International Journal of Information Technology and Knowledge Management
July-December 2011, Volume 4, No. 2, pp. 527-529

ADOPTION OF NEURAL NETWORK APPROACH IN STEGANOGRAPHY AND DIGITAL WATERMARKING FOR COVERT COMMUNICATION AND COPYRIGHT PROTECTION

Divyakant T. Meva[1] & Amit D. Kothari[2]

Now a day, covert communication is one of the most important aspects of internet. When you want to hide the data from intruders, you can use different methods for covert communication. One of the most useful methods is steganography. Other thing in the era of internet is the copyright protection, which can be implemented effectively by digital watermarking. The performance of these methods can be further improved with the use neural network approach adoption. In this paper we will see some of the possible ways to incorporate neural network approach in covert communication.

Keywords: Steganalysis, ANN, CNN, FCNN, Digital Watermarking, Steganography.

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 [9]. The word steganography is of Greek origin and means "concealed writing" from the Greek words steganos meaning "covered or protected", and graphein meaning "to write".

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.

Digital watermarking is the process of embedding information into a digital signal in a way that is difficult to remove [9]. The signal may be audio, pictures or video, for example. If the signal is copied, then the information is also carried in the copy. A signal may carry several different watermarks at the same time. In visible watermarking, the information is visible in the picture or video. In invisible watermarking, information is added as digital data to audio, picture or video, but it cannot be perceived as such.

Digital watermarking and steganography techniques are used to address digital rights management, protect information, and conceal secrets. Information hiding 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 and Digital Watermarking

An attack on a watermark can be defined as an operation, (coincidental or hostile) that may degrade a watermark and possibly make it unreliably detectable. Some of the practical attacks include the following [7].

(a) Compression methods

(b) Geometric transformations

(c) Image enhancement techniques

Steganalysis is "the process of detecting steganography by looking at variances between bit patterns and unusually large file sizes".

Attacks and analysis on hidden information may take several forms: detecting, extracting, and disabling or destroying hidden information. An attack approach is dependent on what information is available to the steganalyst.

[1]Marwadi Education Foundation's Group of Institutions, Rajkot, INDIA
[2]Marwadi Education Foundation's Group of Institutions, Rajkot, INDIA
E-mail: [1]divyakantmeva16@yahoo.co.in, [2]amitdkothari@gmail.com

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 (STEGANALYSIS)

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.

4. NEURAL NETWORK IN DIGITAL WATERMARKING

In the digital watermarking algorithms, a watermark is embedded into the original data in such a way that it remains present as long as the perceptible quality of the content is at an acceptable level. This is the first step in the process. The owner of the original data proves his/her ownership by extracting the watermark from the watermarked content in case of multiple ownership claims. This is the second step in the process.

In most watermarking applications, the watermarked image is likely to be processed in some unsecured channel before it reaches the watermark receiver. During this processing, the watermarked image can be affected by various attacks. There are mainly two popular categories of watermark attacks: removal attacks and geometrical attacks. Removal attacks contain de-noising, compression and collusion attacks, while translation, rotation, pixel-shifting come under the second category. Robustness can be achieved if significant modifications are made to the host image either in spatial or transform domain. However, such modifications are distinguishable and thus do not satisfy the requirement of transparency (invisibility). The design of an optimal watermarking for a given application always involves a trade-off between these requirements. Therefore, image watermarking can be considered as an optimization problem [8]. This optimal problem has been solved by several techniques like genetic algorithm, neural networks and support vector machine in spatial as well as transform domain.

Yu et al. [10] introduced a process introduce the training process for a neural network memorizing the characteristics of the relations between watermark and original image. The signature S is retrieved by using the adaptive capability of the trained neural network. This step is performed in the watermark extraction phase. The original signature is compared with this signature and identifies the copyright of owner's intellectual property.

Full counterpropagation neural network (FCNN) was used by Chuan-Yu Chang et al for image watermarking [2]. Neural networks have been suggested as alternative approaches owning to high fault tolerance and potential for adaptive training. The full counterpropatation neural network is a supervised-learning network with capacity of bidirectional mapping. This watermarking method integrated the embedding and extraction procedure into a full counterpropagation based neural network. The FCNN could resist various attacks. In addition, the watermark embedding procedure and extracting procedure is integrated into the FCNN. By doing so, this approach simplifies traditional procedures. The experimental results show that the application achieved robustness, imperceptibility and authenticity in digital watermarking.

Maher EI Arbi et al. suggested video watermarking based on neural network [6]. They propose a novel digital video watermarking scheme based on multi resolution motion estimation and artificial neural network. A multi resolution motion estimation algorithm was adopted to preferentially allocate the watermark to coefficients containing motion. In 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.

5. CONCLUSION

In this paper, we have seen several methods which adopt neural network approach for steganalysis. Actually with steganalysis, we can find the loop holes in our algorithm and we can improve them. In digital watermarking, we can make our algorithm more robust and fast with the help of the neural approach. Imperceptibility and authenticity can be achieved with neural network support in digital watermarking.

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), p.p. 663-671.