Mode and Multiple Technique: A New Image Steganography Method for Capacity Enhancement of Message in Image

Rahul Rishi
Associate Professor
Department of Comp. Sci. & Engg,
TITS, Bhiwani-127021 (INDIA)

Sudhir Batra
Professor
Department of Mathematics
DCRUST, Murthal-131039 (INDIA)

Rajkumar
Assistant Professor
Deptt. Of Comp. Sc. & Engg.
UIET, MD University, Rohtak-124001 (INDIA)

ABSTRACT

Now a days, a major stress in steganography is to hide the maximum information possible alongwith the consideration of minimum bits used in such a way that image is not significantly degraded after embedding and embedded information is immune to modifications from intelligent attacks or manipulations. In the present paper we are proposing mode and multiple methods which shows an improvement over existing digital logic steganography method with comparatively lesser number of bits used to insert and extract the hidden information from image.

Keywords

Steganography, mode and multiple method, multiplication factor.

1. INTRODUCTION

Steganography is a secret communcitation technique used to transmit secret message that have been embedded into an image. In image steganography, the original image and the embedded image are called the carrier image and the stego image respectively. Digital steganography uses the digital objects such as image, video, music or any other computer file for hiding the data. The idea was first given by simmons in 1983[1].

In this section we propose an improved steganographic method which shows improvement over digital logic method described by parvinder et al [2]. Bit replacement made in host image is negligible compared to existing embedded techniques [3-9]. In the present study, at first we are using digital operations based on logic gates alongwith mode and multiple method to derive the hidden information from image, after that we apply modulus operator for getting remainder and quotient. For doing so, we first selected the cover image and constructed the image matrix and information matrix respectively by converting each pixel of image into bits and the information into binary form. After construction, the image matrix and information matrix is so selected that the number of their columns should be same. We proposed a novel idea of multiplication factor to reduce the number of bits used to hide the information in the image. This factor should be (n)2 as only binary numbers are considered. We take ‘4’ as multiplication factor as there will be only 4 remainders possible 0,1,2,3. But if we take larger number then it will be difficult to select the image. For example, if we take 16 as multiplication factor then there is a possibility of 16 remainders (0, 1, 2… 15). With these more number of remainders it would be difficult to select the specified rows of image matrix for insertion of opcode bits. It means larger the multiplication factor, harder will be the image selection. Proposed methods selected the images based on mode and multiple method alongwith digital logic operations to insert the message such that image is not significantly degraded after embedding and embedded information is immune to modifications from intelligent attacks or manipulations.An upper bound of 0.005 bits/pixel was determined for safe LSB embedding by Jessica et al [10]. Comparative analysis of LSB and digital logic gate with our proposed mode and multiple method given in table (2 & 3) and Figure (1) highlights the significance of present study.

2. DESCRIPTION OF PROPOSED METHOD

2.1 Insertion Method

In our study, we used the concept of modules operation along with logic gate operations (such as AND, OR, XOR and NOT as used by Parvinder et al) to get the information matrix rows from image matrix rows. We used the following opcodes for logic operations

Logic operation	op code
AND	00
OR	01
XOR	10
NOT	11

To make each row of information matrix, the above logic operations are applied one by one for all possible combinations of image rows and to insert the bits of above opcodes for the different logic operations we follow the table 1.

Table 1: Possible Combination of image Row

Reminder	Image rows Selected	Remarks
2	2, 4, 8, 10, … 254	Multiples of 2
3	3, 9, 15, 21, 27… 255	Multiples of 3
1	6, 12, 18, 24,… 252	Multiples of 6
0	0, 1, 5, 7, 11, 13,…253	Rest of rows

For better understanding of the above said method let us suppose the size of image matrix is 256*256 bits and size of information to be hidden is 2 Kb (2048 bits). As per our assumption that the number of columns should be equal in both image matrix and information matrix, the above information of size 2Kb is written as 8*256 in information matrix

Further to get the first row of information matrix, we suggest the following steps:

