A Modified Image Steganography Method based on LSB Technique

Marwa M. Emam
Computer Science Department
Minia university, Egypt

Abdelmgeid A. Aly
Computer Science Department
Minia university, Egypt

Fatma A. Omara
Computer Science Department
Cairo university, Egypt

ABSTRACT
Data hiding techniques are considered very important roles with the rapid growth of intensive transfer of multimedia contents and secret communications. On the other hand, steganography is one of the most important information hiding techniques. By using steganography, information is hidden in carriers such as images, audio files, text files, and video files. In this paper, a modified steganography method based on the spatial domain is proposed. Our proposed method represents the message by six binary bits by using LSBraille method (Braille method of reading and writing for blind people) instead of using the ASCII encoding format. In this method, three bits of the message are hidden in a single pixel, and a true image is composed of three layers (Red, Green, and Blue) layer. Two bits are embedded in the Blue layer, and one bit is embedded in the green layer of the same pixel. In the Blue layer, the message is not only embedded in the least significant bit (LSB), but also the second and the third LSB may be changed. However, during each process of embedding, only one bit of the Blue layer is changed. From the experimental results, it is found that the proposed method achieves a very high Maximum Hiding Capacity (MHC), and higher visual quality as indicated by the Peak Signal-to-Noise Ratio (PSNR).

General Terms
Image Steganography, Data hiding in image.

Keywords
Steganography, Peak Signal-to-Noise Rate (PSNR), Mean Square Error (MSE), LSBraille, Maximum Hiding Capacity (MHC).

1. INTRODUCTION
Since the rise of the Internet, one of the most important factors of information technology and communication is the security of information. Cryptography has been used as a technique for securing the secrecy of communication, and many different methods have been developed to encrypt and decrypt data in order to keep a message secret. However, it is not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The used technique to satisfy that is called steganography [1]. Steganography is a technique used to transport information from one place to another place through public channel in a covert way [2]. The word steganography in Greek means “covered writing” (Greek words “stegos” meaning “cover” and “grafia” means “writing”) [3]. In general, steganography is the art of hiding a message signal in a host signal without any perceptual distortion of the host signal. It hides the secret message within other innocuous looking cover files, called carriers, (i.e. images, text, audio, or video files) so that it can't be observed [4]. The most frequently used carriers are digital images. The using of digital images for steganography makes use of the weaknesses in the human visual system, which has a low sensitivity in random pattern changes and luminance.

The human is incapable of discerning small changes in colour or patterns. Because of this weakness, the secret message can be inserted into the cover image without being detected [5].

Image Steganography is classified into two categories; spatial domain and transform domain [6, 7, and 8]. According to spatial domain, the secret data or secret message is directly embedded into the LSBs of image pixels. One of the most known examples of spatial domain method is LSB (Least Significant Bit insertion [9], while the schemes of transform domain embed the secret data within the cover image that transformed, such as the Fourier transform, discrete cosine transform, or the wavelet transform. Since most images have compressed by manipulating transform domain coefficients, the transform domain techniques add a fair amount of robustness against the destruction of the secret data due to lossy image compression [5]. The work in this paper concerns about the spatial domain.

![Fig 1: Basic Steganography System](image)

The basic model of steganography is shown in Figure 1. It consists of two algorithms, one for embedding, and one for extraction [1]. The embedding process consists of cover file (carrier), which is defined as the original file into which the required secure message is embedded, payload (secret message), and password is known as stego-key. The cover file with the secretly embedded is called the stego. The extraction process is traditionally a simple process, as it is simply an inverse of the embedding process, where the secret message revealed at the end. The challenge of using steganography in cover images is to hide as much data as possible with the fewest noticeable difference in the stego-image, where the final file is obtained after embedding the payload into a given cover file. It should have similar properties to that of the cover file.

