AN EFFICIENT 8-BIT IMAGE STEGANOGRAPHY TECHNIQUE BY REVERSE SEARCHING METHOD

[1]Sitikantha Chattopadhyay
[1]Assistant Professor
[1]Computer Science and Engineering
[1]Brainware University, Barasat, Kolkata, India

Abstract: Image steganography is taking a dominant position in the field of network security. Here an advanced slab-based image steganography technique has been proposed where searching domain to hide a secret message is increased by almost 98%. First a grayscale image is taken and resized with a desired size. Then slab-based image steganography technique with diagonal searching is applied. If no suitable row/column/diagonal has been found, then reverse searching operation is performed with all these row/column to form a completely new searching domain. It maximizes the probability to get exact match with the secret message. In this technique, cover image is slightly modified but gives promising results with respect to other existing techniques.

Index Terms **- Steganography, LSB technique, Reverse Searching Technique.**

I. INTRODUCTION

Steganography is a popular network security technique in which some secret message is inserted into some media (image, audio or video) in such a way that the originality of the original media is not altered or slightly altered (Encryption). In image steganography, this initial image is called input image and after inserting the secret message, this becomes a stego image. It is forwarded over network and at the destination side; receiver applies the reverse process to get the original message (Decryption) [1][2][3].

Among popular image steganography techniques, LSB insertion is a most popular one. Here some of the least significant bit of pixel intensity is changed according to the binary representation of the secret message. Since only least significant bit is changing, the value of pixel intensity is either incremented or decremented by 1[4].

We have divided this paper in following six sections. After introduction about related technologies, slab based image steganography technique is discussed in section II. Then proposed method is given in section III. Result and analysis of the proposed method is given in section IV followed by conclusion in section V and references in section VI.

II. SLAB-BASED IMAGE STEGANOGRAPHY TECHNIQUE WITH DIAGONAL SEARCHING

It is one of the most popular image steganography techniques that use LSB insertion technique. Here an input image will be first divided into some fixed size slab and each slab will be further divided into equal number of sheets representing the respective bit positions of pixel intensity of that slab. The secret message will be also transfer into binary representation. Length of the binary representation of secret message should be same as the number of pixel present in row/column in a slab.

Now all the rows, columns and diagonals of individual sheet of all slabs will be searched for an exact match with the binary representation of the secret message. Only last sheet (LSB Sheet) of all slabs will excluded from this searching process. If any row exactly matches with the message, then corresponding pixel intensity in original slab will be increased by one. Similarly if any column exactly matches with the message, then corresponding pixel intensity in original slab will be decreased by one.

If part of the message is matched with any row, then the above process will be repeated along with some extra work. In this situation, the position of unmatched bits will be marked in last row of LSB sheet.

If the secret message is exactly matches with any one diagonal of a sheet, then at first matching diagonal need to be identified. Every sheet has two diagonals namely top-left to bottom-right (1st diagonal) and top-right to bottom-left (2nd diagonal). In this case, each pixel intensity of last row of a slab will represent individual sheet for a particular slab. If match found in 1st diagonal of a sheet, then corresponding intensity in last row of that slab will increase by 1. Similarly, if match found in 2nd diagonal of a sheet, then corresponding intensity in last row of that slab will decrease by 1. But in both this cases, there will be no change in any other pixels within that block [5][6][7][8].

In Fig. 1, an 8-bit gray-scale image has been taken. Here a slab of the image and corresponding pixel intensities and binary representations has been shown. In Fig. 2, that slab is divided into 8 different sheets. Flow chart of slab-based image steganography with diagonal searching is shown in Fig. 3.

