A DCT-Based Robust Methodology for Image Steganography

[1]Stuti Goel, [2]Arun Rana, [3]Manpreet Kaur
Dept. of E&C, Doon Valley Institute of Engg. & Technology, Karnal, Haryana, India

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, a DCT based robust methodology has been designed. The cover image is segmented into 8*8 blocks and DCT is applied on the image. The text to be hidden is embedded in the diagonal elements of the blocks by substituting a random variable in place of the bits of the text to be embedded. It is observed that the proposed algorithm is more robust with better CER & Normalized coefficient.

Keywords
Least Significant Bit (LSB), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Steganography, MSE, PSNR, NC

I. Introduction

Therapid growth of internet usage over high bandwidth and low cost computer hardware has propelled the explosive growth of steganography [1]. In the present year, secure and hidden communication is the foremost requirement of the people. Therefore steganography is gaining attraction by people due to the security issues over internet. Steganography means covert writing. Steganography has evolved into a digital strategy of hiding a file in some form of multimedia, such as an image, an audio file or even a video file [8]. The objective of steganography is hiding the payload (embedded information) into the cover image such that the existence of payload in the cover image is imperceptible to the human beings [14]. There are different techniques to implement steganography namely Least Significant Bit (LSB), Discrete Cosine Transform (DCT) & Discrete Wavelet Transform (DWT) technique.

There are two types of domains in which steganography is implemented i.e. spatial domain & frequency domain [6]. In spatial domain, processing is applied directly on the pixel values of the image whereas in frequency domain, pixel values are transformed and then processing is applied on the transformed coefficients. LSB technique is implemented in spatial domain while DCT & DWT technique are implemented in frequency domain. In Least Significant Bit (LSB), each pixel of an image is transformed into the binary value and data is hidden into the least significant position of the binary value of the pixels of the image in such a manner that, it doesn't destroy the integrity of the cover image but this scheme is sensitive to a variety of image processing attacks like compression, cropping etc.

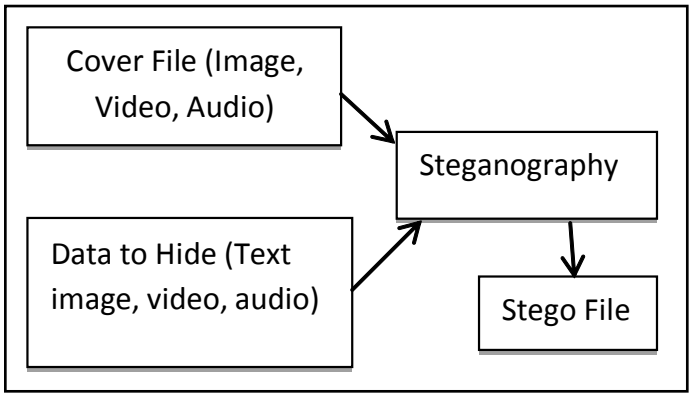


Fig. 1: The Process of Hiding Data

The Discrete Cosine Transforms (DCT) & Discrete Wavelet Transform (DWT) are mathematical function that transforms digital image data from the spatial to the frequency domain. In DCT, after transforming the image in frequency domain, the data is embedded in the least significant bits of the medium frequency components and is specified for lossy compression while In DWT, secret messages are embedded in the high frequency coefficients resulted from Discrete Wavelet Transform and provide maximum robustness.

II. Literature Survey

J.R.Krenn explained steganography and its implementation techniques [1]. Deshpande Neeta, et. al. proposed the Least Significant Bit embedding technique suggests that data can be hidden in the least significant bits of the cover image and the human eye would be unable to notice the hidden image in the cover file. This paper explains the LSB embedding technique and presents the evaluation results for 2, 4, 6 Least significant bits for a .png file and a .bmp file [2]. K.B.Raja, et. al. proposed a challenging task of transferring the embedded information to the destination without being detected. In this paper, the image based steganography that combines Least Significant Bit (LSB), Discrete Cosine Transform (DCT), and compression techniques on raw images to enhance the security of the payload [3]. Vijay Kumar Sharma, et. al. has worked upon a new steganography algorithm for 8bit (gray scale) or 24bit (color image) based on Logical operation to ensure the security against the steganalysis attack [4]. Po-Yueh Chen, et. al. proposed a new steganography technique which embeds the secret messages in frequency domain. According to different users' demands on the embedding capacity and image quality, the proposed algorithm is divided into two modes and 5 cases [5]. Chen Ming, et. al. focused on the steganography tools algorithms. Based on the analyses of the algorithms, various tools are divided into five categories: (1). Spatial domain based steganography tools; (2). Transform domain based steganography tools; (3). Document based steganography tools; (4) File structure based Steganography tools; (5) other categories, e.g. video compress encoding and spread spectrum technique based [6]. Aneesh Jain, et. al. proposed a scheme which hides data in bitmap images, in a way that there is almost no perceptible difference between the original image and this new image and which is also resistant to

JPEG compression [7]. Beenish Mehboob, et. al. discusses the art and science of Steganography in general and proposes a novel technique to hide data in a colorful image using least significant bit [8]. Hassan Mathkour, et. al. seta a criteria to analyze and evaluate the strengths and weaknesses of the presented techniques and a more robust steganography technique has been developed that takes advantages of the strengths and avoids the limitations [9]. NageswaraRaoThota, et. al. attempted to implement basic JPEG compression using only basic MATLAB functions [10]. MamtaJuneja, et. al. discusses the design of a Robust image steganography technique based on LSB (Least Significant Bit) insertion and RSA encryption technique[11]. K.B.Shiva Kumar, et. al. discusses the important issue of modern communication is establishing secret communication while using public channel and is achieved by steganography. In this paper, Coherent Steganography Technique using Segmentation and Discrete Cosine Transform (CSSDCT) is proposed. The cover image is divided into 8*8 blocks and DCT is applied on each block. The number of payload MSB bits is embedded into DCT coefficients of the cover image coherently based on the values of DCT coefficients. It is observed that the proposed algorithm has better PSNR, Security and capacity compared to the existing techniques [12]. Dr. Ekta Walia, et. al. presents analysis of Least Significant Bit (LSB) based Steganography and Discrete Cosine Transform (DCT) based Steganography [13]. K Suresh Babu, et. al. proposed an image Steganography that can verify the reliability of the information being transmitted to the receiver. The method can verify whether the attacker has tried to edit, delete or forge the secret information in the stego-image [14].Atalla I. Hashad, et. al. describe the LSB insertion technique, the Discrete Cosine Transform (DCT) insertion technique is described and finally we will propose a new technique that uses the idea of inserting a bit in the spatial domain combined with the DCT insertion technique[15]. Arvind Kumar, et. al. discusses how digital images can be used as a carrier to hide Messages and also analyses the performance of some of the steganography tools [16]. Vijay Kumar, et. al. intends to observe the effect of embedding the secret message in different bands such as CH, CV and CD on the performance of stego image in terms of Peak Signal to Noise Ratio (PSNR). Experimentation has been done using six different attacks. Experimental results reveal that the error block replacement with diagonal detail coefficients (CD) gives better PSNR than doing so with other coefficients [17]. Ali Al-Ataby, et. al .proposed a modified high-capacity image steganography technique that depends on wavelet transform with acceptable levels of imperceptibility and distortion in the cover image and high level of overall security [18]. T. Narasimmalou, et. al. Proposed an optimal discrete wavelet transform (DWT) based steganography. Experiments show that the peak signal noise ratio (PSNR) generated by the proposed method is better [19]. NedaRaftari, et. al. proposed a novel image steganography technique that combines the Integer Wavelet Transform (IWT) and Discrete Cosine Transform (DCT) is proposed which embeds secret image in frequency domain of cover image with high matching quality [20].

