Analysis of LSB, DFT and DCT Based Approach For Image Steganography

CHAVITI VASANTHA LAKSHMI

Roll Number: 204102302

ABSTRACT

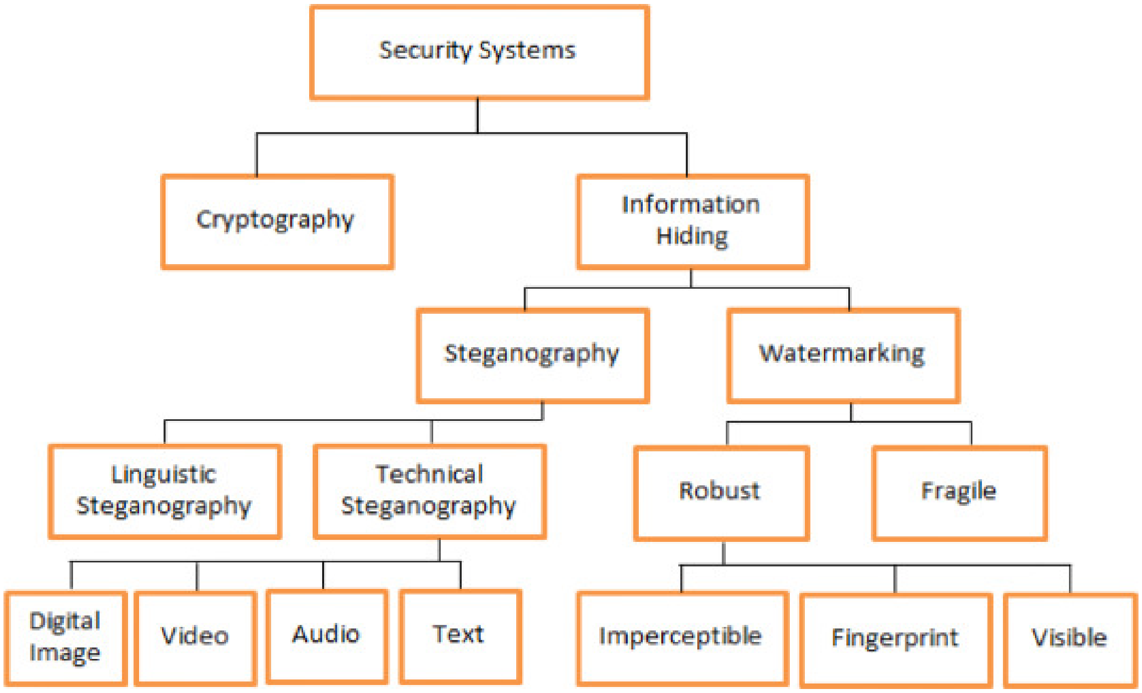
Steganography is a branch of information hiding.It hides the existence of a secret messages or images by embedding it in a cover media.In this paper we propose a new steganography technique which embedds the secret messages and images in frequency domain. Unlike the space domain approaches, secret messages are embedded in the high frequency coefficients resulted from Discrete fourier Transform. Coefficients in the low frequency sub-band are preserved unaltered to improve the image quality. Here we use LSB ,DFT,DCT techiniques on images with block partitioning and we obtain the images with secret messages and images embedded in it. These operations are well-designed so they keep the information away from stealing, destroying from unintended users on the internet and hence provide satisfactory security.

Key words : LSB,DFT,DCT

1 Introduction

In a highly digitalized world we live today, computers help transforming analog data into digital forms before storing or processing. In the mean while, the internet develops very fast and hence becomes an important medium for digital data transmission. However, being a fully open medium, the internet brought us not only convenience but also some hazards and risks.It is convenient for some users to copy, destroy, or change them on the internet. As a result, information security becomes an essential issue. Various schemes for data hiding are developed recently. According to the purposes of data hiding, these schemes are classified into two categories: watermarking and steganography.

