Efficient BEMD Data Hiding Algorithm

Shuchi Agarwal
Mtech Student
R.I.T.S
Ratibad, Bhopal (M.P.) India

Jaipal Singh Bisht, PhD
Director
R.I.T.S
Ratibad, Bhopal (M.P.) India

ABSTRACT

Improved BEMD steganographic algorithm to hide secret text behind cover pixels of image to increase security of digital communication for exchanging private information worldwide using binary coefficient and modulus is proposed. From simulation results, Stego image quality better than 70dB which is higher than BEMD Kuo-Chang scheme thereby reducing mean square error difference between cover image and stego image.

General Terms

History of steganography, Review of steganographic techniques, Experimentation, Proposed algorithm, Results, conclusion, literature review.

Keywords

Data hiding, steganography, stego image, cover image, MSE PSNR, EMD, BEMD, pixel value.

1. INTRODUCTION

Internet came into existence in 1960s and in near decade security of data has become a major concern. Internet has become more popular in era of digital communication all over the world to exchange private and personal information. Data hiding techniques provide a solution to problem of illegal hindrance or interception of data during communication between sender and receiver. Data hiding is the technique of secretly embedding information inside a data source without changing its original integrity. Image steganography is one of the popular techniques of data hiding in such a way that no one except the sender and the intended recipient knows the existence of data in cover medium. Least significant bit replacement (LSB) technique is most common technique in spatial domain due to simplicity in implementation but not secure against the bit plane attack. In 2006 Zhang and Wang proposed data hiding method based on Exploiting modification direction to improve embedding capacity and data security.

To increase stego image quality in terms of high value of PSNR binary exploiting modification direction method is proposed. Data embedding is done using binary coefficient and modulus of radix 2. One major improvement in binary data hiding method proposed by [1] Yu-Chih Huang in 2015 is total number of pixels in cover image is divided into n number of pixels in encoding algorithm to increase the encryption time and image quality. The experimental results show that PSNR is increased to a significant value thereby increases the quality of embedded image. Histogram of stego image is almost similar to that of cover image which shows very little distortion in original image.

2. HISTORY OF STEGANOGAPHY

In 5th century before the advent of computers and electronic media communication can either be done by memorizing the message or hiding it on messenger. Around 440 B.C. greek ruler Histaeus uses the technique to shave the head of one of his most trusted slave and tattoo a message or image on the messenger's head. After allowing his hair growth message is protected until his head is shaved as no one knows that there is message hidden except the sender and receiver. Receiver reads the message by shaving messenger's head and uses the same technique on another slave to send message to sender. Early in World War II another common form of invisible writing is developed by use of invisible inks like milk, vinegar, fruit juices and urine. Message is written with the help of these invisible inks and darkens when heated. In the same time period, another early form of steganography was employed. This method involved Demerstus, who wrote a message to the Spartans warning of eminent invasions from Xerxes. The message was carved on the wood of wax tablet, and then covered with a fresh layer of wax. This seemingly blank tablet was delivered with its hidden message successfully. Germans developed microdot technology Microdots are photographs the size of a printed period having the clarity of standard-sized typewritten pages. The first microdots were discovered masquerading as a period on a typed envelope carried by a German agent in 1941. The message was not hidden, nor encrypted. It was just so small as to not draw attention to itself (for a while). The information on the microdot can be read by the intended recipient using a microscope.

3. REVIEW OF STEGANOGRAPHIC TECHNIQUES

Many EMD-type data hiding schemes have been previously proposed. In this section brief review of these schemes were considered.

3.1 Original EMD data-hiding scheme

Steganographic scheme of exploitation modification direction (EMD) method [2] was first discovered by Zhang & Wang in 2006 uses adjacent pixels of cover image to hide secret message. The data embedding function for n pixels of cover image is defined by weighted modulo (2n+1) using equation 3.1.

$$f(g_1, g_2, \ldots, g_n) = (g_1 * 1 + g_2 * 2 + \ldots + g_n * n) mod(2n+1)$$

where, $g_{1,} g_2, \ldots g_n$ corresponds to pixels of cover image and n is the total number of pixels in cover image.

