IMPACT OF IMAGE PERCEPTIBILITY IN STEGANOGRAPHY

PHANG SHE CHIN

BACHELOR OF COMPUTER SCIENCE
(GARPHICS & MULTIMEDIA TECHNOLOGY)
WITH HONOURS

UNIVERSITY MALAYSIA PAHANG

ABSTRACT

This thesis discusses on the impact of image perceptibility in Image Steganography. By using the steganography to embed the secret message into the cover image. Method of the steganography will applied to the image perceptibility must be in either black and white or grey. The image of steganography generated must have visual quality same with the original version. Schemes of the steganography must be tested and make sure the changes on embedded image is not detect by naked eye from other. In this thesis, one of the steganography schemes for image of image perceptibility is proposed, Least Significant Bit (LSB) technique. LSB scheme will be uses to embed the secret message into a cover image. The result before and after embed the secret message should not produce an obvious different and detect easily by naked eye. So, it is considered as good image. In conclusion, schemes of the steganography will in effect the impact of image perceptibility to enhance security of the information and the concealment of information involve the sender and intended recipient only.

ABSTRAK

Tesis ini membincangkan dan memperkenalkan tentang kesan yang terhasil pada imej dengan melalui teknik steganografi. Dengan menggunakan steganografi, mesej rahsia dapat ditanam atau disembunyikan ke dalam imej. Kaedah steganografi ini akan digunakan pada imej yang berwarna hitam dan putih atau imej yang kelabu sahaja. Imej steganografi yang dihasilkan mesti mempunyai kualiti visual yang sama dengan imej asal. Dengan ini, orng lain tidak akan suspek pada hasil imej tersebut dengan mesej rahsia yang disembuyikan di dalamnya. Skim steganografi yang perlu diuji dan memastikan perubahan pada hasil imej tersebut tidak senang dikesan dengan mata kasar. Dalam tesis ini, salah satu skim steganografi untuk kajian dalam kesan imej adalah Least Significant Bit (LSB). LSB menanamkan atau memyembuyinkn mesej rahsia ke dalam imej perlindungan. Hasil sebelum dan selepas menanamkan atau menyembunyikan mesej rahsia hendaklah sama atau tidak mempunyai perbezaan yangbeasar atau jelas. Dengan itu, mesej rahsia tidak dikesan dengan mudah daripada mata kasar. Oleh itu, kualiti imej tersebut adalah imej yang baik. Kesimpulannya, skim steganografi untuk kajian dalam kesan imej akan meningkatkan keselamatan maklumat dan penyembunyian maklumat dalam imej hanya melibatkan penghantar dan penerima sahaja.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATION

ASCII: American Standard Code for Information Interchange

BMP: Microsoft Windows bitmap format file

BPCS: Bit Plane Complexity Segmentation

CGA: Color Graphics Adapter

dB: Decibels (for perceptible difference)

DCT: Discrete Cosine Transformation

DSS: Digital Signature Standard

EGA: Enhanced Graphics Adapter

GIF: Graphical Interchange Format

GIF: Graphics Interchange Format

JPEG: Joint Photographic Experts Group

LSB: Least Significant Bit

LSBs: Least-Significant-Bits Substitution

MSE: Mean Squared Error

PNG: Portable Network Graphics

PSNR: Peak Signal to Noise Ratio

RGB: Red, Green, and Blue

SHA: Security Hash Algorithm

SVGA: Super Video Graphics Array (True color)

VGA: Video Graphics AdapterXGA: Extended Graphics Array (High color)

CHAPTER 1

INTRODUCTION

This chapter is describes briefly about the image of image perceptibility in steganography. This chapter contains of five section which are background of the research project, problem statement of the research project, objective of the research project, scope of the research project and thesis organization of the research project.

1.1. Introduction

The word Steganography is from Greek origin "stegos" which means "cover" and "grafia" which mean "writing". Mean that, Steganography is the knowledge of hiding the information within other information [29]. It is a way that is hard or even impossible to tell that it is here. Usually, the secret message will be hidden to be something else such as images, articles or cover text. It also can be in an invisible ink between the visible object. Therefore, it plays role on information security.

