Republic Of IRAQ
Ministry Of Higher Education
And Scientific Research
University of Diyala
College of Engineering
Communication Department

Implementation of text hiding within an image using LSB insertion technique

A Project Submitted to the Department of Communications Engineering Diyala University

By

Farah Abbas
Rawnaq Safaa

Supervised by
Assistant Lecture Hussein SH. Mugger

2016

بِسْمِ اللهِ ٱلرَّحْمنِ ٱلرَّحْيِم

اِنَّ في خَلْقِ السَّموَاتِ وَ الْأَرْضِ وَاخْتِلافِ اليَّلِ وَ النَّهَارِ وَ الْفُلْكِ التَّي تَجْرى فيِ الْبَحْرِ بِمَا يَنْفَعُ
النَّاسَ وَمَا أَنْزَلَ اللّهُ مِنَ السماء مِنْ ماء فأحيا بِهِ الأَرْضَ بَعْدَ مَوْتِهَا وَ بَثَّ فيهَا مِنْ كُلّ دَآبّةٍ وَ
تَصْريفِ الرّيَاحِ وَ السَّحَابِ ٱلْمُسَخَّرِ بَيْنَ السماء وَالأَرْضِ لآيات لِقَوْمٍ يَعْقِلوُنَ (164)

صدق الله العلي العظيم

سورة البقرة

Dedication

This project is dedicated to my teacher , who has always given me spiritual and educational support. To the fountain of patience and optimism and hope . To everyone in existence after Allah and his messenger my mother. To the great heart of my father. To the show me what is more beautiful than the life my husband and my brother . To those who paved the way for us science and knowledge our professors dear . To those who tasted the most beautiful moments my friends. I present this project.

Acknolegement

We are greatly thankful to our project advisor, Ass. Lecture Hussein SH. , who has fully supported us, not only throughout our project. He suggested this topic to us, a challenging but interesting topic. He was always very flexible with our work schedule. we know this project would have never been written and finished without his encouragement, guidance, knowledge, and tolerance. Thank you both for taking your precious time to give us advices and comments. we would also like to thank Mr. Hussein for giving us some wonderful questions on our project.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

List of Abbreviations

Abbreviation	**Abbreviated Words**
Stego	Steganography
LSB	Least Significant Bits
PSNR	Peak Signal to Noise Ratio
SIHS	Secure Information Hiding System
SNR	Signal-To-Noise-Ratio
2D	Two dimensional
3D	Three dimensional
HVS	Human Visual System
WWII	World War II
e.g.	exempli gratia
TCP/IP	Transmission Control Protocol/Internet Protocol
DCT	Discrete Cosine Transform
	Spread Spectrum
	Spread spectrum image steganography
B&W	Black and white
RGB	Red green blue
ASCII	American Standard Code for Information Interchange
MSE	Mean Square Error

List of symbols

Symbol	Mean of Symbols
C(i.j)	Cover image
M	Message
S(i.j)	Stego-image
K	Stego-key
I'	Stego-object
I	Cover-object
Σ	
log_{10}	
P	
a	
L	bit of the message
S(i,j)	Stego image
X(i,j)	Original image
Iyi	Is the random number generated
N	height of the two images.
M	width of the two images.
i and j	row and column numbers.
$\hat{X}$(i,j)	the stego image.

Abstract

Image steganography is becoming an important area in the field of steganography. As the demand of security and privacy increases, need of hiding their secret information is going on. LSB algorithm is used to hide the secret messages by using algorithm. LSB changes the image resolution quite clear as well as it is easy to attack. It is clear that LSB changes the image resolution when the least significant bits add in the binary image format, so that image quality become burst and there become so much difference in the original image and encoded image in the respect of image quality. So to overcome this problem, In this project we suggested modifying the LSB technique so that we can get same image quality as it has before the encoding. The basic idea to get good image quality, we are going to modify the hiding procedure of the least significant bit. This work we gave an overview of steganography. It can enhance confidentiality of information and provides a means of communicating privately. We have also presented an image steganographic system using LSB approach. However, there are some advantages and disadvantages of implementing LSB on a digital image as a carrier. All these are define based on the hiding capacity of the method. In future, we will attempt another two approaches of steganographic system on a digital image. This will lead us to define the best approach of steganography to hide information.

1.1 General Introduction

During the last two decades, computer networks created a revolution in the use of information. Authorized people can send and receive information from a distance using computer networks. We are living in an information age; we need to keep information about every aspect in our lives. In other words, information is an asset that has a value like any other assets. As an asset, information needs to be secured from attacks. To be secured, information needs to be hidden from unauthorized access **(confidentiality)**, protected from unauthorized change **(integrity)**, and available to an authorized entity, when it is needed **(availability)**. Although the three previously mentioned requirements have not changed, they now have some new dimensions.
The information be confidential, when it is stored in a computer; there should also be a way to maintain its confidentiality, when it is transmitted from one computer to another[1].Although people have hidden secrets in plain sight now called steganography throughout the ages, the recent growth in computational power and technology has propelled it to the forefront of today’s security techniques [2]. Steganography is the branch of science which deals with embedding secret message on the transmitter side and retrieving it successfully on the receiver side. Whether it is about copyright protection for piracy prevention or private personal communication, steganography is the emerging technique which would be the solution to such issues Strictly speaking, steganography is not only authentication provider through watermarking but a door to confidential communication as well [2][3].

Steganography is an art of hiding some secret message in another message without letting anyone know about presence of secret message except the intended receiver. The message used to hide secret message is called **host message or cover message.** Once the contents of the host message or cover message are modified, the resultant message is known as **stego-message**. In other words, stego-message is combination of host message and secret message. Steganography is often mixed up with cryptography.

Cryptography changes representation of secret message being transmitted while steganography hides presence of secret message [4].

Steganography can be applied to different type of media including text, audio and video. Files are considered to be excellent carriers for the purpose of steganography due to presence of redundancy**.**

1.2 Steganography and Cryptography

Basically, the purpose of cryptography and steganography is to provide secret communication. However, steganography is not the same as cryptography. Cryptography hides the contents of a secret message from a malicious people, whereas steganography even conceals the existence of the message. Steganography must not be confused with cryptography, where we transform the message so as to make it meaning obscure to a malicious people who intercept it. Therefore, the definition of breaking the system is different.

In cryptography, the system is broken when the attacker can read the secret message. Breaking a steganographic system need the attacker to detect that steganography has been used and he is able to read the embedded message. The following table has shown the comparison between Cryptography and Steganography [3][5].

Table (1.1) Comparison Between Steganography and Cryptograp

	Cryptography	Steganography
1	Known message passing.	Unknown message passing.
2	Common technology.	Little known technology.
3	The encrypted latter could be seen by anyone but cryptography message not understandable.	Steganography is hiding the message in another median so that nobody will notice the message.
4	The end result in cryptography is the cipher text.	The end result in steganography hiding is the stego-media.
5	The goal of a secure cryptography is to prevent an interceptor from gaining any information about the plaintext from the intercepted cipher text.	The goal of a secure steganography methods is to prevent an observant intermediary from even obtaining knowledge of the mere presence of the secret data.
6	Steganography cannot be used to adapt the robustness of cryptography system.	Steganography can be used in conjunction with cryptography by hiding an encrypted- -massage

1.3 Advantages of Steganography Based on Chaos

Chaotic maps is used to increase the security. The most attractive feature of chaos in information hiding area is its extreme sensitivity to initial conditions and the outspreading of orbits over the entire space. These special characteristics make chaotic maps excellent choice for information hiding [2].

