A Steganography-Based Optical Image Encryption System Using RGB Channel Integration

Cheng-Hung Chuang

Abstract—An optical image encryption system with adaptive steganography using red, green, and blue (RGB) channel integration is proposed. The optical image encryption system employs a double random phase encoding algorithm to encrypt and decrypt color images. The RGB channel in a color image is first integrated into a large grayscale image. Then the integrated image is encrypted by two random phase masks. The secret data is then embedded into the encrypted image with a specific hiding sequence generated by the zero-LSB (least significant bits) sorting technique which is a content-dependent and low distortion data embedding method. Experimental results show that the proposed method has a good performance in both hiding capacity and decrypted image quality.

Index Terms—Data hiding, data embedding, information security, image steganography, image cryptosystem, optical security.

1. Introduction

With the rapid development of communication technology, it is easy to acquire multimedia data everywhere. Unfortunately, the problem of illegal data access or interception occurs frequently and universally. Therefore, it is important to protect the content and the authorized use of multimedia data against the illegal users. 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 encryption system, 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 intercept ciphered images without knowing the decryption algorithms or the secret keys.

Dissimilarly, steganographic techniques refer to methods of embedding secret data into cover data in such a way that people cannot be aware of the existence of the hidden data. The image steganographic methods (or called virtual image cryptosystems)[2]-[5] are proposed to hide the secret images into cover images which are readable but non-critical. They are designed to reduce the notice of illegal users. Common methods for data hiding can be categorized into spatial and transform domain methods. One of the common spatial domain methods, which have high embedding capacity, embeds data into least significant bits (LSBs) of image pixels. Contrarily, in the transform domain, e.g. the discrete cosine transform (DCT), Fourier transform, or wavelets, transformed coefficients of cover images can be manipulated to hide secret data.

For high speed applications, image encryption methods based on optical theories have been developed. Many optical image encryption algorithms have been proposed for transmission security[6]-[11]. The double random phase encoding technique[6] was 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 [7], an optical image encryption system based on the double random phase encryption and a public-key type of data embedded technique was proposed. The data hiding scheme proposed in [7] always embedded data in a fixed area of the encrypted image. Although it is a simple way to achieve the data embedding and extraction, the visual quality of the decrypted images is lower when the hidden data size is large. In [8], the optical encryption was performed using the fractional Fourier transform. In [9], an adaptive steganographic method was presented to improve the security and visual quality in the optical image encryption system proposed in [7]. However, the input images are limited to the grayscale in those encryption systems. In [10], the encryption method using wavelength multiplexing and lensless Fresnel transform hologram was proposed for the applications of color images. In [11], the optical color image encryption scheme was performed in the fractional Fourier transform domain. In [12], the optical image encryption system based on the adaptive steganographic method[9] was extended to color images. In the proposed system, a color image was separated into three...
channels, i.e. red, green, and blue, and each channel was encrypted individually.

In this paper, an adaptive steganography-based optical color image encryption system using RGB channel integration is presented. The RGB channel in a color image is first integrated into one large grayscale image. The integrated image is encrypted by two random phase masks. Then secret data is embedded into the LSBS of the quantized encrypted image data using the zero-LSB sorting technique. In our experiment, a comparison of steganography methods in the optical image encryption system is performed. Experimental results show that the proposed method obtains a good performance in both hiding capacity and decrypted image quality.

2. Review of Optical Image Encryption System

In optical image encryption systems, the double random phase encoding technique\(^6\) is a famous and common method. In the encoding process, an image \(I\) is multiplied by a random phase mask \(P_1\) in the input spatial plane and Fourier transformed to the 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 encrypted image \(I_E\) in the output spatial plane. In the decoding process, the encrypted image \(I_E\) is Fourier transformed and then multiplied by the conjugate of mask \(P_2\) and inverse Fourier transformed to the spatial domain. It is multiplied by the conjugate of mask \(P_1\) to obtain its decrypted image \(I_D\) in the output spatial plane. The equations are expressed as follows:

\[
I_E = F^{-1}[F(I)P_1P_2] \quad (1)
\]

\[
I_D = F^{-1}[F(I_E)P_2^*P_1^*] \quad (2)
\]

\[
P_1 = \exp(i2\pi p_1) \quad (3)
\]

\[
P_2 = \exp(i2\pi p_2) \quad (4)
\]

where \(p_1\) 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 of the image encryption system is shown in Fig. 1, where \(f\) is the focal length of the lens.

