Implementation and Analysis of Information Hiding Techniques Using DCT and Neural Network

Snehlata
Student, Department of Information Technology CEC,
Landran, India
Snehsoni31@gmail.com

Sachin Majithia
Assistant Professor IT
CEC, Landran
sachinmajithia@gmail.com

Abstract--Hiding Messages in image data, which is generally known as Steganography is used for both illegal and legal scenarios. Here the proposed technique used in this paper is combination of DCT and Neural Network with feed forward back propagation techniques, which generate a Stego-image which has immune against conventional attacks and perform good perceptibility as compared to other steganography approaches. This paper provides a new technique for hiding large amount of secret messages in image by which the quality of image is maintained with good invisibility. The analysis shows improved performance from other technique by using parameter PSNR and MSE which reduces the chances of error and enhances security measures.

Index Terms *-Cover image, Stego image, Discrete Cosine Transform (DCT), Neural Networks (NN), Data Hiding.*

*****

I. INTRODUCTION

In today's world of modern scenarios, many tools and devices can be used which has ability to transmit information from one place to another place, but the data is increasing at rapid speed not only in size but also in variety. So, coming across with these growing data there comes a challenge and difficulties to handle such large amount of data.However,safety and security of long-distance communication is anotherimportant consideration.

So, to achieve these goals, here we have two different types of technique, one is cryptography and another is steganography .Cryptography main aspect is that it is a technique which is used for securing the confidentiality of communication and many different approaches have been used to encrypt and decrypt the data in order to maintain the privacy of the data during transmission or any other tasks.

Whereas steganography[1]differ from cryptography, as cryptography focus on keeping the concept of message secret where steganography is used for ”covered writing”[10] i.e. the information is hidden exclusively in image. There are basically three main components of steganography which are: the key, the carrier, the message. Steganography Technique Involved in Image Processing

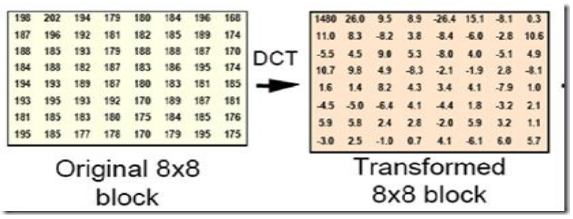
Different Steganography Techniques can be described as:

1.1 *Spatial Domain Based Steganography:* An LSB (Least significant Bit) stenographic [9] technique which is used to hide the message in the LSB (in other words, the 8th bit) of the pixel values without involving any perceptible distortions/errors. Also this technique provides more hiding capacity.

Pixels :(10101111 11101001 10101000)
(10100111 01011000 11101001)
(11011000 10000111 01011001)
Secret Message: 01001001
Result :(10101111 11101001 10101000)
(10100110 01011001 11101000)
(11011000 10000111 01011001)

1.2 *Transform Domain Based Steganography:*It is a more complex way of hiding information's into the image i.e. transforming an image into its frequency domain. For this various algorithm and transformation have been used to hide the information. The main advantage of this technique is that it can hide information in areas of images that are less exposed to compression, cropping and image processing.

1.3 *The Discrete Cosine Transform (DCT):* It helps to separate the image into parts (i.e. expresses the location of pixels values over the part of image)of differing importance. An another important approach used by steganography, as image is broken into 8*8 blocks pixels, and work from left to right and from top to bottom, and the results are quantised [2]and the message is embedded in DCT coefficient[11].



198	202	194	179	180	184	196	168
187	196	192	181	182	185	189	174
188	185	193	179	188	188	187	170
184	188	182	187	183	186	195	174
194	193	189	187	180	183	181	185
193	195	193	192	170	189	187	181
181	185	183	180	175	184	185	176
195	185	177	178	170	179	195	175

1480	26.0	9.5	8.9	-26.4	15.1	-8.1	0.3
11.0	8.3	-8.2	3.8	-8.4	-6.0	-2.8	10.6
-5.5	4.5	9.8	5.3	-8.0	4.0	-5.1	4.9
10.7	9.8	4.9	-8.3	-2.1	-1.9	2.8	-8.1
1.6	1.4	8.2	4.3	3.4	4.1	-7.9	1.0
-4.5	-5.0	-6.4	4.1	-4.4	1.8	-3.2	2.1
5.9	5.8	2.4	2.8	-2.0	5.9	3.2	1.1
-3.0	2.5	-1.0	0.7	4.1	-6.1	6.0	5.7

Figure 1:- DCT Block Transformation

1.4 *Neural Network (NN):* It is a computing system operates via flow of the signals. They are typically organized in form of layers and these layers are made up of highly interconnected nodes which contain an 'activation function'.

