An Overview: Enhanced Steganography Using Rule Base Neural Network

Seema Rani[1], Nitika Kapoor[2], Harish Kundra[3]
[1]Research Scholar, [2,3]Assistant Professor
[1,2]Department of Computer Science, Rayat Institute of Engineering and Information Technology, Railmajra, SBS Nagar, (Punjab) INDIA
[1]Seemaghai23@gmail.com, [2]Er.nitikakapoor@gmail.com, [3]hodcseit@rayatbahra.com

Abstract:- Hiding messages in image data, called steganography, is used for both legal and illicit purposes. The detection of hidden messages in image data stored on websites and computers, called steganalysis, is of prime importance to cyber forensics personnel. This paper describes research On Steganography and artificial neural network (ANN) system. ANN is combined with Rule based System to provide high-performance and immune against conventional attack and performs good perceptibility compared to other steganographic approaches. Neural Networks can be used for steganalysis.

I. INTRODUCTION

The approach for high level secured communication is cryptography, which deals with encryption and decryption. The main difference between cryptography and steganography is the suspicion factor. When we implemented both the cryptography and steganography together, one can achieve a high level security. Steganography refers to the science of invisible communication. The goal of steganography is to secure communication from an eavesdropper; Steganographic techniques strive to hide the very existence of the message itself from an observer. The simplest image Steganographic techniques essentially embed the message in a subset of the LSB (Least Significant Bit). Cryptography and steganography are well known widely used techniques that manipulate message in order to cipher or hide their existence [1]. They are used to protect military images, E-mails, Credit card information, corporate data, personal files and etc. Cryptography encrypts the actual message that is being sent. This uses mathematical schemas and algorithm to scramble data into unreadable text.

1.1Steganography Mechanism

Steganography is the technique of hiding the message in a chosen carrier such that no one except the intended recipient is aware of its existence. Block diagram of steganography mechanism is shown in Figure 1.

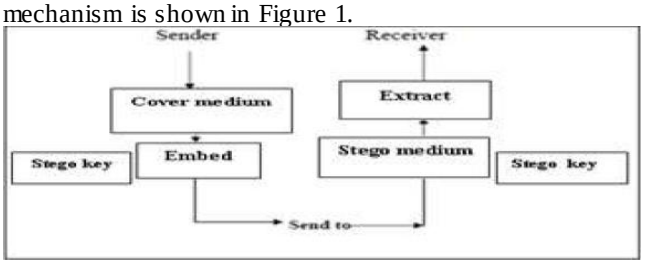


Figure1.1 Block Diagram of Steganography Mechanism.

Here 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 proper stego key is used by the sender for the embedding procedure. The same key is used by the recipient to extract the stego cover image in order to view the secret data. The stego image should look almost identical to the cover image.

1.2 Steganography Terms

Cover File: It is a file in which hidden information will be stored.
Carrier File: A file which has hidden information inside of it.
Steganalysis: The process of detecting hidden information inside of a file.
Stego-Medium: The medium in which the information is hidden.
Redundant Bits: Pieces of information inside a file which can be overwritten or altered without damaging the file.
Payload: The information which is to be concealed.

1.3 Types of Steganography

In modern approach, depending on the nature of cover object, steganography can be divided into five types:

1.3.1 Text Steganography:

Text steganography can be achieved by altering the text formatting, or by altering certain characteristics of textual elements (e.g., characters). It includes line-shift coding, word-shift coding and feature coding.

1.3.2 Image Steganography

Images are the most popular cover objects used for steganography. In the domain of digital images many different file formats exist and for these file formats different algorithms exist. These different algorithms used are least significant bit insertion, Masking and filtering, Redundant Pattern Encoding, Encrypt and Scatter, Algorithms and transformations.

1.3.3 Audio Steganography:

In audio steganography, secret message is embedded into digitized audio signal which result slight altering of binary sequence of the corresponding audio file. There are several methods like LSB coding, Phase coding, spread spectrum, Echo hiding which are used for audio steganography.

