Data Hiding Using Green Channel as Pixel Value Indicator

Saad Ahmed *saad.jaffari@unifiedcrest.com*
Computer Systems Engineering Dept,
Mehran University of Engineering and Technology,
Jamshoro,71000, Pakistan

Rabeea Jaffari *rubeeajaff@gmail.com*
Software Engineering Dept,
Mehran University of Engineering and Technology,
Jamshoro,71000, Pakistan

Liaquat Ali Thebo *liaquat.thebo@faculty.muet.edu.pk*
Computer Systems Engineering Dept,
Mehran University of Engineering and Technology,
Jamshoro,71000, Pakistan

Abstract

Steganography is an art of hiding the existence of data that is it hides the secret message in the digital cover medium. This paper introduces an improved algorithm that uses pixel value indicator technique for the concealment of the secret message in most significant bits (MSBs) of the cover image. Here, Green channel serves as a pixel value indicator for hiding the secret message in 5th and 6th bits of Blue channel or Red channel of RGB cover image. If Green channel has even number of 1's, Blue channel is used for embedding the secret message otherwise Red channel is used for the embedding process. The experimental results of the proposed method are obtained using MATLAB R2017a. The experimental results obtained show that the stego-image formed is of great quality having high PSNR value and it provides good security and in distinguishability.

Keywords: Information Hiding, Steganography, MSB, LSB, Pixel Value Indicator.

1. INTRODUCTION

The advancement in digital technology has brought a revolution in the world by taking the world to a digital era. Exchange of information has become quite easy with every field of life being moved towards digitization. Banks, military, industries, hospitals and other fields have automated their processes with the aid of computers which makes the sensitive data of such systems vulnerable to hackers and unauthenticated users [1]. Such sensitive information if fallen in the wrong hands can lead to destruction and therefore securing such information has turned into a challenging task which can be addressed using a technique called Steganography.

The word "Steganography" is a derivative from a Greek word, 'Steganos' meaning covered and 'Graptos' meaning writing, which means covered writing. The use of this technique dates back to 440 BC. Some of the steganographic techniques at that time used for sending secret messages were scalp of a person, invisible ink, tablets made up of wax and so on. Nowadays, digital approaches are being used for steganography. The steganographic techniques are being implemented in the areas such as identification of piracy in digital content, computer forensics, tracing internet criminal actions and so on [2].

Using steganography, not only the message but its very existence is also concealed from unauthorized users. Thus, a steganographic technique succeeds if it does not attract the attention of unauthorized users. Five parameters are there that mainly express the success of any steganographic algorithm namely: Indistinguishability, Robustness, High Capacity, Accurate

Extraction and High PSNR (Peak Signal to Noise Ratio) value. This research uses PSNR values to calculate the efficiency of proposed steganographic algorithm.

The paper is structured as follows: segment II gives the overall reflections, segment III covers the literature review, segment IV is regarding the ground works for this research, segment V holds the proposed methodology followed by segment VI which holds experimental results of the proposed method. Lastly, the concluding notes are presented in segment VII.

2. OVERALL REFLECTIONS

Cryptography deals with the security of data similar to steganography but it still has some ambiguities that led to the introduction of steganographic techniques. Following are some of the reasons to use steganography in place of cryptography:

- In cryptography the encrypted message attracts the attention of unauthenticated users whereas the use of steganography avoids such unwanted attraction during data transmission.
- The attacks on security systems for hacking the system and hijacking the confidential data takes new forms as technologies matures itself. Thus, steganography delivers benefits over cryptography.

3. SURVEY OF LITERATURE

3.1 Least Significant Bit (LSB) Technique

LSB (Least Significant Bit) is the most common method for concealing the existence of secret message in the LSB of the cover medium because of which the distortions created are negligible. In LSB algorithm [3], the secret message and the cover image are changed into binaries and then secret message is embedded in the LSBs of the cover image, this embedding procedure does not end until every LSB of cover image is utilized or all the secret message bits aren't embedded in the cover image. In this method [4], an improvement to the classic LSB technique is proposed in which some extra bits are embedded to make the stego-image's histogram look similar to that of original image. This approach prevents the histogram attack in the embedding procedure of LSB. According to [5], a steganographic technique proposed consisting of two approaches. In first approach, the image is protected by converting the image into an encrypted text using an algorithm named S-DES and secret key and then concealing this encrypted text into different image while the second approach protects the image by means of S-DES algorithm and a secret key. The method discussed in [6], is an integration of two different techniques namely MP (Matrix Pattern) and LSB (Least Significant Bit) method, in which the secret message is concealed inside the matrix blocks. Research at [7] gives a survey on different steganography techniques for images in spatial and transform domains and the survey of steganalysis techniques that are for the detection of secret message in the image. [8], [9] provide a survey for the LSB embedding techniques.

