Secure Image of Reversible Data Hiding and Deep Learning Algorithms for Image Reconstruction

Somya Jain
M. Tech. Scholar
Department of Computer Science and Engineering
LNCT, Bhopal

Rahul Sahu
Assistant Professor
Department of Computer Science and Engineering
LNCT, Bhopal

ABSTRACT

Steganography is one of the powerful techniques in data hiding. It is the branch of secret communication where the cover image is recovered after the embedded data is extracted from the stego image. One of the applications of steganography is Reversible Data hiding (RDH) and deep learning. RDH is the method in which original cover can be losslessly recovered after the embedded message is extracted. Deep learning models are well known as deep black boxes in which the process from the input to the output is very complex, and thus the deep learning model for information hiding is almost impossible for opponents to reconstruct. An attempt has been made to present a Threshold Based Reversible Data Hiding (TBRDH) and deep learning by creating space before encryption and different metric parameters like mean square error, PSNR, SSIM, NAE and NCC are calculated for the cover image and reconstructed image.

Keywords

Reversible Data, Image Reconstruction, Secure Image, PSNR, SSIM

1. INTRODUCTION

Reversible data hiding (RDH) is one of the important and successful applications of Steganography. It is the branch which deals with covert communication. The word steganography is derived from the Greek word stegnos means covered or concealed and graphine means writing [1].

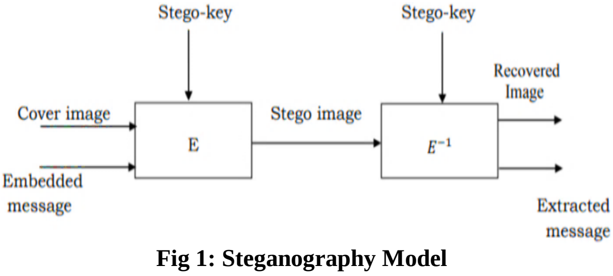


Fig 1: Steganography Model

Not at all like steganography in reversible information concealing mystery messages are inserted into a spread picture by marginally changing its pixel esteems and concentrate the messages at the recipient end with reversibility [2, 3]. The model for steganography is appeared in Fig 1.
The primary standard of information concealing lies in two different ways: one is inserting and the other one is extricating measure. In the principal case i.e., implanting stage secretive data is embedded into spread medium. By doing as such there will be alteration in the spread medium. This embedded secretive data after changed to the spread medium is called as stamped/stego information. In the optional stage i.e., extraction stage the clandestine data is extricated from the checked/stego information and recoups the spread medium. The overall information concealing framework is appeared in Fig 2.

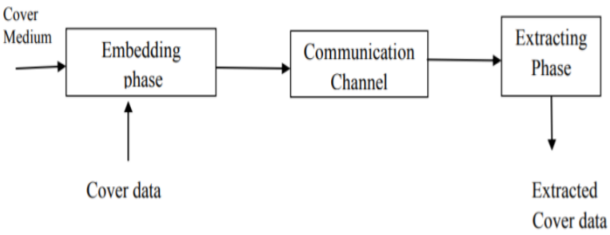


Fig 2: General Data Hiding system

Irreversible Data Hiding:- It is the process of embedding covert data into the cover medium while at the extraction phase only the covert data is extracted but there is a loss in cover medium i.e. from stego medium, input cover medium cannot completely recovered at the receiver end [4].

Reversible Data Hiding:- It is the process of embedding secret data into the cover medium with extraction of the secret data from the cover medium without any loss in the cover medium at the receiver end. As there is loss in cover medium in irreversible data hiding researchers have contributed their work in the field of reversible data hiding and it been challenging area for many researchers to provide solutions [5].

2. DEEP LEARNING

Deep learning is one of AI techniques. It comprises of progressive organized layers that can interpret input information to significant yields in a discovery model. Deep learning strategies include wide applications inside various research investigation, for example, graphical displaying of information, neural systems, parameters streamlining, picture investigation, design acknowledgment furthermore, signal preparing. Numerous profound learning models in different applications depend on the model, proposed by Yann LeCun for transcribed acknowledgments by utilizing profound directed backpropagation convolutional organize [6].
Deep neural system is a straightforward ordinary neural system with progressively concealed layers with the goal that it gets further. The profound neural engineering can be considered as the speculation of a direct or on the other hand calculated relapse neural system designs. Each neuron is enacted in a straight mix of information and a few learning parameters, which are trailed by a component savvy nonlinear development.

