LEAST SIGNIFICANT BIT STEGANOGRAPHY TECHNIQUE USING MODULUS OPERATION WITH PIXEL GROUPING SELECTION DERIVED FROM K-MAP AND GAUSSIAN ELIMINATION

SAYUTHI BIN JAAFAR

UNIVERSITI TEKNOLOGI MALAYSIA

LEAST SIGNIFICANT BIT STEGANOGRAPHY TECHNIQUE USING MODULUS OPERATION WITH PIXEL SELECTION DERIVED FROM K-MAP AND GAUSSIAN ELIMINATION

SAYUTHI BIN JAAFAR

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Doctor of Philosophy (Computer Science)

Faculty of Computer Science and Information Systems
Universiti Teknologi Malaysia

JANUARY 2013

To my beloved wife, sons and daugthters

ACKNOWLEDGEMENT

Alhamdulillah, the utmost gratitude I express to my dearest God, Allah SWT, for bestowing upon me the greatest strength, patience, courage, and determination in finishing this work.

I also wish to express my sincere gratitude and appreciation to my supervisor, Professor Dr. Azizah binti Abdul Manaf, for her never-ending encouragement and support as well as her invaluable guidance towards the success of this research. All of the regular sessions that we have had through out the period of study have proved to be a fruitful effort as the sessions do contribute tremendously to the success of the research.

I am also very grateful to Prof. Dr. Richard Eason from University of Maine, USA, for providing me with accomodation in his faculty for three months. Your support, idea and comment really showed me the right track in persuing this research.

I also want to thank all of my friends for their support and help; and not forgetting their view and tips, both are very useful indeed. Unfortunately, it is not possible to list all of them in this limited space.

Last but not least, I would also like to express my high gratitude to all my family members. My deepest feelings go to my beloved wife, sons and daughters for giving full support, aspiration and high understanding during the period of my studies.

ABSTRACT

As demand for information exchange across the network increases, so is the need for safe covert communication, which can be achieved using steganography. Many steganography techniques have emerged; however the performance of the techniques rely heavily on three major factors, which are the payload, imperceptibility and robustness. These elements are always in trade-off. In this research, a new steganography technique that emphasizes on high imperceptiblity with reasonable embedded capacity is presented. The proposed embedding approach leverages on the LSB substitution technique and neighbourhood operation to precisely determine how much changes is required for each target pixel of host image in terms of its gray scale. Thus, a 9x9 filter called Matrix Distribution Array (MDA) is introduced based on the Karnaugh Map grouping principle to generate nine possible 4-pixel groups for pixels selection. A modulus operation is then performed for each group to obtain a group residue (Res). An initial change of the target pixel value is calculated based on the difference between Res and secret information. Afterwards, the Gaussian Ellimination technique is then applied together with MDA on the change value to obtain a final figure of the change required. Finally, the target pixel is modified and rounded accordingly by subtracting its original gray scale with the change value. The embedding process is repeated until a stego-image is eventually produced, likewise, an extraction process is performed using a similar procedure but in a reverse manner. The experimental results show that the imperceptibility of the proposed method improved significantly by 8% to 16% when tested with fixed embedding capacity ranging from 6 kB to 116 kB as compared to the LSB substitution technique. The result also reveals that the embedding capacity improves up to 50% while maintaining reasonable Peak Signal-to-Noise-Ratio (PSNR) value between 35dB to 40dB.

ABSTRAK

Peningkatan permintaan pertukaran maklumat merentasi jaringan secara berterusan adalah selari dengan keperluan komunikasi rahsia yang selamat yang mana boleh dicapai melalui teknik steganografi. Walaupun terdapat banyak teknik steganografi yang telah diperkenalkan, prestasinya amat bergantung kepada tiga faktor utama, iaitu kapasiti, ketidakbolehnampakan, dan kekukuhan. Ketiga-tiga faktor ini saling bergantung diantara satu sama lain. Dalam kajian ini, satu teknik steganografi baru yang memberi penekanan terhadap pencapaian ketidakbolehnampakkan yang tinggi dengan kapasiti pembenaman yang berpatutan dikemukakan. Pendekatan cadangan adalah lanjutan daripada teknik penggantian Bit Bererti Terkecil (BBT) dengan penambahbaikan melalui operasi kejiranan antara piksel-piksel yang dipilih. Ianya akan menentukan dengan tepat perubahan yang diperlukan untuk setiap sasaran piksel imej hos dari segi nilai skala kelabu. Sehubungan dengan itu, satu penapis 9x9 yang digelar sebagai Matrik Tatasusunan Taburan (MTT) yang berasaskan kepada prinsip perkumpulan Peta Karnaugh diperkenalkan untuk menjana sembilan kemungkinan kumpulan yang bersais 4 piksel setiap satu. Seterusnya, operasi modulus dilakukan terhadap setiap kumpulan untuk mendapatkan nilai sisa berkumpulan. Perubahan awal terhadap piksel sasaran dikira berdasarkan perbezaan diantara sisa tersebut dengan maklumat rahsia. Berikutnya, teknik Penghapusan Gaussian digunakan bersama dengan penapis MTT terhadap nilai perubahan tersebut untuk mendapatkan nilai perubahan sebenar piksel sasaran. Akhirnya, nilai asal piksel sasaran ditolak dengan nilai perubahan sebenar diatas untuk menghasilkan skala kelabu yang baru, dan seterusnya nilai tersebut dibulatkan sewajarnya. Proses pembenaman ini diulangi sehingga imej-stego keseluruhan dihasilkan. Sedemikian juga dengan proses pengekstrakan, ianya dilaksanakan dengan menggunakan prosedur yang sama tetapi dalam keadaan menyongsang. Keputusan eksperimen menunjukkan bahawa ketidakbolehnampakkan meningkat dengan ketaranya berbanding dengan teknik penggantian BBT, iaitu sebanyak 8% hingga 16% apabila diuji dengan kapasiti pembenaman yang ditetapkan daripada 6 kB hingga 116 kB. Hasil ujian juga menunjukkan bahawa kapasiti pembenaman meningkat sehingga 50% untuk nilai Puncak Nisbah-Isyarat-terhadap-Hingar (PNIH) antara 35dB hingga 40dB.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATION

AMBTC	-	Absolute Moment Block Truncation Coding
BPCS	-	Bit Plane Complexity Segmentation
CD	-	Change Distribution
CPT	-	Chen Pan Tseng
CRT	-	Chinese Remainder Theorem
DCT	-	Discrete Cosine Transform
DWT	-	Discrete Wavelet Transform
EW	-	Electronics Warfare
GE	–	Gaussian Elimination
HVS	-	Human Visual System
LSB	-	Least Significant Bit
MDA	–	Matrix Distribution Array
MSE	-	Mean Squared Error
NCC	-	Normalized Cross Correlation
PSNR	-	Peak Signal to Noise Ratio
PDCS	-	Pixel Difference Complexity Segmentation
RDV	–	Rounding Differential Value
RGB	-	Red Green Blue
SNR	-	Signal to Noise Ratio
VER	-	Variable Embedding Rate

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Background

The digital information revolution, from basic analog to digital conversion to the latest and sophisticated applications, has brought about a significant change in our society and daily life. Firstly, the advantages provided by digital information environment have generated new challenges and new opportunities for innovation. This is evident from how the powerful software and high-tech devices have been able to allow users to create**,** manipulate and enjoy the digital multimedia data in its many forms such as text, image, voice and video. Apart from that, the global and easy access communication infrastructures, such as internet and wireless network, also offer unlimited channels to deliver and to exchange information. Therefore, security and fair use of the data, as well as securely delivering or storing the data's contents are very important yet challenging topics (Yang, 2003).