Encoding procedure is discussed as follows:

1. From the pixel values of cover image using above equation to calculate $f_c = f(g_1, g_2, \ldots, g_n)$.
2. Convert secret data into binary form using ASCII values of characters and convert into (2n + 1)-ary system to calculate value of m.
3. Compute the difference ,

$$d = (m - f_c) mod(2n+1).$$

4. If d > n, then $g_{(2n+1)-d} = g_{(2n+1)-d} - 1$; else $g_d = g_d + 1$. Hence stego pixel block is computed.

Decoding algorithm for EMD:

1. Stego pixel block $(g_1, g_2, \ldots, g_n)$ is obtained.
2. Compute $m = f(g_1, g_2, \ldots, g_n)$ using weighted modulo equation 3.1.
3. Convert decimal value of m to binary calculate data stream.

3.2 GEMD data hiding scheme

Generalized exploiting modification direction method (GEMD) proposed by Wang and Kuo [3] introduces a new extraction function [12] mentioned in equation 3.2 using binary coefficient for modulo-2 division to (n+1)-bits of binary secret data into *n* adjacent pixels of cover pixel block.

$$f_b(g_1, g_2, \ldots, g_n) = \left[\sum_{i=1}^{n} g_i * \left(2^i - 1\right)\right] mod2^{(n+1)}$$

Where g_i is i^{th} pixels value of cover image.

Embedding algorithm for GEMD scheme

1. Compute the value of t using extraction function by equation (3.2) $t = f_b(g_1, g_2, \ldots, g_n)$.
2. Convert the binary secret data stream $(s_n, s_{n-1}, \ldots., s_1, s_0)$ to decimal value s using binary to decimal conversion.
3. Calculate the difference D between s and t using $D = (s - t)mod2^{n+1}$.
4. Compare D and 2^n,
   - 4.1. If $D = 2^n$, then $g_n^{'} = g_n + 1$
   - 4.2. Else if, $D < 2^n$ then transform D to binary bits $(d_n, d_{n-1}, \ldots, d_1, d_0)_2$ and For i = n, n-1, …, 2,1
     If ($d_i = 0$ & d_{i-1} = 0) or (bi = 1 &b_{i-1} = 1) then $g_i^{'} = g_i$.
     Else If ($d_i = 0$ & d_{i-1} = 1) then $g_i^{'} = g_i + 1$.
     Else ($d_i = 1$ & d_{i-1} = 0) then $g_i^{'} = g_i - 1$.
   - 4.3. Else transform D to binary bits $(d_n, d_{n-1}, \ldots, d_1, d_0)_2$ and For i=n to 1 ,
     If ($d_i = 0$ & d_{i-1} = 0) or (bi = 1 &b_{i-1} = 1) then $g_i^{'} = g_i$.
     Else If ($d_i = 0$ & d_{i-1} = 1) then $g_i^{'} = g_i - 1$.
     Else ($d_i = 1$ & d_{i-1} = 0) then $g_i^{'} = g_i + 1$.

4. PROPOSED BEMD ALGORITHM

One major modification in proposed technique is that total number of pixels of cover image is divided [14] into n parts to improve the stego image quality and to decrease the embedding time than that of Wang and Kuo data hiding technique [1].

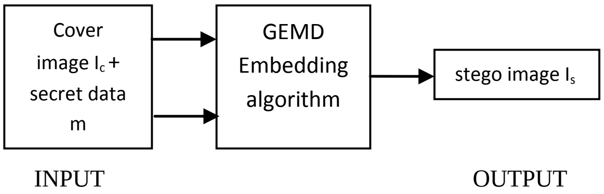


Fig 1: Input cover image and data to get output stego image using GEMD algorithm

4.1 BEMD Embedding Steps

4.1.1 Step 1: From the cover image 512*512 pixels. Divide these pixels into n parts and implement using modulo binary extraction function where coefficient of multiplication with pixel values and modulus are binary.

$$f_b(x_1, x_2, \ldots, x_n) = \left(\sum_{i=1}^{n} x_i * 2{}^\wedge(i-1)\right) mod2^{(n+1)}$$

x_i: i^{th} pixel value.

n = (512*512) / N.

n is number of parts.

