DATA HIDING TECHNIQUES IN STEGANOGRAPHY USING FIBONACCI SEQUENCE AND KNIGHT TOUR ALGORITHM

MOHAMMED ABDULLAH KHALAF

UNIVERSITI TEKNOLOGI MALAYSIA

DATA HIDING TECHNIQUES IN STEGANOGRAPHY USING FIBONACCI SEQUENCE AND KNIGHT TOUR ALGORITHM

MOHAMMED ABDULLAH KHALAF

A project report submitted in partial fulfilment of the
requirements for the award of the degree of
Master of Engineering (Computer & Microelectronics System)

Faculty of Electrical Engineering
Universiti Teknologi Malaysia

JUNE 2016

To my virtuous supervisor who taught me in a truthful, fair, and honorable way

To my colleagues in the Universiti Teknologi Malaysia

To all those who contributed to the success of this research

I dedicate this research to you

ACKNOWLEDGEMENT

Initially, all praise is to Allah, the most kind and the merciful for helping me to accomplish this study. Special appreciation goes to my parents, friends, studying colleagues and supervisors for standing beside me in the good and bad times spent to complete this research. The great effort goes to Dr. Nasrul Humaimi Mahmood for support me to complete this research praying to Allah Almighty to grant him all that is good.

ABSTRACT

The foremost priority in the information and communication technology era, is achieving an efficient and accurate steganography system for hiding information. The developed system of hiding the secret message must capable of not giving any clue to the adversaries about the hidden data. In this regard, enhancing the security and capacity by maintaining the Peak Signal-to-Noise Ratio (PSNR) of the steganography system is the main issue to be addressed. This study proposed an improved for embedding secret message into an image. This newly developed method is demonstrated to increase the security and capacity to resolve the existing problems. A binary text image is used to represent the secret message instead of normal text. Three stages implementations are used to select the pixel before random embedding to select block of (64 × 64) pixels, follows by the Knight Tour algorithm to select sub-block of (8 × 8) pixels, and finally by the random pixels selection. For secret embedding, Fibonacci sequence is implemented to decomposition pixel from 8 bitplane to 12 bitplane. The proposed method is distributed over the entire image to maintain high level of security against any kind of attack. Gray images from the standard dataset (USC-SIPI) including Lena, Peppers, Baboon, and Cameraman are implemented for benchmarking. The results show good PSNR value with high capacity and these findings verified the worthiness of the proposed method. High complexities of pixels distribution and replacement of bits will ensure better security and robust imperceptibility compared to the existing systems in the literature.

ABSTRAK

Keutamaan pertama di dalam maklumat dan komunikasi dalam era teknologi, adalah mencapai sistem steganografi yang cekap dan tepat untuk menyembunyikan maklumat. Sistem yang dibangunkan menyembunyi mesej rahsia, mestilah mampu tidak memberi apa-apa petunjuk kepada musuh mengenai data tersembunyi. Dalam hal ini, meningkatkan keselamatan dan kapasiti dengan mengekalkan Nisbah Puncak Isyarat-Hingar (PSNR) sistem steganografi adalah isu utama yang perlu ditangani. Kajian ini mencadangkan lebih baik untuk menerapkan mesej rahsia ke dalam imej. Kaedah yang baru dibangunkan menunjukkan kebolehan untuk meningkatkan keselamatan dan keupayaan untuk menyelesaikan masalah yang sedia ada. Satu imej teks binari digunakan untuk mewakili mesej rahsia dan bukannya teks normal. Tiga peringkat pelaksanaan digunakan untuk memilih piksel sebelum membenam secara rawak untuk memilih blok (64 × 64) piksel, diikuti oleh algoritma *Knight Tour* untuk memilih sub-blok (8 × 8) piksel, dan akhirnya dengan pemilihan piksel secara rawak. Turutan *Fibonacci* digunakan untuk penguraian piksel dari 8 bitplan ke 12 bitplan untuk membenam maklumat secara rahsia. Kaedah yang dicadangkan diaplikasikan ke seluruh imej untuk mengekalkan tahap keselamatan yang tinggi terhadap sebarang serangan. Imej kelabu dari set data piawai (USC-SIPI) termasuk *Lena*, *Peppers*, *Baboon* dan Jurukamera dilaksanakan sebagai penanda aras. Keputusan menunjukkan nilai PSNR baik dengan kapasiti tinggi dan penemuan ini mengesahkan kebenaran tentang kaedah yang dicadangkan. Kerumitan tinggi taburan piksel dan penggantian bit akan memastikan keselamatan yang lebih baik dan lebih teguh berbanding dengan sistem yang sedia ada.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

DCT	-	Discrete Cosine Transform
DE	-	Difference Expansion
DFT	-	Discrete Fourier Transform
EMD	-	Exploiting Modification Direction
FFT	-	Fractional Fourier Transform
GA	-	Genetic Algorithm
HDWT	-	Haar Discrete Wavelet Transform
HVS	-	Human Visual System
JPEG	-	Joint Photographic Experts Group
KT	-	Knight Tour
LSB	-	Least Segnificant Bit
LZW	-	Lempel Ziv Welch
MSB	-	Most Significant Bit
OPAP	-	Optimal Pixels Adjustment Process
PDF	-	partial difference equation
PND	-	Random
PoV	-	Pairs of Values
PSNR	-	Peak Signal-to-Noise Ratio
PVD	-	Pixel Value Differencing
RGB	-	Red, Green and Blue
RPE	-	Random Pixel Embedding
SIS	-	Steganography Image System
TCP/IP	-	Transmission Control Protocol/Internet Protocol
WFFT	-	Weight Fractional Fourier Transform

LIST OF SYMBOLS

e	-	Exponential
u	-	New x Pixel
v	-	New y Pixel
π	-	Pi Mathematical Constant

CHAPTER 1

INTRODUCTION

1.1 Introduction

In the last decade, problems related to the security of hiding information have received considerable attention. Lately, security of hiding data in images has become attractive to the vision community due to widespread application domain in diversified fields of studies particularly in image security and steganography.

