



REPUBLIC OF TURKEY  
ALTINBAŞ UNIVERSITY  
Institute of Graduate Studies  
Information Technology

**AN EFFECTIVE IMAGE STEGANOGRAPHY  
SCHEME BASED ON LEAST SIGNIFICANT BITS  
AND COVER IMAGE TRANSPORTATION**

**Abbas Luaibi Obaid ALRWEGAOI**

Master's Thesis

Supervisor

Asst. Prof. Dr. Sefer KURNAZ

Istanbul, 2022

**AN EFFECTIVE IMAGE STEGANOGRAPHY SCHEME BASED ON  
LEAST SIGNIFICANT BITS AND COVER IMAGE TRANSPORTATION**

**Abbas Luaibi Obaid ALRWEGAOI**

Information Technology

Master's Thesis

ALTINBAŞ UNIVERSITY

2022

The thesis titled AN EFFECTIVE IMAGE STEGANOGRAPHY SCHEME BASED ON LEAST SIGNIFICANT BITS AND COVER IMAGE TRANSPORTATION prepared by ABBAS LUAIBI OBAID ALRWEGAOI and submitted on 18/08/2022 has been **accepted unanimously** for the degree of Master of Science in Information Technology

---

Asst. Prof. Dr. Sefer KURNAZ

Supervisor

Thesis Defense Committee Members:

Asst.Prof. Dr. Sefer KURNAZ

Faculty Of Engineering and  
Architecture ,

Altinbas University

---

Asst.Prof. Dr. Oguz KARAN

Faculty Of Engineering and  
Architecture ,

Altinbas University

---

Asst.Prof. Dr. serdar kargin

Faculty Of Electronic,

Beykent University

---

I hereby declare that this thesis meets all format and submission requirements of a Master's thesis.  
Submission date of the thesis to Institute of Graduate Studies: \_\_\_/\_\_\_/\_\_\_

I hereby declare that all information/data presented in this graduation project has been obtained in full accordance with academic rules and ethical conduct. I also declare all unoriginal materials and conclusions have been cited in the text and all references mentioned in the Reference List have been cited in the text, and vice versa as required by the abovementioned rules and conduct.

Abbas Luaibi Obaid ALRWEGAOI

Signature

## DEDICATION

To the prophet of mercy "**Muhammad bin Abdullah** (Peace Be Upon Him)" and my beloved country (**Iraq**).

## **PREFACE**

First and foremost, all praise and thanks are due to Allah, and peace and blessings be upon his Messenger, Mohammed (Peace Be Upon Him). Next, I wish to express my sincere appreciation to my main supervisor, Assist Prof. Dr. Sefer KURNAZ. for encouragement, guidance, critics, and friendship. I indeed thank him for showing me how to identify interesting problems and how the research can be started and finished correctly.

In preparing this thesis, I was in contact with many researchers, academicians, and practitioners. They have contributed towards my understanding and thoughts. My sincere appreciation also extends to all my AU postgraduate colleagues for their support and encouragement to get this work done. Their views and tips were useful indeed.

Finally, I am grateful to my lovely wife (Waffaa) and my beloved sons ( Rtaj , Rwan ,Rama ) members for their support and dua'a. In particular, I would like to thank my wife for her patience, encouragement, support, and understanding.

## **ABSTRACT**

### **AN EFFECTIVE IMAGE STEGANOGRAPHY SCHEME BASED ON LEAST SIGNIFICANT BITS AND COVER IMAGE TRANSPORTATION**

Obaid, Abbas

M.Sc., Information Technology, Altınbaş University,

Supervisor: Sefer KURNAZ

Date: 08 /2022

Pages: 134

In this era of information security and communication, a high priority is achieving a robust and secure steganography scheme when considering information concealment. Developing such a scheme for hiding a secret message should ideally disguise the hidden data well within transmission media. Pressing challenges in the context of a steganography system include security, imperceptibility, and capacity issues. Most researchers have highlighted the trade-offs between these issues. The trade-off between payload and security has been neglected by researchers, as fixing one issue has been indicated to affect the other, and vice versa. To overcome the aforementioned issues, an effective method has been proposed for image steganography, known as the Least Significant Bits Permutation Approach (LSBPA). The LSBPA is employed for the improvement of the contributions of the suggested scheme. Three main stages were considered for the achievement of the research objectives, beginning with image and text preparation, followed by embedding, and culminating in extraction. Finally, the evaluation stage employed several evaluations to benchmark results. A standard database from

the Signal and Image Processing Institute (SIPI) containing color and grayscale images with 512 x 512 pixels was utilized in this work. The security and imperceptibility (image quality) of the proposed scheme were evaluated using different parameters. The three important image quality measures are Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM), and Histogram analysis. At the same time, two security measurements used are Human Visual System (HVS) and Chi-square ( $\chi^2$ ) attacks. Based on what was found, the proposed scheme shows how to increase capacity, invisibility, and security to solve problems that already exist.

**Keywords:** Information hiding, Image steganography, LSB, Knight tour, RSA, and Huffman coding.



# TABLE OF CONTENTS

	<u>Pages</u>
<b>ABSTRACT.....</b>	<b>vii</b>
<b>LIST OF TABLES.....</b>	<b>xii</b>
<b>LIST OF FIGURES.....</b>	<b>xiii</b>
<b>ABBREVIATIONS.....</b>	<b>xvii</b>
<b>1. INTRODUCTION .....</b>	<b>1</b>
1.1 PROBLEM BACKGROUND.....	3
1.1.1 Security .....	4
1.1.2 Embedding Process.....	4
1.1.3 Payload Capacity .....	5
1.2 PROBLEM STATEMENT .....	7
1.3 RESEARCH QUESTIONS.....	8
1.4 RESEARCH AIM AND CONTRIBUTIONS .....	8
1.5 RESEARCH OBJECTIVES .....	9
1.6 RESEARCH SCOPE .....	9
1.7 RESEARCH SIGNIFICANT.....	10
1.8 RESEARCH OUTLINE .....	10
<b>2. LITERATURE REVIEW .....</b>	<b>11</b>
2.1 INTRODUCTION .....	11
2.2 INFORMATION SECURITY .....	12
2.3 HISTORY OF STEGANOGRAPHY .....	13
2.4 TERMINOLOGY OF STEGANOGRAPHY .....	15
2.5 PROPERTIES OF STEGANOGRAPHY .....	17
2.5.1 Imperceptibility .....	17

2.5.2	Robustness.....	18
2.5.3	Payload Capacity .....	19
2.6	CLASSIFICATION OF STEGANOGRAPHY .....	19
2.6.1	Classification- Based Cover Medium Types.....	20
2.6.2	Classification –Based Key Types .....	22
2.6.3	Classification- Based Embedding-Techniques.....	23
2.6.4	Classification- Based Extraction Function.....	24
2.7	STEGANALYSIS AND STEGANOGRAPHY ATTACKS.....	25
2.7.1	Types of Steganographic Attacks .....	25
2.8	LITERATURE REVIEW .....	27
2.8.1	Spatial or map domain .....	28
2.8.2	Frequency domain.....	30
2.8.3	Adaptive domain.....	34
2.9	RESEARCH DIRECTIONS .....	35
2.10	RELATED WORKS OF IMAGE STEGANOGRAPHY SYSTEMS .....	37
2.11	SUMMARY .....	42
<b>3.</b>	<b>RESEARCH METHODOLOGY.....</b>	<b>43</b>
3.1	INTRODUCTION .....	43
3.2	RESEARCH FRAMEWORK .....	43
3.3	EXPLANATION OF THE PROPOSED METHOD.....	47
3.3.1	Data Pre-processing Phase .....	47
3.3.1.1	Secret message pre-processing .....	48
3.3.1.2	Cover image pre-processing .....	62
3.4	EMBEDDING PROCESS .....	62
3.4.1	Knight Tour Based- Image Scrambling. ....	63
3.4.2	Applying LSB Permutation Approach (LSBPA). ....	65

3.5	STEGO-IMAGE.....	68
3.6	IMAGE EXTRACTING.....	69
3.7	EVALUATION METRICS .....	71
3.8	DATASET .....	72
3.9	SUMMARY .....	73
<b>4.</b>	<b>RESULT AND DESCUSSION.....</b>	<b>75</b>
4.1.	INTRODUCTION.....	75
4.2.	EXPERIMENTAL EVALUATION OF THE PROPOSED SCHEME.....	75
4.3	SOFTWARE IMPLEMENTATION.....	76
4.4	RESULTS DISCUSSION AND ANALYSES .....	83
4.4.1	Human Visual System Attack (HVS).....	84
4.4.2	Image Visual Quality (Imperceptibility).....	88
4.4.3	Robustness.....	96
4.4.4	Histogram Attacks .....	102
4.5	RESULT'S BENCHMARKING .....	105
4.6	DISCUSSION .....	106
<b>5.</b>	<b>CONCLUSION AND FUTURE WORK.....</b>	<b>107</b>
5.1.	INTRODUCTION.....	107
5.2.	THE PRE-PROCESSING STAGE .....	107
5.3.	THE PROPOSED LEAST SIGNIFICANT BIT PERMUTATION APPROACH..	108
5.4.	EVALUATION METRICS .....	108
5.5.	FUTURE WORK SUGGESTION .....	109

## LIST OF TABLES

	<u>Pages</u>
Table 2.1: Summary of steganographic attacks .....	27
Table 2.2: A study analysis of the related literature study (between the years 2015 to 2020). .38	38
Table 3.1: The encrypted message achieved using the RSA algorithm .....	52
Table 3.2: The decrypted message achieved using the RSA algorithm .....	53
Table 3.3: The detail distribution of the standard dataset images .....	73
Table 4.1: The PSNR value of the Lena Gray-Scale Image using various embedding capacities (EC) .....	90
Table 4.2: The PSNR value of the Baboon Gray-Scale Image using various embedding capacities (EC) .....	90
Table 4.3: The PSNR value of the Pepper Gray-Scale Image using various embedding capacities (EC) .....	91
Table 4.4: The PSNR value of the House Gray-Scale Image using various embedding capacities (EC) .....	91
Table 4.5: The MSE, SSIM, and NCC evaluations metrics for various gray-scale SIPI images .....	98
Table 4.6: The histogram attacks of various SIPI database images with 16384 bytes of embedding capacity .....	102
Table 4.7: Expressed the benchmark of the current results with the existing literature review for Baboon gray-scale image with 32768 Bytes .....	106

## LIST OF FIGURES

	<u>Pages</u>
Figure 1.1: The trade-off between the key issues of image steganography system (Kadhim et al., 2019).....	2
Figure 1.2: A general diagram of steganography model (Kadhim et al., 2019) .....	3
Figure 1.3: A cause-and-effect diagram of research issues related to the design and development of image steganography methods.....	7
Figure 2.1: An all-inclusive history of information hiding system and processes.....	11
Figure 2.2: Classification of the basic security systems (Cheddad et al., 2010) .....	12
Figure 2.3: The basic concepts of the steganographic system.....	15
Figure 2.4: Key issues of steganography system .....	17
Figure 2.5: A comprehensive Classification of steganography .....	19
Figure 2.6: Types of steganography attacks .....	26
Figure 2.7: DFT-based embedding of secret message.....	31
Figure 3.1: The schematic of the proposed scheme .....	44
Figure 3.2: The entire scenario of the embedding process .....	46
Figure 3.3: The whole scenario of the extracting method .....	47

Figure 3.4: The pseudo code of the utilized RSA algorithm. .... 49

Figure 3.5: The flowchart of the RSA encryption and decryption process ..... 50

Figure 3.6: The RSA algorithm..... 51

Figure 3.7: Algorithm ..... 52

Figure 3.8: The General Flowchart of Huffman coding [111]..... 54

Figure 3.9: The Huffman algorithm with secret key ..... 55

Figure 3.10: Huffman coding tree for compressing the message (( $e < \tau \bar{U} < \tau \bar{U} \tau f \hat{a} \hat{h} \alpha < f \hat{a} \hat{R} f \hat{h} \bar{a} \hat{a}$ )). ..... 58

Figure 3.11: The process of transforming the RGB image to the YCbCr ..... 62

Figure 3.12: Dividing the cover image into **4 × 4 blocks** utilizing Knight Tour algorithm .... 64

Figure 3.13: The movement of KTA on the chess-board squares..... 64

Figure 3.14: The process of the applying LSBPA ..... 66

Figure 3.15: The proposed LSBPA ..... 67

Figure 3.16: The embedment and extracting process in the proposed steganography scheme 68

Figure 3.17: Embedding and extracting processes ..... 70

Figure 3.18: USC SIPI dataset ..... 73

Figure 4.1: The main interface of the demo system.....	77
Figure 4.2: The embedding process within proposed system.....	78
Figure 4.3: Selecting a cover image for the embedment of a selected secret bit .....	78
Figure 4.4: Different payload capacities used in the proposed system .....	80
Figure 4.5: The resulted images after embedding process .....	81
Figure 4.6: The Extracting process within proposed system .....	82
Figure 4.7: The use of various methods of the proposed image steganography scheme .....	84
Figure 4.8: The demonstration of the visual attacks with different bit planes for the Pepper image .....	85
Figure 4.9: The demonstration of the visual attacks with different bit planes for the Lina image .....	86
Figure 4.10: The performance metrics of the proposed LSBPA method vs HVS attack for the original gray-scale baboon image .....	87
Figure 4.11: The bit plane (1) of the Baboon and Lina SIPI database images with the proposed LSBPA method .....	88
Figure 4.12: Lina, Baboon, Pepper, and House USC-SIPI database images.....	90
Figure 4.13: The PSNR value of Lina image.....	92
Figure 4.14: The PSNR value of Baboon image.....	93

Figure 4.15: The PSNR value of Pepper image .....	93
Figure 4.16: The PSNR value of House image .....	94
Figure 4.17: Lina, Baboon, Pepper, and Tiffany color USC-SIPI database images .....	94
Figure 4.18: The PSNR value of different colour images with 16400 Bytes .....	95
Figure 4.19: The idea of the proposed LSBP Amethod .....	97
Figure 4.20: The $\chi^2$ -test for the original Lina image.....	99
Figure 4.21: The $\chi^2$ -test for the simple LSB method with embedded 16384 pixels .....	100
Figure 4.22: The $\chi^2$ -test for the suggested scheme after embedment of 16384 bytes.....	100
Figure 4.23: The embedment using the proposed system for the Lena image with (A) 49152 and (B) 32768 bytes .....	101
Figure 4.24: The Histogram distribution of the original RGB Baboon image (c, d and e) virsus stego RGB Baboon image (f, g and h) with (16400 EC bytes).....	105



## ABBREVIATIONS

DCT	:	Discrete Cosine Transform
$\chi^2$	:	Chi-square
DE	:	Difference Expansion
DE	:	Difference Expansion
DFT	:	Discrete Fourier Transform
LSBPA	:	Least Significant Bit Permutation Approach
EC	:	Embedding Capacity
ER	:	Error Rate
FFT	:	Fractional Fourier Transform
HDWT	:	Haar Discrete Wavelet Transform
HVS	:	Human Visual System
ISS	:	Image Steganography Scheme
JPEG	:	Joint Photographic Experts Group
LSB	:	Least Significant Bit
MSB	:	Most Significant Bit
MSE	:	Mean Square Error
NCC	:	Normalized Cross-Correlation
PND	:	Random
POV	:	Pairs of Values

PSNR	:	Peak Signal-to-Noise Ratio
PVD	:	Pixel Value Differencing
RGB	:	Red, Green and Blue
YCbCr	:	Luminance; Chroma: Blue; Chroma: Red (Colour system)
SSIM	:	Structural Similarity Index Measure
SSSM	:	Shuffle the Segments of Secret Message
SVM	:	Support Vector Machine
TCP/IP	:	Transmission Control Protocol/Internet Protocol
TIFF	:	Tagged Image File Format
WFFT	:	Weight Fractional Fourier Transform

# 1. INTRODUCTION

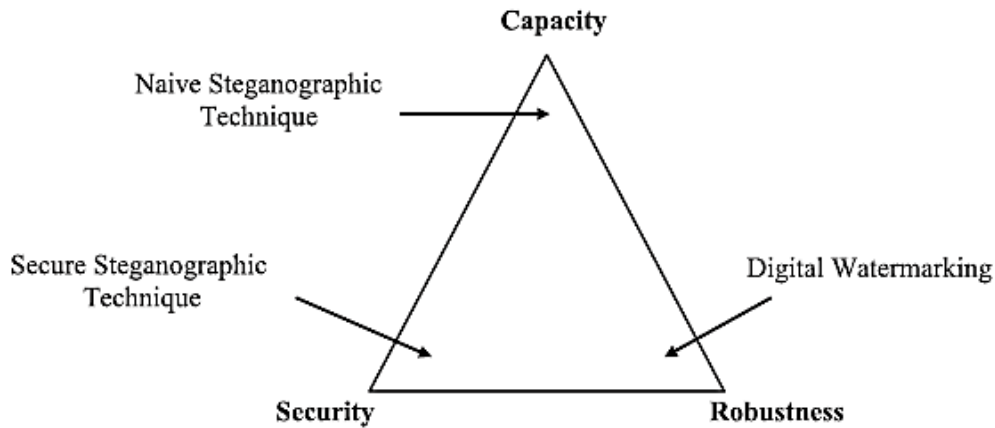
Data transmission in different formats (audio, text, video, and image) has become extremely easy in this age of the Internet. However, many problems have been associated with this increased access to the huge information volume, such as threats to information privacy and security. Hence, securing the secret information over an unsecured network is a challenge. Oftentimes, adversaries or intruders can opt to corrupt information by altering the secret message, thereby causing moral or financial damage. Thus, to obtain secure data communications, various systems of information cryptography (encryption) and information concealing (steganography) have been developed.[1], [2].

Steganography is an emerging and greatly demanding method for secure information communication over the internet using a secret cover media. It can be used for different applications such as industry, health care, safe circulation of secret data in intelligence, habitat, online voting, military, mobile banking[3]. Cryptography, on the other hand, is the study and practice of ways for secure communication in the face of adversarial behavior. Generally, cryptography refers to the steps involved in the creation and analysis of protocols for the prevention of unauthorized access to private information by the general public or third parties [4].

Many types of steganography systems have emerged in the modern era, including (audio, video, text, network, DNA and image). . Over the last decade, several studies have been done on image steganography systems. That's because these systems had become popular because they made it very easy for people to share media contents with low-cost gadgets such as IP cameras and smartphones, as well as social platforms such as Twitter and WhatsApp [5].

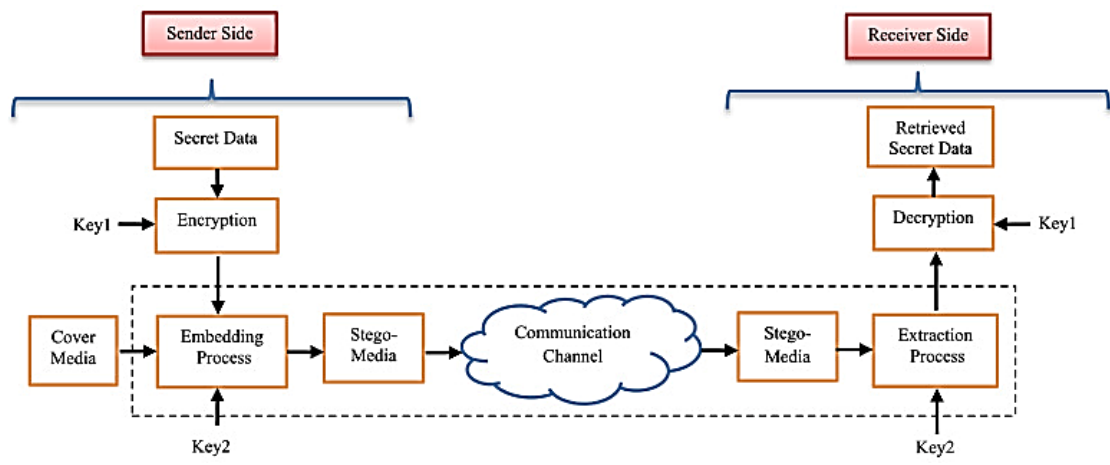
Scholars have come up with many solutions to ensure the applicability of image steganographic methods in many fields, such as medicine, the military, and cloud computing [6], [7]. However, the existing steganography methods suffer from three main problems which are. First, inability to increase the embedding capacity. Second, perceptibility of the hidden information in the cover image. Finally, poor security and resistance of the steganography systems against steganalysis

attacks. These three major key issues (difficulties) of the existing image steganography systems are represented in Figure 1.1.



**Figure 1.1:** The trade-off between the key issues of image steganography system [4]

In image steganography, the stego-image refers to the image that holds the secret data of a level of quality, while the original image is called the cover-image [8]. There is a relationship between the stego image quality and other evaluation criteria like payload capacity, robustness, and security. High payload capacity means less stego quality (imperceptibility). The scenario of image steganography can be described in two main aspects; first, the secret text must be hidden by the sender in the cover image using a secret key; secondly, the receiver must be able to use the secret key provided by the sender to decode the secret message hidden in the stego image [9]. As a result, image steganography is basically aimed at obtaining and receiving the stego image without being detected by hackers [10]. The general scenario of the image steganography system is shown in Figure 1.2.



**Figure 1.2:** A general diagram of steganography model [4]

Several methods for ensuring the security of secret communications transmitted over the internet have been proposed in the literature. Steganography ensures that secret communications are hidden in a trusted cover image and can be retrieved by the intended receiver without modifying the meanings or nature of the hidden data. This data can be concealed in a variety of media, including audio, image, text, DNA, protocol and even text. Each of these methods, however, has advantages and disadvantages [1], [4], [11]. Eventually, the main advantage of image steganography is that the intruder is unaware of the secret text hidden in the chosen image. Images will be employed to host data in the proposed system due to their ability to retain a huge amount of data and the inability of an intruder to detect this data.

**1.1 PROBLEM BACKGROUND**

Due to the huge volume of data exchange over the Internet, and since the digital information revolution has brought about profound changes in daily life, data security has become a major concern and so the data integrity and confidentiality are required for protecting against hackers and unauthorized use. [12], [13]. Today, information hiding and information encryption techniques play a significant role in maintaining information security by increasing in the confidentiality of data security [14].

Because of the advancement of the modern era and the increased utilization of digital images in various applications on the World Wide Web (WWW), image steganography is becoming more practical and powerful at concealing secret data than other types of media [1], [15].

Image steganography refers to the process of concealing secret data in a digital image so that the hidden data is imperceptible to everyone except the intended recipient. Image steganography has received great research attention for many years as a way of processing confidential data and creating secret channels to hide sensitive information [4], [16].

Various embedding methods have been suggested to conceal the secret message in the carrier to improve security as effectively as possible while ensuring the imperceptibility of the stego image. However, highly secure image steganography systems with large amounts of secret bits have not yet been achieved and researches in this field are ongoing [5], [8]. The following sections detail the problems inherent in the proposed study.

### **1.1.1 Security**

In today's world, internet is essential for transmitting data and socializing with others. Securing the data transmitted during the Internet is more important than before due to the development of hacking programs, therefore, it has become important for researchers to develop novel methods for protecting the image steganography systems against malicious manipulation[17].

The security of data concealed within carrier images is dependent on the method of concealing the secret message, and this issue remains to be a challenge [2]. At the present, attackers are increasingly knowledgeable and skilled about decoding the secret message from the carrier (image after embedding) [18]. Therefore, understanding or inventing new ways of embedding process has become a necessity to safeguard the communication of data between approved parties.

### **1.1.2 Embedding Process**

The process of hiding data by replacing the secret bits with image pixels in a certain way is referred to as embedding. Typically three inputs are used in the embedding process; these are

the secret data, an optional secret key, and the cover object [5]. The embedding process embeds secret data into the cover image using a certain method, for example LSB substitution, and produces a stego image (image after embedding). Some methods must be used during the embedding process for the selection of the change locations. Three general selection criteria (are sequential, adaptive, and random) must be followed to maintain control over the change location [4].

To improve the security of image steganography systems, and since an inverse relationship exists between security and high payload capacity in steganography systems, researchers have made great efforts to minimize the number of secret message bits to be included within the image of a host; it has been suggested that this number must be less than the number of the image pixels (Liao et al., 2020).

Several embedding procedures have been suggested in the state-of-the-arts, and the majority of these studies concentrate on concealing secret bits in the “Least Significant Bits (LSB)” of the cover image pixel because of the considerable advantages of this technique such as its simplicity of understanding and ease of usage, undetectable to the naked eye and allows for a large payload capacity for hidden messages [4], [8], [19]. However, simple LSB technology has become understood and is easy to hack nowadays, require the usage of modern theories that select the pixels which hides the secret bits randomly and in turn improves the security of the concealing system [20].

### **1.1.3 Payload Capacity**

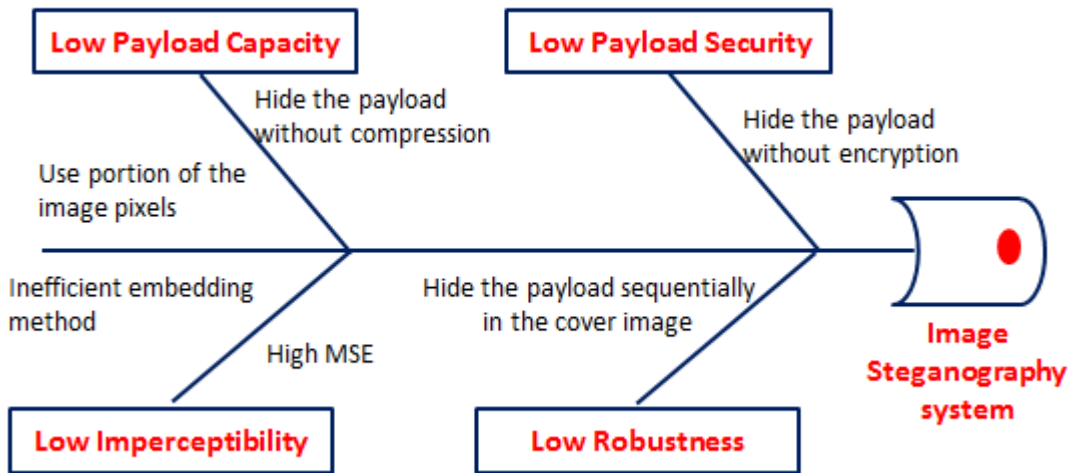
This is a crucial requirement for steganography systems; it is the optimum volume of data that can be concealed in the carrier image. In the domain of image steganography, there are two different types of capacity; these are steganography capacity and embedding capacity (EC) [21]. For an image media, the EC is the optimum number of embeddable bits. For instance, with the LSB replacement method, the grey scale image has an EC that is equal to the entire number of pixels in the image. For the steganography capacity, it is unlike the EC as it is difficult to be estimated even with the simplest embedding technique. It is described as the optimum number

of embeddable bits in an image media with a minimal enough likelihood of detection that the attacker can ignore it.

There is a balance between payload capacity and other evaluation metrics; the greater the payload capacity, the less security, robustness, and imperceptibility [22]. Effective image steganography methods conceal a large amount of hidden bits while maintaining the Stego image's quality as similar as possible to the original. However, no optimal system has been identified in literature (high payload capacity with good imperceptibility)[23]. In other words, the higher the embedding capacity of the hosted image, the more the vulnerability of the stego image to statistical attacks such as (Histogram, Chi-square  $\chi^2$  and the Human Visual system (HVS)), Therefore, the data must be pre-processed before the embedding process (secret text and cover image)

The proposed scheme seems to be quite similar to previous studies in that it hides the secret text using a single bit (LSB). As a result, pre-processing the secret using Huffman coding technique prior to the embed stage is required to solve the problem of low payload capacity. Finally, the problem background of any image steganography system is illustrated by the following scenario (it is a tedious task to increase the payload capacity of the secret message, and the trade-off between durability and security must be maintained). Figure 1.3 illustrates the cause-and-effect diagram of research issues related to the development of Image Steganography Systems (ISS).





**Figure 1.3:** A cause-and-effect diagram of research issues related to the design and development of image steganography methods

## 1.2 PROBLEM STATEMENT

There are many issues with conventional image steganography schemes that must be overcome. Latterly, the main challenge faced by the image steganography developers is associated with the poor imperceptibility of the stego-image. Meanwhile, the attackers became more knowledgeable with sophisticated tools and expert in the field of security, causing more severe attacks on the transferred data over the internet. Therefore, the imperceptibility level must be improved to obtain stego images of better quality. In this regard, the present work aims to develop an effective method based on spatial domain to conceal a secret bit within a trusted carrier by substituting the secret bits to be included in the image pixels in such a way that hackers are unable to distinguish the hosted images from the original images.

The imperceptibility and the security of image steganography systems are characterized by the PSNR values that relate inversely with the MSE. The high PSNR values can be achieved by lowering the MSE of any image steganography system [4], [5]. The high PSNR of the steganography system implies the good image quality. Thus, dividing the selected image into 4x4 blocks and randomly selecting pixels for each block and then using a new LSB Permutation Approach (LSBPA) is necessary to solve the problem associated with existing state-of-the-arts.

Another ongoing problem with previously developed image steganography systems is the limited payload capacity. To get around this limitation, Huffman coding has been used with the proposed scheme to reduce the size of the secret data by up to 30% prior to embedment.

Due to the development of steganalysis systems, retrieving the secret text is another problem that most concealing systems face at the moment. Hence, prior to embedment, the secret text had to be encrypted. For two reasons, the suggested scheme uses the AES algorithm to encrypt the secret text. The first is to introduce a new security level to the suggested system, and the second is to improve the cipher text's randomness, which aids the Huffman algorithm in maximizing the text compression ratio.

### **1.3 RESEARCH QUESTIONS**

The research questions are as follows:

1. What are the limitations of the existing solutions regarding the image steganography system?
2. How could the embedding of the secret message be improved?
3. How to evaluate the improvement that the proposed solution has achieved?

### **1.4 RESEARCH AIM AND CONTRIBUTIONS**

This study aims to design and develop an efficient image steganography scheme that maximizes payload capacity while maintaining the imperceptibility and security of stego images shared online using the LSB Permutation Approach (LSBPA). The contribution to the proposed scheme is made to ensure close resemblance between the stego and original images through the use of several improvements that have been implemented at different stages of the proposed scheme, as described below.

1. *Increase the proposed scheme system:* Scanning the pixels of the cover image which utilized to hide the secret bits using the Knight Tour algorithm that divides the image into four sections, then randomly selects the pixels within the single section.

2. *Increase the payload security:* encrypt the secret text using the AES method to convert the plain text to the unreadable text which in turn increase the redundancy of the secret letters.
3. *Increase the payload capacity:* compress the encrypted secret text up to 30% using Huffman coding.
4. *Increase the robustness:* Divide the chosen image into 4×4 blocks and randomly select pixels in each block to hide the secret bit using Knight Tour algorithm.
5. *Increase the image visual quality (imperceptibility):* Substitute the secret bits with the LSB of the hosted image directly if there is a match between the secret text bit values and the image pixel bits, or swap the secret bits (flip the secret message) and embed it when there is dis-match between the secret bits with the LSB of the hosted image. using LSB Permutation Approach (LSBPA).
6. *Increase the reliability:* benchmarking the achievement results with the existing methods using various statistical and non-statistical metrics.

## **1.5 RESEARCH OBJECTIVES**

1. To examine the issues associated with image steganography systems and the methods for solving such issues.
2. To suggest an LSB Permutation Approach (LSBPA) for embedding a secret bits which improves the imperceptibility and security of the proposed system.
3. To evaluate the proposed scheme using different statistical measures and to compare the improved scheme with existing studies.

## **1.6 RESEARCH SCOPE**

1. The study does not address image manipulation such as zooming, rotating, scaling, etc.
2. The secret bit for embedment in the chosen image is in text format.

3. The proposed scheme used colour and gray images when evaluating used standard USC-SIPI dataset with 512 by 512 pixels.
4. Six evaluation criteria were considered in this study, namely; Chi-Square attack, HVS attack, Histogram attack, PSNR, NCC and SSIM.
5. The proposed scheme does not discuss the speed of the encryption process and its comparison with other studies.

## **1.7 RESEARCH SIGNIFICANT**

It is noticeable that the proposed system aims to overcome some steganography issues, making it more trustworthy in terms of security and capacity. The aim of this research is to maintain the robustness of an image steganography system while achieving a high PSNR. The proposed scheme attempts to address a payload capacity issue and reduce its dependence on some other factors like (security and imperceptibility). Some existing methods in the literature have limitations in the embedding process [4], [24]. Many applications, notably military, medical, cloud computing, and industry, already use image steganography systems-based applications, therefore the proposed system would attempt to improve the robustness to handle the above applications.