The main advantages of the chaotic stenographic approach include:-

- Increasing the security.
- Easy implementation.
- More randomness.
- Sensitivity to initial conditions and parameters.
- Non-periodic.
- Confidential.

1.4 Literature Survey

There are many researches in each cryptography and steganography technique, a brief description of some of these researches are presented:-

- Muhalim Muhamed et. al [6] in 2003, proposed and implementation of steganographic tools for hiding information includes text and image files. Three different approaches being explored which are Least Significant Bit (LSB), masking and filtering and algorithms and transformation**.**
- Rosziati Ibrahim and Teoh Suk Kuan **[7]** in 2010, proposed a new algorithm to hide data inside image using steganography technique. The proposed algorithm uses binary codes and pixels inside an image.
- An algorithm is designed to hide all the data inputted within the image to protect the privacy of the data. Then, the system is developed based on the new steganography algorithm**.**
- Atallah M. Al-Shatnawi [8] in 2012, presented a new Steganography technique, implemented and analyzed.

  The proposed method hides the secret message based on searching about the identical bits between the secret messages and image pixels values. The proposed method is compared with the LSB benchmarking method.
- Dr. Sanjay Kumar Jena [9] in 2013 , proposed 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.

- Debiprasad Bandyopadhyay et al [10] in 2014, proposed to encrypt the secret bits of the message based on chaos theory before embedding into the cover image. LSB insertion method has been used for image steganography.
- N. S. Raghava1et al [11] in 2014 , proposeed a novel technique to improve the conventional LSB technique for image steganography by using pseudo random number generation using Henon chaotic map. The random numbers are used to encrypt the hide image which is embedded in the cover picture. This encryption using pseudo random generator provides sufficient security to the payload as the same set of random numbers cannot be regenerated without knowing the exact random generator function and thus the secret data cannot be retrieved easily.
- Shreenandan Kumar et al [12] in 2015, they have used chaotic Logistic map to generate the pseudo random numbers ; the index values of the sorted pseudo random numbers generated by Logistic map are the positions used to embed the message in the cover image.

1.5 Aims of the Work

The aims of this work are summarized, as follows:-

1- To produce security tool based on the least significant bit (LSB) technique suggested to hide information (text) inside image.

2- To get an acceptable quality of the extracted message , beside the good quality of stego image should.

3- To avoid suspicion to transmission of hidden message ,and to conceal information, making it unseen, such that it is highly secured..

1.6 Thesis Outline

This thesis is organized in five chapters, as follows:

Chapter One: - Gives an introduction about steganography and cryptography and gives a brief description of related literatures and aims of the work.

Chapter Two:- Discusses the proposed steganography and cryptography systems , its basic idea and the main algorithms.

Chapter Three: - Presents the results obtained from the tests (PSNR and histogram) for image

Chapter Four: - Includes the conclusions and some suggestions for future works.

2.1 Introduction

An information hiding system has been developed for confidentiality. However, 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. For embedding the data into an image, we require two important files. The first is the original image so called cover-image. The image (gif) format will hold the hidden information. The second file is the message itself, which is the information to be hidden in the image. In this process, we decided to use a plaintext as the message.

Before embedding process, the size of image and the message must be defined by the system. This is important to ensure the image can support the message to be embedded. The ideal image size is 800x600 pixels, which can embed up to 60kB messages. The cover-image will be combined with the message. This will produce the output called stego-image. Figure 4.1 is illustrated the process. The Stego-image seems identical to the cover-image. However, there are hidden message that imperceptible.

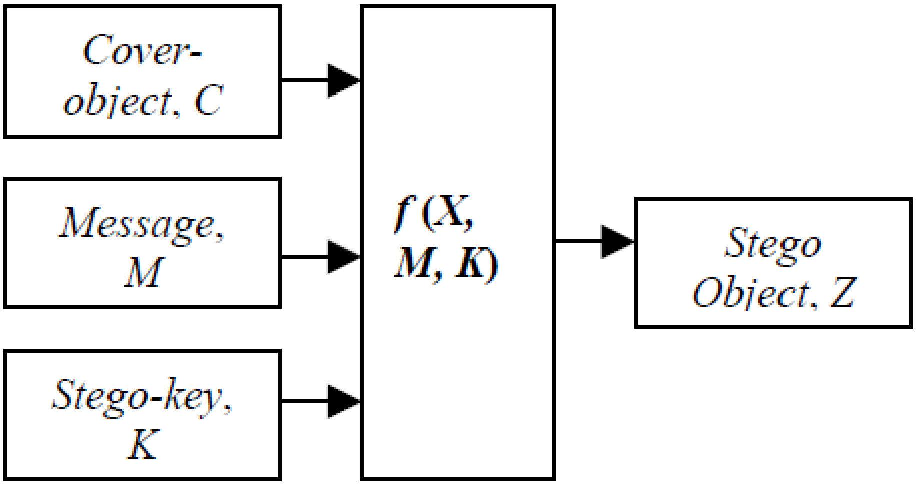


Figure 2.1 Producing Stego-Image Process

Basically, the model for steganography is shown on Figure 4.1 [1]. Message is the data that the sender wishes to remain it confidential. It can be plain text, ciphertext, other image, or anything that can be embedded in a bit stream such as a copyright mark, a covert communication, or a serial number. Password is known as stego-key, which ensures that only recipient who know the corresponding decoding key will be able to extract the message from a cover-object. The cover-object with the secretly embedded message is then called the stego-object. Recovering message from a stego-object requires the cover-object itself and a corresponding decoding key if a stego-key was used during the encoding process. The original image may or may not be required in most applications to extract the message.

2.2 Steganography

Steganography is a very old method of passing messages in secret. Steganography is a type of hidden communication process, this method of message cloaking goes back to the time of the ancient Greeks literally means "covered writing" (according to the Greek, the words stegano or "covered" and graphs or "to write")[13]**.** In the 5th century BC the historian Herodotus wrote about how an agent wrote a message warning of an invasion on the wood part of a wax tablet. To avoid capture, he scraped the wax off of the tablets and wrote the message on the underlying wood. Then, he covered the tablets with wax again. The tablets appeared to be blank and unused so they passed inspection [3].Scientists have developed new chemical substances that, combined with other substances, cause a reaction that makes the result visible. One of them is gallotanic acid, made from gall nuts, that becomes visible when coming in contact with copper sulfate**.** With the continuous improvement of lenses, photo cameras, and films, people were able to reduce the size of a photo down to the size of a printed period. One such example is micro-dot technology, developed by the Germans during the World War II. Generally, micro-dots were not hidden, nor encrypted messages. They were just so small as to not draw attention to themselves. The micro-dots allowed the transmission of large amounts of data (e.g., texts, drawings, and photographs) during the war. There are also other forms of hidden communications, like null ciphers.

The messages are very hard to construct and usually look like strange text. This strangeness factor can be reduced if the constructor has enough space and time. A famous case of a null cipher is the book Hypteronomachia Poliphili of 1499[2][3][13].

2.2.1 Basic Model for Steganographic System

A common model and terminology for information hiding has been established since 1996 in a workshop in Cambridge. This model is shown in Figure (2.1)[2].