Current study addresses some key issues related to security in terms of understanding related to the great unsolved problems of data embedding in an image. A comprehensive solution is expected to open tremendous application possibilities ranging from medical (Aroukatos, N., *et al.*, 2016; Fathimal, P., and Rani, P. 2016) to military (Tuncer, T., and Avci, E., 2016). Presently, the major difficulties relate to the lack of (a) increasing the security of data hiding, (b) payload capacity because the existing one typically has limited data capacity to embed, and (c) maintaining the robustness of the system while increasing the security.

Since the rise of the internet one of the most important factors of information communication is the security of the information. Many methods have been developed in the literature in order to keep the message secret. Information hiding is the practice of concealing messages or information within other non-secret images or data, and it is synonymous with the word steganography.

There are many types of information hiding, as information can be hidden in a text, image, video, audio, or protocol. Each has its pros and cons. On the other hand, most media on the internet use images due to availability and ease of use (Singh, S., *et al*., 2016). Thus hiding information in the image gains more facilities in terms of reliability, capacity, and the ability to hide information without being observed by intruder. Hiding text into images is called steganography, and there are many types of data to be hidden in different host media as shown in Figure 1.1.

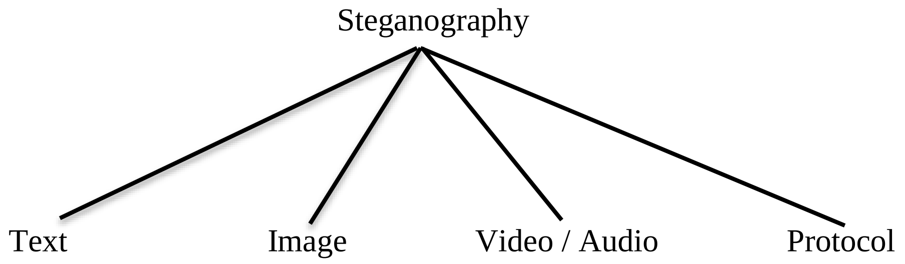

Figure 1.1 Steganography domain

Steganography is the art of hiding sensitive data like text within media in a manner that is not visible or noticeable. Images are used as hosting media because of the ability to absorb large amounts of data and the difficulty of intruders to observe this data.

1.2 Problem background

Most of the effort devoted to hiding information in order to secure the system as best as possible in a way that keeps the image that contain the hidden message is eye-catching. Several approaches are proposed for image steganography (Gupta J., 2015; Rai, P., *et al*., 2015). However, hiding data in carrier image has attracted great interest in terms of security; in contrast, other media like text and protocol are mostly ignored. Security, capacity, and embedding methods remain far from being achieved and research in these fields is ongoing. These issues are discussed in the following sections.

1.2.1 Security Issues in Steganography

Currently, the internet plays a vital role in the field of data transmission and communication. More than ever, data security is required due to privacy issues, as information transmitted over the World Wide Web is sensitive including medical diagnostics, financial, and military information, thus the need for some mechanism for protection from outsiders or intruders. (Rai, P., *et al*., 2015; Sedighi, V., *et al*., 2016; Rani, M., *et al.*, 2016). Due to the popularity of using images in many applications, images have become a very accepted choice among other existing media to host the secret message. Security of the data embedded based on the method that handles the secret message inside the cover image, and the security issue remains an outstanding challenge. At present attackers have become more expert and have more knowledge about security, thus finding or developing new techniques has become a problem that deserves attention in order to safeguard the sending of information between acknowledged parties (Amritha, P., *et al.*,2016).

1.2.2 Embedding Method Issues in Steganography

Reducing the amount of secret message embedded to the system has led to improve the security of a steganography system via reducing bits in the cover image. This happen when secret bits are significantly less than available bits in the hosting image (Al-Dmour, H. and Al-Ani, A., 2016; Kuo, W., 2016). The researches on steganography and steganalysis have attracted more interest during past decade (Vikranth, B.*et al.*, 2015; Rai, P.*et al.*, 2015). Despite the fact that steganography system only considers the bits to be of little importance, there are remains a trace that can be detected by attacks. From this point of view it is easy to imagine the importance of embedding method and how users should be cautious.

Many of the methods introduced in literature regarding embedding secret message all follow the same direction in terms of placing of embedding in digital hosting image. The best place to embed a secret in an image is Least Significant Bit (LSB) (Akhtar, N. 2016). There are many advantages for using LSB e.g. simple to understand and easy to use, and the main issue is that LSB cannot be noticed by the naked eye and allows high payload capacity for secret message. Each method suggested in literature has advantages and disadvantages in terms of special domain, and one of these methods is LSB (Shelke, S. and Jagtap, S. 2015) as shown in Figure 1.2.

