Unique Steganography Technique Using Wavelet Transform and Neural Network

Anupriya Sohal

M Tech Scholar

Department of Computer Science Engineering College

SVIET (Swami Vivekananda Institute of Technology), Banur, Mohali, Punjab.

Dr.Lalita Bhutani

Associate Professor & Head

Department of Computer Science Engineering College

SVIET (Swami Vivekananda Institute of Technology), Banur, Mohali, Punjab.

Abstract- **In communication system hiding capacity of a system plays an important for transmission. Many different ways are for hiding information such as Steganography. In this paper new Steganography technique is proposed for hiding the important information using DWT (Discrete wavelet transform) and back propagated neural network considering LSB. This work over here is performed by a combinational wavelet transformation and Neural Network classification. The image is first segmented using wavelet transformation and then furthermore the segmented bits are send for the classification using Neural Network .It signifies those bits where the data can be embedded and leaves those bits which has a greater threshold than that of the Neural threshold. The embedding scheme presents a resulting PSNR of around 90 to 95.**

Keywords: Image Steganography, Wavelet Transformation, PSNR

I. INTRODUCTION

Over the rapid increase in development of internet requires it has become important to protect the confidential Information from the unauthorized users. This is done by various methods like data hiding using Steganography. Steganography comprises of two words stages and raffia. Stages means cover and grafia means writing that is referred to as “covered writing”. Steganography is the science used for hiding information into information, so that it appears to nothing to be human eyes. There are many different ways for hiding the information such as in hiding inside an image, audio/video, document etc [1]. Many different carrier file formats can be used for hiding the data but digital images are the most popular because of their frequency on the Internet. Image Steganography techniques are discussed for different file formats. Covered communication can be done by encrypting the password for information to be protected and the receiver used to decrypt the information using that password.

DWT (Discrete Wavelet transform)

A ‘wavelet’ is a small oscillating wave having its energy concentrated in time. The oscillating wavelet characteristics enable it for simultaneous time and frequency analysis. Wavelet transforms have an infinite set of basic functions which are derived from single function known as “mother wavelet” as shown below

$$\psi a,b(t) = \frac{1}{\sqrt{|a|}}\psi\frac{(t-b)}{a}, a,b \in R, \quad a\neq 0. \quad \text{Eq (1)}$$

The parameter a, is the scaling parameter or scale, and it measures the degree of compression. The parameter b is the translation parameter which determines the time location of the wavelet. If $|a| < 1$, then the wavelet, is the compressed version (smaller support in time- domain) of the mother wavelet and corresponds mainly to higher frequencies. On the other hand, when $|a| > 1$, then ψa,b(t) has a larger time-width than ψ (*t*) and corresponds to lower frequencies.

Discrete wavelet transform is used for analysis and synthesis of signal as it consists of discrete set of scaling and shifting functions.

Neural networks

The network will receive the 960 real values as a 960-pixel input image (Image size ~ 32 x 30). It will then be required to identify the face by responding with a 94-element output vector. The 94 elements of the output vector each represent a face. To operate correctly the network should respond with a 1 in the position of the face being presented to the network all other values in the output vector should be 0. In addition, the network should be able to handle noise. In practice the network will not receive a perfect image of face which represented by vector as input. Specifically, the network should make as few mistakes as possible when classifying images with noise of mean 0 and standard deviation of 0.2 or less.

Architecture of neural network

The neural network needs 960 inputs and 94 neurons in its output layer to identify the faces. The network is a two-layer log-sigmoid/log-sigmoid network. The log-sigmoid transfer function was picked because its output range (0 to 1) is perfect for learning to output Boolean values.