Open network does not use secured infrastructures. Therefore, information may be vulnerable to various interception activities, allowing for the need to protect information from falling into wrong hands. Thus, multimedia security is a crucial consideration to ensure digital information safely distributed (Tsai, 2010; Khan and Muhammad, 2011).

Steganography, which is schemed to embed secondary data in primary media, has made considerable progress in recent years, thus, grabbing a lot of attention from both academia and industry. Techniques have also been proposed for variety of applications, such as ownership protection, authentication, access control, annotation and secret communication (Petitcolas et al., 1999).

Thus, it is important to rely on the fact that, when information is stored in the network or transmitted over a transmission medium, the information can also be read or received by internal or external attacker. It is quite impossible to prohibit information pilferage as the attacker will utilise all kinds of technology and equipment to monitor the opponent’s communication or to access enemy’s databases. Hence, in order to avoid any attacker activities as mentioned above, it is vital that any communication activities are not visible at all to the enemy’s eyes and ears.

1.2 Information Hiding

One of the possible approaches to ensure security is by representing information in such a way that the resulting datagram will be easily interpreted by the privileged endpoint that has the right key. Apart from that, interpretation of the same data by non-privileged endpoints poses a serious problem which would usually involve incorporating vast computational effort. The system that implements such security is called crypto system. The study of how this system can be constructed is referred to as cryptography, while the study of solving the interpretation-problems posed by cryptosystems is referred to as cryptanalysis (Schneier, 1996; Massey, 1998; Simmons, 1992).

Another approach to security involves the awareness of the very existence of a datagram. Here, information is represented in such a way that the resulting datagram will be known to contain secret information only by privileged endpoints (ones that have been told where to expect hidden information), while testing whether a given datagram does, or does not contain secret information that can pose a serious problem for non-privileged endpoints. Analogously, a system that implements such security is called stega-systems. The study of the stega-system construction is called steganography and the study of testing a given datagram containing a secret message is called steganalysis.

Today, crypto-graphical techniques have reached a level of sophistication as such that any properly encrypted communications can be assumed as secured, well beyond the useful life of the information transmitted. For most users in most applications, the current cryptographic techniques are generally sufficient. Why then, the need for the field of steganography? There are several good reasons as listed by Bender and his associates in 1996 that could answer the question. The reasons are:

(i) The growing use of communicating data via the electronic means (such as Internet) has increased the concern over the security of information being transmitted via the communication network against any potential interceptor. With steganography technique, the secret information can be delivered safely without any suspicions from the third parties.

(ii) With the increase of the computer processor's power, the possibility of breaking the encrypted message still exists. The ciphered message may be exposed to the third party indicating that there is a secret information being sent. Therefore, the intended eavesdropper may attempt to decrypt it. With steganography, it would be extremely difficult for the steganalyst to monitor all the communication and identifies which of the images contain secret information from thousands, or maybe, millions of images available.

(iii) In an ideal world, the sender would be able to openly send encrypted email or files to one another with no fear of reprisals. However there are often cases where this is not possible, either because the sender is working for a company that does not allow encrypted email or perhaps, the local government does not approve of encrypted communications. This is where steganography can come into play.

(iv) In military communication, where the enemy knows that the opponent is sending secret information, the enemy communication group will try to break the secret information, while the artillery and the air force get ready to destruct the opponent's communication center or communication infrastructures. Steganography by its nature will avoid this from happening.

Information hiding is an addition of application-oriented information to the multimedia signal, without causing any perception distortion. The energy of the embedded signal should be low enough when it is projected onto the human perception domain. However, the signal should be strong enough for robust machine detection. In the area of information security, information hiding technique can be divided as how a tree is divided into several branches like in the following Figure 1-1 (Petitcolas et al., 1999).

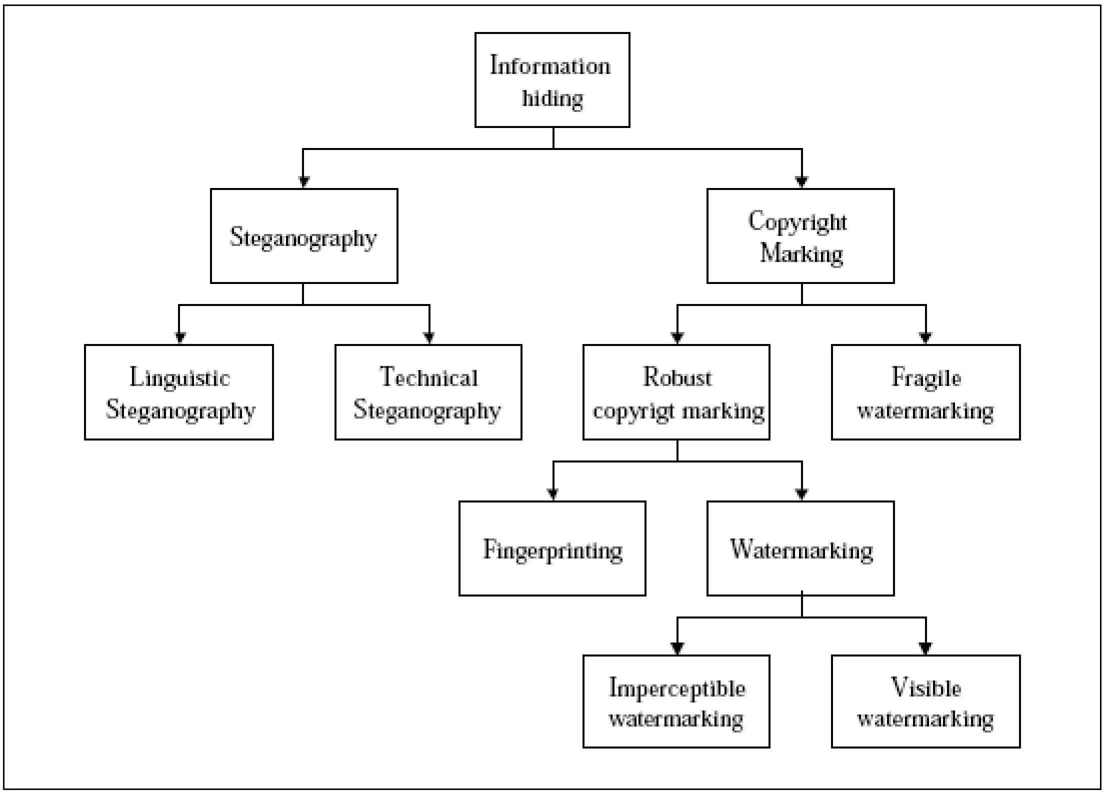

Figure 1-1: A Classification of Information Hiding Techniques (Petitcolas et al., 1999).

