

Republic of Iraq  
Ministry of Higher Education  
& Scientific Research  
University of Baghdad  
College of Education for Pure  
Sciences / Ibn Al-Haitham  
Department of Physics



# **A New Proposed Steganography Method for Lossy Compression Attack Reducing**

*A Thesis*

*Submitted to the College of Education for Pure Science / Ibn Al-Haitham / University of Baghdad in Partial Fulfillment of the Requirements for the Degree of Master of Science in Physics*

*By*

**Mohammed Kamal Saleh**

*(B.Sc. 2007)*

*Supervised by*

**Assist. Prof. Dr. Hameed M. Abduljabbar**

*September 2018 A. D*

*Muharram 1440 A.H*

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

﴿قُلْ لَوْ كَانَ الْبَحْرُ مِدَادًا لَكَلِمَاتِ رَبِّي لَنَفِدَ الْبَحْرُ

قَبْلَ أَنْ تَنْفَدَ كَلِمَاتُ رَبِّي وَلَوْ جِئْنَا بِمِثْلِهِ مَدَدًا﴾

صدق الله العظيم

سورة الرحمن

الآية (109)

### Supervisors Certification

I certify that this thesis was prepared by **Mohammed Kamal Saleh** under my supervision at the Physics Department, College of Education for pure Science / Ibn Al-Haitham, University of Baghdad in partial fulfillment requirements for the Degree of Master of Science in Physics.

Signature



PDF Reducer Demo

Name: *Dr. Hameed M. Abduljabbar*

Title: *Assistant Professor*

Address: *College of Education for pure Science  
/ Ibn Al-Haitham, University of Baghdad*

Date:        /        / 2018

### Certification of the Chairman of the Department

In view of the available recommendations, I forward this thesis for debate by the Examination Committee.

Signature



PDF Reducer Demo

Name: *Dr. Samir Ata Maki*


Title: *Professor*


Address: *Chairman Department of Physics, College of  
Education for pure Science/ Ibn Al-Haitham,  
University of Baghdad*

Date:        /        / 2018

**Committee Certification**

We certify that we have read this thesis "A New Proposed Steganography Method for lossy compression attack Reducing " submitted by (Mohammed Kamal Saleh) and as examining committee examined the student in its content and that in our opinion it is adequate with standard as thesis for the Degree of Master of Science in Physics.

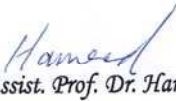
Signature   
Name: Prof. Dr. Zaid M. Abood  
Address: Department of Physics, Collage of Education, Mustansiriyah University

Signature   
Name: Assist. Prof. Dr. Taghreed Abdul Hameed Naji  
Address: Collage of Education for Pure Science / Ibn Al-Haitham, University of Baghdad

(Chairman)  
Date: / / 2018

(Member)  
Date: / / 2018

Signature   
Name: Assist. Prof. Dr. Amal Jabbar Hatem  
Address: Collage of Education for Pure Science / Ibn Al-Haitham, University of Baghdad

Signature   
Name: Assist. Prof. Dr. Hameed M. Abduljabbar  
Address: Collage of Education for Pure Science / Ibn Al-Haitham, University of Baghdad

(Member)  
Date: / / 2018

(Member-Supervisor)  
Date: / / 2018

**Approved by the Council of the College of Education for Pure Sciences  
/ Ibn Al-Haitham / University of Baghdad**

Signature   
Name: Asst. Prof. Dr. Hasan Ahmed Hasan  
Address: Behalf/ The Dean of college of Education for Pure science / Ibn al-Haitham  
Date: / / 2018

## *Dedication*

*To God Almighty*

*To My Supervisor and Dear Brother Dr. Hameed*

*Majeed Abduljabbar*

*To The Spirit of My Dear Father (God Mercy)*

*To My Dear Family, My Mother, My Brothers and*

*Sisters*

*To All Friends*

*For Their Support and Help*

*MOHAMMED*

*2018*

## *Acknowledgments*

*I would like to thank God Almighty, for helping me and enabling me to accomplish this work.*

*I am wholly indebted to my supervisor and dear brother “[Dr. Hameed Majeed Abduljabbar](#)” for his patience in answering my questions and the knowledge and encouragement he gave me during the research period which exceeded the full year*

