Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 09, September-2019

# Advanced Self Reversible Data Embedding on Encrypted Images using MSB Bit Differencing

Krishnendu P.S
M. Tech CSE, Department of CSE
Sree Narayana Gurukulam College of Engineering
Kadayiruppu, India

Saini Jacob Soman
Assoc.Professor, CSE Department
SNGCE, Kadayiruppu, India

***Abstract*— In the modern era of growing cyber-attacks, the confidentiality of information is a vital concern. Protection of information matters everybody, because all are exposed to it every time they go online. Numerous data framework security procedures are available such as cryptography, watermarking, fingerprinting to hide the confidentiality of data.. Steganography is one of the advanced methods for hiding data from an unauthorized access. This technique hides secret data in different file formats such as: image, text, audio, and video. In this process, image is been utilized as the cover medium to embed data to be protected from the security breach. Usually, the hackers focus on least significant bits (LSB) for secret data extraction but the proposed technique utilizes an advanced self-reversible data embedding on encrypted images using MSB bits which can accurately recover the original image and extract the original content.**

***Keywords*— *Steganography, Cover image, Stego image, Most significant bit, Least significant bit, Reversible data embedding, Image encryption, Histogram shift.***

## I. INTRODUCTION

Information security is necessary for the transmission of confidential data in many areas. It includes banks and other financial institutions, military communications as the information transmits are of very sensitive in nature. So in order to keep the transmittal confidentiality a much strong method shall be used which keeps the data more secure. The forms of data hiding techniques are cryptography, watermarking, steganography etc. In cryptography the secret message is encrypted and sent in an unintelligent format that means one can tell that a message has been encrypted, but he cannot decode the message without knowing the proper key. Watermarking is used for authentication and copyrights protection. This technique hides digital information in carrier signals. Consequently, these are more prone to be hacked. Watermarking is used to check the identity and authenticity of the owner of a digital image. They can be visible and invisible and place less amounts of data. In watermarking even if it is invisible the message can be decoded easily by different means. Steganography is converting the image in a way that only the sender and the intended recipient is able to detect the message sent through it. It is also invisible, and thus the detection is not easy. This technique provides a better way of sending secret messages than encoded messages or cryptography as it does not attract attention to itself. In steganography people cannot detect the existence of the message. Using steganography, the user can send the image to multiple recipients without them even realizing that the image contains hidden data, and only the intended recipient can be made aware of this contents and the means of how to extract the original data.

## II. LITERATURE SURVEY

Many researchers have introduced various techniques for steganography. These classification results have many applications in the real world applications such as the, medical imaging, military communication, law forensics and so on. In order to classify these techniques in to their respective categories, there are number of surveys related to image steganography and reversible data hiding techniques.

Deshpande N, Snehal K [1] proposed a method for calculating various bits using LSB strategy. In Least Significant Bit embedding technique data can be hidden in the least significant bits of the original image and the human eye cannot identify the hidden image in the cover file. This method mainly focusses on LSB technique. So this approach is very easy to detect.

H. Yang, X. Sun and G. Sun [2] suggested a method for image data hiding using LSB technique. This method is based on the concept that edge regions undergo a little number of changes than highly finished areas. That is, the strategy inserts more secret information into noise non-sensitive regions than noise sensitive zones. Overall result provides a great hidden capacity, but dataset for experimental results are constrained; there's not a single image which has numerous edges with noise region.

In order to hide data in edge areas of images another method introduced by [3] Cheng-Hsing Yang, Chi-Yao Weng, Shiuh-Jeng Wang which embeds secret data into gray image value without making it visible. This method is complex due to adaptive k generation for substitution of LSB.

Ki-Hyun Jung, Kyeoung-Ju Ha, Kee-Young Yoo in [4] proposed a hiding data in image using multi-pixel differencing with LSB to improve the capacity of hidden secret data and to provide an imperceptible visual quality. This is a new data hiding method using LSB and MPD to improve the hiding capacity of hidden data and provides excellent visual quality. But its experimental data set is too limited.

The next mechanism is the hybrid edge detector by Chen, W. J., Chang, C. C. and Le, T. H. N in [5] is an LSB substitution procedure is the first stage of edge detection method. The least significant bit (LSB) substitution mechanism is the foremost common steganographic strategy for embedding a secret message in an image with high capacity, whereas the human visual system (HVS) would be incapable to notice the hidden message within the cover image. The problem with this existing technique is that, the proposed scheme is tried on restricted images dataset. This strategy isn't tried on broad edges based picture.

