A Sesure Image Steganography Using LSB Technique and Pseudo Random Encoding Technique

A Project Thesis submitted in partial fulfillment of the requirment
for the degree of
Bachelor of Technology in
Computer Science and Engineering

by

Kshetrimayum Jenita Devi

under

Dr. Sanjay Kumar Jena(Professor)

Department of Computer Science and Engineering
National Institute of Technology-Rourkela Odisha -769008

May 2013

Department of Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela-769 008, India. www.nitrkl.ac.in

May 2013

Certificate

This is to certify that the work in the thesis entitled **A Sesure Image Steganography Using LSB Technique and Pseudo Random Encoding Technique** submitted by **Kshetrimayum Jenita Devi**, bearing roll number **109CS0608** has been carried out under my supervision in fulfilment of the requirements for the degree of Bachelor of Technology in Computer Science and Engineering during session 2012-2013 in the Department of Computer Science and Engineering, National Institute of Technology, Rourkela.

To the best of my knowledge, this work has not been submitted for any degree or academic award elsewhere.

Dr. Sanjay Kumar Jena

Professor
CSE Department of NIT Rourkela

Acknowledgements

I would like to take this opportunity to extent my hearty gratitude to my guide and supervisor **Dr. Sanjay Kumar Jena**, Professor of Department of Computer Science and Engineering; National Institute of Technology-Rourkela,Odisha-769008, whose constant guidance and encouragement made the completion of my B.Tech thesis possible.

I am obliged to all the professors of the Department of Computer Science and Engi- neering, NIT Rourkela for instilling in me the basic knowledge about the field that greatly benefitted me while carrying out the project and achieving the goal

Lastly, I am grateful to my friends, for their relentless support in augmenting the value of work; my family, for being considerate and appreciative throughout; and Almighty,for everything.

Kshetrimayum Jenita Devi

Abstract

Steganography is derived from the Greek word steganographic which means covered writing. It is the science of secret communication. The goal of steganography is to hide the existence of the message from unauthorized party. The modern secure image steganography presents a task of transferring the embedded information to the destination without being detected by the attacker. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exist a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points.

In this paper I purposed an image based steganography that Least Significant Bits (LSB) techniques and pseudo random encoding technique on images to enhance the security of the communication. In the LSB approach, the basic idea is to replace the Least Significant Bits (LSB) of the cover image with the Bits of the messages to be hidden without destroying the property of the cover image significantly. The LSB-based technique is the most challenging one as it is difficult to differentiate between the cover-object and stego-object if few LSB bits of the cover object are replaced. In Pseudo-Random technique, a random-key is used as seed for the Pseudo-Random Number Generator is needed in the embedding process [19]. Both the techniques used a stego-key while embedding messages inside the cover image.By using the key, the chance of getting attacked by the attacker is reduced[1,2].

Keywords: Steganography, LSB, Random-key, Image, secret message, stego-key,cover image,Techniques.

List of Figures

List of Tables

Contents

Chapter 1

Introduction

1.1 Steganography

The word steganography is derived from the Greek words stegos meaning cover and grafia meaning writing [1] defining it as covered writing. In image steganography the information is hidden exclusively in images. Steganography is the art and science of secret communication .It is the practice of encoding/embedding secret information in a manner such that the existence of the information is invisible. The original files can be referred to as cover text, cover image, or cover audio. After inserting the secret message it is referred to as stego-medium. A stego-key is used for hiding/encoding process to restrict detection or extraction of the embedded data[2].

1.2 Steganography and cryptography

Steganography differs from cryptography[8]

- **Steganography** Hide the messages inside the Cover medium,Many Carrier formats.
- Breaking of steganography is known as Steganalysis.

- **Cryptography** Encrypt the message before sending To the destination,no need of carrier/cover medium.

- Breaking of cryptography is known as Cryptanalysis.

Watermarking and fingerprinting related to steganography are basically used for intellectual property protection. A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal. The embedded information in a watermarked object is a signature refers the ownership of the data in order to ensure copyright protection. In fingerprinting, different and specific marks are embedded in the copies of the work that different customers are supposed to get. In this case, it becomes easy for the property owner to find out such customers who give themselves the right to violate their licensing agreement when they illegally transmit the property to other groups [1][7].

