Volume 4, Issue 8, August 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

# Comparitive Study of Information Hiding Techniques

**Snehlata[1], Mr. Sachin Majithia[2]**
[1]Department of Information Technology, Chandigarh Engineering College
[2]Department of Information Technology, Chandigarh Engineering College
India

***Abstract-To provides security to the image data from an un-authorized access so that the quality of image remains the same with good invisibility. This paper proposed an enhanced combination technique of using DCT and Neural Network together as that from previously implemented technique. The challenge is to make sending of hidden information untraceable by elaborating the concept of Artificial Neural Network as it provide many alternatives and other applications which can play an important role in today's computer science field.***

***Keywords-Steganography, Discrete Cosines Transform (DCT), Least Significant bit (LSB), Discrete Wavelet Transform (DWT), and Neural Network (NN).***

## I. INTRODUCTION

As the definition says Steganography [3] is a method of secret communication, that hides the existence of hidden message, but with the development of internet technologies the transmission of message over the internet is still facing a security problems. So, therefore in order to protect the secrecy of message during the transmission various Steganographic techniques [6] have been implemented. Some of them are Discrete Cosines Transform, Least Significant bit, Discrete Wavelet Transform, also Neural Network which plays a significant role to solve the specific problems that are phases during transmission.

## II. LEAST SIGNIFICANT BIT

Least significant bit(LSB) generally a Steganographic technique that may be employed to embed data into variety of digital media, but the most important application or factor of using LSB is embedding that is used to hide one image inside another. The technique works by replacing some of the information in a given pixel with information from the data in the image. The LSB embedding allow large amount of data to be embedded without observable changes.

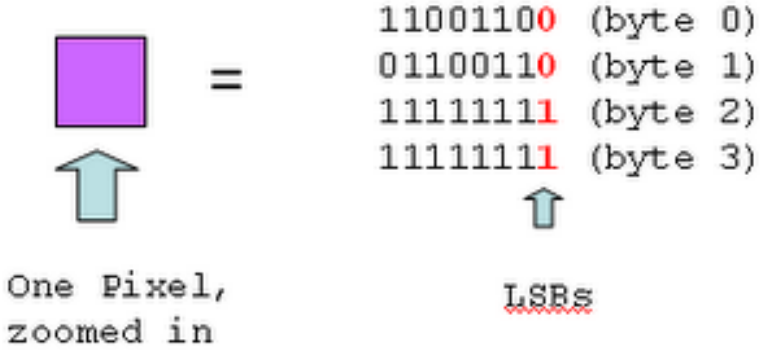


Figure 1: LSB Embedding

### 2.1 DETECTION

Detection [1, 2] of LSB embeddings is done through two types of attacks. The first is a simple visual attack, which relies on the human eye to evaluate an image. The second is a statistical attack, which analyzes images in a statistical manner.

***A) Visual Attack***-A visual attack is the simplest way of trying to detect an embedding. It is particularly effective against LSB embeddings, but it is useless against more advanced algorithms that do not embed into the pixels of the image directly like Jsteg. A visual attack begins by looking at the image as a whole. If an embedding is detected through colour abnormalities the Steganographic algorithm has been successfully attacked. If an embedding is not detected by the observer, the bit planes of the image are then examined, beginning with the least significant plane.

***B) Statistical Attack***-Statistical attacks on LSB embeddings are much more effective than a visual attack. Statistical attacks make use of the relationship between bit-planes in an image or the relationship between pixels within a bit-plane to determine if a message is embedded into an image. Statistical attacks are typically tuned to work against a particular embedding algorithm.

 

## III. DISCRETE COUSINE TRANSFORM

DCT [10] helps separate the image into its parts (or spectral sub bands) of differing importance (w.r.t image visual quality). The general equation of a 2D (N by M image), DCT is defined as

$$S(u,v) = \frac{2}{N}C(u)C(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}s(x,y)\cos\left(\frac{\pi u(2x+1)}{2N}\right)\cos\left(\frac{\pi v(2y+1)}{2N}\right)$$

For JPEG, the 2-d that is DCT-II of N*N blocks are computed and the results are quantised and entropy coded .Here, N is typically 8 and the DCT-II is applied to each row and column of the block. In DCT block lower frequency coefficients are at upper left positions and high frequency coefficients are lower right positions. Low frequency coefficients are of larger value than high frequency coefficients. An example of a 8×8 block of DCT coefficient.