The performance measurements for image distortion due to the embedding are the Mean Squared Error (MSE) and the Peak Signal-to-Noise Ratio (PSNR) between the cover image
and the stego image [10]. PSNR is one of the metrics to
determine the degradation in the embedding image with
respect to the cover image. MSE measures the difference
between two images. PSNR and MSE are defined in equations
1 and 2 [10, 12, 13].

\[
MSE = \left( \frac{1}{MN} \right) \sum_{i=1}^{M} \sum_{j=1}^{N} (X_{ij} - X'_{ij})^2 \quad \text{............. (1)}
\]

\[
PSNR = 10 \log_{10} \frac{I^2}{MSE} \quad \text{......................... (2)}
\]

Where:

- \(X_{ij}\) is the \(i\)th row and the \(j\)th column pixel in the original
  (cover) image.
- \(X'_{ij}\) is the \(i\)th row and the \(j\)th column pixel in
  the reconstructed (stego) image.
- \(I\) is the dynamic range of pixel values, or the maximum value that a pixel can be taken, for 8-bit
  images; \(I=255\).

The rest of this paper is organized as follows; related work
will be discussed in section 2, the proposed method will be
discussed in details in section 3, experimental results will be
given in section 4. Finally, section 5 concludes the paper.

2. RELATED WORK

In [14], the authors have proposed a method that hides
the secret message inside the cover image by representing the
secret message characters by using Braille method of reading
and writing for blind people that can save more than one-
fourth of the required space for embedding. The proposed
method used the Braille method representations of the
characters where each character is represented by only six
dots using the six – dots matrix that called (Braille Cell). The
method starts by representing these characters (dots) as binary
digits, each of which consists of 6 bits only instead of eight
bits as in original LSB embedding method that uses the binary
representation from the ASCII table. Therefore, by using this
representation, two pixels are saved from each secret byte
embedding process or more than one-fourth of the maximum
hiding capacity for each cover image. Therefore, the
maximum hiding capacity (MHC) has been increased and the
PSNR of the LSB embedding technique has been enhanced.

In [15], a new approach for hiding message in digital image in
spatial domain has been presented. According to work of this
paper, a method that embeds two bits of information in a
pixel, and alters one bit from one-bit plane has been
introduced. However, the message does not necessarily place
in the least significant bit of the pixel, the second less
significant bit plane, the fourth less significant bit plane can
also host the message, and only one alteration bit is allowed to
be happen.

In [16], a new steganography technique has been proposed.
According to this technique, nine bits of message can be
hidden in a single pixel. A true image is composed of three
elements R, G, and B components in each component 3 bits of
message hidden. So a total of nine bits can be embedded in to
a single pixel, i.e. more than one character (usually 8 bits are
used to represent the ASCII value of a character). Therefore,
the message is not only embedding in the least significant bit
(LSB), but also the second LSB, third LSB, and the fourth
LSB are susceptible to change. However, during each process
of embedding only two bit of each component are changed.
To have additional security, this method changes only the
even columns of pixels.

In [17], the authors have introduced best approach for least
significant bit (LSB) which based on image steganography
techniques to improve the security level of hidden information.
The new security conception hides secret information within the
LSB of image where a secret key encrypts the hidden information
to protect it from unauthorized users. Hidden information is
stored in different positions of LSB of cover image depending on
the secret key. Therefore, a bit of hidden information placed in
either LSB of Green or Blue matrix of a specific pixel, which
decided by the secret key. The cover image is divided into
three matrices (Red,Green, and Blue). The secret key is
converted into 1, 0 array of bit stream. Secret key and Red
matrix are used only for deciding making to replace hidden
information into either Green matrix or Blue matrix. Each bit
of secret key is XOR with each LSB of Red matrix. The
resulting XOR value decides that the 1 bit of hidden
information will be placed with either LSB of Green matrix or
Blue matrix (i.e. if the XOR value is 1, then the LSB of Green
matrix is replaced by the first bit of hidden information. If the
XOR value is 0, then the LSB of Red matrix is replaced by the
first bit of hidden information). The same process will be
continued until the hidden information is finished.