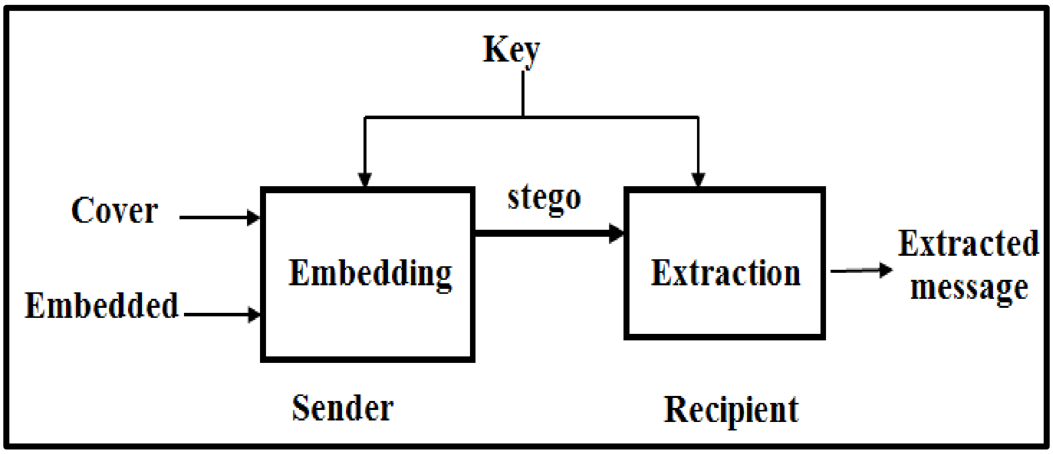


Figure (2.2) The embedding model

A stego-system consists of :-

1. A cover; (an image, an audio file, a data file or any digital file).
2. The embedding algorithm.
3. The secret embedded message.
4. A secret key.

As shown in Figure (2.1) Steganography is comprised of two algorithms, one for **embedding** and one for **extracting**. The embedding process is concerned with hiding a secret message within a cover work, and is the most carefully constructed process of the two. A Steganographic algorithm combines the cover massage with the embedded message, which is something to be hidden in the cover. The algorithm may, or may not, use a Steganographic key (stego key), which is additional secret data that may be needed in the hidden process .

The same key (or related one) is usually needed to extract the embedded massage again. The output of the Steganographic algorithm is the stego message.

The cover massage and stego message must be of the same data type, but the embedded message may be of another data type. The receiver reverses the embedding process to extract the embedded message [3][14].

2.2.2 Steganographic Protocols

There are three types of steganographic protocols which are:-

1. Pure steganography: We call a steganography system which does not require the prior exchange of some secret information (like a stego-key) pure steganography. Both the sender and the receiver must have access to the embedding and extraction algorithm, but the algorithm should not be public[15].

2. Secret Key Steganography: The security of a steganography system should thus rely on some secret information traded by sender and recipient, the stego-key. Without knowledge of this key, nobody will be able to extract secret information out of the cover[15].

3. Public Key Steganography: Public key steganography does not rely on the exchange of a secret key. Public key steganography systems require the use of two keys, one private and one public; the public key is stored in a public database; whereas, the public key is used in the embedding process, the secret key is used to reconstruct the secret message [15].

2.2.3 Types of Steganography

The main five categories of file formats that can be used for steganography are:-

1. **Text Steganography:** Hiding information in text is the most important method of steganography. The method was used to hide a secret message in every nth letter of every word of a text message. After booming of Internet and different types 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 redundant data[3][14]
2. **Image Steganography:** Images are used as the popular cover objects for steganography. A message is embedded in a digital image through an embedding algorithm, using the secret key. The resulting stego-image is sent to the receiver. During the transmission of stego-image, unauthenticated persons can only notice the transmission of an image, but cannot guess the existence of the hidden message. On the other hand, it is processed by the extraction algorithm using the same key[3][14].

3. **Audio Steganography:** Audio stenography is masking, which exploits the properties of the human ear to hide information unnoticeably. 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[3][14].
4. **Video Steganography:** This is a combined image plus audio steganography , since a video consists of frames of images and audios[3][14].
5. **Protocol Steganography:** The term protocol steganography is to embed information within network protocols such as TCP/IP. Information in the header of a TCP/IP packet is hidden in some fields that can be either optional or are never used[3][14].

2.2.4 Steganography Techniques

Many steganography techniques had been proposed during the last few years. These techniques differ in the mechanism or principle being used to hide a secret message or the changes that are taking place during the entire process of embedding. Therefore, there are six categories of steganography techniques:-

A) Substitution Techniques

For a given cover file, it is important to find out some areas or data that can be modified without having any significant effects on this cover file. Therefore, a secret message can be embedded by replacing the redundant or insignificant parts of a cover file with secret message bits, without adding any significant noise to this cover file, so the receiver can extract the secret message if he has knowledge of the right embedding position.

Generally, digital covers have a large number of redundant bits (e.g. Least Significant Bits (LSB)).

In the substitution technique of steganography, the bits of the secret message substitute the LSB of the bytes of the cover file without causing a drastic change to this cover file.

Moreover, the LSB technique is a spatial domain technique since it embeds the secret bits directly in the cover file. Since LSB substitution technique is relatively quick and easy to use, it is the most common technique used for digital steganography and especially with digital images [2].

B) Transform Domain Techniques

This is a more complex way of hiding information in an image. Various algorithms and transformations are used on the image to hide information in it. Transform domain embedding can be termed as a domain of embedding techniques for which a number of algorithms have been suggested**.** It has been noted early in the development of steganographic systems that embedding information in the frequency domain of a signal can be much more robust than embedding rules operating in the time domain. Many transform domain variations exist. One method is to use the Discrete Cosine Transform DCT, another would be the use of Wavelet Transform and Contourlet Transform [2][14].

C) Spread Spectrum Techniques

Spread spectrum communication is defined as ”the process of spreading the bandwidth of a narrowband signal across a wide band of frequencies”. In spread spectrum steganography, the frequency domain of the cover file is considered to be a communication channel and the secret message as a signal that is transmitted through it. Since the secret message is spread through a wide frequency band, this technique is relatively robust against stego-file modification or message removal [2][14].

D) Statistical Techniques

These techniques embed only one bit of secret data in a cover file. Therefore, it is known as “1-bit” steganography scheme. If “1” is hidden in a cover file, some statistical characteristics (e.g. entropy and probability distribution) of this cover file must be changed significantly to clearly indicate the existence of a message.

However, if the hidden bit is “0”, the cover file is left unmodified. Therefore, this technique entirely depends on the ability of the receiver to differentiate between changed and intact cover files [2][14].

E) Distortion Techniques

Most of the steganography techniques are blind, which means that a receiver does not need the original cover file to extract the hidden message from the corresponding stego-file. However, if a distortion technique is used, the receiver requires the original cover file in order to recover the secret message.

For a receiver, the embedded message is the difference between the modified cover file received (the stego-file) and the original cover file [2].

F) Cover Generation Techniques

In contrast to all embedding methods presented above, where secret information is added to a specific cover by applying and embedding algorithm, some steganographic applications generate a digital object only for the purpose of being a cover for secret communication. Such as in generating a fractal images as cover images each of which is uniquely defined by a set of fractal parameters such as type, formula, scale, location, color space etc. In other words, the fractal image can be perfectly restored as long as this set of parameters is known. This set of parameters can be saved as a particular file, which can be transported very easily. Therefore, the cover image can be perfectly restored [2].

