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

A Novel Approach of Data Hiding in Encrypted Digital Images using Hybrid Steganography

Research Scholar Savinder Kaur
Dept. of ECE
Universal Institute of Engineering & Technology,
Lalru, Punjab, India
singhjatinder213@gmail.com

Asst. Prof. Shaveta Bala
Dept. of Electrical Engineering,
Universal Institute of Engineering & Technology,
Lalru, Punjab, India
shavetabala@ugichd.edu.in

***Abstract*- In recent time secrecy of online data is the fundamental step in all types of digital communication and it includes digital transmission as well as storage of data and both should also be efficiently secured. There are various ways to secure data. Cryptography and steganography methods are very popular. But some of these methods are very complex and some takes lot of time for execution. Whenever digital images are transmitted through the digital network then these are vulnerable for attack by different intruders which are at different locations. In present research work digital images will be secured for digital transmission by using the image steganography techniques. Discrete wavelets transform (DWT), Discrete cosine transform (DCT) and Least significant bit (LSB) are used worldwide for hiding data inside the digital images. The proposed technique will be based on the hybrid fusion of steganography methods. The DWT, DCT and histogram shifting methods are fused together so that the strength of these methods can be summed up to get the desired results. The proposed technique will be compared with the other standard technique for proving the worthiness of proposed method. For performing the effective performance evaluation of the results of both the compared techniques two parameters peak signal to noise ratio (PSNR) and embedding capacity (EC) are taken as objective parameters. All the implementation is performed in the Matlab 2016 software.**

Keywords – Steganography, DWT, DCT, Histogram shifting, encryption, peak signal to noise ratio, embedding capacity

I. INTRODUCTION

As the world is transforming digitally and with this transformation concern of security of the data becomes essential and will become primary criteria. At present billion of images, audio, video and text files are sent and received through wireless transmission. Hackers are always in search of finding concealed messages in the transmitted messages. Two well known techniques for securing data are cryptography and steganography.

In steganography data is stored in some cover medium so that it is not available easily for some outsider. There are various types of steganography techniques that are used worldwide for securing the data. In defence, banks, income tax department and in other institutions the secrecy of data is very important for transmission purposes.
So encryption of the data has become essential step in all the digital applications. In this research paper a novel technique for multiple image steganography is proposed. Various images of tagged image file format can be easily saved into colored image of jpeg format with various hybrid algorithms.

II. LITERATURE SURVEY

M. Sharifzadeh et al. [1] in 2020 proposed a statistical framework for the image steganography. Authors used the multivariate Gaussian model where both the cover as well as final stego image was treated as its variables. Here authors tried to find the detection error of the different detectors by using this statistical model. Here authors first embedded the secret message inside and after that encryption process was followed. First the error was detected and then applied to the model for steganography and then further this model was extended for batch image steganography. Authors compared the proposed method with other state of art methods of steganography and the proposed algorithm performed better in comparison to these methods.

D. Watni et al. [2] in 2019 performed a deep analysis of special image format jpeg and performed a comparative analysis with this image format with various known image steganography methods. Author compared jpeg images with other well known methods like F5, Yass, Outguess, jSteg and other methods. Authors took embedding capacity and robustness of the proposed algorithm as objective parameters for evaluation of steganography algorithms. From the results it was cleared that F5, model based steganography, edge adaptive and universal distortion methods were really fast in performing

steganography. While jSteg, Outguess, Yass were quite slow in performing the steganography efficiently.

L. Kothari et al. [3] in 2017 proposed a web relied image steganography method that used the combined effort of steganography and as well as of cryptography. On the sender side authors first encrypted the secret message with some key of particular length and then converted into ASCII code and finally to binary format. Finally this secret text was stored on the web pages. No one was able to find that some secret message was stored on the web. Authors tried to save the secret message with four different ways and showed the efficiency of all the techniques for performing steganography.

