THE CAPABILITY OF IMAGE FILES AS COVER MESSAGE IN STEGANOGRAPHY

HANIZAN SHAKER BIN HUSSAIN

UNIVERSITI UTARA MALAYSIA
2005

THE CAPABILITY OF IMAGE FILES AS COVER MESSAGE IN STEGANOGRAPHY

A dissertation submitted to the Faculty of Information Technology in partial fulfillment of the requirements for the degree Master of Science (Information Technology), Universiti Utara Malaysia

by

HANIZAN SHAKER BIN HUSSAIN

Universiti Utara Malaysia
25th March, 2005

UNIVERSITI UTARA MALAYSIA
2005

PERMISSION TO USE

In presenting this thesis in partial fulfillment of the requirements for a post graduate degree from Universiti Utara Malaysia, I agree that Universiti Library may make it freely available for inspection. I further agree that permission for copying of this thesis in any manner, in whole or in part, for scholarly purposes may be granted by my supervisor or, in their absence, by the Dean of the Faculty of Information Technology. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to Universiti Utara Malaysia for any scholarly use which may be made of any material from my thesis.

Request for permission to copy or to make other use of materials in this thesis, in whole or in part, should be addressed to:

Dean of the Faculty of Information Technology
Universiti Utara Malaysia
06010 UUM Sintok
Kedah Darul Aman

ABSRACT

This paper is focusing on the capability of image files as cover message to send the text files. The images were classified according to their compression technique, lossless and lossy compression. The measurements are identified in order to test their capability in term of the size of file, the color intensity level, the integrity data, and the time execution. All the measurements would be tested by using the developed tool called StegaNo. The result of the study seem to suggest BMP image as a cover message than JPEG image.

Key words: cover message, lossless and lossy compression, StegaNo, BMP, JPEG.

ABSTRAK

Kertas kajian ini, menumpukan kepada keupayaan fail-fail imej sebagai mesej hadapan untuk menghantar fail-fail teks. Manakala fail-fail imej pula boleh dikelaskan mengikut teknik mampatan masing-masing, iaitu samada mampatan jenis 'lossless' (fail-fail BMP) atau 'lossy' (fail-fail JPEG). Kajian dilakukan berdasarkan beberapa parameter bagi menentukan keupayaan jenis-jenis imej tersebut. Parameter-parameter yang digunakan adalah saiz fail, paras intensiti warna, data integriti, dan masa perlaksanaan. Semua parameter tersebut akan dikaji dengan menggunakan alatan yang dibangunkan khusus untuk kajian yang dipanggil *StegaNo*. Hasil kajian mencadangkan imej dari jenis 'BMP' adalah lebih sesuai dijadikan sebagai mesej hadapan berbanding imej dari jenis 'JPEG'.

Kata kunci: mesej hadapan, lossless, lossy, StegaNo, BMP, JPEG.

ACKNOWLEDGEMENT

In The Name of Allah, The Most Gracious and The Most Merciful,

Alhamdulillah, Praised to the Almighty *Allah* for His guidance and blessing, I am able to complete this final year project. It is a great pleasure for me to acknowledge the following list of individuals and organization for their contribution and continues support in completing this research especially to the Management of Northern University of Malaysia for the great facilities and resources provided,

My Supervisor, *Tuan Haji Roshidi bin Haji Din*, for his guidance and support in assisting me to conduct this research study and as well as completing the thesis.

The lecturers of Northern University of Malaysia, their assistance and continues supervise contributed throughout the session of MSc IT,

My friends and fellow colleagues for their support in building the application,

Special dedication for my beloved wife, *Norazizah binti Hamid* and my children, *Hamzi* and *Haiezad* and also to all my family members for their support and unconditional patience during completing this research study.

