A NEW STEGANOGRAPHY TECHNIQUE USING MAGIC SQUARE MATRIX AND AFFINE CIPHER

WALEED S. HASAN AL-HASAN

UNIVERSITI TEKNOLOGI MALAYSIA
A NEW STEGANOGRAPHY TECHNIQUE USING MAGIC SQUARE
MATRIX AND AFFINE CIPHER

WALEED S. HASAN AL-HASAN

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

Faculty of Electrical Engineering
Universiti Teknologi Malaysia

June 2015
Dedicated to my beloved mother
To my beloved father
To my beloved brother and sister
To my beloved wife
To my angel (Melek)

I love you for every second in my life
ACKNOWLEDGEMENT

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

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

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

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

<table>
<thead>
<tr>
<th>CHAPTER</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>DECLARATION</td>
<td></td>
<td>ii</td>
</tr>
<tr>
<td>DEDICATION</td>
<td></td>
<td>iii</td>
</tr>
<tr>
<td>ACKNOWLEDGEMENT</td>
<td></td>
<td>iv</td>
</tr>
<tr>
<td>ABSTRACT</td>
<td></td>
<td>v</td>
</tr>
<tr>
<td>ABSTRAK</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TABLE OF CONTENTS</td>
<td></td>
<td>vi</td>
</tr>
<tr>
<td>LIST OF TABLES</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>LIST OF FIGURES</td>
<td></td>
<td>xi</td>
</tr>
<tr>
<td>LIST OF ABBREVIATIONS</td>
<td></td>
<td>xiii</td>
</tr>
</tbody>
</table>

# INTRODUCTION

1. Overview
2. Background of the Problem
3. Problem Statement
4. Aim of the Study
5. Objectives of the Study
6. Scope of the Study
7. Significance of the Study
8. Research Framework

# LITERATURE REVIEW

1. Introduction
2. Image File Format
2.2.1 Image Parameters
   2.2.1.1 File Identifier
   2.2.1.2 Image Description Information
   2.2.1.3 Compression Types
   2.2.1.4 X and Y Origin

2.2.2 Most Common Used Image Formats
   2.2.2.1 BMP
   2.2.2.2 GIF
   2.2.2.3 PNG
   2.2.2.4 JPEG
   2.2.2.5 TIFF

2.3 Steganography
   2.3.1 The Concept of Steganography
   2.3.2 Different Kinds of Steganography
      2.3.2.1 Steganography in Images
      2.3.2.2 Steganography in Audio
      2.3.2.3 Steganography in Video
      2.3.2.4 Steganography in Documents

2.4 Parameters of Image Steganography
   2.4.1 Capacity
   2.4.2 Imperceptibility
   2.4.3 Robustness

2.5 Steganographic Techniques
   2.5.1 Transform Domain Techniques
      2.5.1.1 Discrete Cosine Transform (DCT)
      2.5.1.2 Discrete Wavelet Transformation
   2.5.2 Image Domain Techniques
      2.5.2.1 Conventional LSB Insertion Method

2.6 Enhanced LSB Algorithms
   2.6.1 SLSB Method
   2.6.2 The Optimal LSB Insertion Method
2.6.3 The Pixel Value Differencing Method (PVD) Method 32
2.6.4 Applying Randomization Concept to LSB Method 32
2.7 PSNR and NCC Formulas 33
2.8 Data Encryption 35
2.9 Summary 37

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

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

5 CONCLUSION 74
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1 Introduction</td>
<td>74</td>
</tr>
<tr>
<td>5.2 Summary of the Work</td>
<td>75</td>
</tr>
<tr>
<td>5.3 Contribution</td>
<td>75</td>
</tr>
<tr>
<td>5.4 Future Work</td>
<td>76</td>
</tr>
</tbody>
</table>

