IMPLEMENTATION OF AN ADVANCED IMAGE STEGANOGRAPHY TECHNIQUE USING MODIFIED DATA IMAGE

Thesis report submission in the partial fulfillment of the

Requirement for the award of the degree of

MASTERS OF TECHNOLOGY

in

VLSI DESIGN

Submitted by

Akash Modi

Roll No: 601361002

Under the Guidance of

Mrs. Manu Bansal

Assistant Professor, ECED

DEPARTMENT OF ELECTRONICS AND COMMUNICATION

ENGINEERING

THAPAR UNIVERSITY, PATIALA (PUNJAB) – 147004

JULY-2015

CERTIFICATE

I hearby declare that the work which is being presented in the thesis entitled "**Implementation of an advanced image steganography technique using modified data image**" in partial fulfillment of the requirement for the award of degree of M.Tech. (VLSI Design) at Electronics and Communication Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of Mrs. Manu Bansal, Assistant Professor, ECED.

The matter presented in this thesis has not been submitted in any other University/Institute for the award of my degree.

Date: 10/7/15

Akash Modi

Roll No: 601361002

It is certified that the above statement made by the student is correct to the best of my knowledge and belief.

Mrs. Manu Bansal 10/7/15

Assistant Professor

ECED, Thapar University

Counter signed by:

Dr. Sanjay Sharma

Professor & Head

ECED, Thapar University

Patiala-147004

Dr. S. S. Bhatia

Dean of Academic Affairs

Thapar University

Patiala-147004

ACKNOWLEDGEMENT

I take this opportunity to express my profound sense of gratitude and respect to all those who helped me through the duration of this thesis. I would have never succeeded in completing my task without the cooperation, encouragement and help provided to me by various people. Words are often too less to reveal one's deep regards. I acknowledge with gratitude and humility my indebtedness to **Mrs. Manu Bansal, Assistant Professor**, Electronics and Communication Engineering Department, Thapar University, Patiala, under whose guidance I had the privilege to complete this thesis. I wish to express my deep gratitude towards her for providing individual guidance and support throughout the thesis work.

I convey my sincere thanks to **HEAD OF THE DEPARTMENT, Dr. Sanjay Sharma** as well as **PG Coordinator, Dr. Amit Kohli** Associate Professor, **Programme Coordinator, Dr. Anil Arora** Assistant Professor**,** Electronics and Communication Engineering Department, entire faculty and staff of Electronics and Communication Engineering Department for their encouragement and cooperation.

My greatest thanks to all who wished me success especially my parents and other family members and friends without whom I would not have been able to complete my thesis work.

I thank and own my deepest regards to all of them and all others who have helped me directly or indirectly.

Akash Modi

ABSTRACT

The science of secret communication is known as steganography. Steganography is a Greek word, which means covered writing. Steganography hides the secret data from unauthorized user. Unlike cryptography, steganography hides the existence of secret information rather than hiding its meaning only. Many different file formats can be use as cover media but these days the digital image based steganography is most popular on internet and web. The capacity of hiding secret data is limited in steganography and it depends on size of the cover image. There is a tradeoff between the stgo image quality and the capacity of steganography. Therefore, the quality of stego image and capacity of steganography are still a challenging field and this is the goal of proposed method.

In this thesis, a new image steganography technique has been proposed. In this technique the secret data is change into a new format. The new data cannot be decoded without knowing the actual algorithm. In this new data, there is less counts of number of '1' compare to original data, due to this mostly the stego image's pixel value follows the cover image pixels value after using the XORing method between the cover image and the secret data. In this thesis, Lenna image has been used as reference image and after applying this method, the count of number of '1' has been reduced by 20%(nearly) compare to the original data. By using proposed method, not only the security of secret data increases but also it increases the quality of the stego image. The result shows that the proposed method improved the value of PSNR and MSE of the stego image and it fulfills all the aspects of image steganography. In this thesis, various data images and various cover images have been analyzed.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

LSB:	Least Significant Bit
MSB:	Most Significant Bit
MSE:	Mean Square Error
JPG:	Joint Photographic Expert Group
TIFF:	Tag Index File Format
GIF:	Graphic Intercharge Format
BMP:	Bitmap Image
PNG:	Portable Network Graphics
AES:	Advanced Encryption Standard
DES:	Data Encryption Standard
MED:	Median Edge Detection
PSNR:	Peak Signal to Noise Ratio
ASCII:	American Standard Code for Information Interchange

CHAPTER 1
INTRODUCTION

The information security has been a big challenge in field of communication since the rise of the internet. This can be achieved by securing the information or the channel. Cryptography was introduced as atechnique for securing the secrecy of communication and many different techniques have been developed to encode and decode information in order to keep the message secret. Unfortunately, sometimes it is not enough to keep the information secret, it may also be necessary to keep the existence of the information secret. The technique used to implement this is called steganography [4].

Steganography is the art and science of invisible communication. This can be accomplished by hiding the information into other information, thus hiding the existence of the communicated information. The word steganography is derived from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing" defining it as "covered writing". In image steganography, the information is hidden exclusively in images.

1.1. HISTORY OF STEGANOGRAPHY

The idea and practice of hiding information has a long history. In histories the Greek historian Herodotus writes of a nobleman, Histaeus, who needed to communicate with his son-in-law in Greece. He shaved the head of one of his most trusted slaves and tattooed the message onto the slave's scalp. When the slave's hair grew back the slave was dispatched with the hidden message. In the Second World War the Microdot technique was developed by the Germans. Information, especially photographs, was reduced in size until it was the size of a typed period. Extremely difficult to detect, a normal cover message was sent over an insecure channel with one of the periods on the paper hidden information. These days steganography is mostly used on computers with

digital data being the secret information and networks being the high speed delivery channels[14] [15].

The term steganography was first coined by an occultist, namely Trithemius. The main aim in steganography is to hide the very existence of the message in the cover medium. steganography includes a vast array of methods of secret communication that conceal the very existence of hidden information. Traditional methods include use of invisible inks, microdots etc. Modern day steganographic techniques try to exploit the digital media images, audio, video etc.

Its ancient origins can be traced back to 440 BC. Although the term steganography was only coined at the end of the 15th century, the use of steganography dates back several millennia. In ancient times, messages were hidden on the back of wax writing tables, or written on the stomachs of rabbits. Invisible ink has been in use for centuries for fun by children and students and for serious undercover work by spies and terrorists. Steganography is an art of conveying secret messages and secret images through cover images in a secret way that only the receiver knows the existence of a message.

Recently, the United States government claimed that the Osama Bin Laden and the al-Qaeda organization have communicated through websites and newsgroups to send messages using steganography. However, until now, no substantial evidence supporting this claim has been found, so either al-Qaeda has used or created real good steganographic algorithms, or the claim is probably false.

Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret [3][19][21]. Steganography and cryptography are the efficient ways to protect information from unwanted parties but technology alone is not perfect and cannot be compromised. If the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated. The strength of steganography can thus be amplified by combining it with cryptography.

Research in steganography has emerged mainly because of the lack of strength in cryptographic systems. Many government organizations have created laws to either limit the strength of a cryptographic system or to prohibit it altogether by forcing people to study other techniques of securing information transfer. Multi-national companies have also realized the potential of steganography in communicating trade secrets or new product information. Avoiding communication through well-known channels greatly reduces the risk of information being leaked in transit. Communication using the photograph of company picnic is less suspicious than through encrypted file.

1.2. OVERVIEW OF STEGANOGRAPHY

The three main terminologies used in the steganography systems are: the cover message, secret data message and embedding algorithm. Secret key terminology can also be introduced to provide more secure communication. The cover message is the carrier of the message such as image, video, audio, text, or some other digital media [14] [15]. The secret message is the information that is needed to be hidden in the suitable digital media. The secret key is usually used to embed the message depending on the hiding algorithms. The embedding algorithm is the idea or the way that is used to embed the secret information in the cover message.

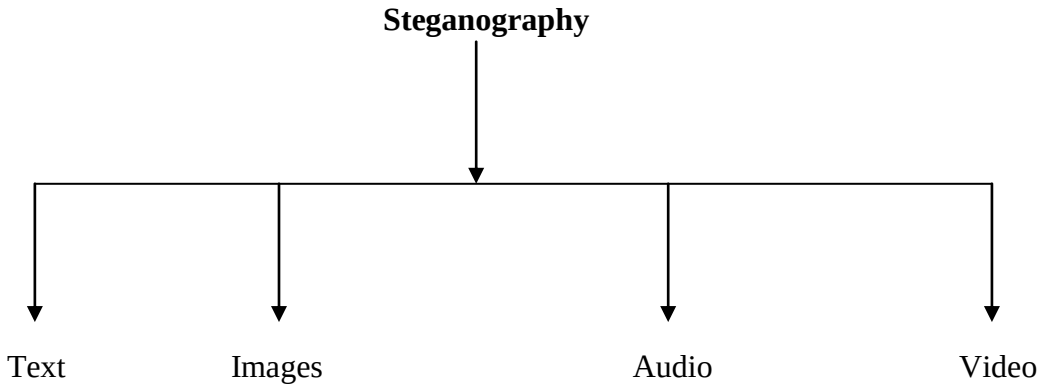


Figure 1.1: Categories of Steganography

All digital file formats can be used for steganography as cover message. The degree of redundancy decides which format is more suitable. Higher the degree of redundancy more suitable is the format. Redundancy can be defined as the bits of an object that

provide accuracy far greater than necessary for the object's use and display. The redundant bits of an object can be altered without the alteration being detected easily. Image and audio files especially comply with this requirement, while research has also uncovered other file formats that can be used for data hiding. Figure 1.1 shows the four main categories of file formats that can be used for steganography.

Hiding information in text is the most important method of steganography. In this method secret message is hidden in every N^{th} letter of every word of a text message. Since the beginning of the Internet and all different digital file formats, it has decreased in importance. Text steganography using digital files is not used very often since text files have a very small amount of redundant data [31][32].

Given the proliferation of digital images, especially on the Internet, and given the large amount of redundant bits present in the digital representation of an image, images are the most popular cover objects for steganography.

To hide information in audio files similar techniques are used for image files. One different technique unique to audio steganography is masking, which exploits the properties of the human ear to hide information unnoticeably. A faint but audible sound becomes inaudible in the presence of another louder audible sound. This property creates a channel in which to hide information. Although nearly equal to images in steganographical potential, the larger size of meaningful audio files makes them less popular to use than images.

Digital steganography is the art and science of hiding communications; a steganographic system thus embeds secret data in public cover media so as not to arouse an eavesdropper's suspicion. A steganographic system has two main aspects: steganographic capacity and imperceptibility. However, these two characteristics are at odds with each other. It is quite difficult to increase the steganographic capacity and simultaneously maintain the imperceptibility of a steganographic system. Additionally, there are very limited methods of steganography with communication protocols, which presents unconventional but promising steganography mediums.

Digital image steganography is a method of secret communication, aims to convey a large amount of secret data, relatively to the size of cover image, between communicating parties. Additionally, the aim is to avoid the suspicion of non-communicating parties to this kind of communication. Thus, this research addresses and proposes some methods to improve these fundamental aspects of digital image steganography. Hence, some characteristics and properties of digital images have been employed to increase the steganographic capacity and enhance the stego image quality (imperceptibility).

