Double-Layer Data Embedding Scheme Based on Three-Pixel Differences

Yi-Hui Chen, Chiao-Chih Huang, and Chi-Shiang Chan

Abstract—Steganography is a technique to hide the secret data into digital media without getting any unexpected notices. The traditional steganographic method, namely least significant bit (LSB) replacement, is a simple but insecure scheme. To overcome the traditional drawbacks, this paper proposes a steganographic scheme, which is called double-layer hiding method. The experimental results confirm that the proposed scheme achieves better hiding capacity with high ability of resisting security analysis.

Index Terms—Hiding capacity, least significant bit replacement, security analysis, steganography, visual quality.

1. Introduction

Steganography, also known as a data hiding scheme, is a technique used to exchange secret messages over the Internet. By altering the least significant bits of the digital media as stego-media for secret communications, the stego-media can not be detected by attackers using any statistical analysis tools[1]. In general, hiding capacity, visual quality, and the ability of security resistant are three main criteria for estimating the performances of a steganographic scheme.

The well-known methods in steganography are least significant bit (LSB) replacement and LSB matching[2]. LSB replacement is a simple method which embeds secret data by replacing k LSBs of a pixel with k secret bits directly[3]. However, LSB replacement is an insure method because the secret data hidden into the stego-image might be detected by statistical steganalysis[1]. To improve the visual quality and the ability of security resistant, LSB matching[4] is proposed. Using LSB matching, a pixel can carry secret bits by adding or subtracting 1 to or from the pixel value for the grayscale image. After that, some researches[2][4] provide the security drawbacks of LSB matching.

In 2007, Zhang et al.[5] proposed a double layered steganographic scheme to hide messages in both of the LSB plane and the second LSB plan[2]. Next year, Liu et al.[6] presented a scheme of LSB matching based on feature mining and pattern recognition techniques. In 2011, Chen et al.[7] also proposed a two-layer steganography method based on Sudoku. Some schemes[3][10] are proposed to provide better performances than that of LSB replacement and LSB matching.

This paper proposed a double-layer steganographic scheme by using three-pixel differences for embedding the secret data. The experimental results show that the hiding capacity is superior to that of Chen et al.’s about 0.09 bpp (bits per pixels) on average. In addition, the visual quality is 50.87 dB on average. Users are difficult to recognize the differences between cover images and stego-images by a human vision system.

The rest of paper is organized as follows. In Section 2, Chen et al.’s method is introduced. In Section 3, we give a detailed description of the embedding and extracting procedures. Section 4 shows the experimental results including the visual quality, hiding capacity, and security analysis. Finally, the conclusions are drawn in Section 5.

2. Related Works

This section briefly introduces Chen et al.’s two-layer steganographic scheme[7]. In the embedding procedure, the image is divided into several groups. Each group consists of four pixels, denoted as \( p_1, p_2, p_3, \) and \( p_4 \). Later on, the encoder computes two differences between pixels \( p_1 \) and \( p_2 \), and pixels \( p_3 \) and \( p_4 \) as \( d_1=|p_1-p_2| \) and \( d_2=|p_3-p_4| \), respectively. The digit \( s \) can be calculated as (1), when the encoder inputs any two differences \( d_1 \) and \( d_2 \):

\[
s = F(d_1, d_2) = \frac{1}{2} \sum_{i=1}^{2} 3^{i-1} d_i \mod 3^2. \tag{1}
\]

The encoder adjusts the differences \( d_1 \) and \( d_2 \) until the digit \( s \) is equal to the secret data, depicted as \( s_1 \). Note that the value of \( s_1 \) ranges from 0 to 8. After adjusting, differences \( d_1 \) and \( d_2 \) are adjusted as \( \bar{d}_1 \) and \( \bar{d}_2 \), respectively.

To embed the second secret data, denoted as \( s_2 \), the two pixels \( p_1 \) and \( p_2 \) can be modified with (2) and (3), respectively, where \( i=1, j=2, w=2, \) and \( k=1 \). By the same
way, the pixels \( p_3 \) and \( p_4 \) can also be modified with (2) and (3) for embedding the third secret data, denoted as \( s_3 \), where \( i=3, j=4, w=3, \) and \( k=2 \). Note that the values of \( s_2 \) and \( s_3 \) are either 0 or 1.

\[
\mathcal{F}_j = \begin{cases} p_j, & \text{if } s_u = \text{LSB}(p_j), \\ p_j + 1, & \text{if } s_u \neq \text{LSB}(p_j), p_i > p_j \text{ and } \Delta d_i > d_i \\ p_j + 1, & \text{if } s_u = \text{LSB}(p_j), p_i \leq p_j \text{ and } \Delta d_i < d_i \\ p_j - 1, & \text{if } s_u \neq \text{LSB}(p_j), p_i \leq p_j \text{ and } \Delta d_i \geq d_i \\ p_j - 1, & \text{if } s_u = \text{LSB}(p_j), p_i > p_j \text{ and } \Delta d_i \leq d_i \\ \end{cases}
\]

where \( \text{LSB}(\cdot) \) is the least significant bit of the pixel value \( p_j \).

