VIDEO WATERMARKING WITH STEGANOGRAPHY USING NEURAL NETWORKS

Rakesh Kumar*

Savita Chaudhary**

Abstract-

In any communication security is the most important issue in today's world. Lots of data security and data hiding algorithms have been developed in the last decade, which worked as motivation for our research. In this paper we combine watermarking techniques and steganography together to increase the security and to make these techniques robust we combine it with neural networking. This paper is the combination of steganography with watermarking, which provides a strong backbone for its security. The proposed system not only hides large volume of data within an image, bt also limits the perceivable distortion that might occur in an image while processing it. The scheme proposed in this paper is robust against attacks of frame dropping, frame averaging, noise addition and statistical analysis. The experimental results shown with neural network provides maximum watermark embed strength and also verify the effectiveness and imperceptibility.

Keywords- Video Watermarking, 5L-DWT, Steganography, Security, Neural network, Robustness, Hidden data.

* Assistant Professor, Department of Information Technology, Maharishi Markandeshwar University, Ambala, India

** Student, Department of Information Technology, Maharishi Markandeshwar University, Ambala, India

I. INTRODUCTION

1.1 Video watermarking

A digital watermark is a digital signal or pattern inserted into a digital document such as text graphics or multimedia and carries information unique to the copyright manner. Video watermarking is an extension of digital watermarking. Video watermarking is most popular secure technique for providing security and copyright protection. Video file is the continuous collection of static images. An image is composed of three color channels: Red, Green and Blue. Watermark is embedding into three different R.G.B channels of the video frame separately. The main advantage of this approach is that same or multi watermark can be embedding into three color channel of the image to increase the robustness of the watermark. Figure 1 represents the digital watermarking, in which digital watermark is embed into the original digital media and finally get the watermarked data.

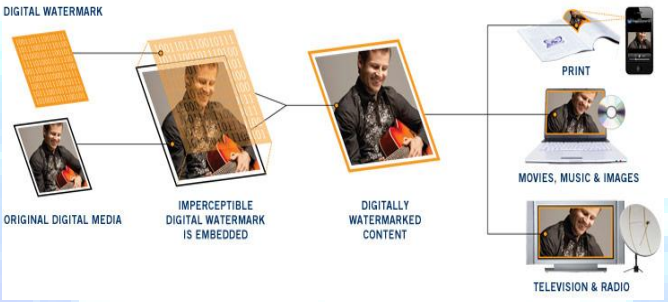

Fig.1: Digital watermarking

Video watermarking techniques are classified according to their working domain [10]. Some techniques embed watermark in the spatial domain by modifying the pixel values in each frame extracted from the video. These methods are not robust to attacks and common signal distortions. In contrast, other techniques embed the watermark in the frequency domain, which are comparatively more robust to distortions [6]. In this paper we used frequency domain techniques. The most commonly used transform are the Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT).

DWT is a mathematical tool for hierarchically decomposing an image. The transformation is based on the small waves called wavelets. Wavelet transformation provides both spatial and frequency description of an image [5]. DWT splits the signal into high and low frequency parts. High frequency part contains information about the edge component, whether the lower part again splits into the high and low frequency parts. Higher frequency component usually used for the watermarking since the human eye is less sensitive to observe the change in edge.

Video watermarking scheme: The new watermarking scheme based on neural networks.

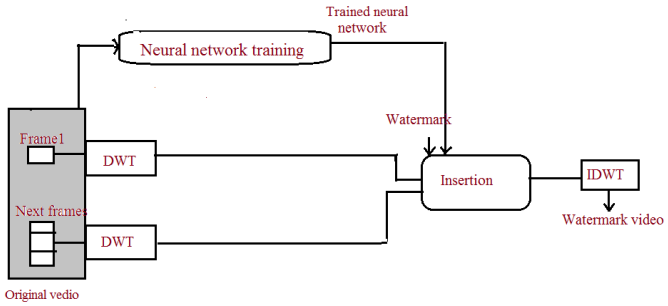

Fig.2: Watermark embedding process

Figure2 shows an overview of watermarking process. In this, a video is taken as the input, and then a neural network is trained to be used later in watermark embedding. Next, the first frame is watermarked as a single image. Afterwards, for the following frames, new positions of the watermark are obtained from motion vectors and selected positions in the previous frame. Once the new positions determined, the same embedding strategy is applied. Finally, the video is transformed back to time domain [16].