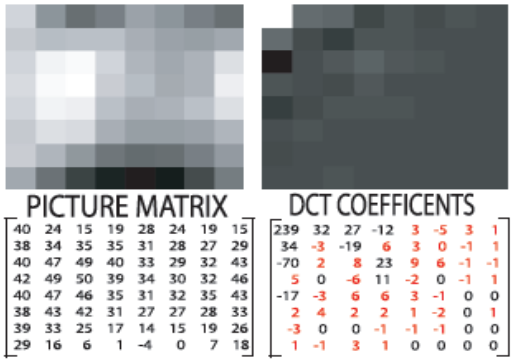


Figure 2: DCT Coefficient

## IV. DISCRETE WAVELET TRANSFORM

In this transform, time domain is passed through low-pass and high-pass filters to extract low and high frequencies respectively. This process is repeated for several times and each time a section of the signal is drawn out. DWT [7] analysis divides signal into two classes (i.e. Approximation and Detail) by signal decomposition for various frequency bands and scales. DWT [4, 7] utilizes two function sets: scaling and wavelet which associate with low and high pass filters orderly. Such a decomposition manner bisects time separability. In other words, only half of the samples in a signal are sufficient to represent the whole signal, doubling the frequency separability.

Here the Haar DWT - simplest type of DWT has been applied. In 1D-DWT average of fine details in small area is recorded.

In case of 2D-DWT we perform one step of the transform on all rows. The left side of the matrix contains down sampled low pass coefficients of each row; the right side contains the high pass coefficients as shown in the figure

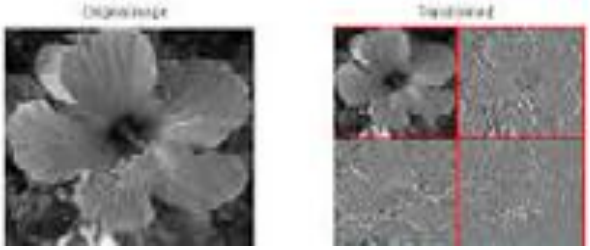

Figure 3: Haar DWT

## V. NEURAL NETWORK

An Artificial Neural Network [5] is a computing system or a information processing system. It is composed of a large number of highly interconnected processing elements (neurons) working in unison to solve specific problems. Neural networks take a different approach to problem solving than that of conventional computers. Conventional computers use an algorithmic approach i.e. the computer follows a set of instructions in order to solve a problem.

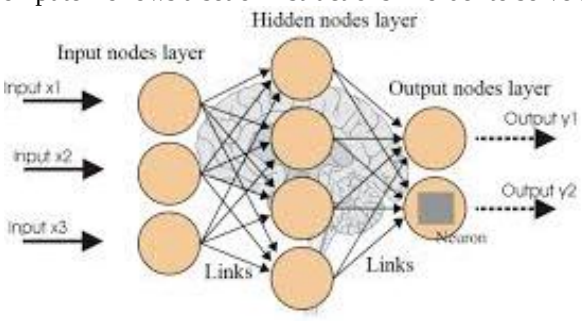


Figure 4: Neural Network

 

There are various applications of neural network which are as follows:-

1) Secret Key protocol-. Both partners begin with their own private key. The communicating networks transmit information between one another using a public protocol, until arriving at a common secret key generated by common transformations. This key is then used for both encryption and decryption of the communicated data

2) Visual Cryptography-Visual cryptography is an approach aimed at the secure transfer of visual secrets across a public network.

3) Pseudo Random Number Generator-A pseudo random number generator may be created to take advantage of the properties of Multi-Layer Preceptor (MLP) neural networks [8, 9]. Neural networks possess powerful generalization capabilities which allow them to produce reasonable outputs to complex problems after being trained on several well known input vectors.

4) Steganalysis-. Neural networks are then used in order to classify images according to whether or not they contain hidden information.

## VI. PROPOSED METHOD

In this section, we will describe how the proposed method hides the image having messaged in it that is by applying DCT and Neural Network both by which the origin of the image remains the same as that of previous image showing good invisibility to the users.

The steps included are:-

1. Select the image, key, message.
2. Frequency Transformation of content-which means DCT, is applied on each block of image.
3. Selection of feature sub block-i.e. the image is broken into block of pixels.
4. Use feature values as input value for neural network.
5. Generation of classifier.

