Neural Network based Steganography for Information Hiding

K.P. Ravi Kumar, H.S. Manjunatha Reddy

Abstract--- Steganography is the method of concealing secret message inside a digital image, video or audio file and is to avoid drawing attention to the transport of hidden information through the communication channel. The Neural Network based Steganography for information Hiding (NNSIH) isproposed. TheNeural network approach is used to select and train the best images. The selected image is converted in to bit planes and IWT is applying on each plane to generate sub bands. The threshold is calculated to determine size of the redundancy cover image coefficients and used to embed the secret image. The result shows that the PSNR is higher in this algorithm as compare to available algorithms due to the use ofneural network and IWT.

Keywords--- Steganography, IWT, Neural Networks, Threshod, PSNR.

I. INTRODUCTION

With the fast technological improvements in information security and the information exchange, a lot of issues have been brought up in the security of text and picture information transmitted through the channels. With the growth [1] and facility of internet, it is easier to reproduce and transmit the digital messagesillegitimately. The transmittedmessages can be copied without any loss of significant content and its quality, which is a major issue to the protection, genuineness and rights to the owner of the confidential information. Steganography has emerged as one of the influential and most efficient system which provides high level for protection when it is encrypted as compare to cryptography and watermarking. Steganography, hides the existence of messages such that unknown persons can't even estimate that communication of message taking place. The main concept behind Steganography [2] is that information to be transmitted is not noticeable to the casual eye and the secret information is embedded into the text, image, video, or audio file so that intruderdoes not aware of the information. The unnecessarydataexisting in digital images are used in steganography and using these images as cover object for steganographic transmission and revealing of secretexchanges.The combination of both Steganography and cryptography are used toprovide high level of protection.

The most of the steganography algorithms are based on the modification of the pixels or mathematical equations are applied on the images before embedding. Based on this the embedded process is perform using spatial domain techniques and transform domain techniques.

II. RELATED WORK

Divya.Aynapur and S.Thenmozhi [3] have proposed Steganography approach of embedding multiple secret colour images into a single cover image. In this method each secret colour images are embedded in RGB planes of cover image using artificial neural network along with LSB substitution method in spatial domain. This approach is to increase the capacity of the secret message by embedding multiple secret images in single cover image while maintain the stego image with high quality using the artificial neural network with Advanced encryption standard (AES) to provide dual layer of security.

Ashley S Kelsey and Cajetan M Akujuobi [4] have proposed system that combines both Crypto system and Steganography techniques. The cryptography consists encrypting the secret message into a non- decipherable secret message. The transform coefficient of Discrete Wavelet Transform (DWT) is used to insert the encrypted information into a cover media to conceal its existence and it is based on fusion of wavelet coefficients with embed strength factors.

Seema S. Girare and Malvika U. Saraf [5] have developed Digital Watermarking and steganography technique using Least Significant Bit (LSB) algorithm to embed the message into the audio file. To investigate the method in which the embedded watermark should protect the data from hackers using common signal processing operations and attacks. To evaluate the type of audio file that can be used for secure communication of information in a complete indiscernible approach and avoid the doubt of transfortatin of cryptic information.

PrasannakumarPatil andSatishShet.K [6] have developed a technique for LSB based Steganographywith box type mapping with unique information embedding. The 4-typesof boxes with 16- different values of each having 4 bits and each value areembeddedinto 4 LSB's of cover object.

Pranita P. Khairnarand V. S. Ubale [7] have developed a method that uses the characteristics of the human visualization system. The human cannot observe any kindof information in a complex binary system. The regions ofnoise in the planes of the vessel images replaced with secret messages without modifying the quality of the image.NavdeepKaur and, Sukhjeet K. Ranade [8] have developedsteganographic system using Discrete Cosine Transform (DCT) and review the existing systems both in spatial and transform domain. It is based on the quantized projection embedding system to achieve higher embedding rates. The

Manuscript received June 10, 2019.

K.P. Ravi Kumar, Department of ECE, JSS Academy of Technical Education, Bengaluru, Karnataka, India. (e-mail: kprk73@gmail.com)

H.S. Manjunatha Reddy, Department of ECE, Global Academy of Technology, Bengaluru, Karnataka, India. (e-mail: manjunathareddyhs@gmail.com)

embedding is done on the quantized DCT coefficients using Hadamard Matrix as base vector.