When discussing different hiding techniques, the following restrictions and features are desirable (Bender *et al.*, 1996). The hidden information:

(i) Shall be very little perceptible.

(ii) Should be directly encoded into the media, rather than into a header or a wrapper.

(iii) Should not be lost if it is modified by conversion, lossy compression, re-sampling, etc.

(iv) Should be embedded using asymmetrical coding (the use of public or private keys), which makes the exchanges of keys easier.

(v) Should include error correction codes since manipulation of the cover media often leads to problems with the data integrity.

(vi) Should be self-clocking or arbitrarily re-entrant. This means that if only a part of the cover media is available, the hidden information within that part should be possible to extract.

1.3 Problem Statement

Steganography problem in most literatures are phrased as a prisoner's dilemma or the prisoner’s problem, and was firstly introduced in the context of subliminal channel (Simmons; Chaum, 1984). It is often used in illustrated steganography. For example, two prisoners named Alice and Bob are allowed to communicate with each other by exchanging messages through Wendy, the warden. Wendy will not allow the messages to be encrypted. Therefore, only plain text will be passed between Alice and Bob. All of the parties agree to these conditions and the communication begins. Unknown to the warden, the prisoners are still able to coordinate their escape plans by using steganography technique to communicate, even under the warden’s tight supervision. Essentially, the prisoners would use some pieces of shared knowledge to hide their real communication in the innocuous message. The warden sees the innocent message, checks and passes it along. The prisoner checks the signature to see whether the warden altered the message, and then extracts the real message from the known shared knowledge.

In Alice and Bob case, Alice wants to submit a secret message, ***M,*** to Bob, and again, a secure key-distribution facility makes sure Bob has an advantage over Wendy when it comes to reconstructing this message. That is, Bob and Alice know exactly which secret key, ***K,*** is used (they could have agreed on one before the imprisonment).

The prisoner dilemma described above can be translated into the present scenario where Bob and Alice could be different organizations, companies or maybe even military commanders, whereas Wendy can be any third-party whose interest lies in the communication between Bob and Alice. She has the capability to monitor and to tap the information that is being transmitted between the other two parties. She also has the capability to download any information from Alice's and Bob's databases. However, steganography permits Bob and Alice to deliver the secret information without the knowledge of Wendy, even though she may get all the information transmitted or stored. Furthermore, Bob and Alice can use public domain website to paste their stega-images that only both of them know which the stega-image is. It would be highly impossible for Wendy to know the stega-image from thousands, or maybe millions of images that could be monitored.

A general design principle for steganography, following from these prisoner's problem observations, assumes that Alice uses the host image, ***H,*** and Bob knows the secret key, ***K***. The secret key is a password used to seed a pseudo-random number generator that could be used to select pixel locations in an image of cover-image.

*Alice performs operation **e: H x M x K → E**, called embedding-function, to embed secret information **M** in the **H** using a secret key **K,** to produce stega-image **E**.*

This operation is subjected to some constraints which make up a model for perceptual similarity. It can be assumed that there would be some functions, which can be used to determine the embedding distortion **(*δ*)** between a host image ***H,*** and a stega-image ***E***. Wendy will see ***E*** as innocuous as long as the ***δ*** is less than the threshold.

*Bob performs operation **d: E x K → M**, called extraction-function, to extract secret information **M** from stega-image **E**, using a secret key **K.***

Problem statement is summarised as below:

(i) A core problem of this research is to formalise what it means by the statement "stego-image must be imperceptible" as well as the level of visibility of the hidden data. In fact, steganography systems need to be somewhat more selective about the set of possible host image ***H***. The host image ***H*** will give different sets of potential pixels to be replaced by secret information ***M***. To determine these regions, the cover image is analysed in order to find the embedding distortion **(δ)** level. If this level is above a certain threshold, the secret information can be embedded in this region without significantly altering the image.

(ii) This research considers steganography as a communication problem, where the embedded data is the signal to be transmitted. Issues regarding multimedia data hiding and its applications in multimedia security and communication security will be addressed. The work that is included in this thesis intends to contribute in the understanding of data hiding by addressing both theoretical and practical aspects, and tackling design problems. Different embedding mechanism targets at different perceptibility-capacity tradeoff will also be studied.

(iii) This study also serves as a guideline for selecting an appropriate embedding algorithm given the design requirements of an application, such as using spatial domain images for covert communication application.

(iv) Furthermore, a new embedding framework/algorithm with improved performance is proposed as well. In addition, this thesis will also discuss a number of modulation/multiplexing techniques for embedding multiple bits in image sources. The principles that will be discussed in this study are used intensively in the algorithm and system designs.

1.4 Research Goal

The goal of this research is to develop a new steganography technique that would contribute towards high imperceptibility with reasonable embedded capacity.

1.5 Research Objectives

The general, measurable objective of this research is to develop new steganography technique. The specific objectives are:

(i) To design and develop new spatial domain image steganography technique.

(ii) To propose a new embedding technique that could improve the imperceptibility.

(iii) To analyze the proposed technique with standard PSNR operating conditions. The standard PSNR for the stego-image must not be less than 30 dB.

1.6 Research Scope

(i) **Host Images -** Twenty (20) standard images (.bmp) are used.

(ii) **Secret Information**. Four types of secret information are used. They are text (secret.txt), image (secret.bmp), document (secret.pdf) and video (secret.wmv).

(iii) There is perfect synchronization between transmitter and receiver.

Thus, it can be assumed that there would be no lost data due to communication or network problem.

1.7 Operational Framework

The operational framework of this research is represented in the following Table 3-1. It is related within the research questions, objectives, activities involved and the outcome of the overall works.

Table 1.1: Operational Framework

Research Questions	**Objectives**	**Activities**	**Outcomes**
How to improve the embedding capacity without degrading the visual quality of the host image?	To design and demonstrate a new technique for embedding information in host image.	i. Observation, reasoning and problem identification. ii. Survey on current Spatial Domain Technique. iii. Identify area where the present LSB substitution technique can be improved	i. Obtain an idea of proposed research's goal. ii. Justify problem statement. iii. Propose research scope. iv. Propose limitation and parameter for benchmarking. v. Introduce relevance new parameters. vi. Identify suitable mathematical technique in solving the problem arose.

