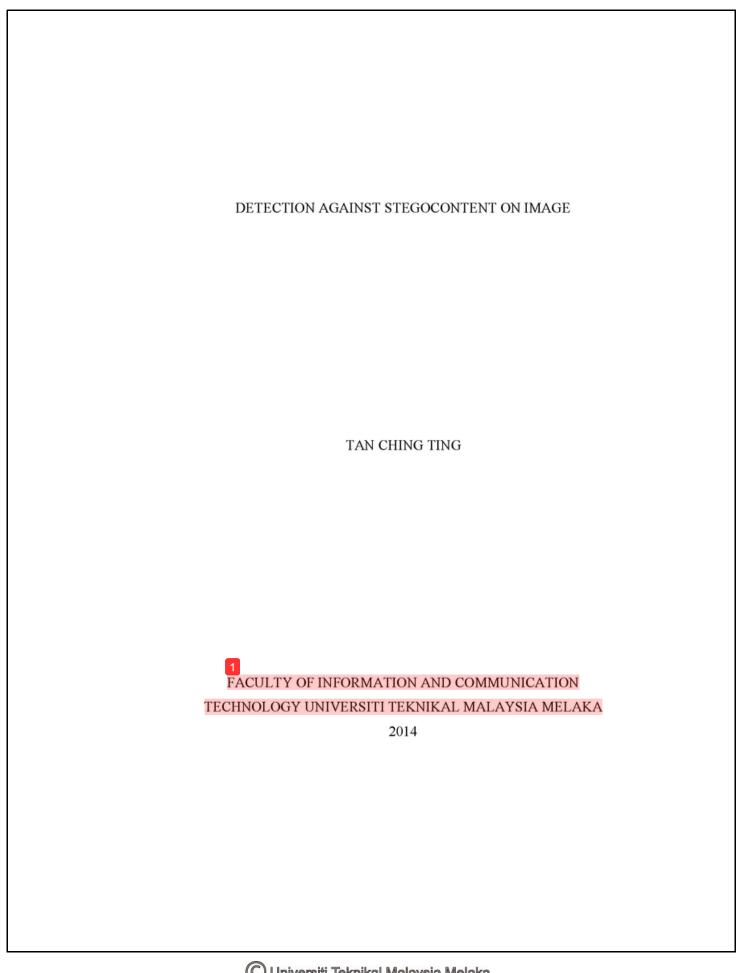
Check PSM

by Tan Ching Ting

FILE FYP-DETECTION_AGAINST_STEGOCONTENT_ON_IMAGE.PDF (1.1M)

TIME SUBMITTED 25-AUG-2014 12:39AM WORD COUNT 10671 SUBMISSION ID 440780684 CHARACTER COUNT 54461





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:

- Tesis dan projek adalah hakmilik Universiti Teknikal Malaysia Melaka.
- Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan untuk tujuan pengajian sahaja.
- Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
- ** 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

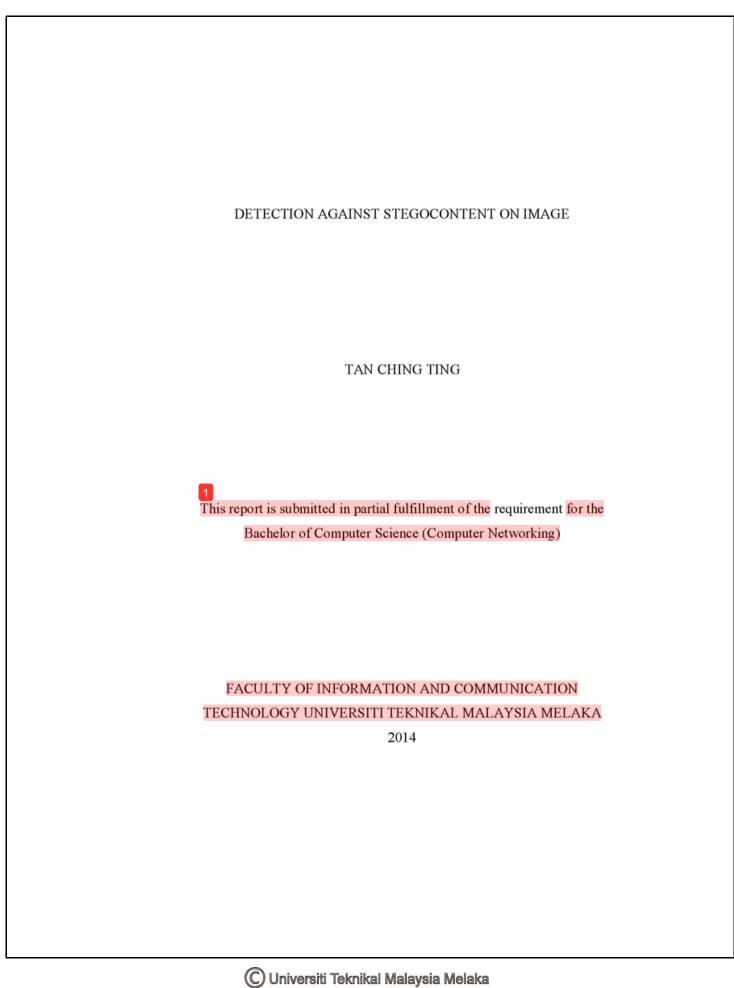
(TANDATANGAN PENULIS) (TANDATANGAN PENYELIA)

