New Steganographic Technique using Neural Network

Akshay Phadke
University of Mumbai
Mumbai, India.

Aditi Mayekar
University of Mumbai
Mumbai, India.

ABSTRACT

Steganographic technique is used to hide the information, a string of characters containing the information, in a carrier image. The information is coded into individual rows of the constituent primaries of the carrier. Using this technique the neural network is employed to detect the presence of the message in the individual rows of the carrier image and to retrieve the contents of the message hidden in the carrier. This technique is able to maintain good visual quality of the carrier image. The results of this technique revealed high PSNR values and significantly less MSE values for the unmodified carrier and the steganographic image.

General Terms

Mean Square Error, Peak Signal to Noise Ratio

Keywors

Digital Image Processing, Steganography, Image Compression, Neural Network

1. INTRODUCTION

An image ay be defined as a two dimensional function f(x, y), where x and y are spatial co-ordinates, and the amplitude f at any pair of co-ordinates is called intensity of the image at that point [1]. Here an image is assumed to be a two dimensional matrix where each point corresponds to certain level of brightness and the image is made up of rows and columns of such points known as pixels.

Steganography is the technique of hiding information in a given medium. Over the years the medium has varied. Nowadays it is more common to find information hidden in a photograph or an image [2], [3]. Here the medium is an image, a matrix of pixels where each pixel has its own distinct co-ordinates. In this technique the RGB colour co-ordinate system is used where each pixel is expressed in terms of Red, Green, and Blue content. Thus for one carrier image, three individual primaries are used as the carriers. Thus three unique message carriers compose one carrier image.
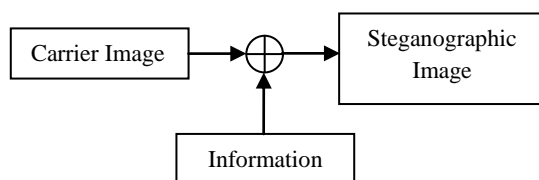

Fig.1: The process of Steganography

Artificial intelligence, cognitive modelling, and neural networks are information processing paradigms inspired by the way biological neural systems process data. Artificial intelligence and cognitive modelling try to simulate some properties of biological neural networks.

Neural network is a processing device which maybe expressed as hardware or an algorithm. It is inspired by the design and functioning of the human brain. It is also known as artificial neural network or a neural net. An artificial neural network (ANN) maybe defined as an information processing model that is inspired by the way biological nervous system, such as the brain, process information [4]. An ANN is composed of a large number of highly interconnected processing elements (neurons) working in unison to solve a particular problem.
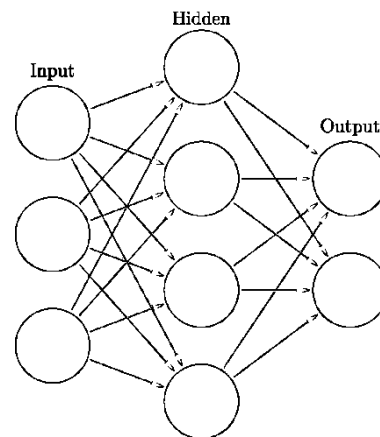

Fig.2: Structure of Artificial Neural Network (ANN)

2. LSB STEGANOGRAPHY TECHNIQUE

The carrier image uses a 24-bit colour image .jpg file format which is manipulated with the individual RGB channels of the image. The 24-bit image can be expressed in terms its constituent 8-bit primaries, namely, Red, Green and Blue. Thus three individual two dimensional matrices are made available for manipulation. The three matrices corresponding to each of the primaries of the carrier have the potential to carry three hidden message by means of the LSB steganography method [5], [6].

The hidden message is in the form of an image which has the same dimensions as that of the carrier image. The message is generally a black and white image having only two levels-black and white.

The LSB technique uses the following algorithm:

1. The carrier image is decomposed into individual primary matrices, namely R, G, and B.

2. Each pixel of the primary matrix is accessed one at a time and its value is then converted to binary form. It is observed that MSB carries most information and the LSB carries least information.

3. The individual pixels of hidden message for each matrix are also converted to binary.

4. The MSB of the pixel of hidden message is extracted along with the LSB of corresponding pixel of the primary carrier matrix.

5. The LSB of each pixel of the carrier matrix is replaced by the MSB of the pixel of the hidden image.

6. This procedure is repeated for all pixels till the entire hidden image gets stored in the carrier

7. This can be repeated for all primary matrices so as to obtain the final stego image which is a combination of all stego primary images.

