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


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 Rosidi 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, Noraziah 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
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.3 Developing Prototype</td>
<td>23</td>
</tr>
<tr>
<td>3.4 Testing</td>
<td>25</td>
</tr>
<tr>
<td>3.4.1 The Size of Files</td>
<td>25</td>
</tr>
<tr>
<td>3.4.2 The Color Intensity Level</td>
<td>26</td>
</tr>
<tr>
<td>3.4.3 The Data Integrity Level</td>
<td>27</td>
</tr>
<tr>
<td>3.4.4 The Time Execution</td>
<td>28</td>
</tr>
<tr>
<td>3.5 Result and Discussion</td>
<td>29</td>
</tr>
<tr>
<td>CHAPTER FOUR</td>
<td>30</td>
</tr>
<tr>
<td>DATA ANALYSIS</td>
<td>30</td>
</tr>
<tr>
<td>4.1 The Size of Files</td>
<td>30</td>
</tr>
<tr>
<td>4.2 The Color Intensity Level</td>
<td>36</td>
</tr>
<tr>
<td>4.3 The Data Integrity</td>
<td>40</td>
</tr>
<tr>
<td>4.4 The Execution Time</td>
<td>43</td>
</tr>
<tr>
<td>CHAPTER FIVE</td>
<td>45</td>
</tr>
<tr>
<td>RESULTS</td>
<td>45</td>
</tr>
<tr>
<td>CHAPTER SIX</td>
<td>48</td>
</tr>
<tr>
<td>CONCLUSIONS AND RECOMMENDATIONS</td>
<td>48</td>
</tr>
<tr>
<td>REFERENCES</td>
<td>50</td>
</tr>
<tr>
<td>APPENDIXES</td>
<td>53</td>
</tr>
<tr>
<td>APPENDIX A</td>
<td>54</td>
</tr>
<tr>
<td>APPENDIX B</td>
<td>66</td>
</tr>
<tr>
<td>APPENDIX C</td>
<td>71</td>
</tr>
<tr>
<td>APPENDIX D</td>
<td>73</td>
</tr>
</tbody>
</table>
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
BR6wbEUsyZBIEFtjyqC9d96qF38sp9IqiJIK1NaZfx2GLRw1kPZwhUX
xB+AA5-lqsG/ELBvRac9XefaYpbbAZ6z6Lk0Q+eE0XASe7aEEPfdxvZ
ZT37dVyiyxuBBRYNln88phdr2zvz/9Ak4/OLnLiJrk05/2UNE5Z0a+3
1cvITMnfGajvRhkXqocavPOKiinn3hv7+Vx88uLLem2/fQH2hGcQvkqZ
```
The contents of the thesis is for internal user only
REFERENCES