The word **Steganography** is derived from the Greeks and literally means covered, "stegano" writing "graphy". Steganography is the art and science of hiding message in communications over a public channel in a way that conceals the fact that there is a hidden message. Steganography should not be confused with cryptography. Cryptography helps only in protect the content of the message where steganography protects the both message and communicating parties. The advantage of steganography over the cryptography that message does not attract attention to them.

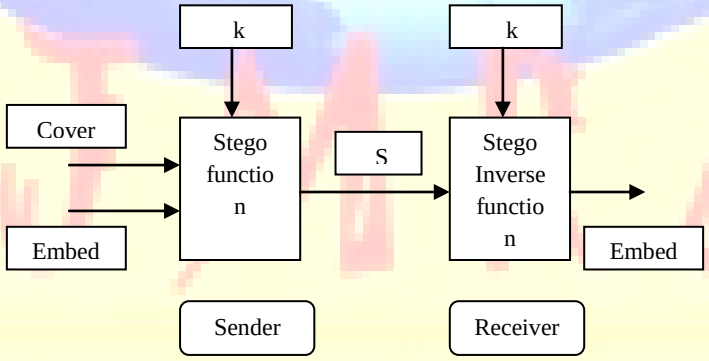

Fig.3: Steganography

Figure3 represents these term "cover" is used to describe the original message; this could be the original digital image file, audio message or text message. The information that is hidden inside of the original message is called the "embedded" data and k define keys.

RSA algorithm: Being a method of public key cryptography, it involves two keys, viz. a private key and a public key. The key-pairs are derived from a large integer which is the product of two prime numbers chosen as per some special rule.

To create an RSA public/private key pair, the basic steps are:

1. Choose two prime numbers, ‘p’ and ‘q’. From these numbers you can calculate the modulus n = pq.
2. Select a third number 'e' that is relatively prime to the product (p-l) (q-l). The number ‘e’ is the public exponent.
3. Calculate an integer’d’ from the quotient (ed-l) / [(p-l) (q-l)]. The number‘d’ is the private exponent. The public key is the number pair (n, e). Although these values are publicly known, it is computationally infeasible to determined‘d’ from ‘n’ and ‘e’ if ‘p’ and ‘q’ are large enough. To encrypt a message, ‘M’ with the public key, creates the cipher text, ‘C’ using the equation:

$$C = M^e \bmod n \quad (1)$$

The receiver then decrypts the cipher text with the private key using the equation:

$$M = C^d \bmod n \quad (2)$$

Therefore the public encryption key is (e, n) and (d, n), the secret private decryption key [21].

A steganographic system is characterized by three different parameters which are deeply interrelated, viz. capacity, security, and robustness. Capacity refers to the amount of data which can be reliably stored in the media, security is the inability of an intruder to extract the hidden data from the media and robustness is the amount of modifications that the stego-media can take without destroying the secret data.

Back propagation neural network: It is a supervised learning method, and is a generalization of the delta rule. It requires a dataset of the desired output for many inputs, making up the training set. It is most useful for feed-forward networks (networks that have no feedback, or simply, that have no connections that loop). The term is an abbreviation for "backward propagation of errors". Back propagation requires that the activation function used by the artificial neurons (or "nodes") be differentiable. It is well-known that neural networks perform a highly adaptive nonlinear decision function from training examples

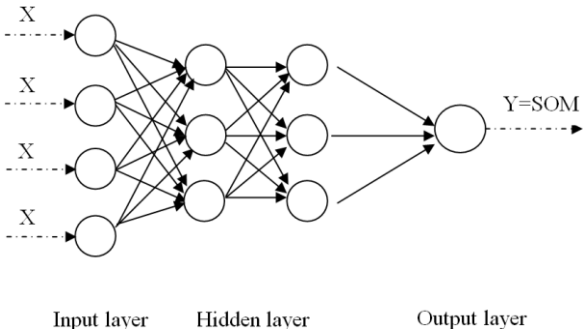

Fig.4: Back propagation neural network

Phase 1: Propagation- Each propagation involves the following steps:

1) Forward propagation of a training pattern's input through the neural network in order to generate the propagation's output activations.

