Novel Image Steganography with Improved Security

By

Arslan Riaz

A thesis submitted to the faculty of Electrical Engineering Department Military College of Signals, National University of Sciences and Technology, Islamabad in partial fulfillment of the requirements for the degree of MS in Electrical (Telecommunication) Engineering

Apr 2018

THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS/MPhil thesis written by Mr/~~MS~~ **Arslan Riaz,** Registration No. **NUST2014-63810-MMCS25014F**, of **Military College of Signals** has been vetted by undersigned, found complete in all respect as per NUST Statutes/Regulations, is free of plagiarism, errors and mistakes and is accepted as partial, fulfillment for award of MS/MPhil degree. It is further certified that necessary amendments as pointed out by GEC members of the student have been also incorporated in the said thesis.

Signature: _____

Name of Supervisor Col (R)Dr Imran Touqeer, PhD

Date: _____

Signature (HoD): _____

Date: _____

Signature (Dean): _____

Date: _____

ABSTRACT

With continues advancement in technology, internet has proved to be a major way of communication between peoples. People are using this medium for communication, sharing important data, resources, technology, research and military related communications. However, the security of data we are sending is a major concern for most of us. In this cyber space, the transmitted information can be very simply modified or copied by unintended users. So, secrecy and privacy has become a hot topic nowadays. Therefore, finding more secure techniques to transmit our data has become a key issue nowadays.

The goal of this research is to develop an algorithm that is more secure. In this paper, we present a secure steganographic technique. The secret image is divided into two parts using a pixel selection algorithm. Both parts contain almost equal number of pixels. These parts are embedded into two cover images using LSB Technique. A sequence key is assigned to both parts. At receiver end, secret image parts are aligned using sequence key. With this technique, it will be more difficult for attackers to crack secret Image from stego images. Experimental results show that original image is identical to stego image. This is proved by the fact that we have comparable visual quality as the Peak Signal to Noise Ratio values lie above 40db. We have also performed statistical security analysis, which shows that proposed technique is resistive to such type of attacks. Statistical properties of host image are same steganographic image due to this fact attackers cannot use statistical attacks.

DEDICATION

This thesis is Dedicated to

My Parents and my supervisor

for their continues backing and encouragement.

ACKNOWLWDGEMENTS

I am thankful to the omnipotent, omnipresent and omniscient Allah who gave me the power and strength to accomplish my thesis. and I am thankful to him for his for his mercy, without his Willing I could not have accomplished a single step in this task.

This thesis is dedicated, with cordial love and endless respect, to many valuable persons. I express my sincere thankfulness to my supervisor Col Dr. Imran Touqeer, Associate Professor, Military College of Signals (NUST), from whom I sought after valuable guidance and help to accomplish this job. This research work will not be done without his continues support. I am very grateful to my committee members, Lt. Col. Dr. Adil Masood Sidiqui and Dr Muhmmad Imran for their continues support and participation in this research work. At last I would like to thank Military College of Signals (MCS), NUST, for providing splendid research atmosphere at the institution.

The never-ending support from my family and friends whose courage and help enable me to complete my Master Degree in Electrical Engineering along with thesis. I am very grateful of the faculty members of Electrical Engineering Department and especially the Head of Electrical Engineering Department for their everlasting encouragement that has fueled my sense of continued determination over the years.

Table of Contents

LIST OF FIGURES

NOTATION

ACRONYMS

1) Peak Signal to Noise Ratio	**PSNR**
2) Mean Square Error	**MSE**
3) Secret Image	**S**
4) Cover Image 1	**C1**
5) Cover Image 2	**C2**
6) First stego image	**Stego 1**
7) Second stego image	**Stego 1**
8) Recovered Image	**R**

Chapter 1

Introduction

1.1.Background

It has been observed that the circulation scheme of internet for digital broadcasting is exceptional due to its inexpensive nature and effectiveness. The common uses of internet particularly in the distribution and broadcasting of digital images are comparatively easier. Nevertheless, the communicated information can be very simply copied or altered by unintended users in World Wide Web. Consequently, discovering methods to communicate data covertly through internet has turn out to be a significant problem. Encryption is the secure earliest methods that uses cipher algorithms and convert the information into a cipher text. It scrambles the text and thus is not understandable to the unauthorized persons. Nevertheless, it can unsurprisingly increase the interests of a spy. In addition, a more judiciousness is provided after the smart implantation of a secret text in the alternative media to keep the secret information hidden from everybody. This makes the stenographic foundations.

Steganography is derived from Greek language which translates into “sheltered writing”. In background of steganography, the information needed to be sent is known as a message. This message is implanted into a stream of bits. The secret message is kept hidden by a medium known as cover medium. It can be an image, a video, or an audio file that hides the message. The stego-medium is generated when we implant the secret data into cover medium. Images are excellent cover mediums for secret messages.

The most important feature of steganography is that it hides the fact that secret communication is happening. It achieves this through hiding info into info. There are different

cover mediums that can be used but images are used most frequently. This mainly is due the fact that for hiding secret info in images, there are many Steganographic techniques. Some techniques are complex in structure while some are not. But every technique has its own importance. Some have strong and some have weak points. This is due the fact that, Diverse applications have various necessities of the steganography method used. For illustration, few applications possibly will need complete hiddenness of the secret data, whereas others require a bigger secret message to be hidden.

1.2.Research motivation

As security of our data is one of the key problems nowadays while using a public channel like internet. The important characteristic of Steganography is that it hides the fact that some secret communication is taking place. Attackers or hacker are threat due to the fact that they can gain access to the secret information and can copy, modify or delete the important information. Thus, steganography makes the attackers job more difficult through hiding the reality that some secret communication is going on. The importance of steganography in preserving secrecy of data can be exemplified with a simple example.

Imagine there are two parties who want to communicate with each other. They have to share something that is secret. The medium in this case will be internet. Let's say an attacker C has access to this communication channel as internet is a public channel. So, C can observe the communication happening between sender A and receiver B. If A asks B for lunch, then C do not find this important neither A and B mind if C observe this communication. So, A and B can communicate on public channel without any encryption. But if A is sending some confidential information to B then they do not want C to observe this. So, A would likely to encrypt the message. But the issue with encryption is that it causes suspicion to attacker C. He starts thinking

that there should be something hidden in this scramble message. Thus, C attempts to crack the message. As the computational power increases, nowadays encryption is becoming easier to break. The solution to this problem is steganography. For instance, A sends his secret message by hiding it in a natural image file for example picture of a garden. C will think that it is just a natural image and it will not put attacker in suspicion.

1.3 Thesis organization

- Chapter 1 Introduction. The chapter discusses the history and methods of secret communication used during old ages. Motivation to do this research. Illustration of a simple example of sharing some secret data and issues faced during this whole process.
- Chapter 2 Literature review: Discusses some techniques already implemented in this field. Difference between steganography, cryptography and water marking. Main components of a steganographic process. Methods of classifying the steganographic process. Also, discussed different types of steganographic methods used nowadays.
- Chapter 3 Proposed methodology: First, encoding process is discussed step by step, illustrating with the help of an example. Followed by detailed discussion on decoding algorithm.
- Chapter 4 Results: Test images used for testing are discussed. The performance of the proposed method is discussed. Experimental results are given in this chapter.
- Chapter 5 conclusions: accomplishes the research work based on the results achieved and offers recommendations for forthcoming work.

Chapter 2

Literature Analysis

2.1 Overview

The word steganography is derived from two Greek letters i.e. ‘stegano’ means protected and ‘graphia’ means writing. It is a process by which messages are written in such a way that the presence of secret message is known only to sender and receiver. There are three components required in steganography i.e. an object that carries the message, the data that is to be kept secret, and an algorithm that embeds the secret data. Additionally, increase the stenography’s security levels, some cases may require an encryption algorithm and secret key. There are various applications of steganography such as transmission security of top secret data between national and international governing bodies, online security of banks and voting systems, secret communication between criminals and terrorists and sending Trojan horses and viruses to attack on systems etc.

2.1.1 What is steganography?

Steganography deals with the composition of secret messages and their existence is only known to the sender and receiver. As, the life of the message is only known by the sender and receiver, therefore, it does now not pull the undesirable attention. The historical method of steganography is known as physical steganography used in ancient times. The examples of steganography include frame based hidden messages, secretly linked written texts, envelope based written messages covered by stamps, etc. Digital steganography is the modern approaches of steganography. This method encompasses noisy images with hidden messages, implantation of a message within a random data, and implantation of picture based messages within video documents.

2.1.2 What is Cryptography?

The process by which the information is kept hidden and used communication over an unsecure medium such as net, wherever info must be protected against different intruders is known as cryptography. Cryptographic algorithms are developed in modern cryptography that

are difficult to break by an opponent because of computational effectiveness, thus, unbreakable practically. Currently, three types of cryptologic algorithms are known; First, symmetric-key cryptography in which same key is used by the sender and receiver for encrypting the hidden data; Second, public-key cryptography in which two completely different keys are used by the sender and receiver but are mathematically connected; and third, hash functions that are not key-based algorithms and use calculated and defined length of hash value from data. Nobody can recover the actual fixed length or actual plain data from the value of hash.

2.1.3 What is Watermarking?

The process of watermarking includes the injection of a specific bit sequence into a file i.e. audio, video, digital image, etc. that identifies or relates the copyright information of file such as files author, specific purpose based rights to use the file and so on. The nomenclature comes from the hardly visible watermarks that are printed on the documents or stationaries that shows the stationery's manufacturer. The digital watermarks have a basic of ensuring the protection of a copyright for the material in digital formats.

2.1.4 Steganography vs Cryptography

There are distinct goals of steganography and cryptography. Cryptography is used only in the obscuring of content or meaning of a spy's secret messages whereas the message presence is concealed by steganography. Additionally, in the sense of more confidentiality, steganography is much better than cryptography because it hides the unimportant presence of hidden message as opposed to just protecting the content of the message. Consequently, one of the first shortcomings of cryptographic systems are that even though the message has been encoded, regardless it exists.

However, despite of the fact that both the cryptographic and steganographic systems are used for delivering secret communications, they are defined differently in the sense of system breaking. If an attacker can read the hidden message, then a cryptographic system can be regarded as a broken system. On the other hand, breaking of a steganographic system is defined by the ability of an attacker to detect the presence or read the hidden message's content. Furthermore, the failure of a steganographic system is based on the suspecting of a spic file by an attacker or a method of steganography even without the message decoding. Therefore, such a consideration of

systems based on steganography leads to more fragility than cryptographic systems in terms of failure. Moreover, steganography based systems must dodge a wide range of doubt to accomplish security and not be considered failed frameworks.

