A NEW STEGANOGRAPHY TECHNIQUE USING MAGIC SQUARE MATRIX AND AFFINE CIPHER

WALEED S. HASAN AL-HASAN

UNIVERSITI TEKNOLOGI MALAYSIA

A NEW STEGANOGRAPHY TECHNIQUE USING MAGIC SQUARE MATRIX AND AFFINE CIPHER

WALEED S. HASAN AL-HASAN

A project report submitted in partial fulfilment of the
requirements for the award of the degree of
Master of Engineering (Electrical-Computer and Microelectronic system)

Faculty of Electrical Engineering
Universiti Teknologi Malaysia

June 2015

Dedicated to my beloved mother

To my beloved father

To my beloved brother and sister

To my beloved wife

To my angel (Melek)

I love you for every second in my life

ACKNOWLEDGEMENT

All praises are due to Allah the cherished, the Sustainer of the entire universe, praise be to him, he who taught man with a pen, what he knew not. I asked Allah Subhanahuwataalla to bestowed Peace and blessings upon His Messenger, Muhammad S.A.W, and all his family and companions.

I like to express my profound gratitude to my supervisor, Associate Professor Muhammad Mun'im A. Zabidi for his patience, advice, time sparing, useful comments, suggestion, correction, concern and interest in my understanding of what a research undertaking is, its development and write -up.

I would like to thank the staff of VeCAD Laboratory, and Faculty of Electrical Engineering, Universiti Teknologi Malaysia for their understanding.

ABSTRACT

Methods that provide effective protection of data have now become necessary due to the huge growth of multimedia applications on networks. Steganography is one of the most widespread approaches of protecting data. The challenge of steganographic methods is to create a rational balance between the quality of the file and the size of data that can be transferred. In addition, the robustness of the technique and security of the obscure data must be maintained. This thesis proposes a new steganography approach to fulfill requirements of steganography which are imperceptibility, payload and robustness. In this study, the color space of the image is first converted from RGB to YCbCr color space. Then, Cb or Cr channel selected to hide the secret data. The secret data is encrypted using the affine cipher to increase the security of data. The Magic Square Matrix is applied to embed the secret code onto the Cb or Cr component using ISB (Intermediates Significant Bits) approach. Finally, the robustness of the cover image is evaluated by applying Salt-and-Pepper noise. The results show that the new proposed method not only improves the security problem but proposed technique can withstand attacks.

ABSTRAK

Kaedah-kaedah yang memberikan perlindungan data kini menjadi kemestian kerana pertumbuhan pesat aplikasi multimedia dalam rangkaian. Steganografi merupakan salah satu pendekatan melindungi data yang paling meluas. Cabaran bagi kaedah steganografi adalah untuk mewujudkan keseimbangan yang rasional antara kualiti fail dan saiz data yang boleh dipindahkan. Selain itu, kemantapan teknik dan keselamatan data yang dilindungi mesti dikekalkan. Tesis ini mencadangkan satu pendekatan steganografi baharu bagi memenuhi keperluan steganografi iaitu tidak dapat dilihat, muat beban dan kemantapan. Dalam kajian ini, ruang warna imej mula-mula ditukarkan dari ruang warna RGB ke YCbCr. Kemudian, saluran Cb atau Cr dipilih untuk menyembunyikan data rahsia. Data rahsia disulitkan dengan menggunakan *affine cipher* untuk meningkatkan keselamatan data. Matriks Segi Empat Sama Ajaib digunakan untuk membenamkan kod rahsia ke dalam komponen Cb atau Cr menggunakan pendekatan ISB (Bit Bererti Pertengahan). Akhir sekali, kemantapan imej pelindung dinilai selepas dikenakan hingar garam dan lada. Hasil kajian menunjukkan kaedah baharu yang dicadangkan bukan sahaja menambah baik masalah keselamatan tetapi teknik yang dicadangkan dapat bertahan terhadap serangan.