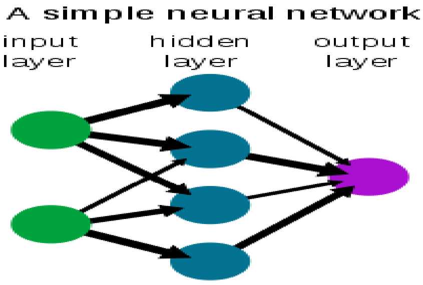


Figure 2:- Neural Network

They works well for capturing association of discovering regularities within a set of patterns, her patterns are presented to network[8] through the 'input layer' which communicates to one or more 'hidden layers' where the processing is done through the system of weighted 'connection'. Back propagation Algorithm is used with NN to apply training patterns, adjustments to the weights and for the back propagation of the associated errors.

II. RELATED WORK

1. In [4],Shaohui et al. describe an ANN model designed for steganalysis applied to still images. The features they use for the input to their ANN are spectral measures of discrete cosine transform (DCT) and the Discrete Fourier transforms (DFT) and four moments of the wavelet transform. The ANN they use is a three layers, 2-output, feed forward network with simple Backpropogation for training. They manually set the number of nodes for the one hidden layer and use a straight forward, time-consuming Backpropogation training algorithm. Their ANN detects only data embedded using the quantization index modulation method [3] and authors do not give the data format they used.

2. Marwaha et al. [5] have proposed an advanced system of encrypting data that combines the features of cryptography, steganography along with the multimedia data hiding. This system will be more secure than any other these techniques alone and also as compared to steganography and cryptography combined system.

3. Usha B A1, Dr. N K Srinth2, Dr N K Canvery in May 2013 proposed a Data Embedding Technique using neural Network. According to them the neural approach to embed information satisfies a secure steganography. Neural approach adds the complexity for the hacker accessing and also presents high potentiality in defence operations. Neural Steganography is a powerful tool that enables people to communicate with possible eavesdroppers even knowing there is a form of communication. [6]

4. Hideki Noda et al [7] the JPEG compression using the DCT (Discrete Cosine Transform) is still the most common compression standard for still Images.QIM (Quantization Index Modulation) is applied in DCT Domain. DCT based stenographic technique are immune to Histogram based attack.2HM-JPEG (Histogram Matching JPEG) steganography method is also present along with QIM-JPEG steganography. In these two methods embedding of secret message takes place during quantization of DCT coefficient only, no by modifying quantized DCT coefficient.

5."Ross J. Anderson, Fabien A.P. Petitcolas"[8] On the Limits of Steganography IEEE Journal of Selected Areas in Communications, 16(4):474-481, May 1998. Talks about the limits of steganography. They say that limits of steganography theory and practice. We started off by outlining a number of techniques both ancient and modern, together with attacks on them (some new); we then discussed a number of possible approaches to a theory of the subject. We pointed out the difficulties that stand in the way of a theory of perfect covertness" with the same power as Shannon's theory of perfect secrecy some of few researchers have already implemented NEURAL NETWORK in their approach for the same.

III. PROPOSED WORK

The practising of hiding information has a long history. The problem with existing technique like DCT, DWT and LSB is that they are limited only to small size image for hiding information which adds complexity to the image showing redundant errors (MSE) and noisy pixels.

This Dissertation proposed a sophisticated approach for protecting the hidden data in Stego image by using parameter PSNR and MSE and they are compared among existence technique of steganography. The results that are evaluated are found to be encouraging showing high performance with security and good invisibility to image, using Quantization table which generates reconstructed image almost identical to source image.

IV. METHODOLOGY

4.1 *Implementation Setup:-*

In order to hide the message also providing security, steganography system involves using DCT [11] with secret key. This key is used for encrypting and decrypting the secret message from the image i.e. by authorised user only. Firstly, insertion or in other words embedding of secret message is done into the image. The steps included are:

- Read the cover image having secret message and convert that message into binary.
- The image is now broken into 8*8 blocks of pixels and DCT on each block for transforming image from spatial domain to frequency domain.
- Calculate LSB of each DC coefficient and replace with each bit of secret message.
- Save the image which is now the Stego image.

