International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-2, December 2019

Design and Implementation of LSB based Minimum Deviation Steganography technique on High Payload Grayscale Images

Arnab Pal, Aritra Bandyopadhyay

Abstract*: The paper discusses the design of a new steganographic method for 8-bit grayscale images. Here, the input cover image is decomposed into 2 × 2 blocks of pixels which are non-overlapping in row major order. Each block can embed 7-bits from secret bit-stream. Successive block embedding operation ensures the concealment of the entire hidden information into the carrier image. The proposed method offers a fixed payload of 1.75 bits per pixel (bpp) which is considered to be a high payload in the field of Steganography. The degradation of the stego-image is also not severe in our method and that can be analyzed by observing the Peak Signal to Noise Ratio (PSNR) of greater than 30 dB. In the reverse way, the receiver decomposes the cover image into 2 × 2 non-overlapping blocks of pixels in row major order. Successive extraction of 7- secret bits from each block ensures the re-generation of the secret information. Simulation results ensure that the proposed method is superior than other schemes in terms of qualitative clarity of the Stego-image.

***Index Terms*: Data hiding, Minimum Deviation Steganography, Grayscale Image, LSB**

I. INTRODUCTION

The study of Steganography is a study about embedding and hiding information in a medium (named a "cover"). Steganography [1] which is related to cryptography was used by the Ancient Greeks to hide messages or any information about company movements by tattooing it on someone's head and then letting the person grow out their hair. Simply put, Steganography is very old like dirt.

LSB technique [2] is the simplest and most popular method among all other image steganographic technique which are existing. Applying this technique to each pixel of 8-bit greyscale image, where into each pixel only one bit can be encoded, because one byte represents each pixel. The pixel indicator technique [3], proposed by Gutub is a technique where one component of a pixel is used as the indicator component and also the other two components are used in secret data hiding. Two least significant bits of the indicator channel is checked in this technique.

Revised Manuscript Received on December 30, 2019.
***** Correspondence Author
Arnab Pal*, Department of Computer Science and Engineering, Supreme Knowledge Foundation Group of Institutions, Mankundu, India. Email: pal.arnab5@gmail.com
Aritra Bandyopadhyay, Department of Computer Science and Engineering, Supreme Knowledge Foundation Group of Institutions, Mankundu, India. Email: aritra.d90@gmail.com

The Steganographic method based on pixel-value differencing [4] proposed by Wu and Tsai in 2003 is more efficient, secured and modified version of simple least significant bit replacement method, based on the characteristics of sensitivity of human vision for grey value variations with effects of smoothness to contrast is about hiding secret messages into a cover image which is grey valued. In the year 2006, J. Mielikainen [5] had proposed a technique Edge Adaptive Image Steganography which is based on LSB Matching (EA-LSBMR), was popular at that time. In this technique one can pick the regions to hide data based on a orbit value. In 2010, Yang and Weng [6] proposed a scheme about shifting pixel value which is leading an increased hiding capacity compared to Wu and Tsai method of processing two pixel at a time. In the year 2011, a novel steganographic technique was proposed by Ghosal [7], which is firstly based on the number (of 1's and of 0's) in the first pixel's Red component. After that, the calculation of ultimate difference between this two is down and ended with dividing by 2. Therefore, the aftermath numbers of bits are hided in other two channels which are Green and Blue. Here, the function of the Red component will be as an indicator. In 2014, Shen [8] [9] proposed a new data hiding method which helps to grow the steganographic security of data embedding scheme from the attacks of pixel-value difference (RS detection attack and the steganalytic histogram attack).

II. PROPOSED DESIGN AND METHODOLOGY

The proposed work is focused to design a new steganographic approach on grayscale images. In our proposed method, the cover image is decayed into 2 × 2 blocks of pixels which are non-overlapping in a row major order. To ensure minimum deviation, either the first row or the first column is chosen for embedding of 7-bits of secret data in each block. Successive step embeds the entire secret information, provides good payload [10, 11-12] and yields well perceptible stego-image. In the reverse way, the receiver decomposes the cover image into 2×2 blocks of pixels (non-overlapping) in row major order. Successive extraction of 7- secret bits from each 2×2 block ensures the re-construction of the confidential data. The suggested method is further classified into two sections: Embedding and Extraction.

