Improved MSE Data Hiding Scheme

Shuchi Agarwal[1], Dr. Jaipal Singh Bisht[2]

[1]*Mtech Student of R.I.T.S. (Bhopal),*[2] *Guide and Director of R.I.T.S. (Bhopal)*

Abstract - In this paper, we propose a new method of data hiding using steganography in which we have made two major improvements one is of the lower values of MSE i.e. mean square error between stego image and cover image of around (10^(-3)) order i.e. 0.005 (calculated as an estimated average value) and second one is higher values of PSNR i.e. peak signal to noise ratio in comparison to other methods like LSB EMD , BEMD , signed digital data hiding scheme etc

Keywords: Data hiding, steganography, stego image, cover image, MSE, PSNR, EMD, pixel value

I. INTRODUCTION

The past few years have seen massive explosion in the field of digital media. One reason can be rapid growth of network and smart phone technology. The main feature in smart phone technology seems the pixel quality of camera inbuilt in smart phone. A lot of private information such as digital photos or videos communicates or circulates in this international network i.e. internet. Major concern is to secure the information that is transmitted globally all over the world via internet to prevent various kinds of attacks such as hacking of passwords , one's personal information etc.

Data hiding is one of the useful schemes for delivering secret messages. In this paper we review various steganographic techniques and propose our technique of data hiding. Steganography is the art and science of writing secret data in such a way that no one except the sender and intended recipient knows the existence of the data.

II. SYSTEM MODEL

The input messages can be in any digital form, we have taken in message i.e. in text form and converted it into a bit stream. Firstly the cover image is taken and then data which is converted to binary form is embedded into it to generate the stego image by following the steps of embedding algorithm. To embed message one stego key i.e. encryption key is used. After getting the stego image we have decoded the hidden message following decoding algorithm of our proposed scheme using decryption key which is same as encryption key. In this way whole procedure of encoding and decoding is performed.

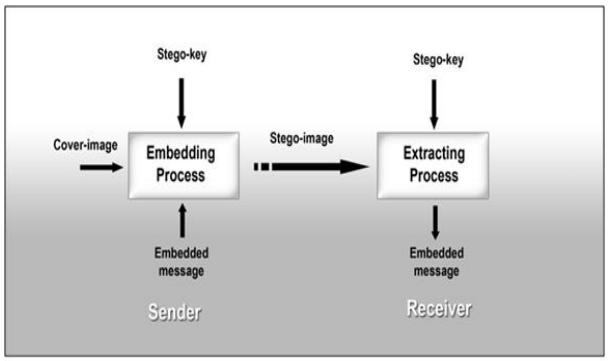

Fig 2.1: Block diagram of our scheme.

III. PREVIOUS WORK

LEAST SIGNIFICANT BIT SUBSTITUTION METHOD

Every pixel in an image indicates a colour and the each image is made up of pixels. The lower values of the pixel in a gray - scale image signifies dark areas and the higher values signify light areas. So in order to adjust the shades of the image its values can be adjusted and 8 bits are required to represent these values.

The procedures used in the LSB method are:

a) Get the input cover image and message image.

b) Resize the message image same as that of cover image.

c) Shift the message image pixel values over four bits to right.

d) Make last four bits (LSBs) in the pixel values of the cover image to zero.

e) Finally add the images obtained from step 3 and 4 to get final image.

Emd Method

To enhance embedding capacity, Zhang and Wang provided a new extraction function equation and a robust data hiding scheme based on EMD.

$$f_e(x_1, x_2, \ldots, x_n) = \left(\sum_{i=1}^{n} x_i * i\right) mod(2n+1)$$

Where x_i is the i^{th} pixel value and n is the number of pixels.

The EMD-scheme uses the relationship of n adjacent pixels to embed a 2n + 1 radix secret data stream. For example, the 5 radix secret data stream will be embedded in two adjacent pixels. In other words it only modifies one of two adjacent pixels by adding one, subtracting one, or no action.