4.1.2 Step 2: Compute the value of t by using extraction function equation.

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

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

4.1.4 Step 4: Compute the difference D_b between m and t using following equation.

$$D_b = (m - t)mod2^{n+1}$$

4.1.5 Step 5: Compare the value of D_b and 2^n.If $D_b = 2^n$ then k = 1; else if $D_b < 2^n$ then k = 2; else k = 3.

4.1.6 Step 6: Switch (k)

4.2 Decoding algorithm

4.2.1 Decoding is simply *done by following steps:*

4.2.2 Step 1: Obtain pixel values $(y_1, y_2, \ldots, y_n)$ for each stego pixel block in I_s.

4.2.3 Step 2: Compute the value of m using equation

$$m = f(y_1, y_2, \ldots, y_n) = \left[\sum_{i=1}^{n} g_i * \left(2^i - 1\right)\right] mod2^{(n+1)}$$

4.2.4 Step 3: With the help of decimal to binary conversion, convert the decimal value of m to get binary data stream.

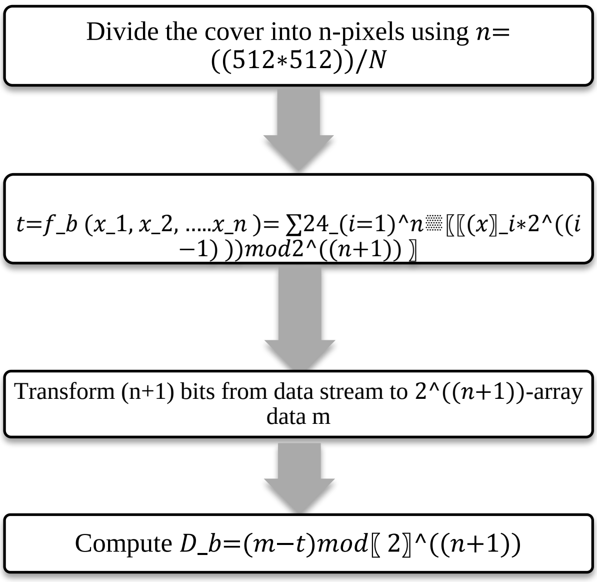

Divide the cover into n-pixels using 𝑛=((512∗512))/𝑁
𝑡=𝑓_𝑏 (𝑥_1, 𝑥_2, ...𝑥_𝑛)= ∑24_(𝑖=1)^𝑛▒〖〖(𝑥〗_𝑖∗2^((𝑖−1)))𝑚𝑜𝑑2^((𝑛+1)) 〗
Transform (n+1) bits from data stream to 2^((𝑛+1))-array data m
Compute 𝐷_𝑏=(𝑚−𝑡)𝑚𝑜𝑑〖 2〗^((𝑛+1))

Fig 2: Flowchart to compute the value of D_b in encoding algorithm.

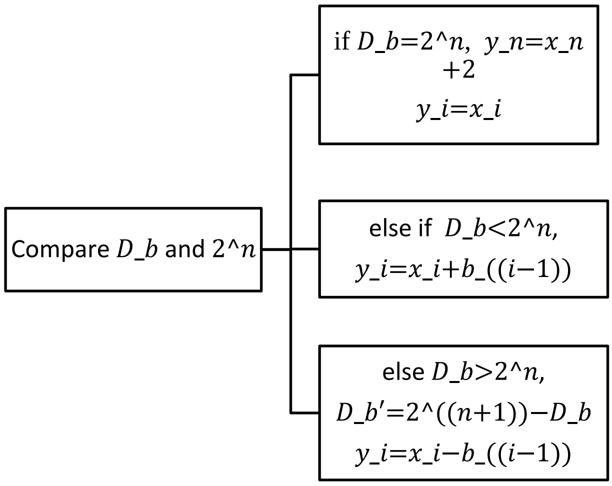


Fig 3: Computation of stego pixel block.

Example
Take the cover pixel block (58, 62, 86, 99) and hide the data stream $(11011)_2$ and n = 4.

Encoding:

$$t = \sum_{i=1}^{4} \left(x_i * 2^{(i-1)}\right) mod 2^{(n+1)}$$

$$t \;= (58 * 2^0 + 62 * 2^1 + 86 * 2^2 + 99 * 2^3) mod 2^5$$

$$t \;= (1318) \text{ mod32}$$

$$t \;= \;6$$

$$m = \;(11011)_2 = 27$$

$$D_b = \;(m - t) mod\; 2^5 = (27 \;- 6) mod 32 = 21$$

$$D_b = 21 > \;2^4$$

If, $D_b < \;2^n$

$$k = 3$$

Case 3:-

$$D_b^{'} = 2^{(n+1)} - D_b = \;2^5 - 21 = 11$$

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

Transform $D_b{}'$ to $\left(b_4 b_2\; b_1\; b_0\;\right)_2 = (1011)_2$

$$y_i = \;x_i - \;b_{(i-1)}$$

$$y_1 = 58 - 1 = 57$$

$$y_2 = 62 - 1 = 61$$

$$y_3 = 86 - 0 = 86$$

$$y_4 = 99 - 1 = 98$$

Therefore the stego pixel block is (57, 61, 86, 98).

