INFORMATION HIDING
USING STEGANOGRAPHY

MUHALIM MOHAMED AMIN
SUBARIAH IBRAHIM
MAZLEENA SALLEH
MOHD ROZI KATMIN

Department of Computer System & Communication Faculty of
Computer Science and Information system

UNIVERSITI TEKNOLOGI MALAYSIA

2003

ABSTRACT

The Internet as a whole does not use secure links, thus information in transit may be vulnerable to interception as well. The important of reducing a chance of the information being detected during the transmission is being an issue now days. Some solution to be discussed is how to passing information in a manner that the very existence of the message is unknown in order to repel attention of the potential attacker. Besides hiding data for confidentiality, this approach of information hiding can be extended to copyright protection for digital media. In this research, we clarify what steganography is, the definition, the importance as well as the technique used in implementing steganography. We focus on the 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.

Keyword*: Steganography, information hiding*

Key Researchers:

Muhalim bin Mohamed Amin,

Puan Subariah Ibrahim,

Puan Mazleena Salleh,

Mohd Rozi Katmin

E-mail: muhalim@fsksm.utm.my
Tel. No: 07-5532385
Vote No: 71847

ABSTRAK

Internet secara menyeluruh yang tidak menggunakan sambungan yang selamat boleh menyebabkan maklumat yang dihantar akan terdedah kepada gangguan. Kepentingan mengurangkan peluang mengesan maklumat semasa penghantaran menjadi isu sekarang ini. Sesetengah penyelesaian yang perlu dibincangkan adalah bagaimana untuk menghantar maklumat dalam keadaan kewujudan mesej tidak diketahui oleh penceroboh. Di samping menyembunyikan data untuk urusan sulit, pendekatan penyeembunyian maklumat boleh digunakan untuk melindungi hak milik bagi media digital. Dalam penyelidikan ini, kami menentukan apakah itu steganografi, definisinya, kepentingannya sebagai kaedah yang digunakan dalam perlaksanaan steganografi. Kami memfokuskan kepada teknik LSB (Least Significant Bit) dalam penyembunyian mesej di dalam sesuatu gambar/imej. Sistem ini meningkatkan teknik LSB dengan menyelerakkan bit mesej secara rawak di dalam imej dan kemudian menyukarkan pihak yang tidak berhak untuk mendapatkan semula mesej asal.

Kata kunci: Steganografi, penyembunyian maklumat

Penyelidik:

Muhalim bin Mohamed Amin,
Puan Subariah Ibrahim,
Puan Mazleena Salleh,
Mohd Rozi Katmin

E-mail: muhalim@fsksm.utm.my
Tel. No: 07-5532385
Vote No: 71847

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.1 Introduction

One of the reasons that intruders can be successful is that most of the information they acquire from a system is in a form that they can read and comprehend. Intruders may reveal the information to others, modify it to misrepresent an individual or organization, or use it to launch an attack. One solution to this problem is, through the use of steganography. Steganography is a technique of hiding information in digital media. In contrast to cryptography, it is not to keep others from knowing the hidden information but it is to keep others from thinking that the information even exists.

1.2 Background of the Problem

Steganography become more important as more people join the cyberspace revolution. Steganography is the art of concealing information in ways that prevent the detection of hidden messages. Steganography include an array of secret communication methods that hide the message from being seen or discovered.

The goal of steganography is to avoid drawing suspicion to the existence of a hidden message. This approach of information hiding technique has recently become important in a number of application areas. Digital audio, video, and pictures are increasingly furnished with distinguishing but imperceptible marks, which may contain a hiddin copyright notice or serial number or even help to prevent unauthorized copying directly.

Military communications system make increasing use of traffic security technique which, rather than merely concealing the content of a message using encryption, seek to conceal its sender, its receiver or its very existence. Similar techniques are used in some mobile phone systems and schemes proposed for digital elections.

Some of the techniques used in steganography are domain tools or simple system such as least significant bit (LSB) insertion and noise manipulation, and transform domain that involve manipulation algorithms and image transformation such as discrete cosine transformation and wavelet transformation. However there are technique that share the characteristic of both of the image and domain tools such as patchwork, pattern block encoding, spread spectrum methods and masking.

1.3 Objective

This project comprehends the following objectives:

(i) To produce security tool based on steganographic techniques.

(ii) To explore techniques of hiding data using steganography.

1.4 Scope

The scope of the project as follow:

(i) Implementation of steganographic tools for hiding information includes text and image files.

(ii) Three different approaches being explored which are least significant bit, masking and filtering and algorithms and transformation.

CHAPTER 2

INFORMATION HIDING USING STEGANOGRAPHY

2.1 Introduction

Due to advances in ICT, most of information is kept electronically. Consequently, the security of information has become a fundamental issue. Besides cryptography, steganography can be employed to secure information. Steganography is a technique of hiding information in digital media. In contrast to cryptography, the message or encrypted message is embedded in a digital host before passing it through the network, thus the existence of the message is unknown. Besides hiding data for confidentiality, this approach of information hiding can be extended to copyright protection for digital media: audio, video, and images.

The growing possibilities of modern communications need the special means of security especially on computer network. The network security is becoming more important as the number of data being exchanged on the Internet increases. Therefore, the confidentiality and data integrity are requires to protect against unauthorized access and use. This has resulted in an explosive growth of the field of information hiding.