Improved Emd Method

EMD scheme was further enhanced. In this, author proposed a new EMD scheme in which data can be embedded in each pixel of the cover image which enhances the embedding capacity further as compared with the previous technique. In this approach, secret data is converted into secret digits in (2n+1)-array notational system and each secret digit d are carried by one cover pixel. In this embedding method, embedding function is

$$f = p_i + x(mod\,(2n+1))$$

where p_i is the pixel value, where $|x| \leq n$, and a new pixel value p_i' is obtained.

$$p_i' = p_i + x$$

where x is selected to satisfy f=d condition.In the extracting method, the extraction function is

$$d = p_i'(mod\,(2n+1))$$

The value of secret digit d is obtained. And after obtaining all the secret digit sequence, they are converted back into binary sequence to obtain the secret message.

IV. PROPOSED METHODOLOGY

Previously, the proposed data hiding schemes are not giving such a lower mean square error. We have developed a new data hiding in which we achieve lowest mean square error as compared to other data hiding techniques i.e. minimum error between stego image and the cover image. We have made this improvement by taking directly the pixel value and further dividing number of pixels into N parts for implementing formula in MATLAB.

The Encoding Algorithm

We have followed the following steps to achieve the desired results, they are described as follows:-

$$\mathbf{mod\ 2\text{^}(n+1)}$$

Step 1: *Divide the cover image into 512*512 pixels. Divide these pixels into N parts and implement by using the following formula*

$$f_b(x_1, x_2, \ldots, x_n) = \left(\sum_{i=1}^{n} x_i * 2\text{^}(i-1)\right)$$

x_i: i^{th} pixel value.

n = (512*512) / N.

N is number of parts.

Step 2: Compute the value of t by using the following formula.

$$t = f_b(x_1, x_2, \ldots, x_n)$$

Step 3: Access (n+1) bits secret data from binary secret data stream M and transform to 2^ (n+1) – array data m.

Step 4: Compute the difference

$$D_b = (m - t) mod 2^{n+1}$$

Step 5: if D_b= 2^n then k = 1; else if $D_b < 2^n$ then k = 2; else k = 3.

Step 6: Switch (k)

Case 1: Let $y_n = x_n + 2$ and $y_i = x_i$ for all i = {1, 2, 3, . . . , n-1}.

Case 2 : Transform D_b to $(b_{n-1}, b_{n-2} \ldots b_1, b_0)_2$.For i = 1 to n,

$$y_i = x_i + b_{i-1}$$

Case 3: Let $D_b = 2^{n+1} - D_b$ and transform D_b to $(b_{n-1}, b_{n-2} \ldots b_1, b_0)_2$. For i=1 to n ,

$$y_i = x_i - b_{i-1}$$

The Decoding Algorithm

To decode the hidden message, following steps were followed by us:-

Step 1:-

Divide the stego image into non-overlapping n-pixel blocks.

Step 2:-

For each pixel group, compute $m = f_b(y_1, y_2, \ldots, y_n)$ and transform m to binary data.

Step 3:-

Combine all binary data to get the secret data stream M i.e. hidden message.

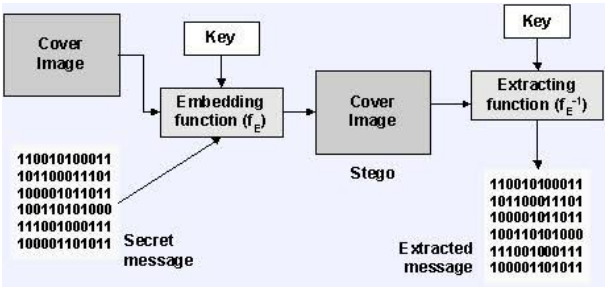

Fig 4.1: Block diagram of our scheme.

V. SIMULATION/EXPERIMENTAL RESULTS

The major concern in data hiding is undetectability by an unintended recipient. Two parameters for determining image quality are mean square error i.e. MSE and peak signal to noise ratio i.e. PSNR. They were calculated as follows:

$$MSE = \frac{1}{M * N}\sum_{i=1}^{M}\sum_{j=1}^{N}(x_{ij} - y_{ij})^2$$

where M and N represent length and width of cover image.

