DEVELOPMENT OF A HYBRID SYSTEM BASED ON CRYPTOGRAPHY AND STEGANOGRAPHY TECHNIQUES

by

SUHAD SHAKIR JABER
(1330211071)

A thesis submitted in fulfillment of the requirements for the degree of Master of Science in Computer Engineering

School of Computer and Communication Engineering
UNIVERSITI MALAYSIA PERLIS

2015

UNIVERSITI MALAYSIA PERLIS

DECLARATION OF THESIS

Author's full name	:	Suhad Shakir Jaber
Date of birth	:	28st July 1978
Title	:	DEVELOPMENT OF A HYBRID SYSTEM BASED ON CRYPTOGRAPHY AND STEGANOGRAPHY TECHNIQUES
Academic Session	:	2015/2016

I hereby declare that the thesis becomes the property of University Malaysia Perlis (UniMAP) and to be placed at the library of UniMAP. This thesis is classified as:

□	**CONFIDENTIAL**	(Contains confidential information under the Official Secret Act 1972)
□	**RESTRICTED**	(Contains restricted information as specified by the organization where research was done)
□	**OPEN ACCESS**	I agree that my thesis is to be made immediately available as hard copy or on-line open access (full text)

I, the author, give permission to the UniMAP to reproduce this thesis in whole or in part for the purpose of research or academic exchange only (except during a period of _ years, if so requested above).

Certified by:

SIGNATURE	**SIGNATURE OF SUPERVISOR**
A5303423	**Dr. HILAL ADNAN FADHIL**
(NEW IC NO. / PASSPORT NO.)	**NAME OF SUPERVISOR**

Date: ______________

Date: ______________

GRADUATE SCHOOL
UNIVERSITY MALAYSIA PERLIS

PERMISSION TO USE

In presenting this thesis in fulfilment of a post graduate degree from the University Malaysia Perlis, I agree that permission for copying of this thesis in any manner, in whole or in part, for scholarly purposes may be granted by my supervisor(s) or, in their absence, by the Dean of the Graduate School. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not allowed without any written permission. It is also understood that due recognition shall be given to me and to University Malaysia Perlis for any scholarly use which may be made of any material from my thesis

Request for permission to copy or to make other use of material in this thesis whole or in part should be addressed to

Dean of Graduate School

University Malaysia Perlis (UniMAP)

No. 112 & 114, Tingkat 1, Blok A, Taman Pertiwi Indah,

Jalan Kangar-Alor Setar,

Seriab, 01000 Kangar, Perlis.

ACKNOWLEDGEMENTS

I would like to thank Allah (SWT) for granting me health, patience and determination to complete this study. I also wish to express my special thanks to my supervisor Dr. Hilal Adnan Fadhil for his patience, motivation, moral support and sincerity in providing the necessary facilities throughout this academic Msc. pursuing journey. I would also like to express my gratitude to my co-supervisor Dr. Zahereel I. Abdul khalib for his guidance, suggestions and insights throughout the whole period of the study. My appreciation goes to the Dean of the School of Computer and Communication Engineering Prof. Dr. R. Badlishah Ahmed for his kind support. A special acknowledgment must be given to the staff members of the UniMAP for their support and eagerness to provide the ideal research environment. Last but not the least; my particular thanks are due to my husband, my parents, my brothers and my sisters for their continuous prayers and moral support throughout my life.

Suhad Shakir Jaber

University Malaysia Perlis (UniMAP)

TABLE OF CONTENTS

CHAPTER 3 RESEARCH METHODOLOGY

CHAPTER 4 RESULTS AND DISCUSSIONS

CHAPTER 5 CONCLUSION AND FUTURE WORK

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AES	Advanced Encryption Standard
AES-LSB	Advanced Encryption Standard with Least Significant Bit
AES-PVD	Advanced Encryption Standard with Pixel Value Difference
APP	Advanced Encryption Standard with Patch Reference Table- Pixel Value Difference
BMP	Bitmap
Bpp	bit pair pixel
DES	Data Encryption Standard
D	The Difference between Two Pixel
dB	Decibel
DCT	Discrete Cosine Transform
DWT	Discrete Wavelet Transform
FFT	Fast Fourier Transform
GF	Galois Field
GIF	Graphics Interchange Format
JPEG	Joint Photographic Experts Group
LSB	Least Significant Bit
MF-PVD	Modulus Function-Pixel Value Difference
MSE	Mean Square Error
OPAP	Optimal Pixel Adjustment Process
PNG	Portable Network Graphics
PRT-PVD	Patch Reference Table- Pixel Value Difference
PSNR	Peak Signal-to-Noise Ratio

