METHODS IN DIGITAL STEGANOGRAPHY

Kiruthika Kannan(2018702001)
Ritu Srivatsava(2018701002)

1 Introduction

Steganography is the science that involves communicating secret data in an appropriate Multimedia carrier, e.g., image, audio, and video files. It comes under the assumption that if the feature is visible, the point of attack is evident, thus the goal here is always to conceal the very existence of the embedded data.

The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable they are, arouse interest and may in themselves be incriminating in countries in which encryption is illegal.

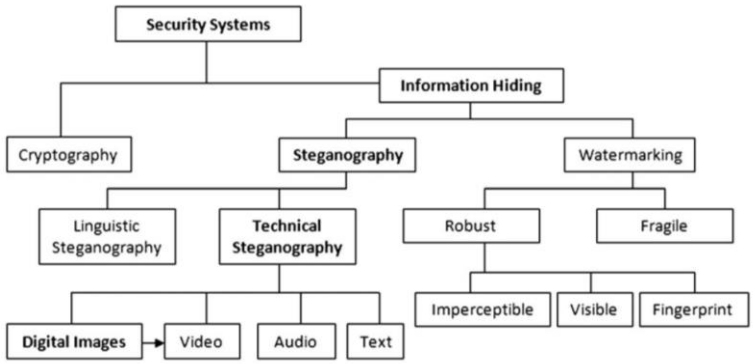


Fig. 1. The different embodiment disciplines of information hiding. The arrow indicates an extension and bold face indicates the focus of this study.

1.1 Problem Statement

To efficiently conceal an image in an image such that the hidden image (payload) in the stego-image is imperceptible to human vision system. The primary goal in Steganography is to improve the amount of information hidden while decreasing the perceptibility by human visual system. The objective is to implement and compare different methods in digital image steganography.

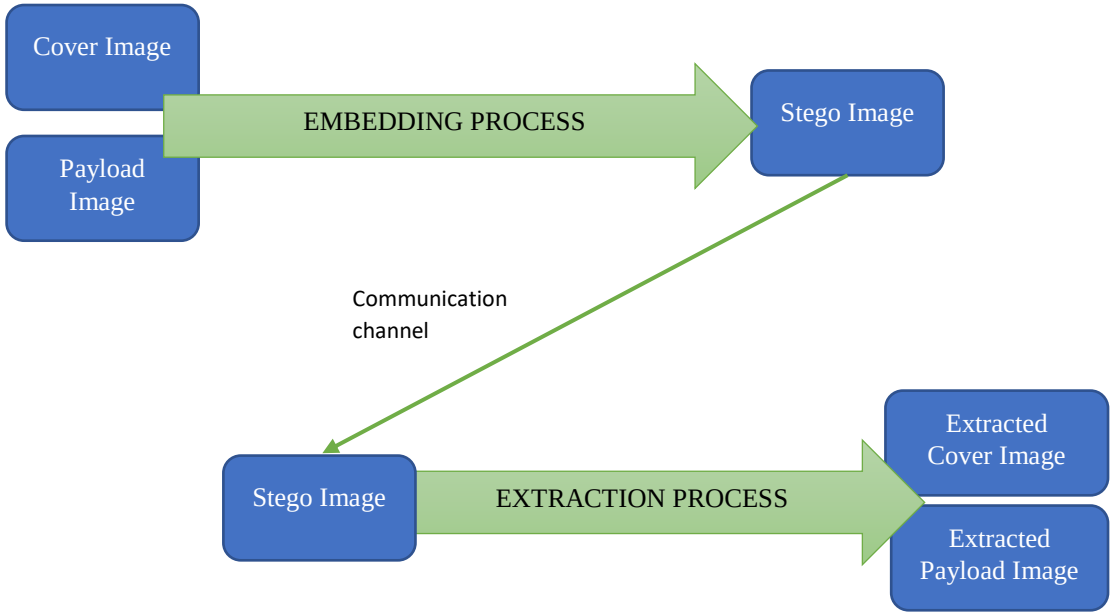
1.2 Problem Motivation

Huge internet usage over high bandwidth and low cost computer hardware has propelled the explosive growth of steganography. 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

2 Overview

The term ‘‘cover image’’ will be used throughout this paper to describe the image designated to carry the embedded bits. The embedded secret image is referred as “payload”. We will be referring to an image with payload data as ‘‘stego-image’’.

The steganography methods include two processes: Embedding takes the cover image and payload as input and outputs the stego-image at the sender side. Extraction separates the cover image and payload from the received stego-image at the receiver side.



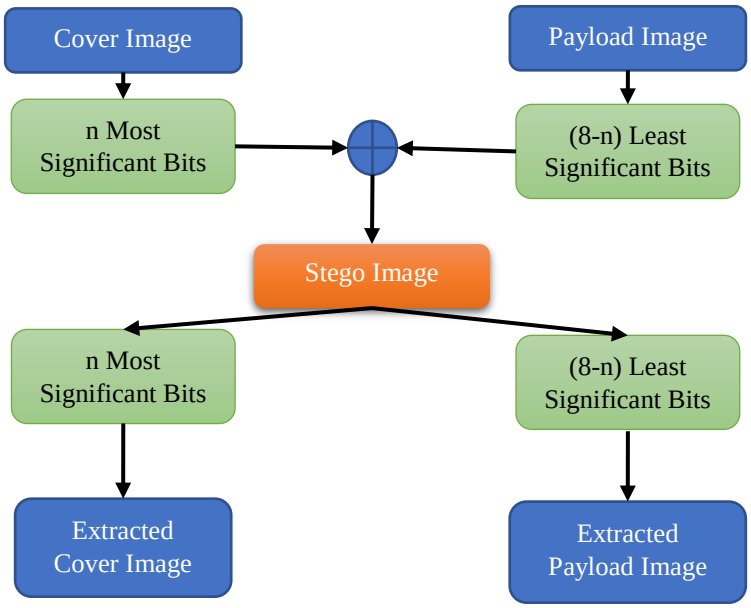
3 Methods Of Steganography

3.1 Least Significant Bit (LSB) Substitution

The easiest way to embed secret information within the cover file is called LSB insertion. The LSBs of the image pixels carry the least information and MSBs contain the most perceptible detail. This techniques exploits this property by replacing the LSBs of cover image with MSBs of payload image.

