Digital Logic Embedding Using Single Row

Jasvinder Kaur
Research Scholar, Department of Computer Science & Engineering
Deenbandhu Chhotu Ram University of Science & Technology, Murthal
Sonepat, India
jkharabanda@yahoo.com

Manoj Duhan
Professor, Department of Electronics Engineering
Deenbandhu Chhotu Ram University of Science & Technology, Murthal
Sonepat, India
duhan_manoj@rediffmail.com

Ashok Kumar
Professor, Department of Computer Application
Kurukshetra University, Kurukshetra
India

***Abstract*— We present a technique to improve embedding capacity of Image using digital logic in this paper. We have applied digital logic operations on two equal halves of an image row to derive the hidden information. We have also compared the change in image using proposed technique and digital logic gate technique. Change in Image using proposed technique is half or more than that of logic gate technique.**

Keywords- Steganogaphy, Data Hiding, Data Embedding, Digital Logic Embedding

I. Introduction

Information Hiding for Secure Communication and Copy Right Protection is a highly multidisciplinary area that includes digital image processing, signal processing, communication engineering, physical properties of electronics devices, coding theory, data compression, cryptography and the theory of visual perception. Steganography is the name given to hide the information in digital objects for secure communication [1]. The most common steganographic technique is the Least Significant Bit embedding (LSB) [2] used in number of tools s-tools, Ez-stego, Hide and seek, Jphs for windows, courier tool. The premise here is that changes to the least significant bit will be masked by noise commonly present in digital images. Actually, in the case of color images, there is even more room for hiding messages because each pixel is a triple of red, green, and blue. Again, replacing two or more least significant bits of each pixel increases the capacity of the scheme but at the same time the risk of making statistically detectable changes also increases [3]. But there is chance that if we will change the last bit or bits of the every image then even if we are not able to extract the message we can destroy the information contained in the image. Data can be hidden in number of new file formats other than images. An Interesting way of data hiding in MS Word is given in [4]. A high-capacity steganography algorithm for embedding data in the inactive frames of low bit rate audio streams encoded by G.723.1 source codec was given in [5]. A Study of Information Hiding Performance can also be done using simple dot pattern [6].

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 [7-8]. An upper bound of 0.005 bits/pixel was experimentally determined for safe Least Significant Bit (LSB) embedding by Jessica at all [9-10]. An edge adaptive scheme which can select the embedding regions according to the size of secret message and the difference between two consecutive pixels in the cover image was described in [11]. A method to improve watermark robustness by exploiting the masking effect of surface roughness on watermark visibility was proposed in [12]. 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 [13-14].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. We have tried to decrease the actual embedding further in Digital Logic technique to make it safer. In proposed technique, we have used only one row address to derive the information matrix.

II. PROPOSED TECHNIQUE

A. *Insertion Scheme*

We have used the Logic gates (AND, OR, XOR, and NOT as proposed by Parvinder et al) on image matrix to derive the information matrix in this technique.

Insertion Scheme is shown in figure 1.The image file and the information to be hidden are read as rows of bits matrices. Preprocessing of matrices is done such that number of columns in Image matrix is double of Information matrix. Logic operation deriver uses logic gate operations such as AND, OR, XOR and NOT to get the rows of information matrix from image matrix rows. We are using following op-codes for logic operations-

Logic Operation 'Op'	Op-Code
AND	00
OR	01
XOR	10
NOT	11

Logic operations will be applied on two equal halves of each Image matrix row to derive the Information matrix row. It is contrast to digital logic technique where logic operations were applied on two rows of Image matrix. As the number of columns in Image matrix is double of Information matrix, the derived information is equal to number of columns in Information matrix.

Take an example of 256*256 bit image matrix and 256 bits information. The 256 bits of Information can be written in single row information matrix. Then we will write the image matrix in form of 128*512 to make number of columns in image matrix double to number of columns in information matrix. Now 256 information bits can be derived applying logic gate one by one on two equal half of each row of Image matrix. Further Suppose Information is derived from 3rd row of Image matrix by applying "AND" operation. Then embedded data will 000000011.Here total insertion will be of 9 bits (2 bits for op-code and 7 bits for address of 128 rows of Image, So total 9 bits). First two bits (00) of embedded data represent op-code for "AND" operation and remaining seven bits (0000011) represent address of 3rd row. In digital logic technique, total embedded data was 18 bits for the same 256 bits information in 256*256 bit image matrix. Further in case of "NOT" logic operation in proposed technique, the 9 bits are required to derive the 512 bits of information as "NOT" operation is applied on entire row of image matrix. It may be noted that, if we will convert the 256*256 bit image matrix in to 64*1024 or 32*2048 or of more columns then this technique will require further less embedding for more data, but probability of getting derived data will be less. Derived data will be inserted in Image using existing embedding techniques.

