Chapter 1: Introduction

1.1 What is covert data hiding?

The standard and concept of “What You See Is What You Get (WYSIWYG)” which we encounter sometimes while printing images or other materials, is no longer precise and would not fool a steganographer as it does not always hold true. Images can be more than what we see with our Human Visual System (HVS); hence they can convey more than merely 1000 words. For decades, people strove to develop innovative methods for secret communication. The remainder of this introduction briefly highlights some historical facts and attacks. A thorough history of steganography can be found in the literature [1, 2, 3]. Three techniques are interlinked, steganography, watermarking and cryptography. The first two are quite difficult to tease apart especially for those coming from different disciplines. Figure 1.1 [4] may eradicate such confusion. The work presented here revolves around steganography in digital images and it does not discuss other types of steganography (such as linguistic or audio).

![Diagram of information hiding disciplines]

Figure 1.1: The different embodiment disciplines of information hiding. (Bold face indicates the focus of this study)
1.2 Cryptography, Steganography & Watermarking – A quick look

- Cryptography is about protecting the content of messages (their meaning).
- Steganography is about concealing the existence of messages
- Watermarking is about establishing identity of information to prevent unauthorized use

**Steganography**: hide existence of the secret message, but do not use encryption

**Cryptography**: encrypt the message, but do not hide the message

**Steganography**: 1). Emphasis on avoiding detection
- 2). Higher the capacity
- 3). Usually fragile

**Watermarking**: 1). Emphasis on avoiding distortion of cover
- 2). Robust
- 3). Smaller capacity

Comparison of steganography, watermarking and encryption in terms of different parameters & criteria is given below in Table 1.1 [4].

<table>
<thead>
<tr>
<th>Criterion/Method</th>
<th>Steganography</th>
<th>Watermarking</th>
<th>Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Carrier</td>
<td>any digital media</td>
<td>mostly image/audio files</td>
<td>usually text based, with some extensions to image files</td>
</tr>
<tr>
<td>Secret data</td>
<td>payload</td>
<td>watermark</td>
<td>plain text</td>
</tr>
<tr>
<td>Key</td>
<td>optional</td>
<td>necessary</td>
<td></td>
</tr>
<tr>
<td>Input files</td>
<td>at least two unless in self-embedding</td>
<td>one</td>
<td></td>
</tr>
<tr>
<td>Detection</td>
<td>blind</td>
<td>usually informative (i.e., original cover or watermark is needed for recovery)</td>
<td>blind</td>
</tr>
<tr>
<td>Authentication</td>
<td>full retrieval of data</td>
<td>full retrieval of data</td>
<td>full retrieval of data</td>
</tr>
<tr>
<td>Objective</td>
<td>secret communication</td>
<td>copyright preserving</td>
<td>data protection</td>
</tr>
<tr>
<td>Result</td>
<td>stego-file</td>
<td>watermarked-file</td>
<td>cipher-text</td>
</tr>
<tr>
<td>Concern</td>
<td>detectability/capacity</td>
<td>robustness</td>
<td>robustness</td>
</tr>
<tr>
<td>Type of attacks</td>
<td>steganalysis</td>
<td>image processing</td>
<td>cryptanalysis</td>
</tr>
<tr>
<td>Visibility</td>
<td>never</td>
<td>sometimes (see Fig. 2)</td>
<td>always</td>
</tr>
<tr>
<td>Fails when</td>
<td>it is detected</td>
<td>it is removed/replaced</td>
<td>de-ciphered</td>
</tr>
<tr>
<td>Relation to cover</td>
<td>not necessarily related to the cover. The message is more important than the cover.</td>
<td>usually becomes an attribute of the cover image. The cover is more important than the message.</td>
<td>N/A</td>
</tr>
<tr>
<td>Flexibility</td>
<td>free to choose any suitable cover</td>
<td>cover choice is restricted</td>
<td>N/A</td>
</tr>
<tr>
<td>History</td>
<td>very ancient except its digital version</td>
<td>modern era</td>
<td>modern era</td>
</tr>
</tbody>
</table>

“Implementation & Analysis of Covert Data Hiding Techniques”
1.3 Classical Steganography – Historical Perspective

The idea and practice of hiding information has a long history. In Histories the Greek historian Herodotus writes of a nobleman, Histaeus, who needed to communicate with his son-in-law in Greece. He shaved the head of one of his most trusted slaves and tattooed the message onto the slave’s scalp. When the slave’s hair grew back the slave was sent with the hidden message [5]. In the Second World War shrinking messages down to the size of a dot became a popular method of steganography since the microdot could be placed at the end of a sentence or above a j or i. The Germans developed the Microdot technique. Information, especially photographs, was reduced in size until it was the size of a typed period. Extremely difficult to detect, a normal cover message was sent over an insecure channel with one of the periods on the paper containing hidden information [6].