*My sincere thanks and appreciation to my family for their patience, help and encouragement throughout my life.*

*My sincere thanks are due to all the members of the teaching staff in physics department for their help and support, particularly member's in the group of thin films and image processing.*

*My sincere thanks and appreciation to my colleagues in the Master's Group in the Department of Physics who I was happy to accompany and know all of them without exception.*

*My sincere thanks and appreciation to my colleagues in secondary “[Amjad Al Shaalan](#)” for their continued assistance and encouragement throughout the study period.*

*My sincere thanks and appreciation to my friends all of them*

*Thank you very much to all who love me and wish me success and happiness*

*MOHAMMED 2018*

## *Abstract*

In this thesis, two approaches are considered to study the case of JPEG attack on a hidden message implanted using steganography methods. The first approach, a statistical analysis for the effect of a JPEG attack on a hidden message implanted using LSB stegano method is presented. The message in its ASCII form and text-image are analysed after the JPEG attack for the quality (100-50) for all possible start depth using single bit. From the results, the retrieved message in its image form is more capable of survived after the JPEG attack comparing to its ASCII form and it is readable if its image quality higher than 13 dB. A full discussion of the results obtained from the cover image and the retrieved message is presented after The LSB stegano method and after the JPEG attack.

In the second approach, a new statistical steganography method (NSSM) to override or reduce the effect of JPEG attack on a cover image is presented. The new method is based on an analysis of the JPEG algorithm, in which it uses the value of the mean and the standard deviation of each cover block to embed the secret message, where the cover image blocks calculated in the same manner of the JPEG algorithm. Two standard images that differ in their amount of texture are used to test the new method, an analysis and discussion are presented for the results of applying this method which proved the validity of this method to reduce or override the JPEG attack.

## List of Contents

Heading No.	Subject	Page
<b>1</b>	<b>Chapter One: General Introduction</b>	<b>1</b>
1.1	Introduction.....	1
1.2	Steganography.....	3
1.3	Literature Survey.....	6
1.4	The Aim of Thesis.....	8
1.5	Thesis Layout:.....	8
<b>2</b>	<b>Chapter Two: Theoretical Background</b>	<b>10</b>
2.1	Introduction.....	10
2.2	Terminology.....	10
2.3	Principles of steganography.....	11
2.3.1	The Storage.....	11
2.3.2	Undetectability.....	11
2.3.3	The Robustness.....	12
2.4	Methods of Hiding.....	12
2.4.1	Injection.....	12
2.4.2	Substitution.....	12
2.4.3	Generation.....	13
2.5	Steganography's Media.....	13
2.5.1	Text Steganography.....	13
2.6	Image Steganography.....	14
2.6.1	Audio Steganography.....	14
2.6.2	Protocol Steganography.....	14
2.7	Steganography Techniques.....	15
2.7.1	Spatial Domain Method.....	15
2.7.2	Transform Domain Method.....	16
2.7.3	Statistical Method.....	16
2.7.4	Distortion Method.....	17
2.7.5	Spread Spectrum Techniques.....	17
2.7.6	Cover Generation Techniques.....	17
2.8	Types of Steganography.....	18
2.8.1	Pure Steganography.....	18
2.8.2	Secret key steganography.....	19
2.8.3	Public key steganography.....	19



