International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 02 | Feb 2021 www.irjet.net p-ISSN: 2395-0072

A Deep Neural Network Spatial Domain Steganography Method In Image Processing

Tajinder Preet Kaur[1], Pratibha[2], G. N. Verma[3]

[1]*M. Tech Student, Department of Computer Science & Engineering, SSIET, IKGPTU, Punjab, India*
[2]*Assistant Professor, SSIET, IKGPTU, Punjab, India*
[3]*Professor, SSIET, IKGPTU, Punjab, India*

Abstract - *In the digital or data communication the most important entity is the data only. If the data is confidential then it becomes essential to wrap or encrypt the data in a manner that no one can access it or not even get a hint about it. One of the well known way of concealing the data is the principle of steganography. This methodology stores one type of data into other or similar type of data such that no one can access it. One of the way is the concealing the secret data inside the digital image so that data becomes invisible in the image. Some techniques store the data in the cover image and then perform some kind of encryption so that complexity of the algorithm will increase and eventually will become hard to find the hidden data. In the present research work a new steganography technique is proposed based on the deep neural network. The technique used various components to store the data so that no one can access it. The proposed technique is compared with other steganography techniques. Various objective parameters like peak signal to noise ratio and mean square error are used for performance evaluation of the proposed technique.*

Key Words: Image Processing, Steganography, Neural network, Deep learning, Matlab, Spatial domain.

1. 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. Most of the time it is found that just the use of cryptography is not enough and there is requirement of some way where the data is not visible at all.

Steganography is the field of hiding of information for the security purpose. Here some message or information gets hide into some kind of media like digital image, digital video and digital audio as well as in text. In steganography main limitation is the volume of how much information can be embedded and visual information of hidden digital image. There are various tools or algorithms which hide the data or information into the digital media such that hidden information becomes inaccessible and imperceptible.

Some algorithms store the digital information in the digital image in a way that it becomes just impossible to distinguish amid original digital image and the stego digital image. Various researchers have proposed various techniques for information hiding in digital images. All have different types of benefits and limitations also.

2. LITERATURE SURVEY

S. Mukherjee et al. [1] proposed a reliable and an efficient digital communication steganographic methodology of hiding the important data or information. In the first phase of the proposed algorithm the author had used Arnold mathematical transform for covering the data with the cover digital image. The outcome of this step was that data bits were scrambled and changed the orientation of image pixels. In the second phase of the proposed algorithm authors had utilized Mid Position Value (MPV) method which took data bits from the secret digital image and embedded it inside the covered digital image. In the last phase of the proposed algorithm authors had applied the inverse Arnold transformation on the final digital image and the result of final step was a stego digital image. Authors had used various objective parameters for benchmark analysis. From the results it was found that algorithm had remarkable results in embedding way but there was some distortion was present in the digital image quality.

S. H. Soleymani et al. [2] proposed a steganography algorithm that could hide some scanned document inside the digital image. The benefit and main purpose of proposed stego algorithm was to increase the capacity of hiding the data. Authors in the first phase applied the halftoning algorithm that changed scanned document image into a binary digital image that was sparse matrix. In the second phase this image was embedded in low significant bits of hidden pixels. Further authors utilized the standard deviation which was further utilized for filtering of hidden stego image pixels and the stego image quality was also preserved. Here the authors had not selected the smooth region for embedding purpose which fell into the human visual system. From the experiments authors had concluded that their proposed algorithm worked better in comparison to other known algorithms and the average value of peak signal to noise ratio and embedding rate was satisfactory.

S. Ash et al. [4] proposed a technique based on the steganographic horizon approach in which secret information was stored in a manner that hackers could not get any clue about it. Also if some intruder got any clue about it then still it

was just impossible to figure out the secret data. In the first step of the proposed algorithm author operated well known two dimensional Haar Discrete Wavelet Transform over the carrier digital image so that coefficient matrices could be obtained. In the second phase authors applied Prime First Mapping (PFM) to embed the data inside the matrices. Authors found that with the help of proposed methodology very high value of embedding capacity was obtained also the average value of peak signal to noise ratio showed the invisibility of the stego digital image which reflected good value of similarity measurement for the stego image.

