International Journal of Scientific Research & Engineering Trends
Volume 7, Issue 4, July-Aug-2021, ISSN (Online): 2395-566X

# A Color Image Steganography Method to Hide Multiple Images with LSB Coding

**Research Scholar Palac Gupta, Deepinder Kaur (HOD)**
Dept. of Computer Science & Engineering,
Shaheed Udham Singh College of Engineering & Technology,
Tangori, Mohali, India
palac1gupta12@gmail.com, deepinderkaurcse@gmail.com

**Abstract- Data and information security is one of the crucial tasks in the digital and data communication. In the ancient time there are various ways to hide data into various objects. In modern day the data security is also very important. Data can be of various types like text, image, audio or any other form. In image steganography image acts as cover image and it can hide text, image and other form of data. In case of multiple image steganography various image can be hidden in a single image. Benefit of this approach is that those hidden images can hide the data also. So it becomes very difficult to access those hidden data. Steganography can be classified into two categories namely spatial domain and transform domain. Both have different advantages. In this paper a novel technique for hiding multiple digital images in a colored digital image with the help of LSB encoding is proposed. 8-bit LSB technique will be used for the embedding of data into the cover image which is also known as stego digital image. The proposed technique will be able to hide various images with the encrypted method and then with the help of decoding method images can be recovered. The proposed technique will be compared with the already existing multiple image hidden steganography technique. Various objective parameters like hiding capacity, file size before steganography and after steganography, mean square error and peak signal to noise ratio will be taken as objective parameters. All the implementation will be performed in the Matalb software.**

**Keywords- Image Steganography, LSB, encryption, Haar transform, peak signal to noise ratio, mean square error.**

## I. INTRODUCTION

Information and data security is the prime concern in the data and digital communication. In this context cryptography is a technique where encryption methodology is used to provide the secure access to the important and confidential information. It uses the keys and its variable length to encrypt and decrypt the data. Usually it is frequently found alone cryptography is not able to solve the problem and so there must be a unique way with the help of which data become invisible. [1-2]

Process of Steganography is known to hide information in various sources for various security purposes. Best part of this phenomenon is that message or information can be hidden into some kind of media like digital image, digital video and digital audio as well as in text. At present still there is a unique issue in steganography which is that how much information as well as visual information of digital image can be saved. There are various tools or algorithms which hide the data or information into the digital media such that hidden information becomes inaccessible and imperceptible. [3-5]

In this research work a novel technique for hiding multiple digital images in a colored digital image with the help of LSB encoding is proposed. 8-bit LSB technique will be used for the embedding of data into the cover image which is also known as stego digital image. The proposed technique will be able to hide various images with the encrypted method and then with the help of decoding method images can be recovered.

## II. LITERATURE SURVEY

**A. Y. Rafiqi et al. [1]** in 2021 used steganography for text hiding in images with the help of various algorithms. Authors used the principal component analysis method for hiding text in image and used Grey Scale Co-occurrence Matrix to create final stego digital image. Author compared the proposed method with the old method using various objective parameters like mean square error, peak signal to noise ratio and entropy. Authors showed the worthiness of the proposed method.

**O. Elharrouss et al. [2]** in 2020 used LSB technique to hide one image into another image using k-least significant bit stegnaography approach. In case of decoding phase of proposed methodology the region detection operation was used which finds out the region where the image was actually hidden. Authors used the single parameter peak signal to noise ratio to measure the effectiveness of the proposed methodology. But proposed methodology was not able to beat the best algorithm.

**P. Marella et al. [3]** in 2019 used text steganography to hide data in facial images with least significant bits algorithm. From the facial features of an image like eyes, nose, mouth authors tried to find the maximum space available to hide the text data into these features. Authors had not used any specific objective parameter for comparative analysis but used the zoom factor analysis. On zooming the image after a significant level it showed the increased chances of present of some data into stego image.

**A. G. Benedict et al. [4]** in 2019 had proposed multiple image steganography technique. Authors tried to store multiple digital images into the single image. Authors used the concept of sequential hashing, enhanced image with hashing and image hashing with password to perform the proposed methodology. Authors used various objective parameters like file size before steganography and after steganography and executed time of algorithm on various formats of digital images.