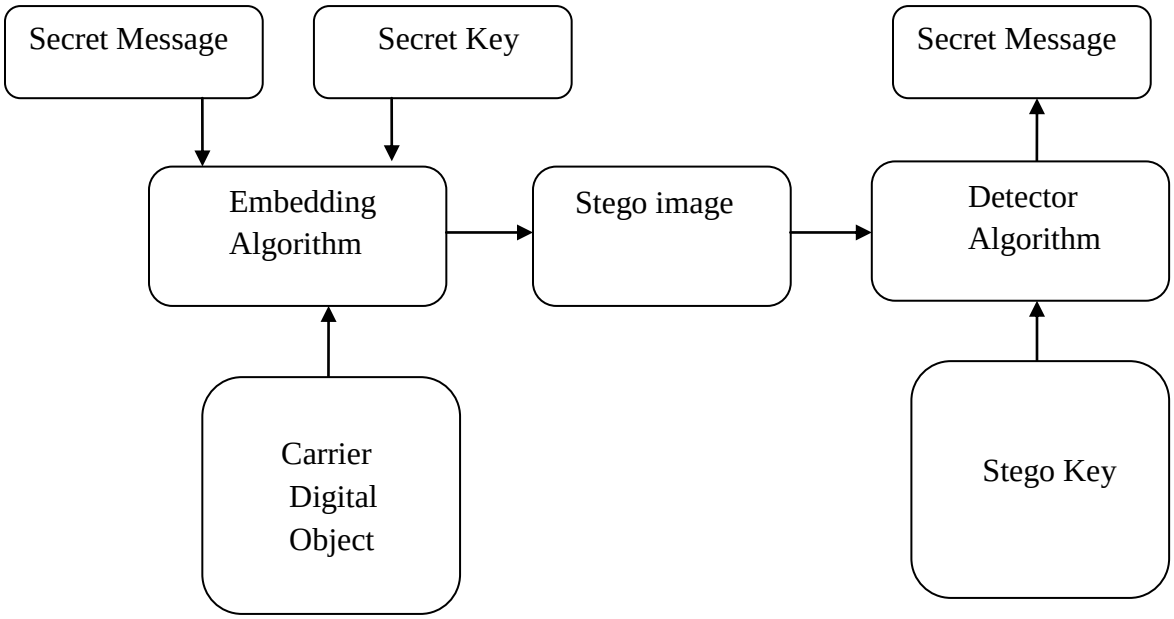


Figure 1.2: A model of Steganography

In steganography system scenario, before the hiding process, the sender has to select the appropriate message carrier (i.e. image, video, audio, text) and choose the effective secret messages as well as the secret key (which suppose to be known by the receiver). The effective and appropriate steganography algorithm must be selected that can encode the message in more secure technique. Then the sender may transfer the stego file by email or chatting, or by other modern techniques. The stego file is the carried message with the secret information. After receiving the message by the receiver, he can decode it by using the extracting algorithm and the same secret key used by the sender. The steganography system scenario is shown in the Figure 1.2.

• The cover message is the carrier of the message such as image, video, audio, text, or some other digital media. The secret message is the information which is needed to be hidden in the suitable digital media.

• The secret key is usually used to embed the message depending on the hiding algorithms. The embedding algorithm is the way or the idea that usually use to embed the secret information in the cover message.

Almost all digital file formats can be used for steganography as cover message, but the formats that are more suitable are those with a high degree of redundancy. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object's use and display. The redundant bits of an object are those bits that can be altered without the alteration being detected easily. Image and audio files especially comply with this requirement, while research has also uncovered other file formats that can be used for information hiding.

1.3. EVALUATION OF DIFFERENT TECHNIQUES

All the above mentioned algorithms for image steganography have different strong and weak points and it is important to ensure that one uses the most suitable algorithm for an application. All steganographic algorithms have to comply with a few basic requirements. The most important requirement is that a steganographic algorithm has to be imperceptible. A set of criteria to further define the imperceptibility of an algorithm has been proposed [14][15][17]. These requirements are as follows:

(i) **Invisibility** – The invisibility of a steganographic algorithm is the first and foremost requirement, since the strength of steganography lies in its ability to be unnoticed by the human eye. The moment that one can see that an image has been tampered with, the algorithm is compromised.

(ii) **Payload capacity** –: Steganography aims at hidden communication and therefore requires sufficient embedding capacity. In the real time systems the payload capacity directly refers to embedding rate for information, which is critical for any real time system.

(iii) **Robustness against statistical attacks** – Statistical steganalysis is the practice of detecting hidden information through applying statistical tests on image data. Various steganographic algorithms leave a 'signature' when embedding information that can be easily detected through statistical analysis. To be able to pass by a warden without being detected, the algorithm must not leave such a mark in the image as be statistically significant.

(iv) **Robustness against image manipulation** – In the communication of a stego image by trusted systems, the image may undergo changes by an active warden in an attempt to remove hidden information. Image manipulation, such as cropping or rotating, can be performed on the image before it reaches its destination. These manipulations may destroy the hidden message depending on the manner in which the message is embedded. It is preferable for steganographic algorithms to be robust against either malicious or unintentional changes to the image.

(v) **Independent file format** – With many different image file formats used on the internet, it might seem suspicious that only one type of file format is continuously communicated between two parties. The most powerful steganographic algorithms thus possess the ability to embed information in any type of file. This also solves the problem of not always being able to find a suitable image at the right moment, in the right format to use as a cover image.

If the probability distribution of the cover and the stego images are identical then this technique is said to be perfectly secure. There exist some steganography schemes which are perfectly secure. The detect-ability function is more suitable for analyzing image steganography schemes where the embedding capacity is very low. More appropriate measure for visual distortion in image steganography with high embedding capacity is Peak Signal to Noise Ratio (PSNR).

Peak signal-to-noise ratio (PSNR) measures the quality of the stego-image compared with the cover image in decibels [35][36]. The higher PSNR value shows the better quality. PSNR is computed using the following equation:

$$\text{PSNR} = 10\log_{10}\frac{255^2}{\text{MSE}} \tag{1.1}$$

Mean Squared Error (MSE) is computed by performing byte by byte comparisons of the cover image and the stego-image [37]. The computation can be expressed as follows:

$$\text{MSE} = \frac{1}{m*n}\sum_1^m \sum_1^n \left(C_{ij} - S_{ij}\right)^2 \tag{1.2}$$

m: number of rows of cover image

n: number of column in cover image

C_{ij}: pixel value from cover image

S_{ij}: pixel value from stego image

Higher value of MES indicates dissimilarity between cover image and stego image.

1.4. TYPE OF STEGANOGRAPHY

Images:

Images have been most popular cover medium to implement steganography. A lot of research has already been done to develop and implement steganographic algorithms involving images. Most of the work has been done to implement these algorithms on software level using image processing tools like MATLAB. A variety of formats are adopted for digital images like .jpg, .gif, .tif, .bmp etc. Images are also preferred due to their omni presence on recent social networking platforms and other websites as well. However, very few implementations of all these algorithms have been done on hardware.

Broadly, steganographical techniques involving image can be classified in these categories:

(i) Spatial Domain Techniques:

In spatial domain methods a steganographer modifies the secret data and the cover medium in the spatial domain, which involves encoding at the level of the LSBs. This method is although simpler and has a larger impact. The pixels gray level and their color values can be directly used to encode the message bits. These algorithms are applicable to lossless image compression schemes like .tiff images

Major drawback of this technique is that spatial domain algorithms are well known. Thus any staganalysis attack aimed to bit manipulation can easily detect secret information. This technique can be developed using MATLAB code.

Advantages:

- Degradation of the original image is not easy.
- Hiding capacity is more i.e. more information can be stored in an image.

Disadvantages:

- Robustness is low.
- Hidden data can be destroyed by simple attacks.
- Additive noise in the stego image.

(ii) Transform Domain:

A more complex way of hiding a secret data inside an image comes with the use and modifications of discrete cosine transformations. Discrete cosine transformations (DCT) are used by the JPEG compression algorithm to transform successive 8 x 8 pixel blocks of the image, into 64 DCT coefficients each.

The LSB of the quantized DCT coefficient can be used to hide information. Lossless compressed images will be susceptible to visual alterations when the LSB are modified. This is not the case with the above described method, as it takes place in the frequency domain inside the image, instead of the spatial domain and therefore there will be no visible changes to the cover image, and image processing. Some transform domain

techniques do not seem dependent on the image format. Transform domain techniques are of different types [22]:

1. Discrete Fourier transformation technique (DFT).
2. Discrete cosine transformation technique (DCT).
3. Discrete Wavelet transformation technique (DWT).

(iii) Masking and Filtering:

Masking and filtering techniques, usually restricted to 24 bits RGB or grayscale images, take a different approach to hiding a message. These methods are effectively similar to paper watermarks, creating patterns in an image. This can be achieved for example by modifying the luminance of parts of the image [21]. While masking modifies the visible properties of an image, it can be done in such a way that the human eye will not notice the difference.

Since masking uses visible aspects of the image, it is more robust than LSB modification with respect to compression, cropping and different kinds of digital image processing. The information is not hidden at the ”noise” level but is inside the visible part of the image, which makes it more suitable than LSB modifications in case a lossy compression algorithm like JPEG is being used.

Advantages:

- This method is much more robust than LSB replacement with respect to compression.

Disadvantages:

- Techniques can be applied only to gray scale images and restricted to 24 bits.

Audio:

Hiding information inside audio files can be done in several ways. Using the LSBs is possible, as modifications will usually not create audible changes to the sounds [14].

Another method involves taking advantage of human hearing system limitations. Human are not able to hear the audio above 20 kHz so by using any frequencies above 20 kHz, messages can be hidden inside sound files and will not be detected by human checks.

Also, a message can be encoded using musical tones with a substitution scheme. For example, a 'A' is tone will represent a 0 and a 'B' tone represents a 1. A normal musical piece can now be composed around the secret message or an existing piece can be selected together with an encoding scheme that will represent a message.

Video:

The collection of images and sounds are known as video files, so most of the presented techniques prescribed on images and audio can be applied to video files as well [14]. The great advantages of video are the large embedding capacity of data that can be hidden inside it and the fact that it is a moving stream of images and sounds. Therefore, any small but otherwise noticeable distortions might go by unobserved by human perception because of the continuous flow of information.

1.5 STEGANALYSIS

Steganalysis is the science of detecting the presence of hidden data in the cover media files and is emerging in parallel with steganography. Steganalysis has gained prominence in national security and forensic sciences since detection of hidden (cipher text or plaint ext) messages can lead to the prevention of disastrous security incidents. Steganalysis is a very challenging field because of the scarcity of knowledge about the specific characteristics of the cover media (an image, an audio or video file) that can be exploited to hide information and detect the same. The approaches adopted for steganalysis also sometimes depend on the underlying steganography algorithms used. Image steganalysis algorithms explore the strong inter-pixel dependencies that are characteristic of natural images. Audio steganalysis algorithms are based on characteristic aspects such as the distortion measure of the audio signal, high-order statistics and etc. Video steganalysis algorithms exploit the spatial and temporal

redundancies in the video signals within the individual frames and at inter-frame level [3] [23].

1.6. COMPARISON OF STEGANOGRAPHY, WATERMARKING AND CRYPTOGRAPHY

Cryptography and steganography are well known and widely used techniques that manipulate information in order to cipher or hide their existence respectively. Steganography is the art and science of communicating in a way which hides the existence of the communication. Cryptography scrambles a message so it cannot be understood; the steganography hides the message so it cannot be seen. Even though both methods provide security, a study is made to combine both cryptography and steganography methods into one system for better confidentiality and security. The trio steganography, watermarking and cryptography serve the same purpose to secure data and to hide it from unauthorized access [16]. There are some stark differences, which can be summarized in table 1.1.

