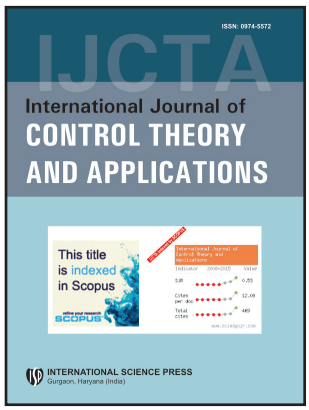


International Journal of Control Theory and Applications

ISSN : 0974-5572

Volume 10 • Number 12 • 2017

Video Steganography using DWT, Fuzzy Logic and NN

Amit Verma[a], Navreet Kaur[b] and Isha Vats[c]

[a]*Professor and Head, Department of Computer Science and Engineering, Chandigarh Engineering College, Landran , Mohali. Email: Dramitverma.cu@gmail.com*
[b]*M.Tech Scholar, Department of Computer Science Engineering, CEC Landran, Mohali, India*
[c]*Assistant Professor, Department of Computer Science Engineering, CEC Landran, Mohali, Indias*

Abstract:

Background/Objective: Video Steganography has become very important topic these days due to the entry of video files in internet. Steganography was used from older times. The first recorded use was in 1499 disguised as a book on magic, example is the hidden message may be in invisible ink between the visible lines of a private letter. In ancient times, the secret messages were hidden in different ways such as tattooed on the scalp of slaves, hidden on tablets covered with wax, or written on the stomachs of rabbits.

Methods/Statistical analysis: Steganalysis is the mechanism of detecting the presence of hidden information in the stego media and it can lead to the prevention of disastrous security incidents.

Findings*:* In this research paper the performance of the algorithm depends on embedding algorithm basically. To improve the security in the algorithm, there is necessity to encode the message strongly. That is why in proposed paper, three techniques has been used with their x factors like DWT for image division, fuzzy logic for generation of rule set and neural network for embedding process. The whole simulation is then tested in MATLAB environment and performance is measured using basic parameters i.e. MSE and PSNR.

Applications: It is concluded that steganography is very efficient technique for sending secret data from one place to another place. It is used in confidential communication and secret data storing, protection of data alteration, access control system for digital content distribution, media database systems.

Keywords: Video Steganography, DWT, Fuzzy Logic, Neural Network.

1. INTRODUCTION

Steganography comes from greek word and it combines the Greek words “stegano” meaning “covered or else protected”, in addition graphed signifying “writing” [1]. Steganography is a substitute on the way to cryptography in which the top-secret information is surrounded inside the transporter in such kind of way in which solitary carrier is noticeable that is directed from transmitter in the direction of receiver left without scrambling [2]. The combination of cryptography as well as steganography makes available great level of security to the secretive data. The basic ideas involved in hiding a secret data in the video carrier document.

The principal step is to choose a cover video. It would seem most appropriate to select a small bit video. Once embedded, we refer to this file as a stego file which can be sent to a receiver. Once the stego file is received, the intended recipient should know how to reverse the process. The same steganography tool is used to extract the hidden message from the stegano file. Figure depicts the flow of the secret communication at sender side and the receiver side [3]. Steganography is further divided into four types for the different file formats that are as below:

1. Text
2. Images
3. Audio/Video
   (i) Spatial Domain technique
   (ii) Transform Domain technique
4. Protocols

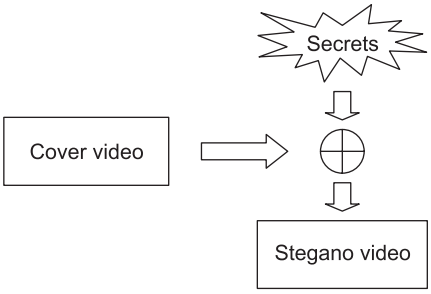


Figure 1: Steganography at sender side mechanism

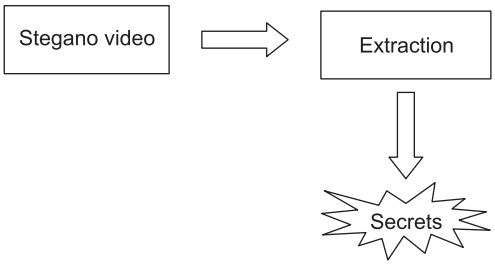


Figure 2: Steganography at receiver side mechanism

In proposed work, video steganography is analyzed using various techniques to get the high rate of accuracy. In proposed work, NN, Fuzzy logic and DWT has been utilized. Usage of video files for steganography is being done to reduce the effects of error and risk [4]. Following methods can be used for achieving the above things:

(i) Based on the non-uniform rectangular baffle video steganography.