Watermarking is a protecting technique which protects (claims) the author's property right for images by some hidden watermarks. On the other hand, steganography techniques apply some cover images to protect the confidential data from unintended internet users.Digital images are one of the well-known medium used for hiding the secret data without perceptibly destroying the original image. The selected image for hiding data is known as cover image. The cover image with the secret message embedded is known as stego image .The stego and the cover images are generally indistinguishable and only the intended receiver can reveal the existence of the hidden message so here we take an image and we embedd the image or message into it by LSB,DFT,DCT techiniques



1.1 Background

This paper proposes a Image steganography based on LSB,DFT,DCT techniques.They depend on frequency transformation and selective block embedding. Efforts have been given to ensure that the technique performs optimally, producing high fidelity stego image along with good resistance to steganalysis attacks.

1.2 Terminologies

Here we work on the LSB (Least Significant Bits) substitution method,Discrete Cosine Transform(DCT) and DFT(Discrete Fourier Transform).

1.2.1 LSB technique

The most frequently used steganography method is the technique of LSB substitution. In a gray-level image, every pixel consists of 8 bits. One pixel can hence display 28 =256 variations. The weighting configuration of an 8-bit number.The basic concept of LSB substitution is to embedd the confidential data at the right most bits (bits with the smallest weighting) so that the embedding procedure does not affect the original pixel value greatly.This method is easy and straightforward. However, when the capacity is greatly increased, the image quality decreases a lot and hence a suspected stego-image results. Furthermore, the confidential data might be easily stolen by simply extracting the k-rightmost bits directly

1.2.2 DFT technique

The frequency domain transform we applied is DFT.Here in DFT we choose a window of size 2 * 2 of the source image Instead of direct embedding a message or image within the source image.we follows the sliding window manner and then convert it from spatial domain to frequency domain using Discrete Fourier Transform (DFT). The bits of the authenticating message or image are then embedded at LSD within the real part of the transformed image. Inverse DFT is performed for the transformation from frequency domain to spatial domain as final step of encoding. Decoding is done through the reverse procedure.

$$\text{DFT: } X(k) = \sum_{n=0}^{N-1} x(n) W_N^{kn} \qquad k = 0, 1, \ldots, N-1$$

$$\text{IDFT: } x(n) = \frac{1}{N} \sum_{k=0}^{N-1} X(k) W_N^{-kn} \qquad n = 0, 1, \ldots, N-1$$

where W_N is defined as

$$W_N = e^{-j2\pi/N}$$

1.2.3 DCT technique

The frequency domain transform we applied is DCT. DCT helps to separate the image into parts (or spectral sub-bands)with respect to the image's visual quality.DCT is similar to the discrete Fourier transform: it transforms a image from the spatial domain to the frequency domain. In this method there are two types (i) the large number of coefficients are modified slightly to accommodate data of the payload, (ii) replacing the smaller number of insignificant coefficients by the data of the payload. Here the data is embedded into the cover image by changing the coefficients of a transform of an image such as discrete cosine transform (DCT) coefficients. There are mainly three transformation techniques (i) Fast Fourier Transform (FFT) (ii) Discrete Cosine Transform (DCT) and (iii) Discrete Wavelet Transform (DWT). FFT introduce round off errors; so this technique is not suitable for hidden communication. The two dimensional

DCT is applied on blocks of 8x8 pixels. This transforms 8x8 pixels blocks into 64 DCT coefficients, modifying one coefficient affects all the 64 image pixels.

$$H(u,v) = \frac{2}{\sqrt{MN}} C(u)C(v) \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} h(x,y) \cos\left[\frac{(2x+1)u\pi}{2M}\right] \cos\left[\frac{(2y+1)v\pi}{2N}\right]$$

$$h(x,y) = \frac{2}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} C(u)C(v)H(u,v) \cos\left[\frac{(2x+1)u\pi}{2M}\right] \cos\left[\frac{(2y+1)v\pi}{2N}\right]$$

$$C(\gamma) = \begin{cases} \frac{1}{\sqrt{2}}\, for\ \gamma = 0 \\ 1 for\ \gamma > 0 \end{cases}$$

1.3 Organization

The rest of this paper is organized as follows. Section 2 reviews the datasets.Section 3 reviews the literature. In section 4, the proposed steganography method is described in step by step.Experimental results and analysis are demonstrated and Finally, some concluding remarks are provided in section 5.

