Image Steganography Using Neural Networks

Dr . N. K Srinath
Prof and Dean,PG studies
Dept of CSE,R.V.C.E
Bangalore
srinathnk@rvce.edu.in

Prof.Usha B. A
Assistant Professor
Dept of CSE,R.V.C.E
Bangalore
Ushaajay1@gmail.com

Sonia Maria D'Souza
Student
Dept of CSE,R.V.C.E
Bangalore
soniamariadsouza@yahoo.com

Abstract— In this paper, we clarify what steganography is and what it can do. We contrast it with the related disciplines of cryptography and traffic security, present a unified terminology agreed the subject, and outline a number of approaches many of them developed to hide encrypted copyright marks or serial numbers in digital audio or video[1]. We then present a number of attacks, some new, on such information hiding schemes. This leads to a discussion of the formidable obstacles that lie in the way of a general theory of information hiding systems .However, theoretical considerations lead to ideas of practical value, such as the use of parity checks to amplify covertness and provide public key steganography[2]. Finally, we show that public key information hiding systems exist, and are not necessarily constrained to the case where the warden is passive. The proposed survey mainly focused on Neural Network to train the inputs and hidden layers in image steganography[3].

Keywords— Cryptography, Copyright protection, Data compression, Image registration, Jitter, Multimedia systems, Music, Observability, Redundancy, Spread spectrum communication, Software protection, Neural networks.

IJERT

I. INTRODUCTION

While classical cryptography is about concealing the content of messages, steganography is about concealing their existence. It goes back to antiquity: Herodotus relates how the Greeks received warning of Xerxes' hostile intentions from a message underneath the wax of a writing tablet, and describes a trick of dotting successive letters in a cover text with secret ink, due to Aeneas the Tactician. Kahn tells of a classical Chinese practice of embedding a code ideogram at a prearranged place in a dispatch; the same idea arose in medieval Europe with grille systems, in which a paper or wooden template would be placed over a seemingly innocuous text, highlighting an embedded secret message. Such systems only make sense where there is an opponent. This opponent may be passive, and merely observe the traffic, or he may be active and modify it.Classical steganography concerns itself with ways of embedding a secret message (which might be a copyright mark, or a covert communication, or a serial number) in a cover message (such as a video an audio recording, or computer code). The embedding is typically parameterised by a key; without knowledge of this key (or a related one) it is difficult for a third party to detect or remove the embedded material. Once the cover object has material embedded in it, it is called a stego object. Thus, for example, we might embed a mark in a cover text giving a stego text; or embed a text in a cover image giving a stego-image; and so on. There has been a rapid growth of interest in this subject over the last two years, and for two main reasons. Firstly, the publishing and broadcasting industries have become interested in techniques for hiding encrypted copyright marks and serial numbers in digital images, audio recordings, books and multimedia products; an appreciation of new market opportunities created by digital distribution is coupled with a fear that digital works could be too easy to copy. Secondly, moves by various governments to restrict the availability of encryption services have motivated people to study methods by which private messages can be embedded in seemingly innocuous cover messages. The ease with which this can be done may be an argument against imposing restriction.

II. THE STATE OF THE ART

Prudent cryptographic practice assumes that the method used to encipher data is known to the opponent, and that security must lie in the choice of key.

III. RELATED WORK

In order to characterize the weakness and the strength of the steganography system, various problems should be considered as: capacity, robustness and the undetectability features where the importance of each one of them depends on the application. Hiding capacity is one of the most important problem in steganographic system which represents the size of information that can be hidden into the cover file or it represents the total number of bits hidden and successfully recovered by the steganography technique. This problem needs to be more investigated by the researchers in order to increase the capacity of the data hidden 8-9. In the field of image based steganography, Kurak and McHugh proposed the earliest method of digital steganography; their method embeds the data into the 4th LSBs (least significant bits). In 2003, Yeshwanth Srinivasan 10 has proposed a method named Bit Plane Complex Steganography (BPCS), where the amount of hidden data reached to (20%) of the size of the image without noticeable distortion. A novel steganographic approach using triway pixel-value differencing (T-PVD) has been proposed by Changa et al . This approach upgraded the hiding capacity of the original PVD method by using three different directional edges to design the triway differencing scheme. Another application was developed by Mittal et al 12, where the relative entropy between content encryption with one key and decryption with several keys, corresponded to the amount of hidden information, as well as in their work, they have proposed the use of machine learning techniques to identify images as suspicious or nonsuspicious.All the previous work could achieve to hide (50%) of size of the cover image. EL-Emam NN 13, has proposed a new method of image steganography, based on machine learning system to hide a large amount of data into bitmap images which reached to (75%) size of cover image.