Research Questions	Objectives	Activities	Outcomes
What is the trade-off between capacity and visual quality of stega-image related to size of secret information?	To implement, analyze and validate relationships on capacity and quality related to the proposed technique.	i. Design and develop prototype of proposed technique using C++. ii. Conduct mathematical modeling to represent all possible data. iii. Test the prototype and the mathematical modeling.	i. Obtain the embedded capacity and stego-image quality measured in PSNR (dB). ii. Conclude the trade off between capacity and the imperceptibility of the stego-image.
How to formulate a new control measure in the proposed technique	To formulate a new control measure and secret key to work with the proposed technique.	i. Design and implement suitable array in solving pixels grouping by using Karnaugh Map (K-Map) square grouping technique ii. Find technique to simplify the process of distributing the changes among pixels.	i. Introduce array called Matrix Distribution Array (MDA) for 9 pixels grouping. ii. Use Gaussian Elimination (GE) technique to find the changes distributed among pixels in the group due to embedding process.

This research involves a huge volume of data that need to be tested. Therefore, it has been decided that two modeling concepts would be used. The concepts are:

(i) **Mathematical Data Modeling**. This modelling involved with a huge data, which are mathematically presented. All possible data are produced and tested.

(ii) **Real Data**. Real host image and real secret information are tested with the proposed technique.

1.8 Significant of the Research

This research will benefit both the government sector and/or companies as this would assist both parties to ensure that their secret information is safely delivered to their counterparts. Furthermore, their communication would not be noticeable by others, thus, preventing unwanted information leakage cases. Other than that, this research will also have a direct benefit on the armed forces. Military secret information converted into meaningless information using modern and sophisticated cryptographic are already available, making it quite easy for the enemy to decode the code. However, if the present encrypted messages were to be sent by steganography mode, it would enhance data security by identifying the position of the sender and the receiver, thus, protecting it from being known by the enemy.

Apart from that, this technique can also be used within the public domain infrastructure. The most famous and easily accessible communication infrastructure would be the internet. Information can be simply accessible to the public by using public domain website, such as the auction web site offered by E-bay. By pretending that a person wants to sell something, he/she can send the stego-image to the website. The intended receiver would then download the image and extract the secret information. There would be no communication between two intended parties in the eyes of the third party. Other example would be the photo gallery in a company database. Such gallery can be used to store company's strategic plan for future retrieval. Company's or organization's website can contain a stego-image that can be downloaded by their counterpart. Of course, the third party can also download the image. However, for the third party, an image is only an image.

Security technique and its algorithm are better if it is developed locally. This research will initiate the requirement of locally designed steganography technique, especially for secret communication application.

1.9 Organization of the Thesis

The organization and the way this thesis would be presented are illustrated in the Figure 1-3 below:

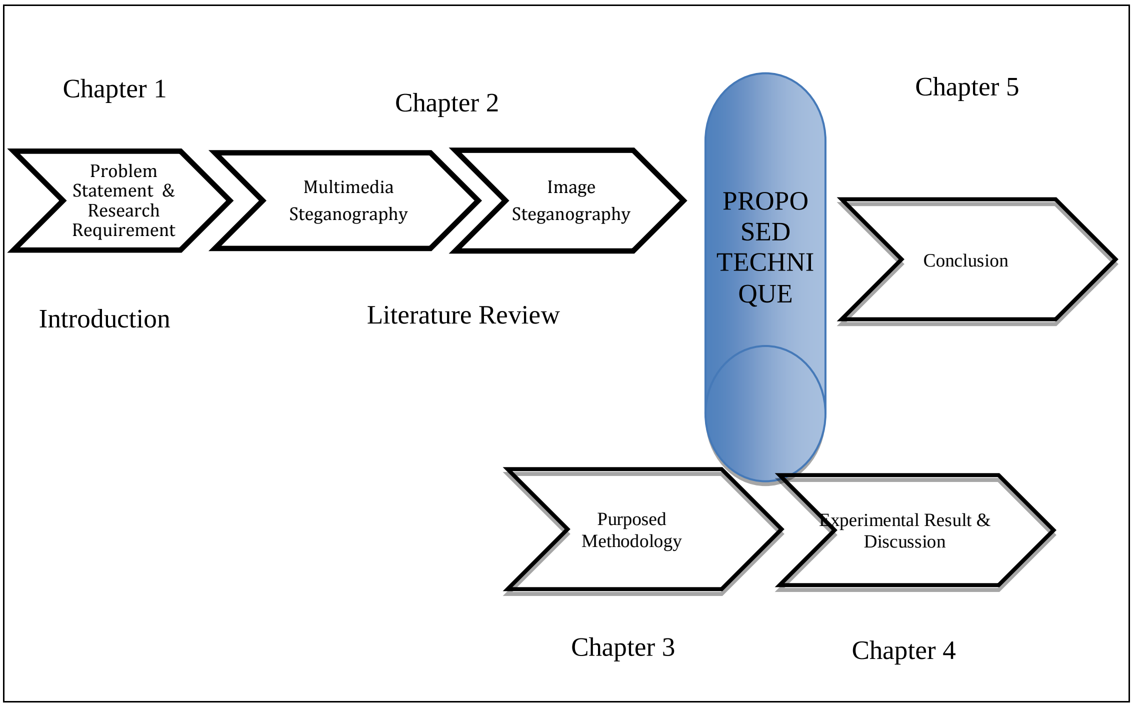

Figure 1.2: Thesis Organization.

Generally, this research comprises six chapters. The first chapter highlights on the overall research requirements; covering from problem statement, research goal, research objective, research framework and the significant of the research.

A literature review on data hiding and steganography is covered in Chapter 2 where some of the related studies have been discussed in detail. This includes the advantages and disadvantages of the techniques proposed in previous studies. Chapter 2 also attempts to explain more on image steganography technique specific to Spatial Domain Technique.

Next, Chapter 3 describes proposed methodology, design and procedures for the proposed technique. The implementation of proposed technique is covered in detail. In addition to that, the control mechanism: Matrix Distribution Array (MDA), Rounding Differential Value (RDV) are determined as well.

Furthermore, a discussion on the result of the study is provided in Chapter 4. The analysis of the proposed method and the threshold value are revealed as well. Other than that, a comparative study between the proposed technique and LSB Substitution Technique is presented and discussed.

Finally, the conclusion of this research is presented in the final chapter (Chapter 5). The perspective and proposed future study are also elaborated in this final chapter.

REFERENCES

Ahmet, B (2002). Watermarking Capacity Improvement by Low Density Parity Check Codes, Master Thesis. Bogazici University, Turkey.

Al-Jaber, A., and Aloqily, I. (2003). High Quality Steganography Model with Attacks Detection. Pakistan Journal of Information and Technology. 2(2), p 116-127.