Decoding:

$$m = \;f_b(y_1,\; y_2,\; \ldots..y_n) = \;\sum_{i=1}^{n} \left(y_i * 2^{(i-1)}\right)\; mod\; 2^{(n+1)}$$

$$m = \;f_b(57, 61, 86, 98)$$

$$m = (57 * 2^0 + 61 * 2^1 + 86 * 2^2 + 98 * 2^3\;) mod 2^5$$

$$m = (1307) mod 32$$

$$m = 27$$

Transform m to (n+1) bits i.e. 5-bits binary data.

$$m = 27 = \;(11011)_2$$

Therefore hidden secret data stream $(11011)_2$ is extracted.

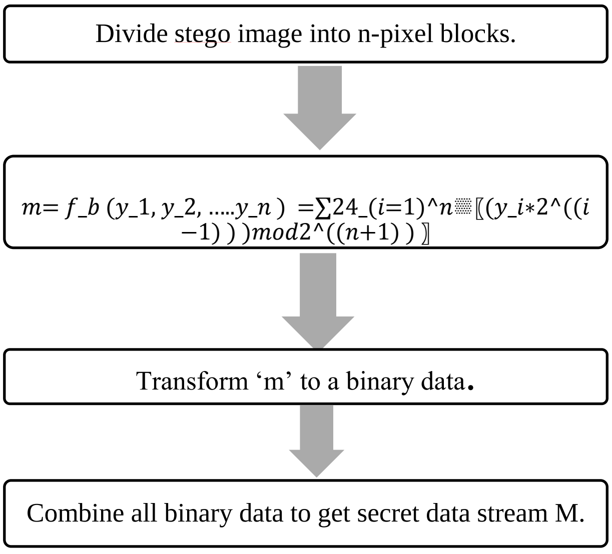

Divide stego image into n-pixel blocks.
𝑚= 𝑓_𝑏 (𝑦_1, 𝑦_2, ...𝑦_𝑛) =∑24_(𝑖=1)^𝑛▒〖(𝑦_𝑖∗2^((𝑖−1)))𝑚𝑜𝑑2^((𝑛+1)) 〗
Transform ‘m’ to a binary data.
Combine all binary data to get secret data stream M.

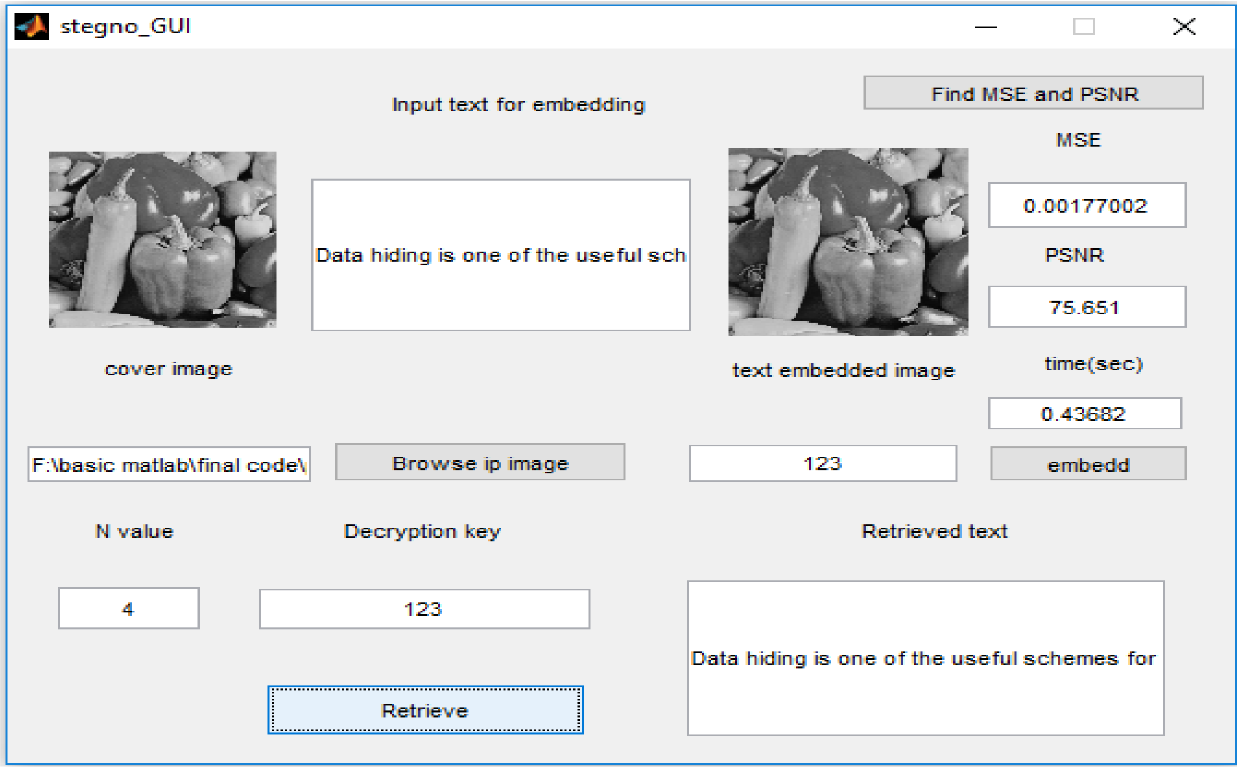
Fig 4: Decoding algorithm flowchart.