Nitinet al., [9]havepresented Image steganography method using LSB and DCT coefficients that provide the embedding of arbitrarily scattered bits directly inside the cover image. The Discrete Cosine Transform (DCT) was applied on the cover media and then the secret image was hidden in LSB of the cover image in random locations based on threshold value. The randomized pixel locations are used to embed secret information were found using DCT coefficients. Vijay and Vignesh [10] proposed Integer Wavelet Transform (IWT) based system forgray level cover image and the secret image bit stream was embedded into the LSB's of the wavelet coefficients of the cover media. The method is used to get higher embedding capacity and minimize the distortion occur instego image.

III. PROPOSED SYSTEM

The related performance parameters of the system NNSIHare discussed.

3.1 Definitions

3.1.1Mean Square Error (MSE): It is the square of error between cover and stegoobject and it is measured using MSE as perequation (1).

$$MSE = \left[\frac{1}{N}\right]^2 \sum_{i=1}^{N}\sum_{j=1}^{N}(X_{ij} - \overline{X_{ij}})^2 \quad (1)$$

Where N: Size of images,

X_{ij} : cover image pixels intensity values,

$\bar{X}_{ij}$: stegoimage pixel intensity values

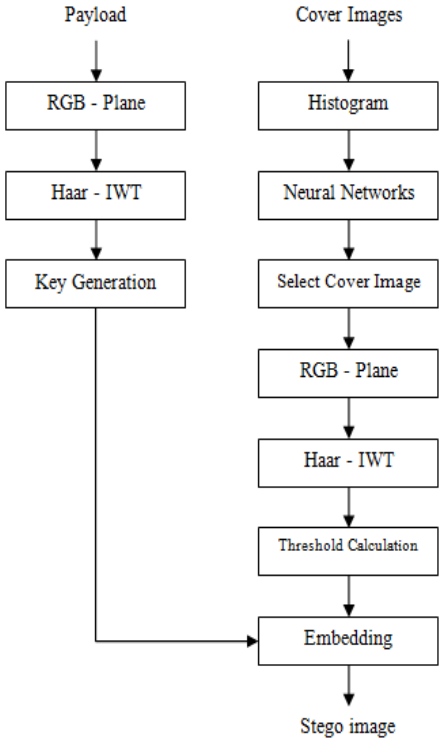


Fig. 1: Proposed NNSIH embedding system

*3.1.2 Peak Signal to Noise Ratio:*It is gives the quality of stego image as compared to cover image, i.e., the noise present in the cover image is measured usingequation (2).

$$PSNR = 10log_{10}\left(\frac{255^2}{MSE}\right)dB \ (2)$$

3.2. Proposed NNSIH System

The proposed work NNSIH is consists of Embedding of secret message into cover mediaand extraction of secret information from stego image.

*3.2.1Cover Image:*It is amedia into which the confidential data is embedded so that there are no significant changes in the statistical properties of the cover media. All cover images are uncompressed and which is ranging from gray scale image to colored image.

3.2.2 Histogram: It gives thebrightness distribution in a image. It gives the details of number of pixels for each value.

3.2.3 Neural Network: Itapproximates functions that are depends on number of inputs which are generally unknown. In steganography, the neural networks are used to select the best cover image among a set of cover images. It is an unsupervised Learning system in the field of neural networks with excellent data-exploring tool. The Self Organizing Map (SOM) maps high dimensional patterns onto a low-dimensional grid of nodes called as neurons. SOM is based on learning activated that learns the neuron.

3.2.4 Selection of Cover Image: In order to achieve high PSNR values in the process of embedding, a hybrid system consist of two types of artificial neural networks will be used to select the required cover image from the available set of cover images.The mapis properlytrained to get desired outputs and alsoto enhance resilient back-propagation neural network. The histogramof the covermedia was taken and these valuesare used as inputs for SOM network. The histogram intensity values are grouped into classes using SOM as ([1 0 0 0], [0 1 0 0], [0 0 1 0] and [0 0 0 1]) and used as desired outputs of the enhanced resilient back-propagation 3.2.5 RGB Plane:The selected cover image is split into R, G, and B layers of 8 bits as given in the figure 2.

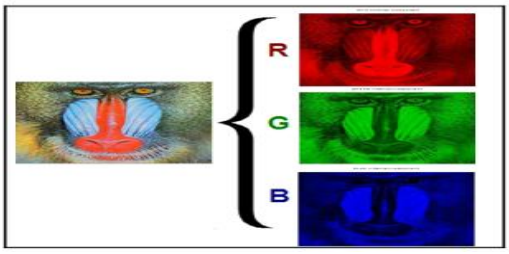


Fig. 2: RGB layer separation of cover image

3.2.6 Haar 4-level Integer Wavelet Transform (HIWT): The IWT is applied on each R, G, B planes of cover media to obtain subbands such as Approximate, Horizontal, Vertical and Diagonal band. The approximation band has a low frequency component and contains important information.