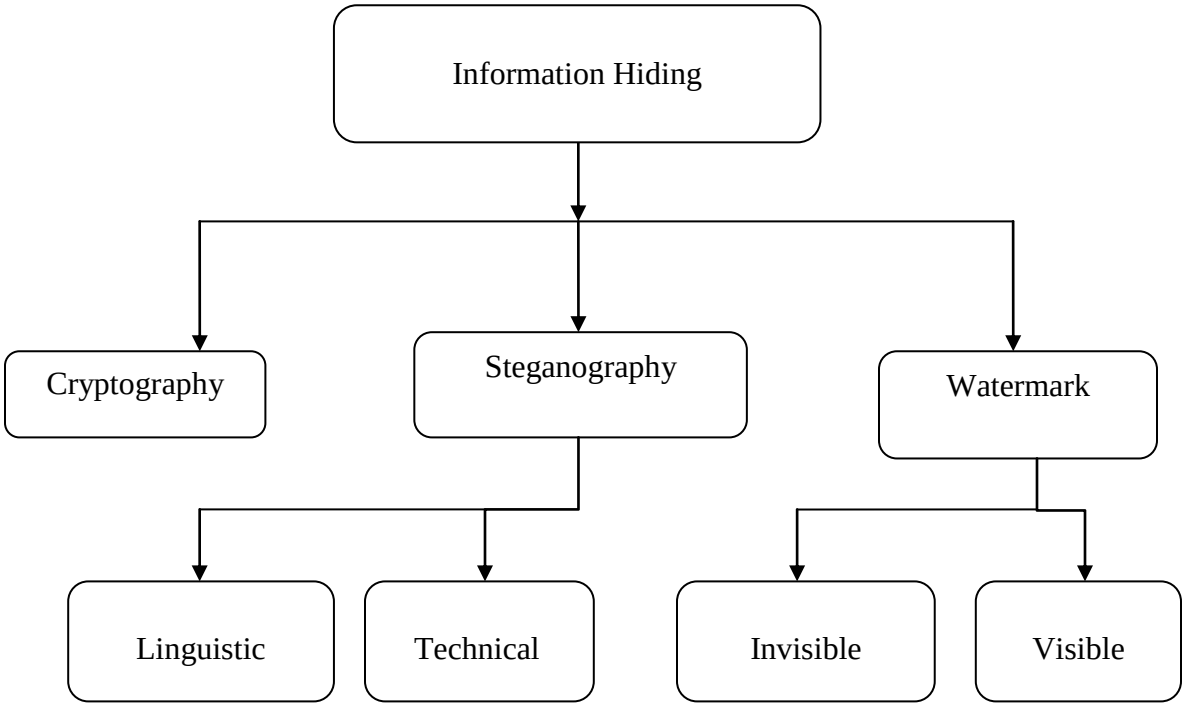


Figure 1.3: Information Hiding Techniques

Table 1.1: Comparison of Steganography, Watermarking and Cryptography

Criterion/ Method	Steganography	Watermarking	Cryptography
Carrier	Any digital media	Mostly image/audio files	Usually text based, with some extensions to image files
Secret Data	Payload	Watermark	Plain text
Key	Optional	N/A	Compulsory
Input File	2	1	1
Objective	Secrete communication	Copyright preserving	Data protection
Concern	Delectability/capacity	Robustness	Robustness
Type of Attack	Steganalysis	Image processing	Cryptanalysis
Detection	Usually Blind	Usually achieved by cross correlation	Full retrieval of data
Visibility	Never	It is removed/replaced	De-ciphered
Flexibility	Free to choose any suitable cover	Cover choice is restricted	N/A

1.7. THESIS ORGANIZATION

This report is organized into five chapters briefed as under:

Chapter1: In this chapter we introduce the steganography, different categories of steganography and compare various information techniques.

Chapter2: This is the literature review which constitutes of various type of previous algorithm used for steganography.

Chapter 3: This chapter gives the description of the proposed work.

Chapter 4: This chapter gives the results and evaluations of the proposed schemes.

Chapter 5: This chapter concludes the work.

CHAPTER 2
PREVIOUS STEGANOGRAPHY TECHNIQUES FOR INFORMATION HIDING

An information hiding system has been developed for confidentiality. However, in this chapter, an image file as a carrier to hide data has been studied. Therefore, the carrier will be known as the cover-image, while result of steganography is known as the stego-image. The implementation of the system will only focus on Least Significant Bit (LSB) as one of the steganography techniques as mentioned in below [39]. There are two main approaches used in image steganography.

- Irreversible image steganography.
- Reversible image steganograhy.

2.1 IRREVERSIBLE IMAGE STEGANOGRAPHY

This type of image steganography deals with the secret data using LSB replacement method. This scheme has higher embedding capacity along with minimum computation time. The embedded information detection is easy in this type of scheme. This type of method embeds the secret message in least significant bit plane of the cover image. The detailed explanation of this LSB method is explained in this chapter. There are some existing steganalysis schemes which can be used to determine whether an image contains secret information, if the embedding process is as trivial as LSB. In Babu et al. [39], a steganographic scheme is proposed to authenticate the secret information from the stego image. In this paper, the secret data is transformed into frequency domain from the spatial domain using discrete wavelet transformation.

A fixed 4-bit LSB method to hide the secret data is proposed in Moon et al.[40]. Using this method the resulting image is not effected and can easily be implemented. Baekl et al.[36] proposed an image steganography code conversion to embed the data. In this paper, binary codes and gray codes are implemented using XOR operation to make meaningful patterns.

2.1.1 Least-Significant Bit (LSB) Technique

In LSB technique last bit of pixels of some or all pixels bytes are changed by the secret data. Basically digital images have two types, these are 24-bit images and 8-bit images. The 24-bit image is also known as a color image or a RGB image (8-bit for each plane) in which 3-bits of data information can be hidden in each pixel (1-bit in each plane). By changing the LSB, it does not affect the the image; so the stego image looks like the cover-image. In 8-bit images also known as a gray image, we can hide only 1-bit of information.

The cover-images are shown in figure 4.1 and the hidden data images are shown in figure 4.2. The stego-images are obtained by using the least significant bit algorithm (LSB algorithm). The secret data image can be generated by the stego image with the help of steganalysis process [33] [34] [35]. The LSB of pixel value of the cover image Co(l,w) is set by the data bit 'd' of the secret data image. The data embedding procedure is given below-

out(l,w) = Co(l,w) - 1, if LSB(Co(l, w)) = 1 and d = 0

out(l,w) = Co(l,w), if LSB(Co(l,w)) = d

out(l,w) = Co(l,w) + 1, if LSB(Co(l,w)) = 0 and d = 1

where LSB(Co(l,w)) stands for the LSB of the cover image Co(l,w) and d is the next data bit to be embedded, out(l,w) is the stego image. Three pixels of the RGB cover image are shown in table 2.1.

Table 2.1 Pixel value of the cover image

10101010	01010100	0001000
11110000	11001100	00110011
10001000	11100011	0001111

Let steganographic programmer wants to hide the letter “B”. The ASCII and the binary value of “B” is 66 and “01000010”. Then the result of LSB technique, the pixel value of stego image are shown in table 2.2.

Table 2.2 Pixel value of the stego image

1010101**0**	0101010**1**	0001000
1111000**0**	1100110**0**	0011001**0**
1000100**0**	1110001**1**	0001110

To insert a character, we have to change only three bits. In this case, the changes are too small to be recognized by the naked eyes, so data is effectively hidden. Simplicity is the main advantage of this method [30]. The following figure 2.1 and figure 2.2 shows the working of LSB method.

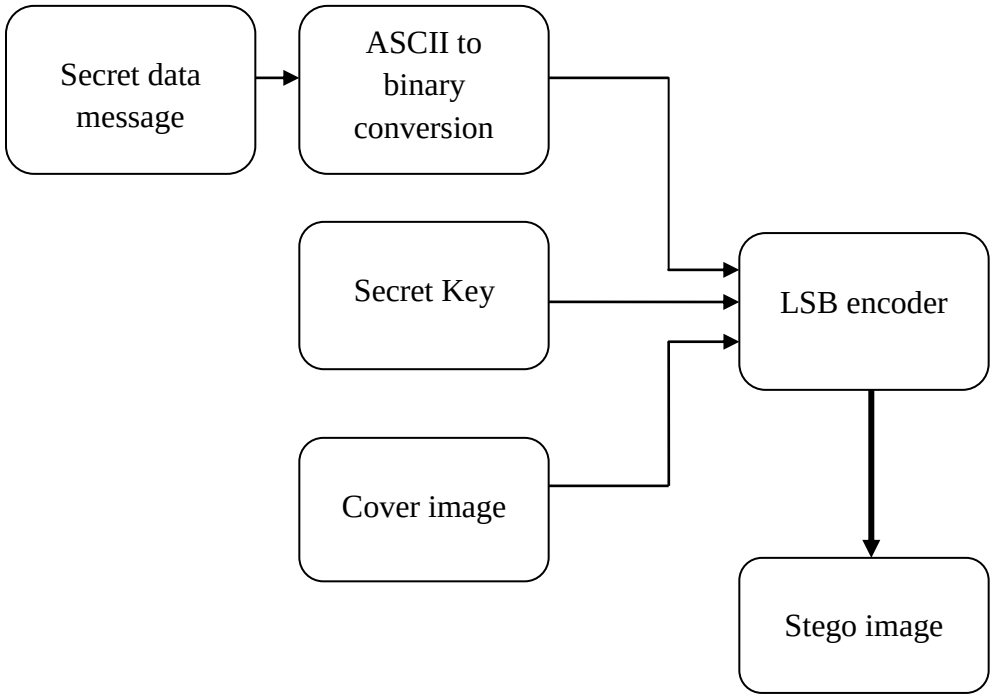


Figure 2.1: LSB insertion Mechanism

2.1.1.1 DATA EMBEDDING

The process of data embedding is as follows.

Inputs: Cover image, stego key and secret message text file.

Output: Stego image.

Procedure:

Step 1: Extract the pixels of the cover image.

Step 2: Extract the characters of txt file and convert it into 8-bit binary value.

Step 3: Extract the characters from the stego key.

Step 4: Choose first pixel of the cover image and pick characters of the stego key and place it in first component of pixel.

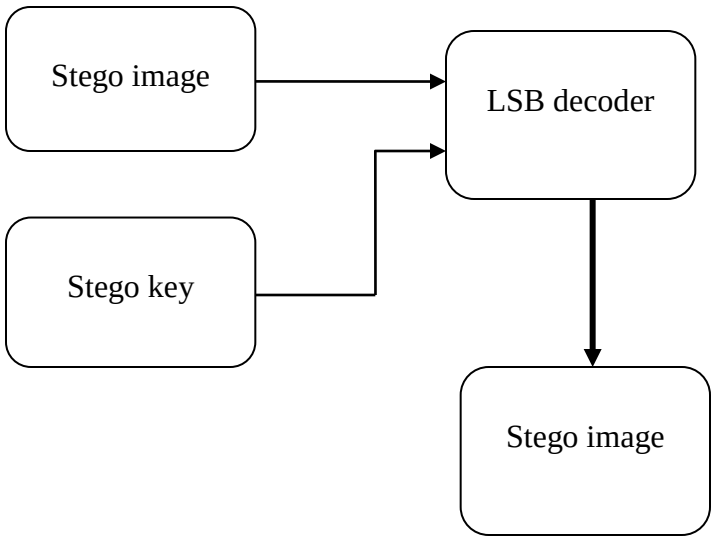


Figure 2.2: LSB extraction Mechanism

Step 5: Place some symbolic message, which indicate the starting of the data. Let 101 has been used as a symbolic data in this technique.