**S. Mukherjee et al. [5]** in 2018 had used the concept of mid value method for performing image steganography. Authors first perform scramble operation over the cover image and then this scrambled image had got hidden in some cover image. Now the secret image was hid into this image. After this operation this intermediate was again unscramble to got the final stego image which was similar to original image. Authors used the mean square error and peak signal to noise ratio and embedding capacity to show the effectiveness of proposed algorithm. Algorithm performed better in comparison to other methods.

## III. PROBLEM FORMULATION AND METHODOLOGY

In image steganography image acts as cover image and it can hide text, image and other form of data. In case of multiple image steganography various image can be hidden in a single image. Benefit of this approach is that those hidden images can hide the data also. So it becomes very difficult to access those hidden data. There is requirement of some new steganography approach which will be able to store data in various multiple cover digital images and then these images would be able to store in a single cover image so that data can be sent easily in a single image and not in multiple images. Also image quality should be preserved so that intruder could not get information about it.

After studying various research papers and comprehensive literature survey, the various research gaps that have been identified are as follows

- Image steganography methods were not able to hide data in a single image efficiently
- Various steganography algorithms were very slow and takes long time for execution
- Various algorithms were not able to hide multiple encoded images in a single image
- Some of the algorithms failed on zooming the image as it showed the image was manipulated.

**1. Methodology:**

Here are the important steps which will be performed to complete this research work.

- **Step 1.** Secret data will be first binarized and then encrypted at the sender side using LSB technique and DES.
- **Step 2.** Now this encrypted data will be hidden into the different cover images at sender side using Haar transform
- **Step 3.** After it these multiple stego images will be hidden into final stego image at sender side.
- **Step 4.** At receiver side internal multiple stego images were extracted.
- **Step 5.** From these multiple image encrypted data is obtained and then decryption and binary to text conversion is performed to get the actual secret text data.

**2. Proposed Algorithm:**

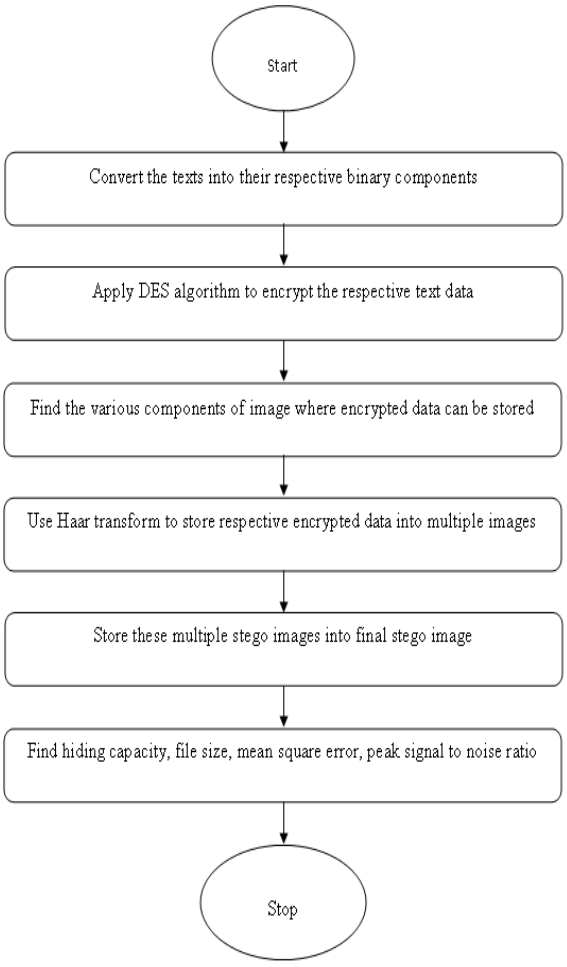


Fig 1. Proposed Algorithm.

**3. Objective Parameters:**
Peak signal to noise ratio, Mean square error and file size are taken as the objective parameters for evaluation.

