

FORMULATING IMAGE STEGANOGRAPHY TO IMPROVE SECURITY OF
THE HIDDEN IMAGE

SIM FU CHENG

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA
2015

BORANG PENGESAHAN STATUS TESIS

JUDUL: FORMULATING IMAGE STEGANOGRAPHY TO IMPROVE SECURITY OF THE HIDING IMAGE.

SESI PENGAJIAN: SESI 2014/2015

Saya SIM FU CHENG 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 hak milik 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)

Alamat tetap : No.1, Jalan Bawal 2,
Taman Mutiara, 42800 Tg. Sepat,
Selangor.

(TANDATANGAN PENYELIA)

Dr. Siti Rahayu Binti Selamat

Tarikh : _____

Tarikh: _____

FORMULATING IMAGE STEGANOGRAPHY TO IMPROVE SECURITY OF
THE HIDDEN IMAGE

SIM FU CHENG

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
2015

DECLARATION

I hereby declare that this project entitled

FORMULATING IMAGE STEGANOGRAPHY TO IMPROVE SECURITY OF
THE HIDDEN IMAGE

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

STUDENT: _____
(SIM FU CHENG)

DATE: _____

SUPERVISOR: _____
(DR.SITI RAHAYU BT SELAMAT)

DATE: _____

DEDICATION

Dear Parents

Thank you for your giving me the big support and encouragement. Your biggest support and care have 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

Thank you for your sharing information, supporting and encouragement when facing difficulties.

ACKNOWLEDGEMENTS

I would like to thank those who had helped me when I faced the problem during the process of completing this final year project. For my supervisor, Dr. Siti Rahayu binti Selamat, you are the best supervisor that I meet in my university life. No matter what the problems that I faced in my final year project, you will spend your precious time in order for me to solve the problems. Besides that, your guidance and opinions you giving to me, I appreciate it. At here, I would like to say, thank you Madam. And for the evaluator, En. Zulkiflee bin Muslim, thank you for the guidance during the presentation on PSM and also for the evaluating and reading this report.

I would also like to thank to my beloved parents and family for giving me the big support whenever I meet with problems. Your all support is strong energy for me to finish my university life.

Last but not least, I would like to give a big thanks to all my friends and BITC coursemates for their support and sharing knowledge. Sharing is caring is our slogan in BITC. I am grateful to have you all because we learning and sharing together.

Thanks to GOD and this is a beginning big task for my life.

ABSTRACT

Image steganography is a technique that can hide the secret message into the image without being noticed by the eyes of the human. In order to ensure the security of the contents for the sensitive message, the steganography technique is being implemented. This project focuses on the least-significant bit (LSB) image steganography techniques and enhancing the security of the hiding image. Thus the project is necessary to know how the image techniques work and which of the techniques can produce the better output on the aspect of security. Besides, the project will provide the comparison between different types of image steganography techniques and identify the effective technique among all of the types of the image steganography. Furthermore, the project will develop a security tool for the image steganography and determine an encryption and decryption method in the hiding process using Microsoft Visual Studio 2010. At the end of this project, the image produced by the LSB technique is enhanced with the cryptography technique and message digest algorithm in order to ensure the security and integrity of the secret message. In the future, a complete application can be developed by enhancing the current script developed in this project that is able to defend against all kinds of intrusion.

ABSTRAK

Imej steganografi merupakan teknik yang dapat menyembunyikan mesej rahsia ke dalam imej tanpa dikesan oleh mata manusia. Dalam usaha untuk memastikan keselamatan kandungan mesej yang sensitif, teknik steganografi telah dilaksanakan. Projek ini tertumpu kepada teknik *Least-Significant Bits (LSB)* imej steganografi dan meningkatkan keselamatan imej yang dihasilkan oleh teknik ini. Oleh itu projek ini adalah perlu untuk mengetahui bagaimana teknik imej berfungsi dan yang mana satu teknik boleh menghasilkan output yang lebih baik dalam aspek keselamatan. Selain itu, projek ini akan menyediakan perbandingan antara pelbagai jenis teknik imej steganografi dan mengenalpasti teknik yang efektif di antara semua jenis imej steganografi. Tambahan pula, projek ini akan membangunkan alat keselamatan untuk steganografi imej dan menentukan kaedah penyulitan dan penyahsulitan dalam proses persembunyian menggunakan Microsoft Visual Studio 2010. Pada akhir projek ini, imej yang dihasilkan oleh teknik steganografi akan dipertingkatkan dengan teknik kriptografi dan juga mesej mencerna algoritma untuk memastikan keselamatan dan integriti mesej rahsia. Pada masa yang akan datang, satu aplikasi lengkap akan dibangunkan dengan menambahbaik skrip yang dibangunkan dalam projek ini di mana aplikasi ini dapat mempertahankan sistem terhadap semua jenis pencerobohan.