A. Embedding

Inputs are the Cover image (CI) and Secret image (HI) and output will be the corresponding Stego image (SI).

- Transform the Secret image (HI) into 1-D array in the form of secret bit-stream S.
- Construct a secret decimal value DVAL equivalent to the 7-bits of S.
- Decompose the cover image (CI) into 2 × 2 blocks which is non-overlapping of pixels $\begin{bmatrix} p_0 & p_1 \\ p_2 & p_3 \end{bmatrix}$ in row major order.
- During embedding, the following pairs are chosen: (p_0, p_1) and (p_0, p_2). To ensure minimal distortion, two deviation parameters DEV1 and DEV2 are computed and then the optimal pair of pixels is chosen for embedding.
- DEV1 Computation:
  Calculate a reference value F as follows:
  $F = (p_0 + 7*p_1) \% 2^7$
  Find the difference value (i.e., deviation),
  D = DVAL - F.
  If D < - 64 then D = D + 128
  If D > + 64 then D = D – 128
  D is decomposed into following two parts:
  D_1 = D / 7 and
  D_0 = D % 7
  The embedding process ensures the following changes: $(p_0', p_1') = (p_0 + D_0, p_1 + D_1)$.
  Compute DEV1= $|p_0' - p_0| + |p_1' - p_1|$
- DEV2 Computation:
  Compute a reference value F as follows:
  $F = (p_0 + 7*p_2) \% 2^7$
  Find the difference value (i.e., deviation),
  D = DVAL - F
  If D < - 64 then D = D + 128
  If D > 64 then D = D – 128
  D is decomposed into following two parts:
  D_1 = D / 7 and
  D_0 = D % 7
  The embedding process ensures the
  $(p_0'', p_2') = (p_0 + D_0, p_2 + D_1)$
  Compute DEV2= $|p_0'' - p_0| + |p_2' - p_2|$
- If DEV1< DEV2 Then Stego pixels: (p_0', p_1') and set LSB $(p_3) = 0$

  Else, Stego pixels: (p_0'', p_2') and set LSB $(p_3) = 1$
- Repeat the above steps until and unless the entire secret bit-steam S is embedded. Successive embedding of secret bits into such 2 × 2 blocks (non overlapping) of the cover image yields the Stego image (SI).
- Stop.

B. Extraction

Input is the Stego image (SI) and corresponding output will be the Secret image (HI).

- Decompose the stego image (SI) into 2 × 2 blocks which are non-overlapping of pixels $\begin{bmatrix} p_0 & p_1 \\ p_2 & p_3 \end{bmatrix}$ in row major order.
- Construct an empty 1-D array S to load the secret bits to be extracted.
- If LSB (p3) = 0
  Compute a reference value F as follows:
  F = (p0+7* p1) % 27
  Else Compute a reference value F as follows:
  F = (p0+7* p2) % 27
- Convert F into 7-bits binary equivalent and form the confidential bit-stream S.
- Reapply steps 1 to 4 till and unless the secret bit-stream S is extracted. The restored secret bit-stream S is transformed into the secret image (HI).
- Stop.

C. Illustration by Example

The first 2 × 2 blocks consisting of four pixels $\begin{bmatrix} 162 & 54 \\ 160 & 59 \end{bmatrix}$ are taken to hide secret bits $(1111000)_2$. We know that the proposed scheme has been classified into two stages, one of them is Embedding and another one is Extraction.
Now, the decimal equivalent of the 7-bit secret bits $(1111000)_2$ is, DVAL=120
During embedding, the following pairs are chosen: (162, 54) and (162, 160)

- DEV1 Computation:
  So, $(p_0, p_1) = (162, 54)$
  F = (162 + 7*54) % 128
  = 540 % 128
  = 28
  Hence,
  D = (S – F) = (120-28) = 92
  Since, D > 64, D = 92-128 = -36
  D_1 = - 36 / 7 = -5
  D_0 = - 36 % 7 = -1
  The modified pair of pixels is:
  $(p_0', p_1') = (p_0+D_0, p_1+D_1)$
  = (162-1, 54-5)
  = (161, 49)
  DEV1= $|p_0' - p_0| + |p_1' - p_1|$
  = |162-161| + |54-49| = 1 + 5 = 6