Step 6: Add characters of txt file in each beginning component of next pixels by using replacing.

Step 7: Repeat previous step till all the characters have been embedded.

Step 8: When the data is end place some terminating symbol again.

Step 9: Obtained the stego image [25].

2.1.1.2 DATA EXTRACTION

The data-extraction process is as follows.

Inputs: Stego image file, stego-key.

Output: Secret text data.

Procedure:

Step 1: Extract the pixels of the stego image.

Step 2: Now, start from first pixel and extract stego key characters from the first component of the pixels. Follow this step up to terminating symbol or starting symbol, otherwise follow the next step.

Step 3: If both the keys are matches (extracted key and the key entered by the receiver), then follow next step, otherwise exit the program.

Step 4: If the key is correct, then go to next pixel and extract the data characters from first component of next pixels. Follow this step till up to terminating symbol or ending symbol. After terminating symbol follow the next step.

Step 5: Extract the secret data [26][27].

2.1.1.3 IMAGE ENCODING ALGORITHM

Inputs: Image file, stego key and image file.

Output: Stego image.

Procedure:

Step 1: The cover image and the secret data image are read and converted into 8-bit binary value or into int8 type.

Step 2: The numbers in the secret data image matrix are converted into 8-bit binary number. Then the matrix is rearrange to a new matrix a.

Step 3: The matrix of the cover image is also reshaped to matrix b.

Step 4: Perform the LSB technique described above.

Step 5: The stego image, which is very similar to the cover image, is achieved by reshaping matrix b.

Step 6: For extracting the data, collect the LSB of stego image. The collected output is then converted into decimal values, which shows the pixel value of the data image [24].

2.1.2 PSEUDO-RANDOM ENCODING TECHNIQUE

In this technique, A random key is used to choose the pixels randomly and embed the data. This will make the data bits more difficult to find and hopefully reduce the realization of patterns in the image [6]. The data can be hidden in LSB of a particular color plane of randomly selected pixel in the RGB color space [28].

2.1.2.1 EMBEDDING ALGORITHM

In this process of encoding method, a random key is use to randomized the cover-image and then hide the bits of the secret data into LSB of the pixels within the cover image. The transmitter side and receiver side share the stego key and random key. The random-

key generate a random number, which is the location of pixel in the cover image for embedding the secret information [23].

Inputs: Cover image, stego-key and the secret data txt file.

Output: Stego image.

Procedure:

Step 1: Read character from txt file that is hidden and convert its American Standard Code for Information Interchange (ASCII) value into equivalent 8-bit binary value.

Step 2: Read the cover image in which the secret data is to be embedded.

Step 3: Read LSB of first plane pixel.

Step 4: Initialize the random key and randomly permute the pixels of the cover image and reshape into a matrix.

Step 5: Initialize the stego-key and XOR with the text file to be hidden and give the data.

Step 6: Insert the bits of the secret data to LSB of the first plane's pixels.

Step 7: Write the above pixel to stego image file [28].

2.1.2.2 EXTRACTION OF HIDDEN DATA

In this section, the process first takes the key and then the random-key. These keys show the least significant bit in which the secret data is randomly distributed [26]. The decoding process searches the hidden bits of the secret data into LSB of the pixels within the cover image by using the random key. In decoding method the random-key must match i.e. the random-key which was used in encoding should match because the random key sets the hidden points of the data in case of encoding. Then receiver can decode the embedded data exactly using only the stego-key. The receiver can't be decode the secret data, if he don't know about the random-key.

2.1.2.3 DATA EXTRACTION ALGORITHM

Inputs: Stego-image file, stego-key, random key.

Output: Secret data.

Procedure:

Step 1: Open the stego file read the RGB color plane of each pixel.

Step 2: Extract the first plane of the stego image.

Step 3: Read LSB of each pixel.

Step 4: Initialize the random-key that gives the position of the data bits in the pixel that are embedded randomly.

Step 5: For decoding, select the pixels and extract the LSB value of first plane pixels.

Step 6: Repeat this for each of pixels then arrange of the array converts into a decimal value that is actually ASCII value of the hidden character.

Step 7: The data file is generated by using XORing these ASCII values and the secret key, which are hide inside the cover image [28].

2.2 REVERSIBLE IMAGE STEGANOGRAPHY

In this image steganography technique, the cover image can be retrieved while extracting the data from the stego image. The secret image embedded inside the cover photo is called the stego image. This technique is very complex and has less embedding capacity. The embedding capacity can be increased using embedding the data near sharper edges. Various papers have been proposed for this technique. In [41] Wu H.C. et al. proposed an reversible image steganography technique in which the secret message is first encrypted using AES or DES and then embedded in a code tree computed using frequency of error values. These values are computed using Median Edge Detection (MED) predictor. Another paper [42] proposed a scheme in which intermediate image is generated in which

pixel values are converted into four hexadecimal values and then into three decimal values. This data is then distributed and embedded into the cover images. Hwang et al. [43] proposed a scheme of histogram shifting. In this paper, each zero or minimum frequency pixels are changed by one gray scale value and it increases the quality of stego image. Original cover image can be extracted from the stego image without any loss. The minimum PSNR value achived by this method is 48dB. This scheme is very effective and without any distortion the watermark can be removed from the watermarked image. Maximum frequency points are used in this to embed the secret data. The location of maximum frequency points of the pixels is stored in the histogram. This location map can be used to get the secret data.

Lin et al. [44] proposed a block based scheme in which image is subdivided into blocks. The difference in the pixel intensities is calculated and their difference is computed. The secret information is then embedded into these values. These methods do not embed the data to the peak points of the cover but embed the secret data to the peak points of the difference image generated from the cover. Using this scheme the hiding capacity can be increased depending upon the application. One more block based image steganography scheme has been proposed [45]. In this technique, reference pixel concept has been used. The reference pixel is the center pixel in each block. Reference pixel is used to differentiate the neighboring pixels value in a block. The secret data is then embedded into each block by modifying these differentiate values.

CHAPTER 3
PROPOSED METHOD

The higher embedding capacity or less mean square error (MSE) is the focal points of proposed method. This can be achieved by reducing the size of data or increasing the cover image size or it can be possible by taking the data in the different form so that maximum data can be hiding in cover image and there will be a less change in the cover image. The proposed algorithm converts the secret data image into a new format and embeds it into the RGB cover image. It achieves higher embedding as it exploits every part of available space in a cover. By using this new secret data the output of steganography (stego image) have very fewer changes compare to cover image. Due to this higher PSNR and lower MES compare to simple LSB method have been achieved.

The proposed algorithm has three phases. In the first phase, the secret message or data image are used. In this section, each pixel of the data image has been changed according to proposed method. After this phase, the resultant data image has less no. of bits so that it will increase the quality of the stego image. After the first phase, in second phase each pixel of the data image will break into 8 different sub pixels. In third phase firstly the cover image is broken into three planes RGB and then each pixel of these planes are XORing with each pixel of the data image of related planes (which is generated after second phase).

3.1 PHASE ONE

In this section, the secret data image are used. First of all the data image is break into 3 planes these are red plane (D_R), green plane (D_G), blue plane (D_B). After breaking the data image, the format of each plane of the data image has been changed according to proposed method. For hiding the data image XORing method has been used, and the behavior of XOR gate shown in table 3.1.

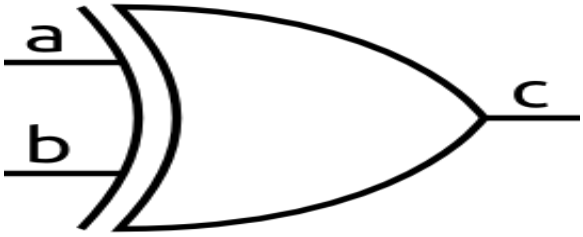


Figure 3.1 Symbol of XOR gate

Table 3.1: Truth Table of XOR gate

Input	Input	Output
A	B	C
0	0	0
0	1	1
1	0	1
1	1	0

According to truth table, if A= '0' then C= B and if A= '1' then C=inverse of B. Means in XOR gate if one input is '0' the output follows the other input, and if one input is '1' the output is inverse of other input. According to proposed method, the two inputs of XOR gate are the cover image pixels and the data image pixels. If the data image have been changed into a new format, so that output of XOR gate follows the cover image and the data image will also be hide in it. The proposed method is based on this phenomena, means if the data image has been changed into a new format, in which number of '1' is less compare to the original data image so that the output image or the stego image can follow the cover image. For converting the data image in a new format various steps are used. They are:

Step 1: Read first plane (red plane) of the data image and make a matrix with these pixels values.

Step 2: Take first element (A) of the matrix as the reference pixel.

Step 3: Take next element of the matrix (B).

Step 4: Compare the value of A and B and store the output in a new matrix called C.

- If B > A then C= 192 + (B – A) and
- If A > B then C= (A – B) and
- If A = B then C=0

Step 5: Repeat from step 3 until the whole element of the matrix does not change.

The flow chart for converting the data image in new form is:

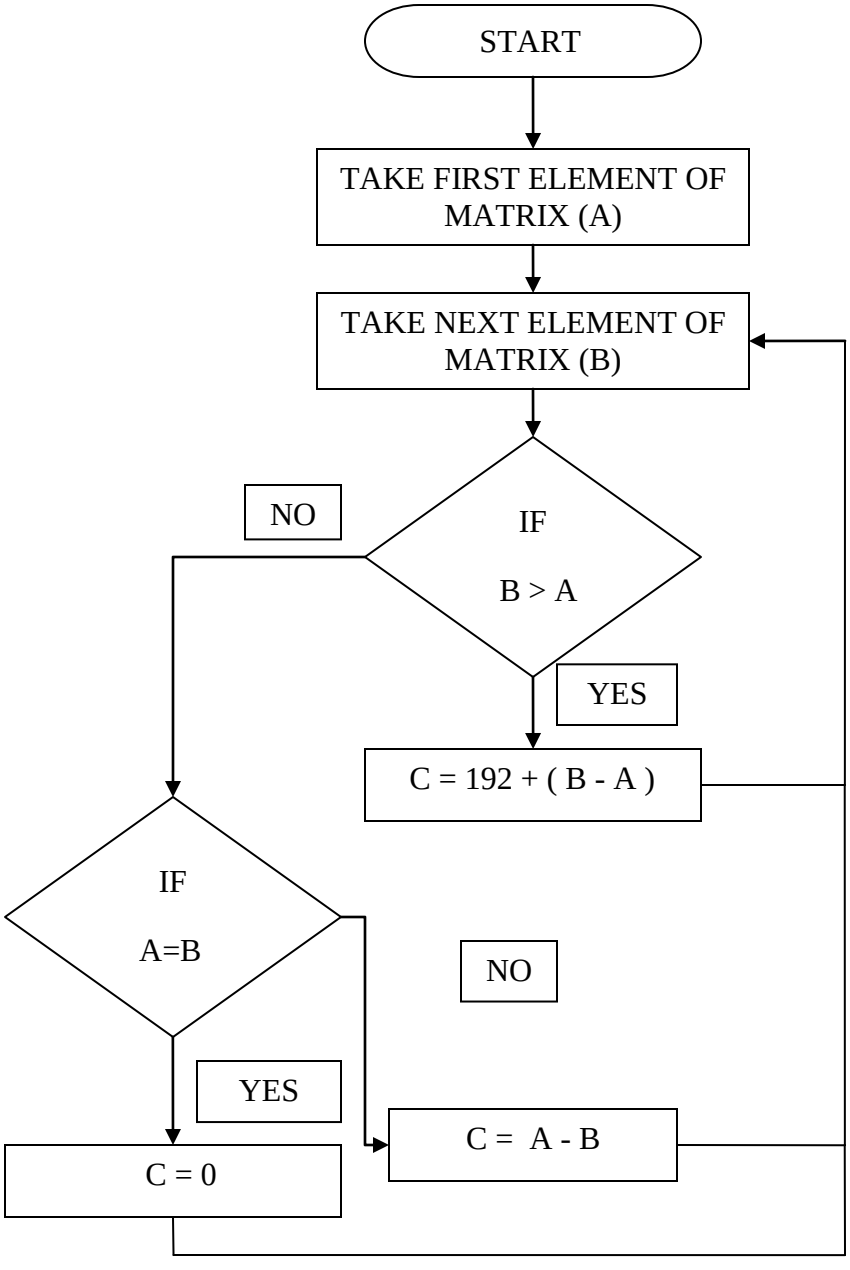


Figure 3.2: Data changing method

The first phase will be completed with the output of the new matrix. This method will be applied on all three planes of the data image. After applying this new data image has been generated with the help of new matrix of each plane, in which the number of '1' is less compare to the original data image. In this method, a case has been arrived in which the output is generated by the summation of 192 and difference of A and B. The reason behind adding 192 is that after adding this special number the upper 2 bits of the pixel are '1'. The region behind this is that after converting the data image matrix into a new format it can be easily determine that which pixel value is greater and which pixel is less compared to reference pixel. Let us take an example: The red plane of original data image having pixels values are shown in table 3.2, and there binary representation shown in table 3.3.

Table 3.2 Pixel value of the original data image

226	226	222	222	224
232	236	217	167	167

Table 3.3 Binary representation of the original data image pixel

11100010	11100010	11011110	11011110	11100000
11101000	11101100	11011001	10100111	10100111

Number of '1' in table 3.3 is 83. Here reference pixel A= 226, then the new pixels values according to proposed method are shown in table 3.4 and there binary representation is shown in table 3.5.

Table 3.4 Pixel value of the modified data image

226	**226**-226=0	**226**-222=4	**226**-222=4	**226**-224=2
192+(232-**226**) =198	192+(236-**226**) =202	**226**-217=9	**226**-167=59	**226**-167=59

Table 3.5 Binary representation of the modified data image pixel

11100010	00000000	00000100	00000100	00000010
11000110	11001010	00001001	00111011	00111011

In table 3.5 number of '1' is 27, which is very less compare to table 3.3.

3.2 PHASE TWO

In this section, new matrix which is the output of phase one has been used. In this phase, each pixel of the data image has been breaking into 8 sub pixels so that each part can easily XOR with the cover image pixel. This process will be done in some steps.

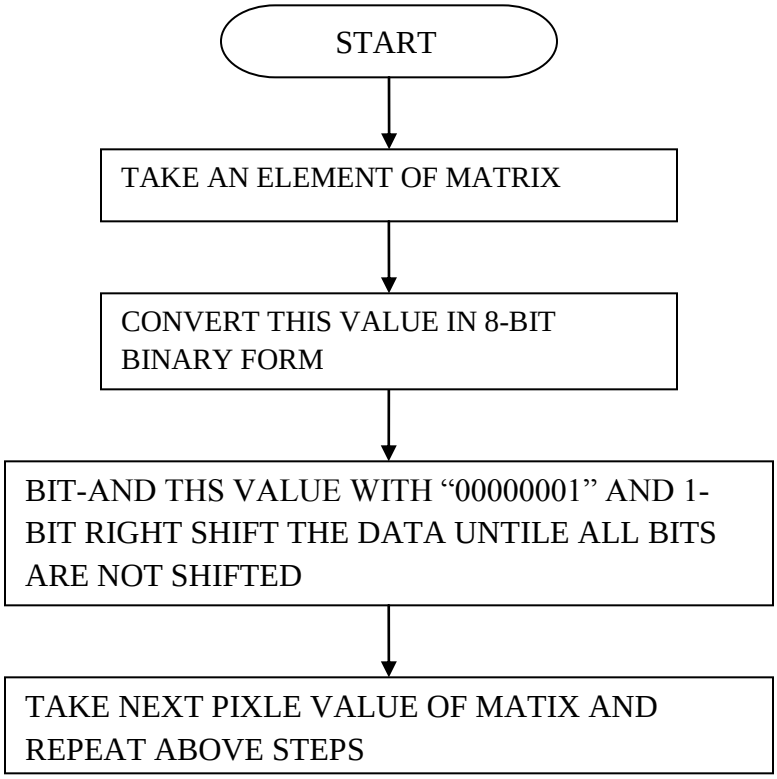


Figure 3.3: Data pixels extraction method

Step 1: Take a pixel value from the new data image.

Step 2: Convert this pixel value in an 8-bit binary format.

Step 3: Bit-And the pixel value with “00000001” and store the output in a new matrix.

Step 4: 1-bit right shift the binary pixel value and repeat from step 3 until all bits are not shifted.

Step 5: repeat step 2, 3, 4 for each pixel of the data image.

Flow chart for this method is shown in figure 3.3.

According to this phase, each pixel is expanded into 8 different sub pixels. The LSB of these 8 different pixels shows the value of the original pixel.

Let a pixel A=226

Binary representation of this pixel is A=11100010

Now Bit-And the value of A with ‘00000001” then

C_1= “11100010” AND “00000001”

C_1= “00000000”

The LSB of A is stored in LSB of C. now 1-bit right shift the value of A then

A= “01110001”

Now again Bit-And the value of A with ‘00000001” then

C_2= “01110001” AND “00000001”

C_3= “00000001”

This process is repeated until all bits of A are not stored in LSB of matrix C’s element. All these process are repeated with all pixel of the data image. In this method if the input has N element then the output of this section have an 8xN element. The output of this section is shown in table 3.6. Let the output of phase one is

226	0	4	4	2

Binary representation of new matrix

11100010	00000000	00000100	00000100	00000010

Table 3.6 Sub pixels of the modified data image

00000000	00000000	00000000	00000000	00000000
00000001	00000000	00000000	00000000	00000001
00000000	00000000	00000001	00000001	00000000
00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000
00000001	00000000	00000000	00000000	00000000
00000001	00000000	00000000	00000000	00000000
00000001	00000000	00000000	00000000	00000000

3.3 PHASE THREE

This is the last and most important section of proposed method. In this section, the data image is completely store or hides into the cover image and generate the stego image. This section is done in various steps.

Step 1: Read the cover image and divide it into three planes: red plane, green plane, blue plane.

Step 2: Convert the pixels values of each plane of data image into 8-bit binary form. With the help of dec2bin command.

Step 3: Take the pixels from the output of phase two & cover image and apply XORing between these two binary values.

Step 4: Repeat step 2 and step 3 for all pixels of the cover image and the data image.

Let the output of phase two is:

0000000**0**	0000000**1**	0000000**0**	0000000**0**
0000000**0**	0000000**1**	0000000**1**	0000000**1**

Table 3.7 Pixel value of the cover image

10100100	00111111	01001011	01011111
10011101	01100011	01011011	00110011

Output of XORing of above two matrices or stego image matrix is shown in table 3.8.

Table 3.8 Pixel value of the stego image

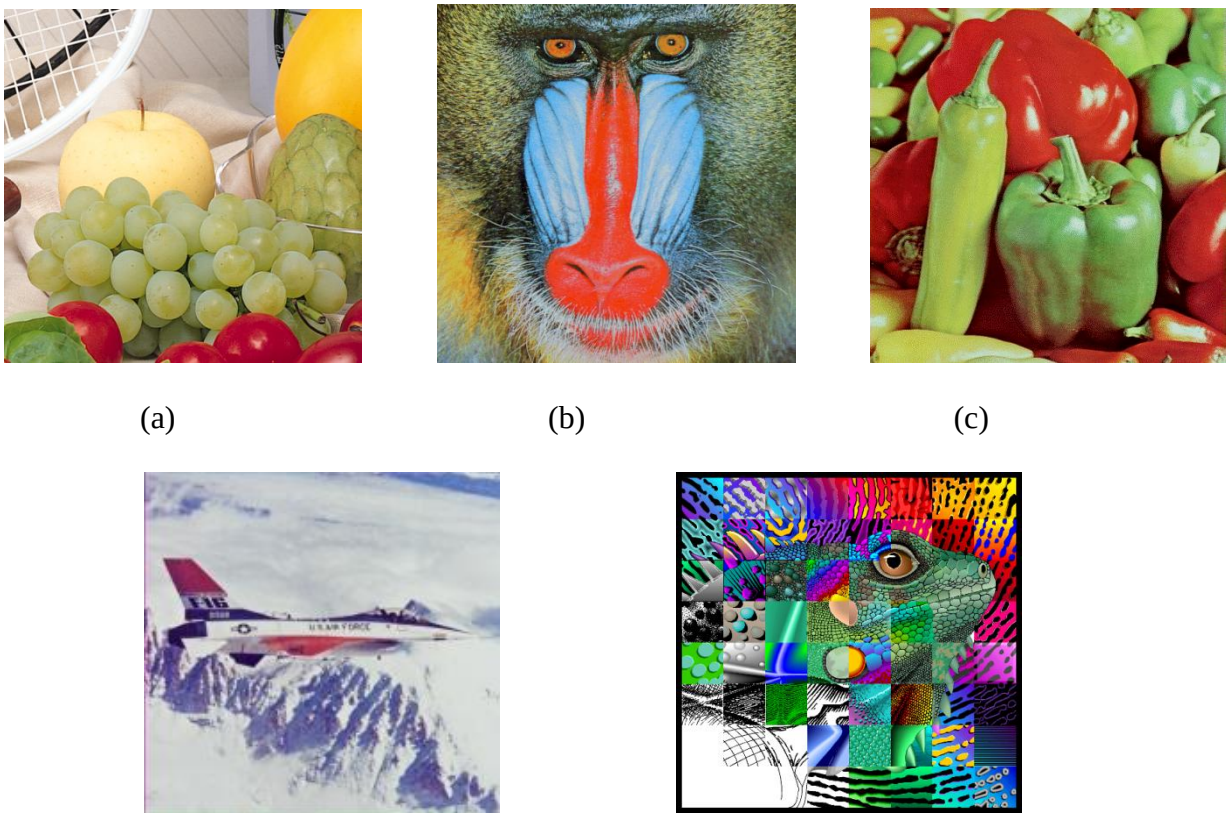
1010010**0**	0011111**0**	0100101**1**	0101111**1**
1001110**1**	0110001**0**	0101101**0**	0011001**0**

CHAPTER 4

RESULTS AND DISCUSSIONS

4.1 DATA SET

In proposed method, different data images are embedded in the different cover images. Fruits, Baboon, Pepper, Jet plane and Fry mire of different complex properties. All these images which are use for the cover image were selected from standard image set. The various cover images are shown in figure 4.1(a) - (e) and the various data images are shown in figure 4.2 (a) - (b). In the proposed method the size of the cover image (I, J) remains same but the size of the data image (i, j) should change according to method required, but in all cases the cover image and the data image satisfied the following relationship I >> i & J >> j.