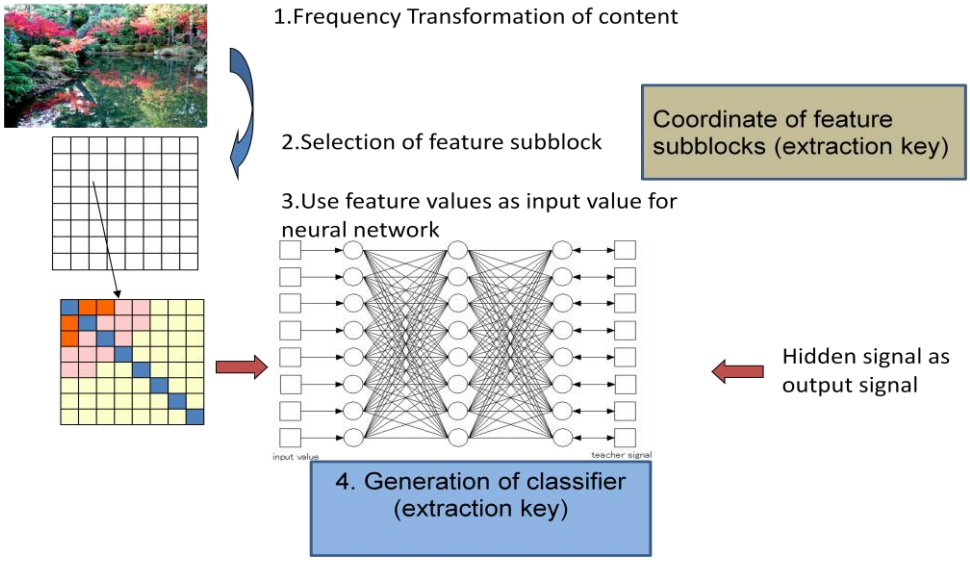


Figure 5: Information hiding process for image

## VII. RESULT ANALYSIS

In this paper we have used DCT technique combination with Neural Network for the image which are in jpeg or bmp format. Following are the some images which are showing different resolution for different techniques. The result of using DCT and NN together are found enhancing.

Figure 6: original image

 

Table 1: Comparision of Different Technique

| **Previous Technique** | | | **Our Technique** |
|---|---|---|---|
| **LSB** | **DCT** | **DWT** | **DCT+NN** |
|  |  |  |  |

## VIII. CONCLUSION

The papers suggested how a selection of different techniques for the image increases the chances of hiding the data or information in much securing and effective ways. From the result it is clear that the use of DCT and NN together reduces the chances of detection of secret message and also provide security for the image as from the previous implemented techniques and from this process the quality of the image remained same as that of original image.

## REFERENCES

[1] Fridrich, J., Goljan, M., & Du, R. (2001). Reliable detection of LSB steganography in color and grayscale images. *Proceedings of the 2001 workshop on Multimedia and security new challenges - MM&Sec '01, 27*. New York, New York, USA: ACM Press. doi:10.1145/1232454.1232466

[2] Provos, N. (2001). Detecting steganographic content on the internet. *Ann Arbor*. Retrieved from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Detecting+Steganographic+Content+on+the+Internet#0

[3] Beenish Mehboob and Rashid Aziz Faruqui, "A Steganography Implementation", IEEE -4244-2427-6/08/$20.00 ©2008

[4] Po-Yueh Chen and Hung-Ju Lin, "A DWT Based Approach for Image Steganography",International Journal of Applied Science and Engineering 4, 3: 275-290, 2006.

[5] J. Benitez, and J. L. Castro, and I. Requena, "Are artificial neural networks black boxes?" IEEE Trans. Neural Networks, vol. 8, no. 5, pp.1156-1164, Sept. 1997.

[6] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for Data Hiding", I.B.M. Systems Journal, 35(3-4): pp.313-336, 1996

[7] Emy V Yoyak, PG Scholar, Jaya Engineering College, Thiruvallur, India, "Three Level Discrete Wavelet Transform Based Image Steganography", International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 4, April – 2013

[8] G. C. Meletiou, D. K. Tasoulis, and M. N. Vrahatis, "A first study of the neural network approach in problems related to cryptography," in Proc. of the FEES conf. on Financial Engineering, E-commerce & Supply Chain, and Strategies of Development, 2002.

[9] W. Kinzel, and I. Kanter, "Neural Cryptography," in Proc. 9th In1'l Conf. on Neural Information Processing (ICONIP'02), vol. 3, pp. 1351-1354, 2002

[10] Zhiping Zhou and Maomao Hui, "Steganalysis for Markov Feature of Difference Array in DCT Domain", Proceedings of Sixth International Conference on Fuzzy Systems and Knowledge Discovery, pp. 581- 584 , Aug. 2009.

[11] Eldon Y. Li,1994;ANN and their business Application, Information and Management, Volume 27,Issue 5,Pages 303-313.

 