



Faculty of Information and Communication Technology

**DIGITAL IMAGE STEGANOGRAPHY
BASED ON INTEGER HAAR WAVELET TRANSFORM
AND COEFFICIENT DIFFERENCE**

Prajanto Wahyu Adi

Master of Computer Science (Software Engineering and Intelligence)

2014

BORANG PENGESAHAN STATUS THESIS*

JUDUL : DIGITAL IMAGE STEGANOGRAPHY BASED ON INTEGER
HAAR WAVELET TRANSFORM AND COEFFICIENT
DIFFERENCE
SESI PENGAJIAN : 2013 - 2014
Saya : PRAJANTO WAHYU ADI

(HURUF BESAR)

Mengaku membenarkan tesis Sarjana 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

(TANDA TANGAN PENULIS)

(TANDA TANGAN PENYELIA)

Alamat Tetap: _____

Dr. Nor Azman bin Abu

Nama Penyelia

Tarikh: _____

Tarikh: _____

CATATAN : * Tesis dimaksudkan sebagai Laporan Akhir Projek Sarjana (PS).

** Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa.

**DIGITAL IMAGE STEGANOGRAPHY
BASED ON INTEGER HAAR WAVELET TRANSFORM
AND COEFFICIENT DIFFERENCE**

PRAJANTO WAHYU ADI

**A thesis submitted
in fulfillment of the requirements for the degree of
Master of Computer Science (Software Engineering and Intelligence)**

Faculty of Information and Communication Technology

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2014

DECLARATION

I declare that this master project entitled “*Digital Image Steganography Based on Integer Haar Wavelet Transform and Coefficient Difference*” is the result of my own research except as cited in the references. This master project has not been accepted for any degree and is not currently submitted in candidature of any other degree.

Signature :

Name : Prajanto Wahyu Adi

Date : January 2014

APPROVAL

I hereby declare that I have read through this project report and in my opinion this project report is sufficient in term of scope and quality for the awarded of the degree of Master of Computer Science (Software Engineering and Intelligence).

Signature :

Name : Dr. Nor Azman bin Abu

Date : January 2014

DEDICATION

Special thanks I dedicated to my family who giving me full support and motivation throughout my project. To my respectful supervisor, Dr. Nor Azman bin Abu who giving me advice and support so that I can finish my this project successfully. To my friends who fought together and always encourage each other.

ACKNOWLEDGEMENT

Alhamdulillah, all praises to Allah for the strength and the blessing in completing this project entitled: *Digital Image Steganography Based on Integer Haar Wavelet Transform and Coefficient Difference*.

Special appreciation goes to my honorable supervisor, Dr. Nor Azman bin Abu, for his invaluable help of constructive comments and suggestions throughout the experimental and project works have contributed to the success of this research.

I also appreciate to Prof. Dr. Mohd. Khanapi bin Abd. Ghani, Dean of Faculty of Information and Communication Technology, and Prof. Dr. Nanna Suryana Herman, Director of International Office, Universiti Teknikal Malaysia Melaka, for their support and help towards my postgraduate studies.

I am especially grateful to University of Dian Nuswantoro (UDINUS) for the opportunity given to me to continue my study and their kindness in giving financial and moral support during my study here. Special thanks also go to Dr. Ir. Edi Noersasongko, Dr. Abdul Syukur, Madam Tri Kusni Ingsih, and others for their support.

Sincere thanks to my best comrades, Andita, Danang, Egia, and Ramadhan. A warm appreciation I addressed to Mr. Affandy, Mr. Fahmi, Mr. Sriyanto, Fatma, Hayati, Herdi, Sidiq, Windi, PPI UTeM, and to all colleagues and others who have provided assistance and moral support during this study.

Finally, the deepest gratitude and sincere love goes to my beloved parents, Mr. Gunawan Witjaksana and Mrs. Etik Waliningsih, also my beloved brothers Pramudo Wicaksono and his Wife Anita Rizky Wijayanti, Probo Kusumo and to my beloved sisters, Pramudi Arsiwi and Probosari for their endless love, prayer and encouragement. To those who had indirectly contributed to this research, I gave you my greatest thanks for your support.