Another method called mapping pixels to letters by M. A. Al-Husainy [6] utilized sufficient number of bits from each pixel in an image and mapping them to 26 alphabetic English characters from a to z with a few special characters which are used in writing a secret message, but it can be used only in text based hiding.

In [7] Shogo Ohyama, Michiharu Niimi,Kazumi Yamawaki,Hideki Noda proposed data hiding in PEG2000 Compressed Bit-Stream .This method is made of three major steps which are the color quantization, the color requesting and the DCT-based information hiding. The objective of this work is to permit free access to the compressed gray-level picture and donate color picture in case you claim a secret key. It has high PSNR value and can be identified easily by embedding data.

Blossom Kaur , Amandeep Kaur , Jasdeep Singh [8] proposed DCT (discrete cosine transform) domain steganographic technique based on watermarking scheme which provides higher resistance to image processing attacks such as JPEG compression, noise, rotation, translation etc.Watermark is inserted by adjusting the DCT coefficients of the image and by using the private key. In this approach, the watermark is embedded in the mid frequency band of the DCT blocks carrying low frequency components and the high frequency sub band components remain unused. Watermark can then be extracted using the same private key. But here high frequency components are easily targeted.

M.Chaumont and W.Puech[9] constructed an indexed picture which is, within the same time, a semantically coherently gray-level picture. It permits free access to the compressed gray-level picture and donate color picture in case you claim a secret key. The reason of this method is to provide gray-level image to everybody but not permitted to those who have same color images with its stego-key. It has high PSNR value and can be identified easily by embedding data.

In [10] Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, and Wei Su proposed a reversible data hiding scheme which can recover the original cover image without any distortion. It can insert more data from the marked image after hiding the information can be extracted. The idea behind this calculation utilizes the zero or the minimum points of the histogram of an image and marginally modifies the pixel grayscale values to insert information into the image. Using LSB technique can lead this method to cause distortion.

Reversible Data Embedding Using a Difference Expansion [11] by Jun Tian proposed a method to recover the original digital content by applying reversible data embedding method for digital images. The performance of a reversible data-embedding calculation can be measured by the following: First is the payload capacity for identifying how much information can be embedded. Second one is visual quality for recognizing quality of the embedded image and finally complexity.Limitation is uncompressed image is used for embedding data.

Reversible data hiding [12] proposed by Mehmet U. Celik, Gaurav Sharma, A. Murat Telkalp, and Eli Sabe use histogram shifting. In histogram shifting, the input picture is divided into blocks and after that histogram shifting is done on each block which upgrades the information hiding capacity and visual quality. This method improves image quality especially the PSNR of the original image In [13] Lixin Luo, Zhenyong Chen, Ming Chen, Xiao Zeng and Zhang Xiong uses interpolation technique can re-establish the original picture without any distortion after the covered up information is extracted. Digital watermarking could be a kind of information covering up innovation. Its basic idea is to insert undercover data into a computerized signal, like digital sound, picture, or video, to follow possession or secure privacy. Limitation for these methods are uncompressed image is used for embedding data.

