



INFORMATION HIDING IN DIGITAL IMAGES

A Thesis Submitted to the Department of Scientific Computing, Faculty
of Computer and Information Sciences, Ain Shams University, in the
Partial Fulfillment of the Requirements for the Master Degree of
Computer and Information Sciences

By:

Amal Said Mohammed Khalifa

*B.Sc. Degree in Computer and Information Sciences (2000)
Demonstrator at Scientific Computing Department,
Faculty of Computer and Information Sciences,
Ain Shams University.*

Supervised By:

Prof. Dr. Mohammed Fahmy Tolba

*Professor at Scientific Computing Department,
Faculty of Computer and Information Sciences,
Vice president for education and student affairs
Ain Shams University.*

Prof. Dr. Mohammed Al-Said Ghoniemy

*Professor at Computer Systems Department,
Vice dean for postgraduate studies and research affairs,
Faculty of Computer and Information Sciences,
Ain Shams University.*

Dr. Eng. Ismail Abdul-Hameed Taha

*Teacher at Military Technical College,
Cairo, Egypt.*

October 2004

ACKNOWLEDGMENTS

I would like to begin by expressing my gratitude to Prof. Dr. Mohammed Said Abd-el Wahab, the dean of the faculty, who provides me and my colleagues a continuous support, time, resources, and encouragement to help us to attain our research goals.

Additionally, I would like to thank my supervisor Prof. Dr. Mohammed Fahmy Tolba for his valuable insight and guidance throughout the period of research. I would also give my grateful thanks to my supervisors Prof. Dr. Mohammed Al-Said Ghoniemy, and Dr. Ismail Taha for their help, care, and encouragement.

I wish also to acknowledge Dr. Yeuan-Kuen Lee; assistant professor at the department of Computer Science and Information Engineering in Ming Chuan University in Taiwan, for his assistance during the evaluation period of my work. He sent me a running program based upon the algorithms he developed along with the image he used for testing and that was a great help.

A big thank-you to my husband for his support and toleration. Also I want to thank my sisters for taking care of my little noisy son, it was really a big help. Finally, and most I would like to thank my parents, who dedicated their lifetime raising me to who I am today. Without their constant sacrifice, I wouldn't have come so far.

Table of Contents

Abstract	v
List of Figures	vii
List of Tables	x
 Chapter 1 Introduction	 1
1.1 Problem Motivation	2
1.2 Objectives	3
1.3 Thesis Organization	4
 Chapter 2 Principles of Steganography	 6
2.1 Introduction	7
2.2 History of Steganography.....	9
2.2.1 Ancient Times	9
2.2.2 Middle Ages	10
2.2.3 Modern Times	12
2.3 Applications	13
2.4 Used Terminology	16
2.5 Classification of Information Hiding Problems.....	18
2.6 A Framework for Steganographic Algorithms.....	22
2.7 Constraints and Practical Requirrments...	26
2.8 Introduction to Steganalysis.....	27

Chapter 3	Survey on Steganographic Techniques.....	30
3.1	Data Hiding in Still Images	32
3.1.1	High Bit-rate Data Hiding.....	32
3.1.2	Low Bit-rate Data Hiding.....	35
3.1.3	Performance Evaluation.....	37
3.2	Data Hiding in Documents.....	38
3.3	Data Hiding in Audio Files	43
3.4	Data Hiding in Video	49
3.5	Data Hiding in File Systems	51
Chapter 4	A Present Colored LSB Algorithm	52
4.1	Introduction	53
4.2	Digital Image Representation.....	54
4.3	Preliminary Definitions.....	57
4.4	Least Significant Bit Substitution.....	58
4.5	Performance Analysis.....	68
4.6	Summary	78
Chapter 5	Proposed Blind Wavelet-Based Steganography	80
5.1	Introduction.....	81
5.2	Wavelets.....	81
5.3	Preliminary Definitions.....	86
5.4	Applying LSB in Wavelet Domain.....	87
5.4.1	Performance Analysis	97
5.4.2	Summary and Discussion	106
5.5	Embedding in Reversible Wavelets.....	107
5.5.1	Performance Analysis	115
5.5.2	Summary and Discussion.....	121

5.6	Summary	122
Chapter 6	Proposed Cover-Screw Wavelet-Based Steganography	123
6.1	Introduction.....	124
6.2	Casting Normalized Coefficients	124
6.1.1	Performance Analysis	131
6.1.2	Summary and Discussion	135
6.2	Using Wavelet-Based Fusion.....	136
6.2.1	Performance Analysis	143
6.2.2	Summary and Discussion	148
6.3	Summary.....	149
6.4	General Performance Evaluation.....	150
Chapter 7	Conclusions & Future Work	157
7.1	Conclusions.....	158
7.2	Future Work.....	160
	Bibliography	161
	Arabic Summary	1

Abstract

Humans are continuously attempting to find new and efficient ways to communicate secretly. A common solution to this problem is to use encryption in order to obscure the information contents of the message. However, we can think of steganography as a complementary solution. Steganographic techniques hide one piece of information inside another cover data so that they appear as a single entity.

