International Journal of Research in Advent Technology, Vol.2, No.2, February 2014

E-ISSN: 2321-9637

Video Steganography Using Neural Network Methods

Shalini Choubey[1], Dr.Ashish Bansal[2]
IT department S.V.I.T.S,Indore[1], M. E.IV student [2]
IT department S.V.I.T.S,Indore[2], Head of the Department [2]
Email: Shalini20choubey@gmail.com[1]

ABSTRACT
Security is nothing new; the way that security has become a part of our daily life is unprecedented. Attacks, misuse or unauthorized access of information is of great concern today which makes the protection of documents through digital media a priority problem. This urges the researcher's to devise new data hiding techniques through Steganography principle to protect and secure the data of vital significance. Video Steganography is the process of hiding some secret information inside a video. The addition of this information to the video is not recognizable by the human eye as the change of a pixel colour is negligible. The performance of this method can be further improved with the use Neural Networks Methods (like Artificial Neural Networks approach adoption (ANN) and Full Counter propagation Neural Networks (FCNN)). In this paper we will see some of the possible ways to incorporate neural network approach in covert communication (Steganography).

Keywords: Steganography, covert communication, ANN, FCNN.

1. INTRODUCTION

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity [8]. The word Steganography is of Greek origin and means "concealed writing" from the Greek words steganos meaning "covered or protected", and graphing meaning "to write".

Steganography is the process of secretly embedding information inside a data source without changing its perceptual quality. Steganography comes from the Greek word ***steganos*** which literally means "covered" and ***graphia*** which means "writing", i.e. covered writing. The most common use of steganography is to hide a file inside another file.

Generally, in data hiding, the actual information is not maintained in its original format. The format is converted into an alternative equivalent multimedia files like images, video or audio.

The figure1 shows a simple representation of the generic embedding and extraction process in steganography. In this example, a secret data is being embedded inside a cover image to produce the stego image. A key is often needed in the embedding process.The embedding procedure is done by the sender by using the proper stego key. The recipient can extract the stego cover image in order to view the secret data by using the same key used by the sender. The stego image should look almost identical to the cover image.

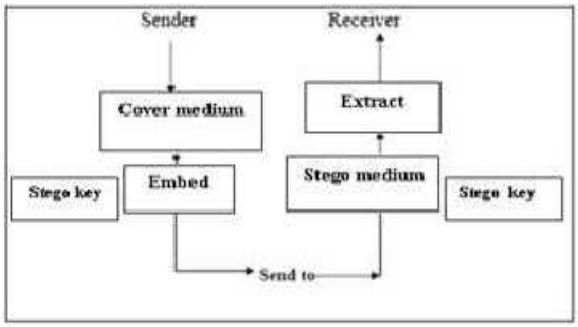

Figure 1: Steganography mechanism

The advantage of Steganography,over cryptography alone, is that messages do not attract attention to themselves. Plainly visible encrypted messages, no matter how unbreakable will arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal. Therefore, whereas cryptography protects the contents of a message, Steganography can be said to protect both messages and communicating parties. Techniques provide an interesting challenge for digital forensic investigations. The term neural network was traditionally used to refer to a network or circuit of biological neurons. The modern usage of the term often refers to artificial neural networks, which are composed of artificial neurons or nodes.

Artificial Neural Networks may either be used to gain an understanding of biological neural networks, or for solving artificial intelligence problems without necessarily creating a model of a real biological system. Artificial Neural Networks have been applied successfully to speech recognition, image analysis and adaptive control, in order to construct software agents or autonomous robots.

2. POSSIBLE ATTACKS ON STEGANOGRAPHY

Steganography techniques Steganalysis are "the process of detecting steganography is used to address digital rights management, protect by looking at variances between bit patterns and unusually information, and conceal secrets. Information hiding large file sizes".

(a) Compression methods
(b) Geometric transformations
(c) Image enhancement techniques

The following types of attacks are possible with Steganography:

(a) Steganography-only attack
(b) Known-carrier attack
(c) Known-message attack
(d) Chosen-steganography attack
(e) Chosen-message attack
(f) Known-steganography attack

3. NEURAL NETWORK IN STEGANOGRAPHY

A neural network represents a highly parallelized dynamic system with a directed graph topology that can receive the output information by means of a reaction of its state on the input actions. The ensembles of interconnected artificial neurons generally organized into layers or fields include neural networks. The behavior of such ensembles varies greatly with changes in architectures as well as neuron signal functions. Artificial neural networks are massively parallel adaptive networks of simple non-linear computing elements called *neurons* which are intended to abstract and model some of the functionality of the human nervous system in an attempt to partially capture some of its computational strengths [11].