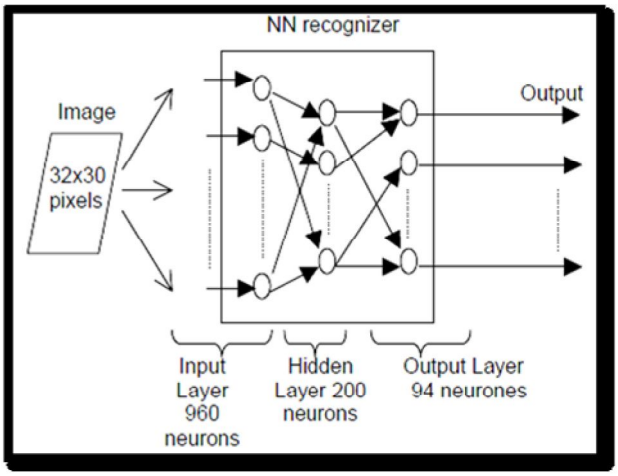

Figure.1 Architecture of neural network [5]

The hidden layer has 200 neurons. This number was picked by guesswork and experience. If the network has trouble learning, then neurons can be added to this layer.

The network is trained to output a 1 in the correct position of the output vector and to fill the rest of the output vector with 0's. However, noisy input images may result in the network not creating perfect 1's and 0's. After the network has been trained the output will be passed through the competitive transfer function. This function makes sure that the output corresponding to the face most like the noisy input image takes on a value of 1 and all others have a value of 0. The result of this post-processing is the output that is actually used.

II. LITERATURE SURVEY

Steganography technique is used for hiding important document from unauthorized persons over internent. C.P.Sumathi (et.al) studied the analysis of various techniques for the Steganography process [2]. Steganography is the process used for hiding a secret message within in such a way that none can understand the presence or hidden within message .The main purpose of Steganography is to maintain the secret communication between two parties. Steganography is used in a modern context while providing a practical understanding of it [3]. Babloo Saha (et.al) presented the recent research work in the field of Steganography concluded in spatial, transform, and compression domains of digital images. Transform domain techniques are preferred over spatial domain techniques as distortion is kept at minimum level and as transform technique changes the frequency coefficients instead of manipulating the image pixels directly. Therefore provides better results [4].Overview of different Steganographic techniques its types are discussed. Analyses of different proposed techniques is done which show that visual quality of the image is degraded when hidden data increased up to certain limit using LSB based methods. And many techniques show the indication of alteration of image as it is incorporated by noise [5].Novel approach is proposed for Steganographic technique for images. To hide the secret information in original image or cover image, the effective channel selection technique is used .In image Steganographic technique, information is hidden in the secret data which consist of two, three or four bits or at most five bits of a pixel in a image and gives the poor value of peak signal to noise ratio (PSNR) and high value of root mean square errors (RMSE).These two parameters shows the better results using proposed algorithm for image Steganography[6].Steganography technique is used to hide the secret information in conventional media for safe transport from various public channels such as the internet. Secure random key can be shared between transmitter and receiver for blind Steganography techniques for image Steganography [7].In P.Thiyagarajan (et.al) [8], a new high capacity Steganographic scheme using 3D geometric models is proposed in which the algorithm re-triangulates a part of a triangular mesh. The secret information is embedded into newly added position of triangular meshes. The vertices of the triangle are used for embedding. Algorithm is proposed in which data is embedded into the red planet of the image and the pixel is selected using a random number generator. It is almost impossible to notice the changes in the image. A key is used to seed the PRNG (Pseudo Random Number Generator) to select pixel locations. Security issues are increased due to the reduction in the distortion rate[d].In S.Shanmuga Praia et. al's [9] article, authors propose a novel method based on LSB in which LSB of the first pixel carries one bit of information and a function to two pixel values carries another bit of information. Proposed results show better result in the form of reducing distortion. In the sharpen edge's embedding is done with threshold. Resulted PSNR values are compared for adaptive and non-adaptive techniques. Shweta Singhal et.al's [10] , new image Steganography scheme is proposed in the spatial Domain where one byte of blue factor of pixels of an image have been replaced with secret bits of text data and results in better image quality.

