A More Secure Steganography Method in Spatia Domain

Thilaga.S[1]

[1] PG Scholar, Dept. of Computer Science and Engineering

M.A.R College Of Engineering and Technology

Trichirapalli, India

[1]thilaga508@gmail.com

Sankareswari.A[2]

[2] PG Scholar, Dept. of Computer Science and Engineering

M.A.R College Of Engineering and Technology

Trichirapalli, India

[2]sankareswarimnp136@gmail.com

Sivaranjani.N[3]

[3] PG Scholar, dept.Of Computer Science and Engineering

M.A.R College Of Engineering and Technology

Trichirapalli, India

[3]ranjanisiva508@gmail.com

***Abstract*— This paper presents a new approach for hiding message in digital image in spatial domain. In this method two bits of message is embedded in a pixel in a way that not only the least significant bit of pixel is allowed to change but also the second bit plane and fourth bit plane are allowed to be manipulated, But the point is in each embedding process only one alternation in one bit plane is allowed to happen. As it is compared by the method LSB-Matching, the results shows this method has an acceptable capacity of embedding data and hardly is detectable for steganalysis algorithm.**

Keywords*—*Steganography; Steganalysis; Stego image; Cover image ;Bit plane; LSB-Matching

I. INTRODUCTION

Safe communication is attracting attention these years. Steganography is considered a good way to reach this goal. Steganography is the art of hiding information in a medium called cover. The information that is supposed to be hidden in the cover is called " message" and the final manipulated signal which carries this message is called stego. Digital image, video, audio, text and etc can all be a good medium to carry a hidden data. Image steganography can be classified in two major groups: special domain methods and transform domain methods. In special domain, the hiding process such as least significant bit(LSB) replacement, is done in special domain, while transform domain methods; hide data in another domain such as wavelet domain.

This feature is appealing in a hidden communication and taking advantage of this of image like histogram. Attackers could be aware of a hidden communication by just checking the Histogram of an image. A good solution to eliminate this defect was LSB matching. LSB-Matching was a great step forward in steganography methods and many others get ideas from it. In our method the probability of change in a bit plane is 1/4 and we hide two

bits of information by each change in a bit plane, but we are allowed to switch between 3 bit planes.

II. SUGESTED METHOD

In this paper it is planned to introduce a method that embed 2 bits information in a pixel and alter one bit from one bit plane but the message does not necessarily place in the least significant bit of pixel and second less significant bit plane and fourth less significant bit plane can also host the massage. Since in our method for embedding two bits message we alter just one bit plane, fewer pixels would be manipulated during embedding message in an image and it is expected for the steganalysis algorithm to have more difficulty detecting the covert communication. It is clear that in return complexity of the system would increase. A convolution decoder (3, 1) is shown in the Fig. 1. This machine is not going to work as a decoder and is supposed to help us to change the amount of pixels in the cover image to produce a new stego image. This machine works in this manner. Each time the 4 less Significant Bits of a pixel will enter this machine.

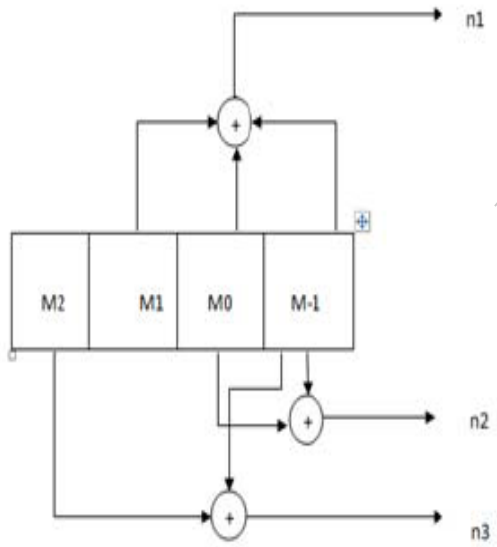

Fig. 1. Cover to stego transformer machine

Three XOR operations create three outputs for this machine. n1, n2, n3 are the outputs of this machine. So as it can be seen, this machine simply do just three XOR operations. Suppose n2, n3 as the hidden message which is embedded in the pixel. If n2, n3 be the same as hidden information, then there is no need to manipulate the original image; If not, then we should change the original image in a way to cause the output of the decoder be equal to the hidden message. Now the question comes to the mind is that how these 4 bits should be altered. Here there is an answer; in this paper the goal is that only one bit is going to be changed. In that case by changing one bit plane in a pixel, two bits of message should be transmitted. In our method there are only three ways that a pixel is allowed to be changed:

- ✓ Its least significant Bit would alter (So the gray level of the pixel would increased or decreased by one level)
- ✓ The second less significant bit plane would alter (So the gray level of the pixel would increase or decrease by two levels)
- ✓ The fourth less significant bit plane would alter (So the gray level of the pixel would increase or decrease by eight levels)

The procedure which changes one of the first four less significant bit plane of pixel is shown in the table 1 and an example for a cover pixel with the four less significant bit planes of [0 0 0 0] is brought on Fig. 2 This method is working very similar to LSB Matching. The similarity is in a way that it sometimes increases the value of a pixel, sometimes decrease the value of the pixel and sometimes do not change it. The different is that it does not consider the Least Significant Bit the only available place to hide the message but also the next bit planes can help. Our experiments over 8000 Digital photos showed that naked eye could not discriminate between stego and cover images.

In the experiment no artifact was observed by adding or subtracting 8 gray levels to a few pixels of an image which is happening in our method. Since with this method of embedding data, altering the fourth less significant bit plane does not create problem, we decided to manipulate fourth less significant bit plane rather than third less significant bit plane. This decision was made, because on the other hand by embedding data with high strength, the cover image is distorted so much that the cover image statistics can no longer be derived reliably from the available stego image. So it would be harder for steganalysis algorithm to detect existence of a hidden communication.

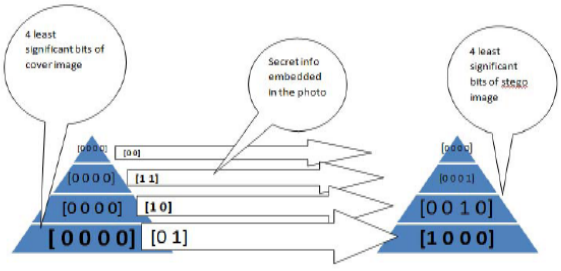

Fig. 2 How cover pixel with four less significant bits of [0 0 0 0] change according to different messages

Table 1. Explains how a two bits message is embedded in the four less significant bit planes of a pixel. The value of four less significant bits of cover pixel is shown at the first column. It means the value of pixel before being manipulated is brought on this column. This value will enter the decoder and the output is brought on the second column. As it was mentioned above, the decoder receives 4 bits andgenerates 3 bits as the output. The second and third bits are considered as the hidden message. So skipping the first bit, the value of the second bit and the third bit are the secret message. This is the message that naturally the cover image is carrying and is demonstrated at the third column of the table. So if the two bits of message are equal to this value, there is no need to cause any change in the original pixel. Two bits can combine and produce at most four states. The three other different states of secret bits and the value of 4 less significant bits of stego pixel which can result them are brought on the fourth column. It means hiding the two bits of message locating at the left side of the fourth column requires the 4 less significant bits of the cover image changes to the value which is brought at the right side of fourth column.

In other words if a stego pixel which its four less significant bits are shown on the right side of the fourth column enter the proposed decoder then a secret message which its value is brought on the left side of fourth column will be generated. Comparing the cover image at the first column with stego image located at the right side of fourth column, shows that generating any two bits message out of the decoder need a change in at most one bit plane from the cover image. At the end the amount of change in the gray level of original pixel, in each case, is shown at the last column.

Now that briefly each column was introduced, as an example the first row of this table will be reviewed. The first four less significant bit planes of Original pixel (cover) is demonstrated at first column by [0 0 0 0]. Entering this value to the decoder, it results [0 0 0] which is showed in the second column. The first bit is ignored and the other two bits which are considered as the value of the natural message lying in the original image is [0 0]. This value is put on the third column. The fourth column says that if the secret message is [0 1] then the fourth bit plane should change to one. So, to create the stego image, the first four less significant bit planes of the cover image should change to [1 0 0 0]. If the message is [1 0] then the first four less significant bit planes of the cover image should alter to [0 0 1 0] and if the message is [1 1] then the first four less significant bit planes of the cover image should alter to [0 0 0 1].