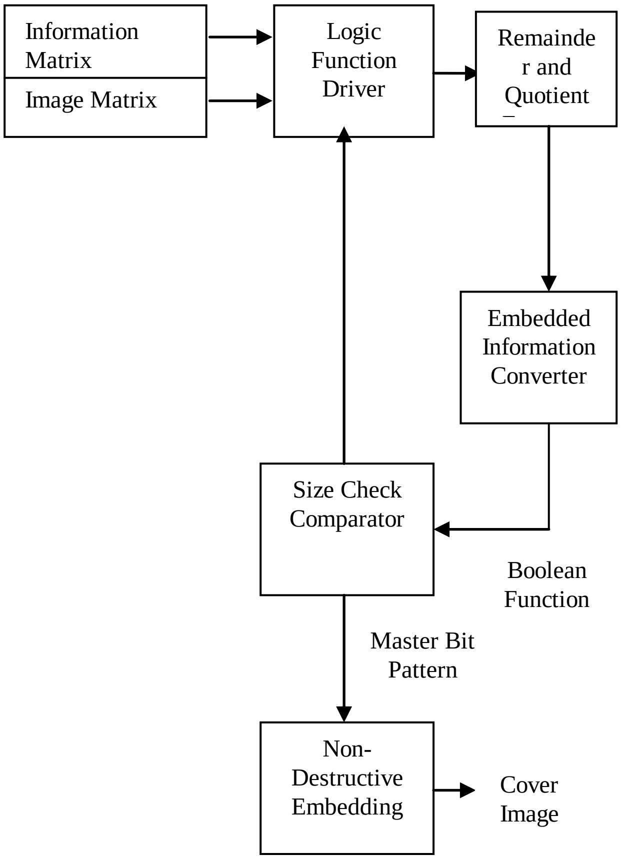
1). Select any two rows of image matrix (e.g. I^{th} row and J^{th} row)

2). Apply any one logic operation from the above said logical operations

3). Divide the selected rows by multiplication factor (i. e. 4)

As it is well known that two rows are required if we apply any one of AND, OR, XOR logic gate operations whereas in case of NOT operation, only one row address of image matrix is needed. So select row/s (I^{th} row and J^{th} row in case of AND, OR and XOR logic gate operations whereas the single row in case of NOT logic gate operation) and then divide these row/s by multiplication factor and get R_1 and Q_1 in case of I^{th} row, R_2 and Q_2 in case of J^{th} row and R and Q (where the logic gate NOT is applied) as reminder and quotient respectively. The first and second bit of opcode, any one of the above stated four logic gates, should be inserted as per table 1 at rows (image).

Now suppose we select 7 as I^{th} row and 13 as J^{th} row and then apply AND logic gate operation between them. After that we divide these rows by multiplication factor (i.e. 4) and get 3 (R_1) and 1 (Q_1) in case of 7th row and 1(R_2) and 3(Q_2) in case of 13th row as reminder and quotient respectively. By applying AND logic gate operation we get 00 as opcode, so the first bit (i.e. 0) of opcode should be inserted at rows (image) 3, 9, 15, 21, 27… 255 and similarly the second bit of opcode (i.e. 0) should be inserted at rows (image) 6, 12, 18, 24… 252 as per table 1. Hence the total number of bits required to insert the 1st row of information matrix are 14 bits (i.e. 2 bits for opcode + 6 bits for Q_1 + 6 bits for Q_2) and the embedded data for first row of matrix would be 00 000001 000010. When we used digital logic method (as described by Parvinder *et al*) we needed 18 bits to insert first row of information matrix for the same case. In case where all the rows of information matrix cannot be derived from image matrix, we will select another image for embedding. As already discussed only one row address of image matrix is needed in case of NOT operation, it further minimizes the size of embedded information to 8 bits (i.e. 2 bits for opcode + 6 bits for single quotient) in place of 14 bits in above example. The insertion method is represented by the following data flow diagram.



2.2 Extraction Method

To retrieve the hidden information from the encoded embedded image first we identify the opcode from the first two bits of the 14 bit message and then find their location. On the basis of location of opcode inserted, the remainder for I^{th} and J^{th} row was estimated. After estimating the remainder, the quotient/s was/were identified from 14 bit message (i.e. Q1 = 6 bits from next two bits of opcode & Q2 = last 6 bits of the message). Now to retrieve the row of image matrix we follow the formula;

I^{th} Row of image matrix =Multiplication factor *Quotient $_1$+ Remainder $_1$

J^{th} Row of image matrix =Multiplication factor *Quotient $_2$+ Remainder $_2$

And then hidden information was retrieved by applying logic gate operation between the I^{th} Row and J^{th} Row.

Suppose that the received 14 bits messege is 00 000001 000011. So opcode should be 00 that represents AND logic gate operation;

Suppose location of first bit of opcode (i.e. 0) is on any one of multiples of 3 (3, 9, 15, 21, 27… 255) which shows that R1 is 3; Similarly, the location of second bit of opcode (i.e. 0) is on any one of multiples of multiples of 6 (6, 12, 18, 24… 252) which shows that R2 is 1

So finally,

Opcode = 00 represents AND logic gate operation

Q1 = 000001 (next 6 bits from opcodes)

Q2 = 000011 (last 6 bits of 14 bits message)

So,

I^{th} Row of image matrix = Multiplication factor * Quotient $_1$+ Remainder $_1$

$= 4*1+3$

$= 7$

J^{th} Row of image matrix = Multiplication factor * Quotient $_2$+ Remainder $_2$

$= 4*3+1$

$= 13$

So the resultant First row of information matrix should be obtained by applying AND logic gate operation between 7th row of image matrix and 13th row of image matrix.