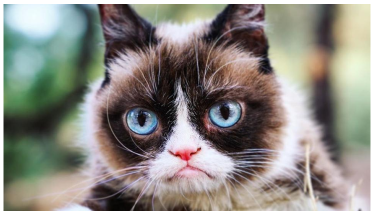
2 Datasets

we work on two set of images one set contains input images and other one is secret image which is need to be embedded

2.1 inputimages

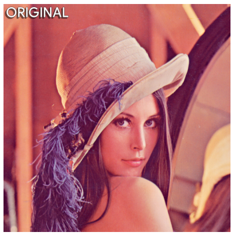
Here in this work i have been using 3input images **-owl,lenna,pepper**

In LSB method owl image is used as input image and cat image as secret image



In DCT method pepper image is taken as input image

In DFT method lenna image is taken as input image



2.2 Evaluation Metrics

we determine the quality of a digital image by evaluating a parameter named PSNR (Peak Signal to NoiseRatio) is defined as follows

$$\mathrm{PSNR} = 10 \times \lg\left(\frac{255^2}{\mathrm{MSE}}\right)$$

$$\mathrm{MSE} = \frac{1}{M \times N} \sum_{i=1}^{N} \sum_{j=1}^{M} \left[I(i,j) - I'(i,j) \right]^2$$

where MSE (Mean Square Error) stands for the mean-squared difference between the cover-image and the stego-image.The mathematical definition for MSE is: The calculated PSNR usually adopts dB value for quality judgement. The larger PSNR has the higher image quality (which means there is only little difference between the cover-image and the stego-image). On the contrary, a small dB value of PSNR means there is great distortion between the cover-image and the stego-image.

