*International Journal of*
*Emerging Research in Management &Technology*
*ISSN: 2278-9359 (Volume-6, Issue-6)*

**Research Article** | **June 2017**

# A Secure Steganography Technique Using MSB

**Aditi Sharma, Monika Poriye, Vinod Kumar**
Department of Computer Science and Applications, Kurukshetra University, Kurukshetra, Haryana, India

***Abstract-***

***Steganography is the process of hiding secret message into a cover medium to conceal the existence of the message. The redundant nature of image pixels make them suitable medium to hide secret information. In this paper, a new improved technique that uses pixel indicator method to hide secret data bits in most significant bits (MSBs) of the cover image is proposed. Moreover, a central portion of image is selected to hide secret message for more security. Here, red channel is used as an indicator to hide secret message in $5^{th}$ and $6^{th}$ bits of either green channel or blue channel of RGB image. If the number of 1's in red channel are even, green channel is used for embedding otherwise blue channel is used. The experimental results obtained by implementation of the proposed algorithm in MATLAB showed that the stego-images images are of high quality having high PSNR values. It provides better security and imperceptibility.***

***Keywords: Data hiding, LSB, Pixel Indicator Technique, Steganography, Stego-image.***

## I. INTRODUCTION

The advancement in digital technology with the advent of computers and internet technology has brought a revolution by transforming the world into a digital village. Exchange of information has become quite easy from any part of the world to another. Nowadays, every field of life is moving towards digitization. In banks, hospitals and industries, computers are used for the storage of confidential information which makes it vulnerable to third party interference and attacks [**1**] . This sensitive information of patients and bank accounts can be misused which is a major issue of concern. As a result, protection of one's private information has become a challenging issue.

The term Steganography is derived from a Greek word, Steganos meaning covered and Graptos meaning writing, which means hidden communication. In this technique, not only the message is kept secret but the existence of message is also concealed. Thus, the success of a steganographic technique depends upon the fact that it does not attract any attention when data is transmitted inside cover medium. The use of the technique in ancient times dates back to 440 BC. Physical techniques of steganography were used that time. For example secret message was sent on the scalp of a person, invisible ink was used to write secret messages and wax tablets crunched into tiny balls. At present, digital techniques are used for hiding information. Information can be hidden inside multimedia content like image, audio, video and text. There are mainly five parameters that define the effectiveness of any steganographic algorithm: Imperceptibility, Robustness, High Capacity, Accurate Extraction, high PSNR (Peak Signal to Noise Ratio). The applications of steganography include identification of piracy in digital content, computer forensics, tracking internet criminal activities [**2**]. These applications of steganography make it very important for security purpose in today's digital era. Consequently, researchers are attracted for constant research in this challenging field.

The rest of the paper is structured as follows: Section II provides the general considerations for steganography. Section III discusses literature review. In section IV, preliminaries used in our technique are described. The proposed method is explained in section V which is then followed by experimental results of the proposed algorithm in section VI. Finally, the concluding remarks are presented in Section VII.

## II. GENERAL CONSIDERATIONS

Cryptography is the classic method that provides data security. Although, it has some loopholes therefore it leads to the use of other methods to secure digital data. Steganography is one of them. Following are the considerations for the use of steganography:

1. In cryptography, the encrypted message attracts the attention of unwanted users due to encoded message while the main advantage in steganography is that it doesn't attract any unwanted attraction as the transmitted message appears normal.
2. The attacks on security systems for confidential data transfer take new forms as technologies change. Thus, Steganography provides advantages over cryptography.
3. Historical physical methods such as invisible ink, tiny pin punctures on specific characters motivated to introduce steganographic techniques to be used with computers. Thus, secret message is hidden inside digital images, audio files and covert network channels.

