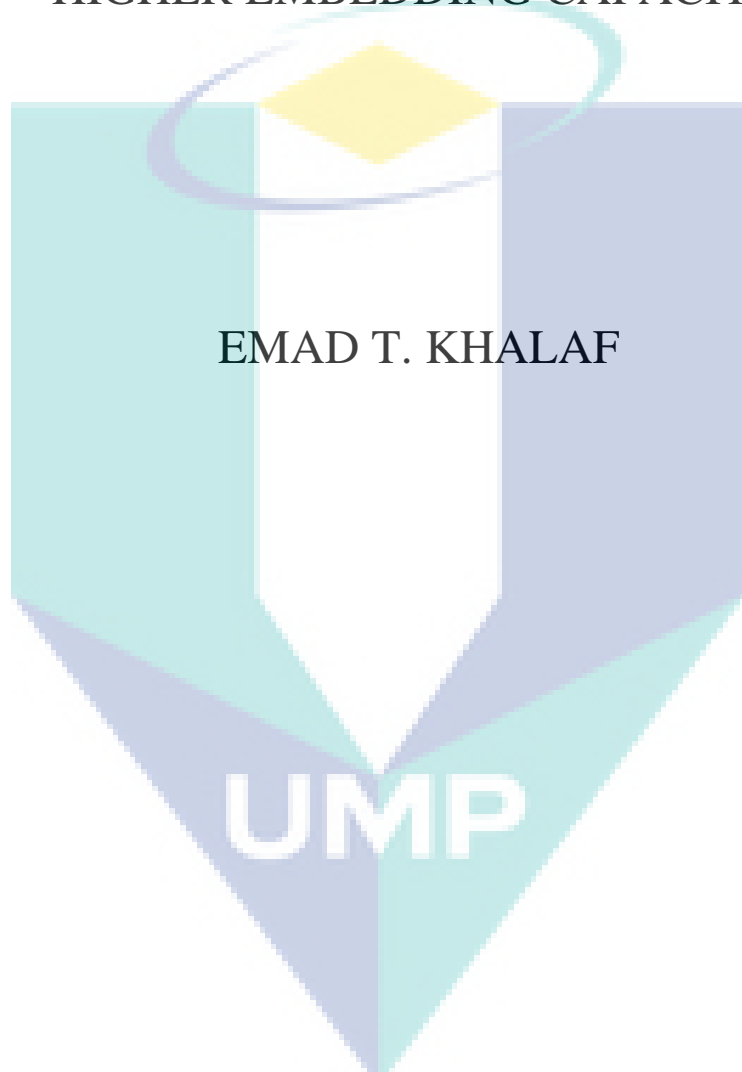


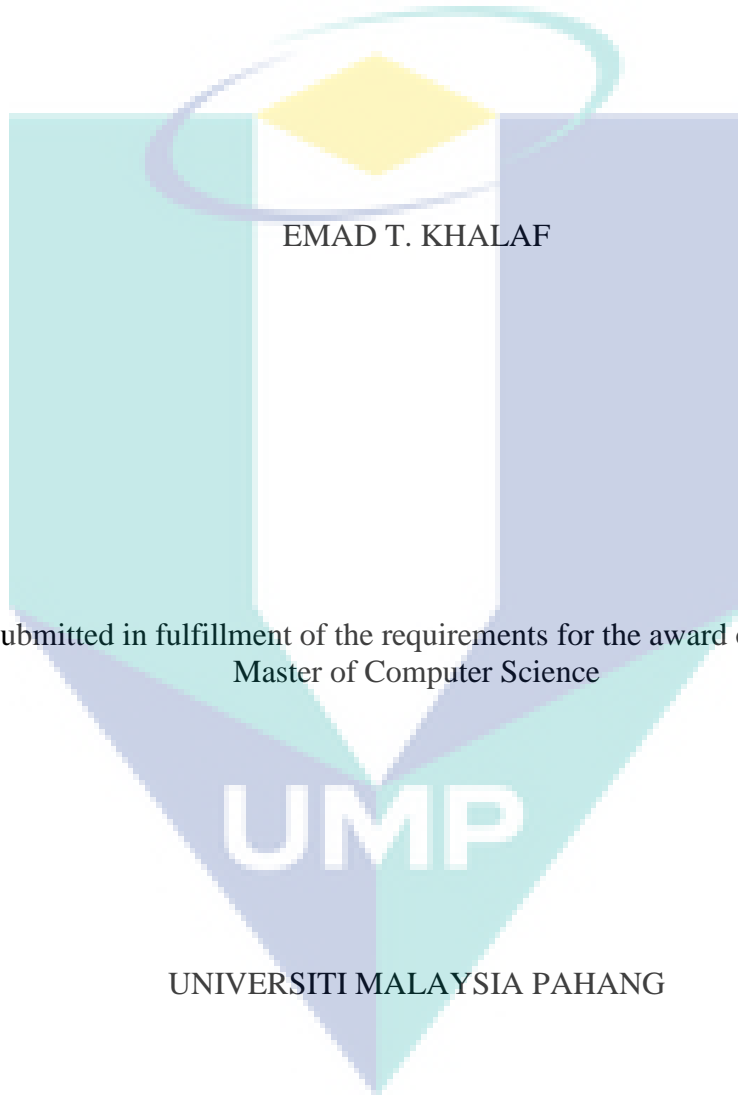
ENHANCEMENT OF CRYPTOGRAPHY AND  
TRANSFORM DOMAIN IN STEGANOGRAPHY FOR  
HIGHER EMBEDDING CAPACITY



EMAD T. KHALAF

Faculty of Computer Systems & Software Engineering  
UNIVERSITI MALAYSIA PAHANG

# ENHANCEMENT OF CRYPTOGRAPHY AND TRANSFORM DOMAIN IN STEGANOGRAPHY FOR HIGHER EMBEDDING CAPACITY



EMAD T. KHALAF

Thesis submitted in fulfillment of the requirements for the award of the degree of  
Master of Computer Science

UMP

UNIVERSITI MALAYSIA PAHANG

2012

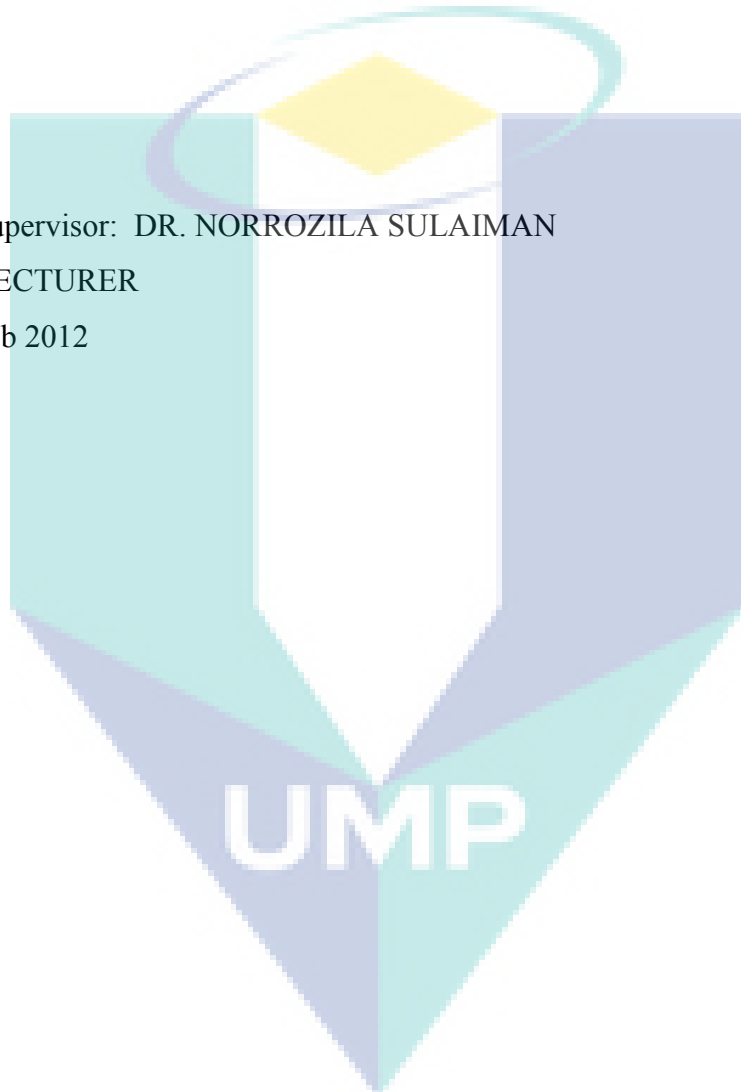
## SUPERVISOR'S DECLARATION

I hereby declare that I have checked this thesis and in my opinion this thesis is satisfactory in terms of scope and quality for the award of the degree of Master of Computer Science.

Name of Supervisor: DR. NORROZILA SULAIMAN

Position: LECTURER

Date: 23 Feb 2012



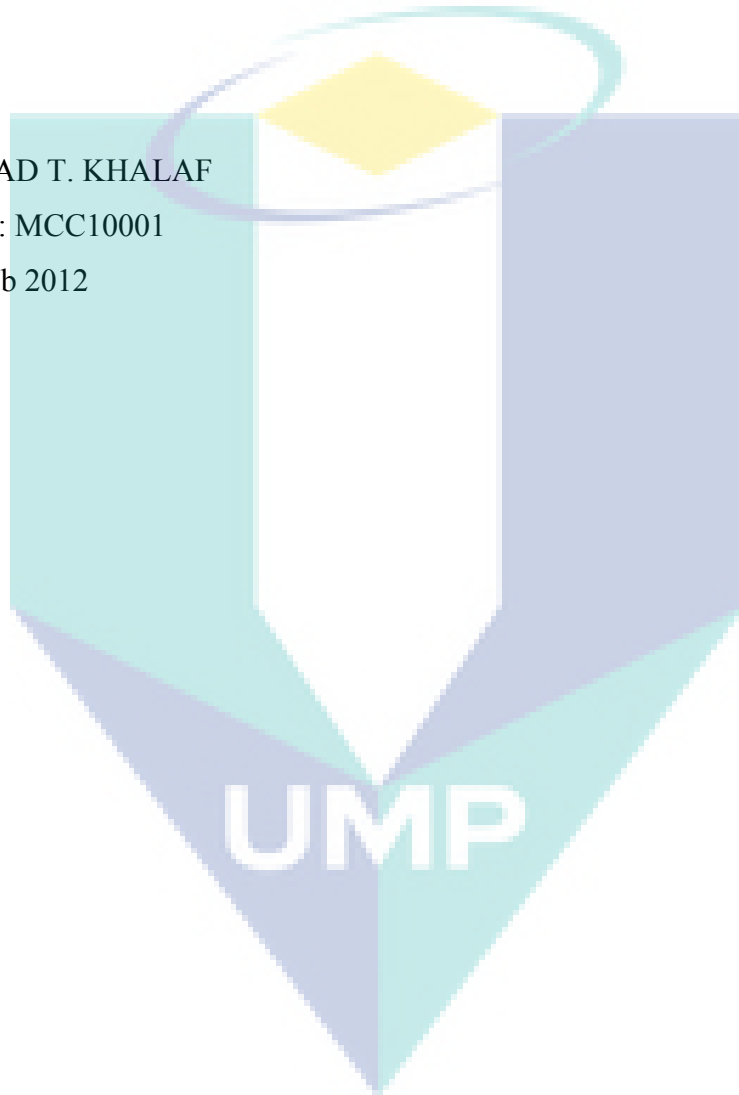
## STUDENT'S DECLARATION

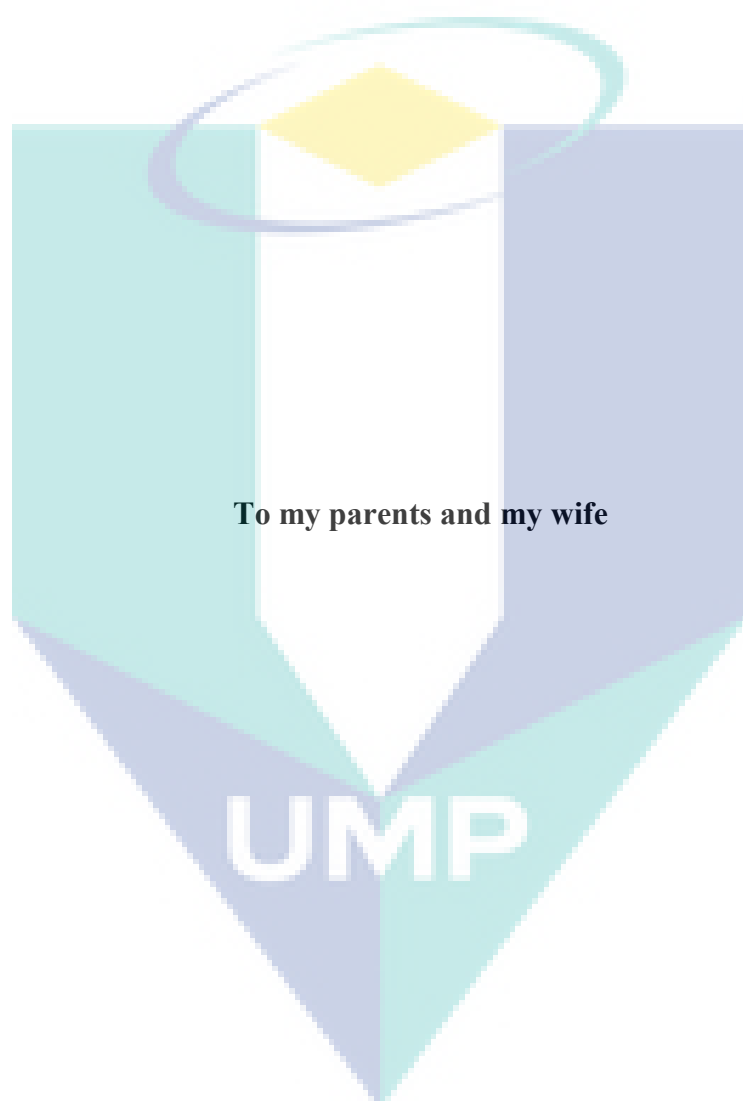
I hereby declare that the work in this thesis is my own except for quotations and summaries which have been duly acknowledged. The thesis has not been accepted for any degree and is not concurrently submitted for award of other degree.

Name: EMAD T. KHALAF

ID Number: MCC10001

Date: 23 Feb 2012





## ACKNOWLEDGEMENTS

In the name of Allah, the Most Benevolent, the most Merciful. First of all, I wish to record immeasurable gratitude and thankful fullness to the One and The Almighty Creator, the Lord and Sustainer of the universe, and the Mankind, in particular. It is only through His mercy and help that this work could be completed, and it is ardently desired that this little effort be accepted by Him to be of some service to the cause of humanity.

I would like to take this opportunity to express my gratitude to my supervisor Dr. Norrozila Sulaiman for her constant guidance and encouragement.

A special thank to Universiti Malaysia Pahang (UMP) for the real support and laboratory facilities. Thanks to Mr. Haider Ismael Almayaly for his help, who is not only a friend that gives me his time and the knowledge that I need, but he is also a brother. To all my friends in Iraq and Malaysia, especially brother Hemin Mohammed and Brother Ali Asghar, thank you for the support.

Finally, but most importantly of all, my father, my mother and my wife, should receive my greatest appreciation for their enormous love. They always respect what I want to do and give me their full support and encouragement over the years.



UMP

## ABSTRACT

In the field of Data Communication, security issues are the top priority. Cryptography and steganography address the necessary elements for secure communication namely privacy, confidentiality, key exchange, authentication, and non-repudiation but reveals the fact that communication is happening. This study proposes a combination of Steganography and Cryptography to enhance security of the transmitted information. Hence this work is composed of two parts: cryptographic and steganographic. In the cryptographic part, an improvement has been proposed to the Hill cipher algorithm to be more secured by using a large and random key with large data block, and also extending it by including the special characters and digits. For the steganographic part, a new method has been proposed by combining Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT), to take the advantageous of both algorithms. The original image is decomposed into four bands using the Haar wavelet LL, HL, LH and HH. Three of these sub-bands have been selected to hiding data (LH, HL and HH) which are less effect to the image than LL sub-band. Then, DCT transform is applied to the selected DWT sub-band, the process of hiding will be in the least significant bit of the DCT coefficients to each sub-band. The distribution of data will be based on the chosen percentages, which is entered by a sender. These percentages will be agreed between both the sender and the receiver as a key of hiding. The proposed system goal is to provide more complexity in encryption and make the embedding capacity as high as possible with high visible quality in a way that it does not allow any attacker to even detect that there are secret messages. The complexity of encryption and concealment was checked out with a number of widely used metrics such as Peak Signal to Noise Ratio (PSNR), Mean Squared Error (MSE), Normalized Absolute Error (NAE) and Normalized Correlation Coefficient (NCC). The experimental results demonstrate the complexity of the proposed method compared with the standard and existing methods.

The logo for UMP (Universitas Muhammadiyah Purwokerto) is a large, stylized letter 'M' composed of four triangles meeting at the center. The top-left triangle is light blue, the top-right is light green, the bottom-left is light purple, and the bottom-right is light teal. The letters 'UMP' are written in white, bold, sans-serif font across the center of the 'M' shape.

UMP

## ABSTRAK

Di dalam bidang Komunikasi Data, isu-isu keselamatan merupakan satu keutamaan. Kriptografi dan steganografi boleh menangani unsur-unsur yang perlu untuk komunikasi yang selamat seperti privasi, kerahsiaan, pertukaran kekunci data dan pengesahan bahawa komunikasi berlaku. Kajian ini mencadangkan gabungan diantara Steganografi dan kriptografi untuk meningkatkan keselamatan maklumat yang dihantar. Oleh itu, pengkajian ini terdiri daripada dua bahagian iaitu kriptografi dan steganografi. Dalam bahagian kriptografi, peningkatan telah dicadangkan bagi algoritma cipher Hill yang lebih selamat dengan menggunakan kekunci besar dan rawak dengan blok data yang besar, dan juga meningkatkan keselamatan data dengan memasukkan simbol khas dan digit. Untuk bahagian steganografi, satu kaedah baru telah dicadangkan dengan menggabungkan diskret kosinus mengubah (DCT) dan diskret koncah Transform (DWT), dengan menggunakan kekuatan yang ada pada kedua-dua algoritma. Pertama, mengurai imej asal kepada empat kumpulan-kumpulan yang menggunakan Haar koncah LL, HL, LH dan HH, tiga-kumpulan kecil telah dipilih untuk menyembunyikan data (LH, HL dan HH) yang kurang berkesan kepada imej daripada 'sub-LL-band'. Kemudian, DCT mengubah digunakan untuk DWT 'sub-band' yang dipilih. Proses penyembunyian dilakukan pada ketara pekali DCT paling rendah untuk setiap 'sub-band', dan taburan data berdasarkan peratusan yang dipilih, yang dimasukkan oleh pengirim. Peratusan ini akan dipersetujui antara kedua-dua penghantar dan penerima sebagai kunci tersembunyi. Matlamat sistem yang dicadangkan adalah untuk menyediakan penyulitan yang lebih kompleks dan meninggikan kapasiti penerapan beserta kualiti setinggi mungkin dimana ia tidak membenarkan penyerang maklumat untuk mengesan bahawa terdapat maklumat yang tersembunyi. Tahap rahsia penyulitan dan penyembunyian telah disemak dengan beberapa metric yang digunakan secara meluas seperti *Peak Signal to Noise Ratio* (PSNR), *Mean Squared Error* (MSE), *Normalized Absolute Error* (NAE) and *Normalized Correlation Coefficient* (NCC). Keputusan kajian menunjukkan kecekapan kaedah yang dicadangkan berbanding dengan kaedah standard dan sedia ada.

The logo of Universiti Malaysia Perlis (UMP) is a large, semi-transparent watermark in the background. It consists of a downward-pointing triangle divided into four quadrants by a vertical and a horizontal line. The top-left and bottom-right quadrants are light blue, while the top-right and bottom-left quadrants are light green. The letters 'UMP' are printed in white, bold, sans-serif font across the center of the triangle.



## TABLE OF CONTENTS

	<b>Page</b>
<b>SUPERVISOR'S DECLARATION</b>	ii
<b>STUDENT'S DECLARATION</b>	iii
<b>DEDICATION</b>	iv
<b>ACKNOWLEDGEMENTS</b>	v
<b>ABSTRACT</b>	vi
<b>ABSTRAK</b>	vii
<b>TABLE OF CONTENTS</b>	viii
<b>LIST OF TABLES</b>	xi
<b>LIST OF FIGURES</b>	xii
<b>LIST OF NOMENCLATURES</b>	xiv
<b>LIST OF ABBREVIATIONS</b>	xv
<b>CHAPTER 1      INTRODUCTION</b>	
1.1      Background	1
1.2      Problem Statement	3
1.3      Objectives	3
1.4      Scopes of Research	4
1.5      Organization of Thesis	4
<b>CHAPTER 2      LITERATURE REVIEW</b>	
2.1      Introduction	5
2.2      Steganography	5
2.3      Cryptography	7
2.3.1      Symmetrical (Secret-Key) Cryptography	8
2.3.2      Asymmetrical (Public-Key) Cryptography	10
2.3.3      Hash Functions	11
2.4      Steganography, Watermarking and Cryptography	11
2.5      Steganography Historical Review	13

2.6	The Digital Era of Steganography	15
2.7	Application of Information Hiding	16
2.8	Types of Covers	16
2.8.1	Hiding in Text	16
2.8.2	Hiding in Image	17
2.8.3	Hiding in Video and Audio	17
2.8.4	Hiding in Network Packets	18
2.8.5	Hiding in File Storage Systems	18
2.9	Digital Image Representation	19
2.9.1	Binary Image	19
2.9.2	Gray - Scale Image	19
2.9.3	Colored Image	20
2.9.4	Multi - Spectral Image	21
2.10	Steganography Techniques	21
2.10.1	Injection Technique	21
2.10.2	Substitution Technique	22
2.10.3	Generation Technique	22
2.11	Steganographic Algorithms	22
2.11.1	Spatial Domain Algorithm	23
2.11.2	Transform Domain Algorithm	24
2.12	Statistical Detection	27
2.13	Related work	29
2.13	Summary	31
<b>CHAPTER 3</b>	<b>DESIGN</b>	
3.1	Introduction	33
3.2	First phase: Encryption	36
3.2.1	Improved Block Cipher Based on Random Key	36
3.3	Second phase: Hiding	37
3.3.1	Secured System Based On Joint DWT-DCT (SSBDD)	37
3.4	Third phase: Combination of Encryption and Hiding	40
3.5	Summary	42

## **CHAPTER 4      METHODOLOGY**

4.1	Introduction	43
4.2	Improved block cipher based on random key	43
	4.2.1 Encryption	43
	4.2.2 Decryption	49
4.3	Secured System Based On Joint DWT-DCT (SSBDD)	53
	4.3.1 Embedding procedure	53
	4.3.2 Extracting procedure	56
4.4	Combination of Encryption and Hiding	58
4.5	Summary	59

## **CHAPTER 5      RESULTS AND DISCUSSION**

5.1	Introduction	60
5.2	Phase I: Analysis of encryption	60
	5.2.1 Encryption Complexity Analysis	61
	5.2.2 Running Time Analysis	66
5.3	Phase II: Analysis of Concealment	67
	5.3.1 Capacity of Concealment for SSBDD	67
	5.3.2 Results of Comparisons	76
	5.3.3 Histogram statistical analysis	79
	5.3.4 Analysis of Extracted Data	81
5.4	Phase III: Encryption and Concealment Combination analysis	82
5.5	Summary	83

## **CHAPTER 6 CONCLUSION AND RECOMMENDATIONS**

6.1	Introduction	84
6.2	Summary of Findings	84
6.3	Contribution of the Study	87
6.4	Recommendation for future research	87

<b>REFERENCES</b>		<b>88</b>
-------------------	--	-----------

**LIST OF TABLES**

<b>Table No.</b>	<b>Title</b>	<b>Page</b>
2.1	Advantages and disadvantages comparison	13
5.1	Comparison of results between the proposed method, and Swain and Lenka's method	61
5.2	Results of comparing running time between "New Block Cipher", RSA and the proposed method	67
5.3	Result of embedding different amount of data in different cover images	68
5.4	Result of embedding using different number of bits used	69
5.5	Result of embedding different amount of data in different type of images	72
5.6	Capacity and quality of images using different percentages	75
5.7	Results of the comparison with the Adaptive LSB and the other methods	77
5.8	Results of the comparison with the previous methods	77
5.9	Result of NC between the original and extracted messages	82

The logo for UMP (University of Management and Practice) is a large, downward-pointing triangle. It is composed of four smaller triangles meeting at the center. The top-left and bottom-right triangles are light blue, the top-right and bottom-left triangles are light purple, and the central area is white. The letters 'UMP' are printed in a bold, white, sans-serif font across the center of the white area.

**UMP**

## LIST OF FIGURES

<b>Figure No.</b>	<b>Title</b>	<b>Page</b>
2.1	A generalized steganographic framework	7
2.2	Symmetrical (Secret-Key) Cryptography	8
2.3	Hill's Machine	10
2.4	Asymmetrical (Public-Key) Cryptography	11
2.5	Hash Functions	11
2.6	Media TV channels usually have their logos watermark	12
2.7	Cardan Grille	14
2.8	Concealment of Morse code, 1945	15
2.9	The header of TCP protocol	18
2.10	Binary image with only two colors white and black	19
2.11	Gray scale image with 256 levels of gray color	20
2.12	Colored image representation (three essential color planes)	21
2.13	Hiding information in LSB of one of the color component	23
3.1	Relation between steganography, watermarking and cryptography	34
3.2	Combine encrypting and hiding	35
3.3	Simplified model of symmetric encryption	36
3.4	Basic model of steganography	37
3.5	Children image before and after one Haar wavelet transform	39
3.6	Proposed system	40
3.7	The proposed system after combining cryptography and steganography	41
4.1	Improved block cipher based on random key (Encryption processes)	48
4.2	Improved block cipher based on random key (Decryption processes)	52
4.3	Secure system based on joint DWT-DCT (SSBDD) embedding processes	55
4.4	Secured system based on joint DWT-DCT (SSBDD) extracting procedure	57
5.1	Samples of secret images before and after encryption using Swain and Lenka's method and the proposed method	63

5.2	Baboon image before and after encryption using different key lengths	64
5.3	Samples of secret images before and after encryption using variety password length.	65
5.4	Sample of text message before and after encryption	66
5.5	Samples of cover images before and after embedding data	71
5.6	Leaving bits in embedding process	72
5.7	Samples of BMP and GIF images before and after embedding data	73
5.8	Result of PSNR to different images sizes	74
5.9	Difference of capacity of three images	74
5.10	Effect of changing the percentages to Lena image	76
5.11	Comparison between SSDBB and Adaptive LSB	78
5.12	A frequency histogram of the Lena cover image	79
5.13	Histogram comparison of Adaptive LSB method and the proposed method after a hidden message of 209720 bits	79
5.14	Histogram comparison of Adaptive LSB method and the proposed method after a hidden message of 419440 bits	80
5.15	A frequency histogram of the Cameraman cover image	80
5.16	Histogram comparison of Adaptive LSB method and proposed method after a hidden message of 209720 bits	81
5.17	Histogram comparison of Adaptive LSB method and proposed method after a hidden message of 419440 bits	81

## LIST OF NOMENCLATURES

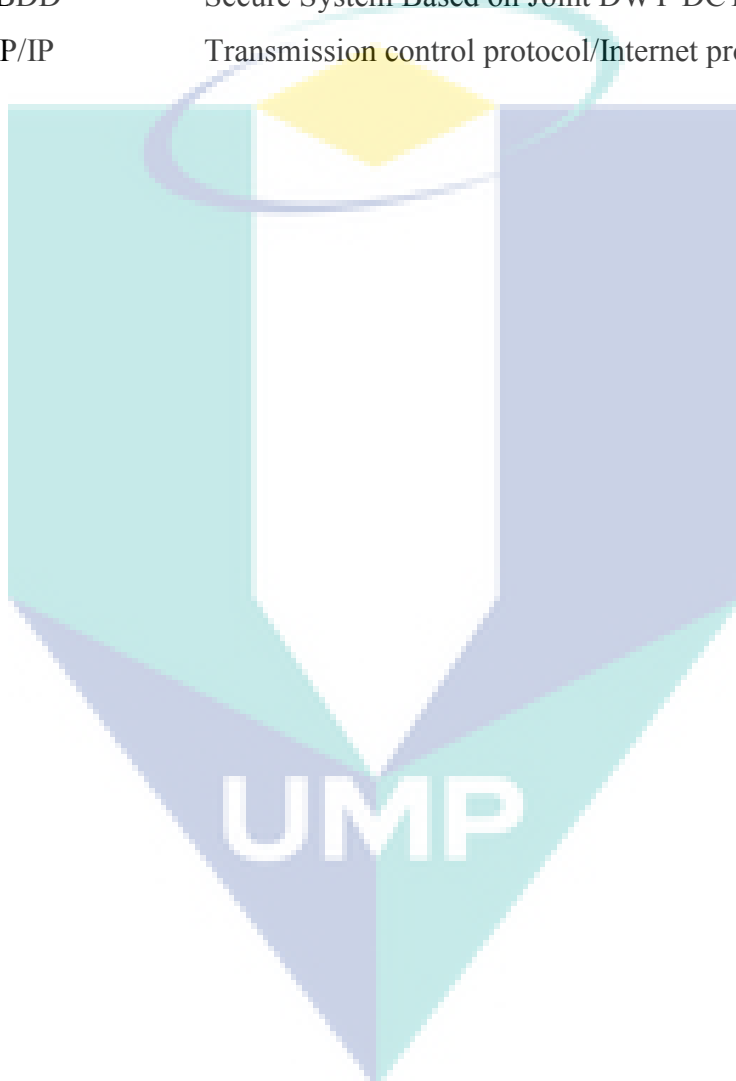
$a_{i,j}$	corresponding pixel values of cover image
$b_{i,j}$	corresponding pixel values of stego image
C	Cipher text
$C(i)$	block of Ciphertext
$C_x$	wavelet coefficients
$f_E$	steganographic function "embedding"
$f_E^{-1}$	steganographic function "extracting"
$h$	image height
I	the Identity of matrix
K	encryption Key
$K^{-1}$	the inverse of the encryption key
L	length of encryption key
$M$	original secret message
$M'$	extracted secret message
N	number of blocks
n	length of message P
$NB$	number of bits that will be not used in embedding
P	Plain text
$P(i)$	block of plaintext
$q$	Length of square matrix rows and columns
R	Reminder of (P/L)
S	Password
w	Image width
$W(x)$	wavelet scaling function
$\delta$	wavelet delta function
$\Phi(x)$	analyzing wavelet

## LIST OF ABBREVIATIONS

AES	Advanced Encryption Algorithm
ASCII	American Standard Code for Information Interchange
BMP	Bit Map image
CMY	Cyan, Magenta, Yellow
DCT	Discrete Cosine Transform
DES	Data Encryption Standard
DFT	Discrete Fourier Transform
DICOM	Digital Imaging Communications in Medicine
DSA	Digital Signature Algorithm
DSP	Digital signal processing
DWT	Discrete Wavelet Transform
GIF	Graphics Interchange Format
HH	Vertical edge data
HL	Vertical edge data
HTML	Hyper Text Markup Language
HVS	Human visual system
ICT	Information Communications Technology
IDCT	Inverse DCT
IDWT	Inverse DWT
JPEG	Joint Photographic Experts Group
LH	Horizontal edge data
LL	Lower resolution version of image
LSB	Least Significant Bit
MD5	Message Digest 5
MSB	Most Significant Bit
MSE	Mean Squared Error
NC	Normalized Cross Correlation
PRG	Pseudo random generator
PSNR	Peak Signal to Noise Ratio



PVD	Wavelet-Pixel Value
RGB	Red Green and Blue
RMSE	Root Mean Square Error
RSA	Rivest, Shamir and Adleman
SHA	Secure Hash Algorithm
SNR	Signal-to-Noise Ratio
SSBDD	Secure System Based on Joint DWT-DCT
TCP/IP	Transmission control protocol/Internet protocol



## CHAPTER 1

### INTRODUCTION

#### 1.1 BACKGROUND

Ever since the old times, the issue of important information hiding preoccupied the minds of many people especially in business, military and political fields due to the secrecy of their information. After the spread of the Internet, most of the individuals prefer using it as the primary medium to transfer data from one end to another across the world, easily, quickly and surely. Thus, there were always secret means and methods that were pursued to send such information. However, at the same time the sent data were easily intercepted and uncovered by hackers.

