NEURAL NETWORK BASED CAMOUFLAGING IN STILL IMAGE

J.Selvaraj, R.Balasubramaniam

Final Year M.E (Student), Department of Computer Science & Engineering, M.S University, Tirunelveli, Tamilnadu, INDIA

Selection Grade Lecturer, Department of Computer Science & Engineering, M.S University, Tirunelveli, Tamilnadu, INDIA

Email: selvarajjayapal@yahoo.com

+914362277655

No: 3751, Bank Staff Colony, 6th Street, M.K Road

Tanjore, Tamilnadu

INDIA

Email: rbalus662002@yahoo.com

+919443695573

Department of Computer Science & Engineering,

M.S University, Abhishekapatti,

Tirunelveli, Tamilnadu

INDIA

ABSTRACT

The communication wing of network renews the modern trends as the threats of network challenges the computer security. This project configures a secure communication through neural based steganography. Steganography is an art of hiding messages inside a multimedia block. Data hiding techniques are achieved through innocuous media like text, images and audio signals. Hackers adopt various detecting techniques to read the secret information. This research provide an idea to overcome the mentioned hurdles by hiding the data indirectly into a graphical image using neural network algorithm which results in unidentified evidence of transmission held as it adds complexity for the hackers. This method hides indirectly the secret binary bits along with some selected graphical image bits, based on neural algorithm to get cipher bits. The generated cipher bits are then placed in the least significant bit position of the carrier image. In retrieval process, this method regenerates the original data bits. XOR propagation network model is used which acts as the multi-layer perceptron.

KEY WORDS

LSB Encoding, XOR Propagation Network, MSB.

NEURAL NETWORK BASED CAMOUFLAGING IN STILL IMAGE

1 INTRODUCTION 1

Information hiding has become the focus of research today. Steganography is the art of hiding information in ways that prevent the detection of hidden messages. The term steganography means “covered writing” and involves transmission of secret messages through apparently innocent files without detection of the fact that message was sent. The innocuous file is known as the cover (image) while the file containing the hidden message referred as stego medium. Image is one of the tools for hiding messages among audio, video files. Binary files with certain degree of irrelevancy and redundancy can used to hide data. The advantage of neural based Steganography is that it can be used to secretly transmit messages without the fact of the transmission being discovered.

The embedding algorithm is used to hide secret messages inside a cover or a carrier document the embedding process is protected by a keyword so that only who possess the secret keyword can access the hidden message. The detector function is applied to carrier nothing to do with the cover and the issue concerned is the bandwidth of the hidden message. The most well-known steganography technique is the LSB encoding.

Recent terrorist activity has been tentatively linked to the use of steganography say SEP 11 attack in New York. US Today printed an article “Terror groups hide behind web encryption” by Tuck Kelley. In his article, he writes “US officials and experts say steganography is the latest method of communication being used by Osama bin Laden and his mission.

1.1 Neural Design for Steganography 2

Initially, training the patterns that is formed from the original data and the selected bits from the graphical image produces cipher text. The cipher text is embedded in the LSB of the image and then transmitted to the receiver. The secrecy lies in the design of the neural algorithm that trains the pattern. The neural algorithm has to be exchanged between the sender and receiver through a secure channel. A neural algorithm accepts “n” input pattern that has to be trained, equals to 2^K+1, for an input pattern having k+1 bits. Here 1 bit is selected from the secret message and k bits from carrier image. Input layer is designed with k+1 neurons. The no. of neurons in the hidden layer depends on the problem domain. An "m" bit secret message can be hidden in m pixels of the image and k+1 bit is encrypted at a time. XOR-Propagation algorithm is implemented in training the bit patterns.

On the decryption section, the input patterns bits are formed by the merging of cipher and selected bits from the image. The retrieval process returns back the original graphical image.