III. Methods of Concealing Data in Digital Image

Steganography is used for covert communication. The secret image which is communicated to the destination is embedded into the cover image to derive the stego image. In this section evaluation parameters and proposed embedding and retrieval techniques are discussed.

A. Least Significant Bit Substitution Technique (LSB)

In LSB steganography, the least significant bits of the cover media's digital data are used to conceal the message. The simplest of the LSB steganography techniques is LSB replacement. LSB replacement steganography flips the last bit of each of the data values to reflect the message that needs to be hidden. Consider an 8-bitgrayscale bitmap image where each pixel is stored as a byte representing a gray scale value. Suppose the first eight pixels of the original image have the following gray scale values [4]:

11010010
01001010
10010111
10001100
00010101
01010111
00100110
01000011

To hide the letter C whose binary value is 10000011, we would replace the LSBs of these pixels to have the following new gray scale values:

11010011
01001010
10010110
10001100
00010100
01010110
00100111
01000011

Note that, on average, only half the LSBs need to change. The difference between the cover (i.e. original) image and the stego image will be hardly noticeable to the human eye.

However, one of its major limitations is small size of data which can be embedded in such type of images using only LSB. LSB is extremely vulnerable to attacks. LSB techniques implemented to 24 bit formats are difficult to detect contrary to 8 bit format [8].

Another example of LSB technique is: Consider a grid for 3 pixels of a 24-bit image and the number 300 is to be embedded using LSB technique. The resulting grid is as follows:

PIXELS: (01010101 01011100 11011000)
(10110110 11111100 00110100)
(11011110 10110010 10110101)

C: 10000011

(01010101 01011100 11011000)
(10110110 11111100 00110100)
(11011111 10110011 10110101)

Here the number C was embedded into the first 8 bytes of the grid, only the 2 bits needed to be changed according to the embedded message .On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size.

B. Discrete Cosine Transform Technique (DCT)

DCT coefficients are used for JPEG compression [10, 12]. It separates the image into parts of differing importance. It transforms a signal or image from the spatial domain to the frequency domain. It can separate the image into high, middle and low frequency components.

In low frequency sub-band, much of the signal energy lies at low frequency which contains most important visual parts of the image

while in high frequency sub-band, high frequency components of the image are usually removed through compression and noise attacks [13]. So the secret message is embedded by modifying the coefficients of the middle frequency sub-band, so that the visibility of the image will not be affected. The general equation for a 1D (N data items) DCT is defined by the following equation: [12]

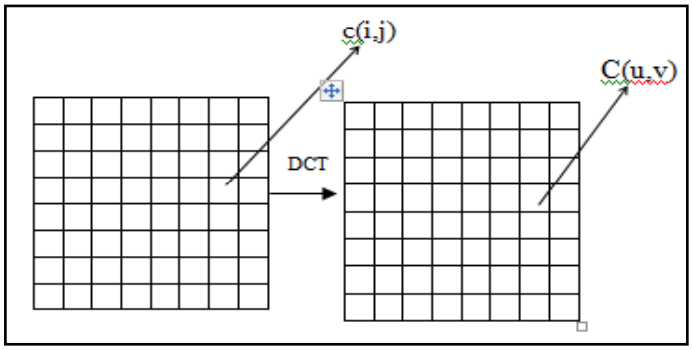


Fig. 1: Discrete Cosine Transform of an Image

$$C(u) = a(u) \sum_{i=0}^{N-1} x_i \cos\left(\frac{(2i+1)u\pi}{2N}\right)$$

Where u= 0, 1, 2….. N-1

The general equation for a 2D (N by M image) DCT is defined by the following equation: [12]

$$C(u,v = a(v) \sum_{i=0}^{N-1} [\, a(u) \sum_{i=0}^{N-1} x_i \cos\left(\frac{(2i+1)u\pi}{2N}\right)]$$

$$\times \cos\left(\frac{(2i+1)v\pi}{2N}\right)$$

Where u , v = 0,1,2….N-1

Here, the input image is of size N X M. c (i, j) is the intensity of the pixel in row i and column j; C (u, v) is the DCT coefficient in row u and column v of the DCT matrix.

DCT is used in steganography as [10]- Image is broken into 8×8 blocks of pixels.

Working from left to right, top to bottom, DCT is applied to each block.

Each block is compressed through quantization table to scale the DCT coefficients and message is embedded in DCT coefficients.

C. Discrete Wavelet Transform Technique (DWT) [5]

The frequency domain transform we applied in this research is Haar-DWT, the simplest DWT [18-19]. A 2-dimensional Haar-DWT consists of two operations: One is the horizontal operation and the other is the vertical one. Detailed procedures of a 2-D Haar-DWT are described as follows:

Step 1: At first, scan the pixels from left to right in horizontal direction. Then, perform the addition and subtraction operations on neighboring pixels. Store the sum on the left

and the difference on the right as illustrated in fig. 3. Repeat this operation until all the rows are processed. The pixel sums represent the low frequency part (denoted as symbol L) while the pixel differences represent the high frequency part of the original image (denoted as symbol H).

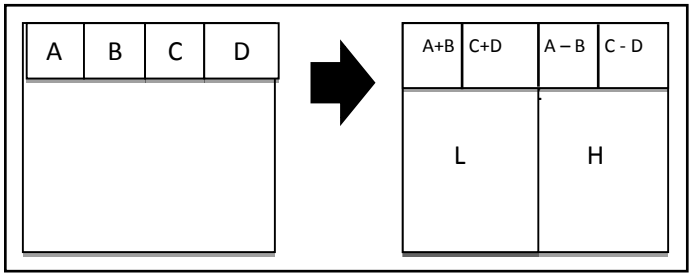


Fig. 2: The Horizontal Operation on First Row

Step 2: Secondly, scan the pixels from top to bottom in vertical direction. Perform the addition and subtraction operations on neighboring pixels and then store the sum on the top and the difference on the bottom as illustrated in fig. 4. Repeat this operation until all the columns are processed. Finally we will obtain 4 sub-bands denoted as LL, HL, LH, and HH respectively. The LL sub-band is the low frequency portion and hence looks very similar to the original image. The whole procedure described is called the first-order 2-D Haar-DWT.

