IMPLEMENTATION OF EXPLOITING MODIFICATION DIRECTION (EMD) - A STEGANOGRAPHY TECHNIQUE USING RASPBERRY PI

[1]Sourabh Joshi, [2]Prof. S.I. Nipanikar
[1] PG Scholar, E&TC Engineering, PVPIT Pune, Savitribai Phule Pune University, Pune, India.
[2] Asst. Prof E&TC Engineering ,PVPIT Pune, Savitribai Phule Pune University , Pune ,India.
Email:[1] sourabhjoshi1990@gmail.com , [2] sanjaynipanikar@rediffmail.com

***Abstract* – Exploiting Modification Direction (EMD) is a spatial domain image steganography technique to conceal secret data into digital images. In this paper, basic EMD method is explained and also two level method is explained. From results it can be seen that two level EMD is having twice the embedding rate than basic EMD by compromising stego image quality. It can also be seen that two level EMD provides more security than basic EMD. Later raspberry pi –a general purpose hardware module is used to implement extraction algorithm of two level EMD.**

***Index Terms* - Exploiting Modification Direction (EMD), Steganography, Stego image**

I. INTRODUCTION

Now a day, internet is the key part of human's day to day life. Since for various kinds of transactions internet is a key element day by day its usage is increasing. Generally, with the help of internet, we can send various kinds of digital messages or information. Although internet provides ease of communication and low cost way there are many kinds of dangers hidden behind its advantages. For ex. secret information can be leaked, changed or being used on any unauthorized cases by hackers during data communication from transmitter to receiver. Thus, there is a necessity to avoid all the kind of unknown third party interference with the system. For this reason, a method is developed known as data hiding. Basically, it deals with hiding of secret message inside the cover image so that no one has any idea about hidden secret message. Such image is called as stego image. Later this stego image is successfully transmitted to its desired recipients where secret data is taken out from the stego image. This method is known as steganography.

Up till now, different data hiding methods were proposed and generally maximum data hiding methods are using LSB (least significant bites) position to conceal the confidential data. Means first confidential information is converted into binary format then it is replaced by least bit. [1, 2, 3]

EMD is a steganographic embedding method [5] used for digital images in which n cover pixels carries each secret digit in (2n+1) ary notational system. Here, only one cover pixel is either increased or decreased by 1 or remain same. In general, there are 2n possible ways of alteration for each group of n cover pixel. These 2n ways of modification and one case in which no pixel is changed form (2n + 1) different values of a secret digit. Since the direction of modification of cover pixel is fully exploited here thus this method is called EMD which achieves high embedding efficiency as compared to other techniques.

Low embedding rate is one of the disadvantages of basic EMD. So it is possible to overcome it with the use of two level EMD [6] in which each pixel group can successfully carries two secret digits. To implement this two level embedding strategy is used. For first level embedding ,first secret digit is embedded into

pixel group by using embedding function 'f1' and for second level embedding second secret digit is embedded into same pixel group by using embedding function 'f2'.Then at the receiving end, by using same embedding functions 'f1' and 'f2',secret message is retrieved from the stego image.

Raspberry pi [4] a general purpose hardware module is used on which decryption algorithm of two level EMD is running to retrieve the hidden data from the stego image which is transmitted from the system on which encryption algorithm is running to hide the secret data within an image.

This paper is arranged as follows: In section II, required literature is given. In section III, proposed system is explained. In section IV, analysis factors for EMD method are given. In section V, test results are given in the table form. In section VI, screenshots of test results are produced. In section VII, overall paper is concluded. In section VIII, acknowledgement for entire work is given. In section XI, references are given.

II. LITRETURE REVIEW STAGE

A deep and profound literature survey is backbone of any successful project. Extensively search has been carried out for past and related work in this field. Internet tool is used as source of information for carrying out this literature survey.

