Image Steganography Technique using Radon Transform and Neural Network with the Wavelet Transform

[1]S. Thenmozhi, [2]Dr. M. Chandrasekaran

[1]Research scholar, Anna University, Chennai, Tamilnadu, India
[2]Professor & Head, Dept of ECE, GCE, Bargur, Tamilnadu, India

Abstract- Steganography is the art and science of communicating secret data by hiding information in plain sight without being noticed within an innocent cover data so as not to arouse an observer's suspicion. The vital goal here is to conceal the very existence of the embedded data. It is used to achieve secure data transmission over internet. In this paper, a novel steganography technique for hiding data in digital images by combining wavelet transform, neural network and radon transform is proposed. The cover image is decomposed into four parts by applying discrete wavelet transform. Radon transform is applied on secret image. Finally Back propagation neural network is used to conceal the transformed secret data in wavelet coefficients of the cover image. From our experimental results it can be shown that the proposed system hides information effectively, better secrecy and maintains a better visual display of stego image than the traditional methods.

Keywords: Back propagation neural network, discrete wavelet transform, frequency domain, Steganography and radon transform

I. Introduction

The enormous development in the internet technology has raised the demand of a private and secured communicational environment. With the increased number of users, the necessity for information concealing has become as a critical issue in the World Wide Web (WW). The users are concerned about maintaining and conserving the confidentiality of the secret messages transmitted through the Internet. Steganography is one of the powerful techniques in which information is being concealed using a carrier for the secret message. There are different types of steganography and every one of them has its own specific characteristics and applications. On the other hand, there are various types of carriers that have been used to conceal the data such as text, audio, video and digital images files. Digital images are extensively used in the steganography area.

Steganography is originally composed of two Greek words steganos (*secret*) and graphic (*writing*) which means "covered writing". Steganography is defined by Markus Kahn as follows, "Steganography is the art and science of communicating in a way which hides the existence of the communication". So, steganography is the process of hiding secret data within public information. Image based steganography is the most common system used since digital images are widely used over the Internet and Web. Digital image steganography is a technique of secret communication that aims to convey a huge amount of secret data relatively to the size of cover image between two communicating parties. Furthermore, it also aims to avoid the suspicion of non-communicating parties to this kind of communication.

There are a number of steganography methods that embed secret message in an image file. These steganography methods can be classified according to the format of the cover image or the hiding method. Based on embedding domain steganography methods are divided into two: Spatial domain and transform domain. The Least Significant Bit (LSB) substitution is the example of spatial domain methods [1]. The main idea in LSB is the direct replacement of LSBs of noisy or unused bits of the host image with the secret message bits. Still LSB is the most preferred system used for data hiding because it is very simple to implement offers high hiding capacity, and provides an easy way to control stego-image quality but it has low robustness to modifications [2] made to the stego-image including low pass filtering and low imperceptibility. Some examples to hide data in spatial domain using LSB approach can be found in [3], [4].

The other type of embedding method is the transform domain techniques which appeared to overcome the robustness and imperceptibility problems found in the LSB substitution techniques. There are many transforms that can be used in data hiding, the most widely used transforms are; Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Discrete Fourier transform (DFT). Examples to data hiding using DCT can be found in [5], [1].Most recent researches are directed to the use of DWT since it is used in the new image compression format JPEG and MPEG4, examples of using DWT can be found in [6], [7], [8]. In [9] the secret message is embedded into the high frequency coefficients of the wavelet transform while leaving the low frequency coefficients sub band unaltered.

In this paper, a new steganography scheme to embed the secret message in the cover image is presented. This proposed technique is based on training Back Propagation Neural Network (BPNN) in the discrete wavelet transform domain. BPNN is implemented for embedding and extracting the message. From the results it is observed that the proposed steganography method can embed the secret message effectively without degrading the quality of cover image.

The rest of this paper is organized as follows: section 2 describes the preliminaries including DWT, radon transform and neural network. Section 4 presents the proposed image steganography approach. The experimental results and performance comparisons are given in section 5. Finally, Section 5 concludes this paper followed by relevant references.