## III. LITERATURE REVIEW

### *A. LSB METHOD*

LSB is the most commonly used method to hide any secret information inside any medium as it leads to minimum distortion in cover medium. In LSB algorithm [**3**], the message and the cover image are converted into binary form that consists of bits. The LSB of the first pixel of image is replaced by the first bit of message. This process is repeated until all message bits are embedded in cover image or all LSBs of image are not used. This is the basic LSB method. A lot of work has been done on LSB method [**4**] [**5**] [**6**] [**7**]. A method in [**4**] is an improvement to existing LSB+ method which resists histogram attack in LSB embedding by embedding some extra bits to make histogram look like the original one. In this method, the overhead in previous method is removed by changing unused pixels such as to restore the frequency of bins. An approach was proposed in [**5**] where steganography was achieved in two ways. In first method, an image is secured directly by encrypting it using S-DES algorithm and secret key then embedding this encrypted text in some other image. In second method, image was encrypted directly using S-DES algorithm and image key. The methods have been implemented using MATLAB and experimental results proved them secure. From time to time, different methods have been used to increase the security and imperceptibility of the steganographic techniques. The next method is the combination of two different methods namely, Matrix Pattern (MP) and Least Significant Bit (LSB) where secret message is hidden inside blocks. [**8**] [**9**] present a survey on LSB techniques. Pixel Value Differencing (PVD) and Pixel Indicator techniques are mostly used in past research methods with LSB [**10**][**11**] [**12**].

### *B. PIXEL INDICATOR METHOD*

This technique uses least significant bits of one of the channels Red, Green or Blue as an indicator of data existence in the other two channels. The indicator bits are set randomly (based on the image nature) in the channel. In [**10**] , this approach was used where a bit of hidden information is placed in either LSB of blue or green matrix depending upon the x-or value of pixel of red matrix and predefined secret key. The results showed that the randomness in selecting pixels for embedding make the technique more secure. Another method in [**11**] embed binary image into RGB image. Here, first two bits decide the color of channel in which data is embedded and values of $4^{th}$ and $5^{th}$ bit decide the difference between current and next stego-pixel and $7^{th}$ and $8^{th}$ bit values decide the number of bits of hidden data that will be embedded. This technique is robust against Sample and Pair Attack (SPA) although hiding capacity is not the main concern. In [**12**], image is split into red, green and blue channels. Then, a matrix of the least significant bits of each Red, Green and Blue channel respectively is generated. Then, LSBs of green channel are X-ORed with randomly chosen control message. Then, resultant bits are hidden inside either blue or red channel. Cryptographic algorithm RSA is used for authentication to prevent forgery of hidden message.

### *C. CONCEPT OF MSB*

Some researchers tried to hide secret data bits in MSBs to enhance robustness and security. In [**13**], $5^{th}$ bit is used to hide secret message using bit differencing method based on $5^{th}$ and $6^{th}$ bit. If the difference obtained is not equal to the bit at secret message, the $5^{th}$ bit of cover image is changed accordingly. Usually hackers focus on LSB bits for secret data extraction but proposed method utilizes the MSB bits to make technique more secure and provides a base for more work on MSB data embedding. Another MSB based steganograpghy technique was proposed in [**14**] where secret data is hidden using 1-bit MSB in chaotic manner using secret key. 8*8 matrix blocks of equal size are taken in cover image with key in first block to determine next positions in image. An indirect MSB data hiding technique is presented in [**15**]. This idea focuses on indirect hiding of secret message in the MSB of cover image using LSBs as an indicator. Secret key is used to hide data. In [**16**], a method is proposed that embeds secret data in significantly higher bits such as $4^{th}$ or $5^{th}$ bit of pixel. According to pixel values, three groups of pixels are maintained which are used for selecting candidate pixels for $4^{th}$ or $5^{th}$ bit embedding. It also uses Optimal Pixel Adjustment Process to minimize visual distortion due to embedding. A method was proposed in [**17**] in which one bit per pixel is hidden inside encrypted images by preprocessing the image to avoid prediction errors which improves the quality of reconstructed images.

## IV. PRELIMINARIES

### 1. X-OR SECRET MESSAGE WITH PREDEFINED SECRET KEY

The secret message bits are x-ored with predefined secret key to increase security. The x-or of secret message bits is as shown in fig.1.