Other methods including using obscure places to put messages such as on the inside of an envelope or shrunken down and place under the postage stamp. In Saudi Arabia at the King Abdul Aziz City of science and technology, a project was initiated to translate some ancient Arabic manuscripts on secret writing, which are believed to have been written 1200 years ago into English. Some of these manuscripts were found in Turkey and Germany [7].

Five hundred years ago, the Italian mathematician Jerome Cardan reinvented a Chinese ancient method of secret writing. The scenario goes as follows: a paper mask with holes is shared among two parties, this mask is placed over a blank paper and the sender writes his secret message through the holes then takes the mask off and fills the blanks so that the message appears as an innocuous text as shown in figure 1.2. Cardan Grille: an illustration, keeping in mind that the Grill has no fixed pattern: (left) the mask, (middle) the cover and (right) the secret message revealed. This method is credited to Cardan and is called Cardan Grille [8].

![Cardan Grille: an illustration](image)

Today steganography is mostly uses computers with digital data being the carriers and networks being the high speed delivery channels.
1.4 Overview of Steganography

Since the rise of the Internet one of the most important factors of information technology and communication has been the security of information. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called steganography.

Steganography is the art and science of invisible communication. This is accomplished through hiding information in other form of information, thus hiding the existence of the communicated information. The word steganography is derived from the Greek words “stegos” meaning “cover” and “grafia” meaning “writing” [12] defining it as “covered writing”. In image steganography the information is hidden exclusively in images.

The term Steganography refers to the art of covert communications. By implementing steganography, it is possible for Alpesh to send a secret message to Alpa in such a way that no-one else will know that the message exists. Typically, the message is embedded within another object known as a cover Work, by tweaking its properties. The resulting output, known as a stegogramme is engineered such that it is a near identical perceptual model of the cover Work, and at the same time it also contains the hidden message. It is this stegogramme that is sent between Alpesh and Alpa.

If anybody intercepts the communication, they will obtain the stegogramme, but as it is so similar to the cover, it is a difficult task for them to tell that the stegogramme is anything but innocent. It is therefore the duty of steganography to ensure that the adversary regards the stegogramme - and thus, the communication - as innocuous.

Data hiding technique is a generic term of designing a very wide set of applications, such as steganography [9]. The term steganography, as discussed above, is derived from the Greek language and means covert writing. It is the technique of encoding secret information in a communication channel in such a manner that the very existence of the information is concealed.
1.4.1 Concept of Steganography

The major goal of steganography is to enhance security of message in communication by inserting secret message into the digital image, modifying the nonessential pixels of the image [10, 11]. A block diagram of a generic blind image steganographic system is depicted in figure 1.3. A message is embedded in a digital image by the stegosystem encoder, which uses a key or password. The image after the embedding of the secret message, so-called stegoimage is transmitted to the receiver through a public channel, where the stegosystem decoder using the same key processes it. During transmission, the stegoimage can be monitored by unintended viewers, who will notice only the transmission of the innocuous image, and will not be able to discover the existence of the hidden message. Graphical Representation is shown in figure 1.3 (a) for sender side and (b) for receiver side.

![Graphical representation of Steganography system](image)

(a) Sender side of steganography

(b) Receiver side of steganography

Figure 1.3: Graphical representation of Steganography system
**Steganography: Common Elements**

<table>
<thead>
<tr>
<th>Cover medium (image)</th>
<th>-- innocuous carrier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Embedded message</td>
<td>-- plaintext, cipher text, images, etc.</td>
</tr>
<tr>
<td>Stego-key</td>
<td>-- password</td>
</tr>
<tr>
<td>Stego-medium</td>
<td>-- secret message</td>
</tr>
</tbody>
</table>

\[ \text{Cover medium (image) + embedded message + stego-key} = \text{stego-medium (image)} \]

### 1.4.2 The Process of Steganography

When a steganographic system is developed, it is important to select how the appropriate cover work should be, and also how the stegogramme is to reach to its recipient. With the Internet offering so much functionality, there are many different ways to send messages to people without anyone knowing that they exist. For example, it is possible that an image stegogramme could be sent to a recipient via email. Alternatively it might be posted on a web forum for all to see, and the recipient could log onto the forum and download the image to read the message. Of course, although everyone can see the stegogramme, they will have no reason to expect that it is anything more than just an image. In terms of development, Steganography is comprised of two algorithms, one for embedding and one for extracting.