TABLE OF CONTENTS

CHAPTER	TITLE		PAGE
	DECLARATION		ii
	DEDICATION		iii
	ACKNOWLEDGEMENT		iv
	ABSTRACT		v
	ABSTRAK		
	TABLE OF CONTENTS		vi
	LIST OF TABLES		x
	LIST OF FIGURES		xi
	LIST OF ABBREVIATIONS		xiii
1	**INTRODUCTION**		1
	1.1	Overview	1
	1.2	Background of the Problem	2
	1.3	Problem Statement	4
	1.4	Aim of the Study	5
	1.5	Objectives of the Study	5
	1.6	Scope of the Study	5
	1.7	Significant of the Study	6
	1.8	Research Framework	6
2	**LITERATURE REVIEW**		8
	2.1	Introduction	8
	2.2	Image File Format	9

2.2.1 Image Parameters 9
2.2.1.1 File Identifier 11
2.2.1.2 Image Description Information 11
2.2.1.3 Compression Types 12
2.2.1.4 X and Y Origin 13
2.2.2 Most Common Used Image Formats 13
2.2.2.1 BMP 13
2.2.2.2 GIF 14
2.2.2.3 PNG 15
2.2.2.4 JPEG 16
2.2.2.5 TIFF 17
2.3 Steganography 18
2.3.1 The Concept of Steganography 19
2.3.2 Different Kinds of Steganography 21
2.3.2.1 Steganography in Images 21
2.3.2.2 Steganography in Audio 21
2.3.2.3 Steganography in Video 22
2.3.2.4 Steganography in Documents 23
2.4 Parameters of Image Steganography 23
2.4.1 Capacity 24
2.4.2 Imperceptibility 24
2.4.3 Robustness 24
2.5 Steganographic Techniques 25
2.5.1 Transform Domain Techniques 25
2.5.1.1 Discrete Cosine Transform (DCT) 25
2.5.1.2 Discrete Wavelet Transformation 26
2.5.2 Image Domain Techniques 27
2.5.2.1 Conventional LSB Insertion Method 27
2.6 Enhanced LSB Algorithms 29
2.6.1 SLSB Method 30
2.6.2 The Optimal LSB Insertion Method 31

2.6.3 The Pixel Value Differencing Method (PVD) Method 32
2.6.4 Applying Randomization Concept to LSB Method 32
2.7 PSNR and NCC Formulas 33
2.8 Data Encryption 35
2.9 Summary 37

3 PROPOSED METHODOLOGY 39
3.1 Introduction 39
3.2 Proposed Method 39
3.3 Sending Phase 43
3.3.1 Affine Cipher (Crypto the Secret Message) 43
3.3.2 Converting Pixel Values to YCbCr 48
3.3.3 Embedding Algorithm 50
3.3.3.1 Magic Square 51
3.3.3.2 ISB (Intermediates Significant Bits) 51
3.4 Attacks 52
3.4.1 Salt-Paper Noise 53
3.5 Measurement and Evaluation 53
3.6 Receiving Phase 54
3.7 Summary 54

4 RESULT AND DISCUSSION 55
4.1 Introduction 55
4.2 Standard Dataset 56
4.3 Implementation and Result 57
4.4 Imperceptibility Result of the Proposed Method 61
4.5 Salt and pepper Measure for Robustness 66
4.6 Comparison with Other Study 72
4.7 Summary 73
5 CONCLUSION 74

5.1 Introduction 74
5.2 Summary of the Work 75
5.3 Contribution 75
5.4 Future Work 76

REFERENCES 77

LIST OF TABLES

TABLE NO.	TITLE	PAGE
2.1	Example of image file parameters	10
2.2	The values of a color image pixel – LSB insertion	30
2.3	The values of a color image pixel – SLSB insertion	31
2.4	Caesar encryption table	36
3.1	Write the numeric values of each letter	45
3.2	The initial steps (four) for the encryption process	46
3.3	The overall table for message encryption in the Affine cipher	46
3.4	The letters and their numeric equivalents in the cipher text 3	47
3.5	The result of both computations in the cipher text	47
3.6	Convert numeric values back into letters in the cipher text	47
3.7	The encrypting of Entire alphabet	48
4.1	Imperceptibility Results of the proposed method	61
4.2	The value of extracted correct character each time after applies different attack	69
4.3	The accuracy of extracted correct character each time after applies different attack	69
4.4	Performance of the proposed method against DWT	72

