Check PSM

by Tan Ching Ting

DETECTION AGAINST STEGOCONTENT ON IMAGE

TAN CHING TING

FACULTY OF INFORMATION AND COMMUNICATION
TECHNOLOGY UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2014

BORANG PENGESAHAN STATUS TESIS

JUDUL: DETECTION AGAINST STEGOCONTENT ON IMAGE

SESI PENGAJIAN: SESI 2013/2014

Saya TAN CHING TING mengaku membenarkan tesis (PSM/Sarjana/Doktor Falsafah) ini disimpan di Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dengan syarat-syarat kegunaan seperti berikut:

1. Tesis dan projek adalah hakmilik Universiti Teknikal Malaysia Melaka.
2. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. ** Sila tandakan (/)

_____ SULIT (Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)

_____ TERHAD (Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi/badan di mana penyelidikan dijalankan)

_____/_____ TIDAK TERHAD

_____ (TANDATANGAN PENULIS)

_____ (TANDATANGAN PENYELIA)

Alamat tetap :68, Lorong Matahari,Taman Tasik Permai,34000 Taiping, Perak.

Dr Siti Rahayu binti Selamat

Tarikh : _____

Tarikh: _____

DETECTION AGAINST STEGOCONTENT ON IMAGE

TAN CHING TING

This report is submitted in partial fulfillment of the requirement for the Bachelor of Computer Science (Computer Networking)

FACULTY OF INFORMATION AND COMMUNICATION
TECHNOLOGY UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2014

DECLARATION

I hereby declare that this project entitled

DETECTION AGAINST STEGOCONTENT ON IMAGE

is written by me and is my own effort and that no part has been plagiarized without citations

STUDENT: _____ DATE: _____

(TAN CHING TING)

SUPERVISOR: _____ DATE: _____

(DR.SITI RAHAYU BINTI SELAMAT)

DEDICATION

Dear Parents

Deepest thanks for giving me an encouragement and full of support from the beginning till the end. Your biggest support has helped me to achieve the final task in my university life.

Dear Lecturer, Supervisors and Evaluator

Thank you for your guidance, encouragement and knowledge.

Dear BITC Friends, Friends

Deepest thanks to all my friends for sharing information, supporting my work and help myself when facing difficulties.

ACKNOWLEDGEMENTS

First and foremost, I would like to deepest thanks to my supervisor Dr Siti Rahayu Binti Selamat as my research supervisor. Also, I would like thanks my supervisor Dr Siti Rahayu Binti Selamat given a valuable guidance, advice and showing me some example that related to my final year project. And for evaluator, Dr Nurul Azma Zakaria, thank you for guidance during the presentation on PSM and also for the evaluating and reading this report.

Furthermore, thanks to my parents and family members for giving me a big support and encouragement during the final year project progress, from the beginning till the end.

Last but not least, thanks to all my BITC friends for sharing information, supporting and encouragement during the final year project progress.

ABSTRACT

The research is about verified and detects the presence marks in stegocontent in image files to assist investigation process. Besides that, will study the current steganography tools and the methods used for detect the stegocontent on image. The research is focuses on develop the steganalysis tools which is implement with *graphical user interface (*GUI) using MATLAB R2011b. In this project, the method will be chose to use in this application software is Peak Signal-to-Noise Ratio (PSNR) steganalysis. Other than that, the research will give us to compare between the current software tools and GUI application which is a better tools. The research is carried out using MATLAB R2011b and the research take about 6 month to finish it. At the end of this research, the result will showed that GUI application is better than current tools.

ABSTRAK

Kajian ini adalah mengesahkan atau mengesan tanda-tanda dalam stegocontent dalam fail imej untuk membantu proses penyiasatan. Selain itu, akan mengaji alat-alat steganografi semasa dan kaedah yang digunakan untuk mengesan tanda-tanda kehadiran di stegocontent. Kajian ini akan tertumpu kepada membangunkan alat steganalysis dengan menggunakan MATLAB R2011b melaksanakan Graphical User Interface (GUI). Dalam projek ini, kaedah yang akan dipilih untuk menggunakan dalam aplikasi perisian ini adalah Peak Signal-to-Noise Ratio (PSNR) steganalysis. Selain itu, kajian ini dijalankan dengan menggunakan MATALB R2011b dan penyelidikan yang mengambil masa 6 bulan untuk menyelesaikannya. Pada akhir kajian ini, keputusan akan menunjukkan aplikasi GUI adalah lebih baik daripada alat-alat steganografi semasa.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Introduction