GUI window of MATLAB as shown in Fig 5 is created after creating m file in editor window in which whole coding is written step by step. Following steps were followed:

1. First of all browse the input grayscale image of *jpg format by clicking browse push button. The image will get appeared in the axes box.
2. Enter the value of N i.e. number of pixels in each stego pixel block.

3. Enter the text in the edit box titled "Input text for embedding" and click on embed push button.
4. After a click on embed button stego image will appear in "text embedded image" axes.
5. To calculate the values of PSNR and MSE click the push button "Find MSE and PSNR". Values get displayed in MSE and PSNR in decibels in their edit boxes.
6. To retrieve the data, enter the decryption key same as encryption key and click on "Retrieve" push button.
7. The hidden data behind the image will get decoded and appear in edit text box titled "Retrieved text".

Fig 5: Standard 512*512 jpg Cover image



Input text for embedding: Data hiding is one of the useful sch

MSE: 0.00177002

PSNR: 75.651

time(sec): 0.43682

F:\basic matlab\final code\

123

N value: 4

Decryption key: 123

Retrieved text: Data hiding is one of the useful schemes for

Fig 6: GUI window for proposed BEMD steganographic technique of data hiding

5. PERFORMANCE ANALYSIS

From the simulation results implemented [12] in MATLAB (R20011a) software on a personal computer with Intel Core I3 2.50 GHz, 4GB RAM performance of proposed BEMD scheme is evaluated. 512*512 grayscale images were taken for experimental analysis using PSNR and MSE as discussed below. Mean Square error (MSE) is calculated using:

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

where M and N represent length and width of cover image respectively. x_{ij} and y_{ij} are the pixel values of i^{th} row and j^{th} column of cover and stego image respectively.

Peak Siganl to noise ratio (PSNR) can be either calculated directly in MATLAB using inbuilt function or by using MSE.

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

Maximum pixel intensity of grayscale image is 255, hence n formula square of 255 is used.

PSNR value is inversely proportional to the amount of embedded information in image i.e. payload. The quality of stego image degrades for more information.

Table 1. Comparison Table of PSNR

x	san 2013 method	BEMD	MSD	EMD	our scheme
2	49.8	49.38	52.11	52.11	71.9893
3	49.8	50.42	51.89	53.35	72.0132
4	49.8	50.72	52.11	55.12	72.1464
6	49.8	50.97	52.11	56.36	72.5425
8	49.8	50.97	52.11	57.33	73.7068
10	49.8	50.97	52.11	58.13	74.3159

12	49.8	50.97	52.11	58.13	75.1562
14	49.8	50.97	52.11	58.13	75.9313
16	49.8	50.97	52.11	58.13	76.8631
18	49.8	50.97	52.11	58.13	77.4062
20	49.8	50.97	52.11	58.13	77.7223