(ii) Compressed Video Steganography using TPVD

(iii) To compress video steganography an adaptive system

(iv) LSB Method

(v) DCT method

(vi) DWT method

(vii) Dynamic Cover Generation

2. RELATED WORK

In this era, most of the research work in video steganography is the extension of image steganography.Each research used different techniques Authors represented different forms of work.

Veerdeep Kaur[6] proposed algorithm for considering mainly four factors like size of secret message, quality of cover and stego image, similarity of cover and stego image. It has been found out if more secret messages embedded then quality will be degraded in addition to time requirement.

Babloo Sha[7] discussed the various steganographic techniques like Spatial and Frequency based steganography methods. In Spatial technique various sub techniques has been reviewed like Stego data hiding scheme, S-Tools, Hide & Seek, Stego Dos, White Noise Storm, Bit plane complexity segmentation steganography, Information Theory-based Data Hiding, Dynamic Programming-based Steganographic Technique, Data Hiding using Convolution Decoder.

Mohit Gargproposed[8] a steganography method that uses html documents. The proposed technique uses html tags as well as html attributes. The proposed technique is essentially composed of three parts viz. Key file generation, hidden processes and extracting process.

ShengDun Hu[10] proposedbased on the non-uniform rectangular partition new video steganography, which is the uncompressed video secret cover-video hidden inside. The advantage of this technique is that having high encoding speed of the image.

Imran Khan[11] presented a steganography algorithm based on Neural Network for still images. In this features were extracted of cover image and embedded secret data and then input these features to neural network to obtain the output. The major advantage of neural network is that it has the capability to approximate any nonlinear functions.

3. BASIC CONCEPTS

This section describes the basic concepts which is used for video steganography is Discrete Wavelet Transformatin, Fuzzy Logic, and Neural Network. This technique improves the security of system.

Discrete Wavelet Transform

The discrete wavelet transform is a valuable way designed for signal exploration as well as picture handling, briefly in multi-resolution description.DWT is good method for signal decomposition in steganography a well as image processing. There are many types of DWT like 1D DWT, 2D DWT in which decomposition will be done into HH, HL, LL, LH parts.

LL	HL
LH	HH

Figure 3: DWT

Fuzzy Logic

In addition to this fuzzy logic is also a good method for steganography. In fuzzy logic IF-THEN rules are utilized for obtaining results. Fuzzy logic can be applied using membership functions. It is based on basic factors like fuzzification, de- fuzzification and I/P, O/P variables [5].

- **Fuzzification Module:** It transforms the system inputs, which are crisp numbers, into fuzzy sets.
- **Knowledge Base:** It store IF THEN rules.
- **Inference Engine:** It stimulates the human reasoning process by making the fuzzy inference on the values and if then rules.
- **De-fuzzification Module:** It transforms the fuzzy set obtained by the inference engine into a crisp value.

- In fuzzy logic everything is a matter of degree.
- Any logical system can be fuzzify.
- In fuzzy logic, knowledge is interpreted as elastic or equivalent; restrict all fuzzy variables in a group.
- Inference process is considered to be the elastic limit of the spread.

The complete data flow for the implemented concept are shown below in the Figures 1 to 3 in form of Level 0 and Level 1 DFD.

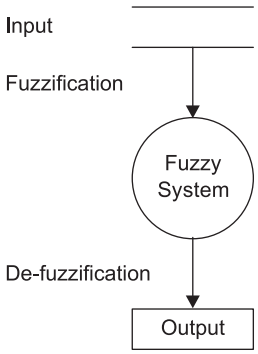


Figure 4: Context Level Diagram

Context level data flow diagram describes the simple view of fuzzy logic. It describe the process which firstly input is provide from the database and after that do the fuzzification in fuzzy system and de-fuzzify the system and get the output.

