A Survey on Video Steganography Using Genetic Algorithm and Artificial Neural Network

Nikita Pathak[1], Disa Ray[2], Saroni Sinha[3], Prof. Uttam Kumar Dash[4], Dr. Anindya Jyoti Pal[5]

Information Technology, Heritage Institute of Technology, Kolkata

***Abstract*-- Nowadays, Steganography has becoming a popular means of sending secret message over the internet without letting anyone know the existence of the secret message. Only the sender and receiver know about the contents of the message and also about its existence. Video Steganography is a form of Steganography where the secret message is hidden in a video file which is then sent over the internet to its intended recipient. The recipient also receives the means with which the secret message can be recovered. Thus, Steganography increases security to a high extent. It was mostly used by the army to communicate secret data over the internet. However, nowadays the use of Steganography has increased. Video Steganography can be implemented through several algorithms. Some of these algorithms include Genetic Algorithm and Artificial Neural Network. This paper includes a survey on how Video Steganography has been implemented by several researches using the above two algorithms. It focuses on the pros and cons of each of these algorithms.**

***Keywords*-- Video Steganography, Genetic Algorithm, Artificial Neural Network, Frames, Secret Data**

I. INTRODUCTION

Video Steganography is the process of hiding some secret data whether it be some text, image, audio or video within a video file.

A. Genetic Algorithm

In Genetic Algorithm, the population is first created where individuals are assigned weights based on a fitness function. After this Mutation and crossover performed on individuals of the population with best weights. Mutation and crossover can be performed in any order. In mutation a few characteristics of the individual are mutated. There are various types of crossovers which include single point, multi point, uniform crossover, etc. Different crossovers use different number of points for performing the crossover operation. After performing mutation and crossover multiple number of times, we get the best fitted population through this algorithm. The steps of Genetic Algorithm as given in [7] are:

Step 1: [Start] Generate random population of n chromosomes (suitable solutions for the problem)
Step 2: [Fitness] Evaluate the fitness f(x) of each chromosome x in the population
Step 3: [New population] Create a new population by repeating following steps 4 to 7 until the new population is complete
Step 4: [Selection] Select two parent chromosomes from a population according to their fitness (the better fitness, the bigger chance to be selected)
Step 5: [Crossover] With a crossover probability cross over the parents to form a new offspring (children). If no crossover was performed, offspring is an exact copy of parents.
Step 6: [Mutation] With a mutation probability mutate new offspring at each locus (position in chromosome).
Steps 7: [Accepting] Place new offspring in a new population.
Steps 8: [Replace] Use new generated population for a further run of algorithm.
Step 9: [Test] If the end condition is satisfied, **stop**, and return the best solution in current population.
Step 10: [Loop] Go to step 2

B. Artificial Neural Network

ANNs act like the neural networks of the brain. These ANNs consist of nodes. These nodes are interlinked to each other. They can communicate with each other via the links. Each of these links consist of a weight which determines the quality of the output signal. ANNs learn with the previous input. They keep improving their quality depending upon the previous inputs. The steps of implementing ANNs as given in [8] include:

Step 1: Collecting data.
Step 2: Creating the network.
Step 3: Configuring the network.
Step 4: Initializing the weights and nodes.
Step 5: Training the network.
Step 6: Validating the network
Step 7: Using the network

II. VIDEO STEGANOGRAPHY SYSTEM

A video steganographic system consists of several parts. The first part is the splitter where the video is split into frames and audio. The frame in which the data is to be hidden is selected. After this, the selected frame is sent to the embeder. Here, the secret data gets embedded in the frame and thus we get the stego frame. Next we need to optimize the stego video so as to reduce its perceptibility. Hence, the video is passed though an optimizer. After optimizing the stego frame, it is combined with all other frames and the audio to produce the stego video.

This is done by the optimizer.

For extracting the secret data from the stego video, it is again passed through the splitter. The stego frame is then selected and sent to the decoder where the secret data is extracted. Thus, in this way the secret data can again be retrieved from the stego video.

III. RELATED WORK

Researchers in paper [1] used the last three bits of the red byte in the pixel, the last three bits of the blue byte in the pixel and the last two bits of the green byte in the pixel to store a byte of the hidden data. Individuals of the population are created. Each pixel of the video forms an individual of the population. The fitness function of the individual is:

E=(w1*f1)+(w2*f2)

The predefined values of w1 and w2 are 0.8 and 0.2 respectively. F1 is the Mean Square Error and f2 is the Human Vision Deviation. After initializing individuals in the population with the fitness function, the individuals are mutated and sent for crossover (single-point). In the mutation process, a bit of the pixels are changed from 0 to 1 or from 1 to 0. Since the crossover is a single point crossover, hence a single point is chosen randomly and the pixel values of two individuals are crossed over from that point. The PSNR Value of this algorithm lies between 20 dB and 40dB. This value is considered to be good. This algorithm only optimizes the stego video so as to reduce any differences between the original video and the stego video. The time complexity of the algorithm is O(n^2). This algorithm produces a stego video with good imperceptibility. As a result of this, there is negligible visible difference between the stego video and the original video.

The paper [2] gives an effective discussion on video steganography by using artificial neural network which is considered the main working tool for the field of artificial intelligence. A secret bit of data is being hidden in a cover image that results in the required stego image. LSB (Least Significant Bit) method is used for this embedding purpose as this method is relatively easy to use. Initially the video is segregated into a number of frames. The input pattern is made by combining the secret data and bits from a particular frame and then the patterns are trained. The training pattern helps to form the network by choosing the number of input neurons, hidden layer neurons and output neurons. Next these patterns are inserted in a trained network and finally the output is stored in LSB of a particular frame of the video file. All frames are finally merged to form the required stego video. Thus, for "n" number of input patterns and k+1 bits for each input pattern, the process occurs 2^k+1 times. The advantage of this algorithm is that, the imperceptibility of the produced stego video is high however, the neural network is shared between the sender and the receiver.