(1) "Steganalysis of LSB Matching in Grayscale Images",by A. Ker IEEE Signal processing Letters, Vol.12, No.6, pp.441- 444, June 2005.
This paper gives the two new methods for detecting steganography in spatial domain.
(2)"Image Hiding by Optimal LSB Substitution and Genetic Algorithm," by R. Z. Wang, C. F. Lin, and J. C. Lin, Pattern Recognition, Vol. 34, No. 3, pp. 671-683, 2001.
This paper gives the new LSB method to embed secret data into cover image in such a way that interceptors will not feel about the existence of the data.
(3)"A Steganographic Method Based on Pixel-Value Differencing and the Perfect Square number", by Hsien-Wen Tseng and Hui-Shih Leng, Hindawi Publishing Corporation Journal of Applied Mathematics, Volume 2013, Article ID 189706
The LSB method used in this paper gives better image quality and higher capacity.
(4)"A Review Paper on Raspberry Pi", by Pritish Sachdeva and Shrutik Katchii International Journal of Current Engineering and Technology E-ISSN 2277 4106, P-ISSN 2347 - 5161 ©2014 INPRESSC
This paper gives the basic information about raspberry pi along with its features and specifications.
(5) "Efficient Steganographic Embedding by Exploiting Modification Direction", by X. Zhang and S. Wang, IEEE Comm. Letters, Vol.10, No.11, pp. 1-3, November 2006
This paper describes that basic EMD is having embedding efficiency and embedding rate more than run length encoding and matrix encoding also Stego image quality is good here.

But it is having som disadvantages like it is less efficient, Safety issues are there, message needs to be converted into another format hence more time is required for embedding. Also embedding capacity is limited.

(6) "A Large Payload Information Hiding Scheme Using Two Level Exploiting Modification Direction", by C.Chang, H.Wu, Tenth International Conference On Intelligent Information Hiding And Multimedia Signal Processing IEEE-2014.
From this paper it can be observed that embedding rate of this method is twice that of basic EMD also it is more efficient than basic EMD.

But it is having disadvantages like poor stego image quality and doubled processing time than basic EMD.

III. PROPOSED SYSTEM

By considering drawbacks & strength of literature survey the proposed system is as

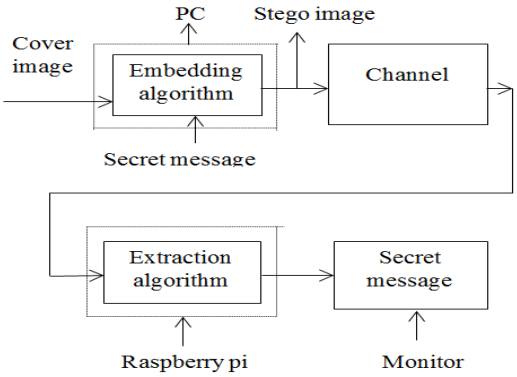

Fig 1: "Block Diagram of Implementation of system for EMD"

Here, encryption algorithm is running on PC can be called as transmitter. The output of this transmitter is stego image which contains hidden data. This stego image is transmitted over internet towards desired receiver. At receiving side, raspberry pi is used on which extraction algorithm is running with which it is possible to find the hidden data within an image. Finally the secret data is displayed on the display connected to raspberry pi.

Raspberry pi is a credit card sized computer manufactured and designed in the united kingdom by raspberry pi foundation with the intention of teaching basic computer science to school students and every other person interested in computer hardware, programing and do it yourself projects.

Raspberry pi is manufactured in three board configurations they are model A, model B, and model B+. Recently in February 2015, a newer raspberry pi model 2 B is launched which is having advanced features than that of previous models.

A) Basic EMD method:-

The basic EMD method [5] was proposed by Zhang and Wang which is having highest embedding efficiency and embedding rate than matrix encoding and run length encoding. In this method, binary confidential data is converted into secret digit (d) in (2n+1) ary notational system in such a way that one secret digit is carried by n pixels. Thus, secret message is first converted into secret digits in (2n+1)-ary notational system and then each secret digit are embedded into pixel group (g_1, g_2… g_n). To embed secret digit (d) into pixel group, value of extraction function f_e is calculated by using equation (1)

$fe\ (g_1,g_2,\ldots g_n) = (g_1*1+g_2*2+\ldots+g_n*n) \bmod (2n+1)$……(1)

If $f_e \neq d$, then only one of the pixels from the pixel group has to be incremented or decremented by one. If $f_e = d$, then there is no need to change any pixel and the process continues until no secret digit is remaining.