Researchers and scientists made a lot of research work to solve this problem until the science of hiding information was founded. Among the methods invented in this new science was hiding information in a text or an image or an audio without any change in the size of the sent file or its distortion. The information will be sent via internet without detecting by the hackers.

Steganography is a technique of hiding information, it is usually implemented computationally where media host carriers such as text files, images, audio files and video files are tweaked in such a way that a secret message can be embedded within them. In data hiding, there are conflicting in requirements (undetectability, capacity and robustness), these requirements are mutually competitive and cannot be clearly optimized at the same time (Al-Najjar et al, 2007). If a large message is to be hidden

inside an image, absolute undetectability and large robustness cannot be expected. A reasonable compromise is always a necessity. On the other hand, if robustness to large distortion is an issue, the message that can be reliably hidden cannot be too long.

The techniques of steganography and digital watermarking are very similar. However there is some distinction between these two techniques. In digital watermarking, the focus is on ensuring that nobody can remove or alter the content of the watermarked data (Du and Zhao, 2011), even though it might be plainly obvious that it exists. While Steganography focuses on making it extremely difficult to tell that a secret message exists at all (Ahmad and Ali, 2011).

The other science of maintaining secure messages is the cryptography art which is closely related to steganography (Maurya et al., 2011). Steganography hide the message so that there is no knowledge of the existence of the message in the first place. Cryptography, on the other hand, protects information by transforming it into unreadable information to those who does not possess its corresponding access key i.e. password. Both sciences can be combined to produce better protection of the message (Muttoo and Kumar, 2009). By using steganography, data become invisible and methodical analysis of all possible files in searching for hidden data would make it possible to uncover them. However by using cryptography, the information is useless as it is encrypted.

For embedding technique, there are two common methods, i.e. spatial embedding and transform embedding (Muttoo and Kumar, 2009). For spatial embedding, messages are inserted directly into the LSBs of the cover-image. On the other hand, for transform embedding, a message is embedded by modifying frequency coefficients of the cover image. A steganography within photographic images need a method that could maximize the payload where a good steganographic technique should have good visual/statistical imperceptibility and a sufficient payload (Zhang and Wang, 2005).

## 1.2 PROBLEM STATEMENT

The fundamental requirement for a steganographic method is imperceptibility, which means that the embedded messages should not be sensible to human eyes. Besides, there are two other requirements, one is to maximize the embedding capacity and the other is security. For spatial domain, messages are inserted directly into the LSBs of the cover-image. The problem of LSB method is that by increasing the embedding capacity, the number of used bits in each pixel will be increased. This will not only increase the risk of making the embedded data detectable but also the image fidelity will be degraded (Cheddad et al., 2010). It is also not secure and some harmful statistics can reveal the secret data (Lee et al., 2009). On the other hand, using steganography only is unsafe (Zaidan et al., 2010). Hill Cipher algorithm is one of the most famous symmetric cryptosystem (Hamamreh and Farajallah, 2009). The problem of Hill Cipher algorithm is that it does not include special characters and digits. It takes the smaller sizes of blocks, hence the key length is shorter, very simple and vulnerable for exhaustive key search attack and the key matrix which entered should be invertible (Swain and Lenka, 2010).

## 1.3 OBJECTIVES

The objectives of this study are as follows:

- i. To design and propose an improvement to the steganography methods by combining Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) to embed secret information.
- ii. To improve the Hill cipher algorithm for encrypting secret information.
- iii. To propose a new security system by combining both the improved Hill cipher algorithm and the improved embedding method.

## **1.4 SCOPES OF RESEARCH**

Data payload and imperceptibility are the most important properties of a steganography system. The scope of this thesis includes improving the digital image steganography, in order to maximize the embedding capacity while maintaining the image fidelity. At the same time it is aimed to improve cryptography system to get more complexity and less time for encryption. Steganography and cryptography will be combined to provide two levels of security to the proposed system.

## **1.5 ORGANIZATION OF THESIS**

This thesis has been prepared to give details on the facts, observations, arguments and procedures in order to meet its objectives. Chapter 1 gives the brief background of information hiding, the problem statement, objectives and scope of the research. Chapter 2 presents the literature review of steganography, comparing it with encryption and watermarking. The old and modern steganography techniques are also discussed which focus on digital image representation and transform algorithms, to be used as host carrier. Chapter 3 discusses the architecture and implementation of the proposed system. Chapter 4 this chapter presents the steps of the proposed system. Chapter 5 contains evaluations of the proposed system and comparison with other related methods in the literature review. Moreover, analysis and results are reported that support the introduced algorithm. The conclusions of the present research are summarized and presented in Chapter 6. Suggestions and recommendations for the future work are also presented in this chapter.

## CHAPTER 2

### LITERATURE REVIEW

#### 2.1 INTRODUCTION

This chapter provides a necessary background study of Steganography and Cryptography. Brief definition and history of the steganography will be presented. Digital steganography and the applications of data hiding will be discussed. A review of other relevant research studies is also provided. In addition, the steganography techniques, spatial domain methods, frequency domain methods and adaptive methods in digital images are reviewed with great details.

#### 2.2 STEGANOGRAPHY

The term steganography comes from Greek which means covered writing. The words steganos (στεγανός) means "covered or protected" and graphein (γράφειν) means "to write" (Kumar and Shunmuganathan, 2010 and Tiwari and Shandilya, 2010 and Marvel et al., 1998). The first recorded use of the term was in 1499 by Johannes Trithemius in his Steganographia, a treatise on cryptography and steganography disguised as a book on magic (Ganeshkumar and Koggalage, 2010). Steganography defined as the hiding of information through a covert channel with the purpose of preventing the detection of a hidden message. Figure 2.1 shows basic steganographic framework. Also, it is the art of hiding the existence message (Kumar and Pooja, 2010). Typical digital media was used as a carrier (called host signal) for hiding private information in such a way that the third parties (unauthorized terminal) cannot delete, insert, change, or even notice the content of the communication (Kekre et al., 2011).

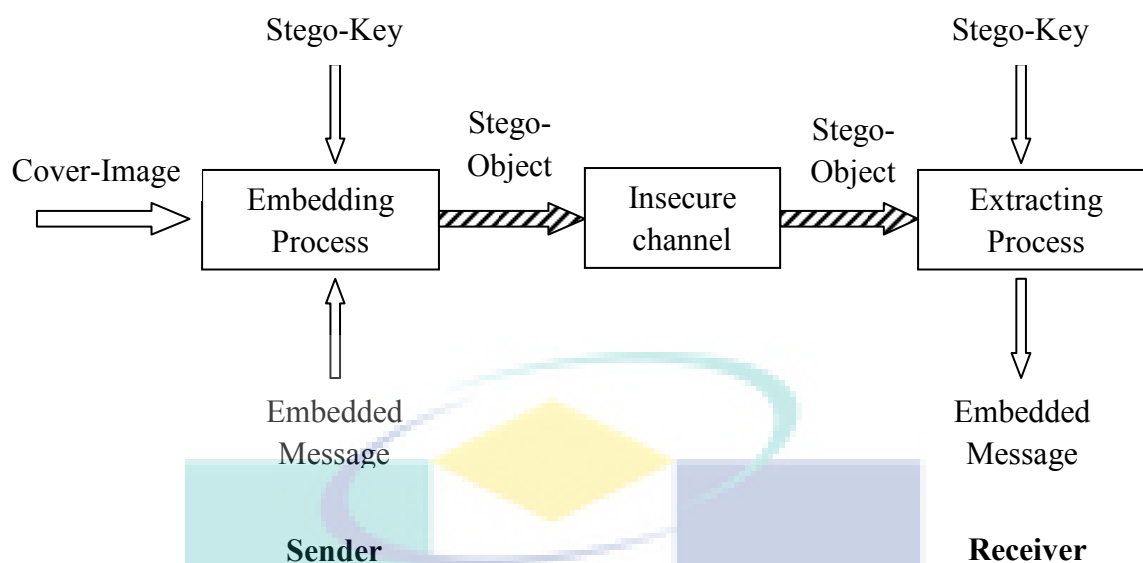
Information hiding is an ancient art, but its new techniques depend on digital communication as the main tool and customer of its products (Shirali-Shahreza and Shirali-Shahreza, 2008). Many types of covers have been used by different techniques in order to hide secret information. In literatures, information hiding is the art and science of concealing study of secretes transmission without any suspicion about the hidden information (Imran et al., 2007).

The increase in use of latest technology for sending information needs to employ a lot of security measures to protect them from infringements. The traditional method of protecting message theft is cryptography (Isbell 2002) and today the most sought research area is information hiding (Moulin and O'Sullivan 2003). Steganography is an approach of information hiding inside digital media unnoticeably (Amin et al. 2003).

According to Provos and Honeyman (2001) in cryptography, the structure of a message is scrambled or jumbled to make it meaningless except the sender and receiver who hold the decrypt key, who/which does not disguise or hide the encoded message. Basically, Cryptography offers the ability of transmitting information between authorized persons and seals the opportunity for intruders to get it. Steganography does not alter the structure of the secret message, instead it hides inside a cover-image so that it cannot be seen (Provos and Honeyman 2001). It is noteworthy that a cipher text might provoke suspicion on the part of the recipient but an invisible steganographic message will not leave any stain of doubt in the minds of attackers.

Zöllner (1998) claimed the system will be broken in cryptography as the attacker decrypts the unreadable data to retrieve the secret message. However, the attacker needs to become conscious about the existence of the secret message to extract a steganographically hidden message.

Digital covers can take different forms of investigation (image, audio, text, video, Network Packets and File Storage Systems) (Imran et al., 2007 and Gunjal and Manthalkar, 2010). However, the image cover is the most effective one which should not draw any suspicion about hidden data, and it also has larger hiding area. Authors used computers to transmit a huge amount of images over the Internet.



**Figure 2.1:** A generalized steganographic framework (Bhattacharyya and Sanyal, 2009)

Many previous steganographic algorithms have used spatial domain, it is the simplest form of image steganography in which the method replaces the LSBs of pixel values with the bits from the message bit stream. However, embedding the message data directly into the spatial domain means it is quite straight forward to detect that embedding has taken place. In this work the transform domain was studied and new methods were developed that embedded the message data in more inconspicuous areas (Kumar and Shunmuganathan, 2010 and Ramani et al., 2008).

### 2.3 CRYPTOGRAPHY

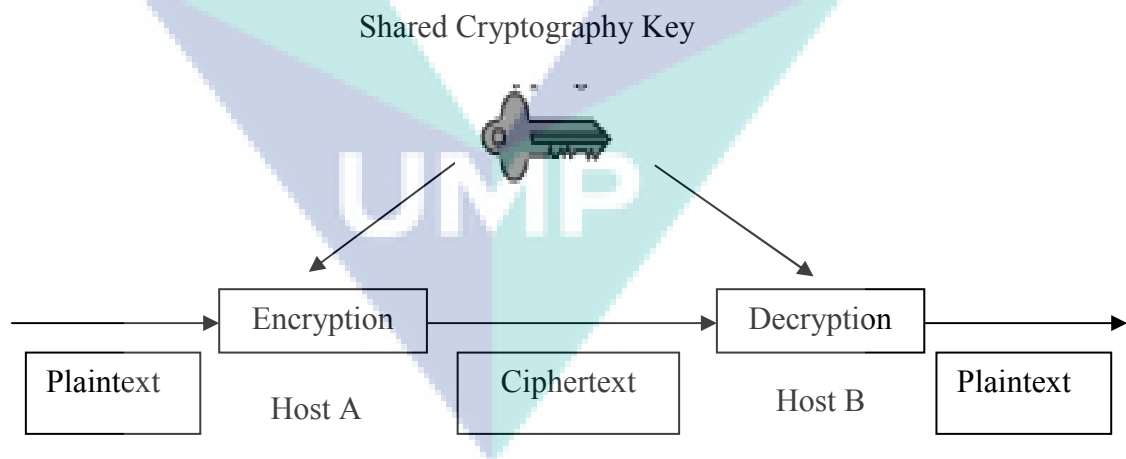
Cryptography is the art of hiding messages in unreadable secret codes to make it possible to exchange messages in such a way that other people cannot understand the message. There are many ways of hiding information. The original text is usually called “plaintext” and the encoded or altered text is called “ciphertext”, the operation of converting plaintext to ciphertext is called “encoding” or “enciphering”, and the opposite of this operation is called “decoding” or “deciphering”. The trying of reading a secret message which was not belong to recipient and recipient who do not know the encoding method is called “cracking” the code. There are three types on cryptographic techniques:



- i. Symmetrical (Secret-Key) Cryptography.
- ii. Asymmetrical (Public-Key) Cryptography.
- iii. Hash Functions.

### 2.3.1 Symmetrical (Secret-Key) Cryptography

This type of cryptographic techniques is called symmetric encryption because the sender and recipient share the same key. Referring to Figure 2.2, the sender uses the key (or some set of rules) to encrypt the plaintext and sends the ciphertext to the receiver. The receiver applies the same key (or rule set) to decrypt the message and recover the plaintext. DES (Data Encryption Standard-1976) and AES (Advanced Encryption Standard-2001) are the popular symmetrical cryptosystems. However, these modern cryptosystem have their origins. The classical cipher such as Caesar Cipher, Hill Cipher and Vigenère Cipher act as the foundation for the cryptology's world today. This study focuses on Hill Cipher which was first described in 1929 by its inventor, the mathematician Lester S. Hill, in the journal "The American Mathematical Monthl" (Eisenberg, 1998).



**Figure 2.2:** Symmetrical (Secret-Key) Cryptography

## Classic Hill Cipher Algorithm

Hill Cipher is a block cipher and symmetric key algorithm which was introduced to the journal of mathematics by Lester Hill as a short paper and published in 1929 (Lester, 1929). Hill Cipher has several advantages such as disguising letter frequencies of the plaintext, simplicity because of using basic matrix operations, high speed and high throughput (Overbey et al., 2005 and Saeednia, 2000). The first Hill's machine is as shown in Figure 2.3. In cryptography a message that has not yet been encrypted is called plaintext. After the encryption process, the encrypted message is called ciphertext. The encryption process of classic Hill cipher algorithm start with encoding each character of the plaintext as a numerical value ( $a=0, b=1, \dots, z=25$ ). Then the encoded plaintext was broken into blocks (vectors) of size  $n$  and multiplied by  $n \times n$  key matrix  $K$ , which is the encryption key. The final process is to perform mod 26. Simply, the plaintext block  $P$  encrypts to  $C$  as:

$$C = P K \pmod{26} \quad (2.1)$$

where:

$C$  is Cipher text

$P$  is Plain text

$K$  is encryption Key

Decryption requires the inverse of matrix  $K$ . The inverse  $K^{-1}$  of a matrix  $K$  is defined by the equation:

$$K K^{-1} = I \quad (2.2)$$

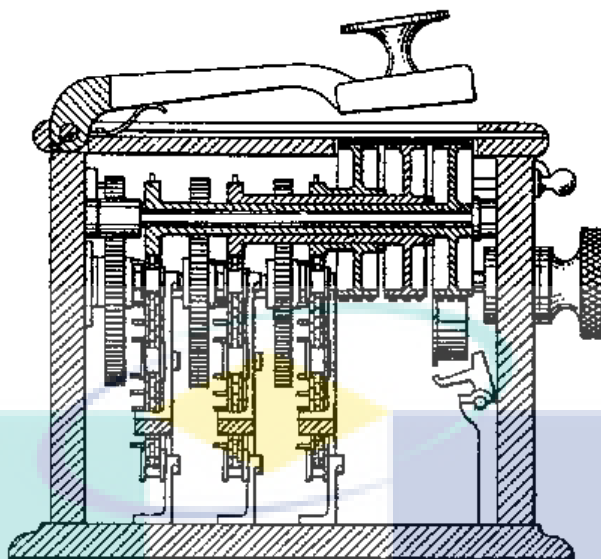
where:

$I$  is the Identity of matrix

$K^{-1}$  is the inverse of the encryption key

Not all the matrices have an inverse, only those that have a determinant which is not zero and does not have any common factors with the modular base. In decryption, the reverse process i.e. deciphering, is computed by:

$$P = K^{-1} C \pmod{26} \quad (2.3)$$

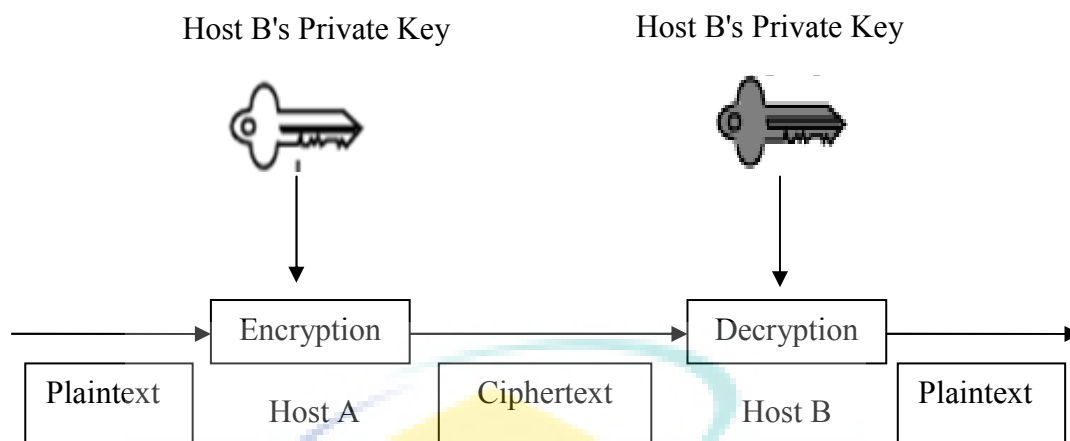


**Figure 2.3:** Hill's Machine (Weisner and Hill, 1932)

The disadvantages of classic Hill cipher are such that it does not include special characters and digits, it takes smaller sizes of blocks so that the key length is shorter. Furthermore, it is very simple and vulnerable for exhaustive key search attack which is known as plain text attack. The key matrix which is entered should be invertible.

### 2.3.2 Asymmetrical (Public-Key) Cryptography

This type of cryptographic techniques uses different keys (public keys) for the encryption and a private key for decryption processes. Whitfield Diffie and Martin Hellman (1976) (Diffie and Hellman, 1976) were the forerunners of this method and they introduced the technique. There are two keys, one for encryption and the other for decryption, as shown in Figure 2.4. The two common asymmetric algorithms are Rivest, Shamir and Adleman (RSA) and Digital Signature Algorithm (DSA).



**Figure 2.4:** Asymmetrical (Public-Key) Cryptography

### 2.3.3 Hash Functions

The third type of cryptographic techniques is one-way encryption, and no key is used as shown in Figure 2.5. It is a complex encryption algorithm which is often primarily used for passwords. Providing with a variable length unique input (message) will always provide a fixed length unique output called hash, or message digest.



**Figure 2.5:** Hash Functions

## 2.4 STEGANOGRAPHY, WATERMARKING AND CRYPTOGRAPHY

There are three techniques of information hiding that are interlinked i.e. steganography, watermarking and cryptography (Cheddad et al., 2010). Steganography is defined by Kahn et al., (Rama et al., 2011) as follows, “Steganography is the art and science of communicating in a way which hides the existence of the communication. In contrast to Cryptography, where the enemy is allowed to detect, intercept and modify messages without being able to violate certain security premises guaranteed by a cryptosystem, the goal of Steganography is to hide messages inside other harmless messages in a way that it does not allow any enemy to even detect that there is a second

message present”. Watermarking has been related to steganography as they both describe techniques that are used to convey information in a hidden manner. Watermarking technique prove the ownership of digital signal in a way that it is difficult to remove and the signal may be audio, pictures or video. Obviously, the copyright information should resist any modifications or manipulations. Figure 2.6 shows that media TV channels usually have their logos watermark for their broadcasting.



**Figure 2.6:** Media TV channels usually have their logos watermark

Basically, cryptography offers the ability of transmitting information between persons in a way that is prevents a third party from reading it. Cryptography can also provide authentication for verifying the identity of someone or something.

In contrast, steganography does not alter the structure of the secret message, but it is hidden inside a cover-image so that it cannot be seen. A message in cipher text, for instance, might arise suspicion on the part of the recipient while an “invisible” message created with steganographic methods will not. In other word, steganography prevents an unintended recipient from suspecting that the data exists. In addition, the security of classical steganography system relies on secrecy of the data encoding system (Peticolas et al., 1999). Once the encoding system is known, the steganography system is defeated.

It is possible to combine the techniques by encrypting message using cryptography and then hiding the encrypted message using steganography. As a result, stego-image can be transmitted without revealing that secret information is being exchanged. Furthermore, even if an attacker were to defeat the steganographic technique and detect the message from the stego-object, he would still require the cryptographic decoding key to decipher the encrypted message (Cachin, 1998). Table 2.1 shows that both technologies have counter advantages and disadvantages.

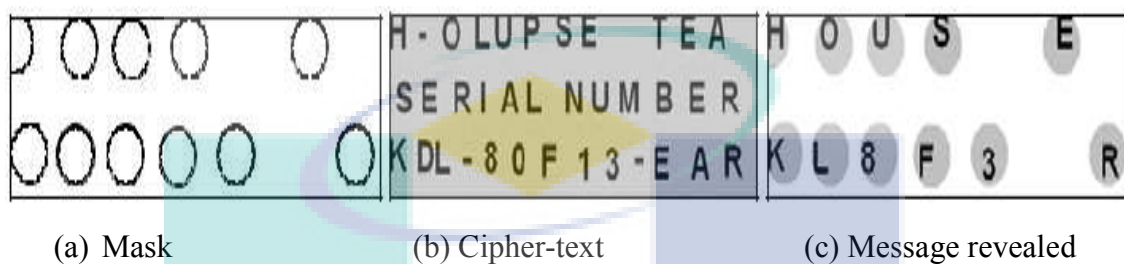
Table 2.1: Advantages and disadvantages comparison (Tanako et al., 2000)

Steganography	Cryptography
Unknown message passing	Known message passing
Little known technology	Common technology
Technology still being developed for certain formats	Most algorithms known to government departments
Once detected message is known	Strong algorithm are currently resistant to brute force attack
	Large expensive computing power required for cracking
	Technology increase reduces strength
Many Carrier formats	

## 2.5 STEGANOGRAPHY HISTORICAL REVIEW

Steganography has a long history, which can be traced back to Ancient Greece. In Herodotus Histories (c. 486-425 B.C.) around 440 B.C. Histiaëus shaved the head of his most trusted slave, wrote the message on his scalp, and then waited for the hair to regrow. The slave messenger, apparently carrying nothing contentious, could travel freely. Arriving at the destination, he shaved his head and pointed it at the recipient (Johnson and Jajodia, 1998), (Judge, 2001), (Provos and Honeyman, 2003) and (Moulin and Koetter, 2005). Chinese ancient method of secret writing was reinvented before five hundred years ago by the Italian mathematician Jérôme Cardan. The scenario were as follows: a paper mask with holes was shared among two parties. This mask was placed over a blank paper and the sender wrote the secret message through the holes

then took the mask off and filled the blanks so that the message appeared as an innocuous text as shown in Figure 2.7. This is an illustration of the phenomenon. Note that the Grille had no fixed pattern: (left) the mask, (middle) the cover and (right) the secret message revealed. This method was credited by Cardan and was called Cardan Grille (Moulin and Koetter, 2005).



**Figure 2.7:** Cardan Grille (Cheddad et al, 2010)

An ordinary letter which contain different message written between the lines was investigated (Rakesh et al., 2011). The author used another common form of invisible writing through invisible inks and such inks were used with much success in both World War I and World War II.

Null cipher was also successfully used. Null cipher means that the secrete message is embedded without any encryption, and it could be extracted according to the communication protocol between the sender and receiver. As a real example, a message was sent by German spy in the World War II (Raphael and Sundaram, 2011).

It was also reported that ancient Chinese wrote notes on small pieces of silk that was wadded into little balls and coated in wax, to be swallowed by a messenger and retrieved at the messenger's gastrointestinal convenience (Clair, 2001). It was also reported that during the World War II, steganography was used extensively. The Nazis invented several steganographic methods such as Microdots and have reused invisible ink and null ciphers. As an example of the latter, a message was sent by a Nazi spy that read: Apparently neutral's protest is thoroughly discounted and ignored. Is man hard hit, blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils." Using the 2nd letter from each word the secret message reveals: "Pershing sails

from NY June 1” (Judge, 2001), (Lyu and Farid, 2006) and (Kahn, 1996). In 1945, Morse code was concealed in a drawing, as shown in Figure 2.8. The hidden information was encoded onto the stretch of grass alongside the river (Delahaye, 1996). The long grass denoted a line and the short grass denoted a point. The decoded message read: “Compliments of CPSA MA to our chief Col Harold R. Shaw on his visit to San Antonio May 11th 1945” (Delahaye, 1996).



**Figure 2.8:** Concealment of Morse code, 1945 (Delahaye, 1996)

There are many types of hiding in different covers until today, every period of time a new technique of hiding appears (Ashok et al., 2010).

## 2.6 THE DIGITAL ERA OF STEGANOGRAPHY

Modern steganography entered the world in 1985 with the boost in computer power and the development of digital signal processing (DSP), information theory and coding theory (Ashok et al., 2010). Hiding a message within an image, audio or video file and used it as an alternate to encryption, takes advantage of useless or unused bits within the file structure or bits that are mostly undetectable if altered (Muttoo and Kumar, 2009). A steganographic message rides secretly to its destination, unlike



encrypted messages which although undecipherable without the decryption key, it can be identified as encrypted.

## 2.7 APPLICATION OF INFORMATION HIDING

Information hiding techniques provide services to many applications in different aspects of life some of them are (Peticolas, 1999), (Anderson and Petitcolas, 1998) and (Kaul, 2011):

- i. Many manufacturers tend to hide copyright in their product in order to ensure the original copies.
- ii. Information senders always need to protect their secret information by hiding them in digital covers.
- iii. In currency industries, watermark, hard curves, or another type of information are hidden in order to prevent currency forgery.
- iv. Computer users tend to hide private information inside their computer especially when another person can use these computers.
- v. Medical imaging systems are used in health care industry. The standards like DICOM systems, is used where the embedding data of the patient will be extracted from the pictures, which is better than saving the picture and the information separately.

## 2.8 TYPES OF COVERS

Steganography researchers tend every time to hide their secret message in a new type of cover but they are most commonly used covers such as hiding in text, image, video, audio, network packets and file storage systems.