LIST OF FIGURES

FIGURE NO.	TITLE	PAGE
1.1	Framework of the study	7
2.1	Steganography process	20
2.2	Data of 3 pixels of a RGB color image	28
2.3	Data of 3 pixels of the RGB color image after LSB insertion of the number 83	28
2.4	Vigenere table	37
3.1	Flowchart of the Embedding phase	40
3.2	Flowchart of the Embedding phase	41
3.3	Flowchart of the Extraction phase	42
3.4	Lena image and its RGB channels	48
3.5	Lena image and its YCbCr channels	49
3.6	Magic square	51
3.7	ISB method	52
4.1	Dataset Airplane, Lena, peppers, Baboon, Goldhill, Sailboat and Tiffany.	56
4.2	Main interface of the implementation software	57
4.3	Interface of the Embedding process	58
4.4	Interface of Loading Image	58
4.5	Interface of Converting pixel values to YCbCr	59
4.6	Interface of the choosing the secret message	59
4.7	Interface of coding the secret message using affine cipher	60

4.8	Interface of extraction the secret message and decoding it using affine cipher	60
4.9	Imperceptibility Results of the proposed method using embedding rate 1KB.	62
4.10	Imperceptibility Results of the proposed method using embedding rate 2KB	63
4.11	Imperceptibility Results of the proposed method using embedding rate 4KB	63
4.12	Imperceptibility Results of the proposed method using embedding rate 8KB	64
4.13	Imperceptibility Results of the proposed method using embedding rate 16KB.	64
4.14	Imperceptibility Results of the proposed method using embedding rate 32KB.	65
4.15	Imperceptibility Results of the proposed with different case of payload size.	65
4.16	Lena Stego-mage after apply salt and pepper 0.1 attack	66
4.17	Lena Stego-mage after apply salt and pepper 0.2 attack	67
4.18	Lena Stego-mage after apply salt and pepper 0.3 attack	67
4.19	Hidden and extracted secret text messages after apply attack salt and pepper 0.3. a) Original embedded text. b) Extracted text	68
4.20	The accuracy of extorted proposed method using attack salt and pepper 0.1	70
4.21	The accuracy of extorted proposed method using attack salt and pepper 0.2	70
4.22	The accuracy of extorted proposed method using attack salt and pepper 0.3	71
4.23	Performance of the proposed method against both DWT	73

LIST OF ABBREVIATIONS

ASCII	-	American Standard Code for Information Interchange
BC	-	Before Christ
BMP	-	Bitmap image file
DCT	-	Discrete Cosine Transform
DWT	-	Discrete Wavelet Transform
EMD	-	Exploiting Modification Direction
GIF	-	Graphic Interchange Format
GLM	-	Gray Level Modification
HVS	-	Human Visual System
ID	-	The value of Identification
ISB	-	Intermediates Significant Bits
JPEG	-	Joint Photographic Experts Group
LSB	-	Lest Significant Bit
LZW	-	Lempel–Ziv–Welch
NCC	-	Normalized cross-correlation
PNG	-	Portable Network Graphic
PSNR	-	Peak Signal to Noise Ratio
RGB	-	Red Green and Blue
TIFF	-	Tagged Image File Format
YCbCr	-	Luminance, Chrominance blue Chrominance red
Cb	-	The blue-difference Chroma component
Cr	-	The red-difference Chroma component
MSB	-	Most Significant Bit

CHAPTER 1

INTRODUCTION

1.1 Overview

In this modern era, the security of transmitted information is very important because the world has become a global village. Methods that provide effective protection of data have now become necessary due to the huge growth of multimedia applications on networks. It is therefore important to create techniques that provide security for the media to protect it from unauthorized, unethical and illegal use by the attackers or hackers.

The most popular techniques dealing with data security are Steganography and Cryptography. Cryptography is a method of protection for data storage using secret key during data transfer. Encryption is still a successful method to protect stored data and to transmit over network. Steganography is an alternative method to protect information by preventing the detection of hidden messages (NehaBatra *et al.*, 2012). Steganography encompasses many secret communication methods that hide the message from being disclosed or seen.

The origin of steganography returns to the ancient Greece where King Darius ordered to shaved the head of prisoners to write the secret messages and when their hair grew back they moved to the recipient, and the secret remain undetected (Norman, 1979; Khan, 1967). Another story reveals that Greeks wrote their secret messages on a wooden medium and then covered them with wax (Silman, 2001). Since, then the steganography techniques gradually changed ranging from using invisible ink and microdots to modern methods like hiding data in digital media (Zim, 1984).

Two procedures are used in steganography. The first procedure is embedding which consists of two inputs: payload and cover image (host image). Payload quantity means the amount of the secret message that is going to embed. The cover image is used as a cover to contain the message inside it. After the embedding process is completed, the resulting image is called stego-image and is ready for transmission to the receiver. The second procedure is detector. The input for this procedure is stego-image, and the detector can recognize the secret message through an extraction process (Ravi Saini, 2014). As a result, the stenography is considered the information protection method that uses the host media as a cover for instance text, images, audio or video.