If m is the number of LSBs replaced in cover image, the stego-image contains (8-m) MSBs of cover image and m MSBs of payload image.

The extraction is a simple process of masking the bits but the number m must be known



’[

3.2 Edge Based

3.2.1 Embedding procedure

This procedure contains two phases:

Phase 1: Applying the Canny edge detector, we obtain the edge image I0 from the grayscale image I. Divide the edge image I0 into a set of blocks. Each block contains n pixels and is called n-pixel block. The n pixels are indexed as P1, P2, . . . , Pn. Herein, we use P1 to store the status of the remaining pixels. The status of each pixel, Pi, is defined as ‘1’ if Pi is an edge pixel. Otherwise, the status of each pixel, Pi, is defined as ‘0’. The status of pixels from P2 to Pn is stored inside P1 by an LSBs substitution operation. In this phase, whether a pixel is considered to be an edge pixel or not is based on the edge image using the canny edge detector.

For example, take a block A = [P1, P2, P3], with n = 3. In this example, assume that P1 and P3 are edge pixels. Thus, the status of the pixels P2 and P3 is ‘01’. And, we will replace two LSBs in the pixel P1 with‘01’.

In our approach, pixel P1 is considered to be the index of n-pixel block. Because the values of the LSBs in P1 are changed by the status of pixels P2, P3, . . . , Pn, the length of block is carefully considered.

If there are n pixels in each block, we need to use (n - 1) bits to represent the status of the pixels P2, P3, . . . , Pn. Thus, we need to change (n - 1) LSBs in the pixel P1. To preserve the quality of pixel P1 as well as to increase the embedding payload, based on the experimental results, it is suggested assigning the values of n as 3, 4 or 5.

Phase 2: To embed the secret message bits into an n-pixel block, we separate the n-pixel block into two categories corresponding to non-edge pixels category and edge pixels category. Each cover pixel in the first category contains 'x' secret message bits using the LSBs substitution technique. Each cover pixel in the second category contains 'y' secret message bits using the LSBs substitution technique. To maintain the quality of the stego image, the value of x here as 1 or 2 and 'y' as 3, 4, or 5 without causing any perceptible distortion

For example, let us consider an image A having four pixels as {[1 0 1 0 1 0 1 0], [1 0 0 0 0 0 0 0], [1 1 1 1 1 1 0 0], [0 0 0 0 1 1 1 1]} corresponding to P1, P2, P3 and P4 with the secret message S = '0 1 1 0 1 0 1'. The image A is considered to be a four-pixel block. Let us assume that based on the Canny edge detector, we determine that P2 and P4 are edge pixels. Obviously, the status of P2, P3 and P4 is '101'. Replace 3 LSBs in pixel P1 with '101'. Thus, the pixel P1 receives the new value of [1 0 1 0 1 1 0 1] and becomes pixel P1'. Let us assume that the values of parameters 'x' and 'y' are 1 and 3, respectively. Herein, we replace three LSBs in pixel P2 with three secret message bits. Also, we replace one LSB in pixel P3 with one secret message bit. Similarly, we replace three LSBs in pixel P4 with three secret message bits. The new values of pixels P2, P3 and P4 are [1 0 0 0 0 0 1 1], [1 1 1 1 1 1 0 0] and [0 0 0 0 1 1 0 1], respectively. Thus, the new value of the image A, which is called stego image A0, is {[1 0 1 0 1 1 0 1], [1 0 0 0 0 0 1 1], [1 1 1 1 1 1 0 0], [0 0 0 0 1 1 0 1]}.