HANIZAN SHAKER BIN HUSSAIN
Faculty of Information Technology
Universiti Utara Malaysia
March, 2005

TABLE OF CONTENTS

PERMISSION TO USE i

ABSTRACT ii

ABSTRAK iii

ACKNOWLEDGEMENT iv

TABLE OF CONTENTS v

LIST OF TABLES vii

LIST OF FIGURES viii

CHAPTER ONE 1

INTRODUCTION 1

1.1 Background and Motivation of the Study 1

1.2 The Problem Statement 8

1.3 The Objectives of the Study 10

1.4 The Scope of the Study 10

1.5 Assumptions 12

1.6 The Significances of the Study 13

1.7 Structure of the Chapters 14

CHAPTER TWO 15

LITERATURE REVIEW 15

CHAPTER THREE 19

RESEARCH METHODOLOGY 19

3.1 Preliminary Study of Image Steganography 20

3.2 Designing Algorithm 20

3.2.1 Steganography Tools 20

3.2.2 Algorithm Description 22

3.3 Developing Prototype 23

3.4 Testing 25

3.4.1 The Size of Files 25

3.4.2 The Color Intensity Level 26

3.4.3 The Data Integrity Level 27

3.4.4 The Time Execution 28

3.5 Result and Discussion 29

CHAPTER FOUR 30

DATA ANALYSIS 30

4.1 The Size of Files 30

4.2 The Color Intensity Level 36

4.3 The Data Integrity 40

4.4 The Execution Time 43

CHAPTER FIVE 45

RESULTS 45

CHAPTER SIX 48

CONCLUSIONS AND RECOMMENDATIONS 48

REFERENCES 50

APPENDIXES 53

APPENDIX A 54

APPENDIX B 66

APPENDIX C 71

APPENDIX D 73

LIST OF TABLES

Table 3.1: The Popular Steganography Tools 21
Table 4.1: The Detail of Image Information for *globe.bmp* 32
Table 4.2: The Detail of Image Information for *lab.jpg* 35
Table 4.3: The Time Consumption and the Structure of Text Files 42
Table 4.4: The Time Consumption to Embed and Extract Messages 44
Table 5.1: The Image Information of *globe.bmp* and *lab.jpg* files 45
Table 5.2: The Values of Mean and Median of *globe.bmp* and *lab.jpg* files 46
Table 5.3: The Time Consumption and the Structure of Text Files 46

LIST OF FIGURES

Figure 1.1: The Stego Application Scenario 6

Figure 3.1: The Research Methodology Steps 19

Figure 3.2: An Information-Theoretic Model 23

Figure 3.3: The Interface of *StegaNo* 24

Figure 3.4: *.txt* File in a Different Size of Files 28

Figure 3.5: The Layout of the Tables 29

Figure 4.1: The Information of BMP File before Embedding Process 31

Figure 4.2: The Image Information for Embedded Files 32

Figure 4.3: The Information of JPEG File before Embedding Process 33

Figure 4.4: The Image Information for Embedded Files 34

Figure 4.5: The Color Histogram of BMP Image 36

Figure 4.6: The Color Histogram of BMP Image after Embedded 37

Figure 4.7: The Color Histogram of JPEG Image 38

Figure 4.8: The Color Histogram of JPEG Image after Embedded 39

Figure 4.9: Reversing Process for *globe.bmp* 40

Figure 4.10: Reversing Process for *lab.jpg* 41

Figure 4.11: The Output from Word Count by Using *globe.bmp* 41

Figure 4.12: The Output from Word Count by Using *lab.jpg* 42

Figure 4.13: The Progress Bar and the Time Box for Embedding Process 43

CHAPTER ONE

INTRODUCTION

1.1 Background and Motivation of the Study

Cryptography is a science of writing in secret codes, addresses all of the elements necessary for secure communication over an insecure channel, namely privacy, confidentiality, key exchange, authentication, and non-repudiation. But cryptography does not always provide safe communication.