1.2 Background of the Problem

Several techniques have been proposed to conceal data inside the cover image, but the most popular approach is LSB, which is based on substituting the least significant bit with bits of embedded information inside the cover data of some or all bytes (Chan, 2004a). Slightly higher protection is provided by sharing secret keys between sender and receiver, by allowing only certain pixels to be changed and in this way it would be difficult to retrieve the message without having the "Stego_key".

In steganography, there is a tradeoff between the need to embed a large amount of data and to preserve the high image quality. Therefore, if it is required to have more payload, the image quality will be lower and vice versa. Steganography algorithms are usually not efficient with high amounts of embedded payload (Nedeljko, 2004).

There are several techniques that have been developed to increase the reliability and security of hiding data, but all of them have some disadvantages. GLM (Gray Level Modification), PVD (Pixel Value Differencing), and DWT (Discrete Wavelet Transform) are examples of steganographic techniques (Ravi Saini, 2014). It is necessary to use the most suitable technique for a particular application. Imperceptibility, payload capacity, robustness against manipulation and statistical attacks are always the main factors that should be taken into consideration.

Steganography of gray level modification also called (Gray Level Modification (GLM)), is a technique to modify the gray level values of the image pixels (neither embedded nor hidden) (Potdar, 2004). GLM maps the data within an image through the concept of odd and even numbers. The mapping is one-to-one between the selected pixels in an image and binary data. A set of pixels are selected form a given image based on a mathematical function. The selected sets of pixels are examined for gray level values and comparison has been made with the bit stream for mapping in the image. The advantages of this technique are optimal insertion of data and ease of implementation. The disadvantage includes the failure due to noise and compression attacks (Ravi Saini, 2014).

Some steganographic approaches focused on security and robustness, but usually the output image presented is either low in quality or has small capacity for hidden data. There is always a requirement to maintain a modified cover image not easily distinguishable by human eye. Obviously, the robustness and invulnerability of these methods are inadequate (Olivier, 2005). A balance between robustness and quality will lead to a successful approach.

Today, the important question, which needs answering, is that how we can increase the amount of the imperceptibility, robustness and maintaining the high quality of the image? In this research, the ISB method, affine cipher and Magic square are applied to embed large amount of secret data, while preserving the high image quality as compared to previous methods and to show high tolerance to statistical attacks such as noise.

1.3 Problem Statement

Due to the rapid growth of computer and communication technology, the digital content is easily distributed on the internet. However, this distribution sometimes causes substantial financial loss and becomes an imperative cause of copyright violation.

- With regard to high payload, previous studies proposed various techniques including LSB, DCT, DWT and EMD. However, the results of these methods revealed that increase in the payload decreases or degrades the quality and vice versa. Now, the question is that how to obtain high capacity and robustness without sacrificing the stego-image quality?
- With regard to security of information, the question is how to improve the security of secret message?
- With regard to robustness, previous studies proved that most of the steganography techniques are vulnerable to various attacks especially salt pepper attack. The question here is that how to design a robust method to tolerate the severe attacks?

1.4 Aim of the Study

This research aims to propose a technique that hides information in color images through an ISB technique, affine cipher and magic square algorithms to improve the imperceptibility and reducing distortion of the image. Furthermore, the system aims to produce a stego-image similar to the original image in terms of human visual system (HVS) measured by Signal-to-Noise Ratio (PSNR).

1.5 Objectives of the Study

This research intends to achieve the following objectives:

- To propose an improved steganography technique for color image based on Hybrid method ISB (Intermediates Significant Bits) and magic square to increase the security.
- To adopt the affine cipher in the secret messages of the proposed technique to make it highly secure.
- To evaluate the robustness of the proposed method against salt pepper attacks.

1.6 Scope of the Study

1. The file to be embedded (secret data) is the ordinary text file format.
2. The proposed method uses the basic concept of ISB insertion method.
3. The affine cipher encryption method is used to encrypt the input text file.

4. The standard images for testing purposes are Lena, Baboon, Airplane, Pepper, Tiffany, Sailboat and Golden hill.
5. The Salt-Pepper statistical attack is applied on the results to evaluate the robustness in terms of security of the proposed method.

