DOI: 10.13140/RG.2.1.4691.8649

Video Steganography using hybrid approach bacterial foraging technique and classification using Multi-Layer Neural Network

Anuradha[1] , Amandeep Verma[2]
Student (M.Tech), Assistant Professor
Department of Computer Science of Engineering
Punjabi University Regional Centre for Information Technology and Management, Mohali

Abstract- Steganography is the method of concealing data into pictures, videos, text files. It has been traditionally used by military and intelligence bureaus, offenders as well as police, circuit switch systems, as well as by civilian in daily life. Now multimedia data has been utilised to make them as cover picture. This dissertation focuses on the video steganography based on Bacteria Foraging Algorithm and Back Propagation Neural Network. It is the technique in which embedding secure information into the simple media with the correction to the cover image is done. Video Steganography means secret information that can be either a secure image or text within a bigger one in such a way that just by looking at it, an unauthorized human can't be detect the any secure information. For secure info in the video / frames there are numerous steganography methods .We implemented the bacteria foraging algorithm for reduce the number of bits and classify the data using back propagation neural network. The classification generates the two networks to show the output i.e., Training Module and Testing Module. Evaluate the performance parameters like mean square error rate, bit error rate and peak signal to noise ratio.

Keywords- *Video Steganography, Image extensions, bacteria foraging Optimization Algorithm and Discrete Cosine Transformation.*

I. INTRODUCTION

Video Steganography is a method to leather some particular type of documents into a transporting Video folder. The utilization of the video dependent Steganography could possibly be extra suitable than any former programme documents, for the reason which is of its size as well as memory necessities. Video Steganography could easily be distributed into two groups. One of them implants top-secret memo in the pixels of the audio-visual structures [1], directly. The further kind of video Steganography hides message inside the compressed area of videos by means of marginally altering the motion vectors forecast manners as well as inconstant elongated cyphers. For video Steganography in particularly spatial domain, this encrypts the text using error rectifying code & also inserts them inside the video file at numerous positions that fight back the video compression to some particular degree but then again restricts the implanting capacity. The other group is specifically intended for compressed video. The aforementioned directly amends the factors which are present in the compressed domain, as a consequence it assimilates Steganography directly inside the compression arrangement however it is quiet delicate to face any kind of distortion, in addition to the implanting capacity is also very restricted, for the reason that there are smaller amount of factors that could easily be altered to transmit clandestine message.Steganography is the talent or exercise of hiding a meaning, picture, or document inside additional memo, picture, or folder. The term steganography is derived from the Greek word Stegano sense enclosed & graphed sense script [2] describing it as exposed script. It combines the Greek words Stegano sense "enclosed or else endangered", in addition graphed signifying "writing". In the present electronic correspondence situation, information safety is main of the significant difficulties. Afterward the World War II, the requirement for a safe & healthy communiqué amongst the collaborating units has improved due to the dread of assassination. The distributers of ordinal sound & video feature are troubled of their everything being tarnished by illegal repetition or redeployment; henceforth it is of essential significance to secure data. Cryptography is the system to conceal mystery information by clambering so that it is ambiguous, [3]on the other hand it doesn't guarantee safekeeping as well as sturdiness as the hacker can perceptibly deduction that there is an intimate memo transitory on from the foundation to the terminus. Steganography is masked inscription as well as it is the systematic method of implanting the top- top-secret information inside[4] a protection broadcasting such that the unlicensed spectators doesn't acquire any type of impression of any data concealed in it. Steganography is a substitute on the way to cryptography in which the top stealthy information is implanted inside the transporter in such kind of method in which solitary carrier is noticeable that is directed from transmitter in the direction of receiver left devoid of climbing. Digital video is one kind of familiar digital media on the Internet.

