International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 3, Issue 11, November 2014 **ISSN 2319 - 4847**

Improved Protection in Image Steganography using Neural Network and Discrete Cosine Transform

Lovepreet Kaur[1] , Geetanjali Babbar[2]

[1]M.Tech Student, Department of Computer Science, CEC, Landran.Punjab (India)

[2]Assistant Professor, Department of Computer Science, CEC, Landran.Punjab (India)

ABSTRACT

The important concern of modern communication is to establish secret communication and is achieved by steganography. It comes under the assumption that if the feature is visible, the point of attack is evident, thus the all time goal is to conceal the very existence of the embedded data. Many techniques have been suggested to hide data but security is one of the major challenges. In the proposed method this issue has been addressed using Discrete Cosine Transform (DCT) and neural network. Using Discrete Cosine Transform (DCT), input image is divided into blocks and is processed to generate quantization matrix of cover and stego images. The neural network is trained using LSB bit value. On the basis of training and segmentation done, neural network provide efficient positions where data can be merge. Experiments demonstrate that the proposed approach gives better PSNR and MSE value.

Keywords:- Steganography, least significant bit, discrete cosine transform, segmentation, quantization matrix, neural network.

1. INTRODUCTION

Information security is essential for confidential data transfer. Steganography is one of the ways used for secure transmission of confidential information. Steganography is the art of hiding information imperceptibly in a cover medium. The word “Steganography” is of Greek origin and means “covered or hidden writing” .The main purpose of steganography is to convey the information secretly by concealing the very existence of information in some other medium such as image, audio or video. The content used to embed information is called as cover object. The cover along with the hidden information is called as stego-object. The cover image containing the secret message is then transferred to the recipient. The recipient is able to extract the message with the help of retrieving process and secret key provided by the sender. In this paper color image is taken as cover. Secret message is embedded in the cover image to get stego image. The major objective of steganography is to prevent some unintended observer from stealing or destroying the confidential information. Steganography techniques are getting significantly more sophisticated and have been widely used. The Steganography techniques are the perfect supplement for encryption that allows a user to hide large amounts of information within an image. There are some factors to be considered when designing a steganography system:

- Invisibility: Invisibility is the ability to be unnoticed by the human.
- Security: Even if an attacker realizes the existence of the information in the stego object it should be impossible for the attacker to detect the information. The closer the stego image to the cover image, the higher the security. Quality factor can enhance the security of image.
- Capacity: The amount of information that can be hidden relative to the size of the cover object without deteriorating the quality of the cover object.
- Robustness: It is the ability of system to cope with errors during the time of execution.

1.1 Motivation

The motivation behind implementing image steganography method according to its use in various organizations to communicate between its member as well as members of military or intelligence operatives or agents of companies use this for communication between them to hide secret messages or in the field of espionage. To avoid drawing attention to the transmission of hidden message is the goal of steganography. If suspicion is raised then this goal that has been considered to achieve the security of the secret message, because if the hackers notice any change in the sent message then the observer will try to know the concealed information inside the message. In the steganography scenario, before the hiding process, the sender must select the appropriate carrier object and select the effective secret messages as well as the robust password (which is only supposed to known by the receiver).

1.2 Techniques Used

1.2.1 Least Significant Bit

Least significant bit (LSB) insertion is the most widely used technique for image embedding. This method became very popular due to its easy implementation. It embeds data in a cover image by replacing the least significant bits (LSB) of cover image with most significant bits (MSB) of message image.

The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message. Pixel: (01101001 11010100 11010001)
(11001000 01011100 11101001)
(00100111 11001001 11101001)
From the above grid the LSB of each byte represents the red, green, blue color, suppose to embed numeric value '15' (00001111), the matrix will be modified as,
(01101000 11010100 11010000)
(11001000 01011101 11101001)
(00100111 11001001 11101001)
The above matrix shows that it needs only 3 bits to be modified to embed numeric value '15' successfully. Since the resulting changes are too small, it is difficult for the human eye to recognize the changes.

1.2.1 Discrete Cosine Transform

The DCT transforms a signal from an image representation into a frequency representation, by grouping the pixels into 8 × 8 pixel blocks. These mathematical transforms convert the pixels in such a way as to give the effect of "spreading" the location of the pixel values over part of the image. The redundant bits selected to embed the hidden data are taken from the least-significant bits of the quantized DCT coefficients. Thus the smoothening of the pixel alteration is virtually impossible for human visual detection.

