IMAGE STEGANOGRAPHY

JENIFFER A/P CHEGARAM

FACULTY OF COMPUTER SYSTEMS & SOFTWARE ENGINEERING
UNIVERSITI MALAYSIA PAHANG

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

ABSTRAK

Internet secara keseluruhan tidak menggunakan rangkaian yang selamat, maka maklumat dalam transit boleh terdedah kepada pemintasan. Kini, ini adalah satu isu yang penting untuk mengurangkan peluang bagi mengesan maklumat semasa penghantaran maklumat. Beberapa penyelesaian yang perlu untuk dibincangkan adalah bagaimana hendak hantar maklumat dengan cara, kewujudan mesej yang dihantar tidak diketahui oleh dan mengagihkan perhatian penyerang lain. Selain menyembunyikan data bagi tujuan kerahsiaan, pendekatan maklumat boleh dilanjutkan kepada perlindungan hak cipta bagi media digital. Dalam kajian ini, kita menjelaskan apakah itu steganografi imej, definisi, kepentingan serta teknik yang digunakan dalam melaksanakan steganografi imej. Kita member tumpuan kepada teknik Bit yang Kurang Penting (LSB) untuk menyembunyikan mesej dalam imej. Sistem ini meningkatkan teknik LSB dengan secara rawak untuk menyuraikan bit mesej dalam imej dan sekaligus menjadikan sukar bagi orang yang tidak dibenarkan untuk melayari mesej asal.

Kata Kunci: Steganografi, maklumat bersembunyi

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

CHAPTER I

INTRODUCTION

This chapter briefly describes about the image steganography. This chapter contains six chapters: The first section explain about the background of the project. Second section describes about the problem statement. The third section describes the objectives for the project. The fourth section describes the scopes for the project. Finally, the thesis organization is described in section five.

1.1 Background

Since the usage of Internet rise, one of the most important in information technology and communication has been the give priority to security of information. Cryptography was one of the methods created as a technique for securing the secret of communication and many different ways have been developed and identify to encrypt and decrypt data to keep the message secret. Unfortunately, sometimes it is not enough to keep secret the contents of a message, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is named steganography. Steganography technique is the art and science of invisible in communication. This is implementing through hiding information in other information, thus hiding the existence of the communicated information. In image steganography system, the information is hidden exclusively in images.

As stated before, images are the most popular cover objects used for steganography system. In the era of digital images there are many different image file formats exist. Most of them used for specific applications. For this different image file formats, different steganographic algorithms used. Image steganography is hiding the file inside an image.

The information to be hidden in the cover data is known as the embedded data. The embedded data is the data containing both the cover image and the embedded information or file. The processing of putting the embedded data, into the cover image, is sometimes known as embedding. Occasionally, especially when referring to image steganography, the cover image is known as the cover.

By implementing this image steganography system, security of privacy and confidential data will be solved. This system will be targeted to be very user friendly in where it will be very easy to handle and provides good security at the same time. Due to this reason, more people will get to know about the product and it is believed to be making use in an appropriate way. This also can help us to keep our data or file in safe and more secure.

1.1 Problem Statement

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

The goal of steganography is to avoid the 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 dramatically with distinguishing but imperceptible marks, which may contain a hidden notice or serial number or even help to prevent unauthorized copying directly.

In this era, there are many hacking cases. Many industries such as bank, company worry that all their personal and industry data will be explore by unauthorized people.

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

The aim of this project is to encrypt the data or hide the data over an image using steganographic technique and to know that algorithms in the context of quality of concealing and to describe their functionality in data security.

So we prepare this application, to make the information hiding simpler and user friendly.

1.2. Objectives

This project comprehends the following objectives:

i. To produce a security level in hiding information based on steganographic techniques.
ii. To learn the techniques of hiding data using steganography.
iii. Testing the efficiency and accuracy of hiding the data through algorithms that used.

1.3. Scope

The scope of the project is to limit the unauthorized access and provide better security during file saving. To meet the requirements, I use the simple and basic approach of steganography. In this project, the proposed approach finds the suitable algorithm for embedding the data inside an image using steganography, which provides the better security pattern for saving the file. For practically implementing the function of the discussed algorithms, Visual Studio software is used. Although the Visual Studio is not particularly known for its top security functionalities, I use this for easier application development and a well defined User Interface.

