A COMPARATIVE ANALYSIS OF STEGANOGRAPHIC TECHNIQUES

Jasvinder Kaur*, Inderjeet** & Manoj Duhan***

This paper analyzes the latest Steganographic technique based on digital logic (STBDL), its limitations and possible solutions to improve it. To remove difficulties arising in STBDL technique, we have proposed a new technique called Enhanced Steganographic Technique Based on Digital Logic (ESTBDL). Like STBDL this technique also selects the carrier image depending upon the information to carry, but overcomes the disadvantages associated with STBDL. ESTBDL technique can also carry more data bits as compared to previous techniques [2-9]. This technique uses digital operations based on logic gates and shift operators to derive the hidden information from image data.

Keywords: Steganography, Hiding Information, Digital Logic, Image Selection

1. INTRODUCTION

Steganography is the name given to techniques used for hiding information in digital objects such as image, video or sound files etc. Research in steganography has shown that bit replacement or bit substitution is inherently insecure with safe capacities far smaller than previously thought. For secure communication, hidden information is strictly restricted to fraction of cover image file [10-12]. An upper bound of 0.005 bits/pixel was experimentally determined for safe Least Significant Bit (LSB) embedding by Jessica at all [13-14]. We have been using many steganographic techniques to embed data into digital image. A very efficient technique known as “Steganographic Technique Based on Digital Logic” was proposed in [16]. Logic gates AND, OR, XOR, NOT and Shift operators SHL, SHR, CIL, CIR are used on image matrix to derive the information matrix in this technique. The addresses of rows that derive the information matrix are embedded along with the code for operator and Gates instead of actual information. In this way very huge information can be hidden with very less actual embedding. Moreover the embedding can be more than image data and effect of hiding is very less distortion to image. Another advantage of these techniques is – Images, which are more suitable for particular embedding, can be selected. However there is one limitation that selection of image become sometime very difficult in STBDL due to nature of image that image contains repeated or near repeated bytes in a row, whereas information generally does not contain repeated or near repeated bytes. We have tried to overcome this disadvantage in this research paper.

STBDL and its limitation are explained with example in section 2. Section 3 describes possible solution to enhance the STBDL. Examples are given in section 4 to show, how ESBDL overcomes the limitations of STBDL. Experimental results and comparisons between different techniques are shown in section 5. Finally conclusions are drawn in section 6.

2. STBDL EXAMPLES

We have used more than thousand images to get experimental data in STBDL and ESTBDL. A sample “leena.bmp” as the carrier image is shown in figure 1. Suppose we wish to hide information “inder” in this image. After applying logical operations on all possible combinations of image rows as in figure 1, it was observed that the information can be derive by applying OR operation on 8th and 143rd rows.

Instead of embedding 40 bits (8 bits for each character) in LSB we can send the same information using only 18 bits (000010001000111101), here first 8 bits for 8th row, next 8 bits for 143rd row and the last 2 bits are for Logical operation OR. One can specify different two bits depending upon logic operation. While embedding these information bits only 9 pixels of the image will get changed. In this case

Figure 1: Leena.bmp
(Carrier Image)

Figure 2: Leena.bmp
(Steganography Image)
pixels value (220 229 230 227 224 226 227 232 235) will be changed to (220 229 228 227 224 225 234 233). In case of LSB technique for sending same information 20 pixels of the digital image had to be changed.

Figure 2 is steganography image having embedded information. At the receiving end, first of all embedded address bits and logic operation bits are taken from earlier specified location. Then information can be derived by applying OR operation (logic operation in This example) on 8th and 143rd rows (Address bits in this example). Experiments show that as the size of the row of information matrix goes beyond 10 bytes the selection of carrier image is very difficult as it is hard to derive out the information.

3. Possible Solutions to Enhance STBDL

We are proposing three solutions to enhance the STBDL.

3.1 By Dividing the Information Row

The technique can be enhanced by dividing the complete set of information in such a way that the size of each row not goes beyond 6-10 bytes. Suppose we want to send information of 100 bytes we must divide the information in 10 rows each having 10 bytes so that each information row can be derived out of two rows of image easily. In Logic Gate and Shift Operators Based Techniques, when we use information dividing method we will have to embed 180 bits (18 bits for every 10 bytes of information) as compared to 800 bits (8 bits for each of 100 bytes) in case of LSB (two least significant bit).

3.2 Using MOD Operation

In this technique a suitable and predefined “MOD” operation is applied on image pixels before applying any logic operation. The MOD operation keeps the pixel value in suitable range. Thus the selection of image become easier as information rows can be derived from “in range” pixel values after applying logic operations.

3.3 Combining both MOD and the Information Dividing Method

MOD operation can also be applied on the value of pixels to restrict them into required range after that the information row is divided into parts. It further improves the efficiency of image selection. However inserted bits increase marginally, but it is still very less than LSB method.

4. Evaluation Examples of ESTBDL

4.1 Example of Dividing the Information Row

Suppose we wish to hide “I want to complete” and the image on which we performed the operation is as shown in figure1, ‘leena.bmp’.