3.2.7 Threshold Calculation:It determines the size of the redundant informationof the selected cover image and it is calculated using equation (3).

$$T = \frac{\beta}{N}\sum_{i=0}^{N}|C_i| \ (3)$$

Where: β – values range from (0-1) attenuates embedding threshold value

C_i- the coefficients of the IWT for the cover image

The obtained threshold value is used at embedding and extraction system without further locations of the IWT coefficients to save the index of the locations and also store the bit streams of secret image sub bands.

*3.2.8 Secret Image:*The text, audio, images or video files are used as secrete image The secrete image is split into R, G and B bit planes.

3.2.9 Integer Wavelet Transform (HIWT): The first level of Integer wavelet transform is applied on each plane of the secret image to generate four sub bands. The sub bands of each bit planes are converted in to stream of 4- bits,where each transformed coefficient of 16 are concatenated to composed in to a single bit stream.

3.2.10 Key Generation and bit Streams Encryption: The entire bit stream is encrypted and secret key is generated by using modified Fibonacci Linear Feedback Shift Register (FLFSR).

The FLLSR consists of a linear feedback register with an (XOR) gate on its fourth and sixth bit then fed back to the first bit each time it's shifted from left to right. The 3rd and 7th bit is given to OR- gate 1 and 4th and 8th bit is given to OR-gate 2. The two output of OR are given to input of XOR to generate a key stream for each 8- bits plane to increases the security level.

3.2.11 Embedding process: The IWT coefficients of the cover media is used to embed the bit stream of each band of the secret informationand then converted into a vector form. The first three coefficient values of each approximate band are considered for the secret key. The remaining coefficients are used for embedding the secret information. These coefficient values arecompared with the threshold value. If coefficient value is greater than threshold value, then it is neglected and if it is less than or equal to the threshold value (T), then the transformed coefficients aretransformedinto 16 bits number and 4- LSB are used to savethe secret information bits.Again the complete bit stream of secret image is further divided into blocks, where four bits of each block are replaced with the four LSB's of the cover image coefficients to generatestego image.

3.3 Extraction process

It is exactly reverse process of embedding as shown in figure 4. The stego image is split into R,G,B bit planes and 4 level IWT is apply on each plane to generate four sub bands. The transformed coefficients of each sub band are converted into vector form. The secrete key is extracted from the first three bits to the extraction the secret message. The transformed coefficient values of each band are compared with the extracted threshold value, if it is greater than the threshold value then ignore it. If it is less or equal to the threshold value, convert it to binary form and used to recover the 4 LSBs. The same process is used for all coefficients, if coefficient value less than or equal to the threshold value to extract the entire bit stream of secret band. Similar process is used for all other sub bands. The encrypted 4-bit binary of the secret image are to be decrypted. The decryption bit streams are further divided to 16-bits blocks and they are converted back to vectors form. The secret image is obtained by applying inverse IWT and combine together to get the full color of the secret image.

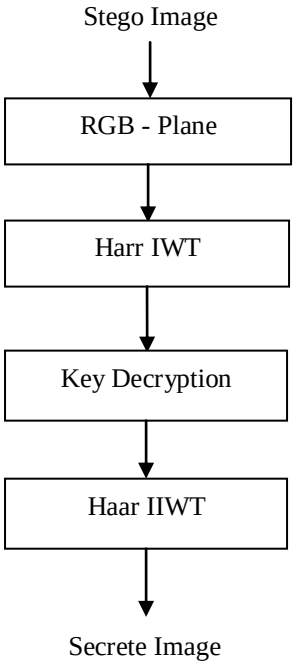


Fig. 3: Proposed NNSIH extractions

IV. ALGORITHMS

Problem definition: The embedding of secret messageinto cover image using Neural Network and IWT to obtainstego image for secure communication. The proposed steganography algorithm is more secured as uses Neural Network and Fibonacci Linear Feedback Shift Register for generating key with encryption.

The objectives are:

(i) To enhance the embedding capacity

(ii) To improve the PSNR

4.1: Embedding algorithm of NNSIH

The Table 1 gives the embedding algorithm of NNSIH using IWT are shown in the table 1.

Table 1: Embedding algorithm of NNSIH

Input: cover image and secret image Output: stego image 1.select the cover image using neural network 2.Split the cover image to RGB bit planes 3. Apply IWT to each plane to obtain the sub bands LL, LH, HL and HH. 4. Split the secret image into bit planes and apply IWT on each plane. 5. Generate a secret key using FLFSR and encrypt it 6.Calculate the threshold of cover image to find the redundancy bits in each plane and embedded the MSB bits of secret information in LSB of the cover media in respective planes to get stego image.