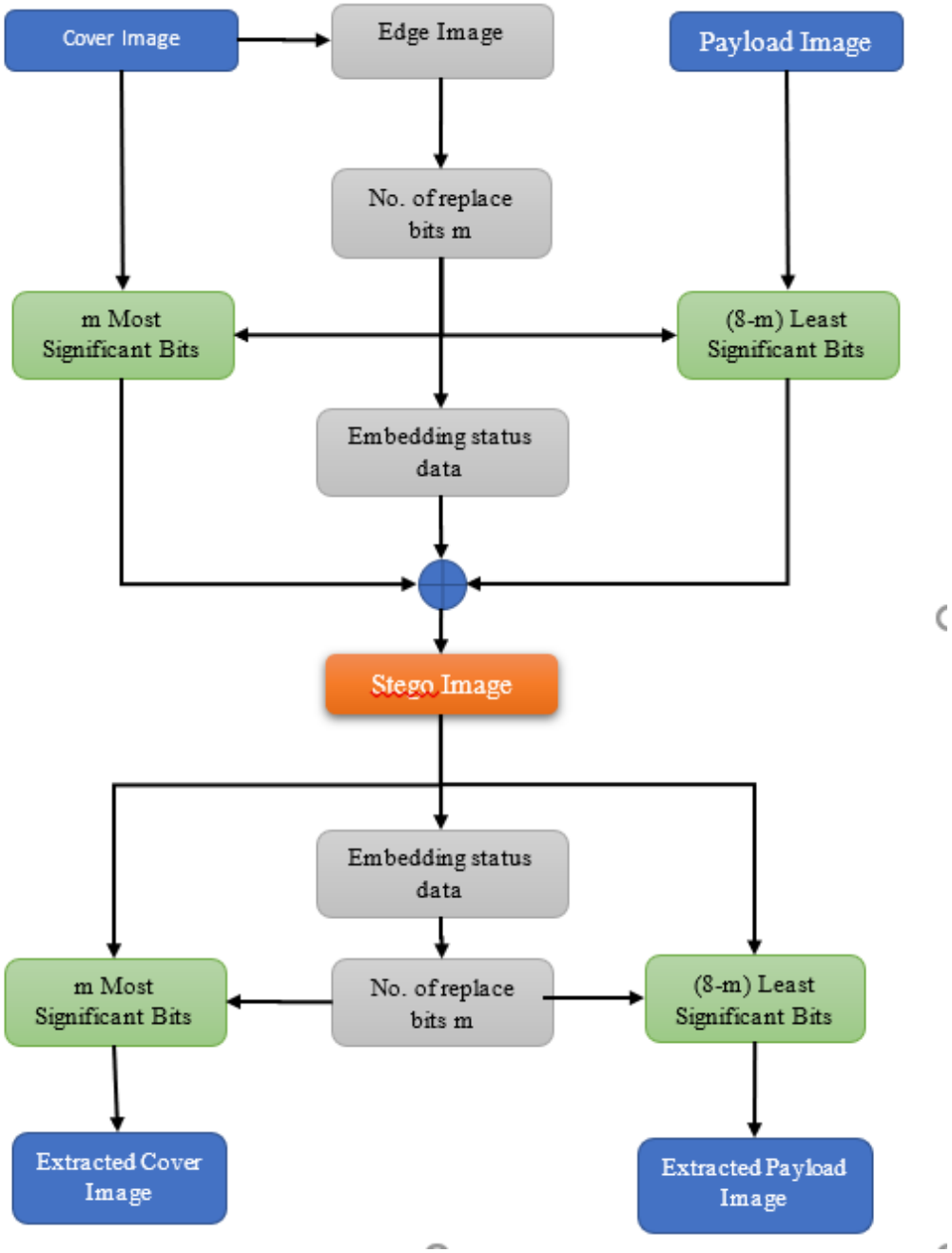
3.2.2 Extracting procedure

Phase 1: Similar to the dividing operation presented in the previous procedure. Here, we divide the stego image into a set of blocks, each block contains n pixels and is called n-pixel block. The n pixels in each block are indexed as P01; P02; . . . ; P0n.

Phase 2: Based on the (n - 1) LSBs in pixel P01, we obtain the status of the remaining pixels from P02 to P0n. From this status value, we can identify two categories corresponding to the non-edge pixels category and the edge pixels category. To extract the secret message bits, we get y LSBs from the first category and x LSBs from the second category. The secret message is generated by appending all of the LSBs from the above two categories.

For example, take a stego image A0 having four pixels as {[1 0 1 0 1 1 0 1], [1 0 0 0 0 0 1 1], [1 1 1 1 1 1 0 0], [0 0 0 0 1 1 0 1]} corresponding to four pixels P01; P02; P03 and P04. Obtain (n - 1) = 3 LSBs in the first pixel, we get three bits as'1 0 1'. Thus the second and the fourth pixels are edge pixels. And, the third pixel is a non-edge pixel. Based on the assumption of the embedding procedure, we will extract three LSBs from the pixel P02 and the pixel P04. Also, we extract one LSB from the pixel P03. The extracted bits from the pixel P02 are '0 1 1'. The extracted bit from the pixel P03 is '0'. The extracted bits from the pixel P04 are '1 0 1'. Be appending these extracted bits, we obtain the secret message as '0 0 1 0 1 0 1'.

