

# A Secure Image Steganography Using DCT and Neural Network

Monika Babbar, Harpreet Kaur

Doaba Institute of Engineering and Technology.

Doaba Institute of Engineering and Technology,

## ABSTRACT

Steganography is an important area of research in recent years involving a number of applications. It is the science of embedding information into the cover image viz., text, video, and image (payload) without causing statistically significant modification to the cover image. The modern secure image steganography presents a challenging task of transferring the embedded information to the destination without being detected. In this paper we present an image based steganography that, Discrete Cosine Transform(DCT), and Neural Network (NN) on raw images to enhance the security. The whole simulation has taken place in MATLAB environment.

**KEYWORDS:** Steganography, DCT, Neural Network, MATLAB, MSE, BER

## I. INTRODUCTION

Steganography is the art of covered or hidden writing. The purpose of steganography is covert communication to hide a message from a third party. This differs from cryptography, the art of secret writing, which is intended to make a message unreadable by a third party but does not hide the existence of the secret communication. Although steganography is separate and distinct from cryptography, there are many analogies between the two, and some authors categorize steganography as a form of cryptography since hidden communication is a form of secret writing (Bauer 2002). Nevertheless, this paper will treat steganography as a separate field.

Although the term steganography was only coined at the end of the 15th century, the use of steganography dates back several millennia. In ancient times, messages were hidden on the back of wax writing tables, written on the stomachs of rabbits, or tattooed on the scalp of slaves. Invisible ink has been in use for centuries-for fun by children and students and for serious espionage by spies and terrorists. Microdots and microfilm, a staple of war and spy movies, came about after the invention of photography (Arnold et al. 2003; Johnson et al. 2001; Kahn 1996; Wayner 2002). Steganography hides the covert message but not the fact that two parties are communicating with each other. The steganography process generally involves placing a hidden message in some transport medium, called the carrier. The secret message is embedded in the carrier to form the steganography medium. The use of a steganography key may be employed for encryption of the hidden message and/or for randomization in the steganography scheme.

This paper is organized as Section II will discuss about DCT, Section III will show the proposed algorithm, Section IV will show the proposed flowchart, Section V will evaluate experimental results and Finally Section VI will discuss the conclusion.

## II. DISCRETE COSINE TRANSFORM

$y = \text{dct}(x)$  returns the unitary discrete cosine transform of  $x$ ,

$$y(k) = w(k) \sum_{n=1}^N x(n) \cos\left(\frac{\pi}{2N}(2n-1)(k-1)\right),$$

$$k = 1, 2, 3, \dots, N$$

Where

$$w(k) = \begin{cases} \frac{1}{\sqrt{N}}, & k = 1 \\ \sqrt{\frac{2}{N}}, & 2 \leq k \leq N, \end{cases}$$

$N$  is the length of  $x$ , and  $x$  and  $y$  are the same size. If  $x$  is a matrix,  $\text{dct}$  transforms its columns. The series is indexed from  $n = 1$  and  $k = 1$  instead of the usual  $n = 0$  and  $k = 0$  because MATLAB<sup>®</sup> vectors run from 1 to  $N$  instead of from 0 to  $N - 1$ .

$y = \text{dct}(x, n)$  pads or truncates  $x$  to length  $n$  before transforming.

The DCT is closely related to the discrete Fourier transform. You can often reconstruct a sequence very accurately from only a few DCT coefficients, a useful property for applications requiring data reduction.

### **III. PROPOSED SYSTEM**

#### **1. Embedding algorithm**

##### **a. Cover Image Transformation**

The transform is applied on the cover image of size 512 X 512

##### **b. Block division and energy calculation of transformed cover image**

The cover image is divided into 16 non-overlapping blocks of size 128\*128 and the energy of each block is calculated.

##### **c. Message image normalization and transformation**

The message image is normalized by dividing each pixel of the image by 255 to reduce the embedding error. The transform is then applied to the image

##### **d. Embedding secret normalized and transformed image**

The message images are then embedded into 8 lower energy blocks of the cover and each of the message planes are embedded into the corresponding cover planes i.e. red message plane into red cover plane and so on

##### **e. Obtaining Stego image by taking inverse transform on modified cover image**

The inverse transform is applied on the cover image. The new image obtained is the Stego image.

#### **2. Extraction Algorithm**

##### **a. Extraction of message using BPA**

- b. Finally get secret message.