PVD	Pixel Value Difference
Q	The Embedding Sequence
RC	Rcon Constant
R_i	Quntazation ranges from 0 through 255
RSA	Rivest, Shamir, and Adleman
SSIS	Spread Spectrum Image Steganography
T	Threshold
TDES	Triple Data Encryption Standard

Pembangunan Sistem Hybrid Berdasarkan Kriptografi Dan Teknik Steganografi

ABSTRAK

Media digital telah menjadi lebih popular daripada media analog tradisional kerana ia menyaksikan penurunan yang pesat dalam kos pemprosesan, penyimpanan, dan jalur lebar. Data digital mudah untuk diedit, diubah suai dan dieksploitasi. Oleh itu, adalah mudah bagi orang ramai untuk menghantar data digital dan maklumat melalui internet. Secara umum ,maklumat boleh diubah suai dengan mudah oleh orang-orang yang tidak berkenaan. Justeru, Keselamatan dan kkesahihan data dalam komunikasi digital telah menjadi isu utama. Teknologi yang berbeza telah dibangunkan untuk melindungi data digital termasuk kriptografi dan steganografi. Kriptografi melindungi data dengan menukar data ke dalam maklumat yang tidak bermakna; Walau bagaimanapun, ia memberikan petunjuk yang jelas mengenai proses perlindungan. Sementara itu, skim steganografi telah diguna pakai untuk mengelakkan tanda-tanda untuk melindungi data dengan menyembunyikan mereka dalam data perlindungan. Dalam projek ini, skim kriptografi dan steganografi digabungkan untuk membangunkan sistem keselamatan hibrid yang boleh memberi komunikasi yang selamat antara penghantar dan penerima. Sistem ini menggunakan imej digital sebagai medium pembawa untuk menanamkan imej rahsia "ciphered". Pertamanya, imej skala kelabu rahsia disulitkan dengan menggunakan algoritma penyulitan popular yang dinamakan sebagai 'Advance Encryption Standard (AES)'. Kemudian, imej yang disulitkan itu disembunyikan dalam imej perlindungan (i.e, berwarna atau skala kelabu) dengan menggunakan teknik steganografi berdasarkan Patch Reference Table Pixel Value Difference (PRT-PVD), yang dinamakan sebagai APP. APP dinilai dari segi Signal Puncak kepada Nisbah Bunyi (PSNR), kapasiti penerapan, dan keupayaan untuk menahan lampiran steganalysis seperti perbezaan histogram. Keputusan eksperimen menunjukkan bahawa pendekatan yang dicadangkan APP menghasilkan stego-imej dengan kualiti persepsi yang baik; ini telah dibuktikan oleh nilai PSNR yang tinggi berbanding dengan teknik PVD, MF-PVD, AES-PVD, AES -LSB. Dan PRT-PVD Selain dari itu, histogram perbezaan imej perlindungan dan stego-imej adalah sangat minima. Untuk imej penutup 128×128 skala kelabu dan muatan 20000 bit, APP mencapai nilai purata PSNR sebanyak 48,7230 dB, manakala nilai PSNR purata bagi teknik PVD, MF-PVD, AES-PVD, AES-LSB dan PRT-PVD ialah 42,3399, 43,8579, 42,3639, 47,2249 dan 48.3877 dB, masing-masing. Tambahan pula, APP juga menghasilkan PSNR yang lebih tinggi untuk semua eksperimen imej perlindungan yang berbeza (iaitu, warna atau skala kelabu) jenis dan saiz (225 × 225, 512 × 512) dengan muatan yang berbeza. Di samping peningkatan prestasi, kajian ini mencadangkan kaedah penigraan secara automatik yang boleh mengira nilai ambang optimum bagi sistem APP ini. Jelasnya, penggunaan pendekatan yang dicadangkan boleh meningkatkan keselamatan penghantaran data melalui saluran terbuka.

Development of a Hybrid System Based on Cryptography and Steganography Techniques