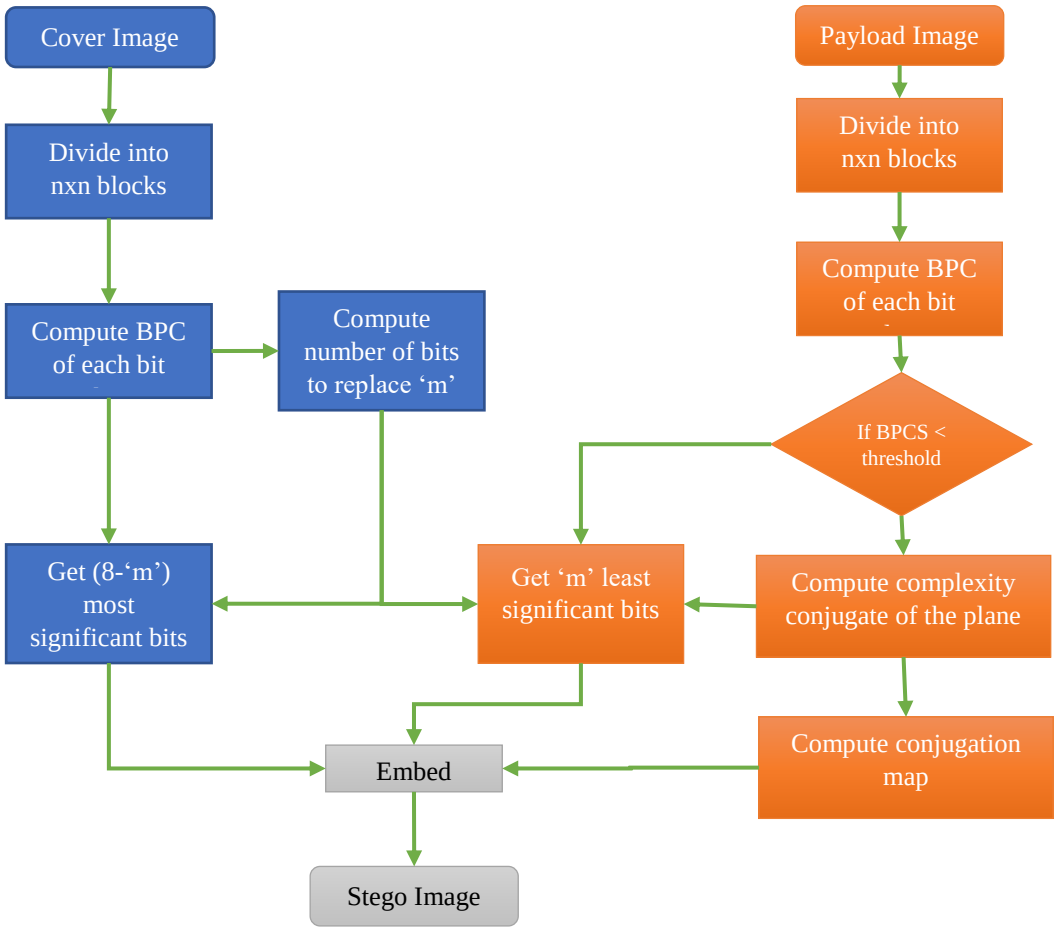
3.2.3 Flow Chart



3.3 Block Complexity Based

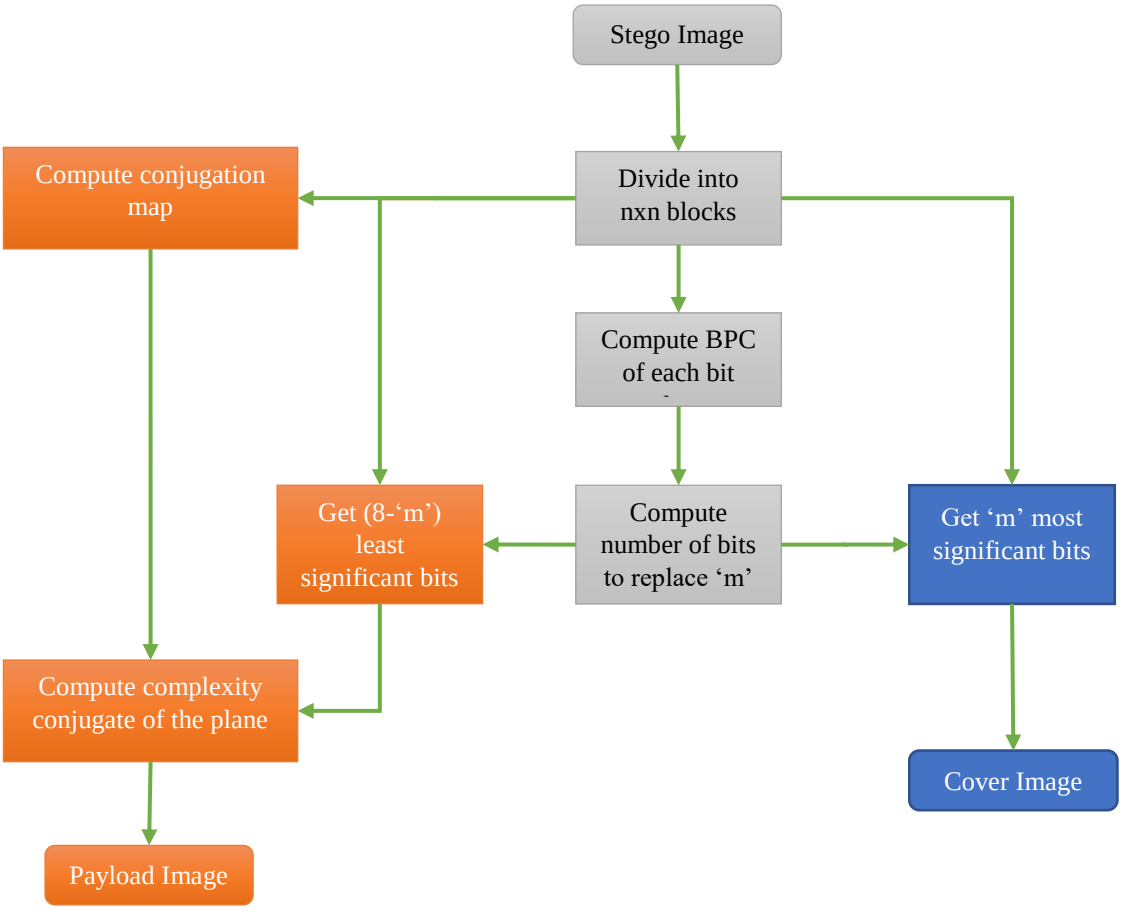
3.3.1 Embedding Process

- Segment cover image and payload image into 8x8 blocks (n=8).
- Compute the bit plane complexity of each plane of payload image
- If a payload block is less complex than the threshold a_0, conjugate it to make it more complex. Here the process called conjugation is the exclusive OR operation with a checkerboard pattern. Create a corresponding conjugation map.
- Then classify the cover image blocks into informative and noise-like blocks using a threshold of the complexity a_0. A typical value of a_0 is 0:3a_{max}, where a_{max} is the maximum possible complexity value.
- The number of bit planes to be substituted 'm' is decided by the number of noise planes in cover image. 'm' least significant bit planes of cover blocks are replaced by most significant bit planes of payload blocks.
- Also embed the conjugation map in the same way to the first pixel of each block.