3 Literature

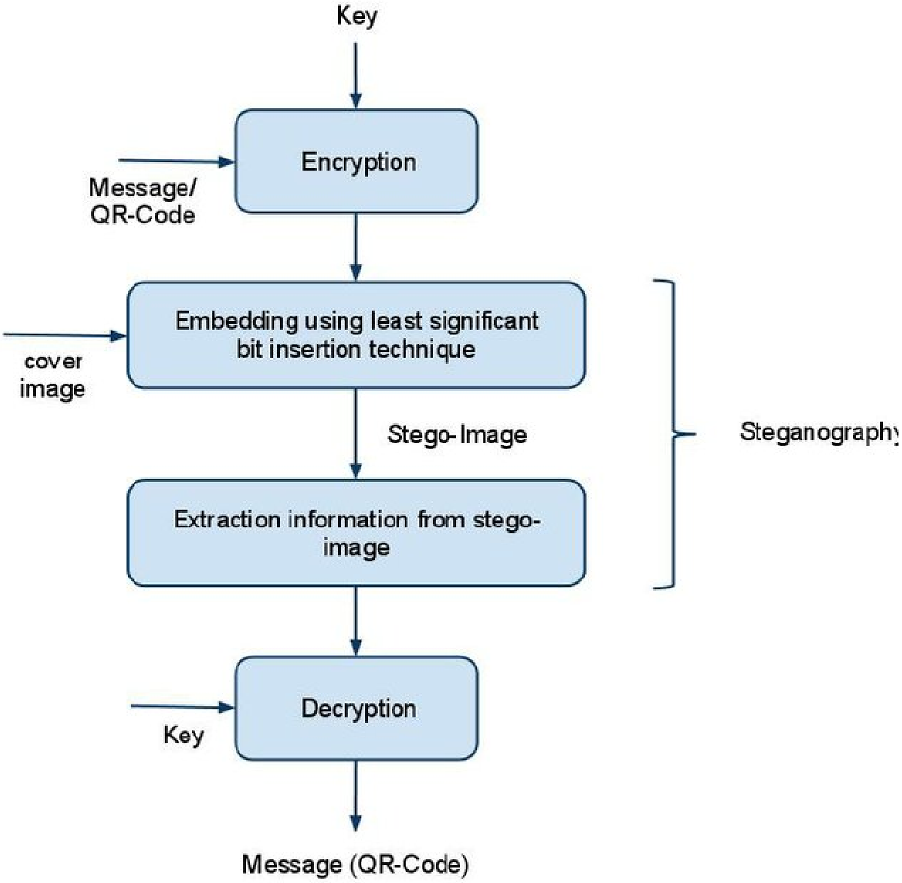
3.1 Previous methods

Previously few DWT based information hiding algorithms have been proposed .At the same time it is observed that there has been many block partitioning based techniques have also been proposed which can embed data in a cover image with an acceptable level of randomness necessary for secure data hiding. Therefore, it is possible to enhance the security of the common DWT based schemes by combining the features of both the frequency domain and the block based methods

3.2 Proposed Method

Here proposed method works on the frequency domain to embed secret bits in the higher frequency components of the cover image by applying LSB,DFT,DCT on cover image .To enforce the security three ways have been followed. At first, a decimal array from the secret bits is formed. Secondly, a dynamic block containing values from three different higher frequency components is constructed and lastly bits are embedded in some selected portions of the block.

4 Methodology and Algorithms


Key
Encryption
Message/ QR-Code
Embedding using least significant bit insertion technique
cover image
Stego-Image
Steganography
Extraction information from stego-image
Decryption
Key
Message (QR-Code)

4.1 LSB-method

In a gray scale image each pixel is represented in 8 bits. The last bit in a pixel is called as Least Significant bit as its value will affect the pixel value only by "1". So, this property is used to hide the data in the image. If anyone have considered last two bits as LSB bits as they will affect the pixel value only by "3". This helps in storing extra data.

The Least Significant Bit (LSB) steganography is one such technique in which least significant bit of the image is replaced with data bit. As this method is vulnerable to steganalysis so as to make it more secure we encrypt the raw data before embedding it in the image. Though the encryption process increases the time complexity, but at the same time provides higher security also. This approach is very simple. In this method the least significant bits of some or all of the bytes inside an image is replaced with a bits of the secret message. The LSB embedding approach has become the basis of many techniques that hide messages within multimedia carrier data. LSB embedding may even be applied in particular data domains – for example, embedding a hidden message into the color values of RGB bitmap data, or into the frequency coefficients of a JPEG image. LSB embedding can also be applied to a variety of data formats and types

There are two important components, cover image and hiding data, in data hiding technique.The cover image I is an 8-bit gray scale image. The size of cover image is m×n. The hiding data H embedded in I is g-bits bit stream.

a N*M image in which each pixel value is represented by a decimal number in the range determined by the number of bits used. In a gray-scale image, with 8 bit precision per pixel, each pixel assumes a value between [0, 255] and each positive number

This property allows the decomposition of an image into a collection of binary images by separating the into n bit planes. In the classical LSB embedding methods, the secret message is inserted into the least-significant bit plane of the cover image either by directly replacing those bits. The amount of data to be embedded may also be fixed or variable in size depending on the number of pixels selected. The main advantage of such a technique is that the modification of the LSB plane does not affect the human perception of the overall image quality as the amplitude variation of the pixel values is bounded by ±1. The masking properties of the Human Visual System allow significant amounts of embedded information to be unnoticed by imperceptible by the average observer under normal viewing conditions. “Masking” refers to the phenomenon where a signal can be imperceptible to an observer in the presence of another signal.

The advantages of LSB data hiding includes high embedding capacity and low computational complexity. The main disadvantages are the weaknesses with respect to robustness, tampering, geometric attacks, filtering, and compression

4.2 DFT-method

The DFT uses gray scale image of size (M x N) to be authenticated .The technique inserts authenticating message or image Xm*n of size (M/2*N/2*3)-16 bits (maximum) as the fIrst 16 bit holds the dimension of the file. DFT, given in equation is used to transform the image from spatial domain to frequency domain.