In addition, the rapid growth of publishing and broadcasting technology also require an alternative solution in hiding information. The copyright such as audio, video and other source available in digital form may lead to large-scale unauthorized copying. This is because the digital formats make possible to provide high image quality even under multi-copying. Therefore, the special part of invisible information is fixed in every image that could not be easily extracted without specialized technique saving image quality simultaneously [12]. All this is of great concern to the music, film, book and software publishing industries.

Information hiding is an emerging research area, which encompasses applications such as copyright protection for digital media, watermarking, fingerprinting, and steganography [14]. All these applications of information hiding are quite diverse [14].

(i) In watermarking applications, the message contains information such as owner identification and a digital time stamp, which usually applied for copyright protection.
(ii) Fingerprint, the owner of the data set embeds a serial number that uniquely identifies the user of the data set. This adds to copyright information to makes it possible to trace any unauthorized used of the data set back to the user.
(iii) Steganography hide the secret message within the host data set and presence imperceptible.

In those applications, information is hidden within a host data set and is to be reliably communicated to a receiver. The host data set is purposely corrupted, but in a covert way, designed to be invisible to an informal analysis. However, this paper will only focus on information hiding using steganography approach.

In section 2.3, we give an overview about steganography in detail in order to avoid confusion with cryptography. The introduction of steganography is usually given as a synonym for cryptography but it is not normally used in other way. The section also discusses several information hiding methods useable for steganographic communication. In section 3, some design issues and comparative studies of the methods employed in steganography are discussed in the paper. The survey also includes the limitations imposed by the technique on a range of steganography applications. Finally, section 4 will outline the summary of the overall information hiding technique using steganography in order to guarantee the confidentiality and data integrity.

2.2 Overview Steganography

The word steganography comes from the Greek *Steganos*, which mean covered or secret and *–graphy* mean writing or drawing. Therefore, steganography means, literally, covered writing. Steganography is the art and science of hiding information such that its presence cannot be detected [7] and a communication is happening [8, 17]. A secret information is encoding in a manner such that the very existence of the information is concealed. Paired with existing communication methods, steganography can be used to carry out hidden exchanges.

The main goal of steganography is to communicate securely in a completely undetectable manner [9] and to avoid drawing suspicion to the transmission of a hidden data [10]. It is not to keep others from knowing the hidden information, but it is to keep others from thinking that the information even exists. If a steganography method causes someone to suspect the carrier medium, then the method has failed [11].

Until recently, information hiding techniques received very much less attention from the research community and from industry than cryptography. This situation is, however, changing rapidly and the first academic conference on this topic was organized in 1996. There has been a rapid growth of interest in steganography for two main reasons [16]:

(i) The publishing and broadcasting industries have become interested in techniques for hiding encrypted copyright marks and serial numbers in digital films, audio recordings, books and multimedia products.

(ii) Moves by various governments to restrict the availability of encryption services have motivated people to study methods by which private messages can be embedded in seemingly innocuous cover messages.

The basic model of steganography consists of *Carrier*, *Message* and *Password*. Carrier is also known as *cover-object*, which the message is embedded and serves to hide the presence of the message.

Basically, the model for steganography is shown on Figure 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.*

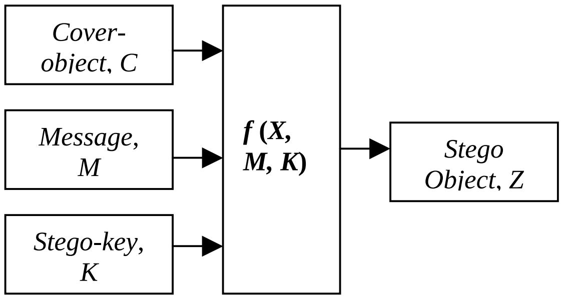


Figure 2.1 Basic Steganography Model

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.

There are several suitable carriers below to be the *cover-object* [19]:

(i) Network Protocols such as TCP, IP and UDP

(ii) Audio that using digital audio formats such as wav, midi, avi, mpeg, mpi and voc

(iii) File and Disk that can hides and append files by using the slack space

(iv) Text such as null characters, just alike morse code including html and java

(v) Images file such as bmp, gif and jpg, where they can be both color and gray-scale.

In general, the information hiding process extracts redundant bits from *cover-object*. The process consists of two steps [4, 8].

(i) Identification of redundant bits in a *cover-object*. Redundant bits are those bits that can be modified without corrupting the quality or destroying the integrity of the *cover-object*.

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

2.2.1 Steganography vs. 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 [6]. 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.

In cryptography, the structure of a message is scrambled to make it meaningless and unintelligible unless the decryption key is available. It makes no attempt to disguise or hide the encoded message. Basically, cryptography offers the ability of transmitting information between persons in a way that prevents a third party from reading it. Cryptography can also provide authentication for verifying the identity of someone or something.

In contras, steganography does not alter the structure of the secret message, but hides it inside a *cover-image* so it cannot be seen. A message in ciphertext, for instance, might arouse suspicion on the part of the recipient while an "invisible" message created with steganographic methods will not. In other word, steganography prevents an unintended recipient from suspecting that the data exists. In addition, the security of classical steganography system relies on secrecy of the data encoding system [4]. Once the encoding system is known, the steganography system is defeated.