However this method was found to have the following drawbacks:

1. Only up to three messages could be hidden using this technique.

2. This technique increased the embedded distortion as LSB of every pixel of carrier was replaced by the MSB of every pixel of hidden image, even in the absence of any meaningful data.

3. Thus efficiency was reduced in this technique, which was reflected in the PSNR and MSE values obtained by comparing the carrier with stego-image.

3. HEBB'S RULE

The Hebb's rule is applied in this context as means of pattern recognition. Hebb's rule states that a change in the strength of a connection is a function of the pre – and postsynaptic neural activities. It is also called the "Hebbian Learning Rule" after D. Hebb [7].

From the point of view of artificial neurons and artificial neural networks, Hebb's principle can be described as a method of determining how to alter the weights between model neurons. The weight between two neurons increases if the two neurons activate simultaneously—and reduces if they activate separately. Nodes that tend to be either both positive or both negative at the same time have strong positive weights, while those that tend to be opposite have strong negative weights [8].

In the proposed technique, there is a need to determine certain parameters of the message that is to be hidden, such as the length of the message and from which row of the image the message is to begin. This information is hidden in the carrier image's 7th bit plane using a pattern. Recognition can be carried out using the Hebb rule.

The algorithm for the Hebb rule is as follows:
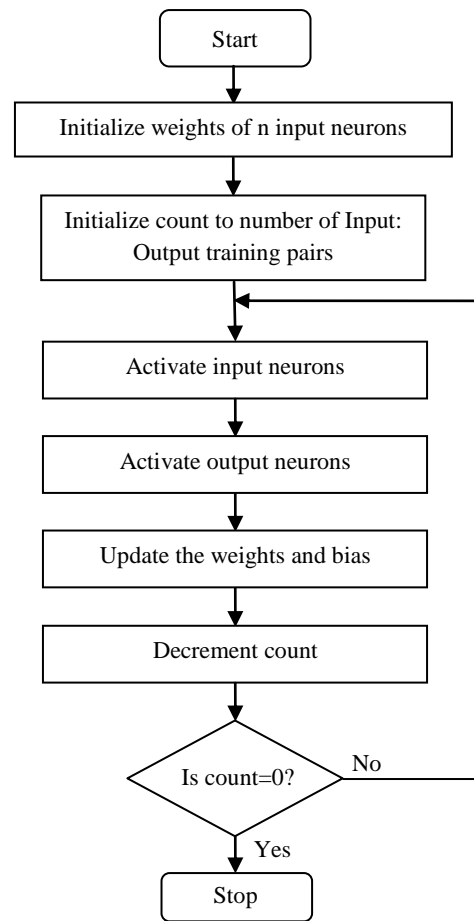
Fig.3: Algorithm of Hebbian Learning Rule

4. NEW PROPOSED STEGANOGRAPHY TECHNIQUE

There are many steganographic techniques that seek to overcome the drawbacks encountered using the simple LSB steganographic technique [9]. The new proposed technique employed the following procedure for hiding the data in the carrier image:

1. The hidden information is in the form of text which is converted character-by-character to its corresponding ASCII value

2. The ASCII value so obtained is then converted to 8-bit binary value and stored in the LSB of the RGB primary of the carrier

3. This string of binary data is not arranged sequentially thus preventing the data to be deciphered and also increasing the amount of data stored.

As an added security measure, the data is not hidden serially from the first row itself. The person wishing to hide the data may choose the row beginning from which the data maybe hidden. This ensures that the data, even if detected, may not be deciphered without prior knowledge of the following:

1. The starting row from which data is hidden

2. The length of the message text.

Thus the advantages of the proposed technique over the LSB technique are as follows:

1. The number of messages that can be hidden is greater than in the LSB technique.

2. Greater efficiency and faster results since only selected pixel values are manipulated as opposed to the entire image in the LSB technique.