As an extra protection layer is added to cryptography by steganographic approaches, combination of both the steganographic and encryption approaches provides the ultimate in personal communications. Thus, the main objective of the steganographic methods is complementing cryptographic and avoiding the increase of doubt of system attackers but not getting the place of cryptography.

2.1.5 Steganography vs Watermarking

The aim of steganography is hiding the communication presence through messages implantation within other covered objects. On the other hand, the aim of watermarking is the owner's rights protection in digital formats such as image, audio, software, video etc. Regardless of the possibility that individuals duplicate or make minor change to the watermarked document, the proprietor can even now demonstrate it is his or her file. Therefore, it can be said that both steganography and watermarking are the approaches used for hiding the data with some shared attributes. However, embedding a message is the goal of steganography whereas covering an object itself is the goal of watermarking.

To hide and protect the digital information i.e. image, files or something else from the copyright removal, the technique of watermarking is used. Regardless of the possibility, if someone is aware of the watermark i.e. visible watermarking, watermark cannot be removed from the original object without destroying or distorting the original object. This property of watermarking is called as robustness. The method of a specific copyright mark implantation into a digital document in similar manner is regarded as watermarking. Then again, this digital document is embedded with a serial number that detects any break of the licensing agreement. This approach is called as fingerprinting. Regardless of the possibility that these markings are distinguished, it ought to be for all intents and purposes difficult to expel them.

2.2 Steganographic systems and Major Components

All the systems based on steganography or techniques contain three main components that are sender receiver and channel through which data is sent. So, the flow of the system is as defined in next few lines, imagine there are two parties who want to communicate with each other. They should share something that is secret. The medium in this case will be internet. Let's say an attacker C has access to this communication channel as internet is a public channel. So, C can observe the communication happening between sender A and receiver B. If A asks B for lunch, then C do not find this important neither A and B mind if C observe this communication. So, A and B can communicate on public channel without any encryption. But if A is sending some confidential information to B then they do not want C to observe this. So, A would likely to encrypt the message. But the issue with encryption is that it causes suspicion to attacker C. He starts thinking that there should be something hidden in this scramble message. Thus, C attempts to crack the message. As the computational power increases, nowadays encryption is becoming easier to break. The solution to this problem is steganography. For instance, A sends his secret message by hiding it in a natural image file for example picture of a garden. C will think that it is just a natural image and it will not put attacker in suspicion. The basic working of systems based on image steganography is shown in Figure 2.1

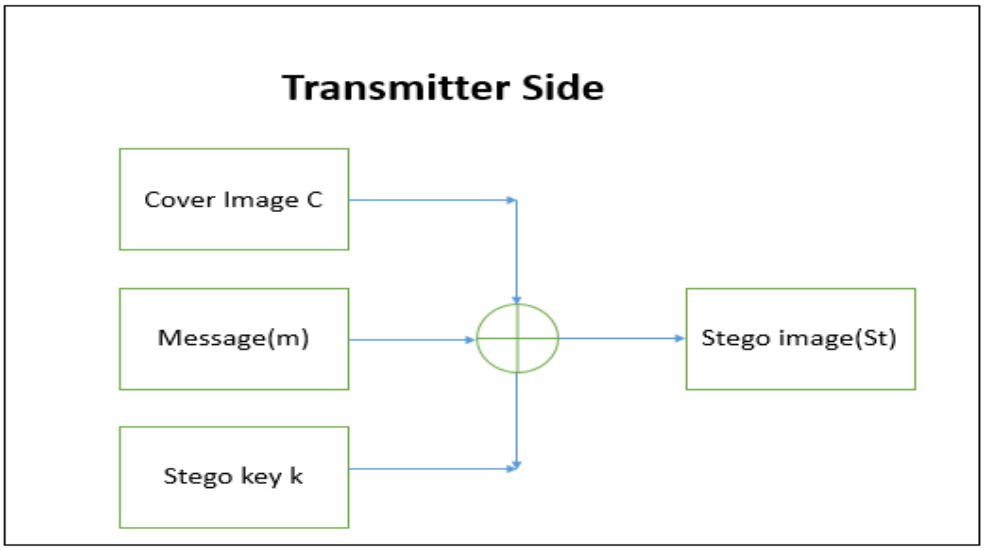


Figure 2.1 Transmitter Side of a Typical Steganography Process

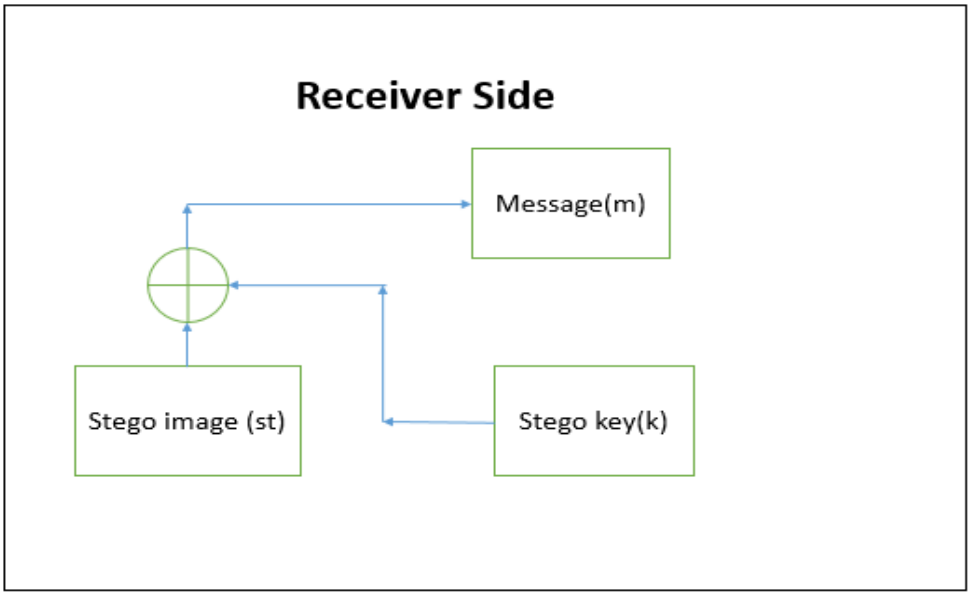


Figure 2.2 Receiver Side of a Typical Steganography Process

Sometimes, unauthorized intruders like Z can recognize a secret message that is hidden in a stego file get some answers concerning the strategy by which the message was implanted, but the extraction or cracking of secret information cannot be done by them. Because of the unreadability of the message or information, it is known as secure steganographic system and the

information is useless the intruder has the relevant stego key. Thus, special care should be taken while choosing these stego keys, so these stego keys must be picked as solid as conceivable to keep intruders from breaking the steganographic frameworks utilizing every single conceivable procedure. Hence, Kirchhoff's principle must be satisfied for the security of steganography based systems. Consequently, the designer must be aware of the fact before designing any steganographic system security that the attacker knows completely the encoding and decoding algorithms. But, the only thing that attackers require is stego key, if they get it they will be able for decoding the hidden secret message. Hence, loss of information to un intended users occurs.

2.3 Methods of Classification

There are two different types of steganographic systems. The first method is primarily based on the medium type used as a cover whereas the second method is based on the method of hiding. In other words we can say it is based on the way in which we embed the secret data into cover medium. In below mentioned sections, these two methods of classification are discussed in detail.

2.3.1 cover Based Classification

Basically, cover medium represent the medium which contains hidden information or secret data. Along with this, few sections or attributes of cover files will be adjusted or altered, changed, or controlled in such an approach to shroud these hidden secret messages. Nevertheless, such types of manipulations exist during the procedure of hiding and remain unnoticeable to anyone involved in the process of communication. Thus, the cover files format or appearance should be completed. It is impossible to utilize all the files or information or files covered with data of steganographic system since every file should contain appropriate terminated space for replacing the secret hidden message. A huge number of files exist that might be utilized as steganographic cover files i.e. files to be executed, files of HTML, XML and TCP headers. Fundamentally, large types of digital files such as audio, text, video, and image might be utilized as steganographic cover files.

Though, such files ability is dependent on the secret data embedding and the available redundant space in these files. Additionally, the hidden data container is represented by the cover files and

their size might determine the size of secret data that are to be embedded. Finally, it can be said that the fundamental components of a steganography based system are the cover files. Although, the discussion about the cover files relationship with the major steganographic components will be done in the next section. As there are many types of digital media might be utilized for steganographic cover files. The initial classification method is to break down the steganography based on used cover file type. Thus, these cover files attributes change from one to another type and such attributes control how the secret information can be kept hide in these cover files. (Cole, 2003).

Generally, the classification of steganography based systems is based on cover file utilized. Consequently, there are various distinguished types of steganography such as text, HTML, audio, and video, etc. For instance, in image-based steganography, the cover files used are the digital images.

There are four types of steganography based on the cover medium type:

- Text Steganography: cover medium is a text file.
- Audio Steganography: cover medium is an audio file.
- Video Steganography: cover medium is a video file.
- Image Steganography: cover medium is a digital image.

There are different types of the cover medium that can be used such as image, audio, video and text. The digital images are the most famous among them due to their easy availability on internet. The images have many redundant pixels that are used for hiding the secret messages. Secondly human eye has a limited capability to detect minor changes in images. Thus, the cover image degradation cannot be detected by naked eye after the bits of secret message are embedded.

2.3.1.1 Image Steganography

When image is used as a cover medium, this type of steganography is identified as Image steganography. In this method, secret information is concealed in cover image by modifying the cover image pixels. As images contains large number of bits, so the hiding capacity in images is large, hence Images are considered as best cover mediums.

2.3.1.2 Text Steganography

When Text is used as a cover medium, this type of steganography is known as Text steganography. Normally in this method, secret data is hidden letters of the cover texts. As there is less redundancy in text so text steganography is more difficult as compared to other types of steganography techniques. Therefore, the hiding capacity is less in text steganography. Text steganography is used where less memory is required for communications.

2.3.1.3 Audio Steganography

When audio files are used as cover mediums, this type of steganography is called Audio Steganography. Due to modern day trends of voice over IP, audio steganography is considered an important type of steganographic technique. Here are different types of audio setups that are used for audio steganography. Some of the formats used are MPEG, MIDI, WAVE and AVI.

2.3.1.4 Video Steganography

When data is hidden in video, such type of steganography is known as Video steganography. When large volume of data is required to be hidden then video steganography is most suitable technique. Due to combinations of frames and images, large number of redundant bits are available. There are different types of video set-ups that are used for video steganography. Some of the formats used are H.264, Mp4 and MPEG.