2.9	<b>Digital Images</b> .....	19
2.9.1	<b>Binary Images</b> .....	20
2.9.2	<b>Gray-Scale Images</b> .....	20
2.9.3	<b>Colour images</b> .....	20
2.9.4	<b>Multi-spectral Images:</b> .....	21
2.10	<b>Least Significant Bit (LSB)</b> .....	21
2.10.1	<b>Embedding methods of LSB Steganography</b> .....	23
2.10.1.1	<b>Sequential Method</b> .....	23
2.10.1.2	<b>Randomized method</b> .....	24
2.11	<b>Image Compression</b> .....	24
2.11.1	<b>The main Aims of Image Compression</b> .....	25
2.11.2	<b>Image compression Methods</b> .....	25
2.11.2.1	<b>Lossy compression</b> .....	25
2.11.2.2	<b>Lossless compression</b> .....	25
2.11.3	<b>JPEG Compression</b> .....	26
2.11.4	<b>JPEG Algorithm Steps</b> .....	26
2.12	<b>Statistical Measurements</b> .....	28
2.12.1	<b>Mean:</b> .....	28
2.12.2	<b>Standard Deviation (<math>\sigma</math>):</b> .....	29
2.12.3	<b>Variance:</b> .....	29
2.12.4	<b>Mean Squared Error (MSE):</b> .....	29
2.12.5	<b>Signal-to-Noise-Ratio (SNR)</b> .....	29
3	<b>Chapter Three: The Proposed system</b>	31
3.1	<b>Introduction</b> .....	31
3.2	<b>The Standard least significant bit (LSB) technique</b> .....	33
3.3	<b>The Proposed Algorithm (NSSM)</b> .....	37
4	<b>Chapter Four: Results and Discussions</b>	42
4.1	<b>Introduction</b> .....	42
4.2	<b>The Standard Least Significant Bit (LSB) Technique</b> .....	42
4.3	<b>A New Statistical Steganography Method (NSSM)</b> .....	55
5	<b>Chapter Five: Conclusions &amp; Recommendations</b>	69
5.1	<b>Conclusions</b> .....	69
5.1.1	<b>Standard Least Significant Bit (LSB) Technique</b> .....	69
5.2	<b>A New Statistical Steganographic Method (NSSM)</b> .....	70
5.3	<b>Recommendations</b> .....	70
6	<b>References</b>	71

## List of Figures

Figures No.	Figure Name	Page
Figure 1-1	The techniques of security system .....	3
Figure 2-1	General steganography system.....	10
Figure 2-2	The types of steganography .....	18
Figure 2-3	Distribution the bits within the byte.....	22
Figure 2-4	Bitmap distribution inside pixel in color image (RGB).....	22
Figure 2-5	The block (8×8) pixel.....	27
Figure 2-6	The JPEG Compression Scheme.....	28
Figure 3-1	Sample images (a) Lena and (b) Baboon (size 512×512 pixel).....	33
Figure 3-2	Block diagram of the standard Least Significant Bit (LSB) steganography .....	36
Figure 3-4	scheme the quality Calculation image and message after JPEG attack on the hidden message using (LSB) steganography. ....	37
Figure 3-4	Block diagram of new Statistical Steganography Method (NSSM) .....	40
Figure 3-5	Scheme the quality calculation of image and message after JPEG attack using the (NSSM) steganography .....	41
Figure 4-1	Stego-image quality (SNR) after LSB by using (ASCII & Text-image) messages for Lena image. ....	43
Figure 4-2	Stego-image quality (SNR) after LSB by using (ASCII and text-image) messages for Baboon image.....	43
Figure 4-3	The amount of distortion in stego-image Lena after embedding using LSB technique. ....	45
Figure 4-4	The cover quality (SNR) after JPEG attack with compression ratio ranging from (100-50) (ASCII) for Lena image .....	46
Figure 4-5	The cover quality (SNR) after JPEG attack with compression ratio ranging from (100-50) (Text-image) for Lena image. ....	47
Figure 4-6	The cover quality (SNR) after JPEG attack with compression ratio ranging from (100-50) (ASCII) for Baboon image.....	48
Figure 4-7	The cover quality (SNR) after JPEG attack with compression ratio ranging from (100-50) (text image) for Baboon image.....	49
Figure 4-8	The error percent in the ASCII message after JPEG attack for different...50	