(a) (b) (c)

(d) (e)

Figure 4.1 Cover images (a)Fruits; (b)Baboon; (c)Pepper; (d)Jet plane; (e)Fry mire.

(a)

(b)

(c)

(d)

Figure 4.2 Data images (a)Arctic; (b)Lenna; (c)Fouviere; (d)Pills.

In steganography the size of the cover image is greater than the size of the data image so that the data image can easily hide into the cover image. The proposed method is based on LSB method. There is a minor difference between the LSB method and the proposed method that is in LSB method the least significant bit of some or all cover image pixels are replaced by the secret data but in proposed method on the place of replacing XORing of the secret data and LSB of the cover image pixels has been used. In 1-bit LSB method, the minimum size of the cover image should be eight time the data image.

$$\text{Size (cover image)} \geq 8 \text{ x Size (data image)} \qquad (4.1)$$

In 2-bit LSB method the size of the cover image is four times of the data image, because in 2-bit LSB method the secret data is store in the last 2 bits of each pixel of the cover image. Similarly in 4-bit LSB method the size of the cover image is twice of the data image.

The major problem in increasing the embedding capacity is the rise in visual distortion in the stego image. It is generally known that the distortion of the stego image is hard to detect by the human eyes as long as the PSNR value is greater than or equal to 30 dB [23].

4.2 EXPERIMENT AND RESULTS

The fundamental method used to determine the noise in the stego image is peak signal to noise ratio (PSNR). Efficiency of any image steganography algorithm depends on hiding capacity and embedding efficiency. So, both aspects have been considered to analyze the results. PSNR is an objective measure for subjective evaluation of degree of similarity between the original image and the stego image. PSNR is defined as;

$$\mathrm{PSNR} = 10\log_{10}\frac{C_{max}^2}{\mathrm{MSE}} \tag{4.2}$$

where C_{max}= 255, maximum gray level for any grayscale image, and the mean squared error MSE (Moon et al., 2007) is defined to be

$$\mathrm{MSE} = \frac{1}{m*n}\sum_1^m\sum_1^n(Cij - Sij)^2 \tag{4.3}$$

Where M and N represent the number of horizontal and vertical pixels of the images respectively. A RGB image have been used as the cover image and the noise introduced in each component of the stego image has to be evaluated. The PSNR of the stego image is defined as the average of the PSNR calculated for different components of the stego image.

Let $C_R(i, j)$ be the pixel intensity of a component of the cover image and $S_R(i, j)$ be the pixel intensity of a component of the stego image. Similarly for green and blue components these values are $C_G(i, j)$, $C_B(i, j)$ and $S_G(i, j)$, $S_B(i, j)$.

MSE for R, G, and B components are calculated using following equations:

$$\mathrm{MSE_R} = \frac{1}{m*n}\sum_1^m\sum_1^n(C_Rij - S_Rij)^2 \tag{4.4}$$

$$\mathrm{MSE_G} = \frac{1}{m*n}\sum_1^m\sum_1^n(C_Gij - S_Gij)^2 \tag{4.5}$$

$$\mathrm{MSE_B} = \frac{1}{m*n}\sum_1^m\sum_1^n(C_Bij - S_Bij)^2 \tag{4.6}$$

PSNR for R, G, and B components are calculated using following equations:

$$\mathrm{PSNR_R} = 10\log_{10}\frac{255^2}{\mathrm{MSE_R}} \quad (4.7)$$

$$\mathrm{PSNR_G} = 10\log_{10}\frac{255^2}{\mathrm{MSE_G}} \quad (4.8)$$

$$\mathrm{PSNR_B} = 10\log_{10}\frac{255^2}{\mathrm{MSE_B}} \quad (4.9)$$

The PSNR is the average of PSNR

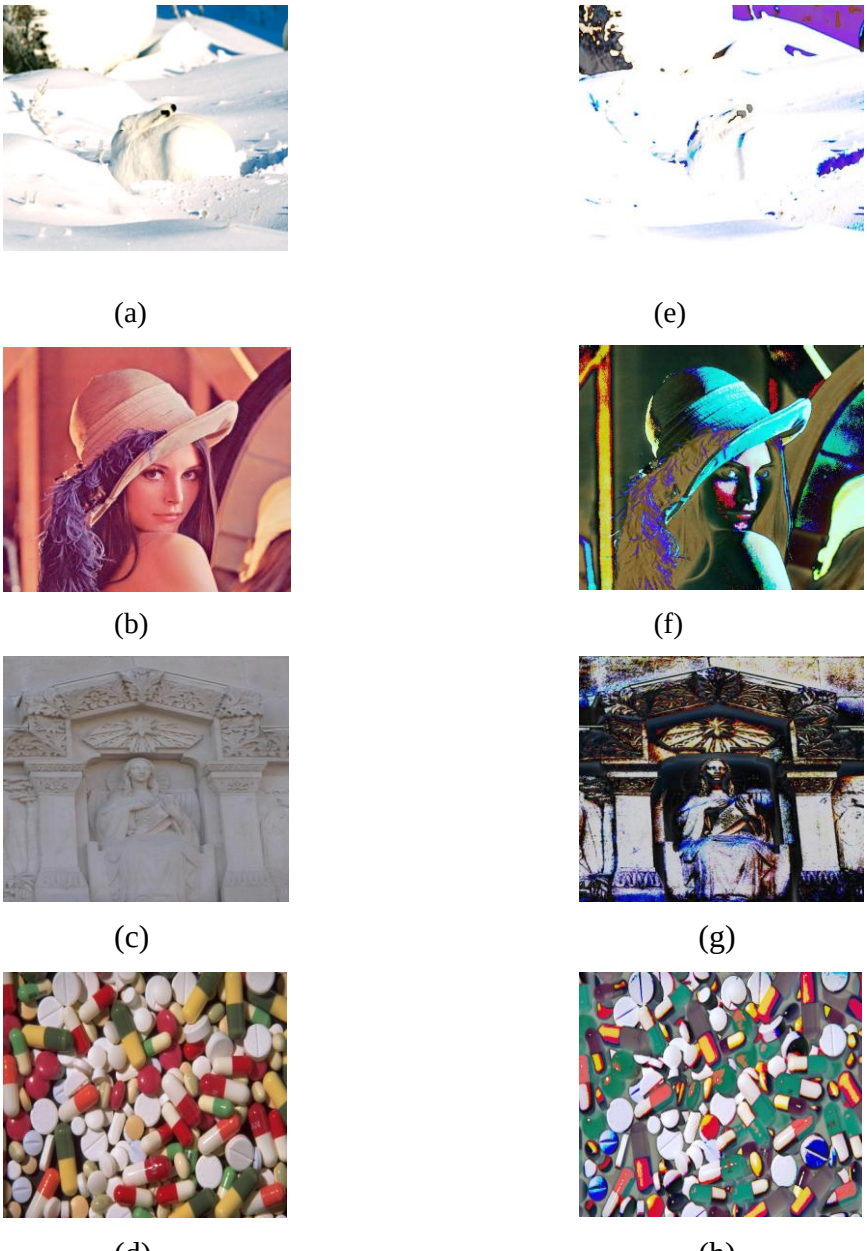
$$\mathrm{PSNR} = \frac{\mathrm{PSNR_R}+\mathrm{PSNR_G}+\mathrm{PSNR_B}}{3} \quad (4.10)$$

4.3 IMPLEMENTATION AND RESULT OF PROPOSED METHOD

The proposed method has three phases, in phase I, the data image has been changed into a new format to decrease the numbers of '1'. In proposed method, various data images have been worked on and some of these original data images and modified data images are analyzed here.

Table 4.1 Comparison between original data image and modified data image

	Data image	Arctic	Lenna	Founviere	Pills
Red plane	Original O_R^1	26502	18563	15074	17269
	Modified M_R^1	30688	13127	11332	15431
Green plane	Original O_G^1	25242	15125	15598	15987
	Modified M_G^1	14332	14353	11470	15142
Blue plane	Original O_B^1	24385	16344	15847	15918
	Modified M_B^1	14659	13385	11791	15332
Total change in count of "1" $O_R^1 + O_G^1 + O_B^1 - (M_R^1 + M_G^1 + M_B^1)$		16450	9167	11926	3269
% Change		21.6081	18.3223	25.6368	6.6478



(a) (e)

(b) (f)

(c) (g)

(d) (h)

Figure 4.3 Original data image (a) – (d); Modified data image (e) – (h)

After modifying the data image, apply the next phase of proposed method.

1. Break the data image and the cover image into three planes red, green, blue.
2. Each pixel of the modified data image is then divided into ‘N’ sub pixels.
3. After all these process applying the M-bit XORing method between the cover image pixels and the modified data image sub pixels.
4. After hiding data stego image is generated, which is use for transmission.

NOTE :- size of the data image and value of "N" depends on XORing method. For 1-bit XORing method N = 8, for 2-bit XORing method N = 4.

4.3.1 QUALITATIVE ANALYSIS OF COVER IMAGE

Figure 4.4 (a) – (j) shows the cover image and the generated stego image. Here the Lenna image has been used as the data image and the modified Lenna image is hiding with the help of 1-bit XORing method. For 1-bit XORing method, 512x512 sized cover image and 64x64 sized data image have been used. Change in the cover image does not affect the features of the data image. Visual distortion in the stego image is minimal, if the cover image has been changed for the same data image. The fundamental requirement of any image steganography algorithm is minimum visual distortion in the resulting stego image and it should be same for the different cover images. The results illustrate that the proposed algorithm conforms to these requirements.

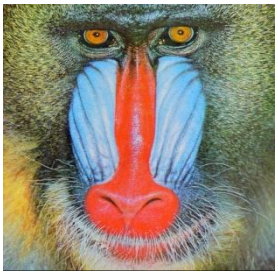
(a1)

(b)

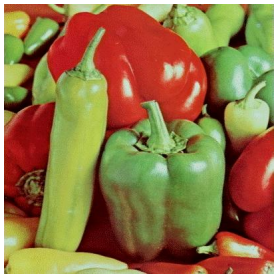
(c1)

(a2)

(b)



(c2)



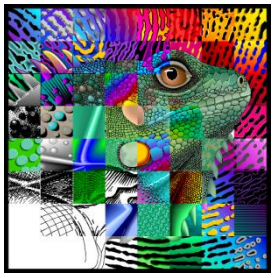
(a3)

(b)

(c3)



(a4) (b) (c4)



(a5) (b) (c5)

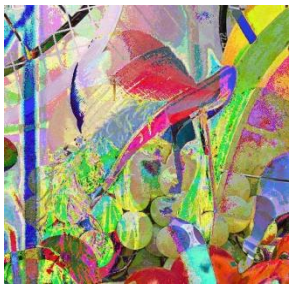
Figure 4.4 1-bit XORing method with cover image(a1)-(a5), data image(b), stego image(c1)-(c5)

Now Consider the same cover image (Fruits) and same the data image (Lenna) with different N-bit XORing method.