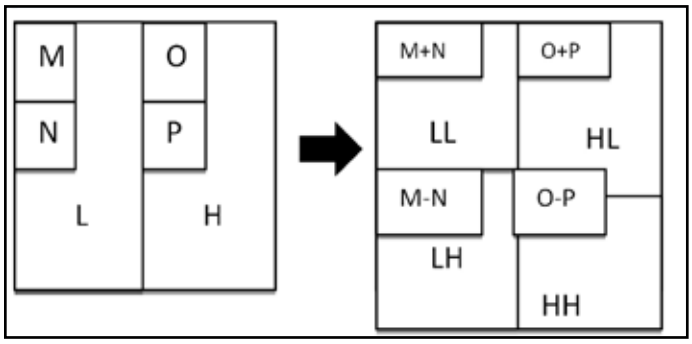


Fig. 3: The Vertical Operation

D. DCT-Based Robust Image Steganography

The Steganography has to guarantee these four requirements i.e. robustness, undetectability, perceptual transparency and security.. From literature review, it is revealed that the LSB based technique provides good picture quality for all types of images like gray scale or color image as compare to the frequency domain techniques. DCT based Steganography scheme works perfectly with minimal distortion of the image quality in comparison to LSB based Steganography. Even though the amount of secret data that can be hidden by using this technique is smaller as compared to LSB based Steganography, DCT based Steganography scheme is being recommended by us as it ensures minimum distortion of image quality. LSB insertion is more vulnerable to even the most harmless and usual transformations whereas, In DWT Based Steganography, coefficients in the low frequency sub-band could be preserved unaltered for improving the image quality. This is due to the different characteristics of DWT coefficients in different sub-bands. Since the most essential portion (the low frequency part) remains unchanged, when the secret messages are embedded in the high frequency sub-bands corresponding to the edges portion of the original image, PSNR is being recommended.

Therefore we are looking for a robust embedding method .In order to find one; a measure of robustness must be defined. An embedding method may be considered robust if the embedded message can be extracted after an image has been manipulated without being distorted.The embedding algorithm must be tested against the different types of attacks (Gaussian noise have been used in this dissertation) in order to determine how much an image can be manipulated before the message is destroyed. If we want to

hide a large message inside an image, we cannot ensure at the same time absolute undetectability and large robustness. On the other hand, if robustness to large distortion is an issue, the message that can be reliably hidden should not be too long. Based on the same embedding capacity, our proposed method improves both image quality in terms of PSNR and CER (Character Error Rate.)

VI. Algorithm of Steganography

A. LSB Based Steganography

Algorithm to embed text message:-
Step 1: Read the cover image and text message which is to be hidden in the cover image.
Step 2: Convert text message in binary.
Step 3: Calculate LSB of each pixels of cover image.
Step 4: Replace LSB of cover image with each bit of secret message one by one.
Step 5: Write stego image
Step 6: Calculate the Mean square Error (MSE), Peak Signal to Noise Ratio (PSNR) of the stego image.

Algorithm to retrieve text message:-
Step 1: Read the stego image.
Step 2: Calculate LSB of each pixels of stego image.
Step 3: Retrieve bits and convert each 8 bit into character.

B. DCT Based Steganography

Algorithm to embed text message:-
Step 1: Read cover image.
Step 2: Read secret message and convert it in binary.
Step 3: The cover image is broken into 8×8 block of pixels.
Step 4: Working from left to right, top to bottom subtract 128 in each block of pixels.
Step 5: DCT is applied to each block.
Step 6: Each block is compressed through quantization table.
Step 7: Calculate LSB of each DC coefficient and replace with each bit of secret message.
Step 8: Write stego image.
Step 9: Calculate the Mean square Error (MSE), Peak Signal to Noise Ratio (PSNR) of the stego image.

Algorithm to retrieve text message:-
Step 1: Read stego image.
Step 2: Stego image is broken into 8×8 block of pixels.
Step 3: Working from left to right, top to bottom subtract 128 in each block of pixels.
Step 4: DCT is applied to each block.
Step 5: Each block is compressed through quantization table.
Step 6: Calculate LSB of each DC coefficient.
Step 7: Retrieve and convert each 8 bit into character.

C. DWT Based Steganography

Algorithm to embed text message:-
Step 1: Read the cover image and text message which is to be hidden in the cover image.
Step 2: Convert the text message into binary. Apply 2D-Haar transform on the cover image.
Step 3: Obtain the horizontal and vertical filtering coefficients of the cover image. Cover image is added with data bits for DWT coefficients.
Step 4: Obtain stego image.
Step 5: Calculate the Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR) of the stego image.

Algorithm to retrieve text message:-
Step 1: Read the stego image.
Step 2: Obtain the horizontal and vertical filtering coefficients of the cover image. Extract the message bit by bit and recomposing the cover image.
Step 4: Convert the data into message vector. Compare it with original message.

D. Proposed Robust Image Based Steganography

Algorithm to embed text message:-
Step 1: Read the cover image and text message which is to be hidden in the cover image.
Step 2: Convert text message in binary.
Step 3: Obtain a block from the image and check either block_Num is equal to zero 0 or Tot_Bit is equal to 1.
Step 4: Now if block_Num is not equal to zero and Tot_Bit is not equal to one. Compute the DCT of 8*8 blocks and as per data bit i.e. 0 and 1.
Step 5: Select two strength random variables K_1 and K_2. Add the value of main diagonal of DCT's AC co-efficient with either K_1 or K_2 depending upon data bits.
Step 6: Read next data bit and obtain next block from the image.
Step 7: If Block_Num=M*N/8*8 or Tot_Bit=1, then Message has been Embedded successfully.
Step 8: Obtain the Stego Image.
Step 9: Calculate the Mean Square Error and Peak Signal to Noise Ratio (PSNR) of the Stego image and Calculatepercentage of the error occurred in the recovered data in terms of CER.
Step 10: Calculate the effect of noise (such as Gaussian noise) by varying the variance on the recovered data in terms of CER.

Algorithm to retrieve text message:-
Step 1: Obtain Stego Image and random variables K_1 and K_2.
Step 2: Read a block from the Stego Image and obtain its 8*8 DCT. Compute the Correlation between the off main diagonal DCT's with both K_1 and K_2.
Step 3: If Correlation (off main diagonal DCT, K1 of the blocks is greater than Correlation (off main diagonal DCT, K_2 of the block, then the message bit is 1 or else 0. Similarly get the data bits of all the 8*8 blocks of stego image. Convert the data bits to message vector 'M'. Compare it with the original message vector 'M'. The Average value of PSNR in the proposed system of Steganography algorithm is 50dB and its CER is 100 percent. This is more Robust than the Spatial and Frequency domain Steganography techniques.

V. Evaluation of Image Quality

For comparing stego image with cover results requires a measure of image quality, commonly used measures are Mean-Squared Error, Peak Signal-to-Noise Ratio and capacity.

A. Mean-Squared Error

The Mean-Squared Error (MSE) between two images I1(m, n) and I2(m, n) is[2]:

$$MSE = \frac{\sum_{M,N}[I1(m,n) - I2(M,N)]^2}{M * N}$$

M and N are the number of rows and columns in the input images, respectively.

B. Peak Signal-to-Noise Ratio

Peak Signal-to-Noise Ratio (PSNR) avoids this problem by scaling the MSE according to the image range [5]:

$$PSNR = 10 \log_{10} \frac{256^2}{MSE}$$

PSNR is measured in decibels (dB). PSNR is a good measure for comparing restoration results for the same image.

C. Capacity

It is the size of the data in a cover image that can be modified without deteriorating the integrity of the cover image. The steganography embedding operation needs to preserve the statistical properties of the cover image in addition to its perceptual quality. Therefore capacity depends on total number of bits per pixel & number of bits embedded in each pixel. Capacity is represented by bits per pixel (bpp) and the Maximum Hiding Capacity (MHC) in terms of percentage [13].

