to get $\Lambda_{QZS}^E=\{\alpha_{qzs_1}^e,\alpha_{qzs_2}^e,...,\alpha_{qzs_N}^e\}$, where $|\alpha_{qzs_i}^e|\le|\alpha_{qzs_{i+1}}^e|$, $\alpha_{qzs_i}^e,\alpha_{qzs_{i+1}}^e\in\Lambda_{QZS}^E$.

Step 4: Now, the set Λ_{QZS}^{E} is equal to the set Λ_{QZS} with the same sequence $S=\{s_1, s_2, ..., s_N\}$. The hidden data is extracted from the LSBs of the set $\Lambda_{QS}^{E}=\{\alpha_{qs_1}^{e}, \alpha_{qs_2}^{e}, ..., \alpha_{qs_N}^{e}\}$, i.e.

$$\begin{cases} b_i = 0, \text{if } \bmod(\alpha_{qs_i}^{e}, 2) = 0 \\ b_i = 1, \text{if } \bmod(\alpha_{qs_i}^{e}, 2) = 1 \end{cases}, i = 1,2,...,N \tag{9}$$

4. EXPERIMENTAL RESULTS

In the experiment, one hundred 24-bit 512×512-pixel various color images (collected from [12-14]) are examined as host images and the peak signal-to-noise ratio (PSNR) is applied to evaluate the visual quality of the decrypted images. The equation is defined as follows.

$$MSE = \frac{MSE_R + MSE_G + MSE_B}{3} \tag{10}$$

$$PSNR = 10 \times \log_{10} \frac{255^2}{MSE} \tag{11}$$

where MSE_R, MSE_G, and MSE_B are mean square errors in three channels, respectively.

The traditional data hiding scheme [8], where the secret data are embedded in the central square area of the encrypted stego-image, is performed for comparison. For a fair evaluation, the size of hidden data is fixed and set to 480,000 bits. Table 1 shows the average PSNR values of the 100 decrypted host images and the retrieved secret images with different quantization levels, i.e. L = 8, 16, 32, 64, 128, and 256. It is clear that the PSNR values increase about 14 dB both in the decrypted host and secret images of the proposed method. Figure 3 plots detailed PSNR values of 100 decrypted host and secret images with L = 8, where the blue and red curves are the results of the proposed and the traditional methods, respectively. Figure 4 shows some original, decrypted host, and decrypted secret images sampled from the 100 test cases, where the quantization level is 8. The first row of Figure 4 shows the original images, where Figure 4(a)-(c) are host images and Figure 4(d) is the secret image. The second row of Figure 4 is the results of the proposed method, where the PSNR values are 19.14, 20.27, 20.22, and 32.10 dB, respectively. The last row of Figure 4 is the results of the traditional data hiding method [8], where the PSNR values are 4.81, 5.52, 5.79, and 16.96 dB, respectively.

L	Average PSNR (dB)			
	Proposed method		Ref. [8]	
	Host images	Secret images	Host images	Secret images
8	20.88	32.14	6.57	16.89
16	26.88	38.19	12.56	23.70
32	32.89	44.22	18.57	29.85
64	38.91	50.24	24.57	35.89
128	44.93	56.26	30.59	41.91
256	50.95	62.28	36.64	47.97

TABLE 1: Comparisons between the proposed method and the traditional scheme [8] of the average PSNR values of the 100 decrypted host images and the retrieved secret images. (hidden data 480,000 bits)