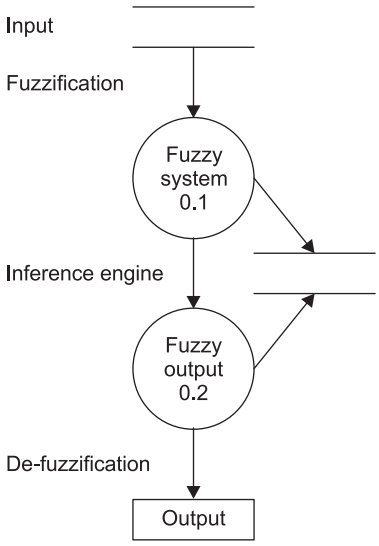


Figure 5: Level 1 Diagram

Neural Network

An individual can easily train a NN to accomplish a particular function by means of amending the values of the weights (connections) amongst several components. Normally, neural networks are trained, or adjusted, so in a particular input directs to a precise target output.

Methodology

In the research, hybrid technique is used in which Discrete Wavelet Transform, Fuzzy Logic, and Neural Network algorithm are used together for better and enhanced results.

The methodology goes in the following manner:

Step 1: START

Step 2: Initially upload any sample video to embed. Then, take a sample from video which is known as frame.

A. Embedding Process starts

Step 3: Once, sample has been taken then we can upload secret message in the uploaded video by using Discrete Wavelet Transform technique, fuzzy logic and neural network technique.

Step 4: After this result obtained required Steganovideo which has hidden image in it.

B. Extraction Procedure begins

Step 5: For extraction procedure gain apply DWT but in reverse direction. Then apply fuzzy logic and neural network.

Step 6: And as a result we will obtain hidden message that is embedded on the video.

Step 7: In the end, evaluate results using given parameters such as: PSNR, MSE.

Step 8: PSNR is most easily defined by the MSE.

$$\text{MSE} = 1/mn \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [\text{I}(i, j) - \text{K}(i, j)]^2$$

Step 9: Mean Square Error

$$\text{PSNR} = 10.\ \log_{10}(\text{MAX}_\text{I}^2/\text{MSE})$$

Lemma 1: Video Division using DWT Algorithm

```
set(handles.dip,'String','Please wait DWT applying....');
mkdir 'DWT Image'
for l = 1:shuttleVideo.NumberOfFrames
image=imread(fullfile('images',sprintf('%d.png',l)));
nbcol = size(image,1);
[cA1,cH1,cV1,cD1] = dwt2(image,'db1');
cod_cA1 = wcodemat(cA1,nbcol);
cod_cH1 = wcodemat(cH1,nbcol);
cod_cV1 = wcodemat(cV1,nbcol);
cod_cD1 = wcodemat(cD1,nbcol);
dec2d = [cod_cA1,cod_cH1;cod_cV1,cod_cD1];
imwrite(uint8(dec2d),fullfile('DWT Image',sprintf('%d.png',l)));
end
```

Lemma 3: Fuzzy Proposed Algorithm

```
function[result_data]= identifyfuzzyruleset(main_image)
% Detailed explanation goes here
[r,c]=size(main_image);
result_data=zeros(r,c);
fori=1:r
mf=mean(main_image(i,:));
for k=1:c
current=main_image(i,j);
if current>mf
result_data(i,j)=current;
end
end
end
```

Lemma 2: NN Proposed Algorithm

```
net=newff(trainingdata',group,10);
net.trainparam.epochs=50;
net=train(net,trainingdata',group);
testdata=notembeddingpos(trainingpercentage:ra,:);
result=sim(net,testdata');
result=round(result);
if result==0
result=1;
end.
```

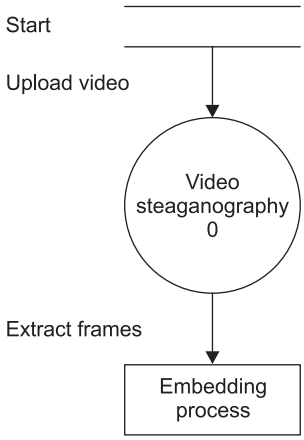


Figure 6: Context Level Diagram

Level 0 depicts that the uploading of video file and extraction of frames for steganography and how to embed video with secret data Almost all digital file formats that can be used steganography, but more suitable format are those with highly redundant and in proposed work. Avi format has been selected.