Figure 4-9 The (Text-image) message quality (SNR) for different compression ratio and Start depth for Lena image. ....	51
Figure 4-10 The error percent in the ASCII message after JPEG attack for different compression ratio(100-50) and Start depth for Baboon image.....	52
Figure 4-11 The quality (SNR) of (text image) message for different compression ratio (100-50) and Start depth for Baboon image. ....	53
Figure 4-12 the quality (SNR) of the retrieved message (text-image) after JPEG attack with compression ratio (Q=90)for Lena image.....	54
Figure 4-13 The cover quality after applying the NSSM for two threshold values (0.5 and 1) for Lena and Baboon image.....	57
Figure 4-14 The mean value of the Baboon image for different threshold values (0.5,1) after JPEG attack for different compression quality .....	58
Figure 4-15 The amount of distortion in stego-image using (NSSM). ....	59
Figure 4-16 The cover quality (SNR) for Lena image after JPEG attack for $\sigma$ threshold =( 0.5 and 1).....	61
Figure 4-17 The cover quality (SNR) for the Baboon image after JPEG attack for $\sigma$ threshold = (0.5 and 1).....	63
Figure 4-18 Comparison between two images before & after JPEG attack (Q=50) ..	64
Figure 4-19 The error percent of retrieved message after JPEG attack for Lena image (TH=0.5) .....	66
Figure 4-20 The error percent of retrieved message after JPEG attack for Lena image (TH=1) .....	66
Figure 4-21 The error percent of retrieved message after JPEG attack for Baboon image (TH=0.5 and 1).....	67

## List of Tables

Tables No.	Table Name	Page
Table 4-1	The Stego-image quality (SNR &MSE) after LSB by using (ASCII & Text-image) messages, for Lena image .....	42
Table 4-2	The Stego-image quality (SNR &MSE) after LSB by using (ASCII & Text-image) messages, for Baboon image.....	43
Table 4-3	The cover quality (SNR (dB)) after JPEG attack with compression ratio ranging from (100-50) (ASCII) for Lena image. ....	45
Table 4-4	The cover quality (MSE) after JPEG attack with compression ratio ranging from (100-50) (ASCII) for Lena image .....	45
Table 4-5	The stego-image quality(SNR (dB)) after JPEG attack with compression ratio ranging from (100-50) (Text-image) for Lena image.....	46
Table 4-6	The cover quality (MSE) after JPEG attack with compression ratio ranging from (100-50) (Text-image) for Lena image .....	46
Table 4-7	The cover quality (SNR (dB)) after JPEG attack with compression ratio ranging from (100-50) (ASCII) for Baboon image.....	47
Table 4-8	The cover quality (MSE) after JPEG attack with compression ratio ranging from (100-50) (ASCII) for Baboon image.....	47
Table 4-9	The cover quality (SNR (dB)) after JPEG attack with compression ratio ranging from (100-50) (text image) for Baboon image. ....	48
Table 4-10	The cover quality (MSE) after JPEG attack with compression ratio ranging from (100-50) (text image) for Baboon image.....	48
Table 4-11	The error percent in the ASCII message after JPEG attack for different compression ratio and Start depth for Lena image .....	50
Table 4-12	The (Text-image) message quality(SNR (dB)) for different compression ratio and Start depth for Lena image.....	50
Table 4-13	The quality (MSE) of Text-image message for different compression ratio and start depth for Lena image.....	51
Table 4-14	The error percent in the ASCII message after JPEG attack for different compression ratio(100-50) and Start depth for Baboon image.....	51
Table 4-15	The quality (SNR (dB)) of (text image) message for different compression ratio (100-50) and Start depth for Baboon image.....	52

Table 4-16 The quality (MSE) of (text image) message for different compression ratio (100-50) and Start depth for Baboon image.....	52
Table 4-17 The cover quality (SNR (dB)) after applying the NSSM for two threshold values (0.5, 1) for Lena and Baboon image .....	55
Table 4-18 The cover quality (MSE) after applying the NSSM for two threshold values (0.5 and 1) for Lena and Baboon image .....	56
Table 4-19 The mean value of the Baboon image for different threshold values (0.5 and 1) after JPEG attack for different compression quality.....	57
Table 4-20 The cover quality (SNR (dB)) after JPEG attack (Lena -TH=0.5 and 1).	60
Table 4-21 The cover quality (MSE) after JPEG attack (Lena -TH=0.5 and 1).....	60
Table 4-22 The cover quality (SNR (dB)) after JPEG attack for Baboon image (TH = 0.5 and 1).....	61
Table 4-23 The cover quality (MSE) after JPEG for Baboon image (TH = 0.5 and 1) .....	62
Table 4-24 The error percent of retrieved message after JPEG attack for Lena image (TH=0.5) .....	64
Table 4-25 The error percent of retrieved message after JPEG attack for Lena image (TH=1) .....	65
Table 4-26 The error percent of retrieved message after JPEG attack for Baboon image (TH=0.5 and 1).....	66