1.3 Literature Review

The term steganography came into use in 1500s after the appearance of Trithemius book on the subject Steganographia.[3]

1.3.1 Past

The word Steganography technically means covered or hidden writing. Its ancient origins can be traced back to 440 BC. Although the term steganography was only coined at the end of the 15th century, the use of steganography dates back several millennia. In ancient times, messages were hidden on the back of wax writing tables, written on the stomachs of rabbits, or tattooed on the scalp of slaves. Invisible ink has been in use for centuriesfor fun by children and students and for serious undercover work by spies and terrorists [9].

1.3.2 Present

The majority of todays steganographic systems uses multimedia objects like image, audio, video etc as cover media because people often transmit digital pictures over email and other Internet communication. Modern steganography uses the opportunity of hiding information into digital multimedia files and also at the network packet level[4].

Hiding information into a medium requires following elements [2]

1. The cover medium(C) that will hold the secrat message.

2. The secret message (M), may be plain text, digital image file or any type of data.

3. The stegonographic techniques

4. A stego-key (K) may be used to hide and unhide the message.
In modern approach, depending on the cover medium, steganography can be divided into five types: 1. Text Steganography 2. Image Steganography 3. Audio Steganography 4. Video Steganography 5. Protocol Steganography

- **Text steganography** Hiding information in text file is the most common method of steganography. The method was to hide a secret message into a text message. After coming of Internet and different type of digital file formats it has decreased in importance. Text stenography using digital files is not used very often because the text files have a very small amount of excess data.

- **Image steganography** Images are used as the popular cover medium for steganography. A message is embedded in a digital image using an embedding algorithm, using the secret key. The resulting stego-image is send to the receiver. On the other side, it is processed by the extraction algorithm using the same key. During the transmission of stego- image unauthenticated persons can only notice the transmission of an image but cant see the existence of the hidden message.

- **Audio steganography** Audio steganography is concerned with embedding information in an innocuous cover speech in a secure and robust manner. Communication andtransmission security and r obustness are essential for transmitting vital information to intended sources while denying access to unauthorized persons. An audible, sound can be inaudible in the presence of another louder audible sound .This property allows to select the channel in which to hide information [2]. Existing audio steganography software can embed messages in WAV and MP3 sound files. The list of methods that are commonly used for audio steganography are listed and discussed below.
- LSB coding
- Parity coding
- Phase coding
- Spread spectrum
- Echo hiding
- **Video steganography** Video Steganography is a technique to hide any kind of files in any extension into a carrrying Video file.
- **Protocol steganography** The term protocol steganography is to embedding information within network protocols such as TCP/IP. We hide information in the header of a TCP/IP packet in some fields that can be either optional or are never used. [10]

1.3.3 Applications of Steganography

- **(i)Secret Communications**[13] The use steganography does not advertise secret communication and therefore avoids scrutiny of the sender, message, and recipient. A trade secret, blueprint, or other sensitive information can be transmitted without alerting potential attackers.

- **(ii)Feature Tagging** Elements can be embedded inside an image, such as the names of individuals in a photo or locations in a map. Copying the stego-image also copies all of the embedded features and only parties who possess the decoding stego-key will be able to extract and view the features.
- **(iii)Copyright Protection** Copy protection mechanisms that prevent data, usually digital data, from being copied.The insertion and analysis of watermarks to protect copyrighted material is responsible for the recent rise of interest in digital steganography and data embedding.[16,17]

1.4 Objective

The project is carried out with the following objectives:[2]

- To hide the message or a secret data into an image which acts as a cover medium using LSB technique and pseudo random technique.
- The primary motivation of my current work is to increase PSNR of the stego image(peak signal to noise ratio).

1.5 Outline of Thesis

The thesis consist of following four chapters:
Chapter 2: Image steganography
Chapter 3: Proposed Work:Sesure Information Hiding
Chapter 4: Performance Analysis
Chapter 5: Conclusion

Chapter 2

Image steganography

2.1 Image definition

An image is a picture that has been created or copied and stored in electronic form. An image can be described in terms of vector graphics or raster graphics . An image stored in raster form is sometimes called a bitmap . An image map is a file containing information that associates different locations on a specified image with hypertext links.An image is a collection of numbers that constitute different light intensities in different areas of the image. This numeric representation forms a grid and the individual points are referred to as pixels (picture element).Greyscale images use 8 bits for each pixel and are able to display 256 different colours or shades of grey. Digital colour images are typically stored in 24-bit files and use the RGB colour model, also known as true colour [5]. All colour variations for the pixels of a 24-bit image are derived from three primary colours: red, green and blue, and each primary colour is represented by 8 bits [4]. Thus in one given pixel, there can be 256 different quantities of red, green and blue [5].