3. PROPOSED METHOD

Our proposed method will concern the spatial domain of the
cover image. It is based on hiding six message bits in two
pixels, the first three message bits will be hidden in the first
pixel and the last three message bits will be hidden in the
second pixel (see Figure 2). According to the proposed
method, only two bits for each character of the cover image
are changed; 1-bit from blue layer and 1-bit from green layer.
According to the proposed method, the cover image and the
secret message are considered as an input, each byte in the
secret message is represented by its binary using LSB/Braille
[14] where the byte from the secret message is represented by
6-bits only. Then, the cover image is converted into three
layers (Red, Green, and Blue) layer. After that each pixel in
the (Blue, and Green) layers is converted by its binary using
the ASCII encoding format. First, we start with the Blue layer,
then the Green layer of the same pixel and so on to embed the
full secret message. In the Blue layer, two bits per pixel are
embedded, the message is not only embedded in the first
least significant bit (LSB), but also the second least significant bit,
and the third least significant bit are allowed to be changed.
However, during each process of embedding only 1-bit of the
Blue layer will allowed to change, this process is done by
taking the last three bits of the Blue layer pixel and entered it
in the XOR Gate, and applying the following equations:

\[
B1 \oplus B2 = N2 \quad \text{.............................. (3)}
\]

\[
B2 \oplus B3 = N3 \quad \text{.............................. (4)}
\]

Where, \(B1\) is the first least significant bit, \(B2\) is the second
least significant bit, and \(B3\) is the third least significant bit of
the Blue layer.
Then the third bit of the message in the least significant bit of the Green layer will be embedded in the same pixel, and so on as.

The pseudo code of our proposed method is as follows:

**Algorithm:** Message Embedding using XOR gate and LSBraile method

**Input:** Cover Image C, Secret Message M.

**Output:** StegoImage S.

**Steps:**

1. **Split the Cover Image C into three channels Red (R), Green (G), Blue (B).**
2. **Convert B, and G into blocks; B= \{b_1, b_2, b_3 \ldots\ldots b_n\} , G= \{g_1, g_2, g_3 \ldots\ldots g_n\} where each block is only one pixel.**
3. **Convert each block from B, and G to its ASCII format.**
4. **Split M into characters, M= \{m_1, m_2, m_3 \ldots\ldots m_n\}.**
5. **Take m_i from M, and Convert it into Braille 6-bit representation by using LSBraile method [14].**
6. **i=1 \text{ \ where \ } i\text{ is B and G counter.}**
7. **Take b_i from B, and g_i from G.**
8. **Take the last three bits from b_i ,**
9. **Apply the equation (2) and (3) to obtain the output N2, N3.**
10. **If (m_i(1)=N2 & m_i(2)=N3) Then**
    
    \[ b(i,6:8) = b(i,6:8) \text{ \ \ // no change occurs to } b_i \]
    
    \[ g(i, end)=m_i(3) \text{ \ // Apply LSB} \]
    
    \[ i=i+1 \]

   **Else If (m_i(1) != N2 & m_i(2) = N3) Then**

   \[ b(i,7:7) = \text{NOT ( b(i,7:7) )} \]
   
   \[ g(i, end)=m_i(3) \text{ \ // Apply LSB} \]
   
   \[ i=i+1 \]

   **Else If (m_i(1) = N2 & m_i(2) ! = N3) Then**

   \[ b(i,6:6) = \text{NOT ( b(i,6:6) )} \]
   
   \[ g(i, end)=m_i(3) \text{ \ // Apply LSB} \]
   
   \[ i=i+1 \]

   **Else If (m_i(1) != N2 & m_i(2) != N3) Then**

   \[ b(i,8:8) = \text{NOT ( b(i,8:8) )} \]
   
   \[ g(i, end)=m_i(3) \text{ \ // Apply LSB} \]
   
   \[ i=i+1 \]