I. Avcibus et al. [8] performed the steganogrpahy analysis of digital images with the help of stego image algorithms. The message between two users was examined by the third user willingly to check whether that user could extract the hidden information or could also modify the data. It was done to check whether the stego algorithms were not sending statistical evidence of the information stored in its image in communication path. Authors had used the analysis of variance (ANOVA) statistical method for recognizing the image quality metrics as feature matrix so that it could become easy to distinguish amid cover as well as stego digital images. Authors trained the classifier with help of multivariate regression and performed three types of experiments. From the simulation results authors found that it was possible to find the difference amid the cover and stego digital images.

2. RESEARCH METHODOLOGY

In this particular research deep convolutional neural network is used for training the dataset. Convolutional neural network provides various features like extracting different features automatically, use of convolution for downsampling and use of prediction layer at the extreme end of the network. Without the knowledge of weights cost no one can know what data is stored. For programming purposes Matlab 2016a is used in the implementation of research work.

2.1 Proposed Technique

There are two stages of the proposed system. First one is applied at sender side and second one is applied at receiver side. Collectively both the sender and receiver side contains the six components. First and second layer contains the binary conversion and encryption of data. In the third layer the data is embedded in stego image. In the fourth and fifth layer from the stego image the encrypted data and cover image is extracted. In the sixth layer binary conversion is performed on the decrypted data to get the original data.

For the sender side the steps followed are given below.

(1) Capture the data to be hidden.
(2) Perform binary conversion of the data.
(3) Perform encryption of the binary converted data.
(4) Take the cover digital image.
(5) Hide the digital data into the cover image so that there is negligible distortion in the histogram.

For the receiver side the steps followed are given below.

(1) Input the encrypted stego digital image.
(2) Extract the encrypted data from the stego image.
(3) Perform decryption of the encrypted data.
(4) Perform the binary conversion of the decrypted data.
(5) Extract the hidden data.

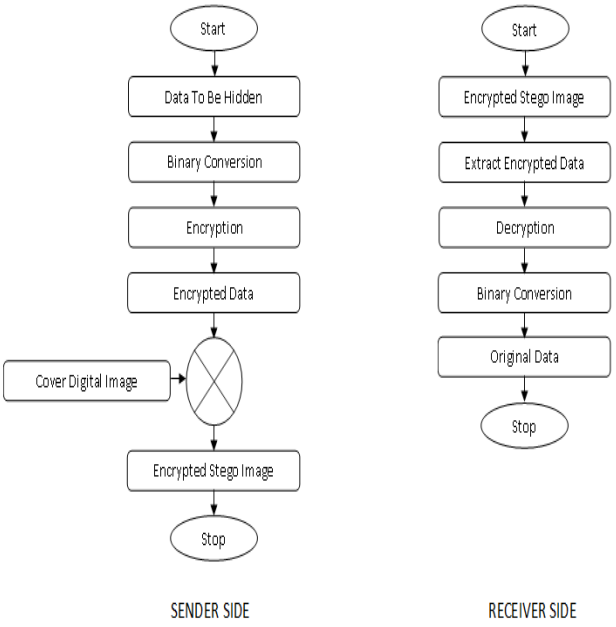

Fig -1: Architecture of proposed system

2.2 Objective Performance Evaluation

For evaluating the performance of the proposed algorithm various objective parameters are used.

(i) Mean Square Error (MSE)

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

(ii) Peak Signal to Noise Ratio (PSNR)

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

Here M, N are row and columns of image and I_1 and I_2 are original and final images.

3. RESULTS

In the experiment analysis the proposed algorithm is compared with the standard steganography technique with LSB.