A neural system design comprises of various layers L of a weighted neuron through which enactment is performed. Multi-Layer Perceptron (MLP) is a class of feedforward neural system with at least two layers between information and yield layers. The feedforward implies that information owes one way from contribution to yield layers. The backpropagation learning calculation is utilized to prepare the MLP. MLP is utilized in numerous applications, for example, design classification, acknowledgment, guess, and expectation. MLP for the most part takes care of the issues which are not directly distinct as appeared in Fig. 3.

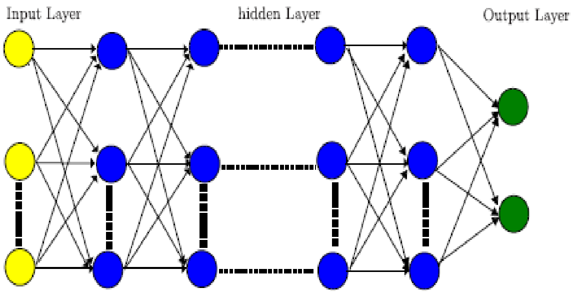


Fig 3: Deep neural network

In any case, there are elective strategies to prepare an entire profound neural arrange start to finish in a directed manner. These other option strategies can be better executed by specified sort of neural arrange, i.e., the convolutional neural system (CNN).

These days, CNN gets increasingly well known in clinical picture preparing what's more, turns into a decent decision for the analysts in clinical picture investigation. The accompanying subsections clarify the fundamental sorts of neural systems and bit by bit usage of the technique with their impediments and points of interest.

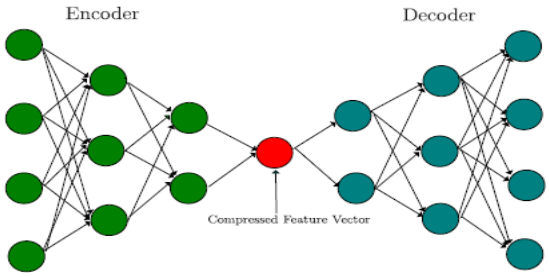


Fig. 4: Deep auto-encoder (AE)

3. REVERSIBLE DATA HIDING METHOD

Data can be embedded into images in two ways: one is Creating Vacant Space after Encryption (CVSAE) and other is Creating Vacant Space Before Encryption (CVSBE). In the primary case there are few limitations: 1) embedded data can be completely recovered from the cover medium but there is distortion in cover medium i.e. cover medium cannot be completely recovered. 2) As embedding capacity keeps on increasing there will be increasing distortion at the receiver end. To overcome these limitations we create vacant space before encryption by taking Threshold value T such that the original cover image can be recovered at the receiver without any errors and also maintains high embedding capacity with improved peak signal-to-noise ratio (PSNR) compared to previous methods. From Fig 3, the vacant space is created by dividing the image into two regions as X and Y using the threshold values. Let T1 and T2 are two different thresholds. In general T1 and T2 are selected as 0.25(max 0.35bpp) and 0.2bpp (max 0.3bpp) respectively so that there will not be much degradation of the quality of the image. The threshold T1 is for choosing the least significant bit plane for the subimage X and the threshold T2 is for replacing pixels in image Y with the pixels of X image whose threshold values are less than 0.35bpp. The pixels whose threshold values are less than 0.35bpp in image X are replaced by embedded data that is to be sent from source to destination.

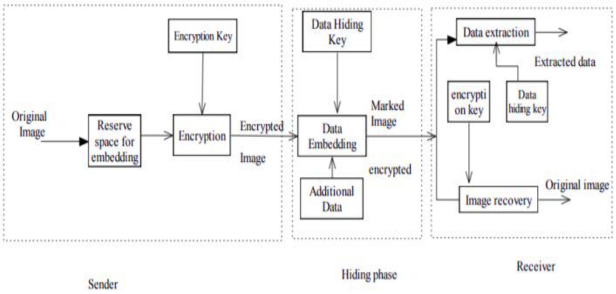


Fig 5: Schematic representation of Reversible Data Hiding

Generating Encrypted Images:- To generate the encrypted images, first the original cover image is divided into two portions as X and Y so as the LSB's of X are reversible embedded into Y using RDH algorithm as shown in Fig 4. The LSB planes of X are used to store information bits.