Alamat tetap :68, Lorong Matahari, Taman Dr Siti Rahayu binti Selamat Tasik Permai, 34000 Taiping, Perak.

1

Tarikh : ____

Tarikh:



	DECLARATION
	DECLINATION
	I hereby declare that this project entitled
DET	ECTION AGAINST STEGOCONTENT <mark>ON</mark> IMAGE
is written by	me and is my own effort and that no part has been plagiarized
	without citations
	1
STUDENT:	DATE:
	(TAN CHING TING)
	(IAN CHING HNG)
SUPERVISOR	:: DATE:
(DR.SI	TI RAHAYU BINTI SELAMAT)
(=100)	
	i e e e e e e e e e e e e e e e e e e e
	Universiti Teknikal Malavsia Melaka

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 alatalat steganografi semasa.

TABLE OF CONTENTS

SUB	JECT	PAGE
ACK ABST ABST TABI	ICATION NOWLEDGEMENT FRACT FRAK LE OF CONTENTS OF TABLES	i ii iv v vi x xi
l.	INTRODUCTION	
1.1	Introduction	1
1.2	Problem Statements	2
1.3	Research Questions	3
1.4	Project Objective	4
1.5	Scopes	5
1.6	Report Organization	5
1.7	Summary	6
2	LITERATURE REVIEW	
2.1	Introduction	7
2.2	Image Steganography	8
	1 DEC. DED. ACK. ABST. ABST. TAB. LIST. LIST. 1.1 1.2 1.3 1.4 1.5 1.6 1.7	DECLARATION DEDICATION ACKNOWLEDGEMENT ABSTRACT ABSTRAK TABLE OF CONTENTS LIST OF TABLES LIST OF FIGURES INTRODUCTION 1.1 Introduction 1.2 Problem Statements 1.3 Research Questions 1.4 Project Objective 1.5 Scopes 1.6 Report Organization 1.7 Summary LITERATURE REVIEW 2.1 Introduction

	2.2.1	Methods of Image Steganography	8
	2.2.2	Analysis of Image Steganography Methods	11
	2.2.3	Popular Steganalytic Methods	13
2.3	3 Stegan	nalysis attacks	14
	2.3.1	Steganalysis Attack Types	14
	2.3.2	Steganalysis Attack Classification	15
2.4	4 Summ	ary	17
23			
CHAPTER 3	METI	HODOLOGY	
3.1	Introd	uction	18
3.2	Resear	rch Approaches	18
3.3	Brojec	t Implementation	20
	3.3.1	Planning Analysis	20
	3.3.2	Analysis Phase	20
	3.3.3	Design Phases	21
	3.3.4	Construction Phase	24
	3.3.5	Testing Phase	24
	3.3.6	Maintenance Phase	25
3.4	4 Projec	t Requirements	25
	3.4.1	Software Requirements	25
	3.4.2	Hardware Requirements	26
3.5	Projec	t Schedule and Milestones	27
	3.5.1	Gantt chart	27
	3.5.2	Milestones	28
3.6	5 Summ	ary	30
18			
CHAPTER 4	DESIG	GN AND IMPLEMENTATION	