1.3.4 Video Steganography:
Video files are generally a collection of images and sounds, so most of the presented techniques on images and audio can be applied to video files too. The great advantages of video are the large amount of data that can be hidden inside and the fact that it is a moving stream of images and sounds.

1.3.5 Protocol Steganography:
The term protocol steganography refers to the technique of embedding information within messages and network control protocols used in network transmission. There are covert channels in the layers of the OSI network model where steganography can be used.

1.4 Uses of Steganography
The three most popular and researched uses for steganography in an open systems environment are covert channels, embedded data and digital watermarking. Covert channels can be very useful for any secure communications needs over open systems such as the Internet. By embedding the hidden data into the cover message and sending it, you can gain a sense of security by the fact that no one knows you have sent more than a harmless message other than the intended recipients Digital watermarking is very important in the detection and prosecution of software pirates/digital thieves. Steganography is used by some modern printers, including HP and Xerox brand color laser printers.

II. HISTORY OF STEGANOGRAPHY

What interests us more is the steganography having relationship with data processing but it will be interesting to retrogress to know the origins of this concept which becomes attracted by the researchers' interests [2]. Steganography is not a new technology. Steganographic techniques have been used for centuries. The first known application dates back to the ancient Greek times, when messengers tattooed messages on their shaved heads and then let their hair grow so the message remained unseen. A different method from that time used wax tables as a cover source. Text was written on the underlying wood and the message was covered with a new wax layer. The tablets appeared to be blank so they passed inspection without question. In the 20th century, invisible inks where a widely used technique. In the Second World War, people used milk, vinegar, fruit juices to write secret messages. Steganography has taken a giant leap forward which started in the 1990's when governments, industries, private citizens, and even terrorist organizations began using software applications to embed messages and photos into various types of media (digital photos, digital videos, audio files, and text files). Today steganography has come into its own on the Internet. Used for transmitting data as well as for hiding trademarks in images and music (called digital watermarking), electronic steganography may ironically be one of the last bastions of information privacy in our world today. Steganographic techniques have been used with success for centuries already. However, since secret information usually has a value to the ones who are not allowed to know it, there will be people or organizations who will try to decode encrypted information many different motives exist to detect the use of steganography, so techniques to do so continue to be developed while the hiding algorithms become more advanced.

2.2.1 Implementing steganography
Secrets can be hidden inside all sorts of cover information: text, images, audio, video and more. However, there are tools available to store secrets inside almost any type of cover source. It is also possible to hide information inside texts, sounds and video films for example. The most important property of a cover source is the amount of data that can be stored inside it, without changing the noticeable properties of the cover. Most steganographic utilities nowadays, hide information inside images; but why hiding information inside images is a most popular technique nowadays? Images are the most popular carrier file for steganography because of The abundance of images available on the Internet i.e. Image with a secret message inside can easily be spread over the World Wide Web or in newsgroups Another reason is the fact that the way images are stored creates a great amount of redundant space which is the ideal place to hide information. Also it is clear that although data hidden within an image is often imperceptible to the human eye.

2.2.2Performance Measures
As a performance measure for image distortion due to embedding, the well-known peak-signal-to- noise ratio (PSNR), which is categorized under difference distortion metrics, can be applied to stego images . It is defined as:
1) PSNR- Peak signal-to-noise ratio, often abbreviated PSNR, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation.
2) MSE- In statistics, the mean squared error of an estimator is one of many ways to quantify the difference between values implied by an estimator and the true values of the quantity being estimated.

