A Novel Method to Improve Data Hiding Embedding Capacity in an Image

Akanchha Tiwari[1], Jaimala Jha[2]
[1]Dept. Of CSE/IT, Madhav Institute of Science and Technology, Gwalior
[2]Dept. Of CSE/IT, Madhav Institute of Science and Technology, Gwalior

Abstract- *Long ago in year 2009 Zhang & Wang proposed the classical method of embedding called as EMD. EMD makes the optimized use of modification in the direction of the cover pixels. This method could initially hide (2n+1)-ary number by making the change LSB of 'n' pixels. In this paper enhanced Generalized EMD methodology has been proposed. We have also studied the impact of adding noise to the input image.*

Keywords- Embedding, EMD, channel, steganographical, E.G.E.M.D.

I. INTRODUCTION

Two critical issues of information concealing systems are saving great picture quality and expanding the installing limit inside and out in the meantime. Be that as it may, this is a beyond reconciliation prerequisite. In the event that we attempt to diminish picture contortion, we need to forfeit the inserting limit. In the event that we increment installing limit, picture quality deteriorates. The original methodology has altered the minimum noteworthy piece (LSB) values. This straightforward strategy is called LSB substitution procedure. This strategy can insert the same number of bits as the aggregate number of pixels. In any case, measurable investigation in view of the chi-square test utilizing neighboring pixel esteem sets can recognize the nearness of a concealed message [1]. Two qualities whose parallel portrayals contrast just in the LSB level are known as a couple of qualities. In general, the frequencies of two neighboring values are statistically rarely equal in number. In any case, after the LSB substitution inserting, perception of Westfeld and Pfitzmann [1] presume that a large portion of their frequencies are drawing nearer. In the event that the message to be covered up is extremely arbitrary, the frequencies of the sets turn out to be almost equivalent in the wake of installing message because of its actual haphazardness. On the off chance that the message isn't arbitrary, the combine of qualities might be ordinary and does not give us any insight. In any case, professionals would prefer not to shroud plain content. They trust that concealing plain content is more perilous than figure content. As an end, the chi-square test is a viable system against LSB alteration techniques. Along these lines, lessening the implanting limit turns into an elective answer for decrease picture debasement. Tseng et al.[2]hide as many as blog $[\log_2(sn+1)]$ bits of data in an m×n binary image block by changing at most two bits in the block. Matrix encoding technique in F5 algorithm [3] changes at most one LSB value to embed k bits into p pixels where p =2k-1. Thus, this encoding technique uses a (1,p,k) Hamming code. Modified matrix encoding technique [4] uses a (2,p,k) Hamming code to modify at most two pixels. This modified matrix encoding technique allows more degree of freedom than the original matrix encoding technique. Hamming code. Modified matrix encoding technique [4] uses a (2,p,k) Hamming code to modify at most two pixels. This modified matrix encoding technique allows more degree of freedom than the original matrix encoding technique. Zhang and Wang [5] have proposed a novel data hiding technique to transform the binary secret data into a stream of secret digits using a (2m+1)-ary notational system. Their embedding method called exploiting modification direction (EMD) uses n cover pixels to carry one secret digit in the (2m+1)-ary number system. The maximum possible error of the modified pixel is +1,-1 because their scheme changes only one LSB value. The pixel division framework proposed by Lee et al.[6] can conceal all the more extensive numbers by altering two pixel esteems. Be that as it may, picture quality gets impressively debased and more terrible than 8 dB. Two new EMD techniques proposed in this paper, 2-EMD and EMD-2, are exceptionally easy to execute. The implanting limit of these techniques is bigger than the pixel division strategy, and significantly bigger than the EMD. In any case, the normal picture nature of the EMD-2 is around 52 dB which is 8 dB higher than the pixel division strategy, however like the EMD and 2-EMD. The effectiveness of the 2-EMD and EMD-2 is contrasted and the EMD under a similar condition.

II. PRELIMINARIE

In this part, we introduce EMD and GEMD methods in data hiding, and show the embedding capacities of them respectively.

A.EMD Method

Exploiting Modification of Direction is a data hiding scheme. For a group, they use m pixels & Equation for

extracting the data use eq.1 this method. The modification of 1-pixel value is done by +1 or -1 to embed (2m+1)-ary secret data.

$$f_{EMD}(g_1, g_2, \ldots\ldots, g_n) = [\sum_{i=1}^{n}(g_i \times i)] mod(2m+1) \text{ ..eq.1,}$$

Algorithm.: *Input Data:* Let the image cover be I_C with m pixels $I_C = (j_1, j_2, \ldots j_m)$binary secret data be K, *Output Data:* Let the Stegoimage be $I_S = (j'_1, j'_2, \ldots, j'_m)$.

1: Modify K into (2m+1)-ary secret data brookK'.

2: Compute $f_{EMD} = [\sum_{i=1}^{n}(g_i \times i)] mod(2m+1)$, and modify K to (2m+1)–ary brook $K_{(2n+1)}$.

3: Obtain (2m+1)-ary data K'_i from K'

4:Compute $d = (K_{(2n+1)} - f_{EMD}) \, mod(2n+1)$ by using cover pixel.

