Analysis of Various Exploiting Modification Direction Techniques of Image Steganography: A Review Paper

Sourabh joshi[1], S.I.Nipanikar[1]
[1]Padmabhooshan Vasantdada Patil Institute of Technology, Pune, MS-India

Abstract— Exploiting Modification Direction (EMD) is a spatial domain image steganography technique to conceal secret data into digital images. In this paper, different types of EMD methods are explained. The important idea behind EMD is to embed the secret data with minimum loss of carrier image. This method provides high embedding efficiency when compared to other techniques. This paper gives the brief idea of different EMD techniques and their comparison.

***Keywords** - Steganography, Exploiting Modification Direction (EMD), 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 [4] 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.

Various types of EMD methods are also developed which are given in this paper. This paper is arranged as follows: In section II, concepts behind EMD technique has been discussed. Various types of EMD schemes have been explained and compared in section III. In section IV, the overall paper is concluded.

II. CONCEPT BEHIND EMD

The basic EMD method was proposed by Zhang and Wang [4] 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:

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

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,……,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 and more processing time. Since message needs to be converted into another format.

III. VARIOUS TYPES OF EMD TECHNIQUES

EMD scheme proposed by Zhang and Wang [4] give high embedding efficiency and also its PSNR value is above 50, but its disadvantage is that it hides only one secret digit in each n pixel group. Thus for improving embedding capacity various improved EMD techniques were proposed. Few of them are described below:

A. Data Hiding By EMD Technique Using Optimal Pixel Grouping

The optimized EMD method was proposed by analyzing the relationship between n and payload by Lin et al [6] in 2010 having high PSNR value than OPAP and LSB method and also it is having good stego image quality. In EMD method, a secret digit in (2n+1)-ary notational system is embedded by a group of n pixels. Here, the value of n decides the amount of pixel group and payload for that group thus its value has to be selected carefully. If n is too large, then it will not support the sufficient space to embed the whole confidential message on the other hand if n is too small, then it will take more numbers of pixels to embed data more than it actually required. The relationship between payload and n which is defined by Lin et al in and it is in equation (1).

$[I_s/n]*[\log_2 (2n+1)]>=p$………………………………...(1)

Here, I_s= total number of pixels in the cover image, n= total number of pixels in a group and p= length of the payload. Generally, we have values of p and I_s, thus maximum value of n can be find out in an easy way which gives the optimal solution. But this method is having certain disadvantages like limited embedding capacity and more processing time.

B. A Robust EMD-Like Steganographic Scheme

This method was proposed by X.Yao [7] in 2010 which provides robustness against noise for noisy communication channel. In this method by finding a relatively invariant replacement for conventional gray value before building the weighted sum function higher robustness against noise such as Gaussian, salt or pepper is achieved. Here first from top to bottom and from left to right cover image of size H*W is scanned using a 2*2 window. Then it constructs a vector, whose elements are matrices of size 2*2 denoting as,$\{M_1, M_2,\ldots,M_m\}$

Where m=(H/2)*(W/2).Then by selecting 4 neighboring pixels as a group, scanning of the cover image of size H*W is done with each group denoting as, $M_i = \{g_{i1}, g_{i2}, g_{i3}, g_{i4}\}$

Since robustness for both of them is different, they have actually almost same representations. After this, statistical function'sʼ is constructed such that

$g_i'=S(M_i)$………………………………………(2)

This basically means adding or subtracting this statistical quantity by 1 equals to adding or subtracting the group by 1 that is,

$g_i'+ -1=S(M_i + -1)$…………………………..…(3)

Thus, we can use any of the above stated EMD like method to conceal the secret bits with some desired robustness if this statistical quantity is noise invariant. Theoretically, to resist the sudden change of a pixel median of the group is very good whereas mean of the group is vulnerable to this change. The demerits of this scheme are that it is limited by embedding capacity and also it is having more processing time than basic EMD.

C. The High Embedding Steganographic Method Based On General Multi-EMD

This method was proposed by W.C.Kuo [8] in 2012 in which there is no requirement of more difficult steps when the secret data is embedded and the additional information when the secret data is recovered. This method not only enhances data hiding technique security but also stego image quality is also upgraded. Its important merit is that this method embeds secret bits more than two on average. For this method, extraction function used is:

$f_c (g_1,g_2,\ldots g_n) = \sum^{n}_{i=1} (g_i*c_i) \bmod 2^{nk+1}$…………………..(4)

Since, modulus is changed from 2^{n+1} to 2^{nk+1}, embedding capacity of this method is increased. After embedding secret digit 'd' with the help of embedding function we get the stego image c'. At the receiver side, stego image is received from which work of secret message 's' extraction is done with the help of same extraction function like (4) .then after extracting the message from the stego image ,it is again converted back into binary format to get the actual message. For this method, due to high embedding capacity PSNR value decreases.