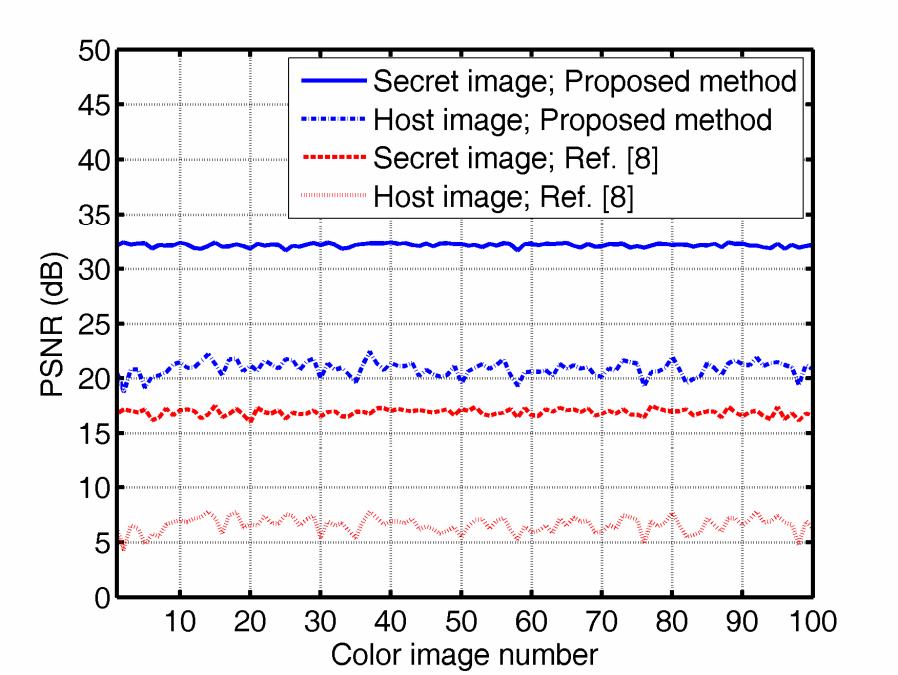

FIGURE 3: PSNR curves of the 100 decrypted host and secret images. The blue and red curves are the results of the proposed and the traditional methods [8], respectively. (L = 8, hidden data 480,000 bits)

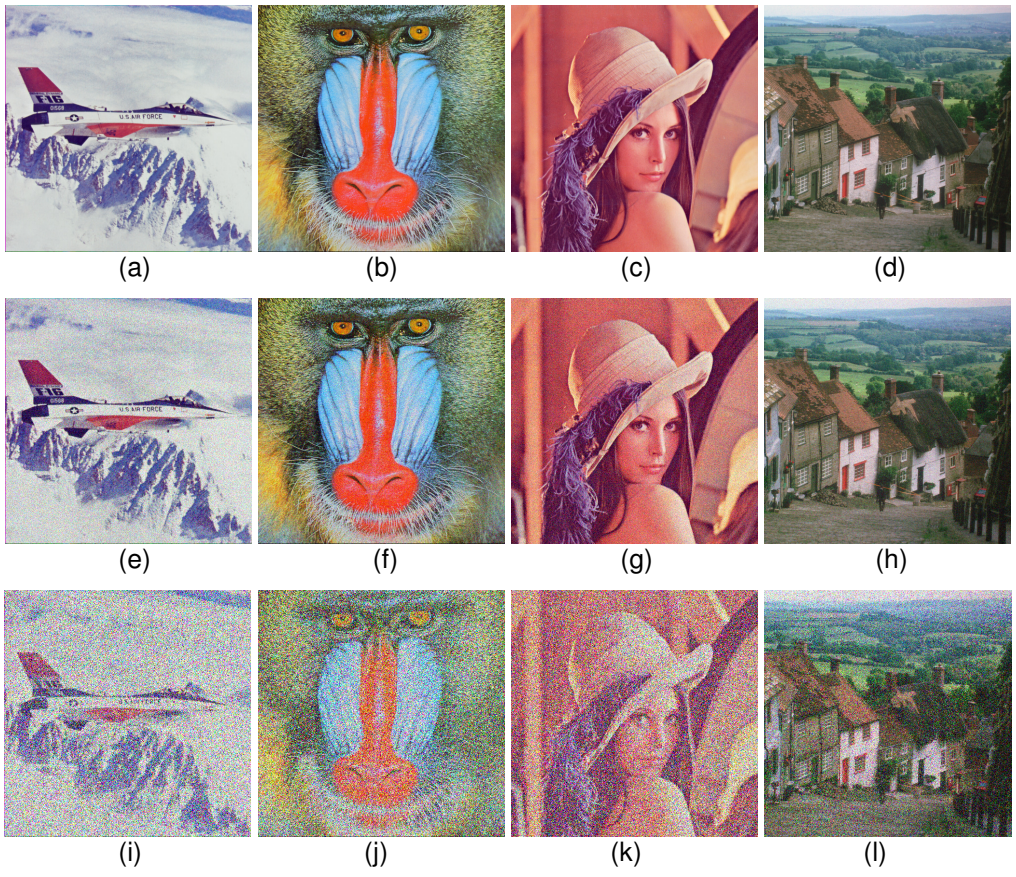

FIGURE 4: (a)(b)(c) The original host images and (d) the secret image, (e)-(h) the decrypted host and secret images by the proposed method, (i)-(l) the decrypted host and secret images by the traditional data hiding scheme. (L = 8, hidden data 480,000 bits)