1.4 Thesis Organization

Chapter-1: Introduction: In this section, the main points discussed are about the Overview, the Background of the project, the objectives and the scopes of the project

Chapter-2: Literature Review: Definitions and overview about the different information security methods to gather knowledge on the existing theories of steganography and review it for proposing an improvised system for providing the required security and discuss about different functionalities of algorithms used for the proposed system.

Chapter-3: Design Structure: This section describes the general architecture of encryption, decryption and data hiding procedures using diagram. Description about the hardware and software requirements for the proposed system also has been explain .Visual Studio software and implementations of different modules like encryption, decryption and data hiding techniques.

Chapter-4: Implementation and Testing: This section will describe about the result that we get over this research.

Chapter-5: Conclusion: This chapter discuss about the limitation about this project and future enhancement.

CHAPTER II

LITERATURE REVIEW

This chapter briefly describes the review on existing techniques related with image steganography. This chapter comprises five sections: The first section describes the review about the existing related systems. In the second section, it describes the details about the algorithm.

2.0 Introduction

Since the beginnings of human communication increase, the desire to communicate in secret has existed. There have been many solutions to this problem, one of them is steganography. Many people describe steganography with cryptography, which is not entirely wrong, because both of them share similar purpose to protect certain information from people that do not have the right to access it. Later in this section, steganography will be explained in details, along with its techniques and with cryptography in the subject of information protection.

This chapter will discuss the main principles of steganography. Firstly, discussing where we currently are in both fields, and then introduce the important background knowledge that is required to fully understand the methods that introduced in this project. The JPEG and BITMAP compression process is also discussed, as it is important that we

understand the significance of embedding the message data within this domain at a later stage. Finally, we introduce the technique that used for image steganography.

In order to improve the security features in data transfers over the internet, many techniques have been developed like Cryptography, Steganography and digital watermarking. While Cryptography is a main method to conceal the information by encrypting it to the cipher texts and transmitting it to the particular receiver using an unknown key, Steganography provides further security by hiding the cipher text into an invisible image or other formats of image.

According to Johnson et al., (2001), “Steganography is the art of hiding and transmitting data through apparently innocuous carriers to conceal the existence of data”. The level of visibility is decreased using many hiding techniques in image modeling like LSB Manipulation, Masking and filtering. Different steganographic algorithms like F5, LSB, and JSteg show these techniques and the step of detecting the hidden information through these algorithms is called Steganalysis.

2.1 Existing System Review

This section is to view the current system and the existing system that related to Image steganography software.

2.1.1 Quick Stego

QuickStego is software that lets you to hide text in pictures so that only other users of QuickStego can explore and read the hidden secret messages. Once text that we choose is hidden in an image the saved picture is still a 'picture', it will load just like any other image and appear as it did before. The image can be saved, emailed, uploaded to the web (see the picture of the lady with a laptop above - this image has hidden text) as before, the only difference will be that it contains hidden text. QuickStego is a "ten-in-one" best of breed security software product in US. It is quick and both through its advanced computer design which allows it to rapidly execute complex security processes, but perhaps even more importantly, as it is so easy to use. Cryptography and Steganography have never been

simpler using this absolutely top encryption and privacy tool. QuickStego use strong encryption software that offer to design to hide the data of encryption, giving you excellent ease of use at the same time, giving you encryption software that you can trust. QuickStego allows you to secure single and multiple files also. It also can secure folders, sub-folders, passwords and emails. It is quickly and easily to implement, and performs most operations with a single mouse click within familiar. There are no limitations on file type, QuickStego encrypts every kind of file format, whether it is text, video, picture, document or audio - any type of file, on USB, floppy, thumb/flash or hard drives. QuickStego is easy to use.

2.1.2 Hide in Picture (HIP)

Hide in Picture is software that allows you to "hide" any kind of file inside the standard bitmap pictures. The pictures look like normal images to everyone, so people will not suspect anything when they see the image. This is called steganography. You can also use a password to hide your files, and only those who know the password are able to view them. The person who don't know the password cannot even be sure there is something hidden in an image.

Features of Hide in Picture

- Encryption - All data will be encrypted before written to a picture. It is to increase the security. HIP offers several encryption algorithms that you can choose from it; all of them are considered very secure, so you don't have to worry about it unless you have a specific reason for wanting to use a specific algorithm. When view a file, HIP tries using all the available algorithms to find the correct data.