II. Preliminaries

A. Discrete Wavelet Transform (DWT)

Wavelet transforms have become one of the most important and powerful tool of signal representation. Nowadays, it has been used in image processing, data compression, and signal processing. The simplest of DWT is Haar - DWT where the low frequency wavelet coefficients are generated by averaging the two pixel values and high frequency coefficients are generated by taking half of the difference of the same two pixels [10]. For 2D-images, applying DWT will result in the separation of four different bands. LL is the lower resolution approximation of the image. HL is the horizontal, LH is the vertical, HH is the diagonal component. These bands are shown in Figure 1.

LL1	HL1
LH1	HH1

Figure 1.Sub bands of 1 level 2 dimensional Discrete Wavelet Transform

With the DWT, the significant part of the spatial domain image exist in the approximation band that consists of low frequency wavelet coefficients and the edge and texture details usually exist in high frequency sub bands, such as HH, HL, and LH. The secret images are embedded to the High Frequency components as it is difficult for the human eye to detect the existence of secret data.

B. Radon Transform

The Radon transform on an image $f(x,y)$ for a given set of angles can be thought of as computing the projection of the image along the given angles. The resulting projection is the sum of the intensities of the pixels in each direction, i.e. a line integral. The result is a new image $R(\rho, \theta)$.An image can be represented as:

$$r = x\cos\theta + y\sin\theta \tag{1}$$

after which the Radon transform can be written as

$$\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f(x,y)\delta(\rho - x\cos\theta - y\sin\theta)\,dx\,dy \tag{2}$$

where $\delta(\cdot)$ is the Dirac delta function.

C. Back Propagation Neural Network (BPNN)

A neural network represents a highly parallelized dynamic system with a directed graph topology that can receive the output information by means of reaction of its state on the input nodes [11]. The ensembles of interconnected artificial neurons generally organized into layers of fields include neural networks. The behavior of such ensembles varies greatly with changes in architectures as well as neuron signal functions. Artificial neural networks are massively parallel adaptive networks of simple nonlinear computing elements called neurons which are intended to abstract and model some of the functionality of the human nervous system in an attempt to partially capture some of its computational strengths. Neural networks are classified as feed forward and feedback networks. Back propagation network is of feed forward type. In BPNN the errors are back propagated to the input level. The aim of this network is to train the net to achieve the balance between the ability to respond correctly to the input pattern that are used for training and the ability to provide good response to the input that are similar. Back Propagation Neural Network has good nonlinear approximation ability. It can establish the relationship between original wavelet coefficients and stego image coefficients by adjusting the network weights and bias before and after embedding watermark. Owning to the use of neural network, we can extract watermark without the original image and thus reduce the limit in practical applications.

III. Proposed Method

In this section, we explain how proposed system embeds secret information in cover image and how we retrieve secret data from the stego-image. In this method, the use of Back Propagation Neural Network (BPNN) is the key technique. First, a cover image is decomposed into four sub bands using haar wavelet filter. Vertical sub band is selected for embedding. Radon transform is applied on both selected sub band and secret message. The back propagation neural network is implemented to embed and extract the watermark in this method.

A. Information Concealing Algorithm

In the proposed scheme, the host image is decomposed into four sub bands using DWT. Vertical sub band is selected for embedding. Radon transform is applied to secret message and sub band. BPNN is used for embedding and extracting the secret message. The training process is completed before embedding. After getting the coefficients from the stego image, the relationship between the wavelet coefficients and the watermark can be established. The additional information is used to train the neural network to make it sure it must have the capability of memorizing the characteristics of relations between the stego image and the secret message. The hidden layer transfer function considered to be sigmoid, and linear for the output layer. Secret message embedding using BPNN in wavelet domain is shown in Fig.2.