It is possible to combine the techniques by encrypting message using cryptography and then hiding the encrypted message using steganography. The resulting *stego-image* can be transmitted without revealing that secret information is being exchanged. Furthermore, even if an attacker were to defeat the steganographic technique and detect the message from the *stego-object*, he would still require the cryptographic decoding key to decipher the encrypted message [1]. Table 1 shows that both technologies have counter advantages and disadvantages [19].

TABLE 1 - Advantages and disadvantages comparison

Steganography	Cryptography
Unknown message passing	Known message passing
Little known technology	Common technology
Technology still being developed for certain formats	Most algorithms known to government departments
Once detected message is known	Strong algorithm are currently resistant to brute force attack
	Large expensive computing power required for cracking
	Technology increase reduces strength
Many Carrier formats	

2.2.2 Steganography Applications

There are many applications for digital steganography of image, including copyright protection, feature tagging, and secret communication [1,2]. Copyright notice or watermark can embedded inside an image to identify it as intellectual property. If someone attempts to use this image without permission, we can prove by extracting the watermark.

In feature tagging, captions, annotations, time stamps, and other descriptive elements can be embedded inside an image. Copying the *stego–image* also copies of the embedded features and only parties who posses the decoding *stego-key* will be able to extract and view the features. On the other hand, secret communication does not advertise a covert communication by using steganography. Therefore, it can avoid scrutiny of the sender, message and recipient. This is effective only if the hidden communication is not detected by the others people.

2.2.3 Steganographic Techniques

Over the past few years, numerous steganography techniques that embed hidden messages in multimedia objects have been proposed [9]. There have been many techniques for hiding information or messages in images in such a manner that the alterations made to the image are perceptually indiscernible. Common approaches are include [10]:

(i) Least significant bit insertion (LSB)

(ii) Masking and filtering

(iii) Transform techniques

Least significant bits (LSB) insertion is a simple approach to embedding information in image file. The simplest steganographic techniques embed the bits of the message directly into least significant bit plane of the *cover-image* in a deterministic sequence. Modulating the least significant bit does not result in human-perceptible difference because the amplitude of the change is small.

Masking and filtering techniques, usually restricted to 24 bits and gray scale images, hide information by marking an image, in a manner similar to paper watermarks. The techniques performs analysis of the image, thus embed the information in significant areas so that the hidden message is more integral to the cover image than just hiding it in the noise level.

Transform techniques embed the message by modulating coefficients in a transform domain, such as the *Discrete Cosine Transform* (DCT) used in JPEG compression, *Discrete Fourier Transform*, or *Wavelet Transform*. These methods hide messages in significant areas of the *cover-image,* which make them more robust to attack. Transformations can be applied over the entire image, to block through out the image, or other variants.

2.3 Secure Information Hiding System (SIHS)

An information hiding system has been developed for confidentiality. However, in this paper, 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 previous section 3.

For embedding the data into an image, we require two important files. The first is the original image so called *cover-image*. The image (Figure 4), which in and *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 (Figure 3).

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.

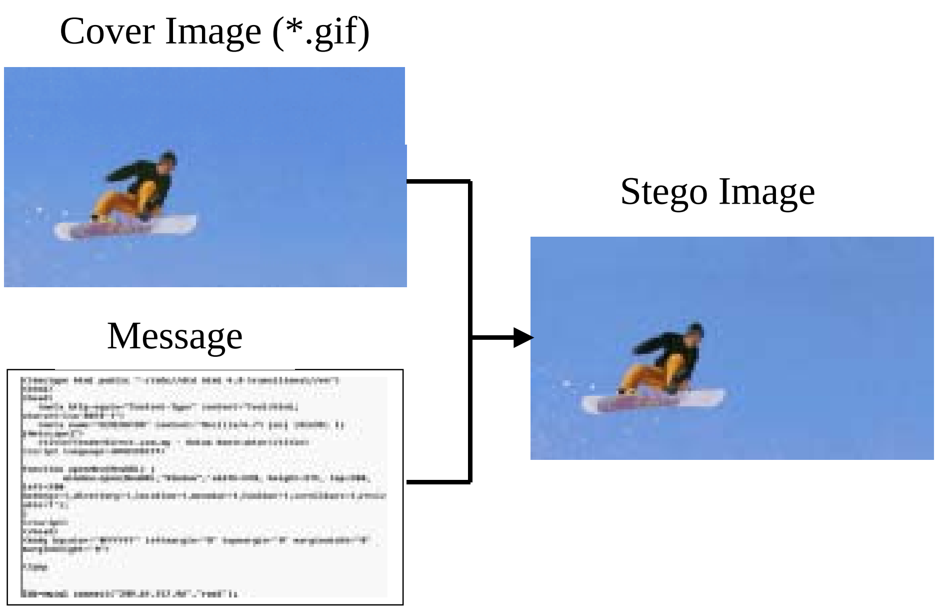


Figure 2.2 Producing Stego-Image Process

The *cover-image* will be combined with the message. This will produce the output called *stego-image*. Figure 2.2 is illustrated the process. The *Stego-image* seems identical to the *cover-image*. However, there are hidden message that imperceptible.

```
<!doctype html public "-//w3c//dtd html 4.0 transitional//en">
<html>
<head>
   <meta http-equiv="Content-Type" content="text/html;
charset=iso-8859-1">
   <meta name="GENERATOR" content="Mozilla/4.71 [en] (Win98; I)
[Netscape]">
   <title>TenderDirect.com.my - Untuk Kontraktor</title>
<script language=JAVASCRIPT>

function openNew(NewURL) {
        window.open(NewURL,"Window",'width=590, height=315, top=200,
left=200
hotkeys=1,directory=1,location=1,menubar=1,toolbar=1,scrollbars=1,resiz
able=1');
}
</script>
</head>
<body bgcolor="#FFFFFF" leftmargin="0" topmargin="0" marginwidth="0"
marginheight="0">

<?php


$db=mysql_connect("209.61.157.96","root");
```

