

# High payload digital image steganography using mixed edge detection mechanism

Biswajit Jena



Department of Computer Science and Engineering  
National Institute of Technology Rourkela  
Rourkela – 769 008, India

# High payload digital image steganography using mixed edge detection mechanism

Dissertation submitted in

*May 2014*

*to the department of*

***Computer Science and Engineering***

*of*

***National Institute of Technology Rourkela***

*in partial fulfillment of the requirements*

*for the degree of*

***Master of Technology***

*by*

***Biswajit Jena***

*(Roll 212cs2469)*

*under the supervision of*

***Prof. Ratnakar Dash***



Department of Computer Science and Engineering

National Institute of Technology Rourkela

Rourkela – 769 008, India

*dedicated to my parents and brothers...*



Computer Science and Engineering  
**National Institute of Technology Rourkela**  
Rourkela-769 008, India. [www.nitrkl.ac.in](http://www.nitrkl.ac.in)

**Dr. Ratnakar Dash**  
Professor

May , 2014

## Certificate

This is to certify that the work in the thesis entitled *High payload digital image steganography using mixed edge detection mechanism* by *Biswajit Jena*, bearing roll number 212CS2469, is a record of research work carried out by him under my supervision and guidance in partial fulfillment of the requirements for the award of the degree of *Master of Technology in Computer Science and Engineering*. Neither this thesis nor any part of it has been submitted for any degree or academic award elsewhere.

*Prof. Ratnakar Dash*  
*Professor, Dept. of CSE*  
*NIT Rourkela, Odisha*

## Declaration

I, Biswajit Jena (Roll No. 212CS2469) understand that plagiarism is defined as any one or the combination of the following

1. Uncredited verbatim copying of individual sentences, paragraphs or illustrations (such as graphs, diagrams, etc.) from any source, published or unpublished, including the internet.
2. Uncredited improper paraphrasing of pages or paragraphs (changing a few words or phrases, or rearranging the original sentence order).
3. Credited verbatim copying of a major portion of a paper (or thesis chapter) without clear delineation of who did or wrote what. (Source: IEEE, the Institute, Dec. 2004)

I have made sure that all the ideas, expressions, graphs, diagrams, etc., that are not a result of my work, are properly credited. Long phrases or sentences that had to be used verbatim from published literature have been clearly identified using quotation marks.

I affirm that no portion of my work can be considered as plagiarism and I take full responsibility if such a complaint occurs. I understand fully well that the guide of the thesis may not be in a position to check for the possibility of such incidences of plagiarism in this body of work.

*Biswajit Jena*  
*Roll: 212CS2469*  
*Department of Computer Science*

# Acknowledgement

This thesis, however an individual work, benefited in several ways from different people. Although it would be easy to enlist them all, it would not be easy to appreciate their efforts.

The patient guidance and support of *Prof. Rantakar Dash* inspired me to work with full strength. His profound insight has guided my thinking to improve the final product. My earnest gratefulness to him.

It is indeed a privilege to be associated with *Dr. S.K. Rath* HOD, Department of Computer Science and Engineering and all faculties from the department. They have made available their support in a number of ways.

Many thanks to my friend and fellow research colleagues at NIT Rourkela. It was delight to work with you all, and special thanks to Ph.D. scholars Soubhagya Sankar Barpanda, Asish Kuamr Dalai and Jitendra Kumar Rout for valuable guidance and suggestions during this work.

Finally, I am grateful to all of my friend for continuous motivation and encouragement. Last but not least to my family having faith in me and always supporting me.

*Biswajit Jena*

## Abstract

The Least Significant Bit(LSB) is a spatial domain embedding technique suggest that data can be hidden in the least significant bits of the cover image and the human visual system(HVS) not able to find the secret data in the cover image. It is most powerful and easily understood method in spatial domain. LSB is widely used steganography technique in both spatial and frequency domain because all other methods in frequency domain are complex to understand and implement. In this thesis, along with using the LSB substitution method as a important stage, edge detection mechanism is used to take advantage for high payload, as edges are sharp areas of an image. In the proposed scheme, mixed edge detection mechanism is employed to achieve high payload steganography. Here, mixed edge detection mechanism is combination of Canny edge detection and Log edge detection techniques. Then applying the embedding algorithm, heavy amount data are stored in the cover image i.e high payload is achieved. Experimental results show that the steganography using mixed or hybrid edge detection mechanism accomplished with better peak signal to noise ratio(PSNR), compare to other steganographic model, for the same number of bits per pixel in embedded image.

**Keywords:** Steganography, Steganalysis, Spatial domain, Frequency domain, LSB substitution, Payload, Peak signal to noise ratio.

# Contents

<b>Certificate</b>	<b>iii</b>
<b>Declaration</b>	<b>iv</b>
<b>Acknowledgement</b>	<b>v</b>
<b>Abstract</b>	<b>vi</b>
<b>List of Figures</b>	<b>ix</b>
<b>List of Tables</b>	<b>xi</b>
<b>1 Introduction</b>	<b>1</b>
1.1 Nomenclature . . . . .	2
1.2 Background . . . . .	4
1.3 Steganography Types . . . . .	5
1.4 Steganographic Application . . . . .	6
1.5 Performance Evaluation Parameters . . . . .	7
1.6 Image Staganalysis . . . . .	9
1.7 Litreture Review on Image steganography methods . . . . .	10
1.7.1 Spatial domain LSB method [6] [7] [14] . . . . .	10
1.7.2 Steganography exploiting the Window Operating System [6]	12
1.7.3 A Novel Secure Communication Protocol Combining Steganography and Cryptography [16] . . . . .	13



1.7.4	A Novel Steganography Method for Image Based on Huffman Encoding [8]	14
1.7.5	Image Steganographic Method based on DCT [6]	14
1.7.6	Adaptive steganography	16
1.8	Motivation	16
1.9	Thesis Layout	17
<b>2</b>	<b>Mixed edge detection mechanism</b>	<b>18</b>
2.1	Edge detection mechanism	18
2.2	Canny Edge Detector	19
2.3	Laplrcian of Gaussian(Log)edge detection	20
2.4	Mixed or Hybrid edge detector	22
2.5	Summary	25
<b>3</b>	<b>Mixed edge detection mechanism for image steganography</b>	<b>26</b>
3.1	Embedding procedure	26
3.2	Extraction procedure	28
3.3	Experimental results	29
3.4	Comparision with classic LSB steganography	30
3.5	Comparison with hybrid edge detection mechanism using fuzzy edge detector	31
3.6	Summary	37
<b>4</b>	<b>Conclusions and Future Work</b>	<b>38</b>

# List of Figures

1.1	Basic block diagram of steganographic system [12] . . . . .	4
1.2	Diagram depicting classification of Information hiding . . . . .	5
1.3	Measurement triangle of steganography . . . . .	7
1.4	LSB Steganography in Spatial domain [6] . . . . .	11
1.5	The secret message revealed when the stego-image is opened using Notepad . . . . .	13
1.6	Data flow diagram depicting the overall embedding procedure in the frequency domain . . . . .	15
2.1	Two $128 \times 128$ test images for experiments.(a) Lena (b) Pepper . . .	19
2.2	Edge image of Lena and Pepper produced by canny edge detector with number of edge pixel 2362 and 2444 respectively . . . . .	21
2.3	The edge image of Lena and Pepper produced by log edge detector with number of edge pixel 1715 and 1593 respectively . . . . .	23
2.4	The edge image of Lena and Pepper produced by hybrid edge detector with number of edge pixel 3395 and 3407 respectively . . .	24
3.1	Embedding procedure of proposed scheme . . . . .	28
3.2	PSNR between cover image and stego image <b>44.0967</b> dB, <b>38.0015</b> dB, <b>31.1596</b> dB, <b>25.9715</b> dB, respectively corresponding to LSBs changes from 1 to 4. . . . .	31
3.3	The quality of stego image when $x = 1$ , $n = 2$ and $y = 1,2,3,4$ . . . .	33
3.4	The quality of stego image when payload changes only and $x=1,y=2,n=2$ . . . . .	34