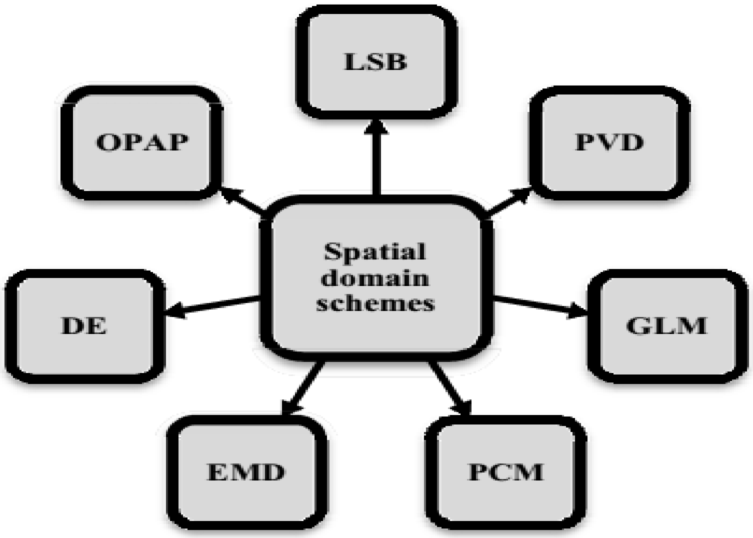

Figure 1.2 Embedding methods for spatial domain

1.2.3 Capacity

A good steganography technique aims to provide capacity, which is defined as the maximum secret information that can be embedded into cover image (Akhtar, N., *et al.*, 2016). One of the weaknesses effecting steganography system is capacity. In the proposed system, LSB method is used for embedding the data. This method actually uses only one bit of the pixel to embed in. To solve this problem Huffman coding (Sun, S., 2016) is used to compress the secret message before embedding. Increasing the capacity payload in cover image is critical, because when evaluating the method by one of the staganalytic methods (chi-square) which perform statistical analysis on embedding data, increasing capacity makes the stego image weak against attacks. Two types of attack considered in this study are very important. First, Chi-square (X^2) (Al-Dmour, H., and Al-Ani, A. 2016) where an attack is sensitive to payload capacity because statistical analysis of the image, and the second is Human Visual System (HVS) (Zargar, A., and Singh, A., 2016) where an attack is sensitive to exchanging in LSB.

Increasing secret data payload capacity in stego image also effects the robustness of the system. In conclusion, the background problem of increasing the capacity of secret message is no easy task and a balance must be kept between security and robustness.

1.3 Steganography model

Steganography refers to the method used to hiding data in digital hosting media to hide the presence of the information. Stego image is the image with hidden information inside while cover image is the image without hidden information and ready to handle it. Some security problems arise with steganography for illegal data embedded via terrorists when the terrorist information used is spread around (Amritha, P., *et al.*, 2016; Li, B., *et al.*, 2011). Steganography in the modern day refers to data or files that have been hidden inside digital image which cannot be detected by human senses. There are two parties using steganography; the sender which sends the stego image with stego key and the receiver which extracts this stego image according to information inside stego key (Seyyedi, S., *et al.*,2016). A good model is one that has maintained the stego image and received this stego image without any doubt of attack and intrusion. Figure 1.3 shows the model of steganography.

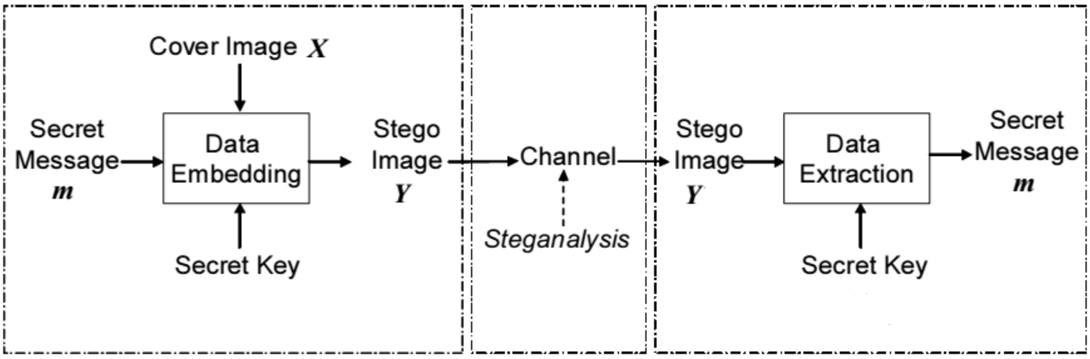

Figure 1.3 The model of steganography and steganalysis

Adoption of a strong and safe method for embedding data in stego image makes the steganography model more robust and suitable. Secret key, sometimes called stego key, includes all the information needed for extracting secret data from stego image. Any weakness in one stage of this model will render the entire model ineffective.

1.4 Problem Statements

Some researchers in literature introduced different methods for hiding secret information in image, or in other words, new steganography system has been developed (Hamed, G., *et al.*, 2016; Rai, P., *et al.*, 2015). In this research, the focus is on embedding secret message in reliable hosting image. There are three main problems:

i. How to increase the capacity of the system while maintaining the Peak Signal-to-Noise Ratio (PSNR).
ii. How to embed the payload capacity of secret message.
iii. How to maintain the robustness and imperceptibility of the system.

In order to answer these primary questions, a set of secondary research questions that address the problem in detail are posed as follows:

i. How to design and development the basic model of a steganography system to be more secure with keeping the PSNR as high.
ii. How to improve the steganography system with high capacity?
iii. How to evaluate and test steganography system using standard and self-created images.

In this study Fibonacci decomposition is used to increase capacity, security and robustness of the system. To improve security the knight tour algorithm used for embedding secret message. Three types of evaluation are used to evaluate the results including PSNR, Chi-square attack, and HVS attack, all with different criteria.

1.5 Objectives of the Study

The main goal of this research is to increase capacity using Fibonacci sequence and to improve the security of hiding information in an image by using new embedding method based on knight tour algorithm. Therefore, this thesis is carried out in order to fulfil the following objectives:

i. To propose steganography algorithm based on simple LSB technique and knight tour embedding method.
ii. To increase security using knight tour algorithm.
iii. To evaluate the robustness of the proposed method against Chi-square attack.

Due to the spread of Internet and its applications that require security information and widely used digital images through the internet, developing a new security system is of utmost necessity especially with the applications that use images. It is worth developing such a system that considers the use of highly secret message capacity inserted in trusted media. Many applications at the present time used images as a main factor, and for this reason, this research tries to come up with a new technique to serve these applications.