TABLE OF CONTENTS

CHAPTER	SUBJECT	PAGE
	DECLARATION	ii
	DEDICATION	iii
	ACKNOWLEDGMENT	iv
	ABSTRACT	v
	ABSTRAK	vi
	TABLE OF CONTENTS	vii
	LIST OF TABLES	xii
	LIST OF FIGURES	xiii
	LIST OF ABBREVIATIONS	xvi
CHAPTER 1	INTRODUCTION	
	1.1 Project Background	1
	1.2 Problem Statement	2
	1.3 Research Questions	3
	1.4 Objectives	4
	1.5 Scopes	5
	1.6 Project Contributions	5
	1.7 Project Significant	5
	1.8 Report Organization	6
	1.9 Summary	7

CHAPTER 2	LITERATURE REVIEW	
2.1	Introduction	8
2.2	Steganography	9
2.2.1	Steganography Definition and Concept	10
2.2.2	Steganography process	12
2.3	Steganography Types	13
2.3.1	Image Steganography Definitions	13
2.3.2	Image Steganography Terminologies	14
2.4	Image Steganography Techniques	14
2.4.1	Spatial domain methods	14
2.4.2	Transform Domain Technique	21
2.4.3	Distortion techniques	23
2.4.4	Masking and Filtering techniques	24
2.5	Analysis of Image Steganography Techniques	24
2.6	Proposed Solution	27
2.7	Summary	28
CHAPTER 3	METHODOLOGY	
3.1	Introduction	29
3.2	Problem Methodology	29
3.2.1	Phase I: Literature Review	30
3.2.2	Phase II: Analysis	30
3.2.3	Phase III: Design Phase	31
3.2.4	Phase IV: Implementation Phase	31
3.2.5	Phase V: Testing and Evaluation Phase	31
3.3	Project framework	32
3.3.1	Develop technique script	32
3.3.2	Implement script on laptop	32
3.3.3	Produce stego-image with encryption	32
3.4	Project requirement	33

3.4.1 Software Requirement	33
3.4.2 Hardware Requirement	33
3.5 Project schedule and Milestones	34
3.6 Summary	36
CHAPTER 4	DESIGN
4.1 Introduction	37
4.2 Steganographic Technique Algorithm	37
4.2.1 Least Significant Bit (LSB)	37
4.3 Cryptography Technique Algorithm	44
4.3.1 Rijndael Algorithm	44
4.4 Message digest algorithm	47
4.4.1 Generation of hash data	47
4.4.2 Validation of hash data	48
4.5 Summary	50
CHAPTER 5	IMPLEMENTATION
5.1 Introduction	51
5.2 Application Development Environment Setup	52
5.3 Configuration Management	53
5.3.1 Hiding image using LSB algorithm process	54
5.3.2 Encrypt the hiding image process	59
5.3.3 Generate hash value by message digest process	64

5.4 Result	68
5.4.1 Print screen of formulation image with LSB algorithm module	68
5.4.2 Printscreen of encryption stego-image with password module	70
5.4.3 Printscreen of generation of hash data using message digest algorithm module	71
5.5 Summary	72
CHAPTER 6	TESTING
6.1 Introduction	73
6.2 Test Plan	73
6.2.1 Test Organization	73
6.2.2 Test Environment	74
6.3 Test Strategy	75
6.3.1 Unit testing	75
6.3.2 Integrate testing	75
6.4 Test Design	75
6.4.1 Test Description	76
6.4.2 Testing process	81
6.5 Test Result and Analysis	87
6.5.1 Test Result of Formulation image with LSB algorithm	87
6.5.2 Test Result of Encryption of stego-image with password	88
6.5.3 Test Result of Generation of hash data using message digest algorithm	89
6.6 Summary	90

CHAPTER 7	CONCLUSION	
	7.1 Introduction	91
	7.2 Project Summarization	91
	7.3 Project Contribution	92
	7.4 Project limitation	92
	7.5 Future work	93
	REFERENCES	94
	APPENDICES	97
	APPENDIX A	98
	APPENDIX B	102
	APPENDIX C	105