D. Domain Type (DOM)

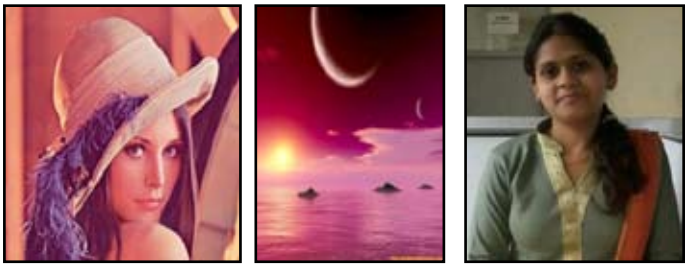
DOM is either Spatial(S) or Transform (T). The techniques that use transform domain hide information in significant areas of the cover images and may be more complex for attackers.

E. Normalized Coefficient (NC)

Correlation is one of the best methods to evaluate the degree of closeness between the two functions. This measure can be used to determine the extent to which the original image and stego image remain close to each other, even after embedding the data.

VI. Results and Discussion

In this section, experimental results are discussed and presented for the evaluation of steganography robustness.Comparative analysis of LSB based, DCT based & DWT based steganography has been done on basis of parameters like PSNR, MSE, CER, NC, Robustness & Capacity on different images and the results are evaluated. Gaussian noise attacks are applied on the three steganography algorithm discussed previously. Figure 6.1 shows the three sample images which are used in the comparison. These are: "LENA" (552120 bytes), "VIEW" (1440000 bytes) and "STUTI" (337689 bytes).The Results of the "STUTI" (337689 bytes) image is shown for all the Steganography algorithms.

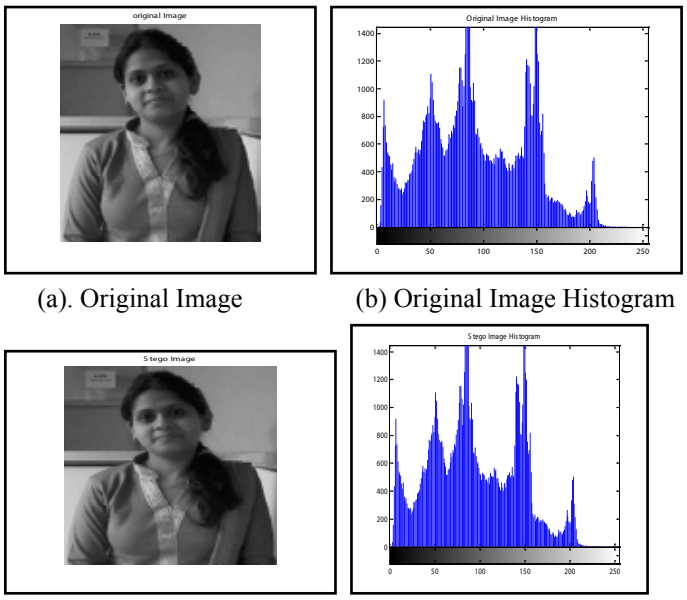


(a). LENA (b) VIEW (C) STUTI

Fig. 4: Three Cover Images

A. LSB Based Steganography

The text hidden inside the Data Base Images is "hello how are u my name is stuti" (32 characters). The Original image and the corresponding Histograms are as shown in fig. 5(a) and (b) and Stego-image and corresponding Histograms are as shown in the fig. 5(c) and (d).



(a). Original Image (b) Original Image Histogram

(c). Stego Image (d). Stego image Histogram

Fig. 5: LSB Based Steganography Algorithm

The average PSNR and MSE values of test images versus LSB Steganography algorithm used in our experiments have been given in Table 1. The value of the PSNR, MSE, CER, time Elapsed in the implementation of algorithm and Correlation coefficient are as shown in the Table. This algorithm is easy for detection/ extraction. There is no theoretical outstanding mark of LSB insertion, until little increase in background noise is done. For the images with different capacity, the average value of PSNR in LSB Based Steganography algorithm has been found to be 80 dB with correlation coefficient as 1 and CER as 100 percent. Fig. 6 shows the PSNR and MSE versus Data Base Images.

Table 1: Performance Evalutation of LSB Based Steganography Algorithm

Image Name	Image Size (Bytes)	%age of Recovered data	MSE	PSNR (in db)	Correlation coefficient
LENA	552120	100	0.00050735	81.077	1
VIEW	1440000	100	0.00028958	83.513	1
STUTI	337689	100	0.00112831	77.606	1

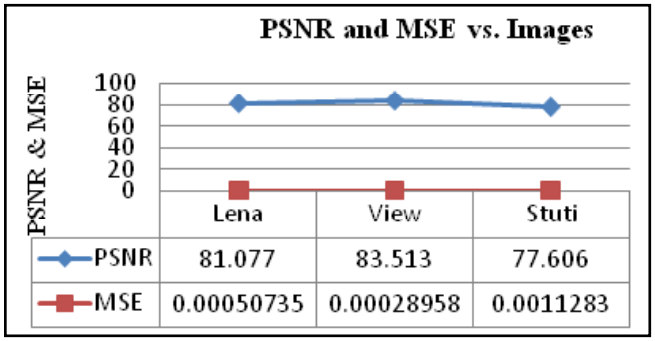
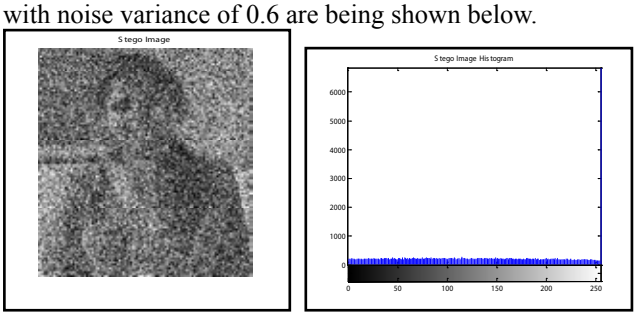


Fig. 6: PSNR and MSE Versus Data Base Images

Robustness

SinceLSB insertion has been found to be very vulnerable to a lot of transformations, even to the most harmless and usual ones. First of all, image has been passed through the Noisy channel or Gaussian

noise has been applied on the stego image with varying noise variance. Next efforts are done to extract the data and to compute the amount of damage done. The analysis has been done in terms of PSNR (in dB) and CER. The stego image and its histogram with noise variance of 0.6 are being shown below.



(a). Stego Image (b) Histogram of the Stego Image

Fig. 7: Image Attack: Gaussian Noise

When we increased the noise density in Gaussian noise, as has been shown in fig. 7 the PSNR and CER are decreased and consequently the image quality. This shows that PSNR decreases as noise density of Gaussian noise is increased.