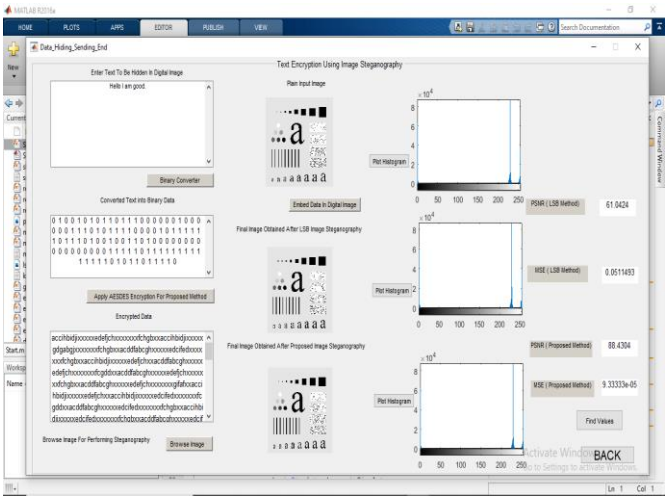

Fig -2: Sender Side Scenario 1

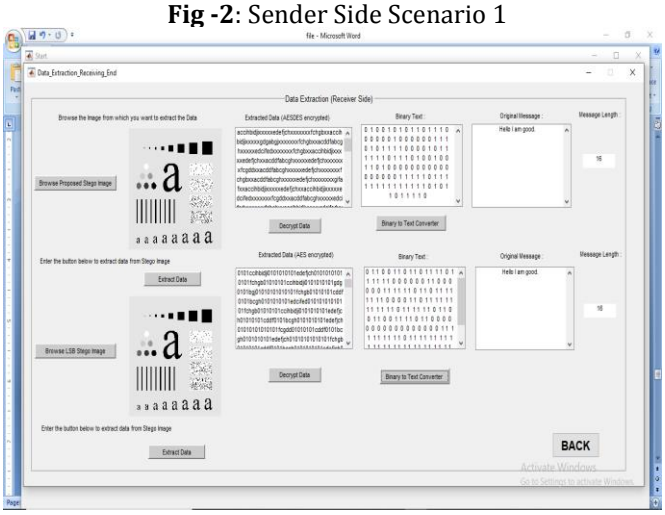

Fig -3: Receiver Side Scenario 1

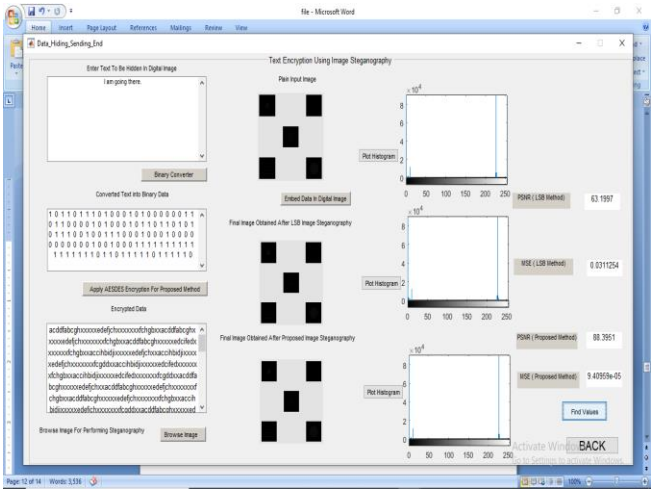

Fig -4: Sender Side Scenario 2

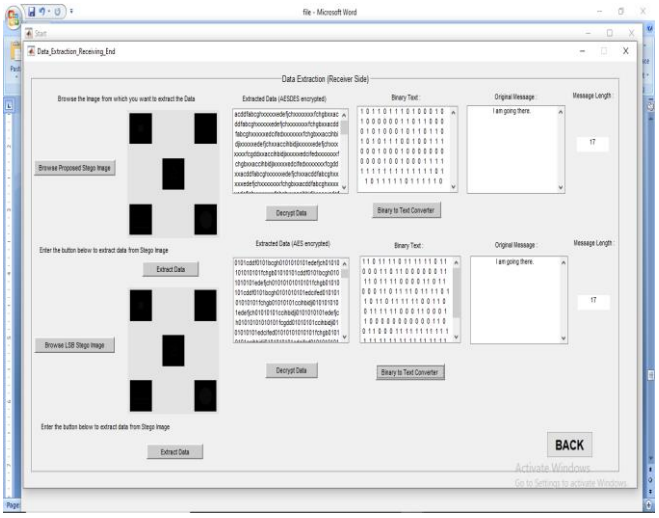

Fig -5: Receiver Side Scenario 2

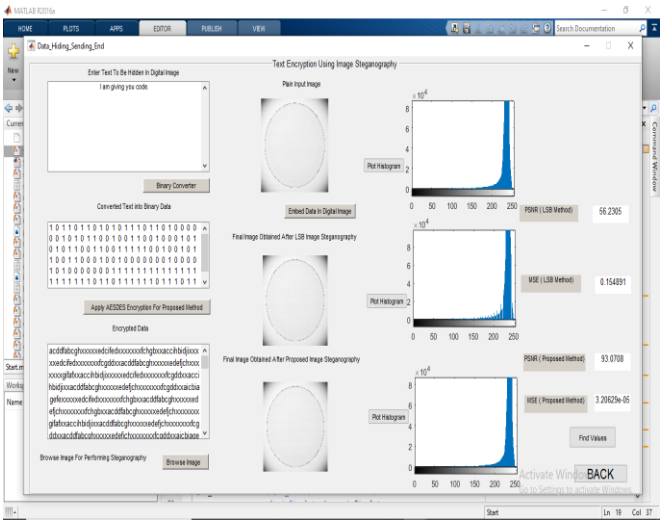

Fig -6: Sender Side Scenario 3

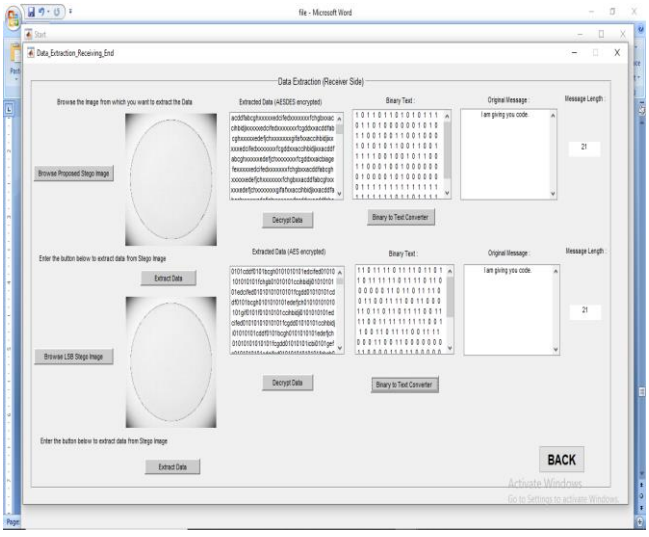

Fig -7: Receiver Side Scenario 3

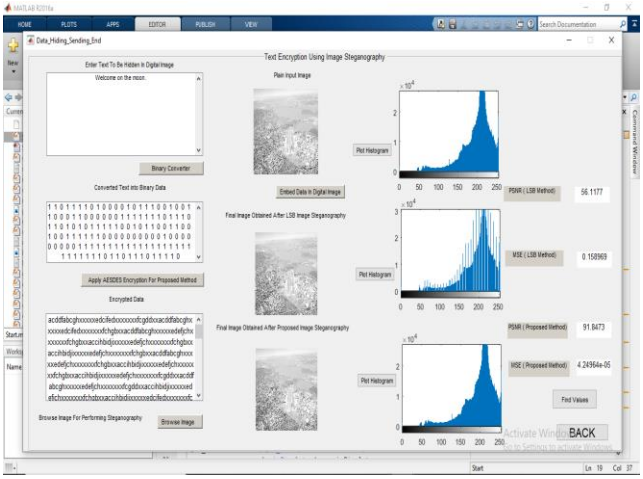

Fig -8: Sender Side Scenario 4

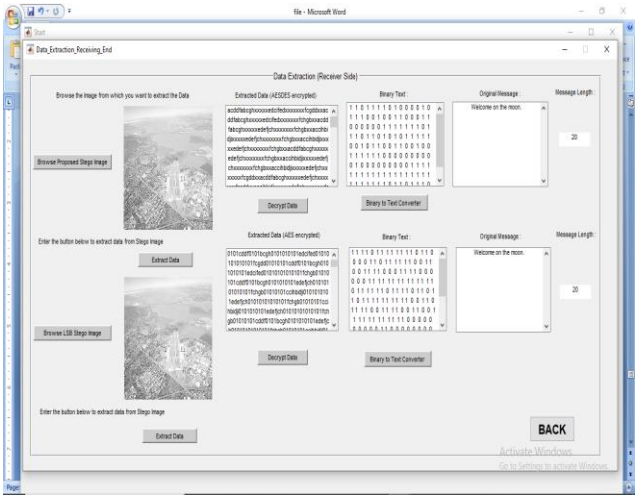

Fig -9: Receiver Side Scenario 4

Table -1: Objective Parameter Analysis

Scenarios	LSB Method		Proposed Method	
	PSNR	MSE	PSNR	MSE
Case 1	61.0424	0.0511	88.4304	0.00009
Case 2	63.1997	0.03112	88.3951	0.00009
Case 3	56.2305	0.15489	93.0708	0.00003
Case 4	56.1177	0.15896	91.8473	0.00004

3. CONCLUSIONS

The performance of the proposed steganography algorithm is compared with the standard LSB algorithm. From the evaluation of the results it is cleared that in all scenarios the