Table 1: Calculated value of MSE

x	San 2013 method	BEMD	MSD	EMD	Our scheme
2	0.68	0.75	0.4	0.4	0.00031
3	0.68	0.59	0.42	0.3	0.00044
4	0.68	0.55	0.4	0.2	0.00034
6	0.68	0.52	0.4	0.15	0.00037
8	0.68	0.52	0.4	0.12	0.00032
10	0.68	0.52	0.4	0.1	0.00044
12	0.68	0.52	0.4	0.1	0.00037
14	0.68	0.52	0.4	0.1	0.00041
16	0.68	0.52	0.4	0.1	0.00033
18	0.68	0.52	0.4	0.1	0.00057
20	0.68	0.52	0.4	0.1	0.00043

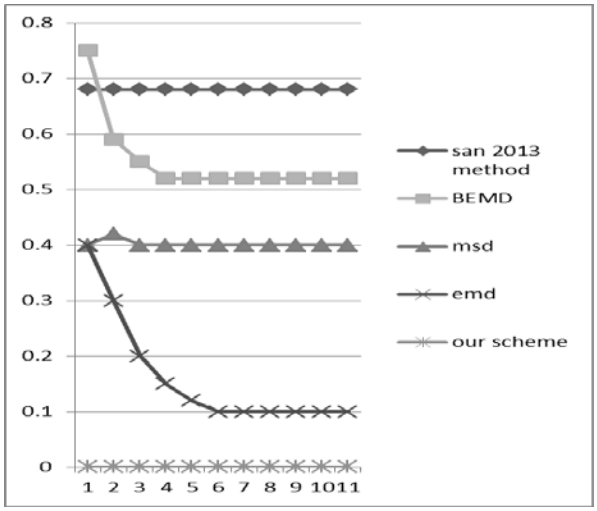

Fig 5.1: Comparison graph of MSE.

$$PSNR = 10 * \log_{10}\frac{255^2}{MSE}$$

Table 2: Calculated value of PSNR

x	san 2013 method	BEMD	MSD	EMD	our scheme
2	49.8	49.38	52.11	52.11	83.217
3	49.8	50.42	51.89	53.35	81.696
4	49.8	50.72	52.11	55.12	82.816
6	49.8	50.97	52.11	56.36	82.448
8	49.8	50.97	52.11	57.33	83.079
10	49.8	50.97	52.11	58.13	81.696
12	49.8	50.97	52.11	58.13	82.448
14	49.8	50.97	52.11	58.13	82.002
16	49.8	50.97	52.11	58.13	82.945
18	49.8	50.97	52.11	58.13	80.572
20	49.8	50.97	52.11	58.13	81.796

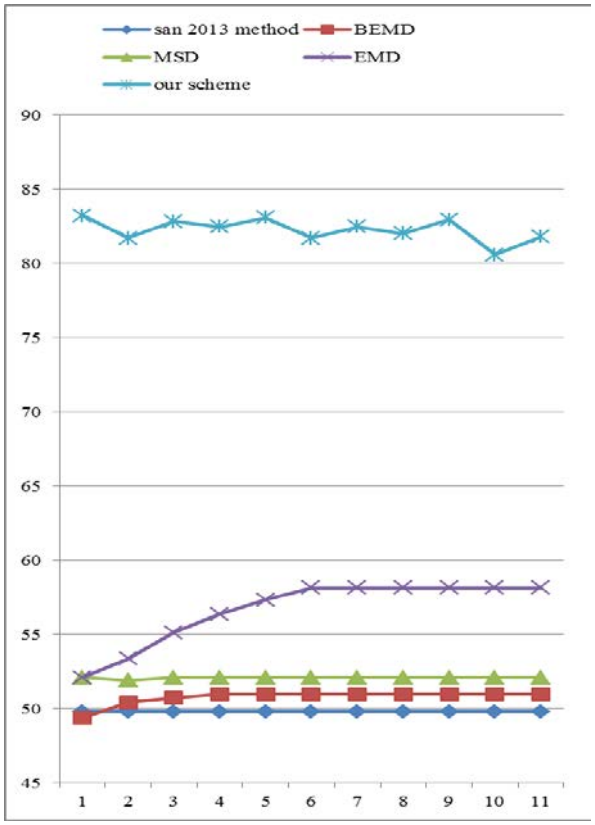

Fig 5.2: Comparison graph of PSNR.