Anderson, R. J. Stretching the limits of Steganography, (1996), in Information Hiding, Springer Lecture Notes in Computer Science, vol 1174, pp 39-48.

Anderson R., 1996, Proceedings of First International Workshop on Information Hiding, volume 1174 of LNCS, Cambridge, UK, May/June 1996. Springer-Verlag

Anderson R. J., and Petitcolas, F. A. P. (1998), On the Limit of Steganography, IEEE J Select Area Communication, vol 16, , pp 474-481.

Aucmith D, 1998, Proceedings of Second International Workshop on Information Hiding, volume 1525 of LNCS, Porland, Oregan, April 1998. Springer-Verlag

Azizah, Akram, Sayuthi, (2004), Watermarking of Digital Images: An Overview, 2nd National Conference on Computer Graphic & Multimedia Proceeding, Malaysia.

Azizah, M., Akram, M. Z., Salehuddin, K., and Sayuthi, J. (2005) Analysis of Image Quality for Steganographic Software, Brunei International Conference on Engineering and Technology 2005 (BICET 2005) Proceeding.

Barni M., Bartolini F., Cappellini V. and Piva A., (1998), A DCT Domain System for Robust Image Watermarking, Signal Process, vol 66, pp 357-372

Barni, M., Bartolini, F., Rosa, A. D. (2005). Perceptual Data Hiding in Still Images, Chapter II, Multimedia Security, Idea Group Publishing.

Bender, W., Gruhl, D., and Morimoto, N. (1995). Techniques for Data Hiding Proceeding of the SPIE. San Jose, CA: 2420-2440.

Bender, W., Gruhk, D., Morimoto N., and Lu, A. (1996). Techniques for Data Hiding. IBM System Journal. 35(3&4): 313-336.

Bhattachatjya A. K., and Ancin, H. (1999), Data embedding in Text for Copier System, in Proc IEEE ICIP 99, vol 2, Japan, pp 245-249.

Boneh, D. (1998). The Decision Diffie_Hllman Problem, Lecture Notes in Computer Science, 1423: 48-63.

Brassil, Low, J. T., Maxemchuk, N. F., and Gorman, O. (1995), Electronic Marking and Identification Technique to Discourage Document Copying, IEEE Area Communication,13 (8), pp 1495-1503.

Brassil, J. L., O' Gorman, Maxemchuk, N. F., Low, S.H. (1995), Document Marking and Identification Using Both Line and Word Shifting, InfoCom, Boston, pp 853-860.

Brian Clair, (2001), Steganography: How to Send a Secret Message, http://www.strangerhorizon.com/2001/20011008/steganography.shtml.

Briffa, J. A., and Das, M. (2002). Channel Models for High Capacity Information Hiding in Images. The International Society for Optical Engineering Journal 135-144.

Burdick, H. W (1997), Digital Imaging Theory and Application, McGraw Hill, NY.

Cachin, C. (1998) An Information-theoretic model for Steganography, Information Hiding, Second International Workshop, Proceeding (LNCS 1525), pages 306-318, Springer-Verlag,1998, Portland, Oregon.

Chae, J. J., and Manjunath B. S., (1998), A Robust Embedded Data from Wavelet Coefficient. Proc SPIE-Int Soc Opt Eng, 3312, pp 308-317

Chan, C. K., and Cheng, L. M. (2001). Improved Hiding Data in Images by Optimal Moderately Significant-bit Replacement. IEEE Electron Letters. 37(16): 1017-1018.

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

Chang, C. C., and Tseng, H. W. (2004). A Steganographic Method for Digital images using side match. Pattern Recognition Letters. 25(Jun): 1431-1437.

Chang, C. C., Hsiao, J. Y., and Chan, c. s. (2003). Finding optimal Least-Significant-bit Substitution in Image Hiding by Dynamic programming Strategy. Pattern Recognition Letters. 36(7): 1583-1595.

Chaum, D, (1984), editor Advances in Cryptography: Proceeding of Crypto ’83: 51-70, NY Plenum Publishing

Chen, P. C. (1999). On the Study of Watermarking Application in WWW- modeling, Performance analysis, and Application of Digital Image Watermarking Systems, PhD Thesis, Monash University.

Chen, W. Y. (2003). A Comparative Study of Information Hiding Schemes Using Amplitude, Frequency and Phase Embedding. PhD Thesis. Department Of Electrical Engineering, national Cheng Kung University, Tainan, Taiwan.

Cheung, W. N. (2000). Digital Image Watermarking in Spatial and Transform Domain. TENCON Proceeding, 2: 374-378.

Chen, D., Luo X. W., and Yu, M. (2006). Steganography Preserving the Property of the histogram for JPEG images. Journal of Electronics and Information Technology, v 28, n 2, p 252 – 256.

Chin, C. C., Guei, M. C., and Lin, M. H. (2004). Information Hiding Based on Search-order Coding for VQ Indices. Pattern Recognition Letters.

Chung, K. L., Shen, C. H., and Chang, L. C., (2001). A Novel SVD and VQ Based Image Hiding Scheme. Pattern Recognition Letters. 22: 1051-1058.

Chung, M. S., Chang, K. H., and Hsiao, S.F. (2000). Robust Spatial-Domain Watermarking Methods Based on a Weighting Table with Fine-Tune technique. ICS.

Counterintelligence News and Developments, Vol 2, June 1998, Hidden in Plain Sight-Steganography Open source: www.nacic.gov/pubs/news/1998/jun98.html

Cox J. J., Kilian J., Leighton E. T and Shamoon T., (1997), Secure spread spectrum watermarking for multimedia, IEEE Trans Image Process, 6 (12), pp 1673-1687

Cox, I., Miller, M. L., and Bloom, J. A. (2002). Digital Watermarking. Morgan Kaufman Publishers, San Francisco, pp 12-36

Craver, S. (1998). On Public-key steganography in the presence of an active Warden, In David Aucsmith, editor, IH, 2nd IH Woksyop, Portland , Oregon, USA, vol 1525 of LNCS Apr 98.

Cummins, J., Diskin, P., Samuel, L., and Robert P. (2004). Steganography and Digital Watermarking, School of Computer Science. The University of Birmingham copyright, 2004.

Currie, D. L., and Campbell, H. (1996). Implementation and Efficiency of Steganography Techniques in Bitmapped Images and Embedded Data

Survivability against Lossy Compression Schemes. Master Thesis, March Naval Postgraduate School, California.

Davern P, Scott M., Steganography: Its history and it Application to Computer baseDataFiles,Open source http://www.jjtc.com/steganography/bib/3000027.htm

Davern, P., and Scott, M. (1996). Fractal Based Image Steganography. Proc. First Internet. Workshop Information Hiding. Lecture Notes in Computer Science. 1174, Berlin. Springer-Verlag: 279-294.