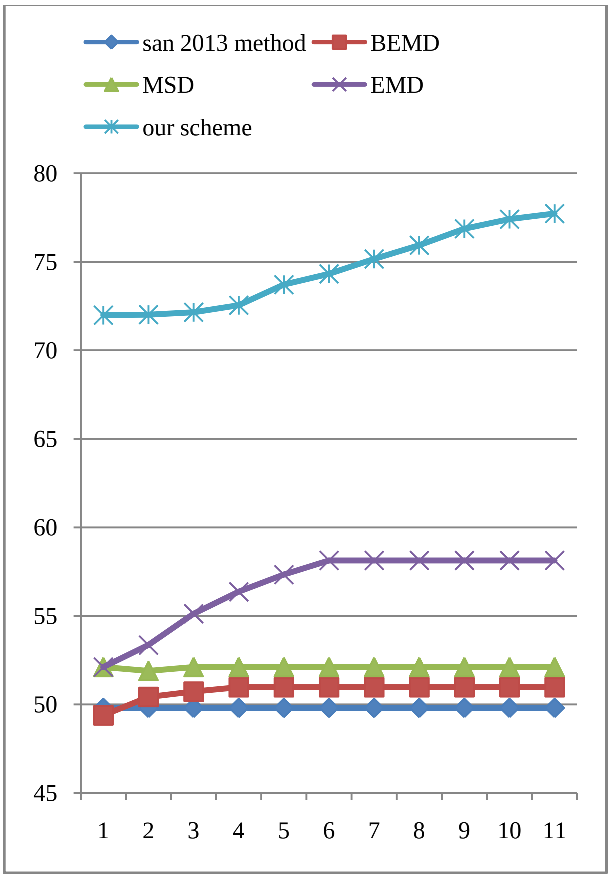


Fig 7: Comparison graph of PSNR

Table 2. Comparison Table of MSE

-x	san 2013	BEMD	msd	emd	our scheme
2	0.68	0.75	0.4	0.4	0.0042
3	0.68	0.59	0.42	0.3	0.00317
4	0.68	0.55	0.4	0.2	0.00315
6	0.68	0.52	0.4	0.15	0.0028
8	0.68	0.52	0.4	0.12	0.0027
10	0.68	0.52	0.4	0.1	0.0024
12	0.68	0.52	0.4	0.1	0.0019
14	0.68	0.52	0.4	0.1	0.0013
16	0.68	0.52	0.4	0.1	0.0014
18	0.68	0.52	0.4	0.1	0.0018
20	0.68	0.52	0.4	0.1	0.0019

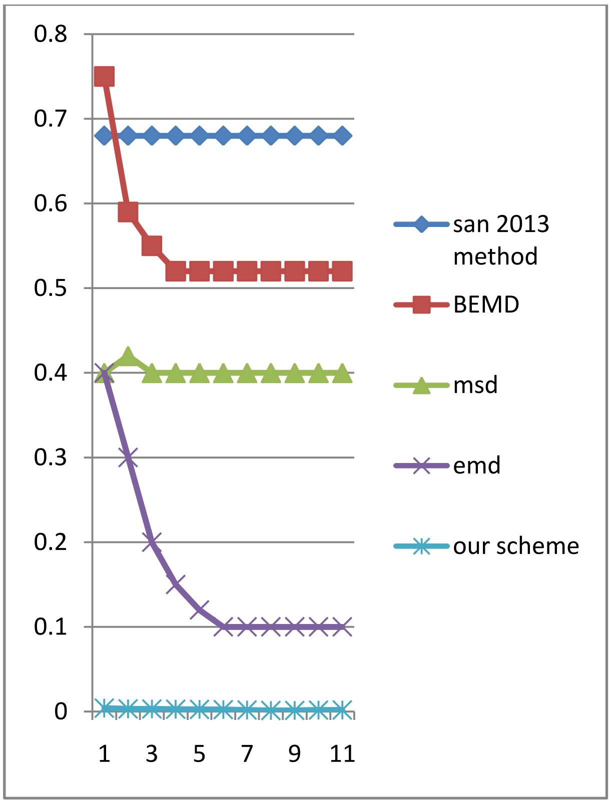


Fig 8: Comparison graph of PSNR

6. CONCLUSION

In proposed method of improved BEMD data hiding scheme significant improvement is made in stego image quality with PSNR greater than 70dB which increases robustness and security of digital communication. Graphical comparative analysis of various data hiding techniques shows best results obtained by proposed BEMD technique. Therefore PSNR is increased by 40 percent in comparison with BEMD method by Kuo-Chang method [1] and thus satisfy all the three requirements i.e. robustness, invisibility and capacity of good steganography [18]. One more significant improvement is value of mean square error of around 0.003dB which is achieved to be very less in comparison with other data hiding schemes as the value of MSE varies in inverse proportion with PSNR value.