For extraction of the secret data, same equation is used for each pixel group ($g_1,g_2,\ldots\ldots,g_n$) to track the secret digits. Then all the secret digits are converted back into binary format from (2n+1)-ary notation to find out the secret message.

But the disadvantage of this method is that it is having less embedding capacity since every pixel group contains only one secret digit and more processing time since message needs to be converted into another format.

B) A Large Payload Information Hiding Scheme Using 2 Levels EMD**:**

This method was proposed by C. Chang [6] in 2014 in which two secret digits can be embedded into one pixel group thus here the embedding rate is doubled to that of basic EMD method. In this method, we embed two secret digits into one pixel group where number of pixel group is not fixed. Thus, first start with embedding first secret digit in a pixel group.

1] First level embedding phase: First secret digit S_{I1} is embedded into pixel group by using extraction function 'f_1' which is given in equation (2)

$f_1 = (g_1^{(1)},g_2^{(1)},\ldots g_n^{(1)}) = (\sum^{n}{}_{i=1} ([gi^{(1)}/3])*i)) \bmod (2n+1)$...(2)

If $s_{I1}=f_1$ then the value of $gi^{(1)}$ is not change. Else compute $di_1= (s_{I1}-f_1) \bmod (2n+1)$ and do the modifications based on different values of di_1.At the end we get the modified pixel group $(MPG_1)=(g_1^{(1)},g_2^{(1)},\ldots g_n^{(1)})$

2] Second level embedding: For second secret digit s_{I2}, input s_{I2} and the corresponding modified pixel group MPG_1.then compute 'f_2' by using equation (3)

$f_2\ (g_1^{(2)},g_2^{(2)},\ldots g_n^{(2)}) = \sum^{n}{}_{i=1}(g_i^{(2)}*i)) \bmod (2n+1)$……...(3)

If $s_{I2}=f_2$ then the value of $gi^{(2)}$ is not change. Else compute $di_2= (s_{I2}-f_2) \bmod (2n+1)$ and do the modifications based on different values of di_2.At the end we get the output stego pixel

group SPG1= $(g_1^{(2)},g_2^{(2)},\ldots g_n^{(2)})$. At the extraction side, receiver receives the stego image as stego pixel group SPG_1 and starts retrieving the original secret pair of message (si_1, si_2) where i=1,2,….k

At extraction side, first input n stego pixel and then compute S_{I1}, S_{I2} by using equation (4) and (5) respectively.

$\mathbf{S_{I1}= f_1} = (g_1^{(2)},g_2^{(2)},\ldots g_n^{(2)}) = (\sum^{n}_{i=1}([gi^{(2)}/3])*i))\text{mod}(2n+1)$……(4)

$\mathbf{S_{I2}=f_2} =(g_1^{(2)},g_2^{(2)},\ldots g_n^{(2)}) = \sum^{n}_{i=1}(g_i^{(2)}*i))$ mod (2n+1)….(5)

At the end, we get secret digit pairs (S_{I1}, S_{I2}).

IV. ANALYSIS OF EMD METHOD:

For doing evaluation of both EMD methods, quality of stego image is analyzed on the basis of factors like MSE and PSNR and embedding rate is calculated.

1) Quality of the stego image:

Stego image quality is one of the important factors for doing comparison of various steganographic schemes. So it is important to keep stego image quality higher even if our system is having higher embedding rate. Hence, there is less possibility of attacks by attacker on image if stego image quality is high.

For judging stego image quality, following two factors are considered.

1.1 Mean Squared Error (MSE):

It is computed by performing byte by byte comparisons of the cover image and stego-image. Higher value of MSE indicates dissimilarity between compared images. The computation can be expressed by using formula (6)

$\text{MSE} = (1/M*N) \sum^{M}_{i=1} \sum^{N}_{j=1} (x_{i,j} - y_{i,j})$……...(6)

M*N is image size. $x_{i,j}$ and $y_{i,j}$ are the pixels of the cover and stego images in the same position (i, j) respectively.