A stego key is used for security purposes. In Weiqi Luo et. al.'s paper [11], the authors propose an edge adaptive scheme. In the data embedding stage, the scheme first initializes some parameters, which are used for estimating the capacity of the selected regions. Finally stego image is obtained after pre-processing. A region adaptive scheme is applied to the spatial LSB domain and the difference between two adjacent pixels is used as a criterion for region selection and LSBMR (LSB Matching Revisited) as the data hiding algorithm. Hemalatha .S (et. Al) [12] has suggested Integer Wavelet Transform (IWT) to hide multiple secret images and keys in a color cover image which is more efficient. The cover image is represented in the YCbCr color space. Two keys are obtained, encrypted and hidden in the cover image using IWT.In [13], the authors introduce an enhanced image Steganography along with a suitable encryption methodology using a symmetric key cryptographic algorithm. The JPEG cover image is broken into pixel of 8 x 8 blocks and then DCT (Discrete Cosine Transform) is applied to each block that is further quantization. The data is encrypted using a new encrypted.

III. METHODOLOGY

1) START
2) Upload Image and perform segmentation using DWT(DB)
3) Perform the segmentation for every image of the training section
4) Initialize Neural Network and set the target pattern
5) Upload Test Image to perform Steganography
6) Identify LSB from the previously trained neural network object
7) Encode characters into bits to be merged
8) Merge data into identified LSB positions

The structure of the Trained Neural Network is presented as below.

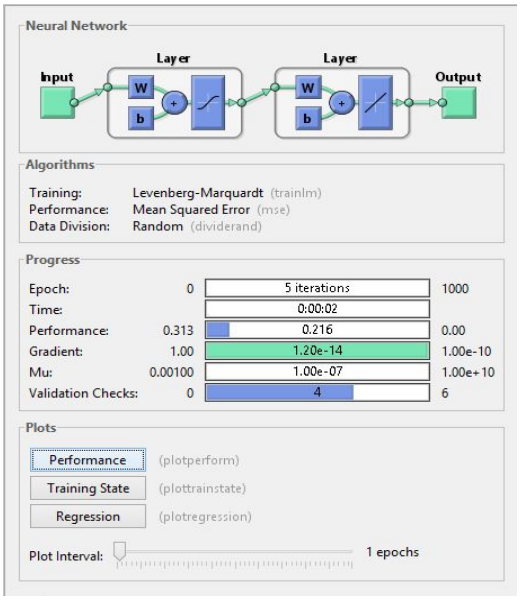

Figure 2 represents Trained Neural Network

The above figure represent the whole architecture of the NEURAL NETWORK in which Epochs represents the number of times the system is running , time represents the execution time , Mu represents the mutation time and 4 validation checks have been performed .

IV. RESULTS AND CONCLUSION

Unique Steganography technique is proposed using DWT (Discrete Wavelet Method) and back propagation neural network. DWT converts the Image into WT (Wavelet transform), from which LSB positions are calculated that are then classified using neural network. To calculate effective values of LSB, training of different images is done, which are then classified with neural network and then data is merged.

A wavelet is a small wave which oscillates and decays in the time domain. The Discrete Wavelet Transform (DWT) is a relatively recent and computationally efficient technique in computer science. Some experiments have been carried out to prove the relationship between expected results and actual results of proposed methods. The proposed two algorithms have been simulated with MATLAB 7.7.0471. After the embedding procedure, the resultant object i.e. the steno object is quiet good in quality with respect to visibility. In extraction procedure it has been aimed to extract the original message intact which has been executed successfully by the above mentioned extraction algorithm.