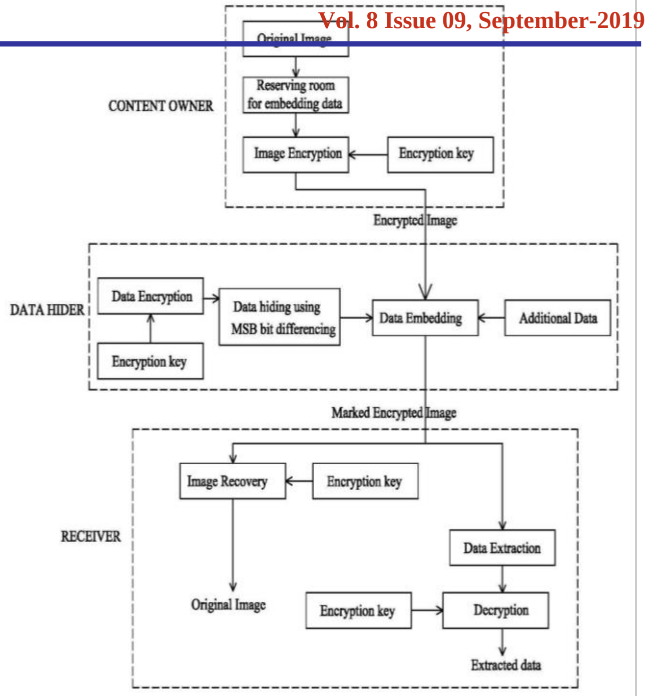


Fig. 1. Proposed system design

In [14] the method introduced by Ammad Ul Islam1, Faiza Khalid, Mohsin Shah, Zakir Khan , Toqeer Mahmood, Adnan Khan, Usman Ali, Muhammad Naeem image steganography using MSB bit differencing. In MSB bit differencing secret data is embedded in the most significant bits of the cover image by using encoding and decoding algorithms. Another method [15] suggested by Kede Ma, Weiming Zhang, Xianfeng Zhao, Nenghai Yu, and Fenghua Lireversible data hiding using self- reversible embedding using LSB. In this work content owner generates an encrypted image using a standard RDH algorithm. This encrypted image is received by the data hider to hide the secret data and finally receiver receives the marked encrypted image to restore the original cover image and extracts the embedded data. Hackers can identify easily due to visual clues.

## III. PROPOSED METHODOLOGY

In the proposed system an advanced self- reversible data embedding of encrypted image using most significant bit differencing strategy is used. First the content owner reserves enough space on original picture and then converts into its encrypted version with the encryption key. The information embedding process in encrypted picture is reversible for the data hider as it should suit information into the saved space previously assigned.

In this new system, we follow the standard idea that losslessly compresses the redundant image content utilizing reversible data hiding techniques and at that point encrypts it to securing privacy. With the new framework which fundamentally comprises of : generation of encrypted image using image partition, self-reversible embedding using histogram shift, image encryption using XOR operation, data hiding using MSB bit differencing and finally data extraction and image recovery.

### *A. Generation of Encrypted Image*

In order to develop the encrypted image, the primary process is separated into three steps: image partition, self-reversible embedding using histogram shift and followed by image encryption using XOR. At the beginning, image partition step separates unique picture into two parts A and B; then, the MSBs of A are reversibly embedded into LSBs of B with a standard RDH calculation, so that MSBs of A can be utilized for keeping messages; at final, scramble the improved picture to generate its last version.

#### *1) Image partition*

The administrator here for saving room before encryption could be a standard RDH strategy, so the objective of image partition is to develop a smoother zone B, on which standard RDH calculations can accomplish better . Without losing the original image quality we accept the original picture is an 8 bit gray-scale picture with its size MxN and pixels Ci,j ϵ[0,255],1≤M,1≤j≤N. First of all, the content owner extracts the cover image, along the rows, several covering blocks whose number is decided by the size of the-embedded messages, indicated by l. This means every block comprises of m lines, where m = [l/N]. For each block, defines a function to degree its first-order smoothness.

$$f = \sum_{u=2}^{m} \sum_{v=2}^{N-1} \left| \left( C_{u,v} - \frac{C_{u-1,v} + C_{u+1,v} + C_{u,v-1} + C_{u,v+1}}{4} \right) \right| \quad (1)$$

f is the block which contain more complex textures. The content owner, hence, chooses the particular block large data capacity f to be A, and puts it to the front of the picture concatenated by the rest portion with less textured areas, as appeared in Fig. 2.

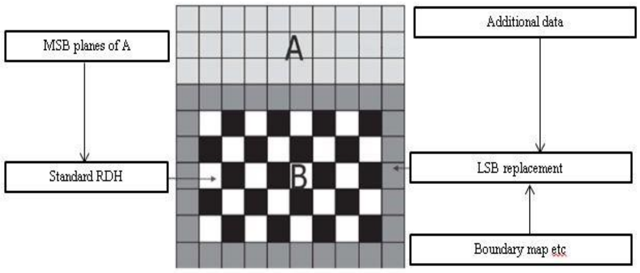


Fig. 2. Outline of image partition and embedding process

From the above figure only single MSB-plane of A is recorded. It is clear that the content owner can moreover insert two or more MSB-planes of A into B which leads to half, or more than half, decrease in size of A.