3.1. Steganography in Digital Mediums

Depending on the type of the cover object there are many suitable steganographic techniques which are followed in order to obtain security.

3.1.1 Image Steganography

Taking the cover object as image in steganography is known as image steganography. Generally, in this technique pixel intensities are used to hide the information.

3.1.2. Network Steganography: When taking cover object as network protocol, such as TCP, UDP, ICMP, IP etc, where protocol is used as carrier, is known as network protocol steganography. In the OSI network layer model there exist covert channels where steganography can be achieved in unused header bits of TCP/IP fields.

IJERT

3.1.3. Video Steganography: Video Steganography is a technique to hide any kind of files or information into digital video format. Video (combination of pictures) is used as carrier for hidden information. Generally discrete cosine transform (DCT) alter values which is used to hide the information in each of the images in the video, which is not noticeable by the human eye. Video steganography uses such as H.264, Mp4, MPEG or other video formats.

3.1.4. Audio Steganography: When taking audio as a carrier for information hiding it is called audio steganography. It has become very significant medium due to voice over IP (VOIP) popularity. Audio steganography uses digital audio formats such as WAVE, MIDI, AVI MPEG or etc for steganography.

3.2. Image Steganographic Techniques

Image steganography techniques can be divided into following domains.

3.2.1. Spatial Domain Methods: There are many versions of spatial steganography, all directly change some bits in the image pixel values in hiding data. Least significant bit (LSB)-based steganography is one of the simplest techniques that hides a secret message in the LSBs of pixel values without introducing many perceptible distortions. Changes in the value of the LSB are imperceptible for human eyes. Spatial domain techniques are broadly classified into:

1. Least significant bit (LSB) .
2. Pixel value differencing (PVD).
3. Edges based data embedding method (EBE) .
4. Random pixel embedding method (RPE) .
5. Mapping pixel to hidden data method .
6. Labeling or connectivity method .
7. Pixel intensity based method .
8. Texture based method .
9. Histogram shifting methods .

General advantages of spatial domain LSB technique are:
1. There is less chance for degradation of the original image.
2. More information can be stored in an image.
Disadvantages of LSB technique are:
1. Less robust, the hidden data can be lost with image manipulation.
2. Hidden data can be easily destroyed by simple attacks.

3.2.2 Transform Domain Technique: This is a more complex way of hiding information in an image. Various algorithms and transformations are used on the image to hide information in it. Transform domain embedding can be termed as a domain of embedding techniques for which a number of algorithms have been suggested . The process of embedding data in the frequency domain of a signal is much stronger than embedding principles that operate in the time domain. Most of the strong steganographic systems today operate within the transform domain Transform domain techniques have an advantage over spatial domain techniques as they hide information in areas of the image that are less exposed to compression, cropping, and image processing. Some transform domain techniques do not seem dependent on the image format and they may outrun lossless and lossy format conversions. Transform domain techniques are broadly classified into:
1. Discrete Fourier transformation technique (DFT).
2. Discrete cosine transformation technique (DCT).
3. Discrete Wavelet transformation technique (DWT).
4. Lossless or reversible method (DCT).
5. Embedding in coefficient bits.

3.2.3. Masking and Filtering: These techniques hide information by marking an image, in the same way as to paper watermarks. These techniques embed the information in the more significant areas than just hiding it into the noise level. The hidden message is more integral to the cover image. Watermarking techniques can be applied without the fear of image destruction due to lossy compression as they are more integrated into the image.

Advantages of Masking and filtering Techniques:
1. This method is much more robust than LSB replacement with respect to
compression since the information is hidden in the visible parts of the image.
Disadvantages of Masking and filtering Techniques:
1. Techniques can be applied only to gray scale images and restricted to 24 bits.