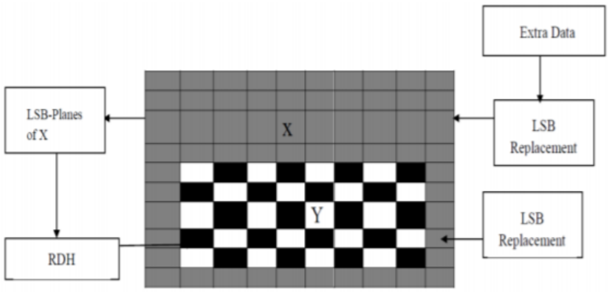


Fig 6: Representation of Image partitioning

Let us consider P as original cover gray scale image of 8-bit with M x N dimensions and pixels ranging from 0 to 255 and let the size of the secret data as Q. Now based on Q the sender extracts overlapping blocks.

Image recovery after Data retrieval: - From the stego images data can be extracted in two ways:

- Extraction from encrypted images.
- Extraction from decrypted images.

In the first case, using data hiding key, the three least significant bits embedded into the encrypted image will be extracted and then the receiver checks the server for updating by LSB replacement. It is secured than other methods as data is extracted from the encryption images. In the second case the sender decrypts the image first and then extracts data from the decrypted images. When compared to Second case all the changes are done in encrypted stage for embedding and extracting data in the first case.

4. SIMULATION RESULT

The simulation results are presented by taking test cover gray scale images as: “Lena”, “Airplane”, “Barbara”, “Baboon”, “Peppers” and “Boat” as in Fig. 7.

Fig. 7: Test cover grey scale images for simulation

Embedding Rate (ER) is the secret amount of data to be embedded into the cover image per pixel denoted as bits per pixel (bpp). The performance metric results are show for all the test cover images at different embedding in Table 1. For Lena image at embedding rate of 0.1 bpp the encrypted form, stego image and recovered images are shown in Fig 8.

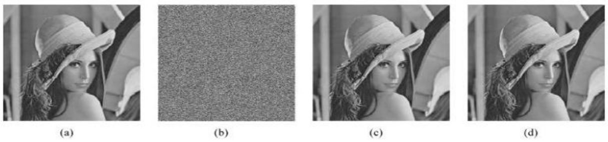
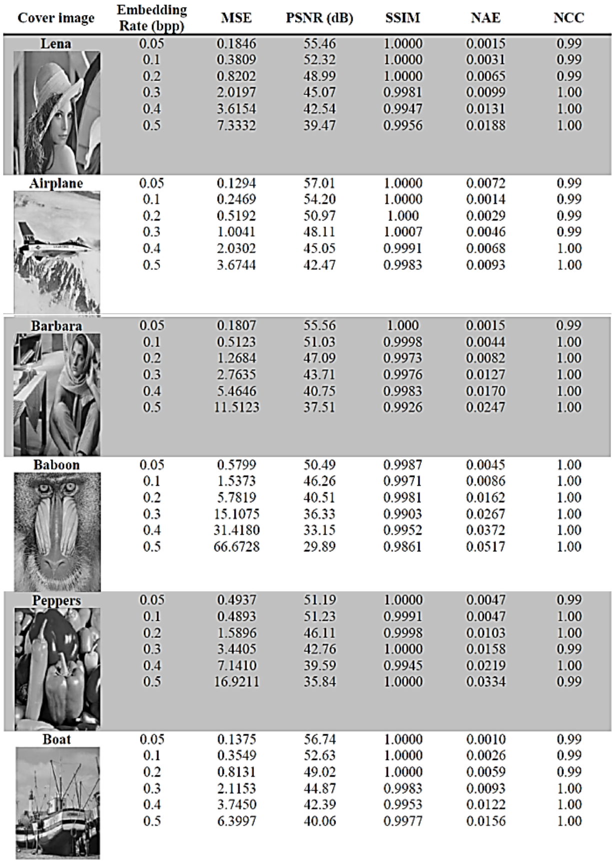