Steganography is a type of skill to hide message into text, audio or image files which not easy to notify by others. According to Kumar & Pojar (2010), cryptography is a different technique from steganography. Steganography is more about secrecy which does not require password to bypass but it just simply hide the message from people while cryptography is more about on privacy which require password to bypass. Few centuries ago, the first user of the steganography is the Sparta's king who is Demaratus. He used the wax to cover the secret message which wrote on the wood then informed the forthcoming attack to Greece. The ancient people use some techniques and method to hide the message secretly. Nowadays, internet becomes very common therefore people like to transfer message with others using steganography. According to Curran & Devitt (2008), "Watermarking is used by steganography. The watermarking sources can detect because the hidden message hides in "carrier"." Therefore, some people may misuse the skill to hide the secret message then commit crime without others notify because it is not easy to detect by the people who lack of knowledge of steganography. There are some existing steganalytic tools used to detect steganocontent but those tools are not so friendly user to those people who lack of knowledge of steganography due to not fully GUI. In conclusion, if the steganalytic tool is

correctly use by people then it can be use to help in investigation to reduce crime which the criminal like to use steganography to hide the message to others to commit crime.

1.2 Problem Statement

There are some people who like to misuse the steganography to commit crime. This characteristic causes the difficulty to detect the hidden message in stegacontent. The Research Problem (RP) is listed as Table 1.1.

Table 1.1: Summary of Problem Statements

RP	Research Problem
RP1	Difficulty on detect presence marks in stegacontent.
RP2	For the current steganalysis tool are lacks of GUI.
RP3	Difficulty to detect the hidden message in the image files to assist crime.

From the research problem in Table 1.1, three research questions are conducted to identify the research problem. The explanation for each of the Research Problems (RP) is explained as follows:

RP1: Difficulty on detect presence marks in stegacontent.

This research problem is identifying the existing tools that can be used to detect the presence marks of stegocontent.

RP2: For the current steganalysis tool are lacks of GUI.

This research problem describes the current tools on steganography are command-based which are difficulty to user to remember the command to be used.

RP3: Difficulty to detect the hidden message in the image files to assist crime.

This research problem describes the difficulty to detect marks in image files and difficulty to identify the content of image file that can be used as evidence of the crime during the investigation process.

1.3 Research Questions

In this study, the research question was identified based on the problem that has been classified in Table 1.2. The research questions were summarizing shown in Table 1.2 below:

Table 1.2: Summary of Research Question

RP	RQ	Research Question
RP1	RQ1	How difficult to detect presence marks in stegacontent?
RP2	RQ2	How to improve the steganalysis tool with GUI?
RP3	RQ3	How to detect the hidden message in image files to assist crime?

RQ1: How difficult to detect presence marks in stegacontent?

This research question is to find out how difficult the people who lack of knowledge of steganography to detect the presence marks in stegacontent.

RQ2: How to improve the steganalysis tool with GUI?

This research question is guide how graphical user interface (GUI) can be implemented in steganalysis tools.

RQ3: How to detect the hidden message in image files to assist crime?

This research question is to find out how the stegocontent can be detected in an image file.

1.4 Project Objectives

Based on the research problems stated in section 1.3, appropriate research objectives are constructed in Table 1.3.

Table 1.3: Summary of Research Objectives

RP	RQ	RO	Research Objectives
RP1	RQ1	RO1	To study the existing steganalytic tools and the technique used to detect hidden message in stegocontent.
RP2	RQ2	RO2	To implement the GUI function to steganalysis tools.
RP3	RQ3	RO3	To detect the hidden message in image files to assist crime.

RO1: To study the existing steganalytic tools and the technique used to detect hidden message in stegocontent.

This research objective is to find out which is the existing steganalytic tools and technique used to detect the hidden message in stegocontent.

RO2: To implement the GUI function to steganalysis tools.

This research objective is to develop a user friendly steganalysis tools to improve current tool.

RO3: To detect the hidden message in image files to assist crime.

This research objective is to detect speeding up using GUI steganalysis tool. This objective will help on process of identifying the status of an image.

1.5 Scope

The scopes of this project are:

i. The steganalysis tool detects on image file only.
ii. The steganalysis tool only can detect the stegacontent on the format of JPEG/JPG and PNG.
iii. The steganalysis tool use Least Significant Bits (LSB) method to detect the stegacontent.

1.6 Report Organization

This report consists of six chapters namely Chapter 1: Introduction, Chapter 2: Literature Review, Chapter 3: Methodology, Chapter 4: Design and Implementation, Chapter 5: Testing and Result Analysis and Chapter 6: Conclusion.

Chapter 1: Introduction

This chapter discusses the introduction, research problem, research question, research objectives, scopes and report organization.

Chapter 2: Literature Review

This chapter discusses the related work of this project such as method of steganalytic, analysis of image steganography and steganalysis attack.

Chapter 3: Methodology

This chapter discusses the methods used to detect stegacontent are analyzed and organize sequence of project work phase by phase.