3. Better quality of the steganographic image than the one obtained using LSB technique.

```
┌─────────────────────────────────────┐
│        Read the cover image.         │
└─────────────────────────────────────┘
                  ↓
┌─────────────────────────────────────┐
│  Provide the messages and their      │
│  positions and calculate message     │
│  lengths.                            │
└─────────────────────────────────────┘
                  ↓
┌─────────────────────────────────────┐
│  Generate pixel patterns for the     │
│  positions and lengths of the        │
│  messages.                           │
└─────────────────────────────────────┘
                  ↓
┌─────────────────────────────────────┐
│  Inscribe the patterns in the        │
│  seventh bit of each primary image.  │
└─────────────────────────────────────┘
                  ↓
┌─────────────────────────────────────┐
│  Convert the messages into 8-bit     │
│  ASCII character sequence and store  │
│  the message bit-by-bit in LSB of    │
│  the individual primaries of the     │
│  cover image.                        │
└─────────────────────────────────────┘
```
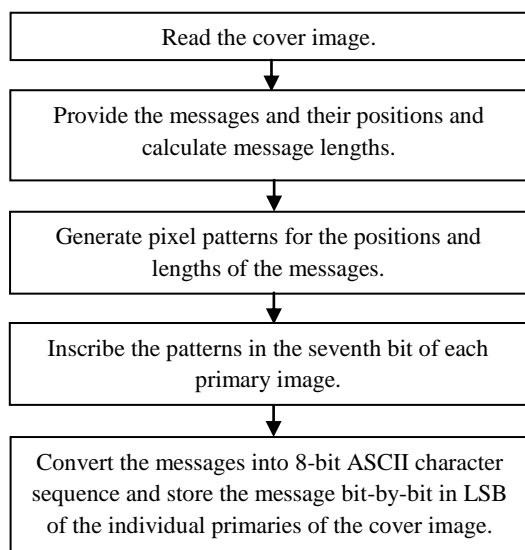
Fig.4: Algorithm to generate the steganographic image

Similarly, the following is a flowchart that demonstrates the steps involved in recovering the hidden information from the steganographic image.

```
┌─────────────────────────────────────┐
│        Read the cover image.         │
└─────────────────────────────────────┘
                  ↓
┌─────────────────────────────────────┐
│  Recognize pattern in the 7th bit    │
│  using ANN                           │
└─────────────────────────────────────┘
                  ↓
┌─────────────────────────────────────┐
│  Determine the row and length of     │
│  message                             │
└─────────────────────────────────────┘
                  ↓
┌─────────────────────────────────────┐
│  Read the message hidden in the 8th  │
│  bit using the parameters obtained   │
│  above                               │
└─────────────────────────────────────┘
                  ↓
┌─────────────────────────────────────┐
│        Display the message           │
└─────────────────────────────────────┘
```
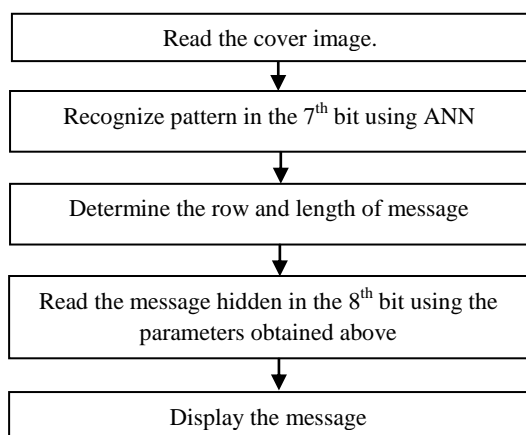
Fig.5: Algorithm to retrieve message from stego-image

5. RESULTS

The proposed technique was implemented using MATLAB and the steganographic image was obtained by providing the messages. It was found that the carrier and the stego-image were visually indistinguishable. The images on which the proposed technique was implemented are very well known images such as Lena, Baboon (Mandrill), Peppers, etc along with the standard images available in Windows XP such as Sunset, Blue Hills, etc.
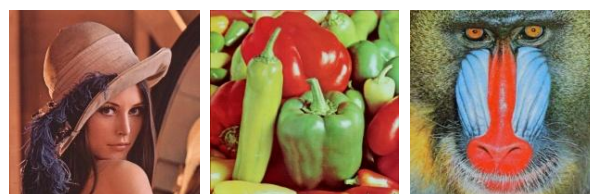

Fig.6: Some carrier images used (Lena, Peppers, and Baboon)

The image was tested for quality using two parameters, namely, Peak Signal-to-Noise Ratio (PSNR) and Mean Square Error (MSE). These parameters are defined as follows:

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j)]^2$$

$$PSNR = 10.\log_{10}[MAX_I^2 / MSE]$$

MAX_I is the maximum possible pixel value of the image.