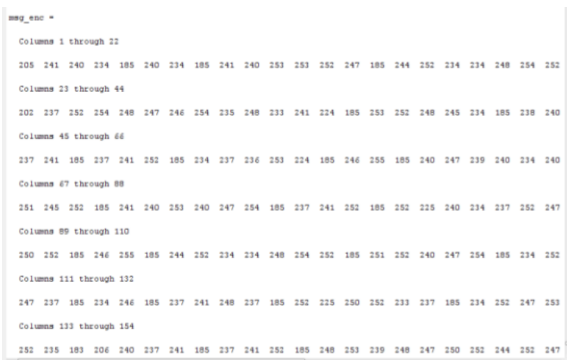



Fig. 1 : X-ored secret message with secret key

The message cannot be decrypted unless secret key will be known.

## 2. MATRIX FORMATION OF IMAGE

The cover image is read as input and split into RGB components. The matrix of each red, blue and green channel is formed to operate on their corresponding bits. A part of the matrix of red channel and green channel are shown as in fig. 2 and fig. 3.

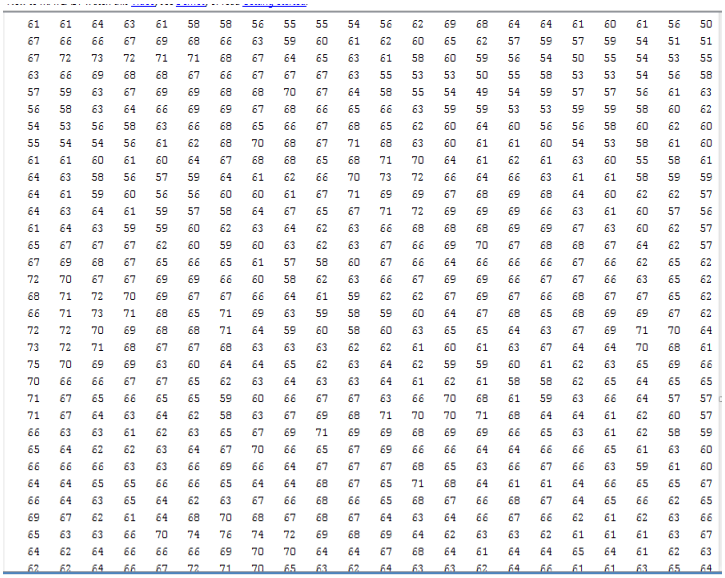


Fig.2: Red Channel Matrix

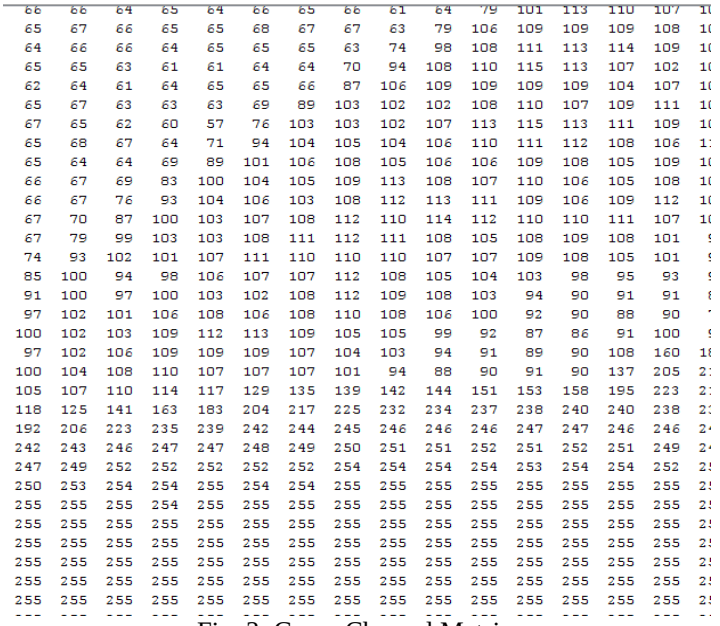


Fig. 3: Green Channel Matrix

## V. PROPOSED METHOD

The proposed methodology combines Pixel Value Indicator and MSB embedding. The pixel Indicator Technique is used to embed data bits in 5th and 6th bit of either green channel or blue channel where red channel is taken as indicator. The data embedding procedure of the proposed technique is as shown in fig 1. Following steps are followed to hide secret message bits inside cover image.