1.1.1 Xor Propagation Network 3

The network consists of three-layer with two input units, one unit in the hidden layer and one output unit. The connection weights are shown on links and the threshold of each unit is shown inside the unit. As far as the hidden unit is concerned, the hidden unit is no different from both of the input units, and simply provides another input. Hidden unit’s threshold of 1.5 means that it is off unless turned on both the inputs on. The behaviour of the network is noted when inputs are off (00), the hidden unit is also off, and there is no net input to the output unit. When the right input only is on (01), the hidden unit does not receive enough net input to turn it on, so it remains off. The output unit sees a net input of +1, which exceeds its threshold, and so it turns it on. The same happens when the left unit only (10) is on. When both inputs are on (11) the hidden unit receives a net input of +2, which exceeds its threshold value, and so it turns on. The output unit now sees a net input of

+1 from each of the input units, making +2, and –2 from the hidden unit, making 0 in all. This is less than threshold and so the unit is off.

The hidden detects when both the inputs are on, since this is the only condition under which it turns on. The hidden unit is acts as a feature detector, detecting when both the inputs are on. It can be viewed as recording the basic inputs and mapping of input patterns to output ones.

The neural based steganography is explained by choosing text as a secret message and the graphical image as the carrier medium. The LSB of the 256 Bitmap Picture (bmp) is used as the graphical image. The secret message and the graphical image bits are combined to form the cipher bits, which are referred as trained input patterns. A single bit secret text is combined with single bit graphical image to form possible input patterns. The neural algorithm is designed with respond to binary. The output bits generated called cipher bits embedded in the LSB of the image. Thus secret message is indirectly hidden in the cover.

1.1.1.1 ILLUSTRATION WITH AN EXAMPLE 4

A message “Attack Postponed” is converted to binary bits equivalent through the process of binarization.In this example, MSB (Most Significant Bit) of the RGB components are selected bits of the graphical image. The secret data bits and selected graphical image bits acts as input. The neural network for the above example is designed with 2 input neurons, 1 hidden neurons and an output neuron. The training pattern is nothing but the XOR.The weight values are set to train the input pattern with definite thresholds. The trained neural network fires the output neurons (cipher bits) after satisfying the thresholds in the network. The output from the output layer is placed in LSB (Least Significant Bit) of the image placing as 7 bits in a pixel array sequentially in rows. The activation function for the given example in hidden layer is given below.

1.1.1.1.1 Algorithm 5

The neural based steganography algorithmic system design as follows.

INPUT: Message Bits, Selected cover image bits, cover image.

OUTPUT: Stego image.

Step 1: Design Principles of Training Pattern

Form the input pattern by selecting one bit of secret text and k image bit.

Choose the number of bits required in the target output pattern.

Step 2: Deign of Neural Network

Design the neural network with the above training pattern by deciding the number of input neurons, middle layer neurons and output neurons.

Step 3: Train the Pattern

While data bits of secret message present do

The input is fed into the trained network and the output generated is stored in the LSB of image.

end while

1.1.1.1.1.1 Performance Analysis 6

The Analysis sketches the graph, determining the comparative rate of training obtained at several threshold values. Rate is represented in milliseconds.

1.1.1.1.1.1.1 Conclusion 7

This paper provides neural approach to embed information satisfying a secure steganography. Neural approach adds the complexity for the hackers accessing and also presents high potentiality

in Defence Operations. Neural Steganography is a powerful tool that enables people to communicate without possible eavesdroppers even knowing there is a form of communication.

