

**Performance Evaluation of Segmentation based
Steganography Technique**

*Dissertation submitted to Jawaharlal Nehru University
in partial fulfillment of the requirements
for the award of the degree of*

MASTER OF TECHNOLOGY

In

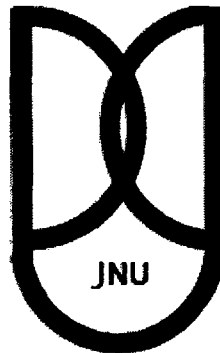
COMPUTER SCIENCE AND TECHNOLOGY

By

Uma Shanker

Under the Supervision of

Dr. R. K. Agrawal



SCHOOL OF COMPUTER AND SYSTEMS SCIENCES

JAWAHARLAL NEHRU UNIVERSITY

NEW DELHI – 110067

JULY-2010

DECLARATION

I hereby declare that this dissertation entitled “**Performance Evaluation of Segmentation based Steganography Technique**”, being submitted by me to School of Computer and Systems Sciences, Jawaharlal Nehru University, New Delhi in partial fulfillment of the requirement for the award of the degree of **Master of Technology** in Computer Science & Technology is an authentic record of my own work, carried in the fourth Semester, during the period **January-July 2009** under the supervision of Associate Professor **Dr. R.K. Agrawal**.

I also mention that the subject matter of this dissertation report has not been submitted by me elsewhere, in part or full for the award of any other degree etc.



Uma Shanker

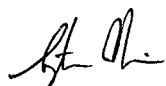
M.Tech. CS and Technology (4th Semester)

School of Computer and Systems Sciences

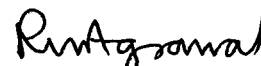
JNU, New Delhi - 110067

CERTIFICATE

This is to certify that the dissertation entitled “**Performance Evaluation of Segmentation based Steganography Technique**” is a bona fide record of the work done at School of Computer and Systems Sciences, Jawaharlal Nehru University, New Delhi in partial fulfillment of the requirement for the award of the degree of **Master of Technology** by **Mr. Uma Shanker**. This work is carried under my supervision and has not been submitted elsewhere, wholly or in part, for the award of any other degree etc.



Professor and Dean
SC & SS, JNU,
New Delhi-110067



Dr. R. K. Agrawal
Associate Professor
SC & SS, JNU,
New Delhi-110067



Uma Shanker
M. Tech (4th Semester)
SC & SS, JNU,
New Delhi-110067

ACKNOWLEDGEMENT

The successful completion of my dissertation work could hardly be possible without the helps and supports from a lot of individuals. I will take this opportunity to thank all of them who helped me either directly or indirectly during this important work.

First of all I wish to express my sincere gratitude and due respect to my supervisor **Dr. R.K. Agrawal**, Associate Professor SC & SS, JNU. I am immensely grateful to him for his valuable guidance, continuous encouragements and positive supports which helped me a lot during the period of my work. I would like to appreciate him for always showing keen interest in my queries and providing important suggestions.

I also express whole hearted thanks to my lab mates, friends and classmates for their care and moral supports. The moments, I enjoyed with them during my M.Tech course will always remain as a happy memory throughout my life.

I owe a lot to my mother for her constant love and support. She always encouraged me to have positive and independent thinking, which really matter in my life. I would like to thank her very much and share this moment of happiness with her.

Last but not the least I am also thankful to entire faculty and staff of SC & SS for their unselfish help, I got whenever needed during the course of my work.

Uma Shanker

ABSTRACT

The steganography has utmost importance in the fields of covert communication, copyright control, medical imaging, etc. Hence, researcher community has made their diligent efforts to nurture this subject during several decades. Scholars incorporated other several fields in this work such as digital signal processing techniques, statistics and spread spectrum technology of communication to cope with the foremost challenges of the steganography. Several significant steganography techniques have been suggested to make the system more robust but still we have long way to go. The purpose of this dissertation work is to present a concise description of some popular steganography techniques used in practice. In this work, the important types of steganography techniques such as spatial domain steganography, transform domain steganography, spread spectrum based steganography, statistical model of steganography and distortion based steganography have been described together with their merits and demerits.

We have proposed segmentation based steganography technique and compared its performance with Least Significant Bit (LSB) Substitution method, Discrete Cosine Transformation (DCT) based method and wavelet based method. The performance is evaluated in terms of Peak Signal to Noise Ratio (PSNR) and entropy measures. We observed that the performance of LSB method is better in form of PSNR in comparison to other methods. However, there is no clear winner among these methods in terms of entropy measure.

CONTENTS

Declaration	ii
Certificate	iii
Acknowledgement	iv
Abstract	v
Contents	vi
Chapter 1: Introduction	1-4
Chapter 2: Data Hiding Techniques	5-12
2.1 Cryptography	6
2.2 Information Hiding	6
2.2.1 Watermarking	7
2.2.2 Steganography	7
2.3 Evaluation Criteria of Steganography Techniques	10
2.4 Importance of Steganography	11
Chapter 3: Different Techniques of Steganography	13-36
3.1 Spatial Domain Steganography Techniques	13
3.1.1 Least Significant Bit (LSB) Substitution Method	13
3.1.2 LSB Substitution with Pseudorandom Permutation	15
3.1.3 Image Downgrading and Covert Channels	15
3.1.4 Cover Regions and Parity Bits	15
3.1.5 Merits and Demerits of Spatial domain Steganography	16
3.2 Transformation Domain Steganography Techniques	16
3.2.1 Discrete Fourier Transform	17
3.2.2 Discrete Cosine Transform	19

3.2.3 Wavelet Transform	20
3.2.4 Merits and Demerits of Transform Domain Steganography	25
3.3 Spread Spectrum Steganography Techniques	25
3.3.1 Spread Spectrum	25
3.3.2 A Spread Spectrum Model of Steganography	26
3.3.3 Merits and Demerits of Spread Spectrum based Steganography	29
3.4 Statistical Method of Steganography Technique	29
3.4.1 Entropy, Relative Entropy and Hypothesis Testing	30
3.4.2 Statistical Steganography Model	31
3.4.3 Merits and Demerits of Statistical Method of steganography	32
3.5 Distortion based Steganography Technique	32
3.5.1 Distortion based Technique for Image	34
3.5.2 Merits and Demerits of Distortion based Steganography Technique	34
3.6 Segmentation based Steganography Technique	34
Chapter 4: Experimental Results	37-47
4.1 Brief Overview	37
4.2 LSB Substitution Method	38
4.3 Transform Domain Steganography	40
4.4 Segmentation based Steganography Technique	43
Conclusions	48
References	49

CHAPTER 1

INTRODUCTION

Steganography [1, 14, 24, 28] has been a very fascinating research area for researchers for last many years. However, in this modern information technological era this field attracted the attention of researchers in early 1980s. The very first work was proposed by Simons [9, 22] in 1983 and gave the impetus to modern digital steganography. The steganography has been used in communicating the covert message since last many years. However, in this modern era apart from covert communication, steganography have many other important fields of applications such as copyright control, medical imaging etc [1]. In this field a lot of diligent efforts have been done by researchers over couple of decades to enhance the quality and performance of steganography models. As a result, many important and robust steganography models have been evolved.

Steganography is art of hiding message into one of the media i.e. image, audio, video and texts [1, 14]. One of the primary and fundamental methods of steganography is spatial domain steganography [23]. In this steganography technique, the steganography operations such as embedding or encoding of message and extraction or decoding of message from stego-cover are performed in spatial domain. The very generic model for steganography in spatial domain is Least Significant Bit (LSB) substitution method [23] in which one of the pixel is selected from cover and its LSB is replaced with message bit. The other several variations such as random selection of pixels of cover and selection of pixels from blocks are also proposed. In these types of techniques cover object gets modified directly during the message embedding step in the cover object. Due to this the statistical property of the cover object gets changed and these types of steganography techniques become vulnerable to statistical steganalysis [1, 14] tests. Apart from this, these types of models are not robust against cover modifications such as image cropping, rotating, compression, etc. Apart from many drawbacks these models possesses simplicity, high payload capacity and good perceptibility as strengths [23].

The Digital Signal Processing [34] played a vital role to enhance the robustness and performance of steganography techniques. The incorporation of digital signal processing in the

field of steganography opens several new routes to improve the performance and robustness of existing techniques. The issues in spatial domain steganography such as cover modifications and several statistical steganalysis tests are dealt in Transform Domain Steganography using signal processing techniques [23, 24, 34]. The Discrete Cosine Transform (DCT) [23, 24, 34], Discrete Frequency Transform (DFT) [23, 34], Wavelet Transform (WT) [3, 23, 34], etc. are used to convert the cover object into other domain. In these types of techniques the cover object is first converted into transform domain using any transformation techniques and then message embedded in low frequency region of cover and it spreads in entire cover object. Since, the encoded message spreads in entire cover. Hence, it makes the technique robust against several attacks such as cover modification and statistical tests.

Spread Spectrum (SS) [16, 29] technology has revolutionised the world of communication. Spread spectrum has the property of communication which fulfills the requirements of steganography techniques. The Spread Spectrum [16, 29] technique of communication spreads the message signal in cover object's high frequency bands. Since, the message spreads in high frequency bands of cover object so the message cannot be removed from different high frequency bands of cover objects without completely destroying the stego-object and it became comparatively hard to detect using statistical steganalysis. In this way SS enhances the quality and performance of steganography techniques. Using spread spectrum technique, Smith and Comiskey [16, 19] presented a model of steganography which shows the improvements in performance and robustness of the technique. Further Marvel [19] presented a steganography system called Spread Spectrum Image Steganography (SSIS) which is a well known work in steganography field.

Statistics is a very lucrative subject because it has enormous fields of application such as economics, engineering, communication, etc; the steganography is also one of them. The steganography techniques have been developed on the basis of the fundamental of statistics such as the entropy, relative entropy and hypothesis testing [4, 26]. The steganography techniques developed on the basis of statistics gives better performance and are robust against statistical tests. In the embedding process the message is embedded in such a way that the statistical properties of cover changes by insignificant amount and due to this it is robust against statistical

tests. At the time of extraction of message from stego-cover the relative entropy is used. The statistical steganography technique has many advantages as discussed above. However, it has several drawbacks also such as difficulty in applying in various cases, sometimes in distinguishing between cover object and stego-object, the distribution must be known for cover object in advance which is not easy to find and many assumptions are made to design such method [23].

Some steganography techniques encode the information in cover objects making the cover distort that are called Distortion Techniques of steganography. Distortion Techniques are mostly used for embedding the message in text files [20, 23]. Significant efforts are made to use these distortion based techniques to hide the message in formatted texts. In research work [20], a model to hide the information in formatted text is discussed in which up and down line movements and the words left and right movements techniques are discussed. In line movement technique, if the line moved up, a '1' is encoded, otherwise a '0'. At decoding process a centroid detection is used. In word movement technique, the word's left and right movement between words encodes the message bit. The total movement must be in such a way that sum of all movements must be zero so that it looks properly aligned. This technique is very vulnerable to page scaling but robust against most of the attacks. An effort to use this technique is to hide information in images. In fact it seems another version of spatial domain steganography [23] because it encodes a '0' in pixel left unchanged; to encode '1' a random amount is added to the selected pixel. At the time of extraction cover object and stego-object are compared, if pixels differ then the message bit is '1' else '0'. There are significant differences between LSB substitution and distortion based techniques such as the random value used to add a pixel can be selected in such a way that its addition to cover pixel leads to change in the statistical properties very less.

The objective of this dissertation work is to present a simple discussion about the techniques which are widely used in the field of steganography, a field of information hiding technique, viz. the spatial domain steganography technique, transform domain steganography technique, spread spectrum based steganography technique, statistical model for steganography and distortion based steganography technique. This dissertation contains four chapters which are

organized as follows: chapter 2 gives the basic concepts of information hiding techniques which leads to introduction of steganography. Chapter 3 make us acquainted with types of steganography techniques and our proposed Steganography technique based on segmentation. Chapter 4 covers the experimental results of fundamental steganography techniques and their performance are evaluated and compared with our proposed steganography technique. After completion of these all chapters, a brief conclusion of the work and the future work are discussed.