### *A. Encoding Algorithm:*

1. Select cover and secret message.
2. Secret message is X-ORed with secret key.
3. Split Red, Green and Blue channels of image.
4. Choose central portion of image.
5. For each pixel of 24-bit image, repeat steps 6 and 7 until secret message is embedded.
6. If number of 1's in red channel is even, place the secret data bit at 5th and 6th bit of green channel.
7. If number of 1's odd in red channel, place the secret data bits at 5th and 6th bit of blue channel.
8. Write the stego-image.

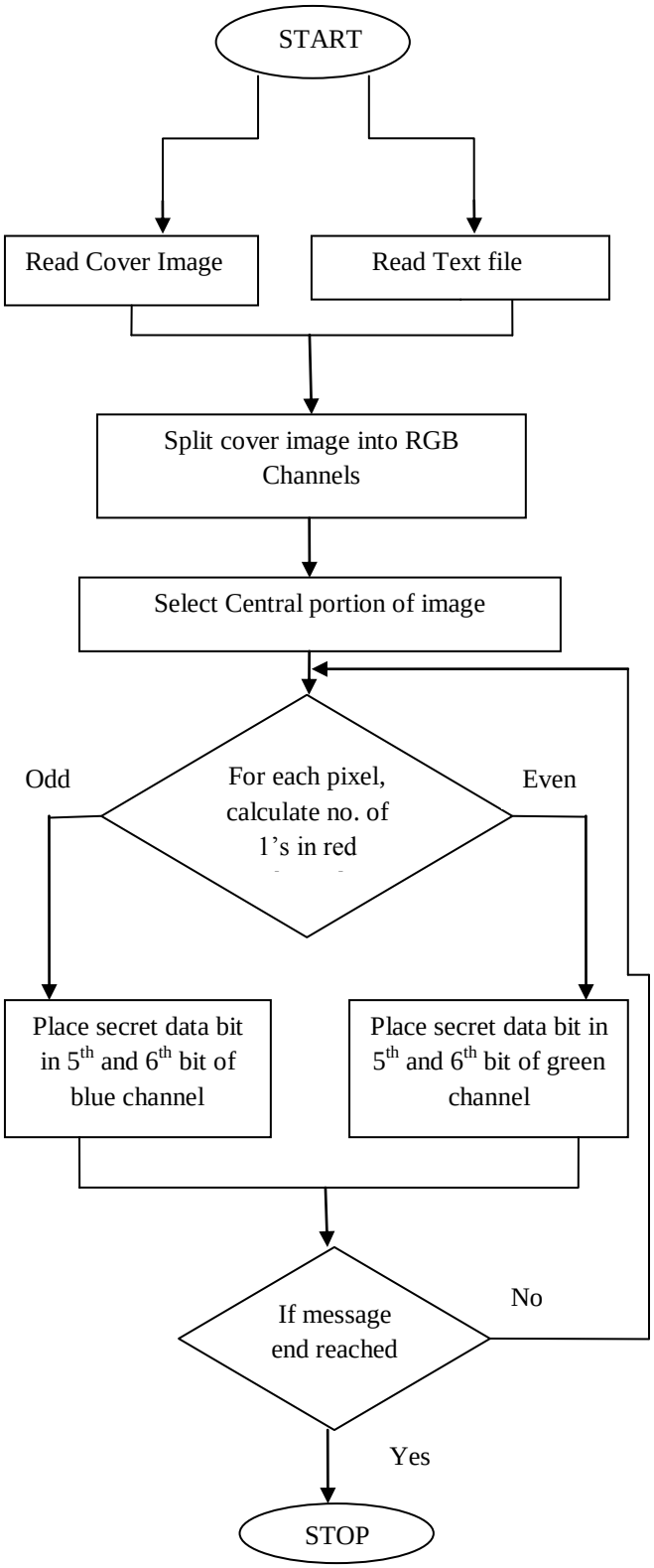



Fig. 4 Flowchart to hide information in cover image

***B. Decoding Algorithm:***

1. Read the stego-image.
2. Find the central portion of image.
3. Split Red, Green and Blue channels of image.
4. For each pixel of 24-bit image, repeat steps 5 and 6
5. If number of 1's even in red channel, read the $5^{th}$ and $6^{th}$ bit of green channel.
6. Otherwise, read the $5^{th}$ and $6^{th}$ bit of blue channel.
7. Write secret message into file.