In history, there was a first recorded on the usage of steganography. Herodotus, an ancient of Greek historian traced back to 440BC by using steganography [11]. He also has been called as "the father of history" who wanted to encourage Aristagoras of Miletus to revolt against the Persian king. In order to securely convey the plan, he shaved the head and tattooed the message on one of the most trusted salves. Then, the salves was assigned to send the hidden message after the hair grew back [11]. Demaratus, the king of Sparta from 515-491BC sent an admonition by writing it directly on the wood before apply the

beeswax surface to attack Greece. During World War II, the invisible ink is used by the French Resistance on the backs of couriers to send some messages [4].

The word perception is from Latin (preceptio, percipio) which means the process of collecting information form the visible light and interpreting it by sensory receptors to understand the visual images [30]. While, image perception is what people can't see simply from the transition of retinal stimuli (receive visual stimuli or signal which sensitive to light). This is because human eye is designed for obtaining information from large object such as daytime hunting, but it really not perfect in analyzing tin detail. This cause different image is seen from people on the same object.

Nowadays, steganography also apply in concealment of information for computer files. Many different carrier file formats can be used, such as image, audio and video file and the speed of deliver channels is high [3]. For example, in digital steganography, coding inside the transport layer for image, document or protocol is included for communication between electronic devices. But, digital images are the most popular and ideal in steganographic transmission. This is because the frequency of digital images on the internet and digital images is obscured by "noise" which are produced impact. In embedding a secret information to the host medium, it affect the original file.

Method of steganography are watermark, fingerprinting, cryptography, encryption and steganographic. While, Least Significant Bit (LSB), Masking and filtering, Transform domain techniques, Bit Plane Complexity Segmentation (BPCS), High Capacity Hiding in JPEG Images (JPEG), Hiding in the Silence of Sound (HISS), Spread spectrum and information hiding, Statistical Steganography, Distortion Techniques and Cover Generation Techniques are the example of technique for steganographic. Besides that, an information hiding system have been developed for confidentiality called as Secure Information Hiding System (SIHS) [3].

As a conclusion, this research project intends to give an overview of steganography which include term, concepts, usage, technique and method of steganography. It also attempts to test the different method of steganography with the requirement of algorithm and briefly reflect on which steganography method are more suitable for which application. Therefore, this research project will discuss about watermark, fingerprinting, cryptography and steganography. This research project also will concentrate on Least Significant Bit (LSB) for steganography techniques.

1.2. Problem Statement

Steganography is the knowledge and skill of invisible or covert communication. This is accomplished to hide information from other information or existence message. A good example is when Alice are going to send a secret message to Bob which nobody else will know about the existence of this information [11].

There are a lot of method and technique of steganography. For example, watermark, fingerprinting, cryptography, encryption and steganography for method of steganography. While, Least Significant Bit (LSB), Transform domain techniques, Bit Plane Complexity Segmentation (BPCS), and High Capacity Hiding in JPEG Images (JPEG) for techniques of steganography which have the specific function on certain case.

The problem of steganography is the size of data that user want to embed into the cover image. This most common technique of steganography is LSB which is not easy to analysis but it is not effective for data hidden quantity which will affect the PSNR value. So, size of data hidden is the problem in steganography. And, it also extend the problem to affect the quality of image in steganography.

As a summary, the main problems in the steganography are stated as below:

a) The size of data hidden
b) Quality of image of image perceptibility (PSNR value)
c) Data protection

Based on the case and the definition of the steganography methods, steganographic is the most suitable method and it is chosen. But, there is a lot of techniques in steganographic with the strength and weakness for image. So, there is a need to investigate methods used in steganography. Moreover, the steganography method is needed to test in image. So, image perceptibility can be measured after the steganographic.

1.3. Objective

The objectives of the research project are to:

a) To investigate the methods used in steganography.
b) To test steganography methods in image.
c) To measure image perceptibility after steganography.