ABSTRACT

The digital media has become more popular than the traditional analog media since it witnessed a rapid decrease in the cost of processing, storage, and bandwidth. The digital data are easy to edit, modify and exploit. Therefore, it is convenient for people to transmit digital data and information through the internet. It is implied that information can be modified easily by unauthorized people. The security and the validity in digital communication have therefore become main issues. Different technologies have been developed to protect the digital data including cryptography and steganography. Cryptography protects the data by converting them into meaningless information; however, it gives an explicit indication about the protection process. Meanwhile, the steganography schemes have been applied to avoid the hint of protecting the data by hiding them in the cover data. In this project, the cryptography and steganography schemes are combined to develop a hybrid security system that can provide a secure communication between the sender and the receiver. This system uses the digital image as a carrier medium to embed the ciphered secret image. Firstly, the secret grayscale image is encrypted by using a popular encryption algorithm called Advance Encryption Standard (AES). Then, the encrypted image is hidden in a cover image (i.e., colour or grayscale) using steganography technique based on the Patch Reference Table Pixel Value Difference (PRT-PVD), which called APP. The APP is evaluated in terms of Peak Signal to Noise Ratio (PSNR), embedding capacity, and the ability to resist the steganalysis attach such as the histogram difference. The experimental results indicated that the proposed approach APP provided stego-images with a good perceptual quality; this was indicated by the obtained high PSNR values in comparison with the PVD, MF-PVD, AES-PVD, and AES –LSB techniques. Apart from that, the difference histograms of the cover images and the stego-images are very minimal. For 128×128 grayscale cover images and payload of 20000 bits, the APP achieved an average value of PSNR of 48.7230 dB, while the average PSNR values of PVD, MF-PVD, AES-PVD, AES-LSB and PRT-PVD techniques are 42.3399, 43.8579, 42.3639, 47.2249, 48.3877 dB, respectively. Moreover, the APP provides a higher PSNR for all experiments of different cover image (i.e., colour or grayscale) types and sizes (225×225, 512×512) with different payloads. In addition to improvement in performance, this study suggested a method that can automatically calculate the optimal threshold value for the APP system. As a result, using the proposed approach can improve the security of data transmission through the open channels.

CHAPTER 1

INTRODUCTION

1.1 Background

Computerized communication has become an essential part of information system. As lots of utilizations are Internet-based, it is important that communication be made secret. Therefore, the security of private data passed over an open channel has become a vital issue where confidentiality and data integrity are required to prevent unauthorized access and use. This has resulted in an unstable growth in the field of data covering up. Cryptography and steganography are the two common methods available to present security; ones embeds the existence of the message and the other scrambles the message itself (Narayana & Prasad, 2010).

Basically, cryptography (also abbreviated as “crypto”) is the technology of secret writing that transforms the original message (plain text) into a scrambled form which is called “cipher text” without revealing the meaning of the information to attackers. The cipher text is sent to the receiver where the original message will be retrieved; the recipient will not be able to retrieve the original message without knowing the secret key (Raphael & Sundaram, 2011). Different encryption methods have been presented to provide security in communication; however, they give an explicit indication about the protection process. To solve this problem of cryptography, steganography techniques have been introduced to hide data in other digital media, such as image, text, audio or video that no one except the sender and the receiver knows that there is a hidden message. The main requirement of a steganography technique is undetectability.

Recently, digital images have been popularly used as a cover-object to covey the secret information. Owing to the high propagation of digital images and the high degree of redundancy they showcase, there is an increased interest in the use of images as a cover object in steganography. A lot of research has focused on the techniques of hiding data in images (Chan & Cheng, 2001; Chang, Lin, & Hu, 2002; Chang & Tseng, 2004; Hussain & Hussain, 2013; S. L. Li, 2005; Tzeng, Yang, & Tsai, 2004). The focus of this project is attaching information to an image file where digital images are selected as the cover-media to transform the secret data. (Chan & Cheng, 2004)

1.2 Basics of Image Steganography Techniques

Steganography techniques are usually used to hide the existence of a secret message rather than making it illegible. An embedded digital media should maintain an imperceptible quality to keep the embedded media from drawing attention. In general, the major concerns of data hiding techniques are embedding capacity and imperceptibility (Hong, Chen, & Shiu, 2009). There are three basic requirements for the steganography techniques which are (Amirtharajan & Rayappan, 2012):

- **Payload capacity:** The maximum amount of secret data that can be embedded into the cover (Chen, Zhang, Chen, Fu, & Wu, 2012).
- **Robustness:** This refers to the strength or the power of the embedded secret information to withstand image manipulations processes (Bahi, Couchot, & Guyeux, 2011).
- **Imperceptibility or undetectability:** The measure of viability of the cover medium to hide secret information without raising doubts about the existence of this information. Moreover, it represents the possibility to prevent human eye

detection. Accordingly, a large imperceptibility can be attained from a higher quality of stego-images (Bahi et al., 2011).

It is impossible to get at the same time the highest level of the maximum embedding capacity and robustness to an acceptable level of imperceptibility. Therefore, a trade off should be made between payload capacity, imperceptibility and robustness. For different applications, the acceptable balance between those three constraints is different depending on the nature of the conditions of the application (S. L. Li, 2005). The relationship between steganography parameters are shown in Figure 1.1.