DOI: 10.13140/RG.2.1.4691.8649

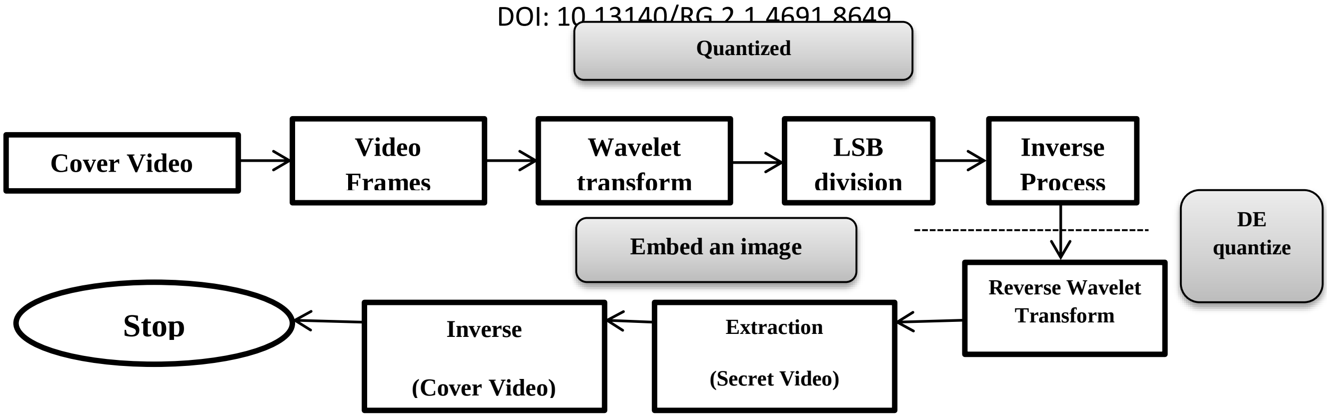


Fig.1 Video Steganography

Through the progress of video compression technique & torrent broadcasting operation, the application area of video is more & more widely,for example, video on demand & video conference. Moreover, the gradual prevalence of portable video camera & the video edit software, people can easily record, edit & release video on the Internet, which makes the video transmission more frequently. In addition, the characteristics of large data amount, abundant content & complicated statistics for video make it must be an important carrier for steganography. Consequently, it is of countless status to learning the technique of video steganography & the opposed technique - video steganalysis[5].

II. MECHANISM OF STEGANOGRAPHY

Here, the basic ideas involved in hiding top- top H secret information 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. The following step is to choose, introduce, as well as run a stenographic device to[6] insert the top-secret in the cover 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 excerpt the hidden memo since the stego file. Figure depicts the flow of the top- top-secret communication.

Sender

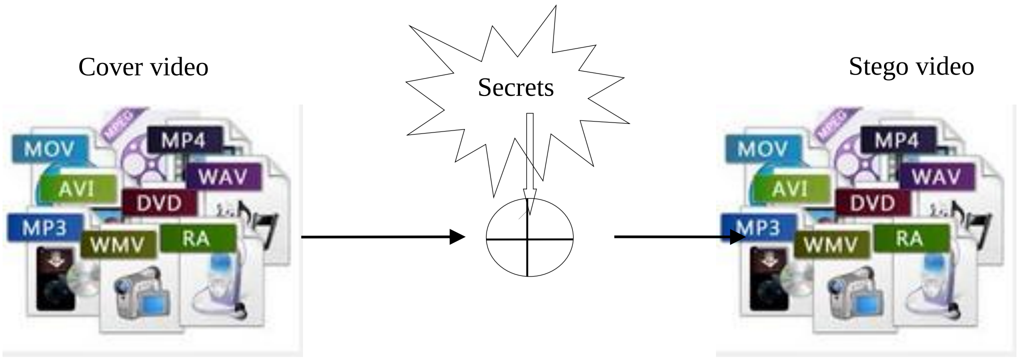


Fig no: 2 Mechanism of Steganography at sender side

Receiver

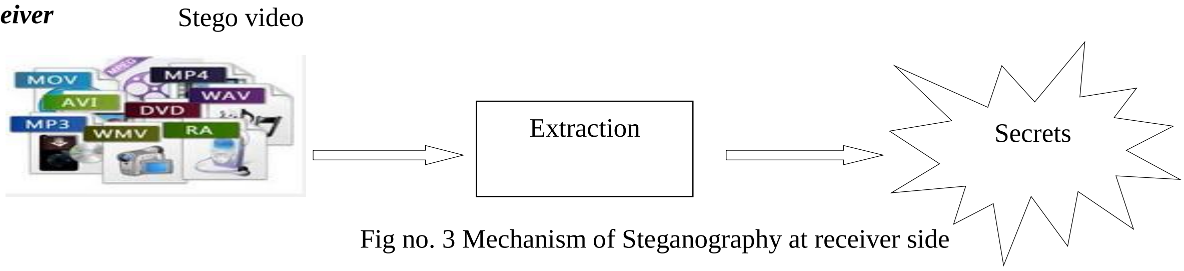


Fig no. 3 Mechanism of Steganography at receiver side

III. RELATED WORK

Kamal et al., 2014 [7] this paper uses the RSA encryption algorithm & Back Propagation Neural Network for the encryption of the message. Firstly DCT is applied to cover picture, after this vector quantization matrix is achieved. After that encryption of message is done using Rsa encryption algorithm & Back propagation algorithm. In the end algorithm comparison is done along with result