2.3.2 Hiding Method-Based Classification

This type of classification is based on hiding method. The cover medium in this case does not matters. The only factor that matters is hiding method. This is furthermost preferred and communal kind of steganographic method used now a day. Consequently, three different types of approaches are utilized for hiding the secret information in in cover mediums. These three types are discussed below:

2.3.2.1 Insertion-Based Method

Such type of system is dependent on after getting a couple runs in archives of cover that are usually unnoticed by applications for reading such cover file and a short time later implanting the

puzzle information in such locations. As the system implants the hidden information within the cover file, the measure of the stego report would be greater as compared to degree of the cover file. Thusly, the standard favored viewpoint of this methodology is that the substance of the cover file will not be varied afterward the implanting strategy because such type of procedure depends on social affair or secret information is added to the cover file.

A word document is an example of this method for making a riddle text in the regions among the end-substance and start content indicators. Considering the setup of word reports that is dependent on after dismissing everything printed in such domains, the covered text won't show up when this record is found in Word.

2.3.2.2 Substitution-Based Method

Not at all like the method of intrusion, the substitution based approach is not added mystery data to information of cover file. Be that as it may, substitution-construct technique depends considering discovering some inconsequential locales or data in cover documents and supplanting this data with the mystery information. Along these lines, both the stego document sizes and the cover record are comparative because a portion of the cover information is recently altered or supplanted with no extra information. Be that as it may, the nature of the cover record can be corrupted after the inserting procedure. Moreover, the constrained measure of irrelevant data in cover documents limits the span of mystery information that can be covered up.

2.3.2.3 Generation-Based Method

Not at all like both strategies clarified over, this technique does not require a cover document since it utilizes mystery information to produce suitable stego records. One of the steganography discovery systems relies on upon contrasting spread documents and their stego records. Thusly, one favorable position of steganography based on generation method is counteracting this sort of location since just stego documents are accessible and none of the cover files are utilized. The significant constraint of such technique is the restricted stego documents that could be created. Also, the produced stego records may be farfetched documents for end clients (e.g. a picture holds diverse shapes and hues with no sense or a content with no significance). Along these lines, the fundamental channel for these strategies are arbitrary observing pictures and English content documents.

2.4 Steganography Techniques

Notwithstanding the general strategies for data covering up exhibited above, numerous steganography methods have been proposed amid the most recent couple of years. These procedures vary in the instrument or standard being utilized to conceal a mystery message or the progressions that are occurring amid the whole procedure of implanting. In this way, there are six classifications of steganography strategies: substitution frameworks, change area procedures, spread range systems, factual techniques, contortion methods, and cover era.

2.4.1 Substitution Systems

For a specified cover record, it is vital to discover a few ranges or information that can be adjusted without having any huge impacts on this cover document. In this way, a mystery text could be inserted through supplanting the excess or unimportant sections of a cover record by means of bits of secret text, lacking addition of any critical clamor to such a cover document.

Computerized covers contain numerous excess bits (e.g. slightest critical bits (LSB)). In the substitution system of steganography, the bits of the mystery message substitute the LSB of the bytes of the cover record without making a radical change this cover document. Also, the LSB method is a spatial area system since it installs the mystery bits straightforwardly in the cover document. Since LSB substitution procedure is generally speedy and simple to utilize, it is the most well-known method utilized for advanced steganography and particularly with computerized pictures. Be that as it may, the inserted data utilizing the LSB strategy is very powerless and could be demolished altogether by applying a slight adjustment to the stego picture, for example, JPEG pressure.

2.4.2 Techniques Based on Domain Transformation

Transfer domain techniques conceal secret data in cover file within significant parts unlike spatial domain technique. Therefore, compare to spatial domain techniques, transform domain techniques are more robust to threats. Hence, today mostly frequency domain techniques re utilized in stenographic system. Many transform techniques are available to map signal in

frequency domain like Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT). However, the whole image rather some part of image is changed when we add a secret data or a noise to components of frequency domain. Thus, spreading of embedded and secret data will be across entire images and are not concentrated to any region or area.

2.4.3 Techniques Based on Spread Spectrum

Wonder et al. characterize techniques of spread spectrum as" the way toward scattering the data transfer capacity of a narrowband motion over a wider frequency bands". In steganography based on spread spectrum, the recurrence space of the cover document is a correspondence medium and the secret text as a flag being across it. As the secret text is spread across a wider recurrence band, such a system is generally powerful against stego record change or text expulsion

2.4.4 Statistical Techniques

In such approaches, only a single bit is embedded in cover file thus known as “1-bit steganographic scheme”. Statistical characteristics must be changed significantly if “1” is concealed in cover file to clearly indicate message existence. However, cover file is unmodified in case “0” is a hidden bit. Therefore, receiver ability to differentiate between intact and changed cover file is a key factor for this technique to be functional.

2.4.5 Distortion Techniques

Steganography is a mostly blind technique i.e. receiver does not require to have unique cover file to excerpt the concealed text from relative stenographic file. Though, for techniques based on distortion, actual cover file is needed by receiver for extraction of secret text. For receiver, the difference between original cover file and received modified cover file is an embedded message.

2.4.6 Techniques of Cover Generation

All above mentioned techniques of steganography required cover files as a container to extract secret data. Stenographic file is created by cover generation techniques to hide information and not required any cover file.

2.5 Techniques Of Network Steganography

Steganography and information hiding main goal is to have hidden communication. So, aim of steganography is to ensure secret, secure and simple way of communication among personal. Hiding data in file is good procedure but the key idea behind steganography is to be able to transmit that secret data or text to others on internet or network. There are four different kinds of network-based information hiding techniques available which are as follow.

2.5.1 Attachment Based Information Hiding

This approach basically represents the most recurrent method of information hiding approaches. Typically, secret message is hide in cover file using different steganography methods. Then, this stego file would be joined to few additional shape of system traffic. Though, three methods are available for doing this, through posting a stego file over website, by email, or by file transfer.

2.5.2 Transmission Based Information Hiding

Methods that have been describe up to now, we wanted either one method, tool, or program to conceal secret message within cover file. Then to transfer that stego file to intended recipient we needed another program. Therefore, an email and steganography program is required to send our secret message. Though, the method which hide our secret info in cover file and transmit that stego file using only single program is called information hiding in transmission. Therefore, a built-in transfer feature is available in this type of steganography techniques that enables the transmission of stego files to other communications party.

2.5.3 Network Headers Based Information Hiding

The major data in networks needed for routing the packets of information in a proper way is included in the header of Internet Protocol (IP). Also, the use of steganographic approach needs few unimportant or redundant components or fields in the cover file that might be altered or

replaced without any effect on communication. There are many fields in the network headers that are either selective or unutilized for usual communication.

There is only one field in the IP header known as the identification number of IP header that might be changed deprived of any impact on its working. Thus, any number can be put as an identification number of IP and protocol will still work in a proper way. Thus, a better possible steganographic candidate is represented by the IP headers.

Moreover, the headers of transmission control protocol (TCP) contain an acknowledgement and sequence of numbers utilized for effective transmission. The amount of data sent is represented by the first number and the second number shows the amount of data reception. Though, the two numbers value are generated in a random manner during the first handshaking process. So, these fields can hide the secret data for the first packet only, since they cannot be used after the communication establishment.

2.5.4 Overt Protocol Based Information Hiding

This steganographic method is based on, the presence, form or secret information format is changed or attuned for making this data looks like an overt protocol. So, we can put this data in normal network traffic deprived of appealing any doubt. Typically, traffic of Web holds HTML. Thus, we can add symbols such as < > </> to the secret data to make this data looks like normal Web traffic. Fundamentally, the method of forming data of other type of similar look is known as camouflaging of data.

The protocol used for transferring the data over Web is known as simple object access protocol (SOAP) is a data transfer protocol over the Web. Moreover, SOAP shows a protocol of communication among users and web facilities. As this investigation examines the information hiding approaches in the protocols of communication, we enlighten and discourse the SOAP basics of messages in the upcoming section.

Chapter 3

Proposed Method

3.1. Introduction

Many steganographic techniques have been implemented in the past. Most of these techniques use single cover image to hide the secret data. This secret data can be a text message or it can be an image file. Similarly, many cover files have been used, this includes images, video, audio and text files. Some of these methods use different encoding algorithms to improve the security but still most of the encryption schemes has been decoded successfully. Secondly the embed the secret message using LSB substitution method. In Least Significant Bit substitution technique, Least Significant Bits of cover images is substituted by secret message bits. Hence successfully inserting the secret data into cover file and then transmit it on a digital channel. Now we will discuss in detail our proposed algorithm.

Our Proposed algorithm consists of two cover images. It can be extended to n cover images. The basic concept of our proposed algorithm is that we divide our secret image into mainly two parts. This depend on the number of cover images used. If we are using n cover images, then accordingly we divided our secret image in maximum n parts. As we will be dividing our secret image into multiple parts so size of the secret image dose not matters. This also shows the increases capacity to hide secret messages and decrease in the probability of finding hidden pixels. Also this will improve the security of our secret image. If attacker becomes successful in cracking the hidden secret data, it will be of no use for him as it looks like a raw data for him. It will be only useful if second part of secret image is cracked. Even still the sequence number matters. We will store a sequence number in any random pixel of cover image. This sequence number will help to rearrange the pixels and recover the secret image fully. This sequence number and its location will be shared with both parties.

Throughout the article, following subscriptions will be used,

- s represents our Secret image with $s_{i,j}$ on behalf of the corresponding pixel at position (i, j) of that image.
- c_n Represents our Cover images with $c_{i,j}$ representing the pixel at location (i, j) of that image. In Our case n =2 so we have two cover images c_1 andc_2.
- s_1 And s_2 represents two different parts of Secret image.
- $Stego_1$ Represents our first stego image.
- $Stego_2$ Represents our second stego image.
- r_1 is image extracted from $Stego_1$ at receiver end.
- r_2 is image extracted from $Stego_2$ at receiver end.
- r Represents recovered image.

