International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 4 Issue: 4

ISSN: 2454-4248
479 – 483

MSE and MAE Based Investigation of Modified LSB Approach

Sachin
Research Scholar,
Department of Computer Science & Engineering,
U.I.E.T, M.D.U, Rohtak , Haryana, India

Abstract:-Modified LSB approach is one of the many techniques to conceal data. Message is hidden in R, G and B components of pixels of a colored host image in Modified manner. Firstly a message bit is inserted on R-component's LSB of 1st pixel then on G-component's LSB of 2nd pixel and further on B-component's LSB of 3rd pixel and so on. In this manner data of different sizes 4KB, 8KB and 16KB are inserted and result is analyzed based on MAE and MSE based parameters.

Keywords: *Steganography; Modified LSB; MAE; MSE*

*****

I. INTRODUCTION AND LITERATURE REVIEW

Steganography is one way of achieving the security of data by concealing it in some cover medium like images , videos , audios and so on [1, 17, 18, 19]. Broadly this technique is divided into Spatial and Transform domain [2, 14, 15, 20]. The prior one focuses on hiding the data by directly changing the gray levels of host image so more vulnerable to attacks. While the latter one works, after changing the image coefficients and the embedding the data [3, 4, 16]. In history a number of steganography techniques are presented. Joshi et. al [5] provided a technique over spatial domain for the robustness of watermark when the stego image is suffered from salt and pepper noise. Chang et. al [6] gave an algorithm based on covering all the possibilities to store the data on LSB. Lin and Thien [7] proposed a modulus function approach on LSB. Chugh et. al [8] gave a steganography mechanism over RGB images using the concept of modulus and modfactor. Joshi and Allwadhi [9] gave a GLM based technique over medical image system wherein data is hidden in various medical images like X-Rays, CT-scans, and MRIs and so on. Avci et. al [10] projected a stegaongraphic algorithm in transform domain based on probabilistic XOR. Joshi et. al [11] implemented a steganography algorithm using LSB approach and investigated the results over different images concealing varying amount of data. Rao and Kumari [12] provided an authentication algorithm using watermarking technique in medical images.

II. MODIFIED LSB METHOD AND EXPERIMENTAL RESULTS

The major limitation of LSB approach is its simplicity. Therefore it is vulnerable to security attacks and easily compromised. So it makes us to use another approach that works on RGB (Color) images. In this 1st bit of message is inserted in the R-component of 1st pixel, 2nd bit of message is concealed into G-component of 2nd pixel, whereas 3rd bit goes into B-component of 3rd pixel and so on. This process repeats in Modified manner until message is over so this method is called "Stego Color Cycle". Insertion Procedure starts from very first pixel (CI_{00}) of an RGB cover image (CI) i.e CI = $\{CI_{mn} | 0 <= m <= R_{CI}, 0 <= n <= C_{CI}\}$ where R_{CI} and C_{CI} denotes the number of rows and columns of cover image respectively. The message (M) of length (l) i.e M = $\{m_k | 0 <= k < l, m_k \varepsilon \{0,1\}\}$ is inserted into 3 components i.e R,G and B successively one by one after selecting one component at a time. For example if we want to insert a bit in CI_{00} i.e decimal (CI_{00}) = 0th indexed pixel then it will select its R-component and inserts corresponding message bit. On second iteration i.e decimal (CI_{01}) = 1st indexed pixel it will select its G-Component and a message bit is inserted and so on. This process repeats until message size is exhausted as shown in figure 1. Now after concealing the message (M) into host image , we get a stego RGB image (SI) i.e SI = $\{SI_{mn} | 0 <= m <= R_{SI}, 0 <= n <= C_{SI}\}$ where $SI_{mn} = \{ R_{mn}, G_{mn}, B_{mn} \}$ and R_{mn}, G_{mn} & B_{mn} ε {0, 1, ….., 255}. First message bit is retrieved from 0th indexed stego pixel i.e (SI_{00}) from its R-component's LSB. Similarly second message bit is retrieved from 1st indexed stego pixel i.e (SI_{01}) from its G-component's LSB and so on. This procedure repeats until complete message of length **l** is retrieved as shown in extraction algorithm in figure 2. Original and the corresponding stego images of dimension 512*512 are shown in Table 1 and Table 2 represents their corresponding MAE and MSE.

III. MAE and MSE

Mean Absolute Error (MAE) and Mean square Error (MSE) are the two basic parameters to analyze the image quality [13]

It is given by the equation:

$$MAE = \frac{1}{N}\sum_{x=1}^{N}|Xx - Yx|$$

 ISSN: 2454-4248
479 – 483

$$MSE = \frac{1}{[N \times M]^2} \sum_{i=1}^{N} \sum_{j=1}^{M} (X_{ij} - Y_{ij})^2$$

MSE is the mean square error. N, is the number of rows in the cover image M, is the number of column in the image, h_{ij} pixel in cover image. S_{ij} is the intensity of S_{ij} pixel in stego image. The mean absolute error is the absolute value of the difference between the forecasted value and the actual value. MAE tells us how big of an error we can expect from the forecast on average.

