International Journal of Intelligent Computing and Technology
IJICT
ISSN: 2457-0249 (Online)
Website: https://ijict.com 2018 (June)–Vol.2, Iss.1 Page: 17–24

Review on Secure Communication System Using Neural Network Approach in Steganography

Dr R Umadevi[1] & A Gayathri[2]

[1,2]Assistant Professor, PG and Research Department of Computer Science and Applications, Vivekanandha College of Arts and Science for Women, Tiruchengodu, Tamilnadu, India

Article History: Received: May 2018; Published: June 2018

ABSTRACT

Now a days, covert communication is one of the most important aspects of internet. When you want to hide the data from prowler, you can use dissimilar methods for covert communication. One of the most useful methods is steganography. Other thing in the era of internet is the copyright guard, which can be implemented effectively by digital watermarking. The concert 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 fit in neural network approach in covert communication.

KEYWORDS: Steganalysis, ANN, CNN, FCNN, Digital Watermarking, Steganography

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 gloom. 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. Clearly 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. 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 procedure 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.

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.

(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. 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\

A DETAILED LOOK AT STEGANOGRAPHY

In this section we will discuss Steganography at length. We will start by looking at the different types of Steganography generally used in practice today along with some of the other principles that are used in Steganography. We will then look at some of the Steganographic techniques in use today. We will then close by going over Steganalysis. Steganalysis concentrates on the art and science of finding and or destroying secret messages that have been produced using any of the various steganographic techniques we will cover in this paper.

To start, let’s look at what a theoretically perfect secret communication (Steganography) would consist of. To illustrate this concept, we will use three fictitious characters named Amy, Bret and Crystal. Amy wants to send a secret message (M) to Bret using a random (R) harmless message to create a cover (C) which can be sent to Bret without raising suspicion. Amy then changes the cover message (C) to a stego-object (S) by embedding the secret message (M) into the cover message (C) by using a stego-key (K). Amy should then be able to send the stegoobject (S) to Bret without being detected by Crystal. Bret will then be able to read the secret message (M) because he knows the stego-key (K) used to embed it into the cover message (C). " In practice, however, this is not always the case. In order to embed secret data into a cover message, the cover must contain a sufficient amount of redundant data or noise. This is because the embedding process Steganography uses actually replaces this redundant data with the secret message. This limits the types of data that we can use with Steganography. In practice, there are basically three types of steganographic protocols used. They are Pure Steganography, Secret Key Steganography and Public Key Steganography.

Pure Steganography is defined as a steganographic system that does not require the exchange of a cipher such as a stego-key. This method of Steganography is the least secure means by which to communicate secretly because the sender and receiver can rely only upon the presumption that no other parties are aware of this secret message. Using open systems such as the Internet, we know this is not the case at all. Secret Key Steganography is defined as a steganographic system that requires the exchange of a secret key (stego-key) prior to communication. Secret Key Steganography takes a cover message and embeds the secret message inside of it by using a secret key (stego-key). Only the parties who know the secret key can reverse the process and read the secret message. Unlike Pure Steganography where a perceived invisible communication channel is present, Secret Key Steganography exchanges a stego-key, which makes it more susceptible to interception. The benefit to Secret Key Steganography is even if it is intercepted; only parties who know the secret key can extract the secret message.

Public Key Steganography takes the concepts from Public Key Cryptography as explained below. Public Key Steganography is defined as a steganographic system that uses a public key and a private key to secure the communication between the parties wanting to communicate secretly. The sender will use the public key during the encoding process and only the private key, which has a direct mathematical relationship with the public key, can decipher the secret message. Public Key Steganography provides a more robust way of implementing a steganographic system because it can utilize a much more robust and researched technology in Public Key Cryptography. It also has multiple levels of security in that unwanted parties must first suspect the use of steganography and then they would have to find a way to crack the algorithm used by the public key system before they could intercept the secret message.

ENCODING SECRET MESSAGES IN TEXT

Encoding secret messages in text can be a very challenging task. This is because text files have a very small amount of redundant data to replace with a secret message. Another drawback is the ease of which text-based Steganography can be altered by an unwanted parties by just changing the text itself or reformatting the text to some other form (from .TXT to .PDF, etc.). There are numerous methods by which to accomplish text-based Steganography. Line-shift encoding involves actually shifting each line of text vertically up or down by as little as 3 centimetres. Depending on whether the line was up or down from the stationary line would equate to a value that would or could be encoded into a secret message. Word-shift encoding works in much the same way the at line-shift encoding works, only we use the horizontal spaces between words to equate a value for the hidden message. This method of encoding is less visible than line-shift encoding but requires that the text format support variable spacing. Feature specific encoding involves encoding secret messages into formatted text by changing certain text attributes such as vertical/horizontal length of letters such as b, d, T, etc. This is by far the hardest text encoding method to intercept as each type of formatted text has a large amount of features that can be used for encoding the secret message. All three of these text based encoding methods require either the original file or the knowledge of the original files formatting to be able to decode the secret message.

NEURAL NETWORK IN STEGANOGRAPHY (STEGANALYSIS)

There is 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.

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.

A discussed an algorithm that utilizes 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.

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. 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.

A process introduces 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 counter propagation neural network (FCNN) was used by Chuan-Yu Chang et al for image watermarking. Neural networks have been suggested as alternative approaches owning to high fault tolerance and potential for adaptive training.

The full counter propagation neural network is a supervised-learning network with capacity of bidirectional mapping. This watermarking method integrated the embedding and extraction procedure into a full counter propagation 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.

ADOPTION OF NEURAL NETWORK APPROACH IN STEGANOGRAPY AND DIGITAL WATERMARKING

Maher EI Arbi et al. suggested video watermarking based on neural network. 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.

Guohua Wu el al., 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.

CONCLUSION

In this paper, several methods which adopt neural network approach for steganalysis. Actually with steganalysis, find the loop holes in our algorithm and improve them. In digital watermarking, 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. Further work to be made on some other secure communication media.

REFERENCES

1. M. Natarajan and Gayas Makhdumi (2009), Safeguarding the Digital Contents: Digital Watermarking, DESIDOC Journal of Library & Information Technology, 29(3), 29-35.
2. Sanjeev kumar, Balasubramanian Raman and Manoj Thakur (2009), Real Coded Genetic Algorithm Based Stereo Image Watermarking, International Journal of Secure Digital Information Age, 1(1).
3. Yu (2001), Digital Watermarking Based on Neural Networks for Color Images, Elsevier Signal Processing, 81, 663-671.
4. Liu Shaohui (2003), Neural Network Based Steganalysis in Still Images, ICME 2003, 509-512.

How to cite this article:

Dr R Umadevi & A Gayathri, "Review on Secure Communication System Using Neural Network Approach in Steganography", IJICT, Vol.2, Iss.1, 17-24, 2018