ABSTRACT

The development of digital information led to the demand for information security technology that protects the confidentiality of information. Digital steganography is one of such technology that able to protect the information from illegal interception due to its capability to hide the existence of the information without attracting the eavesdropper's attention. Among digital media, digital image is the most widely used media for steganography. Discrete Cosine Transform (DCT) is a well-known technique in digital image steganography, but the block calculation of DCT may pose artifact on the images. The disadvantages of DCT can be eliminating by the Discrete Wavelet Transform (DWT) which is more compatible with the Human Visual System (HVS). However the floating point of DWT can causes loss of information. On the other hand, Integer Wavelet Transform (IWT) is represented in finite precision numbers, which can avoid the problem of floating point precision of DWT. In this study, the messages are embedded on the wavelet coefficients of 1-level Integer Haar Wavelet Transform (IHWT) using Coefficient Difference scheme that adopted from Pixel Value Differencing (PVD). The messages are embedded on the difference value of two adjacent wavelet coefficients. Peak Signal to Noise Ration (PSNR) and Structural Similarity (SSIM) are used to measure the quality of stego image. The result shows that the proposed method has outperformed the existing method that employ IHWT and Pixel Mapping Method (PMM) in term of capacity vs. imperceptibility, as well as the maximum capacity. This is due to the high degree of Coefficient Difference that can tolerate larger modification of wavelet coefficients. Moreover, the Coefficient Difference can be applied on all coefficients instead of either significant or insignificant coefficient. These lead to the both high capacity and imperceptibility of digital image steganography system.

ABSTRAK

Pembangunan maklumat digital membawa kepada permintaan untuk keselamatan teknologi maklumat yang melindungi kerahsiaan maklumat . Steganografi Digital adalah salah satu teknologi itu yang dapat melindungi maklumat daripada pemintasan haram kerana keupayaan untuk menyembunyikan kewujudan maklumat tanpa menarik perhatian yang mencuri password ini itu. Antara media digital, imej digital adalah media yang paling banyak digunakan untuk steganografi. *Discrete Cosine Transform* (DCT) adalah teknik terkenal dalam imej steganografi digital, tetapi pengiraan blok DCT boleh menimbulkan artifak pada imej-imej . Kelemahan DCT boleh dihapuskan oleh *Discrete Wavelet Transform* (DWT) yang lebih sesuai dengan *Human Visual System* (HVS), bagaimanapun titik terapan DWT boleh menyebabkan kehilangan maklumat. Sebaliknya, *Integer Wavelet Transform* (IWT) diwakili dalam jumlah ketepatan yang terbatas , yang boleh mengelakkan masalah terapan titik ketepatan DWT. Dalam kajian ini , mesej yang sudah ada pada pekali wavelet 1-tahap *Integer Wavelet Transform* (IHWT) menggunakan skim *Coefficient Difference* yang diambil daripada *Pixel Value Differencing* (PVD). Mesej yang sudah ada pada nilai perbezaan dua pekali wavelet bersebelahan. *Peak Signal to Noise Ratio* (PSNR) dan *Structural Similarity* (SSIM) digunakan untuk mengukur kualiti stego imej. Hasilnya menunjukkan bahawa kaedah yang dicadangkan telah mengatasi kaedah yang menguji IHWT dan *Pixel Mapping Method* (PMM) dari segi keupayaan vs imperceptibility , dan juga kapasiti maksimum. Ini adalah kerana tahap yang tinggi Pekali Perbezaan yang boleh bertolak ansur dengan pengubahsuaian yang lebih besar daripada pekali ombak kecil . Lebih-lebih lagi, *Coefficient Difference* yang boleh digunakan ke atas semua pekali bukannya pekali sama ada penting atau tidak penting. Ini membawa kepada keupayaan kedua-dua tinggi dan imperceptibility imej digital sistem steganografi.