CHAPTER 2

DATA HIDING TECHNIQUES

Communication of information is one of the necessities of human beings. If there is a formal communication then no secrecy is required. There are several cases, when data is important and we want it to communicate in such a way that no person other than the intended person should not know about the contents of the data. In that case we need to communicate data secretly. To accomplish this task of secret message communications, some different kind of communication modes are required.

To develop a secure system to communicate secret message, one of the following techniques can be used [14].

- Cryptography
- Information Hiding

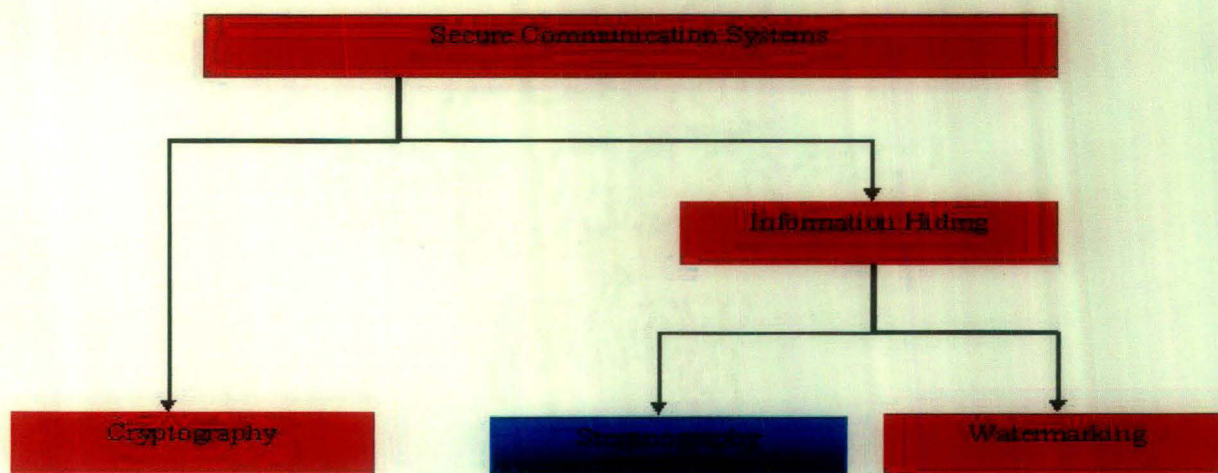


Fig. 2.1: Hierarchical classification of Secure Communication System

These techniques can be further classified and is shown in Fig. 2.1. As shown in the Fig 2.1, the secure communication systems developed can be based on either cryptography or information hiding technique. The cryptography cannot be subcategorized further but information hiding can be either watermarking or steganography. Although, the purpose of

steganography and watermarking are different, both of them involve the similar principle of hiding information.

2.1 Cryptography

The cryptography [1, 30] has been a fascinating subject in the field of secret communication. Cryptography has been in used since 2000 BC. There are many researchers who have contributed in this fascinating field. Among them works of Leonardo Da Vinci and Claude Shannon [30] are interesting. Some people believe that Claude Shannon is the father of modern mathematical cryptography. In the modern cryptography, mathematics also played a vital role. Claude Shannon worked during World War II in this field and gave it new dimensions and now it inspires new generation to work in this fascinating area of security.

In brief the cryptography can be defined as; “cryptography is the art of jumble the message to protect from others to understand but authenticated person with a key” [8, 30]. The further study of cryptography is beyond the scope of this thesis.

2.2 Information Hiding

Information hiding, as name suggests involves embedding the secret message in the object to communicate. Under this there are two subcategories; watermarking and steganography. Both, watermarking and steganography work on the same fundamental of information hiding to communicate the secret message or data. The basic steps of both techniques are shown Fig 2.2. In this Fig 2.2 a generic watermarking or steganography system is depicted. This generic model is constructed by two parts; one is embedder and second is detector. In embedder, payload i.e. a message or logo is embedded in cover object and watermarked cover or stego cover is produced. In detector, that embedded payload i.e. a logo or message is detected. Since, both watermarking and steganography works on same basic primitives, so it is very hard to draw a boundary to differentiate them.

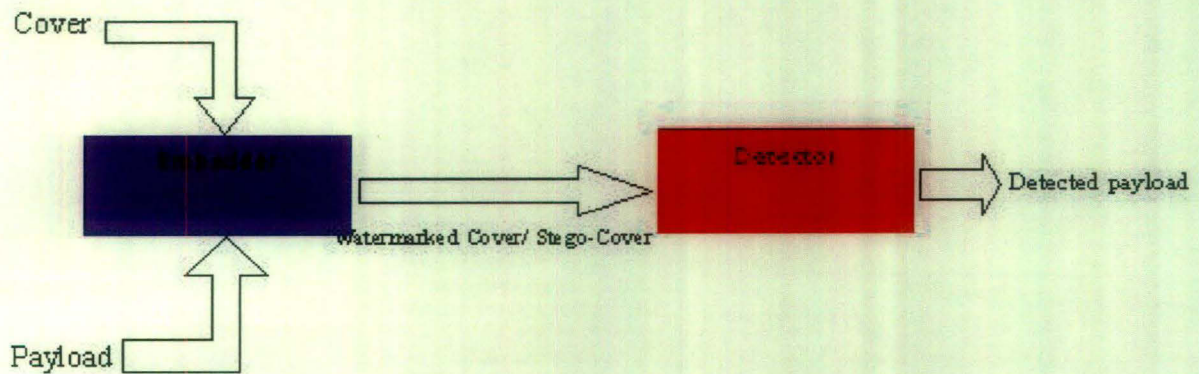


Fig. 2.2: Generic Watermarking or Steganography System

2.2.1 Watermarking

In China around one thousand years ago papermaking was invented and in 1282 in Italy paper watermark was developed. The term watermark came in the mind at the end of the eighteenth century, and at the same time watermarks were used to protect paper money [8, 14, 23].

Digital Watermarking [1, 8, 14] is an art of imperceptibly altering a cover media to embed a message or logo or watermark in the cover media [1, 14].

As discussed above the aim of this thesis is performance evaluation of steganography techniques. So, we will not discuss watermarking in detail here.

2.2.2 Steganography

Steganography has very deep roots in history. The word steganography originally derived from Greek words which mean "Covered Writing" [1, 24, 25, 28]. This technique of communicating the secret message has been used in ancient times for thousands of years in various ways. The story of 5th century BC Histaiacus and his slave's is very popular in which he used his slave to send the message secretly [1]. In Second World War Nazis invented several

steganography techniques to communicate secret messages [1]. Apart from these, there are many events in history where steganography have been used.

Steganography is all about hiding secret information or data in any media. The media used to hide message is called cover media. The secret message or data which is to be hide is called payload and cover media after embedding secret message is called stego-media.

The steganography can be defined as [1]; “steganography is an art of hiding secret data in any multimedia cover that is undetectable to the other person but authenticated one”.

After embedding the message in cover media, stego-cover must not be distorted. This is very basic condition of steganography. There are many other conditions to deal, which will be discussed later on.

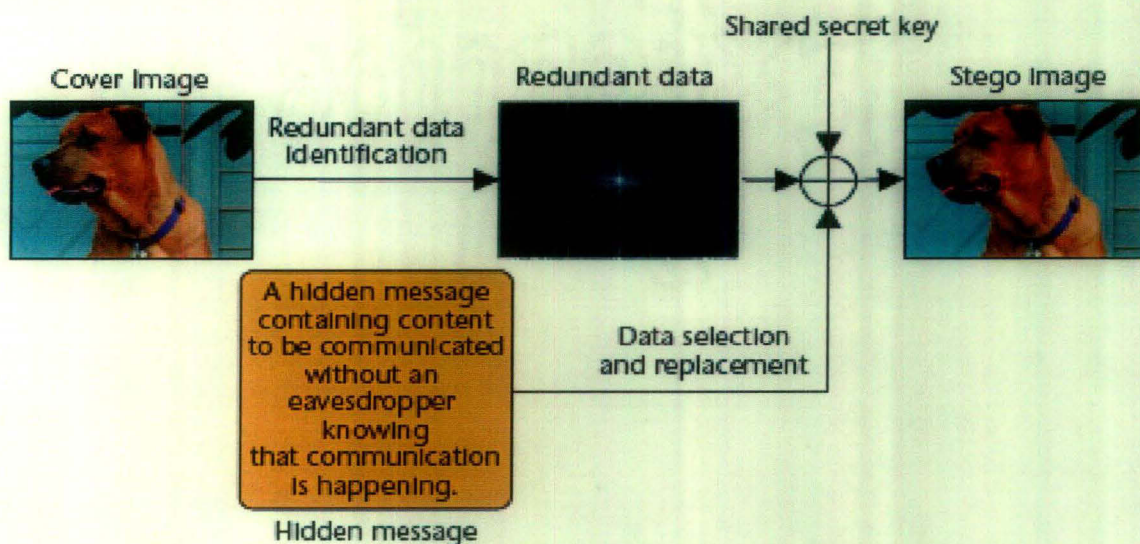


Fig. 2.3: Noble example of steganography, cover image and stego-image [25]

In the above Fig. 2.3, a steganography model is explained. In above Fig. 2.3 a cover image of dog is selected to embed message and a message is selected to be hidden. The redundant data is identified to replace with message to be hidden. The message is embedded in cover image using a shared secret key. Finally stego-image is generated after embedding the message and it is clearly visible that it is difficult to distinguish between cover image before hiding the message and stego-image after hiding the message.

In steganography technique, two steps are required, first the secret data is embedded into an appropriate cover (a media e.g. image, text file, audio, or video) according to an algorithm, called encoding or embedding process and in second step the secret message is extracted from the stego-cover according to appropriate extraction algorithm, that is called decoding or extraction process.

Let C denote the cover media e.g. image, M denote the secret data to be hidden in cover C , and C' denote the stego-image. Let K denote the optional key used to embed and extract the message. E_m is used to denote embedding and E_x is used for extraction. Then, embedding and decoding of message is given by [1]:

$$E_m : C \oplus K \oplus M \rightarrow C' \quad (1)$$

$$\text{Then } E_x(E_m(c,k,m)) \approx m, \text{ for all } c \in C, k \in K, m \in M \quad (2)$$

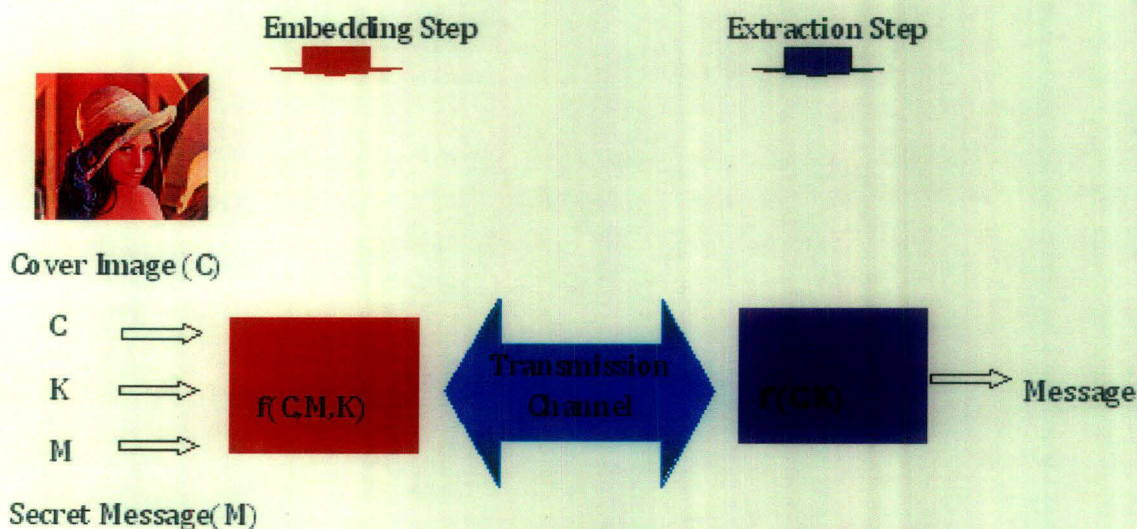


Fig. 2.4: The generic Steganography Algorithm

How the embedding and the extracting processes of generic steganography algorithm works, this is shown in Fig. 2.4. As shown in Fig. 2.4, at the sender's side, the embedding step of the algorithm works. A cover image C is selected and a message M is selected to be hidden. To embed the message M into cover image C using a secret key K , an encoding function $f(C, M, K)$

is used and stego-cover C' is generated. These encoding and decoding functions vary from algorithm to algorithm. After, embedding the message, stego-cover C' is sent through communication channel. At the receiver's end, the extraction algorithm works to extract or decode the message from stego-image C' using secret key K , using an appropriate extraction function $f(C', K)$.