Consider an environment where the very use of encrypted messages causes suspicion. For those who are looking for encrypted messages, they can easily find them. Consider the following text file below; what it would be beside encrypted files?

```
qANQR1DBwU4D/TlT68XXuiUQCADfj2o4b4aFYBcWumA7hR1Wvz9rbv2
BR6WbEUsyZBIEFtjyqCd96qF38sp9IQiJIKlNaZfx2GLRWikPZwchUX
xB+AA5+lqsG/ELBvRac9XefaYpbbAZ6z6LkOQ+eE0XASe7aEEPfdxvZ
ZT37dVyiyxuBBRYNLN8Bphdr2zvz/9Ak4/OLnLiJRk05/2UNE5Z0a+3
lcvITMmfGajvRhkXqocavPOKiin3hv7+Vx88uLLem2/fQHZhGcQvkqZ
```

The contents of the thesis is for internal user only

REFERENCES

Anderson, R. J., & Petitcolas F. A. (1998). On the limit of Steganography. IEEE *Journal of Selected Areas in Communications*, 16(4), 474-481.

Bauer, F. L. (2002). Decrypted secrets: Methods and maxims of Cryptology, 3rd ed. Springer-Verlag, New York.

Bender, W., Grhul, D., Morimoto, N., & Lu, A. (1996). Techniques for Data Hiding. *IBM Systems Journal*, 35, 3-4.

Chen, L. & Dey, S. (2001). Self-Test Methodology. Retrieved February 11, 2005, from http://www.ece.ucsd.edu/

Cachin, C. (1998). An information-theoretic model for steganography. *Information and Computation*, 192(1),41-56.

Davidson, I., Paul, G., & Ravi, S. S. (2004). Steganography using spatially interesting pixels. *Lecture Notes in Computer Science*, 2137, 289–302.

Fixmar, R. (2001). Terrorists and Steganography. *Zdnet News*. Retrieved September 23, 2001, from http://zdnet.com.com/2100-1107-530751.html

Hanna, S. (2004). Security through obsecurity: Steganography. Retrieved January 10, 2005, from http://www.vividmachines.com/Stos.doc

Holmes, P. D. (2002). Introduction to Digital Image Steganography. Retrieved january 28, 2005 from http://www.giac.org/practical/David_P_Holmes_GSEC.doc

Johnson, N. F. (1998). Steganography: seeing the unseen. *IEEE Computer* , 26-34.

Johnson, N. F. ,& Jajodia, S.(1998). Steaganalysis of images created using current Steganography software. *Lecture Notes in Computer Science*,1525. Retrieved December 12, 2004 from, http://link.springer.de/link/service/series/0558/papers/1525/15250273.pdf

Kessler, G.C. (2004). An overview of Steganography for the Computer Forensics Examiner. *Forensic Science Communication*, 45-48.

Lin, E.T.,& Delp, E.J. (1999). A review of fragile image watermarks. Multimedia and Security Workshop in ACM Multimedia '99, Orlando, FL, USA.

Mollin, R.A. (2001). An introduction to Cryptography. Chapman Hall/CRC Press.

Mendall, R. (2000). Steganography-electronic spycraft. Earthweb networking and communications. Retrieved January 25, 2005 from, http://www.eartweb.com/article/010456_624101.00.html

New York Times. (2001). When a picture is worth a thousand secrets: The debate over online Steganography. Retrieved December 15, 2004, from http://www.nytime.com/

Petitcolas, F. A. (2000). Watermarking Schemes Evaluation. Retrieved November 20, 2004. from http://www.petitcolas.net/fabien/publications/ieeespm00evalution.doc

Petitcolas, F. A., Anderson, R. J. & Kuhn, M. G. (1999). Information Hiding – A Survey, *IEEE Computers*, 87(7), 1062-1078.

(*Steganography Thumbprinting*, 1998). Steganography Thumbprinting. *Phrack Magazine*. 8, 52.

Sellars, D. (1999).Introduction to Steganography . Retrieved February 5, 2005, from http://www.cs.uct.ac.za/courses/CS400W/NIS/papers99/dsellers/stego.html

Satyanarayanan, M. (1981). A study of files sizes and functional lifetimes. *Symposium on Operating System Principle,* 96-108.

Wang, H., & Wang, S. (2004). Cyber warfare: Steganography vs. Steganalysis. *Communications of the ACM*, 47(10), 76-82.