5: If (d=0), $j'_i = j_i$, i ϵ[1,m];else if (k ≤ m), $h'_k = h_k + 1$, $j'_i = j_i, i \epsilon [1, m]$,i≠d; else $j'_{2m+1-d} = j_{2m+1-d} - 1$, $j'_i = j_i$, iϵ[1,m] ,$i \neq 2m + 1 - d$.

6: Repeat from case 2 until all secret data get embedded.

The embedding capacity of EMD as $E_{EMD} = \frac{log_2(2m+1)}{m}$ .When m=2, EMD reaches upto 1.161 bpp which is the highest outcome then embedding capacity, the outcome of this result is not practical. The quality of the image quality become good with the EMD process and embedded the function by modulo function. However, two drawback comes out : it should convert binary confidential data to (2m+1) –ary to obtain full capacity before embedding done by act by using equation eq.1.The other one is when m increases the embedding capacity decreases faster.

III. PROPOSED SCHEME

To ameliorate the embedding capacity with the help of enhanced GEMD technique In this method 'm' set of pixels are divided into 2 sets of embedded data. The given below algorithm 3 explain enhanced GEMD:

Embedding Algorithm: *Input Data:* Two cover images $I_1=(p'_1,p'_2,..,p'_{m1})$,$I_2=(q'_1,q'_2,..,q'_{m2})$,$(m=m_1+m_2)$ m+2 bits, Secret data S, *Output Data:* Two stego images $S_{I1}=(p'_1,p'_2,\ldots..,p'_{m1})$,$S_{I2}=(q'_1,q'_2,\ldots.,q'_{m2})$.

EGEMD 1: Covert binary data S into decimal S_{10}

SEGEMD 2: $S_{10} = 2^{m1+1} \times t+u$, here we take t and u as integers and $u<2^{m1+1}$.

EGEMD 3: Using S_{I1},S_{I2} two output Stegoimage & EMD-2 embedding approach to embed t,u into I_2,I_1.

EGEMD 4: Till each confidential data is embedded perform E-GEMD.1 again.

Extracting algorithm: *Input Data:* Two stego-image: Two stego images $S_{I1}=(p'_1,p'_2,\ldots..,p'_{n1})$,$S_{I2}=(q'_1,q'_2,\ldots.,q'_{n2})$,*Output Data*: *m*+2 bits secret data *S.*

EGEMDE 1: With the help of S_{I1} & S_{I2} Recover t & u by using the recover in approached in

$$f_{GEMD} = \left[\sum_{i=1}^{m} j_i \times (2^i - 1)\right] mod\ 2^{m+1}.$$

EGEMDE 2: Compute $S_{10} = 2^{m1+1} \times t+u$.

EGEMDE 3. Change S_{10} into m+2 bits data S, & output S.

Within this, an 'n+1'data replaced by 'n+2' confidential data is embedded in G.E.M.D. Through, Enhanced G.EMD is calculate embedding capacity with the help of [m+k] ÷m.Where, nature of Stegoimage got decreases and the pixels of cover image got change when number of 'k' got increased when embedding capacity is boost[1].

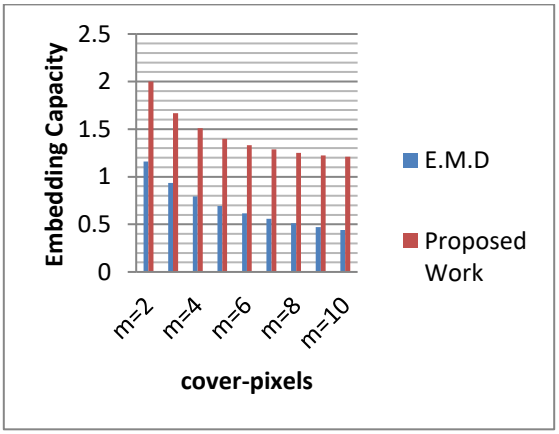
IV. EXPERIMENT RESULT

In this part, comparisons of embedding capacities and Stegoimage qualities between EMD, GEMD and our enhanced GEMD are made to show the properties of data hiding. Section II gives the embedding capacities of EMD, which is $E_{EMD} = \frac{log_2(2m+1)}{m}$. Our enhanced GEMD has embedding capacity of R= $\frac{m+2}{m}$, which is improved from EMD.


The following Table 2 shows the embedding capacities of these three schemes for different m.

Table 2: Comparison of Embedding Capacity.

No. Of Cover Pixel	E.M.D	Proposed Work
m=2	1.161	2
m=3	0.9358	1.668
m=4	0.7925	1.51
m=5	0.6919	1.40
m=6	0.6167	1.332
m=7	0.5581	1.287
m=8	0.5109	1.25
m=9	0.472	1.223
m=10	0.4392	1.21



Graph 1. Between EMD & Proposed of Embedding Capacity.

The quality of stego-images is usually measured by Peak Signal to Noise Ratio (PSNR). The higher PSNR means the better quality of image. If PSNR is lower than 30 dB, the stego-image can be visually distinguished from the cover image. The PSNR and mean square error (MSE) are presented as following equation.