For a steganography-based optical color image encryption system, it is first separated into three channels: red, green, and blue. The three channel images are individually coded by the double random phase algorithm, i.e. multiplied by random phase masks \(P_{1R}, P_{1G}, P_{1B}\), \(P_{2R}, P_{2G}, P_{2B}\). Then the secret data is embedded into the three encrypted channel images by using the LSB replacement technique. That is, the encrypted cover signal should be quantized into bit data first. Then the secret data is embedded into LSBS of the quantized bit data. Next, the quantized bit data must be de-quantized to recover the encrypted stego image. Afterward, the encrypted stego image can be transmitted to the receiver. In the receiver side, one can extract the secret data and decrypt the cover image from the encrypted stego image. Fig. 2 shows the block diagram of the optical color image encryption system.

![Fig. 1. Optical 4f architecture of the image encryption system: (a) encryption architecture and (b) decryption architecture.](image)

![Fig. 2. Block diagram of the optical color image encryption system: (a) encryption process and (b) decryption process (X: multiplication operation; E and E\(^{-1}\): data embedding and extraction processes).](image)
3. Proposed Method

From the above description, the quantization and LSB replacement will cause the loss in image quality. The important issue is how to select the hidden regions or positions that result in low distortion of the decrypted image. It is a simple way to hide the data in fixed positions of the encrypted image. Nevertheless, due to the different image contents, the fixed positions are not always suitable for hiding data. Those positions with smaller absolute values are preferable to hide secret data since they have smaller energy and quantization step size. Therefore, an adaptive steganographic method is applied to choose positions with smaller absolute values. However, for a color image with RGB channel separation, the hidden position selection is restricted to individual channel images. To improve the visual quality of the decrypted image, the RGB channel integration is proposed.

In the proposed method, it is first integrated three channels into one grayscale image. The integrated image is encoded by the double random phase algorithm, i.e. multiplied by random phase masks \( P_{r} \) and \( P_{i} \), where \( P_{r} \) and \( P_{i} \) are of the triple image size. Then the adaptive steganographic method is applied to find those positions that are suitable for hiding data overall. Fig. 3 shows the illustration of three different types of data hiding strategies. There are 16×3 bits secret data hidden in the encrypted color image signal. The first class is the fixed-position type (Type I) which embeds data in the central square area in each encrypted channel image. The second class is the RGB-channel-separation type (Type II) which hides data in those positions that are selected by the adaptive steganographic method in each encrypted channel image. The last class is the RGB-channel-integration type (Type III) which conceals data in those positions that are chosen by the adaptive steganographic method across three encrypted channel images.

Assume that there are \( N \) bits in the secret data, i.e. \( B=\{b_{1}, b_{2}, \ldots, b_{N}\} \). Since the transformation coefficients in the encrypted image are complex numbers, the real and imaginary parts can be selected to embed secret data. In this paper, the real part is chosen to hide data. The detailed data embedding and extraction procedures are described as follows.

3.1 Data Embedding Procedure

Step 1: the values of real part \( \alpha \) in the encrypted integrated image are sorted in ascending order according to their absolute values. The set of the first \( N+2 \) numbers except the maximum and the minimum is chosen and defined as \( \Gamma=[\alpha_{1}, \alpha_{2}, \ldots, \alpha_{N+2}] \), where \( |\alpha_{i}| \leq |\alpha_{i+1}| \) and \( \alpha_{i}, \alpha_{i+1} \in \Gamma \). Note that the maximum and the minimum in the first \( N+2 \) numbers are not used to quantize and hide data, since the quantization step size is computed from them.

Step 2: the set \( \Gamma \) is quantized to be \( \Gamma_{Q}=Q_{\alpha}(\Gamma)=\{\alpha_{1}, \alpha_{2}, \ldots, \alpha_{N}\} \), where \( Q_{\alpha}(\Gamma) \) denotes a quantizer with \( L \) levels.

Step 3: all LSBs of \( \Gamma_{Q} \) are modified to zero to obtain the zero-LSB set \( \Gamma_{QZ}=\{\alpha_{q_{1}}, \alpha_{q_{2}}, \ldots, \alpha_{q_{N}}\} \). The elements in \( \Gamma_{QZ} \) are sorted in ascending order with their absolute values to obtain \( \Gamma_{QZS}=\{\alpha_{q_{1}}, \alpha_{q_{2}}, \ldots, \alpha_{q_{N}}\} \), where \( |\alpha_{q_{i}}| \leq |\alpha_{q_{i+1}}| \) and \( \alpha_{q_{i}}, \alpha_{q_{i+1}} \in \Gamma_{QZS} \).