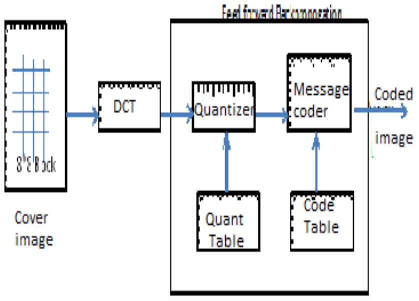


Figure 3:- DCT Based Encoder.

Extracting the message:

- Stego image is given.
- Apply the secret key i.e. the private key to decode the Stego image.
- Similarly, DCT is applied on each block of pixels
- Extract the message from the Stego image.

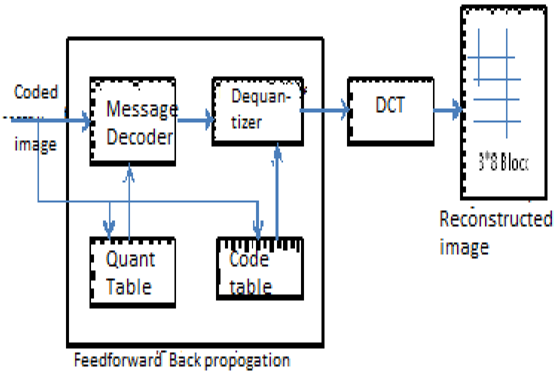


Figure 3:- DCT Based Decoder

4.2 *Methodology Used:-*

(i) *System Parameter*-The process is conducted using Intel i5 32bit processor with 4GB RAM and experimented algorithm that we perform is coded in Mat lab.

(ii) *Experimental Factors*-Following are the evaluation parameters that have been considered for performance analysis:

- *PSNR (Peak Signal to Noise Ratio)*-It is the ratio of maximum possible power of corrupting noise that affects the fidelity of its representation.

$$\text{PSNR} = \frac{20 \log_{10} 256}{\sqrt{MSE}}$$

- *MSE (Mean Square Error)*-Defined as the square of the error between the cover image and Stego image,i.e. the distortion in the image can be measured using MSE.

$$\text{MSE} = \sum_{i=1}^{all\ pixels} \qquad \sum_{j=1}^{all\ pixels} \frac{\left(cov\,(i,j)-steg\,(i,j)\right)^2}{N*N}$$

V. IMPLEMENTATION RESULTS

The result we obtained is after we embedded the message in original image showing high capacity i.e. the cover image and we obtained a Stego image. Using PSNR as Evaluation parameter our proposed work's results for different images is shown below:-

TABLE II: ANALYSIS OF DIFFERENT SCHEMES

S.No.	**Technique**	**Size of Images**	**PSNR value(db)**
1.	DWT	256*256	25.4
2.	DCT	256*256	40.6
3.	LSB	256*256	51.5
4.	DCT+NN (our work)	1024*768	67.2

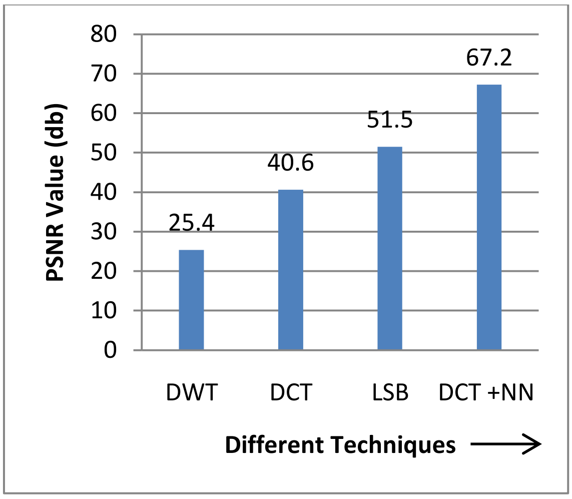


Figure 5:-Analysis of PSNR Value of different technique

Also, Using MSE as Evaluation parameter our proposed work's results for different images are shown below:-

TABLE II: ANALYSIS OF DIFFERENT SCHEMES

S.No.	Technique	Size of Images	MSE
1.	DWT	256*256	9.7820
2.	DCT	256*256	5.5684
3.	LSB	256*256	0.5035
4.	DCT+NN (our work)	1024*768	0.0121