3. BENEFITS

1. Change is image size will reduced
2. Less no of bits are required
3. Less effort will be needed because less no. of bits are needed to be inserted or extracted.

4. RESULTS AND CONCLUSION

In this paper, a new method is proposed using mode and multiplication factor. By using this method the capacity of the message inserted inside the image is enhanced as well as the image quality of the stego image can be improved with low extra computational complexicity. Experiments show the effectiveness of the proposed method. The results obtained also show the improvement over the methods in reference [3], [6] with respect to the change in image quality and capacity of the message insertion. The comparatively analysis of our proposed method with other methods is shown in table 2, 3 and figure 1.

Table 2. (Comparison of logic gate technique, LSB and mode and multiple method in different image sizes)

Image size	Image size(bits)	Bit Inserted InLSB Technique	Bit Inserted In Logic Gate Technique	Bit Inserted In Mode and Multiple Method	Change in Image using LSB Method	Change in Image using Logic Gate Method	Change in Image using mode and multiple Method
32*32	8192	256	18	14	0.03125	0.002197266	0.001709
32*32	8192	512	36	28	0.0625	0.004394531	0.003418
8*128	8192	1024	14	10	0.125	0.001708984	0.0012207
8*128	8192	2048	28	20	0.25	0.003417969	0.0024414
32*64	16384	512	18	14	0.03125	0.001098633	0.0008545
32*64	16384	1024	36	28	0.0625	0.002197266	0.001709
32*64	16384	2048	72	56	0.125	0.004394531	0.003418
64*64	32768	512	20	16	0.015625	0.000610352	0.0004883
64*64	32768	1024	40	32	0.03125	0.001220703	0.0009766
64*64	32768	2048	80	64	0.0625	0.002441406	0.0019531
64*64	32768	4096	160	128	0.125	0.004882813	0.0039063
32*128	32768	1024	18	14	0.03125	0.000549316	0.0004272
32*128	32768	2048	36	28	0.0625	0.001098633	0.0008545
32*128	32768	3072	54	42	0.09375	0.001647949	0.0012817
32*128	32768	4096	72	56	0.125	0.002197266	0.001709
64*128	65536	1024	20	16	0.015625	0.000305176	0.0002441
64*128	65536	2048	40	32	0.03125	0.000610352	0.0004883
64*128	65536	4096	80	64	0.0625	0.001220703	0.0009766
64*128	65536	2120	100	80	0.078125	0.001525879	0.0012207
128*128	131072	1024	22	18	0.0078125	0.000167847	0.0001373
128*128	131072	6144	132	108	0.046875	0.001007080	0.0008238
128*128	131072	8192	176	144	0.0625	0.001342773	0.0010984
32*256	65536	2048	18	14	0.03125	0.000244658	0.0002136
32*256	65536	4096	36	28	0.0625	0.000549316	0.0004272
32*256	65536	6144	54	42	0.09375	0.000823975	0.0006408
64*256	131072	2048	20	16	0.015625	0.000152588	0.0001221
64*256	131072	6144	60	48	0.046875	0.000457764	0.0003663
64*256	131072	4096	40	32	0.03125	0.000305176	0.0002442
128*256	262144	2048	22	18	0.0078125	8.39E-05	0.0000687
128*256	262144	12288	132	108	0.046875	0.000503543	0.0004122
128*256	262144	14336	154	126	0.0546875	0.000587463	0.0004809
256*256	524288	2048	24	20	0.00390625	4.58E-05	0.0000381
256*256	524288	22528	264	220	0.04296875	0.00050354	0.0004191
256*256	524288	24576	288	240	0.046875	0.000549316	0.0004572

Table 3. (**Comparison of logic gate technique, LSB and mode and multiple method by varying size of message in image size of 256*256 bytes)**

Size of inserted message bits	**Change in image using Logic gate technique**	**Change in image using LSB method**	**Change in image using mode and multiple method**
256	4.58E-05	0.00390625	0.0000381
1024	0.000183105	0.015625	0.0001524
1536	0.000274658	0.0234375	0.0002286
2048	0.000366211	0.03125	0.0003048
2304	0.000411987	0.03515625	0.0003429
2560	0.000457764	0.0390625	0.000381
2816	0.000503514	0.04296875	0.0004191
3072	0.000549316	0.046875	0.0004572
3584	0.000640869	0.0546875	0.0005334
5120	0.000915527	0.078125	0.000762
10240	0.001831055	0.15625	0.001524
15360	0.002746582	0.234375	0.002286
20480	0.003662109	0.3125	0.003048
23040	0.004119873	0.351625	0.003429
25600	0.004577637	0.390625	0.00381
28160	0.0050354	0.4296875	0.004191
30720	0.005493164	0.46875	0.004572
35840	0.006408691	0.546875	0.005334
51200	0.009155273	0.78125	0.00762
153600	0.02746582	2.34375	0.02286
204800	0.036621094	3.15	0.03048
102400	0.018310547	1.5625	0.01524