Table 1

<table>
<thead>
<tr>
<th>Techniques</th>
<th>If size of information up to 5 bytes</th>
<th>If size of information up to 10 bytes</th>
<th>If size of information up to 20 bytes or greater</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. LSB</td>
<td>All the 1000 images were suitable as carrier</td>
<td>All the 1000 images were suitable as carrier</td>
<td>All the 1000 images were suitable as carrier</td>
</tr>
<tr>
<td>2. STBDL</td>
<td>912 images were suitable as carrier</td>
<td>103 images</td>
<td>None of the image was suitable as carrier</td>
</tr>
<tr>
<td>3. ESTBDL (Using information dividing)</td>
<td>919 images were suitable as carrier</td>
<td>821 images were suitable as carrier</td>
<td>755 images were suitable as carrier</td>
</tr>
<tr>
<td>4. ESTBDL (Using MOD operation)</td>
<td>914 images were suitable as carrier</td>
<td>157 images were suitable as carrier</td>
<td>None of the image was suitable as carrier</td>
</tr>
<tr>
<td>5. ESTBDL (Using information dividing and MOD combination)</td>
<td>964 images were suitable as carrier</td>
<td>903 images were suitable as carrier</td>
<td>817 images were suitable as carrier</td>
</tr>
</tbody>
</table>

After applying the different logic operations on leena.bmp, it was observed that first 5 characters of information can be derived from the OR of 100th and 483rd rows, next five from the OR of 97th and 346th rows, next five from OR of 21st and 397th rows and the last five can be derived from OR of 40th and 338th rows. In this way only 72 bits (18*4) will be actually embedded.

4.2 Example of Using MOD Operation

Suppose we wish to hide “prevent” in image 1. Experiments show that it is not possible to derive this information from image 1 after applying all combinations of logic operations and image rows. If the values of the pixels of figure1 is restricted between 97 and 123 the information can be derive out by applying OR operation on the rows 14 and 142. The same is the case if we take information ‘inderj’. It can not be derived from image1 in STBDL, but can be derived successfully after “MOD” operation.

4.3 Example of Combining Both MOD and the Information Dividing Method

Suppose we wish to hide “I’m coming on Monday” in image 1. It is not possible to derive this information by using STBDL. If the value of the pixels of figure 1 is restricted between 97 and 123 and the information is divided into four
5. RESULTS

The solutions given in section 3 were applied on more than thousand 512×512 bmp images. The experiments were done on various sizes (5, 10, 20 bytes) of information. The results observed on three different techniques namely Least Significant Bit, Steganographic Technique Based on Digital Logic (STBDL) and Enhanced Steganographic Technique Based on Digital Logic (ESTBDL) using MOD and dividing the information matrix into small parts are shown in Table 1–3. Table 1 shows the number of images that can be selected as the carrier image out of 1000 images.

<table>
<thead>
<tr>
<th>Techniques</th>
<th>Maximum limit of embedding</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. LSB</td>
<td>262144 bits</td>
</tr>
<tr>
<td>2. STBDL</td>
<td>Very difficult to send more than 160 bits</td>
</tr>
<tr>
<td>3. ESTBDL</td>
<td>1165084 bits</td>
</tr>
</tbody>
</table>

Table 2 shows the maximum limit of information that can be transmitted via all the three techniques. The experiment was done on 512×512 bmp images of size 272 KB (2, 62,144 bytes). The number of pixels in 512×512 images is 262144 and each pixel can store single bit so 262144 bits can be inserted in LSB. In ESTBDL 18 bits have to be inserted for every 10 bytes so 10 bytes can be sent through 18 pixels (one bit in each pixel) so 1165084 bits can be sent through 262144 pixels. If size of information is more than 10 bytes it is difficult to derive out the information row so very difficult to send more than 160 bits.

Table 3 shows the number of bits to be embedded in LSB and ESTBDL corresponds to varying size of information.

Table 3: Bits of Information to be Embedded

<table>
<thead>
<tr>
<th>Techniques</th>
<th>If size of information is 10 bytes</th>
<th>If size of information is 50 bytes</th>
<th>If size of information is 100 bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. LSB</td>
<td>80 bits</td>
<td>400 bits</td>
<td>800 bits</td>
</tr>
<tr>
<td>2. ESTBDL</td>
<td>38 bits</td>
<td>180 bits</td>
<td>360 bits</td>
</tr>
<tr>
<td>3. ESTBDL</td>
<td>18 bits</td>
<td>90 bits</td>
<td>180 bits</td>
</tr>
</tbody>
</table>

Though the embedding of information is less when we divide the information into 10 bytes in comparison to 5 bytes. But the success rate of the later case is high. We also have to send two extra bits to tell the receiver about the size of the row (5, 10 bytes) and one bit for method used (whether using MOD or without MOD).

The graph in figure 3 compares the actual bits embedded in LSB and ESTBDL.

Table 2 shows the maximum limit of information that can be transmitted via all the three techniques. The experiment was done on 512×512 bmp image of size 272 KB. The number of pixels in 512×512 images is 262144 and each pixel can store single bit so 262144 bits can be inserted in LSB. In ESTBDL 18 bits have to be inserted for every 10 bytes so 10 bytes can be sent through 18 pixels (one bit in each pixel) so 1165084 bits can be sent through 262144 pixels. If size of information is more than 10 bytes it is difficult to derive out the information row so very difficult to send more than 160 bits.

Table 3 shows the number of bits to be embedded in LSB and ESTBDL corresponds to varying size of information.

6. CONCLUSIONS

This research paper demonstrates to enhance the Steganographic Technique Based on Digital Logic. It was observed that as the size of the row of information matrix goes beyond 10 bytes the selection of carrier image is very difficult as it is hard to derive out the information matrix row from the image matrix rows. We have proposed three solutions to enhance the Steganographic Technique Based on Digital Logic. It is observed that it is easier to derive information matrix by using these solutions. We can also send more information using Enhanced Steganographic Technique Based on Digital Logic than Least Significant Bit insertion and Steganographic Technique Based on Digital Logic.

References

Security and Watermarking of Multimedia Contents IV, San Jose, California, 4675, (Jan 2002).