D. A New High Capacity and EMD Based Image Steganography Scheme in Spatial Domain

EMD scheme was further enhanced by Hajizadeh et al [9].In this author proposed an extended form of EMD scheme where secret message is embedded into cover pixel pair with eight modification directions instead of 5 modification directions. In this method, extraction function used is

$f = f (x_i,x_{i+1})=((m-1) * x_i+ m* x_{i+1}) \bmod m^2$....................(5)

Where $m \geq 2$.

In this method, k (= [$\log_2 m^2$] bits secret message are embedded into a block of 2 cover pixel (x_i, x_{i+1}) by incrementing or decrementing x_i or/and x_{i+1} at most by r (= [m/2]) or remaining same to attain the stego pixel pair.

In this approach two steps of image blocking are used in each step to obtain high degree of security. Here image is first divided into further sub-images. The selection of random sub-images for embedding data is based on a random number which is generated by a pseudo random number generator using secret key. With this way, the data is concealed in distinct parts of the image and extraction of hidden message is only possible to the specified recipient who knows the secret key.

In this method, a new parameter, termed as Data Pattern Modifier (DPM) which is a positive integer lies between 0 to (2^n-1). First the value of this parameter is set then it is converted into k bit binary sequence which is used to define 2 new parameters i.e. XORP (XOR Pattern) and XNORP (XNOR Pattern).

For embedding process, first k bits of secret message are converted into decimal number d and value of extraction function f is calculated by using (5). If d=f, then no changes are required in pixel values. If d !=f then a new pair value is selected from searching area defined via $W_{(2\times r+1,\ 2\times r+1)}$ (m, (x_i, x_{i+1}), r) having f value same as d. Here the selected pair may not provide optimal solution with minimum distortion thus other pairs are also searched from the searching area W with center as the selected pair and the pair having minimum distortion will be selected and at the end final stego image pair will be updated with that value. The entire procedure is repeated until the whole message is not embedded into the cover image. At the receiving end, secret message is extracted by the specified embedding pattern for each and every block. For this process, a 2 bit binary key is used by the sender to each embedding block. Therefore the intended recipient having that secret pattern, will only be able to extract message from the stego image.

The demerits of this method are that stego image quality is not so good and also having large processing overhead.

E. A Large Payload Information Hiding Scheme Using 2 Levels EMD

This method was proposed by C.Chang [10] 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’:

$f_1 = (g_1^{(1)},g_2^{(1)},\ldots.g_n^{(1)}) = (\sum^n{}_{i=1}([gi^{(1)}/3])*i))\text{mod}(2n+1)$………….(6)

If $s_{I1}=f_1$ then the value of $gi^{(1)}$ is not change. Else compute $di_1= (s_{I1}-f_1) \text{ mod } (2n+1)$ 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’:

$f_2\ (g_1^{(2)},g_2^{(2)},\ldots.g_n^{(2)}) = \sum^n{}_{i=1}(g_i^{(2)}*i))\text{ mod }(2n+1)$............(7)

If $s_{I2}=f_2$ then the value of $gi^{(2)}$ is not change. Else compute $di_2= (s_{I2}-f_2) \text{ mod } (2n+1)$ 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 $S_{I1,}\ S_{I2}$

$S_{I1}= f_1 = (g_1^{(2)},g_2^{(2)},\ldots.g_n^{(2)}) = (\sum^n{}_{i=1}([gi^{(2)}/3])*i))\text{mod}(2n+1)$…………….(8)

$S_{I2}=f_2\ (g_1^{(2)},g_2^{(2)},\ldots.g_n^{(2)}) = \sum^n{}_{i=1}(g_i^{(2)}*i))\text{ mod }(2n+1)$……………..(9)

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

F. Improved EMD Steganography With Great Embedding Rate And High Embedding Efficiency Technique

This method was proposed by Zhiguo [5] where to obtain better quality of images embedding modification happen on frequency coefficients than LSB of the pixel. Embedding process of this method has three parts:

(1) Image feature and perceptual analysis: Here host image is first divided into non overlapping blocks of size 8*8 then each block is DCT transformed then analysis of image feature and perceptual is done for all DCT blocks.