### 2.8.1 Hiding in Text

Many techniques can be used to hide secret message inside digital text. Some of these hiding techniques are based on manipulating the positions of lines and words (Changder et al., 2010), (Moerland, 2003) and (Low et al., 1995) where documents are

used as a digital form, secret messages can be hidden in the slack spaces of its form. Hyper Text Markup Language (HTML) files can also be used to carry information since adding space tabs, invisible characters, or extra lines breaks are ignored by web browsers. The extra spaces and lines are imperceptible revealing the source of the web (Castro, 1999 and Bennett, 2004).

### **2.8.2 Hiding in Image**

Images can be considered as one of the most well known covers that are used to carry secret messages because images contain huge amount of data, which means a lot of areas for hiding. In addition, image view may take the detector attention away from the hidden information. This type of covers which is used in this research work, has many types of hiding techniques such as (Khalaf and Sulaiman, 2011 and Amin et al., 2003):

- i. Least significant bit insertion (LSB)
- ii. Masking and filtering
- iii. Transform techniques

### **2.8.3 Hiding in Video and Audio**

Video and audio provide advantages of hiding secret messages in unused changeable fields of their headers. Embedding techniques can range from the replacement of information in imperceptible levels (notes), manipulation of compression algorithms, and modification of carrier properties. In general these hiding techniques may imply: adding small echoes or adding slight delay, or a subtle signal that can be masked by signal of higher amplitude (Mitra and Manoharan , 2009), (Sherly and Amritha, 2010).

### 2.8.4 Hiding in Network Packets

Sending messages using different transmission protocols usually contain features that can be used to hide secret messages. Transmission control protocol/Internet protocol (TCP/IP) packets contain slack spaces that can be used for carrying secret messages (Fraczek et al., 2010) as shown in Figure 2.9.

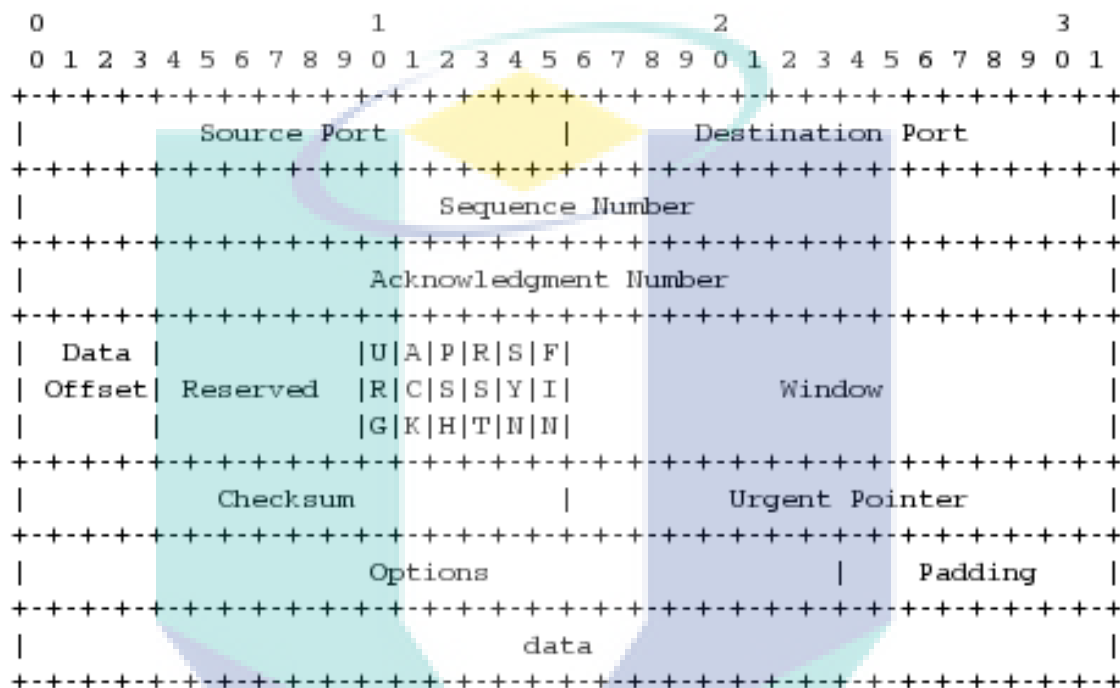


Figure 2.9: header of TCP protocol (Murdoch and Lewis,2005)

### 2.8.5 Hiding in File Storage Systems

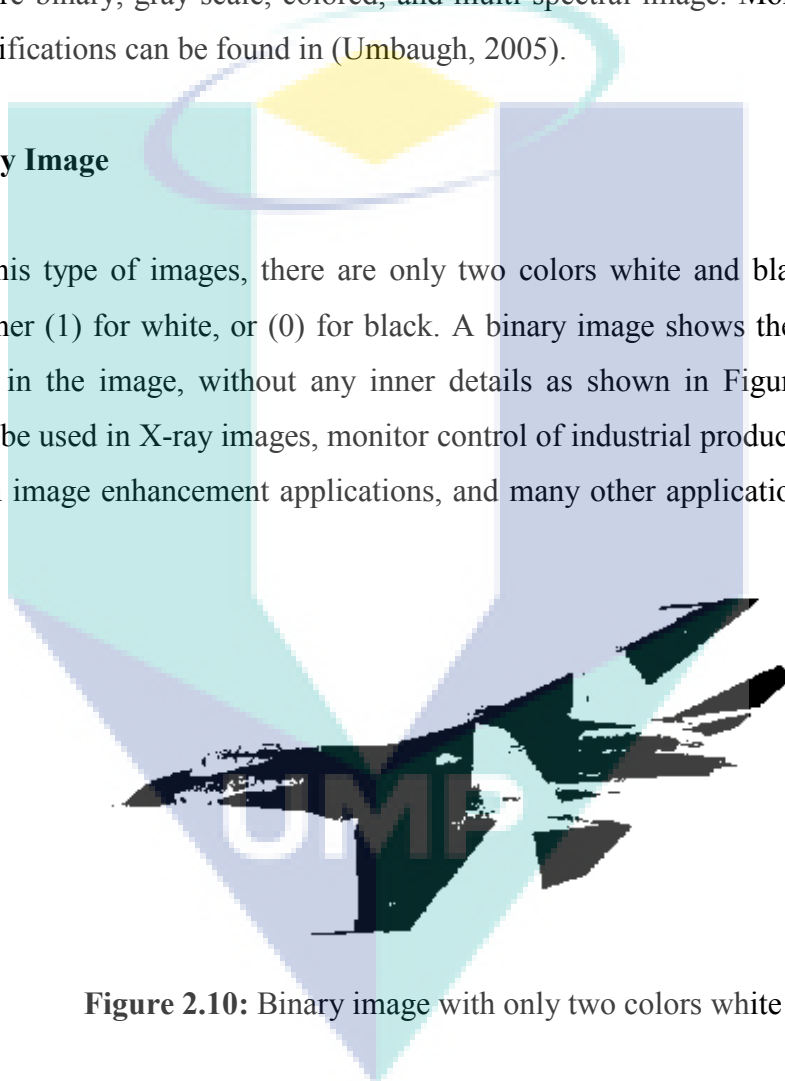
Some hiding techniques depend on finding unused spaces that readily apparent to an ordinary user. Operating systems use storing techniques which results in slack spaces in which these spaces are imperceptible. Another technique creates hidden partitions and if the system stays normally, these partitions cannot be visually detected (Johnson, 1998).

## 2.9 DIGITAL IMAGE REPRESENTATION

Digital images are large two-dimensional array of numbers. These numbers represent brightness intensities at each position  $(x, y)$  of the image  $f(x,y)$ , which can be called pixels (picture elements) (Khalaf and Sulaiman, 2011), (Bharati and MacGregor, 2000). Images can be classified (according to the colors of its contents) into four main types that are binary, gray-scale, colored, and multi-spectral image. More details about image classifications can be found in (Umbaugh, 2005).

### 2.9.1 Binary Image

In this type of images, there are only two colors white and black. Each pixel value is either (1) for white, or (0) for black. A binary image shows the boundaries of the objects in the image, without any inner details as shown in Figure 2.10. Binary images can be used in X-ray images, monitor control of industrial production lines, edge detection in image enhancement applications, and many other applications, (Umbaugh, 2005).

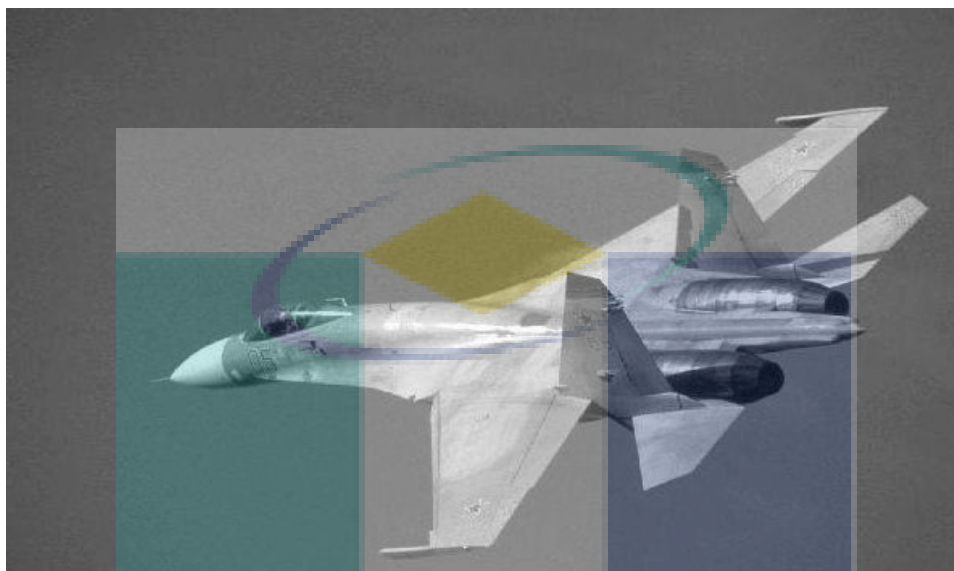


**Figure 2.10:** Binary image with only two colors white and

### 2.9.2 Gray-Scale Image

Pixel values of binary image can be expanded to (0-255) range, in which there are 256 colors available: white, black, and 254 levels of gray color. This image may give a good view when color details are not needed, or less storage area is available, as shown in Figure 2.11. If the color level is either (Red, Green, or Blue) then the image is called Monochrome image, (Umbaugh, 2005). A binary image can be derived from

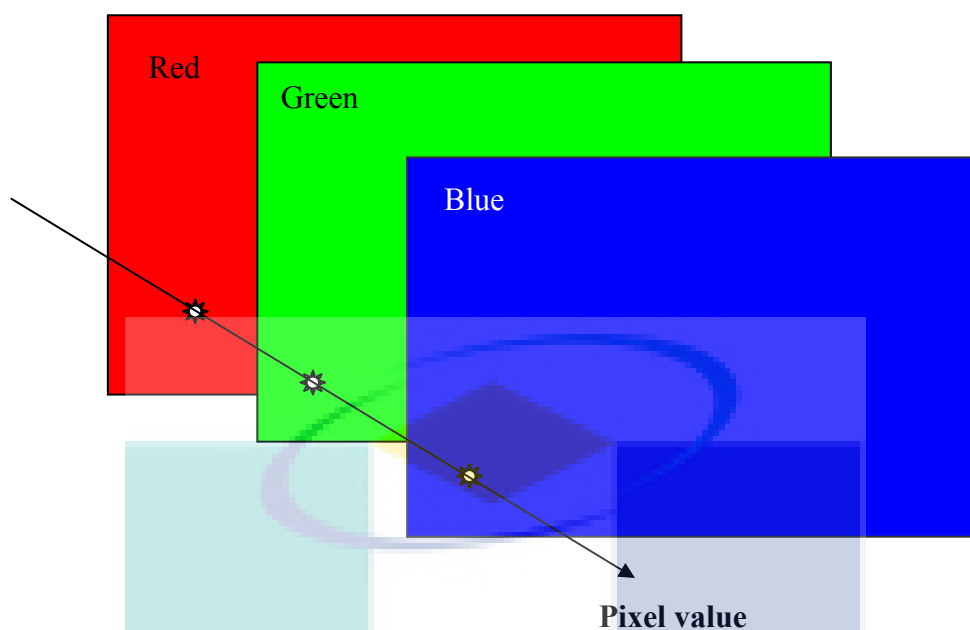
gray scale image by determining a threshold and setting any value greater than threshold to (255) and the other to (0) (Shapiro and Stockman, 2002). Figure 2.11 is derived from Figure 2.10 after thresholding operation was applied.



**Figure 2.11:** Gray scale image with 256 levels of gray color

### 2.9.3 Colored Image

There are three essential colors that are red (R), green (G), and blue (B), and any color can be produced by mixing them. Instead of storing huge number of colors, computers store three values for each pixel R, G, and B respectively and generate colors by displaying these values on the monitor at the same time, as shown in Figure 2.12. This system is called RGB system (Umbaugh, 2005). Besides RGB, the color can also be represented using cyan (C), magenta (M) and yellow (Y), also known as CMY. The brightness information is similar to the brightness information contained in a gray-scale image. The level of brightness will control the intensity of red, green or blue used in an image. If an image uses  $n$  bits for a single color, then the image can have up to  $2^{3n}$  colors.



**Figure 2.12:** Colored image representation (three essential color planes)

#### 2.9.4 Multi - Spectral Image

This form of image typically contains information outside the normal human perceptual range. This may include infrared, ultraviolet, acoustic, or radar images. These are not images in the usual sense because information represented is not directly visible to the human visual system. It can be displayed as a visual form by mapping the different spectral bands to RGB system (Umbaugh, 2005).

### 2.10 STEGANOGRAPHY TECHNIQUES

There are three different approaches that can be used to hide information in a cover object i.e. injection, substitution and generation.

#### 2.10.1 Injection Technique

Using this technique, the data can be hidden in sections of a file that are ignored by the processing application (Mastronardiet al., 2003). Therefore file bits that are relevant to an end-user are not modified and leaving the cover file perfectly usable. The

simplest example is the use of the hidden attribute in the Microsoft Word, which allows for hiding text with a special, hidden font. This very simple technique was used to store notes and references during the creation of this document. The problem with this kind of embedding is that it usually makes the host file larger, and therefore the alteration is easier to detect.

### **2.10.2 Substitution Technique**

Substitution technique is used to replace the least significant bits of information that determine the meaningful content of the original file with new data. However, the substitution method can degrade the quality of the original host file depending on the type of host file and the amount of hidden data. The main advantage of this technique is that the cover file size does not change after the execution of the algorithm. On the other hand, this approach has at least two drawbacks. First, the resulting stego object may be adversely affected by quality degradation and that may arouse suspicion. Second, substitution limits the amount of data that can hide to the number of insignificant bits in the file (Ashok et al., 2010).

### **2.10.3 Generation Technique**

Generation technique does not require an existing cover file, unlike injection and substitution (Shirali-Shahreza, 2008). This technique generates a cover file for the sole purpose of hiding the message. The main problem of insertion and substitution techniques is using the same object. Therefore, people can compare the stego object with any pre-existing copy of the cover object and discover differences between the two. There is some problem when using a generation approach because the result is an original file, and it is therefore immune to comparison tests.

## **2.11 STEGANOGRAPHIC ALGORITHMS**

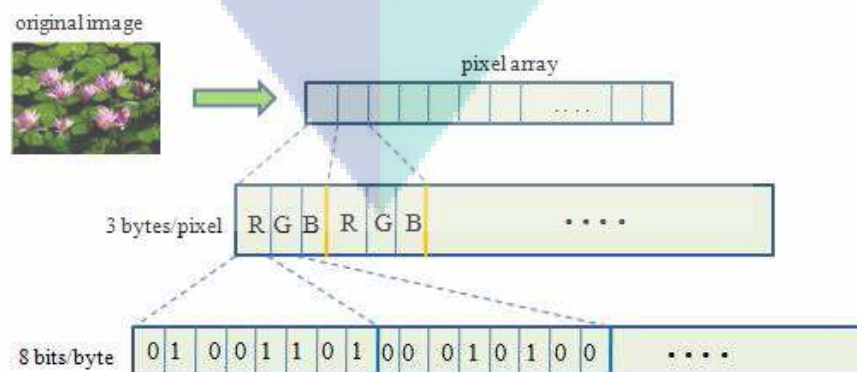
The steganographic algorithms proposed in the literature can broadly be classified into two categories:

1. Spatial Domain Techniques
2. Transform Domain Techniques

Each of these techniques is covered in detail in the next two subsections.

### 2.11.1 Spatial Domain Algorithm

In Spatial domain algorithms, the cover image pixels are directly used to inscribe bits of the secret data (Macq and Quisquater, 1995). LSB-based techniques are the most widely known steganography algorithms. There are some methods to replace the least significant bits of an image pixel. These modifications could be interpreted as random noise according to a secret key. Here is an example of modifying the LSBs, suppose we have three R, G, and B component in an image. Their value for a chosen pixel is green  $(R,G,B) = (0, 255, 0)$ . If a steganography algorithm wants to hide the bit value 1 in R component then the new pixel value has components  $(R,G,B) = (1, 255, 0)$ . As this modification is so small, the new image is indistinguishable to the human eye from the original one (Wilson and bryon, 1992) as shown in Figure 2.13. The disadvantages of these techniques are that they are highly sensitive to signal processing operations and can be easily damaged. For example, lossy image compression could completely defeat the hidden information. In other words, steganography in the spatial domain is easy to destroy using some attacks such as low-pass filtering. As a result, transform domain steganography algorithms are used.



**Figure 2.13:** Hiding information in LSB of the color component (Fridrich et al., 2010)



### 2.11.2 Transform Domain Algorithm

Transform domain algorithms hide data in significant areas of cover image using mathematical functions that are in compression algorithms to makes them robust against various image processing operations like compression, enhancement etc. (Wang and Moulin, 2003). The Spatial domain methods are less complex as no transform is used, but are not robust against attacks. On the other hand, transform-domain techniques are typically much more robust to image manipulation compared to the spatial domain techniques. This is because the transform domain does not use the original image for embedding the secret data.

The Discrete Wavelet Transform: The Discrete Wavelet Transform (DWT) Dilations and translations of the "Mother function," or "analyzing wavelet"  $\Phi(x)$  define an orthogonal basis, the wavelet basis is:

$$A_{mn} = \sum_{p=0}^{M-1} \sum_{q=0}^{N-1} \alpha_p \alpha_q B_{pq} \text{Cos} \frac{\pi(2p+1)p}{2m} \text{Cos} \frac{\pi(2n+1)q}{2n} \quad (2.4)$$

Where:  $s$  and  $l$  are integers that scale and dilate the mother function  $\Phi(x)$  to generate wavelets.

The scale index  $s$  indicates the wavelet's width and the location index  $l$  gives its position.

Notice that the mother functions are rescaled, or "dilated" by powers of two, and translated by integers (Graps, 1995). What makes wavelet bases especially interesting is the self-similarity caused by the scales and dilations. To span the data domain at different resolutions, the analyzing wavelet is used in a scaling equation:

$$W(x) = \sum_{k=-1}^{N-2} (-1)^k c_{k+1} \Phi(2x+k) \quad (2.5)$$

where  $W(x)$  is the scaling function for the mother function  $\Phi(x)$   
 $Cx$  are the wavelet coefficients.

The wavelet coefficients must satisfy linear and quadratic constraints of the form

$$\sum_{k=0}^{N-1} c_k = 2 \quad , \quad \sum_{k=0}^{N-1} c_k c_{k+2l} = 2\delta_{l,0} \quad (2.6)$$

where  $\delta$  is the delta function and  $l$  is the location index.

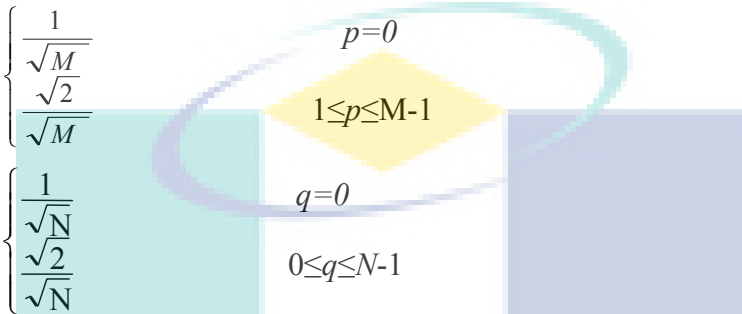
The wavelet coefficient matrix is applied in a hierarchical algorithm, sometimes called a pyramidal algorithm. The wavelet coefficients are arranged so that odd rows contain an ordering of wavelet coefficients that act as the smoothing filter, and the even rows contain an ordering of wavelet coefficient with different signs that act to bring out the data detail. The matrix is first applied to the original full-length vector. Then the vector is smoothed and decimated by half and the matrix is applied again. Then the smoothed, halved vector is smoothed, and halved again, and the matrix is applied once more. The output of the DWT consists of the remaining "smooth (etc.)" components, and all of the accumulated "detail" components (Graps, 1995). The Haar transform preserves the average in the smoothed values. This is not true for all wavelet transforms.

After decomposing the cover image into sub-bands, the DCT transform will be applied on the selected sub-bands. The discrete cosine transform (DCT) is used to decompose the image data into parts (or spectral sub-band) of different importance (depending on the image). The DCT is similar to the discrete Fourier transform. It transforms a signal from the spatial domain to the frequency domain (Jeong et al., 2005). DCT transform does not affect the input image size, i.e. if the input image is of size  $(n \times m)$ , the output image will be of the same size. DCT transform is often used in compression technique because it tends to concentrate image information. The general equation for a 2D  $(N$  by  $M$  image) DCT is defined by the following equation:

$$B_{pq} = \alpha_p \alpha_q \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} A_{mn} \cos\left(\frac{\pi(2m+1)p}{2M}\right) \cos\left(\frac{\pi(2n+1)q}{2N}\right) \quad (2.7)$$

where  $B_{pq}$ : The element of the output image

$$\alpha_p = \begin{cases} \frac{1}{\sqrt{M}} & p=0 \\ \frac{\sqrt{2}}{\sqrt{M}} & 1 \leq p \leq M-1 \\ \frac{1}{\sqrt{M}} & \end{cases}$$

$$\alpha_q = \begin{cases} \frac{1}{\sqrt{N}} & q=0 \\ \frac{\sqrt{2}}{\sqrt{N}} & 0 \leq q \leq N-1 \\ \frac{1}{\sqrt{N}} & \end{cases}$$


Original image can be reconstructed by applying the following equation of the inverse of discrete cosine transform (DCT<sup>-1</sup>) (Khayam, 2003):

$$A_{mn} = \sum_{p=0}^{M-1} \sum_{q=0}^{N-1} \alpha_p \alpha_q B_{pq} \cos\left(\frac{\pi(2m+1)p}{2M}\right) \cos\left(\frac{\pi(2n+1)q}{2N}\right) \quad (2.8)$$

Where  $0 \leq m \leq M-1$ ,  $0 \leq n \leq N-1$

The above equation of DCT works on  $m \times n$  image (typically  $8 \times 8$ ). DCT can be performed by using the following steps:

1. Dividing it into blocks of  $(8 \times 8)$  pixels.
2. Applying DCT equation (2-1) to each block  $B_i$ . The result is a block (vector)  $W^i$  of 64 weights  $W^i$  (where  $i=0,1,2,\dots,63$ ).
3. The  $k$  vectors  $W$  ( $i=1,2,\dots,k$ ) are separated into 64 coefficient vector  $C^i$  where the  $k$  elements of  $C^w$  are  $(W_{j1}, W_{j2}, W_{j3}, \dots, W_{jk})$ . The first coefficient vector  $C^0$  consists of the  $k^{\text{th}}$  DCT coefficients.
4. Each coefficient vector  $C^j$  is quantized separately to produce a quantized vector  $Q^j$ , which is written on the compressed stream.

## 2.12 STATISTICAL DETECTION

Statistical detection methods are based on the fact that hiding information in digital image causes alteration in the statistical properties. Thus steganalysis statistically depends on testing these features (Amin et al., 2007). If the original innocent image is unavailable then the correlation of these properties are tested, else, there are several statistical tests that can be used such as (Zaidan et al., 2010). The detail explanation of the metrics is as described below:

- i. Peak signal to noise ratio (PSNR) (Lu and Liao, 2001 and Yuzhong et al., 2004) to evaluate the performance of the proposed scheme and image quality. It is the most common metric used to evaluate the stego image quality, PSNR is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale (Huynh-Thu and Ghanbari, 2008), which is defined as:

$$PSNR = 10 \log_{10} \left( \frac{255^2}{MSE} \right) dB \quad (2.9)$$

$$MSE = \frac{\sum_{i=0}^{n-1} \sum_{j=0}^{m-1} (a_{i,j} - b_{i,j})^2}{w \times h} \quad (2.10)$$

Where  $w \times h$  is the image size  
 $a_{i,j}$  and  $b_{i,j}$  are the corresponding pixel values of two images

The PSNR is often expressed on a logarithmic scale in decibels (dB). A larger PSNR value means stego-image preserves the original image quality better. In general, the distortion of the stego-image that caused by the embedding can be obvious when the PSNR values fall below 30 dB, while the stego-image is considered as high quality when PSNR value is 40 dB and above (Cheddad et al., 2008).

- ii. Mean Square Error (MSE) is the simplest of image quality measurement, the larger the value of MSE means that the image has poor quality (VORA et al., 2010 and Desai and Kulkarni, 2010). The equation of MSE is as mentioned in the PNSR.
- iii. Normalized Absolute Error (NAE) is used to check the possible pixel value of the image, where the large value means that image has poor quality and the value closer to one indicates better encryption (VORA et al., 2010 and Desai and Kulkarni, 2010 and Udomhunsakul and Hamamoto, 2004). NAE is defined as follow:

$$NAE = \frac{\sum_{m=1}^M \sum_{n=1}^N |x(m,n) - x^{\wedge}(m,n)|}{\sum_{m=1}^M \sum_{n=1}^N |x(m,n)|} \quad (2.11)$$

Where:  $x(m,n)$  is the original MxN pixel image  
 $x^{\wedge}(m,n)$  is the reconstructed image

- iv. Maximum Difference (MD), where the large value means that image has poor quality (VORA et al., 2010 and Desai and Kulkarni, 2010 and Udomhunsakul and Hamamoto, 2004). MD is defined as follow:

$$MD = \text{Max}[|x(m,n) - x^{\wedge}(m,n)|] \quad (2.12)$$

Where:  $x^{\wedge}(m,n)$  is the reconstructed image  
 $x(m,n)$  is the original MxN pixel image

- v. Structural Content (SC), where the large value means that image is poor quality (VORA et al., 2010 and Desai and Kulkarni, 2010). SC is defined as follow:

$$SC = \frac{\sum_{m=1}^M \sum_{n=1}^N x(m,n)^2}{\sum_{m=1}^M \sum_{n=1}^N x^{\wedge}(m,n)^2} \quad (2.13)$$

Where:  $x(m,n)$  is the original MxN pixel image  
 $x^{\wedge}(m,n)$  is the reconstructed image

- vi. Normalized cross-correlation (NC) is a measure to compare between the original and encrypted message. The range of NC metric values is between 0 (dissimilar) and 1 (similar), (Wang et al., 2008). as follows:

$$NC(M, M') = \frac{\sum_{k=1}^N M(k)M'(k)}{\sqrt{\sum_{k=1}^N M(k)^2} \sqrt{\sum_{k=1}^N M'(k)^2}} \quad (2.14)$$

Where  $M$  is original secret message  
 $M'$  is extracted secret message

### 2.13 RELATED WORK

Many data hiding methods have been proposed to hide secret data into an image. The original image was decomposed into four bands using the Haar wavelet and then DCT was performed on each of the bands. The watermark was embedded into the DCT coefficients of each band and a great number of coefficients were used. Each band gave a different detection output. The result was taken as the average detection result of all bands (Fotopoulos and Skodras, 2000). Serkan Emek and Melih Pazarci (2006) compared image dependent and additive blind watermarking algorithms that embedded a watermark in the DWT-DCT domain by taking the properties of the HVS into account (Emek, 2006). The image dependent algorithm modulated the watermarking coefficients with original mid-frequency DWT-DCT coefficients (Emek and Pazarci, 2006). Ali Al-Haj (Al-Haj, 2007) described a combined DWT-DCT digital image watermarking algorithm that embedded the watermark in the first and second level of DWT coefficient sets of the host image, followed by the application of DCT on the selected DWT coefficient sets. However, robustness of common DWT and DCT transform methods was increased by the previous hybrid method. Despite, their robustness against noise and blurring attack was not acceptable. In order to solve this problem, a new image watermarking algorithm based on jointed DWT-DCT method was presented in this paper. In the proposed method, watermarking was done by altering the wavelets coefficients of middle frequency coefficient sets of 3-levels DWT transformed host image, followed by the application of the DCT transform on the selected coefficient sets. The difference between Al-Haj's method and the proposed was in the selection of

sub-band for embedding watermark and novel pre-processing before the extraction procedure. Al-Haj had chosen HL sub-band in 2-level DWT transform to performing block DCT on them. However, the proposed method used all of the HL frequency sub-band in the middle frequency coefficient sets LHx and HLx in 3-levels DWT transformed image. Using this algorithm, coarser level of DWT in terms of imperceptibility and robustness was chosen to apply 4×4 block-based DCT on them, and consequently higher imperceptibility and robustness could be achieved. In addition, pre-filtering operation was used before extraction of the watermark. Sharpening and Laplacian of Gaussian (LoG) filtering were used to increase the different between information of watermark and hosted image.