3.5	The quality of stego image when $x=1,2,3,4$ , $y=2$ , $n=2$ and constant payload . . . . .	35
3.6	The quality of stego image when all parameters changes extremely.(a) $p= 9976$ bits, $y= 2$ , $x= 2$ , $n=2$ (b) $p= 11584$ bits, $y= 3$ , $x= 3$ , $n=2$ (c) $p= 13320$ bits, $y= 4$ , $x= 4$ , $n=4$ (d) $p= 14352$ bits, $y= 5$ , $x= 5$ , $n=4$ . . . . .	37

# List of Tables

3.1	The performance comparison of stego-image produced by the classic LSB steganography method and the proposed scheme. . . . .	30
3.2	The performance comparison of stego-image produced by the hybrid edge mechanism using fuzzy edge and proposed scheme. . . . .	32
3.3	The performance of stego image when $x = 1$ , $n = 2$ and $y = 1,2,3,4$ .	32
3.4	The performance of stego image when payload changes only and $x=1,y=2,n=2$ . . . . .	34
3.5	The performance of stego image when only number of bits in non-edge pixel(x) are changing and all other parameters remain constant . . . . .	35
3.6	The performance of stego image when all parameters changes extremely . . . . .	36

# Chapter 1

## Introduction

In recent times, the need for digital communication has increased dramatically and as a result, the Internet has become essentially means more effective and faster communication to digital communication. At the same time, data on the Internet has become susceptible to copyright infringement, espionage, piracy, etc., which therefore requires secret communication. As a result, a new domain dedicated to information security has evolved and is known as data hiding. Steganography is a relatively novel addition to the area of data hiding but traces its origin to long ago in history.

Steganography employs medium such as image, audio, video, or text file to conceal any information in it, so that does not draw any interest and looks like an innocuous medium. Cover medium such as digital image, video and photo became the obvious choice. Stego media are the media, which contain the secret information while cover media are the plain file. Recently, the images have been a popular choice as a means to cover mainly because of its redundancy in the representation and the ability to penetrate applications in daily life. Over the years, many algorithms have been proposed to hide data in images and developing new algorithms are a topic of current research. In this thesis, some of the most popular and effective among image steganography algorithms are analyzed for their mechanisms, advantages and disadvantages, which could be a valuable guide for future research scope openings.

The three important categories of steganographic methods are: spatial domain method, frequency domain method and adaptive methods. The last one can be employed both in previous two cases, as it is considered as special cases. Again, spatial domain and frequency domain are two broad classification in image steganography. In spatial domain, the hidden data is inserted directly in the intensity of the pixels i.e in spatial domain method, a steganographer made a modification of the hidden message and the cover file, which implies modification at the stage of the least significant bit. This strategy is less complicated and has more effective than the other two types of methods, while in case of frequency domain, first image is transformed to frequency domain or transform domain and then, the hidden data is inserted in the transform coefficients.

There are different file format of image are used in study of image steganography, such as jpeg, bmp, and gif. Digital images are typically stored in either 8-bit or 24-bit files. The significance of 8-bit is due to their small size and 24-bit, due to the high payload they offer and to the fact that the large number of colors they contain make the changes from the secret message undetectable from the human visual system.

Now-a-days there are so many applications of data hiding. Information hiding methods can not easily be classified in either category of steganography or watermarking, and there are so many similarity between these two terms. Therefore, different applications of these two based upon application of the algorithm. So instead of classifying between them, the most common information hiding applications are: fingerprinting, covert communication, copyright protection, secret communication, and secure storage .

## 1.1 Nomenclature

The following terminologies are used frequently in image steganography systems, irrespective of the algorithms by which they are implemented [15].

- (i.) **Image:** An image is an array of numbers that represent light intensities at

different points (pixels) and mathematically an image  $C$  is a discrete function assigning a colour vector  $c(x, y)$  to every pixel  $(x, y)$ .

- (ii.) **Cover Image:** The cover image is the carrier of the secret message. A cover is usually chosen in a way that seems more common and harmless and not arouse suspicion.
- (iii.) **Stego Image:** The cover image with a hidden secret message inside is known as the Stego image. It is employed at the receiver site to pull out the hidden message.
- (iv.) **Stego Key:** Stego key is a key to integrate the information inside cover medium and extract same information from the stego medium. Can be a number generated by a pseudo-random numbers or may be only a password to decode the embedding location.
- (v.) **Embedding Domain:** The Embedding domain refers to the cover medium characteristics that are exploited in embedding message into it. It may be spatial domain when direct modification of the constituent elements of the cover is modified (e.g. pixels in an image) or it can be the frequency domain or transform domain if mathematical transformations are carried on the medium before embedding.

## 1.2 Background

The word steganography is derived from Greek words which mean “Covered Writing”. It has been used in different forms for thousands of years. In ancient times King were used to keep slave, whose skull of the shaved head is used to write secret message and after his hair grew back, the slave was send with the message . Other ways of ancient communication are also made with the help of wax, invisible ink, null ciphers, carrier pigeons and microdot etc. [10].

Steganography is the secret communication between two parties with the goal to conceal the subject of a message. Steganography is complementary to cryptography where it aims at hiding the existence of a message rather than making the message illegible through encryption. Thus Steganography might be useful for secret communication in countries and regions where public use of cryptography is prohibited or restricted [16].

A basic block diagram of steganographic model is depicted in Fig. 1.1. The information is inserted in a cover image by the steganographic encoder, which may employs a key or password. Here the concept of symmetric key steganography having both side the same key( $K_1$ ) is used. [3]. Now the produced stego image is transmitted to the receiver and it is decoded by using the same key to get back the original message. As the stego image is carried over channel, it may be viewed by unintended persons but stego image will behave like an innocent medium without showing the hidden message inside it.

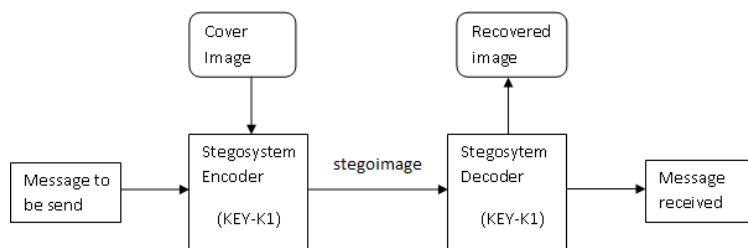


Figure 1.1: Basic block diagram of steganographic system [12]



### 1.3 Steganography Types

Data hiding methods are classified into three main classes such as: steganography, watermarking, and cryptography. Steganography and watermarking are comes under one subclasses as there is no clear boundaries between them. Fig. 1.2 depicting the classifications of all these three classes of data hiding methods.

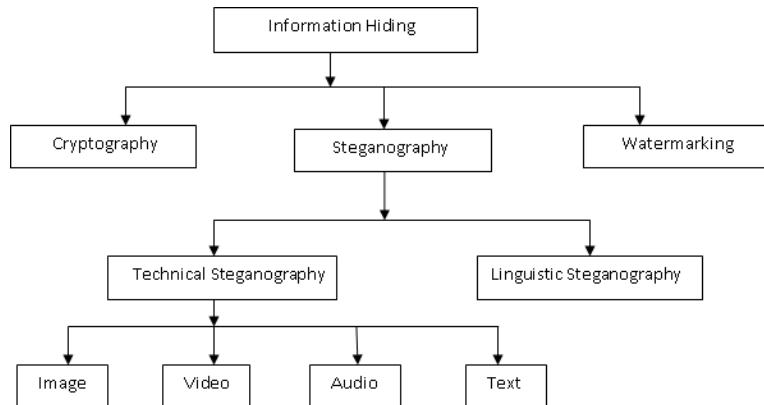


Figure 1.2: Diagram depicting classification of Information hiding

Steganography is the science of concealing data in such a manner that forbid the detection of secret data. Steganography literally means “covered writing” and is generally employed to hiding information inside some cover medium.

Cryptography deals with encryption and decryption process of a message. The advantages of steganography over cryptography is that in steganographic messages do not attract attention to itself but in cryptography, plainly visible encrypted message, no matter how unbreakable will arose suspension. Steganograpgy might be useful for secret communication in countries and regions where public use of cryptography is prohibited or restricted. Unlike cryptography it never uses complex algorithms and arithmetic.