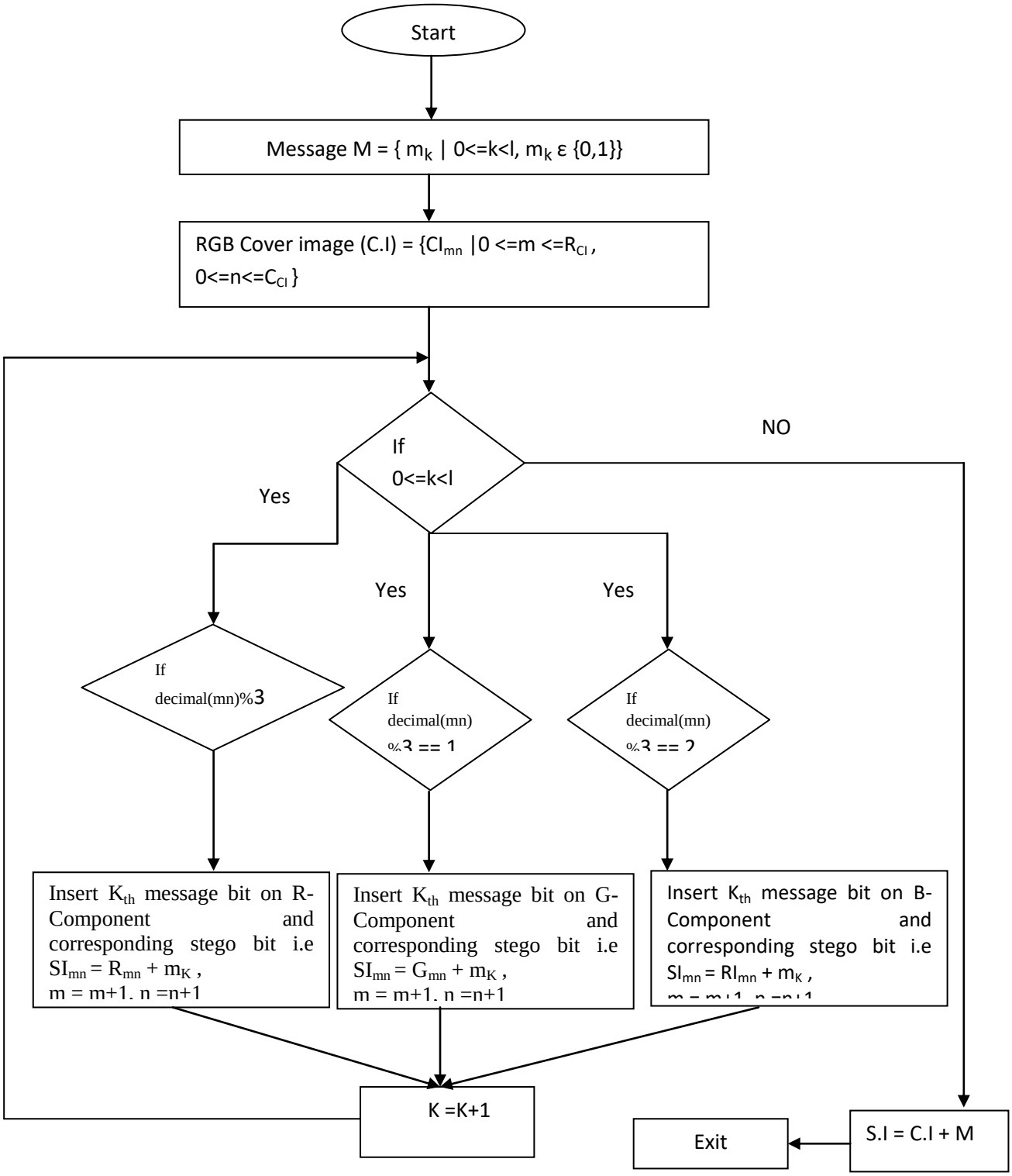

Fig. 1 Insertion Flowchart

ISSN: 2454-4248
479 – 483

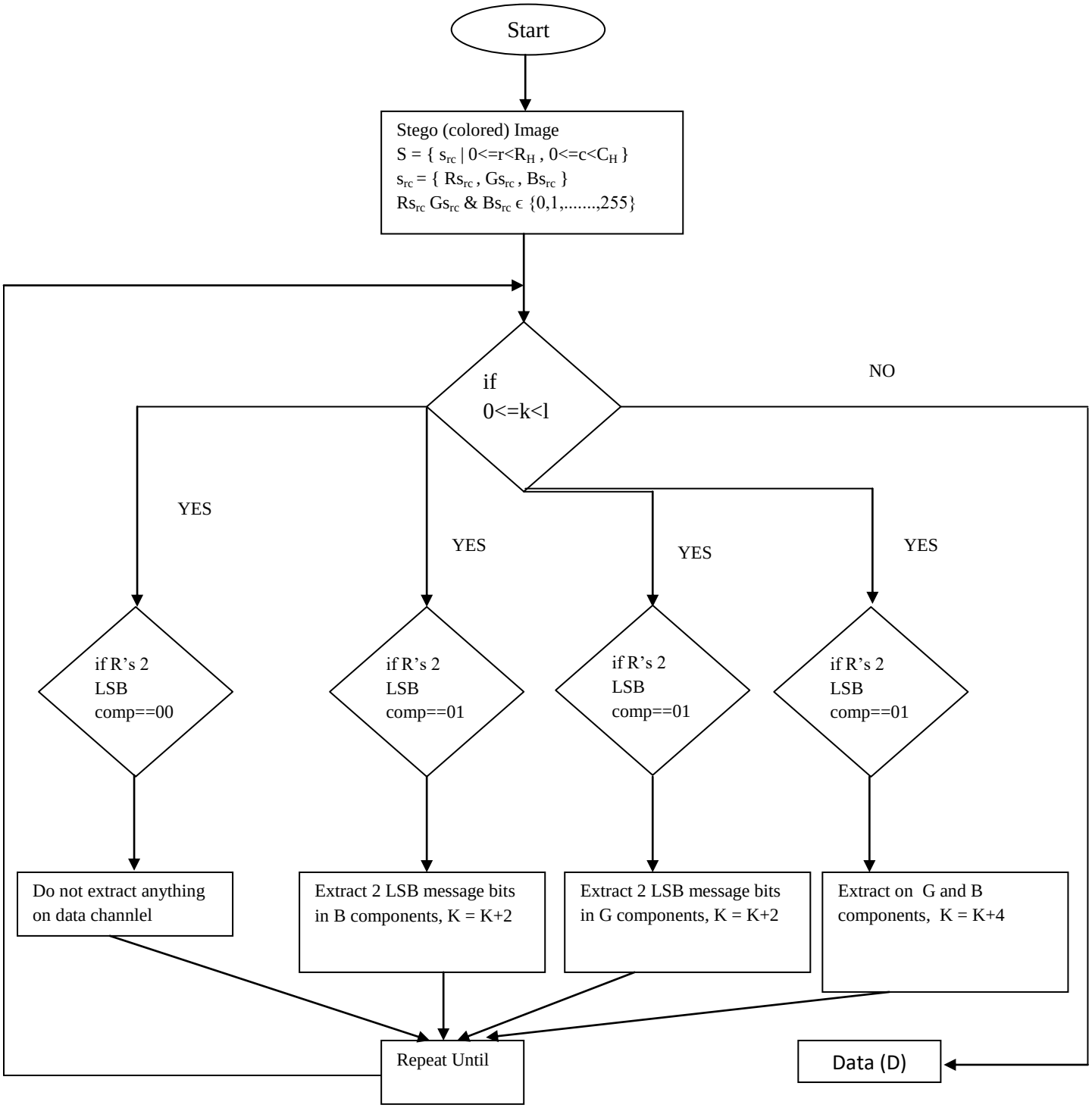

Fig.2 Retrieval Flowchart

ISSN: 2454-4248
479 – 483

Table 1 512*512 Host and Stego images

Sr. No	Host Images	Stego-images		
		Hiding 4KB data	Hiding 8KB data	Hiding 16KB data
Image 1				
Image 2				
Image 3				
Image 4				
Image 5				
Image 6				
Image 7				
Image 8				

Table 2 Shows MAE and MSE of 512*512 Stego-images

Image No.	Data Size = 4KB		Data Size = 8KB		Data Size = 16KB	
	MAE	MSE	MAE	MSE	MAE	MSE
Image 1	0.0821	0.1452	0.0652	0.3332	0.1895	0.6312
Image 2	0.0725	0.1266	0.0568	0.3766	0.1956	0.7042
Image 3	0.0741	0.1342	0.0587	0.2858	0.1836	0.7366
Image 4	0.0845	0.1355	0.0698	0.2652	0.1878	0.5242
Image 5	0.0789	0.1256	0.0611	0.2488	0.1925	0.5369
Image 6	0.0739	0.1468	0.0469	0.2493	0.1911	0.5274
Image 7	0.0856	0.1369	0.0789	0.2462	0.1901	0.6436
Image 8	0.0869	0.1438	0.0569	0.2654	0.1823	0.6894
Average of 100 images	**0.0798**	**0.1368**	**0.0617**	**0.2838**	**0.1890**	**0.6241**

IV. CONCLUSION

The experimental results are obtained over different images of dimension 512*512 for different data sizes and it is found that average MAE for 4KB, 8KB and 16KB data is 0.0798, 0.0617 and 0.1890 respectively whereas MSE obtained for 4KB, 8KB and 16KB data is 0.1368, 0.2838 and 0.6241 respectively.