V. Sharma et al. [4] in 2015 proposed two different methodologies which were hybrid of both the cryptography and of steganography. In the first methodology authors converted the bmp image into text with the help of suitable key and with simplified DES method. In the second methodology authors applied the simplified DES method on the bit map digital image and used a specific image key. These contents were then hid into different digital image. Authors used Matlab software for the evaluation purposes. Results obtained from both the techniques were reliable. For performing the performance evaluation of both methods authors had not used any kind of objective parameter.

III. METHODOLOGY AND PROPOSED ALGORITHM

Research methodology and the proposed algorithm are discussed below.

1. Methodology

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

Step 1. Apply DWT on the first uploaded image
Step 2. Apply DCT on the second uploaded image
Step 3. Now save both images into final stego image at sender side
Step 4. Now perform Histogram Shifting of the final stego image
Step 5. At the receiver side perform Histogram Aligning and both the original images are recovered efficiently

2. Proposed Algorithm

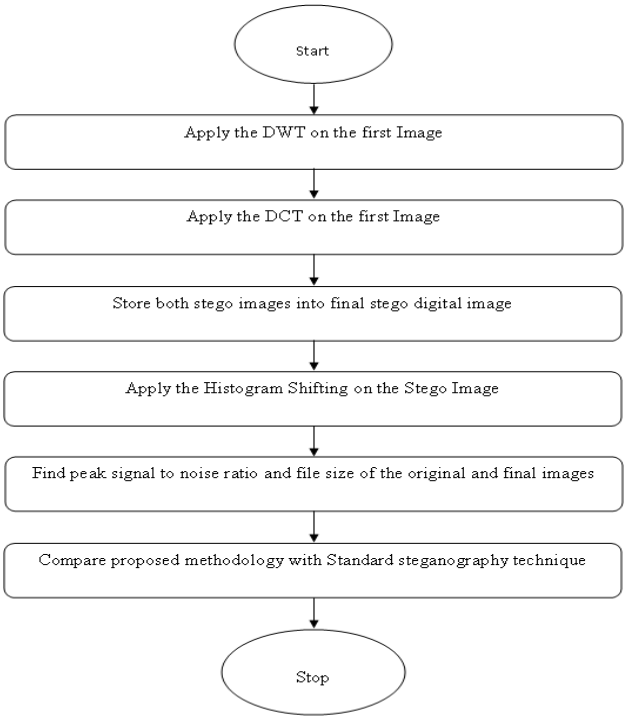

Fig.1. Proposed Algorithm

3. Objective Parameters

Peak signal to noise ratio and file size available on the disk are taken as the objective parameters for evaluation.

1. Peak Signal to Noise Ratio

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

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

2. File Size

It is the multiplication of number of pixels present in the digital image.