- DEV2 Computation:
  So, $(p_0, p_2) = (162, 160)$
  F = (162 + 7*160) % 128
  =1282 % 128
  = 2
  Hence,
  D = (S – F) = (120-2)
  = 118
  Since, D > 64, D =118-128 = -10
  D_1 = -10/7 = -1
  D_0 = -10%7 = -3
  The modified pair of pixels is:
  $(p_0'', p_2') = (p_0+D_0, p_2+D_1)$
  = (162-3, 160-1)
  = (159, 159)

DEV2= $|p_0'' - p_0| + |p_2' - p_2|$ = |159-162| + |159-160| = 3 + 1 = 4
Here, to ensure minimal distortion, two deviation parameters DEV1 and DEV2 are computed and then the optimal pair of pixels is chosen for embedding.
Since, DEV2 < DEV1,
Pair of Stego-pixels = (159, 159) and keep LSB of fourth pixel 59 as '1'.
The final 2 × 2 block is $\begin{bmatrix} 159 & 54 \\ 159 & 59 \end{bmatrix}$.

The extraction process is as hereunder:

F'= (159+ 7*159) % 128
= 1272 % 128
= 120

III. RESULT AND INTERPRETATIONS

The experiment used five gray-scale images such as 'Lena', 'Baboon', 'Peppers', 'Airplane' and 'Boat' of sizes 128×128, 256×256 and 512×512 as shown in Fig. 1 In order to attain a fixed payload of 1.75 bits per pixel (bpp), the differing sizes of 'Barbara', the secret image has been hided into the aforementioned carrier images. The results of the experiments are summed up based on the following parameters: Peak Signal to Noise Ratio (PSNR), Mean Squared Error (MSE), Structural Similarity Index (SSIM), and Universal Image Quality Index (UQI). From Table- I it was seen that the highest PSNR achieved is 40.43 dB for the "Pepper" with dimension 128×128 where the lowest PSNR is 39.71 dB for the "Airplane" with dimension 512×512. The MSE values in Table- II suggested minimum error rate lower than 7. It is noticeable from Table- III that the values of SSIM is greater than 0.95 in all the cases which shows higher similarity . These values ensured higher similarity between the Cover and the Stego images. It is evident from the UQI values at Table- IV that the quantitative quality of the images stays well greater than 0.75 and in most of the cases the values are in the range of 0.9 to 0.99.

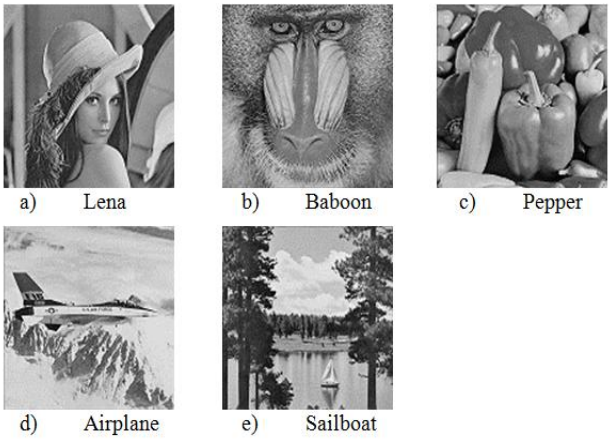

Fig.1 Sample cover images of dimension 512×512

To obtain the more accuracy, we have compared the method which is proposed with Wu and Tsai method[4], Yang and Weng et al's method[6] and Shen et al. [9] in terms of PSNR, MSE, SSIM and UQI in corresponding Table- V,VI,VII and VIII. From Table- V, Table- VI, Table- VII and Table- VIII, it is observed that the change in each pixel is minimal without affecting the image quality. The average PSNR of proposed technique is 0.51 dB more than Shen et al.'s scheme , 0.68 dB more than Yang and Weng et al's method.