1.1.1.1.1.1.1.1 Future Enhancement 8

Steganography is renewed nowadays merging with different fields like Neural Networks, Fuzzy Systems increasing a feasible security and privacy. Using steganographic techniques, software can easily transmit private user information without user's knowledge. Steganography is of immense importance and it is indispensable in the fields of Digital Watermarking, Digital Fingerprinting, Internet Security, Network Security, Authentication, Copyright issues, etc

2 SCHEMATIC REPRESENTATION OF NEURAL NETWORK BASED STEGANPGRAPHY

1.2 Figures

Figure 1/Design Architecture

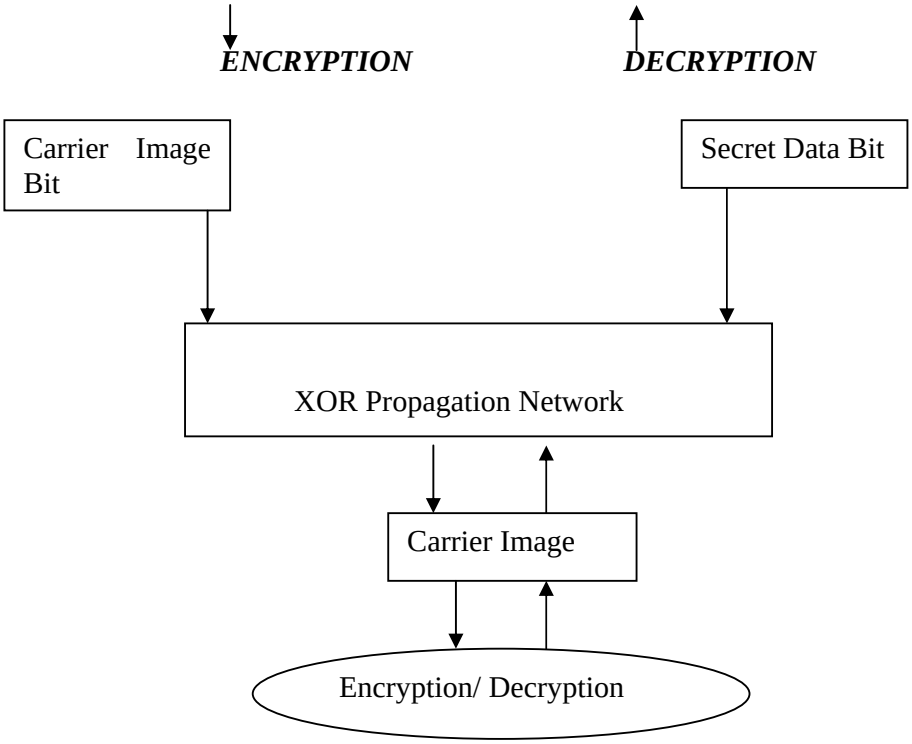


Figure 2/XOR Propagation Network

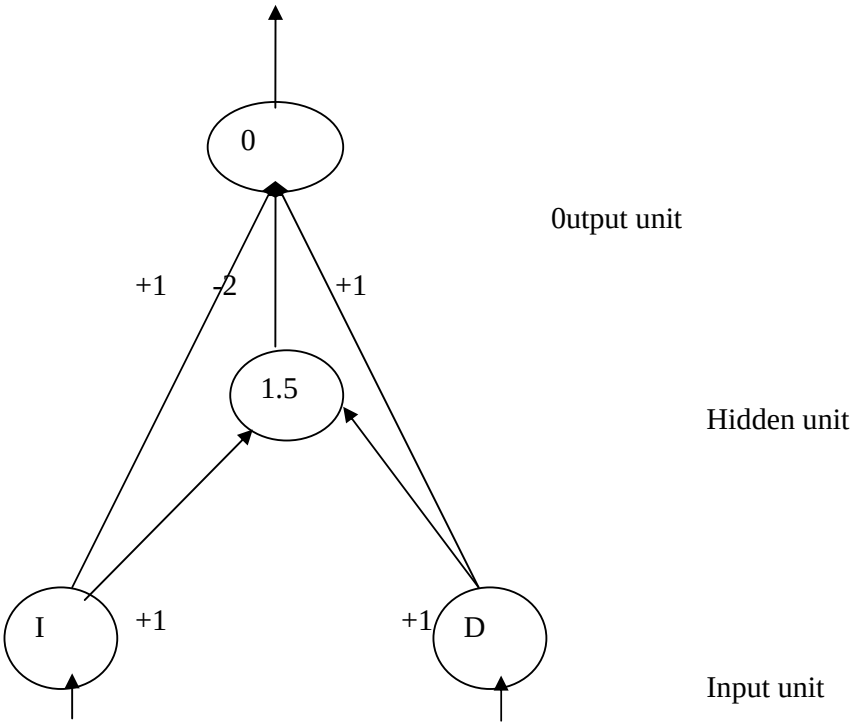
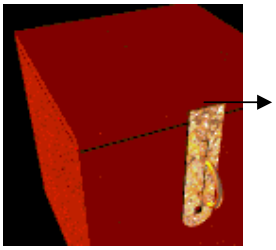