LSB image data hiding is the most classic and simplest techniques, which embeds secret messages in a subset of the LSB plane of the image (Chan and Cheng, 2004). Pixel-value differencing data hiding technique (PVD) proposed by Wu and Tsai in (Wu, and Tsai, 2003) can hide a large amount of secret bits into a still image by modifying the difference values between pairs of adjacent pixels. In this technique, more data were inserted into areas where undulation of pixel-values was large as pixels in these areas can tolerate more changes, this leads to good imperceptibility with a high embedding rate. A grey-valued cover image was partitioned into non-overlapping blocks of two consecutive pixels, states  $p_i$  and  $p_{i+1}$ . From each block a different value i.e.  $d_i$ , can be obtained by subtracting  $p_i$  from  $p_{i+1}$ . All possible different values of  $d_i$  range from -255 to 255, and then  $|d_i|$  ranges from 0 to 255. Therefore, the pixels  $p_i$  and  $p_{i+1}$  are located within the smooth area when the value  $|d_i|$  is smaller and will hide less secret data. Otherwise, it is located on the edged area and embeds more data. From the aspect of human vision it has a larger tolerance that embeds more data into edge areas than smooth areas. PVD+3LSB method proposed in (Wu et al., 2005) aims to increase capacity by using a LSB method and it is still using Wu and Tsai's scheme for edge areas. The division between the 'lower-level i.e. smoothness areas' and 'higher-level i.e. edge areas' of the range table is controlled by the users. Anyone who has extracted the secret data from a stego-image must use the original division. A division is the key of the extracted secret data. In the lower level of the range table, each block of two continuous pixels will hide 6-bit secret data (i.e. each pixel hides 3-bit secret data), otherwise (such as the higher-level of the range table), the bit-number of hidden data

depends on di. Semi-hexagonal PVD method proposed by Awad Kh Al-Asmari and Oyed Al-Gamdi in (Khalaf et al., 2005) presented a new method for data hiding cover image by dividing it into sub-blocks of semi hexagonal shape. The embedding technique is also based on pixel value difference (PVD) approach. In the proposed method, the DWT and DCT transforms have been used, to exploit the advantages of the two methods.

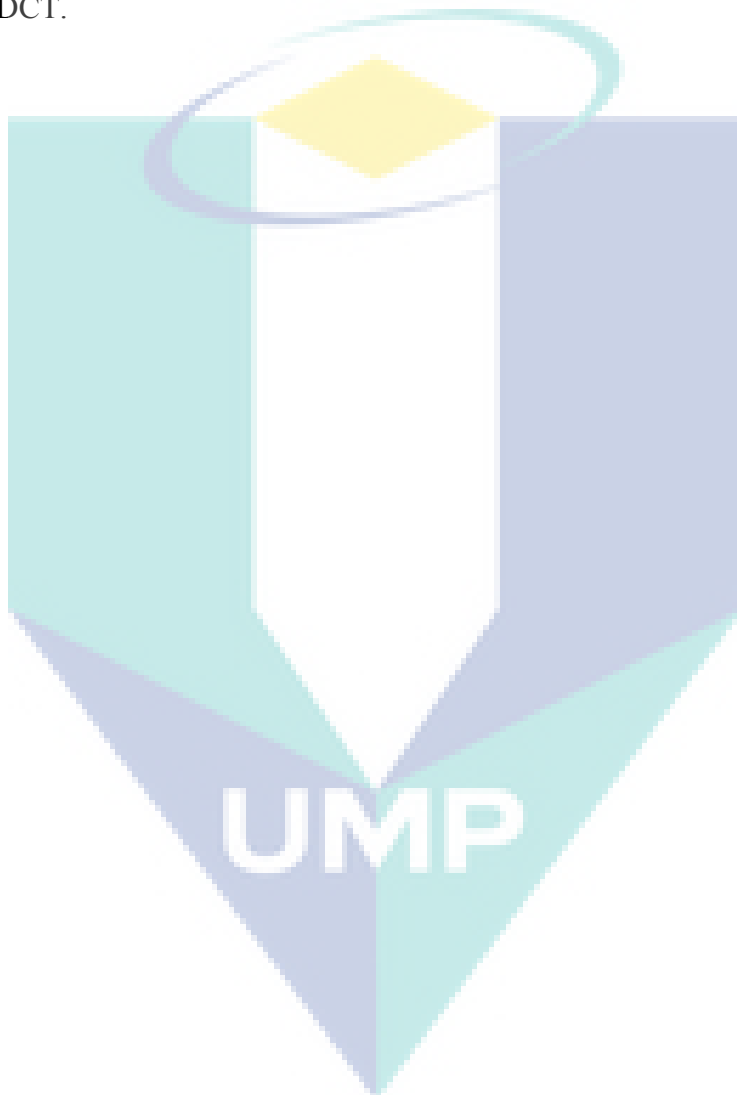
Several researches have been done to improve the security of the Hill cipher. Yeh et al. (Yeh et al., 1991) used two coprime base numbers that are securely shared between the participants. Although their schemes threat the known plaintext attack, it was so time-consuming which required many mathematical manipulations and it was not efficient especially when dealing with a bulk of data. Saeednia (Saeednia, 2000) tried to make the Hill cipher secure by using some random permutations of columns and rows of the key matrix but it was proved that his cryptosystem was vulnerable to the known-plaintext attack (Lin et al., 2004), the same vulnerability of the original Hill cipher. Lin et al. (Lin et al., 2004) tried to improve the security of the Hill cipher using several random numbers generated in a hash chain but their scheme as not efficient. Ismail et al. (Ismail et al., 2006) used an initial vector that multiplied successively by some orders of the key matrix to produce the corresponding key of each block but it had several security problems (Li et al., 2008). In the proposed method, a secure cryptosystem was introduced that overcomes all the security drawbacks of the Hill cipher

## 2.14 SUMMARY

This chapter presented a background of the ancient and modern cryptography as well as steganography. The Hill cipher is a classical symmetric cryptography algorithm which has several advantages such as its capability to disguise letter frequencies of the plaintext, its simplicity because of simple matrix calculations for encryption and decryption, a well as its high speed and throughput. Therefore, this method was chosen as an encryption method in the proposed system. On the other hand, Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) have been widely used in many digital watermarking applications. DWT has been used to



decompose the image into four sub-bands and it is excellent in spatial localization and multi-resolution characteristics, which are similar to the theoretical models of the human visual system. DCT is used to get three frequency coefficient sets: low frequency sub-band, mid-frequency-sub-band and high frequency sub-band. Further performance improvements in DWT-based digital image steganography algorithms could be obtained to get sufficient payload while keeping image quality by combining DWT with DCT.



## CHAPTER 3

### DESIGN

#### 3.1 INTRODUCTION

Transferring digital media across the network became easy with the development of internet applications. Therefore, the issue of protection of confidential communications during transmission becomes important. By using classical cryptographic only, it makes the message look like a clutter data and therefore cannot pass the check point on the web (Schneier, 1996). The utilization of steganography will add additional layer of protection on a secret message (Kahn, 1996) which make a secret message an integral part of other media such as image, audio and video so that the transmitted data will be meaningful and harmless to all. Images are the most widespread carrier medium used as a high hiding capacity.

The relationship between steganography, watermarking and cryptography is as shown in Figure 3.1. Steganography and watermarking are both related to a broader subject known as information hiding. The arrow indicates an extension and boldface indicates the focus of this study.

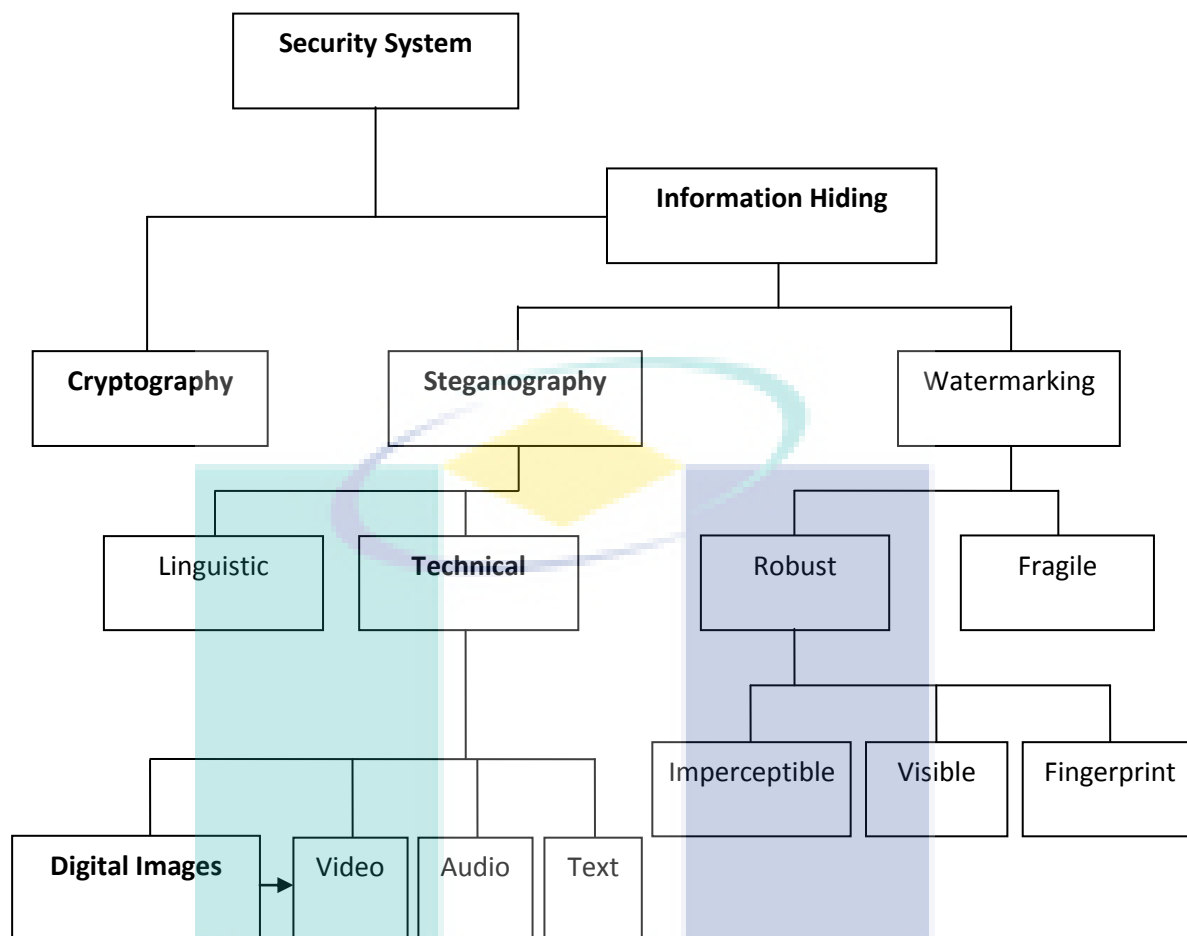


Figure 3.1: Relation between steganography, watermarking and cryptography (Cheddad et al, 2010)

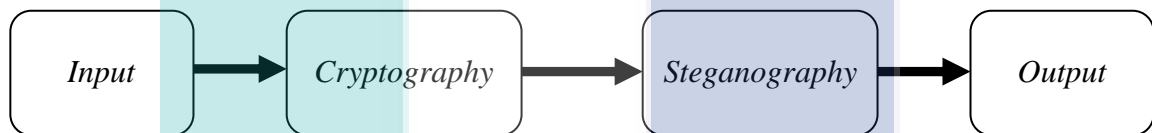
In this work, steganography will be the main approach of information hiding, thus digital watermarking will not be investigated. Steganography and Cryptography are well known and widely used techniques for providing secret communication. However, steganography is different for cryptography. Cryptography scrambles a message so it cannot be understood by a malicious people, whereas steganography hides the message so that it cannot be seen. Although both methods provide security, steganography must not be confused with cryptography. Cryptography transforms the message so that it will become meaningless to a malicious people who intercept it.

The definition of breaking the system was studied by Amin (Amin et al., 2003). In cryptography, the system is broken when the attacker read the secret message.

Breaking a steganographic system needs the attacker to detect that steganography has been used and he is able to read the embedded message.

In cryptography, the structure of a message is scrambled to make it meaningless and unintelligible unless the decryption key is available. It makes no attempt to disguise or hide the encoded message.

This chapter presents the design of the developed system which uses both cryptography and steganography for better confidentiality and security. This method consists of three phases: encrypting using "improved block cipher based on random key", hiding data in a cover image based on joint DWT and DCT transformation, as well as combining encrypting and hiding as shown in Figure 3.2.



**Figure 3.2:** Combine encrypting and hiding (Challita and Farhat, 2011)

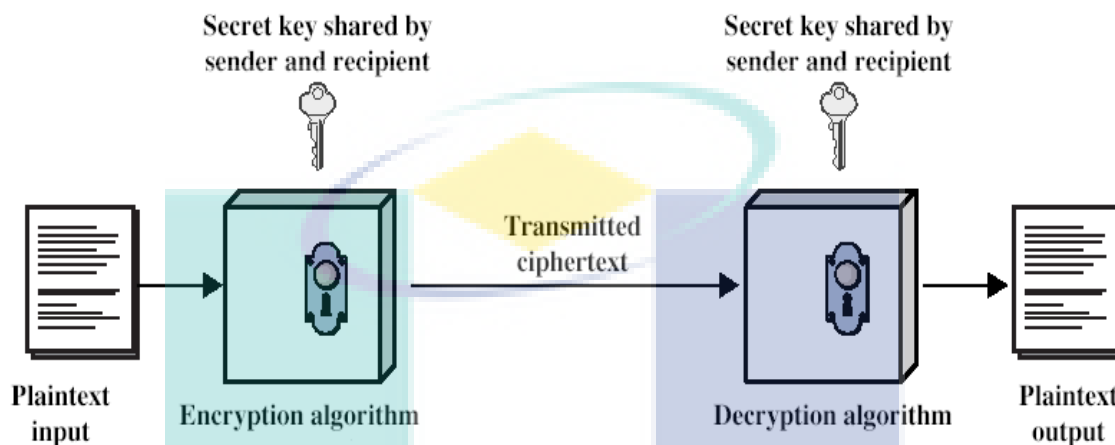
This system will be running on a computer with Windows 7 Ultimate, processor: Genuine Intel (R) CPU 585 @ 2.16 GHz and Memory (RAM) 1.00GB. The algorithms will be implemented using MATLAB 9, Microsoft Picture Manager and Photoshop image editing software.

Several statistical tests will be used for the evaluation purposes (Zaidan et al., 2010). The following metrics are used to evaluate the proposed methods:

- 1- Mean Squared Error (MSE).
- 2- Root Mean Square Error (RMSE).
- 3- Peak Signal-to-Noise Ratio (PSNR).
- 4- Normalized Cross Correlation (NC).
- 5- Histogram Similarity.
- 6- The Normalized Absolute Error (NAE).
- 7- The Maximum Difference (MD).
- 8- The Structural Content (SC).

### 3.2 FIRST PHASE: ENCRYPTION

A common symmetric cryptography Hill cipher method has been improved, where sender and recipient share the same key, as shown in Figure 3.3.



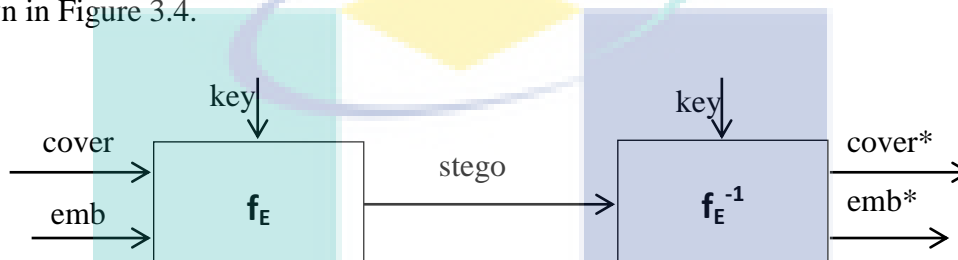
**Figure 3.3:** Simplified model of symmetric encryption

#### 3.2.1 Improved Block Cipher Based on Random Key

The proposed method is called "improved block cipher based on random key". It addresses the issues of the classic hill cipher algorithm. The encryption is extended to include special characters and digits by using the ASCII table for converting to numbers and vice versa. The key matrix will be selected randomly based on the password and variable length. Both the password and the value of the length will be entered by the user. In the classical method the sender must repeat entering the encryption key for N times, besides there were testing processes to check if the matrix is invertible or not, thus making the method not efficient as it takes long time. Therefore, the proposed method is suggested to replace the summation instead of multiplication process.

### 3.3 SECOND PHASE: HIDING

Steganography is not only hiding the confidential message but also making the hackers believe that the source is clean and they cannot even realize that it contains some hidden information. Cover object is any object that can be used to hold secret information inside. This stego object is sent to the receiver where receiver will get the secret data out of the stego image by applying decoding algorithm technique. Basic model of steganography consists of cover object, secret information and stego keys shown in Figure 3.4.



**Figure 3.4:** basic model of steganography (Amin et al., 2003)

$f_E$ : steganographic function "embedding"

$f_E^{-1}$ : steganographic function "extracting"

cover: cover data in which emb will be hidden

where

emb: message to be hidden

key: parameter of  $f_E$

stego: cover data with the hidden message

#### 3.3.1 Secured System Based On Joint DWT-DCT (SSBDD)

For the proposed system (SSBDD), the transform domain approach has been used to address the limitations of spatial domain. Transform domain methods are more complex than the spatial domain ones. However, they are more secure and tolerant to noise, as it takes the advantages of the special properties of transform domains.

Transformation steps cause a set of slack spaces that can be used for hiding information (Santhi and Thangavelu, 2011). Each transformation has different spaces, which can be used for hiding data in completely different way from another (Salvado and Roque, 2004).

The 2-D filters divide the 2-D images into four sub-bands LL, HL, LH and HH. The LL is the coarse-scale wavelet coefficients while HL, LH and HH are the fine-scale of wavelet coefficients. To obtain the next coarser scale of wavelet coefficients, the sub-band LL is further processed until some final scale N is reached. When N is reached they will be  $3N+1$  sub-bands consisting of the multi-resolution sub-bands LL and LH, HL and HH

where

LL – Lower resolution version of image

HL – Vertical edge data

LH – Horizontal edge data

HH – Diagonal edge data

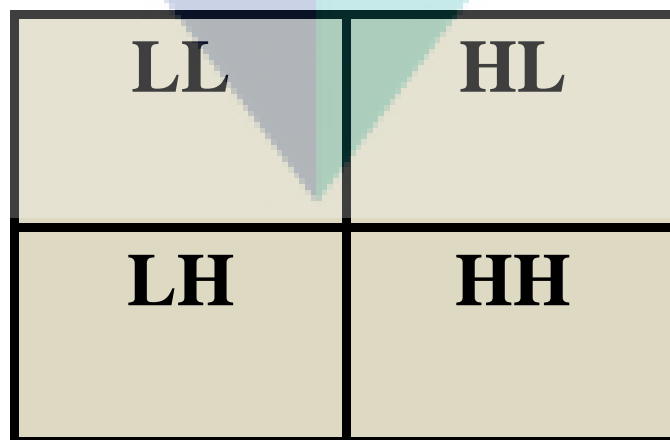
Data can be embedded effectively using DWT and it will be very suitable to identify the areas in the cover image, due to its excellent "spatio-frequency" localization properties. The coefficient sets can be down sampled without loss of the image information because the bandwidth of the coefficient sets for the resulting sub-bands are smaller than that of the original image. In particular, the property of the masking effect of the human visual system can be exploited by only modifying DWT coefficient of the region corresponding. In general, in the lower frequency coefficient sets LL is concentrated the most image energy. So, hiding in this coefficient sets could increase robustness but at same time may degrade the image significantly. On the other hand, changing in the high frequency coefficient sets HH will not be generally sensitive to the human eye where it includes the edges and textures of the image. This allow to embedding data without being perceived by the human eye. The method of hiding data in the middle frequency coefficient sets HLX and LHX of the image is better in perspective of imperceptibility and robustness (Al-Haj, 2007).

The Wavelet transform is closer to human visual system (HVS). It decomposes the cover image into four non-overlapping multi-resolution sub-bands LL, HL, LH and HH. The benefit of decomposing cover image has been exploited in the proposed system to choose the most proper sub-bands. In particular, the Haar wavelet basis has been chosen because the transform is equal to its inverse and operates on data by calculating the sums and differences of adjacent elements. DCT gives three frequency coefficient sets: low frequency sub-band, mid-frequency-sub-band and high frequency sub-band. The first operation of wavelet set on adjacent horizontal elements and then on adjacent vertical elements. Each transform computes the data energy in relocating to the top left hand corner. Figure 3.5 shows the image of children before and after the one Haar wavelet transform.



(a) Original image

(b) After Haar DWT



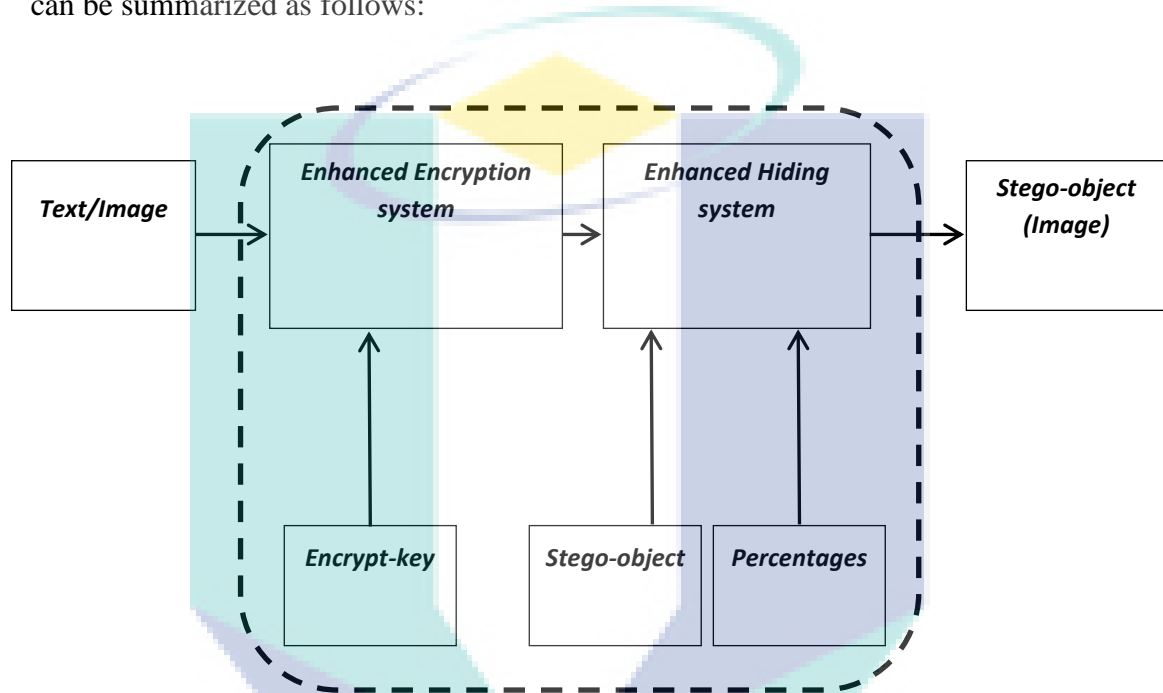
(c) Haar DWT sub-bands

**Figure 3.5:** Children image before and after one Haar wavelet transform



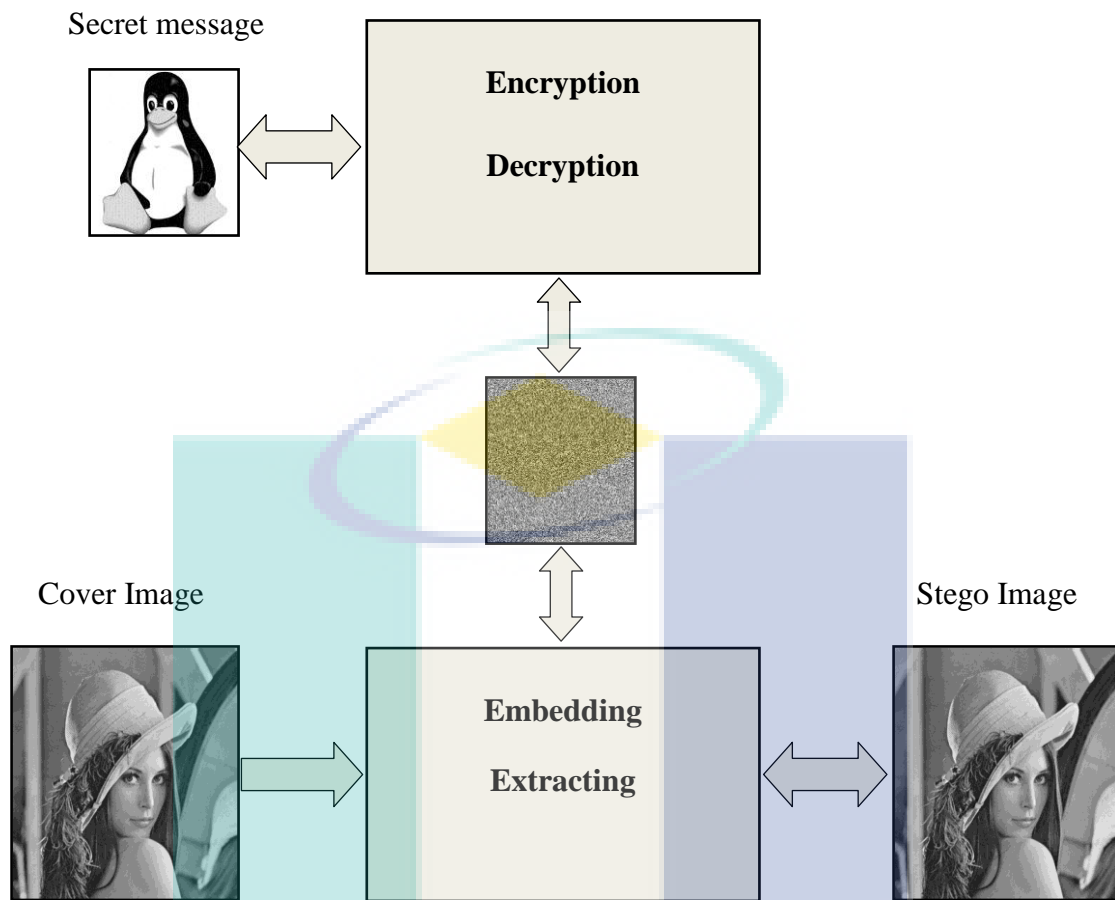
### 3.4 THIRD PHASE: COMBINATION OF ENCRYPTION AND HIDING

This part consists of encryption and hiding information after the completion of message encryption using the improved block cipher based on random key. Hiding encrypted message within the image using the secured system based on joint DWT-DCT (SSBDD) is as shown Figure 3.6. The combinations of the two techniques can be summarized as follows:



**Figure 3.6:** Proposed system (encryp-setogano)

Cryptography and Steganography are popular and widely adopted techniques to hide and code the information. Steganography is the art and science of communicating in a way that hides the existence of the communication. Cryptography scrambles a message to make it difficult to be understood while the steganography is used in message hiding. The key objective of this study is to develop a system that combined both cryptography and steganography to produce a sophisticated system that secures the communication, as shown in Figure 3.7.

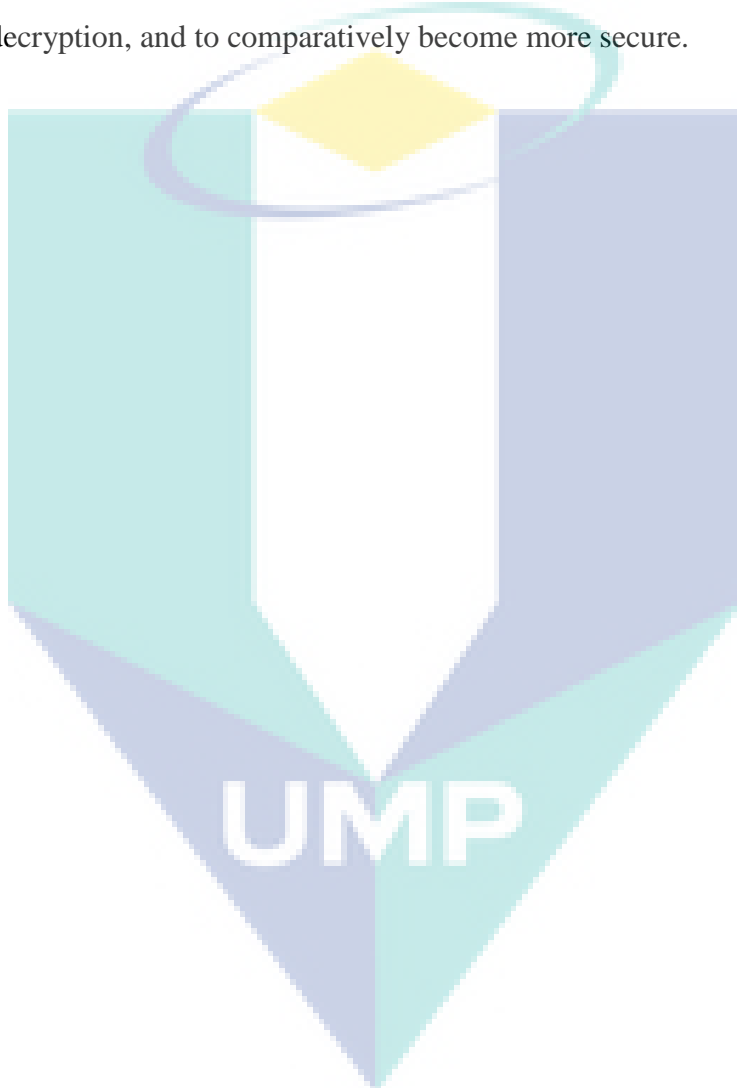


**Figure 3.7:** The proposed system after combining cryptography and steganography

The combination of cryptography and steganography techniques, by encrypting message using cryptography and then hides the encrypted message using steganography, will produce an image that can transmit without revealing that secret information is being exchanged. Moreover, even if the attacker were to defeat the steganography technique and detect the message from the stego-object, the cryptographic decoding key would be required to decipher the encrypted message (Lin & Delp, 1999).