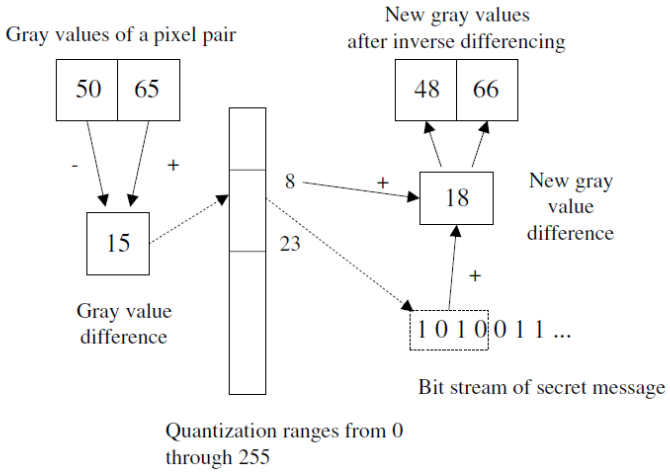
3.3.2 Extraction Process

The decoding procedure to extract the embedded payload data is just the reverse of the embedding procedure. In the decoding process, the embedding threshold a_0 and the number of replacement bits for informative and noise-like blocks.



3.4 Pixel Value Differencing

In the process of embedding a secret message, a cover image is partitioned into non-overlapping blocks of two consecutive pixels. A difference value is calculated from the values of the two pixels in each block. All possible difference values are classified into a number of ranges. The selection of the range intervals is based on the characteristics of human vision's sensitivity to gray value variations from smoothness to contrast. The difference value then is replaced by a new value to embed the value of a sub-stream of the secret message. The number of bits which can be embedded in a pixel pair is decided by the width of the range that the difference value belongs to. The method is designed in such a way that the modification is never out of the range interval. This method provides an easy way to produce a more imperceptible result than those yielded by simple least-significant-bit replacement methods.



3.5 Discrete Cosine Transform

3.5.1 Algorithm

1. Take Input as Cover Image and Secret Image. Find individual dct for both.
2. Do weighted addition in frequency domain. Secret image component will vary depending on weight used.
3. Calculate IDCT of the result of addition in step 2.
4. Write the resulting steganographic image
5. Use steganographic image along with original image to extract secret image using reverse process .
6. Take the stego image, find its DCT , subtract the DCT of original image from stego image.
7. Divide the difference by weight used in 2.
8. Compute inverse to get secret image

Equation for DCT:

The two-dimensional DCT of an M-by-N matrix A is defined as below.:

$$B_{pq} = \alpha_p \alpha_q \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} A_{mn} \cos \frac{\pi(2m+1)p}{2M} \cos \frac{\pi(2n+1)q}{2N}, \quad \begin{matrix} 0 \le p \le M-1 \\ 0 \le q \le N-1 \end{matrix}$$

$$\alpha_p = \begin{cases} 1/\sqrt{M}, & p = 0 \\ \sqrt{2/M}, & 1 \le p \le M-1 \end{cases} \quad \alpha_q = \begin{cases} 1/\sqrt{N}, & q = 0 \\ \sqrt{2/N}, & 1 \le q \le N-1 \end{cases}$$

B_{pq} - *DCT coefficients* of matrix A.

Equation for IDCT:

$$A_{mn} = \sum_{p=0}^{M-1} \sum_{q=0}^{N-1} \alpha_p \alpha_q B_{pq} \cos \frac{\pi(2m+1)p}{2M} \cos \frac{\pi(2n+1)q}{2N}, \quad \begin{matrix} 0 \le m \le M-1 \\ 0 \le n \le N-1 \end{matrix}$$

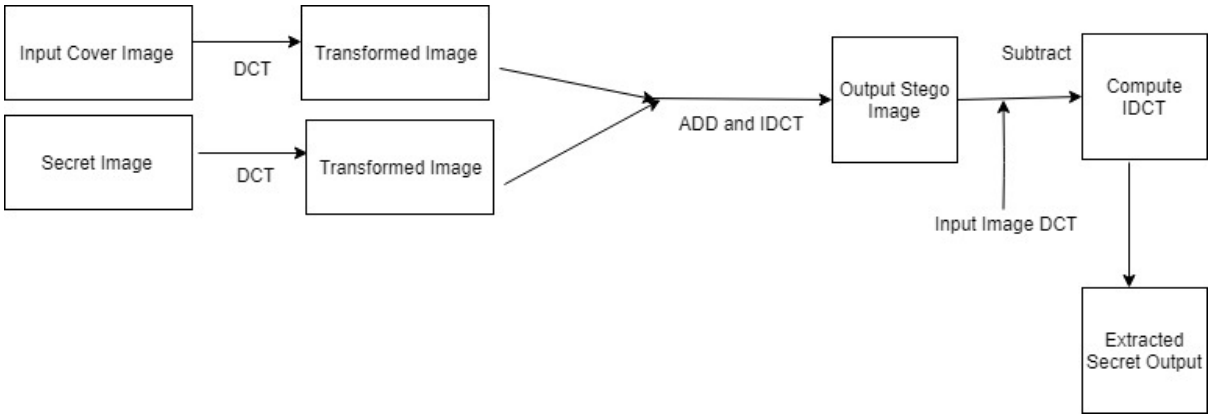
$$\alpha_p = \begin{cases} 1/\sqrt{M}, & p = 0 \\ \sqrt{2/M}, & 1 \le p \le M-1 \end{cases} \quad \alpha_q = \begin{cases} 1/\sqrt{N}, & q = 0 \\ \sqrt{2/N}, & 1 \le q \le N-1 \end{cases}$$

Interpretation of Inverse DCT equation : M-by-N matrix A can be written as a sum of *MN* functions of the form as below:

$$\alpha_p \alpha_q \cos \frac{\pi(2m+1)p}{2M} \cos \frac{\pi(2n+1)q}{2N}, \quad \begin{matrix} 0 \le p \le M-1 \\ 0 \le q \le N-1 \end{matrix}$$

$$\alpha_p = \begin{cases} 1/\sqrt{M}, & p = 0 \\ \sqrt{2/M}, & 1 \le p \le M-1 \end{cases} \quad \alpha_q = \begin{cases} 1/\sqrt{N}, & q = 0 \\ \sqrt{2/N}, & 1 \le q \le N-1 \end{cases}$$

These functions are called the *basis functions* of the DCT. The DCT coefficients B_{pq}, can be regarded as the *weights* applied to each basis function.