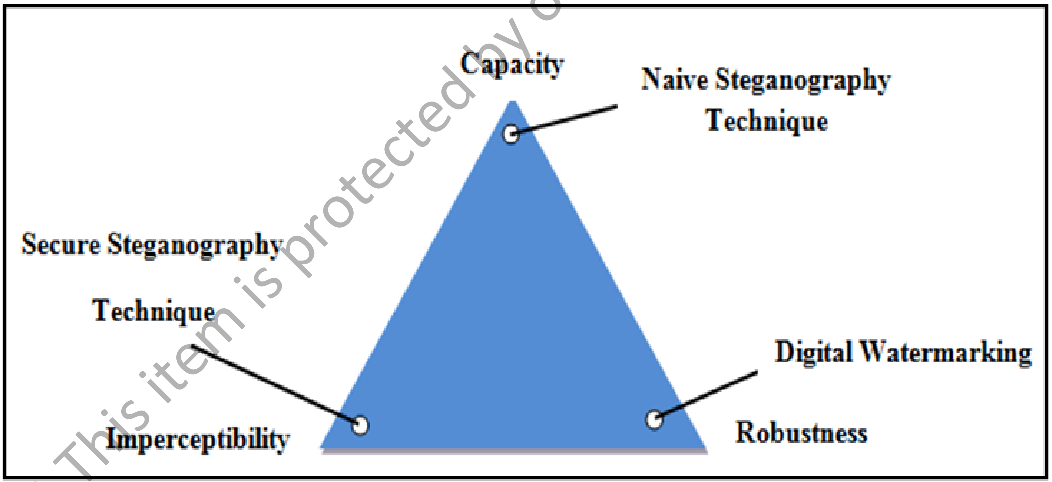

Figure 1.1: The Main Parameters in Embedding Information System (Fridrich, 1999)

Several terms are used in Steganography (Al-Shatnawi, 2012):

- **Cover medium:** This refers to a media such as (video, audio, image, and text) where the secret data has to be hidden.
- **Secret message:** This is the data which must be hidden into a suitable cover or extracted from it.

- **Stego-medium:** The medium which contains both the secret data and the carrier file.
- **Secret Key:** A sequence of bits that are used in some types of steganography techniques to increase the security of the embedding the secret information.
- **Steganalysis:** This is a tool that is used to detect the secret information inside a medium file.

1.3 Problem Statement

The use of Internet is growing day by day in many applications around the world. Therefore, a huge data is transmitted over the network. The security of the transmitted data is very important for many applications such as business and medical reports transport. Two approaches, cryptography and steganography, have been presented to provide a secure transfer of confidential data (Narayana & Prasad, 2010).

Cryptography is an approach of converting the secret data into a scrambled form by using an algorithm or mathematical formula with the assistance of a secret key. Many techniques have been proposed for data encryption over the years such as Data Encryption Standard (DES) (Feistel, 1973), Triple Data Encryption Standard (TDES) (Usman et al., 2007), and Advanced Encryption Standard (AES) (Daemen & Rijmen, 2002; Hodjat & Verbauwhede, 2004). The length of the secret key that is used in DES and TDES is 64 bits, which makes these techniques breakable. AES is better than other cryptography techniques in terms of security, flexibility, complexity, and suitability for different images. AES is a symmetric block algorithm which accepts keys of length 128, 192 or 256 bits (128 bits is already high secure) (Hodjat & Verbauwhede, 2004; Mohan & Reddy, 2011). However, the cryptography technique converts the secret message into a scrambled form, which gives an evident idea to the attacker there is a private exchange of information.

On the other hand, different steganography techniques in the spatial domain have been presented such as the Least Significant Bit (LSB) replacement (Amin, Salleh, Ibrahim, Katmin, & Shamsuddin, 2003), Optimal Pixel Adjustment Process (OPAP) (Chan & Cheng, 2004), the Pixel Value Difference (PVD) (Wu & Tsai, 2003), Modulus Function-Pixel Value Difference (MF-PVD) (C.-M. Wang, Wu, Tsai, & Hwang, 2008). These techniques suffer from low visual quality and limited capacity. Patch Reference Table- Pixel Value Difference (PRT-PVD) is a modern method which appeared in 2013 by (Hong, 2013). Among the aforementioned steganography techniques, it has been proved that the PRT-PVD technique performs better in comparison with previous steganography techniques in terms of payload, visual quality, and resistance of attacking tools such as difference histogram tool (Hong, 2013). Since the steganography technique provides security by hiding the secret message in a cover media. Therefore, the mission of this technique fails when the adversary detects the secret message.