1.3 Neural Network

Neural network mimics some features of a real nervous system that contains a collection of basic computing units called neurons. These are the basic signalling units of the nervous system. Each neuron is a discrete cell whose several processes arise from its cell body. These neurons were represented as models of biological networks into conceptual components for circuits that could perform computational tasks. The basic model of the neuron is founded upon the functionality of a biological neuron.

Feed Forward Neural Network
A feed forward network provides input to the next layer with no closed chain of dependence among neural states through a set of connection strengths or weights. Feed-forward neural network allow signals to travel in 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.
Back Propagation Neural Network
It requires a dataset of the desired output for many inputs, making up the training set. The term is an abbreviation for "backward propagation of errors".

1.4 Computational Parameters Used:

1.4.1 PSNR

Peak signal-to-noise ratio, often abbreviated PSNR, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. The PSNR of the steganography result defined as follows:

$$PSNR = 10log \frac{MAX^2}{\sqrt{MSE}}$$

Where MAX is the maximum value of the pixels and higher the value of the PSNR, better the performance of the steganography algorithm. High PSNR value indicates high security because it indicates minimum difference between the original and stego values. So no one can suspect the hidden information.

1.4.2 MSE

(a) The mean squared error measures the average of the square of the error. The error is the amount by which the estimator differs from the quantity to be estimated.

$$MSE = \frac{1}{MN}\sum_{m=1}^{M}\sum_{n=1}^{N}(I_1(m,n) - I_0(m,n))^2$$

Where I_1 and I_0 are the values of cover image and stego image and M and N are image dimensions. Smaller the value of the MSE, better the performance of the proposed algorithm.

2. LITERTURE SURVEY

Hemalatha et al. [1] proposed a novel image steganography technique to hide multiple secret images and keys in color cover image using Integer Wavelet Transform (IWT). The strength of proposed technique lies in secrecy of parameters that are transmitted separately. Without knowledge of these parameters it is not possible to extract the hidden secret image from given stego image. There is no visual difference between the stego image and the cover image. The extracted secret images are also similar to the original secret images. Very good PSNR (Peak Signal to Noise Ratio) values are obtained for both stego and extracted secret images. The results are compared with the results of other techniques, where single image is hidden. Attalla et al. [2] proposed a new method in image steganography with improved image quality. The proposed method hides the secret message based on searching about the identical bits between the secret messages and image pixels values. The proposed method is compared with the LSB benchmarking method. The results of the proposed and LSB hiding methods are discussed and analyzed based on the ratio between the number of the identical and the non identical bits between the pixel colour values and the secret message values. The proposed method is efficient, simple and fast, robust to attack and improve the image quality. Shamim et al. [4] proposed a technique in which an image is the most common type of digital media used for steganography. Digital images often have a large amount of redundant data and for this reason it is possible to hide message inside image file. To a computer, an image is a collection of numbers that constitute different light intensities in different areas of the image. This technique called compression makes use of some mathematical concepts to reduce the image data, resulting in smaller file sizes and plays a vital role in image based steganography methods. Image formats can mainly be divided into two categories based on compression, lossy and lossless. Both methods save storage space but have different results. Lossy compression (e.g. JPEG format) attains a high level of compression and thus saves more space but in doing so, the bits may be altered largely and the originality of the image may be affect. Khare et al. [6] proposed a system that will allow an average user to securely transfer text messages by hiding them in a digital image file using the local characteristics within an image. The project is a combination of steganography and encryption algorithms, which provides a strong backbone for its security. The proposed system not only hides large volume of data within an image, but also limits the perceivable distortion that might occur in an image while processing if. The software has an advantage over other information security software because the hidden text is in the form of images, which are not obvious text information carriers. The project contains several challenges that make it interesting to develop. The main advantage of the project is a simple, powerful and user-friendly GUI that plays a very large role in the success of the application.

3. PROPOSED METHOD

The proposed method uses the discrete cosine transform and neural network. Using the discrete cosine transform the color image i.e. used as cover image is processed to generate the quantization matrix and then neural network is trained using LSB bits value estimation and then on the basis of training and segmentation done neural network provide efficient positions to merge data. Then extraction is performed in the same way. Algorithms used for proposed work are:

A. The embedding process

For embedding process, the color image is taken as cover image. The embedding algorithm is shown as follows:

Embedding Algorithm
1. Read cover Image.
2. Read hidden message.
3. For every carrier image selected from image pool, image pool is the buffer of various images.
4. Firstly binarization of image will be done then apply DCT to the selected image.
5. After DCT application, generate quantization matrix for the purpose of the image compression.
6. Values will be saved in table of quantization.
7. Now calculate LSB bit.
8. There are no. of LSB bits.
9. Now choose that bit that has to be replaced with the binary bits of message.
10. Then replace the bit.