2) Backward propagation of the propagation's output activations through the neural network using the training pattern's target in order to generate the deltas of all output and hidden neurons.

Phase 2: Weight update for each weight-synapse follow the following steps:

1) Multiply its output delta and input activation to get the gradient of the weight.
2) Bring the weight in the opposite direction of the gradient by subtracting a ratio of it from the weight.

II. IGE]PROPOSED WORK

1. 5 Level Discrete Wavelet Transformation

DWT is the Multi-resolution decomposition of image. It splits the signal into high and low frequency parts. Higher frequency part contains information about the edge component, while the lower part again splits into the high n low frequency part. High frequency component usually used for the watermarking since the human eye is less sensitive to observe the changes in edge.

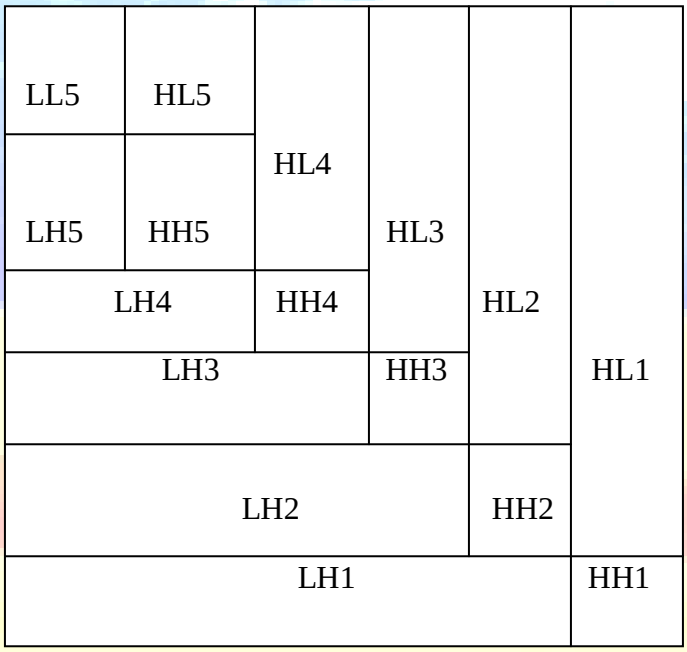

Fig.5: Five level discrete wavelet decomposition

The luminance components of the input video frames are transformed to frequency domain and the middle-frequency range coefficients of the watermark are modified according to the watermark. The basic idea is that the human eyes are sensitive to the low frequency noise and the quantization step of lossy compression may discard the high frequency components. Therefore, the reasonable trade-off is to embed the watermark into the middle-frequency range of the video frames. Here we apply the 5L-DWT. Each video frame is transformed to the wavelet domain

with 5 levels. Haar wavelet is used for simplicity, and only the LH1, HL1, LH2 and HL2, LH3, HL3, LH4, HL4, LH5, HL5 coefficients are embedded with scrambled watermark

In addition, with such a scheme, it is not possible to add more watermark energy at a particular frequency, in which the image energy is high, in order to improve robustness. LL band contains the most of energy of the image, so we apply the watermark in mid frequency bands, it will not creates some artifacts in the image. And invisibility of the watermark can be increased.

2. Proposed watermark embedding process

Here we describe how the watermark and the secret key is embed into the video frames because of the human visual system the watermark apply only in mid frequency band of the image. Figure 6 represents the flow chart of embedding algorithm to embed the watermark into color video.