1.6 Scope of the Study

The proposed method scope is based on the following points:

i. The cover media that is used for hiding the desired secret data is a standard dataset of (512 x 512) pixels, and 8-bits gray-scale image taken from the data base of USC-SIPI. Manipulation of the image such as rotation, zooming, scaling, etc. is not considered in this study.

ii. PSNR formula will be used to evaluate the imperceptibility of stego-image in order to compare with previous works.

iii. Chi-sqaure will be used to evaluate the robustness of the proposed technique.

iv. Proposed algorithm applied by using MatLab R2013a.

1.7 Significance of the Study

Since the expansion in the application of the Internet and wide depending on the internet resources, the World Wide Web has today become non secure in the transmission of data, so they need to make this environment safer has become more urgent and to achieve a secure environment, the implementation of some security technologies has become valuable.

Steganography, being a more secure technology, has been applied to get a secure communication channel between the sender and the receiver using the internet as a communication medium. Since Steganography is under some vulnerability such as, payload capacity is one of the most important factors in addition to the imperceptibility of the stego-image. It will be able to increase the security of such system and high PSNR at the same time. Furthermore it is expected to minimize problems associated with payload capacity dependency. Existing studies on steganography system revealed some methods that are lacking in embedding (Vikranth, B., *et al.*, 2015; Rai, P., *et al.*, 2015), however, proposed method got encouraging result in terms of security and capacity. Currently, numerous applications aim to use image steganography especially in security, medical, military, and industries fields. Security, capacity, and robustness are the main weaknesses in any steganography system and this method is believed to overcome such shortcoming.

1.8 Thesis Overview

This project report is organized in five chapters, each chapter illustrate the dissection and details related with this study. Chapter 1 include the introduction, problem background, objective, significant of the study, also its provide briefing introduction of the field study and specification. In Chapter 2, we present an overview of the data hiding technique in general followed by principles of steganography techniques and some classification on image hiding. The advantages and weaknesses of each study are discussed. In Chapter 3, the research methodology and the full framework and explained in detail. In Chapter 4, we explain the evaluation criteria for steganography system and PSNR evaluation and presents a results of chi-square attack and HVS attack and all the results of the proposed methods are evaluated in this chapter, whereas in Chapter 5, we summarize our contributions and discuss limitations and future work.

REFERENCES

Agrawal, S., and Kumar, M. (2016). An Improved Reversible Data Hiding Technique Based on Histogram Bin Shifting. In *Proceedings of 3rd International Conference on Advanced Computing, Networking and Informatics* (pp. 239-248). Springer India.

Akhtar, N. (2016). An Efficient Lossless Modulus Function Based Data Hiding Method. In *Proceedings of 3rd International Conference on Advanced Computing, Networking and Informatics* (pp. 281-287). Springer India.

Akhtar, N. (2016). An LSB Substitution with Inversion Steganography Method. In *Proceedings of 3rd International Conference on Advanced Computing, Networking and Informatics* (pp. 515-521). Springer India.

Al-Ataby, A., and Al-Naima, F. (2008). A modified high capacity image steganography technique based on wavelet transform. *changes*, *4,* 6.

Al-Dmour, H., and Al-Ani, A. (2016). A steganography embedding method based on edge identification and XOR coding. *Expert Systems with Applications*, *46*, 293-306.

Al-Tamimi, A. G. T., and Alqobaty, A. A. (2015). Image Steganography Using Least Significant Bits (LSBs): A Novel Algorithm. *International Journal of Computer Science and Information Security*, *13*(1), 1.

Amritha, P. P., Induja, K., and Rajeev, K. (2016). Active Warden Attack on Steganography Using Prewitt Filter. In Proceedings of the International Conference on Soft Computing Systems (pp. 591-599). Springer India.

Amritha, P. P., Muraleedharan, M. S., Rajeev, K., and Sethumadhavan, M. (2016). Steganalysis of LSB Using Energy Function. In *Intelligent Systems Technologies and Applications* (pp. 549-558). Springer International Publishing.

Anandpara, D., and Kothari, A. (2015). Working and Comparative Analysis of Various Spatial Based Image Steganography Techniques. *International Journal of Computer Applications*, *113*(12), 8-12.

Aroukatos, N. G., Manes, K., and Zimeras, S. (2016). Social Networks Medical Image Steganography Using Sub-Fibonacci Sequences. In *mHealth Ecosystems and Social Networks in Healthcare* (pp. 171-185). Springer International Publishing.

Baig, F., Khan, M. F., Beg, S., Shah, T., and Saleem, K. (2016). Onion steganography: a novel layering approach. *Nonlinear Dynamics*, 1-16.

Bansal, A., Muttoo, S. K., and Kumar, V. (2015). Secure Data Hiding by Optimal Placement of Queen Along Closed Knight Tour. i-Manager's Journal on Information Technology, 4(3), 18.

Bansal, A., Muttoo, S. K., and Kumar, V. (2016). Secure Data Hiding Along Randomly Selected Closed Knight's Tour. *Journal of Applied Security Research*, *11*(1), 90-100.

Barr, K. C., and Asanović, K. (2006). Energy-aware lossless data compression. ACM Transactions on Computer Systems (TOCS), 24(3), 250-291.

Bhatt, S., Ray, A., Ghosh, A., and Ray, A. (2015, January). Image steganography and visible watermarking using LSB extraction technique. In*Intelligent Systems and Control (ISCO), 2015 IEEE 9th International Conference on* (pp. 1-6). IEEE.

Bhattacharya, D., Chakraborty, S., Roy, P., Kairi, A., and IEM, K. (2015). An Advanced Dictionary Based Lossless Compression Technique for English Text Data. *Biometrics and Bioinformatics*, *7*(1), 4-11.

Böhme, R. (2010). Principles of Modern Steganography and Steganalysis. In*Advanced Statistical Steganalysis* (pp. 11-77). Springer Berlin Heidelberg.