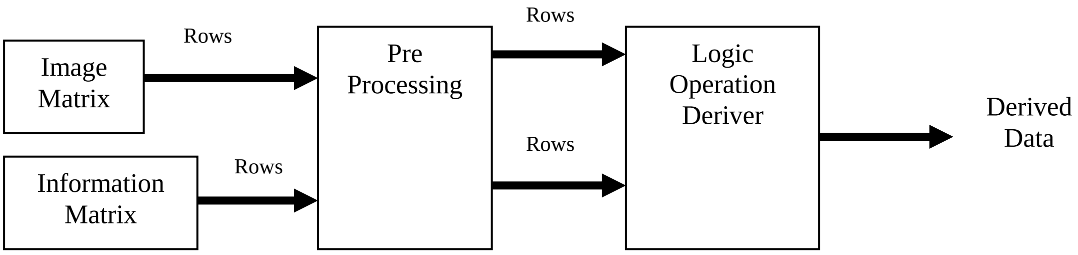

Figure 1 Insertion scheme

B. *Retrieval Scheme*

Retrieval Scheme at receiver end to retrieve the hidden information is shown in figure 2. Embedded Data at known location is fetched from image matrix. This data contains op-code and row address. Op-code is applied logical operation and row address is address of image row on which logic operation is performed. Image matrix is also rearranged to known 'Converted Image matrix' so that logical operation 'op-code' can be applied on the two equal halves of Image row. Logic Operation Converter derives the Information from op-code, row address and converted Image matrix.

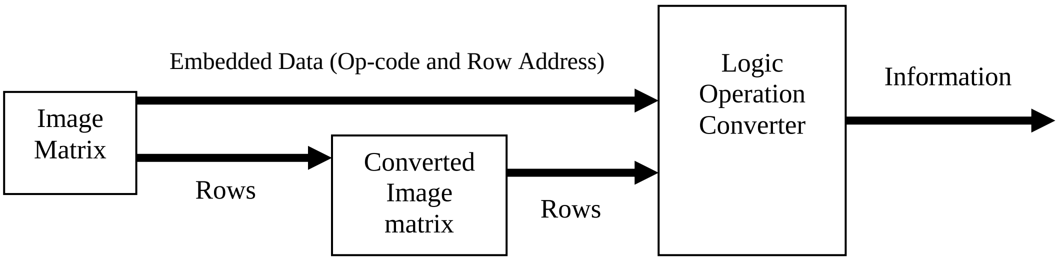
Embedded Data (Op-code and Row Address)
Image Matrix
Rows
Converted Image matrix
Rows
Logic Operation Converter
Information

Figure 2 Retrieval Scheme

III. Results

Results of proposed scheme and logic gate scheme on different Image size and different converted Image size are shown in table 1. Table clearly shows that change in Image using proposed technique is half or more than that of logic gate technique. Figure 3 shows Change in Image using Logic Gate Technique Vs Change in Image using Proposed Scheme.

Image Size	Image Size (Bytes)	No of Information Bits Inserted	No of Bits inserted in Logic gate Technique	Converted Image Size in Proposed Scheme	No of Bits inserted in Proposed Technique	Change in Image using Logic Gate Technique	Change in Image using Proposed Scheme
256*256	524288	256	18	128*512	9	3.43323E-05	1.71661E-05
256*256	524288	256	18	64*1024	8	3.43323E-05	1.52588E-05
256*256	524288	256	18	32*2048	7	3.43323E-05	1.33514E-05
256*256	524288	1024	72	128*512	36	0.000137329	6.86646E-05
256*256	524288	1024	72	64*1024	16	0.000137329	3.05176E-05
256*256	524288	1024	72	32*2048	7	0.000137329	1.33514E-05
256*256	524288	2048	144	128*512	72	0.000274658	0.000137329
256*256	524288	2048	144	64*1024	32	0.000274658	6.10352E-05
256*256	524288	2048	144	32*2048	14	0.000274658	2.67029E-05
128*128	131072	256	32	64*256	16	0.000244141	0.00012207
128*128	131072	256	32	32*512	7	0.000244141	5.34058E-05
128*128	131072	256	32	16*1024	6	0.000244141	4.57764E-05
128*128	131072	1024	128	64*256	64	0.000976563	0.000488281
128*128	131072	1024	128	32*512	28	0.000976563	0.000213623
128*128	131072	1024	128	16*1024	12	0.000976563	9.15527E-05
128* 128	131072	2048	256	64*256	128	0.001953125	0.000976563
128*128	131072	2048	256	32*512	56	0.001953125	0.000427246
128*128	131072	2048	256	16*1024	24	0.001953125	0.000183105