Watermarking is the process of inserting a message on a host signal. Watermarking as compare to steganography has the additional necessity of robustness against public attack. A watermark can be either visible or invisible. Digital watermarking focuses mainly on the protection of authentication of digital

media and intellectual property rights. It holds data regarding (hide) its author, its buyer and the integrity of content. This method help keeping track of the quick and inexpensive distribution of digital information over the Internet. Steganography communication are usually point-to-point (between sender and receiver) while watermarking technique are usually one-to-many.

## 1.4 Steganographic Application

Steganography is utilized in different valuable applications like, improvising robustness of image search engines copyright control of materials, and smart IDs where a person's particulars are inserted in their photographs. Apart from that videoaudio synchronization, TV broadcasting, company's safe circulation of secret data, TCP/IP packets, and checksum embedding are the other applications.

Now-a-day there are different applications of data hiding. Use of information hiding can be done either in ethical or unethical ways. There is no clear boundary between steganography and watermarking. These two terms are very similar to each other and the classification between them is based on the application of the algorithm. So, the most common data hiding applications are printer steganography, distributed steganography, secret communication, fingerprinting, copyright protection and secure storage [4].

**Fingerprinting** helps in tracing owner of particular copy of the media be traced by means of watermarking. The employed watermarking technique must support high degree of robustness against both intentional and unintentional attacks. Digital fingerprint and a digital watermark, are two very different technologies with somewhat similar goals.

**Secret communication** hide presence of communication can be accomplished by virtue of hiding secret information within digital cover file. This application comes under steganography instead of watermarking.

**Secure storage** implies using the cover image as security purpose to store sensitive information. For example, medical record and prescription of patients should be kept as secret so that it cant abused by illegal people as these are

sensitive data of human life.

**Copyright protection** mechanisms that prevent data, usually digital data, from being copied. The term “copyright protection” is occasionally seen in this usage, but is an error; copy protection or Digital Rights Management is the usual term. To protect owner’s data, embed the vital information within the digital cover host file.

## 1.5 Performance Evaluation Parameters

There are so many important parameters to be kept in mind while learning steganographic models. Robustness, Capacity, and Security are the three important steganographic parameter [15]. Steganography triangle is best way expressing the relationship between these parameters as shown in Fig. 1.3. It shows balance among the three parameter involved with steganographic system. They are interdependent on each other and in order to improve a parameter, one or both of other elements needs to be sacrificed.

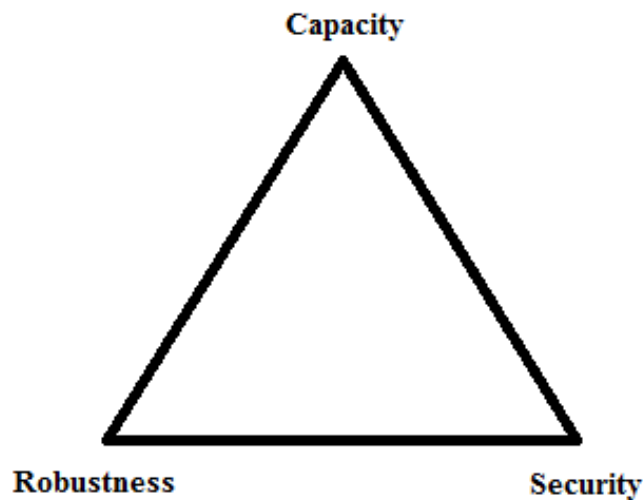


Figure 1.3: Measurement triangle of steganography

**Robustness:** It states the potential of the secret message to survive the process of embedding and extraction, along with manipulations of the stego image

such as compression, filtering, rotating, and cropping. It can be said that, an embedded message has the potential to survive attack by a suspecting intruder during transmission of message. The robustness of steganographic system checked, if the payload has ability to endure when a cover image gradually decays. However, it is most expected that the embedded content be fragile, so as to lower the chance that an interceptor would be able to reassemble the embedded message.

**Capacity:** Capacity of steganographic system states that, the maximum number of bits which could be inserted in the cover image, and at the same time the quality of stego image should be high and human visual system unable to detect the difference between stego image and cover image.

In steganography the cover image is act like a carrier which carries embedded information. So care should be taken for channel capacity i.e stego image like other communication channel and at the same time undetectability should be achieved.

**Security:** It is the ability of an embedding carrier to remain undiscovered. The communication carrier between sender and receiver should be so robust that it does not create any suspicion to the eavesdropper. So undetectability is main motto of steganographic system while taking security as one of the performance parameter. Therefore, proper care should be taken, so that the intruder will unable to distinguish between stego image and cover image.

Apart from the above three parameters, steganographic system also depends upon some other important parameters described below:

**Domain of Embedding:** Domain of embedding plays a vital role in determining the overall performance of the steganographic algorithms. Spatial domain algorithms often offer higher capacity but fall prey to statistical steganalysis. Transform domain algorithms, on the other hand are more resistant to statistical steganalysis.

**Type of Images Supported:** Images are available in a large number of formats. Thus, it is important to understand which types of images are suitable for the steganographic algorithms of the various types. Images primarily use lossy or lossless compression mechanisms and the properties of images affect the steganographic methods applicable to those images. Generally there are two types

of image compression methods are used in image processing. They are lossy compression and lossless compression. Out of it, lossless compression is good for image steganography as it retain original image data exactly. eg GIF and BMP file formats and example of lossy compression is JPEG.

**Time Complexity:** Steganographic algorithms vary according to their domain of embedding. In simpler systems, the embedding job is less time consuming but may not be as secure as some other more complicated ‘systems offering better performance. Nevertheless, time complexity of an algorithm is important for judging the applicability of the algorithm for embedding into large images and also their implementation in low resource systems such as mobile devices etc.

## 1.6 Image Staganalysis

Steganalysis is the study of detecting messages hidden using steganography. It is very similar to Cryptanalysis which is a well known science of information security. Most cases, a steganalysis system is created by steganographers to check the robustness of their method. Steganalysis is accomplished by employing several image processing techniques,such as, rotating, cropping, translating, and image filtering .

In case of passive steganalysis, it tries to ruin the route of secret communication between sender and receiver, without bothering about the detection of the secrete data, by taking help of the following image processing techniques such as, changing the image format, flipping all LSBs or by under-taking a severe lossy compression,e.g.,JPEG. Active steganalys is however, is a special technique that detects the existence of stego-images.

## 1.7 Literature Review on Image steganography methods

Literature Review on image steganography tries to provide a summary of the almost steganographic methods in digital images. Most of the literature on steganography that studied based on the techniques of spatial domain, frequency domain and adaptive method steganography.

Spatial domain methods commonly use a least significant bit (LSB) replacement technique as the simplest and most convenient approach. Discrete cosine transform (DCT), Discrete wavelet transform (DWT) and Fourier transform (FT) are the methods of frequency domain, that are mostly used for image steganography along with the LSB technique. Finally, the last one will enlighten the new contribution in the domain which is called as adaptive steganography (AS). It is otherwise termed as perceptual masking (PM) or “Statistics-aware embedding” or “Masking” or “Model-Based”. Adaptive steganography can be employed both in spatial domain and frequency domain, as it belongs to special cases.

### 1.7.1 Spatial domain LSB method [6] [7] [14]

In spatial domain methods, modification of cover medium and secret data takes place in the spatial domain, that includes changes in the least significant bits of cover medium. This method is simple one and has a more effective than the frequency domain and adaptive methods. A common framework depicting the concept of spatial domain LSB method is illustrated in Fig. 1.4.