Botta, M., Cavagnino, D., and Pomponiu, V. (2016). A modular framework for color image watermarking. *Signal Processing*, *119*, 102-114.

Bower, A., Insoft, R., Li, S., Miller, S. J., and Tosteson, P. (2015). The distribution of gaps between summands in generalized Zeckendorf decompositions. *Journal of Combinatorial Theory, Series A*, *135*, 130-160.

Bucerzan, D., and Raţiu, C. (2016). Image Processing with Android Steganography. In *Soft Computing Applications* (pp. 27-36). Springer International Publishing.

Budiman, G., and Novamizanti, L. (2015). White Spacesteganography On Text By Usinglzw-Huffman Double Compression.*International Journal of Computer Networks and Communications*, *7*(2), 136A.

Chakravarthy, S., Sharon, V., Balasubramanian, K., and Vaithiyanathan, V. (2016). Art of Misdirection Using AES, Bi-layer Steganography and Novel King-Knight's Tour Algorithm. In *Advances in Signal Processing and Intelligent Recognition Systems* (pp. 97-108). Springer International Publishing.

Chandran, S., and Bhattacharyya, K. (2015, January). Performance analysis of LSB, DCT, and DWT for digital watermarking application using steganography. In Electrical, Electronics, Signals, Communication and Optimization (EESCO), 2015 International Conference on (pp. 1-5). IEEE.

Chang, C. C., Chen, T. S., and Chung, L. Z. (2002). A steganographic method based upon JPEG and quantization table modification. *Information Sciences*,*141*(1), 123-138.

Channalli, S., and Jadhav, A. (2009). Steganography an art of hiding data.*arXiv preprint arXiv:0912.2319*.

Charbal, A., Dufour, J. E., Guery, A., Hild, F., Roux, S., Vincent, L., and Poncelet, M. (2016). Integrated Digital Image Correlation considering gray level and blur variations: Application to distortion measurements of IR camera. *Optics and Lasers in Engineering*, *78*, 75-85.

Chary, A. S. (2016) "Invisible Image Watermarking Using Hybrid DWT Compression-Decompression Technique".

Chen, P. Y., and Lin, H. J. (2006). A DWT based approach for image steganography. *International Journal of Applied Science and Engineering*,*4*(3), 275-290.

Das, P., Kushwaha, S. C., and Chakraborty, M. (2015, February). Multiple embedding secret key image steganography using LSB substitution and Arnold Transform. In *Electronics and Communication Systems (ICECS), 2015 2nd International Conference on* (pp. 845-849). IEEE.

Das, S. K., and Dhara, B. C. (2015, April). An Image Secret Sharing Technique with Block Based Image Coding. *In Communication Systems and Network Technologies (CSNT), 2015 Fifth International Conference on* (pp. 648-652). IEEE.

Deval, N. M. (2015) Secure Steganography Algorithm Based on Cellular Automata using Fibonacci Representation and Reverse Circle Cipher Application for Steganography.

Dooley, J. F. (2015). Review of Prisoners, Lovers, and Spies by Kristie Macrakis. *Cryptologia*, 1-6.

El-Emam, N. N., and Al-Diabat, M. (2015). A novel algorithm for colour image steganography using a new intelligent technique based on three phases.*Applied Soft Computing*, *37*, 830-846.

Fathimal, P. M., and Rani, P. A. J. (2016). K Out of N Secret Sharing Scheme with Steganography and Authentication. In *Computational Intelligence, Cyber Security and Computational Models* (pp. 413-425). Springer Singapore.

Fridrich, J., and Goljan, M. (2003, June). Digital image steganography using stochastic modulation. In *Electronic Imaging 2003* (pp. 191-202). International Society for Optics and Photonics.

Fridrich, J., Goljan, M., and Du, R. (2001, October). Reliable detection of LSB steganography in color and grayscale images. In *Proceedings of the 2001 workshop on Multimedia and security: new challenges* (pp. 27-30). ACM.

Ghasemi, E., Shanbehzadeh, J., and Fassihi, N. (2011, March). High capacity image steganography using wavelet transform and genetic algorithm. In*Proceedings of the international multiconference of engineers and computer scientists* (Vol. 1).

Ghebleh, M., and Kanso, A. (2014). A robust chaotic algorithm for digital image steganography. *Communications in Nonlinear Science and Numerical Simulation*, 19(6), 1898-1907.

Gupta, J. (2015). A Review on Steganography techniques and methods.

Gutub, A., Al-Qahtani, A., and Tabakh, A. (2009). Triple-A: Secure RGB image steganography based on randomization.

Hegde, R. and Jagadeesha S., 2015 "Design and Implementation of Image Steganography by using LSB Replacement Algorithm and Pseudo Random

Encoding Technique". *International Journal on Recent and Innovation Trends in Computing and Communication*, Volume: 3 Issue: 7.

Herrigel, A., Voloshynovskiy, S. V., and Hrytskiv, Z. D. (2000, June). Optical/digital identification/verification system based on digital watermarking technology. In *International Workshop on Optoelectronic and Hybrid Optical/Digital Systems for Image/Signal Processing* (pp. 170-176). International Society for Optics and Photonics.

Holub, V., and Fridrich, J. (2013, June). Digital image steganography using universal distortion. In *Proceedings of the first ACM workshop on Information hiding and multimedia security* (pp. 59-68). ACM.

Huang, F., and Kim, H. J. (2016). Framework for improving the security performance of ordinary distortion functions of JPEG steganography. *Multimedia Tools and Applications*, 75(1), 281-296.

Huffman, D. A. (1952). A method for the construction of minimum-redundancy codes. *Proceedings of the IRE, 40*(9), 1098-1101.

Ibrahim, R., and Kuan, T. S. (2011). Steganography algorithm to hide secret message inside an image. *arXiv preprint arXiv:1112.2809*.