IV. RESULTS

Fig. 2: Results of the standard steganography technique on image number 1

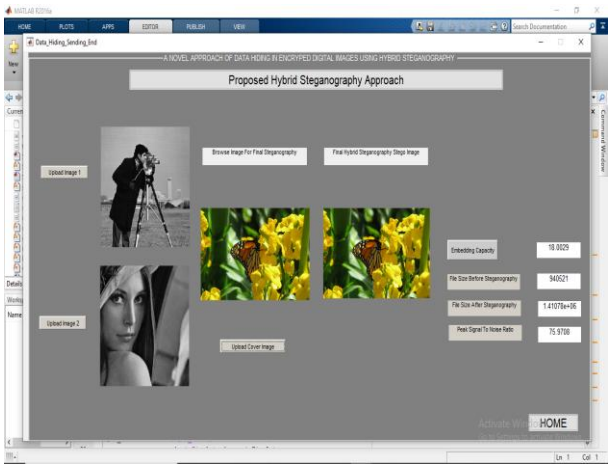

Fig. 3: Results of the proposed steganography technique on image number 1

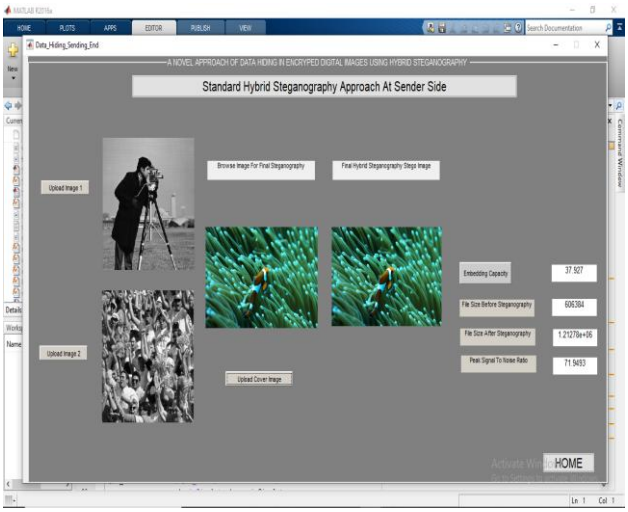

Fig. 4: Results of the standard steganography technique on image number 2

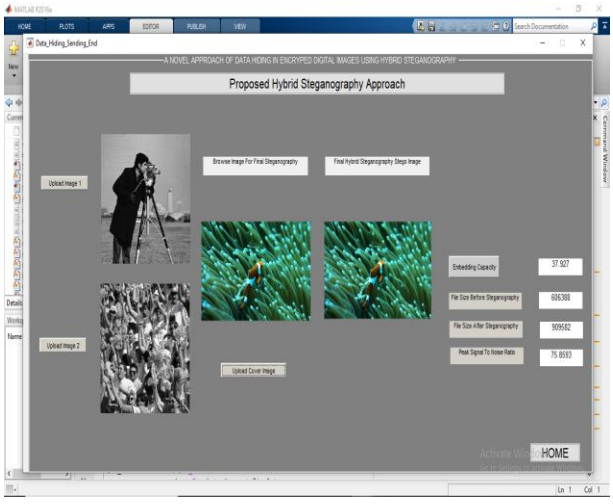

Fig. 5: Results of the proposed steganography technique on image number 2

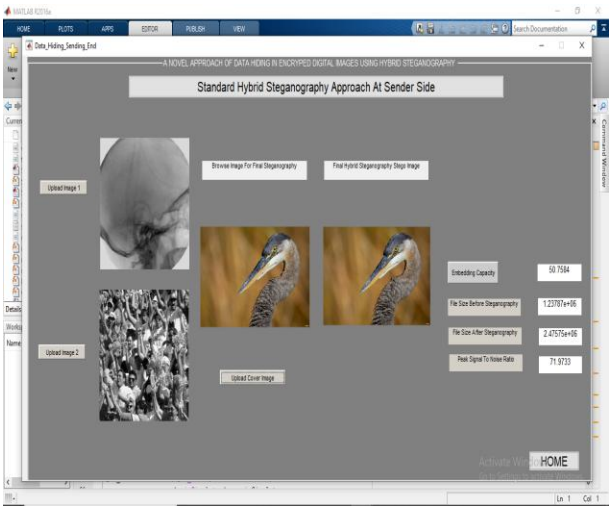

Fig. 6: Results of the standard steganography technique on image number 3

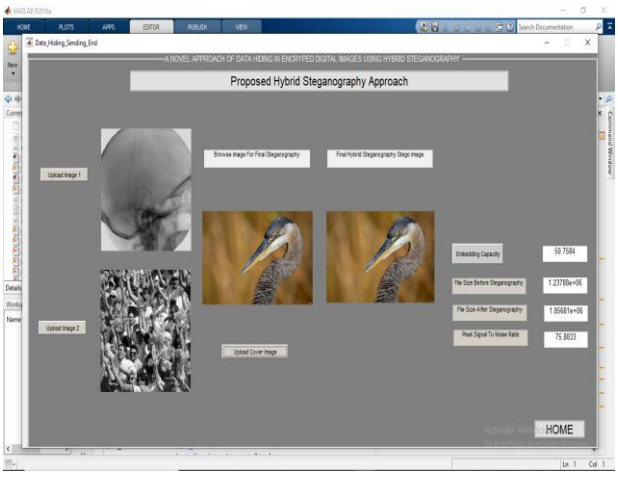

Fig. 7: Results of the proposed steganography technique on image number 3

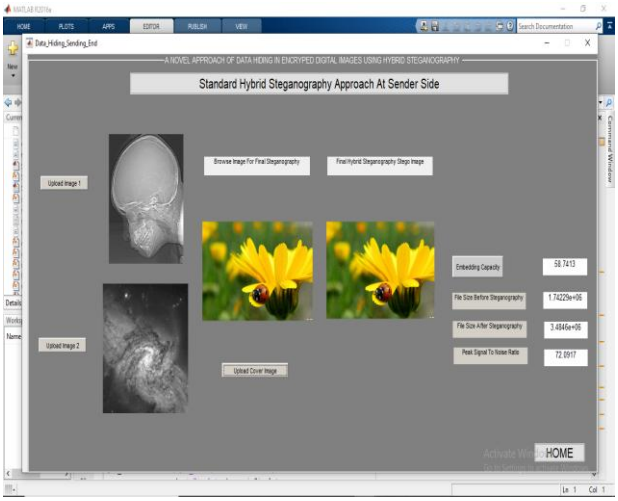