Figure 2.3 Message

This process simply embedded the message into the *cover-image* without supplied any password or *stego-key*. At this stage, we decided to do so because we have to understand the ways of LSB insert the message bit into the image and extract the message from the *stego-image* produced.

Figure 2.4 Cover Image (original)

Figure 2.5 Result of Stego-Image

The advantages of LSB are its simplicity to embed the bits of the message directly into the LSB plane of *cover-image* and many techniques use these methods [15]. Modulating the LSB does not result in a human-perceptible difference because the amplitude of the change is small. Therefore, to the human eye, the resulting *stego-image* (Figure 2.5) will look identical to the *cover-image* (Figure 2.4). This allows high perceptual transparency of LSB.

However, there are few weaknesses of using LSB. It is very sensitive to any kind of filtering or manipulation of the *stego-image*. Scaling, rotation, cropping, addition of noise, or lossy compression to the *stego-image* will destroy the message.

On the other hand, for the hiding capacity, the size of information to be hidden relatively depends to the size of the *cover-image*. The message size must be smaller than the image. A large capacity allows the use of the smaller *cover-image* for the message of fixed size, and thus decreases the bandwidth required to transmit the *stego-image* [1].

Another weakness is an attacker can easily destruct the message by removing or zeroing the entire LSB plane with very little change in the perceptual quality of the modified *stego-image*. Therefore, if this method causes someone to suspect something hidden in the *stego-image*, then the method is not success.

2.4 Summary

In this paper 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 perceptual transparency, hiding capacity, robustness and tamper resistance 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.

CHAPTER 3

STEGANOGRAPHY: RANDOM LSB INSERTION USING DISCRETE LOGARITHM

3.1 Introduction

Due to advances in ICT, most of information are kept electronically. Consequently, 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 paper, 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.

The growing possibilities of modern communications require the use of secure means of protecting information during transmission against unauthorized access and use. The most common method of protecting information is cryptography whereby the information is scrambled into unintelligible stream that cannot be decrypted by the casual viewer [14]. Another technique which has become an emerging research area is information hiding [13]. Steganography is an approach in information hiding whereby the information is hidden inconspicuously inside a host data set such that its presence is imperceptible [6].

Basically, the purpose of cryptography and steganography is to provide secret communication. However, steganography must not be confused with cryptography. Cryptography hides the contents of a secret message from malicious people, whereas steganography conceals the existence of the message. Therefore, the methods used in breaking the system are different [5]. In cryptography, the system is broken when the attacker can decrypt the unreadable data to form back the secret message. But to extract a hidden message that is embedded using steganography, the attacker first of all need to realize the existence of the secret message. Without this knowledge, the secret data can pass through even right under his nose.

In cryptography, the structure of a message is scrambled to make it meaningless and unintelligible unless the decryption key is available. It makes no attempt to disguise or hide the encoded message. Basically, cryptography offers the ability of transmitting information between persons in a way that prevents a third party from reading it. Cryptography can also provide authentication for verifying the identity of someone or something.

In contrast, steganography does not alter the structure of the secret message, but instead hides it inside a *cover-image* so that it cannot be seen. A message in a ciphertext, for instance, might arouse suspicion on the part of the recipient while an “invisible” message created with steganographic methods will not. In other word, steganography prevents an unintended recipient from suspecting that the secret message exists. In addition, the security of classical steganography system relies on secrecy of the data encoding system [11]. Once the encoding system is known, the steganography system is defeated.

It is possible to combine the techniques by encrypting message using cryptography and then hides the encrypted message using steganography. The resulting *stego-image* can be transmitted without revealing that secret information is being exchanged. Furthermore, even if an attacker were to defeat the steganographic technique and detect the message from the *stego-object*, he would still require the cryptographic decoding key to decipher the encrypted message [3].

Common techniques used in steganography are least significant bit insertion (LSB), masking and filtering, and transformation techniques. In this paper we present an LSB technique, which randomly select the pixels of the *cover-object* that is used to hide the secret message. The selection is based on discrete logarithm. Section 2 gives an overview of steganography and Section 3 discusses the LSB technique that employs discrete logarithm. The analysis of the algorithm is given in Section 4.

3.2 Overview of Steganography

The word steganography comes from the Greek *Steganos*, which means covered or secret and *–graphy* means writing or drawing. Therefore, steganography means, accurately, covered writing. Steganography is the art and science of hiding information such that its presence cannot be detected [1]. Secret information is encoded in a way such that the very existence of the information is concealed in a human perceptible.