1.4. Scope

The scope of the research project are to:

a) Exploration of method used in steganography for listing out the concept and term.
b) Implementation of steganography for grey scale images.
c) Implementation of steganography tools for testing the selected method on it perceptibility.

1.5. Thesis Organization

This thesis consists of five (5) chapters. Chapter 1 is giving the introduction and awareness about the research project. Chapter 2 is explaining literature review of the research. Chapter 3 is discussing the methodology of the research.

CHAPTER 2

LITERATURE REVIEW

This chapter is describes in detail regarding techniques, method or technologies on the image of image perceptibility in steganography from the existing research or system. This chapter will gather the related information and discuss of steganography, image and Least-Significant-Bits (LSBs) Substitution. So, it show how people use the existing research or system and what is the difference or impact on it.

2.1. General of Steganography

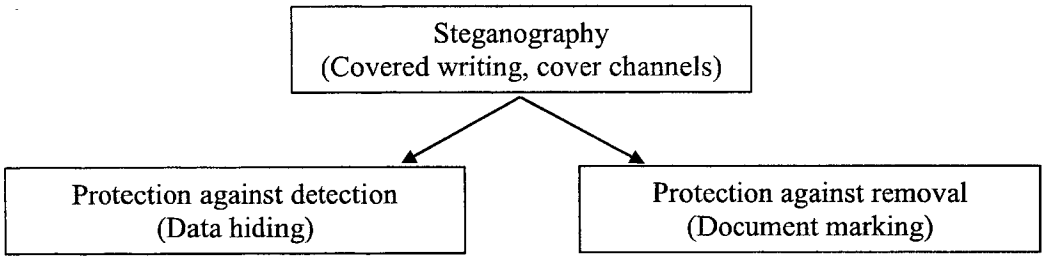

Figure 1 - 2.1 General of Steganography

Steganography is the way to enhance the communication security with covered writing or cover channels. It embed a secret message into a digital image. By this way, it has modify the nonessential pixels of the image and the produced image with secret message is called as stego-image.

2.1.1 Types of Steganography

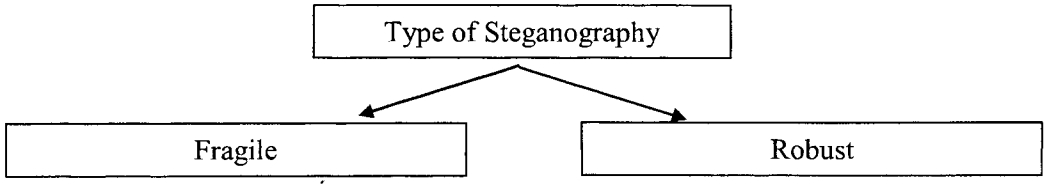

Figure 2 - 2.1.1: Types of Steganography

Two type of Steganography can be categorized, which are fragile and robust [17]. Fragile is the embed file is destroyed if it is modified. Robust is the embed file cannot easily be destroyed.

2.1.2 File Type of Steganography

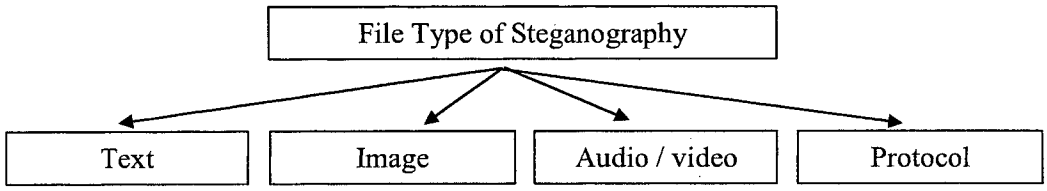

Figure 3 - 2.1.2 File type of Steganography

Besides that, many file type [12] can be used in steganography with high redundancy degree [9]. Redundancy means the bit of the object which provide accuracy and resolution when displaying the object [14]. Steganography is success when the redundant bit of an object is changed when secret message is embed and the changing is not be detected easily [14]. This research project is concentrate on image only.