#### *2) Self-Reversible Data Embedding Using Histogram Shift.*

Reversible data hiding is a strategy which is able to embed basic information into images, audio, video and so on. This framework applies a strategy of hiding information in an image and video by saving room before encryption. The proposed scheme increments the amount of information that can be covered up within the picture or video which ensures the lossless recovery after extraction is completed. All the previous methods of reversible information hiding were created such that they were emptying room for information covering up after encrypting the picture, which results in providing some blunder rates at the time of data extraction and image recovery. The objective of self-reversible embedding of data is to embed the MSB-planes of A into B by employing traditional RDH calculations.

In the proposed system an algorithm called histogram shifting technique is used. Histogram method finds peak or zero points within the histogram and information embedding is done by shifting these peak and zero points. In the histogram-based data hiding, the number of pixels in the peak point, represents hiding capacity .Basically in this technique firstly we have to find a zero point and a peak point. Zero point refers minimal pixels which is a grayscale value with no pixel in the original image whereas peak point corresponds to grayscale value with maximum number of pixels in the cover image. The main aim of finding the peak point is to increase the payload capacity.

Fig. 3 illustrates the thought of selecting legitimate points. Usually, two things can pick up great advancement in terms of PSNR when the length of information is moderately brief, i.e., when x=1.And the predominance of one can be over the other depends exceedingly on insights of normal picture itself.

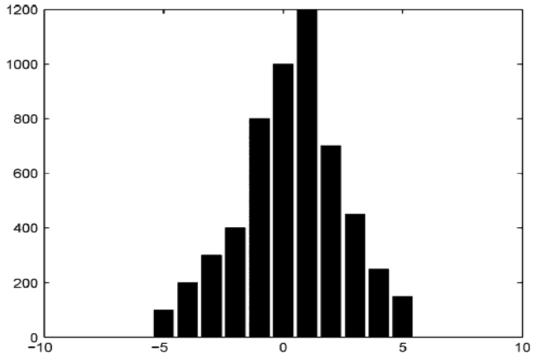


Fig. 3. Interpolated error histogram representation

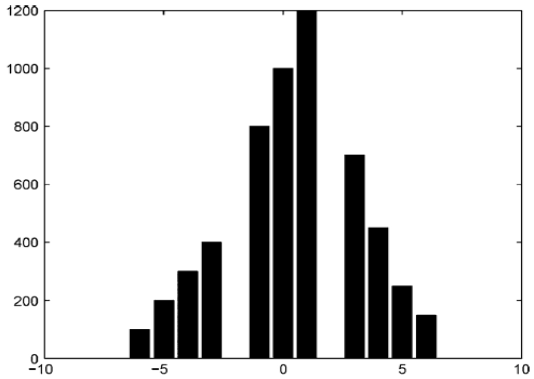


Fig. 4. Shifted histogram representation

### a) Histogram shifting algorithm

In this work, we propose a modified data hiding scheme based on histogram shifting technique, in which peaks of the image histogram is used to hide secret data. In this method, every pixel value is modified at most by 1, so the visual quality of cover image is guaranteed. This method marks the two peak slots of the histogram of cover image to hide the secret data. The peak slots occupies the large number of pixels in the cover image, and hence can embed large number of data. Then the histogram of host image is calculated. Select the pairs of peak represented with $P_L$ and $P_H$ where the minor peak value is $P_L$, and $P_H$ is the superior peak. For data embedding, the next pixel values of peak are shifted to create vacant spaces while the peak values are manipulated to carry hidden data by filling those vacant spaces. The secret data bitstream $S_i$ = [0,1] embedded on peaks based on the formula as given below,

$$p' = \begin{cases} p-1 & for\ p < P_L \\ P_L - Si & for\ p = P_L \\ p & for\ P_L < p < P_H \\ P_H + Si & for\ p = P_H \\ p+1 & for\ p > P_H \end{cases} \tag{3}$$

where p' is the embedded pixel value.

### 3) Image encryption using XOR

Image is in the form of a matrix and a random matrix will be generated. From the given password, random matrixes will be generated. We sequentially XOR with this random matrixes with our RGB matrices. When we reverse this process that means when we XOR this random matrixes we will get back the original image. In order to make the password distributed, that is to increase the diffusion, we will sum the passwords.

Steps:

• First of all take an image and divide it into three matrix ie, RGB matrix. Then receive the key that will be a string and in that string each character is converted into ASCII and then take first character as seed for random matrix generation.

• With this seed value then a set of numbers will be returned, that set of numbers will be the size of our matrix.