In each transformation of a pixel only one bit will vary but this variation can cause in an increase or decrease in gray level of the pixel by one, two or 8 levels which is shown at the last column. The whole operation of changing the first four less significant bits of a pixel in order to embed a specific two bits message on the four less significant bits of cover pixel is summarized in the table 1. In the Fig. 2, as an example, It is explained and demonstrated that How a cover pixel with first four less significant bits of [0 0 0 0] changes regarding to different possible messages and how the four less significant bits of stego pixels are produced due to each message.

A. Distortion and capacity

As explained in the previous section in this method two bits can be stored per pixel of a cover image. So the capacity of embedding data can increase up to two bits per pixel. Depending on how much the maximum capacity of a safe communication with a specific method is, this method can help us to increase it. The distortion occurs in this method is very dependent on the value of original pixel and the value of message. As it was shown in the table.1, value of a pixel can remain fixed, Increase or decrease by 1 level, Increase or decrease by 2 levels and even Increase or decrease by 8 levels. The expectation of change in gray level of a pixel in this method is calculated as below:

Expected gray level change = (1+ 2 + 8 + 0)/4 = 2.75

On the other hand the expected gray level change for the method LSB-Matching is equal to (1+ 0)/2 =0.5 Since the expected gray level change for a pixel in our method is greater than 0.5 which is the expected gray level change for the method LSB-Matching, it is expected that PSNR decreases by our method.

Fig. 3 shows P-SNR of our method and P-SNR for the method LSB-Matching over different rate of embedding data in the image. Blue bars show P_SNR for the method LSB- Matching and red bars show P_SNR for our method. P-SNR should not be below 39 otherwise the quality of image would be degraded more than what is allowed to happen to an image. As it is shown in the Fig.3 the method LSB-Matching has a better P-SNR than our method. It was expected and this is the price we pay to have gain over it.

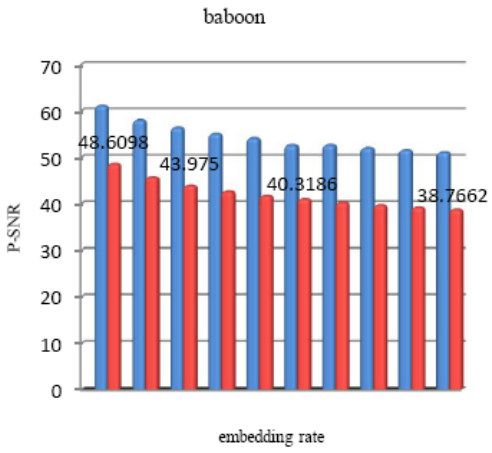

Fig 3. PSNR over various embedding rate for the Baboon image. From left to right embedding rate 0.1 bit/pixel, 0.2 bit/pixel, 0.3 bit/pixel, 0.4 bit/pixel, 0.5 bit/pixel, 0.6 bit/pixel, 0.7 bit/pixel, 0.8 bit/pixel, 0.9 bit/pixel, 1 bit/pixel

As it is shown in the Fig.3 the method LSB-Matching has a better P-SNR than our method. It was expected and this is the price is paid to have gain over it. The good news is that P-SNR of our method is above par and is in an acceptable range for steganography application. In our method P-SNR starts from 48.61 with the embedding rate of 0.1 bit/pixel, with the embedding rate of 0.6 bit/pixel it becomes 40.31 and finally it descended to 38.76 at the embedding rate of 1 bit/pixel. Further experiments with PSNR, for the images of Lena, Camera man, fishing boat and peppers showed the same results and approved that our method does not cause artifacts that can be noticed by naked eye. As it can be seen, P-SNR in our method is lower than P-SNR in the method LSB-Matching. However, in our method, even with a massive embedding rate, P-SNR is still in a good range and the quality of image is not degraded more than what is allowed. So it does not cause any artifact in the stego image and naked eye cannot distinguish the existence of a hidden communication in the stego image. Fig. 4 shows steganalysis algorithm notices the existence of a hidden message in the stego image long before that P-SNR descended 39 and low quality of picture cause us problem. To have a good quality of an image it is suggested that PSNR should be above 39. So in our method, still it is the statistical features of an image which causes us problem and reveals the existence of a hidden communication in the stego image.