IV. INFORMATION DETECTION BASED ON NEURAL NETWORK

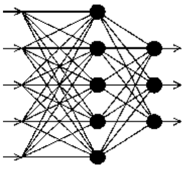
The information detection is based on result that host image must be difference with hidden information host image. Maybe because human eye's mask features, we can't find any difference between host images and hidden information host images. But in essentially, data hiding process have to alter host image for embedding data. In other words, data hiding algorithms reveals statistical evidence or traces which can be used to detect the existence of hidden information in still images.Because now popular data hiding methods can be divided into two major classes: spatial domain and transform domain. Spatial domain is simple and easy to implementation, but their robustness is weaker than other methods' based other domain. Transform domain includes discrete Fourier transform, discrete cosine transform, discrete wavelet transform mainly. And in spatial domain, mainly data hiding method is least significant bit (for short writing LSB) including all kinds of improved LSB methods. In transform domain, methods can be divided into several classes, quantization based, LSB based. Because we hope our method is feasible to all kinds of hiding methods no regardless embedding information in spatial or transform domain. So we try our best to consider all kinds methods' features. But due to methods is too much, so we only consider transforms used in common data hiding methods.

V. Neural Network Methodologies.

5.1 Feed-forward networks

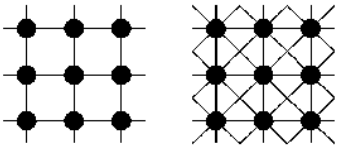
Feed-forward ANNs allow signals to travel one way only; from input to output. There is no feedback (loops) i.e. the output of any layer does not affect that same layer. Feed-forward ANNs tend to be straight forward networks that associate inputs with outputs. They are extensively used in pattern recognition. This type of organization is also referred to as bottom-up or top-down.

IJERT



5.2 Feedback networks

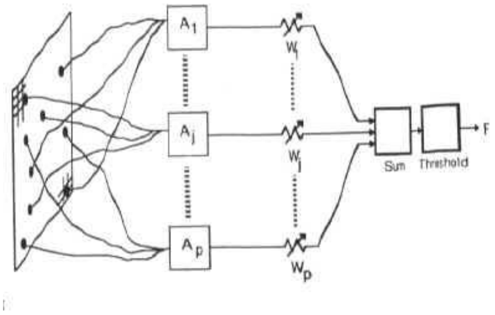
Feedback networks can have signals traveling in both directions by introducing loops in the network. Feedback networks are very powerful and can get extremely complicated. Feedback networks are dynamic; their 'state' is changing continuously until they reach an equilibrium point. They remain at the equilibrium point until the input changes and a new equilibrium needs to be found. Feedback architectures are also referred to as interactive or recurrent, although the latter term is often used to denote feedback connections in single-layer organizations.



5.3 Network layers

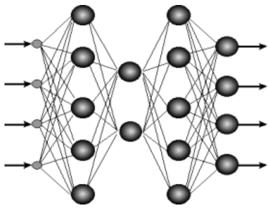
The commonest type of artificial neural network consists of three groups, or layers, of units: a layer of "input" units is connected to a layer of "hidden" units, which is connected to a layer of "output" units. The activity of the input units represents the raw information that is fed into the network.

The activity of each hidden unit is determined by the activities of the input units and the weights on the connections between the input and the hidden units.The behavior of the output units depends on the activity of the hidden units and the weights between the hidden and output units.



5.4 Perceptrons

The most influential work on neural nets in the 60's went under the heading of 'perceptrons' a term coined by Frank Rosenblatt. The perceptron turns out to be an MCP model (neuron with weighted inputs) with some additional, fixed, pre--processing. Units labeled A1, A2, Aj, Ap are called association units and their task is to extract specific, localized featured from the input images. Perceptrons mimic the basic idea behind the mammalian visual system. They were mainly used in pattern recognition even though their capabilities extended a lot more.



VI .PERFORMANCE ANALYSIS

From the measured statistics of training sets of images with and without hidden information, our destination is to determine whether an image has been hidden information or not. Because data hiding process is a nonlinear process, if we only use linear classifier to classify images, it is not a good simulation. And neural network has an excellent capability to simulate any nonlinear relation, so we make use of neural network to classify images.

VII. Encryption and Decryption

Encoding: In the encoding part, the audio file selected bythe user is first read and stored in a matrix. The chosen secret file is opened and length is calculated [7]. This is stored in a variable, also in a secure position of the resulting steg-audio file. The secret message is encrypted as a precaution so that the original message don't fall into wrong hands even it is intercepted, which is of least probability and is placed in a location whichdepends on the size of both the secret file and the audio file. The encoded audio file is then saved and is ready to be transported.