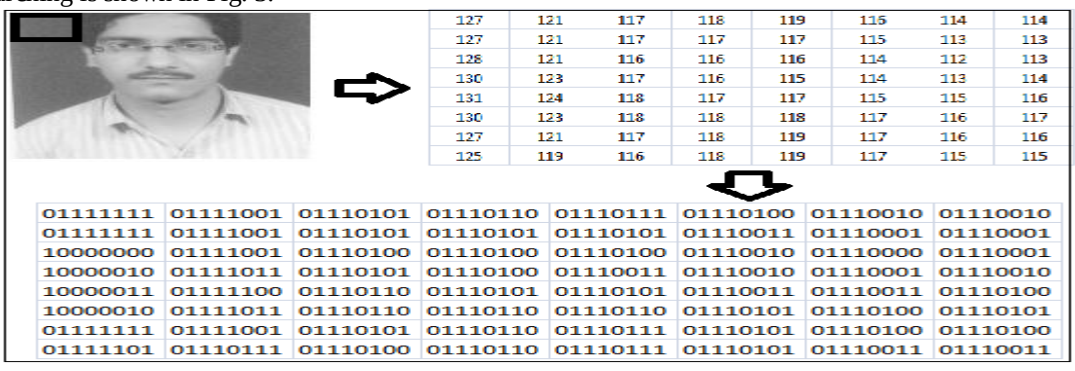

Fig. 1: An Image Slab

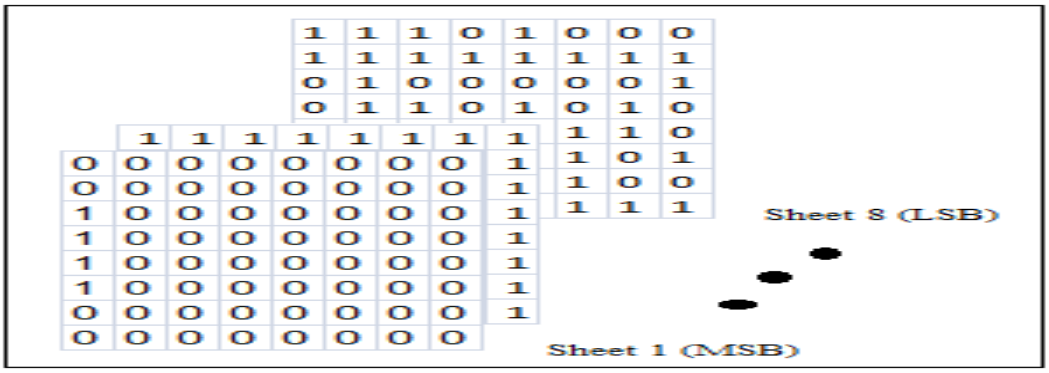

Fig. 2: Division of slab into 8 sheets

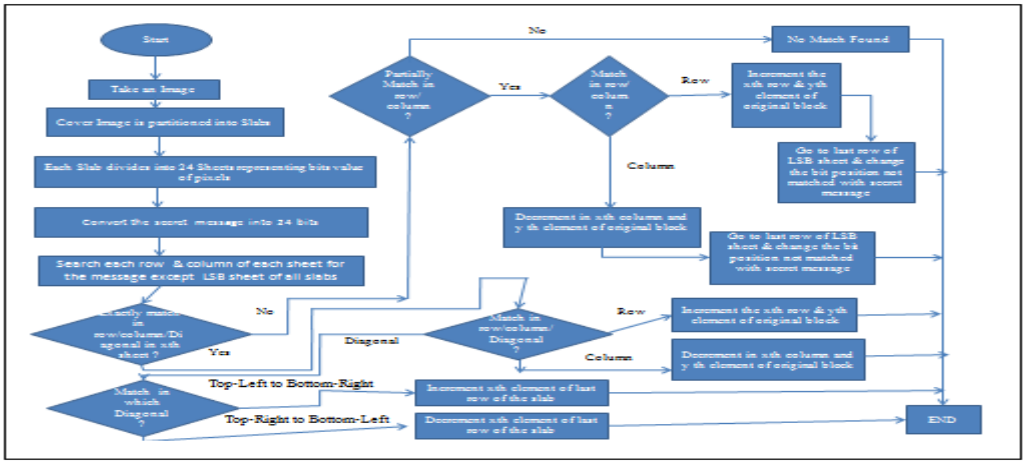

Fig. 3: Flowchart of slab-based image steganography with diagonal searching

III. Proposed Method

This research paper is the extension of standard slab-based image steganography technique with diagonal searching. It will enhance the search domain by almost 98%, so probability to find exact match of secret message with any row/column/diagonal of any sheet of the image is maximized. At first, the secret image will be searched across all row/column/diagonal of all sheets except LSB sheet of all slabs. If there is a match, then according to the conventional method, position of the matching will be stored in the slab. If there is no match, then some additional method will be applied.

Here all row and column will be searched in reverse order to find a match with the secret message. Searching will be started from least significant bit to most significant bit for every row and column. In this method, not only the LSB sheet, but last row of 2nd last sheet is also excluded from the searching domain. In this row, only the last bit will be changed to indicate that reverse searching has been applied. This process is explained in fig. 4.