III. EXPERIMENTAL RESULTS

To check the correct detection rate of this method a blind steganalysis algorithm introduced by Chen is used [3]. It extracts 54 features from the picture and discriminate the stego images from cover images with a good rate. Detection rate is defined by the rates that a stego image is detected as a stego image and a cover image detected to be a cover image.

So

Correct Detection rate = (nss + ncc) / ntot

ntot= nss + ncc + nsc + ncs

nss = number of stego image which detected as stego

ncc = number of cover image which detected as cover.

nsc = number of stego image which detected as cover.

ncs = number of cover image which detected as stego

In the experiment, 2000 image from the Corel database is used for training the steganalysis system and again another 1000 image from the database was selected to test the results. The pictures are selected randomly. We considered training and testing images of size 512 × 512. The detection rate of this method is compared with the LSB Matching and the results are shown in the Fig. 4.

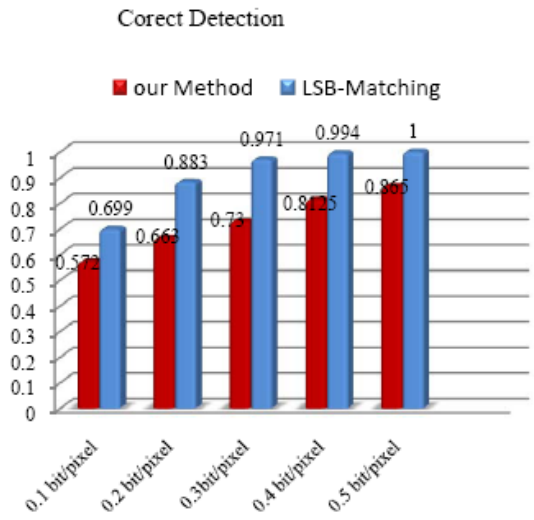

Fig. 4 Correct detection rate with embedding rate of 0.1 bit/pixel, 0.2 bit/pixel, 0.3 bit/pixel, 0.4 bit/pixel, 0.5 bit/pixel

The red bars show the correct detection rate of our method and the blue bars show the corect detection rate of LSB-Matching. As it can be seen, in our method the correct detection rate is up to 24% lower than the correct detection rate of method LSB-M at the embedding rate of 0.3 bit per pixel. It is a great improvement that shows our method is more secure than the method LSB-Matching.

To be more specific, The ROC plot for our method and for the method LSB-Matching is showed and compared in the Fig. 5 The red curve shows the performance of our method and the blue curve is the ROC plot related to the LSB-Matching method. As it can be seen, with the same rate of embedding data in image, the curve related to our method is closer to the diagonal axis which means it is very more secured than the method LSB-Matching.