Cover image (512x512) Data image(256x256) Stego-image(512x512)





Cover image (512x512) Data image(512x512) Stego-image(512x512)

Figure 4.5 4-bit & 8-bit XORing method with same cover image and different size of data image.

4.3.2 QUANTITATIVE ANALYSIS OF THE COVER IMAGE AND THE STEGO IMAGE

Table 4.2 Different values of MSE with different cover image and different data image by using 1-bit xoring

Data image ⇨ / Cover image ⇩	Lenna	Arctic	Fouviere	Pills
Fruits	0.0273	0.0600	0.0226	0.0299
Baboon	0.0266	0.0587	0.0221	0.0295
Papper	0.0265	0.0585	0.0220	0.0294
Jet-plane	0.0263	0.0582	0.0218	0.0292
Frymire	0.0189	0.0421	0.0154	0.0210

Table 4.3 Different values of PSNR with different cover image and different data image

Data image ⇨ / Cover image ⇩	Lenna	Arctic	Fouviere	Pills
Fruits	63.7717	60.3459	64.5852	63.3754
Baboon	63.8810	60.4411	64.6824	63.4387
Papper	63.8949	60.4586	64.7110	63.4532
Jet-plane	63.9328	60.4839	64.7481	63.4783
Frymire	65.3556	61.8901	66.2434	64.9134

Table 4.4 Comparison table of MSE and PSNR for existing method and proposed method

n-bit LSB	MSE		PSNR	
	Existing method[2]	Proposed method	Existing method[2]	Proposed method
1-bit	0.5	0.0273	51.1	63.7717
2-bit	2.5	0.02753	44.1	53.7323
4-bit	42.7	13.1624	31.8	36.9375
8-bit	8640	125.8114	8.6	27.1336

In this table, the value for MSE and PSNR have been compared for existing method [2] and proposed method. In this comparison, the image of Fruits is used as the cover image and the image of Lenna is used as the data image.

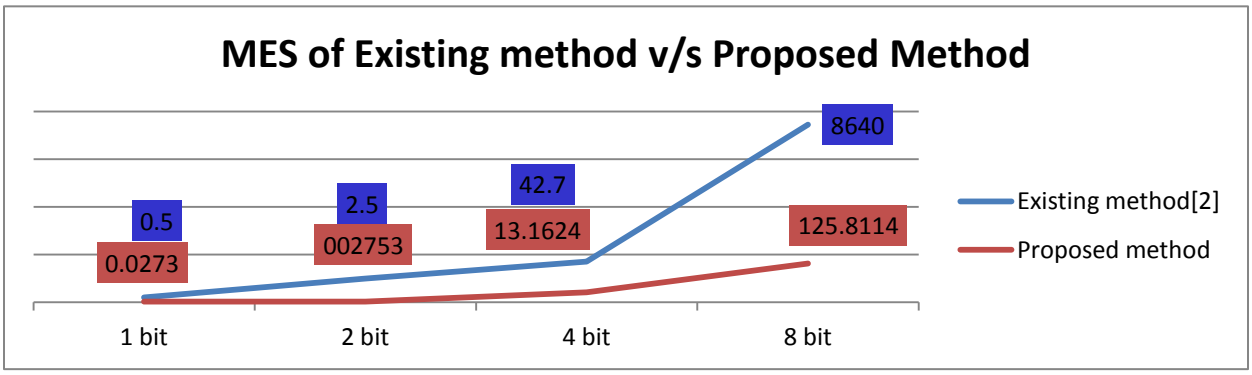


Figure 4.6 MSE comparison between existing method and proposed method

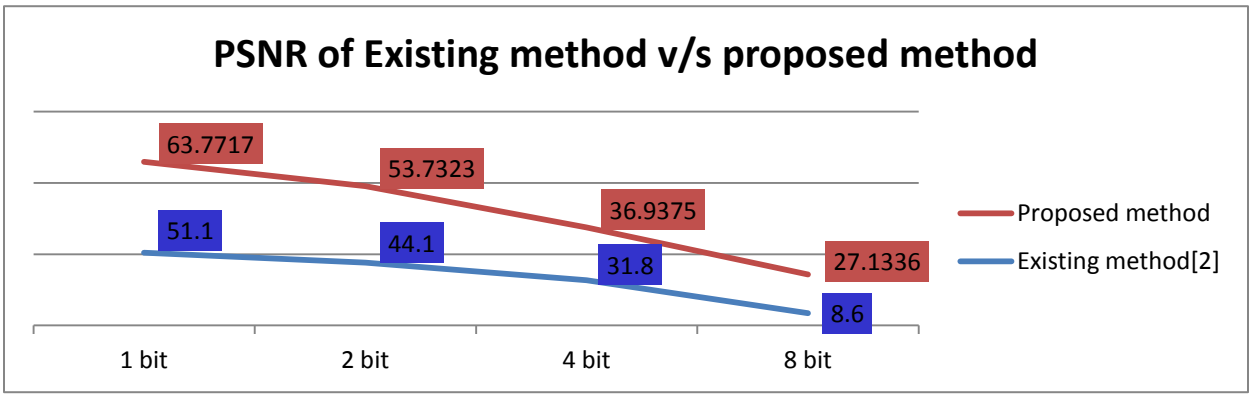


Figure 4.7 PSNR comparison between existing method and proposed method

4.3.3 SIMULATION AND SYNTHESIZABLE RESULT

Simulation Results for proposed algorithm in Xilinx ISE Design Suite is shown in figure 4.8. The simulation result is based on 4x4 cover image and 1x2 data image.

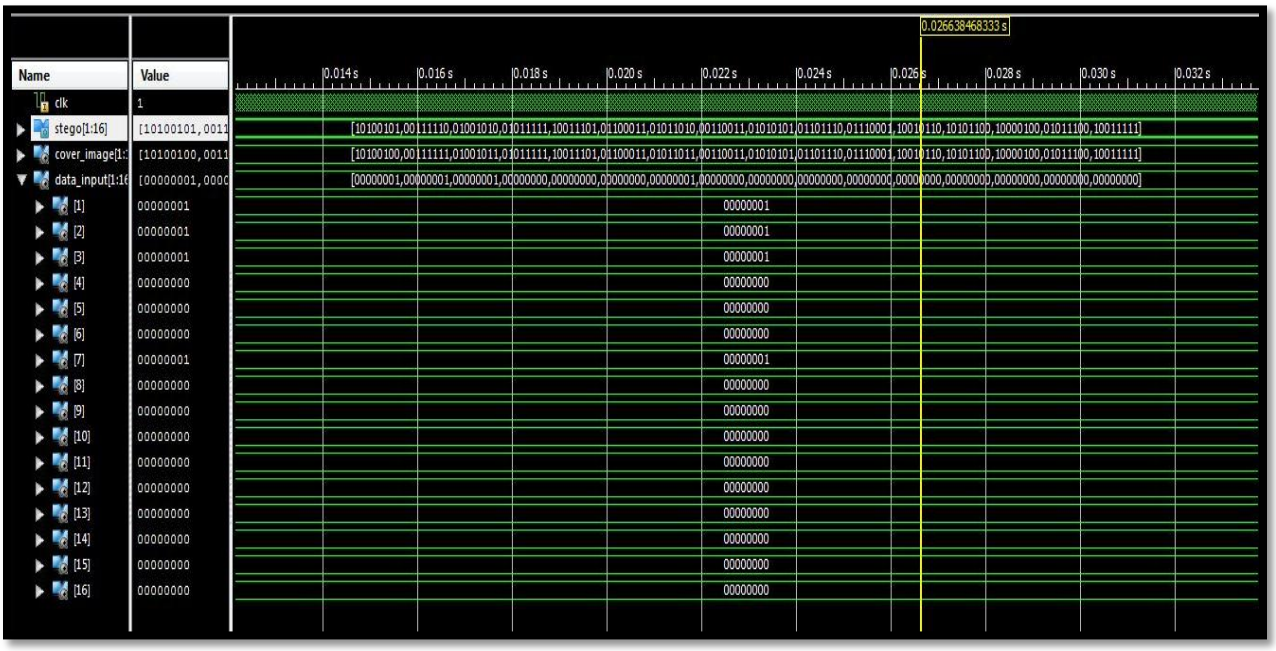


Figure 4.8 Simulation result for 4x4 cover image and 1x2 data image

Power Analysis for 4x4 cover image for 1x2 data image is shown in figure 4.9. It shows the complete information about power analysis of the proposed method.

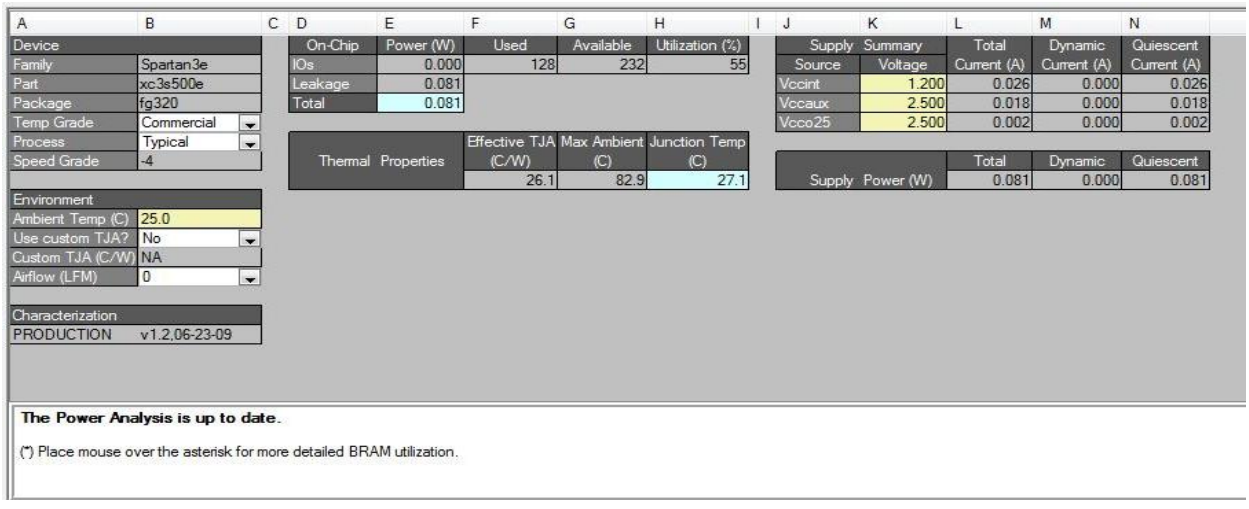


Figure 4.9 Power analysis of proposed method

Table 4.5 Synthesizable summary of proposed method

Parameters	Value
Total REAL time to xst completion	9.00 sec
Total CPU time to Xst completion	8.66 sec
Number of bonded IOBs	128 out of 232(55%)
Registers	116
Flip-Flops	116

CHAPTER 5

CONCLUSION AND FUTURE DIRECTION

5.1 SUMMARY AND CONTRIBUTION

In this thesis, an efficient image steganography scheme has been proposed. This scheme is efficient in terms of quality of image and PSNR. This thesis presents a brief overview of image steganography.

Chapter 1 provides an introduction to general image steganography process. General terms such as cover or carrier image, stego image and steganalysis are defined. Type of steganography and difference between information hidings techniques have been described in this chapter. The motivation to work on the image steganography follows from the challenges that exist in this area.