## **1.8 RESEARCH OUTLINE**

This thesis is divided up into five sections, excluding the introduction: Chapter 2 gives an overview of data hiding strategies in general, then discussions about steganography techniques and how they cooperate, and then classifies image steganography techniques. Each study's pros and cons are looked at. Chapter 3 discusses well about research method and the overall framework in great detail. Chapter 4 talks about and shows the proposed scheme's results with figures and tables. Chapter 5 summarizes the contributions and talks about their shortcomings and

## 2. LITERATURE REVIEW

### 2.1 INTRODUCTION

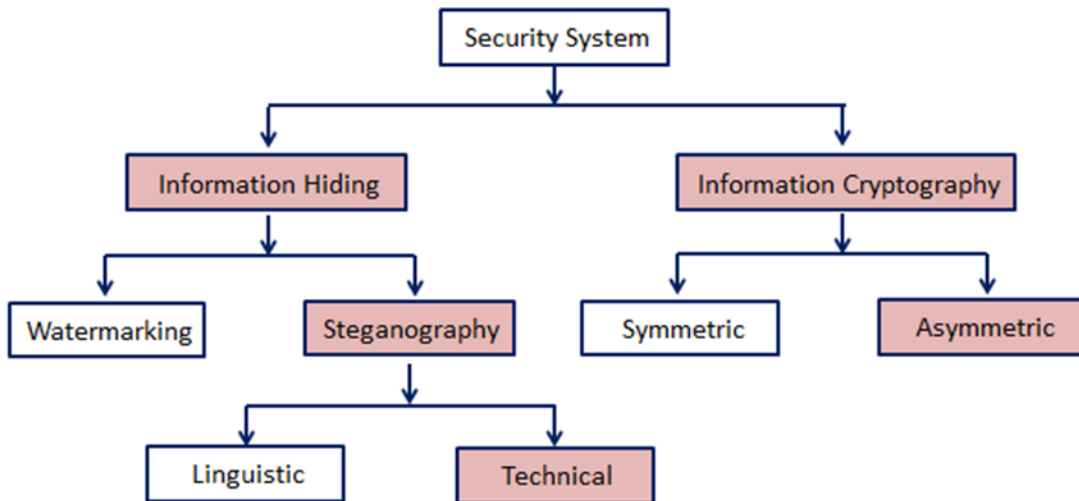
This chapter presents a review of the related literatures in the field of information hiding system in general and image steganography techniques in particular. An all-inclusive summary that aimed to identify all the proposed research objectives and questions based on the research gaps are presented. As mentioned in chapter 1, this chapter also summarizes relevant literature on the subject of this thesis. It begins with an overview of the categorization of the information security domain. The history of steganography was illustrated from ancient times to the digital era. The terminology of digital steganography was explained, along with its components. Additionally, this chapter has discussed in extensively the properties of steganography. Additionally, it classified the cover types, secret key, embedding methods, and extraction methods. Illustrated are the designed and developed concealment methods. Finlay, the related studies are summarized in a table. Figure 2.1 shows the general flow of this chapter where the numbers indicating the corresponding section and subsection.



**Figure 2.1:** An all-inclusive history of information hiding system and processes.

## 2.2 INFORMATION SECURITY

The World Wide Web now allows for the unrestricted and simple transmission of digital data information (video, music, image, text, etc.) through the world wide web (WWW). Meanwhile, such unrestricted access to huge data volumes comes with significant risks to information privacy and security over the WWW, making it difficult to secure information over public networks [25], [26]. Unauthorized users or intruders can frequently corrupt information via modification of the message, causing both ethical and financial problems. As a result, several strategies have been developed for hiding and encrypting information to achieve safe data transfers. Figure 2.2 depicts the classification of various security solutions proposed thus far.



**Figure 2.2:** Classification of the basic security systems [27]

Information hiding schemes (Figure 2.2) are of two types; these are watermarking and steganography schemes [4], [5] and both schemes are used for hiding secret bits. However, both schemes are closely related but with different objectives. Watermarking has the major objective of protecting the integrity of the secret bit with or without keeping it from being noticed by eavesdroppers [28]. Steganography techniques on the other hand aim to hide and protect the communicated data from being detected by outsiders [29]. The secret message is scrambled in a way that makes it unintelligent (encrypted) communication to the eavesdroppers during the information encryption process known as cryptography. An encrypted secret message, on the

other hand, is frequently inapplicable, drawing the attention of or making it evident to eavesdroppers. To overcome this limitation, the invisible communication is essential without enabling any attention to the third party. In short, the development of some robust information hiding systems is mandatory for the secured and privacy preserved communication of the sensitive data over the Internet [30]. In this perception, this thesis explored the feasibility of developing a robust steganography system and tested its performance against various attacks validate its outperforming traits.

### **2.3 HISTORY OF STEGANOGRAPHY**

Steganography is a robust way of hiding secret bits in a reliable carrier in a manner that makes the hosted media that conceals the secret message unrecognisable and unseeable to an intruder or someone else who isn't supposed to see it [31]. Steganography is a term coined from two Greek terms, "Stegos", meaning "cover" and "grafia", meaning "writing"; hence, steganography can be defined deductively as "cover writing" [32].

Information hiding has a long history, beginning when the nobleman was in need to contact his son; he devised the method of tattooed messages on chosen slaves and in their scalp after shaving; then, when the hair has grown again, he will send the slave to his son, with the tattooed message still hidden inside his scalp. This was the first attempt to steganography [22], [33].

During World War II, the famous method used to send secret message was invisible ink with variable extraction code technique. Invisible ink nowadays uses different techniques like Ultraviolet light this is used with anti-counterfeit devices. The first attempt to secret message hiding into innocuous text started with the monk Johannes T. when he considered modern cryptography [34]; this method started with the smart idea to conceal information in the angle name of long invocations when the secret message is collected from the special pattern of letters within the original text as in the following example:

**"Padiel aporsy mesarpon omeuas peludyn malpreaxo"**

And the secret message should be decoding as "Prmus apex."

Null ciphers were employed to hide information during World War II. A null cipher always appears honest (innocent) to the enemy as in the following example:

***"Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils".***

The secret message is taken from the second letter in each word to extract the given message which is in our example (***Pershing sails from NY June 1***).

To go back to ancient history, "Steganographia" is the title of the first book that considered steganography; it consists of 400 pages and was written by Gaspari Schott in 1665. This book includes the ideas almost took from the monk Trithemius. Cryptography on the other hand was first introduced in the book titled "Cryptographie Militaire" which was published by [35]. The book also mentioned the principles of steganography system that took must be considered when suggesting or designing any steganography system [34], [36].

In the digital era, and with the widespread use of information transmission technologies such as the Internet, it has become necessary to develop modern steganography approaches to protect the vital message from the unauthorized people. As a result, Researchers have spent more effort trying to keep the message transferred through the internet secured and many methods have been suggested, each having its advantages and weaknesses[22], [31] .Since the dawn of the hacking era and the widespread adoption of the internet. Researchers are now working on merging cryptographic systems with steganography systems, and the combination of the two approaches offers an extra layer of protection, as the secret text cannot be read even if it is extracted [37].

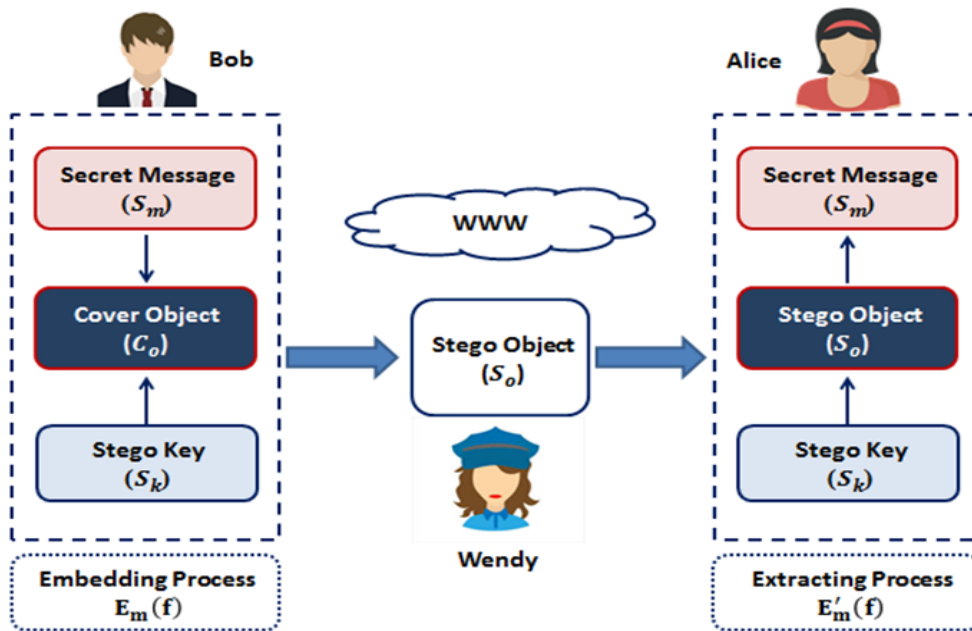
The main objective of both steganography and cryptography is protection of the secret text from hacking during transmission in unsecured communication. Steganography does not like cryptography; with cryptography, the secret text is publicly available, and some people enjoy the challenge of breaking it. While, in steganography, the most important thing is to make the message undetectable for the third party. Cryptography also ensures the secret message can be seen on the other side while steganography is keen to be invisible to human eyes [31].



## 2.4 TERMINOLOGY OF STEGANOGRAPHY

Simmons (1984) used a scenario about two prisoners, Alice and Bob, who try to communicate secret messages without being seen by their warden, Wendy, to help people comprehend the concept of steganography. Wendy instantly cancels Alice and Bob's communication as soon as she discovers any interaction between her two hostages. The application of steganography is always depicted using this two-prisoner scenario in the setting of arbitrary countries. In particular, two sovereign nations may opt to share information without interception by another nation (i.e., the "warden"), and may rely on steganographic tactics in their everyday discussions to avoid suspicion.

**Error! Reference source not found.**3 is an illustration of an steganography based information-theoretic framework previously reported in [39], [40]. This framework comprises two major processes which are namely, embedding  $E_m(f)$  and extraction  $E'_m(f)$ .



**Figure 2.3:** The basic concepts of the steganographic system

The left side of **Error! Reference source not found.**3 shows the sender party that embedded the secret message ( $S_m$ ) in the cover object file ( $C_o$ ) and transmits the modified “stego object” (

$S_o$ ) to the recipient (Bob) on the other right. At the bottom of the figure is Wendy who aims to intercept the communicated secret messages. She keeps trying to catch the message or detect an information exchange between these two parties. Due to the obvious shared secret key ( $S_k$ ) between the transmitter and receiver, this model is designed such that only the intended recipient may extract the secret text. This shared secret key can be an extraction algorithm or certain algorithm parameters, and it is depicted as a "stego key."

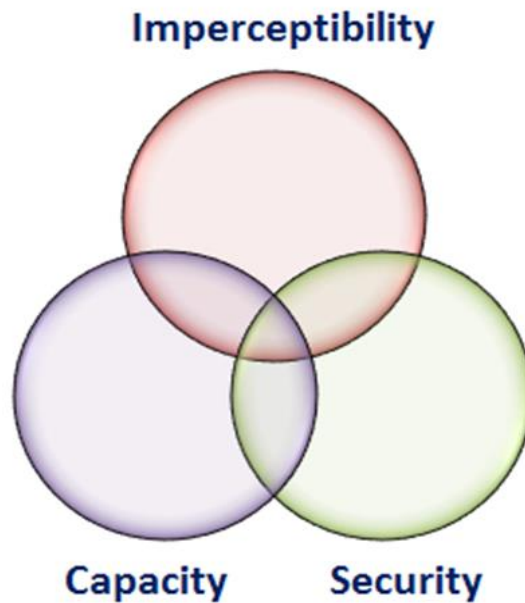
The image steganography method can be mathematically defined as a quintuple  $\vartheta = (C_o, S_m, S_k)$  where ( $C_o$ ) represents the set of cover object for the communication,  $S_m$  represents the set of embeddable secret messages that must be propagated using covers, and  $S_k$  represents a stego key derived from a set key. A steganographic system is formed by two functions, namely, the embedding function  $E : C_o \times S_m \times S_k \rightarrow S_o$  and the extraction function  $D: (E(C_o \times S_m \times S_k)) = S_k$  [41].

The secret message  $S_m$ , which contains secret data, needs a sort of camouflage. The cover object  $C_o$  is the media that hide the secret message inside their bodies. The block ( $E$ ) represents the steps involved in creating the stego-object  $S_o$  by embedding the secret data inside the encrypted cover using  $S_k$ . The stego object  $S_o$  is a combination of  $C_o$  that houses the secret message. The block ( $D$ ) refers to the process of decoding the hidden data from the stego file.  $S_k$  is the stego key that represents the element that governs the procedures of embedding the message inside the cover and extracting it from the stego object.

Steganography simply refers to the activity of hiding confidential information within other object  $C_o$  to produce a stego object  $S_o$  by using a stego key  $S_k$  at the end of the transmission. Steganography may also be utilized by the recipient for the extraction of the hidden message  $S_m$ . **Error! Reference source not found.**3 illustrate the basic concepts of the steganographic system in its entirety.

## 2.5 PROPERTIES OF STEGANOGRAPHY

Every steganography system is evaluated for performance based on its security, robustness, capacity and imperceptibility. For the same reason, in this proposed study, we will solve the problem regarding these issues (Xue, *et al.* 2019). **Error! Reference source not found.** illustrates the three essential properties for designing a steganographic system, which will be discussed in the following subsections.



**Figure 2.4:** Key issues of steganography system

### 2.5.1 Imperceptibility

Since the Human Visual System (HVS) or Human Audio System (HAS) could be invisible, no noticeable distortion should be left if humans are unable to distinguish between carriers carrying secret messages or not. Gutub and Al-Shaarani, 2020; Al-Dmour and Alani, 2016). PSNR, which is computed after the embedding procedure as a way of comparing the original and stego images, is used to determine the quality of any image. If the PSNR computation yields a result

equal to or more than 30 db, the process of embedding data is regarded as undetectable to HVS (Al-tamimi & Alqobaty, 2015) The following equations can be used to determine PSNR.

$$\text{PSNR} = 10 \log_{10} \frac{(255)^2}{\text{MSE}} \quad (2.1)$$

Where, MSE is the mean square error that is computed as follows:

$$\text{MSE} = \frac{1}{mn} \sum_{i=1}^m \sum_{j=1}^n (x_{ij} - y_{ij})^2 \quad (2.2)$$

where,  $m$  and  $n$  are the sizes of the image while  $x$  is the cover image and  $y$  is the stego image.

### 2.5.2 Robustness

In the secure embedded algorithm, the embedded secret message cannot be retracted following a reliable detection by the target attacks based on the complete awareness of the embedded framework (except knowing the secret key), [9], [42]. The following is the list of different known approaches to the practical steganalysis.

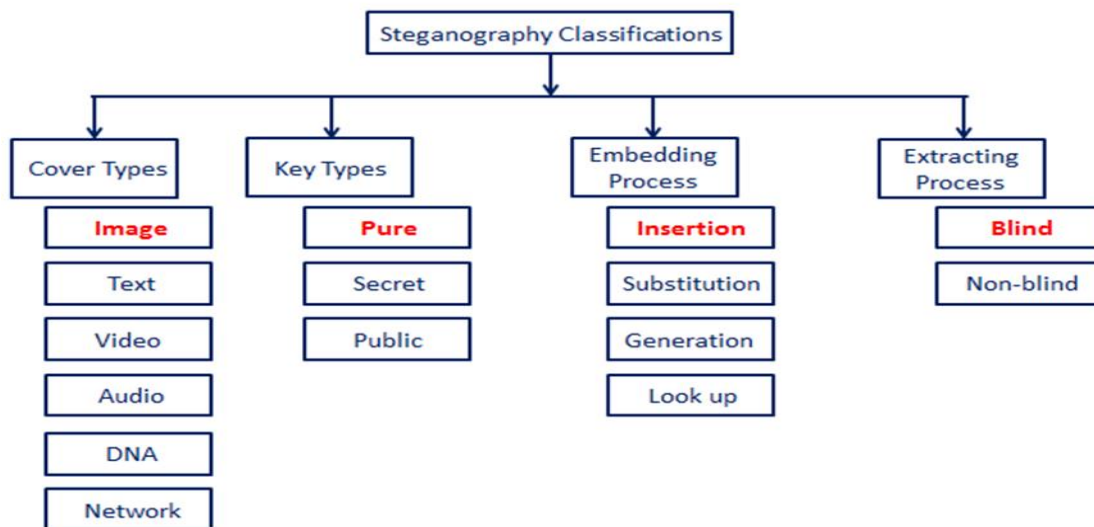
- a) Visual detection.
- b) First order statistics-based detection (histogram analysis).
- c) Image spatial correlation based dual statistics methods.
- d) Higher-order statistics (RS Steganalysis).
- e) Universal blinded detection schemes.
- f) JPEG compatibility steganalysis.
- g) Some other special cases

### 2.5.3 Payload Capacity

Payload capacity is the volume of embeddable data within a cover media compared to the size of this cover [4]. There is a trade-off between the size of the embedded secret and the cover signal distortion [43]. The techniques for data embedding process are either with high embedding rate or with high resistance with the modification, but not all of them. If one theme is increased, the other will decrease [44]. The bitplane tool technique uses LSB insertion and noise manipulation. These steganography approaches are commonly used and are easy to apply for images or audio. The LSB substitution mechanism is used for embedding data with high payload while keeping the high imperceptibility of the stego-object.

## 2.6 CLASSIFICATION OF STEGANOGRAPHY

This section presents the different classifications of steganography. This classification may be reliant on the type of utilized cover object, the stego key used for hiding and extracting hidden messages, the embedding approach, and the extracting approach [45], [46] as shown in Figure 2.5.



**Figure 2.5:** A comprehensive Classification of steganography

As shown in Figure 2.5, this study selects the image file as a cover and embed the secret data using a stego key . The different classifications of steganography are described in subsections until 2.6.4.

### **2.6.1 Classification- Based Cover Medium Types**

The definition of the cover file or the container of the concealed information or secret message is the first point to be clarified in this paragraph. The features of the carrier file or some of its portions can be edited, modified, or manipulated to conceal secret information. The alterations that occur throughout the embedding process, on the other hand, must remain undiscovered by everyone save the intended message recipients. As a result, after concealing the secret data, the format or visual aspect of the carrier files must be preserved.

As a result, secret data can be incorporated in a variety of cover medium. These characteristics nevertheless dictate how secret material is contained in the digital description of cover files, even though the qualities of cover files may differ due to inconsistency in the digital representation and the distinctive cover file structure. In order to accomplish this, the cover (carrier) image is a crucial part of the steganographic system. As shown in figure 2.5, the file types of the cover object can be categorized as text, video, image, audio, or protocol files (Amirtharaj & Rayappan, 2013). The following sections explain various steganographic procedures based on cover media types.

#### **a) Text-based steganography**

In this form of steganography, the cover medium used is text file; it is among the most problematic steganography methods [47], [48] since text files lack the required redundant data to hide the message [49], [50]. This technique is also facing the problem of susceptibility to interception by a third party which can be achieved by just replacing or reformatting the text file itself into another form (such as .txt to .pdf). Over the years, several text-based steganography methods have been proposed, such as open spaces, line shift, word shift, and semantic.

However, text-based steganography remains a commonly used technique due to various motivations. Among these motivation is the fact that the secret message can easily bypass the

attention of attackers by encoding the secret message within an email message or Internet article. Detection may also be prevented by classifying the text as a spam message. Artificial messages may be produced via propagation steganography and such messages are similar to spam messages; hence, they merely receive attention due to their frequent occurrence. Being that the “mimic algorithm” or “mimicry,” can be used for artificial spam messages generation, it has been classified as a propagation steganographic technique. Such texts may be linguistically wrong and could deceive spam filters statistically. Mimic texts, upon investigation, can easily be detected by humans while retaining the basic features of spam messages.

#### **b) Image-based steganography (IBS)**

As the name implies, IBS relies on images as cover object; IBS techniques are the most commonly utilized because they take use of the human visual system's limited capability (HVS) (Mohamed & Mohamed 2016; Sheelu 2013). The considerable volume of repeated information in messages helps to hide confidential data (Subhedar & Mankar 2014; Banerjee et al. 2011). The information that can be encoded using the pixels present in an image is diverse and unintelligible to the stego key, which could be an algorithm. The data might easily escape detection by the human eye due to the intricacy of these pixels.

#### **c) Audio-based steganography**

Here, the cover object used during steganographic processes is audio files [52]. The embedded messages in the audio-based steganographic techniques cannot be easily intercepted by intruders as they are hidden in a manner that made them imperceptible to the human ear (Kaur & Mahajan 2016; Thorat & Kharat 2015; Bheda et al. 2013). It may be hard for some people to listen to tones that immediately follows a louder tone; hence, the secret data may be concealed using such barely audible noises to overcome audio compression and to keep it from the human hearing system. Secret data can also be hidden in faint echo to delay their interception. Audio files for audio steganography can come in different formats, such as .wav, .midi, and .avi (Das & Bandyopadhyay 2015). There are other available audio-based steganography techniques in the literature, such as LSB, parity, phase coding, echo hiding, and spread spectrum [56].

#### **d) Video-based steganography**

Videos are used as cover media in video-based steganography. Because videos are simply a series of images displayed at a fixed frame rate, they can conceal information in the same way that photos can. When embedding data within images in a video, the discrete cosine transform alters the values (such as 8.667 to 9) that are used. This method usually results in information that is unnoticeable to the HVS. Video based steganography use files in .mp4, H.264, .avi, and .mpeg formats (Das & Bandyopadhyay 2015; Hussain & Hussain 2013).

#### **e) Protocol-based steganography**

Here, the carriers used during steganography is network protocols. Typical protocols used include UDP, ICMP, TCP, and IP. In some hidden channels within OSI network layer models, steganography is applied in the unused header bits within the IP and TCP domains (Kaur & Rani 2016; Das & Bandyopadhyay 2015).

#### **f) DNA based steganography**

This approach employs the randomness characteristics in DNA for secret data embedment; a recent technique used the numerical mapping table for DNA sequence mapping during secret data embedment [59].

### **2.6.2 Classification –Based Key Types**

Three types of steganographic protocols were identified in (Rafat & Sher 2013; Dunbar 2002); these are pure, secret key, and public key steganography.

#### **a) Pure steganography**

Here, the system requires no stego key as a cipher; hence, it provides minimal security due to the reliance of the transmitter and receiver solely on presumptions and random guessing about the pattern of behavior of each other to decode the message. Such message may be restricted from sharing on social platforms or over the Internet.

#### **b) Secret key steganography**



Here, the system works with a stego key; cover images are used in this technique and the stego key is kept hidden. Only parties that have the private key can decipher the message. Being that secret key steganography relies heavily on the stego keys, attackers can notice and react to the message with ease but despite this limitation, the message can only be extracted by parties with the secret key.

### **c) Public key steganography**

This form of steganography exploits the concept of public key cryptography; it utilizes both public and private keys to propagate hidden messages. The message sender may encode the message using the public key and provide the receiver with the private key to decode the message. Therefore, this may not be a secure approach for steganographic systems since several studies have focused on public key cryptography and several levels of security have been employed to address the concerns of parties that are not participating in the communication. But as soon as the attackers are aware of the communication and are alerted to this steganographic technique, they may strive to crack the framework that holds the public key in order to intercept the hidden message.

## **2.6.3 Classification- Based Embedding-Techniques**

Three techniques for hiding information within cover media have been proposed in the literature, including substitution-based, insertion-based, & generation-based methods techniques (Baawi et al. 2017; Rafat & Sher 2013; Odeh et al. 2012; Cole 2003).

### **a) Insertion-based technique**

In this technique, the areas to be ignored by the processing application are designated in the cover media; the processing technique can read the cover file and choose appropriate areas within the media for embedding hidden messages. Given that this technique adds secret messages within cover files, one advantage of the insertion-based technique is preserving the original contents of the cover media. However, as one of its major limitations, there may be suspicion due to the large stego file size.

Therefore, the algorithms' main goal is to incorporate hidden messages while avoiding raising the suspicion of attackers. A mark in either EOF or HTML may be found in most files, which is one of their embedding characteristics.

#### **b) Substitution-based technique**

The substitution-based strategy is based on using the secret message to replace a component of the carrier object in a manner that attackers cannot identify. This strategy works by replacing some information or purposefully changing the cover file in order to provide the least level of alteration to the carrier file. As a result, the stego and carrier files size become comparable. To prevent suspicion, a proper replacement technique must be used, requiring only the inconsequential components of the carrier file to be chosen and replaced.

#### **c) Generation-based technique**

The generation-based strategy does not rely on the use of any cover file as it relies on the use of a generation engine that takes the secret bit as an input to build a file that seems regular and can be displayed in graphics, text, or music format.

### **2.6.4 Classification- Based Extraction Function**

Another classification of steganographic systems is based on whether the original media is by the extraction process or not; on this note, they are classified into blind and non-blind schemes, respectively. However, this classification is not receiving much attention in steganographic literature [39].

#### **a) Blind Steganographic Scheme**

In these steganographic systems, it is assumed that the use of cover medium is not important for the recipient to extract the information. Hence, the original cover media is not required during the extraction process and the hidden information can be extracted from the stego media [64]. Consequently, it gives Alice the opportunity to utilize any cover object even when it may not be accessible to Bob.

## **b) Non-blind Steganographic Scheme**

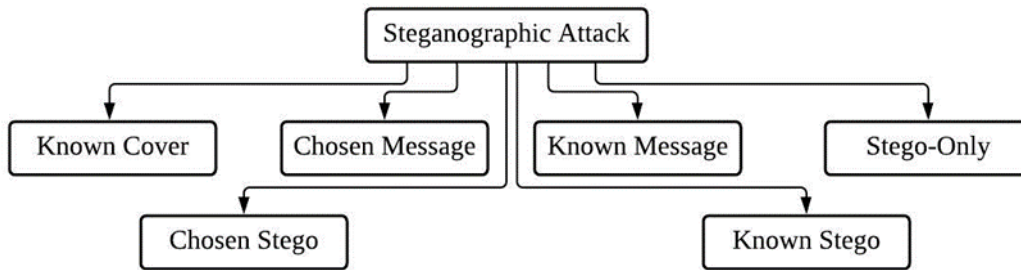
Here, the original cover medium must be available during the extraction process as the hidden content cannot be retrieved without it. Unfortunately, although having possible practical applications, this steganographic system has not caught the attention of steganographers. For instance, the informed extraction procedure might be beneficial in embedding the secret data in a less stressful way if Alice and Bob choose to use the same set of images. Hence, the detection probability would be reduced compared to blind embedding techniques [65].

## **2.7 STEGANALYSIS AND STEGANOGRAPHY ATTACKS**

Steganalysis is the process of identifying whether a media file contains a concealed message, retrieving that message, and analyzing its content. The comparison between cryptanalysis and steganography is established by using the paths taken when disabling cryptographic systems. Cryptanalysis is contemplated useful for cryptographic protocols even when the encrypted message is uncovered by unwanted persons [66]. An additional necessity is appended by steganography that attests the undetectability of the secret message by adverse individuals. Otherwise, adverse persons are also unaware of the actuality of the message. Therefore, steganalysis is truly useful during the compromisations of the invisibility of the secret message ( Arya and Tiwari, 2019).

### **2.7.1 Types of Steganographic Attacks**

Varieties of steganography attacks exist including the stego-only, known message, known cover, chosen message, chosen stego, and known stego. Steganographic procedures have probability of being categorized regarding the tools that unwanted persons may utilize to analyze the steganography image. These kinds of attacks used by the steganalysis are described in the upcoming subsections [59], [68]. Figure 2.6 depicts the various types of steganography attacks.



**Figure 2.6:** Types of steganography attacks

**a) Stego-Only Attacks**

Here, the stego file is solely available for the analysis, while both the stego file and hidden information are vulnerable to attacks [69].

**b) Known Cover Attacks**

Here, the actual cover file is contrasted with the stego file that facilitates the determination of pattern variabilities. Both the actual image and the image that contains the hidden details are obtainable and have the possibility of comparison [70].

**c) Known Message Attacks**

The known message attacks analyze the known patterns related to the secret data and may help to prevent future attacks. Even with the message, these types of attacks may be complicated to address and may even be considered similar to the stego-only attacks [70].

**d) Chosen Stego Attacks**

In the chosen stego attacks, the steganography algorithm (tool) may be a software, stego file, or other similar details [71].

### e) Chosen Message Attacks

Here, a stego file is initiated by the steganalyst from some steganography devices of a specified message. This attack is aimed at examining the comparable samples in the stego file with the chance of pointing toward the usage of certain steganography instruments or algorithms [71].

### f) Known Stego Attack

In known stego attacks, the algorithm (steganography tool) is familiar or the actual stego & cover file are both handy. The attacker may analyze the steganography image by performing these attacks [72]. Table 2.1 summarizes the potential tools that a steganalyst (attacker) may use in certain situations. Table 2.1. illustrates a summary of steganographic attacks.

**Table 2.1:** Summary of steganographic attacks

Type of Attacks	Stego File	Original Cover File	Hidden Message	Stego Tool or Algorithm
Stego only	Yes			
Known cover	Yes	Yes		
Known message	Yes		Yes	
Chosen stego	Yes			Yes
Chosen message	Yes	(see clarification)		
Known stego	Yes	Yes		Yes

## 2.8 LITERATURE REVIEW

The issue of lack of trust, and the need for secret communication, have driven the development of effective embedding approaches to protect the vital data that may be hacked during communication. Embedding methods in image steganography systems can be classified into

three depending on the image nature and hosting locations; these methods are adaptive domain, frequency domain, and spatial domain.

### **2.8.1 Spatial or map domain**

Here, pixels intensity is utilized for the embedment of the secret message. This type of embedding has many advantages for embedding; for instance, it increases the capacity (no limitation), reduces complexity, therefore, imperceptibility of the hidden message is ensured [73]. The disadvantage of this class is lacking in statistical analysis techniques. In the literature, various studies to the spatial domain have been appeared, and some of them are listed below:

Most of the steganography systems use the LSB substitution for the secret message embedding. Huang et al. (2018) developed a new LSB substitution-based system for the message embedding via the “Optimal Pixels Adjustment Process (OPAP).” The main aim was to improve the quality of the stego image containing the secret data and minimize the computational complexity wherein four LSB bits were changed to hide the information. The achieved PSNR value was 51 dB. Another method based on the adaptive LSB substitution steganography was suggested [75]. In this method, the image was partitioned into two parts- sensitive and non-sensitive parts following texture analysis. Majority of the bits in the non-sensitive area were used for bearing the secret message and other bits in the sensitive area. The main supremacy of this procedure was to achieve greater payload magnitude with imperceptibility. Yang (2008) introduced a new LSB-based steganography method for embedding the secret message by normal LSB bit position in the cover image. Inversion of the pixels before embedding was the main contribution of this method which achieved high capacity and PSNR. Recently, a robust color image LSB steganography method based on the enhanced 1D chaotic map was presented by Pak et al. (2020). The proposed study confirmed a high accuracy and better performance than the standard LSB embedding. The results revealed an improved robustness against statistical analysis attacks. The existing methods based on the LSB are simple due to the variation of the LSB bits of the pixels, but they lack capacity and security.

Another study has used Expansion Steganography (DE), this technique is used to solve and enhance the problem of the reversible difference of expansion method. Herein, one-layer

embedding represented by the location is used to solve the embedding method in the cover image. A new DE embedding method was suggested [77] to solve the problem erased by the simplified location and interpolation. This scheme produced good stego image when the bilinear interpolation was used for the embedding inside the image. It achieved good imperceptibility with improved capacity. Meanwhile, a new prediction method was proposed [31] for reversing the secret message embedding. In this scheme, the partial difference equation (PDE) was used to predict the error expansion of the cover image. In the original image, four pixels were in different directions with their gradient. For the next step, the weight was calculated from each iteration magnitude to achieve good prediction. This method was found to be better than the other pixel selection methods used to embed the secret message. Later, Mukherjee & Jana (2019) used the difference expansion (DE) to present a new reversible data embedding technique where the cover image was first divided into  $3 \times 3$ -pixel blocks before classifying the pixels as Type-one and Type-two based on their coordinate values. The associated pixels were then identified by determining the median & correlation coefficients of Type-one pixels. The secret bits were finally hidden in the Type-two pixels based on the correlated pixels and in Type-one pixels based on stego Type-two pixels.

Another spatial domain- based image steganography called Color Model-based Steganography (CMS), this method uses the correlation of gaps in the colors for the embedding. For instance, any change in the RGB channels influences the entire stego image quality, reducing the convenience of the steganography algorithms ambiguously. Numerous color spaces that are used for the embedding include the RGB, YCbCr, HIS [19], [78]. Muhammad et al. (2018) recommended that an adaptive LSB substitution method that uses the uncorrelated color space can enhance the imperceptibility in an evasive way concurrently keeping the possibility of the detection by the human visual senses to a minimal. This method first scrambled the host-image to generate an encrypted image, which was later transformed into the HSV color space. Next, it used the ALSB technique to hide the secret data within the V-plane of the HSV color model. An original unique magic LSB substitution technique (M-LSB-SM) was suggested by (Muhammad et al., 2016) for RGB images. This system applied an achromatic component (I plane) that involved the HSI color model alongside multi-level encryption for the embedment

process. This method achieved more enhanced visual quality and offered different levels of security compared to other existing techniques.