The 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 idea of steganography is to keep others from thinking that the information even exists and not to keep others from knowing the hidden information. If a steganography method causes anybody to suspect there is a secret information in a carrier medium, then the method has failed [2].

Basically, 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 ciphertext, 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]:

$$I' = f\ (I, m, k) \qquad \text{.........(1)}$$

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 redundant bits from *cover-object*. The process consists of two steps [11,12]:

(i) Identification of redundant bits in a *cover-object*. Redundant 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 redundant bits to be replaced with data from a secret message. The *stego-object* is created by replacing the selected redundant bits with message bits.

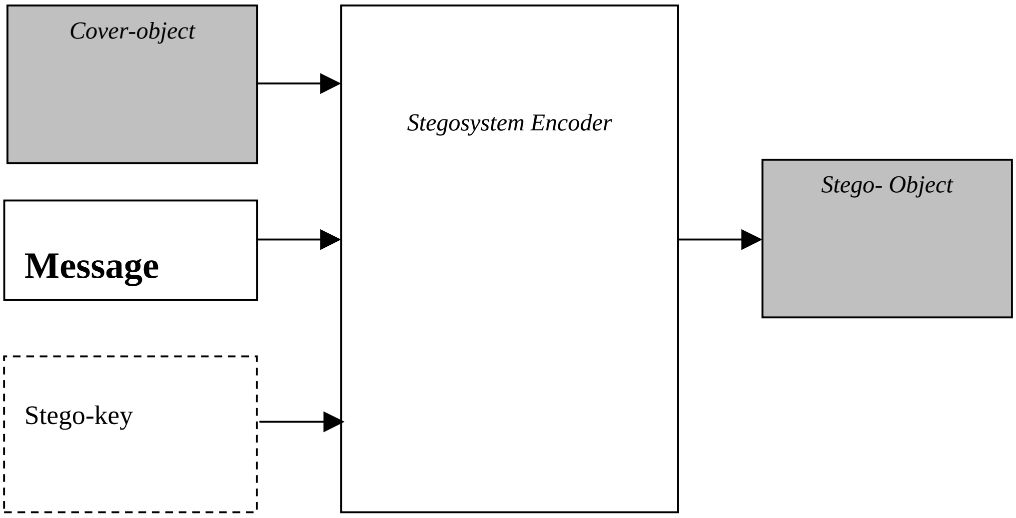


Figure 3.1 Basic Model of Steganography

Many different methods of hiding information in images exist. In [8] a method of hiding information in images includes application of transform domain such as *Discrete Cosine Transform* (DCT). This method hides messages in significant areas of the *cover-image*. Another method employs a *pseudo random number generator* (PRNG) [22] to locate the embedding positions randomly. A secret key is used as a seed to PRNG. In fact, embedding the message randomly is functionally similar to first permutes the message before embeds it in the *cover-image* sequentially. In this technique, a suitable encryption scheme is applied on the compressed message to raise the steganographic security level.

In this paper, 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]. However a different algorithm is used to determine the embedding positions.

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]. The message is embedded with sequence-mapping technique in the pixels of a *cover-image*. Although LSB hides the message in such way that the humans do not perceive it, it is still possible for the opponent to retrieve the message due to the simplicity of the technique. Therefore, malicious people can easily try to extract the message from the beginning of the image if they are suspicious that there exists secret information that was embedded in the image.

Therefore, 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.

3.3.1 Discrete Logarithm

Discrete logarithm calculation can be used to solve sequence-mapping problem. 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]

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

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.

3.3.2 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 stegosystem, 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, 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 stegosystem encoder in the following manner:

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

where M_i is the *i*th bit of the message,

$I\,y_i$ is the *i*th 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.

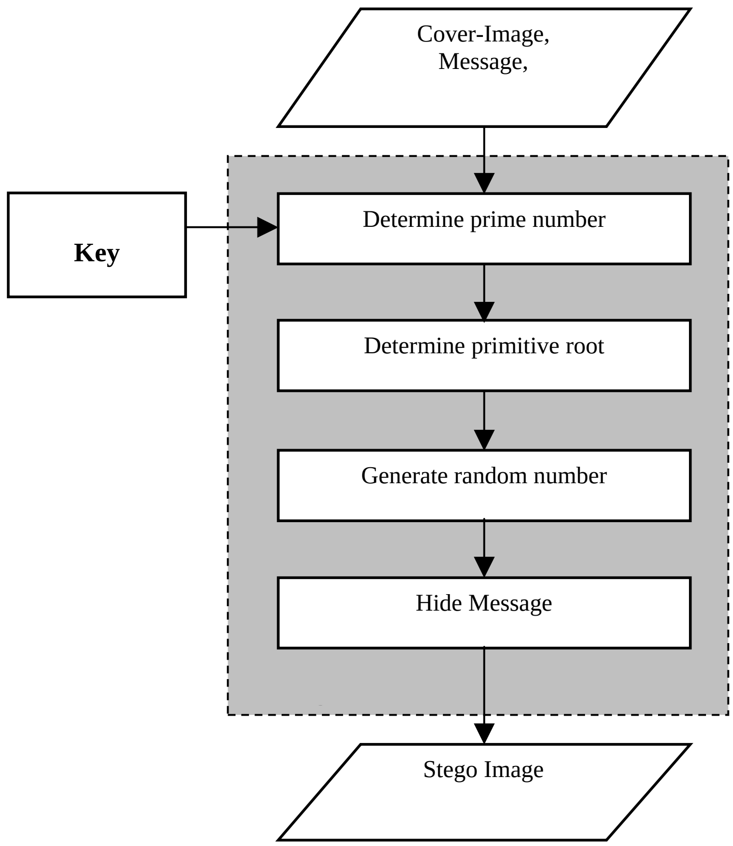


Figure 3.2 Flow Chart for SIHS

3.4 Analysis of SIHS

For the system analysis, we presented three cases. In all cases 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. A GIF 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.