2.3 Evaluation Criteria of Steganography Technique

In the field of steganography, the most appropriate steganography technique is yet to develop. The steganography techniques developed yet are somewhere not satisfying the requirement of steganography techniques. There are three main requirements of steganography technique invisibility, payload capacity and robustness against several attacks. These three requirements are contradictory to each other, so these can be represented by Magic Triangle [10, 21, 31] as shown in Fig. 2.5.

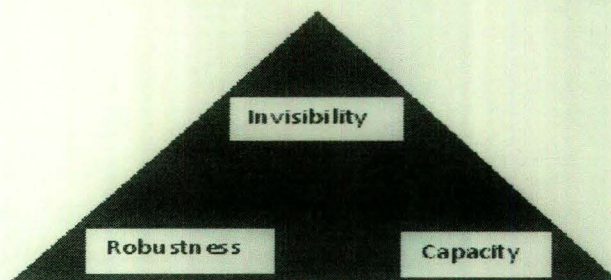


Fig. 2.5: Magic Triangle [10]

Apart from these three requirements, there are few more that can also make the steganography system fragile. After all, a steganography system is evaluated on the basis of these requirements as follows [10, 18, 21]:

- **Invisibility:** Invisibility is the foremost criteria of steganography techniques. After embedding the secret data in the cover image, the stego-image must not be distorted, this is called invisibility criteria. If the stego-image is distorted then it can attract the attention of the security analyst.

- **Payload Capacity:** The steganography technique must be able to embed huge amount of secret data in cover, keeping invisibility criteria in mind. Because, as the payload capacity increases, the distortion also occurs in the stego-image.
- **Robustness against Statistical Attacks:** Staganalysis [1, 14] is the practice of detecting embedded secret data in the cover media. Statistical attacks are techniques of detecting the embedded secret data in stego-cover using various statistical tests. Steganography technique must deal with these statistical tests so that the secret message cannot be perceived by security analyst in stego image.
- **Robustness against Cover Media Manipulation:** While communication of the stego-cover may undergo various changes, such as rotating, cropping etc, to remove or destroy the embedded secret data before reaching the destination. The Steganography technique must be able to deal with such type of manipulation attacks.
- **Independent of File Format:** In the today's digital world there are a number of formats of the cover media. So, the steganography technique must be able to embed the secret data in any format of the cover.
- **Abnormal Behavior:** The cover after embedding the secret data must not behave abnormally, such as drastic change in file size. Such type of behavior may attract the attention of security administration for detecting the embedded data.

2.4 Importance of steganography

In the ancient time the steganography has been used only in the covert communication. Now, in this digital world of modern era, steganography has found several applications apart from covert communication. Few application of steganography are the following [1, 14].

- Copyright control of materials.
- To make more robust and smart ID cards where individual's details are embedded in their photographs.

- In medical imaging systems, the data related to patient such as patient's name, his/her DNA sequence and his/her physician's name can be embedded in the images, which will maintain the confidentiality also.
- Military applications.

CHAPTER 3

DIFFERENT TECHNIQUES OF STEGANOGRAPHY

In the previous chapter, basics of steganography have been discussed. In this chapter the types of steganography techniques and our proposed steganography technique will be discussed in details. In the literature, the steganography techniques have been classified in various ways, some scholars have classified, on how the embedding of secret message is carried out while the others on the basis of how the cover media gets altered [7] to embed the secret message into cover media. On the basis of this, steganography techniques can further be categorized into the following types [5, 23]:

- Spatial Domain Steganography Techniques
- Transform Domain Steganography Techniques
- Spread Spectrum Steganography Techniques
- Statistical Methods of Steganography
- Distortion based Techniques of Steganography

Let us elaborate each steganography technique subsequently.

3.1 Spatial Domain Steganography Techniques

The spatial domain steganography techniques are one of the basic techniques of steganography. In this domain the pixel values of the cover image are directly altered to hide the secret message. This steganography technique itself can be categorized into various subcategories as follows:

3.1.1 Least Significant Bit (LSB) substitution Method [23]

In this steganography technique Least Significant Bit (LSB) of cover image pixel is substituted with the secret message bit. In this technique as in generic steganography we do two steps embedding step and extraction step. In embedding step, the message to be hidden is

converted into binary bit stream and LSB of cover image pixels are replaced with message bits. In the extraction step, the LSB's of stego-cover are lined up and secret message is reconstructed. The outline of algorithms for embedding and extracting the message of the least significant bit substitution method are given as follows [8, 23].

Algorithm: Embedding process

```

Secret message is converted into binary stream, m
for each bit in binary stream, m do
    replace LSB's of a pixel of cover image C with bit stream, m
end for

```

Algorithm: Extraction process

```

for all LSB's get replaced in cover C do
    lined up all LSB's of pixels of stego image S
end for

```

The pictorial representation of this LSB substitution technique is given below. The different pixel values are given in binary form of cover image. Message which is 110010100 is to hide in these pixel's least significant bits. To accomplish this task, LSB of cover image pixel is compared with message bit if it is same there is no need to change else replace it with message bit. In this example red color LSB's are replaced and green color LSB's are left unchanged.

Pixel values of cover image before embedding the message

```

11110100 11110101 10010101 01110101 11110100 11010101
11110101 10110101 10000100 01010101 11110101 01010100
01110100 10110100 10100101 01010101 10110100 01010101
01110111 10110101 10010101 11110101 10010101 11010101

```

Pixel values of cover image after embedding the message

```

11110101 11110101 10010100 01110100 11110101 11010100
11110101 10110100 10000100 01010101 11110101 01010100
01110100 10110100 10100101 01010101 10110100 01010101
01110111 10110101 10110101 11110101 10010101 11010101

```

3.1.2 LSB substitution with pseudorandom permutation [23]

In LSB substitution method, the bits of each pixel of cover are substituted with message bit, in continuous manner. In LSB substitution with pseudorandom permutation techniques, all the secret message bits are scattered in entire cover image by randomly selecting the cover pixel to embed the secret message bits. This scatter the message in entire cover image that makes this technique more robust against various steganalysis [14] attacks.

The measure issue in this technique is, random generation of index to select a pixel from cover, if same index generated twice then the selected pixel's LSB will get updated twice. Hence, it will lead to loss of secret message bit; this problem is called "collision". If the secret message length is much shorter than the cover image length, the probability of collision will be negligible else collision problem persist.

To overcome this problem of collisions, the used pixel's index track is maintained, and unused index is also kept. So, if the generated index is found in used maintained track, then we discard it otherwise we use it. In this way we can deal with the problem of collision.

3.1.3 Image downgrading and covert channels [23]

Image downgrading is a special case of substitution system in which image acts both as secret message and cover image. Given a cover image and secret image of equal dimensions, the sender exchanges the four least significant bits of the cover image's gray scale values with the four most significant bits of the secret image. The receiver extracts the four least significant bits out of the stego-image, thereby gaining access to the most significant bits of the secret image.

3.1.4 Cover-regions and parity bits [23]

In this technique cover image is divided in various disjoint regions $\{R_1, R_2, \dots, R_{l(c)}\}$. Now, after the cover image is divided in several disjoint regions, a single bit of information is stored in single region rather than in a single pixel. A parity bit of a regions R is calculated by

$$p(R) = \sum_{j \in R} \text{LSB}(R_j) \bmod 2 \quad (3.1)$$

In the encoding or embedding process, if the parity bit of one cover image C_i does not match with the secret bit m_i to encode, one LSB of the values in R_i is flipped. This will result in $R(I_i) = m_i$. In the decoding or extraction process, the parity bits of all selected regions are calculated and lined up to reconstruct the secret message.

Although, this method is not more robust than simple bit substitution method, but it is more powerful in some cases. First, sender can choose any region to embed message, which leads to change cover statistics least [23].

The LSB substitution steganography technique is carried out in the spatial domain. Since, in this technique, pixel values get altered, due to this the statistics of the cover media get changed. Hence, this is vulnerable to statistics tests. Apart from statistical analysis a slight manipulation in stego-image, such as image cropping, rotating, compression can also destroy the hidden message in cover image. Despite being vulnerable to these attacks, this technique's main attraction is that the method is simple, easy to implement and high payload capacity [1, 23].

3.1.5 Merits and Demerits of Spatial Domain Steganography

The steganography techniques performed in spatial domain have many advantages such as easy to implement and high payload capacity.

Apart from these merits, these techniques are not robust against various attacks such as various image modification operations e.g. image cropping, rotating and compression, because in encoding process the pixel value is altered.

3.2 Transform Domain Steganography Techniques

A transformation domain steganography technique challenges the above issues in spatial domain steganography techniques. Transformation domain steganography technique is more robust than spatial domain steganography techniques against, image compression, cropping, and some image processing and signal processing techniques. As in [2, 23] noted that, by embedding data in transform domain, the embedded data resides in more robust areas and spreads across the entire image. This provides better resistance against signal processing and statistical attacks.

To transform the image from spatial domain to different domain, the following transformation techniques are used [34].

- Discrete Fourier Transform (DFT)
- Discrete Cosine Transform (DCT)
- Wavelet Transform (WT)

3.2.1 Discrete Fourier Transform [34]

Frequency domain offers some attractive advantages in image processing. It offers large filtering operations in optimal time. It collects some information in different ways that sometimes can separate signal from noise and allow measurements that are very difficult in spatial domain.

For example, we have an image with some periodic noise that is to be eliminated. To do this, convert the image shown in Fig 3.1(a) in frequency domain and we found few white spots in that image as shown in Fig 3.1(c). After removing these white spots the image looks as shown in Fig 3.1(b) and by applying inverse Fourier transform a better image is achieved as shown in Fig 3.1(d).

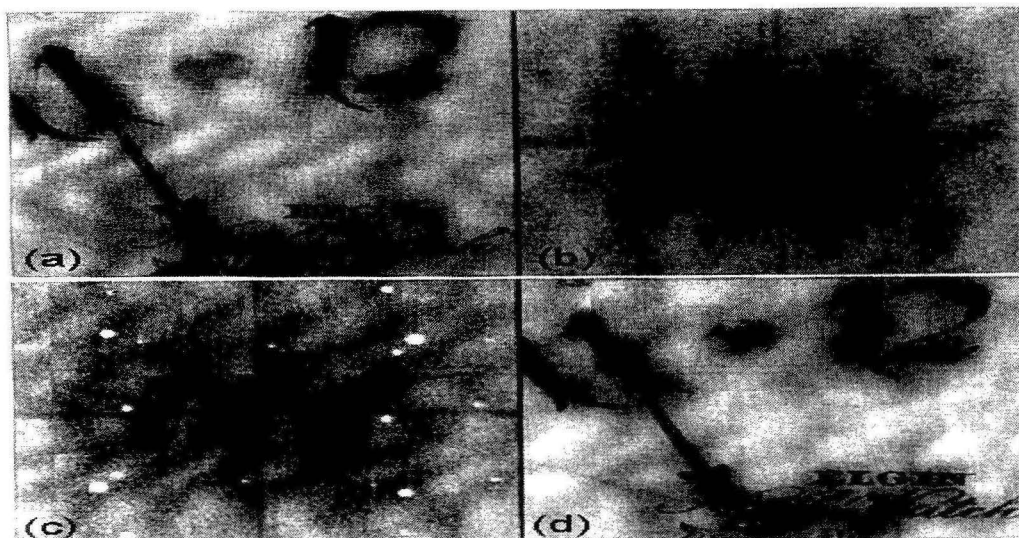


Fig. 3.1: The original image in (a) and better image recovered is shown in (d) after removing the noise data [34]

Let, $f(x)$ be a continuous function of a real variable x , then the Fourier transform of $f(x)$ is given by [34].

$$F(u) = \int_{-\infty}^{\infty} f(x) e^{-i2\pi ux} dx \quad (3.2)$$

The inverse Fourier transform is given by

$$f(x) = \int_{-\infty}^{\infty} F(u) e^{i2\pi ux} du \quad (3.3)$$

In the above pairs of Fourier transform equations, the $F(u)$ and $f(x)$ both must be continuous and integrable.

