Enhancing Quality of LSB Based Image Steganography By Partitioning Method

Diksha[1], Jyoti Saxena[1], Sukhjit Singh[2]
[1]*GZS-PTU Campus, Bathinda, India*
[2]*GTBKIET Chhapainwali, Malout, India*

Abstract- *In* recent years, Steganography is most used with secret (covert) communication. Steganography is the art of secret (covert) communication, that helps us to hide the secret data (image, text, audio, video etc.), into the cover data (image, text, audio, video etc.). In this paper LSB based image steganography used with image partitioning method and improves the quality of stego image so that third person couldn't detect the secret data that hides into the cover image. The proposed method shows good enhancement in consideration to quality and simulation results improved in terms of bit error percentage and PSNR.

Keywords-*Steganography, LSB, Partition method, Bit Error Percentage, Image Quality, PSNR.*

I. INTRODUCTION

Steganography is the art of secret communication that helps us to hide the secret data into the cover. Steganography derived from Greek, literally means "Covered Writing." It helps us the people to communicate secretly. It means any third person can't detect the secret data. The original files shall be referred as cover data or cover image. It is the practice of encoding/ embedding secret data in a way such that the existence of the information is invisible. After inserting the secret data it shall be referred to as stego-image. A stego-key shall be use for hiding/encoding the secret (covert) data and provides the security to the secret or hidden data. [1].

After hide the secret data into the cover data there will be change in the cover data. At the transmitter side, secret data hides into the cover data with help of stego key and at the receiver side, receiver may detect the secret data if and only if receiver have the stego key and stego image. It is also called the de-Steganography [2].

To hide the secret data into the cover so many algorithms have been used. In this paper, LSB based algorithm will be use with Partition Method. In simple LSB method, the secret data will be insert into the cover of LSB bit. By inserting the secret data into the cover of LSB, LSB's of the cover becomes changed. Because of inserting data, stego image becomes changed bits than cover image bits. Because of change in stego image, anybody shall get idea some information that hides behind the image. Simple LSB method has some advantages and disadvantages which are given below as:

Advantages: - It is simple to understand, easy to carry out and produce stego image is almost same as cover image and couldn't judge by naked eyes.

Disadvantages: - It is not more robust because anybody can detect secret data easily; hiding the data capacity is also less and due to sequentially hide the data there is no security of this method [5].

In this paper, we proposed LSB based image steganography with Partition technique and compare with existing technique (Bit Inversion Technique).

II. PROPOSED WORK

In this paper, following steps are used:-

1. Take the secret data size should less than four times the cover image size. In this work cover image used .bmp and message image used .jpg.
2. Secret data or image will encrypt with RC4 stream algorithm [1] [9].
3. After encryption, encrypted data or image hides behind the cover image of 2nd and 3rd LSB and create the stego image.
4. **Bit Inversion Technique (EXISTING METHOD):-** In this method, if the average percentage change in bits will be more than 50% then they invert complete stego image [1]. To understand this we consider following example.
   - Suppose secret data is 1011
   - Cover image is 10001100 10101101 10101011 10101101
   - Stego image becomes 10001101 10101100 10101011 10101101
   - Now two bits are changed in stego image than cover image. According to existing method, they invert only three pixels of stego then results becomes
   - 10001100 10101101 10101011 10101100
   - Their result gives changed bits are now one [1].
5. Improvement Over Bit Inversion Technique

PARTITIONING METHOD:- In this method, if percentage change in bits in any half is more than 50% and other half is less than 50% and average change of bits is less than 50% then we invert that half which half is more than 50%changed bits percentage. Then our method shows better results than existing method. If both halves have changed in bits percentage more than 50% then we invert both halves then our method shows equal result with existing method. If both halves have changed in bits percentage less than 50% then we never invert both halves then our method shows equal results with existing method. To understand this we consider following example.

