Abstract: A huge number of messages circulate through social media, and many of these messages are confidential or carry personal information, which requires protection from intruders. The least significant bit method of data steganography is effective in masking messages, but it is not secure. In this research paper we will present a way to raise the security of the method of hiding messages without affecting the effectiveness of the method by keeping the MSE values low and PSNR values high. The proposed method will base on extracting a secret block from the image, this block will be used as a covering media to hold the secret message, after inserting the secret message the block will be returned back to the covering image.

Keywords: Steganography, covering image, holding image, block, LSB, MSE, PSNR.

1- Introduction

The process of hiding secret or private messages is extremely important [5], [6]. And to implement the process of hiding messages, colored digital images can be used as a medium to hide messages for various reasons, the most important of which are [7], [8], [9]:

- Color images are a massive medium due to the high resolution of the color image [16],[17], [18].
- Color image is widely available and can be obtained easily [19], [20].
- Ease of processing color digital image [21-32].
- The ability to use a specific part of the image to hide the message.

An effective way to hide secret messages by using color images as carrier images must be characterized by the following:

- Not to influence the image much so that the differences between the original image and the carrier image are not noticed with the naked eye, as shown in Figure 1.
- The mean square error (MSE) [10], [11], [12] between the original image and the carrier one must very closed to zero.
- The peak signal to noise ratio (PSNR) [13], [14], [15] between the original image and the carrier one must very high.
One of the most common methods of hiding confidential messages is the least significant bit (LSB) method. In this method, eight pixels of the digital image are allocated to hide a single symbol from the secret message and the least significant bits are used to hold the secret message characters as shown in figure 2.

The process of embedding the message in the color image causes slight changes in the image so that it is impossible to notice these changes with the naked eye, and these changes in the value of each pixel range between -1 and +1, as shown in Table 1.

<table>
<thead>
<tr>
<th>Original image LSB pixel</th>
<th>Character bit</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>No changes</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>Add 1 to the pixel value</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>Subtract 1 from the pixel value</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>No changes</td>
</tr>
</tbody>
</table>
And based on the information shown in Table 1, LSB method can be considered effective through:

- Maximizing PSNR value between the original image and the carrier one.
- Minimizing MSE value between the original image and the carrier one.

2- Color Image Blocking:
Digital color image is a 3D matrix [1], [2], one dimension for each color (red, green and blue), this matrix usually has a huge size, because most color images have a high resolution, thus color image can easily and efficiently be used as a holding media to embed the secret message [3], [4].

Instead of using the whole color image we can select a block from the image to be used to hold the secret message, to do this we have to select the block size by defining the number of rows and number of columns to form a block, these numbers must be kept in secret to raise the security of LSB method. Figure 3 shows an image example of size 165x247x3, while figure 4 shows the obtained blocks for this image [22], [23].

![Figure 3: Color image example](image_url)

![Figure 4: Obtained block for the image example](image_url)
### 3- The Proposed Method

The proposed method is based on LSB method as shown in figure 5, here we have to divide the original image into blocks, by defining the block size (number of rows and number of columns)[28], [30].

![Block diagram of the proposed method](image1)

Figure 5: Block diagram of the proposed method

The proposed method as shown in figure 6 can be implemented applying the following steps:

- Get the original color image.
- Define the block size.
- Select the block number
- Get the message

![Steps of the proposed method](image2)

Figure 6: Steps of the proposed method
- Convert the block and the message to binary.
- Apply LSB method to embed the message into the block.
- Convert the block back to decimal.
- Return the block back to the color image.

4- Implementation and Experimental Results

The proposed method was implemented using MATLAB, the image shown in figure 3 was selected, and block 5 was chosen to hide a secret message "ziad alqadi 55 amman", the message was repeated (block 5 can hold 1687 characters), table 2 shows the results of implementation:

Table 2: MSE and PSNR between the original image and the carrier one

<table>
<thead>
<tr>
<th>Message length</th>
<th>MSE</th>
<th>PSNR</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>0.0025</td>
<td>170.5668</td>
</tr>
<tr>
<td>40</td>
<td>0.0052</td>
<td>163.4127</td>
</tr>
<tr>
<td>80</td>
<td>0.0107</td>
<td>156.2328</td>
</tr>
<tr>
<td>160</td>
<td>0.0205</td>
<td>149.7203</td>
</tr>
<tr>
<td>320</td>
<td>0.0427</td>
<td>142.3545</td>
</tr>
<tr>
<td>640</td>
<td>0.0923</td>
<td>134.6551</td>
</tr>
<tr>
<td>1280</td>
<td>0.1928</td>
<td>127.2879</td>
</tr>
</tbody>
</table>

From table 2 we can see that even for long message the parameters MSE and PSNR remain acceptable, figure 7 shows the relationship between MSE, PSNR [30], [31] and the message length:

Figure 7: MSE, PSNR and message length
Now we select various color images and fix the message length to 1280 characters, table 3 shows the results of implementation:

<table>
<thead>
<tr>
<th>Image number</th>
<th>Image size(byte)</th>
<th>MSE</th>
<th>PSNR</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>122265</td>
<td>0.1928</td>
<td>127.2879</td>
</tr>
<tr>
<td>2</td>
<td>77976</td>
<td>0.3411</td>
<td>121.5817</td>
</tr>
<tr>
<td>3</td>
<td>518400</td>
<td>0.0257</td>
<td>147.4408</td>
</tr>
<tr>
<td>4</td>
<td>5140800</td>
<td>0.0055</td>
<td>162.8005</td>
</tr>
<tr>
<td>5</td>
<td>4326210</td>
<td>0.0057</td>
<td>162.5402</td>
</tr>
<tr>
<td>6</td>
<td>150975</td>
<td>0.1200</td>
<td>132.0296</td>
</tr>
<tr>
<td>7</td>
<td>1890000</td>
<td>0.0520</td>
<td>154.9594</td>
</tr>
<tr>
<td>8</td>
<td>6119256</td>
<td>0.0046</td>
<td>164.6578</td>
</tr>
</tbody>
</table>

From table 3 we can see that it is better to use an image with big size, this will keep MSE low and PSNR high.

5- Conclusion

LSB method of data steganography was implemented, a security issues were added to make this method more secure, an extra operation was added to this method. Instead of using the whole image we focus only on a single block in the image, the block size and the selected block number must be kept in secret to form a private key. The proposed method was implemented and the obtained experimental results showed that using the image block does not negatively affects the LSB parameters MSE and PSNR, it was recommended to use images with huge sizes to embed long messages by keeping MSE low and keeping PSNR high.

References


