International Journal of Emerging Technology and Innovative Engineering
Volume 1, Issue 9, September 2015 (ISSN: 2394 – 6598)

VIDEO STEGANOGRAPHY USING NEURAL NETWORK AND GENETIC ALGORITHM

Heena Goyal
M.tech Student
ECE Department
CEC Landran, Mohali
heenagoyal91@gmail.com

Preeti Bansal
Assistant Professor
ECE Department
CEC Landran, Mohali
cecm.ece.pb@gmail.com

ABSTRACT

Steganography is a strategy for concealing mystery messages into a spread media such that a planned eyewitness won't be mindful of the presence of shrouded messages. In such applications different record arrangements are utilized as spread item which contains private information. Video Steganography is the system of whipping some clandestine message inside a video. The utilization of video dependent steganography could possibly be more suitable than any other multimedia files, because of its size and memory necessities. Information security has become the area of concern as a result of extensive use of communication medium over the internet. Due to the worldwide use of multimedia content over the internet, the emergence for security has been increasing day by day. This paper focuses on the security using combination of optimization technique with machine learning methods to enhance the rate of security in realistic applications. In proposed work GA has been used for optimization whereas neural network has been used for embedding. The results show a considerable improvement in terms of PSNR and MSE values in MATLAB environment.

KEYWORDS- Video Files, Steganography, Genetic Algorithm, Neural Network.

I. INTRODUCTION

In a highly digitalized world, computers help in transforming analog data into digital form before storing or processing. In the mean while, the internet develops very rapidly and hence becomes an important medium for digital data transmission. However, being a fully open access, the internet brought us not only convenience but also some hazards and risks. If the data to be transmitted is confidential, it is often convenient for some malicious users to illegally copy, destroy, or edit them on the internet. As a result, information security becomes an essential issue and thus leads to improvement for secure data transmission [1]. So to hide the data in less time, only one solution occurs that is steganography [2]. The foremost objective of steganography is to interconnect steadily in an absolutely untraceable mode and also to inhibit depiction doubt towards the broadcast of a concealed data. Thus, it is not possible for other persons to guess about the concealed information.

Steganography is the art or practice of hiding a message, picture, or document inside another message, picture, or file. The term steganography is derived from the Greek words stegano means "covered or else protected", in addition graphed signifying "writing". Steganography can be of text, image, video depends on the input file [4].

Video Steganography is a method to hide some particular type of files into a transporting Video file [6]. The utilization of the video dependent Steganography could possibly be more suitable than any other multimedia files, for the reason which is of its size as well as memory necessities [7].

The image steganography tried to improve the capacity but in the literature more than 50% of the original image has been used to hide the secret messages. Since, there is a limitation on how much data can be hidden into an image, making it difficult to use the image methods. In order to increase the security of collaborative documents, video steganography is useful in many ways. The video based steganography has been found to overcome the capacity problem as the video consists of a number of images placed in an order to be presented in sequence one after the other [9].

Earlier, many algorithms have come into existence but the proposed method is based on Genetic algorithm and Neural Network [10].

The rest of the paper is organized as follows. Section II presents mechanics of video. Section III presents the outline of the system. Section IV presents the brief outline of the methodologies that has been used. Section V shows the implementation and results and finally Section V concludes the paper.

II. MECHANICS OF VIDEO

Here, the basic idea involved is in hiding a secret data in the video carrier document. The principal step is to choose a cover video [17]. It would seem most appropriate to select a small bit video. The following step is to choose, introduce, as well as run a steganographic device to insert the secret message in the cover video. Once embedded, the file is referred to as stego file which can be sent to the receiver. Once the stego file is received, the intended recipient should know how to reverse the process [16] and to retrieve the secret data. The same steganography tool is used to extract the hidden message from the stego file. Figure 1 and Figure 2 depicts the flow of the secret communication.

SENDER SIDE

Figure 1: Sender Side

RECEIVER SIDE

Figure 2: Receiver Side

III. OUTLINE OF THE SYSTEM

The issues of the design and implementation of the Video Steganography System (VSS) can be subdivided into two main parts. The first part is image processing and the second part is embedding process. The image processing part consists of Discrete Cosine Transform (DCT) and Genetic Algorithm (GA) in which DCT is used for quantization and segmentation of the selected frame of video file. Genetic Algorithm is used for the optimization of sample image so as to remove useless data bits by using fitness function and it helps in providing best solutions.