The embedding process is concerned with hiding a secret message within a cover Work, and is the most carefully constructed process of the two. A great deal of attention is paid in ensuring that the secret message goes unnoticed even if a third party is able to intercept the cover Work. The extracting process is traditionally a much simpler process, as it is simply an inverse of the embedding process, where the secret message is revealed at the end. The entire process of steganography for images can be presented graphically as;

1. **Secret message**- usually a text file that contains the message you want to transfer
2. **Cover Work** - used to construct a stegogramme that contains a secret message

The next step is to pass the inputs through the Stego-system Encoder, which will be carefully engineered to embed the message within an exact copy of the cover Work, such that minimum distortion is made; the lower the distortion, the better the chances of undetectability. The stegosystem encoder will usually require a key to operate, and this key would also be used at the extraction phase. This is a security measure designed to protect
the secret message. Without a key, it would be possible for someone to correctly extract the message if they managed to get hold of the embedding or extracting algorithms. However, by using a key, it is possible to randomize the way the stegosystem encoder operates, and the same key will need to be used when extracting the message so that the stegosystem decoder knows, which process to use. This means that if the algorithm falls into wrong hands, this extremely unlikely that they will be able to extract the message successfully.

The resulting output from the stegosystem encoder is the stegogramme, which is designed to be as close to the cover Work as possible, except it will contain the secret message. This stegogramme is then sent over some communications channel along with the key that was used to embed the message. Both the stegogramme and the key are then fed into the stegosystem decoder where an estimate of the secret message is extracted [23].

Note that we can only ever refer to the output of the extraction process as an estimate because when the stegogramme is sent over a communications channel, it may be subjected to noise that will change some of the values. Therefore, we can never be sure that the message extracted is an exact representation of the original. Also, the recipient will obviously never know what the original message was, and so they have nothing to compare it to when it is extracted. This is probably the most common system of image stegananography today, with the focus mainly on developing the stegosystem encoder carefully. It is of paramount importance in steganography that the stegogramme contains no trail of embedding a secret message if it is to be successful.

In recent years, many steganographic algorithms have been made publicly available, and so it is very easy for anyone with even a limited knowledge of steganography to be able to communicate covertly. Most of the systems make use of everyday images as the basis for the models, and of course, the information that is hidden within those images can range from anything between harmless gibberish to messages that are a threat to national security.

Subsequently, there is a growing concern as to how we can identify whether any image contains steganography, such that we can be sure the technology is not used for the wrong purposes. This counter-activity is referred to as Steganalysis, and much resource and research have been put into determining whether an image is innocent or not. Steganography simply takes one piece of information and hides it within another. The art and science of writing hidden messages in such a way that no one, apart from the intended
recipient, knows of the existence of the message. The goal of steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second secret message present.

Steganography includes a vast array of techniques for hiding messages in a variety of media. Among these methods are invisible inks, microdots, digital signatures, covert channels and spread-spectrum communications. Today, thanks to modern technology, steganography is used on text, images, sound, signals, and more.

The advantage of steganography is that it can be used to secretly transmit messages without the fact of the transmission being discovered. Often, using encryption might identify the sender or receiver as somebody with something to hide. For example, that picture of your cat could conceal the plans for your company's latest technical innovation.

1.5 Introduction to Steganalysis

1.5.1 What is Steganalysis?

Steganalysis is the art of identifying stegogramme that contain a secret message. The goal of steganography is to avoid drawing suspicion to the transmission of a hidden message. If suspicion is raised, then this goal is defeated. Discovering and rendering unless such covert message is a new art form known as steganalysis [13].

Steganalysis does not however consider the successful extraction of the message; this is usually a requirement for cryptanalysis. Typically, steganalysis begins by identifying any artifacts that exist in the suspect file as a result of embedding a message. None of the steganographic systems that are known today achieve perfect security [17], and this means that they all leave hints of embedding in the stegogramme. This gives the steganalyst a useful way in to identifying whether a secret message exists or not.

Nowadays, the countermove between Steganography and Steganalysis has received significant attention [14, 15]. Extensive investigations indicate that the changes of statistical features can be used to detect the existence of secret messages in images. So it is of great importance to study on the statistical features of natural images for the development of steganalysis techniques [16].