Islam, M. N., Islam, M. F., and Shahrabi, K. (2015). Robust information security system using steganography, orthogonal code and joint transform correlation. *Optik-International Journal for Light and Electron Optics*, *126*(23), 4026-4031.

Jain, N., Meshram, S., and Dubey, S. (2012). Image Steganography Using LSB and Edge–Detection Technique. *International Journal of Soft Computing and Engineering (IJSCE) ISSN*, *223*.

Jana, B., Giri, D., and Mondal, S. K. (2016). Dual-Image Based Reversible Data Hiding Scheme Using Pixel Value Difference Expansion. *International Journal of Network Security*, *18*(4), 633-643.

Jero, S. E., and Ramu, P. (2016). Curvelets-based ECG steganography for data security. *Electronics Letters*.

Jiang, N., Zhao, N., and Wang, L. (2016). Lsb based quantum image steganography algorithm. *International Journal of Theoretical Physics*, *55*(1), 107-123.

Johnson, N. F., and Jajodia, S. (1998, January). Steganalysis of images created using current steganography software. In *Information Hiding* (pp. 273-289). Springer Berlin Heidelberg.

Kanan, H. R., and Nazeri, B. (2014). A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm. *Expert Systems with Applications*, *41*(14), 6123-6130.

Kaur, A., Dhir, R., and Sikka, G. (2010). A new image steganography based on first component alteration technique. *arXiv preprint arXiv:1001.1972*.

Kaur, S. P., and Jindal S. (2016) "A Review on Various Approaches for Data Hiding.", International Journal of Science and Research.

Khan, S., Ahmad, N., and Wahid, M. (2016). Varying index varying bits substitution algorithm for the implementation of VLSB steganography.*Journal of the Chinese Institute of Engineers*, *39*(1), 101-109.

Kim, C., Yun, S., Jung, S. W., and Won, C. S. (2016). Color and Depth Image Correspondence for Kinect v2. In *Advanced Multimedia and Ubiquitous Engineering* (pp. 333-340). Springer Berlin Heidelberg.

Knapp, J. F., and Worrell, S. W. (2015). *U.S. Patent No. 9,002,134*. Washington, DC: U.S. Patent and Trademark Office.

Kolakalur, A., Kagalidis, I., and Vuksanovic, B. (2016). Wavelet Based Color Video Steganography. *International Journal of Engineering and Technology*,*8*(3), 165.

Kumar, A., Ghrera, S. P., and Tyagi, V. (2016). Modified Buyer Seller Watermarking Protocol based on Discrete Wavelet Transform and Principal Component Analysis. *Indian Journal of Science and Technology*, *8*(35).

Kumar, N. (2016). Steganographic Methods: A Survey on Novel Approaches.*International Journal Of Computer Science And Interdisciplinary Research*, *1*(1).

Kuo, W. C., Chang, S. Y., Wang, C. C., and Chang, C. C. (2016). Secure multi-group data hiding based on gemd map. *Multimedia Tools and Applications*, 1-19.

Kuo, W. C., Wang, C. C., and Hou, H. C. (2016). Signed digit data hiding scheme. *Information Processing Letters*, *116*(2), 183-191.

Laha, S., and Roy, R. (2015, December). An improved image steganography scheme with high visual image quality. *In Computing, Communication and Security (ICCCS), 2015 International Conference on* (pp. 1-6). IEEE.

Lee, K. D., and Hubbard, S. (2015). Heuristic Search. In *Data Structures and Algorithms with Python* (pp. 281-297). Springer International Publishing.

Lee, Y. K., and Chen, L. H. (2000, June). High capacity image steganographic model. In *Vision, Image and Signal Processing, IEE Proceedings* (Vol. 147, No. 3, pp. 288-294). IET.

Li, B., He, J., Huang, J., and Shi, Y. Q. (2011). A survey on image steganography and steganalysis.Journal of Information Hiding and Multimedia Signal Processing, 2(2), 142-172.

Liu, J., Tian, Y., Han, T., Wang, J., and Luo, X. (2016). Stego key searching for LSB steganography on JPEG decompressed image. *Science China Information Sciences*, 1-15.

Lunghi, T., Brask, J. B., Lim, C. C. W., Lavigne, Q., Bowles, J., Martin, A., ... and Brunner, N. (2015). Self-Testing Quantum Random Number Generator.*Physical review letters*, *114*(15), 150501.

Maheswari, S. U., and Hemanth, D. J. (2015). Frequency domain QR code based image steganography using Fresnelet transform. *AEU-International Journal of Electronics and Communications*, *69*(2), 539-544.

Meligy, A. M., Nasef, M. M., and Eid, F. T. (2016). A Hybrid Technique for Enhancing the Efficiency of Audio Steganography.

Mishra, A. (2016). An Approach for Information Hiding Using Inverse Z-Transform and Genetic Algorithm. *JIMET, 1*(1).

Mishra, M., Routray, A. R., and Kumar, S. (2014). High Security Image Steganography with Modified Arnold cat map. *arXiv preprint arXiv*:1408.3838.

Mohamed, M. H., and Mohamed, L. M. (2016). High Capacity Image Steganography Technique based on LSB Substitution Method. *Applied Mathematics and Information Sciences, 10*(1), 259.

Mohapatra, C., and Pandey, M. (2015). A Review on current Methods and application of Digital image Steganography. *International Journal of Multidisciplinary Approach and Studies*, *2*(2).

Morkel, T., Eloff, J. H., and Olivier, M. S. (2005, June). An overview of image steganography. In *ISSA* (pp. 1-11).

Muhammad, K., Ahmad, J., Farman, H., and Jan, Z. (2016). A New Image Steganographic Technique using Pattern based Bits Shuffling and Magic LSB for Grayscale Images. *arXiv preprint arXiv:1601.01386*.