Paper [3] provides us some useful information on methods to implement video steganography by artificial neural network. This method involves Artificial Neural Network and Discrete Cosine Transform. Initially DCT is applied on the selected frame which is intended to be the cover image to generate quantization matrix for image compression. The pixels are placed into 8*8 pixel blocks and then the DCT algorithm is applied on this block. Neural networks help to merge data by determining the positions for merging. The quantized image and the data to be hidden are passed through the trained neural network which gives the required stego image as the output. Thus, the secret data is embedded in the stego video formed from the proposed algorithm. There is no damage to the target content and the proposed method is able to conceal and reveal the exact hidden data from video file without disturbing the running application or new application.

In paper [4] both Genetic Algorithm and Artificial Neural Network is used to implement Video Steganography. The embedding process is done via Neural Networks where the Network is divided into 3 layers. The first two layers are the input layers (input and hidden layer) and the last layer is the output layer. The stego video pixels are stored in nodes of the outer layer whereas the original video pixels and the secret data are stored in the nodes of the input layers. The input layer consists of the first input layer and the hidden layer. Nodes of the first input layer represent pixels of the original video frame and nodes of the hidden layer represent pixels of the secret image. The links in the neural network consists of weights. These weights determine the quality of the stego output video. The weights of these links are updated continuously depending upon previous inputs. This improves the quality of the stego video. After embedding, GA is used to optimize the video. Since here, the video gets optimized thus this algorithm produces a stego video which is highly imperceptible.

In paper [5] two algorithms are used to implement video steganography. The video is divided into frames and a single frame is selected to implement this method. The secret data is encrypted in the frame via XOR operation. After performing XOR, Bitwise Rotation is done. This provides protection for the secret data. Genetic algorithm is then implemented on the frame so as to increase the security of the hidden data. In GA, row and column-wise shuffling of the pixels of the frame is done. The frames are then merged with the video to produce the stego video. The secret key is also sent along with the video to the receiver. The receiver decrypts the message from the video using this secret key. Thus, this algorithm increases the security of the hidden data to a high extent.

In paper [6] the audio from the splitter module is used to implement this algorithm. The secret data is hidden in the audio file of the video. The secret data here can only be an image or a text message. The Population is created with the help of the fitness function. The fitness function used here is:

$Pro(x) = f(xi(t))/\Sigma(i=1 \text{ to size}) f(xi(t))$

Where f(x) is the fitness value of chromosome, i is the chromosome number and t is the population number. Then crossover and mutation is performed. After all these, hybrid genetic algorithm is implemented so as to get a population with best fitness value. Thus the secret data gets hidden in the audio of the video file. The stego audio and all frames of the video are merged to form the stego video. This algorithm provides high security. Moreover, it becomes difficult to distinguish the stego video from the original video.

IV. Conclusion

This survey paper includes various reaserch papers produced during the last 5 years on the topic, Video Steganography using Genetic Algorithm and Artificial Neural Network. Thus from these papers we conclude that each of these papers provides a proper method to implement Video Steganography using the proposed methods. However there still exists some limitations. In the papers using Genetic Algorithm to implement Video Steganography, the time complexity is a bit high and the imperceptibility can further be improved. The time complexity is high due to the various steps of initialization, mutation, crossover and repetition involved. The imperceptibility can be improved by using other types of crossovers like multi-point crossover or uniform crossover. The time complexity can be improved by combining both Genetic Algorithm and Neural Network while implementing Video Steganography. The hybrid algorithm also has some limitations like low quality stego video. In algorithms using only ANNs, the imperceptibility can further be improved by repeating the number of times the input is passed through the network. However, this would again increase its time complexity. Thus, we conclude that the hybrid algorithm is the best among these even though the stego video quality will be a bit low.

Acknowledgement

We take this opportunity to express our profound gratitude and deep regards to our mentor Prof. Uttam Kumar Dash for his exemplary guidance, monitoring and constant encouragement throughout the course of this thesis. The blessing, help and guidance given by him time to time shall carry us a long way in the journey of life on which we are about to embark.

We would also like to thank Dr. Anindya Jyoti Pal for providing necessary information regarding the survey & also for his support in completing the survey.

References

[1] Kousik Dasgupta, Jyotsna Kumar Mondal and Paramartha Dutta: Optimized Video Steganography Using Genetic Algorithm (GA) in Procedia Technology 10 (2013),pp. 131-137.
[2] Richa Khare and Rachana Mishra: Data Hiding by Using Neural Network in Video File in IJETAE Volume 4, Issue 7 (July 2014),pp. 913-917.
[3] Fozia R.Khan, Prof. Sujata Anandwani: Efficient and Improved Video Steganography using DCT and Neural Network in IJSRD Volume 3, Issue 10 (2015), pp. 432-434.
[4] Heena Goyal, Preeti Bansal: Video Steganography using Neural Network and Genetic Algorithm in IJETIE Volume 1, Issue 9 (2015), pp. 7-14.
[5] Rehana Begum R.D, Sharayu Pradeep: Best Approach for LSB Based Steganography Using Genetic Algorithm and Visual Cryptography for Secured Data Hiding and Transmission over Networks in IEEE Volume 4, Issue 6 (June 2014), pp. 114-119.
[6] Dr. Ban A. Mitras, Dr. Nada F. Hassan: Using Hybrid Genetic Algorithm in Audio Steganography in IJSS 25 (2013), pp. 150-164.
[7] http://www.obitko.com/tutorials/genetic-algorithms/ga-basic-description.php
[8] http://in.mathworks.com/help/nnet/gs/neural-network-design-steps.html