The second part consists of Feed Forward Neural Network which is used for classification purpose so as to distinguish the pixels in less sensitive areas

from more sensitive areas to embed the secret data. Figure 3 depicts the flowchart for the proposed video steganography system.

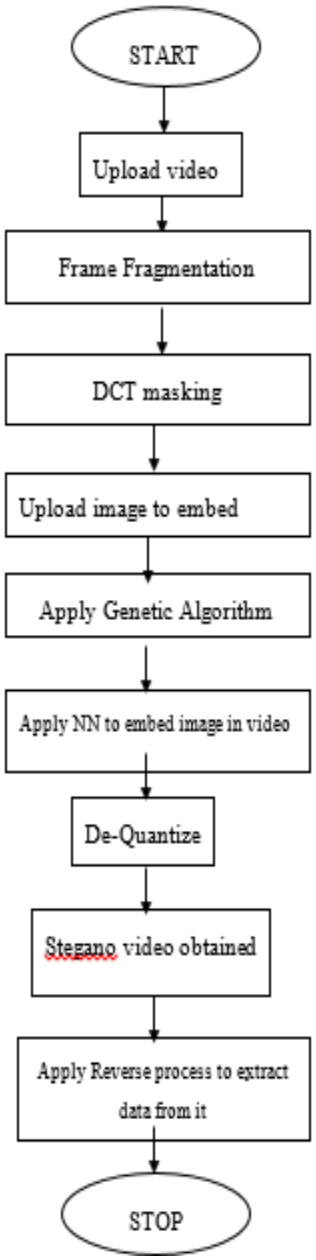

Figure 3: Proposed Flowchart

These are the following steps which are to be followed:

Step 1 : Initially upload video to embed.

Step 2 : Then, take a sample from video which is known as frame.

Step 3 : Once, sample has been taken then quantizes the selected frame by utilizing 16*16 matrix DCT masking.

Step 4 : After quantizing video sample, upload secret image in the system.

Step 5 : Then, apply genetic algorithm designed for removing useless data by using fitness function of genetic algorithm.

Step 6 : After removing useless part/data, apply neural network to embed secret image in video.

Step 7 : Then apply De-quantization.

Step 8 : Stegano video is obtained which has hidden image in it.

Step 9 : Now, for extraction purpose apply reverse process to extract the secret data from video.

IV. PROPOSED ALGORITHM

As mentioned even earlier, the proposed algorithm is divided into two sections namely the training and testing section. The training section includes two algorithms, first for the feature extraction and another is for feature optimization. The details are as follows:

1. Discrete Cosine Transform (DCT)

DCT is a wide-ranging orthogonal transform meant for digital picture handling as well as signal handling using benefits for instance great compression ratio, lesser bit error rate, upright data amalgamation capability as well as good synthetic result of calculation intricacy [15]. DCT allows a picture which is need to be wrecked up inside diverse frequency groups specifically the low, middle as well as high frequency bands consequently making it easier to select the band in which the secret data is to be implanted.

- The input image is N by M; where N is no of rows and M is no. of columns.
- f(i,j) is the intensity of the pixel in row i and column j;
- F (u,v) is the DCT coefficient in row k1 and column k2 of the DCT matrix.
- For most images, much of the signal energy lies at low frequencies; these appear in the upper left corner of the DCT.
- The DCT input is 16 by 16 array of integers.
- This array contains each pixel's gray scale levels from 0 to 255.

2. Genetic Algorithm (GA)

GAs were first described by John Holland in the 1960s and further developed by Holland and then by students and colleagues of the University of Michigan in the 1960s and 1970s [16]. Genetic algorithms (GAs) are computer programs that take off the processes of biological growth in order to explain the problems and to make evolutionary systems. GA helps in specifying the problem to be solved and a bit-string illustration for candidate solutions, the simple GA works as follows:

- At random, produce an initial population M (0).
- Compute as well as help save the actual fitness f(m) for every specific individual m in the current population M(t);
- Specify selection probabilities p (m) for every specific individual m throughout M (t) making sure that p (m) is actually proportional to f (m).
- Crank out M (t+1) by simply probabilistically choosing individuals from M (t) to produce offspring via genetic operators.

3. Neural Network (NN)

Machine learning algorithms facilitate a lot in decision making and neural network has performed well in categorization purpose in various fields. Most of the popular techniques among them are neural network. Neural networks are those networks that are the collection of simple elements which functions in parallel [16].