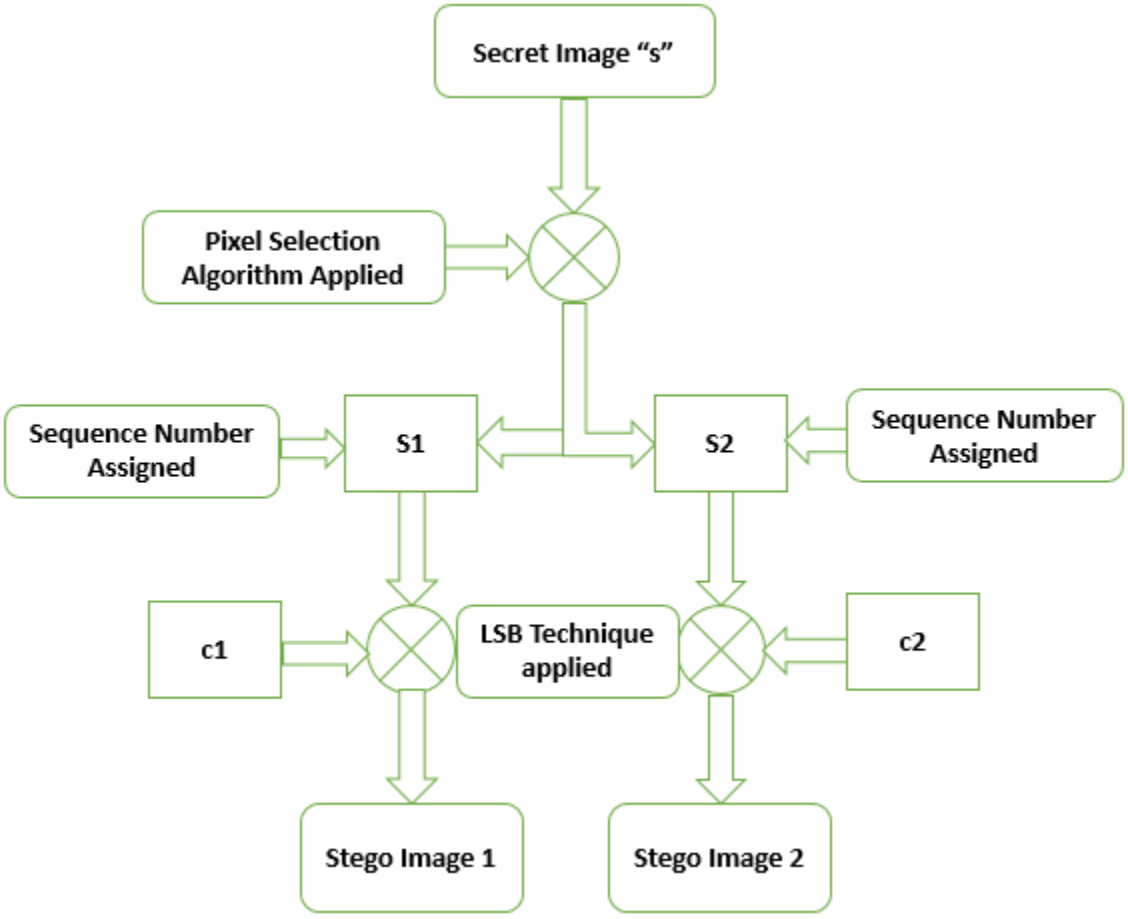


Figure 3.1 Flow Chart of Algorithm

3.2. Encoding Algorithm

Now we will discuss our proposed Encoding algorithm in detail. In general, two cover images are used as input. Our secret image is divided into two random parts and each part is embedded into each cover image. This gives two stego images at output which are then transmitted on a digital channel which is insecure.

Input: Two cover images c_1 and c_2 of size m x n, A secret image *s* of size m x n.

Output: Two stego images $Stego_1$ and $Stego_2$ of size m x n.

3.2.1 Pixel Selection algorithm:

Following are the steps involved in encoding phase. First, divide your secret image into two parts $s_1$and s_2 using pixel selection algorithm. After that these two parts are then hidden in cover images respectively. Pixel selection algorithm is explained below. We have a secret image "s" of dimension 256 x 256.We divide our image into 64 equal blocks and each of these blocks consists of 32 x 32 pixels.

B1	B2	B3	B4	B5	B6	B7	B8
B9	B10	B11	B12	B13	B14	B15	B16
B17	B18	B19	B20	B21	B22	B23	B24
B25	B26	B27	B28	B29	B30	B31	B32
B33	B34	B35	B36	B37	B38	B39	B40
B41	B42	B43	B44	B45	B46	B47	B48
B49	B50	B51	B52	B53	B54	B55	B56
B57	B58	B59	B60	B61	B62	B63	B64

We generate a random series with initial value equals to 1 and final value equals to 64. We have eight different sequences which will be applied to these 64 blocks. Lets say A1=23 is the first random number generated in the series. A1 corresponds to block number 23. Now the first sequence will be applied to block number A1=23. Next sequence two will be applied on A2. Lets say A2 is 59. This will be repeated until A64 In this way all of the blocks will be covered and sequence numbers will be applied on all blocks in a random way. We have use multiple sequences and these sequences are applied based on random number generator. Hence, a factor

of “Randomness” is introduced. Below figure shows that all these 8 sequences are applied to 64 blocks randomly. Each sequence is shown by a unique color.

Sq 6	Sq 2	Sq 1	Sq 5	Sq 4	Sq 2	Sq 8	Sq 3
Sq 4	Sq 6	Sq 4	Sq 7	Sq 8	Sq 7	Sq 2	Sq 5
Sq 2	Sq 7	Sq 6	Sq 3	Sq 7	Sq 1	Sq 5	Sq 4
Sq 8	Sq 4	Sq 3	Sq 6	Sq 2	Sq 3	Sq 7	Sq 1
Sq 7	Sq 5	Sq 2	Sq 1	Sq 6	Sq 4	Sq 6	Sq 3
Sq 1	Sq 8	Sq 5	Sq 8	Sq 1	Sq 8	Sq 3	Sq 7
Sq 5	Sq 1	Sq 7	Sq 4	Sq 3	Sq 5	Sq 1	Sq 6
Sq 3	Sq 8	Sq 2	Sq 3	Sq 5	Sq 6	Sq 4	Sq 2

The complete process is depicted in below mentioned block diagram.

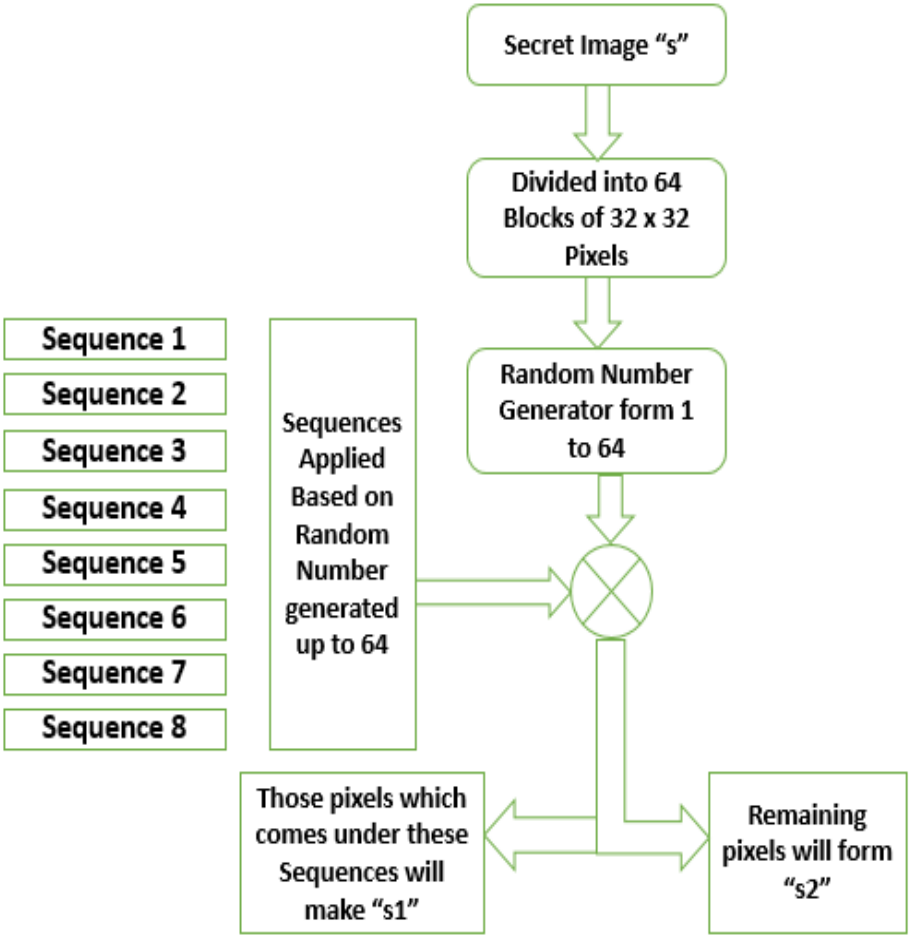


Figure 3.2 Pixel selection algorithm Flow Chart

3.2.2 Embedding Process:

Given below is a sample image, which consist of 9 pixels in total. This is used to illustrate our proposed methodology. Our proposed method will work for any images of any dimension m x n in the same way as it works for below mentioned pixels.

Table 3.1 - A 3 × 3 sample block of the secret image *s*

10101101	11001001	10001101
10100101	11011011	11001010
11010100	11110101	11100111

Table 2 shows randomly picked pixels by our pixel selection algorithm; remaining pixels are shown by zero as these pixels are not selected.

Table 3.2 - s_1 random pixels picked from s

10101101	00000000	00000000
10100101	00000000	11001010
00000000	11110101	00000000

We make LSB, s of s1 equal to zero as show in table 3 and move MSB bit four units rightward. The remaining pixels will not be changed. This is shown below

Table 3.3 - s_1 random pixels picked from s

00001010	00000000	00000000
00001010	00000000	00001100
00000000	00001111	00000000

Now this is our first part of secret image which is ready for the embedding process. Now these pixels' wills be embedded into first cover image. The secret bits will sit on LSB, s of cover

image 1. As remaining pixels are 0, so they will have no effect on the cover image. Hence this will help in maintain the quality of our cover image.

As we have find the first part of secret image, the second part is find by simply subtracting first part from original secret image. The number of pixels in s1 and s2 are almost equal hence sharing the load equally. The remaining pixels form second part of secret image s_2.

$$s_2 = s - s_1$$

In this way, we get two images with pixels located at random places instead of simple sequence. This randomness will improve the security of our secret message. As it will be more difficult for the attacker to pick those random pixels. Even if attacker successfully cracked those random pixels, it will be of no use for him. The attacker gets only half of the information and that too is in random form. Finding both parts of secret image and then integrating those parts will be a tough job for the attackers. As we have distributed our image in two separate parts and each part is hidden in a separate image. Both stego images will be transmitted separately so there is a less chance, that attacker gets the both stego images.