Step 1: First of all we load a color video file using uigetfile command and then convert video into frames.
Step 2: Then upload secret image by using the same uigetfile command.
Step 3: Decompose each image into three color components (R.G.B) and apply 4-Level DWT to each component of video frame using DWT and IDWT commands putting the level as 4.
Step 4: Apply 5-Level DWT to each component of video frame using DWT and IDWT commands putting the level as 5.
Step 5: Then apply watermark into LH and HL bands i.e. mid frequency bands of each level so convert each pixel value into binary.
Step 6: We start to embed the watermark from HL5 (5th level mid frequency band) and then sequence into LH5, HL4, LH4, HL3, LH3, HL2, LH2, HL1 and LH1.
Step 7: Then generate secret key and add message on video by using RSA encryption algorithm.
Step 8: Then we start watermarking process in which we are calling watermark_img.m function in which neural network part has been combined with Image Processing.
Step 9: Last stored the watermarked video file data into array for watermark extraction before applying inverse DWT.

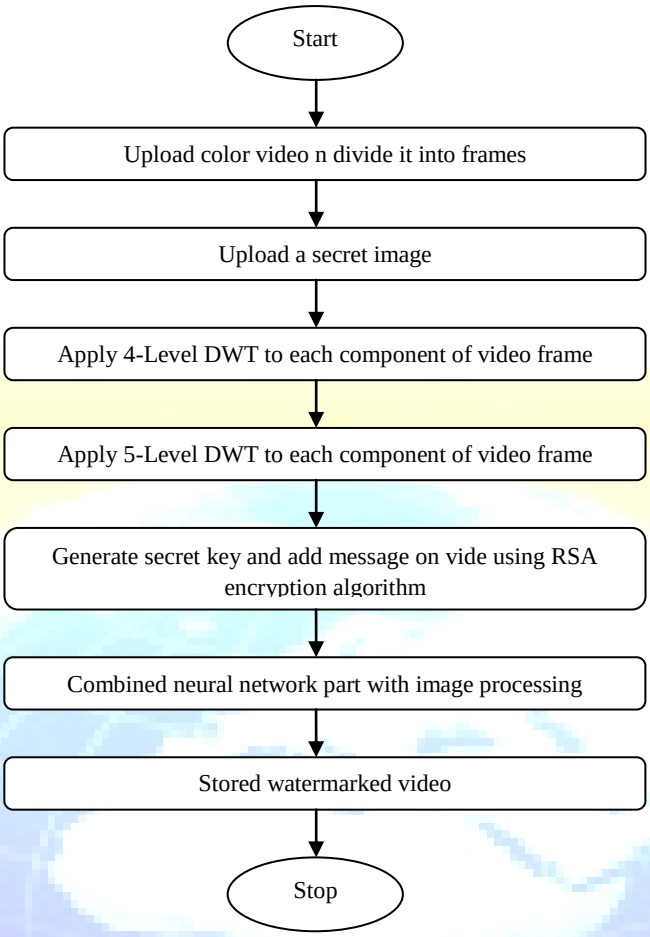

Fig.6: Embedding of watermark process

3. Proposed watermark and secret key extraction process

The extraction process requires the secret key used for selecting the frames, the wavelet transform filter and the channel I which the watermark is inserted. Figure 7 represents the flow chart of extraction algorithm to extract the watermark, hidden message and secret key from the watermarked video.

Step1: Upload the watermarked video or data stored in array using uigetfile command and then separate it into the frames.
Step 2: Convert each pixel of mid frequency band into binary and extract the secret image, secret message by applying the RSA decryption part.
Step 3: Extract image from video file.
Step 4: Process attack on watermarked video file and then again extract image.
Step 5: Combine three arrays for three images R.G.B so that the original video will retrieved.
Step 6: Finally calculate the MSE and PSNR values between the watermarked and input image and compare MSE and PSNR of 4L-DWT and 5L-DWT.