Level 1 shows the uploading of video file with secret message. Apply DWT, fuzzy logic and train with neural network and embed with secret data.

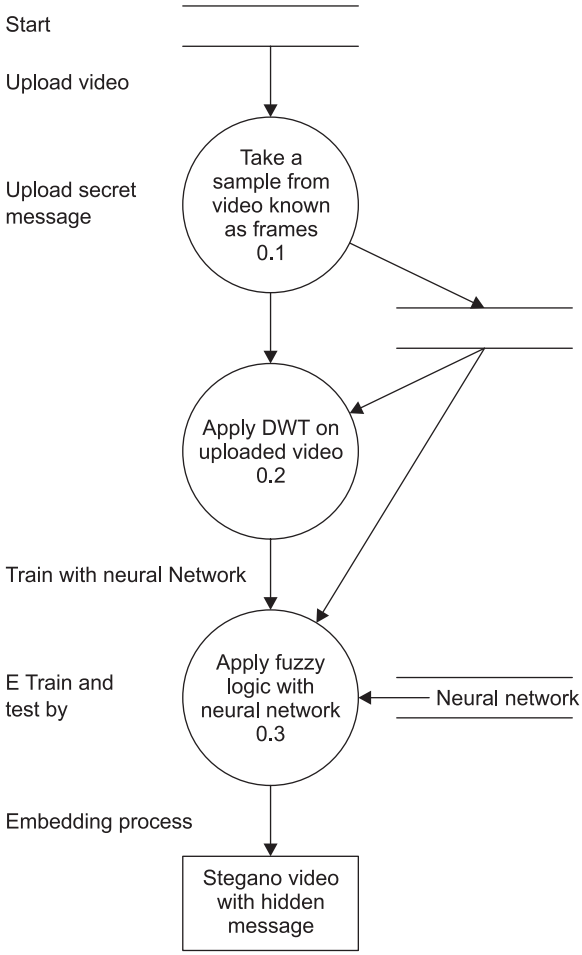


Figure 7: Level 1 Diagram

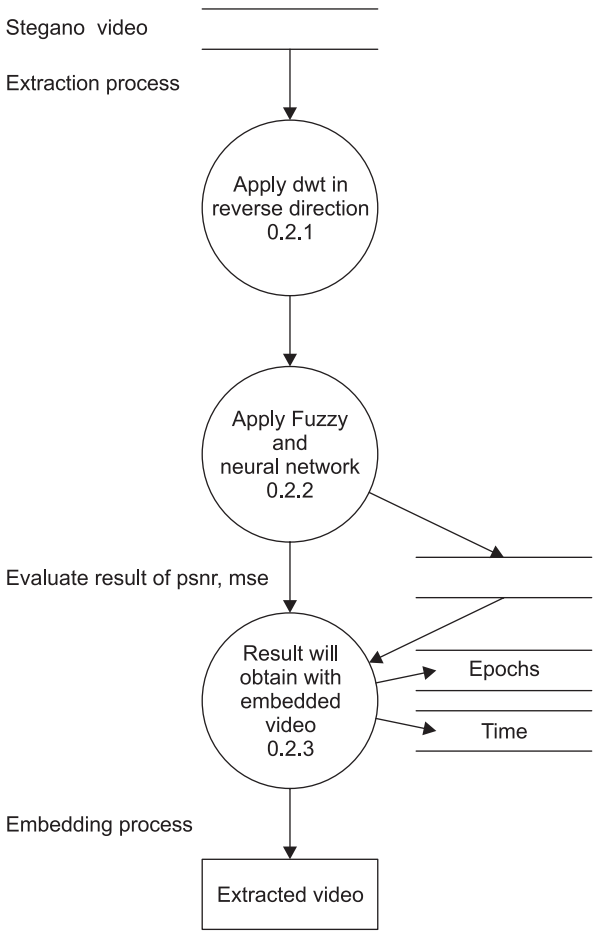


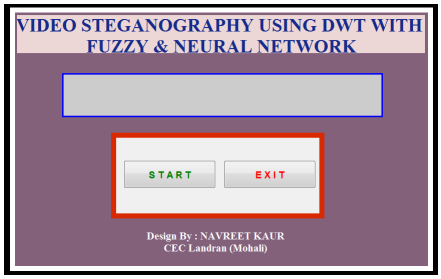
Figure 8: Level 2 Diagram

Level 2 Diagram describes the detailed processing of steganography and training percentage. After computing training data, perform classification operations to evaluate the performance. Performance can be evaluated by the parameters PSNR and MSE.

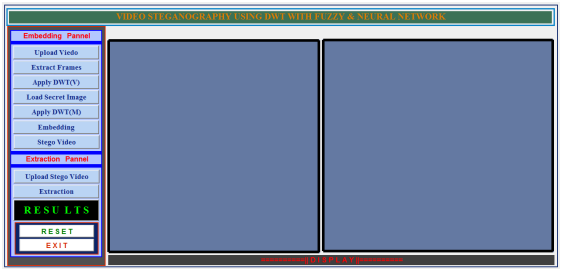
4. EXPERIMENTAL RESULTS AND DISCUSSION

This section evaluates the performance of DWT, Fuzzy Logic, and Neural Network. Windows 7 based system with 4GB of RAM, 500GB of HDD, an Intel(R) Core(TM) i7 CPU, is used for conducting this research. Simulation tool MatlabR2010a is used is