Table- I: PSNR for the cover images of dimensions 128 × 128, 256 × 256 and 512 × 512 for Proposed Method

Images	Dimension of Cover image	Payload (bpp)	PSNR (dB)
Lena	128 × 128	1.75	40.25
	256 × 256	1.75	40.06
	512 × 512	1.75	39.97
Baboon	128 × 128	1.75	40.43
	256 × 256	1.75	40.34
	512 × 512	1.75	40.35
Pepper	128 × 128	1.75	40.20
	256 × 256	1.75	40.09
	512 × 512	1.75	40.05
Airplane	128 × 128	1.75	39.98
	256 × 256	1.75	39.85
	512 × 512	1.75	39.71
Boat	128 × 128	1.75	40.27
	256 × 256	1.75	40.16
	512 × 512	1.75	40.14

Table- II: MSE for the cover images of dimensions 128 × 128, 256 × 256 and 512 × 512 for Proposed Method

Images	Dimension of Cover image	Payload (bpp)	MSE
Lena	128 × 128	1.75	6.12
	256 × 256	1.75	6.40
	512 × 512	1.75	6.54
Baboon	128 × 128	1.75	5.87
	256 × 256	1.75	6.00
	512 × 512	1.75	5.99
Pepper	128 × 128	1.75	6.19
	256 × 256	1.75	6.36
	512 × 512	1.75	6.42
Airplane	128 × 128	1.75	6.52
	256 × 256	1.75	6.72
	512 × 512	1.75	6.94
Boat	128 × 128	1.75	6.17
	256 × 256	1.75	6.26
	512 × 512	1.75	6.28

Table- III: SSIM for the cover images of dimensions 128 × 128, 256 × 256 and 512 × 512 for Proposed Method

Images	Dimension of Cover image	Payload (bpp)	SSIM
Lena	128 × 128	1.75	0.98
	256 × 256	1.75	0.96
	512 × 512	1.75	0.98
Baboon	128 × 128	1.75	0.99
	256 × 256	1.75	0.99
	512 × 512	1.75	0.99
Pepper	128 × 128	1.75	0.98
	256 × 256	1.75	0.96
	512 × 512	1.75	0.98
Airplane	128 × 128	1.75	0.96
	256 × 256	1.75	0.95
	512 × 512	1.75	0.97
Boat	128 × 128	1.75	0.98
	256 × 256	1.75	0.97
	512 × 512	1.75	0.98

Table- IV: UQI for the cover images of dimensions 128 × 128, 256 × 256 and 512 × 512 for Proposed Method

Images	Dimension of Cover image	Payload (bpp)	UQI
Lena	128 × 128	1.75	0.96
	256 × 256	1.75	0.91
	512 × 512	1.75	0.87
Baboon	128 × 128	1.75	0.99
	256 × 256	1.75	0.98
	512 × 512	1.75	0.98
Pepper	128 × 128	1.75	0.97
	256 × 256	1.75	0.93
	512 × 512	1.75	0.90
Airplane	128 × 128	1.75	0.91
	256 × 256	1.75	0.85
	512 × 512	1.75	0.77
Boat	128 × 128	1.75	0.96
	256 × 256	1.75	0.93
	512 × 512	1.75	0.91

Table- V:Performance of Wu and Tsai method with respect to Capacity and PSNR

Images	Wu and Tsai method	
	Capacity	*PSNR*
Lena	406632	41.71
Baboon	437806	38.90
Peppers	401982	41.07
Sailboat	415554	40.67
Average	**415493.5**	**40.59**

Table- VI: Performance of Yang and Weng et al's method with respect to Capacity and PSNR

Images	Yang and Weng et al's method	
	Capacity	*PSNR*
Lena	410854	40.54
Baboon	482515	34.67
Peppers	408281	40.47
Sailboat	430888	38.11
Average	**433134.5**	**38.45**

Table- VII: Performance of Shen et al.'s scheme with respect to Capacity and PSNR

Images	Shen et al.	
	Capacity	*PSNR*
Lena	441972	40.89
Baboon	453123	36.13
Peppers	442711	39.99
Sailboat	451795	41.46
Average	**447400.2**	**39.62**

Table- VIII: Performance of the Method which is Proposed regarding Capacity and PSNR

Images	Proposed Method	
	Capacity	*PSNR*
Lena	458752	39.97
Baboon	458752	40.35
Peppers	458752	40.05
Sailboat	458752	40.14
Average	**458752**	**40.13**

IV. CONCLUSION

Steganography can be used for hidden communication. It has explored the limits of Steganography. In this technique enhancement of the image Steganography has been observed in terms of PSNR only. It is also noticed that the suggested method gives invariable PSNR for all five images and by in no way has the PSNR fallen below the acceptable level (greater than 30 dB) and also gained the value as high as 40dB. The method can further be improved by enhancing the payload up to 3 bpp. Some chaotic sequences may also be incorporated to increase the security of the method which is proposed. This proposed method may help in creating a renaissance in Steganography in future.