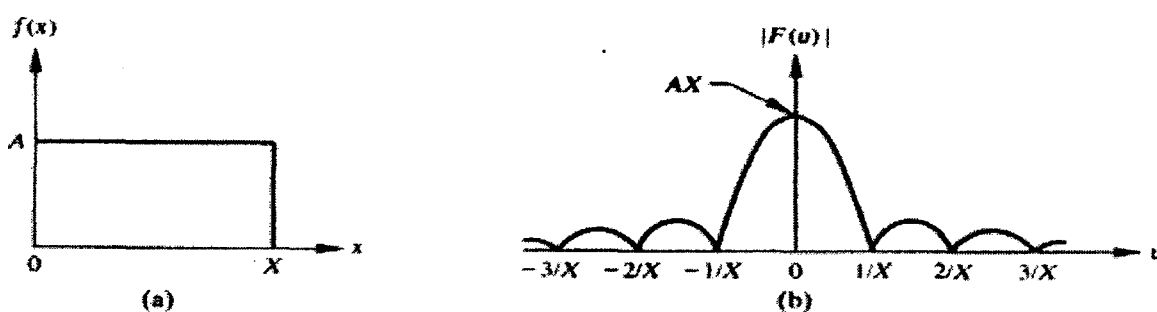


Fig. 3.2: (a) The simple and in (b) its Fourier transform [34].

The Fourier transform equation can also be written as:

$$F(u) = R(u) + iI(u), \quad (3.4)$$

Here $R(u)$ and $I(u)$ are real and imaginary parts of Fourier transform.

If $f(x)$ is a sample of N discrete values then the Discrete Fourier Transform is given by [34]:

$$F(u) = \frac{1}{N} \sum_{x=0}^{N-1} f(x) e^{i2\pi ux/N} \quad (3.5)$$

Where $u=0, 1, 2, \dots, N-1$,

The Inverse of Discrete Fourier Transform is given by:

$$f(x) = \frac{1}{N} \sum_{u=0}^{N-1} F(u) e^{j2\pi ux/N} \quad (3.6)$$

Where $x=0, 1, 2, \dots, N-1$.

A discrete Fourier Transform has computational problem, because to calculate eq(3.5) and eq(3.6) the computation cost is proportional to N^2 . The decomposition of eq(3.6), the computation cost cut down to $N \log_2 N$ that sounds very good comparatively N^2 . The decomposition procedure that cut down the computation task is called Fast Fourier Transform [34].

3.2.2 Discrete Cosine Transform [34]

Discrete cosine transformation is very important tool in image processing to change image from spatial domain to frequency domain. The DCT transforms a signal of spatial image representation to frequency representation. by grouping the pixels into 8x8 pixel blocks and transforming the pixel blocks into 64 DCT coefficients each. The modification of single coefficient will affect all 64 image pixels in that block. The definition of the two- dimensional DCT of any image is given by [2]:

$$F(u, v) = C(u)C(v) \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y) \cos\left(\frac{\Pi(2x+1)u}{2M}\right) \cos\left(\frac{\Pi(2y+1)v}{2N}\right), 0 \leq u \leq M-1, 0 \leq v \leq N-1 \quad (3.7)$$

$$C(u) = \begin{cases} 1/\sqrt{M}, & u=0 \\ \sqrt{2/M}, & 1 \leq u \leq M-1 \end{cases} \quad C(v) = \begin{cases} 1/\sqrt{N}, & v=0 \\ \sqrt{2/N}, & 1 \leq v \leq N-1 \end{cases} \quad (3.8)$$

Where $f(x,y)$ is pixel intensity of a given pixel at coordinate (x,y) and M, N are the row and column size of image, respectively. And the inverse of discrete cosine transform is given by;

$$f(x, y) = \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} C(u)C(v) F(u, v) \cos\left(\frac{\Pi(2x+1)u}{2M}\right) \cos\left(\frac{\Pi(2y+1)v}{2N}\right) \quad (3.9)$$

3.2.3 Wavelet Transform [3, 11, 12, 13, 34]

A wavelet is a mathematical function used to divide a given function or continuous time signal into different frequency components and study each component with a resolution that matches its scale. A wavelet transform is the representation of a function by wavelets. The wavelets are scaled and translated copies known as “daughter wavelets” of a finite length or fast decaying oscillating waveform called as “mother wavelet”.

Wavelet transforms have advantages over frequency transforms for representing function that have discontinuous and sharp peaks, and for accurately deconstructing and reconstructing finite, non-periodic and non-stationary signals.

Continuous Wavelet Transform [3, 34]

The continuous wavelet transform can serve as a wavelet. This wavelet transform of a function $f(t)$ involves a mother wavelet $\psi(t)$. The mother wavelet can be any real or complex continuous function that satisfies the following properties [34]:

- The total area curve under the curve of the function is zero, i.e.

$$\int_{-\infty}^{\infty} \psi(t) dt = 0 \quad (3.10)$$

- The total area of $|\psi(t)|^2$ is finite, i.e.

$$\int_{-\infty}^{\infty} |\psi(t)|^2 dt \leq \infty \quad (3.11)$$

First property suggests that it oscillates above and below, which signifies that wavy nature, and second condition shows that the finite energy of the function, which shows that the function is localized in some finite interval and is zero, or almost zero outside this interval. These properties justify the name wavelet. An infinite number of functions satisfy these conditions and some of them have researched and are commonly used for wavelet transforms [12].

Haar Wavelet Transform [3, 11, 12]

A haar wavelet is the simplest type of wavelet. In simplest form, haar wavelets are related to a mathematical operation called the haar transform. This haar transform serves as a prototype for all other wavelet transforms [11].

A discrete signal is a function of time with values occurring at discrete instants. It is represented by

$$\mathbf{f} = (f_1, f_2, f_3, \dots, f_N). \quad (3.12)$$

Where N is an even positive integer which refers the length of \mathbf{f} . The values of \mathbf{f} are the N real numbers f_1, f_2, \dots, f_N . These values typically measured the values of an analog signal function g , measured at the time values $t = t_1, t_2, \dots, t_N$. i.e.

$$f_1 = g(t_1), \dots, f_N = g(t_N). \quad (3.13)$$

The Haar transform uses a scale function $\phi(t)$ and a wavelet $\psi(t)$. The large number of functions $f(t)$ is given by [3, 34]:

$$f(t) = \sum_{k=-\infty}^{\infty} c_k \phi(t-k) + \sum_{k=-\infty}^{\infty} \sum_{j=0}^{\infty} d_{j,k} \psi(2^j t - k) \quad (3.14)$$

Where c_k and $d_{j,k}$ are coefficients to be calculated.

The basic scale function $\phi(t)$ is the unit pulse

$$\phi(t) = \begin{cases} 1, & 0 \leq t < 1 \\ 0 & \text{otherwise} \end{cases} \quad (3.15)$$

The function $\phi(t-k)$ is a copy of $\phi(t)$, which is shifted k units to the right. Similarly, $\psi(2^j t - k)$ is a copy of $\psi(2^j t - k)$ scaled to half the width of $\psi(t-k)$. The shifted copies are used to approximate $f(t)$ at different times t . The scaled copies are used to approximate $f(t)$ at different times t . Hence, the basic Haar wavelet is the step function

TH-19211



$$\psi(t) = \begin{cases} 1, & 0 \leq t < 0.5, \\ -1 & 0.5 \leq t \leq 1 \end{cases} \quad (3.16)$$

In the given below Fig. 3.3, different types of wavelets are shown in pictorial representation.

Since, wavelet is not the subject of this thesis, so we leave the wavelet discussion here.

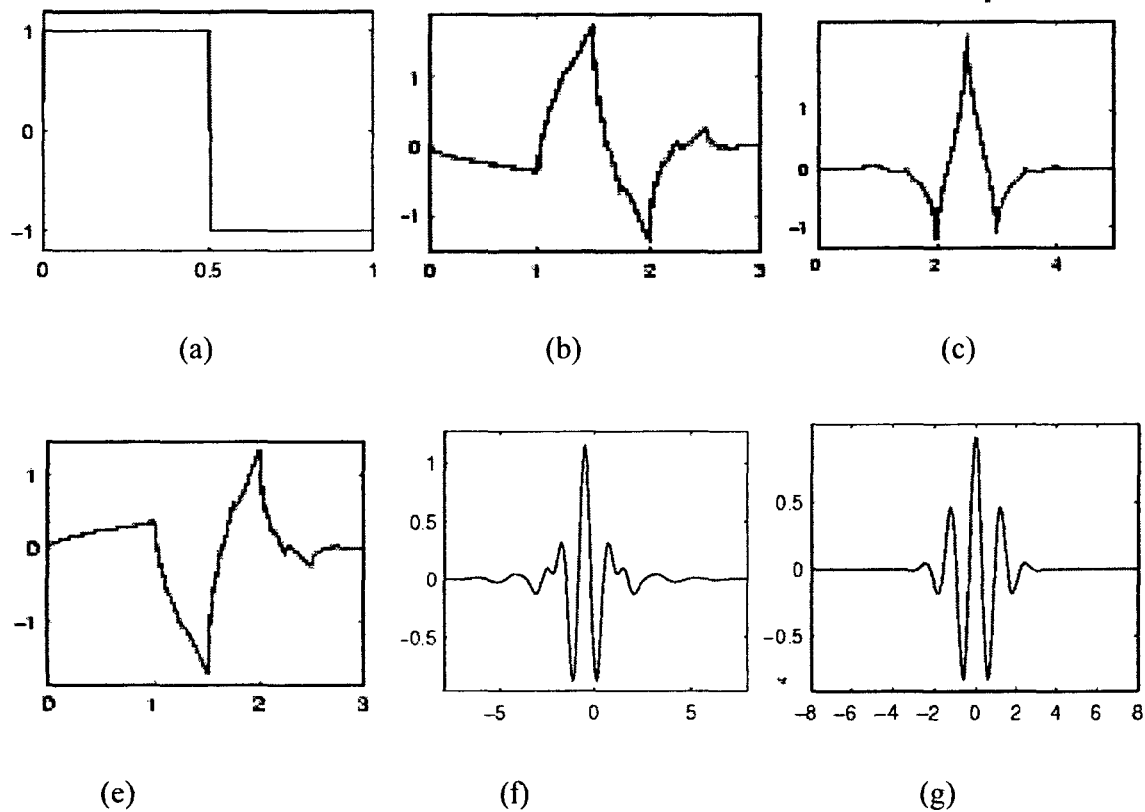


Fig. 3.3: (a) Haar, (b) Daubechies4, (c) coiflet1, (d) Symlet2, (e) Meyer, (f) Morlet [12]

The steganography algorithm given below is fundamental algorithm using DCT transform domain [8, 23].