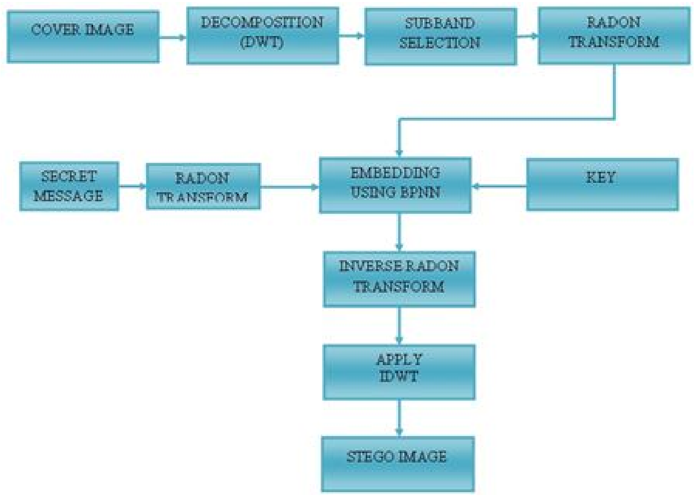

Figure 2. Block diagram of secret message embedding procedure of steganography

Input: An m × n cover image, key and a secret message or image.
Output: An m × n stego-image.
Algorithm:

1. Read the cover image and secret message or image.
2. Apply DWT to decompose the cover image into four sub bands.
3. Select the vertical sub band
4. Apply radon transform to the sub band and secret message.
5. Apply BPNN to embed the secret message
6. Perform Inverse Discrete Wavelet Transform (IDWT) on the output of BPNN.
7. Prepare stego image to display
8. Compute Peak to Signal Noise Ratio between stego image and the cover image

B. Information Extraction Algorithm

In this step extraction of secret message is carried out. The secret message extraction process is the anti-process of message embedding. The trained neural network is used in the extraction process. Secret message extraction procedure using BPNN is shown in Fig.3.

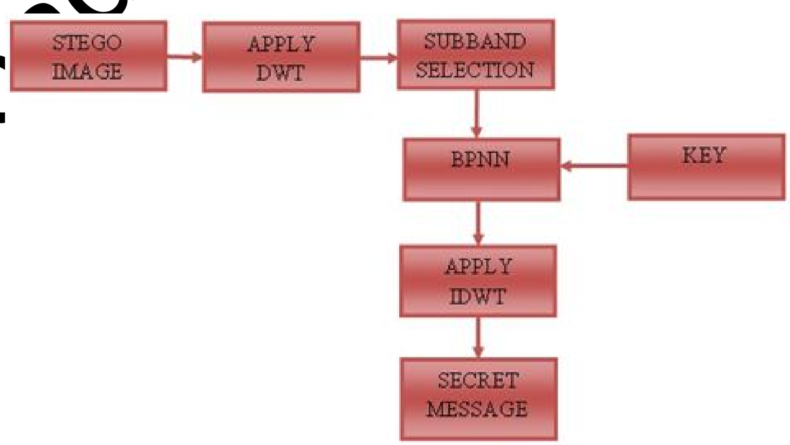

Figure 3. Block diagram of extraction of secret message from a stego object

Input: An m × n stego-image and key.
Output: a secret message or image.
Algorithm:

1. Read the stego image and key
2. Decompose the stego image by using Haar wavelet transform
3. Select the specific sub band
4. Extract the secret message by applying sub band and key as an input to BPNN
5. Prepare secret image to display

IV. Implementation and Measures

MATLAB platform is chosen to develop the above steganography algorithm. In MATLAB software there are extensive libraries and efficient functions of image processing and neural network which is very useful in steganography. Developers may use other programming language also. Peak to Signal Noise Ratio (R) can be used to evaluate the performance of the proposed data hiding scheme.

A. Peak Signal to Noise Ratio (PSNR)

The weighted mean squared error between the cover image and the stego-image can be used as one of the measures to assess the relative perceptibility of the embedded message. Mean square error (MSE) and Peak Signal to Noise Ratio (PSNR) can be used as metrics to measure the degree of imperceptibility.