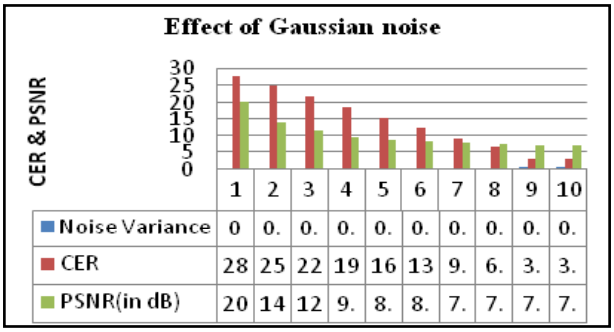
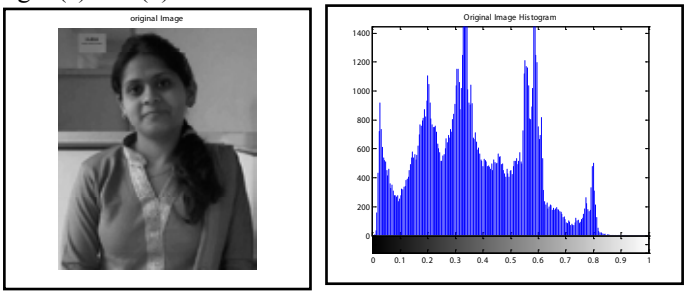


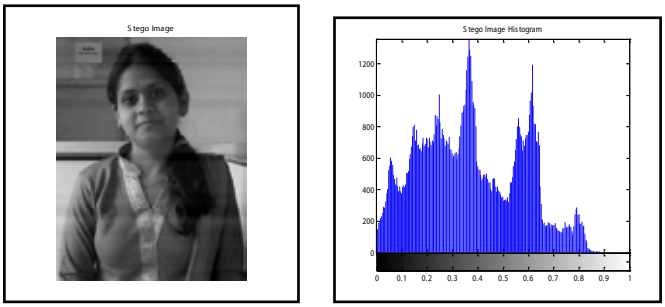
Fig. 8: Effect of Gaussian Noise on PSNR and CER

B. DCT Based Image Steganography

The text hidden inside the Data Base Images is "hello how are u my name is stuti" (32 characters).The Original image and the corresponding Histograms are as shown in fig. 9(a) and (b) and Stego-image and corresponding Histograms are as shown in the fig. 9(c) and (d).



(a). Original Image (b). Original Image Histogram



(c). Stego Image (d). Stego Image Histogram

Fig. 9: DCT Based Steganography Algorithm

The average PSNR and MSE values of test images versus DCT Steganography Algorithm that has been detected as shown in the Table 2. The value of the PSNR, MSE, CER, time Elapsed in the implementation of algorithm and Correlation coefficient found by us have been shown into the Table 2. The greater is the value of PSNR, the more will be the image quality. Mean square error is used to measure the distortion in the image by performing byte by byte comparison between the original image and stego image. The DCT based image steganography doesn't support high capacity to hide data. For the images with different capacity, the average value of PSNR in DCT Based Steganography Algorithm that we got 71dB and CER as 100 percent. The Average value of Correlation coefficient in DCT based Steganography Algorithm is 0.9352.The value of Correlation coefficient is approximately equal to unity.

Table 2: Performance Evalutation of DCT Based Steganography Algorithm

Image Name	Image Size (Bytes)	%age Of Recovered data	MSE	PSNR (in db)	Correlation coefficient
LENA	552120	100	0.0010752	77.815	1
VIEW	1440000	100	0.0470091	61.409	1
STUTI	337689	100	0.0012455	77.177	1

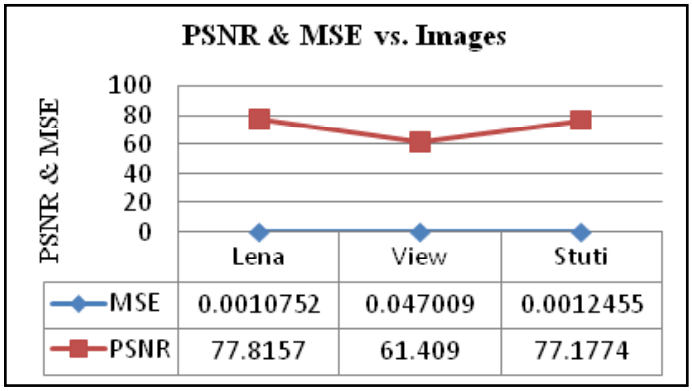
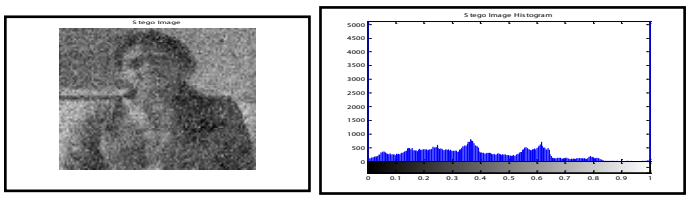


Fig. 10: PSNR and MSE versus Data Base Images

Robustness

First of all, the image is passed through the Noisy channel or Gaussian noise. It was applied on the Stego image with varying noise densities. Next efforts are done to extract the data. The analysis has been done in terms of PSNR (in db) and CER. The Stego image and its Histogram are as have been shown in fig. 10. When the noise variance of Gaussian noise is increased, it is found that the PSNR and CER have decreased as shown in fig. 10, and hence the image quality declined.



(a). Stego Image (b). Histogram of the Stego Image

Fig. 11: Image Attack: Gaussian Noise

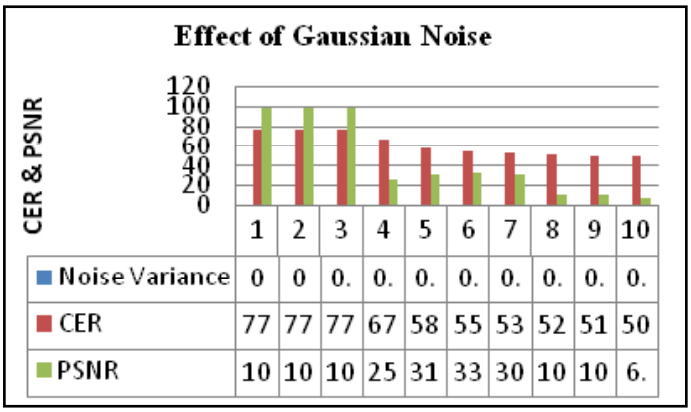
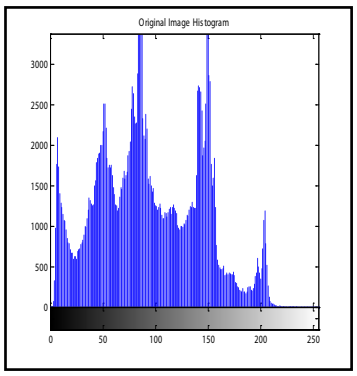


Fig. 12: Effect of Gaussian noise on PSNR and CER

C. DWT Based Image Steganography

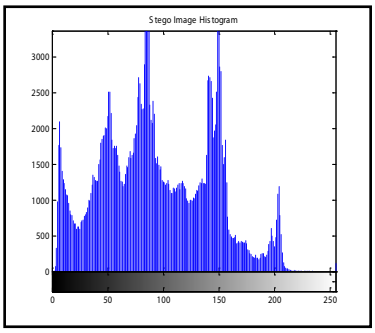
The text hidden inside the Data Base Images is "hello how are u my name is stuti" (32 characters). The Original image and Corresponding Histograms were found to be as shown in fig. 13 (a) and (b) and Stego-image and Corresponding Histograms are given in the fig. 14 (c) and (d). The average PSNR and MSE values of test images versus DWT Steganography algorithm used in our experiments have been given in Table 3. The value of the PSNR, MSE, CER, time Elapsed in the implementation of algorithm and Correlation coefficient found by us have been shown into the Table 3.