used for implementation. For overall evaluation of implemented concept, parameters of kappa coefficient, water percentage and accuracy are considered.

The two parameters are measured in paper one is peak signal to noise ratioand another one is mean square error.PSNR is most commonly used to measure the quality of reconstruction of lossy compression. The signal in this case is the original data, and the noise is the error introduced by compression. 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, in some cases it may not. One has to be extremely careful with the range of validity of this metric; it is only conclusively valid when it is used to compare results from the same codec and same content. The MSE is a measure of the quality of an estimator—it is always non-negative, and values closer to zero are better.



(a)



(b)

(c)

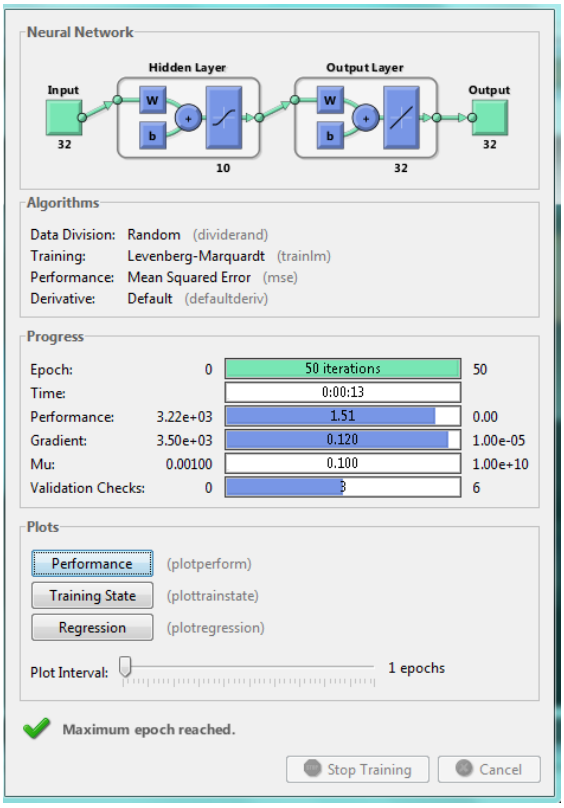
(d)