2.1.3 Method of Steganography

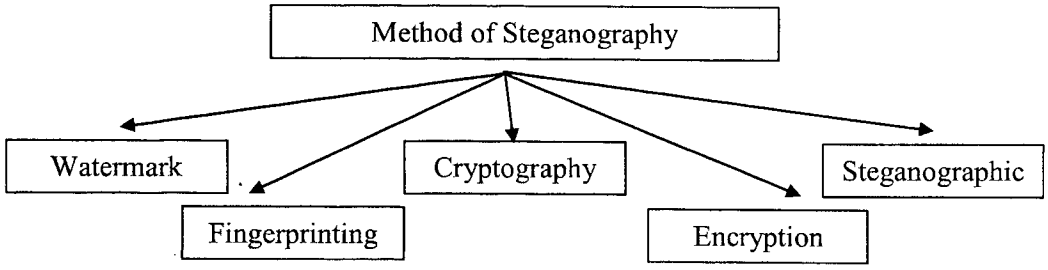

Figure 4 - 2.1.3 Method of Steganography

Many method of steganography, such as watermark, fingerprinting, cryptography, encryption and steganographic. All the steganography method have the same objective which is to protect the image and hide the information within other information. The steganography methods consist its own strong in specify field to give commitment for society. Some methods are selected as below with explanation and example [3].

Table 1 - 2.1.3 Comparison between the methods of Steganography

Watermarking	Fingerprinting	Cryptography	Steganographic
Definition: The signature or symbol in object are "marked" in the same way.	Definition: The different and unique impression from friction ridges of finger is embedded in different copies of the machine.	Definition: The transformation of protecting information into an unreadable format (cipher text).	Definition: The concealment of information which involve the sender and intended recipient only.
Characteristic: It is used for copyright protection to show origin or ownership.	Characteristic: It is used for intellectual property identification to detect who break the licensing agreement which supplying the property to third parties.	Characteristic: The protecting information only can be decrypt by the person who having the secret key	Characteristic: Imperceptibility of the information is crucial.
Example: Postage stamps.	Example: Identity card.	Example: Database protection.	Example: Sudoku.

2.1.4 Technique of Steganography

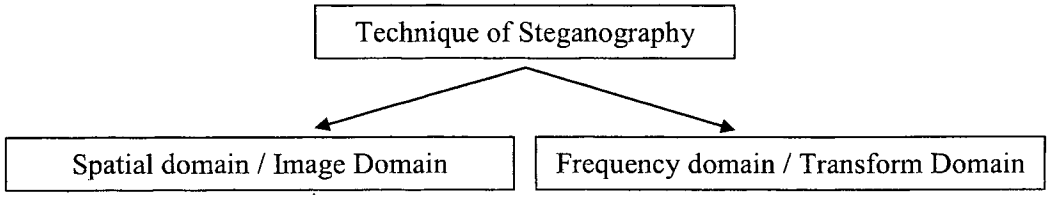

Figure 5 - 2.1.4 Technique of Steganography

Two different domains classify the steganogahic technique, such as spatial domain and frequency domain [13] [18]. In spatial domain, the embedding and hiding process concentrate on bitwise manipulation. It mean this secret message is embed by bit insertion directly for intensity of the pixels [13]. For example, manipulating the LSB in one of the color components in an image. In frequency domain, it concentrate on transformed image manipulation. It mean the image is changed first, then only the message is embedded in the image [13]. For example, Discrete Cosine Transformation (DCT) and wavelet transformation which changing the value of the quantized DCT coefficients.

A lot of existing steganography techniques after the growing of technology. Some steganography techniques is selected as the table below. The table slightly explain the different among the techniques [15] [10] [18].