### 3.5 SUMMARY

This chapter reviewed the design of the proposed security system. This system is composed of three phases: encrypting using improved block cipher based on random key, embedding the text within the image using improved system based on joint DWT-DCT (SSBDD), and then the combination of the above method. The proposed method is expected to overcome the problem of Invertible-Matrix which is a condition in the process of decryption, and to comparatively become more secure.



## CHAPTER 4

### METHODOLOGY

#### 4.1 INTRODUCTION

This chapter presents the steps of the proposed system, which uses both cryptography and steganography for better confidentiality and security. An improvement to the Hill cipher algorithm has been proposed to address its problems in terms of the small size of block and the key, as well as the inability to use the special characters and digits.

#### 4.2 IMPROVED BLOCK CIPHER BASED ON RANDOM KEY:

The proposed algorithm provides a large and random key, which is generated by a function programmed for this purpose depending on the password and the key length which will be entered by a user. This length is also used for segmenting the message vector into blocks of the same key length.

##### 4.2.1 Encryption

The encryption process starts by inputting the secret message (image or text), password and the length of the key. The encryption steps will be as follow:

**Input: secret message/password/length of key**

**Output: encrypted message vector**

Step 1: If the message is image then convert it into vector, if it is a text then convert it into vector of digits using ASCII table.

Step 2: Generate the random key (K) from the entered password. To generate the random key Pseudorandom generator (PRNG) function has been used. As (PRNG) function generate a different random key each time, this will create a problem where the password will be lost during the encryption process. Therefore the original data cannot be recovered in decryption process. Hence, to solve this problem the default seed has been set to a specific value in the process of encryption and decryption in order to generate the same key. On the other hand, one of the advantages of the proposed method is that the length of the password is unspecified, and if the hacker want to try all the possible combinations one by one, he/she need  $2^n$  of times to guess the key ( $n = \text{length of key in bits}$ ), which means tens of years (Fridrich, 1998). To produce a random key of size L, the first process involves finding the length of the key matrix row and the column of the key square matrix:

$$q = \sqrt{L} \quad (4.1)$$

Then, Pseudorandom generator (PRNG) function will be applied

$$K = \text{PRNG}(q, q, S) \quad (4.2)$$

Step 3: Arrange key vector in 2D matrix  $q \times q$

$$K = \begin{bmatrix} q_{11} & q_{12} & \dots & q_{1m} \\ q_{21} & q_{22} & \dots & q_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ q_{m1} & q_{m2} & \dots & q_{mm} \end{bmatrix} \quad (4.3)$$

Step 4: Calculate the length the message vector P and if the length is not a multiple of L, then add some "0" s to the vector as follow:

$$R = (\text{Reminder } P/L) \dots \text{If } (R \neq 0) \quad (4.4)$$

Then:

$$P(n+1 : [n/L] * L + L) = 0 \quad (4.5)$$

Step 5: Segment the message vector into N of blocks depending on L value:

$$P(i) = \{P(1:L), P(L+1:2L), \dots, P([n/L]*L+1 : [n/L] * L + L)\} \quad (4.6)$$

Where:  $i = 1, 2 \dots N$

Step 6: Process each block matrix P(i) individually.

Step 7: Arrange each Block P(i) into 2D square matrix

$$P(i) = \begin{bmatrix} P(i)_{11} & P(i)_{12} & \dots & P(i)_{1m} \\ P(i)_{21} & P(i)_{22} & \dots & P(i)_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ P(i)_{m1} & P(i)_{m2} & \dots & P(i)_{mm} \end{bmatrix} \quad (4.7)$$

Step 8: Perform the encryption equation:

$$C(i) = [P(i) + K] \text{ mod } 255 \quad (4.8)$$

Step 9: Convert the encrypted square block matrix  $C(i)$  into vector.

Step 10: Repeat steps 6 and 9 for  $N$  times, to complete all segments.

Step 11: After encrypting all segments, recombine the segments and remove the added "0"s to get the encrypted vector

$$C = C(1: \text{length}(p))$$

(4.9)

Where:

$P$  = Plaintext

$P(i)$  = block of plaintext

$C$  = Ciphertext

$C(i)$  = block of Ciphertext

$K$  = key

$L$  = length of encryption key

$N$  = Number of blocks

$S$  = Password

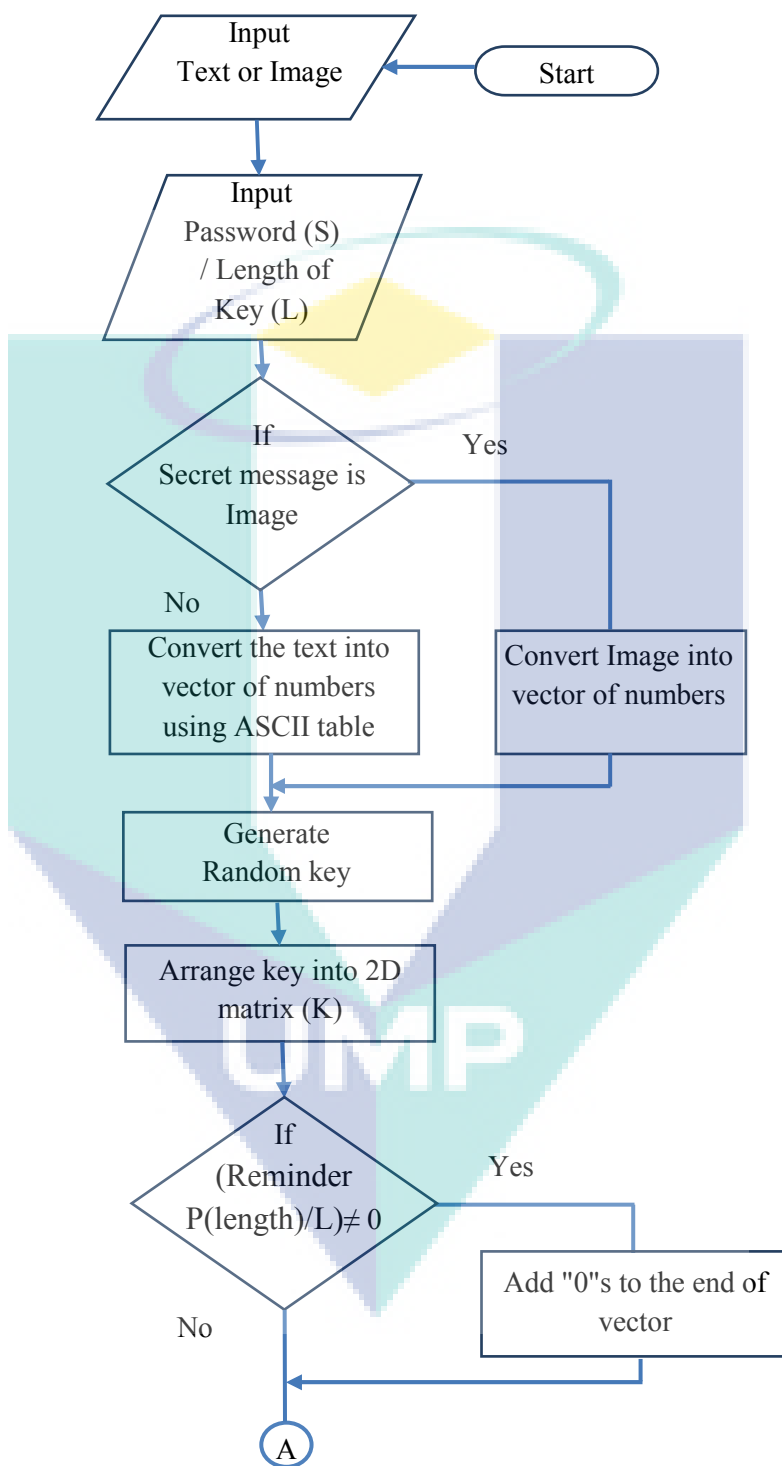
$q$  = Length of square key matrix rows and columns

$R$  = Remainder of  $(P/L)$

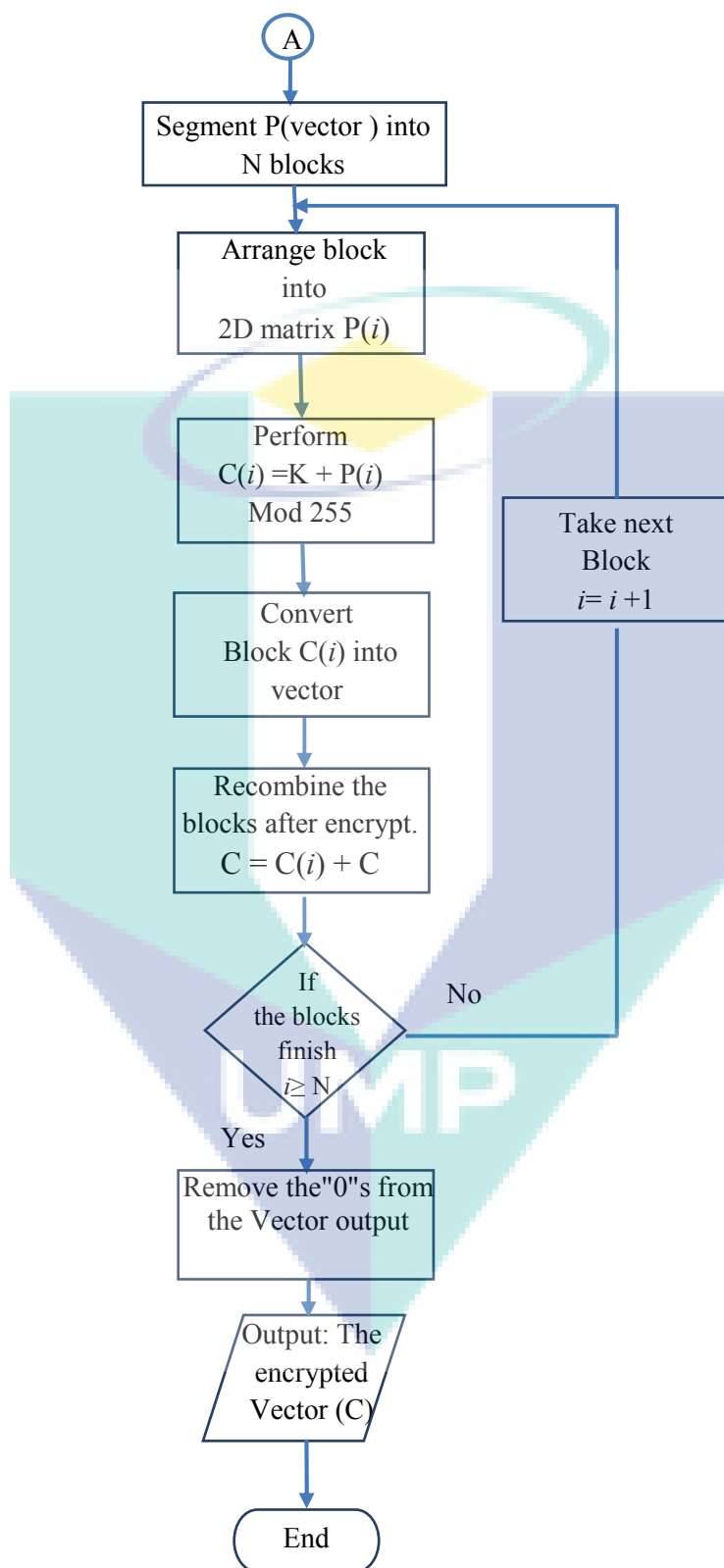
$n$  = length of message  $P$

UMP

The summarized process for the proposed algorithm is as shown in Figure 4.1.







**Figure 4.1:** Improved block cipher based on random key (Encryption processes)

### 4.2.2 Decryption

The decryption algorithm basically follows the reverse process of the encrypting steps to obtain the plaintext. After extracting the ciphertext bit stream from the cover image, decryption processes will begin as follow:

**Input:** encrypted message vector / password/length of key

**Output:** secret message

Step 1: Generate the random key from the entered password by applying Pseudorandom generator (PRNG) function, as in the encryption process. The default seed is first set to the specific value to get the same random key.

Step 2: Arrange Key vector in 2D matrix  $q \times q$

$$K = \begin{bmatrix} q_{11} & q_{12} & \dots & q_{1m} \\ q_{21} & q_{22} & \dots & q_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ q_{m1} & q_{m2} & \dots & q_{mm} \end{bmatrix} \quad (4.10)$$

Step 3: Segment the cipher message vector into N of blocks:

$$C(i) = \{C(1:L), C(L+1:2L), \dots, C(\lceil n/L \rceil * L + 1 : \lceil n/L \rceil * L + L)\} \quad (4.11)$$

Step 4: Arrange each Block  $C(i)$  into 2D square matrix

$$C(i) = \begin{bmatrix} C(i)_{11} & C(i)_{12} & \dots & C(i)_{1m} \\ C(i)_{21} & C(i)_{22} & \dots & C(i)_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ C(i)_{m1} & C(i)_{m2} & \dots & C(i)_{mm} \end{bmatrix} \quad (4.12)$$

Where:  $i = 1, 2, \dots, N$

Step 5: Process each block matrix  $C(i)$  individually.

Step 6: Perform the decryption equation:

$$P(i) = [C(i) - K] \bmod 255 \quad (4.13)$$

Step 7: Convert the encrypted square block matrix  $P(i)$  into vector.

Step 8: Repeat steps 5 and 9 for  $N$  times, to complete all segments

Step 9: After decrypting all segments, recombine the segment vector to get the plain vector

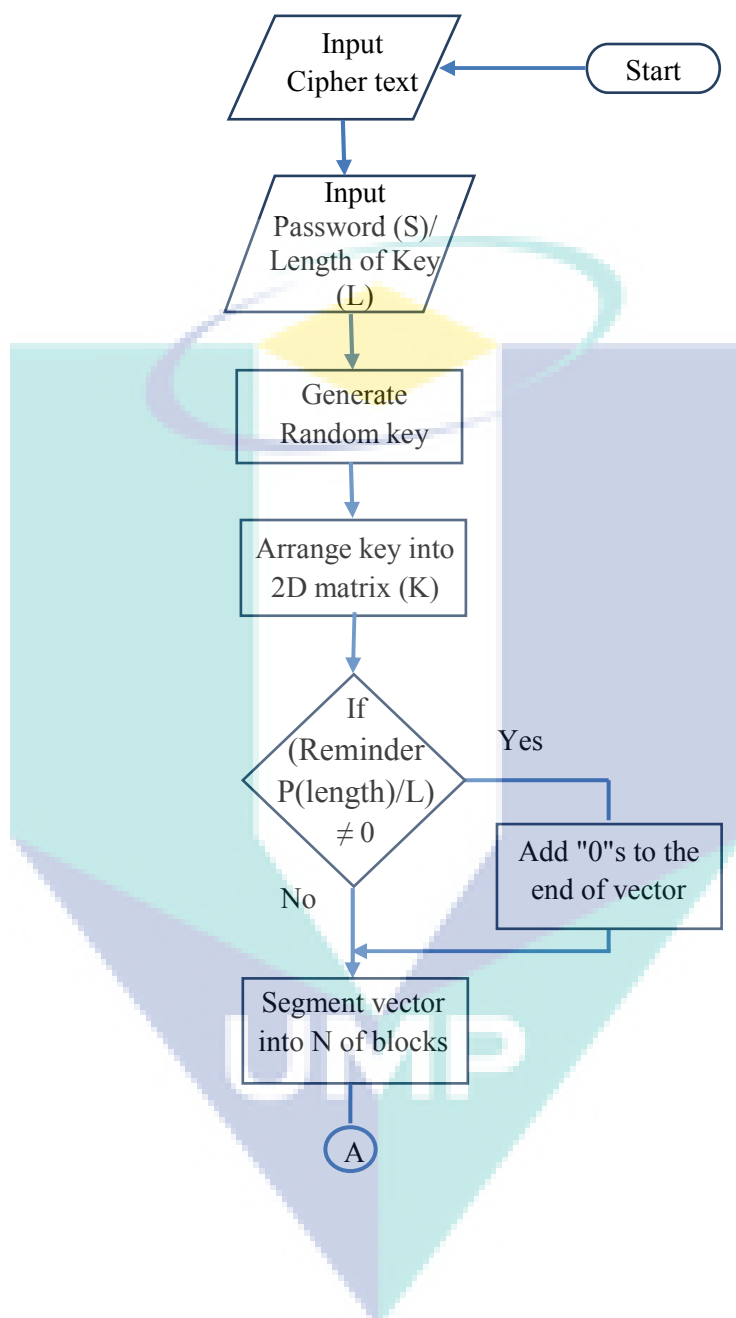
$$P = P(1:N) \quad (4.14)$$

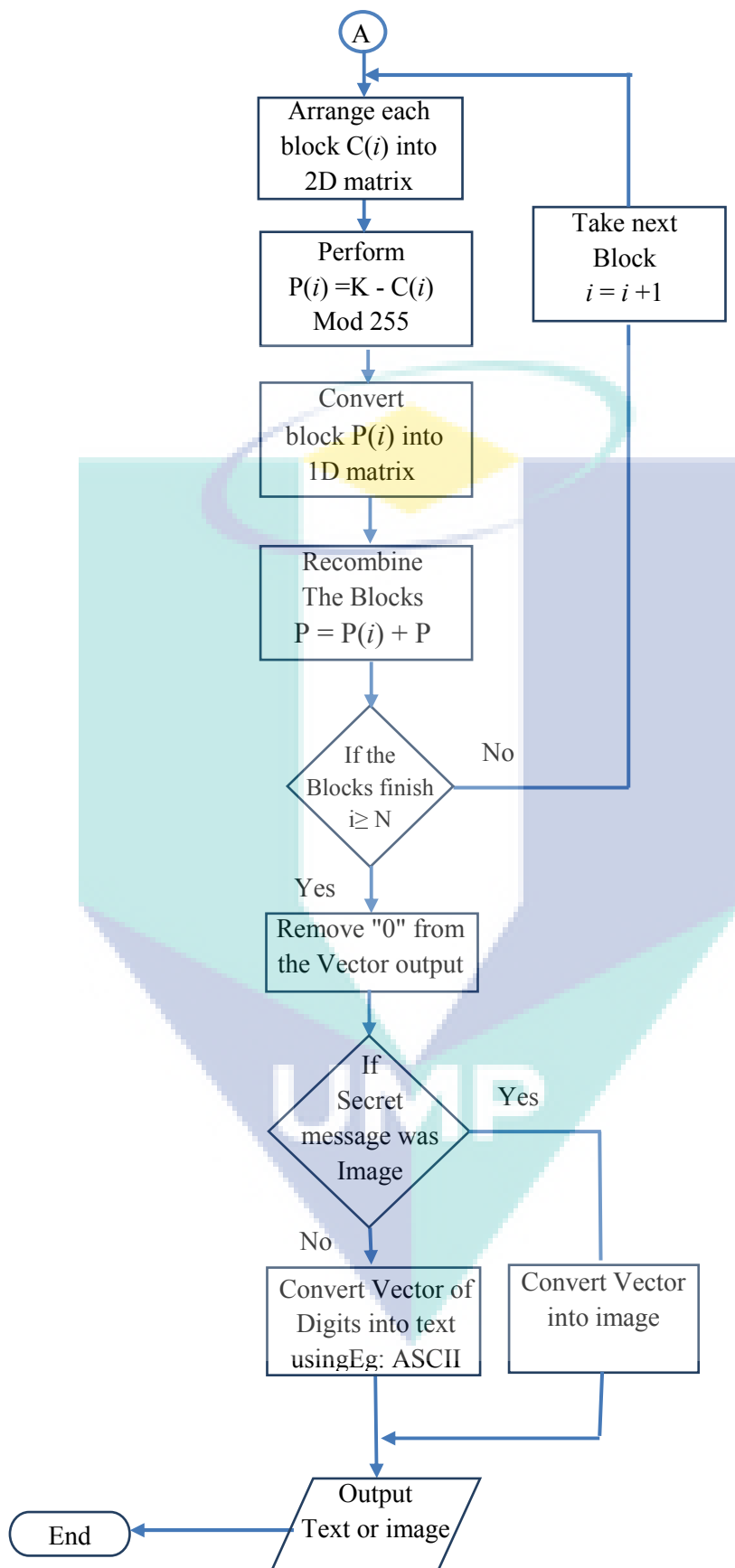
Step 10: If the secret message is an image then convert the vector into image matrix. If the secret message is a text, convert the numbers in the vector with characters and special characters and digits using ASCII table.



UMP

The summarized process is as shown in Figure 4.2.





**Figure 4.2:** improved block cipher based on random key (Decryption processes)

### 4.3 SECURED SYSTEM BASED ON JOINT DWT-DCT (SSBDD)

In the proposed method, the DWT and DCT transforms have been used. The Wavelet filters decompose the image into a set of non-overlapping multi-resolution sub-bands coefficients which can be reassembled later to reconstruct the original image without error.

#### 4.3.1 Embedding process:

In the proposed technique, information are embedded through frequency domain technique based on combination of two Transforms Discrete Wavelet transform (DWT) and Discrete Cosine Transform (DCT). Frequency domain Steganography is very secure and more complex way of hiding a secret inside an image comes with the use and modifications of discrete cosine transformations. It is more secure than spatial domain Steganography because information can be spread out to entire image (Shejul and Kulkarni, 2011), (Gunjal and Manthalkar, 2010).

The embedding process starts by applying 1-level 2D Haar DWT to decompose the host image into four sub-bands since human eyes are much more sensitive to the low frequency part (LL sub-band). Then, data will be embedded in the sub-bands (HL, LH and HH) which is better in perspective of security and quality. After that the 2D DCT will be performed on each of the selected sub-band and the secret data will be embedded in middle frequencies depending on the percentages which will be entered by the user. The data embedding processes is as follow:

***Input: cover image, encrypted message, selected percentages***

***Output: stego image***

Step 1: Perform DWT on the host image to decompose it into four non-overlapping multi-resolution coefficient sets: LL, HL, LH and HH.

Step 2: Perform 2D DCT on each of the chosen coefficient sets (HL, LH and HH). These coefficients sets are chosen to achieve both the security and efficiency of the proposed algorithm.

Step 3: Compute the total length of the secret message and also the length of each message which will be embedded in each sub-band based on the input percentages. Changing percentage for all images was done as follow. First change the percentages of (HL) Sub-band from 10% to 50% and divide the remaining percentage between (LH and HH) Sub-bands. Then, change the percentage of (LH) Sub-band from 10% to 50% and divide the remaining percentage between (HL and HH) Sub-bands. Then repeat the same operation for (HH) Sub-band.

The total length value will be embedded in the first twenty bytes of the three sub-bands. The percentages will be used to embed data message in the sub-bands which will be agreed between sender and receiver. If the entered message is greater than the maximum capacity of the three sub-bands, the program will return an error message to the user to change the cover image.

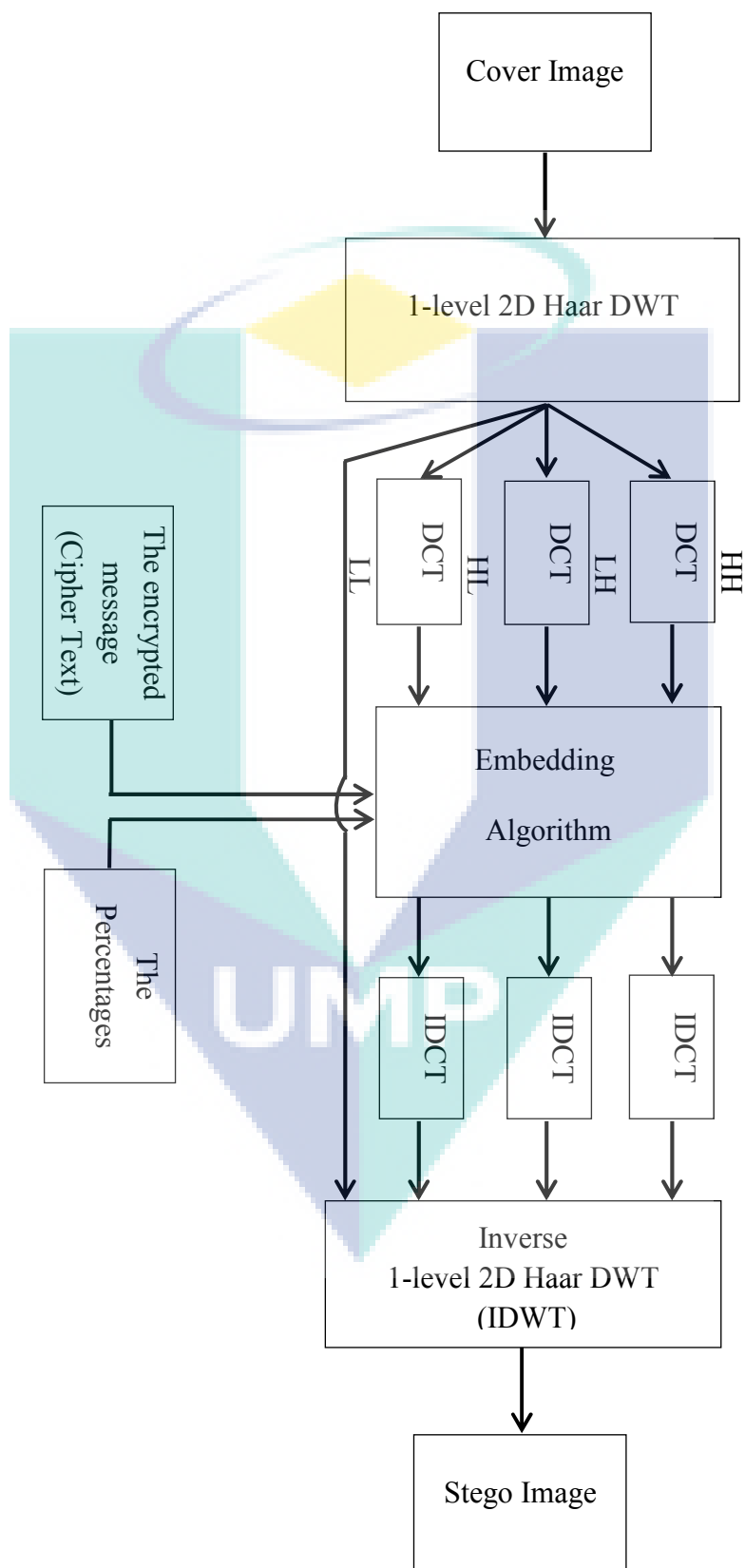
Step 4: Convert the secret message and the cover matrix into binary vector.

Step 5: Embedding process is done by inserting the message vector bits in LSBs of the DCT coefficients of the cover vector. Numbers of bits which will be used for embedding are equal for each pixel of cover vector, where they depend on the amount of the secret data. The process of embedding in sub-bands matrix will be in this sequence of (HL, LH then HH).

Step 6: Convert the resultant modified cover vector for each sub-band from binary to decimal vector. Then perform the inverse DCT (IDCT) on each sub-band after its mid-band coefficients have been modified to embed the message bits as described in the previous step.

Step 7: Perform the inverse DWT (IDWT) on the DWT transformed image, including the modified sub-band, to produce the stego image.

The process can be summarized as shown in Figure 4.3.



**Figure 4.3:** Secure system based on joint DWT-DCT (SSBDD) embedding processes



### 4.3.2 Extracting procedure:

The proposed system is a blind steganography algorithm, in which original host image is not required to extract the data. The extraction procedure is described in details in the following steps:

***Input: stego image, the percentages***

***Output: Cipher message***

Step 1: Perform DWT on stego image to decompose it into four non overlapping multi-resolution coefficient sets: LL, HL, LH and HH.