Secret Image

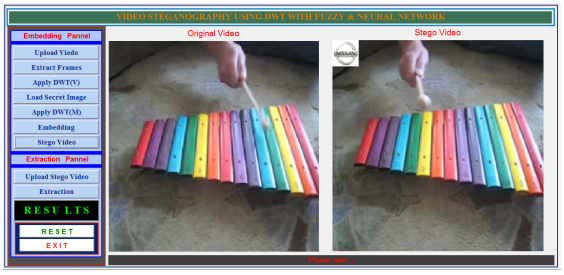
(e)

DWT of Secret Image

(f)



(g)



(h)

(i)

Figure 9: (a) It represents Starting window. It is the main GUI where user interact with system directly. One button is to start the window and another one is for exit, if we want to exit from window. (b) It shows Main Figure Window main GUI of the proposed work that mainly contains 3 panels i.e. embedding, extraction and performance evaluation, Where video is uploaded from database. In this some video samples are in database. (c) In window shows the uploading of video file for steganography. Almost all digital file formats that can be used steganography, but more suitable format are those with highly redundant and in proposed work. Avi format has been selected. Uploaded video and converting into frames. (d) In this figure Applying dwt on video to get optimal value and fragmentation of video file for steganography into 4 parts HH, LL, HL and LH. DWT is applied to get the video of optimal frequency value. (e) It depicts the secret image or data that we want to send to receiver end. This further follows DWT because secret message also divided into bands. (f) It represents DWT on Secret Image. In Embedded image is the embedding algorithm based result. Embedded image is obtained by applying secret data to cover image and to form 16 × 16 size blocks. (g) Neural Network Training Above window shows the embedding procedure using neural network in which chosen parameter values are epochs = 50S, Time = . 01 and performance value = 3.22e. (h) Extracted from the video data as secret video image frame passing no steganographic file. The video contains unused bits or secret data which can be very easily passing freedom of information bits. (i) Above figure is the extracted image from stegano video or the secret data behind the video. This can be done only with the extraction process

Table 1 shows the comparison of PSNR and MSE values of the proposed work and the previous work.

Table 1
Compariosn of PSNR and MSE

Exp No.	*PSNR*		*MSE*	
	Previous Work	*Proposed Work*	*Previous Work*	*Proposed Work*
1	86	92	0.125	0.034
2	84	91	0.312	0.043
3	86	94	0.523	0.0139
4	85	93	0.286	0.0253

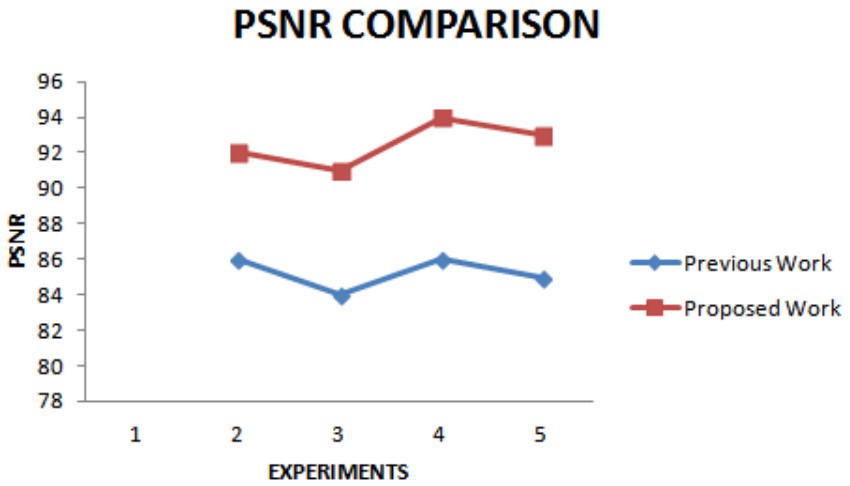


Figure 10: PSNR Comparison

Above figure shows the comparison of PSNR (Peak signal to noise ratio) values of proposed work and previous work. Blue line is for the previous work and red line is for the proposed work. It can be seen from the above figure that the value of PSNR is more in case of proposed work and is less for previous work.