### 3. Flowchart

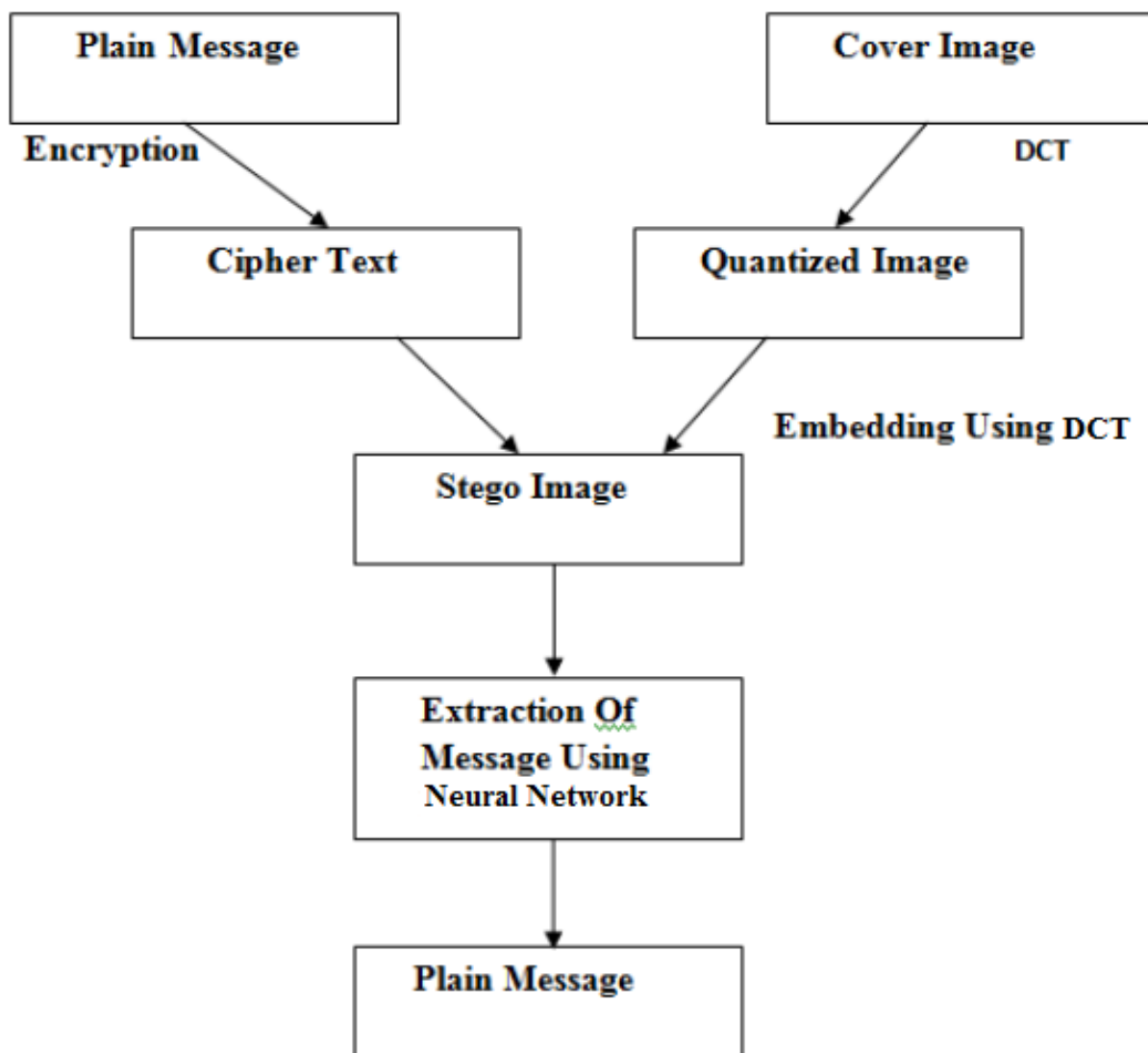


Fig:1

#### IV. EXPERIMENTAL RESULTS

##### i) PSNR (Peak Signal To Noise Ratio):

Term for ratio between Maximum Possible power of signal and power of corrupting noise . R is maximum fluctuation in input image data type. More PSNR means more image quality and less distortion of secret message.

$$PSNR = 10 \cdot \log_{10} \left( \frac{MAX_i^2}{MSE} \right)$$

##### ii) MSE (Mean Square Error)

It is means to quantify difference between values implied by an estimator and true values to quantify. I1 means original image, I2 resultant

image and N are number of rows and columns in input image.

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

Image	PSNR	MSE
Lena	67.46	0.89
Peppers	50.75	0.77
Koala	60.35	0.67
baboon	69.39	0.88

Table 1

## V. CONCLUSION AND FUTURE SCOPE

This research paper presented the work that has been implemented to enhance the Steganography technique so that the quality of the image remains the same. Using DCT for 32\*32 blocks and Neural Network for extraction offers better results. It is concluded that managing the pixels to a deeper level increases the capacity of the image to hide certain messages. The Neural Network has been found effective enough to find pixels to extract the data bits with least affecting the original pattern of the image. Our proposed method offers better PSNR, MSE values, so results offer better image quality and better way of hiding messages. It has been also concluded that if we can encrypt the data up to some level before merging it to the image, it may enhance the chances of security while image embedding.

Future scope lies in the use of the technique for videos or noisy images.

## REFERENCES

- [1] Singla D., "Data Security using LSB and DCT Steganography in images", IEEE International Conference ISSN-2332-1545 Vol 8, 2013
- [2] Usha B.A ,Srinath N.K "Data Embedding Technique in Image Steganography using neural network ,IJARCCE - Vol. 2,Issue 5, 2013
- [3] Goel and Rana .A "Comparison Of Steganography Techniques" International Journal of Computers and Distributed Systems ISSN: 2278-5183, pp 20-31, 2013
- [4] Kumar A, Sharma R, "A Secure Steganography Based On RSA Algorithm and Hash-LSB Technique" IJARCSSE, ISSN: 2277, 2013
- [5] Deepali, "Steganography with data integrity" International Journal Of computational engineering research (IJCER) ,pp. 190-193,2012
- [6] Jbara. H, Kiah.L "Increased Capacity of image based Steganography using artificial neural network" American Institute Of Physics (AIP) Proc. 1482,

International Conference on Fundamental and Applied Science , pp. 20-25.,2012

[7] Karim S., Rahman M , “New Approach for LSB Based Image Steganography using Secret Key” IEEE Proceedings of 14th international Conference On

Computer and Information Technology(ICCIT) ,pp 286-291,2011

[8] Chang, Chen .T “ A Steganography Method Based Upon JPEG And Quantization Table Modification” Information Science – An International Journal, pp 12-14,2002