11. Now find out image size.
12. If image size is optimum then select image to be stego image.

The graphical representation of algorithm is shown in figure 1:

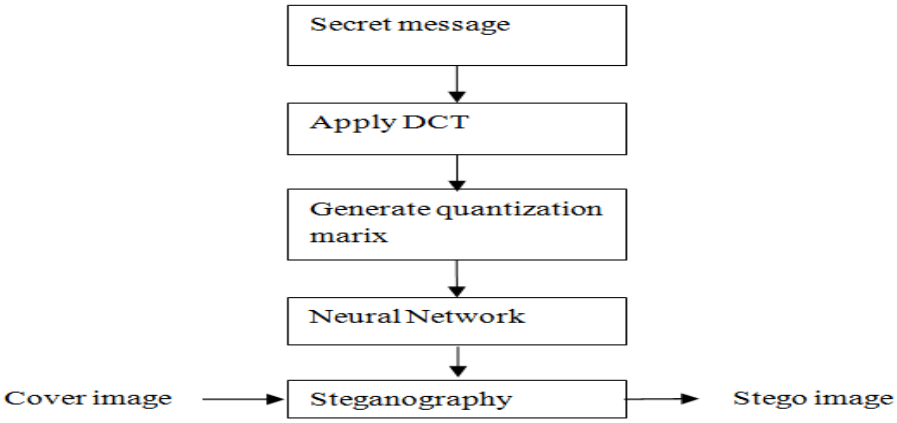


Figure 1: Block diagram of Embedding Process.

B. The extracting process

The extracting algorithm is shown as follows:

Extracting algorithm:

1. Read stego image.
2. Find the traverse image.
3. Then check matrix value.
4. If value of matrix matches the mask pattern then, extract LSB.
5. If value of matrix does not match the mask pattern then move forward.
6. Now on finding matrix value, apply LSB.
7. Now merging of image takes place.
8. If merging of image is done accurately.
9. Call Neural Network.
10. Neural network has basically three layers, input, hidden and output layer. Now output layer gets the value on the account of input value. If error occurred at output then check input values and change accordingly.
11. Extraction of hidden message takes place finally.

The graphical representation of algorithm is shown in figure 2:

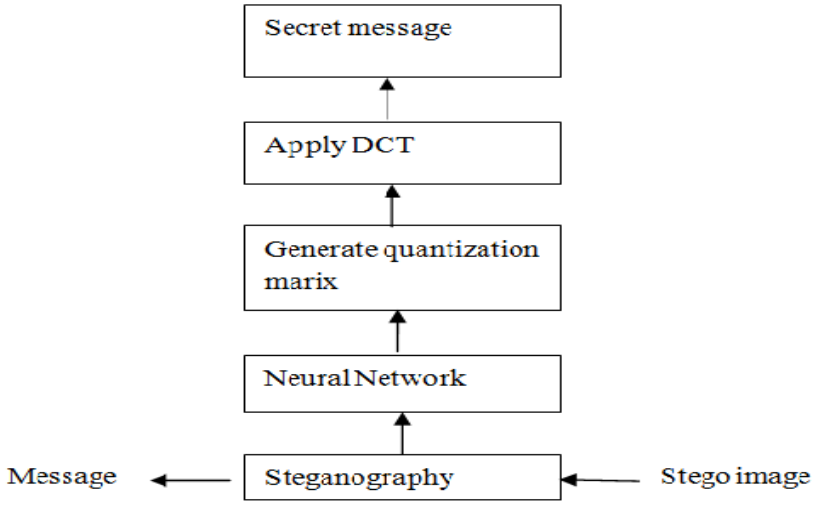


Figure 2: Block diagram of Extracting Process.

4. RESULTS AND DISCUSSIONS

To see performance of the proposed algorithm images of jpg format has been used and are executed on MATLAB. The color images which are desert and jellyfish are used as a cover images. The images shown in the figure 3 (a) cover image of desert (b) stego image of desert and figure 4 shows the cover and stego image of jellyfish.