REFERENCES 77
# LIST OF TABLES

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

<table>
<thead>
<tr>
<th>FIGURE NO.</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Framework of the study</td>
<td>7</td>
</tr>
<tr>
<td>2.1</td>
<td>Steganography process</td>
<td>20</td>
</tr>
<tr>
<td>2.2</td>
<td>Data of 3 pixels of a RGB color image</td>
<td>28</td>
</tr>
<tr>
<td>2.3</td>
<td>Data of 3 pixels of the RGB color image after LSB insertion of the number 83</td>
<td>28</td>
</tr>
<tr>
<td>2.4</td>
<td>Vigenere table</td>
<td>37</td>
</tr>
<tr>
<td>3.1</td>
<td>Flowchart of the Embedding phase</td>
<td>40</td>
</tr>
<tr>
<td>3.2</td>
<td>Flowchart of the Embedding phase</td>
<td>41</td>
</tr>
<tr>
<td>3.3</td>
<td>Flowchart of the Extraction phase</td>
<td>42</td>
</tr>
<tr>
<td>3.4</td>
<td>Lena image and its RGB channels</td>
<td>48</td>
</tr>
<tr>
<td>3.5</td>
<td>Lena image and its YCbCr channels</td>
<td>49</td>
</tr>
<tr>
<td>3.6</td>
<td>Magic square</td>
<td>51</td>
</tr>
<tr>
<td>3.7</td>
<td>ISB method</td>
<td>52</td>
</tr>
<tr>
<td>4.1</td>
<td>Dataset Airplane, Lena, peppers, Baboon, Goldhill, Sailboat and Tiffany.</td>
<td>56</td>
</tr>
<tr>
<td>4.2</td>
<td>Main interface of the implementation software</td>
<td>57</td>
</tr>
<tr>
<td>4.3</td>
<td>Interface of the Embedding process</td>
<td>58</td>
</tr>
<tr>
<td>4.4</td>
<td>Interface of Loading Image</td>
<td>58</td>
</tr>
<tr>
<td>4.5</td>
<td>Interface of Converting pixel values to YCbCr</td>
<td>59</td>
</tr>
<tr>
<td>4.6</td>
<td>Interface of the choosing the secret message</td>
<td>59</td>
</tr>
<tr>
<td>4.7</td>
<td>Interface of coding the secret message using affine cipher</td>
<td>60</td>
</tr>
</tbody>
</table>
4.8 Interface of extraction the secret message and decoding it using affine cipher 60
4.9 Imperceptibility Results of the proposed method using embedding rate 1KB. 62
4.10 Imperceptibility Results of the proposed method using embedding rate 2KB 63
4.11 Imperceptibility Results of the proposed method using embedding rate 4KB 63
4.12 Imperceptibility Results of the proposed method using embedding rate 8KB 64
4.13 Imperceptibility Results of the proposed method using embedding rate 16KB. 64
4.14 Imperceptibility Results of the proposed method using embedding rate 32KB. 65
4.15 Imperceptibility Results of the proposed with different case of payload size. 65
4.16 Lena Stego-mage after apply salt and pepper 0.1 attack 66
4.17 Lena Stego-mage after apply salt and pepper 0.2 attack 67
4.18 Lena Stego-mage after apply salt and pepper 0.3 attack 67
4.19 Hidden and extracted secret text messages after apply attack salt and pepper 0.3. a) Original embedded text. b) Extracted text 68
4.20 The accuracy of extorted proposed method using attack salt and pepper 0.1 70
4.21 The accuracy of extorted proposed method using attack salt and pepper 0.2 70
4.22 The accuracy of extorted proposed method using attack salt and pepper 0.3 71
4.23 Performance of the proposed method against both DWT 73
LIST OF ABBREVIATIONS

ASCII - American Standard Code for Information Interchange
BC - Before Christ
BMP - Bitmap image file
DCT - Discrete Cosine Transform
DWT - Discrete Wavelet Transform
EMD - Exploiting Modification Direction
GIF - Graphic Interchange Format
GLM - Gray Level Modification
HVS - Human Visual System
ID - The value of Identification
ISB - Intermediates Significant Bits
JPEG - Joint Photographic Experts Group
LSB - Lest Significant Bit
LZW - Lempel–Ziv–Welch
NCC - Normalized cross-correlation
PNG - Portable Network Graphic
PSNR - Peak Signal to Noise Ratio
RGB - Red Green and Blue
TIFF - Tagged Image File Format
YCbCr - Luminance, Chrominance blue Chrominance red
Cb - The blue-difference Chroma component
Cr - The red-difference Chroma component
MSB - Most Significant Bit
CHAPTER 1

INTRODUCTION

1.1 Overview

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

The most popular techniques dealing with data security are Steganography and Cryptography. Cryptography is a method of protection for data storage using secret key during data transfer. Encryption is still a successful method to protect stored data and to transmit over network. Steganography is an alternative method to protect information by preventing the detection of hidden messages (NehaBatra et al., 2012). Steganography encompasses many secret communication methods that hide the message from being disclosed or seen.
The origin of steganography returns to the ancient Greece where King Darius ordered to shaved the head of prisoners to write the secret messages and when their hair grew back they moved to the recipient, and the secret remain undetected (Norman, 1979; Khan, 1967). Another story reveals that Greeks wrote their secret messages on a wooden medium and then covered them with wax (Silman, 2001). Since, then the steganography techniques gradually changed ranging from using invisible ink and microdots to modern methods like hiding data in digital media (Zim, 1984).

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

1.2 Background of the Problem

Several techniques have been proposed to conceal data inside the cover image, but the most popular approach is LSB, which is based on substituting the least significant bit with bits of embedded information inside the cover data of some or all bytes (Chan, 2004a). Slightly higher protection is provided by sharing secret keys between sender and receiver, by allowing only certain pixels to be changed and in this way it would be difficult to retrieve the message without having the “Stego_key”.
In steganography, there is a tradeoff between the need to embed a large amount of data and to preserve the high image quality. Therefore, if it is required to have more payload, the image quality will be lower and vice versa. Steganography algorithms are usually not efficient with high amounts of embedded payload (Nedeljko, 2004).

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

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

Some steganographic approaches focused on security and robustness, but usually the output image presented is either low in quality or has small capacity for hidden data. There is always a requirement to maintain a modified cover image not easily distinguishable by human eye. Obviously, the robustness and invulnerability of these methods are inadequate (Olivier, 2005). A balance between robustness and quality will lead to a successful approach.
Today, the important question, which needs answering, is that how we can increase the amount of the imperceptibility, robustness and maintaining the high quality of the image? In this research, the ISB method, affine cipher and Magic square are applied to embed large amount of secret data, while preserving the high image quality as compared to previous methods and to show high tolerance to statistical attacks such as noise.

1.3 Problem Statement

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

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

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

1.5 Objectives of the Study

This research intends to achieve the following objectives:

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

1.6 Scope of the Study

1. The file to be embedded (secret data) is the ordinary text file format.
2. The proposed method uses the basic concept of ISB insertion method.
3. The affine cipher encryption method is used to encrypt the input text file.
4. The standard images for testing purposes are Lena, Baboon, Airplane, Pepper, Tiffany, Sailboat and Golden hill.

5. The Salt-Pepper statistical attack is applied on the results to evaluate the robustness in terms of security of the proposed method.

1.7 Significant of the Study

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

1.8 Research Framework

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


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