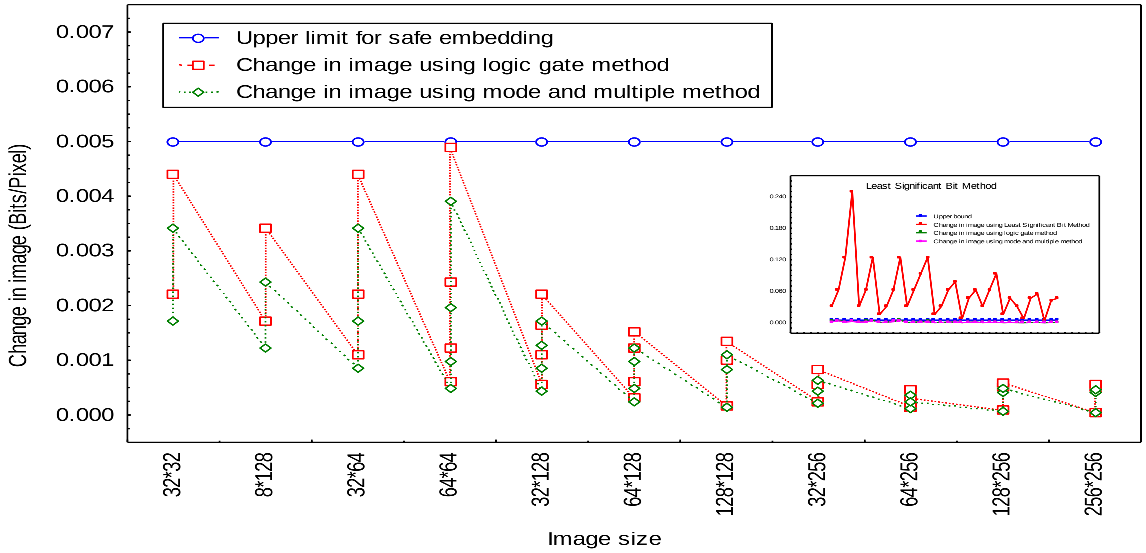


Figure 1: Comparison of multiple and mode method with logic gate method and upper limit for safe embedding in different image sizes. The inset image shows the comparison of least significant bit method with upper limit for safe embedding, logic gate method and mode and multiple method.

5. REFERENCES

[1] G J Simmons, "The Prisoners Problem and the Subliminal Chaunell", Proceedings of cypto" 83, Plenum Press, pp 51-67, 1983.

[2] Parvinder Singh, Sudhir Batra, HR Sharma, "Steganographic Techniques Based on Digital Logic for Minimum Embedding and Maximum Hiding", WSEAS Transactions on Signal Processing, issue 5, vol 3, May 2007, ISSN 1790-5022, pp 346-353.

[3] Neil F Johnson, Sushil Jajodia, "Exploring Stenography: Seeing the Unseen", IEEE Computer, Feb 1998, pp 26-34.

[4] Neil F. Johnson, Sushil Jajodia, "Steganalysis of Images Created Using Current Steganography Software", *Lecture Notes in Computer Science*, vol 1525, 1998, Springer-Verlag.

[5] JJ Eggers, R Bauml, Bernd Grid, "A Communication 4675, Jan 2002, *Security and Watermarking of Multimedia Contents IV*, San Jose, Callifornia.

[6] Parvinder Singh, Sudhir Batra, HR Sharma, "Evaluating the Performance of Message Hidden in 1st and 2nd Bit Plane", *WSEAS Transactions on Information Science and Applications*, issue 8, vol 2, Aug 2005, pp 1220-1227.

[7] Sudhir Batra, Rahul Rishi, Rajkumar , "Insertion of Message in 6th , 7th and 8th Bit of Pixel Values and Its Retrieval in Case Intruder Changes the Least Significant Bit of Image Pixels", International Journal of Security and its Applications, issue 3, vol, 4, July 2010, pp 1-10.

[8] SN Sivanandan, CK Gokulnath, K Prasanna, S Rajeev, "NFD Techniques for Efficient and Secured Information Hiding in Low Resolution Images", *Lecture Notes in Computer Sciences*, vol 3347, Springer Verlag, 2004, pp 458-467.

[9] NF Johnson, S Katzenbeisser, "A Survey of Steganographic Techniques", *Information Hiding*, Artech House, pp 43-78, 2000.

[10] Jessica Fridrich, Miroslav Goljan , Rui Du, "Detecting LSB Steganography in Color and Gray-Scale Images", IEEE Multimedia, issue 4, vol 8, 2001.