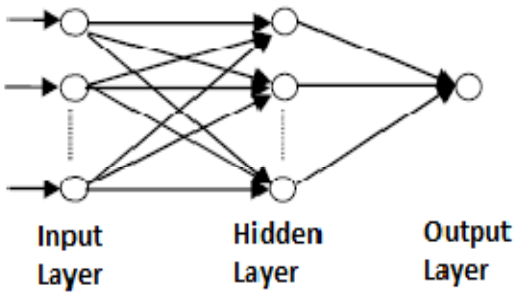

Figure 2: Basic Neural Network

In its most general form, a neural network can be viewed as comprising the following eight components:

(a) Neurons

Neurons can be of three types: input, hidden and output. Input neurons receive the external stimuli presented to the network. Hidden neurons compute intermediate functions and their states are not accessible to the external environment. Outputs from the network are generated as signals of output neurons.

(b) Activation state vector

This is a vector that indicates the activation level of individual neurons in the neural network.

(c) Signal function

A function that generates the output signal of the neuron
based on its activation is called a signal function. Functions may differ from neuron to neuron within the network; although most networks are field-homogeneous i.e. all neurons within a field or layer have the same signal function.

(d) Pattern of connectivity

This determines the inter-neuron connection architecture or the graph of the network.

(e) Activity aggregation rule

This aggregated the activity at a particular neuron.

(f) Activation rule

This function determines the new activation level of a neuron based on its current activation and its external inputs.

(g) Learning rule

The learning rule provides a means of modifying correction strengths based on both the external stimuli and the network performance with the aim of improving the network performance.

There is (or should be!) interest from the counterterrorism and law-enforcement communities in measures that can be used to detect the existence of hidden data. This is steganalysis [3]. A single feature may provide only scant indication of the presence of Steganography, or, several features may on their face conflict in their diagnosis. What is needed is a method of combining multiple features into a single conclusion of "stego" or "innocent". For this we utilize a pattern recognition system called an artificial neural network (ANN). Developing an ANN is a two-stage process. First the network is trained by feeding it the features from a large pool of images, some of which are known to contain stego, and some that are known to not contain stego. Based on the training, the neural net determines computational rules that can then be applied to the features of an image of unknown character.

One particular merit of an artificial neural network is that it is adaptive—as additional data is

provided to the system it refines its prediction function. In this way the pattern recognizer can respond to evolution in the data. For example, if small modifications are made to an existing steganographic algorithm, the software will be able to adapt. Liu Shaohui et al adopted neural network approach for finding the features which has significant effect on data hiding process [5].

Neural network has the super capability to approximation any nonlinear functions. We first extract features of image embedded information, then input them into neural network to get output. C. Manikopoulos et al. [1] discussed an algorithm that utilises the probability density function (PDF) to generate discriminator features fed into a neural network system which detects hidden data in this domain. A group of scientists at Iowa State University are focusing on the development of an innovative application which they call ‘‘Artificial Neural Network Technology for Steganography (ANNTS)’’ aimed at detecting all present Steganography techniques including DCT, DWT and DFT.

Adoption of Neural Network Approach in Maher EI Arbi et al. suggested video watermarking based on wavelet addition, embedding and extraction of the watermark were based on the relationship between a wavelet coefficient and its neighbor's. A neural network was given to memorize the relationships between coefficients in a 3x3 block of the image. Experimental results showed that embedding watermark where picture content is moving is less perceptible. Further, it showed that the scheme was robust against common video processing attacks.

Guohua Wu el al. [4], suggested Counter propagation Neural Network (CNN) based method for fast audio digital watermark. By making use of the capabilities of memorization and fault tolerance in CPN, watermark is memorized in the nerve cells of CPN. In addition, they adopt a kind of architecture with an adaptive number of parallel CPN to treat with each audio frame and the corresponding watermark bit. Comparing with other traditional methods by using CPN, it was largely improve the efficiency for watermark embedding and correctness for extracting, namely the speed of whole algorithm. The extensive experimental results showed that, we can detect the watermark exactly under most of attacks. This method efficaciously trade off both the robustness and inaudibility of the audio digital watermark.

4. PROBLEM DOMAIN

Video hiding uses the digital objects such as Text, message or any other computer file for hiding the data within video file. A most popular and oldest technique for hiding data in Video filed is the Least Significant Bit Method Technique.

One of the major disadvantages associated with LSB techniques is that the hidden message within video file can be destroyed by the intruder by changing the LSB Method. In this way, hidden message can be destroyed but the change in video image quality is in the range of +1 to -1 at each pixel position which is negligible to human eye. Second disadvantage is that least significant bit may be corrupted by hardware imperfections or quantization noise due to which message can be distorted.