2.2 Image Compression

In images there are two types of compression: lossy compression and lossless compression. In Lossless compression,With lossless compression, every single bit of data that was originally in the file remains after the file is uncompressed. All of the information is completely restored.The most popular image formats that use lossless compression is GIF (Graphical Interchange Format) and BMP (bitmap file). lossy compression reduces a file by permanently eliminating certain information, especially redundant information. When the file is uncompressed, only a part of the original information is still there. In this case the resulting image is expected to be something similar to the original image, but not the same as the original. An example of an image format that uses this compression technique is JPEG (Joint Photographic Experts Group) [11].

2.3 Image Steganographic Techniques

There are several Steganographic techniques for image file format which are as follows[11]:

2.3.1 Spatial Domain Technique

There are many versions of spatial steganography, all directly change some bits in the image pixel values in hiding data. Least significant bit (LSB)-based steganography is one of the simplest techniques that hides a secret message in the LSBs of pixel values without perceptible distortions. To our human eye, changes in the value of the LSB are imperceptible. Embedding of message bits can be done either simply or randomly.[4].Least Significant Bit (LSB) replacement technique, Matrix embedding, are some of the spatial domain techniques.

Advantages of spatial domain LSB technique are:

- 1.Degradation of the original image is not easy.
- 2.Hiding capacity is more i.e. more information can be stored in an image. Disadvantages of LSB technique are:
- 1.robustness is low
- 2.Hidden data can be destroyed by simple attacks.

2.3.2 Masking and Filtering

Masking and Filtering is a steganography technique which can be used on grayscale images. Masking and filtering is similar to placing watermarks on a printed image. These techniques embed the information in the more significant areas than just hiding it into the noise level.Watermarking techniques can be applied without the fear of image destruction due to lossy compression as they are more integrated into the image[5].

Advantages of Masking and filtering Techniques:

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

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

2.3.3 Transform Domain Technique

The Frequency domain the message is inserted into transformed coefficients of image giving more information hiding capacity and more robustness against attacks.Transform domain embedding can be termed as a domain of embedding techniques for which a number of algorithms have been suggested [3].Most of the strong steganographic systems today operate within the transform domain Transform domain techniques have an advantage over LSB techniques as they hide information in areas of the image that are less exposed to compression, cropping, and image processing. Some transform domain techniques do not seem dependent on the image format and they may outrun lossless and lossy format conversions. Transform domain techniques are of different types[3]:

1. Discrete Fourier transformation technique (DFT).

2. Discrete cosine transformation technique (DCT).

3. Discrete Wavelet transformation technique (DWT).

2.3.4 Distortion Techniques

In this technique,store information by signal distortion and measure the deviation from the original cover in the decoding process.Distortion techniques need knowledge of the original cover image during the decoding process where the decoder functions to check for differences between the original cover image and the distorted cover image in order to restore the secret message.In this technique, a stego-image is created by applying a sequence of modifications to the cover image. This sequence of modifications is use to match the secret message required to transmit.The message is encoded at pseudo-randomly chosen pixels. If the stego-image is different from the cover image at the given message pixel, the message bit is a 1. otherwise, the message bit is a 0. The encoder can modify the 1 value pixels in such a manner that the statistical properties of the image are not affected.If an attacker interfere with the stego-image by cropping, scaling or rotating, the receiver can easily detect it[4,12].

2.4 Characteristics feature of Data Hiding Techniques

Perceptibility does embedding message distort cover medium to a visually unacceptable level.

Capacity how much information can be hidden with relative to the change in perceptibility.

Robustness to attacks can embedded data exist manipulation of the stego medium in an effort to destroy, or change the embedded data.

Tamper Resistance Beyond robustness to destruction, tamper-resistance refers to the difficulty for an attacker to alter a message once it has been embedded in a stego-image.[13]

2.5 Image Steganalysis

Steganalysis is the breaking of steganography and is the science of detecting hidden information [14]. The main objective of steganalysis is to break steganography and the detection of stego image. Almost all steganalysis algorithms depend on steganographic algorithms introducing statistical differences between cover and stego image.
Steganalysis are of three different types:

Visual attacks it discovered the hidden information, which helps to separate the image into bit planes for further more analysis.

Statistical attacks Statistical attacks may be passive or active. Passive attacks involves with identifying presence or absence of a secret message or embedding algorithm used. Active attacks is used to investigate embedded message length or hidden message location or secret key used in embedding.