The classification of images will be done using NN. Neural network is a network of "neuron like" units entitled as nodes as shown in figure 4 [17]. This neural evaluating method is utilized in fields of optimization, classification, as well as control theory and also for solving regression problems. NN are very effectual in case of classification problems where detection and recognition of target is required. NN is preferred over other techniques due to its active nature.

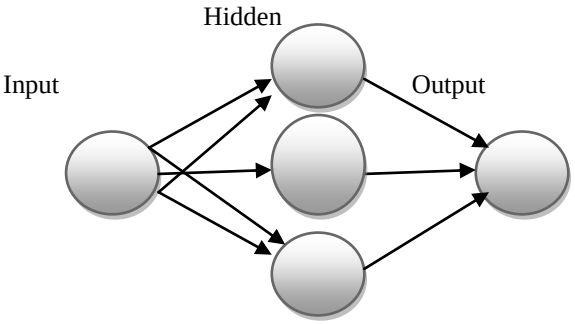

Figure 4: Neural Network

This active nature is attained via amending the weights according to final output and also to applied input information [18]. This amendment of weights takes place iteratively until desired output is obtained.

A neural network can be trained to perform a particular function by adjusting the values of the weights between elements. There are several

activation functions that are used to produce relevant output.

- The output layer provides the trained Neural Object which is used for the classification.
- Run network to get output
- Compute hidden and output layer
- Update weights using previous information.

.

V. RESULTS AND IMPLEMENTATION

The method proposed here effectively hides the secret data into a video using the Neural Network and Genetic Algorithm steganographic techniques in MATLAB environment. The database consists of original videos and embedded images of different sizes. Figure 5 and figure 6 shows the original videos and secret images respectively.

Figure 5: Original Videos

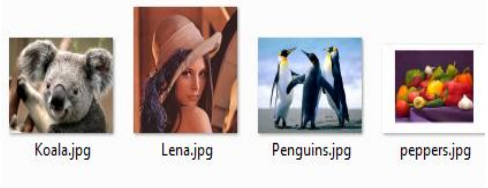

Figure 6: Embedded Images

The whole simulation has been carried out over MATLAB environment 7.10 using following parameters:

PSNR: The Peak Signal-to-Noise Ratio (PSNR) is defined as:

$$\text{PSNR} = 20\ \log_{10}\left(\frac{\text{MAX}}{\sqrt{\text{MSE}}}\right) \qquad (1)$$

Where MAX= Maximum Possible Pixel Value of an image. Generally it is 255.

MSE: The mean-squared error (MSE) is given by:

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

Where m,n- represents the size of image.

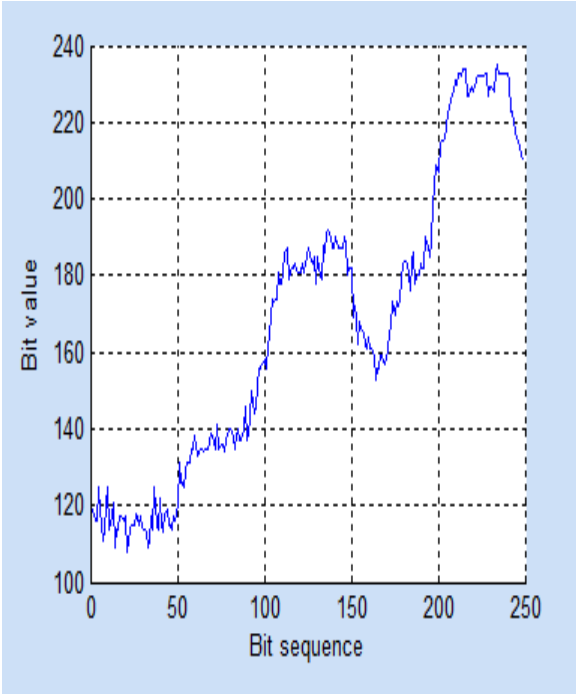

Figure 7: Optimization using GA

The above figure 7 shows the optimization using GA in which fitness function of GA has been chosen so as to remove useless data bits.