4.2 Extracting Algorithm of NNSIH

The secret message is recovered from the stegoobject by applying reverse process of embedding as shown in table 2.

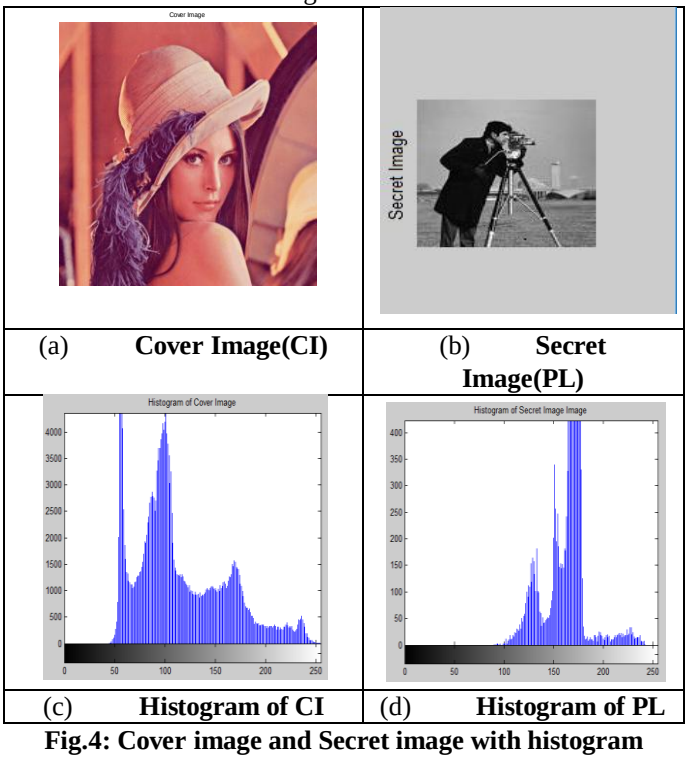
Table 2: Extracting Algorithm of NNSIH

Input: Stego image. Output: extracted secret image. 1. Split thestego imageis converted into bit planes. 2.Apply IWT on each colour plane of stego image to generate sub bands 4. By using threshold and LSB technique extract the MSB bits embedded in the RGB planes. 5. Decrypt the message bits by using key used during the embedding process. 6.Inverse IWT is apply on combined bit planes to obtain the secret image

V. PERFORMANCE ANALYSIS& RESULTS

The cover images of Lena and Payload of cameraman with histogram as shown in Figure 4with different sizes and formats are used for performance analysis. Figure 6 shows the stego image and extracted payload image with histogram.Figure 4 (a) shows secret image of size 64x64 isembedded into cover media of 512x512 to obtainstego image. The obtained stego image has high invisibility and high similarity of appearance as shown in figure 5.

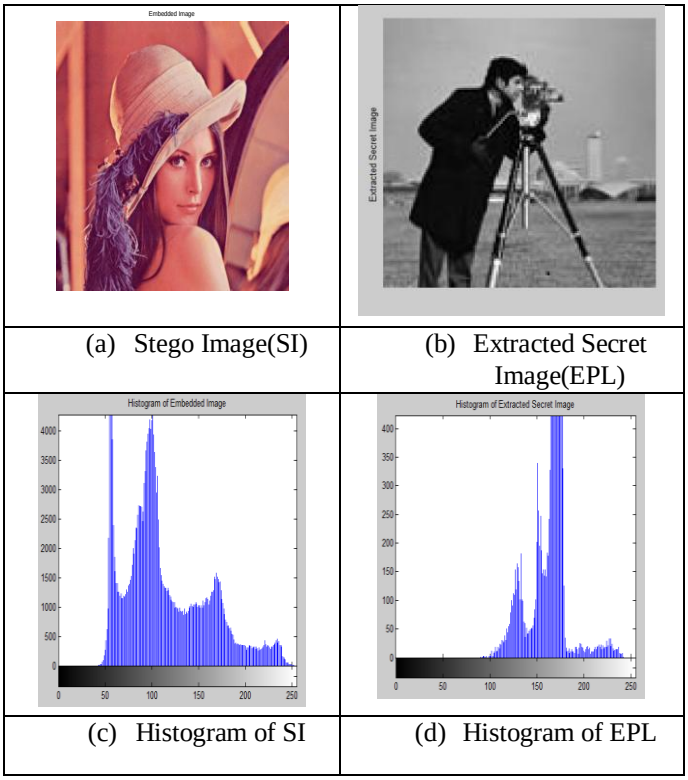
The variations of PSNR value for different payload image formats with cover image Lena of size of size 512 x 512 are given in Table 3.The value of PSNR between cover andstego image is high in case of Tiff and png images as compared with different image formats.The variations of PSNR values for different cover image formats with payload Lena of size of size 64 x 642 are tabulated in Table 4. It is observed that the value of PSNR is high in case of Tiff and png images as compared with other image formats.The PSNR values between payload and extracted payload is very high as compare with existing techniques [12] and [13] and almost constant for all image formats.