In the Spread Spectrum Steganography, the embedding selection is performed differently; a wide frequency range is taken over the signal in the communication bandwidth. To narrow band is modulated using the new pixel frequency modulation spreads as white noise. The narrowband signal energy decreases as the noise spreads across the frequency. In this scenario, the embedding behaves like the Gaussian noise on the image, making the signal easier to identify. The embedding is successful since the low frequency noise distortion cannot be seen with the naked eye. The multiplicative spreading for data hiding was recommended by Eze et al. (2019) in order to estimate the inaccuracy in the capacity & security channel. But considering the host signal's involvement, this method gained credibility with the watermark as opposed to frequency-based steganography.

### 2.8.2 Frequency domain

In this regard, the given image will be changed into frequency class (domain) prior to the embedment of the secret data in the coefficient factors. The benefit of using frequency domain is robustness against statistical attacks but in other hand, it suffers from very low capacity. In literature, spatial domain is widely used because of its simplicity and more efficiency (Gupta, *et al.*, 2019; Prasad and Pal, 2019). In the literature, various methods to the frequency domain have been developed, and some of them are listed below:

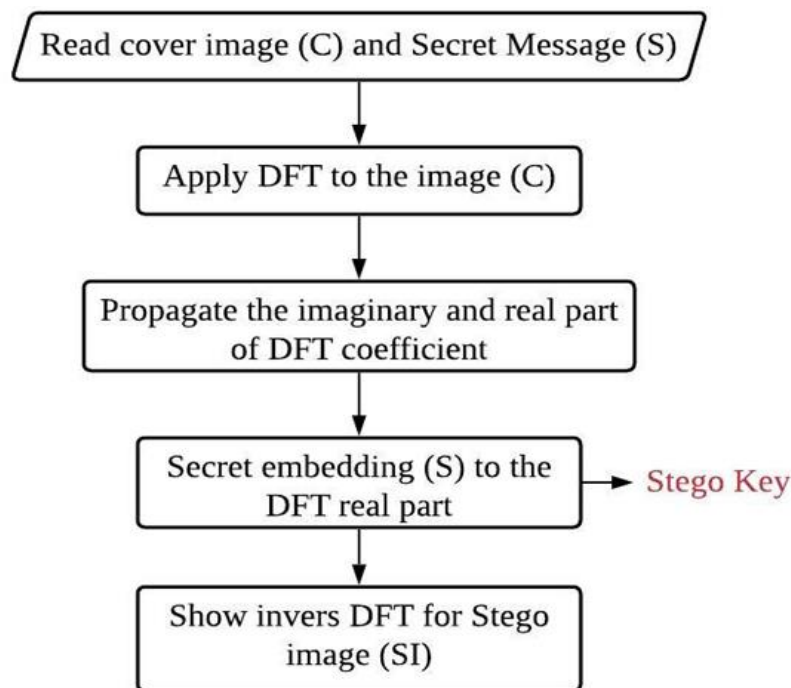
When dealing with the intensity estimates of the pixels in the cover image, meaning the frequency components, the Discrete Fourier Transform (DFT)-based steganography is commonly used. Let,  $F(x, y)$  represents the original image with size  $M \times N$ , the DFT of this image can be represented as:

$$F(u, v) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y) e^{-j2\pi(\frac{ux}{M} + \frac{vY}{N})} \quad (2.3)$$

where  $u$  and  $v$  are ranged from 0 to  $M-1$  and 0 to  $N-1$ , respectively.



The original image must be reconstructed during the conversion from the image after embedding which is performed by the inverse discrete Fourier transform (IDFT) for retrieving the pixels value from the transformed image. Five steps are involved to represent the DFT algorithm. First, the cover image (C) is taken, and the secret data (S) is read. Second, the DFT is implemented on the cover image (C). Then, the real part is split from the given coefficients DFT. Next, the secret embedding bits to the Real space of the DFT is performed. Lastly, the inverse DFT is performed to receive the stego image (C') as seen in Figure 2.7. For the extraction, just the invert the procedure of the embedding from the bottom up is followed.



**Figure 2.7:** DFT-based embedding of 3 secret message

Rathor and Sengupta (2020) proposed a novel N-point DFT study using the high-level transformation; this method is based on crypto-steganography and structural obfuscation. The suggested scheme integrated approaches to get a high robust secured N-point DFT application-specific processor. This design achieved about 75.28 % obfuscation at the gate level structure and 99.5 % security enhancement which were higher respecting the key size compared to the existing state of art hardware steganography approach. Mandal (2020) introduced a discrete Fourier transform (DFT)-based steganography process where the generalized DFT and IDFT

equation pair was used. The sub-image-based (small non-overlapping window) reversible computations were performed using the DFT and IDFT. Practical examples for both 1D and 2D DFT and IDFT transform computation were considered to confirm the reversibility. The LSB encoding on  $8 \times 4$  sub-image was provided completely with the flow diagram. The entire algorithm of DFT-based steganography was developed with the embedding payload (EP) capacity of 0.75 bpp together with a very high PSNR value. In addition, a Fractional Fourier Transform (FRFT) technique was suggested [83]. This method transferred the cover image by FRFT with  $\alpha=0.78$  and  $\beta=0.25$  which attained improved PSNR and security.

The “Discrete Cosine Transform (DCT)-based Steganography” is the studies have been appeared in the frequency domain. The steganography system based on the 2D DCT can be defined as:

$$B_{p,q} = a_p a_q \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} A_{m,n} \cos \frac{\pi(2m+1)p}{2M} \cos \frac{\pi(2n+1)q}{2N} \quad (2.4)$$

where  $A_{m,n}$  represent the image of size  $M \times N$ , and  $B_{p,q}$  represent the coefficient transform.

The extraction process follows the 2D inverse DCT written as:

$$A_{m,n} = \sum_{p=0}^{M-1} \sum_{q=0}^{N-1} a_p a_q B_{p,q} \cos \frac{\pi(2m+1)p}{2M} \cos \frac{\pi(2n+1)q}{2N} \quad (2.5)$$

The 2D DCT is performed in 6 major steps described as follows:

**Step one:** Partitioning of a cover image into sub-image ( $8 \times 8$ ) blocks assigned as  $(B_i)$ , where  $i$  is the  $i^{th}$  of blocks.

**Step two:** Apply 2D\_DCT in each block or sub-image to find the coefficients of DCT (in this case, will get one DC for each block and 63 of AC).

**Step three:** Use the  $(u1, v1)$  with  $(u2, v2)$  to generate the stego key.

**Step four:** Read ( $m_i$ ) as a secret bit of the  $i^{th}$  bits.

**Step five:** Get the original sub-image or block by applying the inverse DCT.

**Step six:** Get the stego image by repeating the above steps for all blocks in the image.

In the receiver side (extracting process), the same steps are followed in embedding the secret message but in the reverse order. Many researchers applied and modified the DCT algorithm to find the goals of the steganography systems. A new method was suggested by [84] that depended on the reversible data embedded using partitioning of cover image into two sections low and high frequency of the components. The embedding was performed in the high frequency section because the low frequency region was more sensitive to the change. In addition, the integer mapping was used to implement the 2D-DCT. During the shifting of the histogram, it looked for the appropriate location for the embedding. The shifting procedure occurred on both side (right and left) and continued until the empty space that was used for the embedding was located. This method achieved the capacity of 170992 bits and PSNR of around 36.80 dB. Substantial improvement was achieved by the DCT method in comparison to other steganography approaches.

Song, Wang, and Niu (2012) introduced a method that consisted of the combination between the DCT-based steganography and affine transformation which achieved good results because the integer of the DCT steganography was less invertible. The Laplacian shape spreading was used to transform the integer DCT. For any statistical attack, this method was considered more robust than others. Integer Wavelet Transform (IWT) with DCT steganography was suggested by Arunkumar et al. (2019) where two steps were used for the embedding including the DCT for the secret message preparation and IWT for the image preparation. Then, Munker's assignment algorithm was used to perform the complete embedding. Shyla and Kumar (2019) suggested a novel DCT-based steganography system for color images. This technique used DCT for cover image by modulating the coefficients produced in the DCT. The first step (pre-processing stage) encrypted the secret message and then embedded the secret message encrypted into the DCT coefficient's part. Due to the use of the frequency coefficient, this method achieved better PSNR. A new algorithm for steganography system called zero-steganography was

presented [88] by applying the low pass filter with noise reduction in the JPEG compression image. This method achieved good imperceptibility and robustness against three kinds of attacks.

### **2.8.3 Adaptive domain**

While revisiting the contributions of image steganography techniques, they fail to overtake the impact of the adaptive techniques. It is an instance when spatial and transformations approaches are used. The phrase "adaptive steganography" is also used to describe “modeling”, “statistics-aware embedding”, and “masking” [4], [5]. This section reviews a number of earlier steganography studies. Data embedding techniques can incorporate the adaptive nature in a variety of ways, including by choosing the target pixels in the cover image, the type of adjustment to be made, the number of bits embedded in a pixel, and more. These systems can be divided into four categories based (Region-, HVS-, Machine Learning (ML), and Artificial Intelligence (AI)-based steganography) on the kind and manner of adaptability they provide. The significant features of each of these techniques are described below. Different methods to the adaptive domain have been developed, and some of them are listed below:

The SVM-based steganography is a supervised learning scheme used mainly in image watermarking as a classifier in both transform and spatial domains [89]. Shankar and Upadhyay (2020) used SVM for the optimization of the steganography-based procedures. It was suitable for establishing the embedded points having greater reliability, imperceptibility, and less extraction error with very speedy execution [91]. It was mostly utilized for identifying the less sensitive regions (for human eyes) in the image avenues. Commonly, this procedure is used in a blue avenue in the RGB color identity and luminance avenue in various color setups (Qader and AITamimi 2017). Several elements such as the chrome value shifts, average pixel intensity, and localization of the edge details was injected to reach the resolution. Depending on the elements and categorization requirements, various kernels were utilized for the expansion of the factor details to a greater element location. Some of the kernels for achieving this target are the polynomial function, radial basis function (RBF), and quadratic function [93].

The FL-based techniques rely on the visual quality preservation to increase the undetectability of the stego media at the expense of the modeling complexity. Intensive studies have been made on the FL-based steganography techniques. Sajasi and Moghadam (2013) developed a “Fuzzy Inference System (FIS) with HVS” to solve the problems related to the texture, local statistical, and brightness information-based feature vectors. It used these elements from the cover identity sub-areas and further explained the semantic regulations necessary for the embedding process. This notion helps in reducing stego image distortion even at the greater embedding rates. A different fuzzy-based study is suggested by Alvi and Dawes (2013). In this procedure, the cover pixel determination relies on fuzzy pixel classification and a secret message undergoes conversion to a mode of fuzzy details prior to the actual embedding procedure. Another watermarking procedure based on fuzzy logic was presented by Kiani and Moghaddam (2009). In addition, it utilized the FL means clustering algorithm based on the transform domain derivative features in various angles. It was shown that the FL can enhance the steganography procedures in various aspects more so during the appearance of vague and/or ambiguous image textures. It favored the arrangement through the recognition of the preferred image patterns faster through the reduction of unnecessary complexities. The outcome is assistance in practical implementations through the suitable imperceptibility.

## **2.9 RESEARCH DIRECTIONS**

In recent times, the major problems of image steganographic systems are related to the hiding of the secret data inside a carrier with high security, high payload, minimum detectability, and robustness against detection attacks. Over the decades, despite dedicated research efforts these requirements concerning any steganography system remain unaccomplished. The strong correlation among various characteristics of the steganography systems is responsible for such failure wherein the overall effectiveness or performance of the scheme degrades at the cost of the improvement of certain properties. Thus, a practical solution is mandatory to resolve all these issues simultaneously. It is realized that the performance of the existing information steganography systems can further be improved by integrating various important concepts related to the information hiding, thereby contributing towards the narrowing of the research gaps as listed hereunder:

1. Due to the existence of an intrinsic balance between the imperceptibility and capacity, all the developed steganographic systems up till now used a less capacity to improve the PSNR (a measure of the imperceptibility).
2. Majority of the proposed steganography systems focused on the quality metrics such as the PSNR and SSIM, leaving the security measure. In fact, the simple image partitioning that was used in the hiding process did not satisfy the security requirement. Consequently, the stego image transmission through the internet network was threatened by the  $\chi^2$  or histogram attack.
3. Imperceptibility, being one of the main determinants in steganographic systems, has its benchmarking process based on the PSNR equation that matches the original and stego images. Recent studies indicated that such metric is rather inaccurate and needs to be substantiated through some other quality metric including the SSIM, NCC and FOBP.
4. The benchmarking process in the steganography is essential for the secure information transmission. Yet, the clear benchmarking process for the medical image steganography, revisable steganography, fragile steganography, and so forth have been lacking.
5. So far, the random or selective attacks that were used by the developers to expose the steganography systems for the performance evaluation and benchmarking appear baseless. These studies seem to have no obvious rationale for the selection of the attacks for testing the robustness of the data hiding schemes. In addition, the clear evidence related to the survival of the developed approaches against other types of attacks remain deficient.
6. To achieve the robust steganography systems, some studies used the genetic algorithms (GAs). Nevertheless, these algorithms are weak against the statistical attacks because a single randomized stage is used to effectively hide the information.
7. Earlier, the researchers mostly focused on the spacial domain-based method wherein the LSB technique was exploited for the embedding process due to its reliability and flexibility. However, the LSB technique has limitation in terms of the security. To improve the security, some studies were conducted on the frequency domain where encouraging results were

obtained using the DCT and DWT. Despite its better security performance, the frequency domain technique suffers from the low imperceptibility and capacity.

8. To reduce the amount of the secret data and improve the security before embedding a secret message, most of the established steganography systems utilized the known compression and encryption techniques. Accordingly, all these approaches can be recognized by the steganalysis tools and statistical attacks.

## **2.10 RELATED WORKS OF IMAGE STEGANOGRAPHY SYSTEMS**

Various image steganography approaches have been introduced throughout the decades with the purpose of protecting data transfer over the Internet, which are summarized in this section. Additionally, the key characteristics of the comprehensive image steganography methods are discussed. As mentioned earlier, the digital image steganography systems have been divided into a spatial, frequency and adaptive domains. Several recent studies related to the steganography in terms of the capacity and the corresponding PSNR are listed in Table 2.2 (between the years 2015 to 2020).

**Table 2.2:** A study analysis of the related literature study (between the years 2015 to 2020)

References	Method	Remarks	Performance
(Rajendran and Doraipandian, 2017)	LSB: CM The proposed study used LSB method based on chaotic map; the chaotic map was used to generate the 1-D logistic map; the embedment of the secret text was based on the generated sequence.	- Low payload capacity. - The system's robustness is suspect since the secret bits are scrambled when it is subjected to loss compression or geometrical attacks.	44.53 dB 2 BPP
(Savithri, Mane, and Banu, 2017)	DCT: Two parallel approaches are proposed: (2D-DCT with RSA) and (2D-DCT with chaotic). The secret bit was encrypted into a set of homogenous pixels before incorporation into the DCT coefficient of the provided original image.	-Low capability. -Low image visual quality - inconclusive robustness against the dynamic attacks	0.5 BPP 25 dB
[99]	LSB-ANN: The proposed method made use of LSB-based ANN and a chaotic edge. First, employing ANN to detect the edge of the original image, then, the hidden data is randomly embedded based key chaotic map.	-Limited EP in the edge region. _ The researchers didn't test the presented scheme against different attacks.	54.5 dB 2.0 BPP
(Nyeem, 2018)	Bit plane + Histogram The separation of the pixel intensity values into two groups was based on the bit-plane values; histogram-shifting based embedding was applied to each histogram bin individually.	-Lack of Defense against an intruder (statistical) attack	40 dB 5.0 BPP (High EP)



**Table 2.2:** A study analysis of the related literature study (between the years 2015 to 2020)

“Tables continued”

References	Method	Remarks	Performance
[101]	DWT: A DWT-based image steganographic system was proposed in which the secret bit is embedded using 3 details coefficients (horizontal, vertical, and diagonal). Distortions in the stego image were eliminated using a secret key computation. A blocking notion is also employed to preserve the cover image's imperceptibility. The embedding procedure involves the use of a matching block between the original and stego image.	- Unsatisfied image visual quality - Low security.	2 BPP 45 dB
[102]	LWT with ANN: -The original image is decomposed into 3-levels of LWT prior to randomization into 2*2 non-overlapping blocks. The next step is the insertion of encrypted binary data within the LWT coefficient component.	-Lack of robustness against compression and rotation - Very low payload capacity	43.8 dB 512 bits
[3]	PVD- MF ISS based on PVD and modulus function was proposed for the enhancement of PSNR and payload.	-Low embedding capacity -Less visual quality	42.04 dB 1.5 BPP

**Table 2.2:** A study analysis of the related literature study (between the years 2015 to 2020)

“Tables continued”

References	Method	Remarks	Performance
[103]	Adaptive QW: The presented system used inverse wavelet transform along and Genetic algorithm (GA).	-Lack of security -Lack robustness against filtering and scaling. - Chi-Square, HVS attacks were missing.	46 dB 1.0 BPP
[104]	LSB: LSB based secret map methods utilizing 3D chaotic maps, specifically 3D logistic and 3D Chebyshev maps.	-Low Image visual quality - Low embedding payload capacity.	46.15 dB 1.0 BPP
(Kadhim, Premaratne, and Vial, 2020)	Edge-based image: The proposed method uses adaptive embedding over Dual-Tree (DT-CWT) subband coefficients and ML-based optimization methods.	- The researchers did evaluate their proposed system with NCC or SSIM. Also, HVS attack was missing.	53.71 dB 1.9 BPP

**Table 2.2:** A study analysis of the related literature study (between the years 2015 to 2020) “Tables continued”

References	Method	Remarks	Performance
Sahu et al. (2021)	MDPVDMF: The original image (OI) is divided into pixels with a size of 2 2. Then, data embedment is carried out by utilizing each block's vertical, horizontal, & diagonal directions. Two difference values can be obtained in any of the 3 directions for a 2 × 2-pixel block. The secret bits are then embedded using the difference values and the remainders of the pixel pair.	<ul style="list-style-type: none"> <li>- Low visual quality</li> <li>- Lack of defence against statistical attacks</li> </ul>	39.17 dB 3.10 BPP
Tang et al. (2021)	Fuzzy-based image hiding Using the characteristics of the cover image as crisp input values, a fuzzy inference system is created as a classifier that generates semantic ideas that correlate to the payload of image subclasses. Additionally, LSB substitution is utilized to adaptively conceal the data in accordance with the results of the FIS and the sensitivity of the HVS to the RGB color components.	<ul style="list-style-type: none"> <li>- The researchers did evaluate their proposed system with NCC or SSIM. Also, and HVS attack</li> </ul>	<b>61.0 dB</b> 2.0 BPP

## **2.11 SUMMARY**

This chapter discusses the primary concerns and considerations of steganographers. The statistical imperceptibility of the embedded secret bit is the most important characteristic of any steganographic system because any steganographic technique is deemed invalid when the presence of the secret bit is discovered. The reasonable capacity, simplicity of usage, and visual imperceptibility of the LSB embedding method makes it the most preferred approach in the spatial domain. The security of steganographic systems can be increased using steganalysis techniques. This could be achieved by eliminating the distortions that increase the likelihood of discovery and by defeating or decreasing those chances.

In the current study, several studies have been reviewed that rely on various methods of embedding (especially between the years 2017-2022). These methods have been used for preparing the secret message setup. These embedding methods include the spatial domain, frequency domain, and adaptive domain. This chapter is expected to provide enough evidence towards the correct selection of the research gaps, research questions, and the proposed objectives of the study.

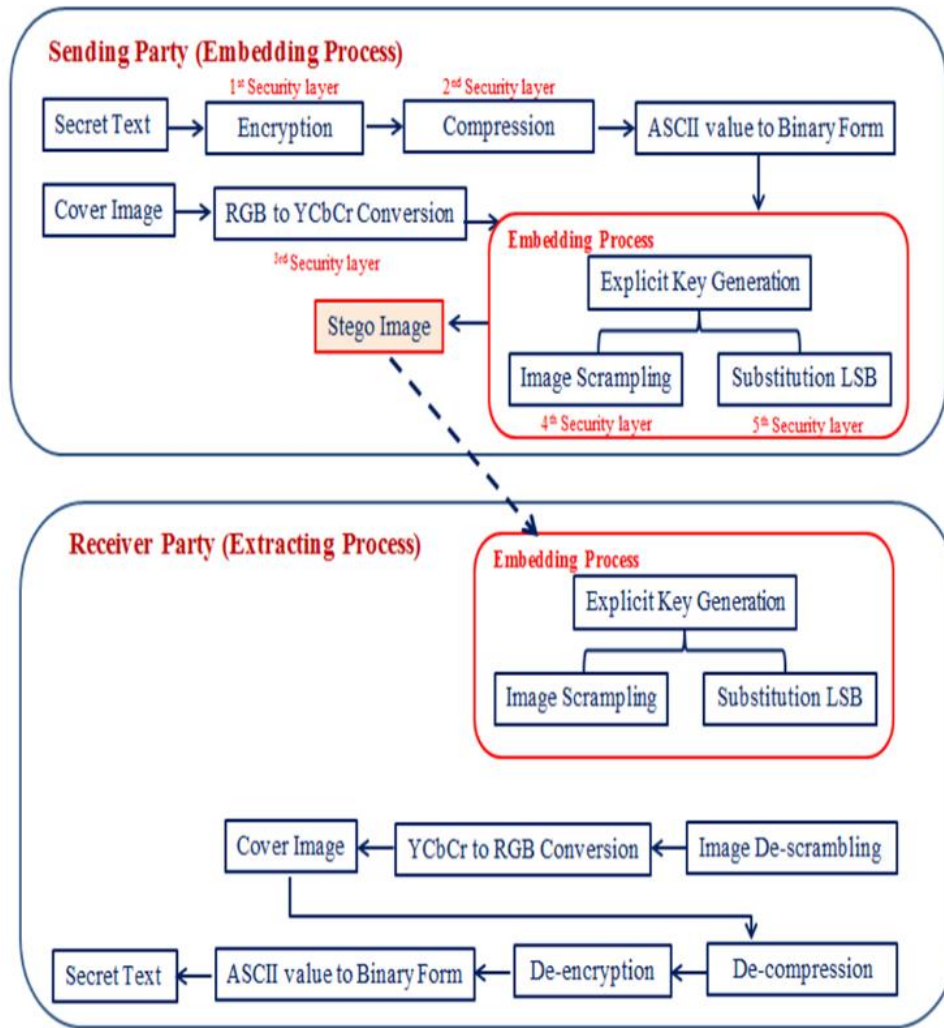
### **3. RESEARCH METHODOLOGY**

#### **3.1 INTRODUCTION**

The research problem, aim and objectives previously instigated in Chapter One and the literature on current image steganography schemes are examined in Chapter Two. This chapter discusses the methodology used by this study to achieve the intended goal. Eight sections constitute this chapter including the introduction and summary. Section 3.2 details a recap detailing the research framework. Then, the data pre-processing represented by secret text and cover image is explained in Section 3.3. After that, the embedding process is fully explained in Section 3.4. The steps involved in retrieving the secret text from the carrier is explained in section 3.5. The estimation measures are then surveyed in Section 3.5. Conclusively, Section 3.6 presents a summary of the chapter.

#### **3.2 RESEARCH FRAMEWORK**

This research aims to build a strong steganography system for hiding secret text with different payload capacities in  $512 \times 512$  imag dimensions. To achieve the desired goal, an effective framework consisting of multilayer security has been prepared; the whole steps of the proposed scheme are shown in Figure 3.1.

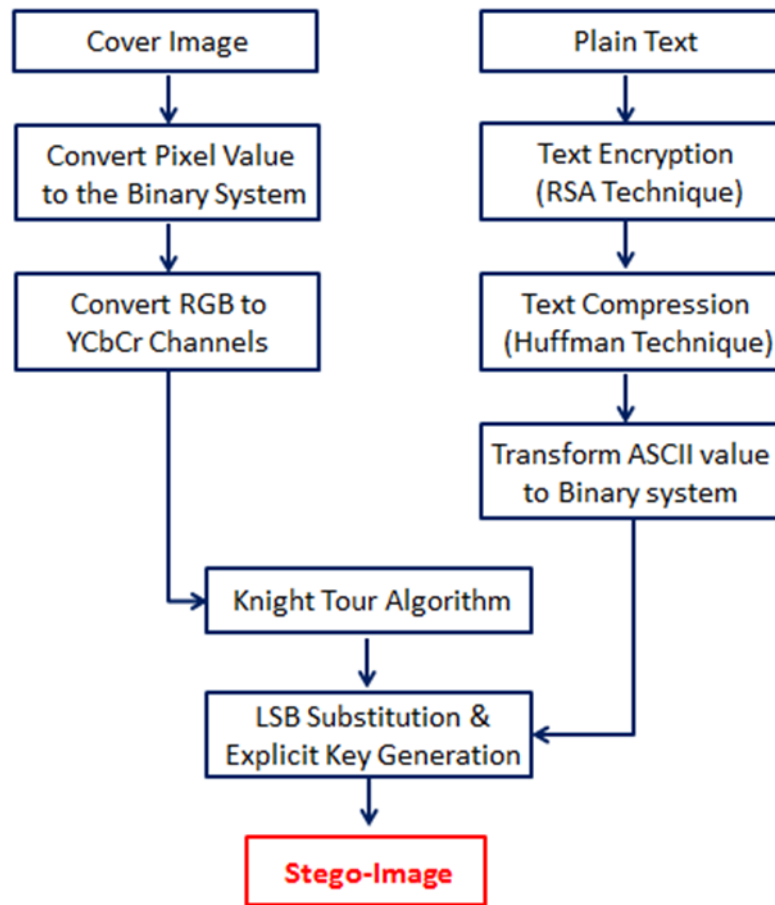


**Figure 3.1:** The schematic of the proposed scheme

There are two main functions of the proposed scheme as seen in the above figure; the sending party embeds the secret data in the carrier, and the receiving party extracts the secret data from the hosted image. The two functions are explained in the sections below:

- 1) Embedding Process (sender side): At this stage, the sending party in charge of concealing the secret text inside the selected image sends the Stego image containing the secret text as well as the Stego key (which contains all the operations and commands that have been created to conceal the secret text inside the cover images) over the Internet. The sending party must execute four main tasks in order to complete this mission. First, RSA technology

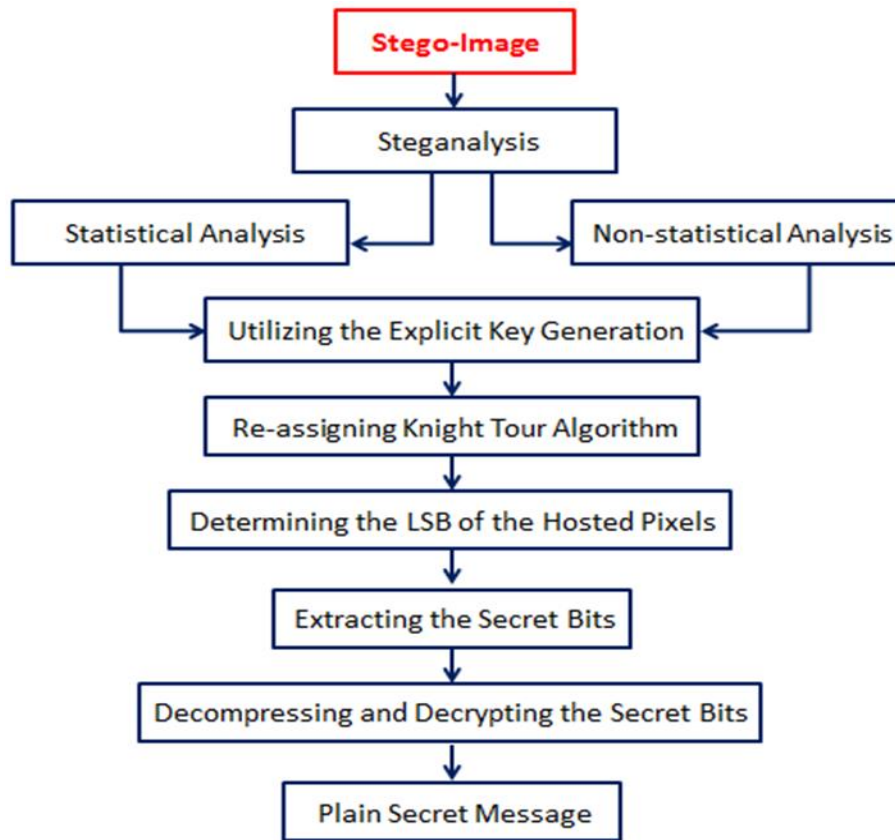
is used to encrypt the secret text [105]. This technology converts the secret text into an unreadable text, raising the proposed system up to a new level of security. This entails achieving the steganography system's most crucial purpose, which is high security. When encrypting, the RSA algorithm increases chaotic characters, which aids the proposed compression method in compressing more data. Second, through compressing the ciphertext with the Huffman algorithm [106], the suggested system is able to hide the greatest number of secret bits possible, which means accomplishing an important goal of image hiding: storage capacity. After encoding and compression, the secret text is transformed from ASCII to binary. Third, transform the RGB channels of the chosen cover image to YCbCr channels so that the image can be used to embed the manipulated text [84]. Finally, using the Knight Tour method [107], LSB substitution technology [108] will be used to insert hidden bits that have been manipulated with the pixels of the hosted image. The use of the Knight Tour algorithm ensures that the embedded bits are secure because only the transmitter and recipient parties can correctly estimate the position of the initial chosen pixel and subsequent routes. The stego image will be the result of the four processes indicated above. Figure 3.2 depicts the sender's entire four-step process.



**Figure 3.2:**The entire scenario of the embedding process

- 2) Extracting Process: (Receiver side): At this point, the authorized party will extract the secret message from the stego image which was sent via public communication from the sender party. To do so, the receiver side can use the stego key (explicit key generation) generated during the embedding process to analyse the Knight Tour technology and recognize the LSB of the pixel hiding the secret bits to retrieve back the secret text from the stego image. The full scenario of the extraction process is illustrated in Figure 3.3.





**Figure 3.3:**The whole scenario of the extracting method

### 3.3 EXPLANATION OF THE PROPOSED METHOD

#### 3.3.1 Data Pre-processing Phase

Being that most of the steganographic systems aim to reduce the gap between payload capacity and other steganography metrics like security and imperceptibility, researchers have taken special care to manipulate the secret message and cover image to assist the system in reaching its objectives. In the data pre-processing phase, two necessary actions take place simultaneously including (i) Preparing the secret text to be concealed in the cover image, and (ii) preparing the selected cover image that will host the secret message.

Robust image steganography systems have three main aspects, high payload, robustness, and imperceptibility. Therefore, using the RSA cipher algorithm and Huffman coding for the secret message as well as the cover image analysis by converting RGB into YCbCr channels to hide

the secret bit will help to satisfy the three mentioned aspects. The following subsections describe the preparation of the cover image and secret message.

### 3.3.1.1 Secret message pre-processing

According to prior research on image steganography systems, the hidden secret messages were in a variety of formats (e.g., characters, numbers, images, etc.) and had a range of storage capacities. The researchers found three embedding capacity (EC) ranges and they were measured by either Bytes or embedding ration (Percentage %) as followed [109], [110]:

- 1) 16384 (Bytes) equals to 6.25 (%) for the chosen image 512×512.
- 2) 32768 (Byte) equals to 12.5 (%) for the chosen image 512×512.
- 3) 49152 (Byte) equals to 18.75 (%) for the chosen image 512×512.

The proposed research will be compared to existing studies of those three embedding capacities to ensure the efficiency of the proposed system.