ACKNOWLEDGEMENT

The work was carried out at The Centre For Machine Learning and Intelligence of Department of Computer Science and Engineering, SKFGI.

REFERENCES

1. L. M. Marvel, C. G. Boncelet, C. Retter, "Spread Spectrum Steganography," *IEEE Transactions on image processing*, vol. 8, no. 8, 2007 pp. 160-178.
2. W. Bender, D. Gruhl, N. Morimoto, A. Lu, "Techniques for data hiding," *IBM Systems Journal*, vol. 35, 1996, pp. 313–336.
3. A. A. A. Gutub, "Pixel Indicator Technique for RGB Image Steganography," *Journal of Emerging Technologies in Web Intelligence*, vol. 2, no.1, 2010, pp.400-403.
4. D. C. Wu, W. H. Tsai, "A steganographic method for images by pixel-value differencing," *Pattern Recognition Letters*, vol. 24, 2003, pp. 1613–1626.
5. J. Mielikainen, "LSB matching revisited," *IEEE Signal Process. Lett.* vol. 13, no. 5, May. 2006, pp. 285–287.
6. C. H. Yang, C. Y. Weng, H. K. Tso, J. S. Wang, "A data hiding scheme using the varieties of pixel-value differencing in multimedia images" *The Journal of Systems and Software* vol. 84, 2011, pp. 669-678.
7. S. K. Ghosal, "A New Pair Wise Bit Based Data Hiding Approach on 24 Bit Color Image using Steganographic Technique," *International Conference on Scientific Paradigm Shift in Information Technology & Management (SPSITM 2011) in collaboration with IEEE, Kolkata*, 2011.
8. S. Shen, L. Huang "A data hiding scheme using pixel value differencing and improving exploiting modification directions," *Comput. Secur.*,vol.48, 2015, pp. 131-141.
9. S. Shen, L. Huang, S. Yu, "A novel adaptive data hiding based on improved EMD and interpolation," *Multimedia Tools Appl.*, vol. 14, 2017, doi: 10.1007/s11042-017-4905-5.
10. J. K. Mandal, S. K. Ghosal, "A High Payload Steganographic Technique for Color Images (HPST)," *International Conference on Information's System Design and Intelligent Applications*, ISBN- 978-981-07-1158-0, 2012, pp. 65-70.
11. S. K. Ghosal, J. K. Mandal, R. Sarkar, "High Payload Image Steganography based on Laplacian of *Gaussian (LoG) Edge Detector," Multimedia* Tools and Applications, Springer, vol.77, no.23, 2018 pp 30403–30418.
12. H. W. Tseng, H. S. Leng, "High-payload block-based data hiding scheme using hybrid edge detector with minimal distortion," *IET Image Process.* vol. 8, 2014, pp. 647-654.

AUTHORS PROFILE

Arnab Pal was born in 1993, received his B.Tech (Computer Science) from Maulana Abul Kalam Azad University of Technology, M.Tech (Computer Science) from Maulana Abul Kalam Azad University of Technology,

India in the year of 2015 & 2019 respectively. He has also completed DOEACC 'O' Level from National Institute of Electronics and Information Technology, India in the year of 2012. His research interest includes Steganography, Image and Signal Processing. He is an Ex-Lecturer of JLD College of Engineering and Management. Presently working as MIS Manager for the State Project Management Unit, West Bengal (Ground Water), National Hydrology Project (central sector scheme of Ministry of Water Resources, River Development and Ganga Rejuvenation, Govt. of India).

Aritra Bandyopadhyay was born in 1988, received his B.Tech (Computer Science) from West Bengal University of Technology, M.Tech (Computer Science) from West Bengal University of Technology, India in the year of 2010 & 2012 respectively. Presently, he is a PhD Registered Scholar at Maulana Abul Kalam Azad University of Technology and working as an Assistant Professor in the department of Computer Science & Engineering at Supreme Knowledge Foundation Group of Institutions Mankundu, Hooghly, West Bengal, India since 2012. He has more than 10 publications in reputed refereed journals and conference proceedings to his credit. His research interest includes Image and Signal Processing.