LIST OF TABLES

TABLE	TITLE	PAGE
1.1	Summary of the Problem Statement	2
1.2	Summary of the Research Questions	3
1.3	Summary of Research Objectives	4
2.1	Comparison of the techniques	25
3.1	Software Requirement	33
3.2	Hardware Requirement	34
3.3	Summary of project schedule and milestones	34
6.1	Responsibility of the person in testing process	74
6.2	Hardware Requirement	74
6.3	Software Requirement	75
6.4	Result of the testing process for the formulation image with LSB module	87
6.5	Result of the testing for the encryption of stego- image with password module	88
6.6	Result of the testing for the generation of hash data using message digest algorithm	89

LIST OF FIGURES

FIGURE	TITLE	PAGE
2.1	Literature review phase	9
2.2	Process of Steganography	12
3.1	Process of Project Methodology	30
3.2	Project framework	32
4.1	Flow chart of LSB embedding process of Application	39
4.2	Flow chart of LSB embedding algorithm	40
4.3	Flow chart of LSB extracting process	42
4.4	Flow chart of LSB extracting algorithm function	43
4.5	Flow chart of encryption process	45
4.6	Flow chart of decryption process	46
4.7	Generation of hash data	47
4.8	Validation of hash data	49
5.1	Overview of the image steganography application	52
5.2	Overview of process based on the modules	54
5.3	Overview of hiding image using LSB algorithm Process	55
5.4	Embedding the secret message process flow	56
5.5	Pseudocode of Embedding the secret message	57
5.6	Extracting secret message from the hiding image process flow	58

5.7	Pseudocode of extracting secret message from hiding image	59
5.8	Overview of encrypt the hiding image process	60
5.9	Encryption the image process flow	61
5.10	Pseudocode of encrypt the image process	62
5.11	Decrypt the image process	63
5.12	Pseudocode of Decrypt the image process	64
5.13	Generate hash value by message digest process flow	65
5.14	Flow chart of Get hash data process	66
5.15	Pseudocode of GetHashData process	67
5.16	Flow chart of Validate hash data process	67
5.17	Pseudocode of Validate hash data	68
5.18	Upload and enter secret message	68
5.19	Secret text hide inside the image selected successfully	69
5.20	Result of formulation image with LSB algorithm Module	69
5.21	Encrypted the secret text into the image by password	70
5.22	Result of encryption stego-image with password Module	70
5.23	Generation of Hash Data	71
5.24	Result of generation of hash data using message digest algorithm module	71

6.1	Output after the secret message embedded into the image	76
6.2	Original Image	77
6.3	Stego-image	77
6.4	File size of original Image	78
6.5	File size of stego-image	78
6.6	Length of password must be more than 6 characters	79
6.7	Error message prompt out	79
6.8	Validation shown True message	80
6.9	False message prompt out	80
6.10	Image 1 before encoding	81
6.11	Stego-image 1 after decoding	81
6.12	Image 2 before encoding	82
6.13	Stego-image 2 after decoding	82
6.14	Result of testing by using secret message that consists of character only	83
6.15	Result of testing by using secret message that consists of character, symbol and space	83
6.16	Less than 6 characters password been entered	84
6.17	6 characters password been entered	84
6.18	More than 6 characters password been entered	85
6.19	Hash data produced from first secret message	86
6.20	Hash data produced from second secret message	86

LIST OF ABBREVIATIONS

ALPHABET	WORD	EXPLANATION
B	bmp	bitmap image file
L	LSB	Least-significant bits
R	RP	Research Problem
R	RQ	Research Question
R	RO	Research Objective

CHAPTER I

INTRODUCTION

1.1 Project Background

Steganography come from a Greek word *steganos*, which indicate as masked or secret, and graphy which mean by drawing or writing. Basically, steganography can defined as anact of hiding secret message into a file that hard or difficult by the eyes of human.

The evolution on the Internet technologyis became one of the most crucial factors of information technology and communication and this caused the issue on security information. In order to ensure the security of the contents for the sensitive message, technique steganography is being implemented. This can be achieve by hiding the secret information in other file, thus conceal the existence of the information from other party. In the aspect of image steganography, the secret message is hidden in

image files. The practice of conceal the sensitive message is came from the Greek historian Herodotus has write a nobleman which is needed to communicate with his son-in-law. As solution, he has razor the head of the slaves and tattooed the secret message onto the slave's scalp. By waiting the slave's hair grew back,the head of slave will dispatched with the conceal message. Other than that, invisible ink was used to write secret message on a pieces of paper and the paper appeared as a blank pieces of paper from the human's eyes during World War II. Liquids like vinegar, milkare used to recover the hidden message, andthe message on the paper will become darken and visible to the others when these substance is heated. Nowadays,most of the steganography are used on computers wherethe digital data act as the carriers and transfer through the high speed transfer networks channels.As contrast cryptography keeping the contents of secret message whereas steganography keeping the existence of a sensitive information from the human's eyes. Both technology are purpose to protect message from unauthorized party.The intensity of steganography can be enhanced with cryptography technology.