**3.1 Mean Square Error:**

$$MSE = \frac{\sum_{M,N} [I_1(m,n) - I_2(m,n)]^2}{M \times N}$$

Here M, N is maximum value of rows and columns of image and I1 and I2 are original and final images.

**3.2 Peak Signal to Noise Ratio:**

$$PSNR = 10 \log_{10} \frac{255^2}{MSE}$$

**3.3 File Size:** It is the product of number of pixels present in the image.

## IV. RESULTS

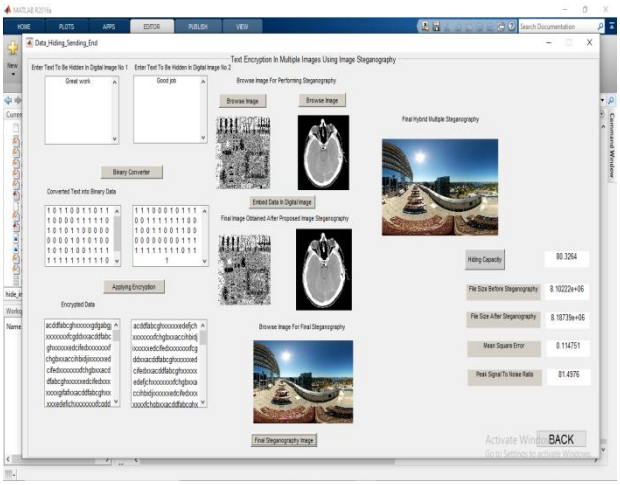

Fig 2. Results of the proposed multiple image steganography technique on Image 1.

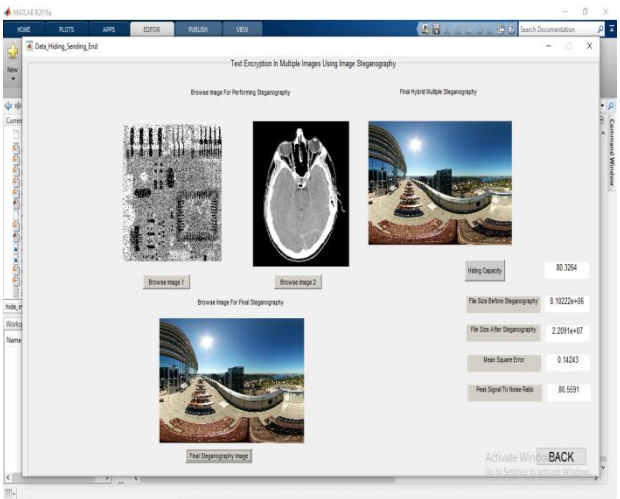

Fig 3. Results of the old multiple image steganography technique on Image 1.

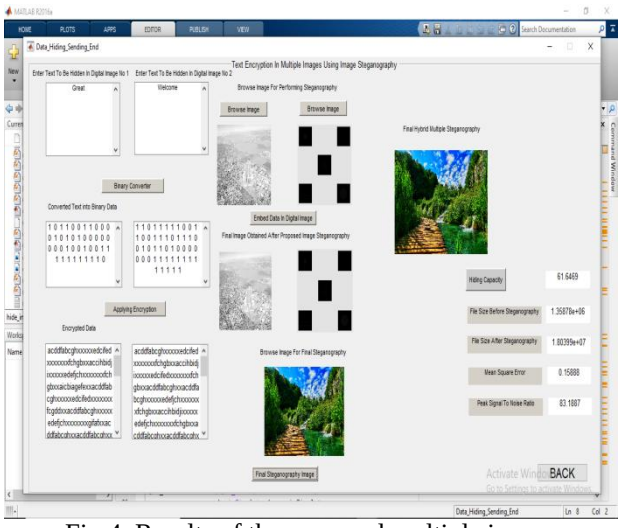

Fig 4. Results of the proposed multiple image steganography technique on Image 2.