#### a) Secret message Coding.

The reason to use the RSA algorithm is that it is more secure than any other symmetric key technology, and its advantages in encryption include reliability and privacy. The used RSA algorithm involves four stages which are: (i) “key generation, (ii) key distribution, (iii) encryption, and (iv) decryption.” A basic concept behind the used RSA algorithm is the practicability of getting 3 large positive integers (e, d, and n) such that with modular exponentiation for all integers  $m$  (with  $0 \leq m < n$ ):

$$(m^e)^d \equiv m \pmod{n} \quad (3.1)$$

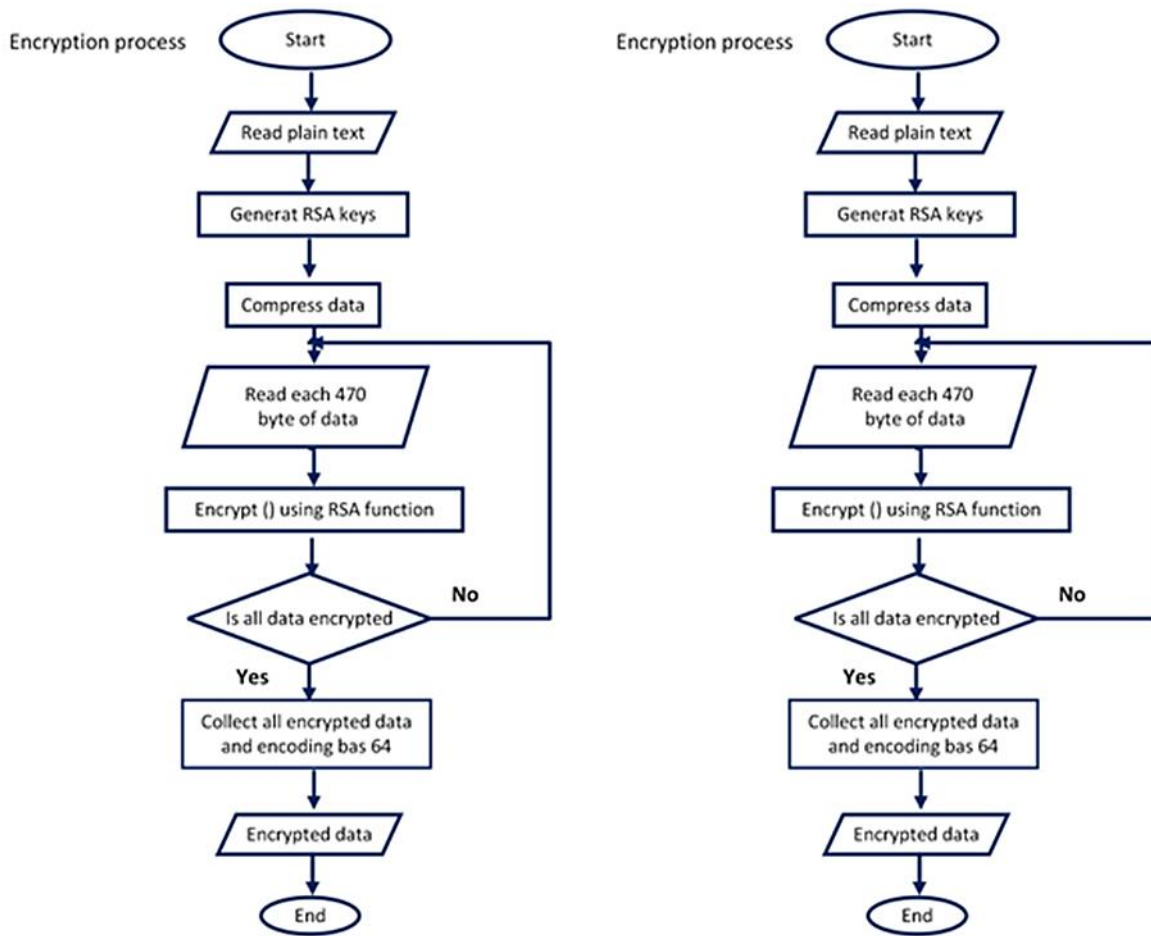
And that it is difficult to find d even after knowing e and n, or even m. Here, the triple bar ( $\equiv$ ) implies modular congruence. It is also convenient for several processes to change the order of the 2 exponentiations such that the following relation can be applied:

$$(m^d)^e \equiv m \pmod{n} \quad (3.2)$$

The RSA algorithm employs both private & public keys. Public key is used for data encryption by everyone that has access to it. The purpose of RSA is for public key-encrypted secret messages to be deciphered in a reasonable length of time only with the private key. The integers  $n$  and  $e$  are normally used to represent the public key, while the integer  $d$  is used for the private key (even though  $n$  is also utilized throughout the decryption process, so it may be taken as an aspect of the private key). The message is represented by the integer  $m$ . Algorithm 3.1 displays the pseudo code for the RSA algorithm that was used. While Figure 3.4 depicts the flowchart of the RSA encryption and decryption process.

- INPUT: Required modulus bit length,  $k$ .
- OUTPUT: The RSA key pair  $((N, e), d)$ : where  $N$  is the modulus, the product of two primes  $(N=p, q)$  not exceeding  $k$  bits in length;  $e$  is the public exponent, a number less than and coprime to  $(p-1)(q-1)$ ; and  $d$  is the private exponent such that  $ed \equiv 1 \pmod{(p-1)(q-1)}$ .
  1. Select a value of  $e$  from integer numbers.
  2. Repeat.
  3.  $p \leftarrow \text{generate prime}(K/2)$ .
  4. Until  $(p \bmod e) \neq 1$ .
  5. Repeat.
  6.  $q \leftarrow \text{generate prime}(k-k/2)$ .
  7. Until  $(q \bmod e) \neq 1$ .
  8.  $N \leftarrow pq$ .
  9.  $L \leftarrow (p-1)(q-1)$ .
  10.  $d \leftarrow \text{modinv}(e, L)$ .
  11. return  $(N, e, d)$

**Figure 3.4:**The pseudo code of the utilized RSA algorithm.



**Figure 3.5:**The flowchart of the RSA encryption and decryption process

The following example shows how the RSA algorithm works; the message is (I AM A MASTER STUDENT).

### A. Encryption Process

In the present project, the following scenario is used: Select two prime numbers,  $p$  and  $q$  that will be large enough and difficult to be detected by any person. Table 1. Displays the encrypted message achieved using the RSA algorithm.

1.  $p=19, q=29$
2. Calculate  $n$
3.  $n=p*q$
4.  $n=19*29=551$
5. Calculate the totient function;  $\phi(n)=(p-1)(q-1)$
6.  $\phi=(19-1)*(29-1)=504$
7. Select an integer  $e$ , such that  $e$  is co-prime to  $\phi(n)$  and  $1 < e < \phi(n)$
8.  $e=17$
9. Public Key =  $(e, n) = (17, 551)$
10. Private Key =  $(d, n) = (89, 551)$
11.  $d=e^{-1} \pmod{\phi(n)}$
12.  $d=17^{-1} \pmod{504}=89$
13. Choose a message: (I AM A MASTER STUDENT)
14. Encryption the message using ASCII numbers:
15. I sp. A M sp. A sp. M A S T E R sp. S T U D E N T
16. 1\
17.  $M = Me \pmod{n}$
18.  $MI = 7317 \pmod{551}$
19.  $MI = 424$
20. 2\
21.  $M = Me \pmod{n}$
22.  $Msp = 3217 \pmod{551}$
23.  $Msp = 60$
24. 3\
25.  $M = Me \pmod{n}$
26.  $MA = 6517 \pmod{551}$
27.  $MA = 430$
28. 4\
29.  $M = Me \pmod{n}$
30.  $MM = 7717 \pmod{551}$
31.  $MM = 362$
32. 5\
33.  $M = Me \pmod{n}$
34.  $MS = 8317 \pmod{551}$
35.  $MS = 429$
36. 6\
37.  $M = Me \pmod{n}$
38.  $MT = 8417 \pmod{551}$
39.  $MT = 259$
40. 7\
41.  $M = Me \pmod{n}$
42.  $ME = 6917 \pmod{551}$
43.  $ME = 293$
44. 8\
45.  $M = Me \pmod{n}$
46.  $MR = 8217 \pmod{551}$
47.  $MR = 339$
48. 9\
49.  $M = Me \pmod{n}$
50.  $MU = 8517 \pmod{551}$
51.  $MU = 530$
52. 10\
53.  $M = Me \pmod{n}$
54.  $MD = 6817 \pmod{551}$
55.  $MD = 102$
56. 11\
57.  $M = Me \pmod{n}$
58.  $MN = 7817 \pmod{551}$
59.  $MN = 257$

**Figure 3.6:** The RSA algorithm

**Table 3.1:** The encrypted message achieved using the RSA algorithm

Message	I	Sp	A	M	Sp	A	Sp	M	A	S	T	E	R	Sp	S	T	U	D	E	N	T
Value	73	32	65	77	32	65	32	77	65	83	84	69	82	32	83	84	85	68	69	78	84
Decimal	424	60	430	362	60	430	60	362	430	429	259	293	339	60	429	259	530	102	293	257	259
Encryption	z	<	Ť	Ū	<	Ť	<	Ū	Ť	f	ã	ĥ	œ	<	f	ã	Ř	f	ĥ	ã	ã

So, the secret message ((I AM A MASTER STUDENT)) is encrypted to ((z< Ť Ū< Ť Ū Ť f ã ĥ œ< f ã Ř f ĥ ã)). Using RSA algorithm

**B. Decryption Process.**

The following procedure was used to decode the ciphertext (z< Ť Ū< Ť Ū Ť f ã ĥ œ< f ã Ř f ĥ ã) into plaintext. Table 3.2 shows the results.

Decrypt the encrypted message using ASCII numbers:

```

1. z< Ť Ū< Ť Ū Ť f ã ĥ œ< f ã Ř f ĥ ã
2. 1\
3. M = Cd mod n
4. MI = 42489 mod 551
5. MI = 73
6. 2\
7. M = Cd mod n
8. Msp = 6089 mod 551
9. Msp = 32
10. 3\
11. M = Cd mod n
12. MA = 43089 mod 551
13. MA = 65
14. 4\
15. M = Cd mod n
16. MM = 36289 mod 551
17. MM = 77
18. 5\
19. M = Cd mod n
20. MS = 42989 mod 551
21. MS = 83
22. 6\
23. M = Cd mod n
24. MT = 25989 mod 551
25. MT = 84
26. 7\
27. M = Cd mod n
28. ME = 29389 mod 551
29. ME = 69
30. 8\
31. M = Cd mod n
32. MR = 33989 mod 551
33. MR = 82
34. 9\
35. M = Cd mod n
36. MU = 53089 mod 551
37. MU = 85
38. 10\
39. M = Cd mod n
40. MD = 10289 mod 551
41. MD = 68
42. 11\
43. M = Cd mod n
44. MN = 25789 mod 551
45. MN = 78
    
```

**Figure 3.7:** Algorithm

**Table 3.2:** The decrypted message achieved using the RSA algorithm

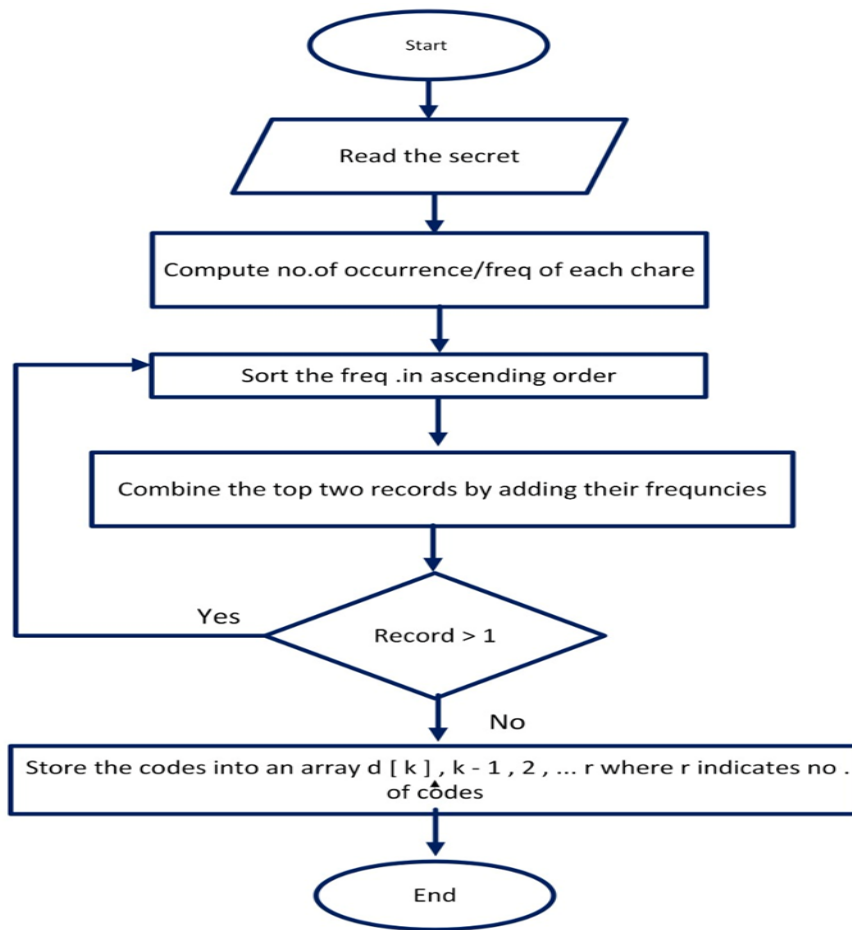
Encryption	z	<	Ŧ	Ū	<	Ŧ	<	Ū	Ŧ	f	ă	ĥ	œ	<	f	ă	Ŕ	f	ĥ	ā	ă
Decimal	424	60	430	362	60	430	60	362	430	429	259	293	339	60	429	259	530	102	293	257	259
Decryption	73	32	65	77	32	65	32	77	65	83	84	69	82	32	83	84	85	68	69	78	84
Message	I	Sp	A	M	Sp	A	Sp	M	A	S	T	E	R	Sp	S	T	U	D	E	N	T

As shown in Table 3.2, the encrypted message ((z< Ŧ Ū< Ŧ Ū Ŧ f ă ĥ œ< f ă Ŕ f ĥ ā ă)) is decrypted and becomes ((I AM A MASTER STUDENT)).

A. Secret Message Compression

**b) Huffman Coding**

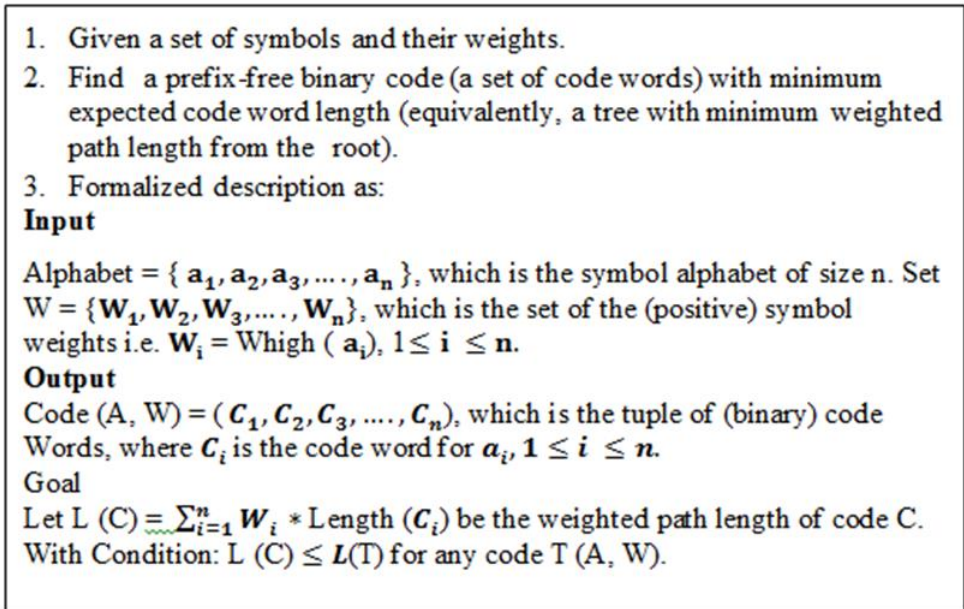
The primary objective of using compression techniques is to enhance payload capacity via secret bits compression. The secret message, in the proposed study, is first reduced in size with Huffman coding before embedding in the cover image. This compression process converts the secret message into streams of bits that are transformed using the Huffman dictionary into a secret code. Figure 3.5, secret code vector is achieved as the outcome of the compression process. The secret message must be in text format to allow the use of Huffman coding to compress its size before the embedment step. The secret message is first encrypted to increase the bit randomness and then compressed for bit size reduction before starting the embedding process.



**Figure 3.8:** The General Flowchart of Huffman coding [111]

According to the requirements of secret message pre-processing which is needed to handle the encrypted message before embedding then compression of message by Huffman algorithm gives facility to increase the size of the secret message embedded into the system. Algorithm 3.3. Illustrates the Huffman algorithm with secret key:





**Figure 3.9:** The Huffman algorithm with secret key

Then the binary tree code will issue and find each path according to frequency of the letters included in this word. Figure 3.5., illustrates the Huffman coding tree using the Huffman compression method to compress the message ((z < T Ū < T Ū T f ä ĥ œ < f ä R f ĥ ā ä)). While Figure 3.6., expresses the using of Huffman coding tree for the message ((I AM A MASTER STUDENT)).

Characters	z	<	T	Ū	f	ä	ĥ	œ	R	f	ā
Frequencies	1	4	3	2	2	3	2	1	1	1	1

1. Step one: Arrange the data in ascending order in a table.

Characters	z	œ	Ŕ	f	ā	Ū	f	ĥ	Ŧ	ǎ	<
Frequencies	1	1	1	1	1	2	2	2	3	3	4

2. Step Two: Combine first two entries of a table and by this create a parent node.

Characters	Ŕ	f	ā	zœ	Ū	f	ĥ	Ŧ	ǎ	<
Frequencies	1	1	1	2	2	2	2	3	3	4

3. Step Three: Repeating the step 2.

Characters	ā	Ŕf	zœ	Ū	f	ĥ	Ŧ	ǎ	<
Frequencies	1	2	2	2	2	2	3	3	4

Characters	zœ	Ū	f	ĥ	āŔf	Ŧ	ǎ	<
Frequencies	2	2	2	2	3	3	3	4

Characters	f	ĥ	āŔf	Ŧ	ǎ	zœŪ	<
Frequencies	2	2	3	3	3	4	4

Characters	āŔf	Ŧ	ǎ	fĥ	zœŪ	<
------------	-----	---	---	----	-----	---

Frequencies	3	3	3	4	4	4
-------------	---	---	---	---	---	---

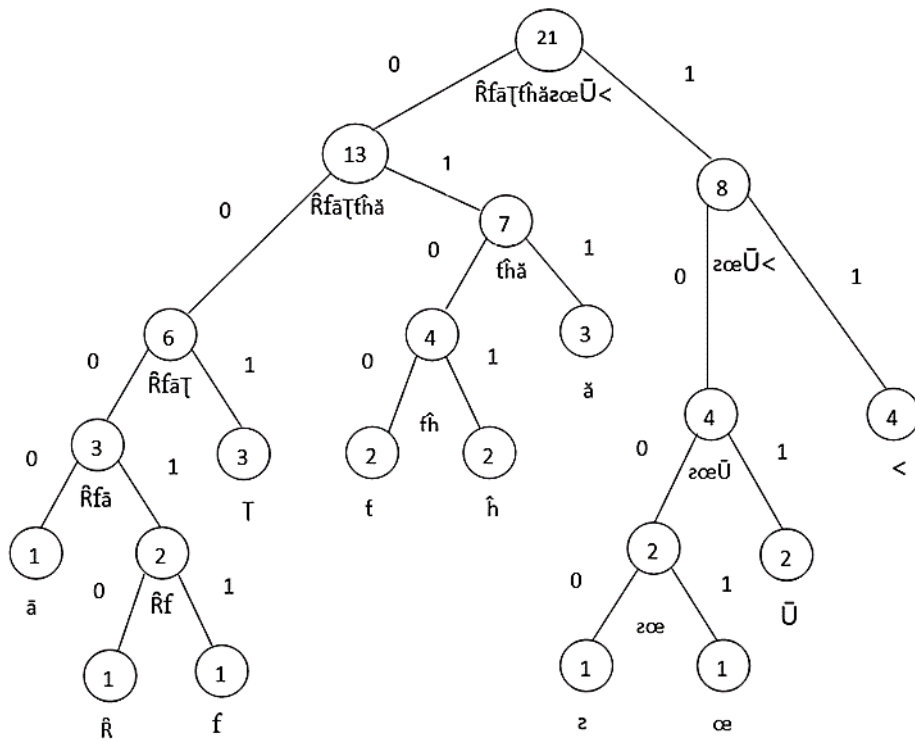
Characters	ǎ	tĥ	zœŪ	<	āRfſ
Frequencies	3	4	4	4	6

Characters	zœŪ	<	āRfſ	ǎtĥ
Frequencies	4	4	6	7

Characters	āRfſ	ǎtĥ	zœŪ<
Frequencies	6	7	8

Characters	zœŪ<	āRfſǎtĥ
Frequencies	8	13

Characters	zœŪ<āRfſǎtĥ
Frequencies	21



**Figure 3.10:** Huffman coding tree for compressing the message (( $a < \tau \bar{U} < \tau \bar{U} \tau f \ddot{a} \hat{h} \text{œ} < f \ddot{a} \hat{R} f \hat{h} \bar{a}$   $\ddot{a}$ )).

Characters	Frequencies	Huffman code	Length
<	4	11	2
ă	3	011	3
Ţ	3	001	3
ĥ	2	0101	4
f	2	0100	4
Ū	2	101	3
ā	1	0000	4
f	1	00011	5
Ŕ	1	01000	5
œ	1	1001	4
z	1	1000	4
Characters	Frequencies	Huffman code	Length
<	4	11	2
ă	3	011	3
Ţ	3	001	3
ĥ	2	0101	4
f	2	0100	4
Ū	2	101	3
ā	1	0000	4
f	1	00011	5
Ŕ	1	01000	5
œ	1	1001	4
z	1	1000	4

While the second example is about compressing the pain text ((I AM A MASTER STUDENT)).

Characters	I am a master student
Frequencies	20

Characters	I	r		u	d	n	m	s	t	e	a	Sp.
Frequencies	1	1		1	1	1	2	2	2	2	3	4

Characters	u	d	n	Ir	m	s	t	e	a	Sp.
Frequencies	1	1	1	2	2	2	2	2	3	4

Characters	n	ud	Ir	m	s	t	e	a	Sp.
Frequencies	1	2	2	2	2	2	2	3	4

Characters	Ir	m	s	t	e	nud	a	Sp.
Frequencies	2	2	2	2	2	3	3	4

Characters	s	t	e	nud	a	Irm	Sp.
Frequencies	2	2	2	3	3	4	4

Characters	e	nud	a	st	Irm	Sp.
Frequencies	2	3	3	4	4	4

Characters	a	st	Irm	Sp.	enud
Frequencies	3	4	4	4	5

Characters	Irm	Sp.	enud	ast
Frequencies	4	4	5	7

Characters	enud	ast	IrmSp.
Frequencies	5	7	8

Characters	IrmSp.	enudast
Frequencies	8	12

Characters	Frequencies	Huffman code	Length
I	1	0000	4
r	1	0001	4
u	1	10000	5
d	1	10001	5
n	1	1001	4
m	2	001	3
s	2	1100	4
t	2	1101	4
e	2	101	3
a	3	111	3
Sp.	4	01	2

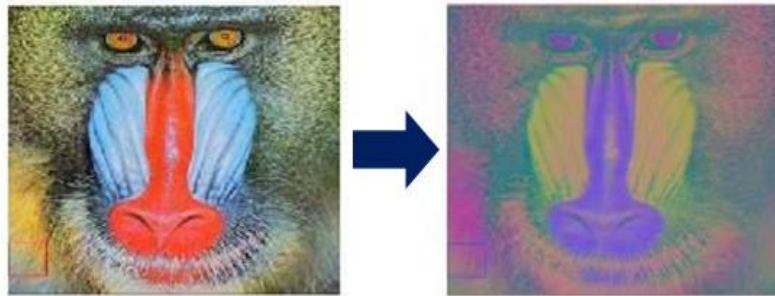
Figure 3.6 Huffman coding tree for compressing the message ((I AM A MASTER STUDENT)).

### 3.3.1.2 Cover image pre-processing

#### a) Image Format Converter (RGB to YCbCr).

A variety of image formats / types were utilized in the image steganography systems to hide secret text (e.g. grayscale, RGB, CMYK, HSV and YCbCr) [4], [5]. Each type has its own set of benefits and drawbacks. However, there is no evidence that one type is preferred over the other [5]. Researchers recently improved the embedding processes by preparing cover images before embedment. According to the suggested system, RGB channels were converting to YCbCr channels before the embedment step.

The conversion of color spaces is the step that matters the most in image processing applications. The reliance of real-time videos and images - sensitivity of color detection cells in the HVS implies that they are recorded in the RGB color space. The use of the YCbCr color space in digital image processing is mainly considered as a way of exploiting the HVS's lower resolution capacity for color with respect to luminance [84]. Thus, RGB to YCbCr conversion is mostly employed in the processing of images and video. Figure 3.6 depicts the process of transforming the RGB image to the YCbCr.



**Figure 3.11:** The process of transforming the RGB image to the YCbCr

## 3.4 EMBEDDING PROCESS

The method of concealing secret data within the pixels of the hosted image using a set of procedures known as the (embedding process). Researchers have contributed a variety of hiding



approaches, some of which are resistant to steganalysis techniques [112] and others fail to withstand hacker attacks [113].

The robustness of the embedding method lies in balancing the concealment of a high payload capacity and other measures (e.g., security, imperceptibility). Therefore, the proposed study mainly aims to design a new embedding method that fits the criteria of strength hiding method. Three main processes were used in the proposed method. First, knight tour-based image scrambling approach. Second, substitution LSB method. Finally, explicit key generation (stego key). Merging these three methods may help any embedding method to hide a large number of secret bits and maintaining the imperceptibility at the same time.

### 3.4.1 Knight Tour Based- Image Scrambling.

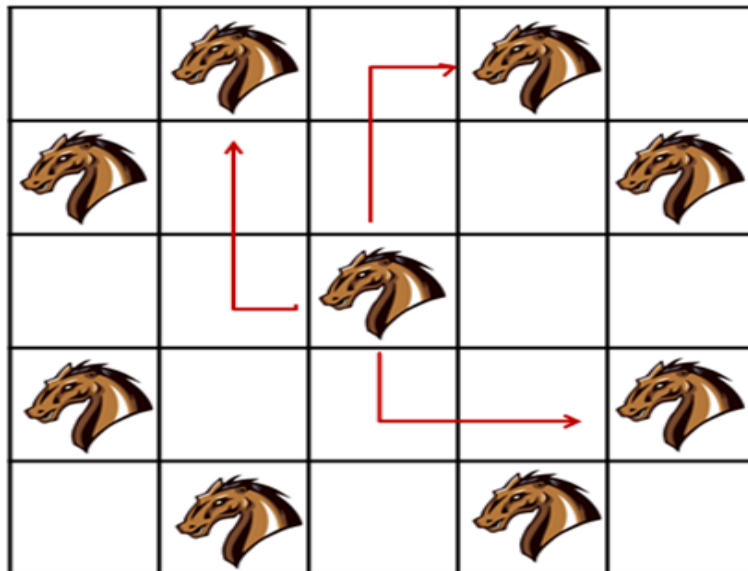
Euler started analyzing the "Knight Tour" approach in 1759. It was considered a useful way of formulating the order of the hidden bit stream within the image pixels. The self-created Knight Tour algorithm was based on the knight tour math problem (Nie et al., 2019). Additionally, it is more effective than the pseudo-random number generator (PRNG) algorithm because of its imperceptibility or identification by people that are not authorized to have it. The chessboard is divided into blocks using the Knight Tour method. The cover image is divided into four equal halves for the proposed study, as shown in Figure 3.7. Hence, knight tour can be used to achieve a high security image steganographic system because the solution space will be considerably high irrespective of whether the starting square of the knight's move is known or not [114].



**Figure 3.12:** Dividing the cover image into  $4 \times 4$  blocks utilizing Knight Tour algorithm

If the selected image is divisible by four blocks, the utilized Knight Tour algorithm (KTA) will cover all pixels. However, additional rows or columns  $<4$  blocks will be non-usable. The steps of the employed KTA are as follows:

- 1- The proposed KTA divides the chosen image into  $4 \times 4$  blocks of pixels and ignore any additional pixels that are not within the quotient of the created blocks.
- 2- The proposed KTA begins by visiting the pixel indicated by the stego key, then moving on to the first block of the  $4 \times 4$  blocks, and so on until all of the pixels in that block have been traversed. Figure 3.8 explains the movement of Knight Tour algorithm on the chess-board squares.
- 3- The proposed KTA must visit all the pixels in one block to move to the other block.
- 4- The proposed KTA repeats all the above processes to traverse all the pixels in the chosen image.



**Figure 3.13:** The movement of KTA on the chess-board squares

After using the suggested KTA to randomly select all of the pixels of a chosen image, the proposed LSB Permutation Approach (LSBPA) will be utilized to exchange the pixels of the chosen image with secret bits.

### **3.4.2 Applying LSB Permutation Approach (LSBPA).**

The Least Significant Bit (LSB) technique [115] is the simplest way to hide secret bits by substituting the image pixel's minimal weighting value with secret bits. The only goal on the receiver's side is to extract secret bits from the corresponding pixels. The KTA was used to control randomly the location where secret bits would be embedded, increasing the difficulty of secret bit detection. Although the security is inadequate, the LSB technique is easy and straightforward to apply, has a good hiding ability, and can easily embed and retrieve information. To conceal the secret bits applying the LSB technique, the proposed study using the following steps.

1. Determine the dimensions of the cover image in binary system manner.
2. Using the Knight Tour Algorithm to select pixels at random and then embed bits in the image's LSB.
3. Using the LSB technique to hide secret bits by swapping the 8<sup>th</sup> bit on each 8-bit pixel with one secret bit while without changing the most significant bits (MSB).

Algorithm 3.4 explains the process of the applying LSB Permutation Approach (LSBPA)

Input: Original Image (CI) of size  $512 \times 512$ , Secret Bits (SB).  
Output: Stego Image (SI).

1. Read the SB and convert it into series of bits with binary system.
2. Read the CI (  $512 \times 512$  ).
3. Convert the pixel's value of the chosen image from the ASCII value to the binary system
4. Convert the RGB channels of the chosen image to the YCbCr channels.
5. Apply the RSA algorithm to the SB.
6. Apply the Huffman coding the encrypted SB.
7. Calculate the size of the SB (the number of characters or bytes).
8. Let  $L$ =length of SB in bits.
9. Select the aim pixels according to matched and dis-matched bits strategy.
10. Create stego key called "RITAG vector" to record the whole steps of the embedding process, the proposed Knight Tour movements and the procedures of the proposed LSBPA.
11. Mark the LSB of each pixel.
12. Then make loop from  $I=1: N$ .
13. Get SM bit (0 or 1).
14. If the number of SB bit is matched with number of chosen CI bit embed directly.
15. If the number of SB bit is dis-matched with number of chosen CI bit, swap the bits and then embed the swapped bits.
16.  $I = I+1$ .
17. Send the SI to receiver party over the WWW.
18. Return the SI.
19. End.

**Figure 3.14:** The process of the applying LSBPA

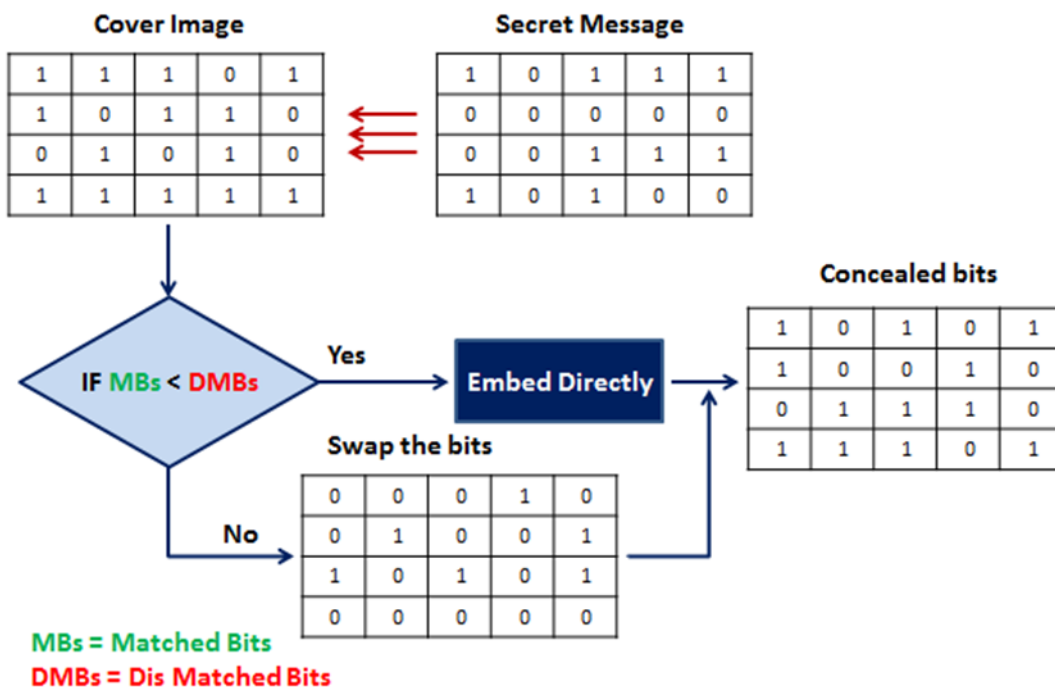
The proposed LSBPA method conceals the secret bit in the cover image. It attempts to solve the weaknesses of the existing embedding schemes/methods by developing an effective and accurate steganography system. For an in-depth understanding of the embedding process, several principles should be considered. The proposed LSBPA aims to keep the stego image which includes the secret bits looks like the original image. In this regard, attackers/intruders cannot notice anything if there is confidential bits inside the chosen image.