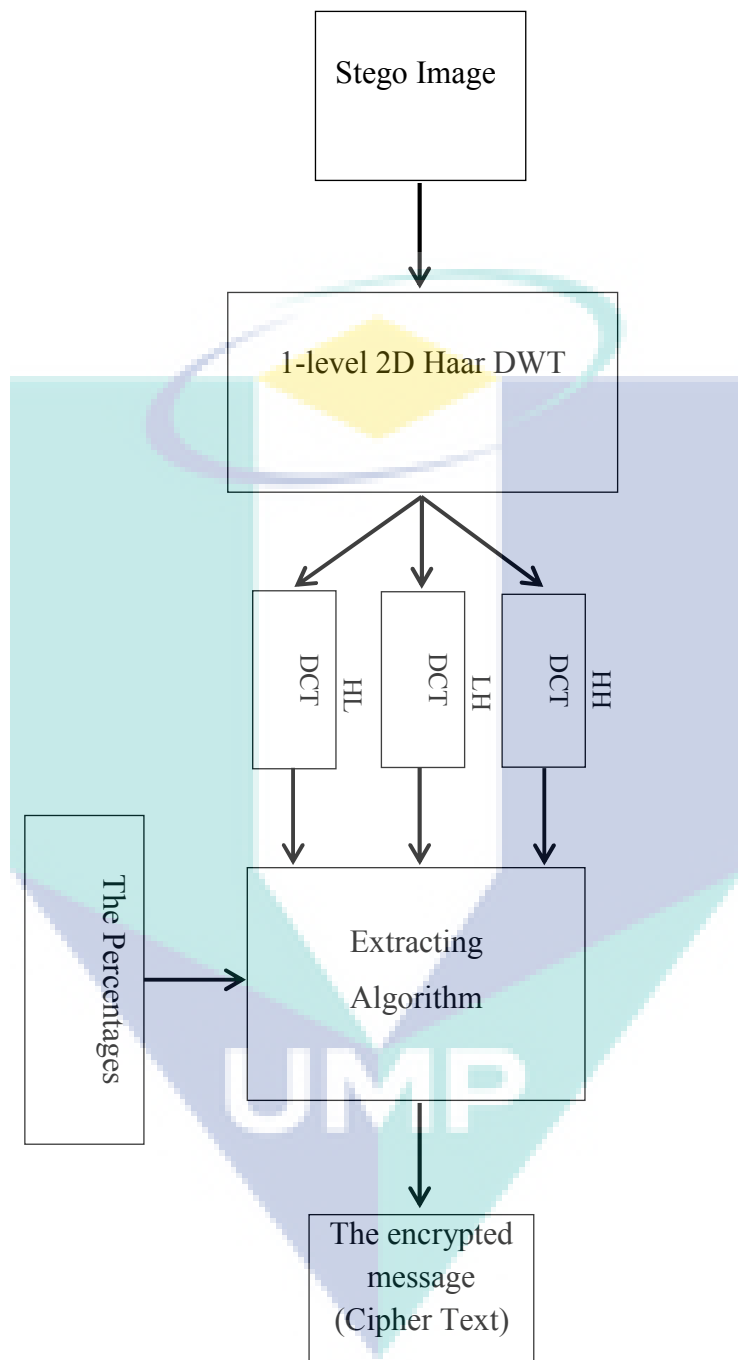
Step 2: Perform DCT on the chosen coefficient sets (HL, LH and HH).

Step 3: Extract the total length of embedded message from the first twenty bytes of the coefficient sets then compute the length of each embedded message based on input percentages.

Step 4: Extract the embedded data vector bits from the LSBs of the coefficient sets (HL, LH and HH).

Step 5: Reconstruct the scrambled cipher message using the extracted data bits.

The summarized of the detail process is as shown in Figure 4.4.



**Figure 4.4:** Secured system based on joint DWT-DCT (SSBDD) extracting procedure

#### 4.4 COMBINATION OF ENCRYPTION AND HIDING

The proposed method is composed of two parts: encryption and hiding the message. The encryption part includes the process of coding the message and encrypted message embeds inside the image. This process can be summarized as follows:

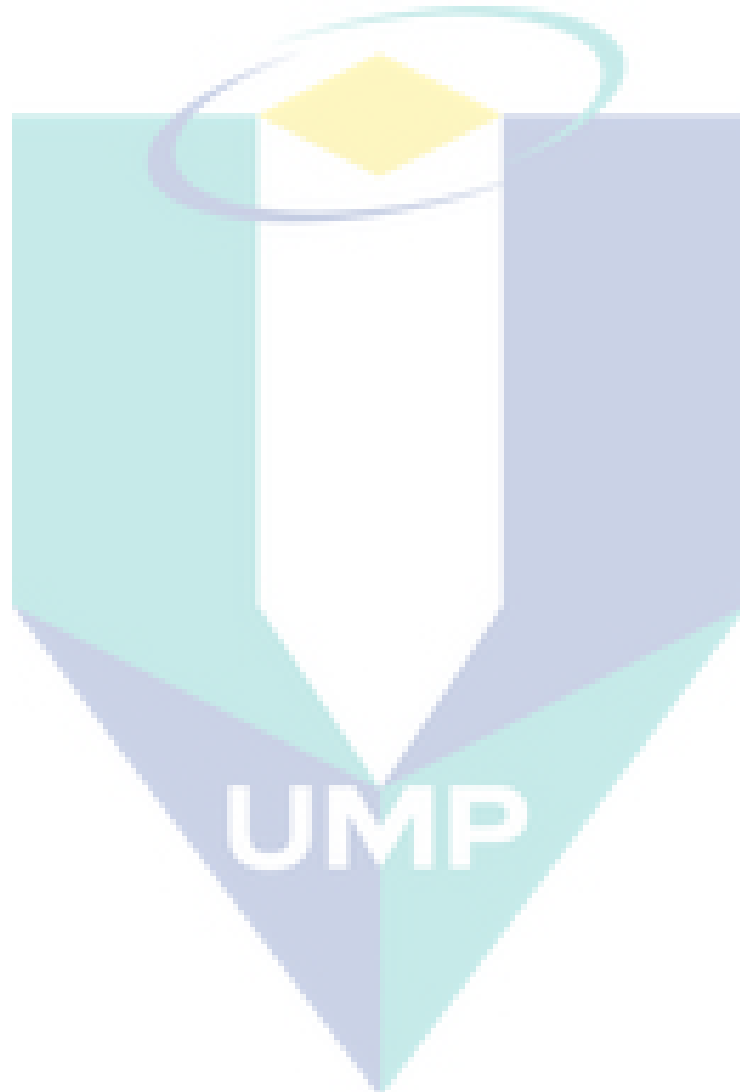
- i. Select the message to be sent.
- ii. Determine the encryption key length and password
- iii. Apply the proposed algorithm for producing the cipher text.
- iv. Select any type of image to be covered image to embed the cipher text.
- v. Choose the percentages to distribute the encrypted message to the selected sub-bands from the cover image used in the process of embedding. These percentages have to be agreed between both the sender and the receiver including the number of bits which will be used to hide the secret data.
- vi. Apply SSBDD algorithm to embed cipher text in the cover image to get stego-image.

This extraction part consists of extracting the data from the image and decrypting the secret message. This process can be summarized as follows:

- i. Enter the stego-image that carry hidden text message.
- ii. Enter the percentages.
- iii. Apply SSBDD algorithm to extract the coded text from an image using the percentages.
- iv. The key length and password are then used to interpret the encrypted message.
- v. Apply of the proposed algorithm for the purpose of producing the plain text.
- vi. The output of this process is the original secret Message.

#### 4.5 SUMMARY

This chapter describes the proposed methods. The first part explains the detail steps for encrypting using improved block cipher based on random key. The second part describe in detail the embedding process using improved system based on joint DWT-DCT (SSBDD), and then third part describes the processed involve in combining between the two methods.



## CHAPTER 5

### RESULTS AND DISCUSSION

#### 5.1 INTRODUCTION

Many standard and non-standard images have been used for testing the performance of the proposed system. Different amounts of data have been experimented as a secret message including image or text. The visual inspection are used to evaluate the ability of the proposed system and the results were tested using a number of encryption metrics such as PSNR, MSE, NAE, MD, SC, NC and histogram.

The results and discussion are basically divided into three phases; the first phase discusses the strength of encryption in terms of complexity and running time. While the second phase experiment the improvement of concealment capacity and the quality of the resulting stego-images including the discussion on the histogram analysis attack. The third phase discusses the power of the Cryptic-Stegano system.

#### 5.2 PHASE I: ANALYSIS OF ENCRYPTION

In this section, the effect of the proposed improvement to the Hill cipher encryption algorithm has been discussed. It involves substituting the secret message (image or text) with uncorrelated encrypted message, number of encryption metrics and the visual inspection. Several images, including standard and non standard images like Lena, Baboon, Cameraman...etc., and text messages were investigated in different sizes.

### 5.2.1 Encryption Complexity Analysis

#### *i. Comparing with another method*

A number of measurements have been performed to check the difference between the original image and the encrypted images. The results were compared with another method that was also proposed an improvement to Hill cipher, which is named "The New Block Cipher with 128 bit key"(Swain and Lenka, 2010). The proposed method was compared with the Swain and Lenka's method, and the results are as shown in Table 5.1.

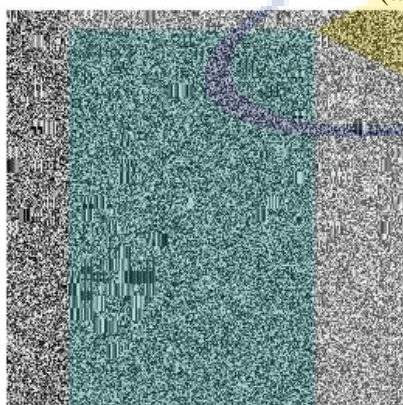
**Table 5.1:** Comparison of results between the proposed method, and Swain and Lenka's method

Image	Method	Measurement				
		PSNR	MSE	NAE	MD	SC
Lena	Swain and Lenka's method	11.2506	4.8755e+003	0.4344	237	0.6542
	Proposed Method	9.2097	7.8003e+003	0.5925	253	0.8135
Flower	Swain and Lenka's method	9.9438	6.5872e+003	0.4686	232	0.8063
	Proposed Method	8.5529	9.0738e+003	0.6069	234	0.9405
CM	Swain and Lenka's method	11.4246	4.6840e+003	0.4470	255	0.6750
	Proposed Method	8.4180	9.3600e+003	0.6701	255	0.8315

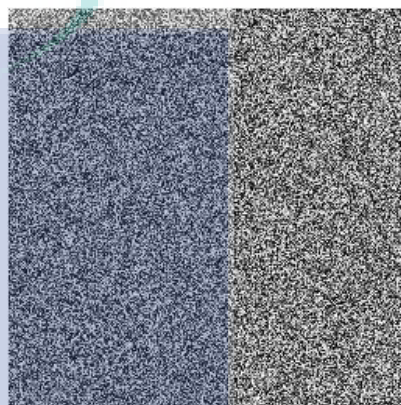
Figure 5.1 presents few samples of images before and after the encryption between the proposed method and Swain and Lenka's method.



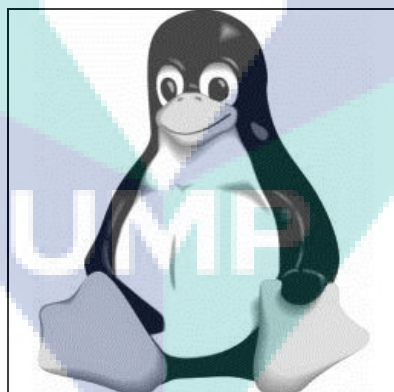
(a) Cameraman



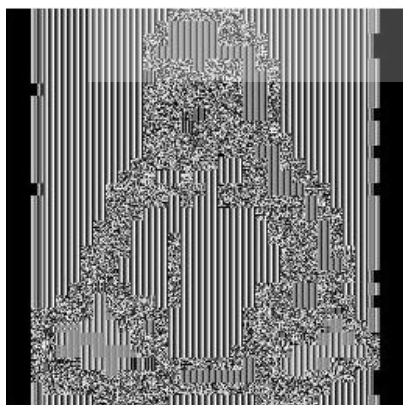
(b) Swain and Lenka's method



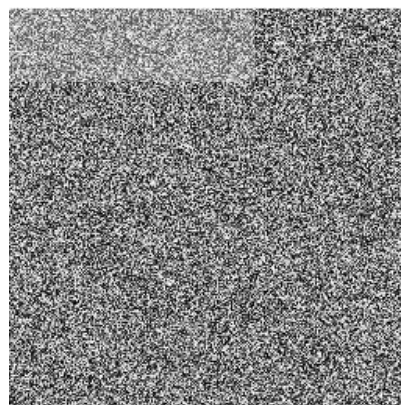
(c) Proposed method



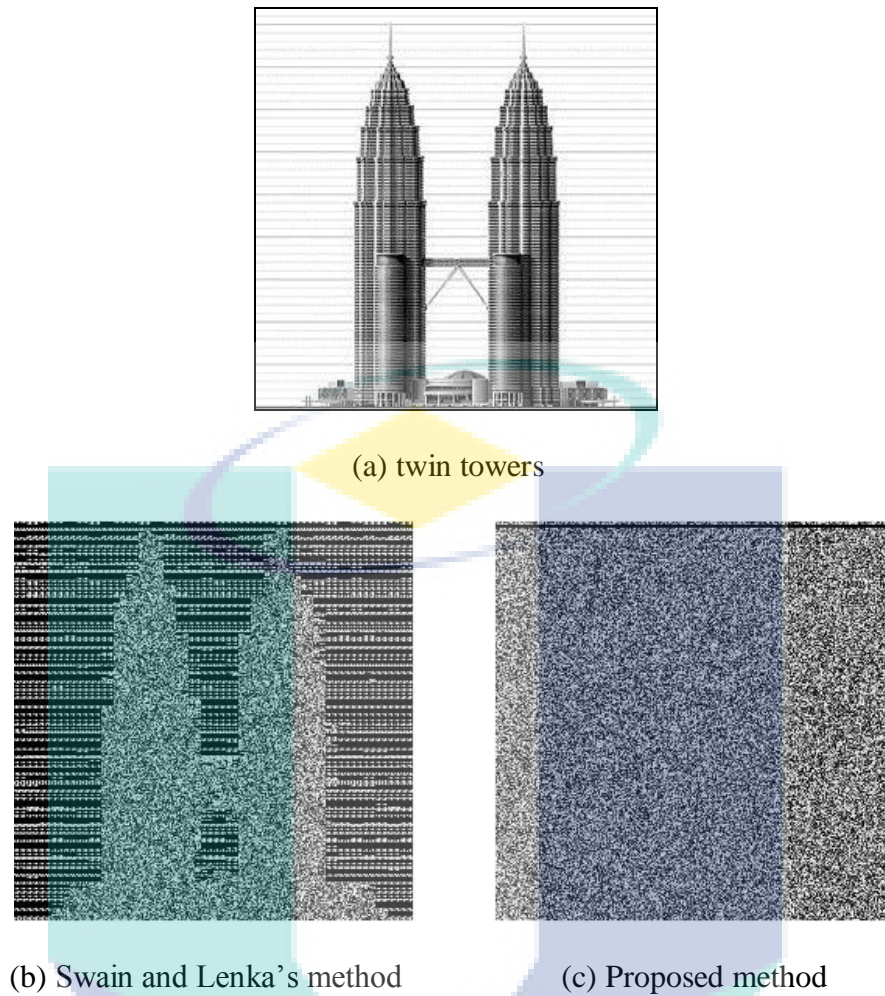
(a) Penguin



(b) Swain and Lenka's method



(c) Proposed method



**Figure 5.1:** Samples of secret images before and after encryption using Swain and Lenka's method and the proposed method

Referring to Table 5.1 and Figure 5.1, the results revealed that the proposed method is better compared to the Swain and Lenka's method. The PSNR in the proposed method is less and the values of MSE, SC, MD and NAE are larger compared with that method. The image samples have also shown clearly that the proposed method is more effective in encryption compared to the Swain and Lenka's method.

*ii. The effect of changing the key length and password value in the proposed method:*

In the proposed method, two values will be entered by the user, i.e. the key length and the password. The key length will be used to determine the length of key matrix, while the password will be used to generate the random values for the key



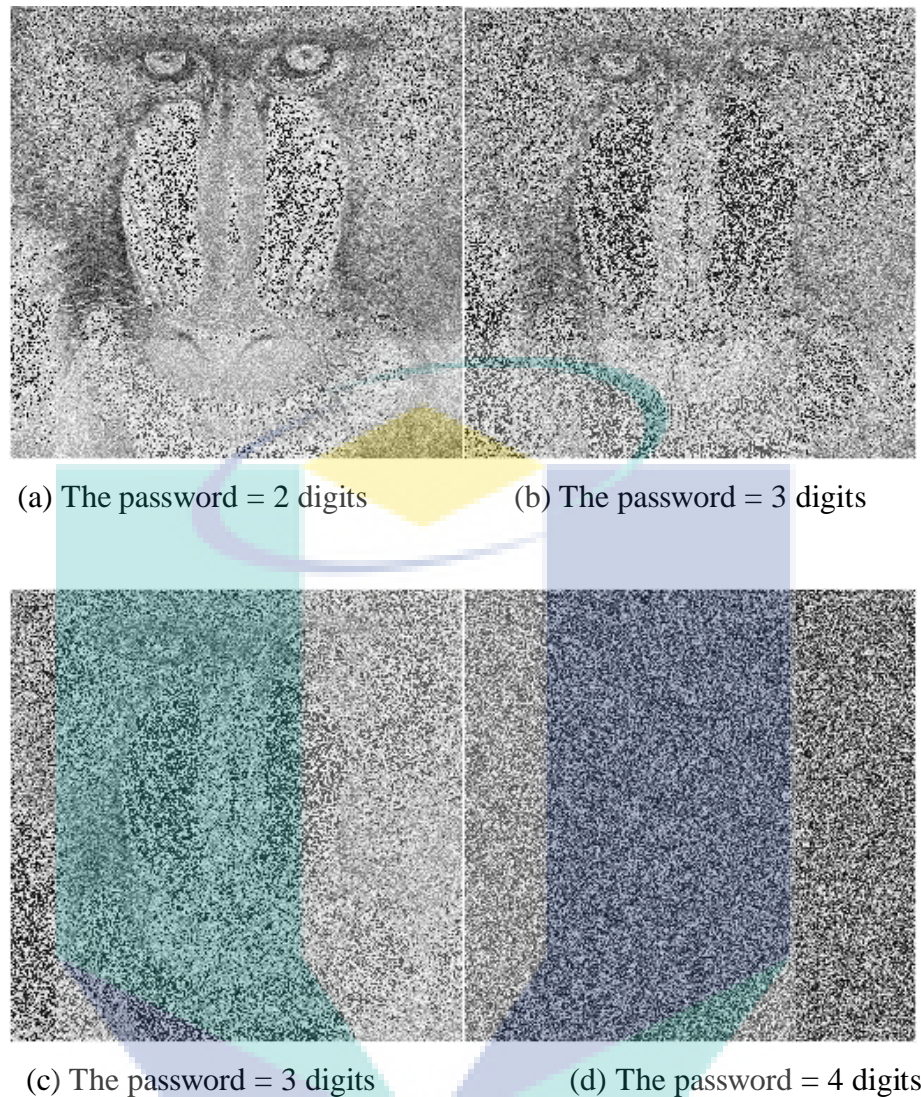
matrix. The effect of changing the value of the key for baboon image is as shown in Figure 5.2.



**Figure 5.2:** Baboon image before and after encryption using different key lengths

The results show that the image distortion has increased whenever the user increases the size of the key. However, increasing the key length with small size of password is not sufficient to get the best encryption.

The effect of changing the length of the password by the user is shown in Figure 5.3. There is possibility to increase the complexity of the password, and thus access to a more distortion of the secret image.

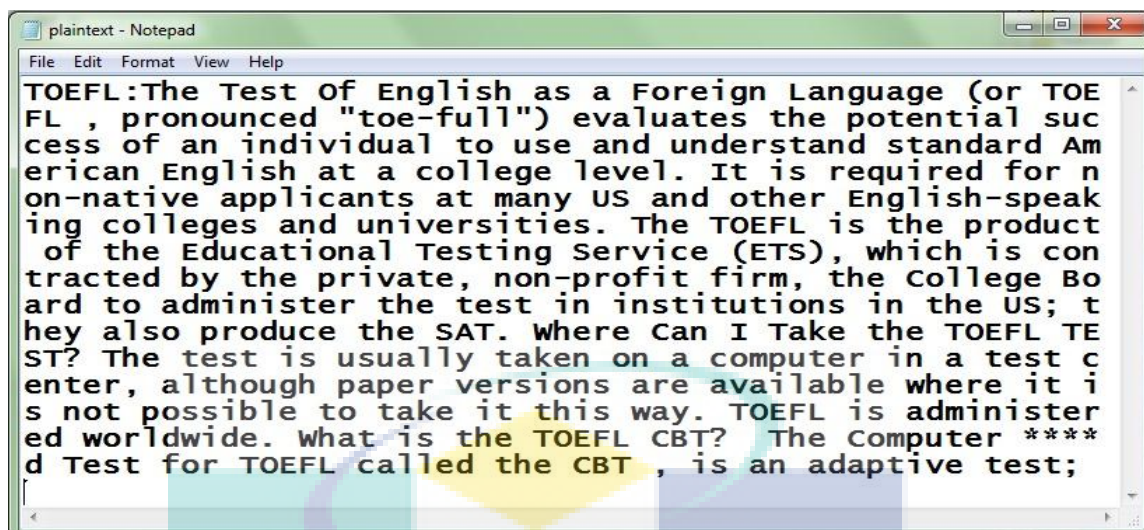


**Figure 5.3:** Samples of secret images before and after encryption using variety password length

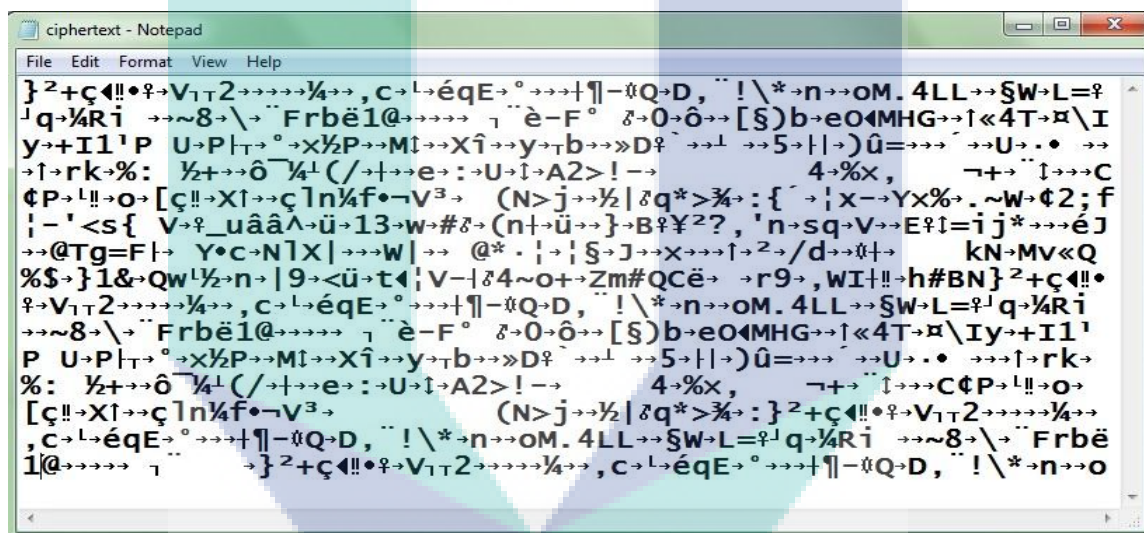
The results proved that increasing the length of the key with increasing complexity of the password will lead to a complete distortion of the secret image and therefore it is difficult and maybe impossible to be detected by enemies.

### *iii. Text encryption*

The proposed method has also been performed on the different sizes of text. Sample of the text message before and after encryption is as shown in Figure 5.4 where the text appears to be changed completely after encryption.



(a) Original text



(b) encrypted text

Figure 5.4: Sample of text message before and after encryption

## 5.2.2 Running Time Analysis

The processing speed of the proposed method was evaluated by comparing the running time with the Swain and Lenka's method, and RSA asymmetric algorithm as shown in Table 5.2. For the proposed method, the results show the running time of the proposed method is less compared to the two other methods, as the size of the secret message increases.

**Table 5.2:** Results of comparing running time between Swain and Lenka's method, RSA and the proposed method

Message size (KB)	Running Time (S)		
	RSA	Swain and Lenka's method	Proposed Method
1	0.150 sec	0.005	0.002
2	0.292 sec	0.007	0.003
5	0.620 sec	0.015	0.005
10	1.781 sec	0.056	0.010
20	5.355 sec	0.180	0.022
50	17.322 sec	0.590	0.066
100	195 sec	8.717	0.627

### 5.3 PHASE II: ANALYSIS OF CONCEALMENT

The SSBDD method has been implemented and tested on a number of gray-scale standard images like "Lena", "Jet", "Baboon", "Cameraman", "Pepper", "Barbara" and medical images like "Mri\_Brain". A number of non standard images and colored images have been used. The standard and non standard size image were used such as 512x512, 256x256, 516x615, 1176x637, etc. The formats of images that have been used are JPEG, BMP and Gif.

#### 5.3.1 Capacity of Concealment for SSBDD

The peak signal to noise ratio (PSNR) is used to evaluate the performance of the proposed scheme and the image quality. Table 5.3 shows the PSNR results when applying the proposed method on different images with different amount of data from 5% up to 65.5%, using 7 bits of each pixel. Table 5.4 shows the PSNR results of

embedding data when variety numbers of bits are used using the image of size 512 x 512. It is impossible for the human eyes to differentiate between most of the resulting stego images and the original images. Some of the samples images before and after embedding using different data capacities are as shown in Figure 5.5. The embedding capacity ratio can be calculated as follow:

$$\text{Embedding Capacity Ratio (\%)} = \frac{\text{amount of data} * 100}{\text{Cover image size}} \quad (5.1)$$

**Table 5.3:** Result of embedding different amount of data in different cover images

Capacity (%)	PSNR			
	Lena	CM	Barbara	Mri_Brain (Medical image)
5%	66.90	65.36	61.27	66
10%	65.33	63	57.25	63.7
15%	61.77	60.95	55.6	61.81
20%	56.92	56.35	50.56	57.25
25%	52.95	53.52	56.85	55.75
30%	51.51	59.97	55.59	51.28
35%	56.02	55.25	51.23	55.39
50%	55.36	53.63	35.81	55.37
55%	50.32	37.58	35.53	38.5
50%	37.51	36.52	29.89	37.63
55%	33.25	31.28	28.75	32.05
60%	26.29	25.33	22.81	25.97
65%	25.98	23.98	21.6	25.65
65.5%	25.95	23.95	21.56	25.61

**Table 5.4:** Result of embedding using different number of bits used

Capacity %	Number of bits used	PSNR					
		Lena	CM	Barbara	Peppers	Baboon	Jet
5	6	62.15	58.65	56.15	55.85	53.80	53.22
	5	56.56	52.89	50.39	59.27	58.08	57.61
	5	50.58	56.95	55.52	53.38	52.16	51.75
	3	55.65	51.03	38.61	37.51	36.26	35.86
	2	38.73	35.11	32.23	29.55	30.37	29.95
15	1	32.85	29.20	26.30	23.56	22.88	21.78
	6	56.06	55.35	55.98	50.25	56.15	58.55
	5	50.17	59.55	39.90	55.50	50.20	52.65
	5	55.23	53.51	33.53	38.59	35.27	36.79
	3	38.10	37.59	29.68	26.29	28.15	30.88
35	2	27.90	26.08	23.51	20.00	19.92	18.32
	6	50.32	38.71	35.60	33.25	32.06	31.55
	5	35.56	32.70	29.90	26.68	26.75	25.00
55	5	28.32	26.28	23.82	19.98	20.59	18.30
	6	26.59	25.56	22.20	18.25	18.87	16.55



(a) Lena – Original image

(b) Lena – Stego image

(Capacity= 50%, PSNR=37.51)



(a) Cameraman – Original image

(b) Cameraman – Stego image

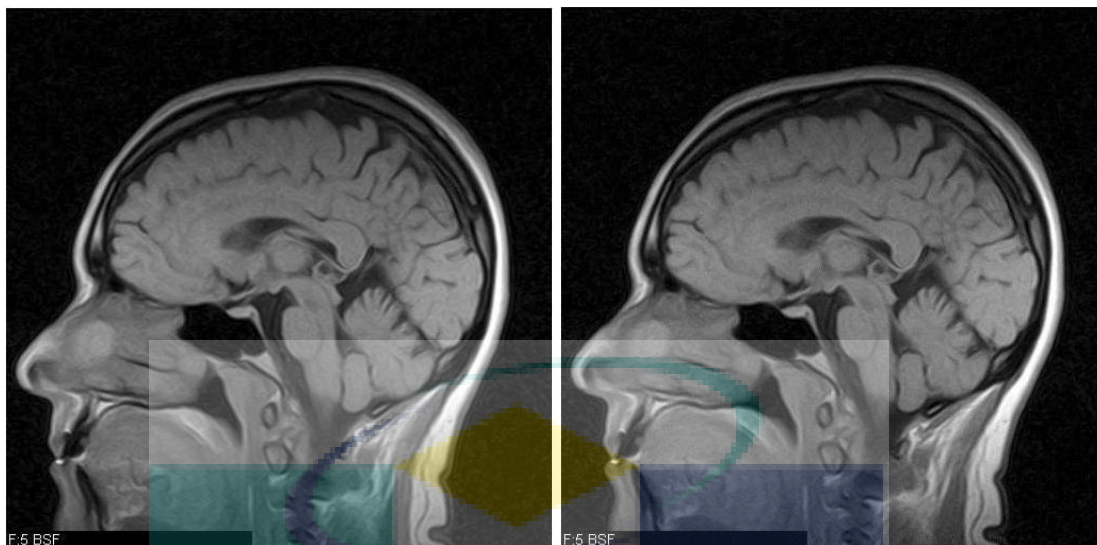
(Capacity= 50%, PSNR=53.63)



(a) Barbara – Original image

(b) Barbara – Original image

(Capacity= 30%, PSNR=55.59)



(a) Mri\_Brain – Original image                      (b) Mri\_Brain – Stego image  
(Capacity= 50%, PSNR=37.63)

**Figure 5.5:** Samples of the cover images before and after embedding data

The results showed that most of the applied resulting images after the concealment process keep the quality high, and the remaining images are of acceptable quality.