3.6 Exploiting Modification Direction (EMD)

3.6.1 Algorithm:

1.Take Input as Cover Image and secret text data .

2 . To do block wise data hiding, group the cover image pixels in block of appropriate size(say n)

2. Compute s =secret mod(2n+1), n- no of pixels in each image block.

4. For each block compute Femd and d using given equations : d = (s – Femd)mod(2n+1)

5. Based on d value one pixel in the block is modified by +/- 1.

6. For reverse process , recover secret data s' using F'emd calculation again

7. Compute output = s' mod(2n+1)

Equation for embedding:

$$f_{EMD} = [\sum_{i=1}^{n}(g_i \times i)] mod(2n+1)$$

gi - the pixel value within selected block

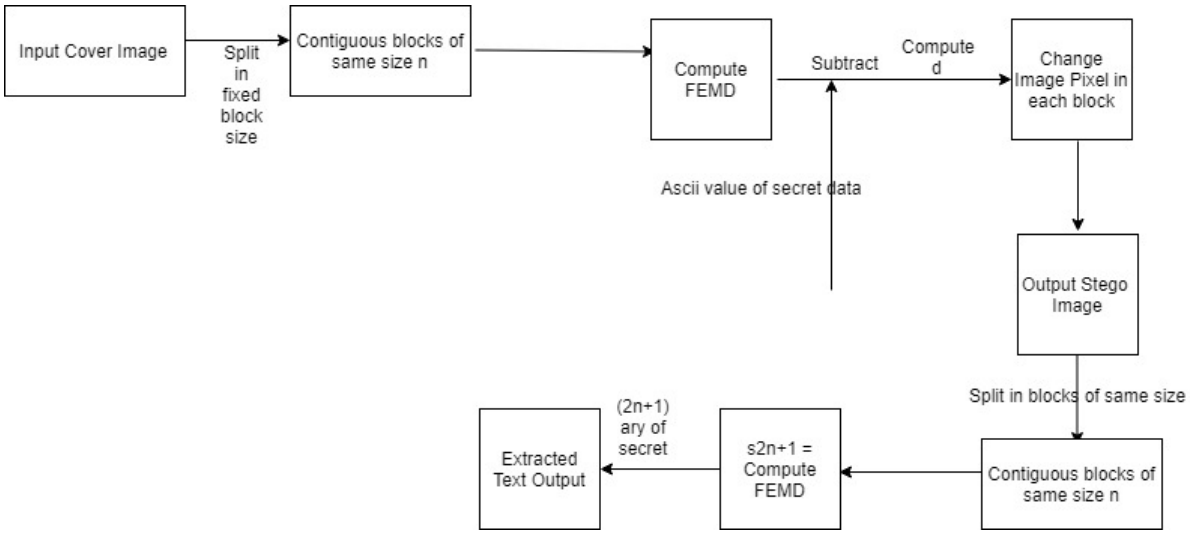
n – number of pixels in selected block

$$d = (s_{(2n+1)} - f_{EMD}) mod(2n+1).$$

$s_{(2n+1)}$ = (ascii of secret character)mod(2n+1)

Equation for extraction

$$\text{Compute } s_{(2n+1)} = f'_{EMD} = [\sum_{i=1}^{n}(g'_i \times i)] \; mod(2n+1).$$



3.7 Sparse pixels from histogram and Euclidean distance Measure in spatial domain

3.7.1 Algorithm:

1.Input is Cover Image and Secret Text . Convert secret text to ascii and then to binary. Secret data can also be an image.