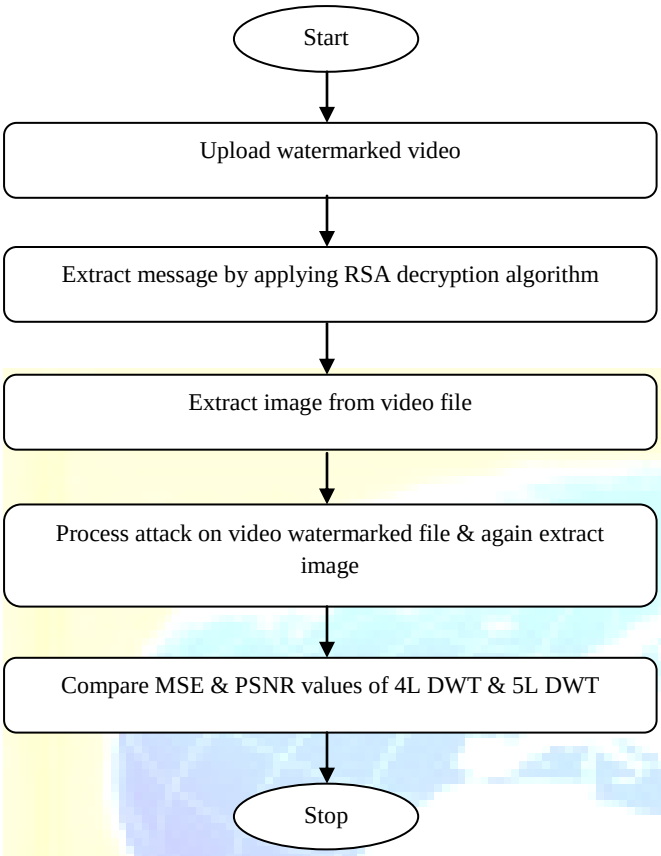

Fig.7: Extraction of watermark process

4. Neural network training process

To properly train the neural network, we feed the model a variety of real life examples, called training sets. The data sets normally contain input and output data.

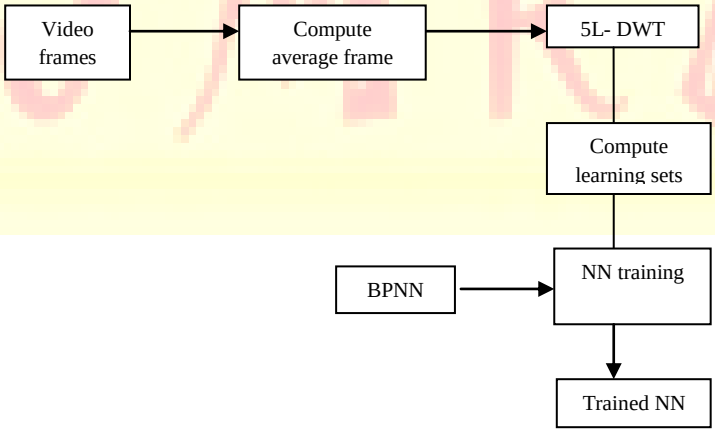

Fig. 8: Neural network training process

The neural network creates connections and learns patterns based on this input and output data sets. Figure 8 illustrates how the training sets are generated. First we compute the average frame

of the video. Then the resulting frame is transformed to the wavelet domain with a five level DWT. Afterwards, it is divided into non overlapping 3x3 blocks. The center of each block is the output while the neighbor's coefficients are the input. Finally we proceed to neural network training until the specified goal or the maximum number of iteration is reached. As a result, we obtain a trained network which will be used later in the watermark embedding process.

III. EXPERIMENTAL RESULTS

Comparison between 4L-DWT & 5L-DWT

Comparing restoration results requires a measure of image quality. Two commonly used measures are Mean-Squared Error and Peak Signal-to-Noise Ratio. The MSE is the cumulative squared error between the compressed ant the original image whereas PSNR is a measure of the peak error. The mathematical formula described below.