Same steps will be repeated for cover image 1 by deploying same pixel selection algorithm , pixels will be generated in cover image 1. Show below in table 4 is a sample cover image c1.

Table 4. A 3 × 3 sample block of the First cover image c_1

11010101	11010101	10101101
11101010	11010111	10111000
10101010	11001100	10011001

Now random pixels from cover image c1 will be picked using same method as used for secret image. Table 5 shows those randomly picked pixels. The pixel locations are same as in secret image part 1 that is s1. Now s1 pixels will be directly embedded in these locations without disturbing remaining pixels. This will help in maintaining the quality of cover image c1. If the quality remains intact, there will be no degradation in image. Nobody will doubt that there is something hidden in this simple image. If looked with the naked eye, no difference between stego image and original image is observed. So, the chances for the attackers are dim.

Table 5. Random picked pixels from First cover image c_1'

11010101	00000000	00000000
11101010	00000000	10111000
00000000	11001100	00000000

The LSB, s of cover image is made zero so that it can embed bits of secret image part 1 s1.this is shown below in Table 6. This group of pixels is represented by c_{11}'. Following equation is used for making LSB, s zero.

$$c_{11}' = c_1' \% 2^4$$

Table 6. c_{11}' Making LSB, s of c_1=0

1101<u>0000</u>	00000000	00000000
1110<u>0000</u>	00000000	1011<u>0000</u>
00000000	1100<u>0000</u>	00000000

Now We Will Find pixels' locations other than random Pixels. This is done by subtracting random pixels from original cover image c1. By performing subtraction operation, we will get the remaining pixels. Table 7 shows pixels other than random. Following equation is used for this purpose. Where c_1 shows original cover image.1

$$t_1 = c_1 - c_1'$$

Table 7. t_1-Remaining Pixels

00000000	11010101	10101101
00000000	11010111	00000000
10101010	00000000	10011001

Now we will Concatenate $t_1$with c_{11}' . this will form our final cover image c1 which will embed secret message. Only random pixels have been modified to embed the secret data as can be seen in table 8. All the remaining pixels are preserved as it is. This will result in less degradation of

cover image. It will embed the secret data more efficiently. Following equation shows concatenation operation.

$$co_1 = t_1 + c'_{11}$$

Table 8. co_1-Final cover image

11010000	11010101	10101101
11100000	11010111	10110000
10101010	11000000	10011001

co_1 is our final cover image 1 co_1. In co_1 LSB, s of random pixels is zero and remaining pixels have retained original value with no change. co_1 is calculated in such a way that it will be helpful in maintaining the quality of cover image intact and it reduces the degradation in cover image. This whole process is repeated P times.

Now we will embed s_1 into cover image co_1 using LSB insertion technique. Now $Stego_1$ is ready to be transmitted. This stego image will be transmitted digitally. The equation is given below. S1 is our secret image where as co1 is our modified cover image. $Stego_1$ is our image which will be transmitted over a digital channel.

$$Stego_1 = co_1 + s_1$$

Same process will be repeated with cover image 2. First, we will find random pixels. Then we will make LSB, s of the random pixels equals to zero. After That remaining pixels will be calculated. Final cover image will be calculated by adding both the images. After that we will embed the remaining part of secret image $s_2$into cover image 2. This is shown by below mentioned equation. Stego 2 will be our final image ready to be transmitted over a digital channel. Where as co_2 is our second secret image.

$$Stego_2 = co_2 + s_2$$

Assign a Sequence number in k_{th} pixel of the stego images. Assign 01 for sequence number 1 and 10 for sequence number 2.

3.3. Decoding Algorithm:

Now we will discuss our proposed decoding algorithm step by step. At receiver end we will receive two images. One is $Stego_1$ and other is $Stego_2$. Both images will be decoded and

relevant information is extracted. After processing this information and identifying labels, we will receive the original secret image.

Input: Two Stego images $Stego_1$ and $Stego_2$ of size m x n.

Output: Recovered secret image *s* of size m x n.

Steps

- At receiver end, we will receive two images $Stego_1$ and $Stego_2$. These are the images which contain information and date of our secret image.
- Now we will Extract Label/sequence number from k_{th} pixel. The k_{th} pixel will be communicated by transmitting party to the receiving party. This sequence number tells us about arrangement of decoded images. This will tell us the sequence in which this extracted data will be combined.
- Using same random pixels algorithm developed during encoding process, we will extract pixels at random locations from $Stego_1$ These random pixels will be stored in r_1. Our data is placed in LSB positions. So, we will extract the bits at LSB positions. Then shift them to MSB Positions. Same process will be applied on $Stego_2$.Data will have extracted from stego 2. These pixels will be stored in r_2. Move relevant data from LSB to MSB. Concatenate r_1 and r_2. This will be our recovered image. This is expressed by equation given below.

$$r = r_1 + r_2$$

Chapter 4

Simulations and Results

4.1 Introduction

Digital images are quickly discovering their way into our everyday lives due to the explosion of info in the form of visual signals. These images frequently pass through numerous processing phases before they grasp to their destination. In most of the scenarios, these end-users are human viewers. After passing through variety of processing phases, for example, acquisition, compression, and transmission, images are exposed to various types of alterations, which damages the quality of them. For illustration, in image compression, lossy compression methods introduce blurring and ringing properties, which results in to quality degradation. Furthermore, in the transmission phase, due to inadequate bandwidth of the communication channels, some information might be loosed, due to which quality of received image is degraded. To preserve, control, and improve the quality of images, it is important for image communication, organization, acquisition, and processing systems to estimate the quality of images at each phase. The performance of a steganographic technique can be rated by following techniques.

- Visual Inspection
- PSNR
- Structural Similarity Index (SSIM)
- Statistical Analysis
- Mean Opinion score MOS

4.2 Visual Inspection

Visual inspection is one of the methods to evaluate an image steganographic technique. By visual inspection, we mean finding difference between two images with humane eye. As for our proposed technique is concerned, by naked eye no one can differentiate between original cover images and stego images.

The stego-images should be imperceptible, means the distortion should not be noticeable. If the distortion is less in stego-images, it means that they are closer to original images. Hence it will be more difficult to extract the hidden data from stego-image, thus increasing the security perspective. The distortion between two images is calculated by MSE and PSNR.

4.3 PSNR

Relating restoration outcomes needs a measure of image quality. Two frequently used procedures are Mean-Squared Error and Peak Signal-to-Noise Ratio. The major problem that exists with mean-squared error is that it is dependent on the intensity scaling of an image. A MSE of 100 for an eight-bit image with pixel values lying between 0 and 255 looks terrible, but a MSE of 100 for a ten-bit image pixel values lying between 0 and 1023 is hardly visible. Peak Signal-to-Noise Ratio (PSNR) evades this issue by scaling the Mean Square Error for the image range.

Peak signal-to-noise ratio (PSNR) can be defined as the ratio between the maximum power level of a signal and the power of noise signal which degrades the quality of an image. Noise is the signal which affects the quality of an image. Because there is a wide gap between the largest value of power and smallest value of power in a signal, so PSNR is usually expressed in terms of logarithmic decibel scale.

Improving the visual quality of an image can be considered as a subjective goal. The visual quality of an image varies from person to person. For some, a certain method provides a better quality of an image. But for others it may not be true. Therefore, there should be some evaluation parameters based on which we can decide which method is most effective and which one is not.

we use same set of test images to compare the performance of different algorithms. This will be helpful in identifying which algorithm performs better and which one did not. The parameter that can be used is peak-signal-to-noise ratio. Based on peak-signal-to-noise ratio, if a certain algorithm performs well, and its image quality is not degraded then we can say that it is a better algorithm as compared to others.

Peak signal-to-noise ratio calculates the PSNR in decibels, amongst reference image and compressed image. This ratio is frequently used as a quality evaluation between the two images. The quality of the image depends on the value of PSNR. higher the value of PSNR, better the quality of compressed image.

Mean Square Error and the Peak Signal to Noise Ratio are the two evaluation parameters that are used to compare image quality. The Mean Square Error represents the collective squared error amongst the compressed and the original reference image. On the other hand, Peak Signal to Noise Ratio characterizes a degree of the peak error. The error will be less if the value of Mean Square Error is small.

4.3.1. Mathematics

Now we will discuss mathematical calculations of PSNR and MSE. The size of the original image matrix and the size of the degraded image matrix must be equal. To compute the PSNR, the block first calculates the mean-squared error using the following equation. where the MSE (Mean Squared Error) is:

$$MSE = \frac{1}{M\ x\ N} \sum_{i=1}^{M} \sum_{j=1}^{N} (c_{1\ i,j} - Stego_{1\ i,j})$$

In the previous equation, M and N are the number of rows and columns in the input images, respectively. The mathematical representation of the PSNR is as follows:

$$PSNR = 10 \times log \frac{255^2}{MSE}$$

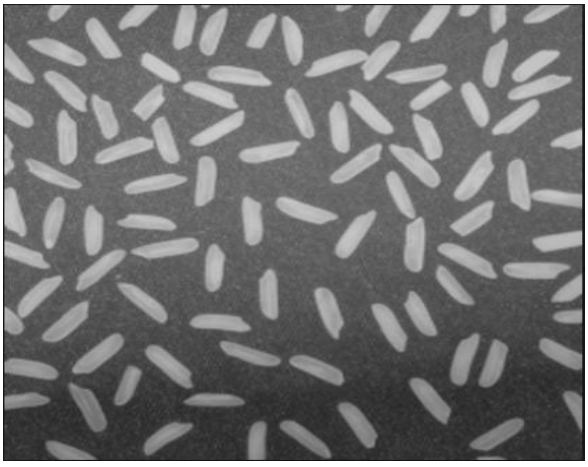
4.3.2 Test images

For assessment of our technique four sets of ordinary test images are used. These set of ordinary test images are shown below.

c) Gold hill

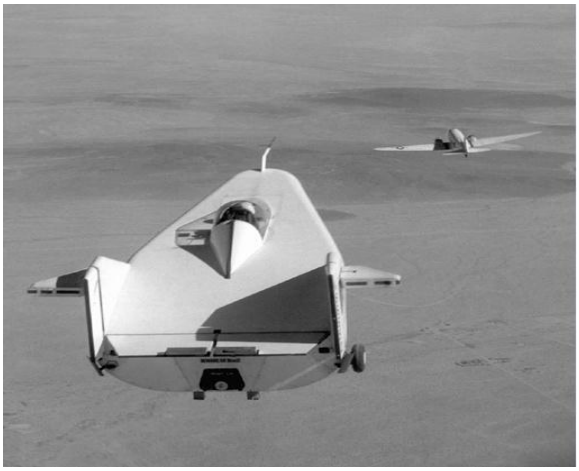
d) Barbara

e) Mandi



f) Rice

g) Cameraman



h) Lifting Body

Figure 4.1 Different type of Test Images used

4.3.3 PSNR Results

In this Segment, we are going to show some experimental results. This will show the effectiveness of our proposed methodology. We have performed several experiments using different cover images. PSNR indicates difference between two images. If PSNR is smaller, it means difference between two images is greater. On the other hand, if PSNR is high, it shows greater similarity between two images. Having high values of PSNR, it is impossible to differentiate between two images with naked eye. PSNR values for different combination of cover images are shown in Table 9. The PSNR values as well as the visual appearance of the stego images shown in Fig. 4 and Fig 5 suggests that the distortion level in our stego image is very less and insensitivity to human eye. Our method improves the security of our secret message. As we have picked the random pixels, so it will be difficult for attacker to find exact location. By dividing your secret image in two parts and using more than one cover images, helped in making your data more secure. Secondly most of the cover image is intact in its original form, as we have only altered those pixels value at which random secret pixels has to be embedded. This helps in maintaining the quality of cover image and achieving good PSNR values.