III. STEGANALYSIS

The process of detecting hidden information inside of a file. Steganalysis is the process of identifying steganography by inspecting various parameter of a stego media. The primary step of this process is to identify a suspected stego media. As the properties of electronic media are being changed after hiding any object into that. This can result in the form of degradation in terms of quality or unusual characteristics of the media: Steganalysis techniques based on unusual pattern in the media or Visual detection of the same. To determine the text encrypted via steganography, plotting a histogram on both the stego media and a simple file written in same format is performed. A simple tool "SBHistogram" will perform this analysis. It generates histograms from simple ASCII data files. It creates both a text output and a graphical chart that can be printed [3]. Simple tool intended for easy use, fully functional with no limitations. In the non-encrypted text file, the frequency of character occurrence is less than the encrypted file. If you have an idea that data might

be hidden in the host file, you can run a histogram on this data and, depending on the results, have a good idea whether encrypted data is hidden in the file.

3.1 The need for steganalysis:

Unfortunately with the good also comes bad. Because steganography is a technology that enables users to hide message from unintended recipients, it can also be used by criminals to hide message from authorities. For this reason the presence of the methods detecting steganography becomes necessary. This method is called Steganalysis. Steganalysis is a relatively new branch of research .Contrast to the goal of information hiding, Steganalysis is the art of discovering and rendering useless such covert messages, hence making information hiding failed; While steganography deals with techniques for hiding information the goal of steganalysis is to detect and/or estimate potentially hidden information from observed data with little or no knowledge about the steganography algorithm and/or its parameters. It is fair to say that steganalysis is both an art and a science. The art of steganalysis plays a major role in the selection of features or characteristics a typical stego-message might exhibit while the science helps in reliably testing the selected features for the presence of hidden information. In general, extraction of the secret message could be a harder problem than mere detection. We classify steganalysis into two categories:

Passive steganalysis: Detect the presence or absence of a secret message in an observed message or identify the type of embedding algorithm. in other words the steganalysis process ends when there is an answer to the question, "Does this media harbor steganographic data?" *f*

Active steganalysis: Estimate/extract some properties of the message or the embedding algorithm. So the process is complete only after the hidden data is removed, destroyed, or strategically altered to render it useless.

IV. ARTIFICIAL NEURAL NETWORKS(ANN) FOR STEGANALYSIS

In the last few years the Neural Networks could prove their effectiveness in many applications, Artificial Neural Networks (ANNs) are recognized as powerful data analysis and modeling tools[4]. They have been shown to capture and accurately represent both linear and non- linear relationships, and are an invaluable tool for approximating functions, clustering data, and recognizing patterns that are otherwise imperceptible; Neural Networks can often be used for steganalysis.

Advantages include:

1. Adaptive learning: An ability to learn how to do tasks based on the data given for training or initial experience.
2. Self-Organization: An ANN can create its own organisation or representation of the information it receives during learning time.
3. Real Time Operation: ANN computations may be carried out in parallel, and special hardware devices are being designed and manufactured which take advantage of this capability.
4. Fault Tolerance via Redundant Information Coding: Partial destruction of a network leads to the corresponding degradation of performance. However, some network capabilities may be retained even with major network damage.

V. APPROACH USED

5.1 RULE BASE NEURAL NETWORK

The structures of FNN emerge at a junction of fuzzy sets and neural network [5]. In this section, we discuss the type of "if-then" rules along with their development mechanisms, that is, the linear fuzzy interface-based FNN as rule base type. By means of the division of fuzzy input space, the model uses the RNN whose faster whose faster learning speed and better convergence characteristics than other FNN models is shown in Fig2.

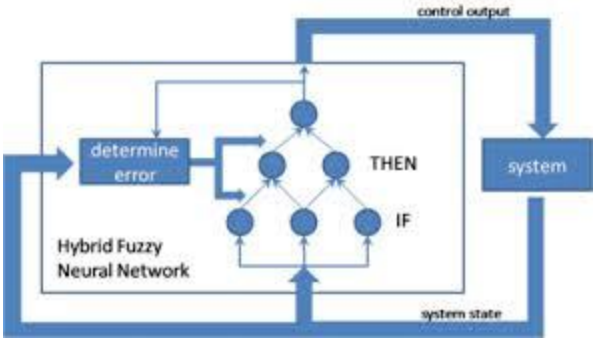
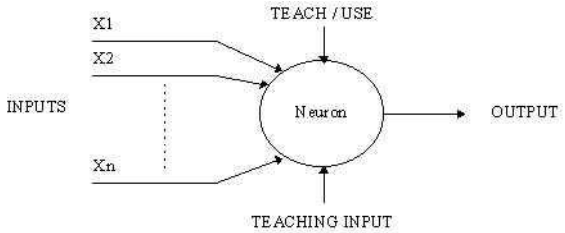