Structural attacks The format of the data files changes as the data to be hidden is embedded, identifying this characteristic structure changes can help us to find the presence of image/text file.

2.5.1 Steganalytic tools

There are several steganalytic tools available in market like PhotoTitle, 2Mosaic and StirMark Benchmark etc. These three steganalytic tools can remove steganographic content from any image. This is achieved by destroying secret message by two techniques: break apart and resample.[14].

Chapter 3

Secure Information Hiding

An information hiding system has been developed for confidentiality. However, in this chapter, we study an image file as a carrier to hide message. Therefore, the carrier will be known as cover-image, while the stego-object known as stego-image. The implementation of system will only focus on Least Significant Bit (LSB) as one of the steganography techniques as mentioned in below [14].

3.1 Least-Significant Bit (LSB) Technique

The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message.Digital images are mainly of two types (i) 24 bit images and (ii) 8 bit images. In 24 bit images we can embed three bits of information in each pixel, one in each LSB position of the three eight bit values. Increasing or decreasing the value by changing the LSB does not change the appearance of the image; much so the resultant stego image looks almost same as the cover image. In 8 bit images, one bit of information can be hidden.

The cover image is shown in Figure 4.7 and a hidden message is shown in Figure 4.8 A stego-image (figure 4.9) is obtained by applying LSB algorithm on both the cover and hidden images. The hidden image is extracted from the stego-image by applying the reverse process[1, 11]. If the LSB of the pixel value of cover image C(i,j) is equal to the message bit m of secret massage to be embedded, C(i,j) remain unchanged; if not, set the LSB of C(i, j) to m. The message embedding procedure is given below-

S(i,j) = C(i,j) - 1, if LSB(C(i,j)) = 1 and m = 0

S(i.j) = C(i,j), if LSB(C(i,j)) = m

S(i,j) = C(i,j) + 1, if LSB(C(i,j)) = 0 and m = 1

where LSB(C(i, j)) stands for the LSB of cover image C(i,j) and m is the next message bit to be embedded.

S(i,j) is the stego image

As we already know each pixel is made up of three bytes consisting of either a 1 or a 0.

For example, suppose one can hide a message in three pixels of an image (24-bit colors). Suppose the original 3 pixels are:[16]

(11101010 11101000 11001011)

(01100110 11001010 11101000)

(11001001 00100101 11101001)

A steganographic program could hide the letter ”J” which has a position 74 into ASCII character set and have a binary representation ”01001010”, by altering the channel bits of pixels.

(11101010 11101001 11001010)

(01100110 11001011 11101000)

(11001001 00100100 11101001)

In this case, only four bits needed to be changed to insert the character succesfully. The resulting changes that are made to the least significant bits are too small to be recognised by the human eye, so the message is effectively hidden. The advantage of LSB embedding is its simplicity and many techniques use these methods [10]. LSB embedding also allows high perceptual transparency.

The following figure3.1,3.2 shows the mechanism of LSB technique

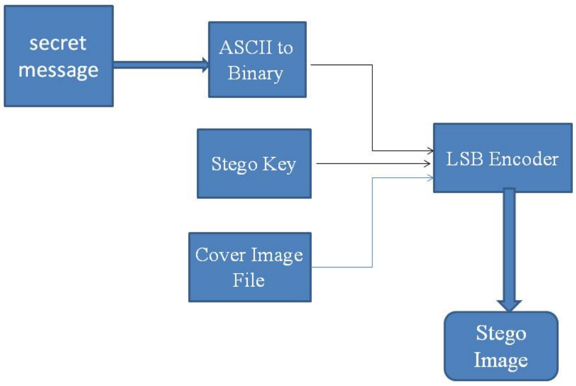

Fig: LSB Insertion Mechanism

Figure 3.1: LSB insertion Mechanism

3.1.1 Data Embedding

The embedding process is as follows.

Inputs Cover image, stego-key and the text file

Output stego image

Procedure

Step 1: Extract the pixels of the cover image.