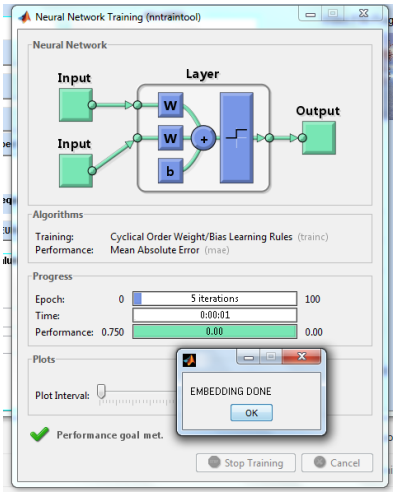

Figure 8: Embedding using neural network

The above figure 8 shows the embedding procedure using neural network in which chosen parameter values are epochs=100, Time = 0.01 and performance value=0.750.

The below Table 1 shows the values of MSE and PSNR for proposed technique. The values of MSE must be low in order to have good quality of stegano videos and the values of PSNR must be high for high security.

Table 1 MSE and PSNR Values

Images	MSE (%)	PSNR (dB)
Koala	0.021	64.50
Lena	0.024	64.51
Pepper	0.032	64.53
Penguins	0.023	64.51

Figure 9 and Figure 10 shows the performance of video steganography system in terms of MSE and PSNR respectively.

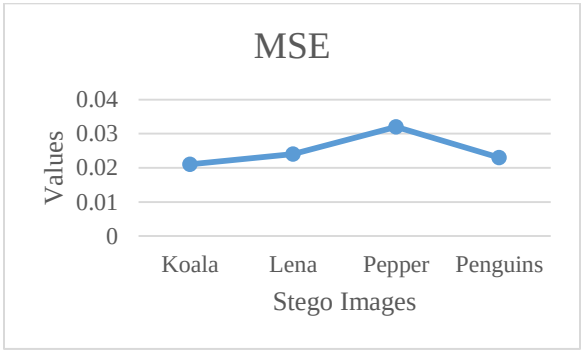

Figure 9: Performance analysis in terms of MSE

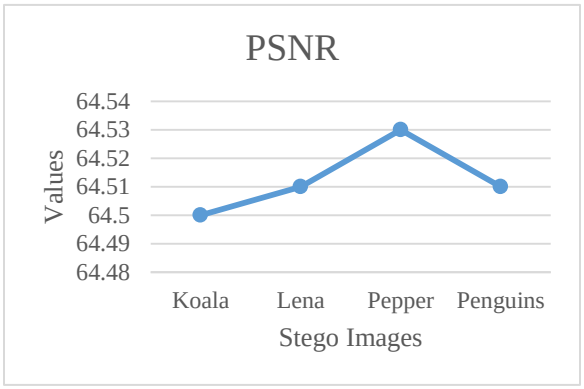

Figure 10: Performance analysis in terms of PSNR

VI. CONCLUSION AND FUTURE SCOPE

In this paper, a new video steganography system is described to increase the capacity and the imperceptibility of the video after embedding the secret image. GA is employed to reduce the error between the original video and the stegano video and also to reduce the algorithm complexity. The utilization of Genetic algorithm helps a lot in reduction of large number of obtained features.

The proposed work overall concluded that managing the pixels to a deeper level increases the capacity of the image to hide certain messages. Now a day's

Artificial Intelligence based Computers are used very rapidly in various fields and Neural Networks has gained a lot of attention. Neural Network has been found effective enough to acquire pixels to merge the data bits without much affecting the original pattern of the image.

The implementation results shows the values of MSE= 0.02% and PSNR= 64.50dB for proposed technique. The values of MSE must be low in order to have good quality of stegano video.

The future scope of this stance depends on the use of Fuzzy systems for high security and privacy. Also 32*32 quantization vectors can be used for further improvement in quality and imperceptibility. Using steganographic technique, private information is very easy to engender and disperse over the network without even noticed by any user. Steganography is of immense importance and it is highly used in the fields of Fingerprinting, Internet security, Copyright issues, Authentication etc.

REFERENCES

[1] Sheng Dun Hu, Kin Tak, U.,"A Novel Video Steganography based on Non uniform Rectangular Partition," IEEE International Conference on Computational Science and Engineering (ICCSE), pp. 57-61, August 2007.

[2] Imran Khan, Vijay K. Chaudhari, "Neural Network Based Steganography Algorithm for Still Images," IEEE International Conference on Emerging Trends in Robotics and Communication Technologies (ICETRACT), pp. 46-51, Dec 2010. DOI: 10.1109/INETRACT.2010.5706192.