Fig. 8: Results of the standard steganography technique on image number 4

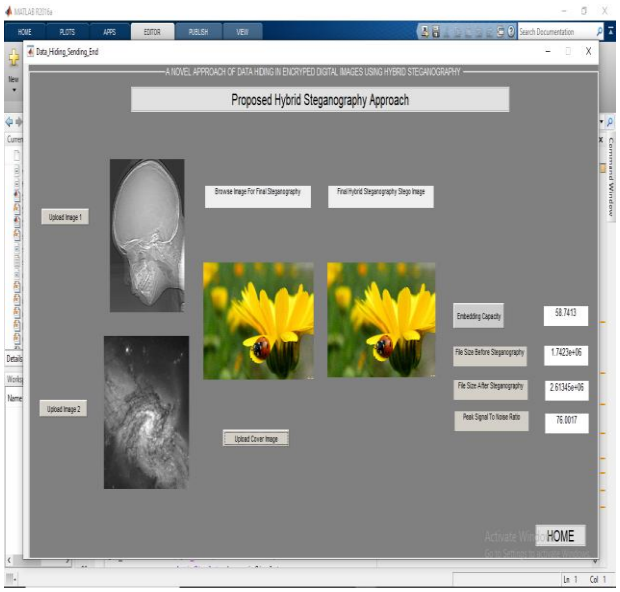

Fig. 9: Results of the proposed steganography technique on image number 4

Table I: PSNR Objective Parameter Values

Image No.	PSNR (Standard Method)	PSNR (Proposed Method)
1	72.0608	75.9708
2	71.9493	75.8593
3	71.9733	75.8833
4	72.0917	76.0017

Table II: File Size Objective Parameter Values

Image No.	FILE SIZE after Steganography (Standard Method)	FILE SIZE after Steganography (Proposed Method)
1	1.88104e+06	1.41078e+06
2	1.21278e+06	.909582e+06
3	2.47575e+06	1.85681e+06
4	3.4846e+06	2.61345e+06

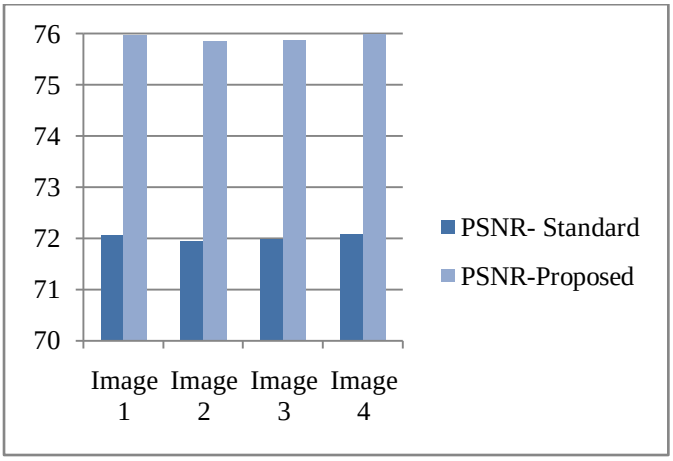

Fig. 10: Graph of peak signal to noise ratio parameter of steganography techniques