The obtained PSNR and MSE values are as follows

IMAGE	METHOD OF EMBEDDING	PSNR	MSE
Leena	DWT-Neural	90.12	.00156
Leena	DCT Vector Quantization	56.14	.96358
Leena	Haar Dwt Transformation	42.56	1.231

Table (1) represents the results of Leena Image

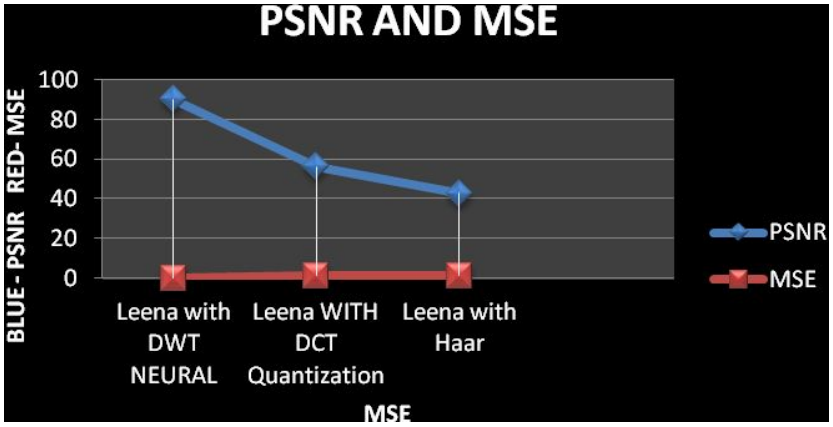

Figure 3 representing results in tabular form

The above graph is the graphical representation of the table drawn above in which the Leena Image is tested against other technique. The graph shows a good growth in the PSNR value and the valuable decrease in the Mean Square Error value with DWT and Neural Network.

REFERENCES.

1. R.Poornima, “An Overview of digital image Steganography”, International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.1, February 2013.
2. C.P.Sumathi (et.al), “A Study of Various Steganographic Techniques Used for Information Hiding” International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.6, pp.9-25, December 2013.
3. Nick Nabavian, “CPSC 350 Data Structures: Image Steganography”.
4. Babloo Saha, “Steganographic Techniques of Data Hiding using Digital Images”,Defence Science Journal, Vol. 62, No., pp. 11-18, 1 January 2012.
5. Mehdi Hussain (et.al), “A Survey of Image Steganography Techniques”, International Journal of Advanced Science and Technology Vol. 54, May, 2013.
6. Vijaypal Dhaka(et.al), “A Novel Algorithm for Image Steganography Based on Effective Channel Selection Technique”, International Journal of Advanced Research in Computer Science and Software Engineering , Volume 3, Issue 8, August 2013.
7. Fariba Ghorbany Beram , “Effective Parameters of Image Steganography Techniques”, International Journal of Computer Applications Technology and Research,Volume 3,Issue 6, 361 - 363, 2014,
8. P.Thiyagarajan (et.al), “Pattern Based 3D Image Steganography”, 3D Research center, Kwangwoon University and Springer 2013, 3DR Express. Pp.1-8, 2013.
9. Shamim Ahmed Laskar(et.al), “Steganography Based On Random Pixel Selection For Efficient Data Hiding”, International Journal of Computer Engineering, and Technology, Vol.4, Issue 2, pp.31-44.
10. S.Shanmuga Priya, K.Mahesh and Dr.K.Kuppusamy, (2012) “Efficient Steganography Method To Implement Selected Least Significant Bits in Spatial Domain”, International Journal of Engineering Research and Applications,” Vol2, Issue 3, pp. 2632-2637.
11. Weiqi Luo, (et.al) “Edge Adaptive Image Steganography Based on LSB Matching Revisited”, IEEE Transactions on Information Forensics and Security, Vol.5.No.2, pp.201-214.
12. Hemalatha.S(et.al) ,“A Secure and High Capacity Image Steganography Technique”, Signal & Image Processing – An International Journal, Vol.4, No.1, pp.83-89.
13. Prosanta Gope, “An Enhanced JPEG Steganography Scheme with Encryption Technique”, International Journal of Computer and Electrical Engineering ,Vol.2.No.5, pp924-930.