Table 2 - 2.1.4 Comparison between the techniques of Steganography

Least Significant Bit (LSB)	Transform domain techniques	Bit Plane Complexity Segmentation (BPCS)	High Capacity Hiding in JPEG Images (JPEG)
The value is given on the bit position in a binary integer to determine it is even or odd (0 and 1). It is hard to defect due to the small cover modification.	The messages is hidden in the significant areas of the cover image. A low amplitude signal with low bandwidth is embed to present a larger bandwidth	The vessel data (carrier, cover, or dummy data) is used to hide the secret message during embedding process. It replace the complex areas with confidential date on the bit planes of the image.	To avoid the significant distortions in stego-image, the capacity table is used to estimate the number of bits that can be hidden in each DCT component

2.1.5 Requirement of Steganography

Steganography can be carried correctly and success when there is a number of rules and requirements are satisfy [17].

a) The secret information has been embedded inside the stego object must be correct.
b) The stego object remain same or not big changes which can't detect by naked eye.
c) The changes in the stego object must no discover by others.
d) Finally, assumption is made which only the sender and receiver knows that there is hidden information inside the stego object and able to read it.

2.1.6 The Process of Steganography

In the transmission process, opponent may try to block the message to be sent or received. The opponent may attack the stego-image if he/she doubt on the stego-image shows obvious in artifacts of carrying the secret message [1]. This is the reason why steganography is important.

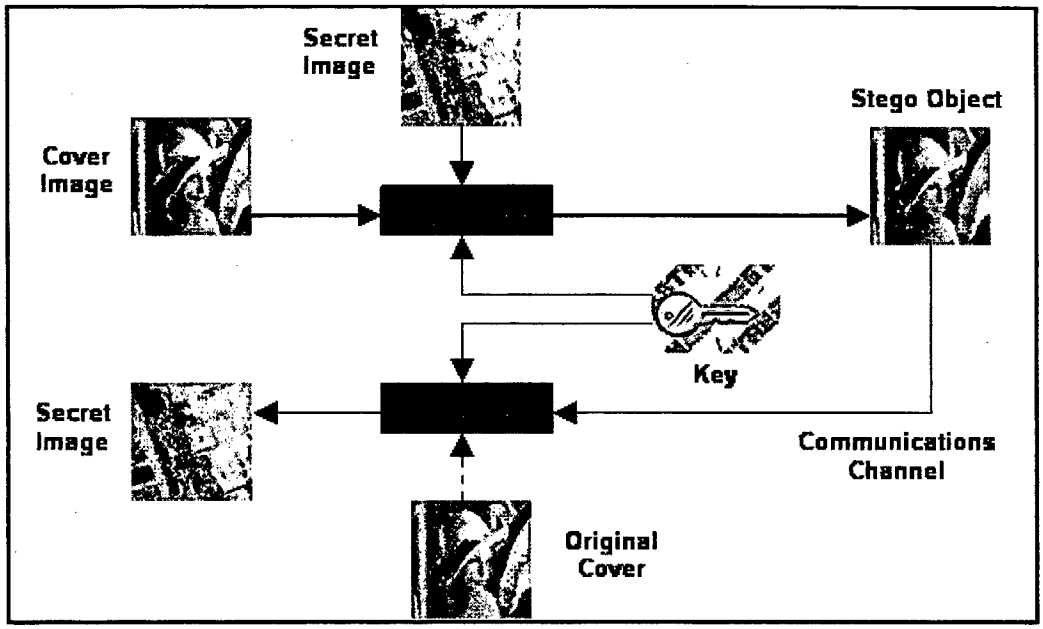

Figure 6 - 2.1.6 The process of Steganography

In the transmission process, opponent may try to block the message to be sent or received. The opponent may attack the stego-image if he/she doubt on the stego-image shows obvious in artifacts of carrying the secret message [1]. This is the reason why steganography is important.

a) The secret message/image is sent to the encoder unit.
b) The encoder with high precision is designed [2] to hide the secret message with a few distortion by changing the cover image.
c) In embedding phase, encoder needs a key to increase the security level of hiding.
d) The output of encoder is called steganograme/stego object which cover in the media [2] [11].
e) In extraction phase, decoder needs the key to unlock/extract the package.
f) The decoder is designed to extract the steganograme/stego object which is exposed. The changing of value of bit and cause different types of noises in (b).
g) Output of the decoder is sent in the receiver side.
h) The secret message is extracted to read.