3.2 Pixel Value Indicator Technique (PVI)

This approach uses LSB of one of the color channels Red, Green or Blue of a color image as an indicator for secret message in the other two-color channels. The bits that perform the indicating process are normally random in nature (depend on the type of the image). A lot of work in this regard has been done some of which is discussed as follow. In the PVI technique discussed in [10], the bit of secret message is hidden in the LSB of blue or green channel depending on the X-ORed values of red channel and secret key. Research in [11] discusses the embedding of a binary image in the RGB image. In this approach the starting two bits select the color channel in which secret message is present, 4th and 5th bit selects the difference in the current pixel and the next stego pixel (stego image pixel) and the 7th and 8th bits decide the number of total bits of the secret message to be embedded. This procedure is good against SPA (Sample and Pair Attack) even though the hiding size is not very good. Another technique as discussed in paper [12] uses color image that first splits into RGB channel resulting in the generation of the matrix of the LSBs of the color channels, next the LSBs of Green colored channel are X-ORed with the chosen control message after which the secret message bits are embedded either in Red or Blue channel. This approach also uses cryptographic Algorithm such as RSA (Rivset-Shamir-Adleman) for the prevention of copying the secret message by unwanted users.

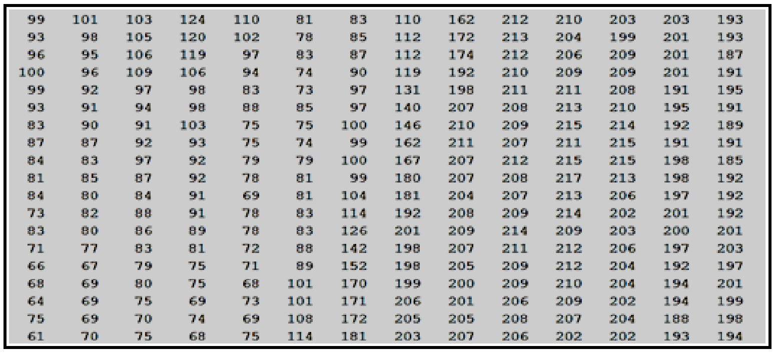
3.3 Most Significant Bit (MSB) Technique

MSB technique as the name implies uses the most significant bits (5-8) for hiding messages in the cover images. According to the research in [13], 5th bit of the cover image is for hiding the secret message by using a method known as bit differencing on 5th and 6th bits. If the result that is obtained after differencing of 5th and 6th is not same as the secret message bit, then the bit of the cover image is altered. In many situations, hackers are aware of LSBs and used it for the extraction of the secret message so the use of MSB in this approach makes it much more secure. Another MSB technique in [14] conceals the secret message by means of 1-bit MSB in chaotic manner with the secret image key. 8x8 size matrix blocks are taken from the cover image with the secret key in first block to determine next upcoming position in the image. Research in [15] presents a technique where the secret message is embedded in the MSB of cover image by using LSB of the cover image as an indicator. In [16], the embedding of secret message takes place in bits such as 4th or 5th bit of pixel. This method forms three-pixel groups based on the pixel values which are used for choosing pixels for 4th or 5th bit for embedding purpose. OPAP (Optimal Pixel Adjustment Process) is also used to lessen distortions that are caused due to the embedding procedure. In [17], a method is proposed according to which one bit per pixel is concealed in encoded images via preprocessing the image to evade errors which revamps the quality of reformed images while in [18], an efficient and dynamic embedding algorithm is proposed that not only hides the secret data but also makes secret code breaking a good annoyance for the attacker and represents an extraction algorithm that effectively extracts the entire secret message without any loss of a single data. Research techniques in [19], categorize different image steganography methods in addition to giving synopsis, importance and trials of steganography procedures. [20] uses two approaches namely Pixel Value Indicator and MSB embedding for splitting the color image in Red, Green and Blue channels. Pixels of Red channel are used as pixel indicator and the embedding takes place in the 5th and 6th bit of either Blue or Green channel depending upon the situation that whether the number of ones in Red channel is even or odd respectively. [21] in this research a reversible data hiding technique that is based on Neighbor Mean Interpolation (NMI) using the R-weighted coding method. [22], in this research a method is proposed that utilizes the pixel value indicator method to hide the secret message in the MSBs of the cover file. [23], In this research an algorithm is proposed that encodes the secret message bits before implanting it in the LSBs of the cover file. The implanting and the encoding process is done on the basis of MSB values of the RGB and on the concept of odd and even parities for that pixels. [24], In this paper, pixel value differencing has been used for implanting the data in the RGB image. Moreover, for providing more security, different number of bits are used for different pixels. [25], in the approach, an improved method for LSB substitution has been proposed. [26], in this paper a closed loop computing framework is proposed. [27], in this paper a novel method has been introduced that conceals the data within the transform domain of the RGB images.