Muhammad, K., Ahmad, J., Farman, H., and Zubair, M. (2015). A novel image steganographic approach for hiding text in color images using HSI color model. *arXiv preprint arXiv:1503.00388*.

Mungmode, S., Sedamkar, R. R., and Kulkarni, N. (2016). An Enhanced Edge Adaptive Steganography Approach Using Threshold Value for Region Selection. *arXiv preprint arXiv:1601.02076*.

Nag, A., Biswas, S., Sarkar, D., and Sarkar, P. P. (2015). Semi Random Position Based Steganography for Resisting Statistical Steganalysis. *IJ Network Security*, 17(1), 57-65.

Nag, A., Singh, J. P., Biswas, S., Sarkar, D., and Sarkar, P. P. (2014). A Huffman Code Based Image Steganography Technique. In *Applied Algorithms* (pp. 257-265). Springer International Publishing.

Nayak, R. (2015). Steganography with BSS-RSA-LSB technique: A new approach to Steganography. *IJSEAT*, *3*(5), 187-190.

Parberry, I. (1997). An efficient algorithm for the Knight's tour problem.*Discrete Applied Mathematics*, *73*(3), 251-260.

Parvez, M. T., and Gutub, A. A. (2008, December). RGB intensity based variable-bits image steganography. In *Asia-Pacific Services Computing Conference, 2008. APSCC'08. IEEE* (pp. 1322-1327). IEEE.

Patel, F. R., and Cheeran, A. N. (2015). Performance Evaluation of Steganography and AES encryption based on different formats of the Image.*Performance Evaluation*, *4*(5).

Patel, K., and Ragha, L. (2015, May). Binary image Steganography in wavelet domain. In *Industrial Instrumentation and Control (ICIC), 2015 International Conference on* (pp. 1635-1640). IEEE.

Patterson, N. M., and Lee, S. F. (2015). Image Steganography.

Philip, A. (2013). A Generalized Pseudo-Knight s Tour Algorithm for Encryption of an Image. *Potentials, IEEE*, *32*(6), 10-16.

Priya, S., and Amritha, P. P. (2016). Information Hiding in H. 264, H. 265, and MJPEG. In *Proceedings of the International Conference on Soft Computing Systems* (pp. 479-487). Springer India.

Raeiatibanadkooki, M., Quchani, S. R., KhalilZade, M., and Bahaadinbeigy, K. (2016). Compression and Encryption of ECG Signal Using Wavelet and Chaotically Huffman Code in Telemedicine Application. *Journal of medical systems*, *40*(3), 1-8.

Rai, P., Gurung, S., and Ghose, M. K. (2015). Analysis of Image Steganography Techniques: A Survey. *International Journal of Computer Applications*, *114*(1).

Raja, K. B., Venugopal, K. R., and Patnaik, L. M. (2006, December). High capacity lossless secure image steganography using wavelets. In *Advanced Computing and Communications, 2006. ADCOM 2006. International Conference on* (pp. 230-235). IEEE.

Ramalingam, M., and Isa, N. A. M. (2015). A steganography approach over video images to improve security. *Indian Journal of Science and Technology*, *8*(1), 79-86.

Ramu, P., and Swaminathan, R. (2016). Imperceptibility—Robustness tradeoff studies for ECG steganography using Continuous Ant Colony Optimization.*Expert Systems with Applications*, *49*, 123-135.

Rani, M. M. S., Mary, G. G., and Euphrasia, K. R. (2016). Multilevel Multimedia Security by Integrating Visual Cryptography and Steganography Techniques. In *Computational Intelligence, Cyber Security and Computational Models* (pp. 403-412). Springer Singapore.

Rao, C. S., and Devi, V. B. (2016). Comparative Analysis of HVS Based Robust Video Watermarking Scheme. In *Microelectronics, Electromagnetics and Telecommunications* (pp. 103-110). Springer India.

Rasheed, Z. A. S. (2015). ’Steganography Technique for Binary Text Image. International Journal of Science and Research (IJSR) ISSN (Online), 2319-7064.

Rayappan, J. B. B. (2013). Kubera kolam: A way for random image steganography. *Research Journal of Information Technology*, 5(3), 304-316.

Sanguinetti, B., Traverso, G., Lavoie, J., Martin, A., and Zbinden, H. (2016). Perfectly secure steganography: hiding information in the quantum noise of a photograph. *Physical Review A*, *93*(1), 012336.

Sedighi, V., Cogranne, R., and Fridrich, J. (2016). Content-Adaptive Steganography by Minimizing Statistical Detectability. *Information Forensics and Security, IEEE Transactions on*, *11*(2), 221-234.

Seyyedi, S. A., Sadau, V., and Ivanov, N. (2016). A Secure Steganography Method Based on Integer Lifting Wavelet Transform. *International Journal of Network Security*, *18*(1), 124-132.

Shelke, S. G., and Jagtap, S. K. (2015, February). Analysis of Spatial Domain Image Steganography Techniques. In *Computing Communication Control and Automation (ICCUBEA), 2015 International Conference on* (pp. 665-667). IEEE.

Silman, J. Steganography and steganalysis: an overview. Retrieved September, 8, 2007.

Singh, J., Kaur, G., and Garcha, M. K. (2015, June). Review of Spatial and Frequency Domain Steganographic Approaches. In *International Journal of Engineering Research and Technology* (Vol. 4, No. 06, June-2015). ESRSA Publications.

Singh, M., Kakkar, A., and Singh, M. (2015). Image Encryption Scheme Based on Knight's Tour Problem. *Procedia Computer Science*, *70*, 245-250.

Singh, S., and Datar, A. (2015). Improved Hash Based Approach for Secure Color Image Steganography using Canny Edge Detection Method. *International Journal of Computer Science and Network Security* (IJCSNS),15(7), 92.