VI. CONCLUSION

The main focus is on text steganography which is one of the most difficult types of steganography technique. Text steganography includes how secret image can be embedded and how it can be sent through the internet by fooling grabbers. Many problems are encountered when transferring important data over the network. A safe and

secure procedure is needed to transfer them easily. For this purpose simple image hiding techniques are used and the quality of stego images is also improved by using different mechanisms. So the hackers may not the stego image and will know nothing about the embedded secret image in it. In this proposed technique one of the major improvements is done. Firstly we have achieved very low values of mean square error which results in very good stego image quality. Therefore it is less likely to be attacked by hacker. Secondly, PSNR(peak signal to noise ratio) is around 82db. Which is very high compared to other techniques.

VII. FUTURE SCOPES

Data hiding has been an evergreen field since its inception in the late 1970‘s with the ever increasing need for security, speed and low cost as part of requirements of any transmission or reception system. Things need to be done at a very rapid rate without any compensation in loss of data or time. Data hiding has proved to be the ideal choice for such applications. It has grown in leaps and bounds with the advent of broadband and communication technologies which is capable of spanning the entire globe within a few minutes. It has played key roles in covert communication, image and video tagging, broadcast monitoring and copyright protection. With the ever existing introduction of new transforms which are improvements over their predecessors in some way or the other also could contribute to the growth of data hiding in an attempt to further bring about the optimality. Directionality features of new transforms like the Curvelet transforms, Slantlet transforms could also be possibly investigated for its exploitation. As far as data hiding is concerned, there cannot be a point of saturation with the ever increasing threats and new hacking techniques in real world. With the advent of tele services, data hiding could cut costs and distance and travel miles and miles within a few minutes. It could also be an important tool in forensics for tracking criminal records and immediate identification of suspects. It could drastically reduce the effort of INTERPOL (International Police) and could bring about a better coordination globally. With the fast booming integrated circuit (IC) technology, data hiding concepts have been exposed to field programmable gate arrays (FPGA) using wavelet transforms, lifting based wavelet transforms. It could greatly aid in real time applications with reduction in space, cost and time. This technology could be a great boon in preventing fake passports and forged identity cards especially in airline industries.

REFERENCES

[1] Wen-Chung Kuo, Chun-Cheng Wang, Yu-Chih Huang, “Binary power data hiding scheme”, Elsevier, 1434-8411, 2015.

[2] Kim et al, Chandreyee Maiti, Debanjana Bakshi, Ipshita Zaminder, Pinky Gorai and Dakshina Ranjan Kisku, “Data hiding in images using some efficient steganography techniques”, Springer-Verlag Berlin Heidelberg 2011, SIP 2011, CCIS 260 pp, 195-203, 2011.

[3] Stuti Goel, Arun Rana and Manpreet Kaur, “A review of comparison techniques of image steganography”, Global journal of computer science and technology, volume 13 issue 4 version 1.0, ISSN: 0975 – 4172, 2013

[4] Mamta Kalra, Parvinder Singh, “EMD techniques of image steganography”, International journal of technological exploration and learning, IJTEL, ISSN:2319-2135, VOL. 3, NO. 2, 2014.

[5] Kuo WC, “Image hiding by square fully exploiting modification directions”, Journal of information hiding and multimedia signal processing, ISSN 2073-4212, volume 4, number 3, July 2013.

[6] B.Subramanan “Image encryption based on key expansion” in IEEE applied second international conference on emerging application of information technology,978-0-7695-4329-1/11,2011.

[7] R.Rathna Krupa, “An overview of image hiding techniques in image processing”ISSN:2321-2381@2014 Published by the standard international journals(The SIJ).

[8] Vipul Sharma and Sunny Kumar, “A new approach to hide text in images using steganography”ISSN:2277 128X,IJARCSSE, 2013

[9] Lee, C. F., Chang, C. C. and Wang, K. H. An improvement of EMD embedding method for large payloads by pixel segmentation strategy. Image Vis. Comput., 26, 1670–1676, 2008.

[10] Kieu TD, Chang CC. A steganographic scheme by fully exploiting mod-ification directions. Expert Systems with Applications;38(8):10648–57, 2011.

[11] http://en.wikipedia.org/wiki/Binary multiplier.