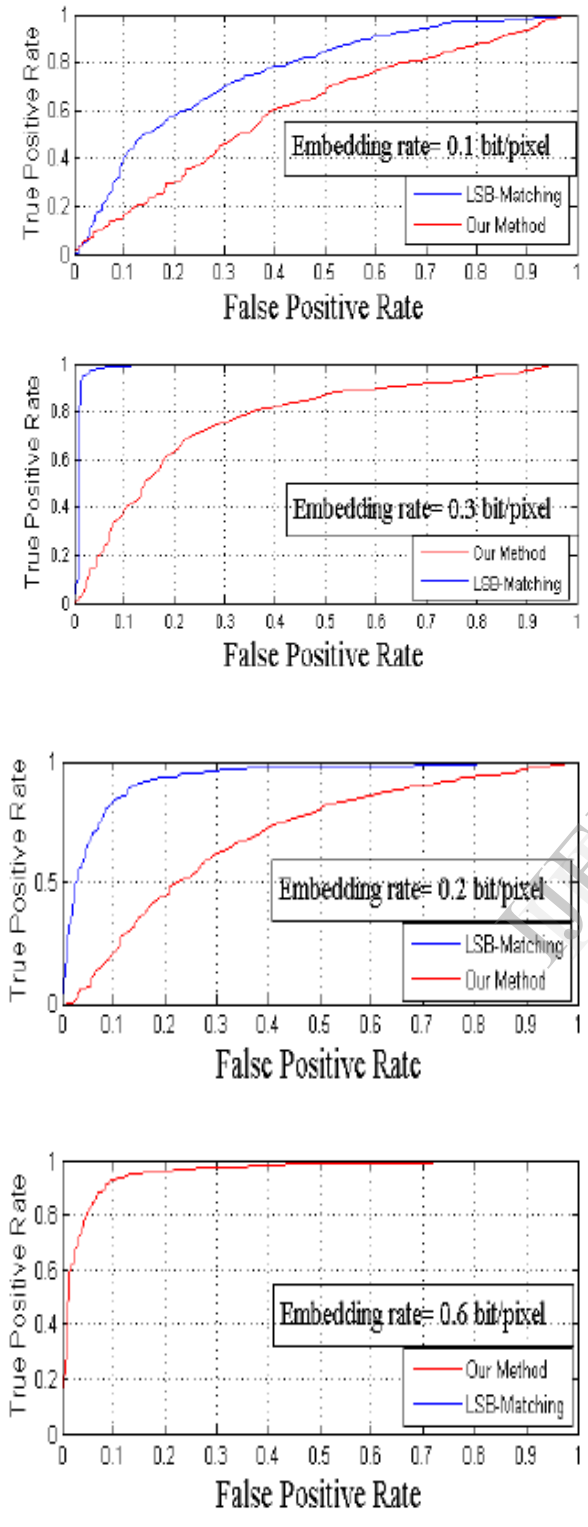

Fig. 5 ROC plot for our method and LSB-Matching method with different embedding rate of 0.1 bit/pixel, 0.2 bit/pixel, 0.3 bit/pixel and 0.6 bit/pixel

I V CONCLUSION

This paper suggests that embedding data in places else than just least significant bit is possible and if it be accompanied by a good plan, it can make the detection of hidden data in an image much harder for the steganalysis algorithm. Not only is the least significant bit the only available place which data can be hidden, Using a good coding, the data can be embedded on the other bit planes without making an intense detectable change that can be noticed with neither the naked eye nor the steganalysis algorithm.

REFERENCES

[1] E. Cole, Hiding in Plain Sight: Steganography and the Art of Covert Communication, Wiley Publishing, USA, 2003.

[2] M. Abolghasemi , H. Aghaeinia , K. Faez ,A . Mehrabi " Steganalysis of LSB-Matching Based on Co-Occurrence Matrix and Removing Most Significant Bit planes“, Intelligent Information Hiding and Multimedia Signal Processing , CHINA , 2008J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[3] Xiaochuan Chen, Yunhong Wang, Tieniu Tan, Lei Guo, "Blind Image Steganalysis Based on Statistical Analysis of Empirical Matrix," icpr, vol. 3, pp.1107-1110, 18th International Conference on Pattern Recognition (ICPR'06) Volume 3, 2006.

[4] A. Ker, “Improved detection of LSB steganography in grayscale images,” in Proc. Information Hiding Workshop, Vol. 3200, Springer LNCS, pp. 97–115, 2004.R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.

[5] Weiqi Luo, Fangjun Huang, Jiwu Huang, “Edge Adaptive ImageSteganography Based on LSB Matching Revisited”, IEEE Transactions on Information Forensics and Security, Vol. 5, No. 2. (June 2010), pp. 201-214.M.

[6] H. Sajedi and M. Jamzad, “Adaptive Steganography Method Based on Contourlet Transform”, ICSP 2008, pp. 745-748, October 2008.

[7] T. Sharp, “An implementation of key-based digital signal steganography,” in Proc. 4th Information Hiding Workshop, 2001, vol. 2137 of Springer LNCS, pp. 13–26

[8] S.Sarreshtedari ,” Steganography *and* Steganalysis” ,Msc thesis Sharif University of technology .2009