To achieve the main objective of image steganography, there are two points that make a Stego image resemble the original version and that is, the secret bits embedment must always occur in the LSB part of the image pixel. Here are two policies that authors must follow to work with image steganography schemes

- a) Select the convenient pixels for secret bits embedment.

b) Embedding the secret bits adaptively according to the determined strategy and applying the embedding process according to certain criteria.

In the proposed LSBPA method, after preparing the secret text (encryption and compression), the secret bits will be fragmented into 64 bits. At this point, 64 bits (from the image) will be replaced by 64 bits (from the secret bits). Before swapping the bits cover image bits with the secret bits, there will be a check for the match between the secret and original image bits; if there are more mismatched bits compared to the matching bits, swap the bits of the secret message (flip the secret message) and embed it, else, directly embed the secret bits. As depicted in Figure 3.9, the red bits indicate the mismatched bits, and the green bits indicate the matched bits.



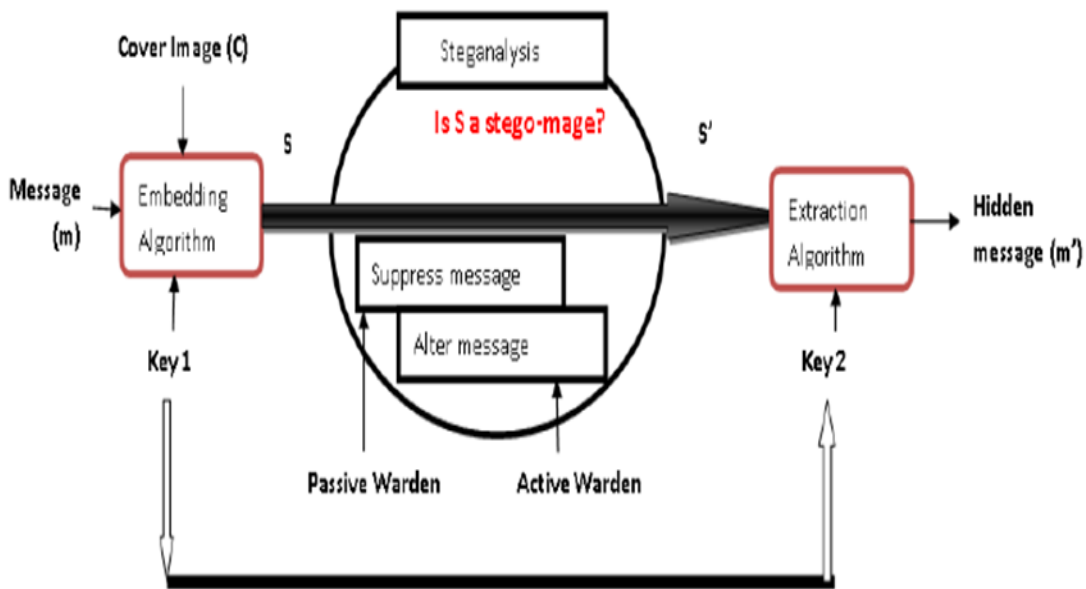
**Figure 3.15:** The proposed LSBPA

The stego key will contain all the information related to the preparation of the secret message and the embedding process. The stego key is stored outside the image and referred to as the explicit stego key. There is an agreement between the parties regarding this key and produced

by the sender to be used by the receiver to extract the secret message form the image. Image that contains the secret message called stego image, should be able to stand against the attacks, therefore many tests applied on the image before sending it to the other part or receiver. These attacks or evaluation happened in sender part and will be discuss in detail in the next paragraph of evaluation stag.

### 3.5 STEGO-IMAGE

To obtain the stego image, the prepared secret data is integrated into the cover image. Steganography refers to the process of hiding a message in an image, and stego images are the images that contain the concealed message. The major stage is always the embedding technique, followed by the secret data. The receiver must be aware of the secret information in this method. Throughout the procedure, the recipient utilizes the stego key, which holds all the information. The embedding process is reversed to extract the hidden message from the stego image, as seen in Figure 3.11.



**Figure 3.16:** The embedment and extracting process in the proposed steganography scheme

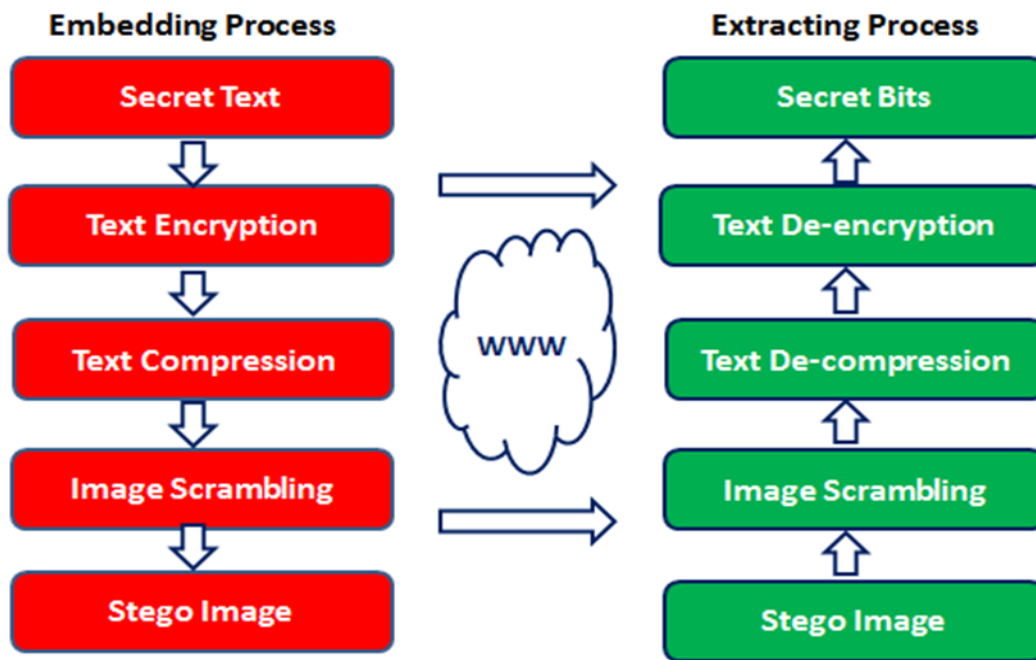
The transmission media that can be the image, audio, video, or protocol are all subjected to attack when transferred through the WWW. In the present study, the transmission media is the

image and most of the attacks involve  $\chi^2$  attack, Histogram attack and HVS attack. The secret bit embedment process from the beginning to the end was recorded in the stego key. Thus, the procedure can be reserved on the other side (receiver) for the extraction of the hidden message from the stego image.

### **3.6 IMAGE EXTRACTING**

The transmission media in the field of information hiding, steganography, in particular, can be video, audio, protocol or image, in the proposed study we consider the image as transmission media due to its availability and the ability to hold a large amount of data [116]. There is a certain possibility that the image may encounter different kinds of attacks when transferring from the sender party to the authorized receiver party. The whole procedures that occurred in the embedding stage are recorded in the implicit stego key as a sequence, once the receiver side receives the stego-image; he/she uses the same sequence of embedding process but in conversely action called extracting. The receiver side uses two kinds of information in the implicit stego key. The first kind of information is the procedures used by the embedding such as sequence operations of pixels' selection, and the mapping order of secret message which defragmented accordingly. The second information on stego key is the general information that agreed by the two parties in advance that may it change.

The extraction process is aimed at obtaining the embedded message (secret bits) from the least significant bits (LSBs) following the steps designed and built in the embedment phase. In the art of image steganography system, most of the information that related to the extraction phase and the other information contained in the stego key that is considered variable and based on environment and nature of the image, is done by agreement between the sender and receiver party. Figure 3.11. depicts the general process of embedment and extraction of secret bits. Figure 3.11.



**Figure 3.17:** Embedding and extracting processes

The sender and receiver know all the steps involved in the embedding and extraction stages; however, some information must be needed to locate the index pixels that are not mutually agreed upon. This extra information can be promptly executed using the stego key at the embedding stage. In this case, the stego key remains updated until the completion of the embedding procedure. Figure 3.8 depicts the stages of embedding and extraction with the goal of security and imperceptibility.

The embedding and extraction steps are responsible for ensuring imperceptibility (image quality), meaning that the pixel selections of the image reflect the robustness and security of the steganographic system. These consider the major objectives in the proposed scheme in addition to increasing the capacity achieved by the pre-processing or preparation stage. Cover images supposed to hosting the secret bits selected from the standard USC- SIPI dataset which will discuss in the next section.



### 3.7 EVALUATION METRICS

The performance of the newly proposed improved image steganography scheme was assessed through the design and implementation using the standard dataset. The developed steganography system dealt with both colour and greyscale images (of various sizes and dimensions) extracted from the SIPI dataset. In addition, the secret text in the cover image was hidden by the implicit secret key and the stego image was achieved. The designed image steganography system was evaluated for performance in terms of various measures (PSNR, MSE, BPP, SSIM, NCC and EC). The robustness of the system was tested against diverse attacks including the HVS, histogram and  $\chi^2$ . To validate the authenticity of the developed scheme, the obtained experimental results were matched with the state-of-the-art literature reports. Majority of the common visual quality analysis metrics that were used to assess the developed image steganography system are demonstrated as follows.

$$\begin{aligned} \text{Peak Signal to Noise Ratio} &= 10 \cdot \log_{10} \left( \frac{255^2}{\text{MSE}} \right) \\ \text{(PSNR)} & \end{aligned} \quad (3.3)$$

---


$$\begin{aligned} \text{Mean Square Error (MSE)} &= \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [\mathbf{I}(i, j) - \mathbf{K}(i, j)]^2 \end{aligned} \quad (3.4)$$

---


$$\begin{aligned} \text{Structural Similarity Index} &= \frac{(2P_0 Q_S + C_1)(2\sigma_{OS} + C_2)}{(P_0^2 Q_S^2 + C_1)(\sigma_0^2 + \sigma_S^2 + C_2)} \\ \text{Measure (SSIM)} & \end{aligned} \quad (3.5)$$

---


$$\begin{aligned} \text{Normalized Cross-} &= \frac{\sum_{x=1}^M \sum_{y=1}^N (S(x, y) \times C(X, Y))}{\sum_{x=1}^M \sum_{y=1}^N (S(x, y))^2} \\ \text{Correlation (NCC)} & \end{aligned} \quad (3.6)$$

---


$$\begin{aligned} \text{Embedding Capacity (EC)} &= \frac{\text{The number of message bits}}{\text{The number of cover images's pixels}} \end{aligned} \quad (3.7)$$

---

$$\text{Chi-square } (\chi^2) = \sum \frac{(\text{Observed} - \text{Expected})^2}{\text{Expected}} \quad (3.8)$$

---

### 3.8 DATASET

A set of images defines the dataset in the image steganography systems. Generally, this dataset is utilized for validating the legitimacy of the developed image steganography systems and benchmarking the outcomes by comparing with the existing state-of-the-art works in the literature. Over the years, numerous sets of images as the standard datasets have been employed in the steganography systems which produced quite encouraging results with good performance. In this spirit, the current investigation adopted the same approach for evaluating and benchmarking the obtained experimental results by the proposed novel image steganography scheme with improved performances. To achieve this goal, both greyscale and colour (red, green, and blue in short RGB) images were used as the reliable datasets. In these datasets, each pixel in the image was comprised of 24 bits wherein 8 bits were assigned to every colour. The proposed image concealing technique treated each part independently as the new pixels due to their difference in the illumination from each other. In addition, the notable advantages of the newly developed steganography scheme were confirmed by selecting different images from the USC-SIPI standard dataset available on the website (<http://sipi.usc.edu/database/database.php?volume=misc>). This dataset contained a total of 44 standard images (16 colour and 28 greyscale) which are extensively utilized by [2], [108], [117] (Figure 3.13). The full dataset images are furnished in the Appendix A. Table 3.3 displays the detail distribution of the standard dataset images [118].



**Figure 3.18:** USC SIPI dataset

**Table 3.3:** The detail distribution of the standard dataset images

Dataset	Image Size	Total	No. of Images	Gray Images	Colour Images
USC-SIPI	1024×1024	44	4	4	-
	512×512		26	18	8
	256×256		14	6	8

### 3.9 SUMMARY

An enhanced image steganography system has been presented in this chapter for concealing a high payload capacity while ensuring the security of the embedded secret data. The proposed system included four main stages which are (i) data preparation, (ii) embedment process, (iii) evaluation of the stego-image with the different evaluation processes, and (iv) extraction process. All messages were encrypted using RSA while Huffman compression method was used to compress the messages before being included. To improve the robustness of the developed scheme, the cover image was also processed prior to embedding by dividing the chosen image

into four portions and then randomly selecting the pixels of each part. using Knight Tour algorithm. LSBPA and explicit key generation were the two main methods of hiding secret texts in image pixels. The proposed system aims to improve the image's PSNR such that it can withstand any attack while also increasing the secret message's payload capacity.

## **4. RESULT AND DESCUSSION**

### **4.1. INTRODUCTION**

Chapter 1 formalized the research problem, aim, and objectives of the study while Chapter 2 covered the literature related to existing image steganography systems was investigated. The methods used to implement the project was outlined in Chapter 3. This chapter will focus into considerable detail about the proposed LSB Permutation Approach's design and implementation (LSBPA). The outcomes of the experimental evaluation are discussed and analyzed. This chapter is divided into six sections, including an introduction and a discussion.

The experimental evaluation of the suggested scheme was presented in Section 4.2, while the result and discussion based on the three key issues are expressed in section 4.3. Section 4.4 covered the comparative analysis with the state-of-the-art. Finally, section 4.5 covered the discussion of this chapter.

### **4.2. EXPERIMENTAL EVALUATION OF THE PROPOSED SCHEME**

The experimental evaluation was carried out using a PC with Intel Core i7-10750H, 2.6GHz, 6MB L2, L3 Cache, 4 GB PC3-10600 (DDR3-1333) RAM, 1 TB (7200 RPM) SATA-3G Hard Disk, Microsoft Windows® 10 Premium Edition (64-bit). The experiments were conducted using several MATLAB libraries and packages like the MATLAB Coder, Embedded Coder, Simulink Compiler, and others.

To evaluate the developed scheme for robustness, this study used the imperceptibility, Human Visual System (HVS), Normalized Cross-Correlation (NCC), structural similarity index measure (SSIM), PSNR, Payload Capacity (PC), and Histogram as the evaluation metrics [2], [16], [119]. Moreover, computational complexity and memory utilization were used for the evaluation of the efficiency of the developed scheme based on the computation theory as normally done in the related works [16], [120]. Equations (4.1), (4.2), (4.3), (4.4), and (4.5) were used to calculate the PC, PSNR, MSE, NCC, and SSIM, respectively.

$$BPP = \frac{\text{Number of secret bits embedded}}{\text{The whole pixels in the cover image}} \quad (4.1)$$

$$PSNR = 10 \cdot \log_{10} \left( \frac{MAX_1^2}{MSE} \right) \quad (4.2)$$

with

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j)]^2 \quad (4.3)$$

$$NCC = \frac{\sum_{i=0}^{N-1} \sum_{j=0}^{M-1} I_c(i,j) I_s(i,j)}{\sum_{i=0}^{N-1} \sum_{j=0}^{M-1} I_c(i,j)} \quad (4.4)$$

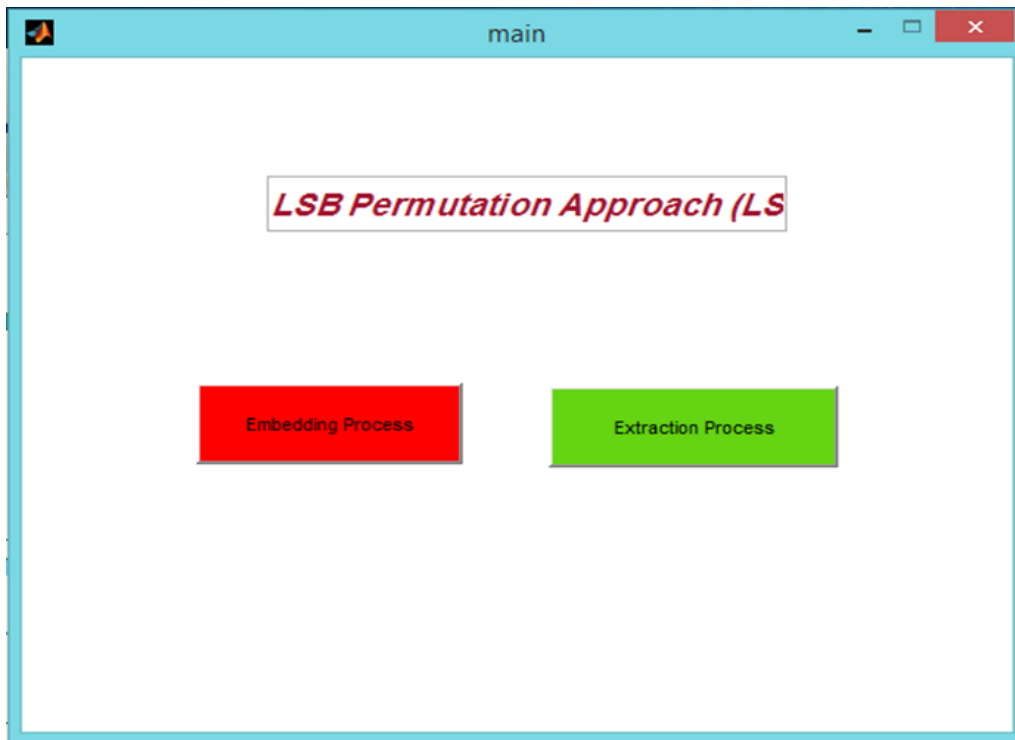
$$SSIM(x, y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \quad (4.5)$$

$$C_1 = (K_1L)^2$$

$$C_2 = (K_2L)^2$$

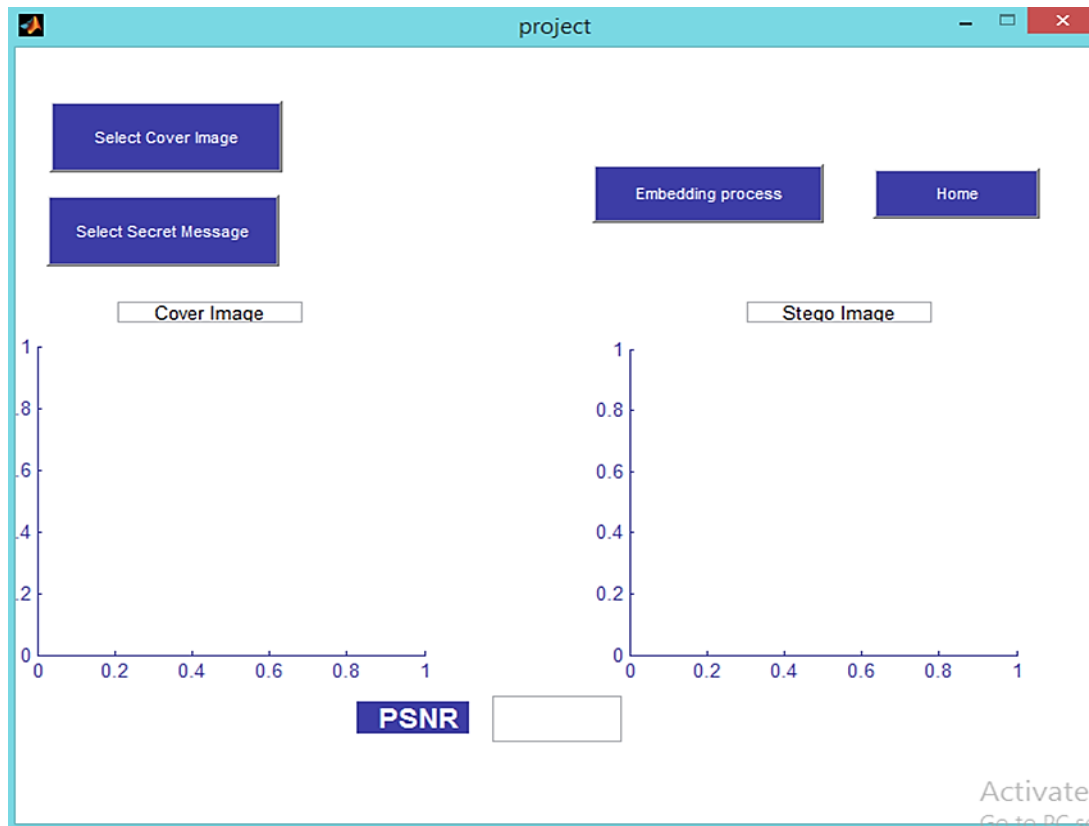
### 4.3 SOFTWARE IMPLEMENTATION

The methods for embedding and extracting hidden text from image pixels are critical components of any image steganography system. The embedding method is implemented in the transmitting stage, whereas the extraction method is implemented in the receiving stage. The proposed system's principal scenario is built on embedding and extraction methodologies. To simulate the method and obtaining results during the execution, the proposed system was developed using Matlab V. 18 software. Figure 4.1 depicts the overall system procedure.



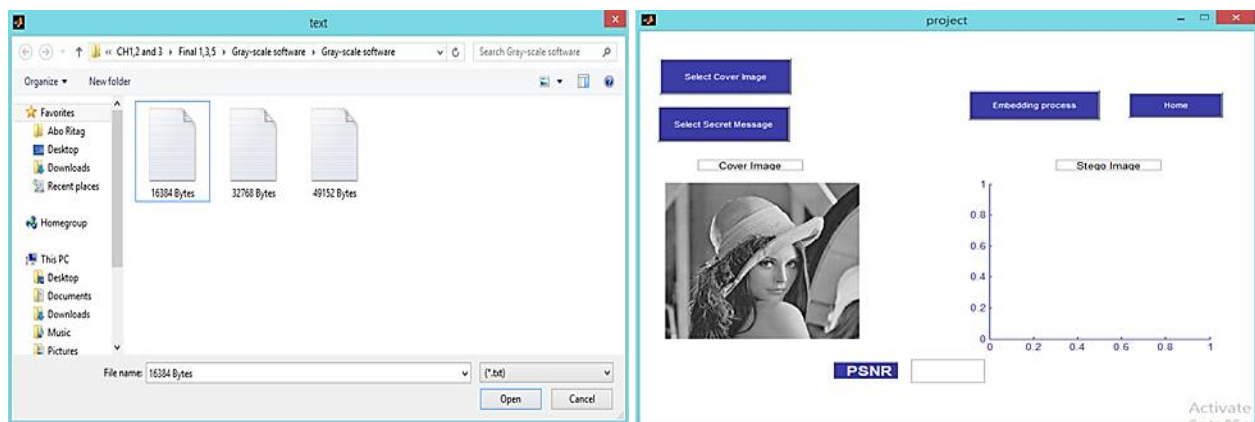
**Figure 4.1:** The main interface of the demo system

This software is compatible and works on both the sender and receiver ends, with the embedding process taking place on the sender's end, which is responsible for concealing a secret bit in the chosen carrier. The extraction process exposes the hidden message in the stego image. As seen in Figure 4.2, one of the two main steps in the embedding process is to select both the cover image and the secret message.



**Figure 4.2:** The embedding process within proposed system

The secret file is first selected, as shown in the figure above, to be ready for embedding in the chosen image, which was also selected at this stage. These two selective items must be present before pressing embedding button, as shown in Figure 4.3. With the several types of SIPI database images, the proposed system can handle both grayscale and color images.



**Figure 4.3:** Selecting a cover image for the embedment of a selected secret bit



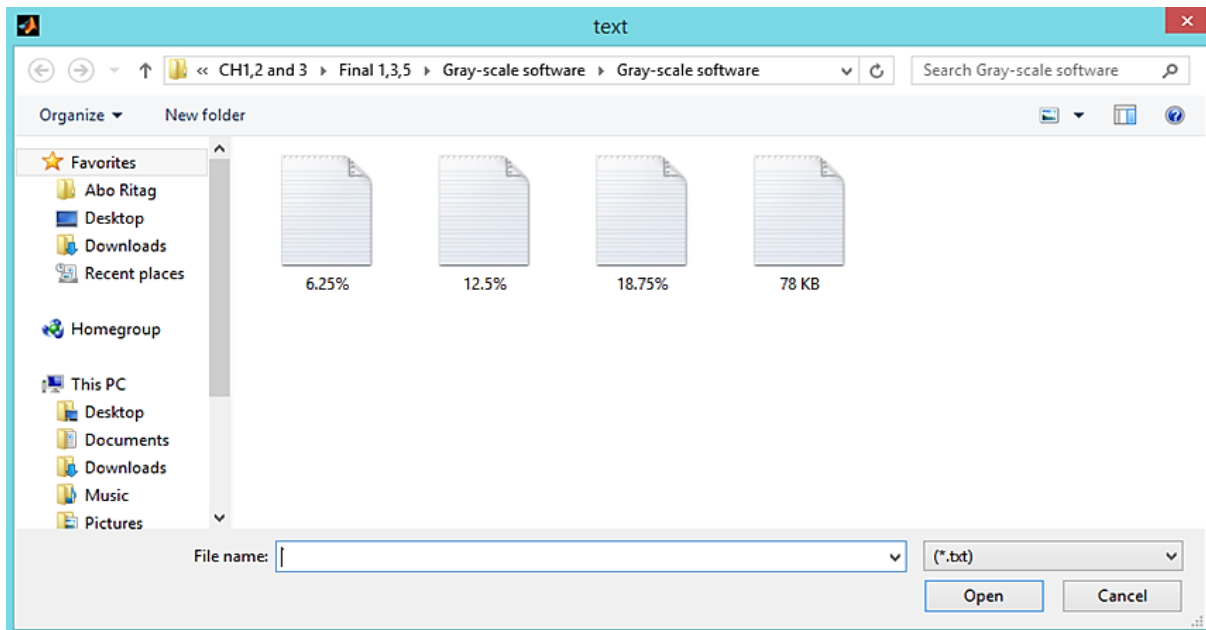
In the literature, the methods of image steganography systems were evaluated using a variety of criteria, one of which was embedding capacity (EC), which may be calculated using the following equation:

$$Ec(bpp) = \frac{\text{No. of embedding bits}}{W \times H} \quad (4.6)$$

Where : bpp means bit per pixel

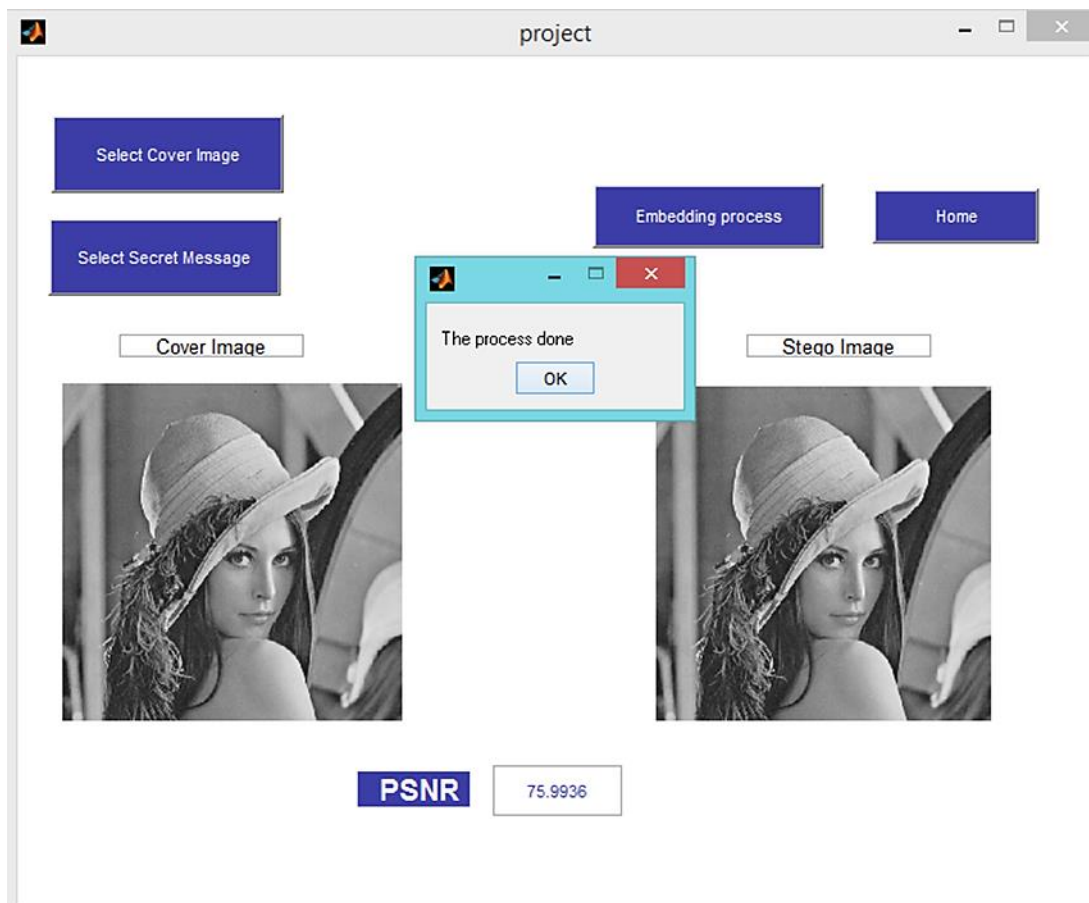
Regarding the payload capacities used in the image steganography systems, there are different standard sizes that researchers who work in the information hiding field use to evaluate their proposed steganography methods, which are 6.25%, 12.5%, 18.75%, 25%, and others. For more clarity when embedding the secret text, various payload capacities have been used with the proposed system and are represented as a percentage to relate with the recent studies in literature. The percentage of 6.25% for the cover image is equal to 16384 bytes, and the percentage of 12.5% for the cover image is equal to 32768 bytes. While the percentage of 18.75% for the cover image is equal to 49152 bytes, these percentages can be calculated based on the number of embeddable secret bits in each cover image pixel, where the ratio of 6.25% comes from embedding one secret bit in every two pixels of the carrier image (**2 pixels = 16 bits, 1/16 = 6.25%**), and the ratio of 12.5% comes from embedding one secret bit in each cover image pixel (**1 pixel = 8 bits, 1/8 = 12.5%**).

The current study interacts with the various sizes outlined in the previous section as well as other sizes to benchmark the suggested method to those suggested in previous studies to determine the performance of the suggested scheme as shown in Figure 4.4.



**Figure 4.4:** Different payload capacities used in the proposed system

After selecting both the carrier and the secret text and pressing the "Embedding Process" button, the conceal procedure begins, which embeds the secret text inside the image pixels using the proposed LSBPA embedding method. Figure 4.5 depicts the complete configuration that appears in the interface of the embedment process.

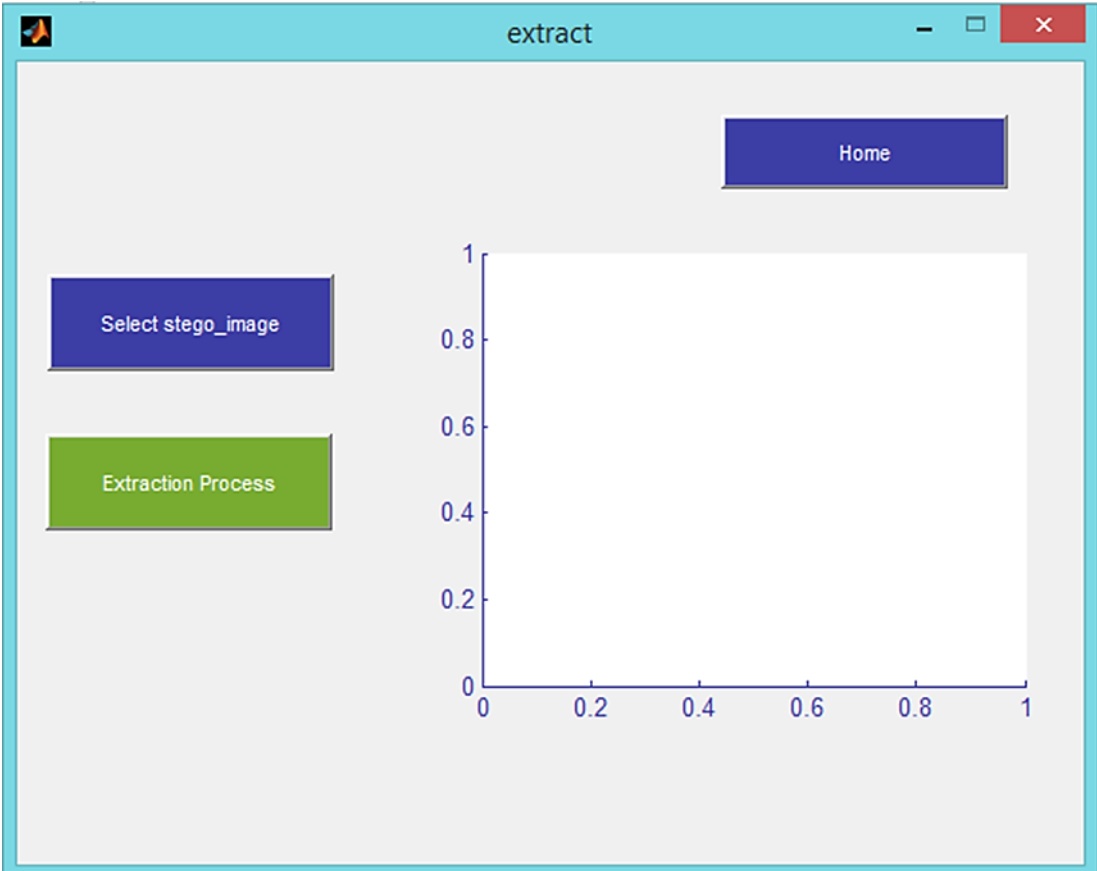


**Figure 4.5:** The resulted images after embedding process

The stego-image is the outcome of hiding the secret text in the chosen carrier in a manner that the stego-image looks exactly like the cover image, or in other words, there are exact matches between the two images. As seen in Figure 4.5, the image on the left appears to be the same as the image on the right; this is the aim of steganography, in which the embedded image cannot be distinguished by naked eyes. No one can recognize the image, whether stego or cover, but the difficulty with statistical evaluations such as PSNR or HVS is that it is easy to distinguish between them.