11. **Repeat steps 9, and 10, but on step 10 change the message bits m_i by the last three bits ; m(4), m(5), m(6).**

12. **Repeat steps from 6 to 11 until the whole M has been embedded in C.**

13. **Convert B, and G from binary to decimal.**

14. **Merge the three channels R, G, B again to construct the stegoImage S.**

Therefore, each byte from the secret message will hide in two pixels only. This will satisfy a very high embedding capacity. We can calculate the maximum number of bytes that can be hidden in any image (Maximum Hiding Capacity) by using this formula:

\[
\text{Maximum Hiding Capacity (MHC)} = (\text{Image width} \times \text{Image height})/2 \]

Suppose we have an (512 x 512) cover image, by using equation 5 we can hide 131,072 bytes or more than 1,048,576 bytes.
bits, which approximately is equal to 30 pages of word file at font size 12 (depending on the font settings).

4. EXPERIMENTAL RESULTS
In this section, the proposed method will be implemented and evaluated by comparing it with SLDIP and ESLDIP, DWT methods, as well as, the method in [16] using different messages with different lengths and hiding them in some cover images (i.e., standard images). The proposed and SLDIP methods are implemented using MATLAB 11.1.0 software running on a personal computer with a 2.27 GHz Intel (R) Core (TM) i3 CPU, 4 GB RAM and windows 7 as the operating system.

The results of the comparative study between our method and the SLDLP[5] and ESLDP[18] methods by using different number of characters (bytes) secret message and 512 x 512 cover images (e.g., Lena, Baboon, Pepper) are presented in Table 1, and Table 2, and Figures 5, 6.

**Table 1: Comparison between PSNRs of method SLDIP [5] and our proposed method**

<table>
<thead>
<tr>
<th>Cover image</th>
<th>Message capacity (bytes)</th>
<th>PSNR (dB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>512 x 512</td>
<td></td>
<td>SLDIP</td>
</tr>
<tr>
<td>Lena</td>
<td>75.836</td>
<td>40.4019</td>
</tr>
<tr>
<td>Baboon</td>
<td>82.407</td>
<td>40.0712</td>
</tr>
<tr>
<td>Pepper</td>
<td>75.579</td>
<td>40.5886</td>
</tr>
</tbody>
</table>

**Table 2: Comparison between PSNR of method ESLDIP [18] and our proposed method**

<table>
<thead>
<tr>
<th>Cover image</th>
<th>Message capacity (bytes)</th>
<th>PSNR (dB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>512 x 512</td>
<td></td>
<td>ESLDIP</td>
</tr>
<tr>
<td>Lena</td>
<td>75.836</td>
<td>45.72295</td>
</tr>
<tr>
<td>Baboon</td>
<td>82.407</td>
<td>45.33670</td>
</tr>
<tr>
<td>Pepper</td>
<td>75.579</td>
<td>45.42819</td>
</tr>
</tbody>
</table>

According to the comparative results, it is found that the PSNR of our method is better than that the SLDIP, and ESLDIP. In addition, the stego image quality of our method is very high relative to the SLDIP, and ESLDIP methods. According to the results in Table 1 and Table 2, the average improvement of SLDIP method and ESLDIP are 40.3539 % and 45.49 % respectively, while the average improvement of our method is 48.19 %. So, the average improvement of our method relative to SLDIP and ESLDIP methods are 7.84%, 2.7% respectively.

According to the comparative results, it is found that the PSNR of our method is better than that the SLDIP, and ESLDIP. In addition, the stego image quality of our method is very high relative to the SLDIP, and ESLDIP methods. According to the results in Table 1 and Table 2, the average improvement of SLDIP method and ESLDIP are 40.3539 % and 45.49 % respectively, while the average improvement of our method is 48.19 %. So, the average improvement of our method relative to SLDIP and ESLDIP methods are 7.84%, 2.7% respectively.