V. REFERENCES

[1] K. Joshi and R.Yadav, "*New Approach toward Data Hiding Using XOR for Image Steganography"* in the proceedings of IEEE, International Conference on Contemporary Computing (IC3), Pages: 1 – 6, Dec 2016.

[2] Al-Taani AT, Al-Issa AM (2009) A novel steganographic method for gray-level images. Int J comput Inform Syst Sci Eng 3:1 2009

[3] Cheng W-C, Pedram M (2004) Chromatic encoding: a low power encoding technique for digital visual interface. Consum Electron IEEE Trans 50:320-328

[4] Dumitreseu S, Wu X, Wang Z (2003) Detection of LSB steganography via sample pair analysis. Signal process IEEE Tarns 51:1995-2007

[5] K. Joshi, R. Yadav, S.Allwadhi, "Exploration of Least Significant Bit Based Watermarking and its Robustness against Salt and Pepper Noise" in Journal of World Academy of Science Engineering and Technology (WASET), Vol 10, No 7, Paper No. 213 Year 2016.

[6] Chang C-C, Hsaio J-Y, Chan C-S "Finding optimal least-significant-bit substitution in image hiding by dynamic Programming Strategy" Pattern Recogn 36:1583-1595, 2003

[7] Thien C-C, Lin J-C, "A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function", PatternRecong 36:2875-2881

[8] G. Chugh, R.Yadav, R.Saini, "A new Image Steganographic Approach Based on Mod Factor for RGB images" International Journal of Signal Processing, Image Processing and Pattern Regcognition, vol. 7 no. 3 (2014). pp 27-44, 2014

[9] K. Joshi and S. Allwadhi, "Image Steganography Model for Medical Images Using GLM" in Journal of COMPUSOFT, An International journal of advanced computer technology, pp. 2120 – 2124 5(5), May – 2016 (Volume –V, Issue-V) ISSN:2320-0790

[10] E. Avci, T.Tuncer, D.Avci, "A Novel Reversible Data Hiding Algorithm Based on Probabilistic XOR Secret Sharing in Wavelet Transform Domain" Springer. DOI 10.1007/s 13369-016-2124-4, March 2016.

[11] K. Joshi, R. Yadav, S.Allwadhi, " PSNR and MSE based Investigation of LSB" in the proceedings of IEEE, International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), pp. no. 178 -183 on March 11-13, 2016

[12] N.V Rao and V.Kumari, "Watermarking in Medical Imaging for security and Authentication" Taylor & Francis DOI 10.1080/19393555.2011.561154, pp 148-155 vol. 20, 2011

[13] M. Aziz, M.H Tayarani-N and M. Afsar, "A cycling chaos-based crptic-free algorithm for image steganography" Nonlinear Dyn. Vol 80. No. 3. pp 1271-1290, 2015.

[14] S. Allawadhi, S.Dhingra, "Steganography Techniques: A Survey" International Journal of Latest Trends in Engineering and Technology, pp 258-263, Vol. 8, 2017.

[15] K. Joshi, R. Yadav, "A new LSB-S image steganography method blend with Cryptography for secret communication", 2015 Third International Conference on Image Information Processing (ICIIP), pp. 86-90, 2015.

[16] K. Joshi, P Dhankhar, R. Yadav, "A new image steganography method in spatial domain using XOR", 2015 Annual IEEE India Conference (INDICON), pp1 – 6, 2015.

[17] Kamaldeep Joshi, Rajkumar Yadav, and Gaurav Chawla. "An Enhanced Method for Data Hiding Using 2-Bit XOR in Image Steganography." International Journal of Engineering and Technology 8.6 (2016).

[18] Anamika Saini, Kamaldeep Joshi, and Sachin Allawadhi. "A Review on Video Steganography Techniques." International Journal of Advanced Research in Computer Science 8.3 (2017).

[19] Joshi, Kamaldeep, Rajkumar Yadav, and Ashok Kumar Yadav. "An Additive Watermarking Technique in Gray Scale Images Using Discrete Wavelet Transformation and Its Analysis on Watermark Strength." World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering 10.7 (2016): 1428-1433.

[20] Joshi, Kamaldeep, and Rajkumar Yadav. "A LL Sub Band Based Digital Watermarking in DWT." IJ Engineering and Manufacturing volume 7, Issue 2, pp 50-63 (2017).