Figure 3/LSB Encoding Symbolic Representation

Carrier Image



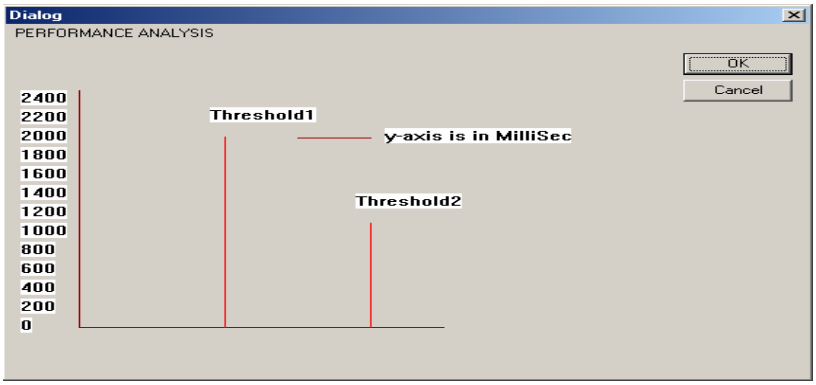
Binarization

256 Colour Image RGB Pixel Array

1	***1***	***1***	***1***	***0***	***0***	***0***	.	.	.	.	***1***	***0***	***0***	***0***	***1***	***1***	***1***
.	.	.	.	.	.	***1***	***0***	***1***	***1***	***0***	***0***	***1***	.	.	.	.	.
1	***0***	***0***	***1***	***1***	***1***	***0***	.	.	.	.	***0***	***1***	***0***	***1***	***0***	***0***	***1***
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.

Indirectly Hidden Secret Message

Figure 4/Performance Analysis at Training Thresholds



2.1 Tables

Table 1/Truth table for XOR network

Input Layer	Hidden Layer	Output Layer
00	**0**	**0**
01	**0**	**1**
10	**0**	**1**
11	**1**	**0**

2 REFERENCES

1. *"Neural based steganogrpahy" by Dr. K.S Easwarakumar., Anna University, Chennai.*

2. *Liu Shaohui, Yao Hongxun, Gao Wen "Neural Network based Steganalysis in Still Images" Proceedings of IEEE ICME 2003.*

3. *F.A.P Peticolas, R.J Anderson and M.G.Kuhn, Information Hiding – A Survey, Proceeding of IEEE Vol: 87 no: 7,1999,pp.1062-1078*

4. *R.J Anderson and F.A.P Peticolas, On the Limits of Steganography, Journal of Selected Areas in Comm., Vol.16, no.4, 1998.pp.474 – 481*

5. *Robert Krenn, "Steganography and Steganalysis".*

6. *S.Rajasekaran, G.A Vijayalakshmi Pai, Neural Networks, Fuzzy Logic and Generic Algorithms Synthesis and Applications, Prentice – Hall of India, Pvt Ltd.NewDelhi, 2003.*

7. *N.F.Johnson and S.Jajodia, "Steganography seeing the Unseen," IEEE Computer, February 26-34, 1998.*

8. *Adel M. Abunawass, Omar Bukhres, Theresia G.Fisher, Kenneth Magel, 300 Minard Hall North Dakota University. "A First Undergraduate Course in Neural Networks".*

3 PERMISSIONS