1.7 Significant of the Study

The need for security especially in transferring the data between the sender and receiver is very important. There is a high demand for implementation of secure techniques. This thesis combined three techniques namely affine cipher coding, ISB algorithm and magic square method to increase the security and the amount of embedding data. The proposed hybrid technique has good results especially in two terms imperceptibility and robustness. In addition, the system embeds the secret message in a complex way and as a result, it is very difficult to reveal the message inside the image.

1.8 Research Framework

This study starts with the collection of requirements such as images and also prepares the secret messages. The second step involves the design and implementation of the proposed method (embedding and extraction process). The next step is the evaluation of the proposed method, which is performed by measuring the imperceptibility and robustness. Finally, the last step is benchmarking the proposed method with current state-of-the-art while discussion about the achieved results and elaboration of future goals. Figure 1.1, depicts the framework of this study.

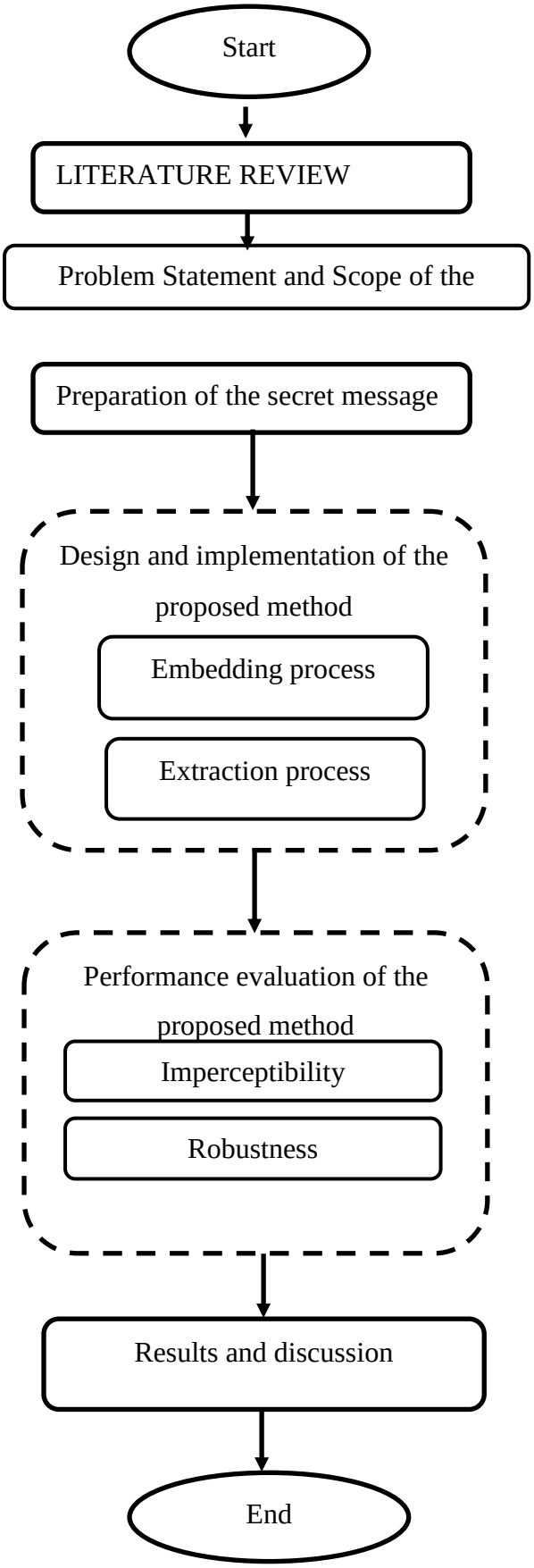

Figure 1.1 Framework of the study

REFRENCES

Almohammad, A. and Ghinea, G. Year. (2010). StegoImage Quality and the Reliability of PSNR. In: *Image Processing Theory Tools and Applications (IPTA), 2010 2nd International Conference on*, 7-10 215-220.

Anand, J. V. and Dharaneetharan, G. D. (2011). New Approach in Steganography by Integrating Different LSB Algorithms and Applying Randomization Concept to Enhance Security. *Proceedings of the 2011 International Conference on Communication, Computing* and #38; Security. Rourkela, Odisha, India: ACM.

Anderson, R. J. and Petitcolas, F. A. P. (1998). On the Limits of Steganography. *Selected Areas in Communications, IEEE Journal on*, 16, 474-481.