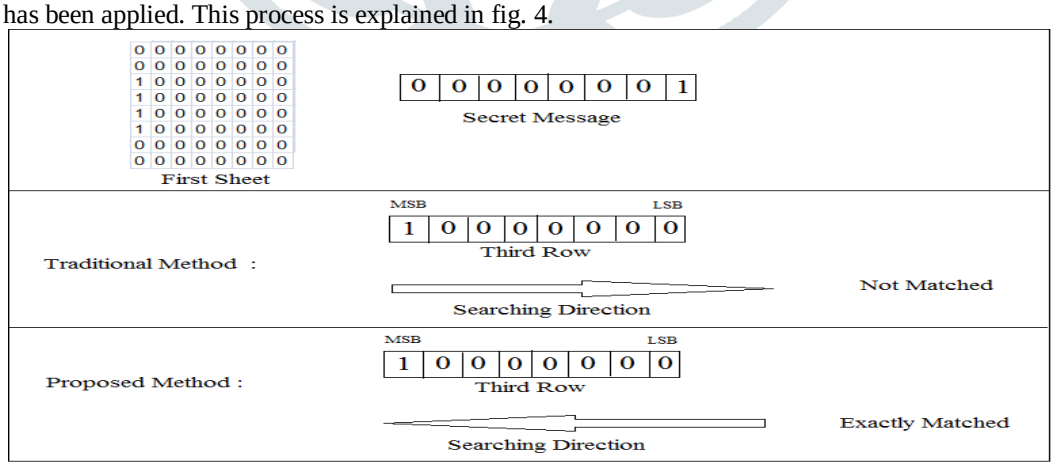

Fig. 4: Matching of secret message with proposed method

IV. Result and Analysis

There are many other techniques are available to hide a secret message in a digital image in both traditional and online literature. Some well known techniques are architecture platform for gray level modification, LSB replacement technique, Secret message hiding in image edges, LSB matching revisited etc. A comparison table is given below with respect to MSE and PSNR parameter for all the above methods along with our proposed method.

Table 1 Comparison between Existing Methods and Proposed Method

Method	MSE	PSNR
LSB replacement[9]	0.0283	66
Hiding gray image using blocks[10]	0.4078	51
Hiding message using edge of images[11]	0.0297	65
Architecture platform for gray level modification[12]	0.0289	66
LSB matching revisited[13]	0.0220	64
Proposed method	0.0131	63

In the above table, MSE is Mean-Square-Error indicates the average squared difference between the desired output and actual output. For a specific method, it should be minimum. The full form of PSNR is Peak-Signal-to-Noise-Ratio. It measures the peak error for a method. These two errors are commonly used to measure the quality of an image, after applied by a specific method [14]. In Fig. 5, the above data has shown graphically.

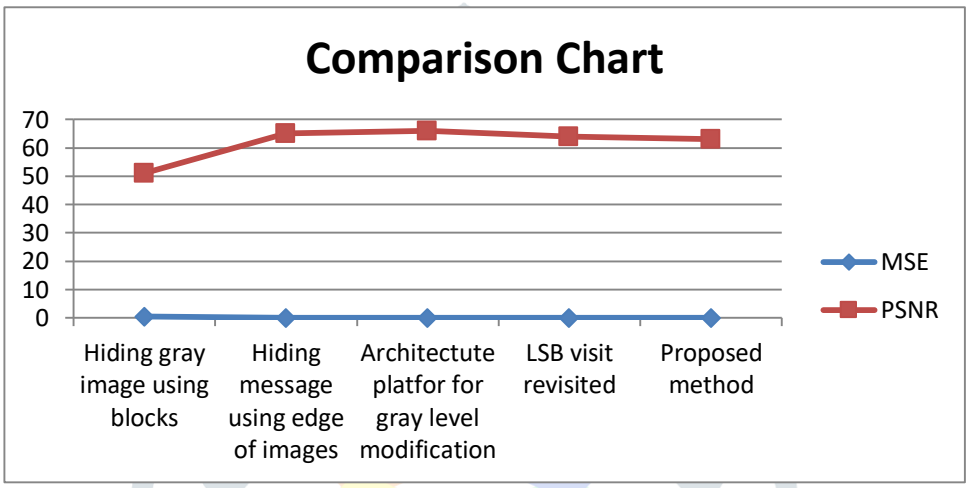

Fig. 5: Comparison with MSE and PSNR

Since the searching is done twice time – according to traditional way for the first time and according to proposed method for second time, the execution time will be more, but the probability to get the exact match is drastically improved. The following figure is showing the comparison-