The PSNR of the watermarked image is calculated using the formula

$$PSNR = 10log_{10}\frac{R*R}{MSE} \quad (3)$$

Where R=256, MSE is defined as:

$$MSE = \sum_{i=1}^{M}\sum_{j=1}^{N}\frac{[I(i,j)-I'(i,j)]^2}{M*N} \quad (4)$$

Where I is the cover image and I' is the stego image. PSNR is measured in Decibels (dB) and the bigger the PSNR value is, the better the message conceals.

V. Result Analysis

In this experiment we used JPEG, PNG and BMP images of various resolutions as cover image. We train a set of 100 images which is randomly taken from web. These images have various memory sizes. The example of opted cover images are as follows:

(a) (b)

Figure.4. (a) Cover images (b) Secret images

Table I. Comparison of PSNR value for different cover and secret images

Cover Image	Secret Image	PSNR
Blue Hills.JPG	horse	36.6977
	taj	37.8191
	tiger	41.26
Flower.JPG	horse	32.3704
	taj	32.6755
	tiger	33.4983
Peppers.PNG	horse	33.7979
	taj	34.2259
	tiger	35.4734
Apple.BMP	horse	34.8935
	taj	35.6777
	tiger	37.4468
Icecream.PNG	horse	32.7179
	taj	33.[illegible]38
	tiger	33.[illegible]354

Table I summarizes the results of proposed steganography method for the images of blue hills, flower, peppers, apple and ice cream. From the above table, we can notice that better results are obtained.

VI. Conclusion

In this paper, a novel steganography algorithm based on radon transform and BPNN in wavelet domain was presented. Wavelet domain is powerful and efficient transform domain than previously used other transforms. The proposed method maintains the prime objective of steganography, which is the secrecy. It has been shown that the stego image preserve the visible quality of the cover image. This approach succeeds to keep intact the original image, after the extraction of embedded secret message. so, this proposed algorithm for steganography can be termed as successful new technique. However for the future work of this technique, we recommend the secret message should be compressed before the hiding process takes place. This is very important because in this way we will reduce the amount of information that is sent, and hence minimizing the chance of degrading the image.

References

1. Chin-Chen Lin,"High capacity data hiding scheme for DCT-based images", Journal of Information Hiding and Multimedia Signal Processing, 1, 2010.
2. N. Wu and M. Hwang. "Data Hiding: Current Status and Key Issues," International Journal of Network Security, Vol.4, No.1, pp. 1-9, Jan.2007.
3. R. Chandramouli and N. Memon, "Analysis of LSB based image steganography techniques," in Proc. ICIP, Oct. 2001.
4. Ajit Danti and Preethi Achary," Randomized embedding scheme based on DCT coefficients for image steganography", IJCA Special Issue on Recent Trends in Image Processing and Pattern Recognition, 2010
5. Ali Al-Ataby and Fawzi Al-Naima," A modified high capacity image steganography technique based on wavelet transform", The International Arab Journal of Information Technology, 7:358–364, 2010.

6. M Anjunatha, H S. and Raja K B," High Capacity and Security Steganography using Discrete Wavelet Transform", International Journal of Computer Science and Security (IJCSS), 3: Issue (6), 2010.
7. V. Kumar and D. Kumar," Performance evaluation of DWT based image steganography. In Proceedings of Advance Computing Conference (IACC)", 2010 IEEE 2nd International, pages 223–228, 2010.
8. Bibi Isac and V. Santhi, "A Study on Digital Image and Video Watermarking Schemes using Neural Networks‖, International Jounal of Computer Applications, Vol. 12, No. 9, Jan 2011.
9. W. Chen, "A Comparative Study of Information Hiding Schernes Using Amplitude, Frequency, and Phase Embedding," PhD Thesis, National Cheng Kung University, Tainan, Taiwan, May 2003.
10. Liu Shaohui, Yao Hongxun and GAO Wen "Neural Network based Steganalysis in Still Images" Proceedings of IEEE ICME 2003.
11. Shadrokh samavi, Vajiheh Sabeti,Mojtaba Mahadevi and Shahram Shirani "Steganalysis of embedding in difference of image pixel pairs by neural network", Journal of ISecure, volume 1, pages 17-26, January 2009.