4. GROUND WORKS

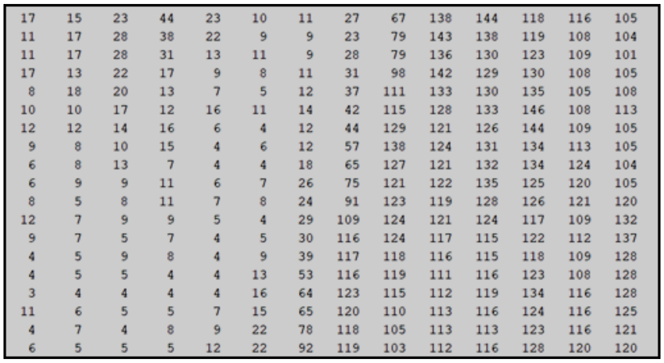
4.1 Matrices of Color Channels of Image

This section covers the ground works that are needed before implementing the proposed algorithm. The cover image is split into RGB channels and a portion of the Red, Green and Blue channels is shown in Figure 1, Figure 2 and Figure 3 respectively.



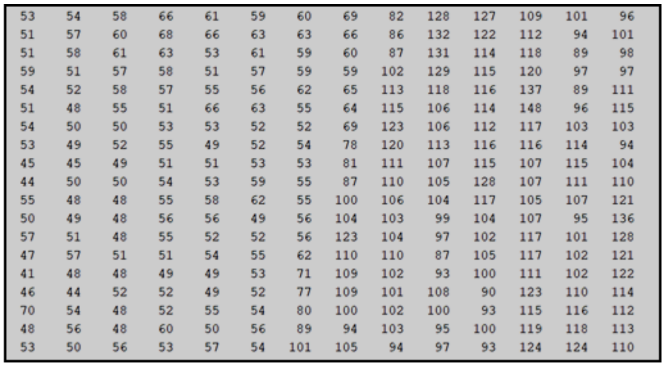
99	101	103	124	110	81	83	110	162	212	210	203	203	193
93	98	105	120	102	78	85	112	172	213	204	199	201	193
96	95	106	119	97	83	87	112	174	212	206	209	201	187
100	96	109	106	94	74	90	119	192	210	209	209	201	191
99	92	97	98	83	73	97	131	198	211	211	208	191	195
93	91	94	98	88	85	97	140	207	208	213	210	195	191
83	90	91	103	75	75	100	146	210	209	215	214	192	189
87	87	92	93	75	74	99	162	211	207	211	215	191	191
84	83	97	92	79	79	100	167	207	212	215	215	198	185
81	85	87	92	78	81	99	180	207	208	217	213	198	192
84	80	84	91	69	81	104	181	204	207	213	206	197	192
73	82	88	91	78	83	114	192	208	209	214	202	201	192
83	80	86	89	78	83	126	201	209	214	209	203	200	201
71	77	83	81	72	88	142	198	207	211	212	206	197	203
66	67	79	75	71	89	152	198	205	209	212	204	192	197
68	69	80	75	68	101	170	199	200	209	210	204	194	201
64	69	75	69	73	101	171	206	201	206	209	202	194	199
75	69	70	74	69	108	172	205	205	208	207	204	188	198
61	70	75	68	75	114	181	203	207	206	202	202	193	194

FIGURE 1: Red Channel Matrix.



17	15	23	44	23	10	11	27	67	138	144	118	116	105
11	17	28	38	22	9	9	23	79	143	138	119	108	104
11	17	28	31	13	11	9	28	79	136	130	123	109	101
17	13	22	17	9	8	11	31	98	142	129	130	108	105
8	18	20	13	7	5	12	37	111	133	130	135	105	108
10	10	17	12	16	11	14	42	115	128	133	146	108	113
12	12	14	16	6	4	12	44	129	121	126	144	109	105
9	8	10	15	4	6	12	57	138	124	131	134	113	105
6	8	13	7	4	4	18	65	127	121	132	134	124	104
6	9	9	11	6	7	26	75	121	122	135	125	120	105
8	5	8	11	7	8	24	91	123	119	128	126	121	120
12	7	9	9	5	4	29	109	124	121	124	117	109	132
9	7	5	7	4	5	30	116	124	117	115	122	112	137
4	5	9	8	4	9	39	117	118	116	115	118	109	128
4	5	5	4	4	13	53	116	119	111	116	123	108	128
3	4	4	4	4	16	64	123	115	112	119	134	116	128
11	6	5	5	7	15	65	120	110	113	116	124	116	125
4	7	4	8	9	22	78	118	105	113	113	123	116	121
6	5	5	5	12	22	92	119	103	112	116	128	120	120

FIGURE 2: Green Channel Matrix.