Future scope of data hiding includes prevention of fake passports by embedding individual's information behind the image for secure communication. Data hiding can help in real time applications with reduction in space, cost and time. Steganography can provide better security in various networks like LAN, MAN and WAN for digital communication. Digital cashless transactions [5] can be done with similar data hiding techniques for securing passwords and account details from an unauthorized access.

7. ACKNOWLEDGMENTS

Sincere thanks to electronics and communication department of Radharaman institute of technology and science, Bhopal. Express deep sense of gratitude to my guide Dr. Jaipal Singh Bisht (Director, R.I.T.S Bhopal) for his valuable guidance and suggestion for publishing my research paper in IJCA journal which has reached to such a high volume.

8. REFERENCES

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

[2] Xinpeng Zhang and Shuozhong Wang, 2006, "Efficient steganographic embedding by Exploiting modification Direction", IEEE Communication Letters.

[3] W-C Kuo, C-C Wang, "Data hiding based on generalized exploiting modification direction method", Imaging Science Journal, 2013.

[4] Ratnakirti Roy, Suvamoy Changder, Anirban Sarkar, Narayan C Debnath, "Evaluating Image Steganography Techniques: Future Research Challenges", IEEE, 2013.

[5] Fabien A.P. Petit colas, Ross J. Anderson, Markus G. Kuhn, "Information hiding-A survey", Proceedings of the IEEE, July 1999, 0018-9219.

[6] Wen-Chung Kuo, Sheng-Yi Chang, "Hybrid GEMD data hiding", Journal of information hiding and multimedia signal processing, July 2014, 2073-4212.

[7] Min WU, Heather Yu, Bede Liu, "Data hiding in image and video: Design and Applications", IEEE transactions on image processing, June 2003, 1057-7149.

[8] R.J.Anderson, "Information Hiding: 1st International workshop (Lecture notes in computer science), Springer-Verlag, 1996, 1174.

[9] Vipul J Patel, Ms. Neha Ripal Soni, "Uncompressed Image Steganography using BPCS: Survey and Analysis", IOSR Journal of Computer Engineering (IOSR-JCE), Dec 2013.

[10] A. Westfeld, "F5-A Steganographic Algorithm: High capacity despite better steganalysis", Proc. 4th International Workshop on Information Hiding., 2001, Springer, 2001, 289-302.

[11] Huang, Y. M. and Jhan, P. W., "Two improved data hiding schemes", Proc. 4th Int. Cong. on Image and signal processing: CISP 2011, Shanghai, China, October 2011, IEEE, pp. 1784–1787.

[12] Wen-Chung Kuo, Lih-Chyau ,Wuu Chia-Nian Shyi Shao-Hung Kuo, "A Data Hiding Scheme with High Embedding Capacity Based on General Improving Exploiting Modification Direction method", Ninth International Conference on Hybrid Intelligent Systems, 2009, IEEE, 978-0-7695-3745.

[13] F. Cayre, C. Fontaine, T. Furon, "Watermarking Security Theory and Practice," IEEE Trans. on Signal Processing, 2005, Vol.53, pp.3976- 3987.

[14] M.D. Swanson, B. Zhu and A.H.Tewfik, "Robust Data hiding for Images", IEEE Digital Signal Processing Workshop, September 1996.

[15] H. C. Wu, N. I. Wu, C. S. Tsai, and M. S. Hwang, "Image Steganographic Scheme Based on Pixel-Value Differencing and LSB Replacement Methods", IEEE Proceedings-Vision, Image and Signal Processing, Vol.152, No. 5, pp.611-615, October 2005.

[16] Y.-C. Tseng, Y.-Y. Chen, and H.-K. Pan, "A secure data hiding scheme for binary images," IEEE Transaction Communication, Vol. 50, pp. 1227-1231, August 2002.

[17] W. Zhang, X. Zhang, S. Wang, "A Double Layered ''Plus–Minus One data embedding scheme", IEEE Signal Processing Letters, 2007, 848–851.

[18] N. Provos and P. Honeyman, "Hide and Seek: An Introduction to Steganography", IEEE Security and Privacy Magazine, 2003.

[19] A. Cheddad, J. Condell, K. Curran and P.M. Kevitt, "Digital Image Steganography: Survey and Analysis of Current Methods", Signal Processing, 90(3), 727-752, 2010.