Due to the limitation size of SIPI dataset images, the amount of embeddable secret bits in the selected carrier is limited and not free; in the proposed system, it has been considered  $512 \times 512$  image pixels. These pixels, however, may contain a limited amount of data, and expanding this quantity is dependent on the proposed LSBPA.

The second part of the proposed system is the extracting process. When a receiver party receives the stego image with the stego key, the receiver can extract the secret bits by using a certain algorithm and the key as a tool to get secret bits as shown in Figure 4.6.

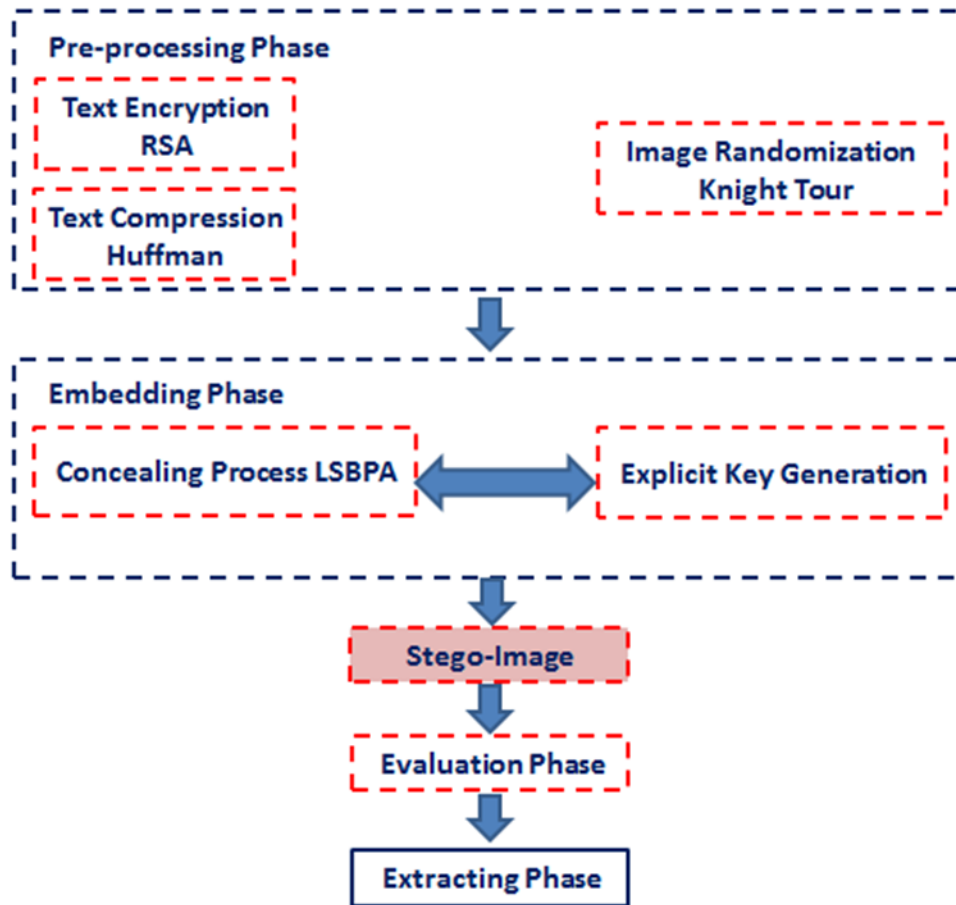


**Figure 4.6:** The Extracting process within proposed system

The evaluation process must be at the sender side when embedding the secret bits, in this case, imperceptibility is the main criteria measured as PSNR will calculate before sending stego image. Hackers always catch the stego image before receiving by the receiver side, so that we evaluate the stego image to avoid any missing in the system. Within the system menu, there is field PSNR located after embedding to ensure that the image is imperceptible.

#### **4.4 RESULTS DISCUSSION AND ANALYSES**

This results of the experiments from using different techniques and methods (as shown in Figure 4.7) are presented in this section. The proposed scheme consists of four stages, the output of each stage being the input to the next stage, these phases are, first, pre-processing phase, second, embedding phase, third, evaluation phase, last, extracting phase. The pre-processing procedures have two main functions, which are text and cover-image pre-processing. The text pre-processing role is represented by two sub-functions: (i) text encryption which is represented by asymmetric encryption (RSA) technology that has been used to add a new level of security by first performing encryption on the secret data prior to the embedment process. Also, the RSA technique contributes to chaotic the encrypted bits, which in turn helps the compression method to compress more as much as possible. (ii) Huffman compression technique is the second pre-process technique that has been used to compress the encrypted secret data to improve the payload of the stego image. Cover image pre-processing is the second function of the pre-processing function; in this function, image randomization was used to partition the chosen cover image into four portions before inserting the previously configured secret data. Later, the proposed LSBPA was used to dynamically (randomly) embed the pre-processed secret bits into the divided cover image to create the stego- image (which should looks like the original image).



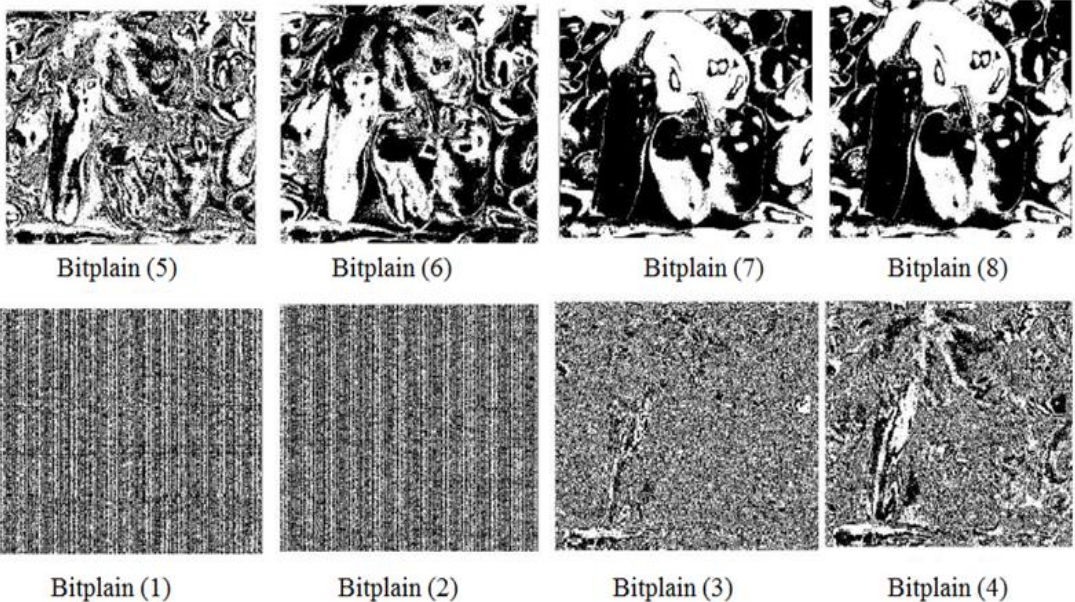
**Figure 4.7:** The use of various methods of the proposed image steganography scheme

The subsections which follow describe the relevant key issues (Human Visual System Attack, Imperceptibility, and Robustness) for the proposed system, which are supported by tables and figures. The present study was compared to existing work and experimentally demonstrated to be immune to any type of attack aimed at retrieving incoming sensitive data.

#### 4.4.1 Human Visual System Attack (HVS)

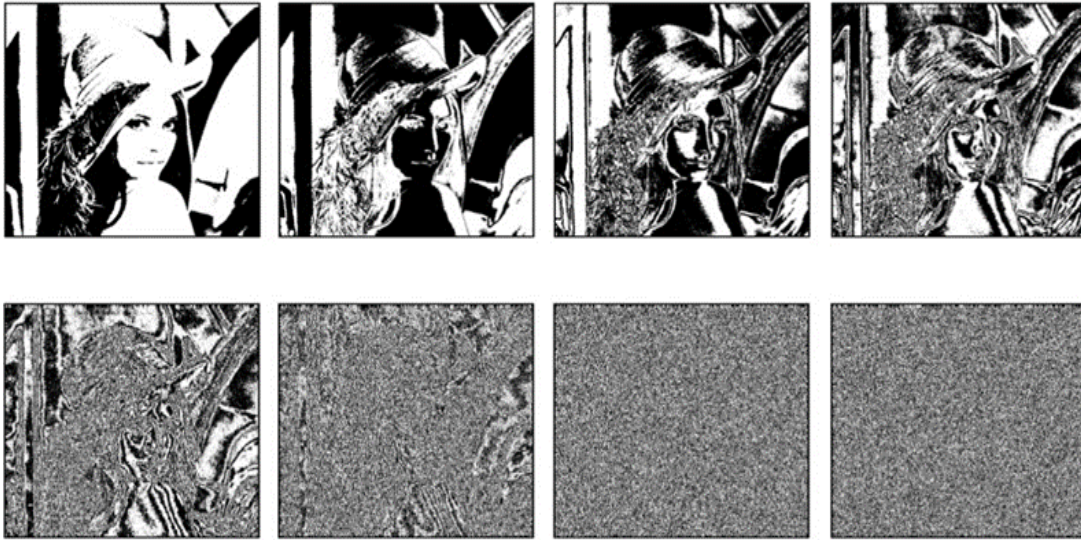
The LSB is the most embedding method used to conceal secret bits in a cover image owing to the impossibility of the human eyes to recognize the stego image pixels while using the LSB method [5]. The replacement of the cover image's LSB values by the secret bits' values makes it difficult for the system to distinguish the LSB and randomize the bits. However, edges can be detected by a system when it becomes blurred or unclear. Consequently, the HVS attack can be

detected by the LSB, and this is still ambiguous to the human sight because it is trained to recognize the known things. The idea behind the HVS attack is to remove the important information represented as the cloud formation. This information does not belong to the LSBs that are located in the MSBs. In this case, the human eye now can distinguish the presence or absence of the hidden data, as shown in Figure 4.8 (pepper image) and 4.9 (Lina image).



**Figure 4.8:** The demonstration of the visual attacks with different bit planes for the Pepper image

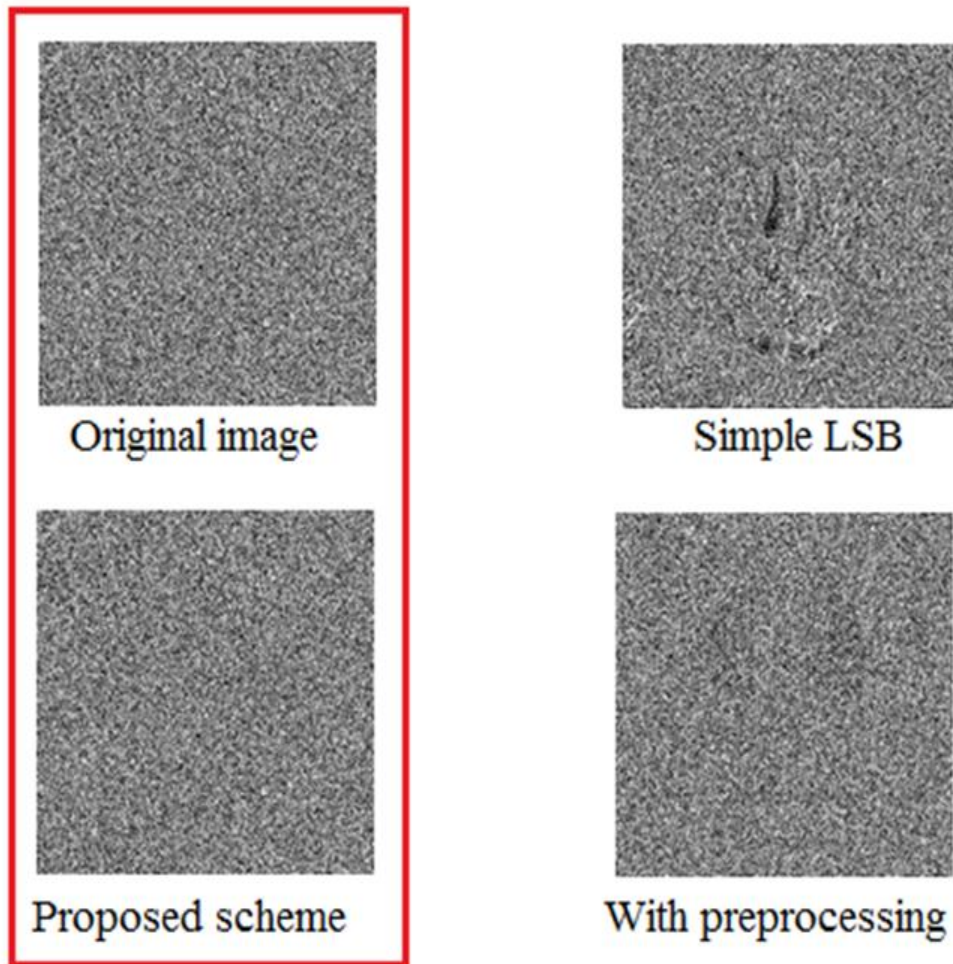




**Figure 4.9:** The demonstration of the visual attacks with different bit planes for the Lina image

The eight-bit planes HVS attack can detect only the LSBs, and the rest are ignored. In Figure 4.14, embedding in the bit planes (1 and 2) is very clear, where the vertical lines refer to the frequencies in their bits, meaning that the secret data is hidden in those 2 pixels. This form of detection is somewhat interactive between the human and the system since the system generates the detected pattern by the human eyes. Therefore, it is an example of the poor embedding method that illustrates the working principle of the HVS attack. To test the efficiency of the proposed system, three methods were applied to the selected images to make it easy to determine the differences when compared. Figure 4.10 depicts these three methods, including the simple LSB, with pre-processing and the proposed LSBPA method.



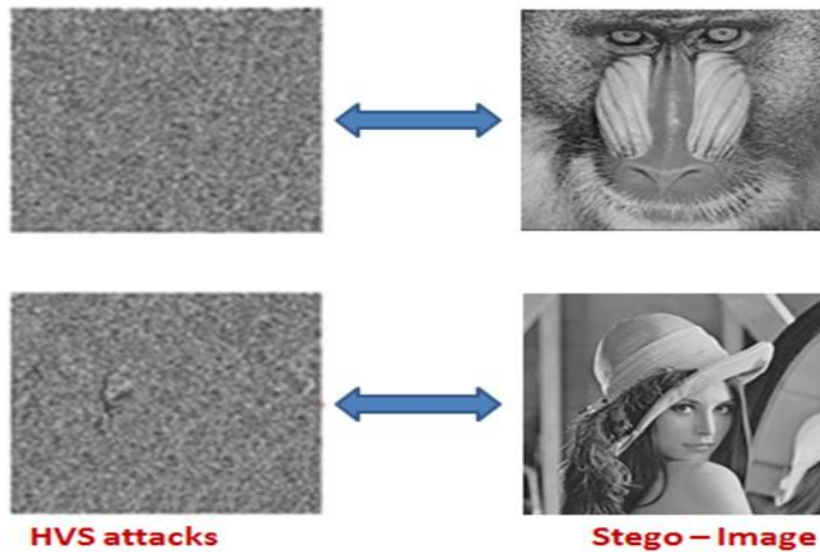


**Figure 4.10:** The performance metrics of the proposed LSBPA method vs HVS attack for the original gray-scale baboon image

It is observed (Figure 4.10) that the embedment of the simple LSB images is not good because it can easily be detected by the HVS due to the insertion of the secret bits directly without manipulation or choosing the bit position. While using the proposed scheme, the values of the secret bits during the embedding process in the pixels will be worthy in terms of the HVS and robustness, where the robustness is reflected in the security of the system. The worthiness of the developed system can also be evidenced by the results that are very close to the original image.

In short, the proposed scheme (Figure 4.11) produced more similar outcomes (after embedding) to the original image (before embedding) than the other methods due to the arbitrary distribution

of the bits. Moreover, it kept the values of the stego image bits identical by mapping the secret bits before embedding. For the training of the scheme, various SIPI database images were used to keep sure that the proposed scheme was worthy. The results were convincing, as displayed in Figure 4.15. This training was for the bit plane (1) of the LSBs, and the results were almost identical to the original image. The HVS attack is of two categories, where the first one is the filter working in the frequency domain, and the second one is the filter working in the spatial domain, which signifies the degree of occupation of the image bits by the embedded data. This type of attack works on certain regions of the stego image but is occluded by other parts of the scene represented by the secret bits. Therefore, this kind of test does not remove the mask from an image but makes it clear to the human eyes.



**Figure 4.11:** The bit plane (1) of the Baboon and Lina SIPI database images with the proposed LSBPA method

#### 4.4.2 Image Visual Quality (Imperceptibility)

Image hiding systems aim to conceal the secret bits to the cover image with different methods and schemes. So, one of the most important key issues and strengths of hiding systems is the visual image quality (imperceptibility); this ensures that stego images (image after embedding) with high imperceptibility remain unrecognized by the HVS or via the statistics [4], [121].

The imperceptibility can be determined by the PSNR, which can be defined as the ratio between a given maximum signal and the corrupted image after the embedment. After the embedding, the stego image can host the secret bits and cause some distortions. However, this corruption is almost inconceivable, especially by the human eyes [73]. The real goal is to ensure the stego image resembles the original image as much as possible. In the proposed scheme, the embedding process used a special condition to keep the visibility of the stego image after hiding secret bits almost identical to the original one using the following scenario:

The secret bits (after the pre-processing) will be fragmented into 64 bits. At this point, 64 bits (from the original image) will be replaced by 64 bits (from the secret bits). Before swapping the cover image bits with that of the secret bit, there will be a check for the match between both bits; if the number of bits that match is below the number that mismatched, the secret message bits is swapped (flip the secret message) and embedded, else, embed the secret bits directly.

During embedding, the most important aspect of the embedment method is to locate the pixel where the secret message will be embedded [122]. This requires finding and locating the location of the embedding process. Furthermore, the correct approach for determining the whole trajectory must be discovered so that the proposed method cannot be tracked by anyone except the partner or receiver. For each steganography design, the major purpose is to provide an unpredictable path for the selection of the pixel. The statistical measure of imperceptibility distinguishes the stego and secret messages from the original image. The PSNR is a metric that is used to assess the image quality after it has been embedded. It is defined as:

$$PSNR = 10 \cdot \log_{10} \left( \frac{MAX_1^2}{MSE} \right) \quad (4.6)$$

with

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j)]^2 \quad (4.7)$$

Where  $MAX$  is the image's maximum possible pixel value;  $m$  and  $n$  are the image's dimensions; and  $I$  and  $K$  are the original and noisy pixels.

The PSNR value is negatively affected by the Mean Square Error (MSE). The PSNR parameters allow equation normalization for all techniques and image formats. Three types of embedding procedures were used with various embedding capacities to evaluate the proposed scheme; these include simple LSB, scheme with pre-processing, and embedding using the Bit Swapping Approach (LSBPA) method.

Tables 4.1, 4.2, 4.3, and 4.4, as well as Figures 4.3, 4.4, 4.5, and 4.6, showed the gray-scale SIPI database results of Lina, Baboon, Pepper, and Zelda images. Figure 4.2 shows various images of the SIPI database.



**Figure 4.12:** Lina, Baboon, Pepper, and House USC-SIPI database images

**Table 4.1:** The PSNR value of the Lena Gray-Scale Image using various embedding capacities (EC)

EC (Byte)	PSNR (dB)		
	Simple LSB	With Pre-processing	Proposed Scheme
16384 Bytes	65.948	62.843	75.9936
32768 Bytes	59.999	57.110	72.914
49152 Bytes	56.001	59.819	69.0993

**Table 4.2:** The PSNR value of the Baboon Gray-Scale Image using various embedding capacities (EC)

EC (Byte)	PSNR (dB)		
	Simple LSB	With Pre-processing	Proposed Scheme

16384 Bytes	67.101	63.343	76.0214
32768 Bytes	61.419	57.990	72.9054
49152 Bytes	56.701	51.902	69.1149

**Table 4.3:** The PSNR value of the Pepper Gray-Scale Image using various embedding capacities (EC)

EC (Byte)	PSNR (dB)		
	Simple LSB	With Pre-processing	Proposed Scheme
16384 Bytes	66.121	62.185	76.0273
32768 Bytes	58.216	57.288	72.8883
49152 Bytes	56.110	59.276	69.1054

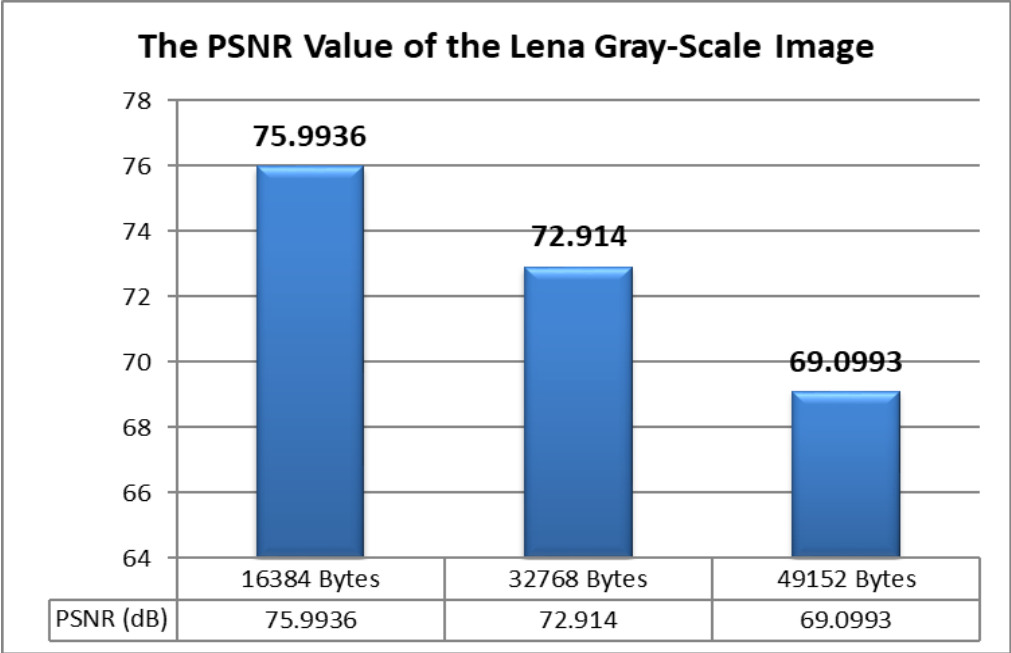
**Table 4.4:** The PSNR value of the House Gray-Scale Image using various embedding capacities (EC)

EC (Byte)	PSNR (dB)		
	Simple LSB	With Pre-processing	Proposed Scheme
16384 Bytes	65.001	61.999	76.0636
32768 Bytes	58.977	57.982	72.9238
49152 Bytes	55.998	59.001	69.1795

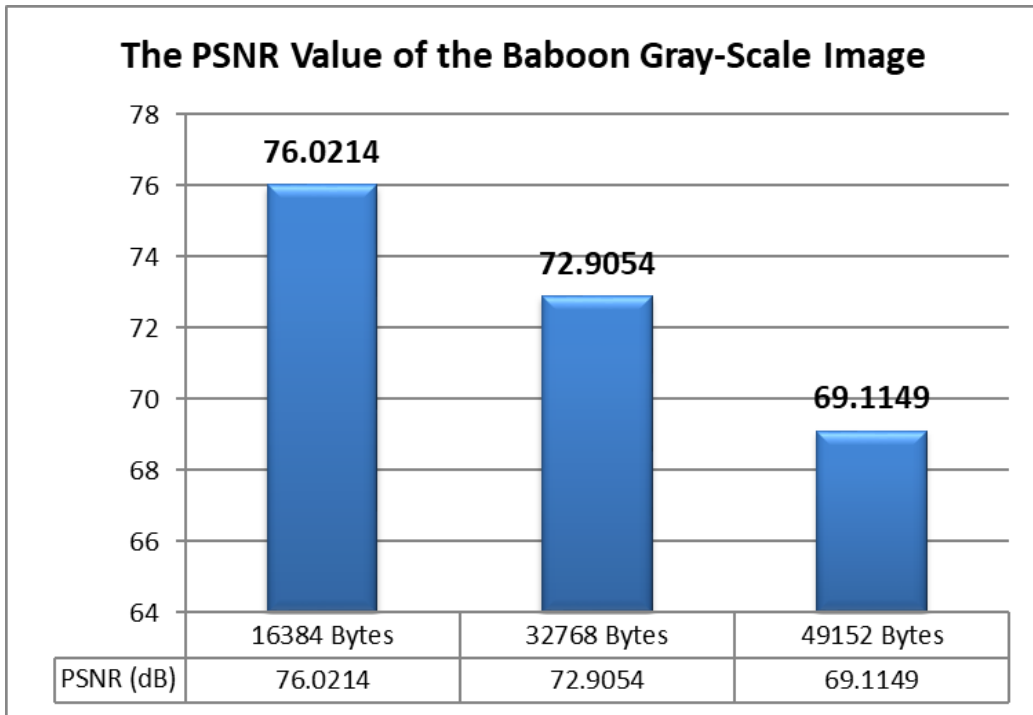
The tables 4.1, 4.2, 4.3, and 4.4 above show the PSNR ratios that can be reached by hiding the secret text inside the cover image. As we've already said, the image as a cover object has a lot of redundant bits, so it can hide as much secure data as possible.

The PSNR values differ from image to image, and the reason for this is that each cover image includes unique recursive data. The tables above illustrate many types of PSNR values (LSB simple, with preprocessing, and preprocessing method). The embedding capacity was lowered when only the simple LSB methodology was used, due to the usage of concealing without preprocessing methods such as compression, encryption, and image manipulation. Hiding secret data with the proposed LSBPA hides more data because there is an integrated concealing strategy that utilizes other technologies such as RSA encryption technology, Huffman coding, and Knight Tour technology.

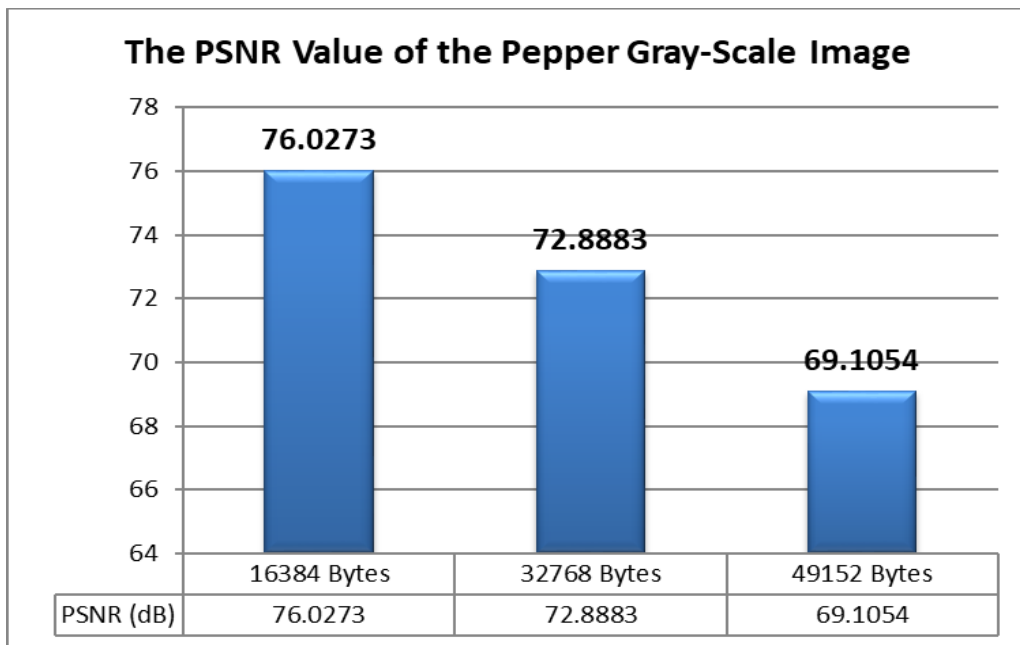
For more understanding, the achievements that have been made utilizing the proposed LSABA with different cover images are listed below with figures 4.3, 4.4, 4.5, and 4.6.



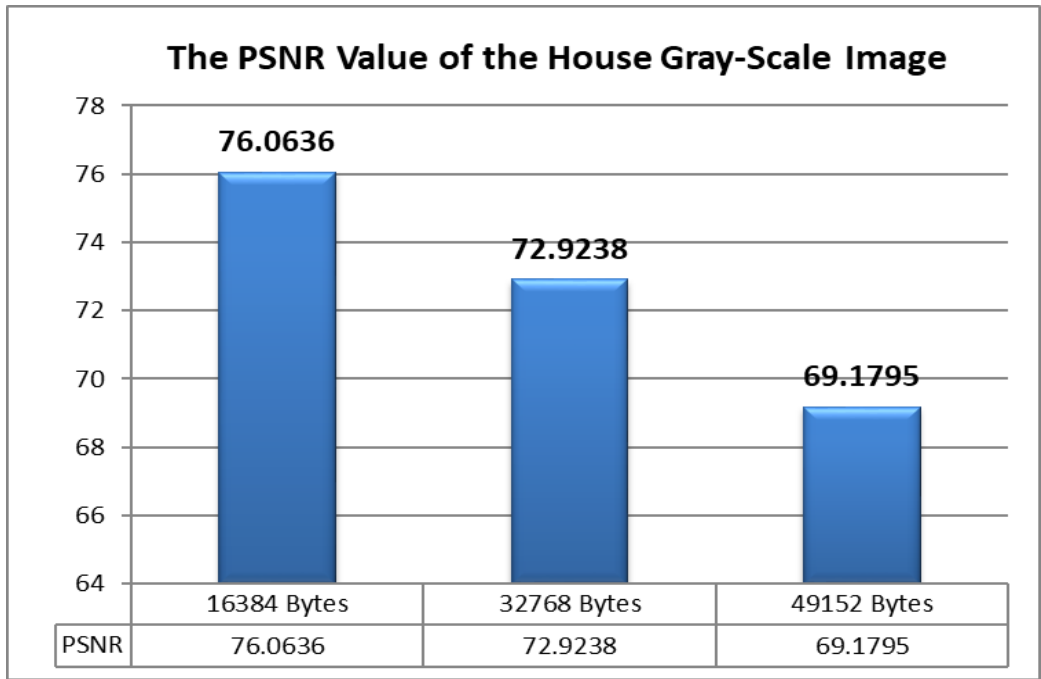
**Figure 4.13:** The PSNR value of Lina image



**Figure 4.14:** The PSNR value of Baboon image



**Figure 4.15:** The PSNR value of Pepper image



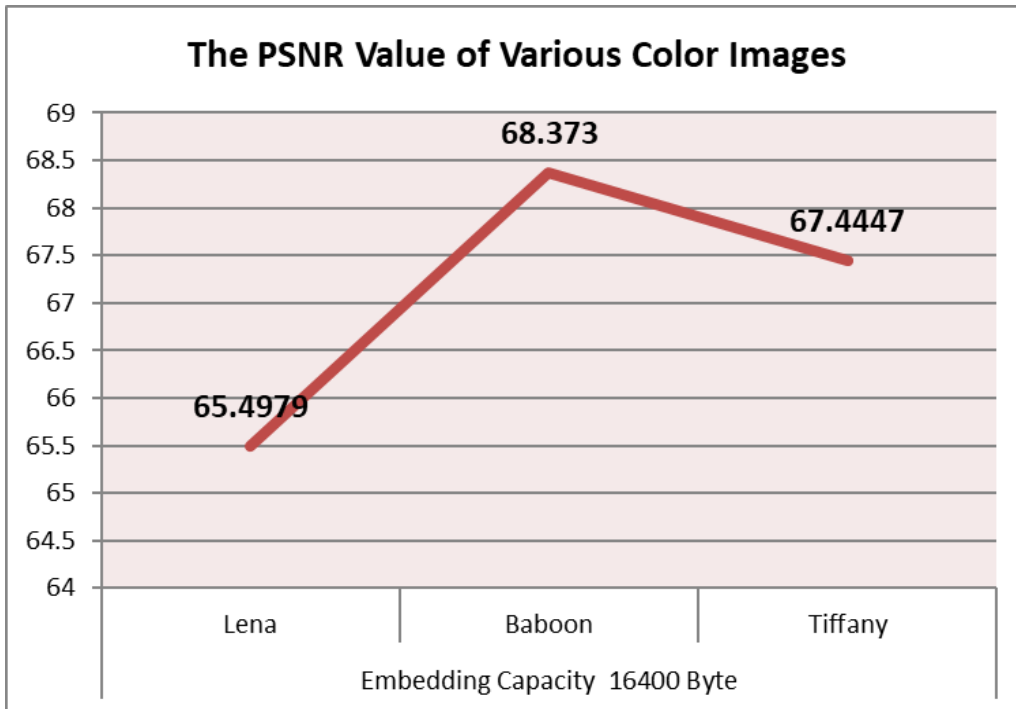
**Figure 4.16:** The PSNR value of House image

Color images normally present lower PSNR values compared to those in gray-scale because of the pixel representation of the color image; color images have 24-bits per pixel representation while that of gray images is 8-bits per pixel. This implies that there is only one byte per pixel for gray images and three bytes per pixel for color images. Figures 4.7, 4.8, 4.9, and 4.10 are graphical presentations of the different PSNR values for different embedding capacities. Tables 4.5, 4.6, 4.7, and 4.8 also depicted the color results.