DOI: 10.13140/RG.2.1.4691.8649

evaluation based on PSNR & MSE parameters. **Akshay et al., 2013[8]** paper overcomes the drawbacks of LSB methods, in this technique firstly Characters are converted to ASCII codes. Then these bits are converted to binary numbers, after that they are stored in LSB bits. The binary bits are not arranged in sequential manner. Therefore amount of storage increases. This inconsequential storage led to the high security. After that if anyone wants to decrypt the data, then he/she has to know following: length of message, number of messages, starting row. The proposed techniques are implemented using MATLAB & it is implemented on the images like Lena, peppers, baboon etc. The proposed technique measure the performance of the proposed algorithm using PSNR & MSE parameters. **Ell effly et al.,2013[9]**paper, combined algorithm has been implemented to enhance the security in the steganography using neural network & Liebenberg-Marquardt neural network learning algorithm. It removes the disadvantage of Back propagation neural network that has the slow learning process. This proposed algorithm has been implemented on the digital pictures contains hidden messages. The idea is to analyze pictures before & after embedding to extract discriminating features & then build a neural network recognition model. The proposed approach is empirically evaluated & compared with four other machine-learning methods. The proposed algorithm gets the 93% detection rate. **Youssef, 2012[10]** proposed algorithm uses the SQL queries in the steganography using text. The message that has to hide is taken, after that it is mapped to the random text. Mapping is done using hash based search algorithm. The random word generation is equal to ASCII words. The generated words are split into two parts using SELECT & WHERE clause. For long SELECT queries, a postprocessor splits them into smaller queries based on a random index. This has no effect on recovering the top-secret message as long as the smaller queries are sent sequentially one after the other to the receiver. In future, use of other queries like INSERT, DELETE etc. can be done & on the other language than the English. **Babloo Sha et al, 2012[11]** discuss the various steganography techniques like Spatial & Frequency based steganography methods. In Spatial technique various sub techniques has been reviewed like EzStego data hiding scheme, S-Tools, Hide & Seek, StegoDos, White Noise Storm, Bit plane complexity segmentation steganography, Information Theory-based Data Hiding, Dynamic Programming-based Steganography Technique, Data Hiding using Convolution Decoder. In frequency technique various sub techniques has been reviewed like JSteg, JSteg-Shell, JPHide, & OutGuess, Genetic Algorithm-based Data Hiding, Data Hiding Techniques: F3, F4 & F5.

IV. EXISTING PROBLEM

The proposed work aims to solve the following problems:

- Steganography mention to a system where particular kind of satisfied is secreted addicted to comparable or different arrangement.
- In such a difference a lot of processes have been castoff at present which possess respectable results.
- The existing work uses wavelet transformation along with optimizing algorithm to check the performance of the hiding capacity of the system.
- The problem of this research work is to optimize the current architecture replacing bfo and enhance the performance according to Multi- layer Architecture. The parameters of judgment would be.

V. PROPOSED ALGORITHM

We implemented the approach in the video steganography proposed Algorithm like Bacteria Foraging Optimization and Classify the Back Propagation Neural Network.

a) Bacteria Foraging Optimization Technique

Throughout scavenging of the physical microorganisms, movement is attained by a usual of ductile flagella. Flagella assistance an E.coli bacterium to somersault or spin, which double basic processes are done by a bacterium at the period of scavenging. Once they replace the flagella in the circular way, every flagellum yanks on the cell. Those fallouts in the touching of flagella self-sufficiently & lastly the bacterium somersaults with smaller amount of plummeting whereas in a harmful place[12] it tumbles frequently to find a nutrient gradient. Touching the flagella in the hostage circular way helps the bacterium to spin at an actual debauched degree. In the aforementioned procedure the microorganisms experiences chemo cabs, where they similar to change near a nutrient incline & evade harmful situation. Generally the microorganisms change for a lengthier coldness in a welcoming situation.