2.2.5 Steganography Attacks

Steganalysis is the art and science of detecting hidden messages from images made from stego-systems. Steganography attacks consist of detecting, extracting and destroying hidden object of the stego-media. There are several types of attacks based on the information available for analysis. Some of these attacks are:-

- Steganography only attack: In this type of attack, only stego-media is available for analysis.
- Known carrier attack: The original cover media and stego-media are both available.
- Known message attack: The hidden message is known in this case.
- Known steganography attack: The cover media, stego-media as well as the steganography tool or algorithm, are known[15].

2.3 Images

An image is a visual representation of an object, a person, or a scene produced by an optical device such as a mirror, a lens, or a camera. This representation is two dimensional (2D), although it corresponds to one of the infinitely many projections of a real-world, three-dimensional (3D) object or scene[16].

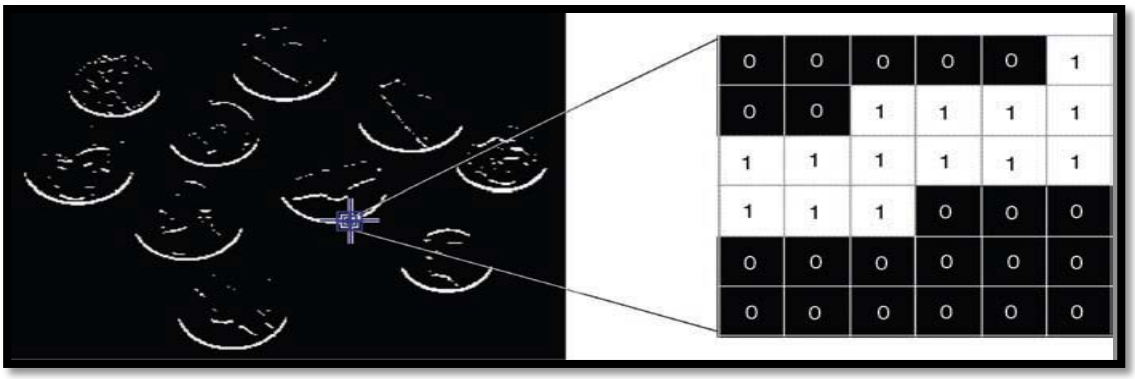
2.3.1 Digital Images

A Digital Image is a representation of a two-dimensional image as a finite set of digital values, called picture elements or pixels. Pixels **(**short for picture elements) are the smallest individual elements in an image (The digital image consists of pixels), holding quantized values that represent the brightness of a given color at any specific point. The position of each pixel is specified in terms of an index for the number of columns and another for the number of rows.

These values are often transmitted or stored in a compressed form. Digital images can be created by a variety of input devices and techniques, such as digital cameras, scanners, etc. there are three general types of digital image:-

2.3.1.1 Binary Images

A binary image is a digital image that has only two possible values for each pixel. It is also called bi-level or two-level. (The names black and white, B&W monochrome or monochromatic are often used for this concept, but may also designate any images that have only one sample per pixel, such as grayscale images). Some systems interpret the bit value of 0 as black and 1 as white, while others reversed the meaning of the values. A binary image is usually stored in memory as a bitmap, a packed array of bits[16]. Figure(2.3) shows a binary image

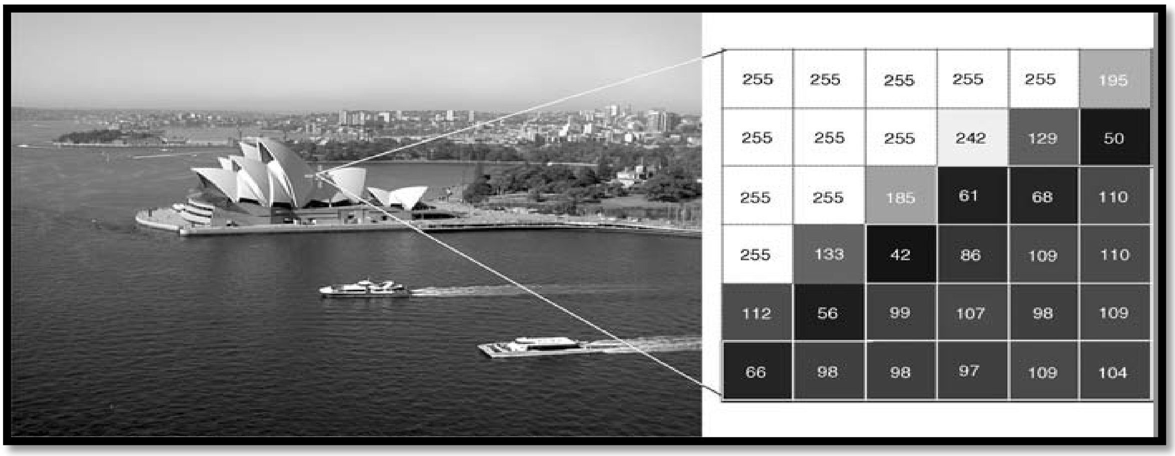


0	0	0	0	0	1
0	0	1	1	1	1
1	1	1	1	1	1
1	1	1	0	0	0
0	0	0	0	0	0
0	0	0	0	0	0

Figure (2.3) Binary Image.

2.3.1.2 Grayscale Images

A grayscale digital image is an image in which the value of each pixel is a single sample. Displayed images of this sort are typically composed of shades of gray, varying from black at the weakest intensity to white at the strongest, though in principle the samples could be displayed as shades of any color, or even coded with various colors for different intensities. Grayscale images intended for visual display are typically stored with 8 bits per sampled pixel, which allows 256 intensities (i.e., shades of gray) to be recorded, typically on a nonlinear scale[16]. Figure (2.4) shows a grayscale image.

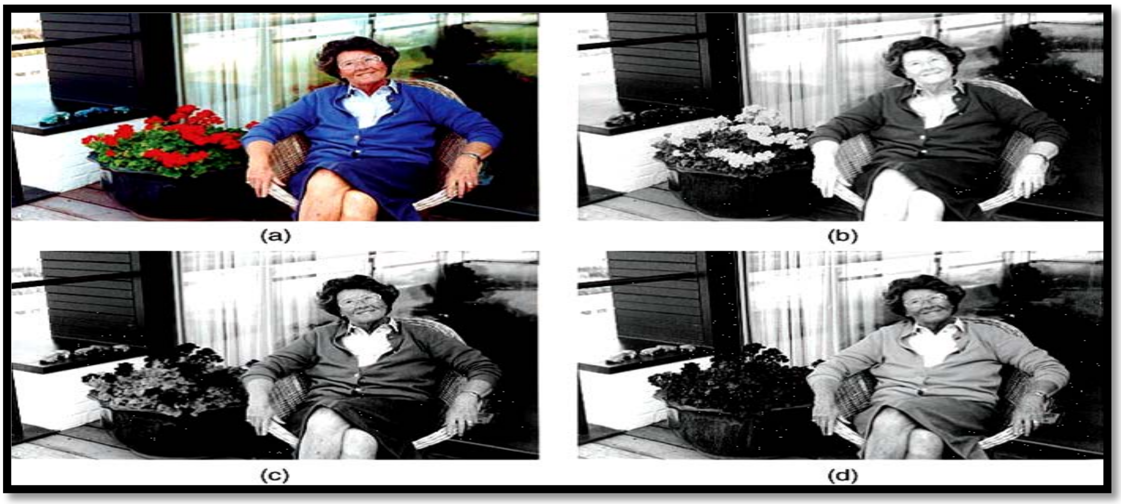


255	255	255	255	255	195
255	255	255	242	129	50
255	255	185	61	68	110
255	133	42	86	109	110
112	56	99	107	98	109
66	98	98	97	109	104

Figure (2.4) Gray Scale Image.

