# An Enhanced Technique for Obscuring Data using Randomly-Chosen Moderate Bit Steganography

Igloo Jain
Research Scholar, Computer Science & Engineering
DAV Institute of Engineering & Technology
Jalandhar, India

P. S. Mann
Assistant Professor, Information Technology
DAV Institute of Engineering & Technology
Jalandhar, India

*Abstract*— **This paper presents a novel algorithm based on randomly chosen moderate significant bit steganography for obscuring data in gray scale images. A new approach of randomly choosing the moderate significant bits for hiding crypto data on the basis of 4-digit numeric key entered by the user has been implemented. The data is encrypted using 16X16 flexible matrix before hiding, the position of bit where data is to be hidden is chosen randomly based on input key and then parity check is applied to hide data at that position. Pixel adjustment is carried out to minimize image quality degradation. This method provides a 3-layer security for hidden data transfer. The new approach is verified on the basis of image quality metrics like PSNR, MSE, entropy and correlation. Further histogram analysis is done to check against steganalysis attacks. This results show that the new method provides higher image quality and robustness against attacks.**

***Keywords—Steganography, Random Moderate Significant Bit, Parity Checker, Flexible Matrix.***

## I. INTRODUCTION

In the present era, there are lots of innovations in techniques and most of the people prefer utilizing the cyber world as the main moderator to communicate data from source to recipient across the world. Many ways of communication are there like: chats, email etc. But main drawback while sending data over internet is loss of data or its privacy. So the imperative consideration is how to transfer data without loss of data or its privacy.

For enhancing and providing better protection to data transmission over cyber world, several methods have been technologically advanced like: Cryptography, Steganography and digital watermarking [9]. Cryptography is a method to cover information by encrypting it to cipher texts and transferring it to the intended receiver using an unknown key, Steganography provides further security by hiding the cipher text into a seemingly invisible image or other formats. Digital watermarking is described as one of the possibilities to close the gap between copyright issues and digital distribution of data.

Steganography is the art of hiding and transmitting data through apparently innocuous carriers to conceal the existence of data [1]. Steganography is derived from two Greek words, which means ―covered writing. While Cryptography is a method to conceal information by encrypting it to “cipher texts” and transmitting it to the intended receiver using an unknown key. Steganography and Cryptography are closely related paradigms. The hidden or embedded image, audio or a video files act as carriers to send the private messages to the destination without any security breach.

Steganography is elaborated as the study of imperceptible communication that usually deals with the methods of hiding the presence of the communicated message [3]. The following formula offers a very generic explanation of the pieces of the steganographic process:

cover_medium + hidden_data + stego_key = stego_medium

In this framework, the cover_medium is the file in which we will hide the hidden_data, which may also be encrypted using the stego_key. The resultant file is the stego_medium (which will, of course. be the same type of file as the cover_medium). The cover_medium (and, thus, the stego_medium) are typically image or audio files.

Least significant bit steganography technique is a technique in which data is stored at least significant bit position [19]. But when image is transmitted at that time image is compressed, so LSB of image is discarded. So the recipient would not be able to extract the data. So to cope up with this moderate significant bit steganography technique can be used in which secret data is embedded at 4th, 3rd or 2nd moderately-significant-bit of pixel of an image as proposed in [20]. Moderate significant bits of each pixel in the cover image are used to embed the secret message as a substitute of LSB substitution steganography technique. Traditional moderate significant bit method hides the data at fixed 2nd, 3rd or 4th bit due to which it is more likely to be detected by hackers. To overcome this drawback, we have proposed a new algorithm.

## II. PROPOSED METHOD

### A. *At Sender Side: Message Encryption & Embedding Module*

Input: Cover Image and Secret data

*a) Encryption*

1. Determine size of given message (S). Compute a (i, j), i. e., ith row & jth column, for size S of data from the selected flexible matrix (size of the message will be embedded before the message).
2. Read data to be embedded character-wise from given text file.

3. Compute a (i, j), i. e., ith row & jth column, for each character of the data from the selected flexible matrix corresponding to ASCII equivalent of that character.
4. Convert each a (i, j) into equivalent 8-bit binary number.