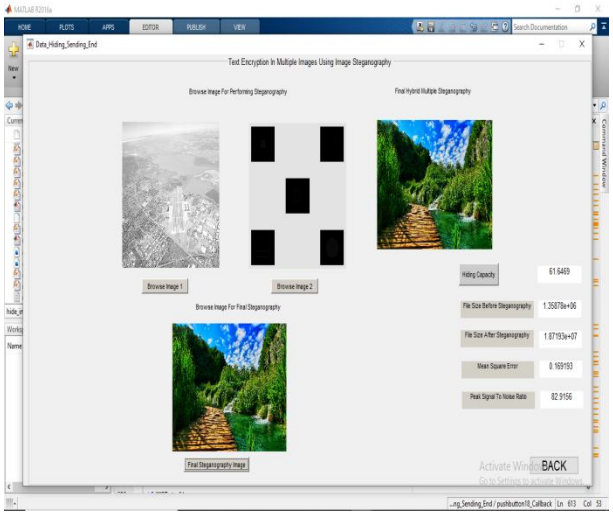

Fig 5. Results of the old multiple image steganography technique on Image 2.

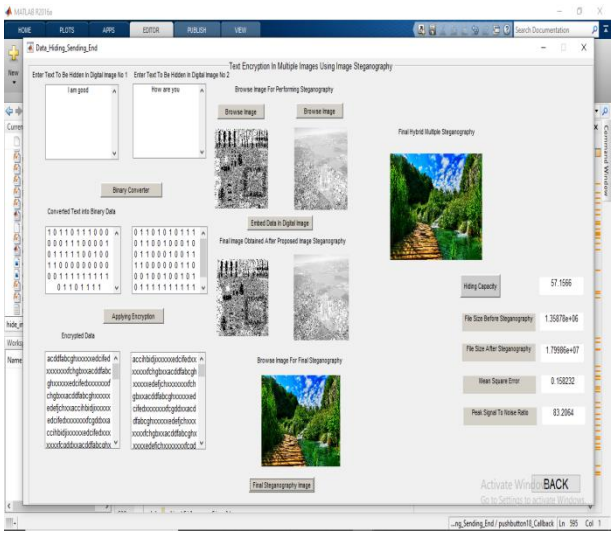

Fig 6. Results of the proposed multiple image steganography technique on Image 3.

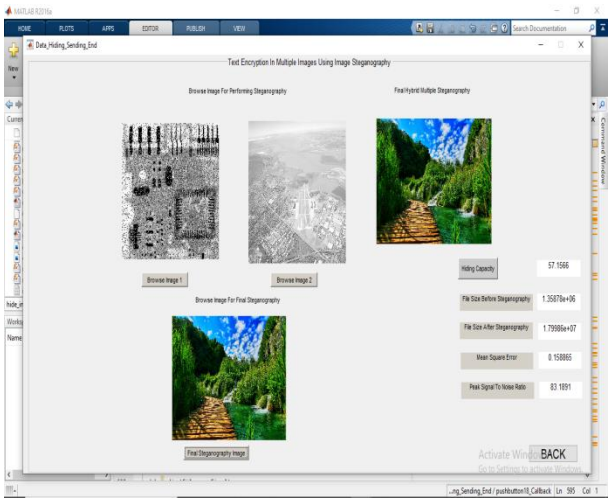


Fig 7. Results of the old multiple image steganography technique on Image 3.

Table 1. PSNR Results of Multiple Steganography.

| Image No | PSNR (Old Method) | PSNR (Proposed Method) |
|---|---|---|
| 1 | 80.5591 | 81.4976 |
| 2 | 82.9166 | 83.1887 |
| 3 | 83.1891 | 83.2064 |

Table 2. MSE Results of Multiple Steganography.

| Image No | MSE (Old Method) | MSE (Proposed Method) |
|---|---|---|
| 1 | 0.14243 | 0.114751 |
| 2 | 0.169193 | 0.15888 |
| 3 | 0.158865 | 0.158232 |

Table 3. File Size Results of Multiple Steganography.

| Image No | FILE SIZE after Steganography (Old Method) | FILE SIZE after Steganography (Proposed Method) |
|---|---|---|
| 1 | 2.2091e+07 | 8.18739e+06 |
| 2 | 1.87193e+07 | 1.80399e+07 |
| 3 | 1.79986e+07 | 1.79986e+07 |


Fig 8. Graph of peak signal to noise ratio parameter of old and proposed Steganography technique.