In the classic LSB steganographic concept, first of all, the secret message is converted into binary values, then inserted into the cover medium by substituting the least significant bits of the cover medium. Let's take an 8-bit gray level cover image, where pixels are represented in bit stream corresponding to a gray scale value. Let the first six pixels 156, 159, 158, 155, 158, 156 of the cover image have the given gray scale values: 10011100, 10011111, 10011110, 10011011, 10011110 and 10011100 respectively. In order to conceal the secret message “HELLO”

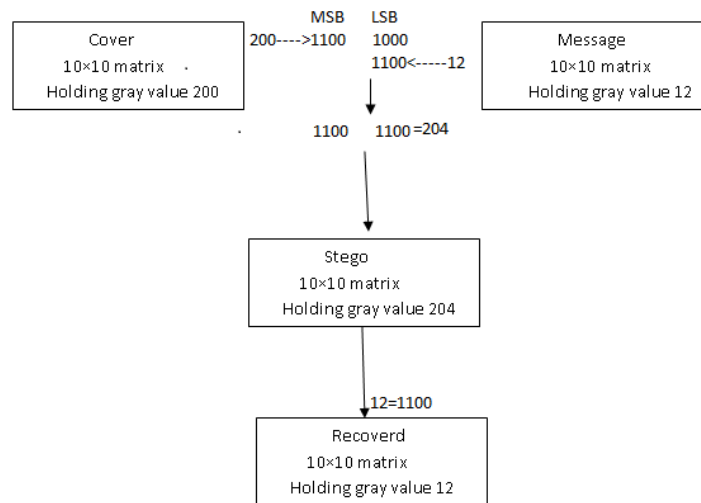


Figure 1.4: LSB Steganography in Spatial domain [6]

whose bit stream presentation is 0 1 1 0 1 0 ..., replace the LSBs of 156, 159, 158, 155, 158, 156 with bit stream of message “HELLO”. These changed stego pixels 156, 159, 159, 154, 159, 156 have the following new greyscale values: 10011100, 10011111, 10011111, 10011010, 10011111 and 10011100 [7].

Digital images are typically stored in either 8-bit or 24-bit files. When a 24-bit color image is used, it give better space to store secret message. The primary color components of a color image are red, green and blue and they are providing all color variation of pixels in image. Each color component is of 1 byte; so a 24-bit images takes 3 bytes per pixel to show a color value and one can place three bits in each selected pixel by altering a bit of each color components. A  $800 \times 600$  pixel image, thus can store a total amount of 1, 440, 000 bits or 1, 80, 000 bytes of data. Here is an another example as previous one, for storing data in color image having three adjacent pixels (9 bytes).

```

10010101 00001101 11001001
10010110 00001111 11001011
10011111 00010000 11001011

```

Suppose the number 300, which bit stream value is 100101100, inserted into the LSBs of this part of the image. If the 9 bits of message is embedded over the

LSB of the 9 bytes above, the following bits pattern of pixel will generated (bits in bold face have been changed).

```

10010101 00001100 11001000
10010111 00001110 11001011
10011111 00010000 11001010

```

So, here the observation states that only 5-bits are changed out of 9 bits when the number 300 was inserted into the grid of pixel. Now its clear that, only half of the bits in an image will need to be changed to hide a secret message using the maximum cover size. Since there are 256 possible intensities of each primary color, altering the LSB of a pixel results in minor changes in the intensity of the colors. The human visual system cannot detect these modification, so the message is successfully hidden [14].

## 1.7.2 Steganography exploiting the Window Operating System [6]

This section says another way of achieving steganography by simply writing commands in command window of Windows OS ,e.g.,Windows 8, Windows 7, Windows XP. The following code helps in to through this method:

```
C : >Copy Cover.jpg /b + Message.txt /b Stego.jpg
```

The above code do the operation like that, it first embeds the secret information of the text file “Message.txt” into the image file “Cover.jpg”, then give the resultant stego-image “Stego.jpg”. The logic behind this method is to abuse the recognition of EOF(End of file). In other words, the message is packed and inserted after the EOF tag. When stego image is viewed using any photo editing application, the latter will just show the picture ignoring any thing coming after the EOF tag. However, when opened in Notepad for example, the message comes out of itself after displaying some data as shown in 1.5. The embedded message does not change the image quality. Neither image histograms nor visual perception



can detect any difference between the two images due to the secret message being hidden after the EOF tag. Unfortunately, this simple technique would not resist any attacks by steganalysis experts nor any kind of editing to the stego-image and not a good method for high payload steganography.



Figure 1.5: The secret message revealed when the stego-image is opened using Notepad

### 1.7.3 A Novel Secure Communication Protocol Combining Steganography and Cryptography [16]

Cryptography and Steganography are two complimentary word in spy class family of security to protect sensitive information. In this paper, cryptography and steganography are combined, to get better communication protocol. Here the concept of LSB matching and well known boolean function for stream cipher is used. Here, grayscale images are used as cover medium, and for encryption and controlling the pseudo-random increment or decrement of LSB, boolean function is used. Both encryption and concealing of message takes place in one step while other methods take two separate stage. So here performance and security will be more as it takes less time for computation.

The use of boolean function in LSB Matching embedding algorithm work like this, the LSB of each pixel of cover image is compared with each bit of secret message, if matching found, do nothing; else, pseudorandomly make a increment or decrement the pixel value of cover image. At the receiving side, by the help of

decoding scheme, the hidden secret message bits are directly come from the LSB of the stego image.

#### **1.7.4 A Novel Steganography Method for Image Based on Huffman Encoding [8]**

This is the case of novel steganography method using Huffman Encoding technique for better performance. Here, first take two 8-bit gray scale image not of same size as cover image and secret image respectively. Then Huffman Encoding is applied to the secret message image before embedding it into the cover image. Here also LSB method is used. So message bits generated by Huffman encoding now inserted into least significant bits of each pixel of cover image. In order to make the stego-image as standalone information holder to the receiver, both the Huffman Encoded bit stream and Huffman table are also embedded inside the cover image .

This method is better than other existing method as it gives better security and high quality stegoimage. Experimental results of this paper shows that, the stego images generated by this method are very similar to the cover images and it is very hard find the difference between them and it accomplished with 99% recovery of the secret image.

#### **1.7.5 Image Steganographic Method based on DCT [6]**

LSB embedding mechanism is the best steganographic method that have been studied as it give good perception to HVS. But it has low resistance to statistical attacks, so that have to think some alternatives. Therefore, its better choice to apply LSB method in frequency domain.

In case of the Frequency Domain to hide a secret message inside the cover image, that cover image has to transformed into DCT (discrete cosine transformation)coefficients. Here the DCT transforms the cover image from an image representation into a frequency representation, by grouping the pixels into

nonoverlapping blocks of  $8 \times 8$  pixels and then transforming the pixel blocks into 64 DCT coefficients block each. A change in a single DCT coefficient will affect all 64 image pixels in that block. The DCT coefficients of the transformed cover image will be quantized, and then modified according to the secret data based on LSB steganography. The definition 2-D DCT for an input image  $A$  and output image  $B$  is:

$$B_{p,q} = \alpha_p \alpha_q \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} A_{mn} \cos \frac{\pi(2m+1)p}{2M} \cos \frac{\pi(2n+1)q}{2N} \quad (1.1)$$

where  $0 \leq p \leq M-1$  and  $0 \leq q \leq N-1$

$$\alpha_p = \begin{cases} \frac{1}{\sqrt{M}}, & p = 0 \\ \sqrt{\frac{2}{M}}, & 1 \leq p \leq M-1 \end{cases} \quad (1.2)$$

$$\alpha_q = \begin{cases} \frac{1}{\sqrt{N}}, & q = 0 \\ \sqrt{\frac{2}{N}}, & 1 \leq q \leq M-1 \end{cases} \quad (1.3)$$

$M, N$  are the rows and columns size of  $A$  respectively.

DCT is used extensively with image and video compression e.g. JPEG lossy compression. Steganography based on DCT JPEG compression goes through different steps as shown in 1.6.