1.2 Problem Statements

Steganography can be applied differently in digital image, audio and video file. Basically, the problem facing by the steganography is stated below. The Problem Statement(PS) of the project are listed in the Table 1.1.

Table 1.1: Summary of the Problem Statement

No.	Problem Statement
PS1	Difficult to choose an effective techniques for image steganography.
PS2	Facing a challenge to retain the security of hidden image when the size of secret message increased providing that the quality of image is preserve.

1.3 Research Question

Based on the project study, the research question was determined based on the problem that has been determined in Table 1.1. The Research Questions(RQ)are listed in Table 1.2.

Table 1.2: Summary of the Research Questions

PP	RQ	Research Questions
PS1	RQ 1	What is the best algorithm for the image steganography technique?
PS2	RQ2	What is the suitable method to maintain the security of the hiding image?
	RQ3	What is the limit on the size of data hidden that user can embed inside an image without affecting the quality of image?

RQ1: What is the best algorithm for the image steganography technique?

This research question is to identify the best and suitable algorithm of the image steganography. The purpose of this research question is to limit the scope on the type of the image steganography.

RQ2: What is the suitable method to maintain the security of the hiding image?

Nowadays, we can facing a challenge to retain the security of hiding images with high rate of data hiding as the stego-image file size will increase after the hiding process. Therefore, this research question is to determine suitable method to maintain the security of the hiding image after embedded with image steganography algorithm.

RQ3: What is the limit on the size of data hidden that user can embed inside an image without affecting the quality of image?

This research question is to find out the limit on the size of data hidden that user can embed inside an image and help us identify the basic requirement and expectation of the user on the size of the data hidden.

1.4 Objective

The research objectives are listed in Table 1.3 based on the problem statement and research questions.

Table 1.3: Summary of Research Objectives

PP	RQ	RO	Objective
PS1	RQ1	RO1	To identify an effective algorithm for the image steganography technique that can make the message conceal with more easy and user friendly.
PS2	RQ2	RO2	To determine an encryption and decryption method in the hiding process.
	RQ3	RO3	To develop a security tool for the image steganography.

RO 1: To identify an effective algorithm for the image steganography technique that can make the message conceal with more easy and user friendly.

In order to improve the security of the hiding image, the first step we must do is limiting the scope of the image steganography based on the research.

RO 2: To determine an encryption and decryption method on hiding process.

After that, we must determine the suitable method to maintain the security of the hiding image and explore the encryption and decryption module in order to improve the security of hiding image.

RO 3: To develop a security tool for the image steganography.

After determine the maximum size of data hidden that can embedded inside the image, then formulate an steganography algorithm and produce security tool based on image steganography technique.

1.5 Scopes

There are many types for the steganography which include audio steganography, image steganography and also text steganography.

In this project, we restrict the scope on the image steganography and find out the suitable technique to improve the security of the hidden image.

1.6 Project Contributions

By the end of this project, the project contributions that must be achieve in this project:

- i. The effective steganography algorithm purpose for data hidden technique in the image success increase the security of hidden data providing that quality of hiding image is preserve.
- ii. The security of the hidden image is still retain with the increasing of the data hidden size is successfully been conduct.

1.7 Project Significant

By formulating the image steganography algorithm, it can enhance the security of hiding image when the data hidden size is increase and maximize the data hiding rate can be use without affecting the quality of images where the third party would be completely ignorant about any hidden information.

1.8 Report Organization

In this report, there are consist of seven chapter which included Introduction, Literature Review, Methodology, Design, Implementation, Testing and Result Analysis and Conclusion.

Chapter 1 Introduction

In this chapter, introduction, project background, problem statement, research question, objective, scope, project significant and report organization are clearly stated.

Chapter 2 Literature Review

In this chapter, the related article of this project, such as algorithm used by the steganography, the process of the steganography are clearly stated.

Chapter 3 Methodology

In this chapter, the project is start from study article about the related image steganography and analysis the problem and finally bring out the solution. All of these are clearly stated within chapter 3.

Chapter 4 Design

In this chapter, the design of coding and formulating steganography algorithm to improve the security of hiding image are clearly stated in the chapter 4.

Chapter 5 Implementation

In this chapter, the implementation of coding into the application where it will formulating steganography algorithm to improve the security of hiding image are clearly stated in this chapter.