(a). Original Image



(b). OriginalImage Histogram

(c). Stego Image



(d). Stego Image Histogram

Fig. 13: DWT Based Steganography Algorithm

For the images with different capacity, the average value of PSNR that we got is 21dB with correlation coefficient as 1 and CER as 100 percent. Fig. 14 shows the PSNR and MSE versus Data Base Images.

Table 3: Performance Evalutation of DWT Based Steganography Algorihtm

Image Name	Image Size (Bytes)	%age Of Recovered data	MSE	PSNR (in db)	Correlation coefficient
LENA	552120	100	446.3196	21.6343	1
VIEW	1440000	100	446.3196	21.6343	1
STUTI	337689	100	446.3196	21.6343	1

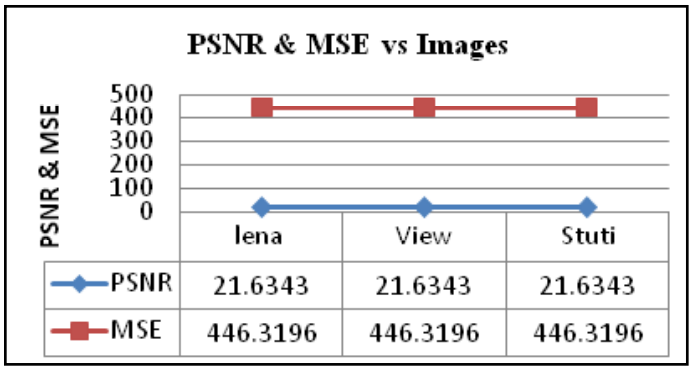


Fig. 14: PSNR and MSE versus Data Base Images

The DWT based Steganography Haar transform has been used. The nth level of Haar Transform has been found to be as shown into the fig. 15

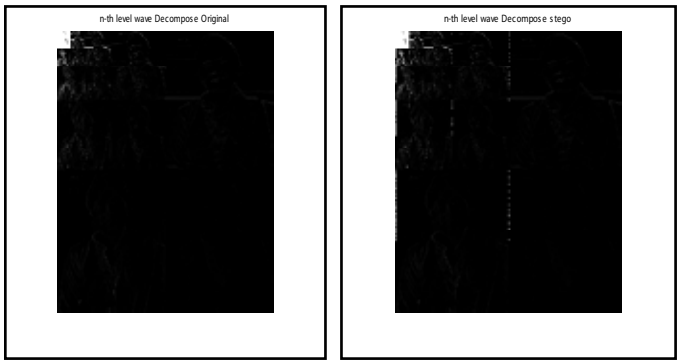
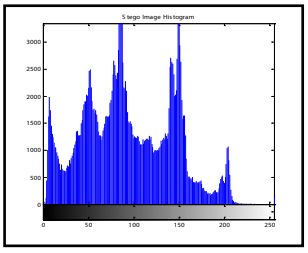


Fig. 15: N^{th} level Haar Transform

Robustness

First of all, the image was passed through the Noisy channel or the Gaussian noise and is applied on the Stego Image having different values of noise variance. Next efforts are done to extract the data. The analysis has been done in terms of PSNR (in db) and CER. The Stego image and its Histogram have been shown in fig. 16. When we increase the noise variance of Gaussian Noise, PSNR is average i.e. 22dB, CER decreased, and hence the image quality.

(a). Stego Image



(b). Histogramofthe Stego Image

Fig. 16: Image Attack: Gaussian Noise

Fig. 17 shows that when an image attack was applied to the DWT based image Steganography PSNRremained constant but the data recovery rate was decreased. The Stego image quality (in terms of PSNR) remained good but the method was not found to be robust.

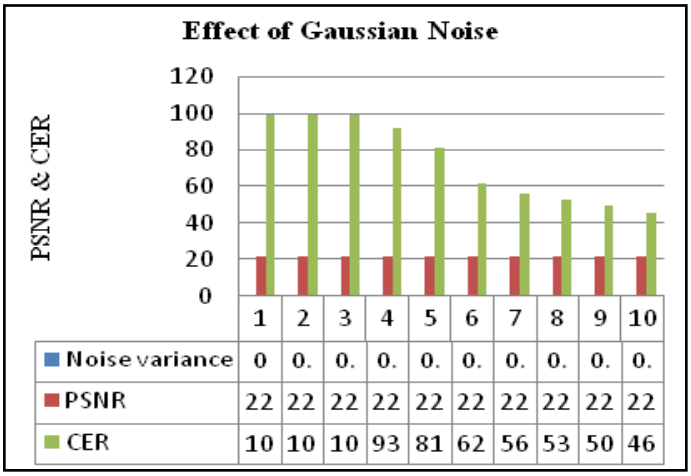
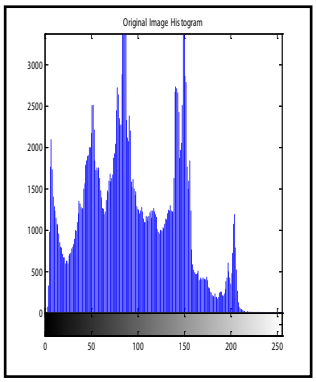


Fig. 17: Effect of Gauusian Noise PSNR & CER

D. Proposed Robust Image Steganography Algorithm

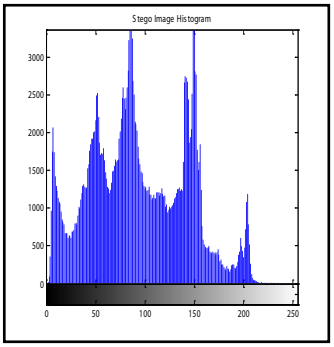
The text hidden inside the Data Base Images is "hello how are u my name is stuti" (32 characters). The Original image and the corresponding Histograms are as shown in fig. 18(a) and (b) and Stego-image and corresponding Histograms are as shown in the fig. 18(c) and (d).

(a). Original Image



(b). Original Image Histogram

(c). Stego Image



(d). Stego image Histogram

Fig. 18: Proposed Robust Steganography Algorithm

The average PSNR and MSE values of test images versus DCT Steganography algorithm used in our experiments have been given in Table 4. The value of the PSNR, MSE, CER, time Elapsed in the implementation of algorithm and Correlation coefficient are as shown in the Table 4. For the images with different capacity, the average value of PSNR in the proposed method Steganography Algorithm is 50db and the CER is 100 percent. The greater is the value of PSNR, the more will be the image quality. Mean square error is used to measure the distortion in the image by performing byte by byte comparison between the original image and stego image.

This has been found to be more robust than Spatial and Frequency Domain Steganography Algorithm. The Correlation coefficient, the degree of closeness between the Original image and the Stego image has been traced as nearly equal to one. An embedding method may be considered robust if the embedded message can be extracted after an image has been manipulated without being distorted. On visual inspection no difference could be observed between the Original image and Stego images.

Table 4: Performance Evalutation of Proposed robust Based Steganography Algorithm

Image Name	Image Size (Bytes)	%age Of Recovered data	MSE	PSNR (in db)	Correlation coefficient
LENA	552120	100	0.82482	48.9672	1
VIEW	1440000	100	0.65022	50.0002	1
STUTI	337689	100	0.32465	53.0162	1

Fig. 19 shows the PSNR and MSE for the Data Based Images. The value of PSNR has been calculated fordifferent capacities of images and the comparison of PSNR and CER values for all the techniques is done to evaluate the percentage of data recovered and image quality.