2.3.1.3 Color Images

A color image is a digital image that includes color information for each pixel. For visually acceptable results, it is necessary (and almost sufficient) to provide three samples (color channels) for each pixel, which are interpreted as coordinates in some color space. It is usually stored in memory as raster map, a two-dimensional array of small integer triples, or (rarely) as three separate raster maps, one for each channel. Eight bits per sample (24 bits per pixel) seem to be adequate for most uses. On the other hand, some widely used image file and graphics cards may use only 8 bits per pixel, only 256 different colors, or 2-3 bits per channel [16].



Figure(2.5) Color Image (a) and its R(b), G (c), and B (d) components.

2.4 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.

(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 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 successfully. The resulting changes that are made to the least significant bits are too small to be recognized 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 figure 2.6,2.7 shows the mechanism of LSB technique.

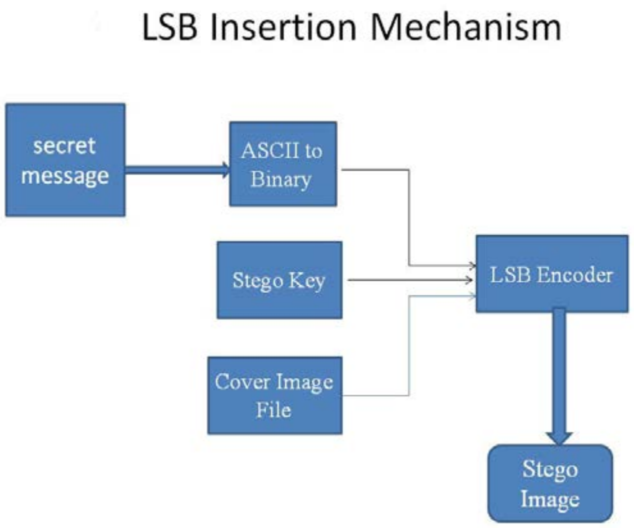


Figure 2.6: LSB insertion Mechanism

2.4.1 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.

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]

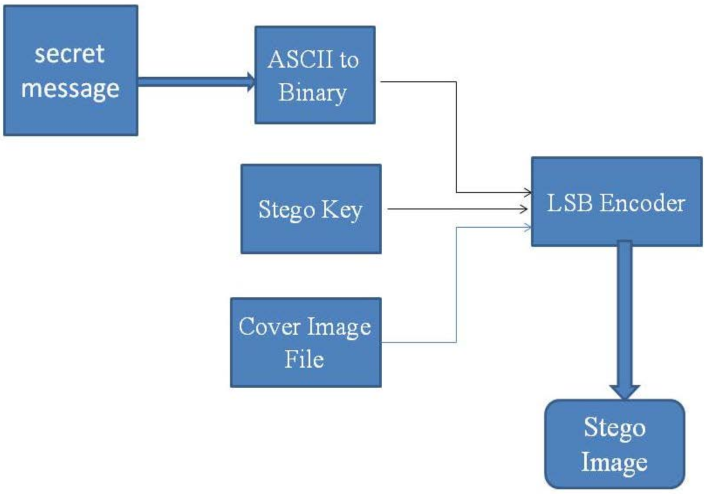


Figure 2.7: LSB extraction Mechanism

2.4.2 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 **Step 3** 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].

2.4.3 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].

3.1 Introduction

The security of information has become a fundamental issue to provide confidentiality and protecting the copyright for digital media such as audio, video, and images. Therefore, the steganography is applied to hide some information in digital media, whereby the message is embedded in a digital media. In this project, we proposed the Secure Information Hiding System (SIHS) that is based on Least Significant Bit (LSB) technique in hiding messages in an image. The system enhanced the LSB technique by randomly dispersing the bits of the message in the image and thus making it harder for unauthorized people to extract the original message.

Discrete logarithm calculation technique is used for determining the location of the image pixels to embed the message. The proposed algorithm provides a stego-key that will be used during the embedding and extracting of the message. Common techniques used in steganography are least significant bit insertion (LSB), masking and filtering, and transformation techniques. Here we present an LSB technique, which randomly select the pixels of the cover-object that is used to hide the secret message as shown in figure below.

3.2 Overview of Steganography

Main goal of steganography is to communicate securely in a completely undetectable manner [15] and to avoid drawing suspicion to the transmission of a hidden data [8]. Therefore, in existing communication methods, steganography can be used to carry out hidden exchanges. the model for steganography is as shown in Figure 1. The cover-object is a carrier or medium to embed a message. There are several suitable medium that can be used as cover-objects such as network protocols, audio, file and disk, a text file and an image file [14]. Message is the data that the sender wishes to keep confidential and will be embedded into the cover-object by using a stegosystem encoder. It can be a plain text, a cipher text, an image, or anything that can be embedded in a bit stream such as a copyright mark or a serial number.

A stego-key is a password, which ensures that only the recipient who knows the corresponding decoding key will be able to extract the message from a cover-object.

The output of the stegosystem encoder is known as the stego-object.
A stegosystem encoder can be represented by using the following relation [17]:

$$I' = f\,(I, m, k) \qquad \ldots\ldots\ldots(1)$$

where I' is the stego-object

I is the cover-object

m is the message

k is the stego-key.

Recovering message from a stego-object requires the cover-object itself and a corresponding decoding key if a stego-key was used during the encoding process. The original image may or may not be required in most applications to extract the message.

In general, the information hiding process extracts disused bits from cover-object. The process consists of two steps [11,12]:

(i) Identification of disused bits in a cover-object

.

Disused bits: are those bits that can be modified without corrupting the quality or destroying the integrity of the cover-object.

(ii) Embedding process. It selects the subset of the disused bits to be replaced with data from a secret message. The stego-object is created by replacing the selected disused bits with message bits.