Algorithm: Embedding Process

for all bits in binary message do

fix a indexes to select two coefficients in selected block

convert cover image C in DCT Transform

```

choose one block out of all given blocks
if message bit = 0 then
    if C1 > C2 then
        swap C1 and C2
    end if
else
    if C1 < C2 then
        swap C1 and C2
    end if
end if
adjust both values of coefficient so that | C1- C2| > x
end for
create stego-image C'

```

Algorithm: Extraction Process

```

for equal number of message bits do
    convert stego-cover in DCT transform
    choose two coefficients C1 and C2 according to fix index
    if C1 ≤ C2 then
        message = 0
    else
        message = 1;
    end if
end for

```

In above DCT transform based algorithm in embedding process, first fix the index to choose two coefficients in a cover block, cover image C is transformed using DCT and

eventually the secret message is converted into binary bit stream. Now, for each message bit, two coefficients are selected in a block. If message bit is '0' and coefficient C1 is greater than C2 then swap these coefficients else to encode '1', C1 is less than C2 then swap coefficients. Finally stego-cover is generated. In, extraction process, stego-cover is converted using DCT and a block is selected and two coefficients selected using fix index are checked if $C1 \leq C2$ message bit is '1' else '0' and whole message is extracted.

This is fundamental algorithm to embed message in DCT transform domain. It is better than the fundamental steganography LSB substitution method in perceptibility and statistical tests [21]. This DCT transform based algorithm has a drawback that the swapped elements could be the significant coefficients which can lead to the image distortion.

In [23], a DCT transform based steganography have been proposed to overcome the above drawback. On the DCT coefficients, the quantization is carried out, and then to encode message bit in block the coefficients must have the additional difference D. Normally $D = 1$ is minimum difference. For higher value of D, the steganography technique against image processing attacks will be more robust.

A steganography technique proposed in [2], used DCT transform coefficients to embed information in cover image. In this technique, first a coded map is generated from spatial domain, this coded map is further modified and then this modified coded map is inserted into DCT transform coefficients of the image. The work [2] claim that this modified steganography technique is more robust than spatial domain steganography technique.

In steganography the wavelet transform domain is also playing a vital role to developing better steganography techniques. In [22], a steganography technique is developed using wavelet transform. In this steganography technique, the message bits are embedded into LSB bits of integer wavelet coefficients of cover image. In addition, the algorithm also adjusts the saturated pixel components, to recover the embedded message without loss. The pay load capacity of this steganography technique is up to 50% of the original cover image size. But, nothing is claimed about statistical attacks. This work [17] is another wavelet based steganography technique, in which the insignificant coefficients whose value is less than one and greater than zero are

replaced with mapped values of alphabets. This technique has not been analyzed against statistical attacks.

3.2.4 Merits and Demerits of Transform Domain Steganography Techniques

As discussed so far, the drawbacks of spatial domain steganography techniques are addressed in the transform domain steganography techniques. As, in these types of steganography techniques the cover modification is carried out in different domain rather than spatial domain and message is embedded in low frequency regions and it scatters the message in entire stego-cover. It is more robust against cover modification operation and it causes least change in statistical properties of stego-cover and due to this reason it becomes robust against statistical test.

3.3 Spread Spectrum Steganography Techniques

In steganography, several transformation techniques have been used to make the steganography system more robust. In this section the Spread Spectrum (SS) [29] technique of communication is incorporated in steganography. So, before introducing steganography using spread spectrum, a brief introduction of the spread spectrum is given below.

3.3.1 Spread Spectrum (SS)

Spread Spectrum (SS) is a method of transmission in which the signal occupies larger bandwidth in comparison to minimum bandwidth required to send the information. The spreading of band is accomplished in a method which is independent of data and the data is recovered from dispersed band using synchronized method [29].

There are many objectives that are fulfilled, using spread spectrum, some of them are given below [29]:

- Anti jamming
- Anti interference
- Low probability of intercept
- They are easily hidden

- They have multiple access capability.

Since, the main use of spread spectrum is in communication, data, sent using spread spectrum is spread over a wide frequency range and it appears as noise. Hence it becomes difficult to detect and jam. This similar situation is desired in the steganography systems.

The spread spectrum is carried out in the following ways [29]:

- Direct Sequence Spread Spectrum (DSSS)
- Frequency Hopping Spread Spectrum (FHSS)
- Time Hopping Spread Spectrum (THSS)
- Hybrid, a combination of above.

In information hiding, the two special types of spread spectrum are generally used. In Direct sequence spread spectrum (DSSS) data to be transmitted is divided into small pieces and each piece is allocated to a frequency channel across spectrum or cover. On the other hand, in Frequency Hopped spread Spectrum (FHSS), frequency of the data carrier signal is modified across a specific range of frequency [29].

3.3.2 A Spread Spectrum Model of Steganography

In literature, Smith and Comiskey [16] presented a generic model for steganography using spread spectrum. This model was initially applied on gray scale images. However, this model can also be extended to all cover on which scalar product can be defined.

In the model images ϕ_i of size $N \times M$ are used, are orthogonal to each other and ϕ_i is used as a stego – key. Stego message $E(x,y)$ is generated using this basic function and message bit b_i as:

$$E(x,y) = \sum_i b_i \phi_i(x,y) \quad (3.17)$$

The images must be orthogonal to each other as,

$$\langle \phi_i, \phi_j \rangle = \sum_{x=1}^N \sum_{y=1}^M \phi_i(x,y) \phi_j(x,y) = G_i \delta_{i,j} \quad (3.18)$$

Where $G_i = \sum_{x=1}^N \sum_{y=1}^M \phi^2(x, y)$ and δ_{ij} is known as Kronecker delta function.

To create the stego-cover $S(x, y)$, the pixel wise sum of both images is taken as,

$$S(x, y) = C(x, y) + E(x, y) \quad (3.19)$$

In the ideal case, cover C is orthogonal to all ϕ_i , (so $\langle C, \phi_i \rangle = 0$). Then in that ideal case i^{th} message bit b_i is extracted by projecting the stego image S onto the i^{th} basis image function ϕ_i and is given as

$$\langle S, \phi_i \rangle = \langle C, \phi_i \rangle + \langle \sum_j b_j \phi_j, \phi_i \rangle \quad (3.20)$$

$$\langle S, \phi_i \rangle = \sum_j b_j \langle \phi_j, \phi_i \rangle \quad (3.21)$$

$$\langle S, \phi_i \rangle = G_i b_i \quad (3.22)$$

Therefore, the secret message can be recovered as

$$b_i = \langle S, \phi_i \rangle / G_i \quad (3.23)$$

It is clear from above equation that at the time of extracting the message, original cover is not required. In practical it is not possible that cover image C is completely orthogonal to all basis function ϕ_i . To deal with this case the error term $\Delta\alpha_i$ is introduced.

$$\langle C, \phi_i \rangle = \Delta\alpha_i \quad (3.24)$$

$$\langle S, \phi_i \rangle = \Delta\alpha_i + G_i b_i \quad (3.25)$$

The $\Delta\alpha_i$ error term is supposed to be zero, under the reasonable assumptions. To show this, let us assume that, cover C and basis function ϕ_i , both are independent of NM dimensional random variables and all basis images are created using a zero-mean random process and they are independent to the message to be communicated. Hence, one can have

$$E[\Delta\alpha_i] = \sum_{x=1}^N \sum_{y=1}^M E[C(x, y)] E[\phi_i(x, y)] \quad (3.26)$$

The error term in eq (3.25) is zero, according to eq (3.24).

In extraction process, the reconstruction of secret message is carried out by projecting the stego-cover S onto basis functions ϕ_i , and is given as

$$m_i = \langle S, \phi_i \rangle = \Delta\alpha_i + G_i b_i \quad (3.27)$$

subject to condition, the expected value of $\Delta\alpha_i$ is equal to zero, then

$$m_i \approx G_i b_i \quad (3.28)$$

Finally the secret message is constructed from m_i as, if secret message is string of -1 and 1 instead of simply binary strings, the secret message can be evaluated using the sign function [16, 19]

$$message(i) = sign(m_i) \begin{cases} -1 & \text{if } m_i < 0 \\ 0 & \text{if } m_i = 0 \\ 1 & \text{if } m_i > 0 \end{cases} \quad (3.29)$$

In some cases, if $m_i = 0$ means embedded information has been lost, as if the quantity of $\Delta\alpha_i$ is very large instead of zero in that case the few bits may not recover. However, these situations arise very rarely and can be handled with any error correcting code.

The main advantage of spread spectrum steganography technique is that it relatively more robust than others in image modification operations. Because, the message to be hidden in cover is spread over a wide frequency band in entire cover and it is very difficult to remove message completely but by completely destroying the cover. It is noticed that stego-cover modification increases the value of $\Delta\alpha_i$. But, these modifications cannot damage the hidden message, until $|\Delta\alpha_i| > G_i m_i$ condition is satisfied [19].

In literature, the steganography system developed in [19] is the most prominent work using spread spectrum in the field of steganography. Let us have a brief view of this system as a case study.

The technique developed by Marvel [19] is called Spread Spectrum Image Steganography (SSIS). SSIS uses spread spectrum technique in embedding and extraction process. These processes can be described as follows. Before embedding the secret message, this

message is preprocessed and encrypted using conventional symmetric encryption scheme and secret message is encrypted using a secret key k_1 . And, the encrypted message is encoded by a low-rate error-correcting code. Further, this encoded secret message is modulated by a pseudorandom sequence and is generated using a secret key k_2 as seed by pseudorandom number generator. Afterward, the resultant signal of previous step is input into an interleaver using the third key k_3 and embedded to the cover. Finally, in last, the stego-image is quantized accordingly.

At the receiver's end the extraction process of information is reversed of the embedding process. The SSIS system's goal was to produce a blind steganographic system. It means a system in which the original cover is not required at the time of extraction process of message. Initially, the estimate of the original image is determined using an image-restoration technique. The subtraction of stego-image and cover image produces an estimate for the modulated and spread stego-message. Then this modulated stego-message bits are deinterleaved and demodulated using the secret keys k_3 and k_2 which were used in embedding process. Due to the poor filter method, the reconstructed message may have few incorrect bits. However, this problem can be solved with the use of an error-correcting code. The secret message is decrypted to get the original secret message.

3.3.3 Merits and Demerits of Spread Spectrum Based Steganography Techniques

These types of steganography techniques are robust against message detection and its removal from the stego-cover. Because, the message is embedded in various frequency band of cover object and it spread across entire cover object. Due to this it becomes more robust against cover modification and statistical tests.

3.4 Statistical Method of Steganography [23]

In this section, statistical method of steganography will be discussed. Statistics is a very fascinating subject and has enormous field of applications. It is not possible to discuss the subject statistics in this thesis. However, the fundamentals which are necessary to understand the statistical methods based steganography, such as entropy, relative entropy and hypothesis testing will be discussed as follows.

3.4.1 Entropy, Relative Entropy and Hypothesis Testing [4, 5, 26, 28]

Entropy measures the amount of information, or uncertainty. The entropy of a random variable X with probability distribution P_X and alphabet X is defined as

$$H(X) = - \sum_{x \in X} P_X(x) \log P_X(x) \quad (3.30)$$

The conditional entropy of X conditioned on a random variable Y is given by

$$H(X|Y) = \sum_{y \in Y} P_Y(y) H(X|Y=y) \quad (3.31)$$

Where $H(X|Y=y)$ is the entropy of the conditional probability distribution $P_{X|Y=y}$.

Hypothesis testing [4] used to decide which one of the two hypotheses H_0 and H_1 is true. In other words, there are two probability distributions P_{Q0} and P_{Q1} in the space Q of possible measurements. According to hypothesis testing if H_0 is true then Q is generated by P_{Q0} , and if H_1 is true then Q is generated according to P_{Q1} . A decision rule decide the space Q that assign one of the hypothesis to the possible $q \in Q$. There are two possible errors. Type I error is made for accepting H_1 hypothesis even H_0 is true and type II error is made if H_0 is accepted even H_1 is true. The probability of type 1 error is denoted by α , and probability of type 2 error is denoted by β .

The method of finding the optimum decision rule is given by the Neyman Pearson theorem. This is specified in term of threshold parameter T and is given by [4, 5].

$$\log (P_{Q0}(q)/P_{Q1}(q)) \geq T. \quad (3.32)$$

To find the optimal decision rule many values of T are examined. The left hand side of above equation is called log-likelihood ratio.