Step 4: the sequence \( S=\{s_{1}, s_{2}, \ldots, s_{N}\} \) generated by the set \( \Gamma_{QZS} \), where \( s_{i}\in\{1, 2, \ldots, N\} \) and \( i=1, 2, \ldots, N \), is used to be the data hiding index. That is, the secret data \( B \) is successively embedded into the LSBs of the set \( \Gamma_{Q} \) with the sequence \( S \), namely \( \Gamma_{QS}=\{\alpha_{q_{1}}, \alpha_{q_{2}}, \ldots, \alpha_{q_{N}}\} \), where \( \alpha_{q_{i}} \in \Gamma_{Q} \). The embedding rule is defined as

\[
\Gamma_{QS}^{E}=\Gamma_{QS}+\text{sgn}(B-\text{mod}(\Gamma_{QS}, 2))
\]

where \( \text{sgn}(\cdot) \in \{-1, 0, 1\} \) is the signum function and the set with hidden data is \( \Gamma_{QS}^{E}=\{\alpha_{q_{1}}^{e}, \alpha_{q_{2}}^{e}, \ldots, \alpha_{q_{N}}^{e}\} \).

Step 5: the set \( \Gamma_{QS}^{E} \) is de-quantized to get \( \Gamma_{s}^{E}=Q_{\alpha}^{-1}(\Gamma_{QS}^{E})=\{\alpha_{s_{1}}^{e}, \alpha_{s_{2}}^{e}, \ldots, \alpha_{s_{N}}^{e}\} \), where \( Q_{\alpha}^{-1}(\cdot) \) denotes the de-quantizer with \( L \) levels.

3.2 Data Extraction Procedure

Step 1: this step is the same as the first step in data embedding procedure. The set is defined as \( \Gamma_{s}^{E} \)

![Fig. 3. Illustration of three different types of data hiding strategies: (a) Type I: fixed position, (b) Type II: RGB channel separation, and (c) Type III: RGB channel integration (gray blocks mean those positions selected to hide data).](image-url)
The sequence in $\Gamma^E$ is different from that in $\Gamma$.

Step 2: the set $\Gamma^E$ is quantized with levels to be $\Gamma^E_0 = Q_s(\Gamma^E) = \{\alpha^E_{s,1}, \alpha^E_{s,2}, L, \alpha^E_{s,N}\}.$

Step 3: all LSBs of $\Gamma^E_0$ are set to zero to obtain the zero-LSB set $\Gamma^E_{QZ} = \{\alpha^E_{qZ,1}, \alpha^E_{qZ,2}, L, \alpha^E_{qZ,N}\}.$ The elements in $\Gamma^E_{QZ}$ are sorted in ascending order with their absolute values to obtain $\Gamma^E_{QZS} = \{\alpha^E_{qZS,1}, \alpha^E_{qZS,2}, L, \alpha^E_{qZS,N}\}.$ The set $\Gamma^E_{QZS}$ is equal to the set $\Gamma^E_{QZ}$ with the same sequence $S = \{s_1, s_2, \ldots, s_N\}.$

Step 4: finally, the secret data is extracted from the LSBs of the set $\Gamma^E_{QZ} = \{\alpha^E_{qZ,1}, \alpha^E_{qZ,2}, L, \alpha^E_{qZ,N}\},$ i.e. the secret bit $b_i \in B=\{b_1, b_2, \ldots, b_N\}$ is computed according to the following equation:

$$b_i = \begin{cases} 0, & \text{if } b_i \text{ mod}(\alpha^E_{qZ_i}, 2) = 0 \\ 1, & \text{if } b_i \text{ mod}(\alpha^E_{qZ_i}, 2) = 1. \end{cases} \quad (6)$$

### 4. Experimental Results

In our simulation and experiment, one hundred 24-bit color images are collected for examination\textsuperscript{[13]–[15]}. All of test images are set to 512×512 pixels. The peak signal-to-noise ratio (PSNR) is applied to evaluate the visual quality of the decrypted color images. The equation is defined as follows.

$$\text{PSNR} = 10 \log_{10} \frac{255^2}{\text{MSE}} \quad (7)$$

$$\text{MSE} = \frac{\text{MSE}_{R} + \text{MSE}_{G} + \text{MSE}_{B}}{3} \quad (8)$$

where $\text{MSE}_{R}, \text{MSE}_{G},$ and $\text{MSE}_{B}$ are mean square errors in three channel images, respectively.

Three different types of data embedding algorithms are performed for comparison. For a fair evaluation, the size of hidden data is fixed and set to 196608 bits. That is, the size of secret data is 65536 bits in each channel image in Type I and Type II methods. Table 1 shows the maximal, minimal, and mean PSNR values (in dB) of the decrypted images of test images with different quantization levels ($\text{QL}=8, 16, 32, 64, 128, \text{and } 256$), i.e., with a range of 3-bit to 8-bit quantization. With 3-bit quantization ($\text{QL}=8$), the image qualities achieved by Type I, Type II, and Type III methods are 16.08 dB, 38.56 dB, and 43.31 dB in average, respectively. It is obvious that there is a significant increase in the PSNR values from 16.08 dB of the Type I method to 43.31 dB of Type III method in average. The methods of Type II and Type III give rise to increases of 22 dB and 27 dB in the PSNR values, respectively.