A.Embedding Algorithm

1. Take a message file or image whose size is less than or equal to (M/2*N/2*3)-16 bits where M x N is the size ofthe cover image.

2. Take 2 x 2 window of the cover image in sliding window manner and repeat step 3 and 4 until the ends ofthe cover image.

3. Apply the Discrete Fourier Transformation. 4. Consider the real part ofthe frequency component and do the following.

• Take three frequency component valuesbut not the first one and do the following.

o Consider the Least Significant Bit position ofthe DFT component.

• Replace the bit by one authenticating bit

5. Apply the Inverse Fourier Transformation.

6. Stop.

B. Extraction Algorithm

1. Take the authenticated image as input.

2. Consider 2 x 2 mask ofthe input image at a time and repeat step 3 and 4 until the ends of the embedded image.

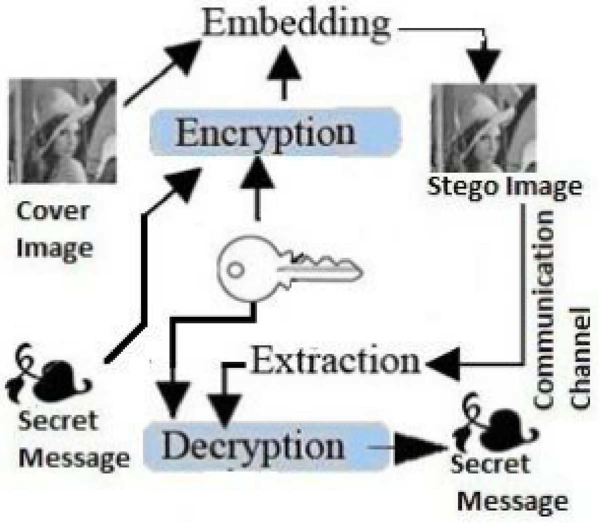
3. Apply the Discrete Fourier Transformation. 4. Consider the real part ofthe frequency component and do the following.

• Take three frequency component values but not the first one and do the following.

o Extract the Least Significant Bit. o Replace this bit position by '1' or by '0'.