When the stego-pixel \( \mathcal{F}_j \) (or \( \overline{\mathcal{F}}_j \)) is less than 0 or greater than 255, which is called underflow or overflow problem, the pixels \( p_i \) (or \( p_j \)) must be adjusted before data embedding until the problem is resolved.

In the extracting procedure, the stego-image is also divided into several groups. Each group consists of three pixels denoted as \( \mathcal{F}_1, \mathcal{F}_2, \mathcal{F}_3, \) and \( \overline{\mathcal{F}}_j \), and calculates two differences \( \Delta d_i = |\mathcal{F}_i - \mathcal{F}_j| \) and \( \overline{\Delta d}_j = |\mathcal{F}_j - \mathcal{F}_j| \). The first secret \( s_1 \) can be extracted with (1), where \( d_i = \Delta d_i \) and \( d_j = \overline{\Delta d}_j \). Finally, the secret data \( s_2 \) and \( s_3 \) can be extracted by computing \( \text{LSB}(\mathcal{F}_1) \) and \( \text{LSB}(\overline{\mathcal{F}}_j) \), respectively.

### 3. Proposed Scheme

The proposed method is a double-layer data embedding scheme for a three-pixel group, including two procedures, namely embedding and extracting procedures. The details of the embedding procedure are described as follows.

Step 1: the image is divided into several groups. Each group consists of three pixels, denoted as \( p_1, p_2, \) and \( p_3 \).

Step 2: compute three values \( d_i = |p_i - p_i| \mod 3 \), \( d_j = |p_j - p_j| \mod 3 \), and the value of \( \text{LSB}(p_i) \).

Step 3: the pixels \( p_1, p_2, \) and \( p_3 \) are modified according to Table 1 for embedding secrets \( s_1, s_2, \) and \( s_3 \), where \( i \in \{0, 1\}, s_1 \in \{0, 1, 2\}, \) and \( s_3 \in \{0, 1, 2\} \). In Table 1, if the secret data \( s_i \) is not identical to the value of \( \text{LSB}(p_i) \), the pixel \( p_i \) must be plus or minus by 1 to make \( s_i \) equal to the value of \( \text{LSB}(p_i) \); otherwise, keep its original value intact. After data embedding, the stego-pixel \( \mathcal{F}_j \) is modified as \( \mathcal{F}_j = p_j + q_1 \).

By the same way, the results \( d_i \) and \( d_j \) must be equal to the secret data \( s_2 \) and \( s_3 \) after data embedding. Additionally, the stego-pixels \( \mathcal{F}_2 \) and \( \mathcal{F}_3 \) will be calculated as \( p_2 + q_2 \) and \( p_3 + q_3 \), respectively, as shown in (4):

\[
\mathcal{F}_1 = p_1 + q_1, \quad \mathcal{F}_2 = p_2 + q_2, \quad \mathcal{F}_3 = p_3 + q_3.
\]

To avoid underflow and overflow problems, when the stego-pixel \( \mathcal{F}_j \) is greater than 255, the original pixel \( p_j \) must be updated as \( p_j = p_j - 1 \), where \( i \in \{0, 1, 2\} \). On the contrary, if the stego-pixel \( \mathcal{F}_j \) is less than 0, the original pixel \( p_j \) must be updated as \( p_j = p_j + 1 \). Next, the new pixels \( p_1, p_2, \) and \( p_3 \) are put into the embedding procedure again for embedding the secret data \( s_1, s_2, \) and \( s_3 \). If there still has an underflow or overflow problem, the pixels before data embedding must be adjusted again and then put into the embedding procedure again as previous description until no overflow or underflow problem is happened.

When the receiver gets the stego-image, it can use the extracting procedure to obtain the secret data. The details of the extracting procedure are described as following steps.

Step 1: the stego-image is divided into several groups, and each group consists of three pixels, denoted as \( \mathcal{F}_1, \mathcal{F}_2, \) and \( \mathcal{F}_3 \).