Delp, E. J., Mitchell, O., R. (1979), Image Coding Using Block Truncation Coding, IEEE Transaction on Communication, vol 27, 1979, pp 1135-1342.

Eason, R. (1998), A Tutorial on BPCS Steganography and Its Application, Department of Electrical and Computer Engineering, University of Maine.

Eason, R. (2002), Digital Steganography: A Perspective Keynote Speech Paper, Proc of Pacific Rim Workshop on Digital Steganography 2002.

Eason, R. (2003). A Tutorial on BPCS Steganography and Its Applications. Proc of the Pacific Rim Workshop on Digital Steganography 2003.

Eason, R., Kawaguchi, E. (1995), Depth-First Coding for Multi-valued pictures using bit-plane Decomposition, IEEE Trans. On Comm., vol 43, no 5 pp 1961-1969.

El-Iskandarani, M.A., Darwish, S.M., and Abubahia, A.M. (2009) Capasity and Quality Improvement in Blind Second Generation Watermarking. Proceedings – International Carnahan Conference on Security Technology. P 139-143

Ettinger, J. M., (1998). Steganalysis and Game Equilibria, In D Aucsmith, editor, Proceedings of Second International Woksyop on IH, vol 1525 of LNCS, pages 319-328, Springer.

Fridrich, J., and Goljan, M. (2002). Practical Steganalysis of Digital Image – State of the Art. Proceeding of SPIE Photonic West. Conference on Security and Watermarking of Multimedia Contents: 4675: 1-13.

Fridrich J., and Rui D., (2000). Secure Steganographic Methods for Palette Images. Proceeding of 3rd International Workshop on Information Hiding. Lecture Notes in Computer Science: Berlin 1768. Springer-Verlag: 61-76.

Fridrich J., Goljan, M., and Baldoza, A. C. (2000). New Fragile Authentication Watermark For Images. IEEE.

Fridrich J., Goljan, M., and Du, R., (2001). Reliable Detection of LSB Steganography in Gray scale and Color Images. Proceeding of ACM Workshop on Multimedia and Security: 27-30.

Gaustavus J Simmons, (1991), Contemporary Cryptology : The Science of Information Integrity, IEEE Press 1991.

Gonzales, R.C., and Woods, R. E. (2008) Digital Image Processing, Prentice Hall.

Gulati, K. (2003). Information Hiding Using Fractal encoding. Master Thesis Indian Institute of technology Bombay, Mumbai.

Habes, A. (2006). Information Hiding in BMP Image Implementations, Analysis and Evaluation. Information Transmission in Computer Networks. 6(1): 1-10.

Hala, H., and Zayed, A., (2005). High Hiding capacity Technique for Hiding Data in Images Based K-bit LSB Substitution. Proceeding of the 13th International conference on Artificial Intelligence Application. February 23-26. Cairo, Egypt.

Hartung, F. and Kutter, M. (1999), Multimedia Watermarking Techniques, Proceedings of the IEEE, vol. 87, no 7, pp. 1079 – 1107.

Hopper, N., and Von L., A. (2001). Public Key Steganography, Eurocrypt 2001

Hopper, N., Langford, J., and Von L., A. (2002). Provably Sceure Steganography, In Moti Young, editor, Advances in Cryptography, Crypto 2002, Proceeding, vol 2442 of LNCS, Springer-Verlag,

Hsu C. T. and Wu J. L., (1998), DCT-Based Watermarking for Video, IEEE Trans Consum Electronic, 44, pp 206-216

Izquierdo, E., Kim, H. J., and Macq, B. (2003). Introduction to the Special Issue on Authentication, Copyright Protection, and Information Hiding. IEEE Transaction on Circuits and Systems for Video technology, 13(8), pp. 729-731.

Jin, H.L. Fujiyoshi, M., and Kiya, H (2007). Lossless Data Hiding in the Spatial Domain for High Quality Images. IEICE Transaction Fundamental. E90-A, 4, p. 771-777.

Johnson, N. F., and Jajodia, S., (1998). Exploring Steganography: Seeing the Unseen. February. IEEE Computer. 26-64.

Johnson, N. F., Duric, Z., and Jajodia, S., (2001), Information Hiding: Steganography and Watermarking – Attacks and Countermeasures, Kluwer Academic Publishers.

Jong, C. H., Kim, H. (2000), Steganalysis on BPCS Steganography, Centre for Information Security Technologies, Korea University.

Kahn, D, (1996), The Code Breakers, 2nd Edition, Macmillan New York.

Kamata, S, Eason, R.O, and Kawaguchi, E. (1995). Depth-First Coding for Multi-valued pictures using bit plane decomposition', IEEE Trans. on Comm, vol 43, no 5 pp 1961-1969.

Katzenbeisser, S. and Petitcolas, F. A. P. (2000), Information Hiding Techniques for Steganography and watermarking, Norwood, MA:Artech House, 2000.

Katzenbeisser, S and Petitcolas, F. (2002). On defining security in Steganography Systems.

Kawaguchi E., Taniguchi, R. (1986). Complexity of Binary Picture and Image Thresholding – An application of DF-Expression to the Tresholding Problem', Proceeding of 8th ICPR, vol 2 pp. 1221-1225.

Kawaguchi, E., Eason, R. (1998) Principle and Application of BPCS-Steganography, SPIE's International Symposium on Voice, Video and Data Communication.

Kawaguchi, E. and Taniguchi, (1989). The DF-Expression as an Image Thresholding strategy', IEEE Trans. on SMC, vol. 19, no 5,pp. 1321-1328.

Khan, and Muhammad, K. (2011). Research Advances in Data Hiding for Multimedia Security. Multimedia Tools and Applications. v 52, n 2-3, p257-261.

Kerckhoff A., (1988) La Crytographie Militaire, Journal des science militaries, vol IX, pp 5-38, (Translate by Fabien A.P. Petitcolas)

Koch, E., Zho, J. (1995), Embedding Roburst Labels Into Image for Copyright Protection, Proc of Int'l Congress on Intellectual Property Rights for Specialized Information Knowledge & New Technologies, Vienna, 1995.

Lu, T.C., and Huang, Y.H. (2009). An Efficient Block-based lossless Information Hiding Technique. Proceedings of the 3rd International Conference on Ubiquitous Information Management and Communication, ICUIMC'09, p 342-347.

Kao, C. H., and Hwang, R. J., (2005). Information Hiding in Loosy Compression Gray Scale image. Tamkang Journal of Science and Engineering. 8(2): 99-108.

Katzenbeisser, S., and Petitcolas, F. A. P., (2000). Information Hiding Techniques for Steganography and Digital Watermarking. Artech House Computing Library.