*b) Embedding using Moderate Significant Bit*

1. Read each pixel of cover image commencing with first pixel
2. Convert each pixel into equivalent eight- bit binary number called image byte
3. On the basis of key entered by the user, detect MSB location (where data is to be hidden) randomly.
4. Based on MSB location, convert image byte into two blocks: a) pixel adjustment block b) parity reflecting block.
5. Determine parity of the parity reflecting block and read first crypto-bit
   - i. If the parity reflecting block is of odd parity and crypto-bit is also 1, then there is no change in both blocks of the image pixel.
   - ii. If the parity reflecting block is of odd parity and crypto-bit is 0, then complement moderate significant bit (either 2nd, 3rd or 4th LSB). Convert all the lower bits to 1 if moderate bit is changed to 0 or vice versa otherwise.
   - iii. If the parity reflecting block is of even parity and crypto-bit is also 0, then there is no change in both blocks of the image pixel.
   - iv. If the parity reflecting block is of even parity and crypto-bit is 1, then complement moderate significant bit (either 2nd, 3rd or 4th LSB). Convert all the lower bits to 1 if moderate bit is changed to 0 or vice versa otherwise.
6. Go to next image byte and next crypto-bit and repeat step 1 to 5 until all the crypto-bits of the secret message are embedded.

### B. *At Receiver Side: Message Extraction and Decryption Module*

Input: Stego Image

*a) Extraction using Moderate Significant Bit*

1. Read Pixel of the stego-image starting from the first pixel
2. Convert each pixel value into equivalent binary number
3. On the basis of key entered by the user, detect MSB location (where data is hidden).
4. Extract first crypto-bit by determining the parity condition of the parity reflecting block. If it is odd parity the embedded crypto-bit is 1 otherwise it is 0.
5. Go to next pixel and repeat step from 1 to 4 until 8 crypto-bits of the secret message is extracted.

*b) Decryption*

1. The extracted data byte is divided into two nibbles (each of four bits), i.e., lower and upper nibbles. First extracted data byte will represent the size of the message.
2. Bits of lower nibble form the ith row and those of upper nibble form the jth column for reading the decimal value from the selected matrix.
3. Decimal value is ASCII equivalent of the given character. Convert decimal values into characters, characters are then combined together to form the secret message.
4. Repeat extraction and decryption process until all the characters are extracted and decrypted.

## III. PROPOSED ALGORITHM

### A. *Message Ciphering and Embedding Module*

Step 1. Save the secret message as text file.

Step 2. Commencing with first character, read secret message character-wise from saved text file.

Step 3. Encrypt each character into eight crypto-bits using flexible matrix.

Step 4. Repeat steps 2 and 3 for all character in the saved text file to obtain a series of crypto-bits.

Step 5. On the basis of key entered by the user, detect moderate significant bit location (where data is to be hidden) randomly.

Step 6. Read each pixel of the cover image commencing with the first pixel.

Step 7. Convert each pixel into equivalent eight-bit binary number called image byte.

Step 8. Convert image byte into two blocks-pixel adjustment block and parity reflecting block on the basis of moderate significant bit position.

Step 9. Determine the parity of the parity reflecting block and read first crypto-bit.

Step 10. If the parity reflecting block is of odd parity and crypto-bit is also 1, then there is no change in both the blocks of the image pixel. The odd parity condition in the parity reflecting block reflects that image pixel has stored 1 as the crypto-bit.

Step 11. If the parity reflecting block is of odd parity and the crypto-bit is 0, then complement moderate significant bit (either 2nd or 3rd or 4th LSB). Convert all the lower bits of the pixel to 1 if moderate bit is changed to 0 or vice versa otherwise.

Step 12. If the parity reflecting block is of even parity and the crypto-bit is also 0, then there is no change in both the blocks of the pixel. The even parity condition of the parity reflecting block reflects that image pixel stores 0 as the crypto-bit.

Step 13. If the parity reflecting block is of even parity and the crypto-bit is 1, then complement moderate significant bit (either 2nd or 3rd or 4th LSB). Convert all the lower bits of the pixel to 1 if moderate bit is changed to 0 or vice versa otherwise.

Step 14. Go to next image byte and next crypto-bit and repeat steps from 6 to 9 until all the crypto-bits of the secret message are embedded.

### B. *Message Extraction and Decryption Module*

Step 1. On the basis of key entered by the user, detect moderate significant bit location (where data is to be hidden) randomly.

Step 2. Read pixel of the stego-image starting from first pixel Convert each pixel value into equivalent binary number.

Step 3. Extract first crypto-bit by determining the parity condition of the parity reflecting block. If it is odd parity then embedded crypto-bit is 1 otherwise it is 0.

Step 4. Go to next pixel and repeat steps from 2 to 4 until all the crypto-bits of the secret message are extracted.

Step 5. Decrypt every eight crypto-bits into character using flexible matrix.

Step 6. Repeat Step 5 for all remaining crypto-bits to obtain characters.