**Figure 4.17:** Lina, Baboon, Pepper, and Tiffany color USC-SIPI database images





**Figure 4.18:** The PSNR value of different colour images with 16400 Bytes

As mentioned, the PSNR increased when reducing the payload capacity of the secret bits and vice versa. The results of PSNR with the pre-processing methods (RSA, Huffman, and Image normalization) are higher than simple LSB embedding because the secret bits and the selected cover have been manipulated, which contributed to the increased PSNR value. Better results were obtained with the proposed LSBPA method that was used along with the text and image pre-processing approach.

The SIPI database images obviously had varying PSNR results owing to the variations in the pixel density per image. The properties of the Baboon image are different because of its multi-color; this implies that the image has numerous densities per pixel. Being that the proposed LSBPA method is reliant on the pixel density differences, the image is expected to hold more bits than the other images that have soft areas (areas without sharp contrast).

This study aims to minimize the distortion between the stego and cover image; since the PSNR (that measures the distortion of image) depends on MSE, this error comes from the difference of checking each cover image pixel with the corresponding stego image pixel. While the

difference is located down the equation of the PSNR and power to (2) mean square, which means it is inversely proportional, this relation makes changing of pixels values worthy and should be considered. The proposed LSBPA method took care of pixels changes and made it as little as possible.

Hackers are always using statistical methods for checking the stego image; so, considering this issue is necessary and inevitable. During the process of embedding, the intensity of the pixels value (pixels while embedding the secret bits) must be less changing in the frequency to improve the image imperceptibility represented by PSNR. However, the existing methods are looking for a technique to reduce the change in an image while embedding fewer amounts of data to it (low payload). In the proposed scheme, better imperceptibility was achieved using RSA encryption and Huffman compression methods for the secret message before embedding to make the stego images carry enough number of secret bits.

From another point of view, getting a high PSNR image steganography system implies that the hidden secret data should not be noticed by the HVS. Hence, there are two scenarios of increasing the imperceptibility of any designed system, which are: first, hiding little secret bits into the cover image; second, the designed embedding scheme in this work itself affects the bits normalization in the pixels of a selected image. We can conclude that imperceptibility is synonymous with PSNR; thus, this section will focus on the two methods used for the evaluation of imperceptibility (PSNR and HVS).

#### **4.4.3 Robustness**

Robustness is commonly measured in the image steganography transform domain, but nowadays, several schemes of image steganography spatial domain are considered during the creation or design of embedding methods. Robustness implies the capability of the stego-image to keep the secret bits even when processed or manipulated by various image processing operations such as noise addition, sharpening, cropping, blurring, and noise addition.

The nature of any image steganography system/scheme can breakdown under various kinds of statistical or non-statistical attacks. The proposed scheme tries to break the behaviour of the

normal cover image structure that consists of pixels (each of 8-bits), where most of the embedding methods fall in the LSB of 8-bits. Due to the expected form of the pixels, many statistical attacks can predict the existence of a secret bit within the image. An enhanced method called LSBPA was used in this work to enhance the robustness of the developed steganography scheme, as depicted in Figure 4.16.

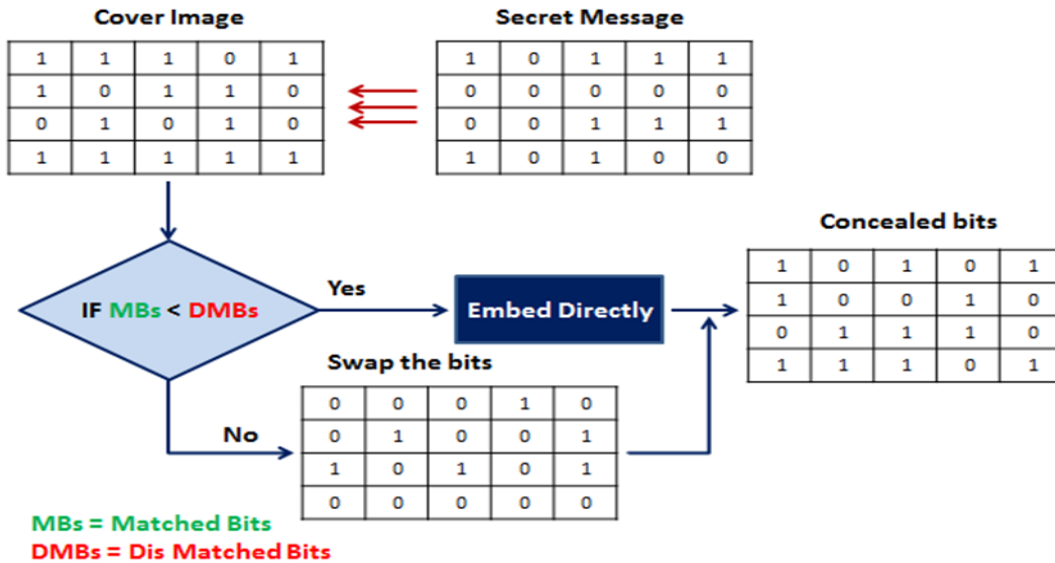


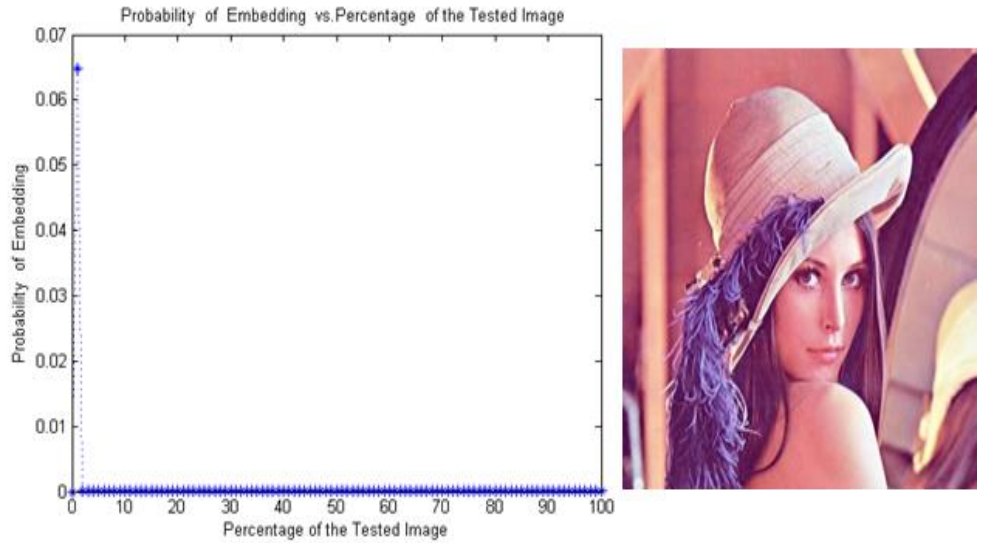
Figure 4.19: The idea of the proposed LSBPA method

The use of the proposed embedding method can confuse the statistical (objective) attacks since the LSB bits are less affected after the embedding process. Table 4.5 shows the statistical attacks (MSE, SSIM, and NCC) that have been obtained from the use of the proposed LSBPA embedding method.

**Table 4.5:** The MSE, SSIM, and NCC evaluations metrics for various gray-scale SIPI images

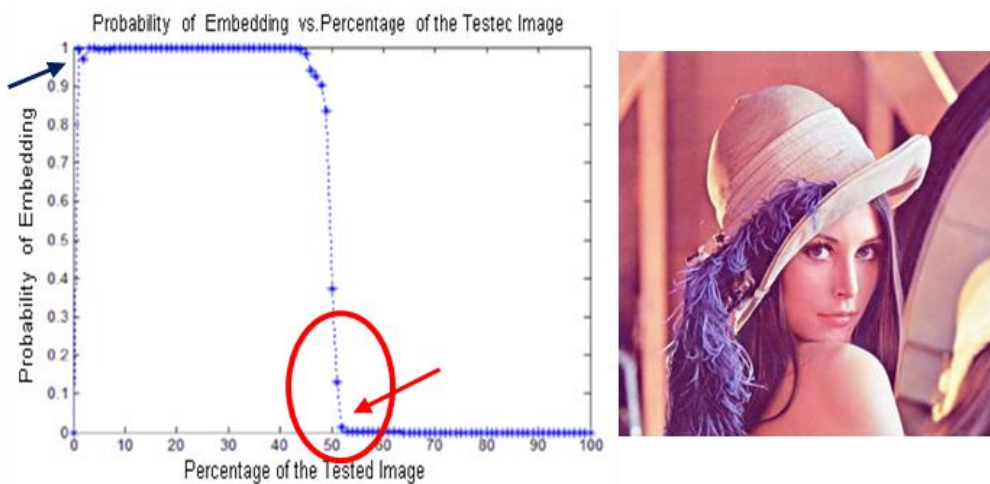
Grayscale	16384 Bytes			32768 Bytes			49152 Bytes		
	MSE	SSIM	NCC	MSE	SSIM	NCC	MSE	SSIM	NCC
<b>Lina</b>	0.0146	1	1	0.0155	0.999	0.987	0.0188	0.987	0.967
<b>Gray-Scale</b>	16384 Bytes			32768 Bytes			49152 Bytes		
	MSE	SSIM	NCC	MSE	SSIM	NCC	MSE	SSIM	NCC
<b>Baboon</b>	0.0152	1	1	0.0150	0.999	0.999	0.0198	0.986	0.977
<b>Gray-Scale</b>	16384 bytes			32768 bytes			49152 bytes		
	MSE	SSIM	NCC	MSE	SSIM	NCC	MSE	SSIM	NCC
<b>Pepper</b>	0.0149	1	1	0.0176	0.999	0.988	0.0210	0.979	0.979
<b>GrayScale</b>	16384 bytes			32768 bytes			49152 bytes		
	MSE	SSIM	NCC	MSE	SSIM	NCC	MSE	SSIM	NCC
<b>Zelda</b>	0.0156	1	1	0.0203	0.999	0.999	0.0288	0.988	0.958

Even during embedment, the secret information resides in the pixels' LSB bits; hence, a sort of modification is done on the first-bit plane based on its status. After examining an image, the human eye is able to discern the systematic alterations that occurs in the first-bit plane during the embedment. Chi-square ( $\chi^2$ ) is a particular attack based on the statistical analysis of the Pairs of Values (PoVs) exchanged during the secret data embedding, which is likewise based on the probability" distribution. The  $\chi^2$  assaults can determine the chance of secret bits embedment in the stego image, given that the regular image behaves as expected. However, embedding modifies this behavior and makes it simple to estimate the order. By examining the LSB frequency in the stego image, the 2-statistical attack reveals the likelihood of embedding hidden data in the image. Figure 4.17 showed the  $\chi^2$  test for the original color Lina image before embedding any secret bits.



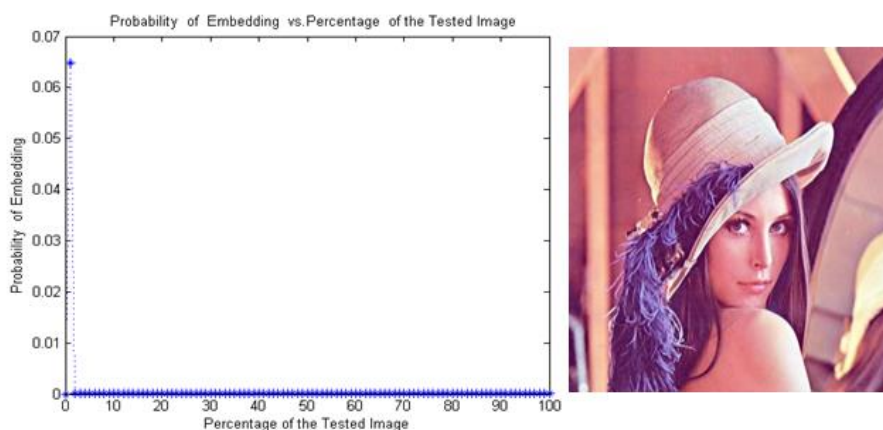
**Figure 4.20:** The  $\chi^2$ -test for the original Lina image.

The x-axis represents the percentage of the whole image, while the y-axis shows the probability of hiding the secret bit in the image (Figure 4.14). In the first 10%, the probability is 0.065 because when the function checks the pixels, most of the characters in the alphabet start with the same value as the frequent bits. Thus, the test detects this frequently and suggests these pixels as the embedded data. For the rest of the images, there is no detection for the embedding, and this is normal because the original image does not have any hidden data. Thus, after embedding the 16384 bytes to the image, different methods generate different results. Figure 4.18 showed a simple LSB method where the  $\chi^2$ -test detects 50% (red arrow) of the image as the hidden data with probability the reaching 1 (blue arrow).



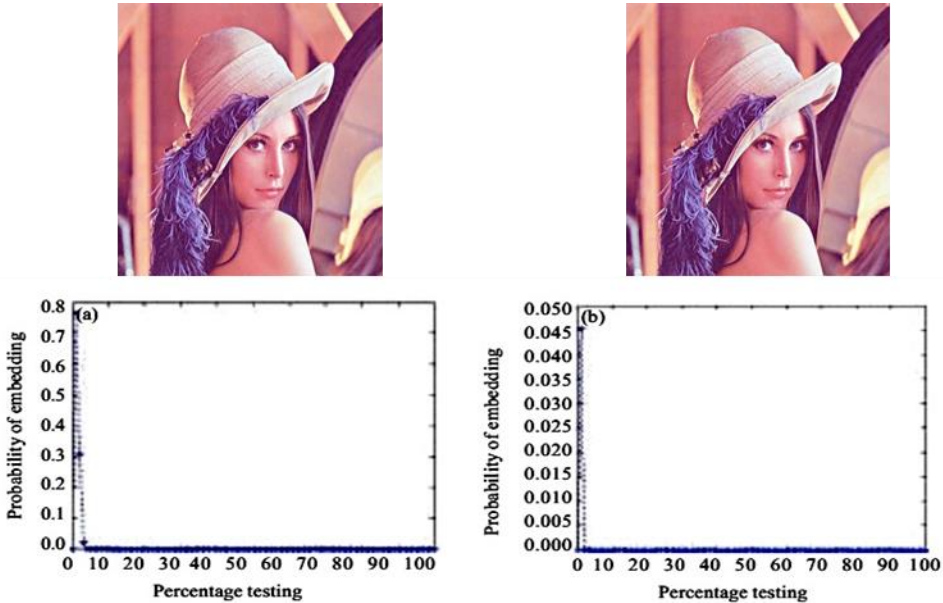
**Figure 4.21:** The  $\chi^2$ -test for the simple LSB method with embedded 16384 pixels

The simple LSB method is easy to detect by the  $\chi^2$  test, but the image cannot be recognized by the naked eye. For this reason, the proposed system considered the statistical analysis to embed the secret bits. By checking the bits before embedding, the big change of the LSB can be lowered, thereby allowing the proposed system to withstand the  $\chi^2$  attacks as shown in Figure 4.19. The behaviour of the  $\chi^2$  curves (Figure 4.19) showed that it covered the entire image with low probability even better than the original image (Figure 4.7). This is because the statistical distributions of the values in the LSB are good due to the careful selection of the segments of the secret bits. The payload also affects the  $\chi^2$  tests in the probability section.



**Figure 4.22:** The  $\chi^2$ -test for the suggested scheme after embedment of 16384 bytes

When 32768 bytes and 49152 bytes are embedded in the Lena’s image, increasing the payload also increases the degree of the probability and vice versa (Figure 4.20). Figure 4.20 (a) showed the embedding of 49152 bytes that makes the probability 0.8. The payload of 32768 bytes in Figure 4.20 (b) produced a probability of 0.045. In this case, the increase in the payload capacity is affected much by the  $\chi^2$  attacks. This is one of the positives of the developed scheme in addition to the security. The compression processes played a key role in preparing the secret data before embedding. This, in turn, made the behaviour of the  $\chi^2$  of the stego image identical to the  $\chi^2$  of the original image.



**Figure 4.23:** The embedding using the proposed system for the Lena image with (A) 49152 and (B) 32768 bytes

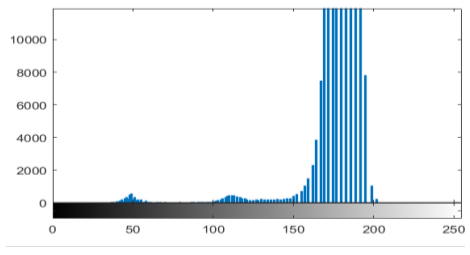
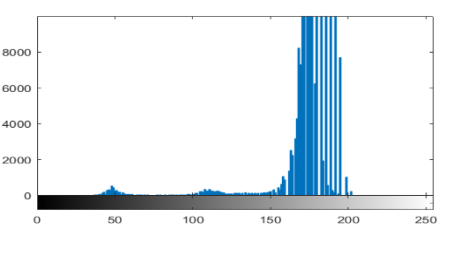
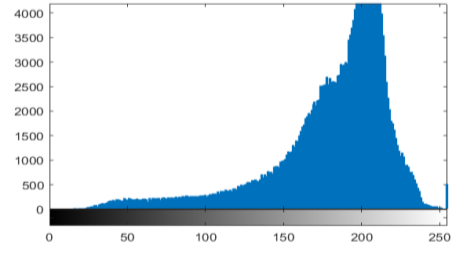
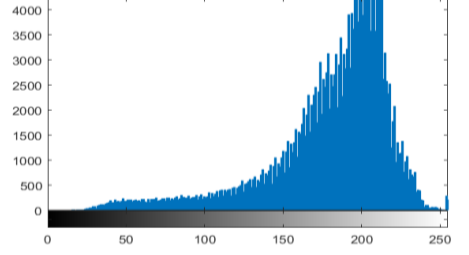
In conclusion, the  $\chi^2$  test can detect the degree of security of the system based on the embedding method. If the statistical distribution of the pixel’s value in the image is considered, then it is possible to accomplish good results. For the first part of the image, around 9% was embedded, and the test behaved as if detecting the hidden data inside, which was due to the identical frequency of all letters starting with the same bits’ value. The  $\chi^2$  relation is as follows:

$$\chi^2 = \sum \frac{(Observed - Expected)^2}{Expected} \quad (4.8)$$

#### 4.4.4 Histogram Attacks

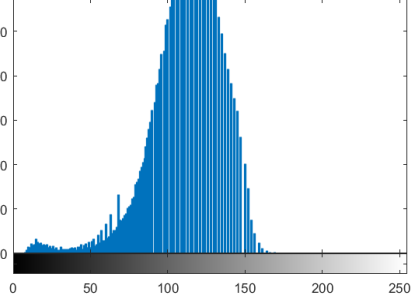
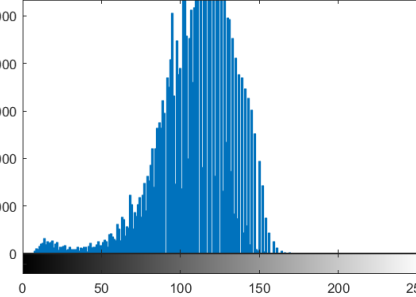
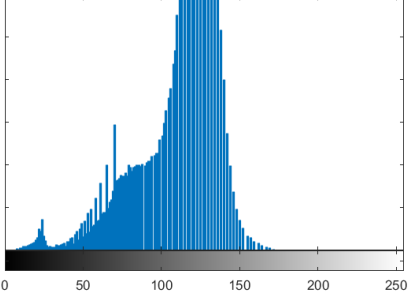
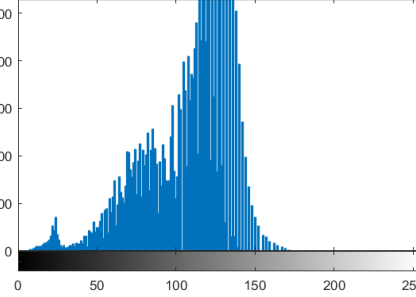
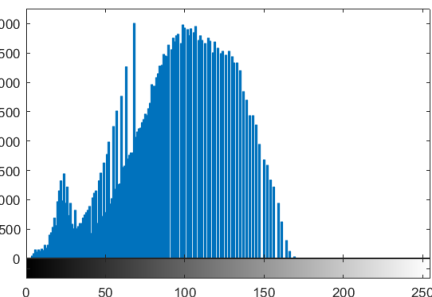
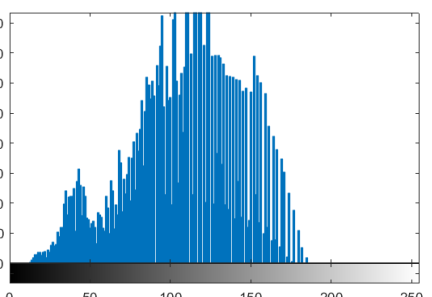
The robustness of new steganographic systems is normally tested using the histogram analysis between the cover image and the stego image [123]. The proposed study has used the histogram analysis attack to check the robustness of the embedding process using a set of grayscale images such as Lina, Baboon, Zelda, Tiffany, Airplane, and Cameraman, as shown in Figure 4.10. In general, the frequency of pixels' values will be changed after the secret bits have been embedded in the cover image and can become perceptible in the histogram analysis. Table 4.9 presents the frequency histogram of the cover images (original images) and the stego images. As shown in the histogram's analyses, the constructed histograms differed less comparatively for the considered images. The results outlined in Table 4.10 and image 4. \$\$\$ showed the differences in the constructed histograms for the cover and stego images which can be clearly noticed by the naked eyes.

**Table 4.6:** The histogram attacks of various SIPI database images with 16384 bytes of embedding capacity

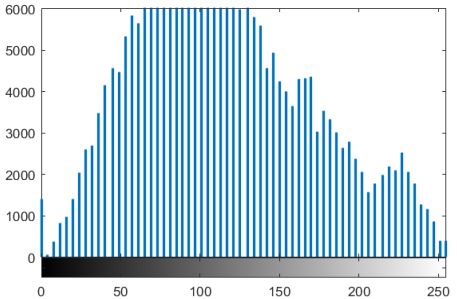
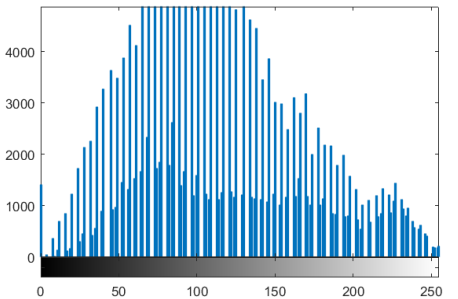
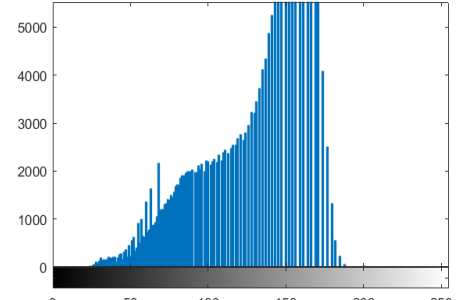
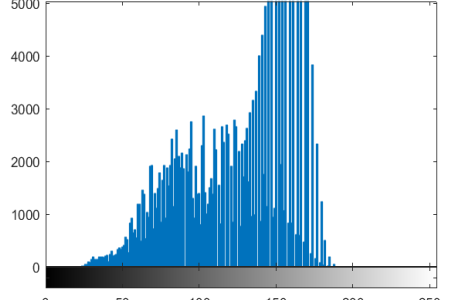
Image Name	Original Image Histogram	Stego Image Histogram
Lina		
Baboon		

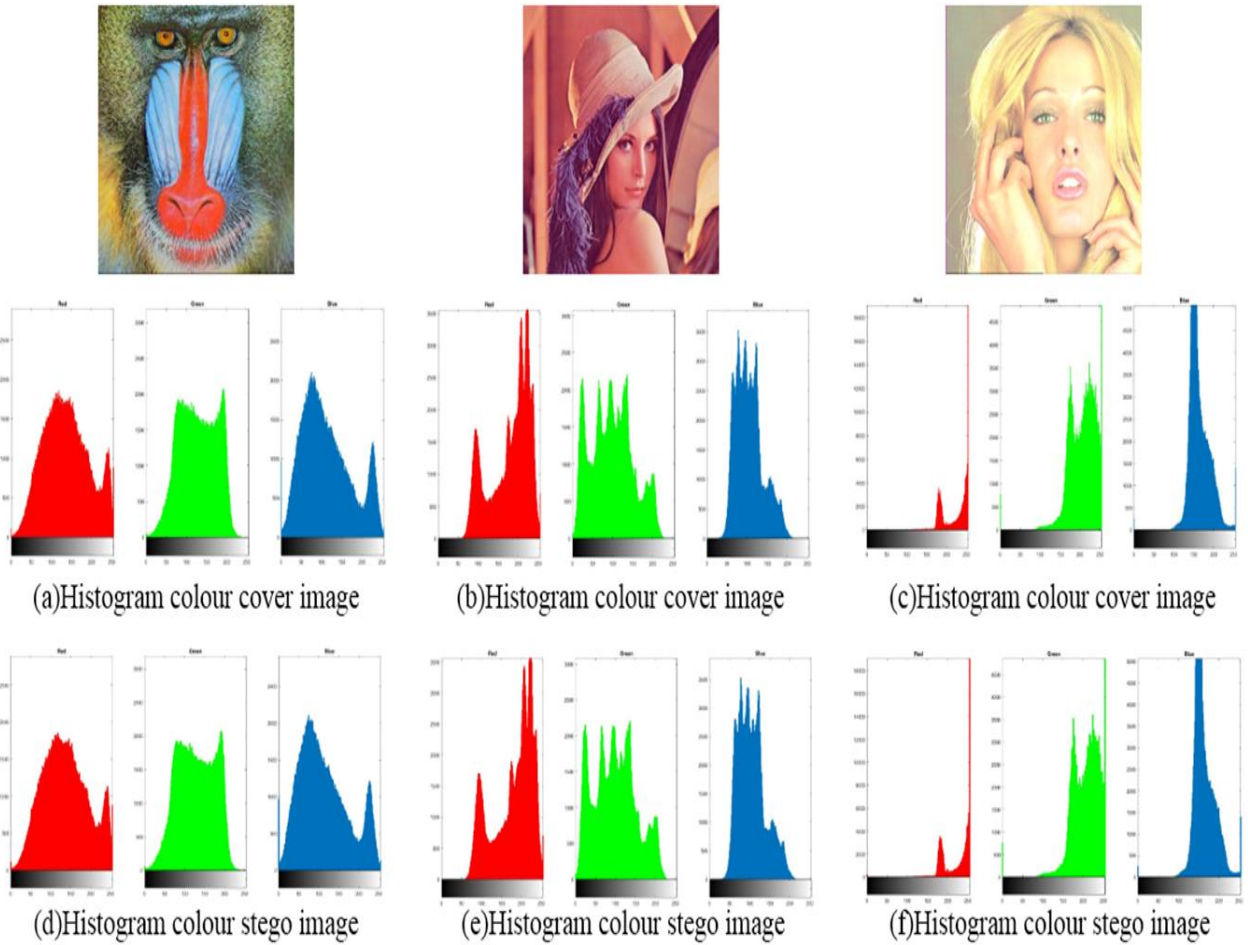


**Table 4.6:** The histogram attacks of various SIPI database images with 16384 bytes of embedding capacity “Tables continued”

Image Name	Original Image Histogram	Stego Image Histogram
<b>Pepper</b>	 <p>The original histogram for the Pepper image shows a very sharp and narrow peak centered at an intensity of approximately 120. The y-axis represents frequency, ranging from 0 to 5000, and the x-axis represents intensity from 0 to 250.</p>	 <p>The stego image histogram for the Pepper image shows a broader peak centered at the same intensity of approximately 120. The distribution is significantly wider than the original, indicating that the embedding process has introduced noise or spread into the intensity values.</p>
<b>Tiffany</b>	 <p>The original histogram for the Tiffany image shows a peak centered at an intensity of approximately 120. The distribution is broader than the Pepper image, with a y-axis ranging from 0 to 5000.</p>	 <p>The stego image histogram for the Tiffany image shows a peak centered at an intensity of approximately 120, which is broader than the original histogram, indicating the effect of the embedding process.</p>
<b>Airplane</b>	 <p>The original histogram for the Airplane image shows a broad peak centered at an intensity of approximately 120. The y-axis ranges from 0 to 4000.</p>	 <p>The stego image histogram for the Airplane image shows a peak centered at an intensity of approximately 120, which is broader than the original histogram, indicating the effect of the embedding process.</p>

**Table 4.6:** The histogram attacks of various SIPI database images with 16384 bytes of embedding capacity “Tables continued”

Image Name	Original Image Histogram	Stego Image Histogram
<b>Cameraman</b>	 <p>The histogram shows the frequency distribution of pixel intensities for the original Cameraman image. The x-axis represents pixel intensity from 0 to 255, and the y-axis represents frequency from 0 to 6000. The distribution is roughly bell-shaped, peaking around 100-150 intensity.</p>	 <p>The histogram shows the frequency distribution of pixel intensities for the Cameraman image after embedding 16384 bytes. The distribution is very similar to the original, with a peak around 100-150 intensity, indicating that the embedding process has not significantly altered the overall histogram.</p>
<b>Zelda</b>	 <p>The histogram shows the frequency distribution of pixel intensities for the original Zelda image. The x-axis represents pixel intensity from 0 to 255, and the y-axis represents frequency from 0 to 5000. The distribution is skewed towards higher intensities, peaking around 150-200 intensity.</p>	 <p>The histogram shows the frequency distribution of pixel intensities for the Zelda image after embedding 16384 bytes. The distribution is very similar to the original, with a peak around 150-200 intensity, indicating that the embedding process has not significantly altered the overall histogram.</p>



**Figure 4.24:** The Histogram distribution of the original RGB Baboon image (c, d and e) versus stego RGB Baboon image (f, g and h) with (16400 EC bytes)

#### 4.5 RESULT'S BENCHMARKING

In this section, the achieved results were compared with various studies using deferent of the statistical evaluation metrics. Table 4.11 expressed the benchmark of the current results with the existing literature review for Baboon grey scale image.

**Table 4.7:** Expressed the benchmark of the current results with the existing literature review for Baboon gray-scale image with 32768 Bytes

The current results			[2]			[3]			[124]		
PSNR	NCC	SSIM	PSNR	NCC	SSIM	PSNR	NCC	SSIM	PSNR	NCC	SSIM
72.9111	0.999	0.999	58.22	0.9994	0.981	51.22	0.8999	0.968	50.21	0.8998	0.957

#### 4.6 DISCUSSION

The results of the experiments using the proposed LSBPA method were discussed and analysed in this chapter. Various objective and subjective attacks were tested and presented with different payload capacities. Many tables and figures were presented to depict the findings of the analyses in terms of payload capacity, imperceptibility, robustness, and HVS. Other evaluation metrics were also used to evaluate the proposed system, such as NCC, SSIM, and MSE. Also, this chapter described the PC requirements for the implementation of the system codes to get the stated results. Finally, the achieved results in this work were benchmarked with state-of-the-art studies.

## **5. CONCLUSION AND FUTURE WORK**

### **5.1. INTRODUCTION**

Image steganography is described as the art and science of concealing information by inserting secret bits in a trusted cover image without raising suspicion. Recently, many steganographic approaches have been proposed (Kadhim et al., 2019; Meng et al., 2021; L. Tang et al., 2021), However, the problem of low security and poor visual quality (imperceptibility) after hiding information using such methods remains unsolved (Mukherjee et al., 2020). Considering these problems, this study proposed an enhanced method to embed the secret message into an image in a manner that cannot be detected by intruders or hackers. The proposed method can withstand any kind of attacks, objective, and subjective attacks, such as HVS attacks or chi-square attacks.