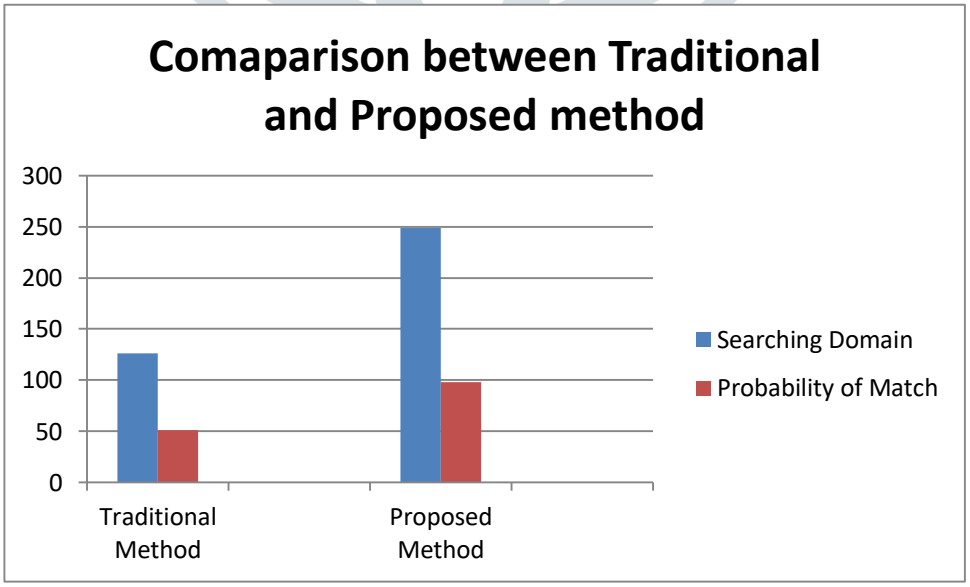

Fig. 6: Comparison with Searching domain and Probability of Match

In the above comparison, searching domain implies the total numbers of row, column and diagonal, which will searched for exact match with the secret message. The probability of match is the chance to find the exact match with respect to the corresponding searching domain. Since searching will be done in reverse order after applying traditional method, the chance to get exact match will be almost double.

V. CONCLUSION

Since searching will be done in reverse order after applying traditional method, the chance to get exact match will be almost double. The execution time will be proportionally double but if the method can be implemented using parallel processors, then the desired result can be achieved with minimum time.

REFERENCES

[1] Pevni. T, Filler. T and Bas. P. 2010. Using high-dimensional image models to perform highly undetectable steganography. Lecture notes in Computer Science, 6387: 161-177.

[2] Kahate. A. 2014. Cryptography and Network Security (3rd ed.). New Delhi: McGraw Hill.

[3] Fridrich. J, Goljan. M, and Soukal. D. 2005. Perturbed quantization steganography. ACM Multimedia System Journal, 11(2): 98-107.

[4] Chan, Chi-Kwong and Cheng. L. M. 2004. Hiding data in images by simple LSB substitution. Pattern Recognition, vol. 37(3): 469-474.

[5] Thenmozhi. M. J and Menakadevi. T. 2016. A new secure image steganography using LSB and spiht based compression method. International Journal of Engineering, 16(1).

[6] Tyagy. S. and Agarwal. A. 2011. Multy layers sequrity scheme for embedding secrets in stego image. International Journal of Advanced Engineering Sciences and Technologies, 3(1): 29-33.

[7] Bhattacharya. D. Das. P. Bandyopadhyay. K. S. and Kim. Tai-Hoon 2009, Text steganography: a novel approach. International Jornal of Applied Science and Technology, 3(2).

[8] Sutaone. M. S. Khandare. and M. V. 2008. Image based steganography using LSB insertion technique. Proc. IEEE WMMN, 146-151.

[9] T. Sharp 2001. An implementation of key-based digital signal steganography. Proc. Information Hiding Workshop. Springer LNCS, 2137: 13-26.

[10] S. Atawneh. 2006, A new algorithm for hiding gray images using blocks. Information and Communication Technologoes, 2(1): 1484-1488.

[11] Singh. K. M. Singh. L. S. Singh. A. B. and Devi. K.S. 2007. Hiding secret message in edges of the images. Information and Communication Technologies: 238-241.

[12] Khan. M. A, Potdar. V and Chang. E. 2004. An architecture platform for gray level modification steganography. Proc. 30th IEEE Annual Conference of Industrial Electronics Socity, 1: 463-471.

[13] Mielikainen. J. 2006. LSB matching revisited. IEEE Signal Processing Letters, 13(5): 285-287.