(a) (b)

Figure 3: (a) cover image 'desert' (b) stego image 'desert'

(a) (b)

Figure 4: (a) cover image 'jellyfish' (b) stego image 'jellyfish'

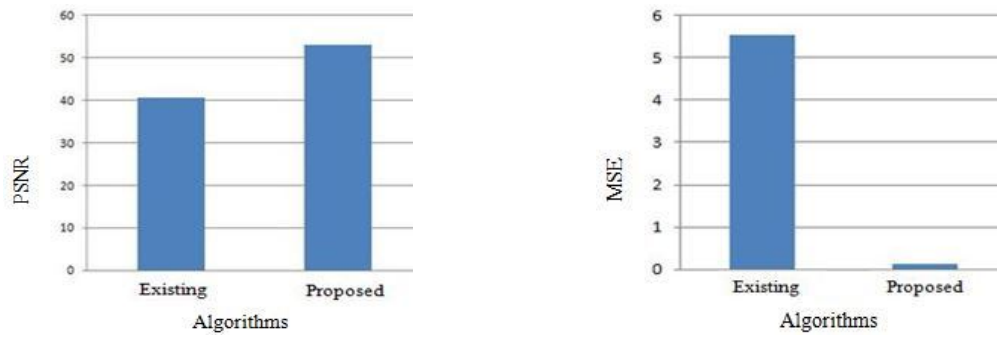
The PSNR and MSE using proposed method is a very good improvement as compared to the existing technique.

Table 1.1: Comparison table of the steganography techniques using parameters with the existing values.

Image name	**Previous value of PSNR**	**Proposed value of PSNR**
Desert	40.67	**53.16**
Jelly Fish	39.39	**46.72**
Image name	**Previous value of MSE**	**Proposed value of MSE**
Desert	5.56	**0.04**
Jelly Fish	7.46	**0.19**

4.1 Graphical Representation

The figure 5 shows the comparison of the proposed algorithm to the existing algorithm. Here, PSNR shows higher value and MSE shows the lower value by applying proposed algorithm.



(a) PSNR graph (b) MSE graph

Figure 5: PSNR and MSE graph of desert image

6. CONCLUSION

Image Steganography is an emerging and one of the most important areas of research. It is emerging in its peak because it does not attract anyone by itself. Compared with previous works, proposed method uses the Discrete Cosine Transform and quantization matrix based approach using neural network to embed and extract the data successfully. Experiments demonstrate that the proposed algorithm give results better. As the image quality metrics i.e. higher Peak Signal to Noise Ratio (PSNR) and lower Mean Square Error (MSE) itself are proving that the proposed technique for steganography is good one.

REFERENCES

[1] Hemalatha S., U. Dinesh Acharya, A. Renuka, and Priya R. Kamath., "A Secure and High capacity Image Steganography Technique." Signal & Image Processing: An International Journal (SIPIJ), vol.4, no.1, pp. 83-89, 2013.

[2] Attalla M., Shatnawi A., "A New Method in Image Steganography with Improved Image Quality", Applied Mathematical Sciences, vol. 6, no. 79, pp.3907 – 3915, 2012.

[3] Mahajan, Manish, and Navdeep Kaur, "Adaptive Steganography: A Survey of Recent Statistical Aware Steganography Techniques." International Journal of Computer Network and Information Security (IJCNIS), vol.4, no.10, 2012.

[4] Shamim Ahmed Laskar and Kattamanchi Hemachandran, "High Capacity Data Hiding using LSB Steganography and Encryption", International Journal of Database Management Systems (IJDMS) vol.4, no.6, 2012.

[5] Wu, H.C., Wu, N.I. and Hwang, M.S., "Image steganographic scheme based on pixel-value differencing and LSB replacement methods", IEEE Processing-Vision. Image Signal Processing, vol. 152, no. 5, pp. 611-615, 2005.

[6] Akhil Khare, Meenu Kumara, Pallavi Khare, "Efficient Algorithm for Digital Image Steganography" Journal of Information, Knowledge and Research in Computer Science and Applications, vol. 1, issue 1, pp.1-5, 2010.

[7] Cheddad, Abbas, Joan Condell, Kevin Curran, and Paul Mc Kevitt., "Digital image steganography: Survey and analysis of current methods." Signal processing 90, no. 3, pp. 727-752, 2010.

[8] Mamta Juneja, "Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption", Proceedings of the International Conference on Advances in Recent Technologies in Communication and Computing, pp. 203-209, 2009.

[9] Younes, Mohammed Ali Bani, and Aman Jantan., "A New Steganography Approach for Images Encryption Exchange by Using the Least Significant Bit Insertion." International Journal of computer science and network security, no. 6, pp: 247-257, 2008.

[10] Eggers, Joachim J., Robert Baeuml, and Bernd Girod., "Communications approach to Image Steganography.", International Society for Optics and Photonics, pp.26-37, 2002.