Three primary evaluation criteria were considered in the proposed study: security, imperceptibility, and robustness. The security ensures the absolute protection of the sensitive data that is embedded and hidden in the cover image. The imperceptibility of steganographic systems signify the briefness of the stego image enclosing the secret data and its closeness to the original image without any sign of detecting the existence of the hidden data. The robustness of the steganography system reflects its rigged and protective strength from any attack. The key steps of any stenographic procedure are, in general, the pre-processing, embedding, testing, and extraction stages, as explained below. The proposed scheme addressed all the limitations of the current methods and outperformed them in terms of effectiveness.

### **5.2. THE PRE-PROCESSING STAGE**

Two significant processes are being successfully obtaining at this stage to improve the proposed scheme. The first step involves creating the secret text, while the second step involves randomizing the cover images. Text pre-processing is indeed divided into two stages: text encryption and text compression. The RSA approach was utilized in the first stage to provide an extra security layer and to increase the redundancy of encrypted characters. In the second function, the Huffman algorithm was used to compress encrypted secret data to reduce the amount of data contained in the image, hence improving the capabilities of the steganographical

system by eliminating redundant characters in the secret message. Additionally, this step increases the system's robustness, as the attacker cannot easily fully understand this parsing format

The second phase (image randomization) occurs prior to the embedding stage; the image randomization stage would be just as critical as the text processing stage, as the combined work of these two stages produces superior outcomes. The selected image must be divided into four blocks using the Knight Tour technique, with randomly selected pixels from each block. The RGB channels were then analyzed and transformed to YCbCr channels to improve the proposed scheme's security and robustness.

### **5.3. THE PROPOSED LEAST SIGNIFICANT BIT PERMUTATION APPROACH**

In the literature, most embedding methods directly embed secret bits in LSBs of the cover image which means that the embedding process is not robust. Therefore, the proposed embedment scheme partitions the cover image adaptively into four blocks using Knight Tour algorithm and LSBPA method to hide the secret bits in the elected cover image using an explicit key (stego key) to carry the whole embedding processes to the recipient for extraction using the stego key.

The concealing procedure in the proposed system hides the secret text after the steps of preparing the secret text and preparing the cover image. The secret bits after the pre-processing stage will be fragmented into 64 bits. At this point, 64 bits (from the image) will be replaced by 64 bits (from the secret bits). Before swapping the cover image bits with that of the secret message, there will be a check for the match between both bits; if the number of bits that match is less than the mismatched bits, the secret message bits is swapped and embed, else, embed the secret bits directly.

### **5.4. EVALUATION METRICS**

The evaluation of the developed scheme was done based on certain objective and subjective evaluation metrics; the considered objective metrics are Chi-square(X<sup>2</sup>), PSNR, MSE, NCC, and histogram, while the subjective metric is HVS. The extent of normalization of the bits inside the embedded image was checked via objective evaluation metrics/attacks works based on the

LSB frequencies of the stego image and statistical issues. Hence, the proposal for the LSBPA in this study was based on statistical calculations. The outcome of the evaluations proved the robustness of the suggested scheme against the utilized types of attacks.

## **5.5. FUTURE WORK SUGGESTION**

A major gap in the image steganography systems is the balance between the payload capacity and the other evaluation metrics like security and robustness. The large value of the embedding capacity means less PSNR value which in turn means weak image steganography systems. Therefore, it is recommended to pre-process the secret message and cover image before the embed step, as well as design a dynamic embedding method that randomly hides the secret text.

This study aimed at achieving certain objectives, which were duly achieved; however, perfect, personalized results have not been achieved and require further studies. One of the recommended directions for future studies is to enhance the robustness of the suggested scheme by initializing the cover image and secret text before the embedding process. The design of new, lightweight encryption or compression techniques to encrypt and compress secret bits helps increase the security and robustness of image concealing systems.

Furthermore, the security and robustness of the system can be enhanced by merging the frequency-domain and spatial domain techniques. The proposed LSBPA method in this work can also be combined with the DWT method to achieve high coefficients based on the design framework in Chapter 3.

## REFERENCES

- [1] A. Das, J. S. Wahi, M. Anand, and Y. Rana, ‘Multi-Image Steganography Using Deep Neural Networks’, *arXiv preprint arXiv:2101.00350*, 2021.
- [2] I. J. Kadhim, P. Premaratne, and P. J. Vial, ‘High capacity adaptive image steganography with cover region selection using dual-tree complex wavelet transform’, *Cogn Syst Res*, vol. 60, pp. 20–32, 2020, doi: 10.1016/j.cogsys.2019.11.002.
- [3] A. K. Sahu and G. Swain, ‘An Optimal Information Hiding Approach Based on Pixel Value Differencing and Modulus Function’, *Wirel Pers Commun*, vol. 108, no. 1, pp. 159–174, 2019, doi: 10.1007/s11277-019-06393-z.
- [4] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran, ‘Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research’, *Neurocomputing*, vol. 335, pp. 299–326, 2019, doi: 10.1016/j.neucom.2018.06.075.
- [5] M. Hussain, A. W. A. Wahab, Y. I. Bin Idris, A. T. S. Ho, and K. H. Jung, ‘Image steganography in spatial domain: A survey’, *Signal Process Image Commun*, vol. 65, no. December 2017, pp. 46–66, 2018, doi: 10.1016/j.image.2018.03.012.
- [6] A. H. Mohsin *et al.*, ‘Real-Time Medical Systems Based on Human Biometric Steganography: a Systematic Review’, *J Med Syst*, vol. 42, no. 12, 2018, doi: 10.1007/s10916-018-1103-6.
- [7] A. Gutub and M. Al-Ghamdi, *Image Based Steganography to Facilitate Improving Counting-Based Secret Sharing*, vol. 10, no. 1. 3D Display Research Center, 2019. doi: 10.1007/s13319-019-0216-0.
- [8] A. Anwer Abdulla, S. A. Jassim, and H. Sellahewa, ‘Efficient High Capacity Steganography Technique’, *ArXiv*, p. arXiv-2004, 2020.



- [9] A. Gutub and M. Al-Ghamdi, ‘Hiding shares by multimedia image steganography for optimized counting-based secret sharing’, *Multimed Tools Appl*, vol. 79, no. 11–12, pp. 7951–7985, 2020, doi: 10.1007/s11042-019-08427-x.
- [10] C. D. Nisha and T. Monoth, ‘Analysis of Spatial Domain Image Steganography Based on Pixel-Value Differencing Method’, in *Soft Computing for Problem Solving*, Springer, 2020, pp. 385–397.
- [11] M. N. Islam, M. F. Islam, and K. Shahrabi, ‘Robust information security system using steganography, orthogonal code and joint transform correlation’, *Optik (Stuttg)*, vol. 126, no. 23, pp. 4026–4031, 2015, doi: 10.1016/j.ijleo.2015.07.161.
- [12] K. Kordov, ‘TEXT ENCRYPTION ALGORITHM FOR SECURE COMMUNICATION’, *Int J Appl Math (Sofia)*, vol. 34, no. 4, p. 705, 2021.
- [13] K. Gurunathan and S. P. Rajagopalan, ‘A stegano-visual cryptography technique for multimedia security’, *Multimed Tools Appl*, vol. 79, no. 5, pp. 3893–3911, 2020.
- [14] S. Farrag and W. Alexan, ‘Secure 2D image steganography using recamán’s sequence’, *Proceedings - 2019 International Conference on Advanced Communication Technologies and Networking, CommNet 2019*, pp. 1–6, 2019, doi: 10.1109/COMMNET.2019.8742368.
- [15] X. Tang, H. Wang, and Y. Chen, ‘Reversible data hiding based on a modified difference expansion for H. 264/AVC video streams’, *Multimed Tools Appl*, pp. 1–14, 2020.
- [16] A. Selvaraj, A. Ezhilarasan, S. L. J. Wellington, and A. R. Sam, ‘Digital image steganalysis: A survey on paradigm shift from machine learning to deep learning based techniques’, *IET Image Process*, vol. 15, no. 2, pp. 504–522, 2021.
- [17] L. Tang, D. Wu, H. Wang, M. Chen, and J. Xie, ‘An adaptive fuzzy inference approach for color image steganography’, *Soft comput*, vol. 25, no. 16, pp. 10987–11004, 2021, doi: 10.1007/s00500-021-05825-y.

- [18] R. Rawat, B. Singh, A. Sur, and P. Mitra, ‘Steganalysis for clustering modification directions steganography’, *Multimed Tools Appl*, vol. 79, no. 3–4, pp. 1971–1986, 2020, doi: 10.1007/s11042-019-08263-z.
- [19] X. Liao, Y. Yu, B. Li, Z. Li, and Z. Qin, ‘A New Payload Partition Strategy in Color Image Steganography’, *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 30, no. 3, pp. 685–696, 2020, doi: 10.1109/TCSVT.2019.2896270.
- [20] S. Sun, ‘A novel edge based image steganography with 2k correction and Huffman encoding’, *Inf Process Lett*, vol. 116, no. 2, pp. 93–99, 2016, doi: 10.1016/j.ipl.2015.09.016.
- [21] I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, *Digital Watermarking and Steganography, Second Edition*. 2008.
- [22] F. Q. A. Alyousuf, R. Din, and A. J. Qasim, ‘Analysis review on spatial and transform domain technique in digital steganography’, *Bulletin of Electrical Engineering and Informatics*, vol. 9, no. 2, pp. 573–581, 2020.
- [23] A. Charbal *et al.*, ‘Integrated Digital Image Correlation considering gray level and blur variations: Application to distortion measurements of IR camera’, *Opt Lasers Eng*, vol. 78, pp. 75–85, 2016, doi: 10.1016/j.optlaseng.2015.09.011.
- [24] M. Das and S. K. Bandyopadhyay, ‘Survey and Analysis of Current methods of Steganography’, *International Journal of modern Trends in Engineering and Research*, vol. 2, no. 7, pp. 527–537, 2015.
- [25] J. Hou and G. Situ, ‘Image encryption using spatial nonlinear optics’, *eLight*, vol. 2, no. 1, pp. 1–10, 2022.
- [26] R. Patel, K. Lad, M. Patel, and M. Desai, ‘An efficient DCT-SBPM based video steganography in compressed domain’, *International Journal of Information Technology*, vol. 13, no. 3, pp. 1073–1078, 2021.

- [27] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, 'Digital image steganography: Survey and analysis of current methods', *Signal Processing*, vol. 90, no. 3, pp. 727–752, 2010, doi: 10.1016/j.sigpro.2009.08.010.
- [28] E. Salah, K. Amine, K. Redouane, and K. Fares, 'A Fourier transform based audio watermarking algorithm', *Applied Acoustics*, vol. 172, p. 107652, 2021.
- [29] M. A. F. Al-Husainy and D. M. Uliyan, 'A secret-key image steganography technique using random chain codes', *International Journal of Technology*, vol. 10, no. 4, pp. 731–740, 2019, doi: 10.14716/ijtech.v10i4.653.
- [30] X. Yu, K. Chen, Y. Wang, W. Li, W. Zhang, and N. Yu, 'Robust adaptive steganography based on generalized dither modulation and expanded embedding domain', *Signal Processing*, vol. 168, p. 107343, 2020.
- [31] P. Maniriho and T. Ahmad, 'Information hiding scheme for digital images using difference expansion and modulus function', *Journal of King Saud University - Computer and Information Sciences*, vol. 31, no. 3, pp. 335–347, 2019, doi: 10.1016/j.jksuci.2018.01.011.
- [32] A. A. Abd EL-Latif, B. Abd-El-Atty, and S. E. Venegas-Andraca, 'A novel image steganography technique based on quantum substitution boxes', *Opt Laser Technol*, vol. 116, no. December 2018, pp. 92–102, 2019, doi: 10.1016/j.optlastec.2019.03.005.
- [33] T. Tuncer and E. Avci, 'A reversible data hiding algorithm based on probabilistic DNA-XOR secret sharing scheme for color images', *Displays*, vol. 41, pp. 1–8, 2016, doi: 10.1016/j.displa.2015.10.005.
- [34] S. M. Thampi, 'Information Hiding Techniques: A Tutorial Review', *CoRR*, 2008.
- [35] F. Petitcolas, 'La cryptographie militaire'. 1883.
- [36] I. Banerjee, S. Bhattacharyya, and G. Sanyal, 'Text steganography using article mapping technique (AMT) and SSCE', *Journal of Global Research in Computer Science*, vol. 2, no. 4, pp. 69–75, 2011.

- [37] L. B. Muthukrishnan SenthilKumar, Vijayalakshmi Ramasamy, Shina Sheen, C Veeramani, Anthony Bonato, ‘Computational Intelligence, Cyber Security and Computational Models’, p. 586, 2016, doi: 10.1007/978-981-10-0251-9.
- [38] G. J. Simmons, ‘The Prisoners’ Problem and the Subliminal Channel’, *Advances in Cryptology, Springer-Verlag*. pp. 51–67, 1984.
- [39] G. Cancelli, G. Doërr, M. Barni, and I. J. Cox, ‘A comparative study of±steganalyzers’, in *2008 IEEE 10th Workshop on Multimedia Signal Processing*, 2008, pp. 791–796.
- [40] X. Zhang and S. Wang, ‘Steganography using multiple-base notational system and human vision sensitivity’, *IEEE Signal Process Lett*, vol. 12, no. 1, pp. 67–70, 2005, doi: 10.1109/LSP.2004.838214.
- [41] D. Dumitrescu, I.-M. Stan, and E. Simion, ‘Steganography techniques’, *Cryptology ePrint Archive*, pp. 1–20, 2017.
- [42] Z. S. Younus and M. K. Hussain, ‘Image steganography using exploiting modification direction for compressed encrypted data’, *Journal of King Saud University - Computer and Information Sciences*, no. xxxx, 2019, doi: 10.1016/j.jksuci.2019.04.008.
- [43] R. Meng, Q. Cui, Z. Zhou, Z. Li, J. Q. M. Wu, and X. Sun, ‘High-Capacity Steganography Using Object Addition-based Cover Enhancement for Secure Communication in Networks’, *IEEE Trans Netw Sci Eng*, 2021.
- [44] K. Muhammad, J. Ahmad, N. U. Rehman, Z. Jan, and M. Sajjad, ‘CISSKA-LSB: color image steganography using stego key-directed adaptive LSB substitution method’, *Multimed Tools Appl*, vol. 76, no. 6, pp. 8597–8626, 2017, doi: 10.1007/s11042-016-3383-5.
- [45] A. Odeh, A. Alzubi, Q. B. Hani, and K. Elleithy, ‘Steganography by multipoint Arabic letters’, *IEEE Long Island Systems, Applications and Technology Conference, LISAT 2012*, pp. 1–7, 2012.

- [46] Prof. Dr. T. A. Abbas, 'Steganography Using Fractal Images Technique', *IOSR Journal of Engineering*, vol. 4, no. 2, pp. 52–61, 2014, doi: 10.9790/3021-04225261.
- [47] I. Karadogan and R. Das, 'An examination on information hiding tools for steganography', *International Journal of Information Security Science*, vol. 3, no. 3, pp. 200–208, 2014.
- [48] E. N. C. Wai and M. A. Khine, 'Syntactic Bank-based linguistic steganography approach', *International Conference on Information Communication and Management*, vol., vol. 16, pp. 108–113, 2011.
- [49] A. A. Obeidat, 'Arabic text steganography using Unicode of non-joined to right side letters', *Journal of Computer Science*, vol. 13, no. 6, pp. 184–191, 2017.
- [50] P. M. Vidhya and V. Paul, 'A method for text steganography using malayalam text', *Procedia Comput Sci*, vol. 46, pp. 524–531, 2015.
- [51] M. H. Mohamed and L. M. Mohamed, 'High capacity image steganography technique based on LSB substitution method', *Applied Mathematics & Information Sciences*, vol. 10, no. 1, p. 259, 2016.
- [52] Sheelu, 'Enhancement of Data Hiding Capacity in Audio Steganography', *IOSR Journal of Computer Engineering (IOSR-JCE)*, vol. 13, no. 3, pp. 30–35, 2013.
- [53] A. S. Thorat and G. U. Kharat, 'Steganography Based Navigation of Missile', *International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)*, vol. 4, no. 6, pp. 1662–1665, 2015.
- [54] E. Bheda, C. Khubdikar, A. Patwardhan, M. Kalebere, and S. Raksha, 'Multimedia steganography with cipher text and compression', *International Journal of Emerging Technology and Advanced Engineering*, vol. 3, no. 4, pp. 322–324, 2013.
- [55] R. Kaur and M. Mahajan, 'Random pattern based sequential bit (RaP-SeB) steganography with cryptography for video embedding', *International Journal of Modern Education and Computer Science*, vol. 8, no. 9, pp. 51–59, 2016.

- [56] R. Patil and D. Pawar, 'Secure audio steganography by LSB for hiding information', *International Journal of Innovations in Engineering Research and Technology*, vol. 3, no. 4, pp. 1–6, 2016.
- [57] M. Hussain and M. Hussain, 'A survey of image steganography techniques', *International Journal of Advanced Science and Technology*, vol. 54, pp. 113–124, 2013.
- [58] H. Kaur and J. Rani, 'A Survey on different techniques of steganography', *International Research Journal of Engineering and Technology (IRJET)*, vol. 03, no. 09, pp. 1146–1151, 2016.
- [59] M. Sabry, T. Nazmy, and M. E. Khalifa, 'Steganography in DNA Sequence on the Level of Amino acids', in *2019 Ninth International Conference on Intelligent Computing and Information Systems (ICICIS)*, 2019, pp. 317–324.
- [60] B. Dunbar, 'A detailed look at steganographic techniques and their use in an open-systems environment', *Sans Institute*, 2002.
- [61] K. F. Rafat and M. Sher, 'Secure digital steganography for ASCII text documents', *Arab J Sci Eng*, vol. 38, no. 8, pp. 2079–2094, 2013.
- [62] E. Cole, *Hiding in Plain Sight : Steganography and the Art of covert communication*. 2003.
- [63] S. S. Baawi, M. R. Mokhtar, and R. Sulaiman, 'New text steganography technique based on a set of two-letter words', *J Theor Appl Inf Technol*, vol. 95, no. 22, pp. 6247–6255, 2017.
- [64] N. Jiang, N. Zhao, and L. Wang, 'LSB Based Quantum Image Steganography Algorithm', *International Journal of Theoretical Physics*, vol. 55, no. 1, pp. 107–123, 2016, doi: 10.1007/s10773-015-2640-0.
- [65] S. Chakraborty, A. S. Jalal, and C. Bhatnagar, 'LSB based non blind predictive edge adaptive image steganography', *Multimed Tools Appl*, vol. 76, no. 6, pp. 7973–7987, 2017.

- [66] A. Gambhir and R. Arya, ‘Performance analysis and implementation of DES algorithm and RSA algorithm with image and audio steganography techniques’, in *Computing, Communication and Signal Processing*, Springer, 2019, pp. 1021–1028.
- [67] K. Bennett, ‘Linguistic steganography: Survey, analysis, and robustness concerns for hiding information in text’, 2004.
- [68] R. Böhme, ‘Principles of modern steganography and steganalysis’, *Information Security and Cryptography*, no. 9783642143120, pp. 11–77, 2010, doi: 10.1007/978-3-642-14313-7\_2.
- [69] M. A. Karem M and A. S. Nori, ‘Blind Steganalysis using One-Class Classification’, *AL-Rafidain Journal of Computer Sciences and Mathematics*, vol. 13, no. 2, pp. 28–41, 2020.
- [70] D. K. Sarmah, A. J. Kulkarni, and A. Abraham, ‘Steganalysis on All Approaches/Vulnerability Analysis of Stego Image (s)’, in *Optimization Models in Steganography Using Metaheuristics*, Springer, 2020, pp. 147–161.
- [71] T. D. Sairam and K. Boopathybagan, ‘Computational intelligence-based steganalysis comparison for RCM-DWT and PVA-MOD methods’, *Automatika*, vol. 60, no. 3, pp. 285–293, 2019.
- [72] K. Bennett, ‘Linguistic steganography: Survey, analysis, and robustness concerns for hiding information in text’, 2004.
- [73] A. Singhal and P. Bedi, ‘Multi-class blind steganalysis using deep residual networks’, *Multimed Tools Appl*, vol. 80, no. 9, pp. 13931–13956, 2021.
- [74] C.-W. Huang, C. Chou, Y.-C. Chiu, and C.-Y. Chang, ‘Embedded FPGA Design for Optimal Pixel Adjustment Process of Image Steganography’, *Math Probl Eng*, vol. 2018, pp. 1–8, 2018, doi: 10.1155/2018/5216029.
- [75] S. S. Bharti, M. Gupta, and S. Agarwal, ‘A novel approach for audio steganography by processing of amplitudes and signs of secret audio separately’, *Multimed Tools Appl*, vol. 78, no. 16, pp. 23179–23201, 2019, doi: 10.1007/s11042-019-7630-4.

- [76] C. Pak, J. Kim, K. An, C. Kim, K. Kim, and C. Pak, 'A novel color image LSB steganography using improved 1D chaotic map', *Multimed Tools Appl*, vol. 79, no. 1–2, pp. 1409–1425, 2020.
- [77] Z. Syahlan and T. Ahmad, 'Reversible data hiding method by extending reduced difference expansion', *International Journal of Advances in Intelligent Informatics*, vol. 5, no. 2, pp. 101–112, 2019.
- [78] A. Nolkha, S. Kumar, and V. S. Dhaka, 'Image Steganography Using LSB Substitution: A Comparative Analysis on Different Color Models', in *Smart Systems and IoT: Innovations in Computing*, Springer, 2020, pp. 711–718.
- [79] K. Muhammad, M. Sajjad, I. Mehmood, S. Rho, and S. W. Baik, 'Image steganography using uncorrelated color space and its application for security of visual contents in online social networks', *Future Generation Computer Systems*, vol. 86, pp. 951–960, 2018.
- [80] K. Muhammad, M. Sajjad, I. Mehmood, S. Rho, and S. W. Baik, 'A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image', *Multimed Tools Appl*, vol. 75, no. 22, pp. 14867–14893, 2016, doi: 10.1007/s11042-015-2671-9.
- [81] M. Rathor and A. Sengupta, 'Design Flow of Secured N-Point DFT Application Specific Processor Using Obfuscation and Steganography', *IEEE Lett Comput Soc*, vol. 3, no. 1, pp. 13–16, 2020.
- [82] J. K. Mandal, 'Discrete Fourier Transform-Based Steganography', in *Reversible Steganography and Authentication via Transform Encoding*, Springer, 2020, pp. 63–98.
- [83] G. K. Birajdar, V. A. Vyawahare, and M. D. Patil, 'Secure and Robust ECG Steganography Using Fractional Fourier Transform', *Cryptographic and Information Security Approaches for Images and Videos*, p. 19, 2018.



- [84] P. Chowdhuri, B. Jana, and D. Giri, 'Secured steganographic scheme for highly compressed color image using weighted matrix through DCT', *International Journal of Computers and Applications*, vol. 7074, 2018, doi: 10.1080/1206212X.2018.1505024.
- [85] X. Song, S. Wang, and X. Niu, 'An integer DCT and affine transformation based image steganography method', *Proceedings of the 2012 8th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IIH-MSP 2012*, pp. 102–105, 2012, doi: 10.1109/IIH-MSP.2012.30.
- [86] S. Arunkumar, V. Subramaniaswamy, V. Vijayakumar, N. Chilamkurti, and R. Logesh, 'SVD-based robust image steganographic scheme using RIWT and DCT for secure transmission of medical images', *Measurement (Lond)*, vol. 139, pp. 426–437, 2019, doi: 10.1016/j.measurement.2019.02.069.
- [87] M. K. Shyla and K. B. S. Kumar, 'Novel Color Image Data Hiding Technique Based on DCT and Compressed Sensing Algorithm', in *Emerging Research in Electronics, Computer Science and Technology*, Springer, 2019, pp. 1151–1157.
- [88] M. Bilal, S. Imtiaz, W. Abdul, and S. Ghouzali, 'Zero-steganography using DCT and spatial domain', *Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, AICCSA*, 2013, doi: 10.1109/AICCSA.2013.6616431.
- [89] A. Rai and H. V. Singh, 'Machine learning-based robust watermarking technique for medical image transmitted over LTE network', *Journal of Intelligent Systems*, vol. 27, no. 1, pp. 105–114, 2018.
- [90] D. D. Shankar and P. K. Upadhyay, 'Steganalysis of Very Low Embedded JPEG Image in Spatial and Transform Domain Steganographic Scheme Using SVM', in *Innovations in Computer Science and Engineering*, Springer, 2020, pp. 405–412.
- [91] A. Rai and H. V. Singh, 'SVM based robust watermarking for enhanced medical image security', *Multimed Tools Appl*, vol. 76, no. 18, pp. 18605–18618, 2017.

- [92] A. AbdelQader and F. AlTamimi, 'ANovel IMAGE STEGANOGRAPHY APPROACH USING MULTI-LAYERS DCT FEATURES BASED ON SUPPORT VECTOR MACHINE CLASSIFIER', *The International Journal of Multimedia & Its Applications*. <https://doi.org/10.5121/ijma>, 2017.
- [93] M. Islam and R. H. Laskar, 'Geometric distortion correction based robust watermarking scheme in LWT-SVD domain with digital watermark extraction using SVM', *Multimed Tools Appl*, vol. 77, no. 11, pp. 14407–14434, 2018.
- [94] S. Sajasi and A. M. E. Moghadam, 'A high quality image steganography scheme based on Fuzzy Inference System', *13th Iranian Conference on Fuzzy Systems, IFSC 2013*, 2013, doi: 10.1109/IFSC.2013.6675666.
- [95] A. K. Alvi and R. Dawes, 'Image steganography using fuzzy domain transformation and pixel classification', *Proceedings of the International Conference on Software Engineering and Knowledge Engineering, SEKE*, vol. 2013-Janua, no. January, pp. 277–282, 2013.
- [96] S. Kiani and M. E. Moghaddam, 'Fractal based digital image watermarking using fuzzy c-mean clustering', *Proceedings - 2009 International Conference on Information Management and Engineering, ICIME 2009*, pp. 638–642, 2009, doi: 10.1109/ICIME.2009.72.
- [97] S. Rajendran and M. Dorai Pandian, 'Chaotic map based random image steganography using LSB technique', *International Journal of Network Security*, vol. 19, no. 4, pp. 593–598, 2017, doi: 10.6633/IJNS.201707.19(4).12.
- [98] G. Savithri, S. Mane, and J. S. Banu, 'Parallel Implementation of RSA 2D-DCT Steganography and Chaotic 2D-DCT Steganography', in *Proceedings of International Conference on Computer Vision and Image Processing*, 2017, pp. 593–605.
- [99] S. Alam, T. Ahmad, and M. N. Doja, 'A Novel Edge Based Chaotic Steganography Method Using Neural Network', in *Proceedings of the 5th International Conference on Frontiers in Intelligent Computing: Theory and Applications*, 2017, pp. 467–475.

- [100] H. Nyeem, ‘Reversible data hiding with image bit-plane slicing’, *20th International Conference of Computer and Information Technology, ICCIT 2017*, vol. 2018-Janua, no. December, pp. 1–6, 2018, doi: 10.1109/ICCITECHN.2017.8281763.
- [101] V. Kumar and D. Kumar, ‘A modified DWT-based image steganography technique’, *Multimed Tools Appl*, vol. 77, no. 11, pp. 13279–13308, 2018.
- [102] M. Islam, A. Roy, and R. H. Laskar, ‘Neural network based robust image watermarking technique in LWT domain’, *Journal of Intelligent & Fuzzy Systems*, vol. 34, no. 3, pp. 1691–1700, 2018.
- [103] E. R. L. Yadav, E. C. Kumar, and E. R. Yadav, ‘High Capacity Embedding And Secured Steganography Model By Using GA And Integer Wavelet Transform’, no. July, 2019.
- [104] A. ALabaichi, M. A. A. Al-Dabbas, and A. Salih, ‘Image steganography using least significant bit and secret map techniques.’, *International Journal of Electrical & Computer Engineering (2088-8708)*, vol. 10, 2020.
- [105] R. Nayak, ‘Steganography with BSS-RSA-LSB technique: A new approach to Steganography .’, vol. 3, no. 5, pp. 187–190, 2015.
- [106] M. L. Rahman, P. Sarker, and A. Habib, ‘A Faster Decoding Technique for Huffman Codes Using Adjacent Distance Array’, in *International Joint Conference on Computational Intelligence*, 2019, pp. 309–316.
- [107] B. S. Shashikiran, K. Shaila, and K. R. Venugopal, ‘Minimal block knight’s tour and edge with lsb pixel replacement based encrypted image steganography’, *SN Comput Sci*, vol. 2, no. 3, pp. 1–9, 2021.
- [108] R. Shanthakumari and S. Malliga, ‘Dual layer security of data using LSB inversion image steganography with elliptic curve cryptography encryption algorithm’, *Multimed Tools Appl*, vol. 79, no. 5–6, pp. 3975–3991, 2020, doi: 10.1007/s11042-019-7584-6.
- [109] A. M. FADHIL, ‘BIT INVERTING MAP METHOD FOR IMPROVED STEGANOGRAPHY SCHEME’. Universiti Teknologi Malaysia, 2016.

- [110] M. M. Hashim, S. H. Rhaif, A. A. Abdulrazzaq, A. H. Ali, and M. S. Taha, ‘Based on IoT Healthcare Application for Medical Data Authentication: Towards A New Secure Framework Using Steganography’, in *IOP Conference Series: Materials Science and Engineering*, 2020, vol. 881, no. 1, p. 12120.
- [111] S. T. Klein, S. Saadia, and D. Shapira, ‘Forward looking Huffman coding’, in *International Computer Science Symposium in Russia*, 2019, pp. 203–214.
- [112] S. A. Seyyedi, V. Sadau, and N. Ivanov, ‘A secure steganography method based on integer lifting wavelet transform’, *International Journal of Network Security*, vol. 18, no. 1, pp. 124–132, 2016.
- [113] A. Saeed *et al.*, ‘An accurate texture complexity estimation for quality-enhanced and secure image steganography’, *IEEE Access*, vol. 8, pp. 21613–21630, 2020, doi: 10.1109/ACCESS.2020.2968217.
- [114] Z. S. Younus and G. T. Younus, ‘Video steganography using knight tour algorithm and LSB method for encrypted data’, *Journal of Intelligent Systems*, vol. 29, no. 1, pp. 1216–1225, 2020.
- [115] N. Sai Ravi Chandra, V. Sneha, and P. Victor Paul, ‘A Novel Image Steganography Model Using LSB with Extended ASCII Codes’, in *Smart Innovation, Systems and Technologies*, 2020, vol. 159, pp. 107–116. doi: 10.1007/978-981-13-9282-5\_11.
- [116] M. Bachrach and F. Y. Shih, ‘Survey of image steganography and steganalysis’, *Multimedia Security: Watermarking, Steganography, and Forensics*, pp. 201–214, 2017, doi: 10.1201/b12697.
- [117] G. Swain, ‘Very High Capacity Image Steganography Technique Using Quotient Value Differencing and LSB Substitution’, *Arab J Sci Eng*, vol. 44, no. 4, pp. 2995–3004, 2019, doi: 10.1007/s13369-018-3372-2.
- [118] A. G. Weber, ‘The USC-SIPI image database version 5’, *USC-SIPI Report*, vol. 315, no. 1, 1997.

- [119] N. Mukherjee, G. Paul, S. K. Saha, and D. Burman, ‘A PVD based high capacity steganography algorithm with embedding in non-sequential position’, *Multimed Tools Appl*, pp. 1–31, 2020.
- [120] J. Liu, Y. Tian, T. Han, J. Wang, and X. Luo, ‘Stego key searching for LSB steganography on JPEG decompressed image’, *Science China Information Sciences*, vol. 59, no. 3, pp. 1–15, 2016, doi: 10.1007/s11432-015-5367-x.
- [121] D. Q. Zeebaree, ‘Robust watermarking scheme based LWT and SVD using artificial bee colony optimization’, *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 21, no. 2, pp. 1218–1229, 2021.
- [122] A. Saleema and T. Amarunnishad, ‘A New Steganography Algorithm Using Hybrid Fuzzy Neural Networks’, *Procedia Technology*, vol. 24, pp. 1566–1574, 2016, doi: 10.1016/j.protcy.2016.05.139.
- [123] A. K. Pal, K. Naik, and R. Agarwal, ‘A steganography scheme on JPEG compressed cover image with high embedding capacity’, *International Arab Journal of Information Technology*, vol. 16, no. 1, pp. 116–124, 2019.
- [124] C. A. Sari, G. Ardiansyah, D. R. I. Moses Setiadi, and E. H. Rachmawanto, ‘An improved security and message capacity using AES and Huffman coding on image steganography’, *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 17, no. 5, pp. 2400–2409, 2019, doi: 10.12928/TELKOMNIKA.v17i5.9570.