<table>
<thead>
<tr>
<th>( s_1, \text{LSB}(p_i) )</th>
<th>( s_2, d_i )</th>
<th>( s_3, d_j )</th>
<th>( (q_1, q_2, q_3) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( (0, 0) )</td>
<td>( (1, 1) )</td>
<td>( (2, 2) )</td>
<td>( (0, 0, 0) )</td>
</tr>
<tr>
<td>( (0, 1) )</td>
<td>( (1, 2) )</td>
<td>( (2, 0) )</td>
<td>( (0, 0, 1) )</td>
</tr>
<tr>
<td>( (0, 2) )</td>
<td>( (0, 2) )</td>
<td>( (0, 0) )</td>
<td>( (0, 1, 0) )</td>
</tr>
<tr>
<td>( (1, 0) )</td>
<td>( (1, 0) )</td>
<td>( (2, 1) )</td>
<td>( (1, 1, 0) )</td>
</tr>
<tr>
<td>( (1, 1) )</td>
<td>( (1, 1) )</td>
<td>( (2, 2) )</td>
<td>( (1, 1, 1) )</td>
</tr>
<tr>
<td>( (0, 2) )</td>
<td>( (0, 2) )</td>
<td>( (0, 1) )</td>
<td>( (1, 1, 0) )</td>
</tr>
<tr>
<td>( (0, 1) )</td>
<td>( (0, 1) )</td>
<td>( (2, 0) )</td>
<td>( (1, 0, 0) )</td>
</tr>
<tr>
<td>( (1, 2) )</td>
<td>( (1, 2) )</td>
<td>( (2, 1) )</td>
<td>( (1, 0, 1) )</td>
</tr>
<tr>
<td>( (0, 2) )</td>
<td>( (0, 2) )</td>
<td>( (0, 1) )</td>
<td>( (1, 0, 0) )</td>
</tr>
<tr>
<td>( (0, 1) )</td>
<td>( (0, 1) )</td>
<td>( (2, 0) )</td>
<td>( (1, 0, 1) )</td>
</tr>
<tr>
<td>( (1, 2) )</td>
<td>( (1, 2) )</td>
<td>( (2, 1) )</td>
<td>( (1, 0, 0) )</td>
</tr>
</tbody>
</table>
CHEN et al.: Double-Layer Data Embedding Scheme Based on Three-Pixel Differences

299

Fig. 1. Test images and the corresponding stego images: (a) cover image of Lena, (b) stego image of Lena, (c) cover image of Baboon, and (d) stego image of Baboon.

Table 2: Performance of various schemes with different cover images

<table>
<thead>
<tr>
<th>Schemes</th>
<th>Performance</th>
<th>Lena</th>
<th>Baboon</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Hiding capacity (bytes)</td>
<td>Visual quality (dB)</td>
<td>Hiding capacity (bytes)</td>
</tr>
<tr>
<td>Chen et al. [7]</td>
<td>42,270</td>
<td>51.14</td>
<td>42,270</td>
</tr>
<tr>
<td>Mielikainen's scheme [10]</td>
<td>32,768</td>
<td>52.38</td>
<td>32,768</td>
</tr>
<tr>
<td>Proposed scheme</td>
<td>45,220</td>
<td>50.87</td>
<td>45,220</td>
</tr>
</tbody>
</table>

Step 2: do step 2.1 and step 2.2 for all the three-pixel groups until all groups are processed as follows.

Step 2.1: compute the value of LSB ($\bar{p}_1$) to obtain the secret data $s_1$.

Step 2.2: compute two digits $\bar{d}_1 = |\bar{p}_1 - \bar{p}_2| \mod 3$ and $\bar{d}_2 = |\bar{p}_2 - \bar{p}_3| \mod 3$ to obtain the secret data $s_2$ and $s_3$, respectively.

4. Experimental Results

Three measuring criteria of the experimental results, the hiding capacity, the visual quality, and the security analysis, are used to evaluate the performances of the proposed method. In the experimental results, we use two big different grayscale images, “Lena” and “Baboon”, which are smooth and complex images as shown in Fig. 1 (a) and (c), respectively. The size of each image is 256×256 pixels. After data embedding, the stego-images are shown in Fig. 1 (b) and (d). The visual quality is good enough so that people can not recognize the differences between the cover images and the stego-images.