1. MSE between watermark and input image

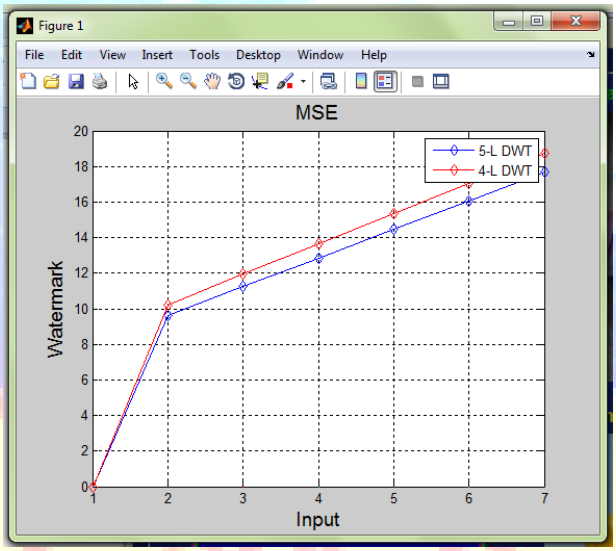

Fig. 9: Mean squared error

Compute the mean squared error (MSE) of the reconstructed image as follows

$$MSE = \sum[f(i,j) - F(I,j)]^2 / N^2$$

The summation is over all pixels. A source image f(i,j) that contains N by N pixels and a reconstructed image F(i,j) where F is reconstructed by decoding the encoded version of f(i,j). Error metrics are computed on the luminance signal only so the pixel values f(i,j) range between black (0) and white (255). Lower value of MSE means less error.

2. PSNR between watermark and input image

PSNR is usually expressed in terms of the logarithmic decibel scale. The signal in this case is the original data, and the noise is the error introduced by compression.

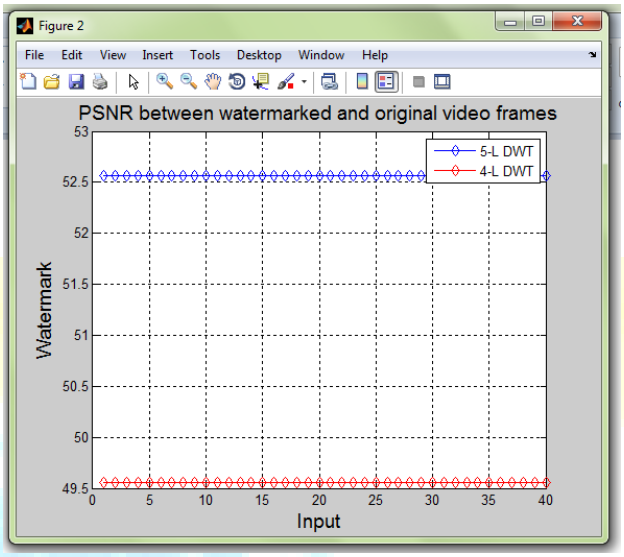

Fig. 10: Peak signal to noise ratio

When comparing compression codecs, PSNR is an approximation to human perception of reconstruction quality. Although a higher PSNR generally indicates that the reconstruction is of higher quality

The PSNR is defined as:

$$PSNR = 10.\log_{10}(MAX^2_I/MSE)$$
$$= 20.\log_{10}(MAX_I/\sqrt{MSE})$$
$$= 20.\log_{10}(MAX_I) - 10.\log_{10}(MSE)$$

Here, MAX_I is the maximum possible pixel value of the image. When the pixels are represented using 8 bits per sample, this is 255.

Higher value of PSNR means ratio between signal to noise is higher.

Neural networking training process

The neural network training process is represented in figure 11. The training window will appear during training, as shown in the following figure. This window shows that the data has been divided using the dividerand function, and the Levenberg-Marquardt (trainlm) training method has been used with the mean square error performance function. Recall that these are the default settings for feedforwardnet. During training, the progress is constantly updated in the training window. Of most interest are the performance, the magnitude of the gradient of performance and the number of validation checks. The magnitude of the gradient and the number of validation checks are used to terminate the training. The gradient will become very small as the training reaches a minimum of the performance. If the magnitude of the gradient is less than 1e-5, the training will stop.