Step 7. Save all characters in the form of text file

TABLE I. COMPARISON OF PSNR, MSE, ENTROPY & CORRELATION COEFFICIENT FOR BABY.BMP

| Data Size (in Bytes) | Algorithm | Moderate Significant Bit | PSNR | MSE | Entropy | | Correlation Coefficient |
|---|---|---|---|---|---|---|---|
| | | | | | Original Image | Stego Image | |
| 500 | Existing [20] | 2nd | 61.2369 | 0.048909 | 7.68921 | 7.68939 | 0.999996 |
| | | 3rd | 57.0607 | 0.127941 | 7.68921 | 7.68806 | 0.999989 |
| | | 4th | 50.6006 | 0.566262 | 7.68921 | 7.68838 | 0.999964 |
| | Proposed | Random | 54.434 | 0.234252 | 7.68921 | 7.68982 | 0.999987 |
| 1000 | Existing [20] | 2nd | 58.3179 | 0.095783 | 7.68921 | 7.68907 | 0.999992 |
| | | 3rd | 53.9054 | 0.264573 | 7.68921 | 7.68596 | 0.999978 |
| | | 4th | 47.7398 | 1.0942 | 7.68921 | 7.68307 | 0.999925 |
| | Proposed | Random | 51.5143 | 0.458825 | 7.68921 | 7.69004 | 0.999973 |
| 1500 | Existing [20] | 2nd | 56.6302 | 0.141274 | 7.68921 | 7.68795 | 0.999988 |
| | | 3rd | 52.0514 | 0.405452 | 7.68921 | 7.68252 | 0.999966 |
| | | 4th | 46.0384 | 1.61896 | 7.68921 | 7.67509 | 0.999887 |
| | Proposed | Random | 49.7612 | 0.687012 | 7.68921 | 7.68964 | 0.999959 |
| 2000 | Existing [20] | 2nd | 55.3423 | 0.190044 | 7.68921 | 7.68616 | 0.999984 |
| | | 3rd | 50.7591 | 0.545975 | 7.68921 | 7.67834 | 0.999955 |
| | | 4th | 44.8146 | 2.14594 | 7.68921 | 7.66634 | 0.999845 |
| | Proposed | Random | 48.4717 | 0.924504 | 7.68921 | 7.68933 | 0.999943 |
| 2500 | Existing [20] | 2nd | 54.3084 | 0.241126 | 7.68921 | 7.68397 | 0.99998 |
| | | 3rd | 49.7443 | 0.689679 | 7.68921 | 7.67305 | 0.999943 |
| | | 4th | 43.91 | 2.6429 | 7.68921 | 7.65599 | 0.999805 |
| | Proposed | Random | 47.5711 | 1.13754 | 7.68921 | 7.68838 | 0.999929 |