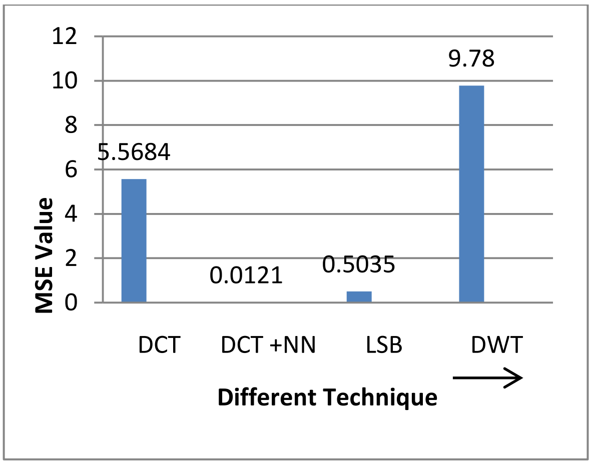


Figure 6:- Analysis of MSE Value of different technique

VI. CONCLUSION AND FUTURE WORK

We come across many literature reviews on different types of technique for protecting our documents and they have their own advantages and disadvantages. But no technique is capable for all types of applications. Several parameters have been considered to hide information and their approximate value is calculated which enhances the level of security. By which the outcome values provide good quality image with high capacity and invisibility to the user as compared to other recent approaches.

As the research in the field of steganography is an ongoing process. So, for future work it will be more desirable to use standard tools and technique in more sophisticated manner. In order to make an effective result the use of Neural Networks can be used as they have ability to extract or analysis the pattern and detect the trends that are too complex to ne noticed by human or by computer.

VII. REFERENCES

[1] "Ross J. Anderson, Fabien A.P. Petitcolas" On The Limits of Steganography IEEE Journal of Selected Areas in Communications, 16(4):474-481, May 1998. Talks about the limits of steganography . They say that limits of steganography theory and practice.

[2] "Adel Almohammad Robert M. Hierons" High Capacity Steganography Method Based Upon JPEG The Third International Conference on Availability, Reliability and Security The JPEG standard uses 8x8 quantization tables, but it does not specify default or standard values for quantization tables.

[3] B.Chen and G.W.Wornell,"Quantization Index Modulation: a class of provably good methods for Digital Watermarking And Information Embedding"IEEE Trans. on Information Theory,Vol.47,pp.1423-1443,May 2001.

[4] L.Shauhui,4.Hongxun and G.Wen"Neural Network nasedsteganalysis in still images",Proc.Internatinal Conference on Multimedia and Expo,ICME 2003,Vol.2,pp.509-512,2003.

[5] Marwaha P. and Marwaha P."VISUAL CRYPTOGRAPHIC STEGANOGRAPHY IN IMAGES" second Internal conference on Computing, Communication and Networking Technologies, Pages(s):1-6,IEEE 2010.

[6] "Usha B A1,Dr. N K Srinath 2,Dr. N K Cauvey"DATA EMBEDDING TECHIQUE IN IMAGE STEGANOGRAPHY USING NEURAL NETWORKS International Journal of Advanced Research in Computer and Communication Engineering Vol.2,Issues 5,May 2013.

[7] "Ross J. Anderson, Fabien A.P. Petitcolas" On The Limits of Steganography IEEE Journal of Selected Areas in Communications, 16(4):474-481, May 1998.

[8] " Ms. P. T. Anitha1, Dr. M. Rajaram2 ,Dr. S. N. Sivanandham" AN EFFICIENT NEURAL NETWORK BASED ALGORITHM FOR DETECTING STEGANOGRAPHY CONTENT IN CORPORATE MAILS: A WEB BASED STEGANALYSIS IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 3, No 1, May 2012.

[9] SuhailaAbd Halim and Muhammad Faiz Abdulla Sani,"Embedding Using Spread Spectrum Image Streganography with GF" Proceedings of thr 6th IMT-GT Conference on Mathematics,Statistics and its Application(ICMSA2010).

[10] Moerland, T ,"Steganograhy and Steganalysis",leiden Institute of Advanced Computing Science.www.liacs.nl/home/tmoerl/privtet.pdf.

H.-W. Tseng and C.-C.Chang,"Steganography using JPEG-Compressed images",The Fourth International Conference on Computer and Information Tecchnology,CIT'04,14-16 September 2004,pp.12-17.ss