	4.1	Introdu	action	31
	4.2	GUI A	pplication Interface Layout	31
		4.2.1	File Function	33
		4.2.2	Test Function	36
		4.2.3	Remove Function	39
		4.2.4	About Menu Layout	42
		4.2.5	Exit Function	43
	4.3	Algorit	thm Detecting Marks in Stegocontent	44
	4.4	Summa	ary	45
1 CHAPTER 5		TESTI	ING AND RESULT ANALYSIS	
	5.1	Introdu	ection	46
	5.2	Test Pl	an	46
		5.2.1	Test Organization	46
		5.2.2	Test Environment	47
		5.2.3	Test Dataset	48
		5.2.4	Test Result of Steganography Software Tool	149
		5.2.5	Test Result of GUI Steganalysis Application	151
	5.3	Result	Analysis	52
		5.3.1	Analysis of Result Testing	52
	5.4	Discus	sion of Result	54
	5.5	Summa	ary	55
CHAPTER 6		PROJ	ECT CONCLUSION	
	6.1	Introdu	action	56
	6.2	Project	Summarization	56
	6.3	Contrib	oution	57

	1	
6.4	Observation on Weaknesses and Strengths	57
<mark>6</mark> .5	Future Work	58
REFERENCES		59
APPENDIX A		63
APPENDIX B		64

1 LIST OF TABLES

TABLE	TITLE	PAGI
1.1	Summary of Problem Statements	2
1.2	Summary of Research Questions	3
1.3	Summary of Research Objectives	4
2.1	Popular Steganalytic Methods	13
2.2	Classification of attack and Description	16
2.3	Summary of Steganalysis Attack	17
3.1	Software Requirements	26
3.2	Hardware Requirements	27
3.3	PSM 1 Milestones	29
3.4	PSM 2 Milestones	30
5.1	Responsibilities of person in testing process	47
5. <mark>2</mark>	Summary of Dataset for Testing	49
5.3	Result Testing of Tool 1 (4t HIT Mail Privacy LITE)	50
5.4	Result Testing of Tool 2 (Image Steganography)	50
5.5	Result Testing of Tool 3 (OpenStego)	51
5.6	Test Result of GUI Steganalysis Application	51
5.7	Result of PSNR value with size and three file embedded	1 53
5.8	Summary result of Tool 1, Tool 2 and Tool 3	54
5.9	Summarization of experimental result	54
6.1	Strength and Weaknesses of GUI Steganalysis Applicat	ion 57

7 LIST OF FIGURES

FIGURE	TITLE PAG	E
2.1	Operational framework	7
2.2	Summary charts for Methods of Image Steganography	8
2.3	Summary of proposed project	12
2.4	Type of attack used by steganalyst	16
3.1	Agile modeling	19
3.2	Prototype Interface Design	22
3.3	GUI Application Systems	23
3.4	Use-case diagrams	24
3.5	Project Gantt chart	28
4.1	GUI Application Interface Layout	32
4.2	Codes to display the image box in twice	33
4.3	File Image Layout	33
4.4	Codes of display input file information	34
4.5	Flow chart of File Function	35
4.6	Interface's Layout when File button clicked	36
4.7	Codes of testing the chosen image	37
4.8	Flow chart of Test Function	38
4.9	Interface's Layout when Test button clicked	39
4.10	Codes of remove all the input file information and result	40
4.11	Flow chart of Remove Function	41
4.12	Interface's Layout when Clear button clicked	42

4.13	Code of message box	43
4.14	About Menu Layout	43
4.15	Code of exit the GUI application system	43
4.16	Formulas of PSNR and MSE	44
5.1	Test Environment Design	48



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 GUL

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.

3

1 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.
- The steganalysis tool only can detect the stegacontent on the format of JPEG/JPG and PNG.
- 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.

25 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.

6



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.

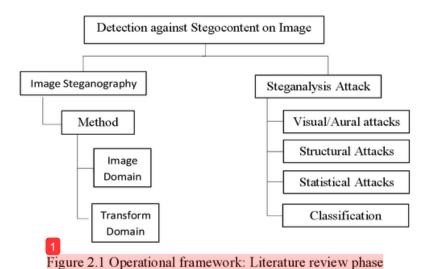


Figure 2.1 shows the main topic will be focused in this project which are Detection against Stegocontent on Image. It divided into two main categories

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

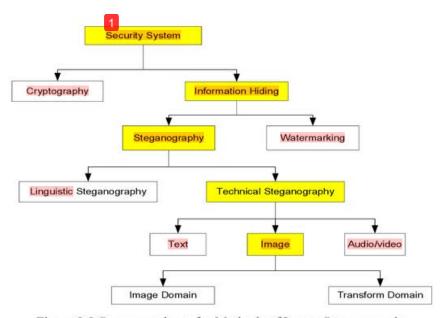


Figure 2.2 Summary charts for Methods of Image Steganography

8