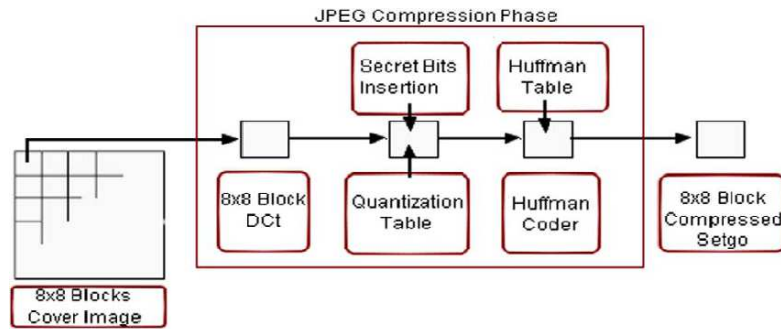


Figure 1.6: Data flow diagram depicting the overall embedding procedure in the frequency domain

### 1.7.6 Adaptive steganography

Adaptive steganography is a new area in steganography. It is the combination of both spatial domain and frequency domain methods. The other terms for adaptive steganography are “perceptual masking” or “Statistics-aware embedding”, or “Model-Based”. In this approach, before working with LSB or DCT coefficients of cover image, study the statistical global features of the image. This statistical report will indicate the pixel where modification have to done in the image. This model is characterized by a random adaptive selection of pixels depending on the cover image and the selection of pixels in a block with large local standard deviation. Here local standard deviation is used to avoid areas of uniform color(smooth areas). This behaviour makes adaptive steganography seek images with existing or deliberately added noise and images that demonstrate color complexity.

## 1.8 Motivation

Keeping the research directions a step forward, it has been realized that there exists enough scope to new research work. The previous work used to implement steganographic concept but high payload cant achieved and simultaneously facing statistical attack. In this work, an effort has been made to propose new high payload digital image steganography using hybrid edge detection mechanism. In particular, the objectives are narrowed to —

- (i) In order to store more data i.e to enhance the embedding payload, more than one bit of each pixel is used in LSB substitution method for embedding the message. But at the same time, care should be taken for the quality of stegoimage.
- (ii) A good steganography method always take care about the quality of stegoimage while increasing the payload. Therefore to develop a better LSB steganography scheme, edge detection mechanism is used which resist statistical attack.

## 1.9 Thesis Layout

The organization of thesis is as follows —

**Chapter 2:Hybrid edge detection mechanism** In this chapter, a depth discussion regarding two most important edge detection mechanism are presented. Along with pros and cons of canny edge and log edge detection mechanism, it also describe how to exploit maximum number of edge from image. The experimental result also displayed with suitable test images.

**Chapter 3:High payload digital image steganography using hybrid edge detection mechanism** In this chapter, the procedure of embedding and extraction are explained in detail with suitable example. The experimental results for the proposed scheme is also given in this chapter showing the quality and performance of stego image. It include also comparison with the previous scheme like classic LSB steganography and image steganography using hybrid edge mechanism, where hybrid is made by fuzzy and canny edge.

**Chapter 4:Conclusion and Future Work** This chapter provides the qualitative and quantitative comparisons of the outputs of proposed technique tested over various image with the other existing methods of image steganography.

# Chapter 2

## Mixed edge detection mechanism

In this chapter discussion regarding edge and different type of edge of an image are presented. Also concept of hybrid edge are presented to exploit maximum number of edge pixel present in the cover image.

### 2.1 Edge detection mechanism

An edge is defined as the points in an image where brightness changes abruptly. Edges are substantial local modification in intensity of an image. They are the boundaries between image segments.

Image processing, machine vision and computer vision generally require edge detection mechanism as an important tool, particularly in the field of feature detection and feature extraction as edges are main components for analysis of the most essential contained information in an image. The process of getting meaningful transitions in an image, is called edge detection. The points where sharp modification in the brightness takes place generally from the boundaries between distinctly separate objects. Many classical edge operators are available in the literature of image processing. Such as:

1. Sobel Edge Detector
2. Prewitt Edge Detector



(a) Lena

(b) Pepper

Figure 2.1: Two  $128 \times 128$  test images for experiments.(a) Lena (b) Pepper

3. Robert Edge Detector
4. Laplacian of Gaussian(Log) Edge Detector
5. Canny Edge Detector
6. Fuzzy Edge Detector

Among the above edge detection methods, the most popular, efficient and widely used edge detection is the canny edge detection mechanism. Good localization, good detection, and single response to an edge are the three important attributes of canny edge operator, for which it chosen best among the other operator available. Here four  $128 \times 128$  grayscale image are used for experiment in fig.2.1 such as: lena, pepper.

## 2.2 Canny Edge Detector

The best thing about canny edge detector is that it has three characteristics for which it is mostly employed in machine vision and image processing to find the sharp intensity modification and the object boundaries in an image. They are:

- All the important edges are preserved, no false edges are considered and at the same time magnitude of error detection should be low.

- Minimum distance should be maintained between the real and located position of the edge.
- There is only one response to a single edge.

In case of canny edge operator, a pixel is considered to be an edge pixel, if the gradient magnitude of that particular pixel is more than those of the pixels on either sides of it and in the direction of utmost intensity modification. The procedure for Canny edge detector implementation is summarized in the following steps [9]:

- 1 First, the image is smoothed by applying Gaussian filter with a fixed standard deviation, to reduce the noise. ( $\rho$ ) .
- 2 The gradient magnitude  $g_x^2 + g_y^2$  and edge direction  $\tan^{-1}(\frac{g_x}{g_y})$  are calculated at each point. A point whose strength is locally maximum in the direction of gradient is defined as an edge point.

The Canny edge detector's performance, in the simulation of "Lena" and "Pepper" as the test images are provided here. Fig 2.2 depict the visual quality of original image and edge image produced by the canny edge detector and the number of edge pixel present in it.

## 2.3 Laplacian of Gaussian(Log)edge detection

In case of Laplacian operator the main source of performance reduction is the noise in the image. So before the enhancement of edge, smoothing can be done to reduce the noise. The image is smoothed by convolution between Log operator and Gaussian shaped kernel followed by the use of Laplacian operator. [9].

Gaussian function is given by:

$$G(x, y) = e^{-\frac{x^2+y^2}{2\sigma^2}} \quad (2.1)$$

where  $\sigma$  -standard deviation, is a smoothing function which if convolved with an image, will blur it. The degree of blurring is determined by the value of  $\sigma$

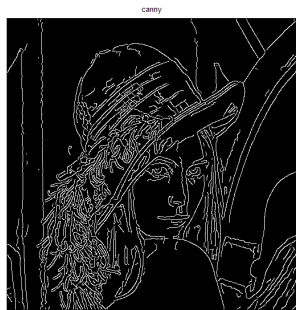




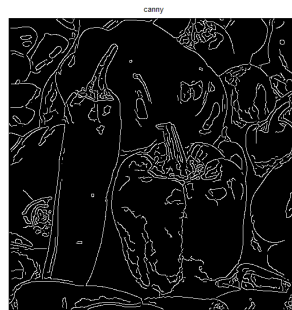
(a) original image



(b) original image



(c) no. of edge pixel 2362



(d) no. of edge pixel 2444

Figure 2.2: Edge image of Lena and Pepper produced by canny edge detector with number of edge pixel 2362 and 2444 respectively

Laplacian of Gaussian function is then:

$$\nabla^2 G(x, y) = \frac{\partial^2 G(x, y)}{\partial x^2} + \frac{\partial^2 G(x, y)}{\partial y^2} = \left[ \frac{x^2 + y^2 - 2\sigma^2}{\sigma^4} \right] e^{-\frac{x^2+y^2}{2\sigma^2}} \quad (2.2)$$

The laplacian  $L(x, y)$  of an image with pixel intensity  $I(x, y)$  is given by :

$$L(x, y) = \frac{\partial^2 I}{\partial x^2} + \frac{\partial^2 I}{\partial y^2} \quad (2.3)$$

Convolution of image with  $\nabla^2 G(x, y)$  knowing that it has two effects. (a) It smoothes the image (thus reducing the noise) (b) It computes the Laplacian, which yeilds a double edge image.

The Log edge detector's performance, in the simulation of "Lena" and "Pepper" as the test images are provided here. Fig 2.3 depict the visual quality of original image and the edge image produced by the canny edge detector and the number of edge pixel present in it.

## 2.4 Mixed or Hybrid edge detector

The word hybrid shows that, combination of two or more cases. So here the hybridization takes place by the help of the Log edge detector and canny edge detector. This hybridization helps in finding more amount of edge pixel in the image along with clear, precise object boundaries in the image. Hybrid edge detector find the object boundaries that are far better than those are generated by either of canny edge or log edge detector.