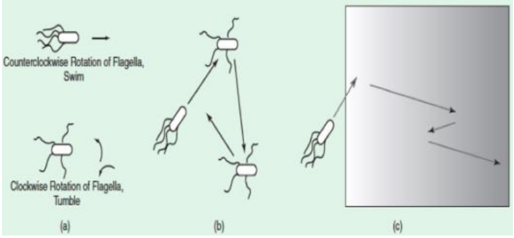

Counterclockwise Rotation of Flagella, Swim
Clockwise Rotation of Flagella, Tumble
(a)
(b)
(c)

Fig.5 Bacteria Foraging Optimization Motion

b) Back Propagation Neural network

Classification is a field of learning in which attributes are matched. These algorithms are called machine learning algorithms. Figure 6shows a simple architecture of an organization scheme.

There are 2 chief phases in an arrangement structure:

- Training stage;
- Testing stage.

DOI: 10.13140/RG.2.1.4691.8649

Back Propagation Neural Network is an organically stimulated organization algorithm. It consists of amount of simple neuron like processing units, prearranged in layers. Every unit in a layer is related with all the units in the preceding layer. These connections are not all equal: each joining may have a different strength or weight. The bulks on these contacts encode the information of a network. Frequently the units in a neural network are also called nodes [13].

Data arrives at the inputs & permits through the network, layer by layer; pending it arrives at the productivities. Throughout consistent process, that is when it acts as a classifier, there is no comment between layers. This is why they are identifying back propagation neural system [14].

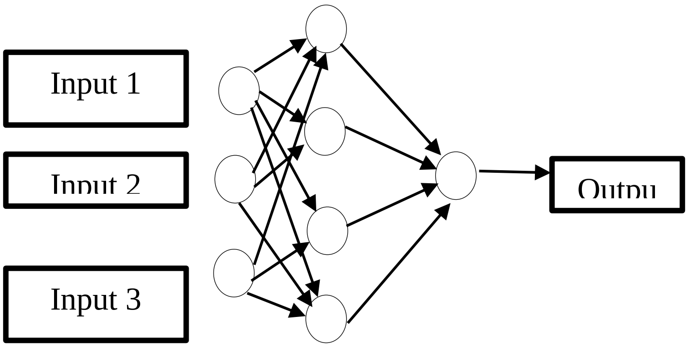


Fig.6 Back Propagation Neural Network

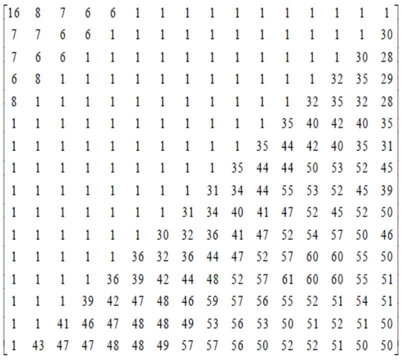
VI. DESIGN AND IMPLEMENTATION

In embedding process, initially the cover picture is distributed into non-overlapping blocks of 16*16. The top-secret information is implanted inside the quantized DCT coefficients afterwards of quantization [15]. The phases are as follows:

1. A gray scale picture is occupied as well as a message is produced for hiding inside the picture.
2. Top-secret data message is encoded as well as transformed to binary format.
3. Then, the cover picture is segmented into non-overlapping blocks of 16*16. Then they are additionally converted into DCT coefficients in transform domain.
4. Discrete Cosine Transform changes every single block into DCT coefficient matrix.
5. A quantization table is designated & is DCT coefficients are quantized with the quantization table utilizing the formula as given below:

ROUND (DCT 8 *8 block/ Quantization Table) = Sparse Matrix.

6. Run-length encrypting is implemented on the deliberated quantized coefficients so as to accomplish the compressed picture. Figure below demonstrates the 16*16 quantization table utilized in our technique.