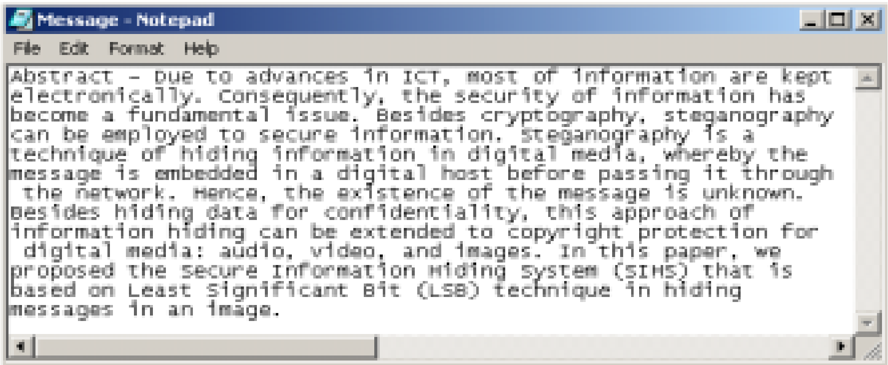


Figure 3.3 A Message Open with Notepad

In the first 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 3.5. 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.

In order to demonstrate the difference between sequence-mapping and random-mapping of the pixel, we applied the stego process of SIHS using a white *cover-image*. Since the embedding of the message into the white cover-image will show the area on the cover-image where the message is embedded.

Figure 3.4 Cover-Image

Figure 3.5 Stego-Image

Figure 3.6 shows the embedded message of Figure 3.3 is sequentially embedded on top of the *cover-image*. Since each bit from the message is sequentially ordered on the *cover-image*, then it will be easy for the third party to recover the message by retrieving the pixels sequentially starting from the first pixel of the image.

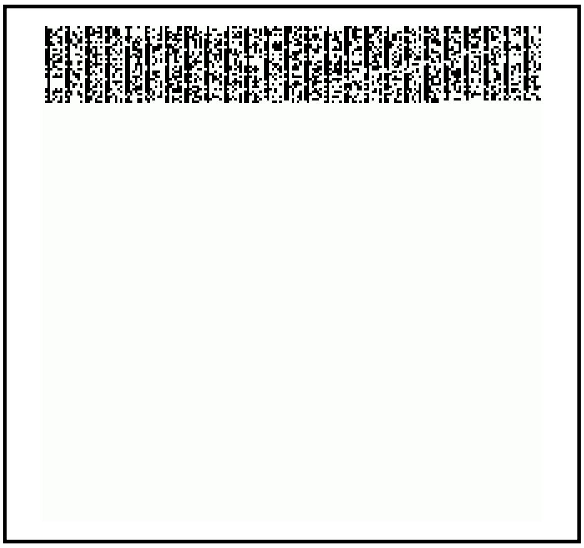


Figure 3.6 Basic LSB with sequence-mapping

However by using discrete logarithm calculation, the problem of sequence-mapping can be solved. Figure 3.8 illustrates a message embedded using random-mapping technique. In this technique, the selected pixel for embedding the message bits depends on the random number generated by the SIHS and a key, *k*. Although the third party could determine where the message bits are embedded, he has a difficulty to recover it because the message bits are embedded in a random order. The recovered message will be a nonsense symbols as shown in Figure 3.7.

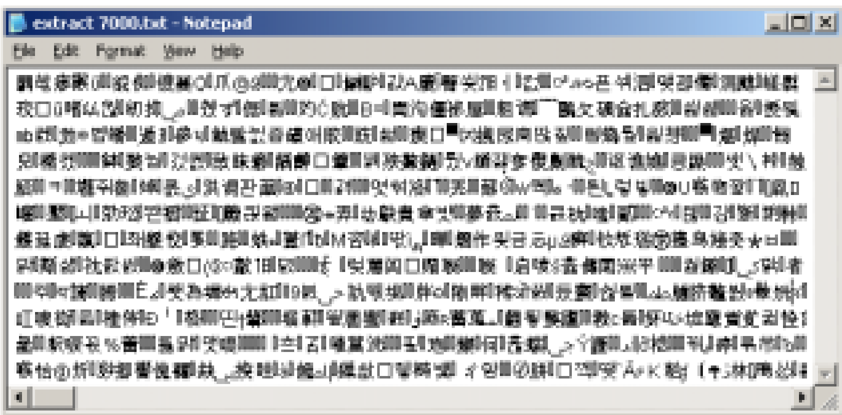
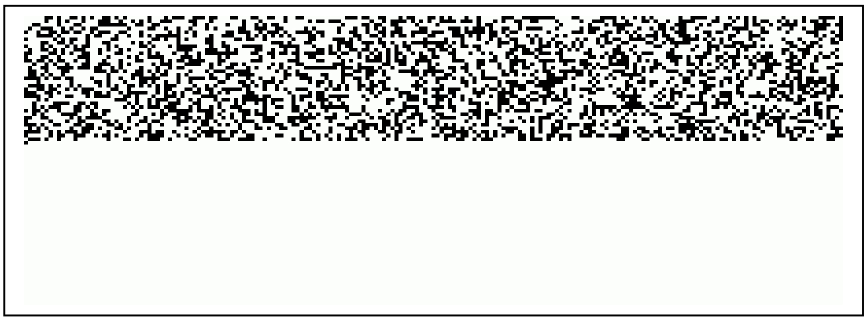