The secret image is also of 256 x 256 as shown in fig 1. We have chosen “cameraman.png” as our secret image. This secret image is divided into two parts by using our random sequence generator. Then each part is embedded into two cover images respectively. The secret image

remains same in all the experiments whereas cover images have been changed in every experiment.

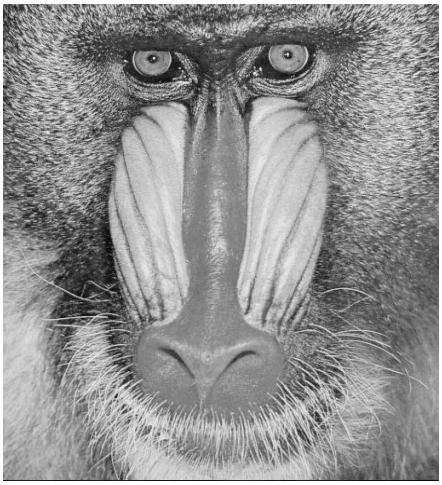


Figure 4.2 Secret Image s

We are showing results for some of the cover images used. We have used 256 x 256 (m x n) cover images. Figure 2 shows cover image 1. We have chosen “goldhill.png” as our first cover image. Figure 3 shows cover image 2. We have chosen “mountain.png” as our second cover image.

Figure 4.3 First cover image c_1

Figure 4.4 Second cover image c_2

As explained in previous chapter, secret image will be divided into two parts. Then each part will be embedded into one of the cover images at random locations. This randomness

will be helpful in keeping the data secure. Hence making our system more robust. The output after embedding will be transmitted digitally over an unsecured channel. These outputs encoded images will be known as Stego images. The stego images $Stego_1$and $Stego_2$ generated by encoding secret image are shown in Fig 4 and Fig 5 respectively. The indicators for the effectiveness are peak-signal-to-noise ratio (PSNR) and visual quality of stego images.

Figure 4.5 First Stego image $Stego_1$

Figure 4.6 Second Stego Image $Stego_2$

By seeing those stego images, no one can judge that some secret data is hidden. As there is no visible difference between original cover images and stego images. These stego images contains our secret data. These will be transmitted digitally. At receiver end, these stego images will be received and further processed to extract our original data. Firstly, we will extract the secret sequence key from the predefined pixel location. This pixel location will be communicated by the transmitting party to the receiving party. This key will help in arranging the data in sequence. First we will decode the stego image 1. The information extracted will be stored. Then stego image 2 will be decoded and secret data is extracted. Then we will combine these two set of information's. The resultant will be our secret image. Hence secret data is successfully extracted at the receiver end.

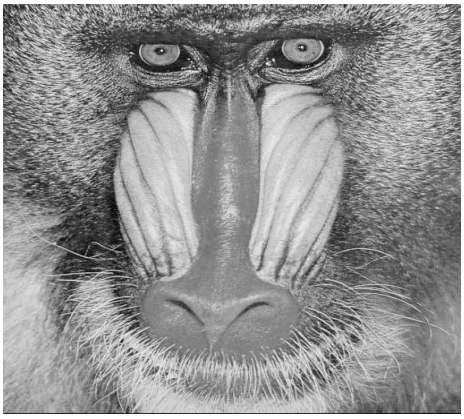


Figure 4.7 Recovered secret image at receiver end

In table 9, PSNR values are shown against different cover images. Secret image will be same for all these experiments. The first and second Column shows first and second cover images respectively. All the cover images are of size 256 x 256. In last two columns, PSNR values for stego images is shown.

Table 9. PSNR for different pair of cover images

Sr. No	Secret Image	Cover Image C1	Cover Image C2	PSNR Stego 1	PSNR Stego 2
1	Liftingbody	Moon	concordorthophoto	45.44	42.33
2	Baboon	Goldhill	Barbara	42.01	40.68
3	Cameraman	Rice	Mandi	38.23	37.41
4	Lena	Cameraman	Liftingbody	37.81	36.88

PSNR values for our results shows the effectiveness of our algorithm. The greater the PSNR value, the better the image quality. Higher value of PSNR shows less degradation in original image. So, it will be less doubtful. With naked eye the degradations are hard to identify. It will be more difficult for the attacker to crack the stego image. As the pixels are located at random locations find by our algorithm. So, first it will be impossible for the attacker to find those random locations. Even if in worst case scenario, he finds those locations and extract the data. This will be of no use for him, as it is only one part of the data. He must find the second part and then aligned them in a sequence to reconstruct the secret message. This shows that our data is more secure in this way.

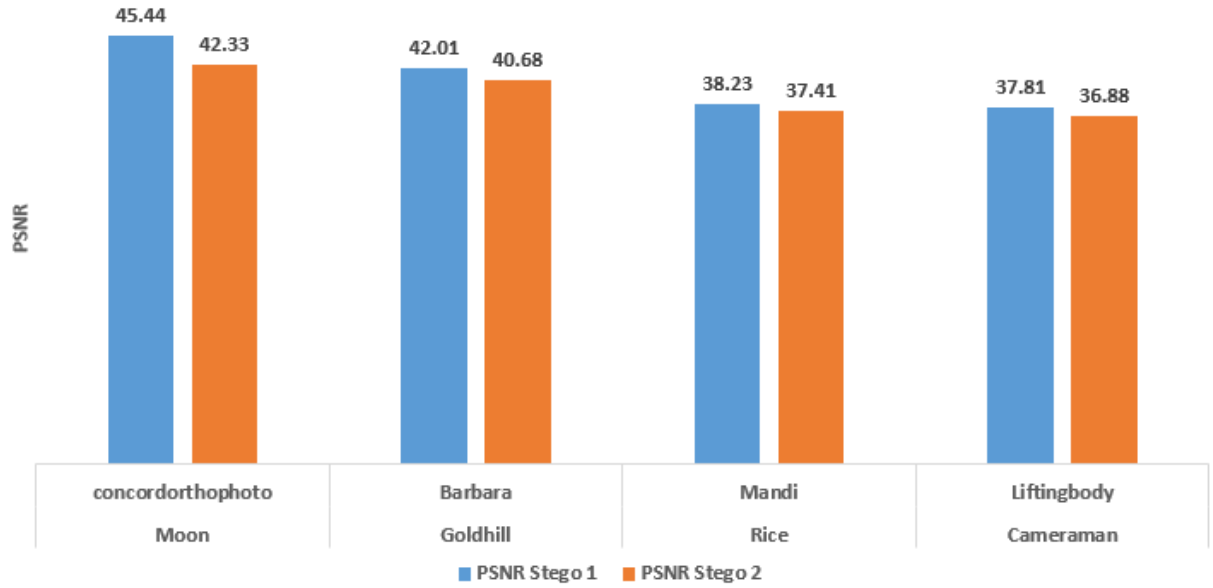


Figure 4.8 PSNR Graph for different cover image combinations

4.3.4 Percentage of Data hidden in each Cover Image:

In table given below, we have defined the percentage of data that is hidden in each cover image respectively.

Table 10. Percentage data hidden in each cover image

Sr. No	Secret Image	Cover Image C1	Cover Image C2	% of secret date hidden in c1	% of secret date hidden in c2
1	Liftingbody	Moon	concordorthophoto	47.70%	52.30%
2	Baboon	Goldhill	Barbara	47.70%	52.30%
3	Cameraman	Rice	Mandi	47.70%	52.30%
4	Lena	Cameraman	Liftingbody	47.70%	52.30%

The table clearly shows that the amount of data hidden in each cover image is almost equal.

4.3.5 Stego Images

In this section, we will show the stego images obtained by using different cover images. As can be seen, visually no one can feel any difference from original cover images.

4.3.5.1 Goldhill and Barbara

The cover images used are “Goldhill” and “barbara “. The first image is stego image 1 obtained by hiding secret data in cover image 1. Similarly, second stego obtaining by hiding secret data in cover image 2. The PSNR value for stego image 1 is 42.69 and for stego image 2 is 40.02. These PSNR values shows that quality of our images is high. Hence it is difficult for attacker to be suspicious.