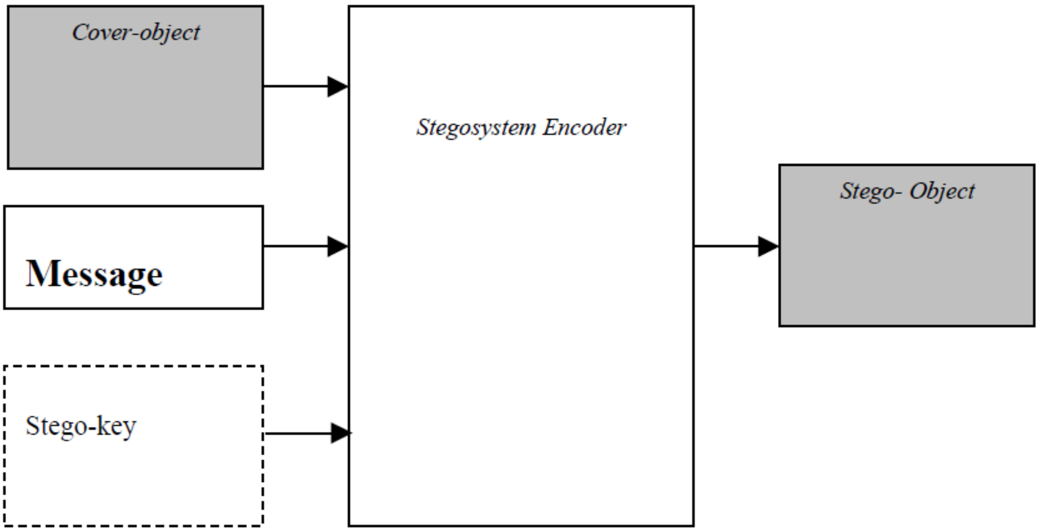


Figure 3.1 Basic Model of Steganography

We proposed the Secure Information Hiding System (SIHS) that is based on Least Significant Bit (LSB) technique in hiding messages in an image. The proposed method embeds the message into random positions as in [22].

3.3 Secure Information Hiding System (SIHS)

LSB is the most simple and a straight forward approach to embed or hide a message into a cover-image [11]. A system named Secure Information Hiding System (SIHS) is proposed to improve the LSB scheme. SIHS overcome the sequence-mapping problem by embedding the message into a set of random pixels, which are scattered on the cover-image. The bits of the secret message is embedded in pixels of the cover-image that are generated by discrete logarithm calculation.The main idea here is to generate random numbers without any repetition. With this set of random numbers, a random-mapping can be done. Briefly, we defined discrete logarithm in the following way to produce random numbers. First, we defined a primitive root of a prime number **p** as one whose powers generate all the integers from **1 to (p – 1)**.

That is, if **a** is a primitive root of the prime number **p**, then the numbers

$a \bmod p, a^2 \bmod p, \ldots, a^{p-1} \bmod p$

are distinct and consist of the integers from 1 through (p – 1) in some permutation. Therefore, if a is the primitive root of p, then its powers

$a, a^2, \ldots, a^{p-1}$

are all relatively prime to p with distinct numbers. For any integer y and a primitive root a of prime number p, one can find a unique exponent i such that [17]

$$y = a^i \bmod p \ldots\ldots\ldots\ldots(2)$$

where $0 \leq i \leq (p - 1)$.

The exponent i is referred to as the discrete logarithm, or index, of y for the base a, mod p.

3.3.1 Workflow of SIHS

The flowchart in Figure 2 illustrates the implementation of the system. The stego-process starts with the selection of a cover-image to hide a message. The user will then select a key k, which will depends on the size of the message, m and the image, I. The value of k lies in the range,

$$m < k < I$$

On this stego-system, a prime number, p is obtained by searching for the first prime number that exceeds the key, **k**.

Then a primitive root, **a**, is derived by using equation(1).The primitive root, **a**, is then used to generate a set of random numbers, $\mathbf{y_i}$. This set of random numbers will determine the position of the pixel to embed the bits from the message.The discrete logarithm ensures that the pixels chosen are distinct. The message bits are then mapped onto the cover-image by the stego-system encoder in the following manner:

$$M_i \rightarrow I\ y_i\ ,$$

Where:

M_i is the ith bit of the message,

$I\ y_i$ is the ith random number generated.

Recovering message from a stego-image requires the corresponding decoding key, **k**, which was used during the encoding process. Therefore, both the sender and receiver must share the stego-key during the communication. The key is then used for selecting the positions of the pixel where the secret bits had been embedded.

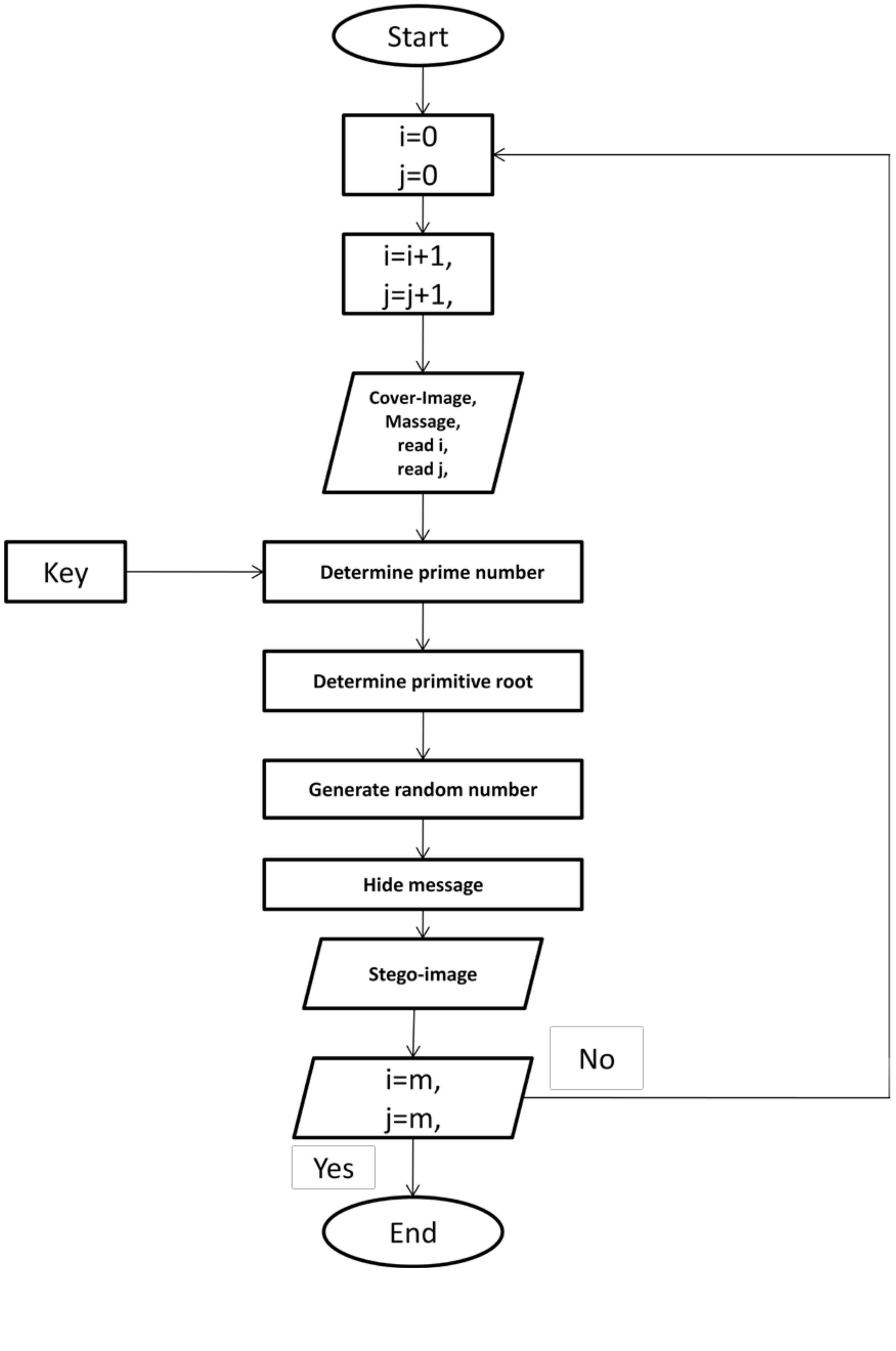
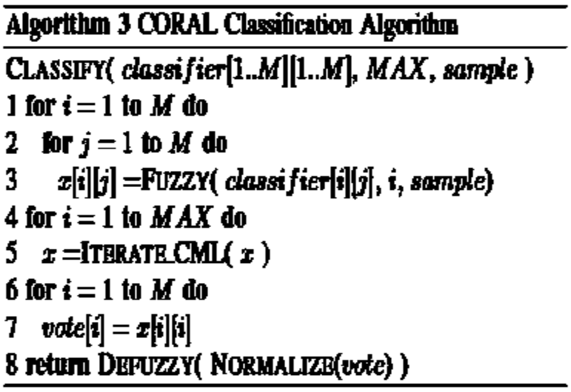