53	54	58	66	61	59	60	69	82	128	127	109	101	96
51	57	60	68	66	63	63	66	86	132	122	112	94	101
51	58	61	63	53	61	59	60	87	131	114	118	89	98
59	51	57	58	51	57	59	59	102	129	115	120	97	97
54	52	58	57	55	56	62	65	113	118	116	137	89	111
51	48	55	51	66	63	55	64	115	106	114	148	96	115
54	50	50	53	53	52	52	69	123	106	112	117	103	103
53	49	52	55	49	52	54	78	120	113	116	116	114	94
45	45	49	51	51	53	53	81	111	107	115	107	115	104
44	50	50	54	53	59	55	87	110	105	128	107	111	110
55	48	48	55	58	62	55	100	106	104	117	105	107	121
50	49	48	56	56	49	56	104	103	99	104	107	95	136
57	51	48	55	52	52	56	123	104	97	102	117	101	128
47	57	51	51	54	55	62	110	110	87	105	117	102	121
41	48	48	49	49	53	71	109	102	93	100	111	102	122
46	44	52	52	49	52	77	109	101	108	90	123	110	114
70	54	48	52	55	54	80	100	102	100	93	115	116	112
48	56	48	60	50	56	89	94	103	95	100	119	118	113
53	50	56	53	57	54	101	105	94	97	93	124	124	110

FIGURE 3: Blue Channel Matrix.

5. METHODOLOGY

The proposed methodology uses two techniques named as Pixel Value Indicator (PVI) and MSB embedding. The Pixel Value Indicator technique is used to implant the secret message in 5th and 6th bits of the Red or Blue channel of the cover image where Green channel is used as the indicator. Following are the steps that are used for embedding the secret message in the cover image.

5.1 Embedding Algorithm

The embedding algorithm is discussed below and is depicted in Figure 4.

- Select cover image and secret message.
- Divide the cover image in Red, Green and Blue channels.

- For each pixel in the Green channel of cover image, repeat steps 4 and 5 until secret message is embedded.
- If number of 1's in Green channel is even, place the secret message bits in 5th and 6th bits of blue channel.
- If number of 1's odd is Green channel, place the secret message bits in 5th and 6th bits of red channel.
- Recombine the color channels to form the stego-image.

5.2 Extracting Algorithm

The extracting algorithm is discussed below and is depicted in Figure 5.

- Read the stego-image
- Divide the stego-image in Red, Green and Blue channels.
- For each pixel in the Green channel of stego-image, repeat step 4 and 5 till secret message is extracted.
- If number of 1's in Green channel is even, read the secret message bits at 5th and 6th bit of Blue channel.
- If number of 1's in Green channel is odd, read the secret message bits at 5th and 6th bit of Red channel.
- Write the secret message on the file.