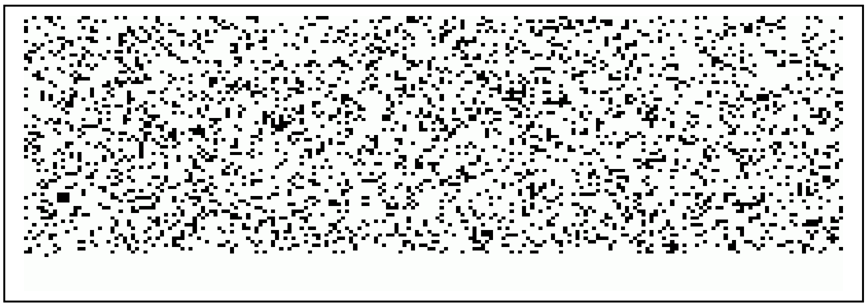
Figure 3.7 Recovered Message with Normal Extraction

In addition, different key supplied by the user will also generate different set of random numbers. If a bigger key size is chosen, the bigger the range of random numbers will be generate, therefore the message bits will be scattered in a larger area as shown in Figure 3.8. Figure 3.8(a) and 3.8(b) used key *k* of 7000 and 14000 respectively.

In the last case, we used a black image as the *cover-image*. However, after embedding the message, the *stego-image* did not show any changes as illustrated in Figure 3.9.



(a)



(b)

Figure 3.8 Stego-Image with Different Key Size

Steganography that uses a key has a better security than non-key steganography. This is so because without the knowledge of the valid key, it is difficult for a third party or malicious people to recover the embedded message. However there are still some issues need to be tackled to implement LSB on a digital image as a *cover-object* using random pixels. They are:

- We noticed that in the approach discussed above, the time taken for generating the random numbers depends on the size of the key. In our approach it means that it also depends on the *cover-image* size.
- Although the LSB embedding methods hide data in such a way that the humans do not perceive it, such schemes can be easily destroyed by an opponent such as using lossy compression algorithms or a filtering process.
- Any process that modifies the values of some pixels, either directly or indirectly, may result in degrading of the quality of the original object.

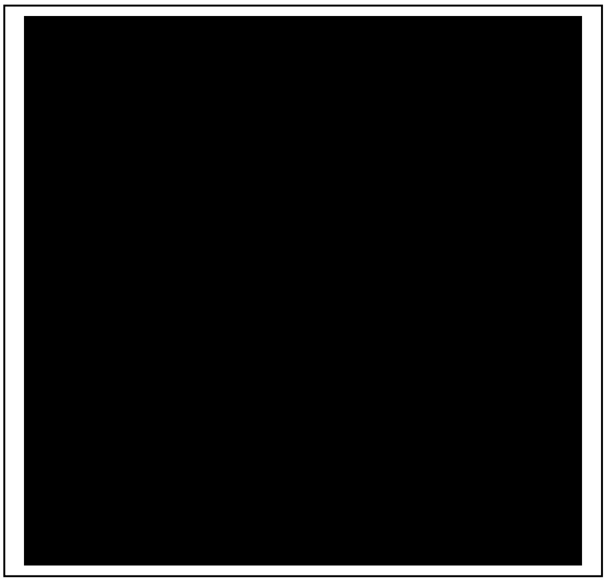


Figure 3.9 Stego-Image using Black Image

3.5 Summary

In this paper we have presented an 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.

Future work we would to extend the system to be more robust and efficient. The research will include the enhancement of the algorithm that will utilize the entire image for embedding the message. We will also analyze the processing time to generate the random number and introduce method(s) to minimize the time.

CHAPTER 4

CONCLUSION

4.1 Discussion

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. Finally, 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, it is difficult for a third party or malicious people to recover the embedded message. However there are still some issues need to be tackled to implement LSB on a digital image as a *cover-object* using random pixels.

4.2 Recommended Guidelines

The knowledge of the technology is still limited to mainly the research individuals and academia, however there is a growing understanding that this technology could be used widely. UTM should carry out more research into the field of information hiding. In future, we would extend the system to be more robust and efficient. The research will include the enhancement of the algorithm that will utilize the entire image for embedding the message. We will also analyze the processing time to generate the random number and introduce method(s) to minimize the time.

4.3 Technical Paper Published

These are the published papers related to the project as described in the following chapters:

- M.M. Amin, .M. Salleh, S. Ibrahim, M.R Katmin (2003) , "Steganography Using Least Significant Bit (LSB)", Malaysian Science And Technology Congress 2002 (MSTC2002), 19-21 September 2002, Puteri Pan Pacific Hotel, Johore Bahru.