Aruljothi, S. and Venkatesulu, M. (2010) Symmetric Key Cryptosystem Based on Randomized Block Cipher. In: *Future Information Technology (FutureTech), 2010 5th International Conference* on, 21-23 May 2010. 1-5.

Avcibas, I., Memon, N. and Sankur, B. (2003). SteganalysisUsing Image Quality Metrics. *Image Processing, IEEE Transactions on*, 12, 221-229.

Bender, W., Gruhl, D., Morimoto, N. and Lu, A. (1996). Techniques for Data Hiding. IBM Systems Journal, 35, 313-336.

Chai, P., Liu, J., Pei, D. and Yang, Z. (2005). LPC Prediction Error Combined with LSB Steganography for Blind Speech Authentication. In: *Multimedia Signal Processing, 2005 IEEE 7th Workshop on*, Oct. 30 2005-Nov. 2 2005. 1-4.

Chan, C. K. and Cheng, L. M. (2004a). Hiding Data in Images by Simple Lsb Substitution.

Chan, C. K. and Cheng, L. M. (2004b). Hiding Data in Images by Simple LSB Substitution. *Pattern Recognition*, 37, 469-474.

Chang-Chu Chen and Chin-Chen Chang, (2007). Secret Image Sharing Using Quadratic Residues, *Intelligent Information Hiding and Multimedia Signal Processing,2007. IIHMSP 2007. Third International Conference on*. 515 – 518.

Cheddad, A., Condell, J., Curran, K. and McKevitt, P. (2010). Digital Image Steganography: Survey and Analysis of Current Methods. *Signal Processing*, 90, 727-752.

Cox, I. J. (2008). *Digital Watermarking and Steganography*, Morgan Kaufmann Publishers.

Dennie, V. T. (1970). Cryptographic Techniques for Computers: Substitution Methods. *Information Storage and Retrieval*, 6, 241-249.

Dumitrescu, S., Xiaolin, W. and Zhe, W. (2003). Detection of LSB Steganography via Sample Pair Analysis. *Signal Processing, IEEE Transactions on*, 51, 355-372.

Dunbar, B. (2002). *A Detailed Look at Steganographic Techniques and Their Use in an Open-Systems Environment*, SANS Institute.

Gardner, M. (1972). *Codes, Ciphers, and Secret Writing*, Dover.

Gardner, M. (1972). *Codes, Ciphers, and Secret Writing*, Dover.

Hore, A., Ziou, D. (2010). Image Quality Metrics: PSNR vs. SSIM. *In: Pattern Recognition (ICPR), 2010 20th International Conference on*, 23-26 Aug. 2010. 2366-2369.

Jianwen, L. and Konofagou, E. E. (2010). A Fast Normalized Cross-Correlation Calculation Method for Motion Estimation. Ultrasonics, *Ferroelectrics and Frequency Control, IEEE Transactions on*, 57, 1347-1357.

Johnson, N. F. and Jajodia, S. (1998). Exploring Steganography: Seeing the Unseen. *Computer*, 31, 26-34.

Johnson, N. F., Duric, Z., Jajodia, S. and Memon, N. (2001). *Information Hiding: Steganography and Watermarking, Attacks and Countermeasures*, SPIE.

Kahn, D. 1967. *The Code breakers*, New York: Macmillan.

Katzenbeisser, S. and Petitolas, F. (2000). *Information Hiding Techniques for Steganography and Digital Watermarking*. EDPACS, 28, 1-2.

Ke, Z., Jiangbo, L., Lafruit, G., Lauwereins, R. and Luc Van, G. (2009). Robust Stereo Matching with Fast Normalized Cross-Correlation over Shape-

Adaptive Regions. In: *Image Processing (ICIP), 2009 16th IEEE International Conference on*, 7-10 Nov. 2009. 2357-2360.

Li, L. and Ya-Qi, S. (2009). Experimental Research on Parameter Selection of Echo Hiding in Voice. *In: Machine Learning and Cybernetics, 2009 International Conference on*, 12-15 July 2009. 2423-2426.

Liping, J., Xiaolong, L., Bin, Y. and Zhihong, L. (2010) Year. A Further Study on a PVD Based Steganography. In: *Multimedia Information Networking and Security (MINES), 2010 International Conference on*, 4-6 Nov. 2010. 686-690.

Moerland, T. *Steganography and Steganalysis*[Online]. Leiden Institute of Advanced Computing Science. Available: www.liacs.nl/home/tmoerl/privtech.pdf [Accessed].