To evaluate the data hiding capacity versus the visual quality of the decrypted host and secret images, the encrypted stego-images are embedded with different data size ranged from 108 to about 740,000 bits. The quantization level is set to 8. The average PSNR values of the 100 decrypted host and secret images are computed for evaluating the visual quality. Figure 5 shows the curves of the data hiding capacity versus the average PSNR values, where the blue and red curves are the results using the proposed and traditional methods, respectively. The PSNR values in the results of the proposed method are larger than those in the results of the traditional scheme when the sizes of hidden data are the same. It is obvious that the proposed method has a better performance than the traditional one.

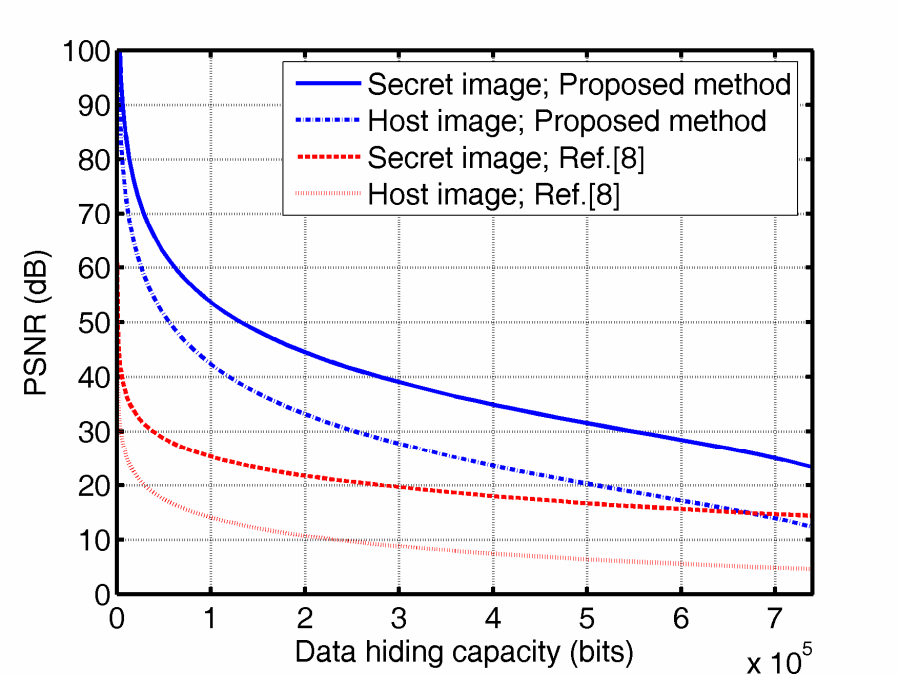

FIGURE 5: Curves of the data hiding capacity versus the visual quality of the decrypted host and secret images. The blue and red curves are the results of the proposed and the traditional methods [8], respectively. (L = 8)

In real applications, pirates may attempt to maintain the reconstructed images recognizable by modifying the encrypted stego-images. However, when the encrypted stego-images are attacked, it is expected that the hidden data will be altered. If the hidden data can not be correctly extracted, the stego-images can not be properly decrypted. In this part of experiment, it is assumed that the hidden data are completely cracked and the amplitude parts of the encrypted stego-images are suffered from three common attacks, i.e. noising, smoothing, and JPEG compression. The Gaussian noise (with zero mean and 0.01 variance) and the 3×3 averaging filter are exploited to disturb the encrypted stego-images for the noising and smoothing attacks. In the JPEG compression, 56.25% (36/64) of the DCT coefficients in the high frequency part in each 8×8 block were discarded (set to zero). The size of hidden data is set to 480,000 bits. The quantization level is also set to 8. The average PSNR values of the 100 decrypted host and secret images are calculated and listed in Table 2, where the encrypted stego-images are suffered from attacks. Without attacks, the average PSNR values in the decrypted host and secret images (shown in Table 1) are 20.88 and 32.14 dB by the proposed method and 6.57 and 16.89 dB by the

traditional scheme, respectively. With the three attacks, the PSNR values of all the decrypted host and secret images are reduced. The visual quality of the decrypted host and secret images in the smoothing attack is almost the worst. However, the results of the proposed method are still better than those of the traditional scheme.