5. Apply the Inverse Fourier Transformation.

6. Stop.



4.3 DCT- method

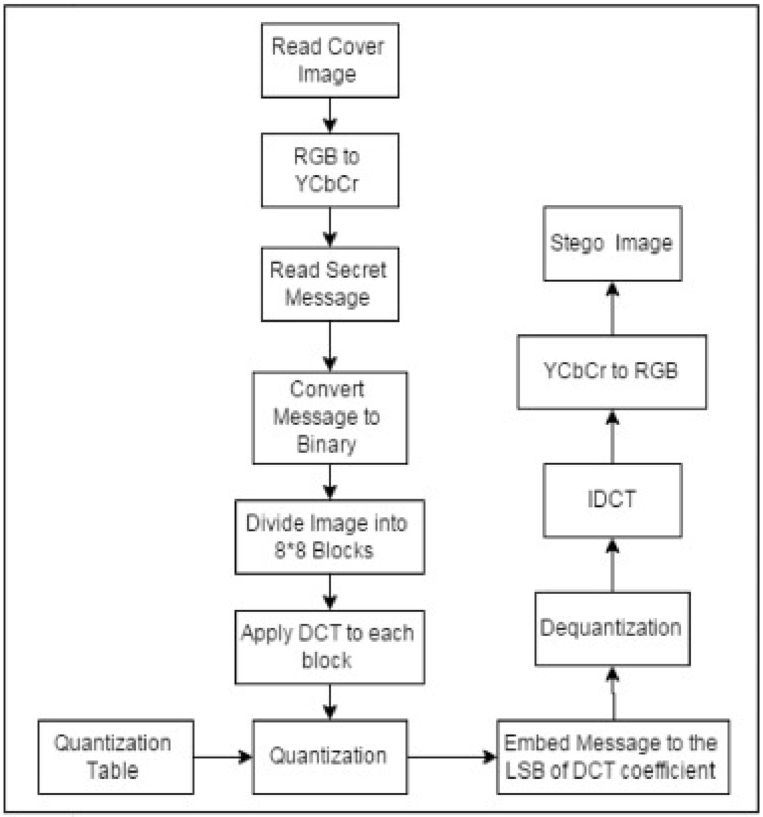
A.Embedding process

The embedding procedure includes the transformation of spatial domain to the frequency domain utilizing a DCT algorithm then embedding step takes place and finally reverse transform from frequency domain to spatial domain is carried out. The embedding process hides the payload in the used cover-image, where it is converted into a different color scale and is split into non-overlap 8×8 blocks, then is converted into the frequency domain and quantized. Finally the payload is embedded, then the stegoimage is transformed back to the spatial domain and dequantizated.

Embedding algorithm

Input: A cover image, message, and key.

Output: A stegoimage



Step 1: Input the cover image of size NxM.

Step 2: Input The payload and the shared Key.

Step 3: Convert the Message and the Key to Binary representation for later embedding.

Step 4: Convert image from the RGB color scale to the YCbCr color scale.

Step 5: Divided image into non-overlapping blocks of 8×8 blocks, each block will do the same process individually.

Step 6: Apply DCT to each block.

Step 7: Quantize the DCT coefficient by using Quantization tables.

Step 8: Embed the message to least significant bits of the quantized DCT coefficients of selected frequency components.

Step 9: Dequantize the DCT coefficient by using Dequantization tables.

Step 10: Apply IDCT to each block.

Step 11: Convert YCbCr to RGB again.

Step 12: Stego image has created

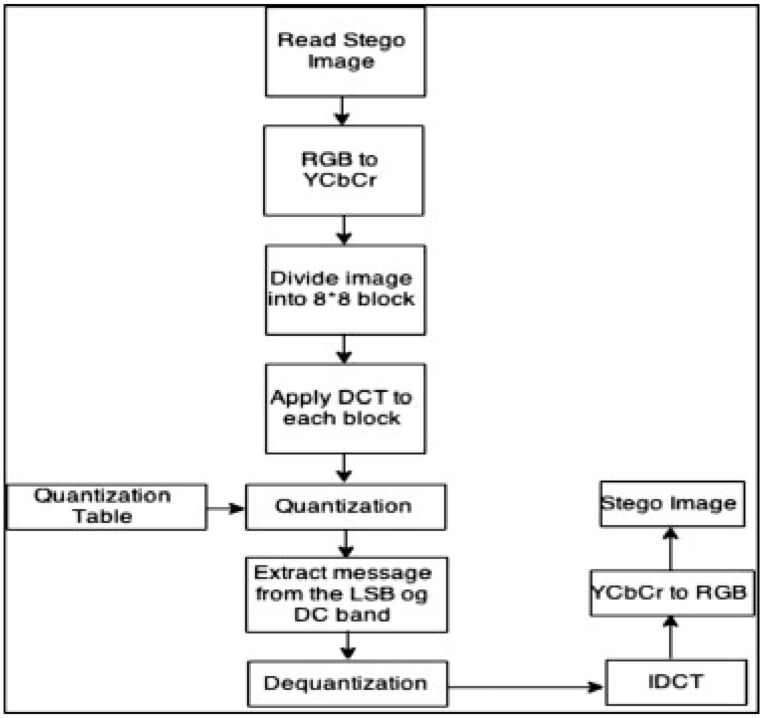
B.Extracting process

The extracting procedure includes the transformation of spatial domain to the frequency domain utilizing a DCT algorithm then extracting step takes place and finally reverse transform from frequency domain to spatial domain is carried out. The extracting algorithm retrieves the payload from the stegoimage, where it is transformed into a different color scale and is split to non-overlap 8×8 blocks, then, transformed into the frequency domain and quantized. Finally the payload is extracted, then the stegoimage is transformed back to the spatial domain and dequantizated

Extracting algorithm.