For example, if the size of our matrix is mxn which means, mxn numbers will be generated. Then we are performing XOR operation with this generated random numbers with RGB matrices. Repeat this process for second character by converting it into ASCII then sum it with the ASCII of first character. By doing this for the entire password, we get ASCII value and make it as seed and again random number matrix is generated. This XOR is performed for all characters and a set of matrixes are generates with this process.

After image encryption, the information hider or a third party cannot get to the substance of original picture without the encryption key, hence protection of the content owner being secured.

## B. Data Hiding in Encrypted Image using MSB bit differencing

Once the data hider obtains the encrypted picture,he can embed a few information into it, the fact is that he does not get to the original picture. The information hider basically uses MSB technique to substitute the accessible bit-planes with extra information.

### 1) MSB differencing techniques

MSB bit differencing means hiding data in most significant bits and in the proposed scheme bit number five is used to hide the data .The most significant bits of pixels are taken in order to hide secret information bits. The distinction between bit No. 5 and 6 is used for covering up secret data bits. Bit 0 is supposed to be hidden when the difference between bit No. 5 and bit No. 6 is zero and bit 1 covered up when their distinction is one. In case the incoming secret information bit does not match with the distinction between bit No. 5 and 6, at that point bit No. 5 is changed to make them equal.

#### a) Encoding steps

The steps for encoding the secret information in cover picture are given as beneath:

i. Read the secret data bits

ii. Read the cover image

iii. For each pixel of cover Image

iv. Read bit No. 5 and 6

v. Compute the difference

vi. Compare the contrast with secret information bit, in case information bit isn't rise to the distinction then transverse bit No. 5

vii. Type in the stego picture.

#### b)Decoding steps.

i. Read the stego image

ii. For all pixels of stego image

iii. Calculate the difference between 5th and 6th bits:

Data bit = Difference

iv. Write the secret data to file.

After taking every pixel of stego image, then calculate the difference between 5th and 6th bit. The result will be the difference of the value of data bit.

## C) Data extraction and image recovery

The information extraction is totally autonomous from image decryption the arrangement of them suggests two distinct viable applications.

*Case 1- Extracting Data from Encrypted Images*

In this case only data is receiving. First of all, load the hidden data image that will be the same encrypted image as marked encrypted image and provide the same key used for hiding data in order to extract data back to normal.

*Case 2: Extracting Data from Decrypted Images*

In Case 1, both inserting and extraction of the information are controlled in encrypted space. On the other hand, there's a distinctive situation that the client needs to decode the picture to begin with and extracts the data from the decrypted picture when it is required.

## IV. RESULTS AND ANALYSIS

Last chapter discussed about the steps we had used to classify the self-reversible embedding on encrypted images.

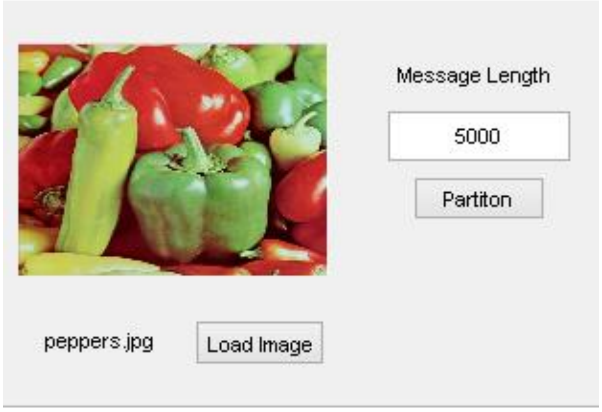
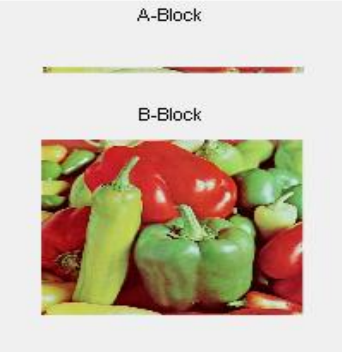
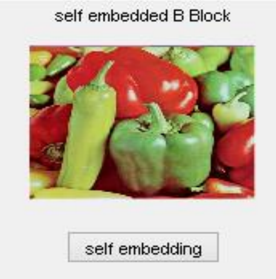