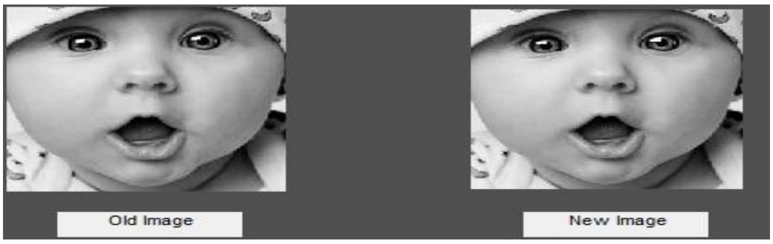

Fig 1. Cover Image and Stego Image

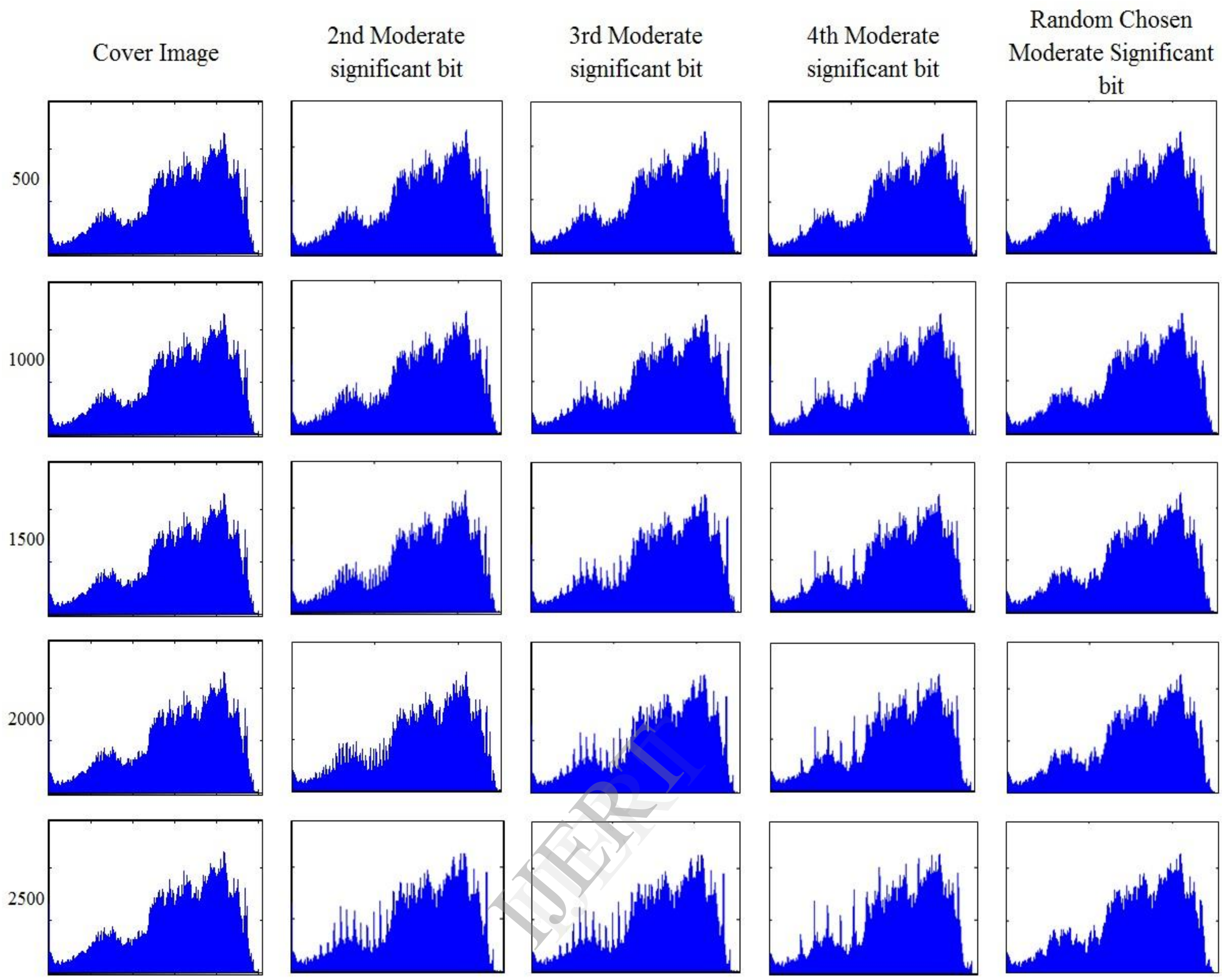

Fig 2. Histograms for baby.bmp with 4 different input data sizes (in bytes)

## IV. Results and Discussion

The experimental results of the newly proposed method are presented in table I. The algorithm is implemented using MATLAB programming language. The proposed method is validated on four grayscale images of different sizes. Different amounts of data ranging from 500 bytes to 2500 bytes are hidden into every image. The simulations are carried out using MATLAB image tools. The original and stego images are compared on the basis of Image Quality Metrics like PSNR, MSE, Entropy, correlation and histograms. The results are compared with the results of old algorithm. The results confirm that PSNR of newly proposed algorithm is better than 4th MSB Insertion method which means image quality of cover image is better in randomly chosen bit method. Though PSNR value is less in 2nd and 3rd MSB Insertion method but still newly proposed algorithm is better in the way that, it will provide greater security as position of insertion bit is unknown due to randomly chosen bit.

MSE of newly proposed algorithm is much lower than 4th MSB Insertion method which means errors in cover image as compared to actual image are lesser in new algorithm. MSE value for 2nd and 3rd MSB Insertion method is lesser than our algorithm but chances of loss of data is more in 2nd bit insertion method as 1st and 2nd bits may be discarded during compression.

Histogram analysis shown in Fig 2. verifies that there is no visual difference in the histograms of cover and stego images in newly proposed algorithm even with higher amounts of data. Thus the newly proposed algorithm provides 3 layered security:-a) Encryption of data before hiding to image b) Randomly choosing moderate bit on the basis of key entered by user c) Parity check and pixel adjustment to hide crypto bit in image pixel. These results show the newly proposed algorithm is highly secure, robust, provides better stego image quality and is difficult for hackers to break as the data is secured by key which only the sender and receiver will know.

## V. CONCLUSION

In this paper, a novel algorithm based on moderate significant bit steganography has been designed and implemented, which is advancement to the existing algorithm [20]. The use of randomly chosen moderate significant bits based on the key entered by user not only adds third layer of protection but also provide better results in terms of stego image quality. The new algorithm has been compared with the existing algorithm on the basis of image quality metrics like PSNR, MSE, entropy, correlation coefficients and histograms. The experimental results of this algorithm are quite favorable.