$$\begin{bmatrix}
16 & 8 & 7 & 6 & 6 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
7 & 7 & 6 & 6 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 30 \\
7 & 6 & 6 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 30 & 28 \\
6 & 8 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 32 & 35 & 29 \\
8 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 32 & 35 & 32 & 28 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 35 & 40 & 42 & 40 & 35 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 35 & 44 & 42 & 40 & 35 & 31 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 35 & 44 & 44 & 50 & 53 & 52 & 45 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 31 & 34 & 44 & 55 & 53 & 52 & 45 & 39 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 31 & 34 & 40 & 41 & 47 & 52 & 45 & 52 & 50 \\
1 & 1 & 1 & 1 & 1 & 1 & 30 & 32 & 36 & 41 & 47 & 52 & 54 & 57 & 50 & 46 \\
1 & 1 & 1 & 1 & 1 & 36 & 32 & 36 & 44 & 47 & 52 & 57 & 60 & 60 & 55 & 50 \\
1 & 1 & 1 & 1 & 36 & 39 & 42 & 44 & 48 & 52 & 57 & 61 & 60 & 60 & 55 & 51 \\
1 & 1 & 1 & 39 & 42 & 47 & 48 & 46 & 59 & 57 & 56 & 55 & 52 & 51 & 54 & 51 \\
1 & 1 & 41 & 46 & 47 & 48 & 48 & 49 & 53 & 56 & 53 & 50 & 51 & 52 & 51 & 50 \\
1 & 43 & 47 & 47 & 48 & 48 & 49 & 57 & 57 & 56 & 50 & 52 & 52 & 51 & 50 & 50
\end{bmatrix}$$

Fig no: 4 Quantization Table 16*16

These are the following steps which are followed:

STEP 1 : First step is to upload the video.

STEP 2 : Sample is taken from the video.

STEP 3 : Quantization of the sample picture is done using DCT masking.

STEP 4 : Image to embed is uploaded

STEP 5 : Bacteria foraging algorithm is applied for optimization.

STEP 6: Back propagation neural network is used for embedding.

STEP 7 : De-quantization is applied.

STEP 8 : Stego video is obtained.

STEP 9 : Secret image is extracted from stego video.

A. Implementation

We find the three parameters like Mean square error rate, Bit Error Rate and Peaks Signal To Noise Ratio.

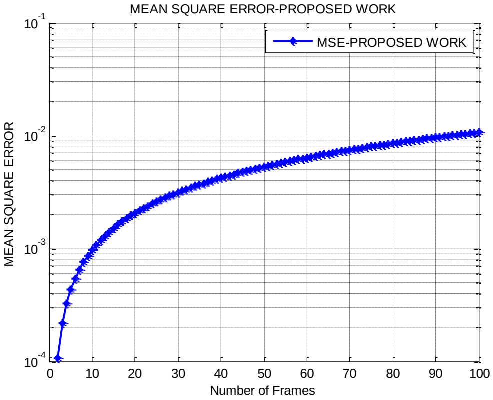


Fig.5 Mean Square Error Rate

The above figure define that the mean square error rate implemented the proposed work parameter is decrease to improve the quality of the video frames.

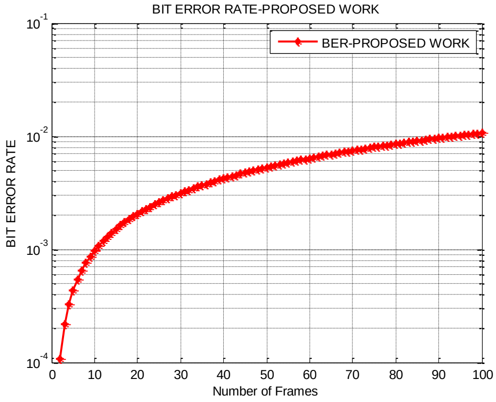


Fig.6 Bit Error Rate

The above figure defines the error of the bit error in the video steganography. BER means loss the data (bits) in the frames.

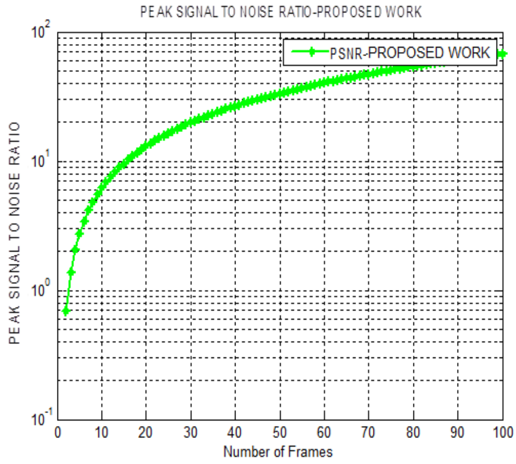


Fig.7 Peak Signal To noise Ratio

Above figure defined that the peak signal to noise ratio means increase the value to better video quality and error must be reduced.