TABLE OF CONTENT

	PAGE
DECLARATION	ii
APPROVAL	iii
DEDICATION	iv
ACKNOWLEDGEMENT	v
ABSTRACT	vi
ABSTRAK	vii
LIST OF TABLE	xii
LIST OF FIGURE	xiv
LIST OF ABBREVIATION	xxi
CHAPTER 1 INTRODUCTION	1
1.1 Introduction	1
1.2 Background of Study	2
1.3 Problem Statement	4
1.4 Research Question	4
1.5 Research Objective	4
1.6 Scope of Study	4
1.7 Significant of Study	5
1.8 Thesis Outline	5
1.9 Chapter Summary	6

CHAPTER 2 LITERATURE REVIEW	7
2.1 Introduction	7
2.2 Information Hiding	7
2.2.1 Cryptography and Steganography	8
2.2.2 Steganography and Watermarking	8
2.3 Digital Images	8
2.4 Steganography	9
2.5 Type of Steganography	10
2.5.1 Based on Domain of Steganography	10
2.5.2 Based on Recoverable of Media	11
2.5.3 Based on Extraction Scheme	11
2.6 Steganography Methods	11
2.6.1 Steganography in Spatial Domain	12
2.6.2 Steganography in Frequency Domain	16
2.7 Performance Measurement	30
2.7.1 Mean Squared Error (MSE) and Peak Signal to Noise Ratio (PSNR)	30
2.7.2 Structural Similarity (SSIM)	31
2.8 Chapter Summary	33
CHAPTER 3 RESEARCH METHODOLOGY	35
3.1 Introduction	35
3.2 Type of Research Method	35
3.3 Research Method	35
3.4 Proposed Model	37
3.4.1 Embedding Process	37
3.4.2 Extraction Process	41

3.5	Data Collection	42
3.6	Chapter Summary	42
	CHAPTER 4 EXPERIMENT AND RESULT	44
4.1	Introduction	44
4.2	Images and Message Used	44
4.2.1	Cover Image	44
4.2.2	Message	47
4.3	Determination of Threshold	48
4.3.1	Color Images Measurement	48
4.3.2	Grayscale Images Measurement	51
4.4	The Stego Images	56
4.4.1	Messages Encryption	56
4.4.2	The Embedding of Image Messages	57
4.4.3	The Extraction of Image Message	72
4.4.4	The Embedding and Extraction of Text Message	73
4.5	The Stego Image under JPEG2000 Compression	76
4.5.1	Message Embedding under JPEG 2000 Compression	77
4.5.2	The Extracted Message from Compressed Stego Image	80
4.6	Comparison with Existing Method	82
4.6.1	Image Quality	82
4.6.2	Maximum Capacity	83
4.7	Chapter Summary	84
	CHAPTER 5 CONCLUSION	86
5.1	Introduction	86
5.2	Research Background and Purpose of Study	86

5.3	Literature Review	87
5.4	Proposed Method	87
5.5	Experimental Result	88
5.6	Conclusion	89
5.7	Future Work	89
	REFERENCES	91

LIST OF TABLE

TABLE	TITLE	PAGE
Table 4.1	Capacity vs. Imperceptibility of Baboon	48
Table 4.2	Capacity vs. Imperceptibility of F16	49
Table 4.3	Capacity vs. Imperceptibility of House	49
Table 4.4	Capacity vs. Imperceptibility of Lena	50
Table 4.5	Capacity vs. Imperceptibility of Peppers	50
Table 4.6	Capacity vs. Imperceptibility of Sailboat	51
Table 4.7	Capacity vs. Imperceptibility of Aerial	52
Table 4.8	Capacity vs. Imperceptibility of Bridge	52
Table 4.9	Capacity vs. Imperceptibility of Couple	53
Table 4.10	Capacity vs. Imperceptibility of Elaine	53
Table 4.11	Capacity vs. Imperceptibility of Fishingboat	54
Table 4.12	Capacity vs. Imperceptibility of Truck	54
Table 4.13	Qualities of the Color Stego Images	64
Table 4.14	Qualities of the Grayscale Stego Images	71
Table 4.15	Qualities of Extracted ColorMessage	72
Table 4.16	Qualities of Extracted GrayMessage	72
Table 4.17	Qualities of Color Stego Images after Embedding Text Message	73

Table 4.18 Qualities of Grayscale Stego Images after Embedding Text Message	75
Table 4.19 Qualities of Extracted ColorMessage under JPEG2000 Compression	81
Table 4.20 Comparison of Imperceptibility	83
Table 4.21 Comparison of Maximum Capacity	83