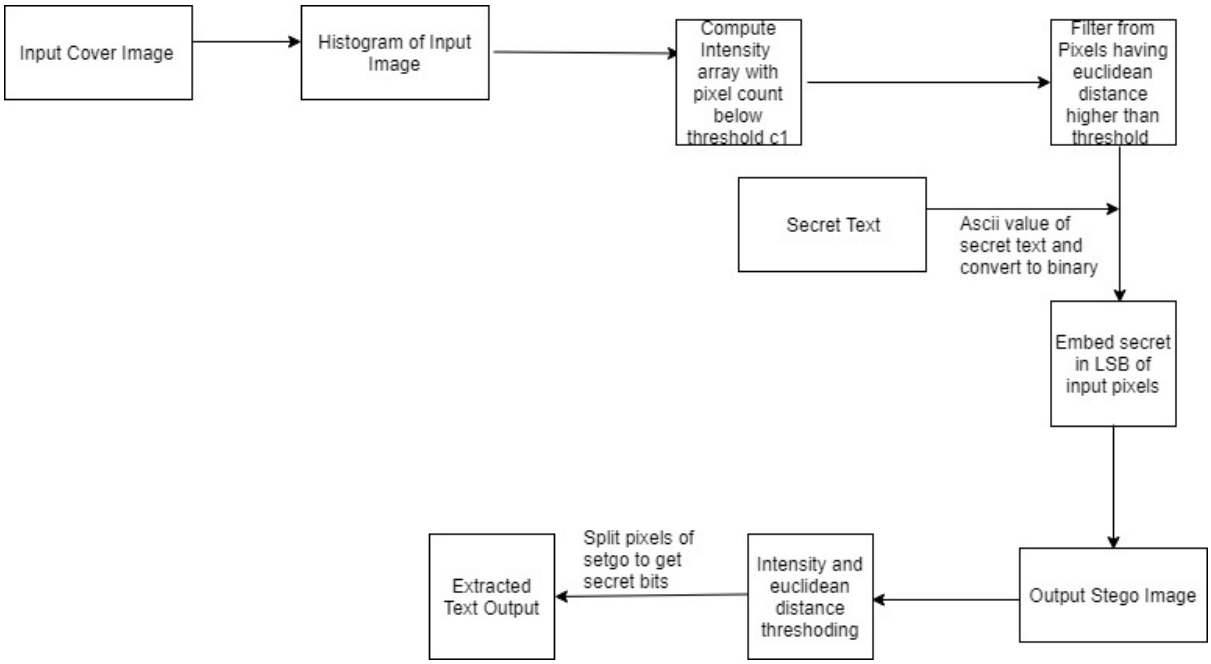
2. Create Histogram of Input Image

3. Create an array of intensity values having pixel count below some value(idea is to use sparse pixels)

4. For embedding secret data pick the pixels having intensity values from step 2 and have euclidean distance above certain threshold.

5. Insert bits from secret data into LSB bits of image pixels picked in step 4.

6. For extraction process do the same steps. Instead of adding bits, split the bits of pixels in stego image.



4 Experimental Results and discussions

4.1 Evaluation metric:

Mean square error and peak signal to noise ratio given by:

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

The PSNR is defined as:

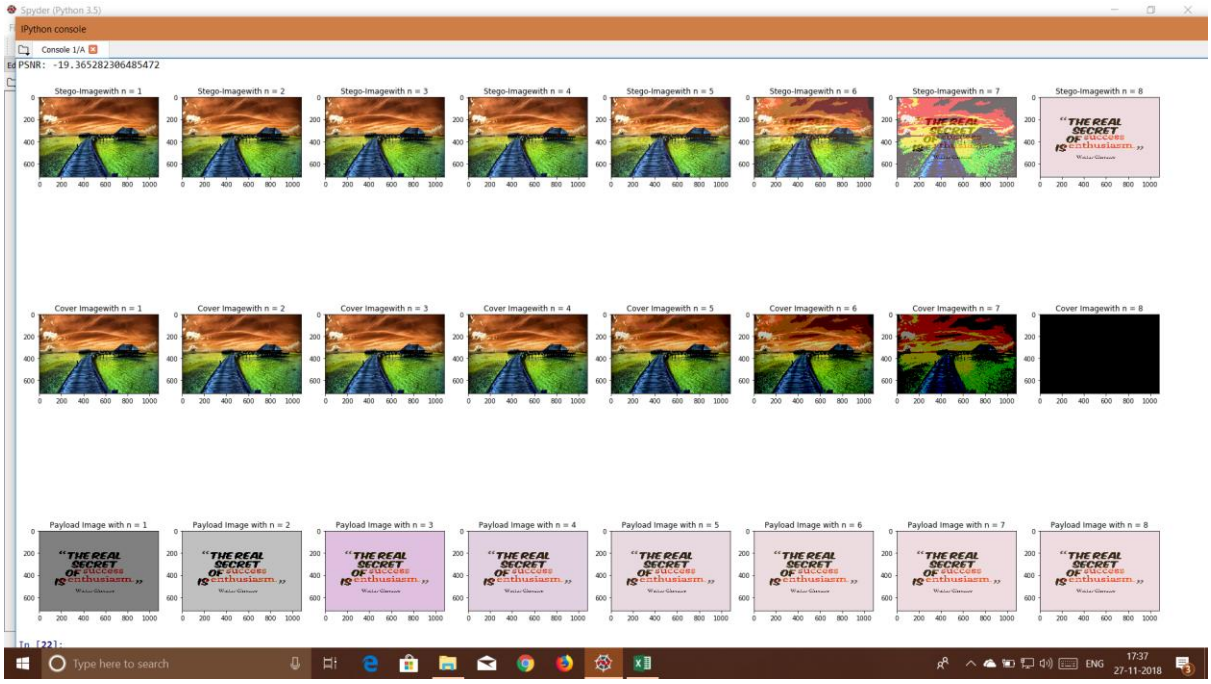
$$PSNR = 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$
$$= 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right)$$

4.2 Least Significant Bit Substitution

4.2.1 Output images

Input cover and payload:

Stego and extracted images:



4.2.2 Analysis:

NO. OF REPLACE BITS	PSNR	MSE
3	36.12	15.88
4	29.646	70.54
5	27.794	108.04
6	27.55	114.27

LSB substitution is the simplest method.

But it does not take into account the characteristics of cover or payload image.

Increasing the number of bits n decreases the visual quality of stego-image

4.3 Edge Based

4.3.1 Output images

Cover image Payload Image

Stego Image:

Extracted cover and payload images:

4.3.2 Analysis

Images with more edges can be embedded with more bits on these images. This method exploits this property.

Embedding status bits causes an overhead reducing the size of payload that can be embedded.