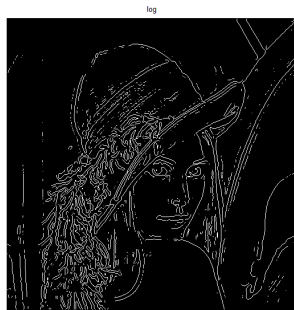
Let us take a cover image  $I$ ,  $I_1$  the edge image produced by the Log edge detector and  $I_2$  the edge image produced by canny edge detector respectively. Now, perform a OR operation between  $I_1$  and  $I_2$  , which will produce  $I_0$ , is the edge image produced by hybrid edge detector. Fig. 2.4 depict the hybrid edge images and the number of edge pixels that are produced by this operation.



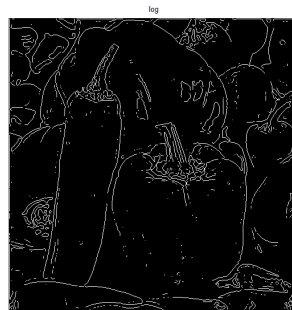
(a) original image



(b) original image



(c) no. of edge pixel 1715



(d) no. of edge pixel 1593

Figure 2.3: The edge image of Lena and Pepper produced by log edge detector with number of edge pixel 1715 and 1593 respectively



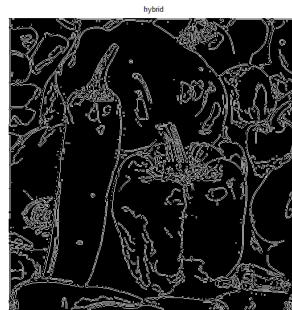
(a) original image



(b) original image



(c) no. of edge pixel 3395



(d) no of edge pixel 3407

Figure 2.4: The edge image of Lena and Pepper produced by hybrid edge detector with number of edge pixel 3395 and 3407 respectively

## **2.5 Summary**

In this chapter, a depth discussion regarding two most important edge detection mechanism are presented. Along with pros and cons of canny edge and log edge detection mechanism, it also describe how to exploit maximum number of edge from image. The experimental result also displayed with suitable test images.

# Chapter 3

## Mixed edge detection mechanism for image steganography

This chapter proposes a new LSB steganography model based on hybrid edge detection mechanism. Embedding procedure and extracting procedure are two important modules of this scheme like any other steganographic system.

### 3.1 Embedding procedure

The embedding method of this proposed scheme contains three steps [7]:

Step-1: In this step by employing the hybrid edge detector mechanism, get the edge image  $I'$  from the original image  $I$ .

Step-2: This is the most important stage of the embedding procedure. In this case, divide the edge image  $I'$  into a number of blocks. Each block contains  $n$  pixels and is called  $n$ -pixel block. The  $n$ -pixel blocks are listed as  $B_1, B_2, \dots, B_n$ . Here, the first pixel  $B_1$  is employed to keep the status value of the other pixels of the block. The status value of each pixel  $B_i$ , is defined as '1', if  $B_i$  is edge pixel, otherwise, it is '0'. By, the well known LSBs substitution method, the status value of pixels from  $B_2$  to  $B_n$  is stored inside  $B_1$ .

For better understanding consider this example, take a block  $A =$

$[B_1, B_2, B_3]$ , with  $n = 3$ . In this example, assume that  $B_1$  and  $B_3$  are edge pixels. So, the status value of the pixels  $B_2$  and  $B_3$  is '01'. And, as per the rule two LSBs in the pixel  $B_1$  will be '01'.

In this step, the edge image of the original image determine whether a given pixel is refereed as edge pixel or not. The hybrid edge detector which is generated in step 1 is responsible for this.

In this method, pixel  $B_1$  is known to be the starting pixel(index) of n-pixel block, since the bits of the LSBs in  $B_1$  are altered by the status of pixels  $B_2, B_3, \dots, B_n$ . and the length of block is carefully chosen. The length of the block is another important issue, which should be chosen carefully. If there are n pixels in each block, care should be taken to employ n-1 number of bits to act as the status value of the pixels  $B_2, B_3, \dots, B_n$ . Thus, there is change of n-1 number least significant bits in the pixel  $B_1$ . In order to maintain the quality of pixel  $B_1$  and to maximize the insertion rate, the proposed values of n as 2,3,4 or 5, that are generally chosen.

Step-3 The n-pixel block of cover image according to edge image, first, divided into edge pixel and non-edge pixel category in order to hide the secret message. The non edge pixel category corresponding to cover pixel of original image then will contain x bits of secret message and edge pixel category corresponding to cover pixel of original image will contain y bits of secret message by employing least significant bit substitution method. For experimental purpose the value of x are 1, or 2 and value of y are 3, 4 or 5, which are generally chosen to preserve the quality of stego-image.

Lets take an example, 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  $B_1, B_2, B_3$  and  $B_4$  with the secret message  $S = '0\ 1\ 1\ 0\ 1\ 0\ 1\ 1'$  and considered image A is a four-pixel block.

Its come to know that  $B_2$  and  $B_4$  are edge pixels from hybrid edge image that is generated in step 1 . So, the status of  $B_2, B_3$  and  $B_4$  is '101'. Thus,

substitute three least significant bits in pixel  $B_1$  with '101' and the new value of  $B_1$  became  $[1\ 0\ 1\ 0\ 1\ 1\ 0\ 1]$  and denoted as  $B'_1$ .

In this example lets take parametric value for non-edge pixel(x) as '1' and edge pixel(y) as '3', respectively. Therefore, there will be substitute of 3 least significant bits in pixel  $B_2$  and one least significant bits in pixel  $B_3$  from the secret message bits. Similarly, replace three LSBs in pixel  $B_4$  with three secret message bits. The changed pixel value of  $B_2$ ,  $B_3$  and  $B_4$  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 and the changed value of the image A, will be denoted by stego image  $A'$ , is  $[1\ 0\ 1\ 0\ 1\ 1\ 0\ 1]$ ,  $[1\ 0\ 0\ 0\ 0\ 0\ 1\ 1]$ ,  $[1\ 1\ 1\ 1\ 1\ 1\ 0\ 0]$ ,  $[0\ 0\ 0\ 0\ 1\ 1\ 0\ 1]$ .

The whole embedding procedure of this example are illustrated in the Fig. 3.1.

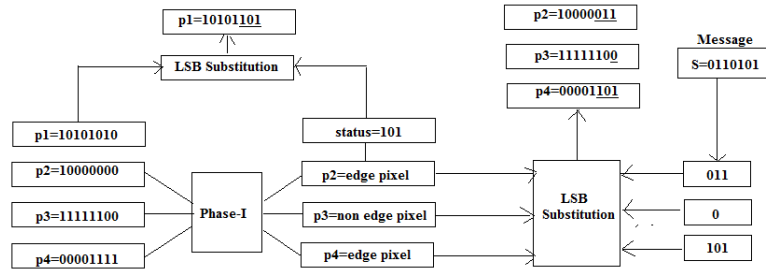


Figure 3.1: Embedding procedure of proposed scheme

## 3.2 Extraction procedure

In this case, like embedding procedure, divide the stego image into a number of blocks. Each block contains  $n$  pixels and is called  $n$ -pixel block. The  $n$  pixel blocks are listed as  $B'_1, B'_2, \dots, B'_n$ .

The status value of the pixels from  $B'_2$  to  $B'_n$  are obtained from the  $(n-1)$  LSBs in pixel  $B'_1$ . Now identify which pixel belongs to the non-edge pixel category and which one belongs to the edge pixel category from this status value. Then  $y$  LSBs from the edge pixel category and  $x$  LSBs from the non edge pixel category are



extracted to get the secret message. Finally, by adding all the LSB from both category in sequence, will get back my original message back.

Consider the example, the stego image  $A'$  with 4 pixels values 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  $B'_1, B'_2, B'_3, B'_4$ .