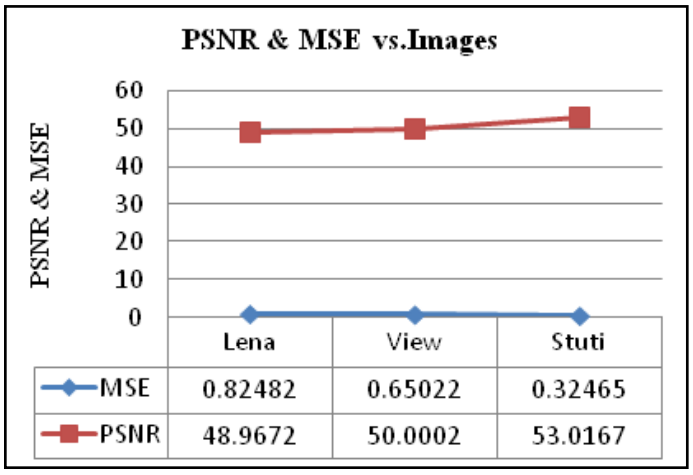
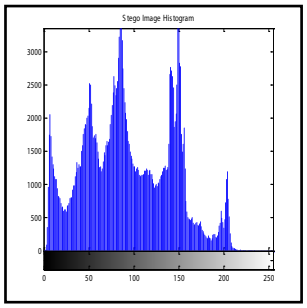


Fig. 19: PSNR and MSE for the Data Based Images

Robustness

First of all, the image was passed through the Noisy channel or Gaussian noise was applied to the Stego image with different values of noise variance. Next efforts are done to extract the data. The analysis has been done in terms of PSNR (in db) and CER. The Stego image and its Histogram were found to be as shown in fig. 20. When we increased the percentage of noise in Gaussian noise, PSNR average traced as 50dB and the Percentage of recovered data as 100, hence the image quality was remained maintained as has been, shown in fig. 21.



(a). Stego Image (b). Histogram of the Stego image

Fig. 20 Image Attack: Gaussian Noise

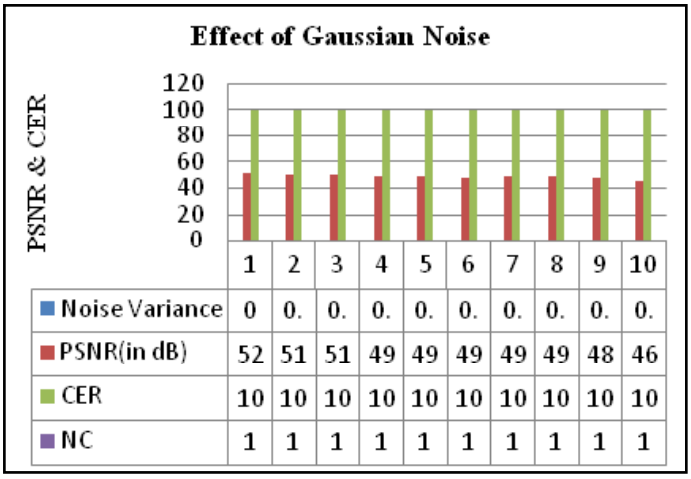


Fig. 21: Effect of Gauusian Noise on Proposed Robust Steganography

Now the comparison of the proposed method with spatial and frequency domain methods is performed. It is observed from the results that the proposed system is more robust and it gives good image quality(in terms of PSNR). The effect in PSNR with and without image attacks is being shown in fig. 22. The results have been shown for the Gaussain noise (with noise variance=0.3).

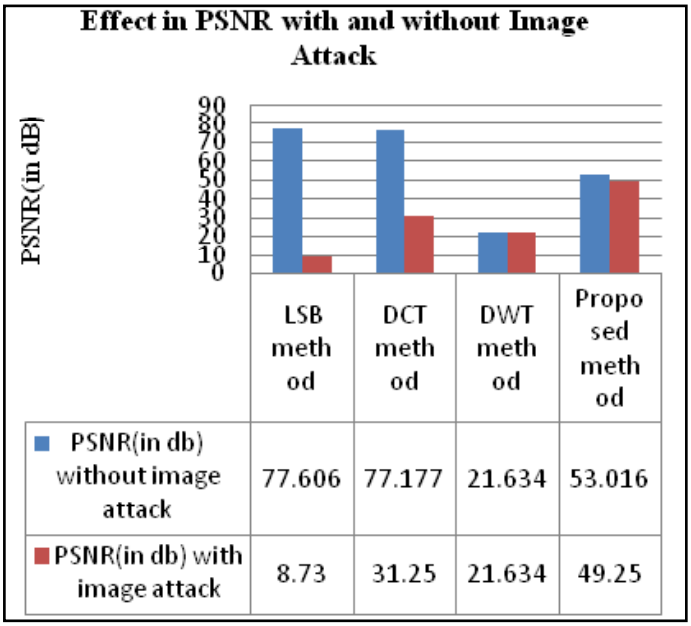


Fig. 22: Effect of Gauusian Noise on Steganography Algorithms

The effect in CER with and without image attacks has been shown in fig. 4.36. The results are shown for the Gaussain noise with noise variance is 0.3.