Figure 3.2 Flow Chart for SIHS

3.3.2 Analysis of SIHS

For the system analysis, the testing are done through the normal viewing of the human eyes. As mentioned before, this system has been developed to overcome a sequence-mapping problem when using LSB. An image with 200x200 in size and a message of 1 KB as shown in Figure 3.3 and Figure 3.4, respectively, have been chosen to test the technique.

the secret image



```
Algorithm 3 CORAL Classification Algorithm
CLASSIFY( classifier[1..M][1..M], MAX, sample )
for $i = 1$ to $M$ do
    for $j = 1$ to $M$ do
        $x[i][j]$ =FUZZY( classifier[i][j], i, sample)
for $i = 1$ to $MAX$ do
    $x$ =ITERATE_CML( $x$ )
for $i = 1$ to $M$ do
    $vote[i] = x[i][i]$
return DEFUZZY( NORMALIZE(vote) )
```

Figure 3.3 A text Message

In this case we used a color image as shown in Figure 3.4. With a stego-key of 7000, we embedded the message of Figure 3.3 into the cover-image and the resulted stego-image is as shown in Figure 4.5. From normal eyes perception, the result of the stego-image looks identical to the cover-image. This is because there is a little changes of the pixel values and thus no significant difference.

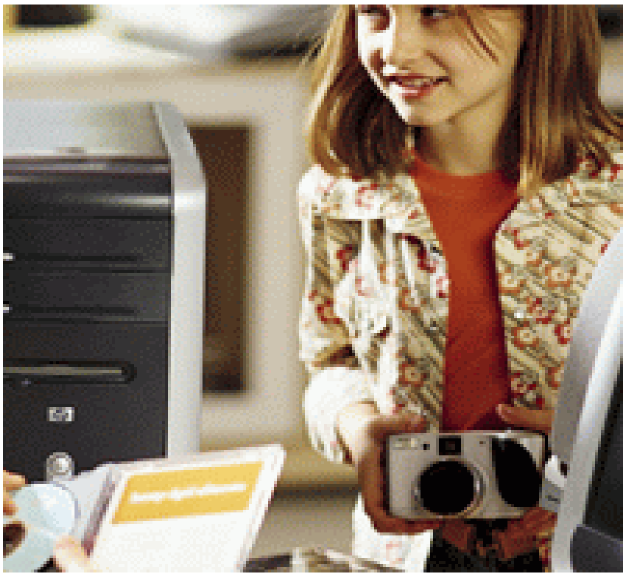


Figure 3.4 Cover-Image

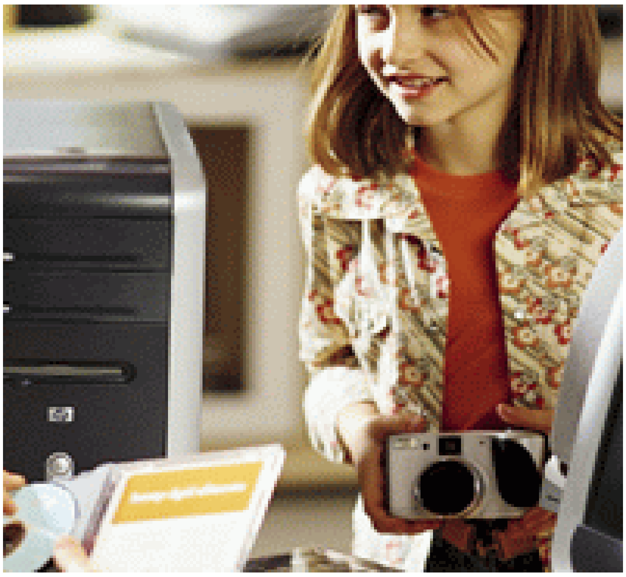


Figure 3.5 Stego-Image

3.4 Measures of Quality of the Proposed System

As a performance measure for image distortion due to hiding 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:

3.4.1 Peak-Signal-to-Noise-Ratio (PSNR)

According to the human visual system (HVS), some amount of distortion between the original image and the modified one is allowed. Signal-to-Noise Ratio (often abbreviated SNR or S/N) is a measure used in science and engineering to compare the level of a desired signal to the level of background noise[2].

Here, for the purpose of measuring the quality of the reconstructed image, The **P**eak **S**ignal-to-**N**oise **R**atio known as **PSNR** is used. PSNR is usually measured in dB. To compute the peak signal to noise ratio, then:-

$$\mathbf{PSNR = 10log_{10}\frac{255^2}{MSE}} \qquad (\mathbf{3-4})$$

Where; **MSE** which measures the cumulative **M**ean **S**quare **E**rror between the original and the reconstructed image. The mean square error (**MSE**) is defined as: -

$$\mathbf{MSE = \frac{1}{N\times M}\sum_{i=0}^{N-1}\sum_{j=0}^{M-1}[X(i,j) - \widehat{X}\,(i,j)]^2} \quad (\mathbf{3-5})$$

Where:- N: height of the two images

M: width of the two images.

i and j : row and column numbers.