[3] Balaji, R., Naveen, Garewal,"Secure Data transmission using Video Steganography," IEEE International Conference on Electro/ Information Technology (EIT), pp. 1-5, May 2011. DOI: 10.1109/EIT.2011.5978601.

[4] Feng Pan, Li Xiang, Xiao Yang, "Video Steganography using Motion Vector and Linear Block Codes," IEEE International Conference on Software Engineering and Service sciences (ICSESS), pp. 592-595, July 2010.

[5] Elham Ghasemi, Jamshid Shanbehzadeh, Nima Fassihi, "A Steganographic method based on Integer Wavelet Transform and Genetic Algorithm," IEEE International Conference on Communication and Signal Processing (ICCSP), pp. 42-45, Feb 2011.

[6] Danti, A. ,Manjula, G. R., "Secured data hiding of Invariant Sized secret image based on discrete and hybrid wavelet transform," IEEE International Conference on Computational Intelligence and Computing Research(ICCIC), pp. 1-6, Dec 2012. DOI: 10.1109/ICCIC.2012.6510181.

[7] Paul, R., Acharya, A. K., Yadav, V. K., Batham, S., "Hiding large amount of data using a new approach of Video Steganography," IEEE 4th International Conference on Information Technology (CIT), Sep 2013. DOI: 10.1049/CIT 2013.2338.

[8] Hanafy, A. A., Salama, G. J., Mohasseb, Y. Z., "A Secure Covert Communication model based on Video Steganography," IEEE Military Communication Conference (MILCOM), pp. 1-6, Nov 2008. DOI: 10.1109/MILCOM 2008.4753107.

[9] Sunil K. Moon, Rajeshree. D. Raut, "Analysis of secured Video Steganography using Computer Forensics Technique for Enhance Data Security," IEEE International Conference on Image Information Processing (ICIIP), pp. 660-665, 2013.

[10] Bhattacharyya S., Banerjee I., Sanyal G. ,"A Survey of Steganography and Steganalysis Technique in Image, Text, Audio and Video as Cover Carrier," Journal of Global Research in Computer Science (JGRCS), April 2011.

[11] Bhautmage P., Jeya Kumar, Dahatonde, "Advanced Video Steganography Algorithm," International Journal of Engineering Research and Applications (IJERA), vol. 9, no. 5, pp. 85-90, February 2013.

[12] R. Poornima , "An Overview of digital Video Steganography," International Journal of Computer Science and Engineering Survey (IJCSES), vol.4, pp.80-84, February 2013.

[13] Liu B., Liu F. and Wang, "Inter-Frame Correlation Based Compressed Video Steganalysis", IEEE Conference Publications on Image and Signal Processing (CPISP), vol. 3, pp. 42-46, May 2008.

[14] Ansari N., Zhicheng Ni, Yun-Qing Shi, "Reversible data hiding", Circuits and Systems for Video Technology, IEEE International Transactions on Image Processing (ITIP), vol. 16, no. 3, pp. 354-362, March 2006.

[15] Ali Kanso, Own, Hala S., "Steganographic algorithm based on a chaotic map", Communications in Nonlinear Science and Numerical Simulation (CNSNS), vol. 17, no. 8, pp. 3287-3302, Dec 2011.

[16] Yadav, Pooja Mishra, Nishchol Sharma, "A secure video Steganography with encryption based on LSB technique", IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), pp. 1-5, Dec. 2013. DOI: 10.1109/ICCIC.2013.6724212.

[17] Ki-Hyun, Kee-Young, "Steganographic method based on interpolation and LSB substitution of digital images", Multimedia Tools Appl: Springer Science+ Business Media New York, January 2014. Print ISSN 1380-7501.

[18] El- Sayed, M. El Alfy, "Detecting pixel-value differencing steganography using Levenberg-Marquardt neural network", IEEE International Conference on Computational Intelligence and Data Mining (CIDM), pp. 160-165, April 2013. DOI: 10.1109/CIDM.2013.6597231.

[19] Akshay Phadke and Aditi Mayekar, "New Steganography Technique using Neural Network", International Journal of Computer Applications (IJCA), vol. 82, no. 7, pp. 39-42, Nov 2013.

[20] Pritish Bhautmage, JeyaKumar, Ashish Dahatonde, "Advanced Video Steganography Algorithm," International Journal of Engineering Research and Applications (IJERA), vol. 3, no. 1, pp. 1641-1644, February 2014.