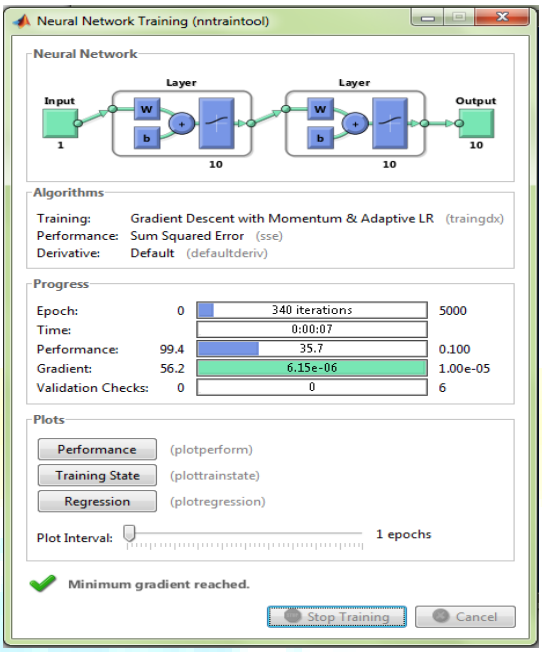

Fig. 11: Neural network training

Weights assign between the input and hidden neurons and between the hidden and output neurons.

W1=a + (b-a) *rand(S1,R);
W2=a + (b-a) *rand(S2,S1);
b1=a + (b-a) *rand(S1,1);
b2=a + (b-a) *rand(S2,1);

Then calculates the values and plots the different graphs of performance, training state and regression.

Neural networking training performance

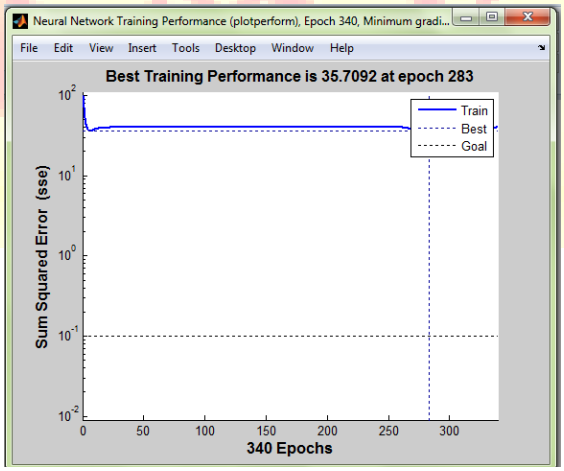

Fig. 12: Graph between epochs and sum squared error

In figure 12, plot the graph between epochs and sum squared error. Sum squared error measure the performance according to the sum of squared errors. The performance plot shows the value of the performance function versus the iteration number. It plots training, validation and test performances.