Fig 8: a) Lena Image b) Encrypted form c) Stego image and d) Recovered image

Table 1: Performance metrics at different embedding rates



Cover image	Embedding Rate (bpp)	MSE	PSNR (dB)	SSIM	NAE	NCC
Lena	0.05	0.1846	55.46	1.0000	0.0015	0.99
	0.1	0.3809	52.32	1.0000	0.0031	0.99
	0.2	0.8202	48.99	1.0000	0.0065	0.99
	0.3	2.0197	45.07	0.9981	0.0099	1.00
	0.4	3.6154	42.54	0.9947	0.0131	1.00
	0.5	7.3332	39.47	0.9956	0.0188	1.00
Airplane	0.05	0.1294	57.01	1.0000	0.0072	0.99
	0.1	0.2469	54.20	1.0000	0.0014	0.99
	0.2	0.5192	50.97	1.000	0.0029	0.99
	0.3	1.0041	48.11	1.0007	0.0046	0.99
	0.4	2.0302	45.05	0.9991	0.0068	1.00
	0.5	3.6744	42.47	0.9983	0.0093	1.00
Barbara	0.05	0.1807	55.56	1.000	0.0015	0.99
	0.1	0.5123	51.03	0.9998	0.0044	1.00
	0.2	1.2684	47.09	0.9973	0.0082	1.00
	0.3	2.7635	43.71	0.9976	0.0127	1.00
	0.4	5.4646	40.75	0.9983	0.0170	1.00
	0.5	11.5123	37.51	0.9926	0.0247	1.00
Baboon	0.05	0.5799	50.49	0.9987	0.0045	1.00
	0.1	1.5373	46.26	0.9971	0.0086	1.00
	0.2	5.7819	40.51	0.9981	0.0162	1.00
	0.3	15.1075	36.33	0.9903	0.0267	1.00
	0.4	31.4180	33.15	0.9952	0.0372	1.00
	0.5	66.6728	29.89	0.9861	0.0517	1.00
Peppers	0.05	0.4937	51.19	1.0000	0.0047	0.99
	0.1	0.4893	51.23	0.9991	0.0047	1.00
	0.2	1.5896	46.11	0.9998	0.0103	1.00
	0.3	3.4405	42.76	1.0000	0.0158	0.99
	0.4	7.1410	39.59	0.9945	0.0219	1.00
	0.5	16.9211	35.84	1.0000	0.0334	0.99
Boat	0.05	0.1375	56.74	1.0000	0.0010	0.99
	0.1	0.3549	52.63	1.0000	0.0026	0.99
	0.2	0.8131	49.02	1.0000	0.0059	0.99
	0.3	2.1153	44.87	0.9983	0.0093	1.00
	0.4	3.7450	42.39	0.9953	0.0122	1.00
	0.5	6.3997	40.06	0.9977	0.0156	1.00

The simulation results are performed using MATLAB on windows 8, 64-bit operating system with 4 GB RAM and 1.90 GHZ processor speeds. From the result it is observed for Airplane image the PSNR value is 57.01 dB at 0.05bpp which is higher than other cover images because more smooth region areas were present in that image. At a bit rate of 0.5bpp excluding Barbara image all the other cover images have higher PSNR. As Barbara image has complex textures such that it degrades the image quality with low PSNR value of 29.89 dB. For Peppers image since it contains both complex textures and smooth regions at an embedding rate of 0.5bpp the PSNR value is 35.84 dB which is moderately high compared to Barbara image. When compared to the other reference images for Lena image 2-3 dB of the PSNR value was increased at different embedding rates. As Boat and Airplane images have more smooth blocks so that data will easily be retrieved and at an embedding rate of 0.05 bpp the image quality will be improved with PSNR of 57.01 and 56.74 dB.

5. CONCLUSION

By reserving space before encryption and embedding data into the images better performance is achieved in terms of PSNR at various embedding rates. Also data is extracted from stego image which is free from errors with PSNR ≥ 35.84 dB by reducing the normalized absolute error with minimum structural similarity index of 0.98.