Input: The stegoimage and key.

Output: The cover image, Message.



Step 1: Input the stegoimage of size NxM.

Step 2: Input the Shared Key.

Step 3: Authenticate the shared key

Step 4: Convert the stegoimage from RGB color scale to YCbCr color scale.

Step 5: Divided the stegoimage into non-overlapping blocks of 8×8 blocks.

Step 6: Apply DCT to each block.

Step 7: Quantize the DCT coefficient by using Quantization tables.

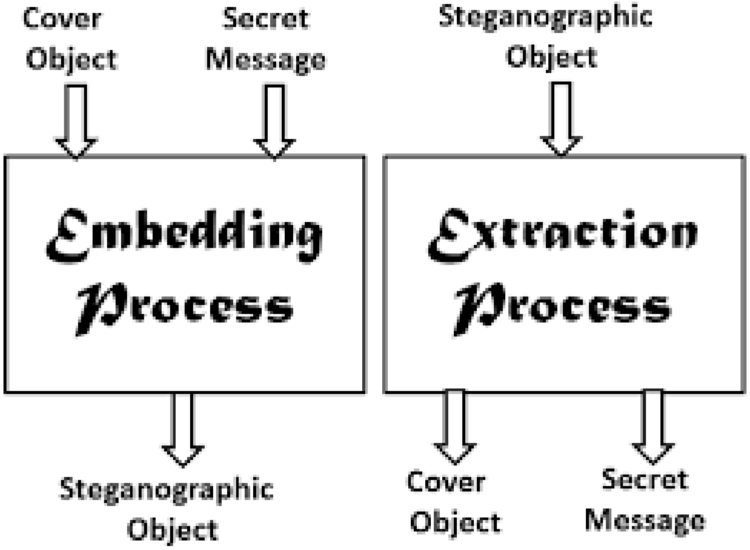
Step 8: Extract the message from the least significant bit of the quantized DCT coefficients of the selected frequency components in each block.

Step 9: Dequantize the DCT coefficient by using Dequantization tables.

Step 10: Apply IDCT to each block.

Step 11: Convert stegoimage YCbCr to RGB again.

4.4 implementation of embedding and extracting algorithm



4.5 outputimages

These are the output steganographied images

The final steganographied output image of owl contains secret image

The final steganographied output image of pepper contains secret message

The final steganographied output image of lenna contains secret image

5 Conclusions

In this paper we implemented LSB,DFT,DCT algorithms approach for image steganography, LSB and DCT algorithms had used quantization on raw images to obtain secure stego-image. The LSB technique has been used to accommodate maximum payload. The entire payload is embedded into the cover image to obtain the stego-object. The stego-object in the spatial domain is transformed into frequency domain by applying DCT. The DFT algorithm used here is the bit level image insertion and extraction in the frequency domain. PSNR shows the quality of image after hiding the data. PSNR of DCT is high as compared to the other two techniques. This implies that DCT provides best quality of the image. An embedding algorithm is said to be ROBUST if the embedded message can be extracted after the image has been manipulated without being destroyed. DCT is a highly robust method in which the image is not destroyed on extracting the message hidden in it and provides maximum security.

6 References

1.M. Pavani1, S. Naganjaneyulu, C. Nagaraju, ”A Survey on LSB Based Steganography Methods” International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 2 Issue 8 August, 2013 Page No. 2464-2467

2.Stuti Goel, Arun Rana, Manpreet Kaur,”A Review of Comparison Techniques of Image Steganography”, IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE) e-ISSN: 2278-1676,p-ISSN: 2320-3331, Volume 6, Issue 1 (May. - Jun. 2013), PP 41-48

3.A DWT based Steganography Scheme with Image Block Partitioning,Sabyasachi Kamila,Ratnakirti Roy,Suvamoy Changder,2015

https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=arnumber=7095311