To measure the hypothesis testing the required basic information is relative entropy or discrimination between two probability distributions P_{Q0} and P_{Q1} and is defined as

$$D(P_{Q0}||P_{Q1}) = \sum_{q \in Q} P_{Q0}(q) \log (P_{Q0}(q)/P_{Q1}(q)). \quad (3.33)$$

The relative entropy between two distributions is always non negative. If it is zero then it implies both probability distributions are equal.

In research work [4] the information theoretic model for steganography is introduced. The theory proposed is based on hypothesis testing. Given original cover C and stego-cover S . The investigation to find the message's presence in stego-cover and is accomplished by statistical hypothesis testing. Thus, the relative entropy $D(P_C||P_S)$ between probability distributions of original cover P_C and stego-cover's P_S is calculated and if it is 0, this implies that, the difference between both probability distribution are same and the steganography system is perfectly secure and by observing stego-cover it is not possible to guess about secret message.

3.4.2 Statistical Steganography Model [23]

Statistical steganography techniques embed 1 bit in the cover in such a way that statistical properties change significantly. That helps the receiver to extract message from the stego-cover, by distinguishing modified cover from unmodified cover.

To embed the secret data in cover image, cover image is divided into $l(m)$ disjoint blocks $B_1, \dots, B_{l(m)}$. A secret bit, m_i is inserted into a i_{th} block by placing a 1 into B_i if $m_i = 1$. Otherwise block is left unchanged. In the extraction process of the secret message from stego-image, to detect specific bit, a test function is used [4, 32] which is given as:

$$g(B_i) = \begin{cases} 1, & \text{block } B_i \text{ was modified,} \\ 0, & \text{otherwise.} \end{cases} \quad (3.34)$$

The f function is called hypothesis testing function. The receiver successively applies f to all cover block to retrieve the whole secret message.

The hypothesis testing function f has an issue i.e. how to create it. To form such type of hypothesis testing function, the theory of hypothesis testing of statistical mathematics is used. To create such type of formulae $g(B_i)$, the various statistical distributions of the cover block are found out. Then in the embedding process, the secret data is inserted to alter that distribution of cover block. So, that at the time of extraction the secret data can be extracted easily by comparing $g(B_i)$ of stego-cover and original cover.

3.4.3 Merits and Demerits of Statistical Steganography Model

Statistical steganography model are robust against statistical and cover modification attacks in compare to spatial domain technique. However, the main obstacle is to design such model which is hard.

Statistical steganographic techniques are difficult to apply in many cases for the following reasons [23];

- A good hypothesis test is required to distinguish between cover and stego-cover.
- The probability distributions for cover and stego-cover must be known in advance to calculate the relative entropy.
- Many assumptions are made to find the probability distributions for cover and stego-cover.

3.5 Distortion Based Steganography Techniques [20, 23]

Till this, the information hiding techniques only for image are discussed. In this section, how the text files are used to hide information will be discussed. Data embedded in text files is accomplished by distortion based techniques. In this technique, the modulation of words, blank spaces, tabs, lay out of page; line breaks etc. are used as a tool to embed information in text files. HTML files are good to hide data until source code is displayed. It can be seen in fig.5; the page layouts have enormous space to hide the bulk of data without noticing.

To embed information in formatted text, there are two basic approaches [20, 33]. In first approach line movement is used to encode the information by shifting the line upward or downward. In second approach the words shifting is used to encode the information.

In line shifting approach to encode information, one secret bit is encoded in one line that is moved; if line is shifted up, a '1' is embedded, else a '0'. To extract or decode secret message, any technique which measure the total shifting can be used. The centroid in that case defined as the center of mass of the line about horizontal axis [33].

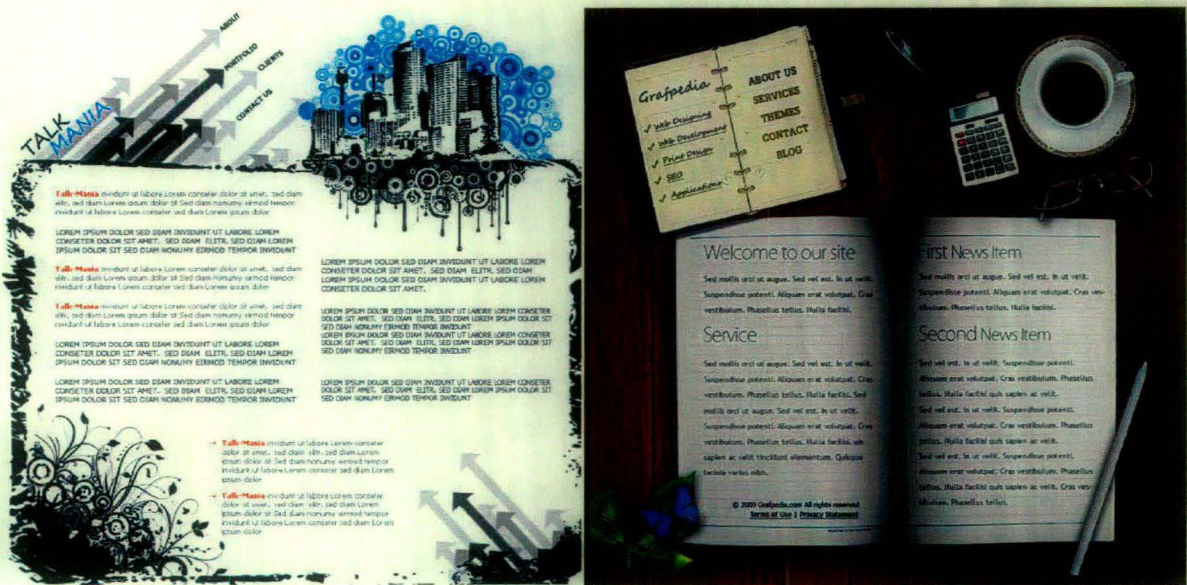


Fig. 3.4: Page Layout which have enough space to hide data [13]

Let us assume that Δ_{R+} is the distance between the centroid of a shifted line and the stationary line next to it and Δ_{R-} is the distance of centroid between shifted line and unmodified line below it. Δ_{X+} and Δ_{X-} are centroids distances in unmodified document. Line shifted can be evaluated as follows. The distance above one line increased if [23]

$$\frac{\Delta_{R+} + \Delta_{R-}}{\Delta_{R+} - \Delta_{R-}} > \frac{\Delta_{X+} + \Delta_{X-}}{\Delta_{X+} - \Delta_{X-}} \quad (3.35)$$

Similarly, if the distance above the line is decreased then [23]

$$\frac{\Delta_{R+} + \Delta_{R-}}{\Delta_{R+} - \Delta_{R-}} < \frac{\Delta_{X+} + \Delta_{X-}}{\Delta_{X+} - \Delta_{X-}} \quad (3.36)$$

However, this technique is not much robust, just scaling of the page can cancel all this shifting of lines.

In word-space encoding, shifting of the words are used to encode the message bits [20, 33]. In this technique the space between the selected words are altered according to message bit. The condition, while altering the space between words, the sum of all movements in one specific

line equals to zero so that line looks properly aligned. This is shown with the following example [20].

This is |just | a pen

This is | just| a pen

This is |just | a pen

3.5.1 Distortion Based Technique for Image

Distortion based techniques can easily be applied to the digital images. In this technique at the sender's side cover pixels are chosen as in substitution approach. To encode a '0' leave the pixel unchanged and to encode '1' adds a random value ' Δx ' to this pixel. Although, this method sounds same as LSB substitution method, but there are some significant differences. Here the LSB of selected pixel need not be same as message bits and no cover modification required to encode '0'. Apart from these, the most important thing is that the selection of Δx can be done in such a way that lead to least change in statistics of cover image. At the receiver's end, compare the selected pixels of original cover and stego-cover. In this, if the pixel differs, the message bit is '1' else '0' [23].

3.5.2 Merits and Demerits of Distortion Based Steganography Techniques

These techniques are very useful in information hiding in text files. But, have many challenges to deal with because of low payload capacity and vulnerable against text modifications.

3.6 Segmentation based Steganography Technique

After understanding the merits and demerits of various steganography techniques, we will adopt the merits of different existing techniques to develop a steganography technique that meets the requirements of contemporary challenges in steganography. Statistical characteristics of image can be taken into consideration to take into account more invisibility from human eye. To achieve this, segmentation of image can be carried out to obtain portion of image which are more

similar in terms of color, intensity or texture of image. This will enable us to embed the message which does not change the properties of the similar portion of image into different ways.

Before going to proposed technique, we need to understand the fundamental of image segmentation. The purpose of segmentation is to divide an image into different disjoint regions. This task is carried out on the basis of image's pixel intensity and texture [6, 27]. More precisely, image segmentation is the process of assigning a label to every pixel in an image such that pixels with the same label have certain specific characteristics and according to these characteristics they are categorized into different disjoint regions R_1, R_2, \dots, R_N . Each of the pixels in a region is similar with respect to these characteristics such as color, pixel intensity and texture. Mathematically if the domain of the image is given by I , then the segmentation problem can be defined as to determine the disjoint regions R such that $R = \{R_1, R_2, R_3 \dots R_N\}$, whose union is the entire image I . Thus, the sets that make up segmentation must satisfy the following conditions [6]:

$$I = \bigcup_{j=1}^N R_j \quad \text{and} \quad R_j \cap R_k = \varnothing \text{ for } j \neq k \quad (3.34)$$

Where N is number of segments.

There is several segmentation techniques have been discussed in the literature. These segmentation techniques can be classified in the following categories [6]:

- Thresholding Approach
- Region Growing Approach
- Clustering Approach
- Using Classifiers Approach

In our proposed segmentation based steganography technique, we used Normalized Cut (NCUT) [15] method which one of the robust segmentation technique among them.

In this endeavor, at the sender's end, before, hiding the message in cover image, the cover image is segmented using Normalized Cut Method (NCUT). Then message is embedded into these different segments. After doing that we will divide secret message into several parts as number of segments of cover image. Then we will hide this message in observed cover image segments of cover image. At last all segments will be combined together to obtain the stego image.

At the receiver end to extract the message, the stego image is segmented. Then message is extracted accordingly from stego segment elements. The message extracted from different segments is combined together to obtain the original message.

The outline of proposed algorithm for sender's and receiver's ends is given below:

Sender's side algorithm

- Select randomly a cover image from the set of available images.
- Select the message which is to be transmitted.
- Segmentation of image is performed.
- Segment the encoded message based on the number of segmented image.
- Embed the message in the segmented portion of the image.
- Assemble the stego objects to generate the stego image.

At the receiver end the reverse procedure is applied to extract the message without any loss. In extraction process at the receiver end the following steps are involved.

Receiver end algorithm

- Carry out the segmentation of the stego image.
- Extract the message from the stego segment image.
- Reassemble the message segments.

CHAPTER 4

EXPERIMENTAL RESULTS

4.1 Brief Overview

This is the most coveted chapter in this dissertation. After discussing the state of art of the steganography and various techniques of steganography techniques, let us move towards its implementation and comparison.

To carry the task of implementation of steganography techniques and their comparisons, four images lena, pout, rice and cameraman [MATLAB] are considered for experiment. Spatial domain based steganography techniques and transformation domain based steganography techniques are implemented and tested over these four images. To compare performance of the different steganography techniques, Peak Signal to Noise Ratio (PSNR)[10, 18, 22, 31, 35] value of stego images and entropy value measures are used.

PSNR is used to calculate the quality of stego image and is given by [10, 22, 35]

$$\text{PSNR} = 10 \cdot \log(255 \cdot 255 / \text{MSE}) \quad (4.1)$$

Where MSE is mean square error and is given by

$$\text{MSE} = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} (((\text{stego}(x,y) - \text{cover}(x,y)) * (\text{stego}(x,y) - \text{cover}(x,y)))) / N * N) \quad (4.2)$$

Where $\text{stego}(x,y)$ and $\text{cover}(x,y)$ are the pixel values of stego image and cover image at x and y coordinate. N is the number of rows and columns of the cover image.