In the past, steganography avoided any visual distortions in the stego images. Hence, majority of the stego images do not reveal any visual clues as to whether a certain image contains any hidden message or not. Current steganalysis aims to focus more on detecting
statistical anomalies in the stego images, which are based on the features extracted from typical cover images without any modifications.

Cover images without any modification or distortion contain a predictable statistical correlation, which when modified in any form will result in distortions to that correlation. These include global histograms, blockiness, inter and intra block dependencies and other first and second order statistics of the image. Most steganalysis algorithms are based on exploiting these strong dependencies, which are typical of natural images [18].

1.5.2 Classification of Steganalysis
Steganalysis can be classified into two broad categories:

1) Specific/Targeted Steganalysis: Specific steganalysis, also sometimes knows as targeted steganalysis, is designed to attack one particular type of steganography algorithm. The steganalyst is aware of the embedding methods and statistical trends of the stego image if embedded with a known algorithm.

   This attack method is very effective when tested on images with the known embedding techniques whereas it might fail considerably if the algorithm is unknown to the steganalyst. For example, Jsteg [19], which simply changes the LSB of a coefficient to the value desired for the next embedded data bit, can be detected by the effect it has of equalizing adjacent pairs of coefficient values [20].

2) Blind/Generic/Universal Steganalysis: Blind steganalysis also known as universal steganalysis is the modern and more powerful approach to attack a stego media since this method does not depend on knowing any particular embedding technique. This method can detect different types of steganography content even if the algorithm is not known [18]. However, this method cannot detect the exact algorithm used to embed data if the training set is not trained with that particular stego algorithm.

   The method is based on designing classifiers, which depends on the features or correlations, existing in the natural cover images. The most current and popular methods include extracting statistical characteristics (also known as features) from the given set of images.
1.6 Various types of Steganography

Almost all digital file formats can be used for steganography, but the formats that are more suitable are those with a high degree of redundancy. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object’s use and display [22]. The redundant bits of an object are those bits that can be altered without the alteration being detected easily [21]. Image and audio files especially comply with this requirement, while research has also uncovered other file formats that can be used for information hiding. Figure 1.4 shows steganography in different types of media by using various techniques.

1.6.1 Steganography in Text

- **Soft Copy Text**
  - In this method encode data by varying the number of spaces after punctuation. Slight modifications of formatted text will be immediately apparent to anyone reading the text. Use of White Space (tabs & spaces) is much more effective and less noticeable. This is most common method for hiding data in text. Encode data in additional spaces placed at the end of a line.
INTRODUCTION

- Hard Copy Text
  - **Line Shift Coding:** Shifts every other line up or down slightly in order to encode data. In this method, text lines are vertically shifted to encode the document uniquely. Encoding and decoding can generally be applied either to the format file of a document, or the bitmap of a page image.
  - **Word-Shift Coding:** In word-shift coding, code words are coded into a document by shifting the horizontal locations of words within text lines, while maintaining a natural spacing appearance. This encoding can also be applied to either the format file or the page image bitmap. The method, of course, is only applicable to documents with variable spacing between adjacent words, such as in documents that have been text-justified. As a result of this variable spacing, it is necessary to have the original image, or to at least know the spacing between words in the un-encoded document. Shifts some words slightly left or right in order to encode data.

1.6.2 Steganography in Audio

1. Low Bit Coding
2. Phase Coding
3. Spread Spectrum
4. Echo Data Hiding

- **Low Bit Coding**
  - In this method, most digital audio is created by sampling the signal and quantizing the sample with a 16-bit quantized value. The rightmost bit, or lower order bit, of each sample can be changed from 0 to 1 or 1 to 0. This modification from one sample value to another is not perceptible by most people and the audio signal still sounds the same.

- **Phase Coding**
  - This method work on the relative insensitivity of the human auditory system to phase changes. Substitutes the initial phase of an audio signal with a reference phase that represents the data. More complex than low bit encoding, but it is much more robust and less likely to distort the signal that is carrying the hidden data.
Direct Sequence Spread Spectrum
- It spreads the signal by multiplication, which is a maximal length pseudorandom sequence. DSSS introduces additive random noise to the sound file [12;24]

Echo Data Hiding
- Discrete copies of the original signal are mixed in with the original signal creating echoes of each sound. By using two different time values between an echoes ends are used for hiding secret information.