X(i,j): is the original image. $\widehat{X}$(i,j): is the stego image

By using Visual basic program, the result of PSNR as follows:-

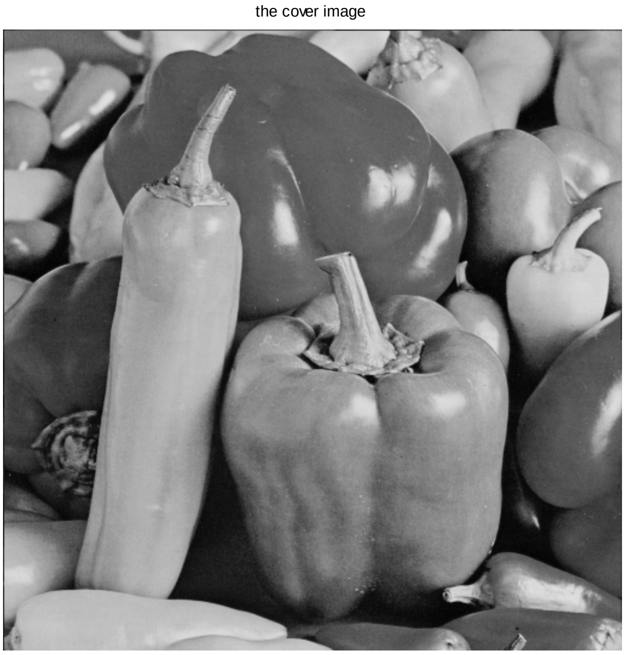

the cover image

Figure 3.6 The cover image

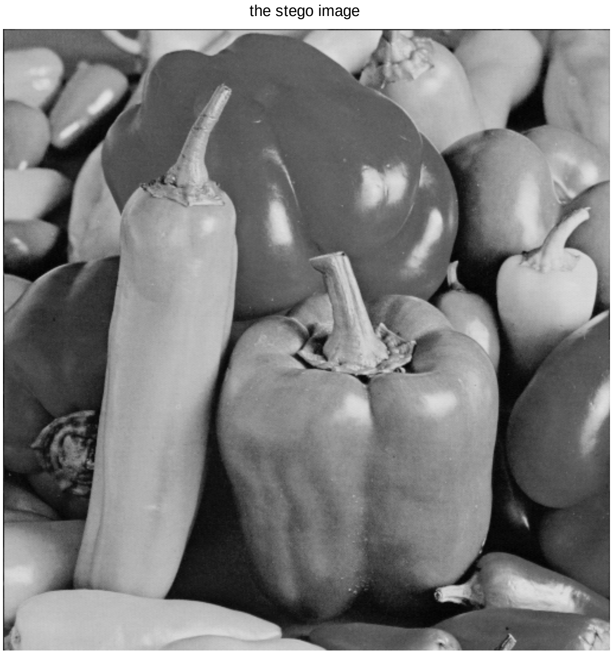

the stego image

Figure 3.7 The stego-image

Table (3.2.a): PSNR of Least Significant Bits Encoding

Cover Image	Secret Message	Stego-Image	MSE	PSNR(dB)
Gray image	Text Message	Gray image	0.0463	61.4733

Table (3.2.b): PSNR of Pseudo-Random Encoding [20]

Cover Image	Secret Message	Stego-Image	MSE	PSNR(dB)
Gray image	Text Message	Gray image	0.0449	61.6065

By using the LSB Technique on images to obtain secure stego-image. Table (3.2.a) and Table (3.2.b) 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 other insertion. 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.

The algorithm is usage for 8 bit image of the same size of cover and secret image, so it is easy to be implementing in grayscale image. This work focuses on the approach like increasing the security of the message and increasing PSNR and reducing the distortion rate.

4.1 Conclusion

Steganography can be used for hidden communication. We have explored the limits of steganography theory and practice. We pointed out the enhancement of the image steganographic system using LSB approach to provide a means of secure communication. A stego-key has been applied to the system during embedment of the message into the cover-image. In our proposed approach, the message bits are embedded randomly into the cover-image pixels instead of sequentially. Still efforts have to be made to increase the embedding capacity and maintain secrecy. Efforts can be made to hide text files having more size than image size. At last, we have shown that steganography that uses a key has a better security than non-key steganography. This is so because without the knowledge of the valid key.

A technique can be evolved so that these keys can be generated and distributed covertly. The transform domain method can be utilized if more security is required. If Steganography is used with Cryptography, it will prove to be an unbeatable tool in secure communication links. Security of the scheme can be improved by using advanced cryptography techniques and also improve the efficiency by using data compression techniques.The proposed system offers high level of security in term of transmitting the resultant stego-image without raising suspicion. It hides the secret message based on searching about the identical bits between the secret messages and image pixels values.

It was compared with the LSB method for hiding the secret message which hide the secret message directly in the least significant bit of the image pixels. The proposed method is more efficient, simple and appropriate. It search about the identical then start hiding, hence the change in the image resolution is quite low, as well as it makes the secret message more secure. This project concluded that the LSB hiding method is the improved case of the proposed method.

4.2 Suggestions for Future Works

As the information hiding system has been made successfully in this work, the following recommendations are suggested for further research work in this field:

1. Applying LSB to hide another multimedia such as audio and video.
2. Increase the system complexity by using multi-chaotic system to generate random number and add additional layers of encryption.
3. It is possible to use video or sound as the cover image.
4. Using another   hiding method include transform domain in which the signal is more sparse, and; therefore, little details . such as using wavelet, lifting wavelet and multi-wavelet.

REFERENCES:

1. Shashikala Channalli And Ajay Jadhav, "Steganography An Art Of Hiding Data", Sinhgad College Of Engineering, Pune, Shashikala Channalli Et Al /International Journal On Computer Science And Engineering Vol.1(3), 137-141,2009.
2. Zaynab Najeeb Abdulhameed," High Capacity Steganography Based On Chaos And Contourlet Transform For Hiding Multimedia Data", M.Sc. Thesis, Department of Electronics & Communications Engineering ,University of AL-Mustansiriy 2014.
3. T. Morkel , J.H.P. Eloff , M.S. Olivier" An Overview Of Image Steganography" Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science, University of Pretoria, Pretoria, South Africa,2005.
4. FAHIM IRFAN ALAM "An Investigation into Encrypted Message Hiding Through Images Using LSB", International Journal of Engineering Science and Technology (IJEST), 2011.
5. Jing Xia, Suwen Zheng, Baohong Lv, Caihong Shan"Harmonic Solutions of Duffing Equation with Singularity via Time Map", Applied Mathematics, 2014, 5,1528-1534.

6. Shreenandan Kumar, Suman Kumari, Sucheta Patro, Tushar Shandilya and Anuja Kumar Acharya"Image Steganography using Index based Chaotic Mapping", International Conference on Distributed Computing and Internet Technology (ICDCIT), 2015.
7. Vaibhav Poonia and Dr. Narendra Singh Yadav" Analysis of modified Blowfish Algorithm in different cases with various parameters", International Journal of Engineering Research and General Science Volume 3, Issue 1, January-February, 2015.
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 (IJC-SET) "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 _les." 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 e_cient 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.

الخلاصة

لقد أصبح لإخفاء الصورة مساحة واسعة في موضوع الإخفاء . بسبب ازدياد الحاجة إلى الحماية والسرية أدى ذلك الضرورة الملحة لحماية المعلومات . خوارزمية البت الأقل أهمية هي من الخوارزميات المهمة لإخفاء الرسائل . تعتمد هذه النظرية على تغيير البت الأقل أهمية . وهذا يؤدي إلى تغيير في ملامح الصورة الأصلية يتم الإخفاء فيها وهذا يؤدي إلى ظهور اختلافات بين الصورة الأصلية والصورة بعد إخفاء المعلومات فيها . لذلك في هذا البحث تم التغلب على هذه الحالة للحصول على صورة ذات دقة واضحة . هذا العمل يعطي نظرة عن الإخفاء ويعزز موثوقية المعلومات المخفية وسريتها بالإضافة إن هذا العمل يبين الفوائد والمضار باستخدام خوارزمية البت الأقل أهمية .

جمهورية العراق

وزارة التعليم العالي والبحث العلمي

جامعة ديالى

كلية الهندسة / قسم الأتصالات

أخفاء نص داخل صورة بأستخدام خوارزمية البت الأقل أهمية

مشرروع مقدم الى قسم هندسة الأتصالات

في جامعة ديالى - كلية الهندسة

كجزء من متطلبات نيل درجة البكلوريوس

في هندسة الأتصالات

من قبل:

فرح عباس

رونق صفاء الدين

بأشراف:

م.م حسين شكور مغير

May/2016