Table no: 1 Comparison between Base paper and Proposed work in 12 frames

Comparison between Frames base work and proposed Work	12 frames(bp)	12 frames (pp)
Maximum of PSNR between H and ST	37.68DB	40.45 DB
Minimum of PSNR between H and ST	34.75 DB	42.3DB
Average of PSNR between H and ST	36.45 DB	43.56 DB

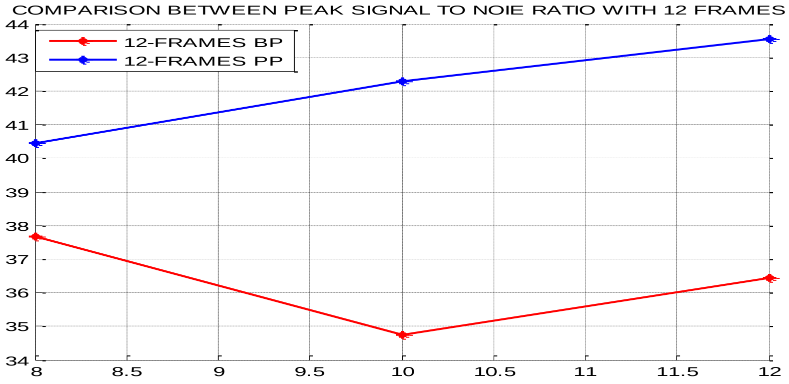


Fig.8 Comparison between PSNR (bp) and PSNR(pp) with 12 frames

Figure described that the comparison between peak signal to noise ratio base paper and proposed work with 12 frames.

V. CONCLUSION AND FUTURE SCOPE

The proposed system combines a number of earlier methods in order to get improved reconstruction quality. In addition to this arrangement, some novel methods are also proposed to improve the efficiency of the previous methods. As we have now deliberated about the requirement of the video steganography & its usages. This investigation effort has been realized to improve the steganography method so that the excellence of the video remnants the similar. Here, the basic ideas involved in hiding a top-secret information 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. The following step is to choose, introduce,

DOI: 10.13140/RG.2.1.4691.8649

as well as run a steganography device to insert the top-secret in the cover 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. To implement our objectives, we have used Back Propagation Neural Network in a combination with, BFOA Algorithm.

Video Steganography using BFO and BPNN is realized in this study. This Work can further be extended. In this study we used single image to hide in a video. In future work we can use more than one image to hide or we can hide a video in other video. In this study we used only .avi videos so in future other formats can be used as a cover medium.

VII. REFERENCES

[1]. Sandeep Kumar Behera et al., 2010, "Colour Guided Colour Picture Steganography", Universal Journal of Computer Science & Engineering Technology, Vol. 1, pp. 16-23, Oct. 2010.

[2]. Weiji Luo, 2010, "Edge Adaptive Picture Steganography Based on LSB Matching Revisited", IEEE, Vol.5, pp.201-208.

[3]. Lorenzo et al, 2009, "Peak-Shaped-Based Steganographic Technique for JPEG Pictures", *EURASIP Journal on Information Security, 2009.*

[4]. Mamta Juneja et al., 2009, "Designing of Robust Picture Steganography Technique Based on LSB Insertion & Encryption**"**, ARTCOM '09 Proceedings of the 2009 International Conference on Advances in Recent Technologies in Communication & Computing, pp.203-209.

[5]. Samir Kumar et al., 2008, "A Novel Steganographic Technique Based on 3D-DCT Approach", Computer & Information Science, Vol. 3, pp. 229-235.

[6]. G. Sahoo et al., 2008, "Designing an Embedded Algorithm for Data Hiding using Steganographic Technique by File Hybridization", MISC.

[7]. Kamal et al., 2014, "Enhancement Key Of Cryptography & Steganography Using RSA & Neural Network", IJARCET, vol. 3, pp. 1707-1710.

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

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

[10]. Youssef, 2012, "A Generation-based Text Steganography Method using SQL Queries", IJCA, Vol. 57, pp. 27-31.

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

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

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

[14]. Deeply (Nov 2012) "Steganography with Data Integrity", International Journal of Computational Engineering Research (ijceronline.com), Vol.2, Issue 7.

[15]. T. Morel, J.H.P. Elf, M.S. Olivier, "An Overview of Picture Steganography", Information & Computer Security Architecture (ICSA) Research Group Department of Computer Science, University of Pretoria, 0002, Pretoria, South Africa.