Fig. 4 shows the inferior and superior examples with in the 100 cases. The original, encrypted stego, and decrypted images of No. 58 and No. 80 with 3-bit quantization ($\text{QL}=8$) are shown. The PSNR values are 11.91 dB, 19.59 dB, 34.13 dB, 42.10 dB, 38.93 dB, and 46.85 dB in Fig. 4 (e), (f), (g), (h), (i), and (j), respectively. It is apparent that noise exists in Fig. 4 (e) and (f). And it is hard to identify the difference between the decrypted images of Type II and Type III methods and the original images. Fig. 5 shows the PSNR plot of the decrypted images for the 100 test images with 3-bit quantization ($\text{QL}=8$), where the solid, dashed, and dotted lines are the results using the methods of Type III, Type II, and Type I, respectively. In Fig. 5, the average PSNR values are 43.31 dB, 38.56 dB, and 16.08 dB from top to bottom curves.

To evaluate the visual quality of the decrypted images versus the data hiding capacity, the encrypted images are embedded with different size of data ranged from 108 bits to 750000 bits for test images. The quantization level is set to 8, i.e. 3-bit quantization. The average PSNR value of the decrypted images is calculated for the distortion evaluation. Fig. 6 shows the average PSNR for different values of data hiding capacity for test images by three data hiding methods, where the solid, dashed, and dotted lines are the results using Type III, Type II, and Type I methods, respectively. When the hidden data size is more than 30000 bits, the average PSNR value is less than 25 dB using Type I method. In the results of the Type III method, it is about 68 dB when the hidden data size is 30000 bits. If the PSNR value is set to 25 dB in the results of the Type III method, the hidden data size can be reached about 668190 bits that is 22 times the data size of the Type I method. It is demonstrated that the proposed steganography-based optical color image encryption system has a better performance than the other two methods.

<table>
<thead>
<tr>
<th>QL</th>
<th>Type I</th>
<th>Type II</th>
<th>Type III</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Maximum</td>
<td>Minimum</td>
<td>Mean</td>
</tr>
<tr>
<td>8</td>
<td>21.98</td>
<td>10.65</td>
<td>16.08</td>
</tr>
<tr>
<td>16</td>
<td>27.57</td>
<td>17.07</td>
<td>22.04</td>
</tr>
<tr>
<td>32</td>
<td>33.93</td>
<td>23.03</td>
<td>28.01</td>
</tr>
<tr>
<td>64</td>
<td>39.54</td>
<td>28.85</td>
<td>34.06</td>
</tr>
<tr>
<td>128</td>
<td>45.78</td>
<td>34.90</td>
<td>40.07</td>
</tr>
<tr>
<td>256</td>
<td>51.21</td>
<td>41.00</td>
<td>46.08</td>
</tr>
</tbody>
</table>

![Table 1: PSNR (in dB) evaluation of the decrypted images with different quantization levels (QL) for three different methods](image-url)
5. Conclusions

In this paper, the optical color image encryption system based on the RGB channel integration steganography is presented. The double random phase encoding algorithm and the adaptive data embedding technique are applied in the proposed system. The color images are encrypted by the double random phase encoding algorithm. Then the secret data can be embedded into the encrypted signal by the adaptive data hiding method with the strategy of RGB channel integration. In comparison with the conventional techniques, a higher data embedding capacity and better visual quality of the decrypted image are performed. It is verified that the proposed image encryption system provides data hiding characteristics of content-dependence, low distortion, and security.

![Sampling of the experimental images (QL=8): (a) and (b) original images of No. 58 and 80, (c) and (d) the encrypted stego images, (e) and (f) the decrypted images of the Type I method (PSNR=11.91 and 19.59 dB), (g) and (h) the decrypted images of the Type II method (PSNR=34.13 dB and 42.10 dB), and (i) and (j) the decrypted images of the Type III method (PSNR=38.93 dB and 46.85 dB).](image)

![PSNR plot of the decrypted images for test images (QL=8). The solid (top), dashed (median), and dotted (bottom) lines are the results using Type III, Type II, and Type I methods, respectively.](image)

![Distortion performance of three different methods versus data hiding capacity for test images (QL=8).](image)
References


Cheng-Hung Chuang received his B.S. degree in electrical engineering from Tatung Institute of Technology, Chiayi, Taiwan in 1994, and his M.S. and Ph.D. degrees in electrical engineering from National Chung Cheng University, Chiayi, Taiwan in 1996 and 2003, respectively. From 2003 to 2007, he was a postdoctoral fellow at the Institute of Statistical Science, Academia Sinica. In 2007, he entered the Department of Computer Science and Information Engineering, Asia University, as an assistant professor. His research interests include image/video processing, optical and biomedical signal processing, computer vision, and pattern recognition.