Koch E., and Zhao J., (1995), Towards robust and Hidden Image Copyright Labeling, Proc of IEEE Worksyop on Nonlinear Signal and Image Processing, Thessaloniki, Grecce, pp 452-445

Kutter, M., and Hartung, F., (2000). Introduction to Information Technology for Watermarking and Steganography Techniques. Artech House Computing Library.

Lampson B. W., 1973, A note on the confinement problem, Communication of the ACM, 16(10):613-615, October 1973

Lee, Y. K., and Chen, L. H., (2003). Secure error-Free Steganography for JPEG Images. World Scientific Publishing Company, International Journal of Pattern Recognition and Artificial Intelligence. 17(6): 976-981.

Lema, M. D., Mitchell, O., R. (1994), Absolute Moment Block Truncation Coding and it Application to Color Image, IEEE Transaction on Communications, vol COM-32, pp 1148-1157.

Li, S. L., Leung, K. C., and Chan C. K., (2006). Data Hiding in Images by Adaptive LSB Subtitution Based on the Pixel-Valued Differencing. Proceeding of the 1st International Conference on Innovative Computing, Information and Control (ICICIC 06).

Liaw, M. S., and Chen L. H. (1997), An Effective Data Hiding Method, Proc of IPPR Conference on ‘ Computer Vision, Graphics and Image Processing’, Taiwan ROC, pp 146-153.

Lie, W. N., and Chang L. C., (1999). Data hiding in Image with Adaptive Numbers of LSB Based on the Human Visual System. IEEE International Conference on Image Processing, Oct 28: 286-290.

Lin, C. C., and Tsai W. H., (2004). Secret Image Sharing with Steganography and Authentication. Journal of System and Software. Nov (73): 405-414.

Lou, D. C., Liu, J. L. (2002). Steganographic Method for Secure Communication. Computer and Security. June (21): 449-460.

Lu, C. S. (2005). Multimedia Security, Steganography and Digital watermarking Technique for Protection of Intellectual Property. Idea Group Publishing

Massey, J. (1988). An Introduction to Contemporary Cryptology. Proceeding of the IEEE, May 76(5): 533-549.

Maxemchuk, N. F., and Low, S. (1997), Marking Text Documents, in Proc IEEE ICIP 97.

McAndrew, A. (2004). Introduction to Digital Image Processing with Matlab. Thomson Course Technology. ISBN 0534400116.

Megalingam, Rajesh K. N., and Mithun, S.R. (2010). Performance Comparison of Novel Robust Spatial Domain Digital Image Watermarking with the Conventional frequency Domain Watermarking Techniques. International Conference on Signal Acquisition and Processing. P 349-353.

Niimi, M., Noda, H., and Kawaguchi, E. (1997). An Image Embedding in Image by a Complexity Based Region Segmentation Method' ICIP 97, Vol 3 pp 74-77.

Mittelholzer. (1998). An Information-theoretic Approach to Steganography and Watermarking, In A Pfitzmann, editor, Proceeding of Third International Worksyop on Information Hiding, volume 1768 of LNCS, Springer-Verlag.

Noda, H, Spaulding J., Shirazi, M. N., and Kawaguchi, E (2002). Application of Bit-Plan Decomposition Steganography to JPEG 2000 Encoded Image. IEEE Signal Processing Letters. 9(12): 410-413.

Ohnishi, J., and Matsui K., (1995), Embedding a seal into a picture under orthogonal wavelet transform, Proc of multimedia 96 (IEEE Press, Piscataway, NJ), pp 514-521

Open Source, Counterintelligence News and Developments, Vol 2, June 1998, Hidden in PlainSight-Steganography Opensource: www. nacic.gov/pubs/news/1998/jun98.html

Open Source, USA Today, 11/03/2001, Researchers: No Secret bin Laden messages on sites, Open source http://www.usatoday.com.life/cyber/tech/2001/10/17/bin-laden-site.html.

Pal S. K, Saxena P. K., Muttoo S.K., Smart Wardens: Smarter Steganography, Proc of the Pacific Rim Workshop on Digital Steganography 2003, Japan Jul 3-4, 2003.

Pan, G., Wu, Z., and Pan, Y., (2002). A Data Hiding Method for Few Color Images. Proceeding of IEEE International Conference on Acoustic, Speech, and Signal Processing (ICASSP 02). 13-17 May. Orlando, Florida: 3469-3472.

Peter Wyner, (2002), Disappearing Crytography, Information Hiding : Steganography & Watermarking, 2nd Edition, Morgan Kaufman Publishers, 2002.

Petitcolas, F. A. P., Anderson, R. J., and Kuhn, M. G. (1999). Information Hiding : A Survey, Proc of IEEE 87(7): 1062-1078.

Pfitman A., editor, Proceeding of Third International Woksyop on Information Hiding, Dresden, Germany, September/October 1999, Springer-Verlag.

Pfitzmann, B. Information Hiding terminology, (1996), Proc of First International Woksyop on Information Hiding, Lecture Notes in Computer Science no 1174 (Springer-Verlag, Berlin), pp 347-349.

Potdar, V., and Chang, E. (2004). Grey Level Modification Steganography for Secret Communication. Proceeding of the 2nd IEEE International Conference on Industrial informatics (INDIN2004). 24-26 Jun: Berlin, Germany.

Rabah, K (2004). Steganography – The Art of Hiding Data. Information Technology Journal ISSN 1682-6027. 3(3): 245-269.

Ramkumar, M., (2000). Data Hiding in Multimedia – Theory and Applications. PhD Thesis. January 2000. New Jersey Institute of Technology, Newark, New Jersey.

Reyzin, L. and Russell, S. (2003). More Efficient Provably Secure Steganography, Technical Report, IACR ePrint Archive 2003/093.

Rivest, R. L., Shamir, A., and Adelson, L. M. (1978). A Method for Obtaining Digital Signatures and Public Key Cryptosystems, Communication of the ACM, 21(2): 120-126.

Rosenbaum, R., Schumann, *H.,* (2001), A steganographic Framework for Reference Color Based Encoding and Cover Image Selection, University of Rostock.

Salman, M. (2009), Watermarking and Steganography of 3-D Models. Doctor Philosophy, University of Surrey.

Sayuthi, Azizah, Akram, (1995), Transmission Security – Steganography Approach, International Conference in Defence Technology 2005 proceeding, Malaysia.

Sayuthi Jaafar Mej, (1997), Information System and Future Warfare, UM-MTAT Research Paper, 1997.

Schneier, B., (1996). Applied Cryptography. (2nd Edition). New York, NY: John Wiley & Sons, Inc.

Schyndel, R. G. V., Tirkel A. Z., and Osborne, C. F. (1994), A Digital Watermark, in Proc IEEE Int Conf Image Processing, vol 2 1994 pp 86-90.

Sekgwathe, Virginiah Talib, and Mohammad (2011). Cyber Crime Detection and Protection: Third World Still to Cope-up. Communications in Computer and Information Science, v 171 CCIS, P 171-181.