The most simple and straightforward steganography scheme is the Least Significant Bit Substitution(LSB), where the message bit-stream is embedded into the least significant bits of the image pixels. In this thesis, we will introduce some wavelet-based techniques for modern steganography in digital imagery. The proposed techniques promote security, maximization of payload, high imperceptibility, as well as message error free recovery.

Actually, we have implemented four algorithms for embedding a message into the wavelet transform of true-colored images. Each one of them introduces a different idea and hence provides a certain advantage over the others. The first algorithm (*WLTCodedBinHide*) applies the standard technique of LSB on wavelet coefficients of the cover image. It also proposes using linear block codes in order to detect and possibly correct the truncation errors that may result from the floating point representation of the wavelet coefficients.

The second scheme (*IntWLTBinHide*) exploits the idea of reversible wavelets to store message bits directly in the LSBs of the integer coefficients. However, this requires applying a preprocessing step on the cover image to adjust the saturated pixel components in order to guarantee that the embedded message will be recovered correctly.

The next algorithm (*WLTCastBinHide*) uses the idea of casting message bits onto normalized cover coefficient using an embedding strength parameter. The extraction process, on the other hand, involves retrieving the message bit-stream by comparing the DWT coefficients of original image with the corresponding coefficients of the stego-image to decide upon the value of the embedded bit.

The last algorithm (*WLTFusedHide*) is based on merging the wavelet decomposition of the normalized cover image and the normalized secret image into a single fused result using an embedding strength factor (α). The algorithm also applies an adjustment operation on the normalized cover pixels before the embedding process takes place in order to guarantee that the embedded coefficients would not go out of range and hence the message will be recovered with acceptable accuracy even with a small value of α .

Experimental results showed the *IntWLTBinHide* provided approximately the same capacity as the most recent spatial domain (LSB-based) hiding schemes. However, it achieved a better invisibility performance. In addition, the *WLTFusedHide* achieved the best invisibility performance over all the presented algorithms, while it can embed a gray-scale image that is three times the cover image size. Generally, we can say that the proposed algorithms achieved our primary goals by providing high payload, high invisibility, and good signal recovery.

List of Figures

<u>Figure</u>		<u>Page</u>
Figure 2.1	Schematic description of Steganographic channel	9
Figure 2.2	The Core of Steganography.....	16
Figure 2.3	Steganography Processes	18
Figure 2.4	A classification of Information Hiding Techniques.....	19
Figure 2.5	A General Steganographic Model.....	24
Figure 3.1	Embedding watermark in frequency domain.....	34
Figure 3.2	An example of line shift coding	40
Figure 3.3	An example of word shifting encoding	41
Figure 3.4	The LSB scheme for data hiding in Audio Files	45
Figure 4.1	The Color Planes of a true color Image	55
Figure 4.2	The embedding process of the LSB algorithm...	58
Figure 4.3	Viewing the pixel as a point in three-dimensional RGB color space.....	73
Figure 4.4	The visual quality measured for the Lena image after Gaussian noise addition.....	75
Figure 4.5	The invisibility performance for the LSB algorithm measured in PSNR.....	77
Figure 4.6	The invisibility performance for the LSB algorithm measured in RMSE.....	77

Figure 5.1	One level of wavelet decomposition and reconstruction.....	84
Figure 5.2	A Two dimensional wavelet Transform	85
Figure 5.3	2-level wavelet decomposition of an image....	86
Figure 5.4	The process of block error control coding	87
Figure 5.5	Block diagram for Binary Embedding in Wavelet coefficients of a True Colored Image using error control coding	90
Figure 5.6	The visual quality of the embedded image using <i>WLT coded Bin Hide</i> for different wavelet families	102
Figure 5.7	The visual quality of the embedded image using <i>WLT coded Bin Hide</i> for different wavelet sub-bands	102
Figure 5.8	The invisibility performance for the <i>WLT coded Bin Hide</i> algorithm measured in PSNR.....	105
Figure 5.9	The invisibility performance for the <i>WLT coded Bin Hide</i> algorithm measured in RMSE.....	105
Figure 5.10	Block diagram for a steganography model based on binary embedding in integer wavelet coefficients of a true colored image...	110
Figure 5.11	The invisibility performance for the <i>IntWLT Bin Hide</i> algorithm measured in PSNR.....	120
Figure 5.12	The invisibility performance for the <i>IntWLT Bin Hide</i> algorithm measured in RMSE.....	120