LIST OF FIGURE

FIGURE	TITLE	PAGE
Figure 2.1	Hierarchical Structure of Information Hiding	7
Figure 2.2	Basic of Steganography in Digital Image	10
Figure 2.3	LSB substitutions method by altering up to 4 th LSB (Cheddad et al., 2010)	12
Figure 2.4	Non-overlapping block of two adjacent pixels via zigzag scanning.	13
Figure 2.5	Illustration of data embedding process	13
Figure 2.6	Embedding Process in Spread Spectrum Image Steganography	15
Figure 2.7	Extraction Process in Spread Spectrum Image Steganography	16
Figure 2.8	Luminance Quantization Table	18
Figure 2.9	Chrominance Quantization Table	18
Figure 2.10	General process of embedding in frequency domain	18
Figure 2.11	Two Dimensional Wavelet Decomposition	20
Figure 2.12	Discrete Wavelet Transformation of an Image	20
Figure 2.13	Image decomposition using 1-level of HWT	22
Figure 2.14	Decomposition of 512x512 Lena .bmp Image using 1-level HWT	23
Figure 2.15	Frequency Distribution Function of LL Band of Lena Image	24
Figure 2.16	Frequency Distribution of HL Band with 3Standard Deviation	25
Figure 2.17	Frequency Distribution of LH Band with 3Standard Deviation	26

Figure 2.18 Frequency Distribution of HH Band with 3Standard Deviation	27
Figure 2.19 Diagram of Structural Similarity (SSIM) measurement system	31
Figure 3.1 Research Method	36
Figure 3.2 Embedding Process	38
Figure 3.3 Extraction Process	41
Figure 4.1 Baboon.tiff	45
Figure 4.2 F16.tiff	45
Figure 4.3 House.tiff	45
Figure 4.4 Lena.tiff	45
Figure 4.5 Peppers.tiff	45
Figure 4.6 Sailboat.tiff	45
Figure 4.7 Aerial.tiff	46
Figure 4.8 Bridge.tiff	46
Figure 4.9 Couple.tiff	46
Figure 4.10 Elaine.tiff	46
Figure 4.11 Fishingboat.tiff	46
Figure 4.12 Truck.tiff	46
Figure 4.13 ColorMessage.bmp	47
Figure 4.14 GrayMessage.bmp	47
Figure 4.15 Text Message	47
Figure 4.16 Capacity vs. Imperceptibility of Baboon	48
Figure 4.17 Capacity vs. Imperceptibility of F16	49
Figure 4.18 Capacity vs. Imperceptibility of House	49
Figure 4.19 Capacity vs. Imperceptibility of Lena	50
Figure 4.20 Capacity vs. Imperceptibility of Peppers	50

Figure 4.21 Capacity vs. Imperceptibility of Sailboat	51
Figure 4.22 Capacity vs. Imperceptibility of Aerial	52
Figure 4.23 Capacity vs. Imperceptibility of Bridge	52
Figure 4.24 Capacity vs. Imperceptibility of Couple	53
Figure 4.25 Capacity vs. Imperceptibility of Elaine	53
Figure 4.26 Capacity vs. Imperceptibility of Fishingboat	54
Figure 4.27 Capacity vs. Imperceptibility of Truck	54
Figure 4.28 Capacity vs. Imperceptibility (SSIM) of Color Images	55
Figure 4.29 Capacity vs. Imperceptibility (SSIM) of Grayscale Images	56
Figure 4.30 Key for ColorMessage	57
Figure 4.31 Key for GrayMessage	57
Figure 4.32 Encrypted ColorMessage	57
Figure 4.33 Encrypted GrayMessage	57
Figure 4.34 Encrypted Text Message	57
Figure 4.35 Cover Baboon.tif	58
Figure 4.36 Stego Baboon.bmp (T=2)	58
Figure 4.37 Stego Baboon.bmp (T=3)	58
Figure 4.38 Enhanced Difference between Cover and Stego Baboon (T=2)	58
Figure 4.39 Enhanced Difference between Cover and Stego Baboon (T=3)	58
Figure 4.40 Cover F16.tif	59
Figure 4.41 Stego F16.bmp (T=2)	59
Figure 4.42 Stego F16.bmp (T=3)	59
Figure 4.43 Enhanced Difference between Cover and Stego F16 (T=2)	59
Figure 4.44 The Difference between Cover and Stego F16 (T=3)	59
Figure 4.45 Cover House.tif	60