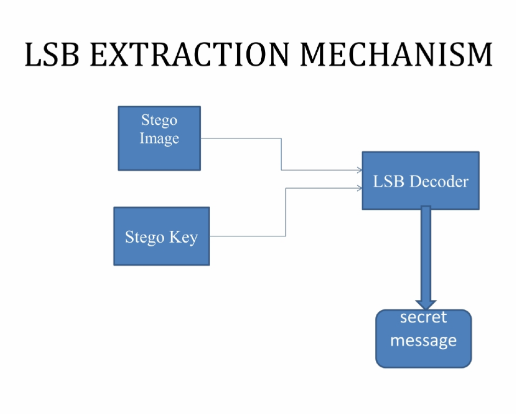

Figure 3.2: LSB extraction Mechanism

Step 2: Extract the characters of the text file.

Step 3: Extract the characters from the Stego key.

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

Step 5: Place some terminating symbol to indicate end of the key. 0 has been used as a terminating symbol in this algorithm.

Step 6: Insert characters of text file in each first component of next pixels by replacing it.

Step 7: Repeat step 6 till all the characters has been embedded.

Step 8: Again place some terminating symbol to indicate end of data.

Step 9: Obtained stego image.[17]

3.1.2 Data Extraction

The extraction process is as follows.

Inputs Stego-image file, stego-key

Output Secret text message. Procedure:

Step 1: Extract the pixels of the stego image.

Step 2: Now, start from first pixel and extract stego key characters from first component of the pixels. Follow Step3 up to terminating symbol, otherwise follow step 4.

Step 4: If this extracted key matches with the key entered by the receiver, then follow Step 5, otherwise terminate the program.

Step 5: If the key is correct, then go to next pixels and extract secret message characters from first component of next pixels. Follow Step 5 till up to terminating symbol, otherwise follow step 6.

Step 6: Extract secret message[18,20].

3.1.3 Image Encoding Algorithm

Inputs Image file, stego key and image file

Output Stego image.

1. The cover and secret images are read and converted into the unit8 type.

2. The numbers in secret image matrix are conveyed to 8-bit binary. Then the matrix is reshaped to a new matrix a.

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

4. Perform the LSB technique described above

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

6. While extracting the data, the LSB of the stego image is collected and they are reconstructed into the decimal numbers. The decimal numbers are reshaped to the secret image[10].

3.2 Pseudo-Random Encoding Technique

In this technique, A random key is used to choose the pixels randomly and embed the message. This will make the message bits more difficult to find and hopefully reduce the realization of patterns in the image [9]. Data can be hidden in the LSB of a particular colour plane (Red plane) of the randomly selected pixel in the RGB colour space[19].

3.2.1 Embedding Algorithm

In this process of encoding method, a random key is used to randomised the cover image and then hide the bits of a secret message into the least significant bit of the pixels within a cover image. The transmitting and receiving end share the stego key and random-key. The random-key is usually used to seed a pseudo-random number generator to select pixel locations in an image for embedding the secret message[3].

Inputs Cover image, stego-key and the message

Output stego image

1) Read character from text file that is to be hidden and convert the ASCII value of the character into equivalent binary value into an 8 bit integer array.

2) Read the RGB colour image(cover image) into which the message is to be embedded.

3) Read the last bit of red pixel.

4) Initialize the random key and Randomly permute the pixels of cover image and reshape into a matrix.

5) Initialize the stego-key and XOR with text file to be hidden and give message.

6) Insert the bits of the secret message to the LSB of the Red plane's pixels.

7) Write the above pixel to Stego Image File[19].

3.2.2 Extraction of Hidden Message

In this process of extraction, the process first takes the key and then random-key. These keys takes out the points of the LSB where the secret message is randomly distributed [18]. Decoding process searches the hidden bits of a secret message into the least significant bit of the pixels within a cover image using the random key. In decoding algorithm the random-key must match i.e. the random-key which was used in encoding should match because the random key sets the hiding points of the message in case of encoding. Then receiver can extract the embedded messages exactly using only the stego-key.

3.2.3 Message extraction algorithm

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

Output Secret message.

1) Open the Stego image file in read mode and from the Image file, read the RGB colour of each pixel.

2) Extract the red component of the host image.

3) Read the last bit of each pixel.

4) Initialize the random-key that gives the position of the message bits in the red pixel that are embedded randomnly.

5) For decoding, select the pixels and Extract the LSB value of red pixels.

7) Read each of pixels then content of the array converts into decimal value that is actually ASCII value of hidden character.

8) ASCII values got from above is XOR with stego-key and gives message file, which we hide inside the cover image[19].