Some Major problems are as followed:-

1. Mostly technique does not support encryption technique for extract the information within video file.
2. Least Significant Bit Method Technique or other technique takes more time consumed for embedded information within video file.
3. Traditional Algorithm like LZW, LSB cannot embedded large amount of data within video.
4. It is difficult to quickly establish a signature for the latest Data Hiding tools technique.

5. PROPOSED SOLUTION

Data hiding is a method of hiding secret messages into a video such that an unintended observer will not be aware of the existence of the hidden messages. We propose a new information hiding technique in video data without embedding any information into the target content by using neural network trained on frequency domain.

Proposed method can detect a hidden bit codes from the content by processing the selected feature sub blocks into the trained neural network. Hidden codes are retrieved from the neural network only with the proper extraction key provided. The extraction key, in proposed method, are the coordinates of the selected feature sub blocks and the network weights generated by supervised learning of neural network. The supervised learning uses the coefficients of the selected feature sub blocks as set of input values and the hidden bit patterns are used as teacher signal values of neural network. With our proposed method, we are able to introduce a information hiding scheme with no damage to the target content.

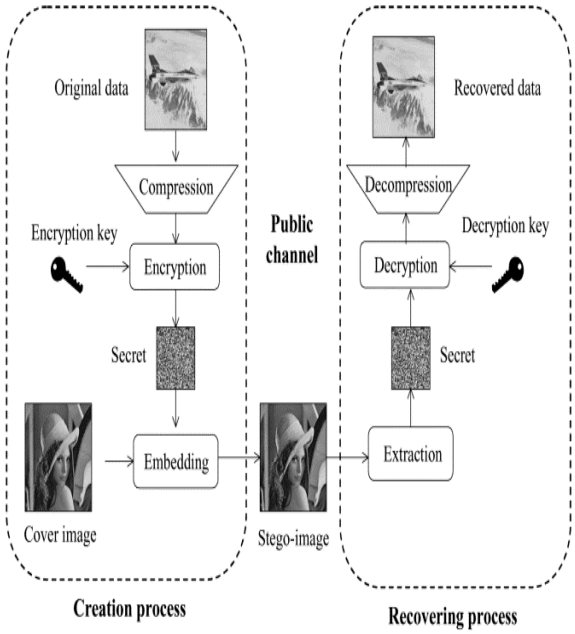

Figure 3

6. CONCLUSION

In this paper, we have seen several methods which Adopt Neural Network method for Steganography and Full Counter propagation Neural Network for watermarking. We improve performance of Steganography method with the use Neural Networks Methods.

References

[1] C. Manikopoulos, S. Yun-Qing, S. Sui, Z. Zheng, N. Zhicheng, Z. Dekun, "Detection of Block DCT-based Steganography in Gray-scale Images", Proceedings of the IEEE Workshop on Multimedia Signal Processing, 9–11 December 2002, pp. 355–358.

[2] Chuan-Yu Chang et al, "Using a Full Counterpropagation Neural Network for Image Watermarking", International Computer Symposium, Dec. 15-17, 2004, Taipei, Taiwan.

[3] Clifford Bergman, Jennifer Davidson, "An Artificial Neural Network for Wavelet Steganalysis", Final Report to Midwest Forensics Resource Center.

[4] Guohua Wu, Xiaodong Zhou, "A Fast Audio Digital Watermark Method Based on Counter-propagation Neural Networks", International Conference on Computer Science and Software Engineering, 2008, pp. 583-586

[5] Liu Shaohui et al, "Neural Network Based Steganalysis in Still Images", ICME 2003, pp. 509-512.

[6] Maher El' Arbi et al, "Video Watermarking Based On Neural Networks", ICME 2006, pp. 1577-1580.

[7] M. Natarajan, Gayas Makhdumi., "Safeguarding the Digital Contents: Digital Watermarking", DESIDOC Journal of Library & Information Technology, 29, No. 3, May 2009, pp. 29-35.

[8] Sanjeev kumar , Balasubramanian Raman And Manoj Thakur, "Real Coded Genetic algorithm Based Stereo Image Watermarking", International Journal of Secure Digital Information Age, 1, No.1, June 2009

[9] www.en.wikipedia.org

[10] Yu et al, "Digital Watermarking Based on Neural Networks for Color Images", Elsevier Signal Processing, 81 (2001),

[11] "A Study on Digital Image and Video Watermarking Schemes using Neural Networks" *International Journal of Computer Applications (0975 – 8887 Volume 12– No.9, January 2011*