Three sub-bands can be used for embedding data, which means 75% of total image size and the number of bits per pixel is 8 bits. So, the maximum storage capacity of the proposed method can be calculated as:

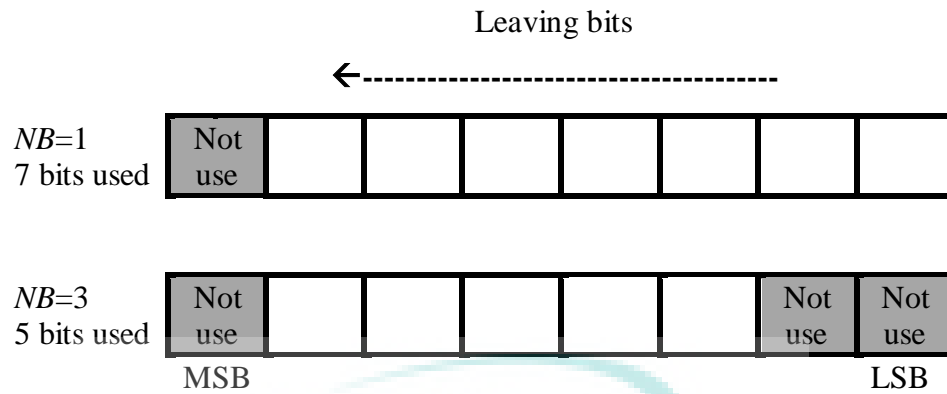
$$Max\ Capacity = 0.75 - \frac{NB}{8} * 0.75 \quad (5.2)$$

Where:  $NB$  is number of bits that will be not used in embedding

The first Most Significant Bit (MSB) from each pixel in cover sub-band kept out the embedding process, but leaving bits from the least to the most significant bit as shown in Figure 5.6. From the above equation, the maximum capacity if the  $NB=1$  and all the 7 bits are used:

$$Max\ Capacity = 65.63\ \% \quad (5.3)$$





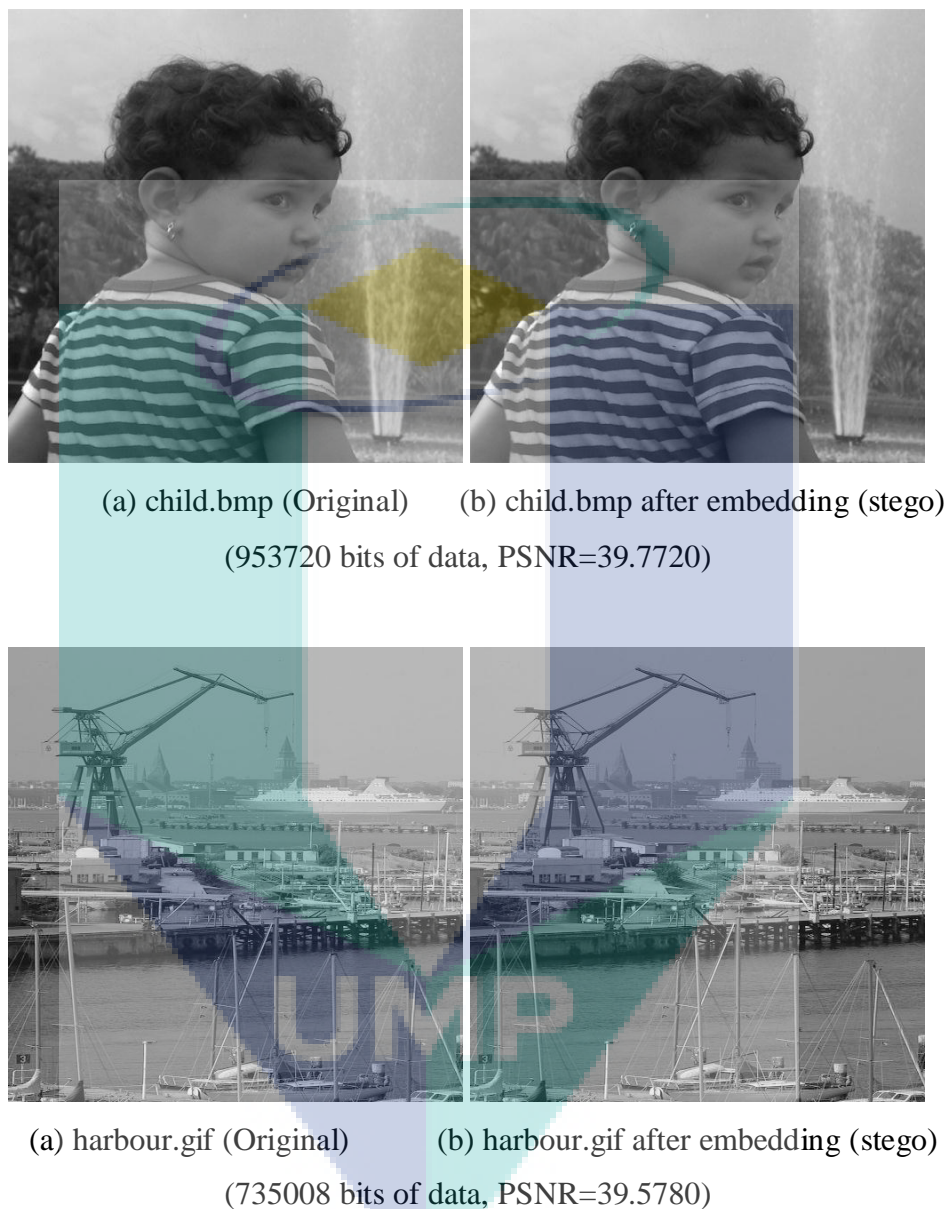
**Figure 5.6:** leaving bits in embedding process

The proposed method could be applied with different type of images while maintaining the imperceptible requirement. Table 5.5 shows results of embedding different amount of data in different types of images. PSNR is slightly decrease when the capacity is increase.

**Table 5.5:** Result of embedding different amount of data in different type of images

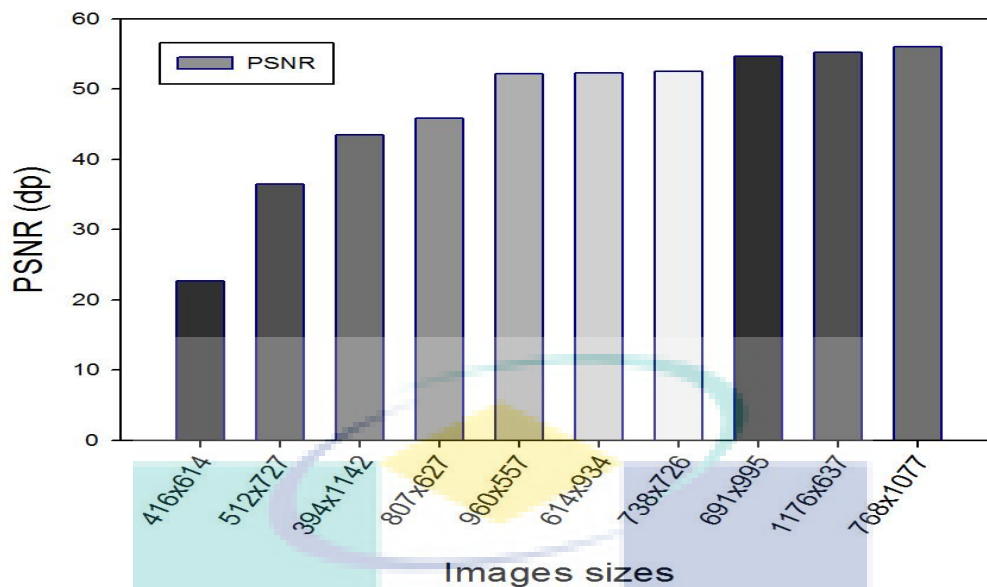
Capacity (Bit)	PSNR			
	flower.jpg	harbour.gif	goldhill.bmp	child.bmp
209720	63.7963	57.0861	62.7705	61.2561
315576	61.7521	55.5155	60.1306	59.5151
519532	57.0797	59.5258	55.5322	55.9737
525288	55.0865	55.5319	55.0250	52.8580
629152	50.1997	52.5765	59.2301	59.8566
735008	55.3755	39.5780	55.2850	56.0321
838865	55.2636	36.9651	52.6620	52.7019
953720	39.6285	32.6600	37.7531	39.7720

Figure 5.7 shows samples of the cover before and after embedding the data and the size of all images are 512x512. The value of PSNR is acceptable.



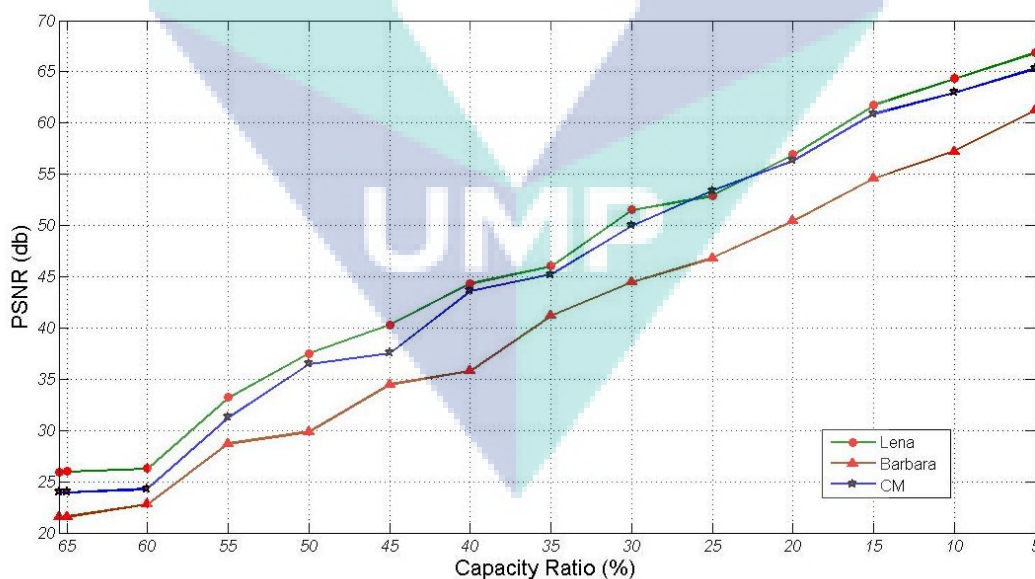
**Figure 5.7:** Samples of BMP and GIF images before and after embedding data

In addition, different sizes of images were applied for testing the method. Figure 5.8 shows the effect of PSNR when different cover images sizes are used.



**Figure 5.8:** Result of PSNR to different images sizes

Capacity of the image depends on the nature of the image which varies from one image to another. Figure 5.9 shows three different images which have the same size with different capacity.



**Figure 5.9:** Difference of capacity of three images

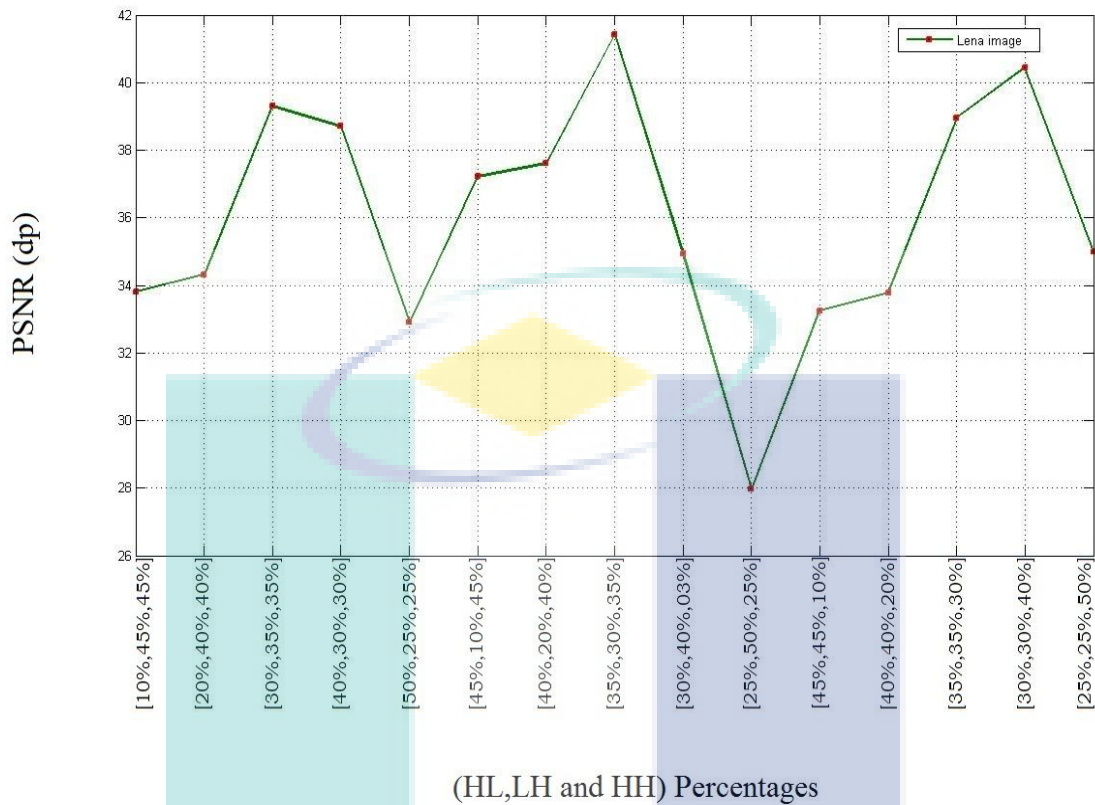
Obviously, the steganography with security key is preferable. This is due to the fact that the attacker is unable to recover the embedded message without knowing that key. The chosen percentages which distribute the message bits in the sub-bands will be

the key between the sender the receiver. So, attacker will not know the amount of data in each sub-band, not even the number of bits used in hiding. It should be noted that the chosen percentages will determine the quality of the stego image. Table 5.6 explains the effect of changing the percentages to stego image quality using different images size of images are 256x256 MB with 15% data capacity.

**Table 5.6:** Capacity and quality of images using different percentages

Percentages [HL , LH , HH]	PSNR					
	Lena	CM	Barbara	Peppers	Baboon	Jet
[10%,55%,55%]	52.56	51.06	58.61	57.15	59.51	56.5
[20%,50%,50%]	57.18	55.56	53.56	51.55	55.02	51.1
[30%,35%,35%]	57.12	55.58	53.58	50.88	53.27	50.83
[50%,30%,30%]	57.31	55.55	53.75	50.79	53.08	50.95
[50%,25%,25%]	55.35	51.03	52.11	57.57	59.81	58.65
[60%,20%,20%]	55.89	50.89	52.88	57.57	59.71	58.97
[55%,10%,55%]	55.63	51.29	50.05	58.69	59.2	59.85
[50%,20%,50%]	59.5	55.72	55.55	52.69	53.77	53.3
[35%,30%,35%]	57.38	55.62	53.58	51.05	53.19	51.1
[30%,50%,30%]	56.79	55.35	53.56	50.51	53.16	50.53
[25%,50%,25%]	52.33	50.83	50.08	56.39	50.13	55.95
[20%,60%,20%]	51.93	50.58	59.98	56.01	50.22	55.31
[55%,55%,10%]	51.95	59.25	59.87	55.18	58.5	55.33
[50%,50%,20%]	56.83	55.18	55.3	50.13	53.28	50.22
[35%,35%,30%]	57.02	55.38	53.58	50.67	53.1	50.66
[30%,30%,50%]	57.55	55.83	53.57	51.25	53.31	51.25
[25%,25%,50%]	56.38	53.99	50.27	51.85	51.17	51.3
[20%,20%,60%]	57.66	55.51	50.3	55.57	51.71	55.01

Figure 5.10 shows changing of PSNR values to Lena image with changing percentages when size of image is 256x256 MB and 50% data capacity.



**Figure 5.10:** Effect of changing the percentages to Lena image

### 5.3.2 Results of Comparisons

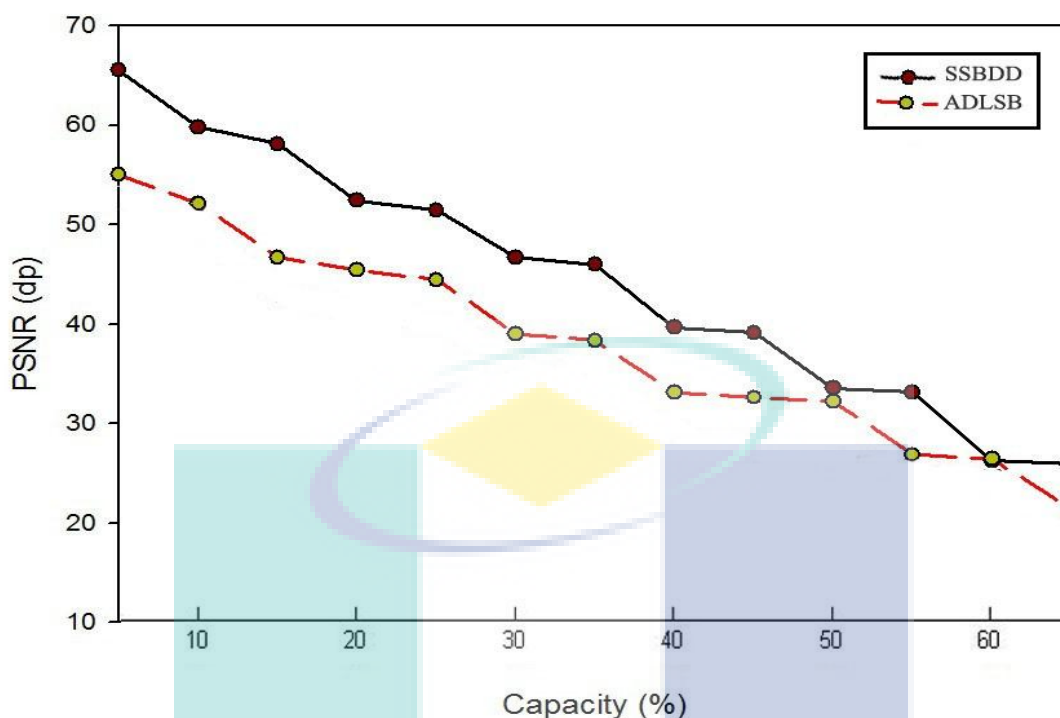
The proposed method (SSBDD) was compared with the standard and existing methods. The adaptive LSB method (ADLSB) was the enhancement of the classic LSB. It was compared with a method which uses the same proposed technique but using DWT transform only, and with another method using wavelet transform W-PVD (Al-Asmari et al., 2011). The comparison is as shown in Table 5.7. Another comparison is made with number of existing methods that use a technique similar to the proposed technique PVD (Wu and Tsai, 2003), PVD+3LSB(Wu and et al., 2005). Overlapping PVD (Chang et al., 2006), SH-PVD Method(Al-Asmari and Al-Gamdi, 2009) and W-PVD, is as shown in Table 5.8. Finally, the graph in Figure 5.11 clearly shows the different between the proposed method (SSBDD) and the Adaptive LSB.

**Table 5.7:** Results of the comparison with the Adaptive LSB and the other methods

Image	Size (bit)	PSNR			
		Adaptive LSB	W-PVD	SSBD (DWT only)	SSBDD
<b>Lena</b>	776520	38.1359	50.2367	51.8573	55.7176
<b>Baboon</b>	757850	38.2906	38.6597	38.3607	39.1661
<b>Peppers</b>	780250	38.1155	50.1937	31.6990	51.5601
<b>Jet</b>	770558	38.1671	50.0953	39.3296	51.3036

**Table 5.8:** Results of the comparison with the previous methods

Measure	Method					
	PVD	PVD+3LSB	Overlapping PVD	SH-PVD Method	W-PVD	SSBDD
Capacity (Bits)	509753	766052	763138	776390	776520	776520
PSNR (dB)	51.025	37.0951	36.92	37.65	50.2367	55.5158
Visual Quality	Excellent	Acceptable	Acceptable	Excellent	Excellent	Excellent



**Figure 5.11:** Comparison between SSDBB and Adaptive LSB

The results show stego-image can be transmitted without revealing that secret information which is being exchanged. The proposed method showed a significant improvement in capacity compared with ADLSB method and similar methods based solely on the DWT transform.

The results also showed the ability of the proposed method to conceal large amount of data up to 50% of capacity by keeping the high quality of stego image, even if the data is above 50%. The PSNR is better and acceptable compared to the other methods. In addition, various types of images were used as a cover has shown success in the ratio of concealment and retrieval of data. It also shows the ability of the proposed method to work with all images types. The comparison between images which have different sizes in the concealment has been clarified, where the concealment will be more efficient and gives a high stego image quality. The capacity of images which is different from one to another, depending on the nature of image, has also been shown. The proposed method showed complexity in providing capacity of storage in the image while maintaining its quality, in the case of determining distribution of the data percentages manually.

### 5.3.3 Histogram statistical analysis

Stego-images can draw suspicion or be easily detected from statistical analysis. LSB technique is vulnerable to steganalysis which is based on histogram analysis. All the existing schemes detection of a secret message in a cover message can be easily detected from the histogram analysis and statistical analysis. Therefore, developing new steganography algorithms against histogram analysis is the prime requirement (Nagaraj, et al., 2010). Histogram in Figure 5.12 shows a frequency histogram of the Lena cover image. Figure 5.13 shows that a comparison result of adaptive LSB method with the histogram results of the proposed method after a hidden message of 209720 bits. Figure 5.14 shows that a comparison result of adaptive LSB method with the histogram results of the proposed method with a hidden message of 519550 bits.

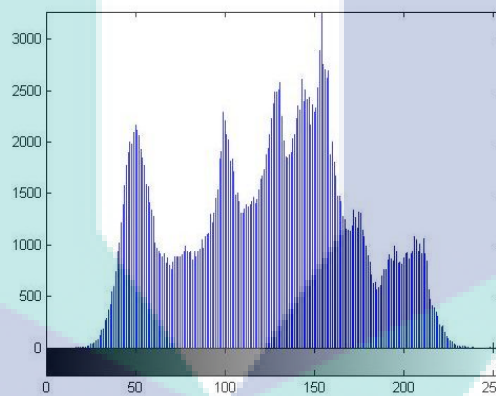


Figure 5.12: A frequency histogram of the Lena cover image

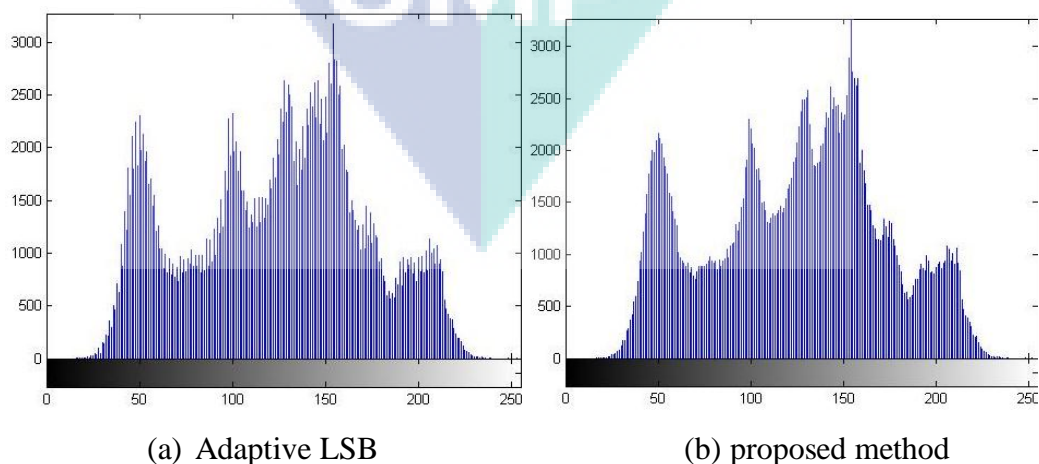
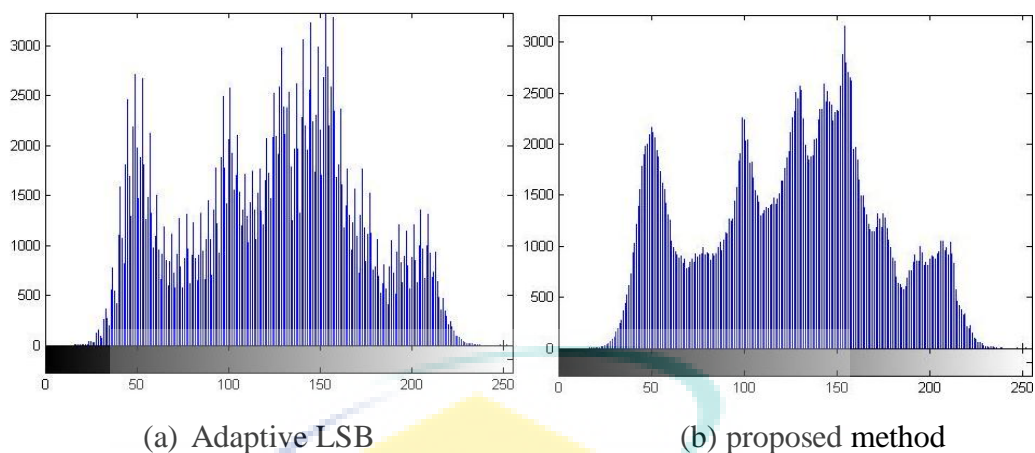


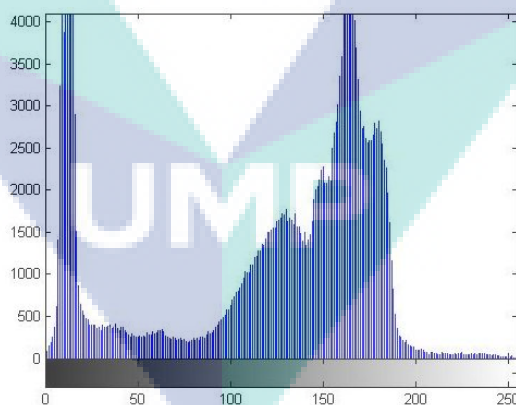
Figure 5.13: Histogram comparison of Adaptive LSB method and the proposed method after a hidden message of 209720 bits



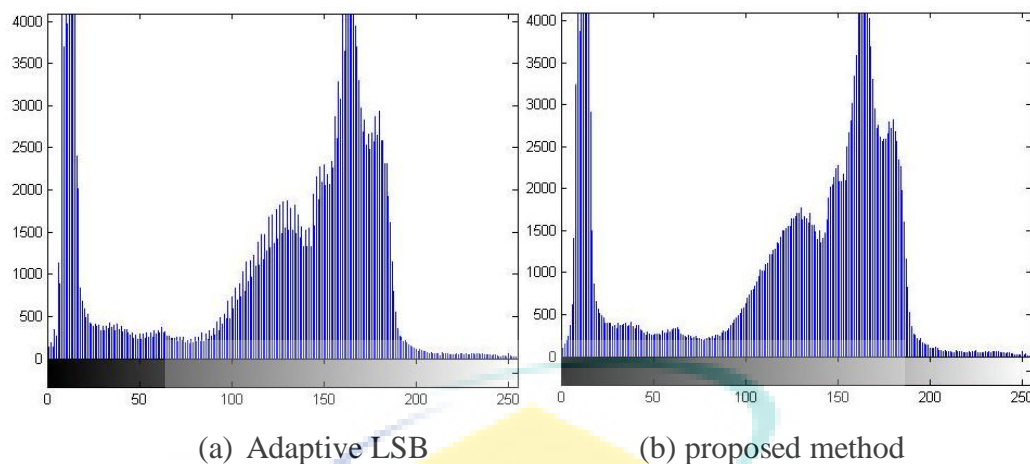


**Figure 5.14:** Histogram comparison of Adaptive LSB method and the proposed method after a hidden message of 519550 bits

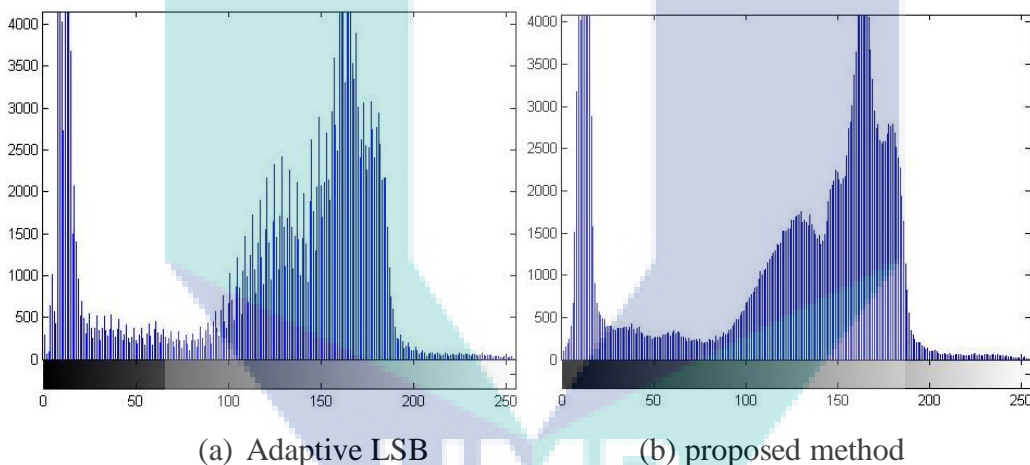
Another frequency histogram is shown in Figure 5.15 for the Cameraman cover image. Figure 5.16 shows that a comparison result of adaptive LSB method with the histogram results of the proposed method after a hidden message of 209720 bits. Figure 5.17 shows that a comparison result of adaptive LSB method with the histogram results of the proposed method with a hidden message of 519550 bits.