Get the three LSB from  $B'_1$  i.e '1 0 1' as it is four block image. From this status value, its come to know that 2nd and 4th pixels are edge pixels and 3rd pixel is non edge pixel. So as per the rule of embedding scheme, 3 bits of LSB will pull out from  $B'_2$  and  $B'_4$  and one bits from  $B'_3$ . So the pull out bits from  $B'_2$  are '0 1 1', from  $B'_4$  are '1 0 1' and from  $B'_3$  is '0'. Now I will get the secret message as '0 0 1 0 1 0 1' by adding these extracted bits.

### 3.3 Experimental results

The experimental results presented in this section demonstrate the performance of the proposed scheme. To conduct the experiments, two  $128 \times 128$  grayscale images are used, "Lena" and "Pepper". These test images are shown in Fig 2.1.

Peak-signal-to-noise ratio (PSNR) which computes the PSNR ratio, in decibel, between two images is used here to measure the performance for image distortion. PSNR ratio is generally employed as performance measure among cover image and stego image. High PSNR value gives, better the quality of the stego image. PSNR value falling bellow 30 dB suggest a fairly low quality i.e distorted image caused by embedding is high. However, a high quality stego image should strive for 40 dB and above.

The PSNR formula is defined as:

$$PSNR = 10 \log_{10} \left( \frac{R^2}{MSE} \right) \quad (3.1)$$

where,  $R = \max.$  fluctuation in i/p image and MSE=Mean Square Error

$$MSE = \frac{\sum_{M,N} [f(m,n) - g(m,n)]^2}{M \times N}$$

Where M,N are height and width of image.

In this proposed scheme, payload(p), number of bits substituted in the LSB of non-edge pixel(x), number of bits substituted in the LSB of in edge pixel(y) and number of blocks of cover image(n), are taken as the different parameters and PSNR is calculated as performance parameter

### 3.4 Comparison with classic LSB steganography

In this proposed scheme, when substituting four LSBs of each edge pixel, by the secret message on cover image, not only is the PSNR high, but the quality of stego image is also good as perceived by the human visual system. To prove that this scheme provide better stego image quality than the normal LSB steganography methodology, with the help of same size test image and with same payload ratio, the performance of classic LSB steganography is compared with proposed scheme. Figure 3.2 gives the quality of stego image when the number of LSBs in each pixel is chosen from 1 to 4.

Table 3.1: The performance comparison of stego-image produced by the classic LSB steganography method and the proposed scheme.

Payload(p)	no.of bits of LSB	PSNR of LSB scheme	no.of bits of edge pixel(y)	no.of bits of non edge pixel(x)	no.of block(n)	PSNR of proposed scheme
8192 bits	1	44.0967 dB	1	1	2	50.7855 dB
9432 bits	2	38.0015 dB	2	1	2	49.7845 dB
10662 bits	3	31.1596 dB	3	1	2	46.8719 dB
118904 bits	4	25.9715 dB	4	1	2	41.8819 dB





No. of LSBs	1	2	3	4
Stego images				
PSNR	44.0967 dB	38.0015 dB	31.1596 dB	25.9715 dB

Figure 3.2: PSNR between cover image and stego image **44.0967 dB**,**38.0015 dB**,**31.1596 dB**, **25.9715 dB**, respectively corresponding to LSBs changes from 1 to 4.

### 3.5 Comparison with hybrid edge detection mechanism using fuzzy edge detector

Canny edge detector is the most popular and widely employed edge detection operator in image processing. Excellent detection, well localization, and single response to an edge, are three important criteria of canny edge detection mechanism for which it is globally used.

Apart from it, Log edge detection mechanism which is second order derivative method of detecting edge in an image is considered here. In this proposed work, hybridization takes place with help of canny edge along with Log edge detection mechanism. In [7], fuzzy edge detection is used along with canny edge as hybrid edge detection method. This scheme results better performance but the rigidity is the use of fuzzy edge method. Its a complex edge detection mechanism with complex coding procedure, where as Log edge detection method having simple coding procedure and also a default edge detection mechanism in image processing toolbox.

Here is the result table of [7], which uses the same input parameters and performance parameter that is used in this proposed work. The PSNR value in both the case are nearly same, with slight better performance in case of fuzzy edge but of its complexity, the proposed scheme with Log edge detection mechanism as one of the hybrid edge detection mechanism is better approach in

image steganography.

Table 3.2: The performance comparison of stego-image produced by the hybrid edge mechanism using fuzzy edge and proposed scheme.

Payload(p)	no.of bits of edge pixel(y)	no.of bits of non edge pixel(x)	no.of block(n)	PSNR	PSNR of proposed scheme
8192 bits	1	1	2	51.1 dB	50.7855 dB
9432 bits	2	1	2	50.0 dB	49.7845 dB
10662 bits	3	1	2	47.1 dB	46.8719 dB
118904 bits	4	1	2	42.3 dB	41.8819 dB

Apart from the above comparison, here four different cases are considered by using different parameter values for better understanding of the the proposed scheme.

Case-I Figure 3.3 and Table 3.5 depicts the quality and performance of the stego image produced by the new scheme: Here modification on the non edge pixel is one bit( $x=1$ ) and number of bits change in edge pixel(y) are varies from 1 to 4 by LSB, with number of block of cover pixel as constant value 2. In this case, change in PSNR value changes slowly and distortion is less because here more number of bits stored in edge pixel.

Table 3.3: The performance of stego image when  $x = 1$ ,  $n = 2$  and  $y = 1,2,3,4$

Payload(p)	no.of bits of edge pixel(y)	no.of bits of non edge pixel(x)	no.of block(n)	PSNR
8192 bits	1	1	2	50.7855 dB
9432 bits	2	1	2	49.7845 dB
10662 bits	3	1	2	46.8719 dB
118904 bits	4	1	2	41.8819 dB

(a)  $y=1$ (b)  $y=2$ (c)  $y=3$ (d)  $y=4$ 

Figure 3.3: The quality of stego image when  $x = 1$ ,  $n = 2$  and  $y = 1, 2, 3, 4$ .

Case-II Figure 3.4 and Table 3.5 shows the quality and performance of the stego image produced by this proposed scheme: with varying payload of 8160 bits, 8232 bits, 8680 bits and 8968 bits but number of bits change in non-edge pixel( $x$ ), number of bits change in edge pixel( $y$ ) and number of blocks of cover image( $n$ ) remain constant.

Table 3.4: The performance of stego image when payload changes only and  $x=1,y=2,n=2$

Payload(p)	no.of bits of edge pixel(y)	no.of bits of non edge pixel(x)	no.of block(n)	PSNR
8160 bits	2	1	2	63.1202 dB
8232 bits	2	1	2	63.0858 dB
8680 bits	2	1	2	62.0453 dB
8968 bits	2	1	2	61.7865 dB



(a)  $p= 8160$  bits



(b)  $p= 8232$  bits



(c)  $p= 8680$  bits



(d)  $p= 8968$  bits

Figure 3.4: The quality of stego image when payload changes only and  $x=1,y=2,n=2$ .

Case-III Figure 3.5 and Table 3.5 shows the quality and performance of the stego image produced by this scheme, when only number of bits in non-edge pixel(x) are changing and all other parameters remain constant. So here

quality of stego image will be distorted more as more bits are substituted in non-edge pixel instead of edge pixel.

Table 3.5: The performance of stego image when only number of bits in non-edge pixel(x) are changing and all other parameters remain constant

Payload(p)	no.of bits of edge pixel(y)	no.of bits of non edge pixel(x)	no.of block(n)	PSNR
8680 bits	2	1	2	62.8453 dB
8680 bits	2	2	2	61.3760 dB
8680 bits	2	3	2	57.3677 dB
8680 bits	2	4	2	55.8977 dB



(a) x= 1



(b) x= 2



(c) x= 3



(d) x= 4

Figure 3.5: The quality of stego image when x=1,2,3,4, y=2, n=2 and constant payload

Case-IV Figure 3.6 and Table 3.5 shows the quality and performance of the stego image produced by the this scheme, when all the parameters are changing extremely. Here too much payload is taken as compared to previous cases along with varying number of bits of non-edge pixel(x), edge pixel(y) and number of blocks of cover image(n).