Message Length: 5000

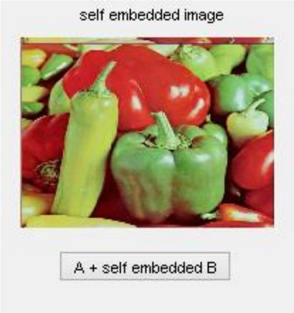
Fig. 5 Uploading cover image





i

Fig. 6. Partitioning Image Fig. 7. Partitioning Image



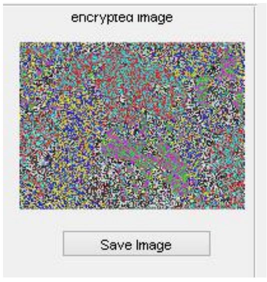
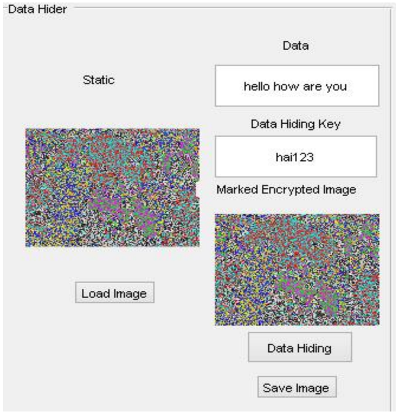
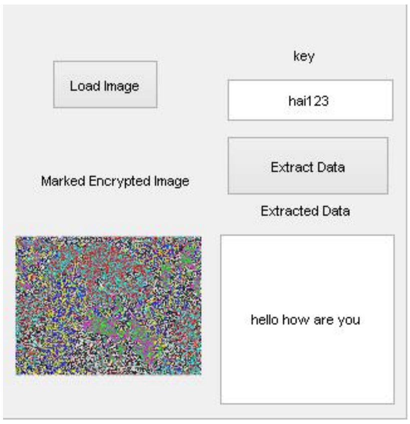


Fig. 8. Self- embedded image Fig. 9. Encrypted Image



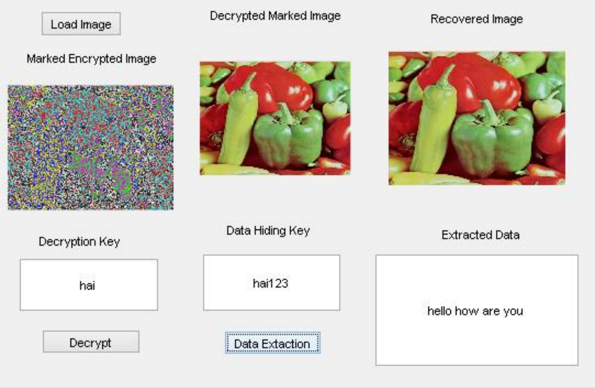
Data: hello how are you
Data Hiding Key: hai123

Fig. 10. Data hiding



key: hai123
Extracted Data: hello how are you

Fig. 11. Data extraction



Decryption Key: hai
Data Hiding Key: hai123
Extracted Data: hello how are you

n

Fig. 12. Data extraction and Image recovery

TABLE.I. PSNR comparison for single MSB plane under various embedding rates

| PSNR results | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Embedding rate (bpp) | | 0.005 | 0.01 | 0.05 | 0.1 | 0.2 | 0.3 | 0.4 | 0.5 |
| Lena | 1MSB - planes | 67.16 | 63.44 | 55.46 | 52.33 | 49.07 | 45.00 | 40.65 | 35.84 |
| Airplane | 1MSB - planes | 65.94 | 63.18 | 57.02 | 54.20 | 50.98 | 48.26 | 44.67 | 40.78 |
| Baboon | 1MSB - planes | 57.49 | 55.71 | 50.19 | 46.17 | 40.68 | 35.87 | 31.16 | 25.92 |
| Peppers | 1MSB - planes | 63.77 | 61.30 | 54.17 | 51.02 | 46.00 | 42.08 | 36.91 | 32.05 |