(a) **Cover Image(CI)** (b) **Secret Image(PL)**

(c) **Histogram of CI** (d) **Histogram of PL**

Fig.4: Cover image and Secret image with histogram



(a) Stego Image(SI) (b) Extracted Secret Image(EPL)

(c) Histogram of SI (d) Histogram of EPL

Fig.5: Stego image and Extracted image with histogram

Table 3: Variations of PSNR for different secret image formats with cover image lena.(512X512)

Secret image (128x128)	PSNR of CI and SI	PSNR of PL and EPL
Bmp	41.03	82.74
Jpeg	41.06	82.74
Png	41.12	80.41
Tiff	41.24	82.63
Gif	41.01	82.44

Table 4: PSNR variations for different cover image formats with secret image cameraman (64X64)

Cover Image format(512x512)	PSNR of CI and SI	PSNR of PL and EPL
Bmp	41.01	81.61
Jpeg	41.00	81.16
Png	41.91	82.74
Tiff	41.23	81.61
Gif	41.00	81.61

VI. CONCLUSION

Steganography is a method of embedding the secretmessage into a cover mediato hide the existence of confidential information.In this paper Neural Network based Steganography for information Hiding (NNSIH) is proposed. The cover image is selected using Neural Network and converted into bit planes. The IWT is applied on each bit plane to generate sun bands. The transformed coefficients of each sub bands are converted into bit stream. The embedding process is performed based on the threshold value.The value of PSNR is very high in thedeeloped algorithm as compare to existing algorithms.

REFERENCES

1. SumeetKaur, SavinaBansal and R. K. Bansal, "Steganography and Classification of Image Steganography Techniques", IEEE International Conference on Computing for Sustainable Global Development, pp. 870-875, 2014.
2. MunishKatoch and ReenuJaswal, "Image Steganography- A Review", International Journal of Advanced Research in Computer and Communication Engineering vol. 5, issue 4, pp. 827-830, 2016.
3. Divya.Aynapur and S.Thenmozhi, "A secure steganography approach of multiple secret images using ANN",International Journal of Recent Trends in Engineering and Research, vol. 02, issue. 04, pp.468-473, 2016
4. Ashley S Kelsey and Cajetan M Akujuobi, "Discrete Wavelet Transform approach for Enhanced security in image Steganography", International Journal of Cyber-Security and Digital Forensics, vol. 5, issue. 1, pp. 10-20, 2016
5. Seema S Girare and Malvika U Saraf, "Literature Review on Different Watermarking and Steganography Technique",International Research Journal of Engineering and Technology, vol.03, issue. 04, pp. 1097-1102,2016
6. PrasannakumarPatil and SatishShet.K, "Implementation of an Image Steganography Technique using X(X-OR)-Box Mapping", International Journal of VLSI system design and Communication system, vol. 03, issue. 03, pp. 0282-0287, 2015
7. Pranita P. Khairnar and V. S. Ubale, "Steganography using BPCS technology",International Journal of Engineering and Science, vol.3, issue. 2, pp. 08-16, 2013
8. NavdeepKaur and Sukhjeet K. Ranade, "High Capacity Data Embedding System using Projection Quantization", International Journal of Advanced Research in Computer and Communication Engineering,vol. 1, issue. 4, pp. 234-237, 2012
9. Vijaysinh J, kirit R, Avalik k, and AshishV,Nitin K, "A Novel technique for image Steganography techniques Based on LSB and DCT coefficient", International Journal for Scientific Research and Development, vol. 1, issue. 11, pp.2479-2482, 2014
10. V.Vignesh and M.Vijay "Image Steganography Method Using Integer Wavelet Transform" International Journal of Innovative Research in Science, vol. 3, issue. 3, pp. 1207-1211,2014
11. Anitha, M. Rajaram and Sivanandham, "An Efficient Neural Network Based Algorithm for Detecting Steganography content in Corporate mails: A Web Based Steganalysis", International Journal of Computer Science Issues, Vol. 9, Issue 3, No 1, 2012
12. JasmeenKaurPandher andKamalpreetkaur, "A Secure Image Steganography Method Based on Neural Network", International Journal of Computer Science and Engineering Technology, vol. 7, no. 06, pp. 285-291, 2016.