This decoding algorithm follows the reverse steps of encoding procedure and provides accurate extraction of the encoded message.

## VI. EXPERIMENTAL RESULTS

The implementation of the proposed algorithm has been done using MATLAB as a tool. The images that have been used mostly in all steganographic experiments are used by us. These are: Color Lena 256×256×3, Color Baboon 1600×1008×3, Color Peppers 512×512×3, and Color Nature 2560×1600×3 as shown in Fig.5.

(a)Baboon Cover Image (b) Peppers Cover Image

(c) Lena Cover Image (d) Nature Cover Image

Fig. 5 Original Cover Images

A random text file is used as input for secret message. The resultant stego-images from our proposed work is shown in Fig. 6.

Fig. 6 Resultant Stego-Images

Fig.6 shows that the image quality is not affected by embedding thus, cannot be detected by naked eyes that there is any hidden message inside cover image. Moreover, the use of 2 bits of each pixel has provided good payload capacity to the technique and has increased the security as well. The PSNR values obtained for each stego- images are given in table.

### *A. PSNR*

The PSNR values obtained for different images are shown in Table I.

Table I. Results of Proposed Technique

| Cover Image | Size of cover image | PSNR |
|---|---|---|
| Lena.png | 256×256 | 48.0002 |
| Peppers.png | 512×512 | 54.6469 |
| Baboon.png | 1600×1008 | 61.7972 |
| Nature.png | 2560×1600 | 66.2866 |

The PSNR value of our method is greatly better as it has value above 40 db. Moreover, the value of PSNR increases as the size of cover image increases.

Table II. Comparison Table

| Technique | PSNR |
|---|---|
| [**13**] | 50.2918 |
| Proposed | 54.6469 |

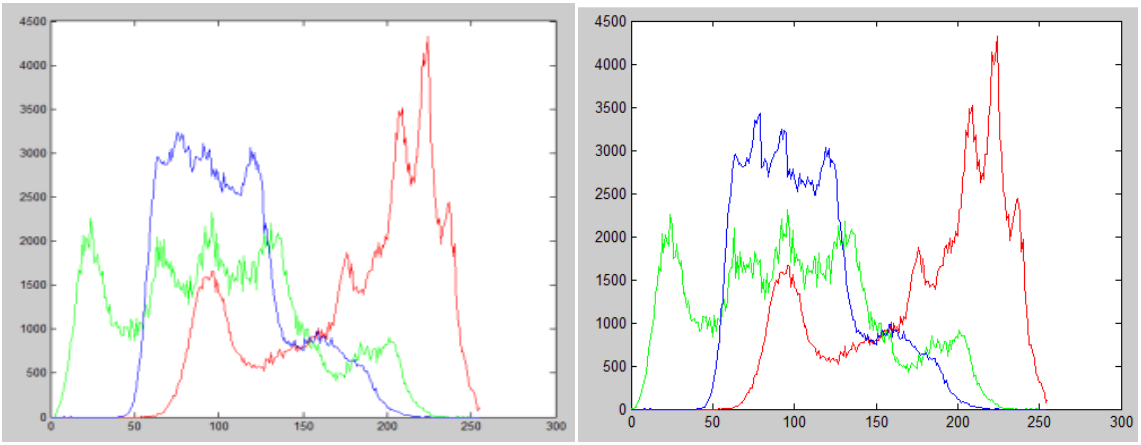
The comparison results against the Peppers color and Baboon color images (512×512) are shown in table I calculated for the same payload.

### *B. Security*

The technique is robust against statistical attacks as the value of mean doesn't vary for stego-image. It is resistant to cropping of images. Moreover, it is robust to histogram steganalysis as our algorithm doesn't make visible changes in the histogram of stego-images when compared with the histogram of original image.