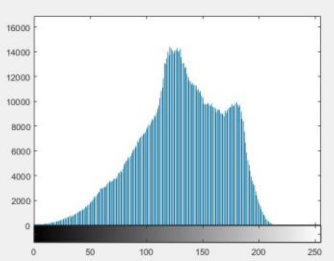


Fig. 13. Histogram of Original image

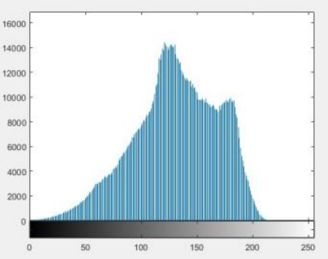


Fig. 14. Histogram of Recovery image

## V. CONCLUSIONS

In this paper, advanced method for self- reversible data embedding of encrypted image using MSB strategy with efficient data hiding method known as histogram shifting is presented. The embedding operation performed based on histogram shifting can embed significantly more data. The information hider can take advantage from the additional space emptied out in past stage to make information hiding process effortless. The proposed strategy can take advantage of all traditional reversible data hiding methods for plain images and accomplish great performance without loss of culminate secrecy. Usually, the LSBs are more prone to hackers. To overcome this MSB bit differencing is used. Besides, this novel method can accomplish genuine reversibility, partitioned information extraction and enormously enhancement on the quality of checked decrypted images.

## REFERENCES

[1] Deshpande N, Snehal K An overview of image steganography using LSB technique.Published in IEEE Explore Conference :Digital Information Management. (2012)

[2] H. Yang, X. Sun and G. Sun, A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution, Publication: Radio Engineering, vol. 18, pp. 509-516,( 2009)

[3] Cheng-Hsing Yang, Chi-Yao Weng, Shiuh-Jeng Wang, Adaptive Data Hiding in Edge Areas of Images With Spatial LSB Domain Systems, Publication: IEEE Transactions on Information Forensics and Security, vol. 3, no. pp. 488-497. 3rd September.(2008)

[4] Ki-Hyun Jung, Kyeoung-Ju Ha, Kee-Young Yoo, Image data hiding method based on multi-pixel differencing and LSB substitution methods, Publication: n Proc. 2008 International Conference on Convergence and Hybrid Information Technology (ICHIT '08). Daejeon (Korea), Aug. 28-30, p. 355-358, (2008)

[5] Chen, W. J., Chang, C. C. and Le, T. H. N, High Payload Steganography Mechanism Using Hybrid Edge Detector, Publication: Expert Systems with Applications, vol. 37, pp. 3292-3301,( 2013)

[6] M. A. Al-Husainy, Image Steganography by Mapping Pixels to Letters, Publication: Journal of Computer Science, vol. 5, pp. 33-38, (2009)

[7] Shogo Ohyama, Michiharu Niimi,Kazumi Yamawaki,Hideki Noda, Lossless Data Hiding Using Bit-Depth Embedding for JPEG2000 (2008)

[8] Blossom Kaur , Amandeep Kaur,Jasdeep Singh,Steganographic Approach For Hiding Image In DCT Domain, International Journal in Advances of Engineering and Technology.Department of Computer Science and Engineering ( 2011)

[9] M. Chaumont and W . Puech, A DCT-based data-hiding method to embed the color information in a JPEG grey level image, Publication: 14th European Signal Processing Conference (EUSIPCO 2006), Florence, Italy, September 4-8, (2006), copyright by EURASIP

[10] Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, and Wei Su, reversible data hiding Publication: Ieee transactions on circuits and systems for video technology,vol. 16,no:3 , march (2006)

[11] Jun Tian, Reversible Data Embedding Using a Difference Expansion, Publication: IEEE Transactions on Circuits and Systems for Video Technology, VOL 13, No 18. pp. 890-896(2003)

[12] Mehmet U. Celik, Gaurav Sharma, A. Murat Telkalp, and Eli Sabe, reversible data hiding, Publication: IEEE ICIP.pp.157–160(2011)

[13] Lixin Luo, Zhenyong Chen, Ming Chen, Xiao Zeng and Zhang Xiong, Reversible Image watermarking using Interpolation technique, Publication: ” IEEE Transactions on Information Forensics and security, vol. 5, no. 1, pp. 187–193.(2010)

[14] Ammad Ul Islam1, Faiza Khalid, Mohsin Shah, Zakir Khan , Toqeer Mahmood, Adnan Khan, Usman Ali, Muhammad Naeem, image steganography using MSB bit differencing, Publication:The sixth international conference on innovative technology( 2016)

[15] Kede Ma, Weiming Zhang, Xianfeng Zhao, Nenghai Yu, and Fenghua Li, Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption Publication:IEEE transcations on information forensics and security(Volume: 8 , issue:3, March (2013 )

.