The entropy [26, 28, 31] defined the randomness of the system [4]. It is given by

$$E = - \sum_i p_i \log p_i \quad (4.3)$$

Where p_i is the probability of i th gray value of pixel.

$$\Delta E = \text{Entropy}(\text{Stego}) - \text{Entropy}(\text{Cover}) \quad (4.4)$$

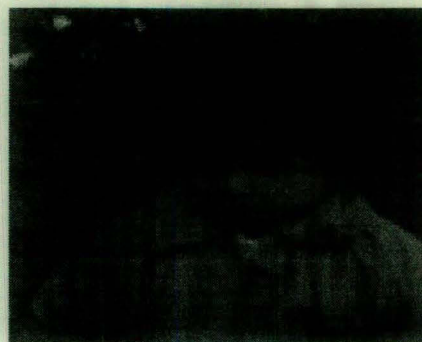
The difference between stego image entropy and cover image entropy ΔE measures the robustness against statistical attacks. If it is equal to zero then the embedded data is highly secure [4, 26, 31].

4.2 LSB Substitution Method

In the spatial domain technique of steganography, the basic method is LSB substitution method. We considered four images pout, lena, rice and cameraman of size 256×256 to hide the message. We embed the following message [Times of India, Sacred Space 22nd January, 2010] *“You were born with potential. You were born with goodness and trust. You were born with ideals and dreams. You were born with greatness. You were born with wings. You are not meant for crawling, so don’t. You have wings. Learn to use them and fly.”* in each one of the given images. The cover and stego images of all the four images are shown Fig. 4.1 (a)-(h). It can be observed that by human naked eyes, it is difficult to distinguish the two images and hard to guess the embedded message. After embedding the message, PSNR and Entropy values are calculated. The PSNR values and entropy difference for each image set for LSB substitution is shown in Table 4.1.



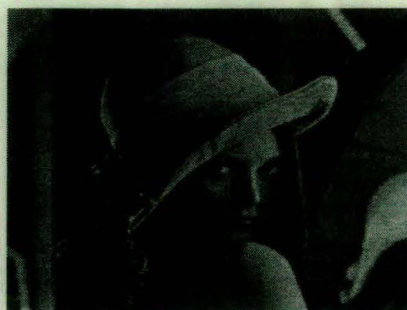
(a) Cover Image of pout



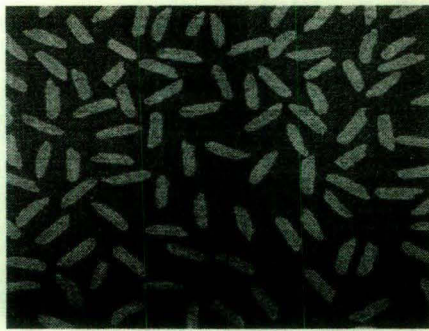
(b) Stego Image of pout



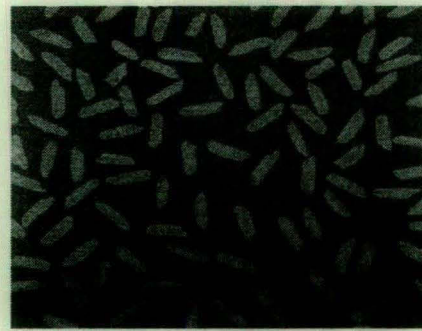
(c) Cover Image of Lena



(d) Stego Image of Lena



(e) Cover Image of rice



(f) Stego Image of rice



(g) Cover Image of Cameraman



(h) Stego Image of Cameraman

Fig. 4.1 (a) and (b) are cover and stego image of pout, (c) and (d) are cover and stego image of lena, (e) and (f) are cover and stego image of rice, (g) and (h) cover and stego image of cameraman respectively using LSB substitution method steganography

Table. 4.1 The PSNR and Entropy of stego and cover image Using LSB Substitution Method

S.No.	Cover Image	PSNR (dB)	Entropy (ΔE)
1.	pout.tif	63.1824	0.0732
2.	lena.png	63.9266	0.0013
3.	rice.png	63.9546	0.0003
4.	cameraman.tif	63.7999	0.0014

It can be observed from Table 4.1 that the variations in PSNR values are not significant but greater than average PSNR value which is 40 dB [31, 35]. In literature, it is pointed that any image with PSNR value more than 40 dB reflects better image quality. Hence, the quality of embedding is better with LSB substitution technique. ΔE indicates the security of hidden

message against statistical attacks. $\Delta E = 0$ signifies that hidden message is secure completely [4, 5]. However, it is impossible to achieve.

4.3 Transform Domain Steganography

In transform domain based steganography technique we implemented two methods (i) DCT based steganography and (ii) wavelet based steganography technique. The same set of image (pout, lena, rice and cameraman) are used. The cover images and stego images are shown in Fig. 4.2(a)-(h). It can be observed that human bare eyes cannot distinguish the cover and stego image. The PSNR and ΔE are calculated and shown in Table 4.2. In the transform domain, wavelet based steganography is also implemented and the respective PSNR values and entropy difference is shown in Table 4.3. The cover images and its corresponding stego images are shown in Fig 4.3 (a)-(h).

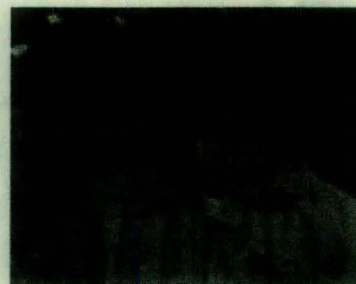
It can be observed from Tables 4.2 and 4.3 that the performance of wavelet based steganography technique is better in terms of PSNR and entropy for all images other than pout image.

Table. 4.2 The PSNR and Entropy of stego and cover image Using DCT based steganography

S.No.	Cover Image	PSNR (dB)	Entropy (ΔE)
1.	pout.tif	61.1642	0.0975
2.	lena.png	43.0872	0.0031
3.	rice.png	43.1621	0.0149
4.	cameraman.tif	41.0899	0.0459



(a) Cover Image pout



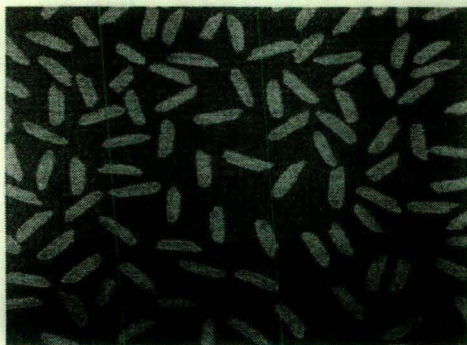
(b) Stego Image pout



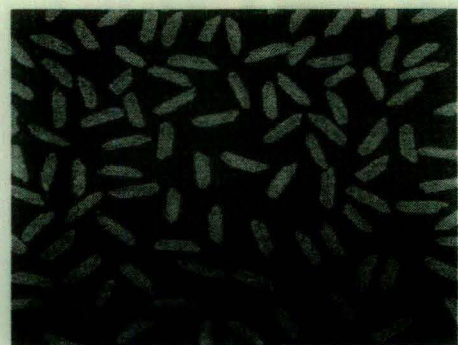
(c) Cover Image lena



(d) Stego Image lena



(e) Cover Image rice



(f) Stego Image rice



(f) Cover Image cameraman



(g) Stego Image cameraman

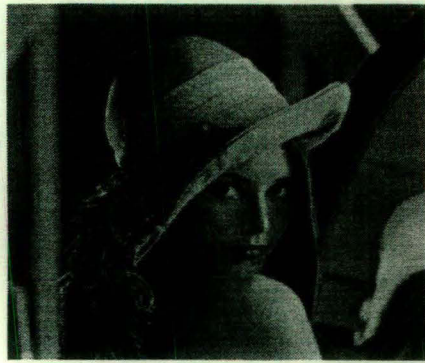
Fig. 4.2 (a) and (b) are stego and cover image, (c) and (d) are stego and cover image, (e) and (f) are stego and cover image, (g) and (h) are stego and cover image respectively using DCT transform domain method steganography



(a) Cover Image pout



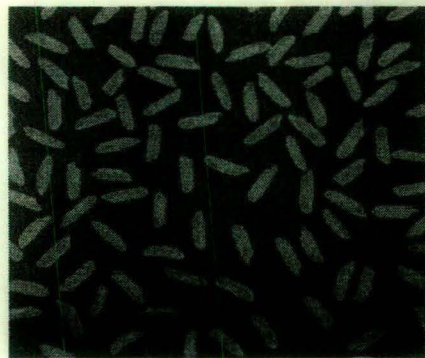
(b) Stego Image pout



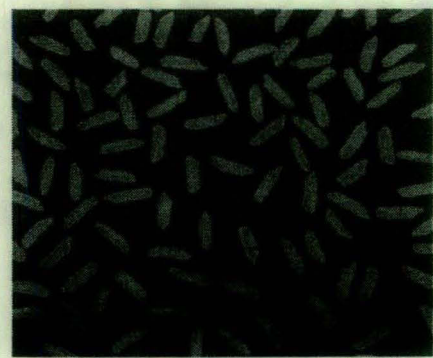
(b) Cover Image lena



(c) Stego Image lena



(d) Cover Image rice



(e) Stego Image rice



(f) Cover Image cameraman



(g) Stego Image cameraman

Fig. 4.3 (a) and (b) are stego and cover image, (c) and (d) are stego and cover image, (e) and (f) are stego and cover image, (g) and (h) are stego and cover image respectively using Wavelet based method steganography

Table. 4.3 The PSNR and Entropy between stego and cover image using wavelet

S.No.	Cover Image	PSNR (dB)	Entropy (ΔE)
1.	pout.tif	60.5468	0.1131
2.	lena.png	60.5655	0.0001
3.	rice.png	60.5609	0.0046
4.	cameraman.tif	60.5515	0.0027

It can be observed that PSNR value is greater and entropy difference is smaller for spatial domain steganography methods in comparison to transform domain steganography techniques. Hence, the performance of spatial domain steganography is better in comparison to transform domain steganography techniques.

4.4 Segmentation based Steganography Technique

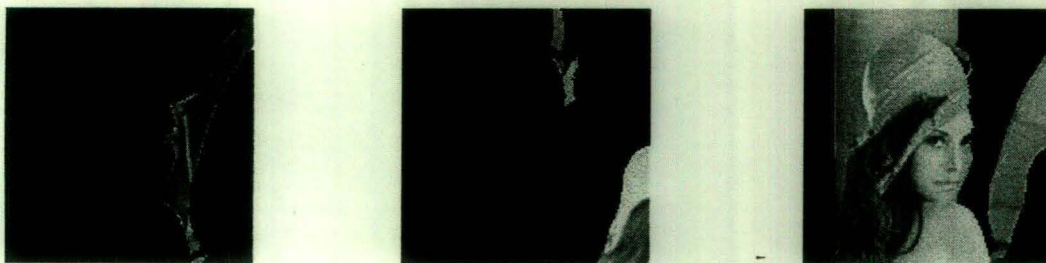
In this segmentation based steganography technique, the cover image is first divided in various parts using Normalized Cut (NCUT) segmentation technique [11]. The message is embedded in these segments and each one of this part is called stego segment. All these stego

segments are combined together to get the stego image. The reverse process is carried out to extract the message.

Segmented portion of lena image using NCUT method is shown in Fig. 4.10(a)-(c). After embedding the message using LSB method in these segmented cover elements, the corresponding stego segment elements are shown in Fig. 4.11(d)-(f). Combining together the stego segment elements, we obtain the stego image. The original lena image and its stego image using segmentation based technique is shown in Fig. 4.12(g)-(h) respectively.