- Transparent color support - One color of the picture may be set as 'transparent'. Nothing will be stored in areas of this color palette. This can be useful to all. For an example is when hiding a file inside an image from a Web page, its transparent areas will remain as before. To retrieve a hidden file using this option, you must set the transparent color to the same used when hiding it.
- Erase file option - If you want to remove a file hidden in a picture, use have to use this option. It will overwrite the file with random data, so the file will be unrecoverable. If you know the password with which the file was hidden, you can

provide it and only the necessary areas will be overwritten, resulting in a very small quality loss; however, if you provide the wrong password, the file will not be erased properly. If you do not provide a password, HIP will overwrite more of the picture to account for all the possible passwords, causing a larger quality loss.

2.1.3 Chameleon

Chameleon is steganography software that allows users to hide confidential or important files within a standard digital picture. This is particularly useful in distribute covert communications over the Internet. Images will be embedded with secret documents, for example is it may be transmitted as an email attachment or it is posted on a web forum or bulletin board.
The main feature of Chameleon is its adaptive encoding algorithm which optimizes the use of hiding space in a particular cover image.

In bitmaps, steganography is usually performed by replacing the least-significant bit (LSB) of the color values of each pixel with the data bits of the file or message to be hidden. Since LSBs represent only a small portion of the actual color values, such changes in an image are often invisible to the human eye. Consider, for example, a 640x480 true-color bitmap. True color images are composed of red, green, and blue color channels. In each pixel, the intensity or color value for each channel is represented by an 8-bit number. Using the LSBs of the three color values of each pixel would generate a hiding space of 115,200 bytes (or 921,600 bits), 1/8 of the total image size.

The comparison of this software as below:

Software	Algorithm	Usability	Speed	Security	Accuracy
Quick Stego	Advanced Encryption Standard (AES)	Easy	Very Fast	Secure	Less
Hide In Picture	Blowfish	Very Easy	Fast	Very Secure	High
Chameleon	Least Significant Bit (LSB)	Hard	Slow	Less Secure	Very Less

Table 2.1: Comparison of different Steganographic Software

2.2 History of Steganography

The first explanation of the use of steganography is back to the Greeks. Herodotus tells everyone how a message will pass to the Greeks about Xerses' hostile intentions underneath the wax of a writing tablet, and describes a technique of dotting successive letters in a cover text with a secret ink, due to Aeneas the Tactician. Pirate legends tell of the practice of tattooing secret information, such as a map, on the head of someone, so that the hair would conceal it.

Kahn tells of a trick used in China of embedding a code ideogram at a prearranged position in a dispatch; a similar idea led to the grille system used in medieval Europe, where a wooden template would be placed over a seemingly innocuous text, highlighting an embedded secret message.

During WWII the grille method or some variants were used by spies. In the same period, the Germans developed microdot technology, which prints a clear, good quality photograph shrinking it to the size of a dot (Bender, 1996).

There are rumors that during the 1980's Margaret Thatcher, then Prime Minister in UK, became so irritated about press leaks of cabinet documents, that she had the word processors programmed to encode the identity of the writer in the word spacing, thus being able to trace the disloyal ministers.

During the "Cold War" period, US and USSR wanted to hide their sensors in the enemy's facilities. These devices had to send data to their nations, without being spotted. Today, steganography is researched both for legal and illegal reasons.

Among the first ones there is war telecommunications, which use spread spectrum or meteor scatter radio in order to conceal both the message and its source. In the industry market, with the advent of digital communications and storage, one of the most important issues is copyright enforcement, so digital watermarking techniques are being developed to restrict the use of copyrighted data.

Another important use is to embed data about medical images, so that there are no problems with matching patient's records and images. Among illegal ones is the practice of hiding strongly-encrypted data to avoid controls by cryptography export laws.