- M.M. Amin, .M. Salleh, S. Ibrahim, M.R Katmin (2003), "Information Hiding Using Steganography", 4th National Conference on Telecommunication Technology Proceeding 2003 (NCTT2003), Concorde Hotel, Shah Alam, Selangor, 14-15 January 2003, pp. 21-25.

- M.M. Amin, .M. Salleh, S. Ibrahim, M.R Katmin (2003), "Steganography: Random LSB Insertion Using Discrete Logarithm", Conference on Information Technology in Asia (CITA'03), Universiti Malaysia Sarawak, Kota Samarahan, Sarawak, Malaysia, July 17-18, pp. 234-238.

REFERENCES

[1] C. Cachin, “An Information-Theoretic Model for Steganography”, in *proceeding 2nd Information Hiding Workshop,* vol. 1525, pp. 306-318, 1998.

[2] D. Artz, “Digital Steganography: Hiding Data within Data”, *IEEE Internet Computing*, pp. 75-80, May-Jun 2001.

[3] E.T. Lin and E.J. Delp, "A Review of Data Hiding in Digital Images," *in Proceedings of the Image Processing, Image Quality, Image Capture Systems Conference*, PICS '99, Ed., Apr. 1999, pp. 274--278.

[4] F.A.P Peticolas, R.J. Anderson and M.G. Kuhn, “Information Hiding – A Survey”, in *proceeding of IEEE*, pp. 1062-1078, July 1999.

[5] J. Zollner, H. Federrath, H. Klimant, et al., “Modeling the Security of Steganographic Systems”, in *2nd Workshop on Information Hiding*, Portland, April 1998, pp. 345-355.

[6] M.M. Amin, M. Salleh, S. Ibrahim, et al., “Information Hiding Using Steganography”, *4th National Conference On Telecommunication Technology Proceedings (NCTT2003),* Shah Alam, Malaysia, pp. 21-25, January 14-15, 2003.

[7] M. Ramkumar & A.N. Akansu. “Some Design Issues For Robust Data hiding Systems”, *<http://citeseer.nj.nec.com/404009.html>*

[8] N.F. Johnson, S. Jajodia, “Staganalysis: The Investigation of Hiding Information”, *IEEE,* pp. 113-116, 1998.

[9] N.F. Johnson & S. Jajodia, “Steganalysis of Images Created Using Current Steganography Software”, in *Proceeding for the Second Information Hiding Workshop,* Portland Oregon, USA, April 1998, pp. 273-289.

[10] N.F. Johnson and S. Jajodia, "Exploring Steganography: Seeing the Unseen", *IEEE*, pp. 26-34, 1998.

[11] N. Provos, P. Honeyman, "Detecting Steganography Content on the Internet". CITI Technical Report 01-11, 2001.

[12] N. Provos, "Probabilistic Methods for Improving Information Hiding", *CITI Technical Report 01-1*, January 31, 2001.

[13] P.Moulin & J.A. O'Sullivan, "Information – Theoretic Analysis of Information Hiding", at *IEEE International Symposium on Information Theory*, Boston, MA, October, 1999.

[14] R A Isbell, "Steganography: Hidden Menace or Hidden Saviour", *Steganography White Paper*, 10 May 2002.

[15] R. Chandramouli, N. Memon, "Analysis of LSB Based Image Steganography Techniques", IEEE pp. 1019-1022, 2001.

[16] R.J. Anderson, F.A.P. Petitcolas, "On The Limits of Steganography", *IEEE Journal of Selected Area in Communications*, pp. 474-481, May 1998.

[17] R.Popa,"An Analysis of Steganographic System", The "Politehnica" University of Timisoara, Faculty of Automatics and Computers, Department of Computer Science and Software Engineering, May 25, 1998.

[18] S. Katzenbeisser and F.A.P. Peticolas, "Defining Security in Steganographic Systems", *in Proceeding of Electronic Imaging*, Photonics West, SPIE, vol. 4675, pp. 50-56, 2002.

[19] S. Tanako, K. Tanaka and T. Sugimura, "Data Hiding via Steganographic Image Transformation", *IEICE Trans. Fundamentals*, vol. E83-A, pp. 311-319, February, 2000.

[20] W. Bender, D. Gruhl, N. Morimoto and A. Lu, “Techniques for Data Hiding”, *Systems Journal*, vol. 35, 1996.

[21] W. Stallings (1999). “Cryptography And Network Security: Principles and Practice”, Prentice Hall International, Inc, United State: America.

[22] Y.K. Lee and L.H. Chen, “A Secure Robust Image Steganographic Model”, *in Tenth National Conference on Information Security*, Hualien, Taiwan, pp. 275-284, May 5- 6, 2000.

[23] Y.K. Lee and L.H. Chen, “High Capacity Image Steganographic Model”, *IEE Proceedings Vision, Image and Signal Processing*, vol. 147, pp. 288-294, Issue 3, June 2000,

[24] Z. Hrytskiv, S. Voloshynovskiy & Y. Rytsar “Cryptography of Video Information In Modern Communications”, *Electronics And Energetics*, vol. 11, pp. 115-125, 1998.

APPENDIX