1.2 Peak Signal To Noise Ratio (PSNR) :

The quality of the stego image compared with the cover image .The higher PSNR then the quality of stego image will be better. It can be calculated by using formula (7)

$\text{PSNR}=10 * \log_{10} (255^{2}/ \text{MSE})$…….(7)

2. Embedding rate(R):

Embedding rate gives the clear idea of no of secret bits that can be carried by each original pixel group. For basic EMD method it can be calculated by using following formula (8)

$R = 2 * \log_2 (2n+1)/n$…….(8)

While for two level EMD method it can be calculated by using following formula (9)

$R = \log_2 (2n+1)/n$……(9)

Where R=no of bits/pixels (bpp)

V TEST RESULTS

Table I. Results for basic EMD method

Image	Basic EMD For secret message = 123; for n=5		
	MSE	PSNR	Embedding Rate
Lena	1.9802e-13	127.0330	0.6919
Penguins	8.9516e-16	150.4810	0.6919
Pepper	1.8602e-13	127.3045	0.6919

Table II. Results for two level EMD method

Image	Two level EMD For secret message = 123; for n=5		
	MSE	PSNR	Embedding Rate
Lena	6.6606e-12	111.7649	1.3838
Penguins	3.1878e-14	134.9651	1.3838
Pepper	6.4986e-12	111.8718	1.3838

VI RESULT SCREENSHOT

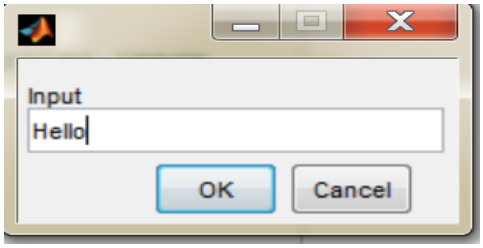

Fig 2: Entered secret messa

Fig 3: Carrier image

Fig 4: Stego image

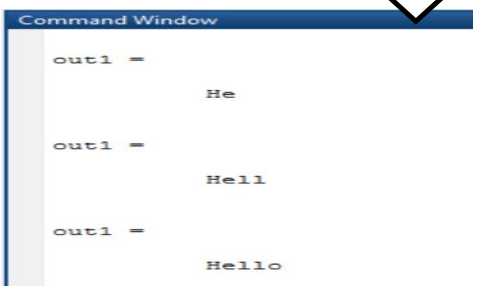

Fig 5: Retrieved secret message

VII CONCLUSION

In this paper, basic EMD method and two level EMD method are successfully implemented using raspberry pi. Their results are produced which indicates two level EMD has twice embedding rate than basic EMD but the quality of stego image is more affected in two level EMD than basic EMD**.** Two level EMD method gives high payload as compared to other methods like LSB and OP-AP method.

VIII ACKNOWLEDGEMENT

I would like to acknowledge all the people who have been of the help and assist me throughout my analysis of project work. It gives me a great pleasure in bringing out the project work entitled, "IMPLEMENTATION OF EXPLOTTING MODIFICATION DIRECTION (EMD) – A STEGANOGRPHY TECHNIQUE USING RASPBERRY PI". It is observed outcome of the exciting work, done under the inspiring guidance of my guide Prof. S. I. Nipanikar.

XI REFERENCE

[1] A. Ker, "Steganalysis of LSB Matching in Grayscale Images," IEEE Signal processing Letters, Vol.12, No.6, pp.441- 444, June 2005.

[2] R. Z. Wang, C. F. Lin, and J. C. Lin, "Image Hiding by Optimal LSB Substitution and Genetic Algorithm," Pattern Recognition, Vol. 34, No. 3, pp. 671-683, 2001.

[3] Hsien-Wen Tseng1 and Hui-Shih Leng, "A Steganographic Method Based on Pixel-Value Differencing and the Perfect Square number" Hindawi Publishing Corporation Journal of Applied Mathematics, Volume 2013, Article ID 189706

[4] Pritish Sachdeva and Shrutik Katchii "A Review Paper on Raspberry Pi", International Journal of Current Engineering and Technology E-ISSN 2277 4106, P-ISSN 2347 - 5161 ©2014 INPRESSC

[5] X. Zhang and S. Wang, "Efficient Steganographic Embedding by Exploiting Modification Direction," IEEE Comm. Letters, Vol.10, No.11, pp. 1-3, November 2006

[6] C.Chang, H.Wu, "A Large Payload Information Hiding Scheme Using Two Level Exploiting Modification Direction", Tenth International Conference On Intelligent Information Hiding And Multimedia Signal Processing IEEE-2014.