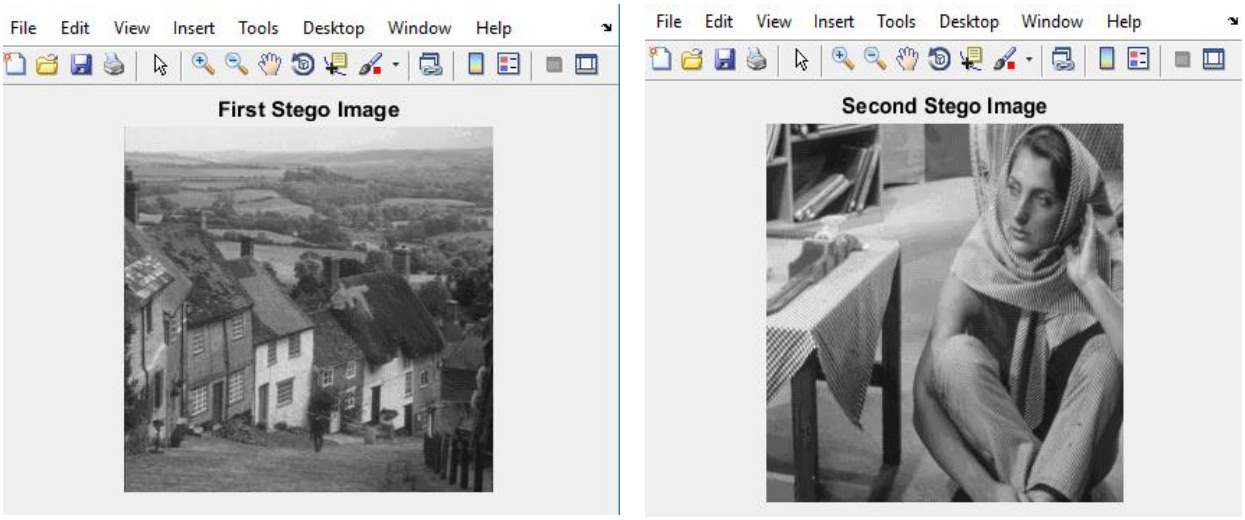


Figure 4.9 Stego images Goldhill and Barbara

4.3.5.2 Concordorthophoto and Moon

The cover images used are concordorthophoto and moon. The first image is stego image 1 obtained by hiding secret data in cover image 1. Similarly, second stego obtaining by hiding secret data in cover image 2. The PSNR value for stego image 1 is 45.27 and for stego image 2 is 42.33. These PSNR values shows that quality of our images is high. Hence it is difficult for attacker to be suspicious.

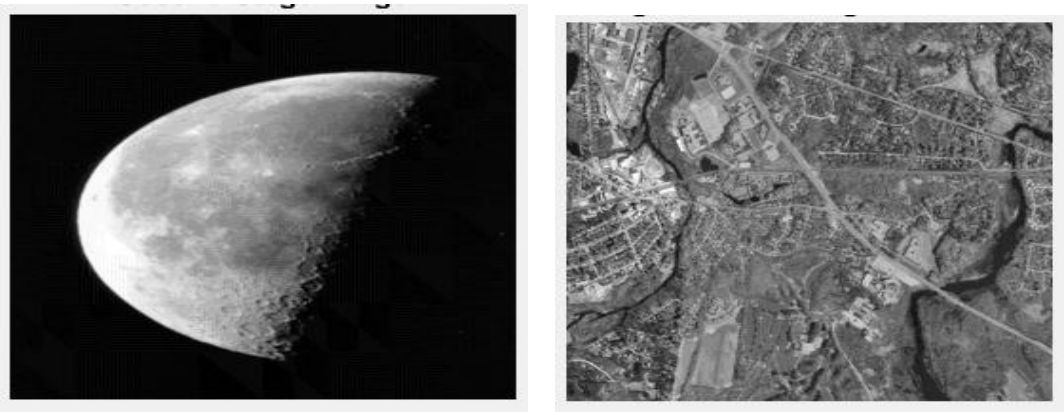


Figure 4.10 Stego images Moon and concordorthophoto

4.3.5.3 Rice and Mandi

The cover images used are Rica and Mandi. The first image is stego image 1 obtained by hiding secret data in cover image 1. Similarly, second stego obtaining by hiding secret data in cover image 2. The PSNR value for stego image 1 is 38.27 and for stego image 2 is 37.60. These PSNR values shows that quality of our images is high. Hence it is difficult for attacker to be suspicious.

Figure 4.11 Stego images Rice and Mandi

4.4 Statistical Analysis:

By observing the results that are assembled in table 11 and table 12, we can clearly observe that original image and stego images are nearly similar to each other. Hence, it shows that our technique is very efficient. The most important factor is that when stego image is identical to original image, an attacker cannot attack using statistical attacks. This is due to the fact that steganographic image and original image has almost same statistical properties, which is clearly evident from table 11 and table 12. Table 11 show statistical values for cover image one and stego image 1. Similarly, Table 12 show statistical values for cover image 2 and stego image 2.

Correlation: Shows similarity between original image and stego image. For our proposed work, we have perform correlation between original and stego image.

Information entropy: Information entropy is a vastly used parameter which shows randomness of the data. Claude E. Shanon in 1949 has introduced the concept of information entropy. Entropy values for different pairs of cover images and stego images is given in Table 11 and table 12.

Homogeneity: The homogeneity analysis is a metric that returns a value, for determining the closeness of the distribution of element.

Contrast: Contrast is another parameter of statics analysis. It returns an intensity value between two adjacent pixels. This parameter helps to better recognize an image.

Energy: This analysis is used to calculate the energy in images. In below given table, energy of an image is calculated before embedding and after embedding.

Table 11. Statistical analysis of cover and stego image 1

Statistical Analysis	Image	Original Cover Image C1	Steganographic Image Stego 1
Entropy	Moon	5.4294	5.508
	Goldhill	7.4448	7.3321
	Rice	7.0115	6.8267
	Cameraman	7.0097	7.0843
Correlation	Moon	0.9712	0.9712
	Goldhill	0.8995	0.8995
	Rice	0.8364	0.8364
	Cameraman	0.9005	0.9005

Homogeneity	**Moon**	0.9469	0.9469
	Goldhill	0.8223	0.8223
	Rice	0.8418	0.8418
	Cameraman	0.8672	0.8672
Contrast	**Moon**	0.2999	0.2999
	Goldhill	0.494	0.494
	Rice	0.5969	0.5969
	Cameraman	0.7565	0.7565
Energy	**Moon**	0.4588	0.4588
	Goldhill	0.0957	0.0957
	Rice	0.1402	0.1402
	Cameraman	0.1686	0.1686

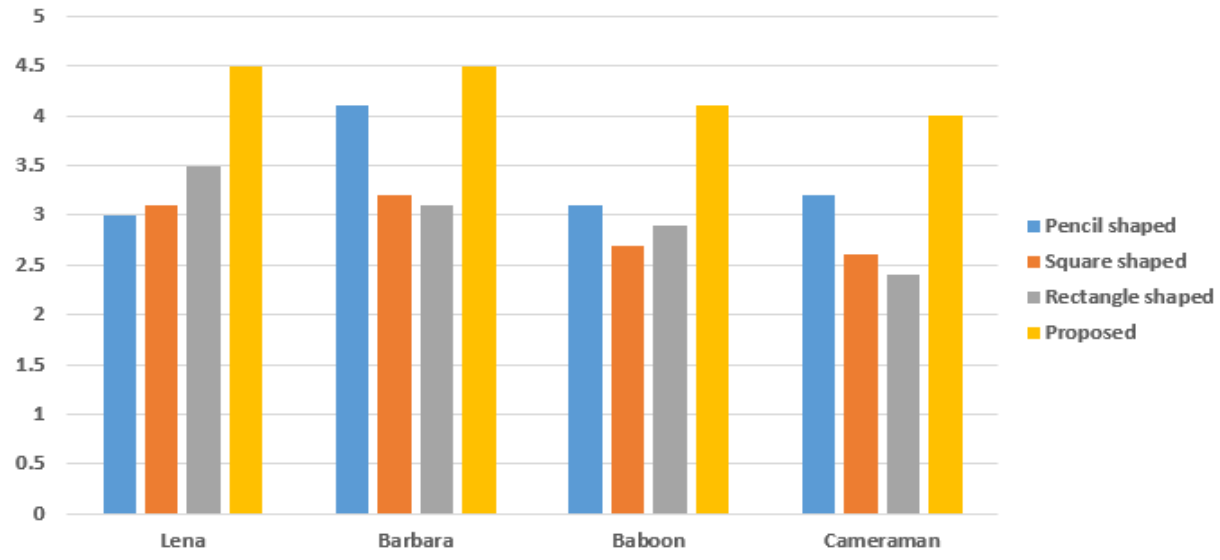
Table 13. Statistical analysis of cover and stego image 2

Statistical Analysis	Image	Original Cover Image C2	Steganographic Image Stego 2
Entropy	**concordorthophoto**	7.0995	6.6811
	Barbara	7.5838	7.4888
	Mandi	7.0704	6.8073
	Liftingbody	6.4641	6.4011
Correlation	**concordorthophoto**	0.5911	0.5911
	Barbara	0.8894	0.8894
	Mandi	0.9498	0.9498
	Liftingbody	0.8468	0.8468
Homogeneity	**concordorthophoto**	0.7187	0.7187
	Barbara	0.8224	0.8224
	Mandi	0.9065	0.9065
	Liftingbody	0.9173	0.9173
Contrast	**concordorthophoto**	0.9855	0.9855
	Barbara	0.6143	0.6143
	Mandi	0.2197	0.2197
	Liftingbody	0.3046	0.3046
Energy	**concordorthophoto**	0.0974	0.0974
	Barbara	0.0801	0.0801
	Mandi	0.1999	0.1999
	Liftingbody	0.3787	0.3787

4.5 Mean opinion score (MOS):

MOS is the arithmetic mean over all individual “values on a predefined scale that a subject assigns to his opinion of the performance of a system quality. The final MOS is an average across the participants, resulting in a score between 0-5, with 5 being an excellent quality call, and 0 being indecipherable

MOS	QUALITY
1	Unacceptable
2	Poor
3	Fair
4	Good
5	Excellent



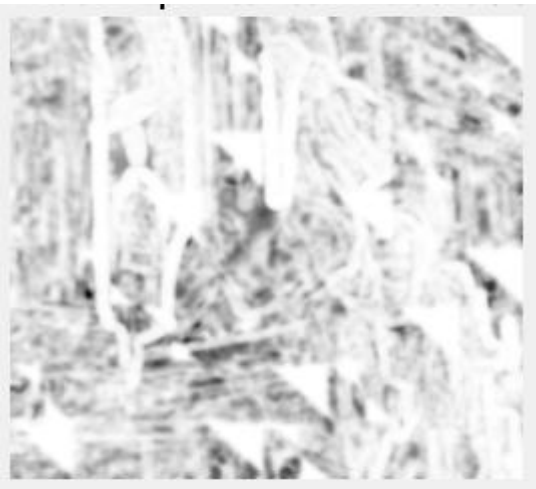
4.6 Structural similarity index (SSIM):

Structural similarity index defines the similarity between two images. One image is the reference image against whom the second image is measured. In our case, our original cover image is our reference image and stego image is measured against reference image. SSIM is invented to improve the existing methods of peak signal to noise ratio PSNR and

mean square error MSE.A histogram is an exhibition of numerical data that SSIM value lies between 1 and -1. Negative one means both images are very different to each other. They have no similarity between them. Normally SSIM is calculated on an 8 x 8-window size. The next table shows SSIM values for cover and stego images used in our experiments. These figures shows that stego image is similar to cover image. Hence, no one can differentiate between these two images, which makes it resistant to attacks. Therefore, our proposed technique is resistant to attacks.