Chapter 2 categorizes the existing image steganography schemes. Broadly categorize the image steganography as reversible and irreversible image steganography. A detailed account of each of the state of art reversible as well as irreversible image steganography schemes has been presented in this chapter.

Chapter 3 identifies the possibilities to improve upon the existing schemes and proposes an efficient image steganography scheme which achieves higher PSNR, higher stego image quality, and lesser MSE. The detailed clarification as to how the proposed scheme should work has been presented in this chapter.

Chapter 4 presents detailed evaluation parameters and analysis of the proposed scheme. The proposed scheme is evaluated using qualitative analysis where the quality of the stego image is shown and compared with the quality of the original cover. The proposed method is compared with LSB image steganography schemes presented in chapter 2.
The proposed method has the following advantages.

1. The PSNR value of stego image is higher compare to other steganography method; due to this a high-quality stego image has been achived.
2. In proposed method, the format of the data image has been changed. New data image have less number of ‘1’ compare to the original data image. With the help of proposed method, the quality of the stego image is increase by 20% (nearly).
3. Security of the data image is also increased by using proposed method.

Chapter 5 summarizes the thesis. The brief summary of all the chapters is given. The proposed methodology is summarized. A brief overview of the future possibility is also provided in this chapter.

5.2 FUTURE WORK

As steganography continues on its evolutionary path researchers have discover the new platforms where steganographic techniques could be used to hide information absolutely. Most of the research is going on this field.

1. The proposed steganography algorithms can be improved by floating point binary representation. Using floating point mechanism, it may be possible to reduce more numbers of ‘1’ in the data image which improve the quality of the stego image.

2. In place of images as cover media, other medias like video, text, and audio can be used. By using these medias higher embedding capacity cab be achieved.

3. Other operations can be applied to the data image for reducing the data image pixels values, the number of pixels of the data image and increasing the quality of the stego image.

4. In the place of the cover media the secret data can be hide in the noise signal or distorted signal to achieve the higher security.

5. In steganography, the security of the data can be increased if the concept of security key and timer are added.

Reference

[1] Mr. Vikas Tyagi, Mr. Atul kumar, Roshan Patel, Sachin Tyagi,"Image Steganography Using Least Significant Bit with Cryptography", *Journal of Global Research in Computer Science*, vol.3, no.3, 2012.

[2] Bassam Jamil Mohd, Saed Abed and Thaier Al-Hayajneh,"FPGA Hardware of the LSB Steganography Method", *IEEE potentials*, 978-1-4673-1550-0, 2012.

[3] R.Anderson and F. Petitcolas,"On the limits of steganography", *IEEE Journal of Selected Areas in Communications*, Vol. 16, No. 4, May 1998.

[4] Atallah M. Al-Shatnawi,"A New Method in Image Steganography with Improved Image Quality", *Applied Mathematical Sciences*, vol.6, no.79, 3907–3915, 2012.

[5] Himanshu Gupta, Prof Ritesh Kumar and Dr. Soni Changlani,"Enhanced Data Hiding Capacity using LSB-Image Steganography Method", *International Journal of Emerging* Technology *and Advanced Engineering*, vol.3, June 2013.

[6] Samir K Bandyopadhyay, Debnath Bhattacharyya1, Debashis Ganguly1, Swarnendu Mukherjee1 and Poulami Das,"A Tutorial Review on Steganography", Heritage Institute of Technology.

[7] Youssef Bassil,"Image Steganography method based on brightness adjustment", *Advances in computer Science and its application*, vol.2, no.2, 2012.

[8] Fangjun Huang,"New Channel Selection Rule for JPEG Steganography", *IEEE Transactions on Information Forensics and Security*, vol.7, no.4, 2012.

[9] Bassam Jamil Mohd, Saed Abed and Thaier Al-Hayajneh,"FPGA Hardware of the LSB Steganography Method", *IEEE potentials*, 978-1-4673-1550-0, 2012.

[10] Souvik Bhattacharyya, Indradip Banerjee, Gautam Sanyal,"A survey of steganography and steganalysis technique in image, text, audio, and video as cover carrier", *Journal of global research in computer science*, vol. 2, no.4, 2011.

[11] Mohammed Salem Atoum,"A Steganography Method Based on Hiding secrete data in MPEG/Audio Layer III", *IJCSNS International Journal of Computer Science and Network Security*, vol.11, no.5, 2011.

[12] Weiqi Luo, Fangjun Huang, Jiwu Huang,"Edge Adaptive Image Steganography Based on LSB Matching Revisited", *IEEE Transactions on Information Forensics and Security,* vol.5, no.2, pp. 201-214.M., 2010.

[13] Arvind Kumar and Km Pooja,"Steganography-A hiding Technique", *International journal of Computer Application,* vol. 9, no. 7, November 2010.

[14] J.R.Krenn,"Steganography & Steganalysis", accessed 21/03/2015. http://www.krenn.nl/univ/cry/steg/article.pdf

[15] G. Kessler, Steganography,"Hiding Data within Data", accessed 21/03/2015. http://www.garykessler.net/library/steganography.html

[16] Abbas Cheddad, Joan Condell, Kevin Curran, Paul McKevitt,"Digital image steganography: Survey and analysis of current methods", *Elsevier journal of Signal Processing 90,* 727–752, 2010.

[17] Ozdemir Cetin, A. Turan Ozcerit,"A new steganography algorithm based on color histograms for data embedding into raw video streams", *Computers & Security,* vol. 28, no. 7, pp. 670-682, October 2009.

[18] Leung, H.Y., Cheng, L.M., Cheng, L.L., Chi-Kwong Chan,"Hardware Realization of Steganographic Techniques", *Intelligent Information Hiding and Multimedia Signal Processing,* Third International Conference on IIHMSP 2007, vol.1, pp.279,282, 26-28, November 2007.

[19] Ran-Zan Wang, Chi-Fang Lin, Ja-Chen Lin,"Hiding data in images by optimal moderately significant-bit replacement" *IEE Electron. Lett.,* vol. 36, no. 25, 2000.

[20] Chi-Kwong Chan, L.M. Cheng ,"Hiding data in images by simple LSB substitution", Department of Computer Engineering and Information Technology, City University of Hong Kong, Hong Kong, May 2002.

[21] Johnson, N.F. Jajodia, S.,"Exploring Steganography: Seeing the Unseen", *Computer Journal*, February 1998.

[22] K B Raja, Venugopal K R and L M Patnaik,"A Secure Stegonographic Algorithm using LSB, DCT and Image Compression on Raw Images", Department of Computer Science and Engineering, University Visvesvaraya College of Engineering,Bangalore University, December 2004.

[23] A. Cheddad, J. Condell, K. Curran and P.M. Kevitt.,"Digital image steganography: survey and analysis of current methods", *Signal Processing Journal*,2010.

[24] Pratap Chandra Mandal,"Modern Steganographic technique: A Survey", *International Journal of Computer Science Engineering Technology*.

[25] Mamta Juneja,"Data hiding Algorithm for Bitmap Images using Steganography", Department of computer science and Engineering, RBIEBT, Sahuran.

[26] Vijay kumar sharma, Vishal shrivastava,"A steganography algorithm for hiding image in Image by improved lsb substitution by minimize Detection", *Journal of Theoretical and Applied Information Technology*, vol. 36, no. 1, February 2012.

[27] Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav,"Steganography Using Least Signicant Bit Algorithm", *International Journal of Engineering Research and Applications*, vol. 2, no. 3, May2012.

[28] Shamim Ahmed Laskar and Kattamanchi Hemachandran,"steganography based on random pixel selection for efficient data hiding", *International journal of computer engineering technology*.

[29] Jessica Fridrich, Miroslav Goljan, and Rui Du,"Detecting LSB Steganography in Color and Gray-Scale Images", State University of New York, Binghamton.

[30] Clair and Bryan,"Steganography: How to Send a Secret Message", www.strangehorizons.com/2001/20011008/steganography.shtml, 2001.

[31] A. Westfeld, and G. Wolf, "Steganography in a Video conferencing system", *in proceedings of the second international workshop on information hiding*, vol. 1525, springer, pp. 32-47, 1998.

[32] C. C. Lin, and W. H. Tsai,"Secret Image Sharing with Steganography and Authentication", *Journal of Systems and Software*, vol. 73, no. 3. pp. 405-414, 2004.

[33] K. Rabah,"Steganography - The Art of Hiding Data", *Information technology Journal*, vol. 3, no. 3, 2004.

[34] T. Morkel, J. H. P. Eloff and M. S. Olivier, "An Overview of Image Steganography", *in Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005)*, Department of Computer Science, University of Pretoria, SA, 2005.

[35] J. Baekl, C. Kim, P. S. Fisherl and H. Cha, "(N, 1) Secret Sharing Approach Based on Steganography with Gray Digital Images", *In proceedings of IEEE International*

Conference on Wireless Communications, Networking and Information Security (WCNIS), pp. 325 – 329, 2010.

[36] B. Li, J. He, J. Huang and Y. Q. Shi "A Survey on Image Steganography and Steganalysis", *Journal of Information Hiding and Multimedia Signal Processing*, vol. 2, no. 2, pp. 142–171, 2011.

[37] C.Y. Yang, C.H. Lin and W.C. Hu "Reversible Data Hiding for HighQuality Images Based on Integer Wavelet Transform", *Journal of Information Hiding and Multimedia Signal Processing*, vol. 3, no. 2, pp. 142–150, 2012.

[38] S. Dumitrescu, W.X. Wu and N. Memon,"On steganalysis of random LSB embedding in continuous-tone images", *in Proceedings of International Conference on Image Processing*, Rochester, NY, pp.641-644, 2002.

[39] K. S. Babu, K. B. Raja, K. K. Kumar, T. H. Manjula Devi, K. R. Venugopal, and L. M. Pataki,"Authentication of secret information in image steganography", *IEEE Region 10 Conference TENCON*, pp.1-6, 2008.

[40] S. K. Moon and R.S. Kawitkar,"Data Security using Data Hiding", *IEEE International conference on computational intelligence and multimedia applications*, vol. 4, pp. 247- 251, 2007.

[41] H. C. Wu, H. C. Wang, C. S. Tsai and C. M. Wang,"Reversible image steganographic scheme via predictive coding", *Displays*, Elsevier, vol. 31, pp. 35–43, 2010.

[42] G. Ulutas, M. Ulutas and V.V. Nabiyev,"Secret image sharing with reversible capabilities", *International Journal Internet Technology and Secured Transactions*, vol. 4, no. 1, pp. 1-11, 2012.

[43] J. Hwang, J.W. Kim, J.U. Choi,"A reversible watermarking based on histogram shifting", LNCS vol. 4283, pp.348–361, 2006.

[44] C.C. Lin, W.L. Tai, C.C. Chang,"Multilevel reversible data hiding based on histogram modification of difference images", *Pattern Recognition*, vol. 41, no. 12, pp.3582–3591, 2008.

[45] P.Y. Tsai, Y.C. Hu, H.L. Yeh, "Reversible image hiding scheme using predictive coding and histogram shifting", *Signal Processing*, vol. 89, no. 6, pp.1129−1143, 2009.

Papers Communicated/Accepted/Published

1. Akash Modi, Manu Bansal "**An Enhanced LSB Steganography Algorithm**" *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 5, pp 224-229, May 2015.
   (Published in IJARCSSE Journal)