**Figure 5.15:** A frequency histogram of the Cameraman cover image



**Figure 5.16:** Histogram comparison of Adaptive LSB method and proposed method after a hidden message of 209720 bits



**Figure 5.17:** Histogram comparison of Adaptive LSB method and proposed method after a hidden message of 519550 bits

From the histograms, it will infer that histogram of the stego image for the proposed method is nearly equal to the histogram of the cover image. Thus, it is difficult for a steganalyst to find a secret data hidden in the stego image. Even if the hidden data was larger, the histogram is much better than the existing adaptive LSB.

### 5.3.4 Analysis of Extracted Data

The performance of secret information extracted is evaluated using the normalized cross-correlation (NC). The results showed that there is no error in the extracted information and it is exactly the same information that has been embedded. Results of extracting various amounts of data in various sizes of images are as shown in Table 5.9.

**Table 5.9:** Result of NC between the original and extracted messages

Capacity (%)	Normalized Cross Correlation (NC)						
	Lena	CM	Barbara	Peppers	Baboon	Jet	Mri_Brain
10	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
20	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
30	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
50	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
50	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
60	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
65	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000

## 5.4 PHASE III: ENCRYPTED AND CONCEALMENT COMBINATION ANALYSIS

Encryption has become very secure cryptography technique through enhancing the Hill Cipher algorithm by generating the key array randomly and dynamically using the length. Further more, by extending it to include special characters and digits, and the steganography method which combine two transform methods DWT and DCT with dynamic data distribution, it will be highly secured. Through combining the above two techniques, there is less chance for the original message to be detected by the attacker.

In case the data is extracted, it will be encrypted, but still there is a chance that the interloper can break the code. In the proposed method, instead of applying existing techniques directly, the approach will be used. In this system, to get the original message, one should know the keys of cryptography and steganography.

Whenever the attacker knows the concealment and encryption keys, he will not be able to extract the encrypted text hidden within the image without knowing the mechanism of storage within the image.

The advantage of Crypto/Stegano system is that the method uses large and multi keys that increase the complexity of the process of encryption and decryption. In the steganography technique, two of the transform domain techniques have been combined, the wavelet and cosine transform to embed data to take the advantageous of both two algorithms to increase robustness and imperceptibility.

## 5.5 SUMMARY

In this chapter the results of the proposed method were compared and evaluated with the existing similar techniques. Starting from the phase of encryption, where different images and text sizes are presented. It also includes the before and after encryption including comparing the encryption complexity with the Swain and Lenka's method using different measurements. The review had also included comparing the running times with the mentioned method as well as with the RSA algorithm. In phase of hiding data, the results of concealment of different amount of data in different cover images has been presented using PSNR value as a measurement by showing some samples. Also, the results using different types of images have been presented with two image samples. The difference of capacity between multi images sizes has also been shown. The key of the proposed percentages that will be entered by the user have to be agreed between sender and receiver. The results of changing the percentages were shown clearly in the table. On the other hand, extracting the secret message correctly and without mistakes has been presented using NC value as a measurement. The results of the proposed method have been compared with the standard method as well as with other recent methods which uses similar technique.

## CHAPTER 6

### CONCLUSIONS AND RECOMMENDATION

#### 6.1 INTRODUCTION

With the emergence of computers and the wide use of the internet among individual, government institutions and other organizations, a need to electronic storage and exchange information has arisen. Therefore, the evolutions of computers and internet help in achieving this need. These entire characteristics made computer the essential equipment in all companies, hospitals, government institutions and commercial reorganizations to exchange information including research findings, private documents, confidential data concerning employees and production data. In fact, many studies have been carried out to assist in providing secure data exchange and to contribute in finding new methods for protection. This thesis mainly focuses on developing a new system with more capacity by combining security techniques like cryptography and steganography.

#### 6.2 SUMMARY OF FINDINGS

The aim of this thesis is to give new insights and directions on how to improve existing methods of hiding secret messages, in order to maximize the embedding capacity while maintaining the image fidelity. At the same time, the improved cryptography system increases the efficiency and reduces the time for encryption. By combining steganography and cryptography, it gives strength to the proposed system. A

brief background of the ancient and modern steganography and cryptography with their techniques, have been studied and documented.

In the proposed system there were an improvement to the both Steganography and cryptography. In Steganography, the discrete wavelet transform (DWT) and the discrete cosine transform (DCT) were combined to achieve a better distribution of the data on the cover image and the exploitation of the places with least impact on the quality of the image. The wavelet transform has been used to decompose the cover host image into four non-overlapping multi-resolution sub-bands: LL, HL, LH, and HH where three of them have been chosen (HL, LH, and HH) that they have less effect to the image quality. Then, the DCT transform was applied on the selected sub-bands and the distribution of data will be the coefficients of the middle frequency sub-bands according to percentages that entered by the user. These percentages are used later as a stego-key between the sender and the recipient.

In cryptography, there is an improvement to the Hill cipher algorithm. The proposed algorithm provides a large and random key, which is generated by a function programmed for this purpose depending on the password and the key length which will be entered by a user. This length is also used for segmenting the message vector into blocks of the same key length.

A number of testing with different measurements has been carried out for the proposed cryptography method (improved Hill Cipher algorithm Based on Random Key) to gather the experimental results. Although there is a difference in measurement values from an image and text to another, it is better than the existing methods. The results of encrypting some of images showed clearly the efficiency of the proposed method compared with the existing method. In addition, the method of using a random key matrix that was generated based on the password entered by a user shows an effect to the secret message through a number of images that have been tested.

Also, the results proved that the speed of the encryption process for the proposed method is higher compared with the existing method, as well as with the common

method of RSA. Although the results shows a lower speed when the secret message is small, and in some cases the same speed that the existing method needs, it is much faster when the size of the message is larger.

On the other hand, the experimental results of the proposed steganography method (SSBDD) showed the effectiveness of the proposed method compared with the LSB direct insertion method and the existing methods that use similar techniques. It gives best values for the PSNR measure, which means that there is no difference between the original and the stego-images. The values of PSNR become less than 35dp when the payload exceeds 55%, especially in some images, but the stego-image is still acceptable. However, the results are better than the existing methods. Also, the proposed method can be used for all kinds of images in any size, including medical images. The use of percentages was very useful to determine the largest possible amount of data that will be accepted by the image sub-bands while maintaining the stego-image quality. Testing of the extracted data correctness for different types of images and different amounts of data has shown that there are no errors in the message after the extraction processes.

Regarding the confidentiality of the hidden data, the results show that the proposed method can effectively resist image steganalysis based on histogram analysis where the existing LSB technique is vulnerable to this kind of steganalysis. Although hiding a large amount of data may show a little change in the histogram of the image, it still difficult to distinguish it by the human eye.

The proposed system proved that improvement of the both techniques i.e. Steganography and Cryptography, and their combination provides an enhancement to the embedded capacity while keeping the image quality. As well as maintaining the confidentiality of information, even if the data have been discovered, they will be encrypted and difficult to be detected due to the efficiency of the encryption method.

### 6.3 CONTRIBUTION OF THE STUDY

- i. Steganography and cryptography can be implemented separately, as well as the combination of both.
- ii. Using two levels of security makes it difficult to break the information even realizing the existence of a confidential data.
- iii. Encryption has become efficient by the improved hill cipher method.
- iv. By using percentages for embedding, it will maximize the embedding capacity and keep the quality of cover image.
- v. Combining two transformation methods, discrete wavelet transform (DWT) and discrete cosine transform (DCT), it helps to hide the data and increase the difficulty to recognize the data.

### 6.4 RECOMMENDATIONS FOR FUTURE RESEARCH

- i. The data protection has been improved but the complexity can be increased by using more than one key for encryption and decryption.
- ii. The capacity and security of hiding technique can be improved by adding compression function of the message before the hiding operation.
- iii. The proposed system can be developed to deal with other cover files created by other operating systems like (LINUX, UNIX or OS/2).



## REFERENCES

- Abu Taha, M., Farajalla, M. and Tahboub, R. 2011. A Practical One Way Hash Algorithm based on Matrix Multiplication. *International Journal of Computer Applications*. 23(2):33–37.
- Ahmad J. M. and Ali Z. M. 2011. Information Hiding using LSB technique. *International Journal of Computer Science and Network Security*. 11(4).
- Al-Asmari, A. Kh. And Al-Gamdi, O. 2009. High Capacity Data Hiding Using Semi-Hexagonal Pixels Value Difference. *International Conference of Computing in engineering, science and information*. 14-17.
- Al-Asmari, A. Kh., Al-Qodah, M. A., Salama, A. S. 2011. Wavelet-Pixel Value Differencing Technique for Digital Images Data Hiding. *IEEE International Conference on System Engineering and Technology (ICSET)*. (27-28): 15 – 18.
- Al-Ataby A. and Al-Naima F. 2010. A Modified High Capacity Image Steganography A Modified High Capacity Image Steganography. *The International Arab Journal of Information Technology*, 7( 4).
- Al-Haj, A. 2007. Combined DWT-DCT Digital Image Watermarking. *Journal of Computer Science* 3 (9): 740-746.
- Al-Najjar A. J., Alvi A. K., Idrees S. U. and Al-Manea A. M. 2007 .Hiding Encrypted Speech Using Steganography. *7th WSEAS International Conference on Multimedia, Internet & Video Technologies* .(15-17).
- Amin, M.M. Salleh, M. Ibrahim, S. Katmin, M.R. and Shamsuddin, M.Z.I. 2003. Information Hiding Using Steganography. *National Conference on Telecommunication Technology Proceedings*. (14-15): 21-25.
- Amin, P.K., Liu, N. and Subbalakshmi, K.P. 2007. Statistical Attack Resilient Data Hiding. *International Journal of Network Security*. 5(1): 112–120.
- Anderson, R.J. and Petitcolas, F.A.P 1998. On The Limits of Steganography. *IEEE Journal of Selected Areas in Communications*. 16(4): 474-481.
- Ashok, J., Raju, Y., Munishankaraiah, S. and Srinivas, K. 2010. Steganography: An Overview. *International Journal of Engineering Science and Technology*. 2(10): 5985-5992.
- Bhattacharyya, S and Sanyal, G. 2009 .Hiding Data in Images Using PCP. *International Journal of Computer and Information Engineering*.3(3)
- Bennett, K. 2004. Linguistic Steganography: Survey, Analysis, and Robustness Concerns for Hiding Information in Text. *Purdue University, CERIAS Tech. Report 2004-13*.

- Bharati, M.H. and MacGregor, J.F. 2000. Texture Analysis of Images Using Principal Component Analysis. *Proceedings of the SPIE; Process Imaging for Automatic Control*. 4188: 27-37.
- Cachin, C. 1998. An Information-Theoretic Model for Steganography. *In: Proc. 2nd Information Hiding Workshop, Springer LNCS.1525* : 306-318.
- Castro, E. 1999. HTML 4 for the World Wide Web. *Fourth Edition, USA: Peachpit Press* : 384.
- Challita, K., and Farhat, H. 2011. Combining Steganography and Cryptography: New Directions. *International Journal of New Computer Architectures and their Applications*. 200-209.
- Chan, C. and Cheng, L.M. 2004. Hiding data in images by simple LSB substitution. *Pattern Recognition*. 37:469-474.
- Chang, C., Chuang, J., and Hu, Y. 2006. Spatial Domain Image Hiding Scheme Using Pixel-Values Differencing. *In Proceedings of Fundam. Inform* 70(3): 171-184.
- Changder, S., Ghosh, D. and Debnath, N.C. 2010. Linguistic Approach for Text Steganography through Indian Text. *International Conference on Computer Technology and Development*. (2-4): 318 – 322.
- Cheddad, A, Condell, J., Curran, K. and McKeivitt, P. (2008). Enhancing Steganography In Digital Images. *The Fifth Canadian Conference on Computer and Robot Vision* (28-30): 326-332.
- Cheddad, A., Condell, J., Curran, K. and McKeivitt, P. 2010. Digital Image Steganography: Survey and Analysis of Current Methods. *Journal of Signal Processing*. 90(3): 727-752.
- Clair, B. 2001. Steganography: How to send a secret message. <http://www.strangehorizons.com/2001/20011008/steganography.shtml>. Accessed on 13 October 2011.
- Delahaye, J.P., 1996. Information noyée, information cache. *Pour la Science*. (229): 142-148.
- Desai, S. D. and Kulkarni, L. 2010. A Quantitative Comparative Study of Analytical and Iterative Reconstruction Techniques. *International Journal of Image Processing* . 4(4):307-319.
- Diffie, W and Hellman, M. 1976. Multiuser cryptographic techniques. Diffie and Hellman, *AFIPS Proceedings*. 45(8):109–112.
- Du M. and Zhao M. 2011, Text Watermarking Algorithm based on Human Visual Redundancy. *Advances in Information Sciences and Service Sciences*. 3(5): 229 - 235.
- Dumitrescu, S., Wu, X. and Wang, Z. 2002. Detection of LSB steganography via sample pair analysis. *Proc. 5-th Int. Workshop on Information Hiding*. 355–372.

- Eisenberg, M. 1998. Hill ciphers and modular linear algebra. Mimeographed notes. *University of Massachusetts*, 1998. 19 pages.
- Emek, S. 2006. DWT-DCT Based Digital Watermarking Techniques for Still Images and Video Signals. *PhD's Thesis, Institute of Science, Yildiz Tech. Univ.* 1(2006).
- Emek, S. and Pazarci, M. 2006. A Cascade DWT-DCT Based Watermarking Scheme. *13th European Signal Processing Conference*. 9(2005).
- Emek, S. and Pazarci, M. 2006. Additive vs. Image Dependent DWT-DCT Based Watermarking. *MRCIS 2006, LNCS 4105*.(98-105).
- Fotopoulos, V. and Skodras, A. N. 2000. A Subband DCT Approach to Image Watermarking. *10th European Signal Processing Conference*. 9(2000).
- Fraczek, W., Mazurczyk, W. and Szczypiorski, K. 2010. Stream Control Transmission Protocol Steganography. *International Conference on Multimedia Information Networking and Security*. (4-6): 829 – 834.
- Fridrich, J. 1998. Symmetric Ciphers Based on Two-Dimensional Chaotic Maps. *Int. J. Bifurcation and Chaos*. 8(6):1259-1284.
- Fridrich, J., Goljan, M. and Du, R. 2001. Reliable detection of LSB steganography in color and grayscale images. *Proc. ACM Workshop on Multimedia and Security*. 27-30.
- Ganeshkumar, V. and Koggalage, R.L.W. 2010. A Language Independent Algorithm to Send Secret Messages using Steganography. *International Conference on Advances in ICT for Emerging Regions*. (29-1): 15-21.
- Ghasemi, E., Shanbehzadeh, J. and Fassihi, N. 2011. High Capacity Image Steganography using Wavelet Transform and Genetic Algorithm. *Lecture Notes in Engineering and Computer Science*. 2188(1): 495-498.
- Graps, A. 1995. An Introduction to Wavelets. *IEEE Computational Science and Engineering*. 2(2).
- Gunjal B. L., Manthalkar, R. R. 2010. An Overview of Transform Domain Robust Digital Image Watermarking Algorithms. *Journal of Emerging Trends in Computing and Information Sciences*. 2(1):37-42.
- Gunjal, B.L. and Manthalkar, R.R. 2010. An overview of transform domain robust digital image watermarking algorithms. *Journal of Emerging Trends in Computing and Information Sciences*. 2(1):37-42.
- Hamamreh, R. and Farajallah, M. 2009. Design of a Robust Cryptosystem Algorithm for Non-Invertible Matrices Based on Hill Cipher. *International Journal of Computer Science and Network Security*. 9(5): 11-16.
- Hill, L. S. 1929. Cryptography in an algebraic alphabet, *Amer. Math. Monthly*. 36 : 306–312.

- Huynh-Thu, Q. and Ghanbari, M. 2008. Scope of validity of PSNR in image/video quality assessment. *Electronics Letters*. 44(13): 800–801.
- Imran, A.S., Javed, M.Y. and Khattak, N.S. 2007. A Robust Method for Encrypted Data Hiding Technique Based on Neighborhood Pixels Information. *International Journal of Computer Science and Engineering*. 1(3): 159-164.
- Isbell, R. 2002. Steganography: Hidden Menace or Hidden Saviour. *Steganography White Paper*.10.
- Ismail, I.A., M. Amin and H. Diab, 2006. How to repair the hill cipher. *Journal of Zhejiang University-Science A*. 7(12): 2022-2030.
- Jeong, S., Hong, S. and Won, C.S. 2005. Dual Detection of Watermarks Embedded in the DCT Domain. *47th International Symposium*.( 8-10): 103 – 106.
- Johnson, N.F. 1998. Steganalysis: The Investigation of Hidden Information. *Information Technology Conference,IEEE*. (1-3): 113-116.
- Johnson, N.F. and Jajodia, S. 1998. Exploring steganography: Seeing the unseen. *IEEE Computer*. 31(2): 26-34.
- Judge, J.C., 2001. Steganography: Past, Present, Future. [http://www.sans.org/reading\\_room/whitepapers/steganography/steganography\\_past\\_present\\_future\\_552?show=552.php&cat=steganography](http://www.sans.org/reading_room/whitepapers/steganography/steganography_past_present_future_552?show=552.php&cat=steganography). Accessed on 10 October 2011.
- Kahn, D. 1996.The History of Steganography. *First Workshop of information, Hiding Proceedings, U.K., Lecture Notes in Computer Science*, 1174: 1-5.
- Kahn, D. 1996. The Codebreakers: The comprehensive history of secret communication from ancient times to the Internet. USA: Simon & Schuster.
- Kaul, M. 2011. Information Hiding Systems. *International Journal of Computer Science and Information Technologies*. 2(2): 866-870.
- Kekre, H.B., Athawale, A.A. and Patki, S.A. 2011. Improved Steganalysis of LSB Embedded Color Images Based on Stego-Sensitive Threshold Close Color Pair Signature. *International Journal of Engineering Science and Technology*. 3(2): 836-842.
- Ker, A.2004.Improved detection of LSB steganography in grayscale images.in *Proc. Information Hiding Workshop, Springer LNCS 3200*. 97–115.
- Khalaf, A., Al-Asmari and Al-Gamdi, O. 2009. High Capacity Data Hiding Using Semi-Hexagonal Pixels Value Difference. *International Conference of Computing in engineering, science and information*.
- Khalaf, E. T. and Sulaiman, N. 2011. A New Method of Image Watermarking Based on Lowest Effective Bits. *International Conference on Machine Learning and Computing*. 5(26-28): 504-508.

- Khalaf, E. T. and Sulaiman, N. 2011. A Robust Data Hiding Technique based on LSB Matching. *International Conference on Computer Science (ICCS 2011)*. (26-28): 117-121.
- Khalaf, E. T. and Sulaiman, N. 2011. Segmenting and Hiding Data Randomly Based on Index Channel. *International Journal of Computer Science Issues*. 8(3): 522-529.
- Khare, P., Singh, J. and Tiwari, M. 2011. Digital image steganography. *Journal of Engineering Research and Studies*. 2(3): 101-104.
- Khayam, S.A. 2003. The Discrete Cosine Transform (DCT): Theory and Application. *Information Theory and Coding*. 41(1):32.
- Kumar P.M. and Shunmuganathan, K.L. 2010. A Multilayered architecture for hiding executable files in 3D images. *International Journal of Computer Science and Technology*. 3(4): 402-407.
- Kumar, A. and Pooja, Km. November 2010. Steganography-A Data Hiding Technique . *International Journal of Computer Applications* . 9(7): 19-23.
- Kumar, K.B.S., Raja, K.B., Chhotaray, R.K. and Pattnaik, S. 2010. Coherent steganography using Segmentation and DCT. *Computational Intelligence and Computing Research (ICCIC)*. (28-29) .1 – 6.
- Kumar, S., P., Anusha, K. and Ramana, R., V. 2011. A Novel Approach to Enhance Robustness in Steganography Using Multiple Watermark Embedding Algorithm . *International Journal of Soft Computing and Engineering (IJSCE)*. 1(1): 50-56.
- Lee, Y.K., G. Bell, S.Y. Huang, R.Z. Wang and S.J. Shyu, 2009. An advanced least-significant-bit embedding scheme for steganographic encoding. *Adv. Image Video Technol.*, 5414: 349-360.
- Li, C., Zhang D. and Chen G. 2008. Cryptanalysis of an image encryption scheme based on the Hill cipher. *Journal of Zhejiang University - Science A*. 9(1118-1123):8.
- Lin, C.H., Lee, C.Y. and Lee, C.Y. 2004. Comments on Saeednia's improved scheme for the Hill cipher. *Journal of the Chinese institute of engineers*. 27(5):743-746.
- Lin, E. T. and Delp, E. J. 1999. A review of data hiding in digital images. *Proceeding of the Image Processing, Image Quality, Image Capture System Conference (PICS '99)*, Savannah Georgia : 274- 278.
- Low, S.H., Maxemchuk, N.F., Brassi, J.T. and O'Gonnan, L. 1995. Document marking and identification using both line and word shifting. *IEEE Computer and Communications Societies*. 2(2-6): 853 - 860.
- Lu C.-S., Liao H.-Y.M. 2001. Multipurpose watermarking for image authentication and protection. *IEEE Transactions on Image Processing*. 10 (10): 1579-1592.

- Lyu, S. and Farid, H. 2006. Steganalysis using higher-order image statistics. *IEEE Transactions on Information Forensics and Security*. 1(1): 111-119.
- Macq, B.M. and Quisquater, J.J. 1995. Cryptology for Digital TV Broadcasting. *IEEE*. 83(1): 944-957.
- Marvel, L.M., Retter, C.T., Charles, G. and Boncelet, Jr. 1998. *Hiding Information in Images. International Conference on Information Sciences and Systems*. 2(4-7):396 – 398.
- Mastronardi, G., Castellano, M. and Marino, F. 2003. Intelligent Data Acquisition and Advanced Computing Systems. *Proceedings of the Second IEEE International Workshop*. 11(8-10):116 – 119.
- Maurya A., Saini P. K. and Goel N. 2011 Chaffing and winnowing without using Steganography and encryption technique. *International Journal of Information Technology and Knowledge Management* 4(2):515-517.
- Mitra, S. and Manoharan, S. 2009. Experiments with and Enhancements to Echo Hiding. *International Conference on Systems and Networks Communications*. (20-25): 119 – 124.
- Moerland, T. 2003. Steganography and Steganalysis, [www.liacs.nl/home/tmoerlan/privtech](http://www.liacs.nl/home/tmoerlan/privtech). accessed on 11 October 2011.
- Moulin, P. and Koetter, R. 2005. Data-hiding codes. *IEEE*. 93(12): 2083-126.
- Moulin, P. & O'Sullivan, J. A. 2003. Information-theoretic analysis of information hiding. *Information Theory, IEEE Transactions on*. 49 (3): 563-593.
- Muttoo, S.K. and Kumar, S. 2009. Data Hiding in JPEG images. *International Journal of Information Technology (IJIT)*. 1(1): 13-16.
- Murdoch, S. J and Lewis, S .2005. Embedding Covert Channels into TCP/IP .*Draft for Information Hiding Workshop*.29: 1159.
- Nagaraj, V., Bharathiraja, M., Venkatesh, R., Rajkumar, S. and Sadiq Khan, B. 2010. Image Steganography Method Against Histogram Analysis. *International Conference On Information Science And Applications*. (6): 126.
- Overbey, J., Traves, W., Wojdylo, J., 2005. On the keyspace of the Hill cipher. *Cryptologia*, 29(1):59-72.
- Peticolas, F.A.P., Anderson, R.J. and Kuhn, M.G. 1999. Information Hiding – A Survey. *IEEE*. 1062-1078. *PIEEE*. 87(7): 1062-1078.

- Provos, N. & Honeyman, P. 2001. Detecting steganographic content on the internet. Ann Arbor, MI, Technical Report 01-11, 31 Aug. 2001. (<http://www.citi.umich.edu/techreports/reports/citi-tr-01-11.pdf>)
- Provos, N. and Honeyman, P. 2003. Hide and seek: An introduction to steganography. *IEEE Security and Privacy*. 01(3): 32-44.
- Rakesh R., Devathi, S., Sekaran P.S.C. and Kumar, S.S. 2011. Adaptive Randomization in Image Steganography Pertaining to Most Significant Nibble. *International Journal of Computer Applications*. 22(3).
- Rama, K., Thilagam, K., Manju, P.S.,Jeevarathinam, A.,Lakshmi, K. 2011. Survey and analysis of 3d steganography. *International Journal of Engineering Science and Technology*. 3(1): 638-643.
- Ramani, K., Prasad, E.V., Varadarajan, S. and Subramanyam, A. 2008. A Robust Watermarking Scheme for Information Hiding. *International Conference of Advanced Computing and Communications*. (14-17): 58–64.
- Raphael, A.J. and Sundaram, V. 2011. Cryptography and Steganography – A Survey. *International Journal of Computer Technology and Applications*. 2 (3).
- Roque, J. J. and Minguet, J. M. 2009.SLSB: Improving the steganographic algorithm LSB. *Proceedings The Ibero-American Congress on Information Security (CIBSI)*. (398-408).
- Saeednia, S., 2000. How to make the Hill cipher secure. *Cryptologia*, 24(4):353-360.
- Salvado, J. and Roque B. 2004. Evaluation of Transform Based Image Coders, Using Different Transforms and Techniques in the Transform Domain. *WSEAS Transactions on Computers Journal*. 3(1).
- Santhi, V. and Thangavelu, A. 2011. DC Coefficients Based Watermarking Technique for color Images Using Singular Value Decomposition. *International Journal of Computer and Electrical Engineering*. 3(1).
- Schneier B., 1996. *Applied Cryptography*. 2nd ed. New York: John Wiley & Sons.
- Shapiro L. and Stockman G.2001. *Computer Vision*. Prentice Hall.156-176.
- Shejul, A. A. and Kulkarni U. L.2011.A Secure Skin Tone based Steganography Using Wavelet Transform. *International Journal of Computer Theory and Engineering*. 3(1).
- Sherly, A.P. and Amritha, P.P. 2010. A Compressed Video Steganography using TPVD. *International Journal of Database Management Systems*. 2(3): 67-80.
- Shirali-Shahreza, M. and Shirali-Shahreza, M.H. 2008. An Improved Version of Persian/Arabic Text Steganography Using "La" Word. *National Conference on Telecommunication Technologies*. (26–28).

- Shirali-Shahreza, M. and Shirali-Shahreza, S. 2008. *High capacity persian/arabic text steganography. journal applied science.* 8(24): 4173-4179.
- Swain, G. and Lenka, S.K. 2010. A Hybrid Approach to Steganography Embedding at Darkest and Brightest Pixels. *International Conference on Communication and Computational Intelligence: 529 – 534.*
- Tanako, S. Tanaka, K. and Sugimura, T. 2000. Data Hiding via Steganographic Image Transformation. The Institute of Electronics, Information and Communication Engineers. E83-A: 311-319.
- Tiwari, N. and Shandilya M. 2010. Secure RGB Image Steganography from Pixel Indicator to TripleAlgorithm-An Incremental Growth. *International Journal of Security and Its Applications.* 4(4).
- Udomhunsakul, S. and Hamamoto, K. 2004. Wavelet filters comparison for ultrasonic image compression. *Conf. IEEE TENCON.* 1(21-24):171-174.
- Umbaugh, S.E. 2005. *Computer Imaging: Digital Image Analysis and Processing.* CRC Press.
- Vora, V. S., Suthar, A. C., Makwana, Y. N. and Davda, S. J. 2010. Analysis of Compressed Image Quality Assessments. *International Journal of Advanced Engineering Application.* 230: 225-229.
- Wang, Y. and Moulin, P, 2003. Statistical Signal Processing. *IEEE.* 56(11): 339 – 342.
- Wilson, V. and bryon. 1992. Linear, colorseparablehuman visual system model for vectordiffusioning system. *Journal of Electronic Imaging.* 1:277-292.
- Wu, D.C. and Tsai, W.H.2003. A Steganographic Method for Images by Pixel-Value Differencing. *Pattern Recognition Letters.* 24:1613–1626.
- Wu, H. C., Wu, N.I., Tsai, C.S. and Hwang, M. S.2005. Image Steganographic Scheme Based on Pixel-Value Differencing and LSB Replacement Methods. *IEE Proc. Vis. Image Signal Process.*(611-615).
- Yeh, Y. S., Wu, T. C., Chang, C. C., and Yang, W. C. 1991. A New Cryptosystem Using Matrix Transformation. *Proceedings of 25th Annual IEEE International Carnahan Conference.* (1-3):131-138.
- Yuzhong, P., Qin, CH., Jian, Z. 2004. Fragile watermarking self-embedded authentication algorithm of color image. *Computer Engineering and Design.* 24(12):2208-2212.
- Zaidan, B.B., Zaidan, A.A., Taqa, A., Alam, G.M., Kiah, M.L.M. and Jalab, A.H. 2010. StegoMos: A secure novel approach of high rate data hidden using mosaic image and ANN-BMP cryptosystem. *International Journal of the Physical Sciences.* 5(11): 1796-1806.
- Zhang, X. and Wang, S. 2005. Steganography using multiple-base notational system and human vision sensitivity. *IEEE Signal Process. Lett.,* 12(1):67-70



Zöllner, J., Federrath, H., Klimant, H., Pfitzmann, A., Piotraschke, R., Westfeld, A., Wicke, G. & Wolf, G. 1998. Modeling the security of steganographic systems. *In Proceedings of Information Hiding 98*: 344-354.