Figure 6.1	Block diagram for a steganography model based on Casting Wavelet Coefficients of a True Colored Image.....	126
Figure 6.2	The invisibility performance for the <i>WLTCastBinHide</i> algorithm measured in PSNR.....	134
Figure 6.3	The invisibility performance for the <i>WLTCastBinHide</i> algorithm measured in RMSE.....	134
Figure 6.4	Block diagram for a steganography model based on Wavelet fusion between a true colored cover image and another secret image	138
Figure 6.5	The invisibility performance for the <i>WLTFusedHide</i> algorithm measured in PSNR.....	147
Figure 6.6	The invisibility performance for the <i>WLTFusedHide</i> algorithm measured in RMSE.....	147
Figure 6.7	The invisibility comparison for the proposed wavelet-based steganography algorithms.....	151
Figure 6.8	The maximum hiding capacity offered by the proposed wavelet-based steganography algorithms.....	151
Figure 6.9	The retrieval rate computed for the proposed wavelet-based steganography algorithms.....	152
Figure 6.10	Original test images used in the general performance comparison.....	154

List of Tables

<u>Table</u>		<u>Page</u>
Table 2.1	Number of publications on Steganography during the past few years	19
Table 3.1	Commonly used pixel-based distortion metrics...	38
Table 4.1	An algorithm for the basic embedding process of LSB substitution.....	59
Table 4.2	An algorithm for the basic extraction process of LSB substitution	60
Table 4.3	An algorithm for computing pseudorandom permutation.....	62
Table 4.4	The algorithm for general LSB Embedding for true-color images	63
Table 4.5	The algorithm for general LSB Extraction for true-color images	65
Table 4.6	The effect of parameter N on an image embedded using <i>LSBHide</i>	71
Table 4.7	The effect of the message size on the visual quality of Lena image embedded using <i>LSBHide</i>	76

Table 5.1	Algorithm for binary embedding in wavelet coefficients of a true-color image using error control coding	92
Table 5.2	Algorithm for binary extraction from wavelet coefficients of a true colored image using error control coding	94
Table 5.3	The effect of the parameter N on the visual quality of an image embedded using <i>WLTCodedBinHide</i>	100
Table 5.4	The effect of the message size on the visual quality of an image embedded using <i>WLTCodedBinHide</i>	104
Table 5.5	Algorithm for Binary Embedding in Integer Wavelet coefficients of a True Colored Image.....	111
Table 5.6	Algorithm for Binary Extraction from Integer Wavelet coefficients of a True Colored Image.....	113
Table 5.7	The effect of the parameter N on the visual quality of an image embedded using <i>IntWLTBinHide</i>	117
Table 5.8	The effect of the message size on the visual quality of an image embedded using <i>IntWLTBinHide</i>	119

Table 6.1	Algorithm for Casting Binary Message in Wavelet Domain of a True Colored Image.....	127
Table 6.2	Algorithm for Extracting Casted Binary Message from Wavelet Domain of a True Colored Image	129
Table 6.3	The effect of the message size on the visual quality of an image embedded using <i>WLTCastBinHide</i>	133
Table 6.4	Algorithm for embedding a gray scale Message in a True Colored Image using Wavelet-Based fusion	139
Table 6.5	Algorithm for extracting a gray scale message from a true colored image using wavelet-based fusion	141
Table 6.6	The effect of the message size on the visual quality of an image embedded using <i>WLTFusedHide</i>	146
Table 6.7	A comparison between the LSB-based methods and the proposed wavelet-based algorithms for gray-scale images.....	155
Table 6.8	Capacity comparison between the LSB-based methods and the proposed wavelet-based algorithms for gray-scale images.....	156

Chapter One

Introduction

1.1 Problem Motivation

Humans are continuously attempting to find new and efficient ways to communicate. Historical examples include cave drawings, fire, and drums. Advances in civilization and technology introduced new ways including written language, telegraph, radio/television, and most recently the Internet and the electronic mail. As more and more communications are conducted electronically, new needs, issues, and opportunities are born.

When communication takes place, it may be preferred to keep the message *secret*. A common solution to this problem is to use encryption in order to obscure the information contents of the message. Although the encryption is still used in many fields, we can think of steganography as a one more tool to communicate in a hidden manner. While encryption masks the mean of communication, steganographic techniques hide the communication existence by means of other data usually referred to as *cover data*. In today's electronic world, A multitude of multimedia objects can serve as potential covers.

Privacy is not the only motivation of steganography. By embedding one piece of information inside another, they become a single entity, and so they should appear. This means that the embedded data should not affect the over all integrity of the cover data.

1.2 Objectives

Much of the recent work in data hiding is the area of *watermarking*, motivated by the desire for the copyright protection of multimedia on the internet. Thus far, less attention has been given to another type of data hiding: steganography. The objective of steganography is to imperceptibly embed significant amount of information into some cover media.

In this thesis, we will address the subject of modern steganography, and introduce some techniques for data hiding that uses digital imagery as a cover. The proposed techniques promote maximization of payload, allowing error free recovery of the embedded message, as well as achieving high imperceptibility. The research also encompasses a detailed performance measurement of the proposed techniques using some existing metrics.

We can summarize our objectives as follows:

1. Survey on the principal information hiding techniques & tools.
2. Implementation of some wavelet-based algorithms for hiding information in container image files.
3. Performance analysis of the proposed algorithms in terms of computational complexity, payload, imperceptibility, as well as recovery rate.