Neural network training state

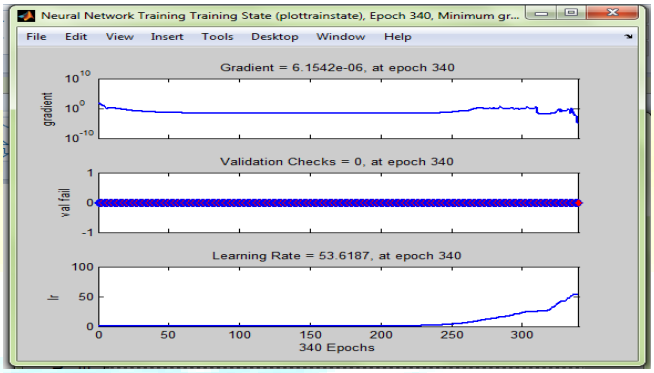

Fig. 13: Training states

Neural network regression plot

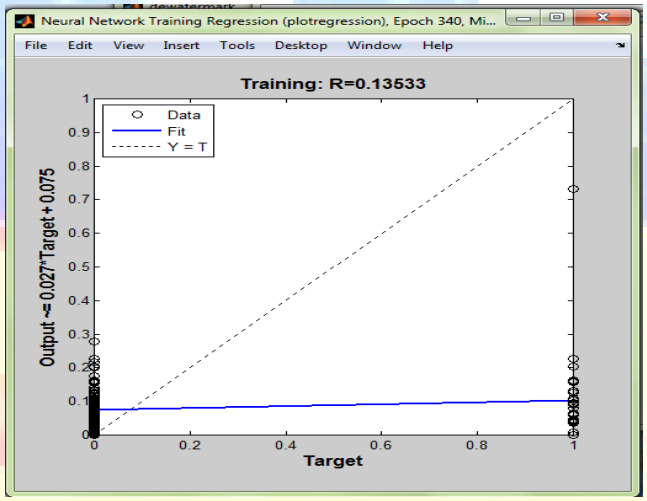

Fig.14: Regression plot

IV. CONCLUSION AND FUTURE WORK

In this paper we have presented a new system for the combination of steganography with watermarking which could be proven as a highly secured method for data communication in near future. . Combination of the 5L-DWT with RSA algorithm and neural network yields the best PSNR value that is it can transmit secret data with minimum distortion of the cover image. Use of Back propagation Neural Network provides additional advantage of hiding the trained network weights within the original cover image. Back propagation neural networking is applied to improve its imperceptibility and robustness. The watermarked image has a good robustness

and the imperceptibility of the cover image is also highly preserved. The comparison of PSNR and MSE values of 5l-DWT are better than the 4l DWT .Thus, this work leads to a successful watermarking scheme.

Future work may be further enhancement of results by applying some another algorithm and robustness can be further increased by applying the other advanced neural network modals.

REFERENCES

[1] A. Bansal and S. Bhadauria**,** "Watermarking using Neural Network and Hiding the Trained Network within the Cover Image", Journal of Theoretical and Applied Information Technology 2005, Vol. 4, No. 1, pp. 663-670.

[2] B. Isac and V. Santhi, "A Study on Digital Image and Video Watermarking Schemes using Neural Networks", International Journal of Computer Applications, Vol. 12, No. 9, January 2011, pp. 1-6.

[3] C. Rey, G. Doerr, J. L. Dugelay and G. C. Surka, "Toward Generic Image De-watermarking", In IEEE International Conference, Image Processing, June 2002, Vol.3, pp. 633-636

[4] K. Raghavendra and K. R. Chetan, "A Blind and Robust Watermarking Scheme with Scrambled Watermark for Video Authentication", In IEEE International Conference, Internet Multimedia Services Architecture and Applications (IMSAA), December 2009, pp. 1-6.

[5] N. Kashyap and G. R. Sinha, "Image Watermarking Using 2-Level DWT", Advances in Computational Research, Vol.4, Issue 1, March 2012, pp. 42-45.

[6] N. J. Janwe and A. A. Hood, "Robust Video Watermarking Techniques and Attacks on Watermark – A Review", International Journal of Computer Trends and Technology, Vol.4, Issue1, 2013, pp. 30-34.

[7] S. Bhattacharaya, T. Chattopadhyay and A. Pal, "A Survey on Different Video Watermarking Techniques and Comparative Analysis with Reference to H.264/AVC", IEEE 10th International Symposium, Consumer Electronics, 2006, pp. 1-6.

[8] S. Rai and R. Dubey, "A Novel Keyless Algorithm for Steganography", In Students Conference, Engineering and Systems (SCES), IEEE, March 2012, pp. 1-4.

[9] T. Tabassum and S. M. M. Islam, "A Digital Video Watermarking Technique Based on Identical Frame Extraction in 3-Level DWT", In 15th International Conference, Computer And Information Technology (ICCIT), IEEE, December 2012, pp. 101-106

[10] T.Jayamalar, Dr. V. Radha "Survey on Digital Video Watermarking Techniques and Attacks on Watermarks" International Journal of Engineering Science and Technology, Vol. 2(12), 6963-6967, 2010.