The following table presents the PSNR and MSE values for some of the standard images on which the technique was implemented. It was observed that the proposed technique gave better performance than the LSB technique in terms of the PSNR and MSE values.

Table1: Some sample cover images and results

Image	PSNR	MSE	PSNR(LSB)	MSE(LSB)
Sunset	57.7939	0.1089	51.2588	0.4905
Water Lilies	77.2736	0.0012	50.9896	0.5218
Blue Hills	63.4869	0.0294	51.2072	0.4963
Winter	63.3057	0.0306	51.0135	0.5190
Lena	54.7396	0.2200	51.2309	0.4936
Baboon	66.5937	0.0144	51.1818	0.4992
Peppers	53.9088	0.2664	51.0282	0.5172

This information has been represented graphically in the following two graphs. The first graph represents the PSNR values for the proposed technique against those obtained using LSB technique. The second graph represents the MSE values for the same.
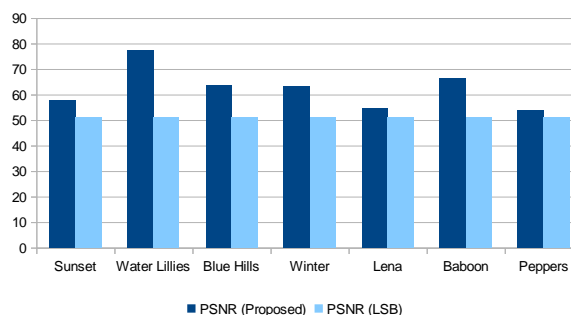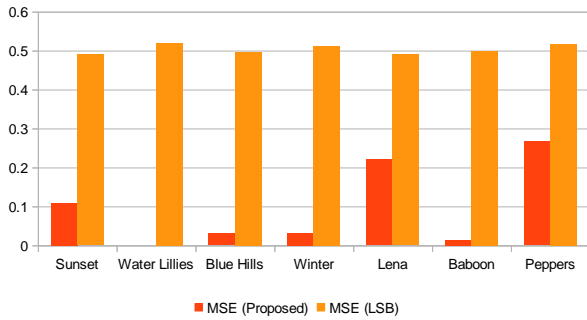

Fig.7: PSNR of proposed technique and LSB technique

Fig.8: MSE of proposed technique and LSB technique

It is desirable to have low Mean Square Error (MSE) values and high values of Peak Signal to Noise Ratio (PSNR) which is an indication of good quality of the image. The LSB technique produced high MSE values irrespective of the image. In all cases the proposed technique produced better results but it fared better for some images than others. As a result the PSNR values were also better for the proposed technique.

6. CONCLUSION

The proposed technique seeks to produce better results than the LSB steganographic technique in terms of the amount of messages that can be hidden, the time required to retrieve the hidden information, and the visual quality of the image. By making use of artificial neural network, and on comparing the new proposed technique with the LSB technique, it is clear that the new proposed technique has better results than the LSB technique. The proposed technique succeeds in these all the regards. It also provides additional security to the message hidden in the image. The better performance is demonstrated by the superior PSNR and MSE values of the tested images and proves the successful outcome of this technique.

8. REFERENCES

[1] Image definition, Gonzalez, Woods – Digital Image Processing.

[2] Z Neil F. Johnson and Sushhil Jajodia. "Steganalysis: The Investigation of Hidden Information" - Proceedings of the IEEE Information Technology Conference, Syracuse, New York, USA, 1998.

[3] I.Aveibas, N.Memon, B.Sankur. "Steganalysis based on image quality metrics" - Multimedia Signal Processing, 2001 IEEE Fourth Workshop on, 2001.

[4] Artificial Neural Network definition, S.N. Sivanandan, S.N. Deepa - Principles of Soft Computing.

[5] R.Chandramouli and N. Memon, "Analysis of LSB based image steganography techniques," in Proc. ICIP, Oct. 2001.

[6] Chandramouli, M. Kharrazzi, and N. Memon Image steganography and steganalysis: Concepts and Practice, Springer-Verlag, vol. 2939, 2004.

[7] Hebb Rule definition, Wikipedia URL: http://en.wikipedia.org/wiki/Hebbian_theory

[8] E.I. Papageorgiou et al. /Internet J. Approx. Reason. 37 (2004) 219–249.

[9] Jessica Fridrich, Miroslav Goljan. Practical Steganalysis of Digital Images - State of the Art.