In the experiments, the hiding capacity of the stego-images in the proposed scheme is 1.38 bpp, and the visual quality PSNR (peak signal-to-noise ratio) value of the stego-images is 50.87 dB calculated by (5) and (6).

$$\text{PSNR} = 10 \log \left( \frac{255^2}{\text{MSE}} \right) \text{dB}$$ \hspace{1cm} (5)

$$\text{MSE} = \frac{1}{WH} \sum_{i}^{W} \sum_{j}^{H} (p_{jk} - \bar{p}_{jk})^2$$ \hspace{1cm} (6)

where mean squared error (MSE) is used to compute the average distortion after data embedding. Note that the original pixel and the stego-pixel located at $(j, k)$ position, are denoted as $p_{jk}$ and $\bar{p}_{jk}$, respectively.

Generally, it is a trade-off between the hiding capacity and the visual quality, because a higher hiding capacity often makes a lower visual quality.

In Table 2, we compare the performances of the proposed scheme with that of some schemes [7],[10]. As shown in Table 2, the visual quality of the proposed scheme is similar to that of Chen et al.’s [7], but the hiding capacity of the proposed scheme is superior to that of the scheme in [7] about 0.09 bpp on average.

The visual quality (PSNR value) of the proposed scheme is close to that of Mielikainen’s scheme [10], but the hiding capacity of our scheme is much higher than that of Mielikainen’s scheme [10].

In Fig. 2, security analysis: (a) Lena, (b) with no secrets, (c) with LSB replacement, (d) proposed scheme, (e) Baboon, (f) with no secrets, (g) with LSB replacement, and (h) proposed scheme.
To make sure the scheme can resist against the traditional security analysis, such as visual attacks\textsuperscript{3,4}, the results of the security analysis are shown in Fig. 2. Fig. 2 (b) and Fig. 2 (f) show the analysis results without embedding any secrets into Fig. 2 (a) and Fig. 2 (e), respectively. The analysis results are like random pads so that the attackers judge no secrets hidden in the digital images. When embedding some secrets into the digital images using LSB replacement, there are some regular patterns as shown in Fig. 2 (c) and Fig. 2 (g). This is because the traditional LSB replacement replaces the lowest bit plane of pixels with the secret data, which makes the statistical analysis easily analyze the regular embedding rules. When the regular patterns are detected, the attackers might doubt some secrets embedded in these transmitting digital images. But in the proposed algorithm, since the hidden data are embedded into the digital images using two different layers by applying the proposed scheme, the statistical tool is difficult to detect the regular patterns as shown in Fig. 2 (d) and (h). As a result, the proposed scheme can successfully resist against the visual attack.

5. Conclusions

This paper proposed a steganography based on the three-pixel differences and modular operation. Experimental results show the visual quality of the proposed algorithm is better than that of LSB replacement algorithm, and the hiding capacity of the proposed algorithm is superior to that of Chen et al.’s scheme. In the future, we are planning to propose a higher hiding capacity as well as better visual quality using the sudoku concept.

References


Chiao-Chih Huang was born in Taiwan in 1989. He received the B.S. and M.S. degrees in computer science and information engineering in 2001 and 2004, respectively. Afterward, she got her Ph.D. degree in computer science and information engineering from the National Chung Cheng University, in 2009. From 2009 to 2010, she worked with Academia Sinica as a postdoctoral fellow. Later on, she served for IBM Taiwan Collaboratory Research Center as a research scientist. She is now an assistant professor with the Department of Applied Informatics and Multimedia, Asia University. Her research interests include image processing, watermarking, steganography, and XML techniques.

Chi-Shiang Chan was born in Taiwan in 1975. He received the B.S. degree in computer science in 1999 from the National Cheng Chi University and the M.S. degree in computer science and information engineering in 2001 from the National Chung Cheng University. He received his Ph.D. degree in computer engineering in 2005 also from the National Chung Cheng University. From 2007 to 2010, he has worked as an assistant professor with the Department of Information Science and Applications, Asia University. He is currently an associate professor with the Department of Applied Informatics and Multimedia, Asia University. His research interests include image and signal processing, image compression, information hiding, and data engineering.

Yi-Hui Chen was born in Taiwan in 1979. She received the B.S. and M.S. degrees in information management from Chaoyang University of Technology, in 2001 and 2004, respectively. Afterward, she got her Ph.D. degree in computer science and information engineering from the National Chung Cheng University, in 2009. From 2009 to 2010, she worked with Academia Sinica as a postdoctoral fellow. Later on, she served for IBM Taiwan Collaboratory Research Center as a research scientist. She is now an assistant professor with the Department of Applied Informatics and Multimedia, Asia University. Her research interests include image processing, watermarking, steganography, and XML techniques.