Chapter 4

Performance Analysis

4.1 Performance Analysis

As a performance measure for image distortion due to hidding of message, the well-known peak-signal-to noise ratio (PSNR), which is categorized under difference distortion metrics, can be applied to stego images. It is defined as:

PSNR = 10log(Cmax)$^2/MSE$.
$MSE = mean - square - error$,

which is given as:

MSE = 1/MN((S-C)^2).
$Cmax = 255$.

Where M and N are the dimensions of the image,

S is the resultant stego-image, and C is the cover image.

PSNR values below 30 dB indicate low quality (i.e., distortion caused by embedding is high). A high-quality stego image should strive for a PSNR of 40 dB, or higher[6].

4.2 Implementation and Evaluation of above two techniques

We have implemented the above two techniques in MATLAB and the above mentioned algorithms with respect to image steganography are not void of weak and strong points. Consequently, it is important to decide the most suitable approach to be applied. As defined before, there are several parameters to measure the performance of the steganographic system. Some parameters are as follows[13]:

Perceptibility does embedding information distort cover medium to a visually unacceptable level.

Capacity how much information can be hidden (relative to the change in perceptibility)
item **Robustness to attacks** can embedded data survive manipulation of the stego medium in an effort to destroy, remove, or change the embedded data.

Table 4.1: Comparision of characters of above two techniques

SL.No	Imperceptibility	Robustness	Capacity	Tamper Resistance
Simple LSB	High*	Low	High	Low
Pseudo-Random Encoding	Higher*	Low	High	High**

*: Indicates dependency on the used cover image

**: Indicates dependency on the used key and random seed

4.3 Results and calculation

We consider gray scale/RGB image as cover image as shown in Figure 4.1, Figure 4.4, Figure 4.7 and text file/image as secret message for both the Techniques and then produced stego image.

Figure4.2 and 4.3 is the result of cover image with text file.

Figure 4.5 and 4.6 are the result of RBG image with text file.

Table 4.2: PSNR of Pseudo-Random Encoding

SL.No	Cover Image	Secret Message	Stego-Image	SNR(dB)	MSE	PSNR(dB)
1	Gray image	Text message	Gray image	59.6374	0.0449	61.6065
2	RBG image	Text message	sisbr	61.3787	0.0111	67.6835
3	RBG image	Image	Images	53.9847	0.0911	58.5346

Table 4.3: PSNR of Least Significant Bits Encoding

SL.No	Cover Image	Secret Message	Stego-Image	SNR(dB)	MSE	PSNR(dB)
1	Gray image	Text message	Gray image	59.5043	0.0463	61.4733
2	RBG image	Text message	sisbr	61.3649	0.021	67.6697
3	RBG image	Image	Hydrang	53.9812	0.0912	58.5311

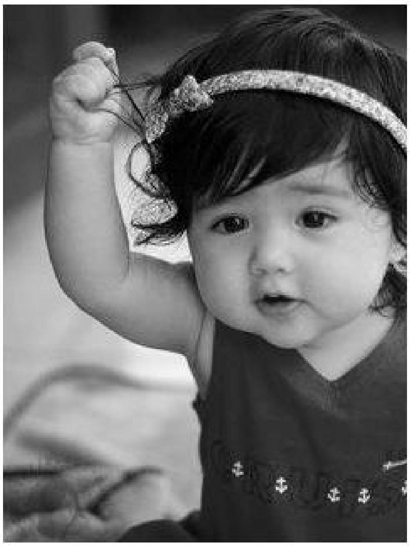

Figure 4.1: cover image

The difference images are shown in figures 4.11 to 4.15, where white pixels indicate the spatial locations where the images differ.

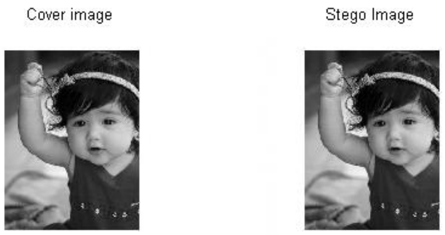

FIGURE 4.2: LSB technique

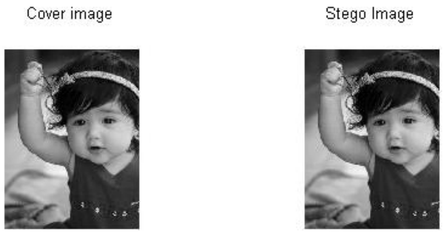

FIGURE 4.3: Pseudo-Random Encoding

FIGURE 4.4: RBG(cover image)