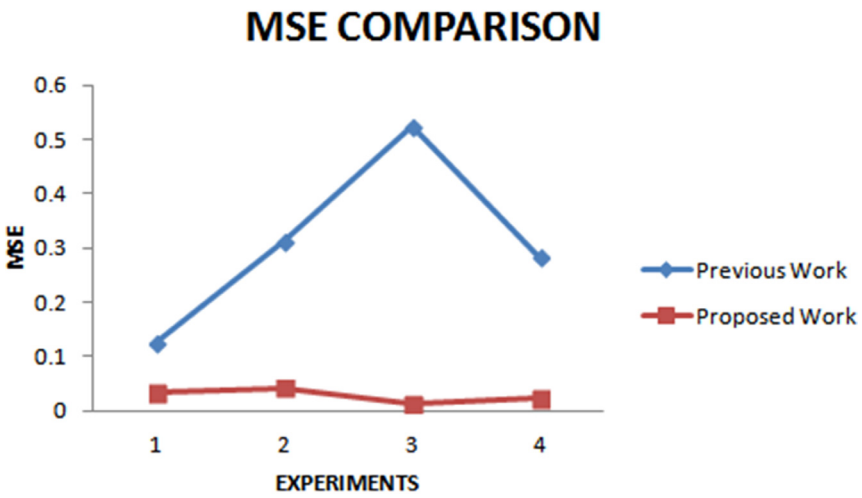


Figure 11: MSE Comparison

Above figure is for MSE (Mean Square Error) that shows the comparison of previous work and the proposed work. It can be seen from the above figure that the value of proposed work is less as compare to the work done before. Red line shows the proposed work and blue line is for the previous work done

5. CONCLUSION AND FUTURE SCOPE

There are numerous techniques for Video Steganography. But in proposed system video steganography has been achieved using DWT, Fuzzy and NN based method which results in good data hiding method. Utilization of Fuzzy and NN is done to get the steganography done at good accuracy rate. The proposed model is tested using MSE and PSNR metrics. We can conclude that this technique works well in data hiding within video files. Future work lies in the use of 32×32 quantization vector.

REFERENCES

[1] Kamal et. al., (2014), "Enhancement Key Of Cryptography And Steganography Using RSA And Neural Network", IJARCET, Vol. 3, pp. 1707-1710.

[2] Akshay et. al., (2013), "Steganography Technique using Neural Network", International Journal of Computer Applications", Vol. 82, pp. 39-42.

[3] Ell effly et. al., (2013), "Detecting pixel-value differencing steganography using Levenberg-Marquardt neural network", IEEE, Computational Intelligence and Data Mining (CIDM), pp. 160-165.

[4] Zhang, S. Wang, and X. Zhang, "Improving embedding efficiency of covering codes for applications in steganography," IEEE Communications Letters, Vol. 11, pp. 680-682, August 2007.

[5] MamtaJuneja et. al., (2009), "Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption", ARTCOM '09 Proceedings of the 2009 International Conference on Advances in Recent Technologies in Communication and Computing, pp. 203-209.

[6] Veerdeep Kaur Mann, Harmanjot Singh Dhaliwal, "32×32 Colour Image Steganography" International Journal of Engineering Trends and Technology (IJETT) – Volume 4 Issue 8- August 2013.

[7] Babloo Sha et. al., (2012), "Steganographic Techniques of Data Hiding using Digital Images", DESIDOC, Vol. 62, pp. 11-18.

[8] Mohit Garg, (2011), "A Novel Text Steganography Technique Based on Html Documents", JJAST, Vol. 35, pp. 129-135.

[9] Weiji Luo, (2010), "Edge Adaptive Image Steganography Based on LSB Matching Revisited", IEEE, Vol. 5, pp. 201-208.

[10] Ching-Sheng Hsu, Shu-Fen Tu, "Finding Optimal LSB Substitution using Ant colony Optimization Algorithm," IEEE, 2010.

[11] I. Khan, B. Verma, V.K. Chaudhari and I. Khan, "Neural network based steganography algorithm for still images," Emerging Trends in Robotics and Communication Technologies (INTERACT), 2010 International Conference on, Chennai, 2010, pp. 46-51