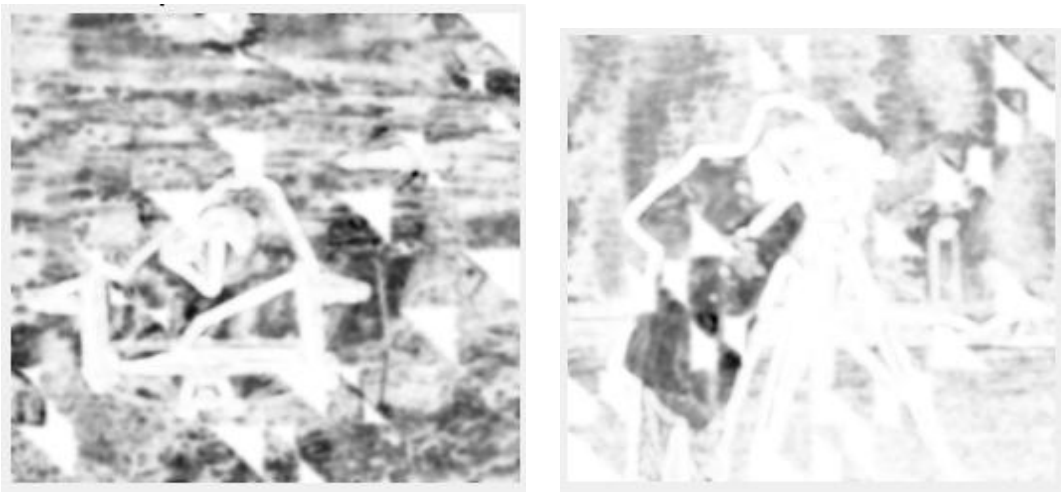
Table 14. SSIM values for cover image

Sr. No	Secret Image	C1	C2	SSIM1	SSIM2
2	Loftingbody	Moon	concordorthophoto	0.8456	0.9005
4	Baboon	Goldhill	Barbara	0.9489	0.951
7	cameraman	Rice	Mandi	0.9272	0.9062
10	Lena	Cameraman	Loftingbody	0.8912	0.8891



SSIM Index Map “Mandi”

SSIM Index Map “Barbara”



SSIM Index Map “Lifting Body” SSIM Index Map “Cameraman”

Figure 4.11 SSIM Index maps of different Test Images

Chapter 5

Conclusion and Future Work

The results of statistical parameters like correlation, entropy, homogeneity, and contrast and energy analysis are explained earlier. From above shown results, it is clear that, the original image and steganographic image are identical. This proves that our proposed method not only has good efficiency, but also it produces an image with high quality. A key point is that when the steganographic image be the same as host image, an adversary cannot use statistical attacks, due to the fact that all statistical characteristics of host image are the same as steganographic one. Therefore, our scheme is robust against statistical attacks.

The second key point is that, this paper proposes new methods for selection of pixels from an image using pixel selection algorithm. Pixels are selected in such a way that it will be difficult for attacker to trace the sequence or pattern in which pixels are selected. Hence, a factor of "Randomness" is introduced.

We have presented a novel image stenographic technique, in which instead of hiding the whole secret image in to a single cover image, we divide our secret image into sub images. This is achieved by extracting random pixels from secret image. The randomness will help in improving the security of our secret image. As it will be more difficult for attacker to crack the image. This forms our first sub image. The remaining pixels are grouped into second sub image. This randomness provides a better security as it is hard to detect random pixels. Even if some part of images is cracked, it still will not reveal the secret image. To obtain the complete secret image, one needs to have all parts of image and then they must be integrated with proper sequence. For this purpose, sequence number is embedded into a predefined pixel and communicated to both parties. Our method achieves PSNR values above 40 dB which shows effectiveness of our algorithm.

In future, research can be done on reducing the block size and adding more randomness in pixel selection. LSB techniques and it can be integrated with above mention algorithm. It will further enhance the security of our data and it will be harder and harder for the attacker to crack the secret image.

APPENDICES

APPENDIX A

BIBLIOGRAPHY

[1] Chin-Feng Lee, Ying-Xiang Wang, and An-Tong Shih "Image Steganographic Method Based on Pencil-Shaped Pattern" Mobile and Wireless Technologies 2017, Lecture Notes in Electrical Engineering 425, DOI 10.1007/978-981-10-5281-1_70

[2] Chang CC, Liu Y, Nguyen TS (2014) A novel Turtle shell based scheme for data hiding. In: Proceedings of the tenth international conference on intelligent information hiding and multimedia signal processing, Kitakyushu, Japan

[3] Khushboo Jain, Amrit Kaur, "Shape based data Hiding Steganography as well as Steganalysis for Secure Communication System"International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 6, June 2015

[4] Chang CC, Chou YC, Kieu TD (2008) An information hiding scheme using Sudoku. In: Proceedings of the computing, information and control (ICICIC 2008), Homburg, German

[5] Dr. Diwedi Samidha, Dipesh Agrawal, "Random Image Steganography in Spatial Domain" 978-1-4673-5301-4/13/$31.00 ©2013 IEEE

[6] Khalil Challita and Hikmat Farhat "Combining Steganography and Cryptography: New Directions" International Journal on New Computer Architectures and Their Applications (IJNCAA) The Society of Digital Information and Wireless Communications, pp. 199-208 (2011)

[7] Cheddad, A., Condell, J., Curran, K., McKevitt, P.: Digital image steganography: Survey and analysis of current methods. Signal Processing 90, 727–752 (2010)

[8] Fabien A P Peticolas, Ross J Anderson and Markus J Kuhn "Information Hiding – A survey" Proceedings of the IEEE, July 1999

[9] Amitava Nag, Jyoti Prakash Singh, Sushanta Biswas "A Huffman Code Based Image Steganography Technique" Springer International pp. 257-265

[10] Shaveta Chutani and Himani Goyal "Image Steganography using Multi Level Hiding Technique"

[11] Amitava Nag, Jyoti Prakash Singh, Sushanta Biswas "A Huffman Code Based Image Steganography Technique" Springer International pp. 257-265

[12] Jithesh K, Dr. A V Senthil Kumar "Multi-Layer Information Hiding -A Blend of Steganography and Visual Cryptography" Journal of Theoretical and Applied Information Technology pp. 109-116

[13] Shaveta Chutani and Himani Goyal "Image Steganography using Multi Level Hiding Technique"

[14] Nimbria, Manju. "Steganography: The Art of Hiding Text in Image using Matlab." International Journal of Advanced Research in Computer Science 4, Vol. 3 pp. 219-228 (2014).

[15] Lip Yee Por, Delina Beh, “An Enhanced Mechanism for Image Steganography Using Sequential Color Cycle Algorithm” The International Arab Journal of Information Technology, Vol. 10, No. 1 pp. 51-60
[16] Fabien A P Peticolas, Ross J Anderson and Markus J Kuhn “Information Hiding – A survey” Proceedings of the IEEE, July 1999
[17] Doshi, Ronak, Pratik Jain, and Lalit Gupta. "Steganography and its Applications in Security." International Journal of Modern Engineering Research (IJMER) 2.6 pp. 4634-4638 (2012).
[18] Al Hasib, Abdullah, and Abul Ahsan Md Mahmudul Haque. “A comparative study of the performance and security issues of AES and RSA cryptography” Convergence and Hybrid Information Technology, 2008. ICCIT'08. Third International Conference. Vol. 2. IEEE, 2008.
[19] Chandramouli R and Memin N, “Analysis of LSB based image steganography techniques” Proceedings International Conference on image Processing Vol. 3 Issue June 2001, pp.1019-102
[20] Reyadh Naoum1,Ahmed Shihab2, Sadeq AlHamouz3 “Enhanced image steganography system based on discrete wavelet transform and resilient Back-propagation” IJCSNS International Journal of Computer Science and Network Security, VOL.15 No.1, January 2015
[21] Hanzhou Wu & Hongxia Wang & Hong Zhao & Xiuying Yu “Multi-layer assignment steganography using graph-theoretic approach” Springer International 20 May 2014
[22] Khalil Challita and Hikmat Farhat “Combining Steganography and Cryptography: New Directions” International Journal on New Computer Architectures and Their Applications (IJNCAA) The Society of Digital Information and Wireless Communications, pp. 199-208 (2011)
[23] Cheddad, A., Condell, J., Curran, K., McKevitt, P.: Digital image steganography: Survey and analysis of current methods. Signal Processing 90, 727–752 (2010)
[24] Stallings, W.: Cryptography and Network Security: Principles and Practices, 4th edn. Pearson Education Pvt. Ltd., India (2004)
[25] Shamir, A.: How to share a secret. Communications of the ACM 22(11), 612–613 (1979)
[26] Tsai, C.S., Chang, C.C., Chen, T.S.: Sharing multiple secrets in digital images. The Journal
of Systems and Software 64(2), 163–170 (2002)
[27] Thien, C.C., Lin, J.C.: Secret image sharing. Computer & Graphics 26(1), 765–770 (2002)
[28] Lin, C.C., Tsai, W.H.: Secret image sharing with steganography and authentication. The
Journal of Systems and Software 73(3), 405–414 (2004)

[29] Wu, Y.S., Thien, C.C., Lin, J.C.: Sharing and hiding secret images with size constraint. Pattern Recognition 37(7), 1377–1385 (2004)
[30] Chang, C.-C., Lin, P.-Y., Chan, C.-S.: Secret image sharing with revertible steganography., International Conference on Computational Intelligence and Natural Computing (2009)
[31] Fabien A. P. Peticolas, Ross J. Anderson, and Markus J. Kuhn, "Information Hiding- A Survey", proceedings of the IEEE, July 1999,pp 1062-1078.
[32] Kevin Curran, Karen Bailey, University of Ulster, Institute of Technology (2003), Letterkenn, "An Evaluation of Image Based Steganography Methods", International Journal of Digital Evidence Fall 2003.
[33] Hassan Mathkour, Ghazy M.R. Assassa, Abdulaziz Al Muuharib, Ibrahim Kiady, "A Novel Approach for Hiding Messages in Images", 2009 International Conference on Signal Acquisition and Processing, 2009
[34] Artz, D. "Digital steganography: Hiding data within Data", IEEE Internet Computing, May/June 2001.
[35] Chandramouli, R. and Memon, N., "Analysis of LSB based image steganography techniques",Proceedings, International Conference on Image Processing, vol.3, Issue June 2001, pp.1019-1022.
[36] Implementing Random Encoding for Image Steganography "International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 "