Fig 9. Graph of peak signal to noise ratio parameter of old and proposed Steganography technique.

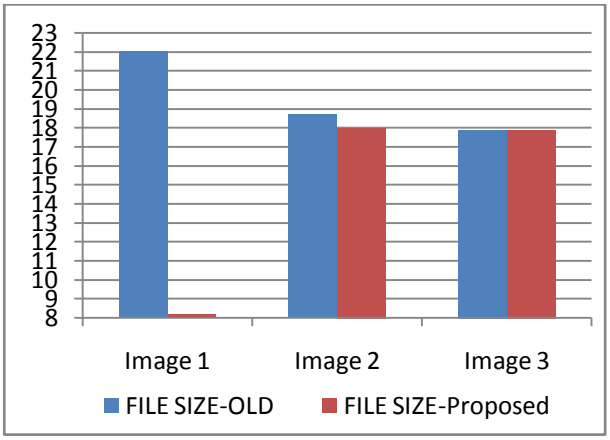


Fig 10. Graph of file size after steganography of old and proposed Steganography technique.

## V. CONCLUSIONS

From the results obtained by performing multiple steganography over various images it is found that the proposed technique performed better in comparison to other old technique. The value of objective parameter mean square error is always less for the case of proposed methodology. Also the value of peak signal to noise ratio is always better in comparison to old technique. File size after steganography is considerably less in maximum cases of proposed methodology.

The proposed system is able to hide text in multiple images after encryption and also these multiple images are successfully hidden into another cover image and then successfully recovered data at receiver side.

In the future work researchers can compare this technique with other multiple steganography techniques which will be proposed in future. Also quality of the proposed technique can also be evaluated by other objective parameters like entropy, correlation so that more information can be gathered about proposed steganography technique.

## VI. ACKNOWLEDGMENT

I am very thankful to my supervisor Mrs. Deepinder Kaur, Head and Assistant professor at the department of computer science & engineering at Shaheed Udham Singh College of Engineering & Technology Tangori Mohali to guide me throughout this research work and continuously encouraging me to move forward.

## REFERENCES

[1] Y. Rafiqi and A. Singh, "Features Analysis and Extraction Techniques for the Image Steganography", Turkish Journal of Computer and Mathematics Education, Vol. 12, No.8, pp. 2103-2109, 2021.
[2] O. Elharrouss, N. Almaadeed, S. Al-Maadeed, "An image steganography approach based on k-least significant bits (k-LSB)", IEEE, pp. 131-135, 2020.
[3] P. Marella, J. Straub, B. Bernard, "Development of a Facial Feature Based Image Steganography Technology", IEEE International Conference on Computational Science and Computational Intelligence, pp. 675-678, 2019.
[4] A. G. Benedict, "Improved File Security System Using Multiple Image Steganography", IEEE International Conference on Data Science and Communication, pp. 1-5, 2019.
[5] S. Mukherjee, S. Roy, G. Sanyal, "Image Steganography Using Mid Position Value Technique", International Conference on Computational Intelligence and Data Science, Vol. 132, pp. 461-468, 2018.
[6] X. Liao, and J. Yin, "Two Embedding Strategies for Payload Distribution in Multiple Images Steganography", IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 1982-1986, 2018.
[7] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," Signal Processing, vol. 90, no. 3, pp. 727–752, 2010.
[8] A. Li, J. He, J. Huang, and Y. Q. Shi, "A survey on image steganography and steganalysis," Journal of Information Hiding and Multimedia Signal Processing, vol. 2, no. 2, pp. 142–172, 2011.
[9] J. Vreugdenhil, K. Iverson, and R. S. Katti, "Image Encyption using Dynamic Shuffling and XORing Processes," in ISCAS , IEEE, 734-737, 2009.
[10] A. Almohammad and G. Ghinea, "Stego-Image Quality and the Reliability of PSNR," Image Processing Theory, Tools and Applications, IEEE, 2010.