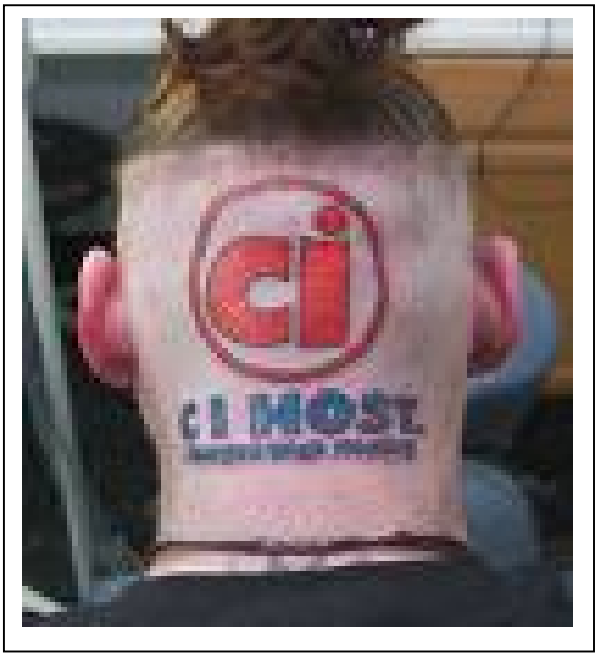

Figure 2.1 on the head of someone

Figure 2.2 Writing tablet

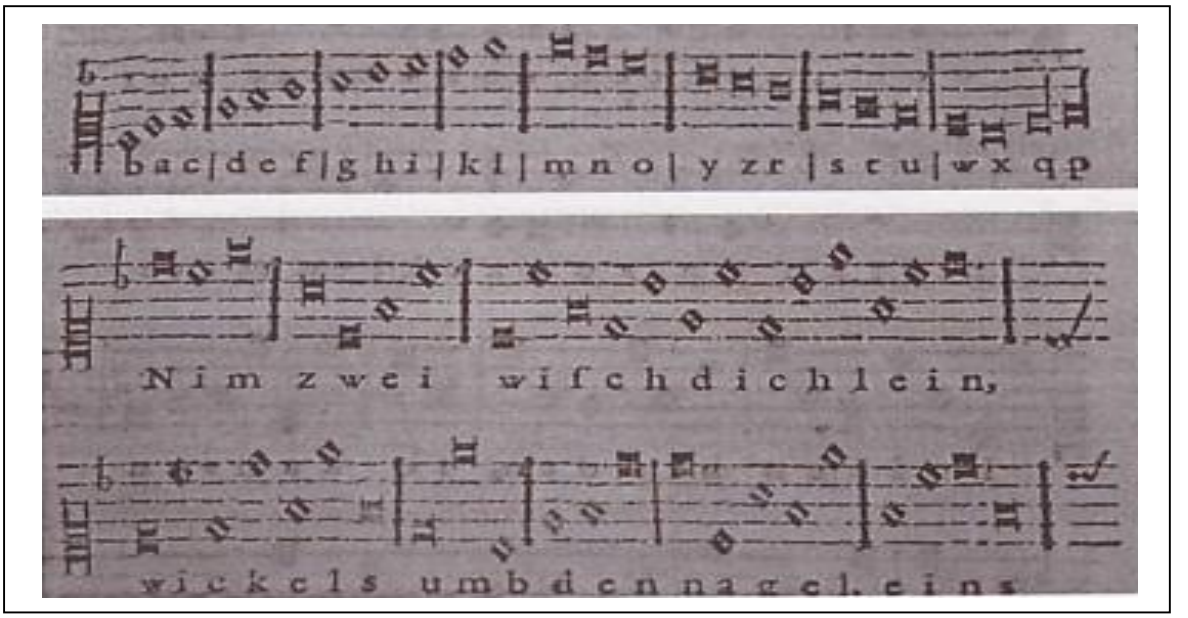

Figure 2.3 Hiding information in music scores

2.2.1 Steganography vs. Cryptography

Basically, the need of cryptography and steganography is to provide secret data saving. However, steganography is not the same as cryptography. Cryptography hides the contents of a secret message from an unauthorized people, but 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 (Amin, 2003). 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 contrast, steganography does not change the structure of the secret message, but hides it inside a cover-image so it cannot be seen. A message in cipher text for instance might bring a suspicion on the part of the recipient while an "invisible" message created with steganographic methods will not. In other word, steganography prevents an unauthorized recipient from suspecting that the data exists. In addition, the security of steganography system relies on secret of the data encoding system. Once the encoding system is known, the steganography system is detected.

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 (Cachin, 1998). Table 1 shows that both technologies have counter advantages and disadvantages (Tanako, 2000).

Table 2.2 - 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
Many Carrier formats	Technology increase reduces strength

2.3 Steganography Applications

There are many applications in market for digital steganography of image. It include copyright protection, feature tagging, and secret communication. Copyright notice or watermark selection can embedded inside an image to identify it as intellectual property. If someone attempts to use this image without permission, we can prove by remove 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 certain parties who possess 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 suspicion of the sender, message and recipient. This is effective only if the hidden communication is not detected by the others people.

2.3.1 Steganographic Techniques

Over the past few years, there are big number of steganography techniques that embed hidden messages in digital objects have been proposed. There have been many techniques for hiding information or messages in images. Common approaches are including:

(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.