- Suppose secret data is 1011
- Cover image is 10001100 10101101 10101011 10101101
- Stego image becomes 1000110**1** 1010110**0** 1010101**1** 1010110**1**
- Now two bits are changed in stego image than cover image. We have employed partitioning method to improve the quality of stego image.
- According to partitioning method, divide the stego image into two halves. First half becomes 1000110**1** 1010110**0** and second half becomes 1010101**1** 1010110**1**. Now calculate changed bits in first half are two and changed bits in second half are zero. So, according to partitioning method invert only first half of the stego image. Now result gives changed bits become zero. So, partitioning method improves than existing method.

6. Divide that part of stego image into two halves or two parts where data will embed.
7. After that, calculate the changed bits and total bits embed in first half of the stego image and then similarly calculate in second half.
8. Find out the percentage changed bits in first half and in second half. It is known as bit error percentage. Bit error computes the actual number of bit positions that will change in the stego image as compare to cover image. It will calculate by formula:

- Bit Error Percentage= (changed bits/total bits)*100
- Total bits= changed bits+ unchanged bits

9. In this work, take four cases and compare the results with existing method.

Case-1 If bit error percentage in first half is 60% and bit error percentage in 2nd half is 40%then according to existing method average bit error percentage is 50%. Hence no need of inversion. But with our improved method, we invert first half and bit error percentage gets 40% without inverting the second half. Hence we get 40% average change which is better than existing method.

Case-2 if bit error percentage in first half is 75% and bit error percentage in 2nd half is 85% then according to existing method average bit error percentage is 20%. Our improved method, also invert both halves and bit error percentage gets also 20%. So, in this case results are same as existing method.

Case-3 if bit error percentage in first half is 40% and bit error percentage in 2nd half is 55%then according to existing method average bit error percentage is 47.5% . Hence no need of inversion. But with our improved method, we invert second half and bit error percentage gets 42.5% without inverting the first half. Hence we get 42.5% average change which is better than existing method.

Case-4 if bit error percentage in first half is 35% and bit error percentage in 2nd half is 25% then according to existing method bit error percentage is 30%. Our improved method also no invert any part of stego image and bit error percentage is also 30%. So, in this case results are same as existing method.

So from above cases, case-1 and case-3 gives better result than existing method and case-2 and case-4 gives equal results with existing method. So, partitioning method is improved than bit inversion method.

10. After complete partitioning method calculate the improved PSNR value. PSNR is usually expressed in terms of logarithmic decibel scale. PSNR will use to measure the quality of the reconstructed image.

$$\mathbf{PSNR = 10\log_{10} (256\text{^}2)/MSE}$$

Where, MSE is mean square error.

III. RESULT AND ANALYSIS

In this work, results are analyses on 2nd and 3rd LSB and use cover.bmp and secret data.jpg shown in Figure 1. For analysis, five data images will use and one cover image will use. The results shown in Table-1, Table-2 and Table-3. Table -1 shows bit error percentage in first and second half before and after partition method. Table -2 shows average bit error percentage before and after partition method and Table-3 shows PSNR value before and after partition method.

TABLE 1: BIT ERROR PERCENTAGE IN FIRST AND SECOND HALF AFTER PARTITION METHOD

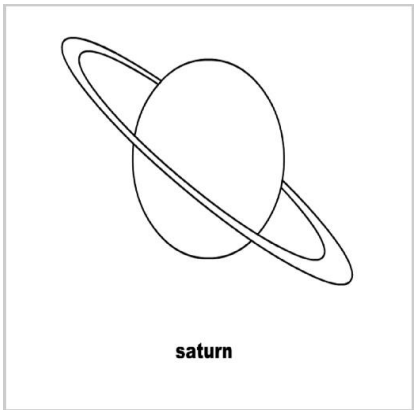
Secret data	Before partition method Bit error %age in first half	Before partition method Bit error %age in second half	Inverted half	After partition method Bit error %age in first half	After partition method Bit error %age in second half
Data 1	50.78	47.47	Ist Half	49.22	47.47
Data 2	53.25	45.83	Ist Half	46.75	45.83
Data 3	60.74	48.62	Ist Half	39.26	48.62
Data 4	56.46	47.45	Ist Half	43.54	47.45
Data 5	51.95	50.40	Ist Half	48.05	50.40