Figure 4.5: LSB technique

Figure 4.6: Pseudo random technique

Figure 4.7: RBG image

Figure 4.8: secret image

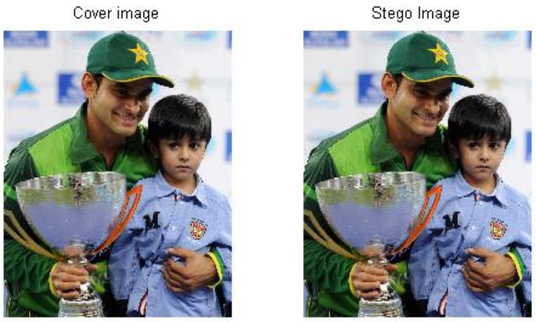

Figure 4.9: LSB Technique

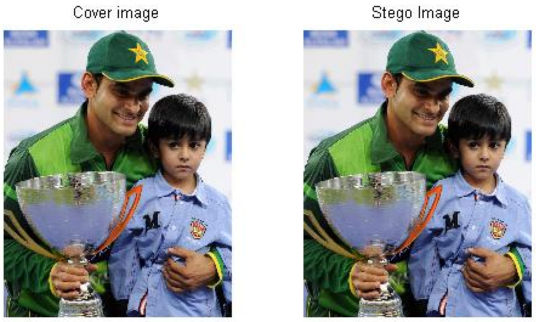

Figure 4.10: Pseudo random Technique

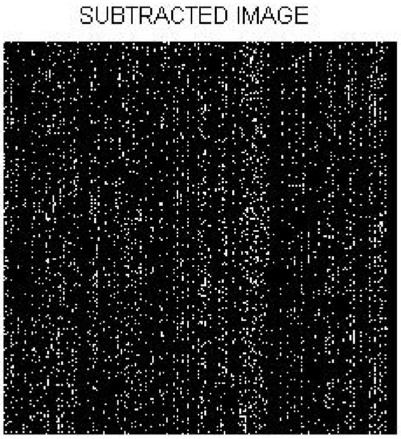

Figure 4.11: Difference image of fig.4.2

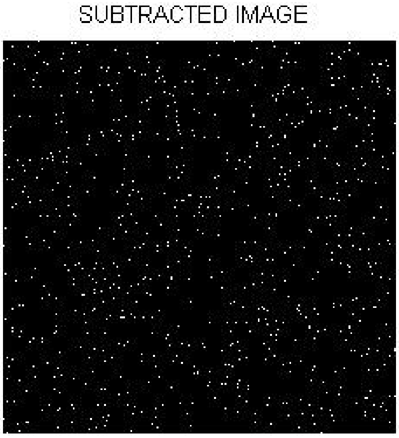

FIGURE 4.12: Difference image of fig.4.3

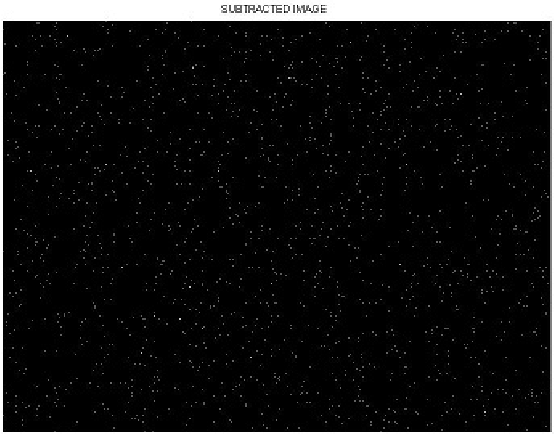

FIGURE 4.13: Difference image of fig.4.5

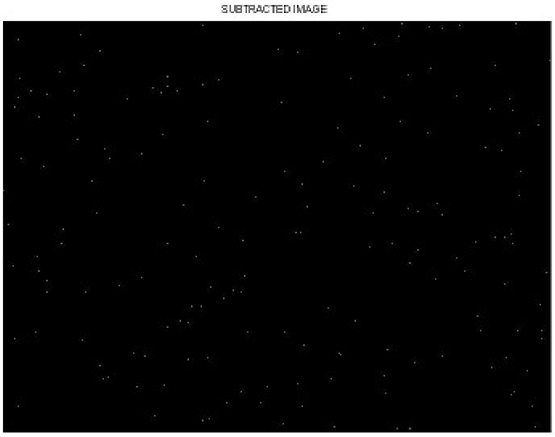

FIGURE 4.14: Difference image of fig.4.6

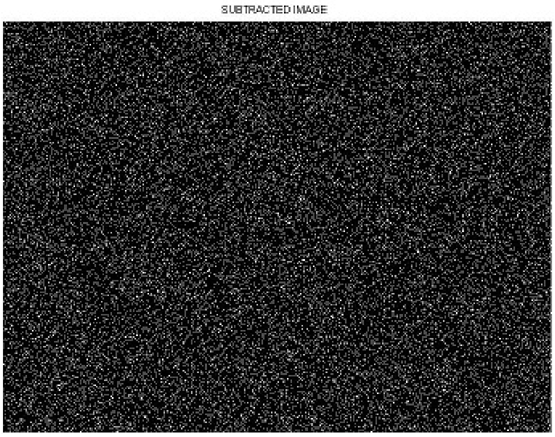

FIGURE 4.15: Difference image of fig.4.9

Chapter 5

Conclusions

Steganography is an effective way to hide sensitive information. In this paper we have used the LSB Technique and Pseudo-Random Encoding Technique on images to obtain secure stego-image.Table 4.2 and Table 4.3 shows that PSNR of Pseudo random encoding is higher than PSNR of LSB encoding. Our results indicate that the LSB insertion using random key is better than simple LSB insertion in case of lossless compression.The image resolution doesn't change much and is negligible when we embed the message into the image and the image is protected with the personal key. So, it is not possible to damage the data by unauthorized personnel . The algorithm is usage for both 8 bit and 24 bit image of the same size of cover and secret image, so it is easy to be implementing in both grayscale and color image.This paper focuses on the approach like increasing the security of the message and increasing PSNR and reducing the distortion rate [18].

Chapter 6

References

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

2). Niels Provos, Peter Honeyman, "Hide and Seek: An Introduction to Steganography," IEEE computer society,2003.

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

4). An overview of image steganography by T. Morkel , J.H.P. Eloff, M.S. Olivier. Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science University of Pretoria, 0002, Pretoria, South Africa.

5). Johnson, N.F. Jajodia, S., "Exploring Steganography: Seeing the Unseen", Computer Journal, February 1998.

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