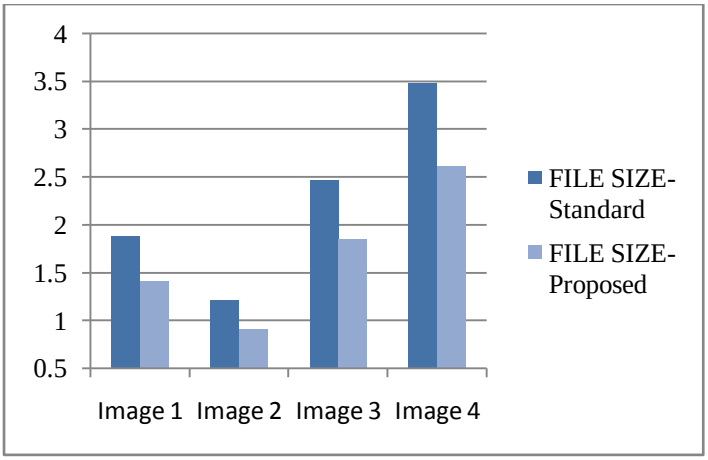

Fig. 11: Graph of file size in MB after steganography of steganography techniques

V. CONCLUSIONS

From the outcomes of the experiment it is cleared that proposed technique performed better in comparison to standard technique for image steganography. Value of peak signal to noise ration of proposed technique is always better in comparison to standard technique. Also the value of file size after steganography is always less in comparison to standard technique. Proposed algorithm always performed better in comparison to standard multiple image steganography technique. In the future more algorithms can be compared with the proposed algorithm. Various other objective parameters can also be taken for more effective performance evaluation of algorithms.

REFERENCES

[1] M. Sharifzadeh, M. Aloraini and D. Schonfeld, "Adaptive Batch Size Image Merging Steganography and Quantized Gaussian Image Steganography," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 867-879, 2020.
[2] D. Watni and S. Chawla, "A Comparative Evaluation of Jpeg Steganography," 5th International Conference on Signal Processing, Computing and Control (ISPCC), pp. 36-40, 2019.
[3] L. Kothari, R. Thakkar and S. Khara, "Data hiding on web using combination of Steganography and Cryptography," International Conference on Computer, Communications and Electronics (Comptelix), pp. 448-452, 2017.
[4] V. Sharma and Madhusudan, "Two new approaches for image steganography using cryptography," Third International Conference on Image Information Processing (ICIIP), pp. 202-207, 2015.
[5] K. Thangadurai and G. Sudha Devi, "An analysis of LSB based image steganography techniques," International Conference on Computer Communication and Informatics, pp. 1-4, 2014.
[6] V. Holub, J. Fridrich, and T. Denemark, "Universal distortion function for steganography in an arbitrary domain," EURASIP Journal on Information Security, vol. 2014, no. 1, pp. 1–13, 2014.
[7] T. Denemark, V. Sedighi, V. Holub, R. Cogranne, and J. Fridrich, "Selection-channel-aware rich model for steganalysis of digital images," IEEE International Workshop on Information Forensics and Security (WIFS), pp. 48–53, 2014.
[8] 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.
[9] T. Pevny, P. Bas, and J. Fridrich, "Steganalysis by subtractive pixel adjacency matrix," IEEE Transactions on Information Forensics and Security, vol. 5, no. 2, pp. 215–224, 2010.
[10] https://support.microsoft.com/en-us/windows/wallpapers-5cfa0cc7-b75a-165a-467b-c95abaf5dc2a
[11] http://www.imageprocessingplace.com/DIP-3E/dip 3e_bo ok_ images_downloads.htm