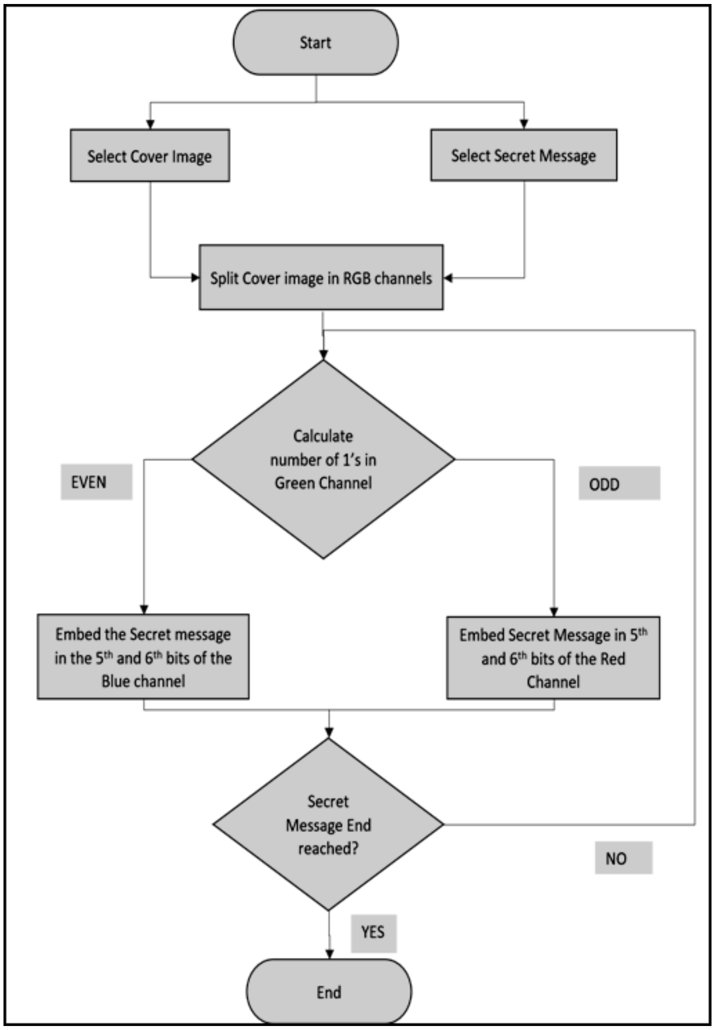

Start
Select Cover Image
Select Secret Message
Split Cover image in RGB channels
Calculate number of 1's in Green Channel
EVEN
ODD
Embed the Secret message in the 5th and 6th bits of the Blue channel
Embed Secret Message in 5th and 6th bits of the Red Channel
Secret Message End reached?
NO
YES
End

FIGURE 4: Flow Chart of Embedding Procedure.

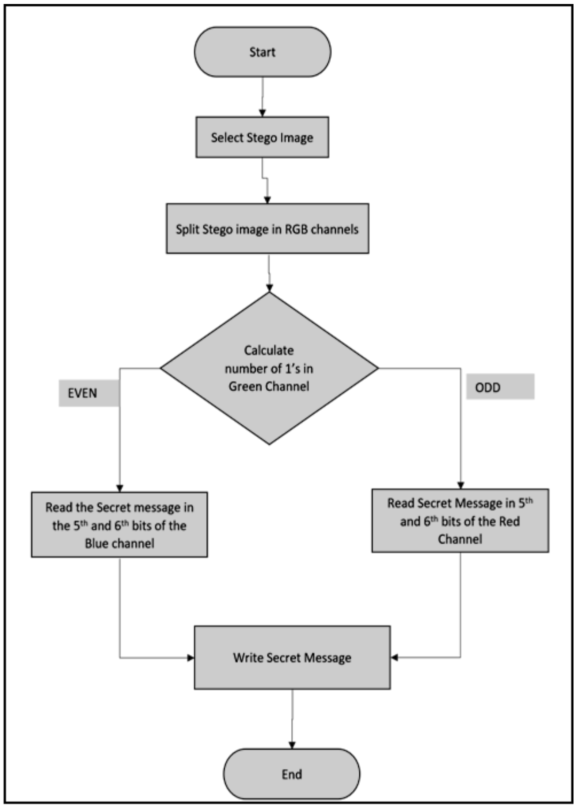

Start
Select Stego Image
Split Stego image in RGB channels
Calculate number of 1's in Green Channel
EVEN
ODD
Read the Secret message in the 5th and 6th bits of the Blue channel
Read Secret Message in 5th and 6th bits of the Red Channel
Write Secret Message
End

FIGURE 5: Flow Chart of Extracting Procedure.

6. EXPERIMENTAL RESULTS

The proposed method is implemented using MSB technique in MATLAB R2017a. Images that are used for the experiments are Lena.png 512x512x3, Baboon.png 512x512x3, Peppers.tif 512x512x3 and galaxy.jpeg 537x800x3 as shown in Figures 6-7. The proposed approach is different from [10] and [11] because both of those techniques use LSBs this approach is based on MSB.

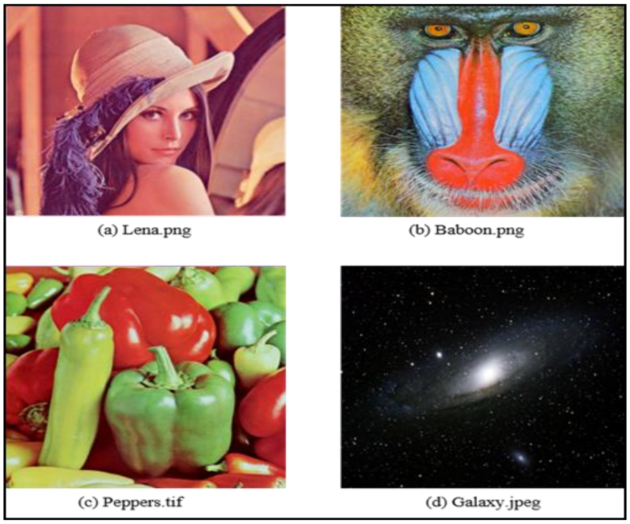

(a) Lena.png
(b) Baboon.png
(c) Peppers.tif
(d) Galaxy.jpeg

FIGURE 6: Cover Images.