7). Ran-Zan Wang, Chi-Fang Lin, Ja-Chen Lin, "Hiding data in images by optimal moderately significant-bit replacement" IEE Electron. Lett. 36 (25) (2000) 20692070.

8). Hiding data in images by simple LSB substitution by Chi-Kwong Chan, L.M. Cheng Department of Computer Engineering and Information Technology, City University of Hong Kong, Hong Kong Received 17 May 2002.

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

10). International Journal of Computer Science Engineering Technology (IJCSET) "Modern Steganographic technique: A Survey" by Pratap Chandra Mandal Asst. Prof., Department of Computer Application B.P.Poddar Institute of Management Technology .

11). A. Cheddad, J. Condell, K. Curran and P.M. Kevitt. (2010). "Digital image steganography: survey and analysis of current methods." Signal Processing Journal.

12). P. Kruus, C. Scace,M. Heyman, and M. Mundy. (2003), "A survey of steganography techniques for image files." Advanced Security Research Journal.

13). A Review of Data Hiding in Digital Images by E Lin, E Delp Center for Education and Research Information Assurance and Security Purdue University, West Lafayette, IN 47907-2086.

14). W Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," IBM Systems Journal, Vol. 35, No. 3 and 4.

15). M.M. Amin, M. Salleh, S. Ibrahim, et al., "Information Hiding Using Steganography", 4th National Conference on Telecommunication Technology Proceedings (NCTT2003), Shah Alam, Malaysia, 2003.

16. Steganography and Steganalysis by J.R. Krenn January 2004.

17. Data hiding Algorithm for Bitmap Images using Steganography by Mamta Juneja Department of computer science and Engineering,RBIEBT,Sahuran.

18.Journal of Theoretical and Applied Information Technology 15th February 2012. Vol. 36 No.1. A steganography algorithm for hiding image in Image by improved lsb substitution by minimize Detection by vijay kumar sharma, 2vishal shrivastava M.Tech. scholar, Arya college of Engineering IT, Jaipur , Rajasthan (India).

19. International journal of computer engineering technology (ijcet) ”steganography based on random pixel selection for efficient data hiding’.Shamim Ahmed Laskar and Kattamanchi Hemachandran (Research Scholar, Department of Computer Science, Assam University).

20. Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 3, May-Jun 2012, Steganography Using Least Signicant Bit Algorithm.