Table II. Statistical Analysis Result

| | MEAN VALUES OF IMAGES | |
|---|---|---|
| | Original Image | Stego-image |
| Baboon | 100.0083 | 100.0778 |
| Lena | 128.2948 | 128.2948 |
| Peppers | 81.8180 | 81.9024 |
| Nature | 133.3884 | 133.3928 |




(a) (b)

Fig. 8: Histogram of (a) original Image (b) Stego-image

## VII. CONCLUSION

This work presented a steganographic strategy using color image as a cover medium. MSBs are used to conceal secret message inside cover to increase the security of the technique. Instead of embedding message starting from top left corner or bottom right, central portion is selected for embedding. This provides more robustness to the technique.
Furthermore, the PSNR values obtained from experimental results demonstrate the effectiveness of this strategy in terms of security and payload capacity as well. The experimental results show that the technique is better in terms of security than the previous techniques.

## REFERENCES

[1] J. Condell, K. Curran, P. Kevitt A. Cheddad, "Biometric Inspired Digital Image Steganography," in 15th Annual IEEE International Conference and Workshop on the Engineering of Computer Based Systems, 2008, pp. 159-167.

[2] M. Jamzad H. Sajedi, "Cover Selection Steganography Method based on Similarity of Image Blocks ," in IEEE 8th International Conference on Computer and Information Technology Workshops, 2008, pp. 379-384.

[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] S. Ghaemmaghami, S. Khosravi K. Ghazanfari, "LSB++ : An Improvement to LSB+ Steganography," in TENCON 2011- IEEE, pp. 364-368.

[5] Madhusudan Vipul Sharma, "Two new approaches for Image Steganography using Cruyptography," in International Conference on image information processing, 2015, pp. 202-207.

[6] A. Nilchi Amirfarhad Nilizadeh, "A novel Steganography method on Matrix Pattern and LSB algorithms in RGB Images," 2016.

[7] Themrichin Tuithung, Kh. Manglem Singh Yambern Jina Chanu, "A short survey on Image Steganography and Steganalysis Techniques," 2012.
[8] Tejaswini A. Jois, "Survey on LSB Data Hiding Techniques," in IEEE WiSPNET 2016 Conference, pp. 656-660.
[9] S. Aravind Kumar, J.Ramesh, K. Gunavathi S. Ahwin, "Novel and Secure Encoding and Hiding Techniques using Image Steganography:A Survey," in International Conference on Emerging Trends in Electrical Engineering and Energy Management, Coimbatore,India, 2012, pp. 171-177.
[10] Md. Saifur Rahman, Md. Ismail Hossain S.M. Masud Karim, "A new approach for LSB based Image Steganography using secret key," in Proceedin), Dhaka, Bangladesh, 2011.
[11] M. Sharma K.Gupta, "Signature Hiding Standard(Hiding Binary Image into RGB Based Image)," 2014.
[12] W. Gong , WenLong Fu, LianJing Jin Xinyi Zhou, "An improved method for LSB based color image steganography combined with cryptography," 2016.
[13] F. Khalid,M. Shah, Z. Khan ,T. Mahmood,A. Khan A. Islam, "An Improved Image Steganography Technique Based On MSB using Bit Differencing," IEEE, pp. 265-269, 2016.
[14] Madhusudan GN, Bharatesh S, K Suresh Babu, K raj, Venugopal N Sathisha, "Chaos Based Spatial Domain Steganograpghy using MSB," in 5th International Conference on Industrial and Information Systems, ICIIs, 2010, pp. 177-182.
[15] Dr. Ban N. Dhannoon, "An Indirect MSB Data Hiding Technique," Life Science Journal , pp. 263-266, 2013.
[16] R. Roy, S. Changder P. Gupta, "A secure Image Steganography Technique with Moderately Higher Significant Bit Embedding," in 2014 International Conference on Computer Communication Informatics(ICCCI-2014).
[17] D. Trinel, W. Puech P. Puteaux, "High Capacity Data Hiding in Encrypted Images using MSB Prediction," IEEE.
[18] S. Hossain, Md. Shariful T. Mahjabin, "A Block Based Data Hiding Method in Images Using Pixel Value Differencing and LSB Substitution Method," IEEE, pp. 168-72, 2012.
[19] Savina Bansal, R.K. Bansal Sumeet Kaur, "Steganography and classification of Image Stegangraphy Techniques," IEEE, pp. 870-875, 2014.