(a) Lena Stego Image

(b) Baboon Stego Image

(c) Peppers Stego Image

(d) Galaxy Stego Image

FIGURE 7: Stego Images.

Figure 7 illustrates that the quality of image is not altered by inserting the secret message. Additionally, the use of 2 bits that is the 5th and 6th bit of each pixel delivers decent payload capacity to this technique and increases its security.

6.1 PSNR and MSE

The PSNR and MSE values obtained from each of the stego images are shown in Table 1.

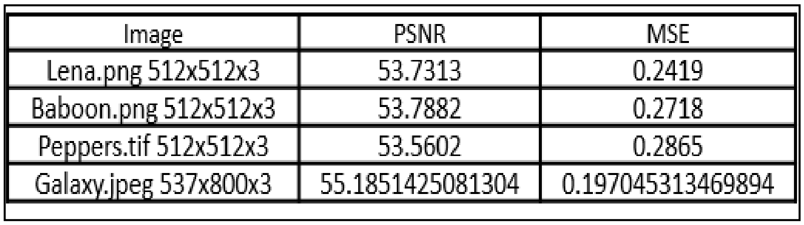
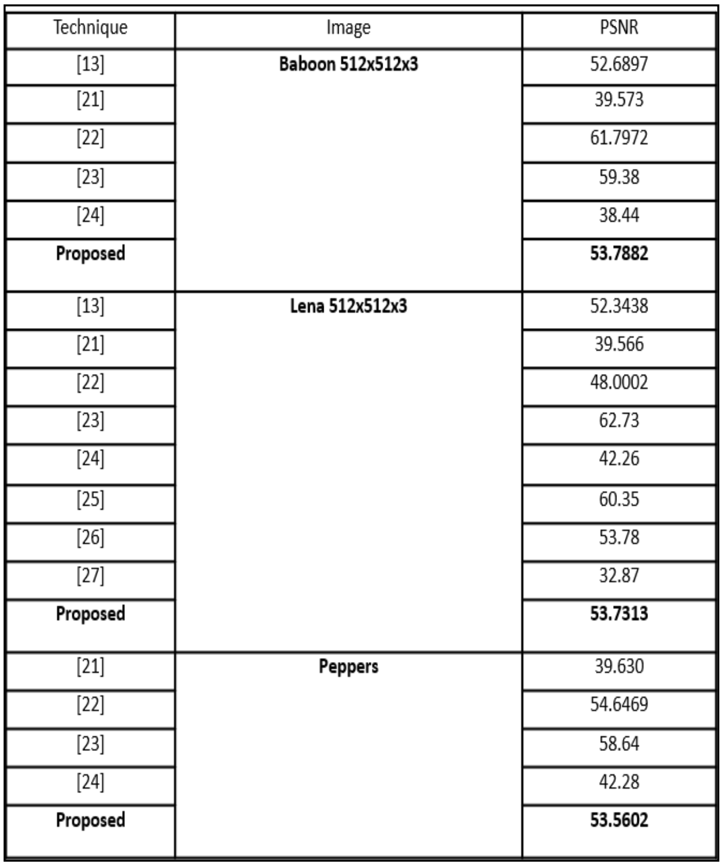


Image	PSNR	MSE
Lena.png 512x512x3	53.7313	0.2419
Baboon.png 512x512x3	53.7882	0.2718
Peppers.tif 512x512x3	53.5602	0.2865
Galaxy.jpeg 537x800x3	55.1851425081304	0.197045313469894

TABLE 1: PSNR and MSE.

The PSNR and MSE results of the proposed method are quite decent as their values are above 45 decibel (db) and the squared error values do not exceed 0.5. A comparison of the PSNR values obtained from [13] and the proposed method is depicted in Table 2 below.



Technique	Image	PSNR
[13]	**Baboon 512x512x3**	52.6897
[21]		39.573
[22]		61.7972
[23]		59.38
[24]		38.44
Proposed		**53.7882**
[13]	**Lena 512x512x3**	52.3438
[21]		39.566
[22]		48.0002
[23]		62.73
[24]		42.26
[25]		60.35
[26]		53.78
[27]		32.87
Proposed		**53.7313**
[21]	**Peppers**	39.630
[22]		54.6469
[23]		58.64
[24]		42.28
Proposed		**53.5602**

TABLE 2: Comparison Table.

6.2 Security

The proposed method is strong against statistical strikes as the value of mean doesn't differ too much for stego-image and original image as shown in Table 3. Moreover, it is robust against histogram steganalysis as it can be seen in Figure 8 and Figure 9 that the histogram of proposed algorithm is similar to that of the original image and doesn't make any detectable fluctuations in the histogram of stego-images when related with the histogram of original image.