Singh, S., Singh, R., and Siddiqui, T. J. (2016). Singular Value Decomposition Based Image Steganography Using Integer Wavelet Transform. In *Advances in Signal Processing and Intelligent Recognition Systems* (pp. 593-601). Springer International Publishing.

Srinivasan, B., Arunkumar, S., and Rajesh, K. (2015). A Novel Approach for Color Image, Steganography Using NUBASI and Randomized, Secret Sharing Algorithm. *Indian Journal of Science and Technology*, *8*(S7), 228-235.

Stanley, C. A. (2005). Pairs of Values and the Chi-squared Attack. *Master's Thesis, Department of Mathematics, Iowa State University*.

Sun, S. (2016). A novel edge based image steganography with 2 k correction and Huffman encoding. *Information Processing Letters*, *116*(2), 93-99.

Tang, W., Li, B., Luo, W., and Huang, J. (2016). Clustering Steganographic Modification Directions for Color Components.

Thakur, P., Kushwaha, S., and Rai, Y. (2015). Enhance Steganography Techniques: A Solution for Image Security. *International Journal of Computer Applications*, *115*(3).

Thampi, S. M. (2004). Information hiding techniques: A tutorial review. *ISTE-STTP on Network Security and Cryptography, LBSCE*.

Thanikaiselvan, V., and Arulmozhivarman, P. (2013). Horse Communication against Harsh Attack: A Stego Ride. *Research Journal of Information Technology*, *5*(3), 263-276.

Thanikaiselvan, V., and Arulmozhivarman, P. (2015). RAND-STEG: an integer wavelet transform domain digital image random steganography using knight's tour. *Security and Communication Networks*.

Thomas, E. (2015). *The Fibonacci Sequence Through a Different Lens* (Doctoral dissertation).

Tolba, M. F., Ghonemy, M. S., Taha, I. A. H., and Khalifa, A. S. (2004, July). High capacity image steganography using wavelet-based fusion. In*Computers and Communications, 2004. Proceedings. ISCC 2004. Ninth International Symposium on* (Vol. 1, pp. 430-435). IEEE.

Tuncer, T., and Avci, E. (2016). A reversible data hiding algorithm based on probabilistic DNA-XOR secret sharing scheme for color images. *Displays*,*41*, 1-8.

Tutuncu, K., and Hassan, A. A. (2015). New Approach in E-mail Based Text Steganography. *International Journal of Intelligent Systems and Applications in Engineering*, *3*(2), 54-56.

Udhayavene, S., Dev, A. T., and Chandrasekaran, K. (2015). New Data Hiding Technique in Encrypted Image: DKL Algorithm (Differing Key Length).*Procedia Computer Science*, *54*, 790-798.

Venkatachalam, S., Banu, A. S., and Padmaa, M. (2015). A Robust Image Steganography using CDF Lifting Scheme and Huffman Encoding.*International Journal of Computer Applications*, *110*(11).

Venugopal, D., Mohan, S., and Raja, S. (2016). An efficient block based lossless compression of medical images. *Optik-International Journal for Light and Electron Optics*, *127*(2), 754-758.

Vikranth, B. M., Momin, M. H., Mohsin, S. M., Rimal, S., and Pandey, S. R. (2015, April). A SURVEY OF IMAGE STEGANOGRAPHY. In *Journal of Emerging Technologies and Innovative Research* (Vol. 2, No. 4 (April-2015)). JETIR.

Wang, X., Wei, C., and Han, X. (2015). Steganography forensics method for detecting least significant bit replacement attack. *Journal of Electronic Imaging*, *24*(1), 013016-013016.

Weng, S., and Pan, J. S. (2016). Integer transform based reversible watermarking incorporating block selection. *Journal of Visual Communication and Image Representation*, *35*, 25-35.

Wu, B., Chang, M., Shastri, B., Ma, P., and Prucnal, P. (2016). Dispersion Deployment and Compensation for Optical Steganography Based on Noise.

Yan, F., Iliyasu, A. M., and Venegas-Andraca, S. E. (2016). A survey of quantum image representations. *Quantum Information Processing*, *15*(1), 1-35.

Yang, B., Rozic, V., Mentens, N., and Verbauwhede, I. (2015). On-the-Fly Tests for Non-Ideal True Random Number Generators. In *IEEE International Symposium on Circuits and Systems (ISCAS 2015)*.

Yang, C. H., Lin, Y. K., Chang, C. H., and Chen, J. Y. (2016). Data Hiding for H. 264/AVC Based on the Motion Vector of 16 Grids. In *Advanced Multimedia and Ubiquitous Engineering* (pp. 389-395). Springer Berlin Heidelberg.

Yiannakou, M., Trimikliniotis, M., Yiallouras, C., and Damianou, C. (2016). Evaluation of focused ultrasound algorithms: Issues for reducing pre-focal heating and treatment time. *Ultrasonics*, *65*, 145-153.

Zanganeh, O., and Ibrahim, S. (2011). Adaptive image steganography based on optimal embedding and robust against chi-square attack. *Information Technology Journal*, *10*(7), 1285-1294.

Zargar, A. J., and Singh, A. K. (2016). Robust and imperceptible image watermarking in DWT-BTC domain. *International Journal of Electronic Security and Digital Forensics*, *8*(1), 53-62.

Zeckendorf, D. T. D. E. (1972) "Generalized Zeckendorf Theorem".

Zhang, W., Wang, S., and Zhang, X. (2007). Improving embedding efficiency of covering codes for applications in steganography. *Communications Letters, IEEE*, *11*(8), 680-682.

Zhang, X., and Wang, S. (2005). Steganography using multiple-base notational system and human vision sensitivity. *Signal Processing Letters*, *IEEE*,*12*(1), 67-70.

Zhelezov, S. (2016). Modified Algorithm for Steganalysis. *Mathematical and Software Engineering*, *1*(2), 31-36.