Three common attacks	Average PSNR (dB)			
	Proposed method		Ref. [8]	
	Host images	Secret images	Host images	Secret images
Noising	9.08	19.85	4.42	14.02
Smoothing	7.25	16.31	5.34	12.31
JPEG compression	9.06	19.12	5.69	13.71

TABLE 2: Comparisons between the proposed method and the traditional scheme [8] of the average PSNR values of the 100 decrypted host images and the retrieved secret images when the encrypted stego-images are attacked. (L = 8, hidden data 480,000 bits)

5. CONCLUSION & FUTURE WORK

In this paper, the optical color image cryptosystem with data steganography is proposed. The double random phase encoding algorithm and the adaptive data hiding technique are applied in the proposed color image cryptosystem. The confidential image is hidden in the phase term of the host image. Then the stego-image is encrypted by the double random phase encoding algorithm. The seeds to generate random phase data are embedded into the encrypted stego-image by the proposed data hiding method. In comparison with the traditional hiding scheme, a larger data embedding capacity and higher visual quality of the decrypted host and confidential images are achieved.

For the advanced security, the confidential image and the secret data can be disordered by the scrambling technique before they are hidden. The secret or session keys for scrambling can also be embedded in the encrypted stego-image. Moreover, they can be encrypted by the asymmetric cryptographic algorithm, e.g. the RSA (Rivest-Shamir-Adleman) method. It is verified that the proposed cryptosystem provides a confidential image steganographic method and secret data hiding scheme to improve transmission security of the secret information.

6. ACKNOWLEDGEMENT

This research was supported by the National Science Council, Taiwan, under the grant of NSC97-2221-E-468-006.

7. REFERENCES

1. M. Yang, N. Bourbakis, and Li Shujun, "*Data-image-video encryption*," IEEE Potentials, vol. 23, no. 3, pp. 28-34, 2004.
2. Y. Govindarajan and S. Dakshinamurthi, "*Quality - security uncompromised and plausible watermarking for patent infringement*," International Journal of Image Processing, vol. 1, no. 2, 2007.
3. T.-S. Chen, C.-C. Chang, and M.-S. Hwang, "*A virtual image cryptosystem based on vector quantization*," IEEE Trans. Image Processing, vol. 7, no. 10, pp. 1485-1488, 1998.
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. W.-Y. Chen, "*Color image steganography scheme using set partitioning in hierarchical trees coding, digital Fourier transform and adaptive phase modulation*," Applied Mathematics and Computation, vol. 185, no. 1, pp. 432-448, 2007.
7. P. Refregier and B. Javidi, "*Optical image encryption based on input plane and Fourier plane random encoding*," Optics Letters, vol. 20, pp. 767-769, 1995.
8. 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.
9. C.-H. Chuang and G.-S. Lin, "*An optical image cryptosystem based on adaptive steganography*," Optical Engineering, vol. 47, 047002 (9 pages), April 2008.
10. L. Chen and D. Zhao, "*Optical color image encryption by wavelength multiplexing and lensless Fresnel transform holograms*," Optics Express, vol. 14, pp. 8552-8560, 2006.
11. M. Joshi, Chandrashakher, and K. Singh, "*Color image encryption and decryption using fractional Fourier transform*," Optics Communications, vol. 279, pp. 35-42, 2007.
12. Computer Vision Group (CVG), Department of Computer Science and Artificial Intelligence, University of Granada. Retrieved from http://decsai.ugr.es/cvg/, August 2008.
13. Kodak Lossless True Color Image Suite. Retrieved from http://r0k.us/graphics/kodak/, August 2008.
14. Programming, Image Processing, and Video Codecs Resourses. Retrieved from http://www.hlevkin.com/, August 2008.