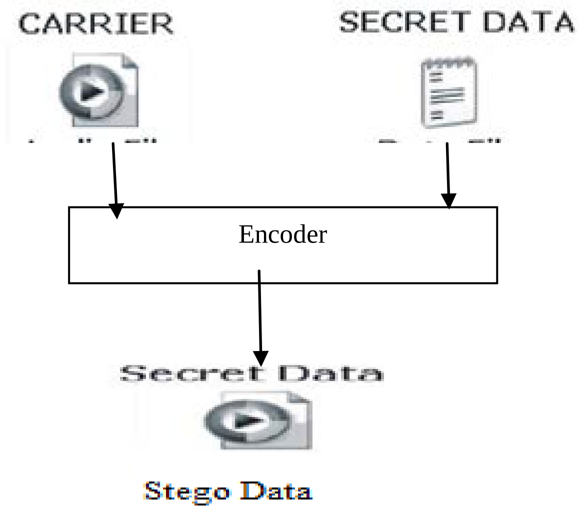


Fig: Encoding Process

Decoding: The secret message from the steg file can be retrieved only using the decoding program. At the receiver end, the length of the secret message is read from the audio file. This will in turn serve the purpose of calculating the starting position of the secret message also. The secret message is then read and decrypted.This is then read to a matrix and saved to the output file and hence the original secret message is obtained.

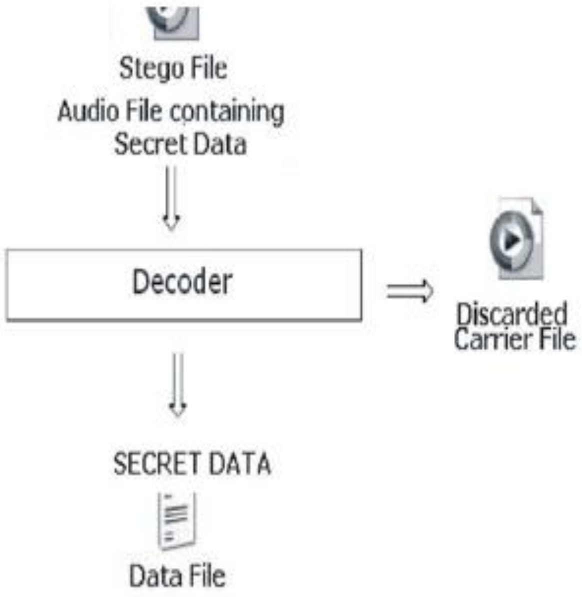


Fig: Decoding Process

VII. Comparative Study

Characteristics	Neural Network Based steganalysis in Still Images	Steganalysis Based on Moments of characteristic Function using Wavelet Decomposition,Prediction Error Image and NN	TextureBasedsteganalysis
Type of steganalysis	Passive	Passive	Passive
Features	Transform domain includes:DFT,DCT ,DWT	Moments of characteristics function,Prediction error-image	LBP(Local Binary Pattern)
Type of Neural Network	Back-Propagation Neural Networks	FFNN with BP	Nil
Use of ANNs	For classifying	For classifying	For Selecting
Image Used	Each image is divided into 8*8 sub-blocks	1096 sample images included in the coreldraw	1000 clean color JPG images and 1000 stego-images
Results	Hidden images:85.4%	Hidden images: 97.1%	Hidden images: 96%

VIII. CONCLUSION

In this survey paper we discussed about the basic concept of steganography and how it is used in image, audio, video and text with the help of different neural networks and done the comparative study.

IJERT

REFERENCES

[1] Anderson, J. A., An Introduction to Neural Networks, Prentice Hall of India Pvt. Ltd., New Delhi, 2004.

[2] Chandramouli, R. and Subbalakshmi, K. P., Active steganalysis of spread spectrum image steganography, IEEE International Symposium on Circuits and Systems, Bangkok, Thailand, 3, 830-833, May 2003.

[3] Freeman, J. A. and Skapura, D. M., Neural Networks-Algorithms, Applications, and Programming Techniques, Pearson Education Ltd. 2005.

[4] Liu Shaohui, Yao Hongxun, Gao Wen “Neural Network based Steganalysis in Still Images” Proceedings of IEEE ICME 2003.

[5] El-Emam, N., 2008. Embedded a large amount of information using high secure neural based steganography algorithm. International Journal of Information and Communication Engineering.