Table 1 Comparison of Logic Gate Technique and Proposed Technique

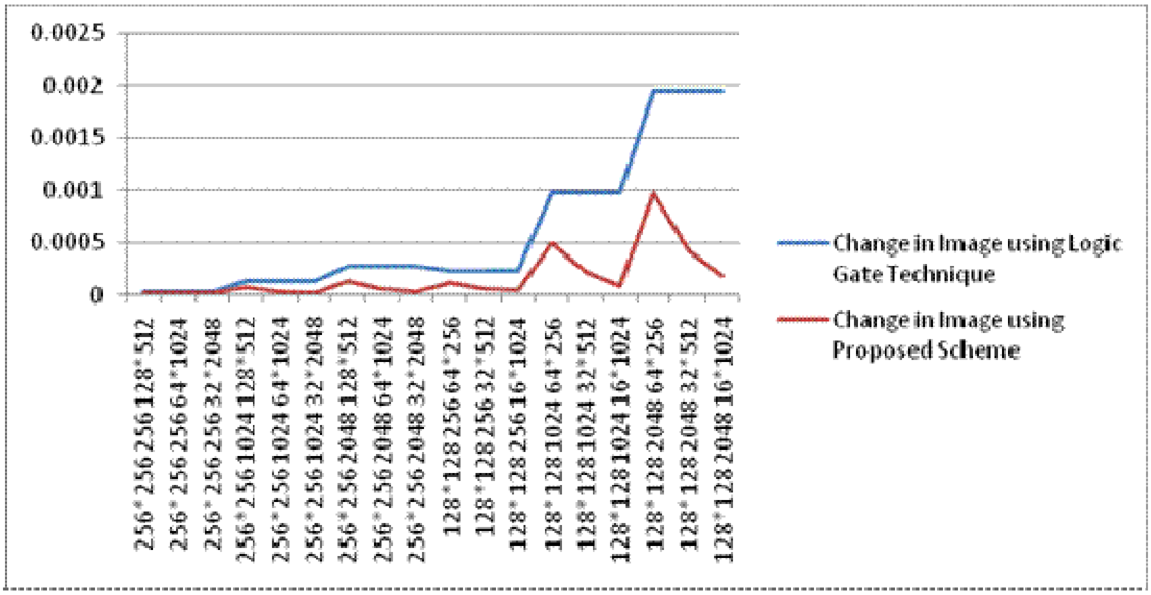

Figure 3 Change in Image using Logic Gate Technique Vs Change in Image using Proposed Scheme

REFERENCES

[1] Neil F. Johnson and Sushil Jajodia: Exploring Steganography: Seeing the Unseen, IEEE Computer Mag., pp.26-34, Feb. 1998.

[2] Jonathan Watkins: Steganography - Messages Hidden in Bits, Multimedia System Conference 2002, University of Southampton, U.K., 2002.

[3] Chunfang Yang, Fenlin Liu, Xiangyang Luo, Bin Liu, Steganalysis Frameworks of Embedding in Multiple Least-Significant Bits, IEEE Transactions on Information Forensics and Security, Dec 2008, Vol 3, Issue 4, pp 662-672.

[4] Tsung-Yuan Liu, Wen-Hsiang Tsai, A New Steganographic Method for Data Hiding in Microsoft Word Documents by a Change Tracking Technique, IEEE Transactions on Information Forensics and Security, March 2007, Vol 2, Issue 1, pp 24-30.

[5] Yong Feng Huang, Shanyu Tang, Jian Yuan, Steganography in Inactive Frames of VoIP Streams Encoded by Source Codec , IEEE Transactions on Information Forensics and Security, June 2011, Vol 6, Issue 2, pp 296-306.

[6] R Chandramouli, Nasir Memmon, Analysis of LSB based Image Steganography Techniques, Proccedings of ICIP 2001, Greece, Oct 2001, pp 1019-1022.

[7] R Chanramouli, “A Mathematical Framework for Active Steganalysis”, ACM Multimedia Systems Journal, 2003.

[8] RJ Anderson, FAP Petitcolas, On the Limits of Steganography, IEEE Journal of Selected Areas in Communication, Special issue 16 no 4, 1998, pp 474-481.

[9] J Fridrich, MGoljan, R Du, Reliable Detection of LSB Steganography in Grayscale and Color Images, Proccedings of ACM Workshop on Multimedia and Security, Canada, Oct 2000, pp 27-30.

[10] J Fridrich, MGoljan, R Du, Detecting LSB Steganography in Color and Grayscale Images, IEEE Multimedia, Nov 2001, pp 22-28.

[11] Weiqi Luo, Fangjun Huang, Jiwu Huang, Edge Adaptive Image Steganography Based on LSB Matching Revisited, IEEE Transactions on Information Forensics and Security, June 2010, Vol 5, Issue 2, pp 201 – 214.

[12] Kwangtaek Kim Barni, M. Tan, Roughness-Adaptive 3-D Watermarking Based on Masking Effect of Surface Roughness, IEEE Transactions on Information Forensics and Security, Dec 2010, Vol 5, Issue 4, pp 721 – 733.

[13] Parvinder Singh,Sudhir Batra, HR Sharma, Steganographic Methods Based on Digital Logic, Proceedings of the 6th WSEAS International Conference on SIGNAL PROCESSING, Dallas, Texas, USA, March 22-24, 2007, pp 157-162.

[14] Parvinder Singh,Sudhir Batra, HR Sharma, Steganographic Technique Based on Digital Logic for Minimum Embedding and Maximum Hiding , WSEAS Transaction Signal Processing Issue 5 vol 3, May 2007, pp 346-353.