A combination approach based on both cryptography and steganography as a two stages of security, was suggested such as Advanced Encryption Standard with Pixel Value Difference (AES-PVD) (Phad Vitthal, Bhosale Rajkumar, & Panhalkar Archana, 2012) and Advanced Encryption Standard with Least Significant Bit (AES-LSB) (Ramaiya, Hemrajani, & Saxena, 2013). However, these techniques achieved more security, but the weakness of PVD and LSB methods in steganography stage still arise the suspicious about the embedding data.

To exploit the impact security of cryptography and the ability of steganography to hide the secret data without arousing suspicious about the existence of this data, a combination between a secure cryptography method and a secure steganography method will achieve a more secure system.

1.4 Research Objectives

The main goal of this thesis is to improve the security systems by combining cryptography with steganography. The objectives of this research can be summarized as follows:-

1. To develop a hybrid approach in the spatial domain by combining the AES cryptography technique with the PRT-PVD steganography technique and analyze its performance in terms of visual quality and embedding capacity. The proposed approach (i.e., the combined AES cryptography and PRT-PVD steganography techniques) is named (APP) for short.
2. To investigate the effectiveness of the threshold value on the performance of the proposed APP approach and improve its performance by computing the optimal threshold for each cover image (colour and grayscale) with different sizes.
3. To compare the performance of the proposed APP with different spatial domain methods in terms of Peak signal-to-noise ratio (PSNR), embedding capacity, and difference histogram.

1.5 Scope of Work

In this project, two cryptography and steganography techniques have been combined to solve the problem of securing communication networks. If steganography fails, the secret data cannot be returned because the cryptography technique has been used (EL-Emam, 2007; Raphael & Sundaram, 2011).

First of all, the secret grayscale image entered by the sender is encrypted using the AES cryptography algorithm before the embedding process. Secondly, the encrypted image is hidden in the cover image (colour or grayscale) by using the PRT-PVD steganography technique based on optimal threshold case. A colour and grayscale images with sizes 128×128, 225×225 and 512×512 are used to evaluate the proposed approach. The algorithms of the encryption, embedding, extract and decryption are implemented using MATLAB2012a Package programming. The visual quality of the stego-images has been evaluated using the well-known PSNR, payload capacity, and difference histogram.

1.6 Thesis Outline

This thesis is constructed from five chapters, and is organised as follows:

i. Chapter 1 gives a brief introduction of both the cryptography and the steganography and outlines the main project aims. Additionally, this chapter gives the problem statement followed by the objectives, scope of work, and thesis layout.

ii. Chapter 2 introduces a general literature survey of the cryptography and steganography techniques. The review starts by explaining multi cryptography and steganography schemes then show the comparison between steganography techniques in spatial domain. This chapter explains the general approaches of image steganography and a performance measure of steganography. In addition a definition and the goal of the steganalysis method is presented. Finally, there is a summary at the end of this chapter.

iii. Chapter 3 explains the details of the proposed APP approach including the AES encryption technique, as well as the details of the PRT-PVD steganography technique.

iv. Chapter 4 details the simulation results of the proposed method, and assesses the performance of the proposed approach. This chapter explains the evaluation between the PVD, MF-PVD, AES-LSB, AES-PVD, PRT-PVD techniques and the APP in terms of payload capacity, PSNR and difference histogram of each cover (colour and grayscale) images with sizes 128×128, 225×225, and 512×512. Moreover, the results of calculation the optimal threshold are shown in this chapter.

v. In Chapter 5 the conclusion of this thesis are given and ideas for future work are discussed.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

In recent time, the computers and the Internet have been considered to be the main correspondence media that connect various regions of the world as one global virtual world. Thus, individuals can easily exchange information and distance is no longer a barrier to communication. However, the safety and security of long-distance communication is still an issue. This is especially important on account of secret information. Cryptography and steganography techniques are developed to solve this problem. Steganography is an effective security method to give a high level of security; particularly when it is combined with cryptography (Cheddad, Condell, Curran, & Mc Kevitt, 2010).

Cryptography is one of the methods used to transmit data securely by changing it to an unreadable form. Steganography takes cryptography a step farther because it is used to hide the existence of the secret information. At times, sending scrambled data may draw attention, while steganography will not. Cryptography is not the best answer for securing correspondence; it is just part of the arrangement. Both methods can be merged together to better ensure data. In this situation, regardless of the possibility that steganography fails, the message cannot be retrieved because a cryptography technique is also utilized (EL-Emam, 2007).