According to the comparative results, it is found that the PSNR of our method is better than that the SLDIP, and ESLDIP. In addition, the stego image quality of our method is very high relative to the SLDIP, and ESLDIP methods. According to the results in Table 1 and Table 2, the average improvement of SLDIP method and ESLDIP are 40.3539 % and 45.49 % respectively, while the average improvement of our method is 48.19 %. So, the average improvement of our method relative to SLDIP and ESLDIP methods are 7.84%, 2.7% respectively.

**Table 3: Comparison between PSNR of DWT [19] method and our method**

<table>
<thead>
<tr>
<th>Cover image</th>
<th>Message capacity (bytes)</th>
<th>PSNR (dB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>256 x 256</td>
<td></td>
<td>DWT</td>
</tr>
<tr>
<td>Lena</td>
<td>1000</td>
<td>60.3033</td>
</tr>
<tr>
<td>Baboon</td>
<td>1000</td>
<td>60.2393</td>
</tr>
<tr>
<td>Pepper</td>
<td>1000</td>
<td>60.1</td>
</tr>
</tbody>
</table>

According to the comparative results in Table 3, Figure 5, the average improvement of DWT [19] method is 60.2142%, while average improvement of our method is 63.04%. So, the average improvement of our method relative to DWT [19] method is 3.2%.
Finally, Table 4 represents the comparative result of our method and method in [16] by using different messages as seen in cases 1, 2, 3, and case 4, and 512 x 512 cover image (Pepper).

Table 4: comparison between PSNR of method in [16] and our method

<table>
<thead>
<tr>
<th>Cover image Pepper 512 x 512</th>
<th>Message Cases</th>
<th>PSNR (dB)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Message in [16]</td>
<td>Proposed method</td>
</tr>
<tr>
<td>Case 1</td>
<td>72</td>
<td>77.0270</td>
</tr>
<tr>
<td>Case 2</td>
<td>69</td>
<td>74.2454</td>
</tr>
<tr>
<td>Case 3</td>
<td>67</td>
<td>72.3467</td>
</tr>
<tr>
<td>Case 4</td>
<td>65</td>
<td>66.5551</td>
</tr>
</tbody>
</table>

Where, case 1, 2, 3, and 4 are the hidden message which are used in [16].

The message in case 1: “Steganography seeks to provide a covert communication channel between two parties.”

The message in case 2: “Steganography seeks to provide a covert communication channel between two parties. It is commonly framed as the prisoners’ problem. Two prisoners, Alice and Bob.”

The message in case 3: “Steganography seeks to provide a covert communication channel between two parties. It is commonly framed as the prisoners’ problem. Two prisoners, Alice and Bob, are permitted to communicate between one another, while under the surveillance of a Warden.”

The message in case 4: “Steganography seeks to provide a covert communication channel between two parties. It is commonly framed as the prisoners’ problem. Two prisoners, Alice and Bob, are permitted to communicate between one another, while under the surveillance of a Warden.”

Figure 6 shows the image that is used as a cover image and the histogram of its R, G, and B layers which are used to embed the message given in case 3. Figure 7 shows the stego image which is obtained after embedding that message and its corresponding histograms.
According to the comparative result in Table 4, and Figure 8, it is found that our method has more PSNR value than that the method in [16] which means the stego image quality of our method is also higher. Therefore, the average improvement of method in [16] is 68.25 %, while the average improvement of our method is 72.6%. So, our method outperforms the method in [16] by 4.35%.

Generally, our method outperforms the DWT [19], method in [16], and SLDIP and ESLDIP methods by producing high quality stego image.

5. CONCLUSION

In this paper, a new Steganographic method has been proposed, which uses the LSBBraille method to improve the capacity of the hidden data, and provides high embedding capacity and PSNR. To evaluate the proposed Steganographic method, a comparative study has been done among our proposed method, SLDIP, ESLDIP, and DWT methods, as well as, with the method in [16]. According to the experimental results, it is found that the proposed method is considered an effective Steganographic method because it satisfies the Steganographic system goals with high quality and PSNR.

6. REFERENCES