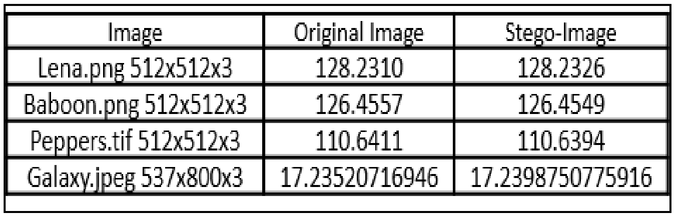


Image	Original Image	Stego-Image
Lena.png 512x512x3	128.2310	128.2326
Baboon.png 512x512x3	126.4557	126.4549
Peppers.tif 512x512x3	110.6411	110.6394
Galaxy.jpeg 537x800x3	17.23520716946	17.2398750775916

TABLE 3: Mean Values.

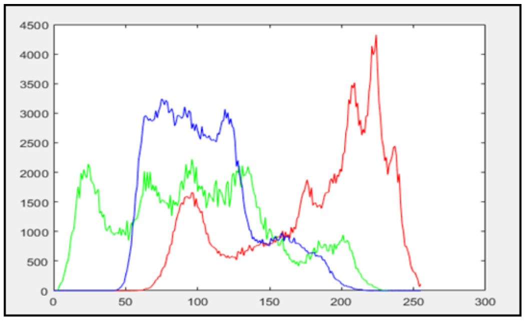


FIGURE 8: Histogram of Original Image Lena.

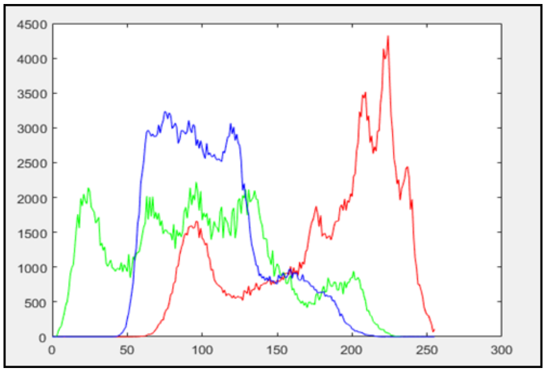


FIGURE 9: Histogram of Stego Image Lena.

7. CONCLUSION

This research presented a steganographic technique where MSBs were used to embed secret message in the cover image to increase the security of the message. The PSNR values obtained for the proposed method were of high quality and showed the effectiveness for the proposed method in terms of security and payload capacity. The MSE values showed that the error is not much high to cause distortion and the mean values of the original and stego-images are not of high difference as they did not vary too much from each other. It was evident from the results that this technique is good in terms of security as compared to its former counter parts.

8. REFERENCES

[1] Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. (2008, March). Biometric inspired digital image steganography. In Engineering of Computer Based Systems, 2008. ECBS 2008. 15th Annual IEEE International Conference and Workshop on the (pp. 159-168). IEEE.

[2] Sajedi, H., & Jamzad, M. (2008, July). Cover selection steganography method based on similarity of image blocks. In Computer and Information Technology Workshops, 2008. CIT Workshops 2008. IEEE 8th International Conference on (pp. 379-384). IEEE.

[3] G. Sudha K. Thangadurai, "An analysis of LSB Based Image Steganography Techniques," in 2014 International Conference on Computer Communication and Inforatics(ICCI-2014), Coimbatore,India , 2014.

[4] Ghazanfari, K., Ghaemmaghami, S., & Khosravi, S. R. (2011, November). LSB++: an improvement to LSB+ steganography. In TENCON 2011-2011 IEEE Region 10 Conference (pp. 364-368). IEEE.

[5] Sharma, V. (2015, December). Two new approaches for image steganography using cryptography. In Image Information Processing (ICIIP), 2015 Third International Conference on (pp. 202-207). IEEE.

[6] Nilizadeh, A., & Nilchi, A. R. N. (2016, March). A novel steganography method based on matrix pattern and LSB algorithms in RGB images. In Swarm Intelligence and Evolutionary Computation (CSIEC), 2016 1st Conference on(pp. 154-159). IEEE.

[7] Chanu, Y. J., Tuithung, T., & Singh, K. M. (2012, March). A short survey on image steganography and steganalysis techniques. In Emerging trends and applications in computer science (NCETACS), 2012 3rd national conference on (pp. 52-55). IEEE.