Table 3.6: The performance of stego image when all parameters changes extremely

<b>Payload(p)</b>	<b>no.of bits of edge pixel(y)</b>	<b>no.of bits of non edge pixel(x)</b>	<b>no.of block(n)</b>	<b>PSNR</b>
9976 bits	2	2	2	60.7434 dB
11584 bits	3	3	2	54.5652 dB
13320 bits	4	4	4	50.5153 dB
14352 bits	5	5	4	45.6157 dB



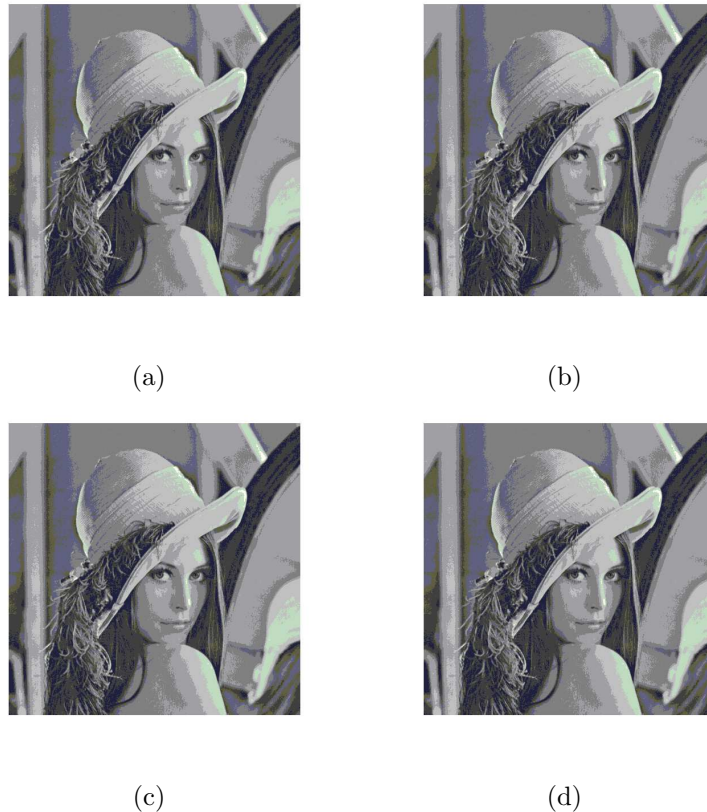


Figure 3.6: The quality of stego image when all parameters changes extremely.(a)  $p= 9976$  bits,  $y= 2$ ,  $x= 2$ ,  $n=2$  (b)  $p= 11584$  bits,  $y= 3$ ,  $x= 3$ ,  $n=2$  (c)  $p= 13320$  bits,  $y= 4$ ,  $x= 4$ ,  $n=4$  (d)  $p= 14352$  bits,  $y= 5$ ,  $x= 5$ ,  $n=4$

### 3.6 Summary

In this chapter the procedure of embedding and extraction are explained in detail with suitable example. The experimental results for the proposed scheme is also given in this chapter showing the quality and performance of stego image. It include also comparison with the previous scheme like classic LSB steganography and image steganography using hybrid edge mechanism, where hybrid is made by fuzzy and canny edge.

# Chapter 4

## Conclusions and Future Work

In this thesis, the proposed technique for novel steganography scheme which is based on the LSB steganography mechanism along with a hybrid edge detector mechanism, is a joint venture between the log edge detector and canny edge detector. The new proposed method also producing a good quality stego-image as it takes the help of hybrid edge detector. When, comparing with other steganography schemes which generate the same PSNR value for stego-image, the new proposed method generate better quality stego-images under the perception of human visual system, because of the involvement of the hybrid edge detector mechanism. Not only that, but the simulation results says that, the new methodology is fruitful in accomplishing a heavy amount of embedding payload, and also receiving acceptable quality of stego-images. Furthermore, it has better resistance to steganalysis which are grounded on statistical attacks.

### Scope for Further Research

This thesis has opened several research directions which have scope of further investigation. This proposed work can be extended to color images. The computational performance parameter (psnr) can be improve by increasing payloads. This technique can be extended to steganography of videos and can be used for color videos as it is most used medium now-a-days.

# Bibliography

- [1] <http://www.itworld.com/answers/topic/hardware/question/do-all-printers-put-identifiable-marks-every-document>.
- [2] ANAND, D. and NIRANJAN, U., “Watermarking medical images with patient information,” in *Engineering in Medicine and Biology Society, 1998. Proceedings of the 20th Annual International Conference of the IEEE*, vol. 2, pp. 703–706, IEEE, 1998.
- [3] BENLCOURI, Y., ISMAILI, M., AZIZI, A., and BENABDELLAH, M., “Securing images by secret key steganography,” *Applied Mathematical Sciences*, vol. 6, no. 111, pp. 5513–5523, 2012.
- [4] BIN SAHIB, S. and ZAMANI, M., “An introduction to image steganography techniques,”
- [5] CHANU, Y., TUITHUNG, T., and MANGLEM SINGH, K., “A short survey on image steganography and steganalysis techniques,” in *Emerging Trends and Applications in Computer Science (NCETACS), 2012 3rd National Conference on*, pp. 52–55, IEEE, 2012.
- [6] CHEDDAD, A., CONDELL, J., CURRAN, K., and MC KEVITT, P., “Digital image steganography: Survey and analysis of current methods,” *Signal Processing*, vol. 90, no. 3, pp. 727–752, 2010.
- [7] CHEN, W.-J., CHANG, C.-C., and LE, T., “High payload steganography mechanism using hybrid edge detector,” *Expert Systems with Applications*, vol. 37, no. 4, pp. 3292–3301, 2010.

- [8] DAS, R. and TUITUNG, T., “A novel steganography method for image based on huffman encoding,” in *Emerging Trends and Applications in Computer Science (NCETACS), 2012 3rd National Conference on*, pp. 14–18, IEEE, 2012.
- [9] GONZALEZ, R. C., WOODS, R. E., and EDDINS, S. L., *Digital image processing using MATLAB*. Pearson Education India, 2004.
- [10] JUDGE, J. C., “Steganography: Past, present, future,” tech. rep., Lawrence Livermore National Lab., CA (US), 2001.
- [11] LI, Y., LI, C.-T., and WEI, C.-H., “Protection of mammograms using blind steganography and watermarking,” in *Information Assurance and Security, 2007. IAS 2007. Third International Symposium on*, pp. 496–500, IEEE, 2007.
- [12] MARVEL, L. M., BONCELET JR, C. G., and RETTER, C. T., “Spread spectrum image steganography,” *Image Processing, IEEE Transactions on*, vol. 8, no. 8, pp. 1075–1083, 1999.
- [13] MIAOU, S.-G., HSU, C.-M., TSAI, Y.-S., and CHAO, H.-M., “A secure data hiding technique with heterogeneous data-combining capability for electronic patient records,” in *Engineering in Medicine and Biology Society, 2000. Proceedings of the 22nd Annual International Conference of the IEEE*, vol. 1, pp. 280–283, IEEE, 2000.
- [14] NEETA, D., SNEHAL, K., and JACOBS, D., “Implementation of lsb steganography and its evaluation for various bits,” in *Digital Information Management, 2006 1st International Conference on*, pp. 173–178, IEEE, 2006.
- [15] ROY, R., CHANGDER, S., SARKAR, A., and DEBNATH, N. C., “Evaluating image steganography techniques: Future research challenges,” in *Computing, Management and Telecommunications (ComManTel), 2013 International Conference on*, pp. 309–314, IEEE, 2013.

- [16] SONG, S., ZHANG, J., LIAO, X., DU, J., and WEN, Q., “A novel secure communication protocol combining steganography and cryptography,” *Procedia Engineering*, vol. 15, pp. 2767–2772, 2011.
- [17] ZEKI, A. M., MANAF, A. A., IBRAHIM, A. A., and ZAMANI, M., “A robust watermark embedding in smooth areas,” *Research Journal of Information Technology*, vol. 3, no. 2, pp. 123–131, 2011.