Fig2.Rule base Fuzzy Neural Network

A simple neuron

An artificial neuron is a device with many inputs and one output. The neuron has two modes of operation; the training mode and the using mode. In the training mode, the neuron can be trained to fire (or not), for particular input patterns. In the using mode, when a taught input pattern is detected at the input, its associated output becomes the current output. If the input pattern does not belong in the taught list of input patterns, the firing rule is used to determine whether to fire or not.



A simple neuron

5.2 Firing rules

The firing rule is an important concept in neural networks and accounts for their high flexibility. A firing rule determines how one calculates whether a neuron should fire for any input pattern. It relates to all the input patterns, not only the ones on which the node was trained. A simple firing rule can be implemented by using Hamming distance technique. The rule goes as follows:

Take a collection of training patterns for a node, some of which cause it to fire (the 1-taught set of patterns) and others which prevent it from doing[9] so (the 0-taught set). Then the patterns not in the collection cause the node to fire if, on comparison, they have more input elements in common with the 'nearest' pattern in the 1-taught set than with the 'nearest' pattern in the 0-taught set. If there is a tie, then the pattern remains in the undefined state.

5.2 Advantage Of Ann& Rule Base Neural Network

An RB/ANN integrated approach is proposed to facilitate the development of an expert system which provides:-

- High-performance.
- Knowledge-based network.
- An explanation facility.
- Input/output facility.

VI. CONCLUSION

Obviously, the battle between steganography and steganalysis is never-ending. This paper introduced the concept of combination of steganography. It also proposed a new approach to overcome steganalysis. In this paper Rule Base Neural Network approach is studied in order to discern its effectiveness in steganalysis [6]. Neural Networks can often be used for steganalysis & provide better performance than other techniques.

REFERENCES

[1] "M.P. Craven, K.M. Curtis, B.R. Hayes-Gill and C.D. Thursfield" A HYBRID NEURAL NETWORK/RULE-BASED TECHNIQUE FOR ON-LINE GESTURE AND HAND-WRITTEN CHARACTER RECOGNITION Fourth IEEE International Conference on Electronics, Circuits and Systems, Cairo, Egypt, December 15-18 1997, Volume 2, pp 850-853

[2] "Ho-Sung Park and Sung - Kwun Oh" RULE BASED FUZZY NEURAL NETWORK USING THE IDENTIFICATION ALGORITHM OF THE GA HYBRID SCHEME.

[3] "Hamsah A. Ghaleb Al-Jbara[1], Miss Laiha Binti Mat Kiah[2], Hamid A. Jalab" Increased Capacity of Image Based Steganography Using Artificial Neural Network International Conference on Fundamental and Applied Sciences 2012.

[4] "Usha B A1, Dr. N K Srinath2, Dr. N K Cauvery" DATA EMBEDDING TECHNIQUE INIMAGE STEGANOGRAPHY USING NEURAL NETWORK International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 5, May 2013

[5] "Ms. P. T. Anitha1, Dr. M. Rajaram2 ,Dr. S. N. Sivanandham" AN EFFICIENT NEURAL NETWORK BASED ALGORITHM FOR DETECTING STEGANOGRAPHY CONTENT IN CORPORATE MAILS: A WEB BASED STEGANALYSIS IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 3, No 1, May 2012

[6] "Nameer N. EL-Emam " Efficient Steganography using NEURAL.