For Lena cover image at an embedding rates of 0.1, 0.2, 0.3,0.4 and 0.5 bpp the percentage improvement in PSNR are 4.72 %, 4.70 %, 2.47 %, 1.50 % and 1.20 % in comparison with RRBE method.

6. REFERENCES

[1] Chang CC, Lin MH, Hu YC. "A fast and secure image hiding scheme based on LSB substitution". International Journal of Pattern Recognition and Artificial Intelligence. Vol 16 No 4, Jun 2002, PP.399-416.

[2] Wang ZH, Kieu TD, Chang CC, Li MC. "A novel information concealing method based on exploiting modification direction". Journal of Information Hiding and Multimedia Signal Processing. Vol 1 No 1, Jan 2010, PP.1-9.

[3] Zhang J, Zhang D. "Detection of LSB matching steganography in decompressed images". IEEE Signal Processing Letters. Vol 17 No 2, Feb 2010, PP.141-144.

[4] Hong W, Chen TS. "A novel data embedding method using adaptive pixel pair matching". IEEE transactions on information forensics and security. Vol 7 No 1, Feb 2012, PP.176-84.

[5] Sharmila B, Shanthakumari R. Efficient Adaptive Steganography for color images based on LSBMR algorithm. ICTACT Journal on image and video processing. Vol 2 No 3, Feb 2012, PP.387-392.

[6] Muhammad K, Sajjad M, Mehmood I, Rho S, Baik SW. "A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image". Multimedia Tools and Applications. Vol 75 No 22, Nov 2016, PP.14867-93.

[7] Tsai YY, Tsai DS, Liu CL. "Reversible data hiding scheme based on neighboring pixel differences". Digital Signal Processing. Vol 23 No 3, May 2013, PP.919-927.

[8] Peng F, Li X, Yang B. "Improved PVO-based reversible data hiding". Digital Signal Processing. Vol 25, Feb 2014, PP.255-265.

[9] Jung KH, Yoo KY. "Data hiding method using image interpolation". Computer Standards & Interfaces. Vol 31 No 2, Feb 2009, PP.465-470.

[10] Avci E, Tuncer T, Avci D. "A Novel Reversible Data Hiding Algorithm Based on Probabilistic XOR Secret Sharing in Wavelet Transform Domain". Arabian Journal for Science and Engineering. Vol 41 No 8, Aug 2016, PP.3153-3161.

[11] Q. Wang, W. Zeng, and J. Tian, “A compressive sensing based secure watermark detection and privacy preserving storage framework,” *IEEE Transactions on Image Processing*, vol. 23, no. 3, pp. 1317–1328, 2014.

[12] B. Zhao, W. D. Kou, H. Li, L. Dang, and J. Zhang, “Effective watermarking scheme in the encrypted domain for buyer-seller watermarking protocol,” *Information Sciences*, vol. 180, no. 23, pp. 4672–4684, 2010.

[13] A. V. Subramanyam, S. Emmanuel, and M. S. Kankanhalli, “Robust watermarking of compressed and encrypted JPEG2000 images,” *IEEE Transactions on Multimedia*, vol. 14, no. 3, pp. 703–716, 2012.

[14] T. Bianchi and A. Piva, “Secure watermarking for multimedia content protection: a review of its benefits and open issues,” *IEEE Signal ProcessingMagazine*, vol. 30, no. 2, pp. 87–96, 2013.

[15] J. Guo, P. Zheng, and J. Huang, “Secure watermarking scheme against watermark attacks in the encrypted domain,” *Journal of Visual Communication and Image Representation*, vol. 30, pp. 125–135, 2015.

[16] H. Liu, D. Xiao, R. Zhang, Y. Zhang, and S. Bai, “Robust and hierarchical watermarking of encrypted images based on Compressive Sensing,” *Signal Processing: Image Communication*, vol. 45, pp. 41–51, 2016.

[17] D. Xu, R. Wang, and Y. Q. Shi, “Data hiding in encrypted H.264/AVC video streams by codeword substitution,” *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 4, pp. 596–606, 2014.