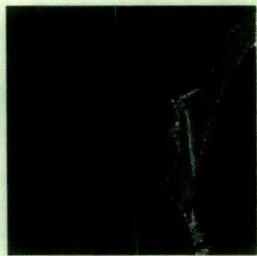
Similarly, for pout image, the segmented portion using NCUT method is shown in Fig. 4.13(a)-(c). After embedding the same message using LSB method in these segmented cover elements, the corresponding stego segment elements are shown in Fig. 4.14(d)-(f). Combining together the stego segment elements, we obtain the stego image. The original pout image and its stego image using segmentation based technique is shown in Fig. 4.15(g)-(h) respectively.

Similarly, for cameraman image, the segmented portion using NCUT method is shown in Fig. 4.16(a)-(c). After embedding the same message using LSB method in these segmented cover elements, the corresponding stego segment elements are shown in Fig. 4.17(d)-(f). Combining together the stego segment elements, we obtain the stego image. The original cameraman image and its stego image using segmentation based technique is shown in Fig. 4.18(g)-(h) respectively.

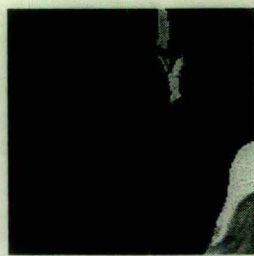


(a) cover segment 1 of lena (b) cover segment 2 of lena (c)cover segment3 of lena

Fig. 4.10 (a)-(c) different segment of Lena Image



(d) stego of segment 1



(e) stego of segment 2



(f) stego of segment3

Fig. 4.11 (d)-(f) different stego segments of Lena Image after embedding the message



(g) original cover image of Lena



(h) stego image of Lena

Fig. 4.12 (g) and (h) are original and stego image of lena after combining the all stego elements respectively



(a) cover segment 1 of pout

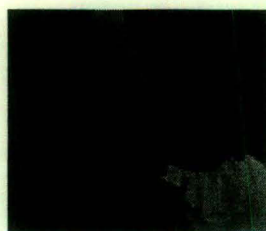


(b)cover segment 2 of pout

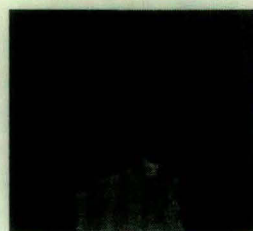


(c)cover segment3 of pout

Fig. 4.13 (a)-(c) different segment of pout image



(d) stego of segment 1

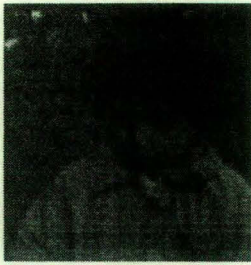


(e) stego of segment 2



(f) stego of segment3

Fig. 4.14 (d)-(f) different stego segments of pout Image after embedding the message



(g) original cover image of Lena



(h) stego image of Lena

Fig. 4.15 (g) and (h) are original and stego image of pout after combining the all stego elements respectively



(a) cover segment 1 of cameraman



(b) cover segment 2 of cameraman



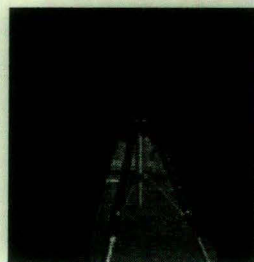
(c) cover segment 3 of cameraman

cameraman

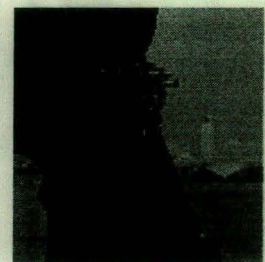
Fig. 4.16 (a)-(c) different segment of cameraman image



(d) stego of segment 1



(e) stego of segment 2



(f) stego of segment 3

Fig. 4.17 (d)-(f) different stego segments of cameraman Image after embedding the message



(g) cover image of cameraman

(h) stego of cameraman

Fig. 4.18 (g) and (h) are original and stego image of cameraman after combining the all stego elements respectively

Table 4.4: The PSNR and Entropy values of different images lena, cameraman and pout using Spatial domain (LSB), and Transform domain (Wavelet based) and Amalgamation based steganography techniques.

Image	PSNR				Entropy			
	LSB	Wave	DCT	Segmenta -tion	LSB	Wave	DCT	Segmenta -tion
Lena	63.9266	60.5655	43.0872	32.8735	0.0013	0.0001	0.0031	0.0367
Camera -man	63.7991	60.5515	41.0899	30.9523	0.0014	0.0027	0.0495	0.0495
Pout	63.1824	60.5468	61.1642	32.8735	0.0732	0.1131	0.0975	0.0367

It can be observed from Fig. 4.12(a)-(h), Fig. 4.15(a)-(h) and Fig. (g)-(h) that visibly it is very difficult to distinguish the cover and its stego image. We have computed PSNR and entropy difference for all the three images. Table 4.4 shows comparisons of PSNR and entropy differences using LSB, DCT, Wavelet and segmentation based steganography techniques.

Form Table 4.4 it can be observed, that the performance of LSB method is significantly better in comparison to other methods in terms of PSNR measure. In terms of entropy no method is clear winner over others.

CONCLUSION

In this dissertation work state-of-the-art of the subject is presented which includes fundamental works and recent works of the subject. The fundamental techniques of steganography are discussed with their merits and demerits as follows:

- Spatial Domain Steganography Techniques vital technique, high payload capacity but vulnerable to several attacks.
- Transform Domain Steganography Techniques overcome some demerits of spatial domain steganography technique.
- Spread Spectrum Steganography Techniques spread the message signal in high band width which incorporates the robustness against message detection and destruction.
- Statistical Methods of Steganography statistics is incorporated to make system more robust against statistical attacks.
- Distortion Techniques generally used to embed message in text file.

To evaluate the performance of various steganography techniques PSNR and entropy measures are used. Spatial domain steganography, transform domain steganography techniques performance are evaluated on the basis of these criteria. Apart from that segmentation based steganography technique is proposed and its performance is compared with spatial domain steganography and transforms domain steganography techniques in terms of PSNR and entropy measures are used.

We observed that the performance of LSB method is better in terms of PSNR in comparison to other methods. However, there is no clear winner among these methods in terms of entropy measure.

In future, we propose to embed the message in transform domain to analyze the robustness of this steganography method.

REFERENCES

1. A. Cheddad, J. Condell, K. Curran, P. Mc. Kevitt “*Digital image steganography: Survey and analysis of current methods*,” Signal Processing, Elsevier. 2009.
2. A.I. Hashad, A. S. Madani A.E.M.A. Wahdan, “*A Robust Steganography Technique Using Discrete Cosine Transform Insertion*,” IEEE Explorer 2005, vol. 16, pp. 555-563.
3. Alasdair, M. Andrew, “*Introduction to Digital Image Processing with Matlab*,” Course Technology Cengage Learning, 2004.
4. C. Cachin, “*An Information-Theoretic Model for Steganography*,” Springer, Information Hiding, LNCS 1556, 1998, pp. 306-318.
5. C. Cachin, “*Digital Steganography*,” Encyclopedia of Cryptography and Security, February 2005, pp. 1-7.
6. D. Pham, C. Xu and J. Prince, “*A survey of current methods in medical image segmentation*,” Annual review of biomedical engineering, vol. 2, pp. 315-337, 2000.
7. E. Walia, P. Jain, Navdeep, “*An Analysis of LSB & DCT based Steganography*,” Global Journal of Computer Science and Technology, April 2010, vol. 10, pp. 4-8.
8. F. Y. Shih. “*Digital watermarking and Steganography: Fundamentals and Techniques*,” CRC Press Inc, 2007.
9. G.J. Simmons, “*The prisoners, problem and subliminal channel*,” Advances in Cryptology: Proceedings of Crypto 83, Plenum Press, 1984, pp. 51-67.
10. H.J. Zhang, H.J. Tang, “*A Novel Image Steganography Algorithm against Statistical Analysis*,” IEEE, Proceedings of the Sixth International Conference on Machine Learning and Cybernetics, August 2007, pp. 3884-3888.
11. <http://users.rowan.edu/~polikar/WAVELETS/WTtutorial.html>
12. <http://www.dtic.upf.edu/~xserra/cursos/TDP/referencies/Park-DWT.pdf>
13. <http://www.grafpedia.com/wp-content/uploads/2009/05/159.jpg>
14. I.J. Cox, M.L. Miller, J.A. Bloom, J. Fridrich, T. Kalker, “*Digital Watermarking and Steganography, Second Edition*,” Morgan Kaufman Publishers.

15. J. Shi, J. Malik, "Normalized Cuts and Image Segmentation," IEEE Transactions on Pattern Analysis and Machine Intelligence, August 2000, vol. 22, no. 8, pp. 888-905.
16. J. Smith, B. Comiskey, "Modulation and Information Hiding in Images," Springer Proceedings, Information Hiding: First International Workshop, 1996, vol. 1174, pp. 207-227.
17. L. Driskel, "Wavelet-based Steganography," Cryptologia, 2004, vol. 28 :2, pp. 157-174.
18. L. Jozsef. "Steganographic Methods," Periodica Polytechnica Ser. El. Eng. ,2000, vol. 44, pp. 249-258.
19. L.M. Maevel, C.G. Boncelet, C.T. Retter, "Spread Spectrum Image Steganography," IEEE Transactions Image Processing, August 1999, vol. 8, pp. 1075-1083.
20. L.Y. Por, T.F. Ang, B. Delina, "WhiteSteg: A New Scheme in Information Hiding Using Text Steganography," WSEAS Transactions on Computers, June 2008, vol. 7, Issue. 6, pp. 735-745.
21. M. Zamani, A.A. Manaf, R.B. Ahmad, A.M. Zeki, S. Abdullah, "A Genetic-Algorithm-Based Approach for Audio Steganography," World Academy of Science, Engineering and Technology, 2009, vol. 54, pp. 360-363.
22. M.F. Tolba, M.A. Ghonemy, I.A. Taha, A.S. Khalifa, "Using Integer Wavelet Transforms in Colored Image-Steganography," IJICIS, 2004, vol. 4 no. 2, pp. 75-85.
23. N. F. Johnson and S. C. Katzenbeisser, "Information hiding techniques for steganography and digital watermarking," Artech House books, December 1999.
24. N. F. Johnson and S. Jajodia, "Exploring Steganography: Seeing the Unseen," Computer, 1998, vol. 31, no. 2, pp.26-34.
25. N. Provos, P. Honeyman, "Hide and Seek: An introduction to Steganography," IEEE Computer Society, IEEE Security & Privacy, 2003, pp. 32-43.
26. P. Sallee, "Model-Based Steganography," Springer, LNCS 2939, 2004, pp. 154-167.
27. R. C. Gonzalez and R. E. Wood, "Digital image processing using Matlab," Pearson education, Inc. and Dorling Kindersley Publishing Inc.
28. R.J. Anderson, F.A.P. Piticolas, "On The Limits of Steganography," IEEE Journal of Selected Areas in Communications, May 1998, vol. 16, pp. 474-481.

29. R.L. Pickholtz, D.L. Schilling, L.B. Milstein, "*Theory of Spread Spectrum Communications-A Tutorial*," IEEE Transactions on communications, May 1982, vol. com-30, pp. 855-884.
30. S. A. Vanstone, P. C. V. Oorschot, A. J. Menezes, "*Handbook of Applied Cryptography*," CRC Press, 1997.
31. S. Vankatraman, A. Abraham, M. Parzycki, "*Significance of Steganography on Data Security*," IEEE, Proceeding of ITCC04, 2004.
32. V.M. Potdar, S. Han, E. Chang, "*Fingerprinted Secret Sharing Steganography for Robustness against Image Cropping Attacks*," IEEE, Proceeding of 3rd IEEE International Conference on Industrial Informatics (INDIN), 2005, pp. 717-724.
33. W. Bender, D. Gruhl, N. Marimoto, A. Lu, "*Techniques for data hiding*," IBM Systems Journal, 1996, vol. 35, pp. 313-336.
34. W. Walker, "*Digital Signal Processing and Applications 2nd edition*," 2004.
35. W.J. Chan, C.C. Chang, T.H. Ngan Le, "*High payload Steganography mechanism using hybrid edge detector*," Expert Systems with Applications, 2009, vol. 30, pp. 1-10.