(2) Choice rule: This rule helps to find out suitable pairs of coefficient to be embedded in. Here the pairs of coefficients whose values are same or exactly same are selected.

(3) Improved EMD method of embedding: Here the decimal values of each secret piece‘d’ is find out using:

d =c+(2n+1)*m…………………………………… (10)
k’=(c-f’) mod (2n+1)…………..................................(11)

Then with the help of embedding function f’, embedding of secret piece k’ with frequency coefficient is done.

$F' = [\sum^n{}_{r=1}((a'r/l)*r)] \text{ mod } (2n+1)$………………………….(12)

At extraction side, extraction function is calculated by using formula (10) and (11) with which we get the value of k’ then finally secret message d can be calculated by using formula (12). But the disadvantage of this method is that embedding capacity is less and security issues are also there.

Below comparison among various EMD techniques are given on the basis of their merits and demerits.

Table I. Comparison of Various EMD Techniques

Researcher with paper name	Year	Merits	Demerits
"efficient steganographic embedding by EMD" - Zhang et al [4]	2006	• Least distortion. • More secure. • Embedding efficiency and embedding rate are more than run length encoding and matrix encoding.	• Embedding capacity is less. • Less efficient. • Safety issues are there. • Message needs to be converted into another format hence more time is required for embedding.
"Improved EMD steganography with great embedding rate and high embedding efficiency technique" –Q.Zhiguo [5]	2009	• High embedding efficiency and embedding rate than basic EMD. • Stego image quality is better.	• Safety issues are there. • More time required for embedding process. • Embedding capacity is still less.
"Data hiding by EMD technique using optimal pixel grouping" -Lin et al[6]	2010	• High PSNR value than OPAP and LSB. • Achieves more desired stego image quality.	• Limited Embedding capacity. • Safety issues are there. • More processing time
"A robust EMD like steganographic scheme" - X.Yao [7]	2010	• Detector is robust under the disturbance of usual noise such as Gaussian or salt or pepper. • Stego image quality is good.	• More processing time. • Safety issues are there. • Limited Embedding capacity.
"The high embedding steganographic method based on general multi-EMD" -W.C.Kuo [8]	2012	• Embedding capacity is more. • Stego image quality is also good.	• More processing time. • Due to high embedding capacity PSNR value decreases.
"A new high capacity and EMD based image steganography scheme in spatial domain" -Hajizadesh et al[9]	2013	• Probability of discovery of hidden data is reduced. • Embedding capacity is also high.	• Stego image quality is not so good. • More processing time.

"A large payload information hiding scheme using 2 level EMD" -C.C.Chang [10]	2014	• Embedding rate is twice that of basic EMD. • More efficient.	• Stego image quality is not so good. • Doubled processing time than basic EMD.

IV. CONCLUSION

In this paper, we have studied various EMD methods to conceal secret data into image. A basic EMD method is having higher embedding efficiency and embedding rate than matrix encoding and run length encoding. EMD method proposed in having higher embedding efficiency and embedding rate than basic EMD. Further optimized EMD in has been developed which is having High PSNR value than OPAP and LSB. Then in robust EMD method detector is robust under the disturbance of usual noise such as Gaussian or salt or pepper. General Multi-EMD method gives high embedding capacity. High capacity EMD method gives higher security than all the previous EMD methods. A novel two level EMD method in is having embedding rate twice that of basic EMD.

V. REFERENCES

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

[5] Q.Zhiguo, F.Yu, N.Xinxin, Y.Yixian, Z.Ru, "Improved EMD Steganography with Great Embedding Rate And High Embedding Efficiency", Fifth International Conference On Intelligent Information Hiding And Multimedia Signal Processing IEEE-2009

[6] Kai Yung Lin, Wien Hong, Jeanne Chen, Tung Shou Chen, Wen Chin Chiang, "Data Hiding by Exploiting Modification Direction Technique Using Optimal Pixel Grouping" 2nd International Conference on Education Technology and Computer (ICETC),2010.

[7] X.Yao, W.Du, W.Wu, M.Huang, J.Fu, "A Robust EMD Like Steganographic Scheme", Third International Symposium on Intelligent Information Technology and Security Informatics IEEE-2010

[8] W.Kuo, L.Wuu, S.Kuo ,"The High Embedding Steganographic Method Based On General Multi-EMD",IEEE-2012

[9] Hamzeh Hajizadeh, Ahmad Ayatollahi and Sattar Mirzakuchaki, "A New High Capacity and EMD-based Image Steganography Scheme in Spatial Domain", IEEE-2013.

[10] 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.