NedeljkoCvejic, TapioSeppänen, Increasing Robustness of LSB Audio Steganography Using a Novel Embedding Method, *Proceedings of the International Conference on Information Technology: Coding and Computing IEEE(2004).*

NehaBatra, *et al.*, (2012) Implementation of Modified 16×16 Quantization Table Steganography on Color Images, *International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 2, Issue 10, October 2012.

Nishikawa, K., Munadi, K. and Kiya, H. (2008). No-Reference PSNR Estimation for Quality Monitoring of Motion JPEG2000 *Video over Lossy Packet Networks. Multimedia, IEEE Transactions on*, 10, 637-645.

Norman, B. 1973. *Secret Warfare*, Washington, D.C.: Acropolis Books.

Olivier, T. M. a. J. H. P. E. a. M. S. (2005) An Overview of Image Steganography. In: *Hein S Venter, J. H. P. E., Les Labuschagne And Mariki Meloff, Ed. Fifth Annual Information Security, June/July* 2005 Sandston, South Africa.

Pan, F., Li, J. and Yang, X. (2011). Image Steganography Method Based on PVD and Modulus Function. In: *Electronics, Communications and Control (ICECC), 2011 International Conference on*, 9-11 Sept. 2011 282-284.

Paruchuri, J. K. and Cheung, S. c. S. (2008). *Joint Optimization of Data Hiding and Video Compression. In: Circuits and Systems, 2008. ISCAS 2008. IEEE International Symposium on*, 18-21 May 2008. 3021-3024.

Pieprzyk, J. P. and Rutkowski, D. A. (1985). Modular Design of Information Encipherment for Computer Systems. *Computers* and *Security*, 4, 211-218.

Platoš, J., Snášel, V. and El-Qawasmeh, E. (2008). Compression of Small Text Files. *Advanced Engineering Informatics*, 22, 410-417.

Potdar, V. and Chang, E. (2004), Gray Level Modification Steganography for Secret Communication, *IEEE International Conference on Industrial Informatics*, Berlin, Germany.

Ramkumar, M. and Akansu, A. N. (2001). Capacity Estimates for Data Hiding in Compressed Images. *Image Processing, IEEE Transactions on*, 10, 1252-1263.

Ravi Saini, (2014). Review of Different Techniques of Image Steganography" *International Journal of Computer Applications* and *Information Technology*, Vol. 5, Issue I Feb-March 2014 (ISSN: 2278-7720).

Roque. J.J., M. J. M. (2009). SLSB: Improving the Steganographic Algorithm LSB in 7th *International Workshop on Security in Information Systems, WOSIS*, and 2009 Milan, Italy. INSTICC Press, 57-66.

Scott R, E. (2009). Chapter 2 - *A Cryptography Primer*. In: JOHN, R. V. (ed.) Computer and Information Security Handbook. Boston: Morgan Kaufmann.

Silman, J. (2001). *Steganography and Steganoanalysis: An Overview*, SANS Institute.

Simmons, G. J. (1983). *The Prisoners' Problem and the Subliminal Channel*. CRYPTO. New York, 1984.

Tariq Al, H., Mahmoud Al, Q. and Hassan, B. (2003). A Test Bed for Evaluating Security and Robustness of Steganography Techniques. In: *Circuits and Systems, 2003 IEEE 46th Midwest Symposium on*, 27-30 Dec. 2003. 1583-1586 Vol. 3.

Tsung-Yuan, L. and Wen-Hsiang, T. (2007). A New Steganographic Method for Data Hiding in Microsoft Word Documents by a Change Tracking Technique. *Information Forensics and Security, IEEE Transactions on*, 2, 24 30.

Wu, H. C., Wu, N. I., Tsai, C. S. and Hwang, M. S. (2005). Image Steganographic Scheme Based on Pixel-Value Differencing and LSB Replacement Methods. *Vision, Image and Signal Processing, IEE Proceedings* -, 152, 611-615.

Xiangyang, L., Bin, L. and Fenlin, L. (2005). Detecting LSB Steganography Based on Dynamic Masks. In: *Intelligent Systems Design and Applications, 2005.*

*ISDA '05. Proceedings. 5th International Conferenc*e on, 8-10 Sept. 2005 251-255.

Zim, H. S. (1984). *Codes and Secret Writing*, New York, William Morrow.