Figure 4.46 Stego House .bmp (T=2)	60
Figure 4.47 Stego House .bmp (T=3)	60
Figure 4.48 Enhanced Difference between Cover and Stego House (T=2)	60
Figure 4.49 Enhanced Difference between Cover and Stego House (T=3)	60
Figure 4.50 Cover Lena .tiff	61
Figure 4.51 Stego Lena .bmp (T=2)	61
Figure 4.52 Stego Lena .bmp (T=3)	61
Figure 4.53 Enhanced Difference between Cover and Stego Lena (T=2)	61
Figure 4.54 Enhanced Difference between Cover and Stego Lena (T=3)	61
Figure 4.55 Cover Peppers .tiff	62
Figure 4.56 Stego Peppers .bmp (T=2)	62
Figure 4.57 Stego Peppers .bmp (T=3)	62
Figure 4.58 Enhanced Difference between Cover and Stego Peppers (T=2)	62
Figure 4.59 Enhanced Difference between Cover and Stego Peppers (T=3)	62
Figure 4.60 Cover Sailboat .tiff	63
Figure 4.61 Stego Sailboat .bmp (T=2)	63
Figure 4.62 Stego Sailboat .bmp (T=3)	63
Figure 4.63 The Difference between Cover and Stego Sailboat (T=2)	63
Figure 4.64 The Difference between Cover and Stego Sailboat (T=3)	63
Figure 4.65 Qualities of the Color Stego Images	64
Figure 4.66 Cover Aerial .tiff	65
Figure 4.67 Stego Aerial .bmp (T=2)	65
Figure 4.68 Stego Aerial .bmp (T=3)	65
Figure 4.69 Enhanced Difference between Cover and Stego Aerial (T=2)	65

Figure 4.70 Enhanced Difference between Cover and Stego Aerial (T=3)	65
Figure 4.71 Cover Bridge.tiff	66
Figure 4.72 Stego Bridge.bmp (T=2)	66
Figure 4.73 Stego Bridge.bmp (T=3)	66
Figure 4.74 Enhanced Difference between Cover and Stego Bridge (T=2)	66
Figure 4.75 Enhanced Difference between Cover and Stego Bridge (T=3)	66
Figure 4.76 Cover Couple.tiff	67
Figure 4.77 Stego Couple.bmp (T=2)	67
Figure 4.78 Stego Couple.bmp (T=3)	67
Figure 4.79 Enhanced Difference between Cover and Stego Couple (T=2)	67
Figure 4.80 Enhanced Difference between Cover and Stego Couple (T=3)	67
Figure 4.81 Cover Elaine.tiff	68
Figure 4.82 Stego Elaine.bmp (T=2)	68
Figure 4.83 Stego Elaine.bmp (T=3)	68
Figure 4.84 Enhanced Difference between Cover and Stego Elaine (T=2)	68
Figure 4.85 Enhanced Difference between Cover and Stego Elaine (T=3)	68
Figure 4.86 Cover Fishingboat.tiff	69
Figure 4.87 Stego Fishingboat.bmp (T=2)	69
Figure 4.88 Stego Fishingboat.bmp (T=3)	69
Figure 4.89 Enhanced Difference between Cover and Stego Fishingboat (T=2)	69
Figure 4.90 Enhanced Difference between Cover and Stego Fishingboat (T=3)	69
Figure 4.91 Cover Truck.tiff	70
Figure 4.92 Stego Truck.bmp (T=2)	70
Figure 4.93 Stego Truck.bmp (T=3)	70