## REFERENCES

[1] N. F. Johnson, and S. Jajodia, “Steganography: Seeing the Unseen”, IEEE Computer, Feb. 1998,pp. 26-34.

[2] Wu and W.-H. Tsai, “A steganographic method for images by pixel-value differencing,” Pattern Recognition Letters, vol. 24, no. 9-10, pp. 1613–1626, 2003.

[3] T Morkel, JHP Eloff and MS Olivier, "An Overview of Image Steganography," Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, June/July 2005 (Published electronically)

[4] Hassan Mathkour, Ghazy M.R. Assassa, Abdulaziz Al Muharib, Ibrahim Kiady,“A Novel Approach for Hiding Messages in Images”, International Conference on Signal Acquisition and Processing,2009

[5] M. Sitaram Prasad, S. Naganjaneyulu, Ch. Gopi Krishna, C. Nagaraju, “A Novel Information Hiding Technique For Security By Using Image Steganography”,Journal of Theoretical and Applied Information Technology, Vol 8. No. 1 – 2009

[6] Balkrishan and Amar Partap Singh, “Hiding Encrypted Data using Randomly Chosen Moderate Bit Insertion in Digital Image Steganography,” Journal of Computer Science and Engineering, vol. 1, issue 2, pp. 21-27, June 2010.

[7] Arvind Kumar, Km. Pooja, “Steganography- A Data Hiding Technique”, International Journal of Computer Applications (0975 – 8887) Volume 9– No.7, November 2010

[8] Rajkumar, Rahul Rishi and Sudhir Batra, “A New Steganography Method for Gray Level Images using Parity Checker”, International Journal of Computer Applications (0975 – 8887) Volume 11– No.11, December 2010

[9] V.Sathya Preiya , S.Sathish Kumar,M.Shanmuganathan, “Provide Secure Authenticity For Propagating”, International Journal of Engineering Trends and Technology- May to June Issue 2011

[10] Pallavi Khare, Jaikaran Singh, Mukesh Tiwari, “Digital Image Steganography”, Journal of Engineering Research and Studies Vol.II Issue III July- pg 101-104, September,2011

[11] N Verma, “Review of Steganography Techniques”, International Conference and Workshop on Emerging Trends in Technology (ICWET 2011)

[12] Jindal, A. P. Singh, “Moderate Bit Insertion for Hiding Crypto-Data in Digital Image for Steganography”, Special issues on IP Multimedia Communications (1):136-138, October 2011.

[13] Ajit Singh and Upasana Jauhari, "A Symmetric Steganography with Secret Sharing and PSNR Analysis for Image Steganography", International Journal of Scientific & Engineering Research Volume 3, Issue 6, June-2012

[14] Ronak Doshi,Pratik Jain,Lalit Gupta “Steganography and Its Applications in Security”, International Journal of Modern Engineering Research (IJMER), Vol.2, Issue.6, pp-4634-4638, Nov-Dec. 2012

[15] Kanzariya Nitin K. and Nimavat Ashish V, “Comparison of Various Images Steganography Techniques”, International Journal of Computer Science and Management Research Vol 2 Issue 1, January 2013

[16] Mehdi Hussain and Mureed Hussain “A Survey of Image Steganography Techniques”, International Journal of Advanced Science and Technology,Vol. 54, May, 2013.

[17] C.Gayathri , V.Kalpana “Study on Image Steganography Techniques”, International Journal of Engineering and Technology (IJET), Vol 5 No 2 Apr-May 2013

[18] Bharti Ahuja, Rashmi Lodhi “Different Algorithms used in Image Encryption: A review “,International Journal of Computer Science & Engineering Technology (IJCSET), Vol. 4 No. 07 Jul 2013

[19] Anubha Prajapati “Steganography Using Lsb Technique”, Proceedings Of National Conference On Recent Advancements In Futuristic Technologies (Ncraft’13), 2013

[20] B. Jindal, A. P. Singh, “Camouflaging in Digital Image for Secure Communication”, Journal of The Institution of Engineers (India): Series B June 2013, Volume 94, Issue 2, pp 85-92

[21] Mukesh Garg, A.P. Gurudev Jangra, “An Overview of Different Type of Data Hiding Scheme in Image using Steganographic Techniques”, International Journal of Advanced Research in Computer Science and Software Engineering , Volume 4, Issue 1, January 2014

[22] K.B.Bini, R.Sreejith, “Secure Reversible Data Hiding with Image Encryption”, International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE), Volume 3, Issue 2, February 2014