Chapter 4: Design and Implementation

This chapter is about design a GUI application to detect hidden message in stegocontent. The coding process will be carried out during implementation process in order to produce a functional application. This application will use MATLAB to design.

Chapter 5: Testing and Result Analysis

This chapter is about testing the developed GUI steganalysis tool to get the PSNR and MSE result.

Chapter 6: Conclusion

This chapter will discuss the project summarization, observation on weaknesses and strengths, future work and contribution of the project.

1.7 Summary

In this chapter, research problem, research question and research objective had been discussed and identified. Next chapter will be discussed about the literature review of this project.

CHAPTER 2

Literature Review

2.1 Introduction

In previous chapter, research problem, research question and research objective had been discussed and identified. For this chapter, literature review will be discussed. In order to understand how the message is hided, the knowledge on the information hiding is needed. Figure 2.1 shows the operational framework: Literature review phase.

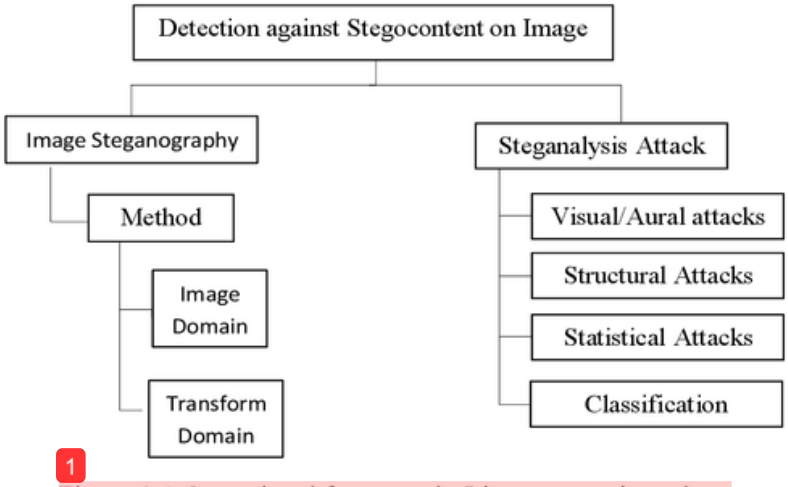

Figure 2.1 Operational framework: Literature review phase

Figure 2.1 shows the main topic will be focused in this project which are Detection against Stegocontent on Image. It divided into two main categories

namely Image Steganography and Steganalysis Attack. The information hiding is discussed further in Image Steganography category.

2.2 Image Steganography

Devitt & Curran (2008) stated that "digital images are the most widely used medium for steganography today and it takes advantage of our limited visual perception of color. The most popular image formats on the internet are the graphics interchange format (GIF), joint photographic experts group (JPEG) format, the portable network graphics (PNG) format and the bitmap format (BMP)". "Large images are the most desirable for steganography because they have more space to hide the data" (Queirolo, 2006). According to Calpe (2006), "This field is expected to continually grow as fast development of computer graphics power and technology".

2.2.1 Methods of Image Steganography

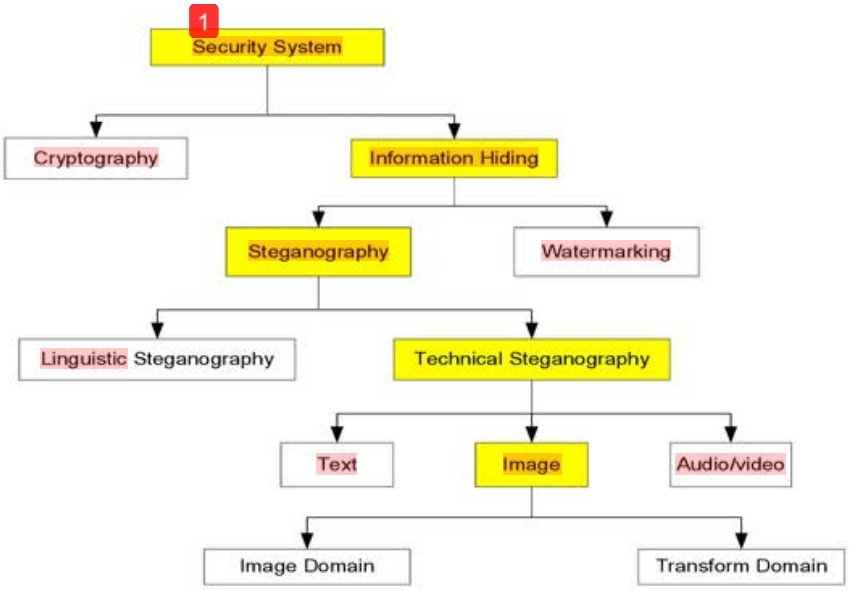

Figure 2.2 Summary charts for Methods of Image Steganography