Figure 4.94 Enhanced Difference between Cover and Stego Truck (T=2)	70
Figure 4.95 Enhanced Difference between Cover and Stego Truck (T=3)	70
Figure 4.96 Qualities of the Grayscale Stego Images	71
Figure 4.97 Extracted ColorMessage from Color Stego Images	73
Figure 4.98 Extracted GrayMessage from Grayscale Stego Images	73
Figure 4.99 Qualities of Color Stego Images after Embedding Text Message	74
Figure 4.100 Qualities of Grayscale Stego Images after Embedding Text Messages	75
Figure 4.101 Text Message is Extracted without Error	76
Figure 4.102 Cover Lena.tiff	77
Figure 4.103 Stego Lena.jp2 with 50% Compression Ratio (T=2)	78
Figure 4.104 Enhanced Difference of 50% Compressed Stego Lena.jp2 (T=2)	78
Figure 4.105 Stego Lena.jp2 with 25% Compression Ratio (T=2)	78
Figure 4.106 Enhanced Difference of 25% Compressed Stego Lena.jp2 (T=2)	78
Figure 4.107 Stego Lena.jp2 with 10% Compression Ratio (T=2)	78
Figure 4.108 Enhanced Difference of 10% Compressed Stego Lena.jp2 (T=2)	78
Figure 4.109 Stego Lena.jp2 with 50% Compression Ratio (T=3)	79
Figure 4.110 Enhanced Difference of 50% Compressed Stego Lena.jp2 (T=3)	79
Figure 4.111 Stego Lena.jp2 with 25% Compression Ratio (T=3)	79
Figure 4.112 Enhanced Difference of 25% Compressed Stego Lena.jp2 (T=3)	79
Figure 4.113 Stego Lena.jp2 with 10% Compression Ratio (T=3)	79
Figure 4.114 Enhanced Difference of 10% Compressed Stego Lena.jp2 (T=3)	79
Figure 4.115 Extracted ColorMessage from 50% Compressed Stego Lena (T=2)	80
Figure 4.116 Extracted ColorMessage from 50% Compressed Stego Lena (T=3)	80
Figure 4.117 Extracted ColorMessage from 25% Compressed Stego Lena (T=2)	80
Figure 4.118 Extracted ColorMessage from 25% Compressed Stego Lena (T=3)	80

Figure 4.119 Extracted ColorMessage from 10% Compressed Stego Lena (T=2)	80
Figure 4.120 Extracted ColorMessage from 10% Compressed Stego Lena (T=3)	80
Figure 4.121 Qualities of Extracted ColorMessage under JPEG2000 Compression.	81
Figure 4.122 Grayscale Lena .bmp	82
Figure 4.123 Comparison of Imperceptibility	83
Figure 4.124 Comparison of Maximum Capacity	84

LIST OF ABBREVIATION

DCT	-	Discrete Cosine Transform
DWT	-	Discrete Wavelet Transform
HVS	-	Human Visual System
HWT	-	Haar Wavelet Transform
IHWT	-	Integer Haar Wavelet Transform
IIHWT	-	Inverse Integer Haar Wavelet Transform
IWT	-	Integer Wavelet Transform
LSB	-	Least Significant Bit
MSE	-	Mean Squared Error
PSNR	-	Peak Signal to Noise Ratio
PMM	-	Pixel Mapping Method
PVD	-	Pixel Value Differencing
RMSE	-	Root Mean Squared Error
SSIM	-	Structure Similarity
SSIS	-	Spread Spectrum Image Steganography

CHAPTER 1

INTRODUCTION

1.1 Introduction

Along with the existence of internet technology and rapid growth in consumption of digital information in past decade cause attention in security issue such as digital right management, authenticity, and content security (Mali et al., 2012). Various cyber crimes such as forgery, modification, duplication, and interception have reached alarming level (Tsai et al., 2009).

To solve the problem of illicit interception, several techniques such as cryptography, and information hiding had been proposed (Yu et al., 2005). Cryptography is a known method for protecting the information by encrypt the message to become unreadable (Highland, 1997), but the unreadable message may attract the eavesdroppers' attention (Yu et al., 2005; Liao et al., 2011; Yang et al., 2011).

Information hiding has been widely used to protect the digital media contents (Lee et al., 2010), it plays an important role in information security (Luo et al., 2011). One of the branch of information hiding which aimed for secret communication is steganography (Petitcolas et al., 1999). Steganography conceal the existence of the message which prevent the attention of eavesdroppers (Artz, 2001; Wang and Wang, 2004). This makes steganography a good manner to communicate secret information (Yang et al., 2011).

Originally, steganography is the art and science of writing secret message inside the media, and transferring the media to the addressee in such way that only the intended