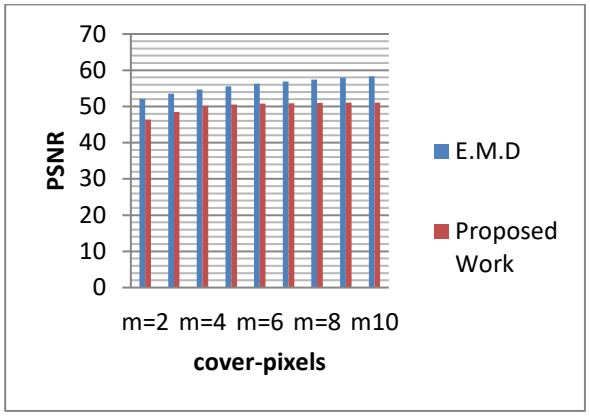
$$PSNR = 10 \times \log_{10} \frac{255^2}{MSE} \text{.....eq.1}$$

$$MSE = \frac{1}{U \times V} \sum_V^U \sum_U^V (I(x,y) - I'(x,y))^2 \text{.....eq.2}$$

Where U & V be image length and width. The comparison between EMD, GEMD, enhanced GEMD and our scheme are shown in Table 1. In the proposed methodology PSNR output is lesser than E.M.D, E.M.D-2 and enhanced G.E.M.D and still than also it could not de dectected by the human eye. From this table, it is shown that the quality of the Stegoimage is good enough to keep away from detection of the human eye, which is more than 40 dB. In our proposed work, we maintain the embedding capacity to 2bpp where 'n' is independent value. However other methods endure when 'n' expand.

Table 3. Comparison of PSNR.

No. Of Cover Pixel	E.M.D	Proposed Work
m=2	52.12	46.37
m=3	53.56	48.51
m=4	54.67	50.17
m=5	55.54	50.54
m=6	56.26	50.79
m=7	56.88	50.92
m=8	57.43	51.00
m=9	57.91	51.04
m10	58.34	51.08



Graph.1: Between E.M.D & Proposed of PSNR.

V. CONCLUSION

Unconditionally the embedding capacity should increase the quality of the stego image should be high enough to pass cyber-attacks. The hackers try to add the noise to the stego image to study the PSNR values of the resultant image. If there is large change in PSNR values beyond 60% then the Stego image cannot be tempered. The results of our proposed works show that the Enhanced Generalized EMD technique is robust & it can withstand cyber-attacks.

REFERENCES

[1] Yaniao Liu, Chingnug Yang, and Qindong Sun, "Enhance Embedding Capacity of Generalized Exploiting Modification Directions in Data Hiding", IEEE Access, vol.6, pp.5374-5378,2018.

[2] Arun Agarwal, S.K. Patra, "Performance prediction of the OFDM based digital audio broadcasting system using channel protection mechanisms",3rd International Conference on Electronics Computer Technology vol. 2,pp.57– 61, 07 July 2011, 07 July 2011.

[3] C.-K. Chan and L. M. Cheng, ''Hiding data in images by simple LSB substitution,'' Pattern Recognition, vol. 34, no. 3, pp. 671-683, Mar. 2001.

[4] R.-Z. Wang, C.-F. Lin, and J.-C. Lin, ''Image hiding by optimal LSB substitution and genetic algorithm,'' Pattern Recognit., vol. 34, no. 3, pp. 671-683, Mar. 2001.

[5] S. Dumitrescu, X. Wu, and Z. Wang, ''Detection of LSB steganography via sample pair analysis,'' IEEE Trans. Signal Process., Jul. 2003.

[6] J. Fridrich, M. Goljan, and D. Rui, ''Detecting LSB steganography in color, and gray-scale images,'' IEEE Multimedia, vol. 8, no. 4, pp. 22-28, Oct./Dec. 2004.

[7] X. Zhang and S. Wang, "Efficient steganographic embedding by exploiting modification direction," IEEE Commun. Lett., vol. 10, no. 11, pp. 781-783, Nov. 2006.

[8] X. Zhang, W. Zhang, and S. Wang, ‘‘Efficient double-layered steganographic embedding,’’ Electron. Lett., vol. 43, no. 8, pp. 482-483, Apr. 2007.
[9] X. Zhang, W. Zhang, and S. Wang, ‘‘A double layered ‘plus-minus one’ data embedding scheme,’’ IEEE Signal Process. Lett. , vol. 43, no. 8, pp. 482-483, Apr. Nov. 2007.
[10] K. H. Jung and K. Y. Yoo,“Improved exploiting modification direction method by modulus operation,” Int. J. Signal Process., Image Process. Pattern,2009.
[11] C.-F. Lee, Y.-R. Wang, and C.-C. Chang,‘‘A steganographic method with high embedding capacity by improving exploiting modification direction,’’ in Proc. 3rd Int. Conf. Intell. Inf. Hiding Multimedia Signal Process., Nov. 2007.
[12] W.-C. Kuo and C.-C. Wang, ‘‘Data hiding based on generalised exploiting modification direction method,’’ Image Sci. J., Nov. 2013.