proposed algorithm worked better in comparison to LSB algorithm. Further peak signal to noise is always higher for the proposed algorithm. Also it is found that mean square error is totally negligible for the proposed algorithm. It means it will become nearly impossible to trace whether it is original image or a stego image.

In the future work the algorithm can be evaluated with other known algorithms to check its efficiency. Also various other objective parameters can be used to check the performance of the proposed algorithm.

REFERENCES

[1] S. Mukherjee, S. Roy and G. Sanyal, "Image Steganography Using Mid Position Value Technique," ICCIDS, pp. 461-468, 2018.

[2] S. Soleymani, A. Taherinia, "High capacity image steganography on sparse message of scanned document image (SMSDI)." Multimed Tools Appl. Vol. 76, pp. 20847-20867, 2017.

[3] X. Ma, Z. Pan, S. Hu,L. Wang, "Large capacity and high quality reversible data hiding method based on enhanced side match vector quantization," Multimedia Tools Appl., Vol. 75(1), pp. 71–91, 2016.

[4] S. Ash, S. Mukherjee and G. Sanyal, "A DWT Based Steganographic Method using Prime First Mapping (PFM)," Advances in Computing and Communicational Engineering, ICACCE, pp. 471-476, 2015.

[5] Y. Yamaguchi, "Extended visual cryptography for continuous-tone images: effect of the optimum tone mapping," IJICT, Vol. 7(1), pp. 25- 39, 2015

[6] J. Vreugdenhil, K. Iverson and R. S. Katti, "Image Encyption using Dynamic Shuffling and XORing Processes," in 'ISCAS' , IEEE, Vol. 734-737, 2009.

[7] V. Potdar and E. Chang, "Gray level modification steganography for secret communication," IEEE International Conference on Industrial Informatics, pp. 355–368, 2004.

[8] I. Avcibas, N. Memon, and B. Sankur, "Steganalysis using Image Quality Metrics", IEEE Trans. on Image Processing, vol. 12, pp. 221-229, 2003.

[9] A. Sehgal, A. Jagmohan, N. Ahuja, "High capacity data embedding in the wavelet domain", in 'ICIP(3)', pp. 979-982, 2001.

[10] T. H. Lan, M. F. Mansour and A. H. Tewfik, "Robust High Capacity Data Embedding," in 'ICIP' , pp. 581-584, 2000.