TABLE 2: AVERAGE BIT ERROR PERCENTAGE BEFORE AND AFTER PARTITION METHOD

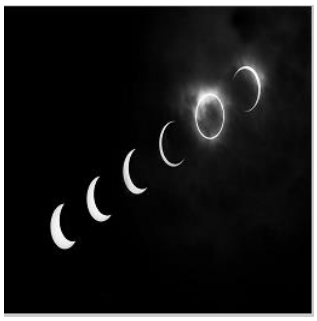
Average bit error %age before partition method	Average bit error %age after partition method
49.125	48.345
49.54	46.29
54.68	43.94
51.955	45.495
51.175	49.225

TABLE 3: PSNR VALUE BEFORE AND AFTER PARTITION METHOD

PSNR before partitioning method	PSNR after partitioning method
52.4253	53.3926
52.3726	53.3966
52.3704	53.4953
52.3682	53.4250
52.3660	53.3726

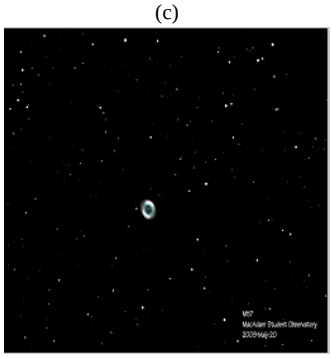


(a)



(b)

(c)



(d)

(e)

(f)

Fig.1: (a) Cover.bmp, (b) Data1.jpg, (c) Data2.jpg, (d) Data3.jpg, (e) Data4.jpg, (f) Data5.jpg

IV. CONCLUSION AND FUTURE SCOPE

From the results obtained in section 4, it is gathered that as the bit error percentage reduces after partitioning method as compare with before partitioning method. PSNR also increases after partitioning method as compare with before partitioning method. It means if PSNR increases quality of stego image also increases. The improvement in PSNR shall be very large with some other images. By partitioning method, image quality is improved very much. For future security and quality enhancement, other algorithms can be used rather than RC4 and by other techniques bit error percentage can more reduced and increased the PSNR.

V. REFRENCES

[1] Nadeem Akhtar, Pragati Johri and Shahbaaz Khan, "Enhancing the Security and Quality of LSB Based Image Steganography", Proceedings of IEEE International Conference of Computational Intelligence and Communication Networks, September 2013, pp.385-390.

[2] Shilpa Thakar and Monika Aggarwal, "A Review-Steganography", International Journal of Advanced Research in Computer Science and Software Engineering, December 2013, pp.528-532.

[3] Zaidoon Kh.Al-Ani, A.A Zaidan, B.B Zaidan and Hamdan.O.Alanazi, "Overview: Main Fundamentals for Steganography", Journal of Computing, vol.2, March 2010, pp.158-165.

[4] A.Cheddad, Joan Condell, K.Curran and P.McKevitt, "Digital Image Steganography:-Survey and Analysis of Current Methods", Signal Processing, vol. 90, 2010, pp. 727-752.

[5] Vipul Sharma and Sunny Kumar, "A New Approach to Hide Text in Images Using Steganography", International Journal of Advanced Research in Computer Science and Software Engineering, vol.3, April 2013, pp.701-708.

[6] Stuti Goel, Arun Rana and Manpreet kaur, "Comparison of Image Steganography Techniques", International Journal of Computers and Distributed Systems, vol.3, May 2013, pp. 20-30.

[7] Juned Ahmed Mazumder and K.Hemachandran, "Review of Different Techniques Used in Recent Steganography Researches", International Journal of Engineering Research and Technology, vol.1, October 2012, pp.1-9.

[8] Mrs. Kavitha, Kavita Kadam, Ashwini Koshti and Priya Dunghav, "Steganography Using Least Significant Bit Algorithm", International Journal of Engineering Research and Applications, vol.2, May-June 2012, pp.338-341.

[9] William Stallings, "The RC4 Stream Encryption Algorithm", Copyright 2005, pp.2-6.