1.6.3 Steganography in Image
1. Least Significant Bit Insertion
2. Masking and Filtering
3. Transformations

Least Significant Bit Insertion:
The most common and popular method of modern day steganography is to make use of the LSB of a picture’s pixel information. Thus the overall image distortion is kept to a minimum while the message is spaced out over the pixels in the images. This technique works best when the image file is larger than the messages file and if the image is grayscale. Many stego tools make use of least significant bit (LSB). For example, 11111111 is an 8-bit binary number. The rightmost bit is called the LSB because changing it has the least effect on the value of the number. The idea is that the LSB of every byte can be replaced with little change to the overall file. The binary data of the secret message is broken up and then inserted into the LSB of each pixel in the image file.

The larger the cover message is (in data content terms — number of bits) relative to the hidden message, the easier it is to hide the later. For this reason, digital pictures (which contain large amounts of data) are used to hide messages on the Internet and on other communication media. It is not clear how commonly this is actually done. For example: a 24-bit bitmap will have 8 bits representing each of the three color values (red, green, and blue) at each pixel. If we consider just the blue there will be $2^8$ different values of blue. The difference between say 11111111 and 11111110 in the value for blue intensity is likely to be undetectable by the human eye. Therefore, the least significant bit can be used (more or less undetectably) for something else other than color information. If we do it with the green and the red as well we can get one letter of ASCII text for every three pixels. LSB
insertion works well with gray-scale images as well. It is possible to hide data in the least and second least significant bits and the human eye would still not be able to discern it [1, 26].

- Consider a 24 bit picture
- Data to be inserted: character ‘A’: (10000011)
- Host pixels: 3 pixel will be used to store one character of 8-bits
- The pixels, which would be selected for holding the data, are chosen on the basis of the key, which can be a random number.

Ex: 

00100111 11101001 11001000
00100111 11001000 11101001
11001000 00100111 11101001

- Embedding ‘A’

00100111 11101000 11001000
00100110 11001000 11101000
11001001 00100111 11101001

According to researchers on an average only 50% of the pixels actually change from 0 to 1 or 1 to 0.

Masking and Filtering:

Masking and filtering techniques, usually restricted to 24 bits or grayscale images, take a different approach to hiding a message. These methods are effectively similar to paper watermarks, creating markings in an image. This can be achieved, for example, by modifying the luminance of parts of the image. While masking does change the visible properties of an image, it can be done in such a way that the human eye will not be able to notice the anomalies. Since masking uses visible aspects of the image, it is more robust than LSB modification with respect to compression, cropping and different kinds of image processing. The information is not hidden at the “noise” level but is inside the visible part of the image, which makes it more suitable than LSB modifications in case a lossy compression algorithm like JPEG is being used [26,27].

Transformations:

This technique hides data in mathematical functions that are often used in compression algorithms like DCT (Discrete Cosine Transform). The idea of this method is to
take 8x8 pixel block, apply DCT, divide DCT coefficients by quantization table & hide the secret message bits in LSB of quantized DCT coefficients.

**1.7 Research Aims**

The aim of the current research in the field of steganography and steganalysis is to present a variety of techniques for both. We have started with discussion on several techniques for hiding a secret message in an image, and then considered how this can be detected from a steganalyst viewpoint. The most important aspects of image steganographic systems are capacity, detect-ability & robustness. This thesis is focused to increase the performance of various algorithms to enhance capacity, image quality and robustness against attack.

Our major research aim is to improve the current steganography techniques in terms of capacity, apparent (cleanness of image), robustness, PSNR etc.

**1.8 Outline of thesis**

- Chapter 1 gives brief introduction & hypothesis about research area and compares steganography technique with other data hiding technology. In this chapter history of steganography, various Medias, which are used in research, types of stegnography etc. are also discussed.

- Chapter 2 emphasizes the methods for steganography and steganalysis that will be necessary to build up a clear picture of both fields. This chapter will discuss the main principles of steganography and steganalysis by firstly discussing, where we currently stand in both fields, and then introducing the necessary background knowledge that is required to properly understand the methods. It will also present some basic stego analytical schemes associated with "targeted" Steganalysis, including visual and statistical attacks.

- Chapter 3 is to raise awareness of the magnitude of known embedding techniques. It will also discuss some of the most documented steganographic approaches, splitting them into appropriate groups to illustrate, how they differ from each other.

- Chapter 4 is focused on existing spatial domain and frequency domain data hiding techniques.
Chapter 5 will be focused on newly proposed techniques. It will also compare them with existing techniques.

Chapter 6 is based on results and analysis. It will explain results based on comparison of proposed techniques with existing techniques in terms of different parameters like capacity, PSNR (Peak Signal to Noise Ratio), Robustness, Execution time etc.

Conclusion of the thesis will be discussed Chapter 7.

Chapter 8 describe about scope of future work