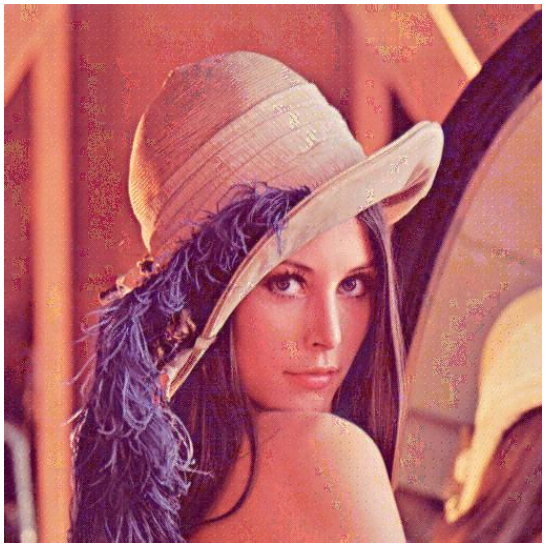
This method gave an average PSNR of 44.803 and MSE of 2.14

4.4 Block Complexity Based

4.4.1 Output images

Cover image Payload Image

Stego Image:



Extracted cover and payload images:

4.4.2 Analysis

Block complexity method relies solely on the complexity of the blocks estimated. This does not guarantee the classification of noise and informative blocks. Moreover the performance ifs affected by the block size. This method gave an average PSNR of 30.68 and MSE of 60.40

4.5 Pixel Value Differencing

4.5.1 Output images

Cover image Payload Image

Stego Image:

Extracted cover and payload images:

4.5.2 Analysis

PVD uses difference between pixels to extract embedding parameters and hence does not require any external parameter.

It embeds more bits where gradient is large (i.e. edges). It has faster performance than edge based method. The amount of quantization can be tuned in the algorithm for better visual quality.

4.6 Discrete Cosine Transform

4.6.1 Output Images:

Input Image

Secret Image

Output Stego Image:

Output Secret Image:

4.6.2 Evaluation result:

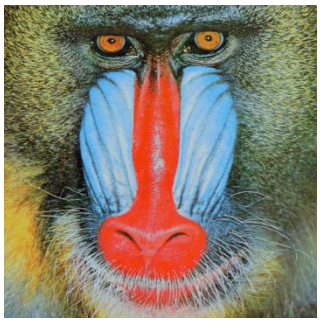
Method	**Image**	**Weight**	**PSNR**	**MSE**
DCT				
	Cameraman.png	0.1	29.09	80.14
		0.5	28.319	95.749
	Room_512.jpeg	0.07	28.588	90.007
		0.5	27.92	104.81
	House_225.jpeg	0.007	27.87	106.18
		0.5	27.81	108.59

4.6.3 Analysis:

Discrete Cosine Transform Method: In spatial domain anyone who knows the steganographic system can retrieve the hidden message. This is not easily possible with the DCT insertion method, as changes takes place in the frequency domain inside the image . Frequency Domain creates comparatively robust system as compared to spatial domain. If the weight of emebedding is kept high the secret image is visible in cover image but extraction of secret image is less lossy(can be recovered).However if weight of embedding is kept low then secret image is not visible in cover image but extraction of secret image doesnot happen properly. There is information loss.

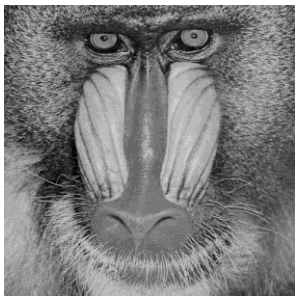
4.7 Exploiting Modification Direction (EMD)

Input Cover Image:



Input Text : fly high

Output Stego Image:



4.7.1 Analysis:

It uses a group of n cover-pixels to embed secret data due to which it achieves good image quality and high security level of resisting RS detection.

4.8 Sparse pixels from histogram and Euclidean distance Measure in spatial domain

Input Cover Image:

Input Text : conference

Output Stego Image:

4.8.1 Analysis:

In this method since sparse pixels are used along with euclidean distance criteria, it is not obvious to decode and extract secret message. Moreover we can change the number of bits and position in cover image pixel where the secret message should be inserted which makes it even more robust.

5 Successes:

5.1 DCT Method

Can embed and extract secret image without breaking secret image in blocks. Whole secret image can be used with one time operation of embedding.

6 Failures:

6.1 Discrete Cosine Transform Method:

DCT being lossy method involving magnitude and phase components , breaking the image in standard 8 by 8 block for embedding and extraction requires better handling which is yet to be implemented.

6.2 Exploiting Modification Direction Method:

Extraction is partly successful.

6.3 Sparse Pixels and Euclidean distance:

There appears to be problem in extraction with colour images. Since there is change in intensity values, few pixels in stego image may not meet the criteria of intensity and Euclidean threshold. Since all the bits are not embedded (4 MSB from secret embedded in 4 LSB of cover image), extraction is lossy.

7 Conclusion And Future Work

This project presented a background discussion on the basic algorithms of image steganography deployed in digital imaging. The algorithms have been implemented and the output has been evaluated.

Steganography is an developing field of data cryptography. Future work must focus on improving the imperceptibility of the stego image. Many other adaptive features based on the content can be used to increase the embedding capacity of the images. Like DCT other transforms like DWT can also be used. Steganography system must be made robust to compression and other image processing application. It can also be incorporated with traditional cryptography.

8 References

Digital image steganography: Survey and analysis of current methods, Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt.

A steganographic method for images by pixel-value differencing, Da-ChunWua, Wen-Hsiang Tsaib.

High payload steganography mechanism using hybrid edge detector, Wen-Jan Chen, Chin-Chen Chang, T. Hoang Ngan Le

Principle and applications of BPCS steganography, E.Kawaguchi, R.O.Eason.

BPCS steganography using EZW lossy compressed images, Jeremiah Spaulding, Hideki Noda, Mahdad N.Shirazi , Eiji Kawaguchi

Enhance Embedding Capacity of Generalized Exploiting Modification Directions in Data Hiding, Y. Liu, C. Yang and Q. Sun.

A comparative analysis of image steganography based on DCT algorithm and steganography tool to hide nuclear reactors confidential information, Sahar A.El_Rahman.