[8] Jois, A., & Tejaswini, L. (2016, March). Survey on LSB Data hiding techniques. In Wireless Communications, Signal Processing and Networking (WiSPNET), International Conference on (pp. 656-660). IEEE.

[9] Ashwin, S., Ramesh, J., Kumar, S. A., & Gunavathi, K. (2012, December). Novel and secure encoding and hiding techniques using image steganography: A survey. In Emerging Trends in Electrical Engineering and Energy Management (ICETEEEM), 2012 International Conference on (pp. 171-177). IEEE.

[10] Karim, S. M., Rahman, M. S., & Hossain, M. I. (2011, December). A new approach for LSB based image steganography using secret key. In Computer and Information Technology (ICCIT), 2011 14th International Conference on(pp. 286-291). IEEE.

[11] Gupta, K., & Sharma, M. (2014, November). Signature hiding standard: Hiding binary image into RGB based image. In Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies (p. 71). ACM.

[12] Zhou, X., Gong, W., Fu, W., & Jin, L. (2016, June). An improved method for LSB based color image steganography combined with cryptography. In Computer and Information Science (ICIS), 2016 IEEE/ACIS 15th International Conference on (pp. 1-4). IEEE.

[13] Islam, A. U., Khalid, F., Shah, M., Khan, Z., Mahmood, T., Khan, A., ... & Naeem, M. (2016, August). An improved image steganography technique based on MSB using bit differencing. In Innovative Computing Technology (INTECH), 2016 Sixth International Conference on (pp. 265-269). IEEE.

[14] Sathisha, N., Madhusudan, G. N., Bharathesh, S., Babu, K. S., Raja, K. B., & Venugopal, K. R. (2010, July). Chaos based spatial domain steganography using MSB. In Industrial and Information Systems (ICIIS), 2010 International Conference on(pp. 177-182). IEEE.

[15] Dhannoon, B. N. (2013). An Indirect MSB Data Hiding Technique. Life Science Journal, 10(11s).

[16] Gupta, P. K., Roy, R., & Changder, S. (2014, January). A secure image steganography technique with moderately higher significant bit embedding. In Computer Communication and Informatics (ICCCI), 2014 International Conference on (pp. 1-6). IEEE.

[17] Puteaux, P., Trinel, D., & Puech, W. (2016, December). High-capacity data hiding in encrypted images using MSB prediction. In Image Processing Theory Tools and Applications (IPTA), 2016 6th International Conference on (pp. 1-6). IEEE.

[18] Mahjabin, T., Hossain, S. M., & Haque, M. S. (2012, December). A block based data hiding method in images using pixel value differencing and LSB substitution method. In Computer and Information Technology (ICCIT), 2012 15th International Conference on (pp. 168-172). IEEE.

[19] Kaur, S., Bansal, S., & Bansal, R. K. (2014, March). Steganography and classification of image steganography techniques. In Computing for Sustainable Global Development (INDIACom), 2014 International Conference on (pp. 870-875). IEEE.

[20] Sharma, A., Poriye, M., & Kumar, V. (2017). A Review of Image Steganography Techniques: Development Trends to Enhance Performance. International Journal of Advanced Research in Computer Science, 8(5).

[21] .Y. Yalman, F. Akar, and I. Erturk, "An image interpolation based reversible data hiding method using R-weighted coding," IEEE 13th International Conference on Computational Science and Engineering, pp. 346-350, 2010

[22] Sharma, Aditi, Monika Poriye, and Vinod Kumar. "A Secure Steganography Technique Using MSB." International Journal of Emerging Research in Management and Technology 6.6 (2018): 208-214.

[23] Mandal Ashish Kumar and M N M Kahar, “Variant of LSB Steganography Algorithm for Hiding Information in RGB Images”, International Journal of Signal Processing, Image Processing and Pattern Recognition, pp. 35-48, 2017.

[24] Mandal, J. K., and Debashis Das. "Colour image steganography based on pixel value differencing in spatial domain." International journal of information sciences and techniques 2.4 (2012).

[25] Islam, Md Olioul. "A high embedding capacity image steganography using stream builder and parity checker." Computer and Information Technology (ICCIT), 2012 15th International Conference on. IEEE, 2012.

[26] Lin, Guo-Shiang, Yi-Ting Chang, and Wen-Nung Lie. "A framework of enhancing image steganography with picture quality optimization and anti-steganalysis based on simulated annealing algorithm." IEEE Transactions on Multimedia 12.5 (2010): 345-357.

[27] Abduallah, Wafaa Mustafa, Abdul Monem S. Rahma, and Al-Sakib Khan Pathan. "Mix column transform based on irreducible polynomial mathematics for color image steganography: A novel approach." Computers & Electrical Engineering 40.4 (2014): 1390-1404.