Shor, P. W. (1994). Algorithm for Quantum Computation: Discrete Algorothm and Factoring, In IEEE Symposium on Foundation of Computer Science, pages 124-134.

Simmons G.J., 1984, The prisoner's problem and the subliminal channel. In David Chaum, editor, Advances in Cryptography, Proceeding of Crypto'83, pages 51-70, New York, USA, 1984, Plenum Publishing

Simmon, G.J, (1992). Contemporary Cryptography: The Science of Information Integrity. Piscatoway, NJ: IEEE Press.

Simmons, G. J., 1996, The History ofSubliminal Channels. In R Anderson, editor, Information Hiding, Fist International Woksyop on Data Hiding, LNCS 1174, pages 237-256, Spinger_Verlag, 1996, Cambridge, UK, May 30-Jun 01.

Simon Singh, (1999), Code Book : The Secret History of Codes and Code Breaking, Irish Times.

Swanson, M., Kobayashi, M., and Tewfik, A. (1998), Multimedia Data Embedding and Watermarking Technology, Proceeding of IEEE, vol 86, No 6, pp 1064-1087.

The Oxford English Dictionary (1993): being a corrected re-issue, Clarendon Press, Oxford.

Thien, C. C., and Lin, J. C., (2003). A simple and High Capacity Method for Hiding Digit-by-Digit Data in Image Based on Modulus Function. Pattern Recognition. 36(12): 2875-2881.

Tsai, P., Hu, Y. C., and Chong, C. C. (2002), An Image Hiding Technique Using Block Truncation Coding, Proc of Pacific Rim Workshop on Digital Steganography 2002, pp 55-64.

Tseng, Y. C., Chen, Y. Y., and Pan, H. K. (2002), A Scure Data Hiding Scheme for Binary Images, IEEE Transactions on Communication, vol 50, no 8.

Tirkel A.Z., Rankin G. A., Schyndel R. G. V., Ho W. J., Mee N. and Osborne C. F., 1993 Electronic Watermark, in Digital Image Computing, Technology and Applications (DICTA '93), Sidney, Australia, 1993, pp 666-673

USA Today, 11/03/2001, Researchers: No Secret bin Laden messages on sites, Open source http://www.usatoday.com.life/cyber/tech/2001/10/17/bin-laden-site.html.

Venkatraman, S., Abraham, A., and Paprzycki, M. (2004). Significance of Steganography on Data Security. Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC 04). IEEE Computer Security.

Wang, C. C., Tsai, S. C., and Yu, C. S., (2000). Repeating Image Watermarking Technique by the Visual Cryptography. IEICE Trans. Fundamental. August E83-A(8): 1589-1598.

Wang, C. M., Wu, N. I., Tsai C. S., and Hwang, M. S., (2008). A High Quality Strganography Method with Pixel-Value Differencing and Modulus Function. The Journal of System and Software. 81:150-158.

Wang H., Wang S., (2004), Cyber Warfare: Steganography vs Steganalysis, Communication of the ACM, vol 47.

Wang, S. J., (2005). Steganography of Capacity Required Using Modulo Operator for Embedding Secret Image. Applied Mathematics and Computation. January. 164: 99-116.

Wang, Z., Bovik, A.C., Sheikh, H. R. and Simoncelli, E.P. (2004), Image Quality Assessment: From Error Visibility to Structural Similarity, IEEE Transaction on Image Processing.

Westfeld, A., and Pfitzmann, A.,(2000). Attack on Steganography Systems. Proceeding of 3rd International Workshop on Information Hiding. In: Lecture Notes in Computer Science. Springer-Verlag, Berlin, 1768:61-75.

Wu D. C., and Tsai, W., H. (2000), Spatial- domain Image Hiding using Image Differencing, IEEE Proc Visual Image Signal Process, Vol 147, no 1, Feb 2000, pp 29-37.

Wu, D. C., and Tasi, W. H., (2003). A Steganographic Method for Images by Pixel-Value Differencing. Pattern Recognition Letters. 24(9-10):1613-1626.

Wu, H. C., Wu, N. I., Tsai, C. S., and Hwang M. S., (2005). Image Steganographic Scheme Based on Pixels-value Differencing and LSB Replacement Methods. IEEE Proceeding of Visual Image Signal Processing. Oct 152:611-615.

Wu M. and Lee J. H., (1998) A Novel Data Embedding Method For Two-Color Facsimile Images, in Proc Int Symp Multimedia Inform Processing, Chung-Li, Taiwan, ROC.

Wu M., Liu B., (2003), Data Hiding in Image and Video: Part 1 – Fundamnetal Issues and Solution and Part 2 – Design and Application, IEEE Trans Image Processing, vol 12, pp 685-695 and 696-705.

Wu, M., and Liu, B. (2004). Data Hiding in Binary Image for Authentication and Annotation’ IEEE Transactions on Multimedia, Vol 6 No 4.

Wu M., Tang E. and Liu B, (2000), Data Hiding in Digital Binary Images, Proc IEEE Int’l Conference on Multimedia and Expo, New York.

Yang, Z., (2003). Dual Domain Semi-fragile Watermarking for Image Authentication. Master Thesis, University of Toronto, Canada.

Yeuan, K. L., and Ling, H. C., (2000). High Capacity Image Steganographic Model. IEE Proceeding of Visual and Signal Processing. June 147(3).

Yu, Y. H., Chang, C. C., and Hu, Y. C., (2005). Hiding Secret Data in Images via Predictive Codding. Pattern Recognition. May. 38: 691-705.

Zebbiche, K. (2009). Data Hiding for Securing Fingerprint Data Access. Doctor Pholosophy, Queen's University Belfast.

Zeki, A.M., Azizah, A. M., and S. S. (2011). High Watermarking Capacity Based on Spatial Domain Technique. Information Technology Journal. V10, n7, p 1367-1373.

Zeki, A.M., (2009). Watermarking Techniques Using Intermediate Significant Bit. Doctor Philosophy, Faculty of Computer Science and Information System, University Technology Malaysia.

Zhang, X and Wang S., (2004). Vulnerability of Pixel-Value differencing Steganography to Histogram analysis and Modification for Enhanced Security. Pattern Recognition Letters, 25: 331-339.

Zhang, X., Zhang, F., and Xu, Y. (2011). Quality Evaluation of Digital Image Watermarking. Lecture Note in Computer Science (including in subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). V 6676 LNCS, n PART 2, p 241-250.

Zheng, D., Liu, Y., Zhao, J. and Saddik, A. E. (2007). A Survey of RST Invariant Image Watermarking Algorithms. ACM Computing Survey, 39.

Zollner, J., Federrath, H., Klimant, H., Pfitzmann, A., Piotraschke, R. Westfeld, A., Wicke, G. and Wolf, G. (1998). Modelling the Security of Steganography Systems, In Information Hiding, pages 344-354.