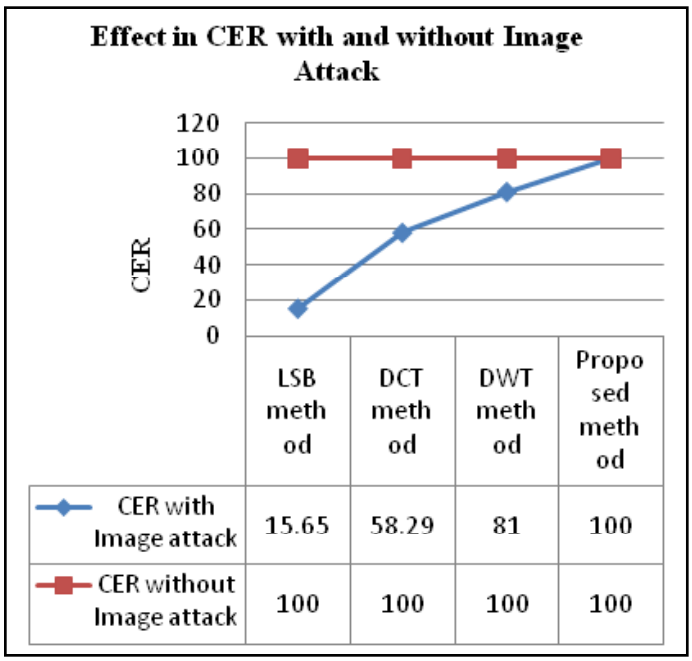


Fig. 23: Effect of Gauusian Noise On Steganography Algorithms

V. Conclusion

In this paper, various techniques of Steganography in Spatial domain and Frequency domain are implemented in order to suggest a Robust Algorithm that could give the best results in image quality when image is passed through the noisy channel. The LSB based Steganography, DCT based Steganography and DWT based Steganography were applied to compute PSNR, CER and to find out the Correlation coefficient ratio. It is observed that if PSNR ratio is high then images are of better quality. CER is used for the measurement of recovered data. The robustness of spatial and transform domain Steganography algorithms on digital images have been evaluated by using Gaussian Noise. For the Images without noise attack, Comparison of LSB based, DCT based and DWT based Stego images revealed that PSNR ratio of LSB based Steganography scheme is higher than Frequency domain based Steganography scheme for all types of images. DCT based Steganography scheme works perfectly with minimal distortion of the image quality in comparison to LSB based Steganography as when the image is passed through the noisy(Gaussian noise) channel, the MSE of LSB based Steganography changes at an alarming rate as compared to the DCT based steganography . Even though the amount of secret data that can be hidden by using this technique is smaller as compared to LSB based Steganography, DCT based Steganography scheme is being recommended as it ensures minimum distortion of image quality. LSB insertion is more vulnerable to even the most harmless and usual transformations whereas, in DWT Based Steganography, coefficients in the low frequency sub-band could be preserved unaltered for improving the image quality. This is due to the different characteristics of DWT coefficients in different sub-bands. Since the most essential portion (the low frequency part) remains unchanged, when the secret messages are embedded in the high frequency sub-bands corresponding to the edges portion of the original image, DWT is being recommended and is the more robust as compare to the LSB based and DCT based Steganography. But as the noise variance of Gaussian noise is increased, the data recovery rate decreases and hence the robustness also decreases. Therefore, DCT based Robust Image Steganography is proposed in which the data recovery rate

is 100 percent as the noise variance increases.

It can be concluded that

1. Spatial domain based Steganography Algorithm found it to be a less little robust technique for hiding data whereas Transform domain based Steganography Algorithm worksperfectly with minimal distortion of the image quality.
2. Therefore, Proposed Robust Image based Steganography is more robust as its data recovery rate is 100 percent as compared to the other techniques and it also maintain quality of the image even when the image is passed through the noisy channel(Gaussian noise).
3. We may tentatively conclude that PSNR, MSE, CER, Correlation function of the proposed system ismore robust than the existing ones.

References

[1] J.R. Krenn,"Steganography and Steganalysis", January 2004.

[2] Deshpande Neeta, Kamalapur Snehal, Daisy Jacobs, "Implementation of LSB Steganography and Its Evaluation for Various Bits", 2004.

[3] K.B.Raja, C.R.Chowdary, Venugopal K R, L.M.Patnaik, "A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images", IEEE 2005.

[4] Vijay Kumar Sharma, Vishal shrivastava,"A Steganography Algorithm for Hiding Images by improved LSB substitution by minize detection", Journal of Theoretical and Applied Information Technology, Vol. 36, No. 1, 15th February 2012.

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

[6] Chen Ming, Zhang Ru, NiuXinxin, Yang Yixian, "Analysis of Current Steganography Tools: Classifications & Features" , International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP'06), IEEE-2006.

[7] Aneesh Jain, Indranil Sen. Gupta,"A JPEG Compression Resistant Steganography Scheme for Raster Graphics Images", IEEE 2007.

[8] Beenish Mehboob, Rashid Aziz Faruqui,"A Steganography Implementation", IEEE 2008.

[9] Hassan Mathkour, Batool Al-Sadoon, Ameur Touir,"A New Image Steganography Technique", IEEE 2008.

[10] Nageswara RaoThota, Srinivasa Kumar Devireddy, "Image Compression Using Discrete Cosine Transform", Georgian Electronic Scientific Journal: Computer Science and Telecommunications, No.3 (17), 2008.

[11] MamtaJuneja, Parvinder Singh Sandhu,"Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption", International Conference on Advances in Recent Technologies in Communication and Computing, 2009.

[12] Dr. Ekta Walia, Payal Jain, Navdeep,"An Analysis of LSB & DCT based Steganography", Global Journal of Computer science & technology, Vol. 10 Issue 1 (Ver 1.0), April 2010.

[13] K.B.Shiva Kumar, K.B.Raja, R.K.Chhotaray, Sabyasachi Pattnaik,"Coherent Steganography using Segmentation and DCT", IEEE 2010.

[14] K Suresh Babu, K B Raja, Kiran Kumar K, Manjula Devi T H, Venugopal K R, L M Patnaik,"Authentication of Secret Information in Image Steganography".

[15] Arvind Kumar, Km. Pooja,"Steganography: A Data Hiding Technique", International Journal of Computer Applications, Vol. 9, No. 7, November 2010.

[16] Atalla I. Hashad, Ahmed S. Madani,"A Robust Steganography Technique Using Discrete Cosine Transform Insertion".

[17] Vijay Kumar, Dinesh Kumar,"Performance Evaluation of DWT Based Image Steganography", IEEE 2010.

[18] Ali Al-Ataby, Fawzi Al-Naima,"A Modified High Capacity Image Steganography Technique Based on Wavelet Transform". The International Arab Journal of Information Technology, Vol. 7, No. 4, October 2010.

[19] T. Narasimmalou, Allen Joseph .R,"Optimized Discrete Wavelet Transform based Steganography", IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), 2012.

[20] Neda Raftari, Amir Masoud Eftekhari Moghadam, "Digital Image Steganography Based on Assignment Algorithm and Combination of DCT-IWT", Fourth International Conference on Computational Intelligence, Communication Systems and Networks, 2012.

[21] AnkitaSancheti,"Pixel Value Differencing Image Steganography Using Secret Key", International Journal of Innovative Technology and Exploring Engineering (IJITEE), Vol. 2, Issue 1, and December 2012.

[22] Neha Batra, Pooja Kaushik,"Implementation of Modified 16×16 Quantization Table Steganography on Color Images", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, Issue 10, October 2012.

[23] ElhamGhasemi, Jamshid Shanbehzadeh, Nima Fassihi,"High Capacity Image Steganography using Wavelet Transform and Genetic Algorithm", proceedings of international multiconfrence of engineers & computer science, IMECS-Volume I , March 16-18, 2011

[24] Gurmeet Kaur, Aarti Kochhar,"A Steganography Implementation based on LSB & DCT", International Journal for Science and Emerging, Technologies with Latest Trends 4(1), pp. 35-41, 2012.

Stuti Goel received her B.Tech.degree in Electronics & Communication from Doon Valley Institute of Engineering, Karnal (KUK)& Technology in 2011 and pursuing M.Tech. in Electronics & Communication from Doon Valley Institute of Engineering & Technology, Karnal (KUK). Her Research interest includes Image Processing & Digital Signal Processing.

Arun Rana received his B.Tech. degree in Electronics & Communication from Doon Valley Institute of Engineering & Technology, Karnal (KUK) & received his M.Tech. degree in Electronics & Communication from MMEC, Mullana. He is an Assitant Professor of Electronics & Communication at Doon Valley Institute of Engineering & Technology, Karnal and has 6 years of teaching experience in the field of Electronics & Communication Engineering. Her Research interest includes Image Processing, Micro-processing & Embedded System. He has published various papers in national and international conferences and journals. He has published various books for engineering students.

Manpreet Kaur received her B.Tech. degree in Electronics & Communication from Doon Valley Institute of Engineering & Technology, Karnal (KUK) & received her M.Tech. degree in Electronics & Communication from Deen Bandhu Chhotu Ram University of Science and Technology (Formerly Known as C.R.S.C.E) Murthal, Sonepat. She is an Assitant Professor of Electronics & Communication at Doon Valley Institute of Engineering & Technology, Karnal. Her Research interest includes Image Processing & Digital Signal Processing.