## *List of Abbreviations*

<b>Symbol</b>	<b>Meaning</b>
<b>ASCII</b>	<b>American Standard Code For Information Interchange</b>
<b>BMP</b>	<b>Bitmap Picture</b>
<b>BPP</b>	<b>Bit Per Pixel</b>
<b>dB</b>	<b>Decibel</b>
<b>DCT</b>	<b>Discrete Cosine Transform</b>
<b>DFT</b>	<b>Discrete Fourier Transform</b>
<b>DIF</b>	<b>Deference of <math>\sigma</math></b>
<b>DWT</b>	<b>Discrete Wavelet Transform</b>
<b>GIF</b>	<b>Graphics Interchange Format</b>
<b>HVS</b>	<b>Human Visual System</b>
<b>JPEG</b>	<b>Joint Photographic Expert Group</b>
<b>LSB</b>	<b>Least Significant Bit</b>
<b>MSB</b>	<b>Most Significant Bit</b>
<b>MSE</b>	<b>Mean Square Error</b>
<b>NSSM</b>	<b>New Statistical Steganography Method</b>
<b>PIXEL</b>	<b>Picture Element</b>
<b>RGB</b>	<b>Red, Green, Blue</b>
<b>SD</b>	<b>Start Depth (0-7)</b>
<b>SNR</b>	<b>Signal-to-Noise Ratio</b>
<b>TCP/IP</b>	<b>Transfer Control Protocol / Internet Protocol</b>
<b>v</b>	<b>Variance</b>
<b><math>\sigma</math></b>	<b>Standard Deviation</b>
<b>TIFF</b>	<b>Tagged Image File Format</b>

# *CHAPTER ONE*

## *GENERAL*

### *INTRODUCTION*

# Chapter One: General Introduction

## 1.1 Introduction

The concept of communication appeared with the beginning of the human civilization on the earth. Over the years, a grown idea of the secret communicating with the human was developed. The communicating between two people in a method of indirectly and unreadable from anyone to other, especially with the development and growth in the field of information and communication technology (ICT) where a lot of information is store and keep electronically (digital files). The security of the data has become the main issue, according to developments in modern communication technology, the search for special means to provide high-security level has become a very urgent need. As a result of the increasing number of data being exchanged continuously on the internet, the internet security becomes a very important issue, therefore, the security information is required to protect it against unauthorized persons. [1] [2] [3] [4]

There are important information need to high protection such as, military coup, security information, technology, science, personal information and so on [5]. These informations require a technique in order not be detected and to be successfully transmitted from the first party (sender) to the second party (recipient). There are several methods to hide and protect the sensitive information. These methods are different in the methods use to implement the process hide of the sensitive information and protect it. [6] [7] [8]



Historically, the importance information (sensitive) being protected by the encryption. Encryption technique was created in order to protect the secrecy of communication and has devised many different methods for encryption in order to maintain the secret message (secret information) [2] [4].

Encryption uses a complex mathematical formula to convert the plain text readable to ciphertext unreadable from anyone else except the person who owned the encryption key (Secret Key) both (sender and recipient). The secret key is the tool or algorithm used to convert the information from the readable form (public) into an unreadable form (secret). [9] [10]

Encryption works to hide and protect the content of secret information but not hiding the existence sensitive information being transmitted it to two people. Therefore, the secret message becomes more susceptible to attacks by the enemies (the third party), especially, with the development of steganalysis science to analyze the message to extract the content of the secret message or at least destroying it significantly. Sometimes preserving the contents of the secret message is insufficient without hiding the existence of a secret message originally. The technology used to implement this, i.e. to hide the existence of any secret communication, is called Steganography [9] [11].

The information security system can be divided into two main parts: encryption and hiding information . There is a difference in terms of the method used to protect and secure information. In addition, the hiding information is divided into two important parts, watermarking and steganography, where they work to maintain sensitive information as well as property rights, etc [5]. There are several types of steganography depending on the electronic media used such as text, image, audio, and

video. The information security system is classified into cryptography and hiding information (watermarking and steganography). [12] [10] [13]

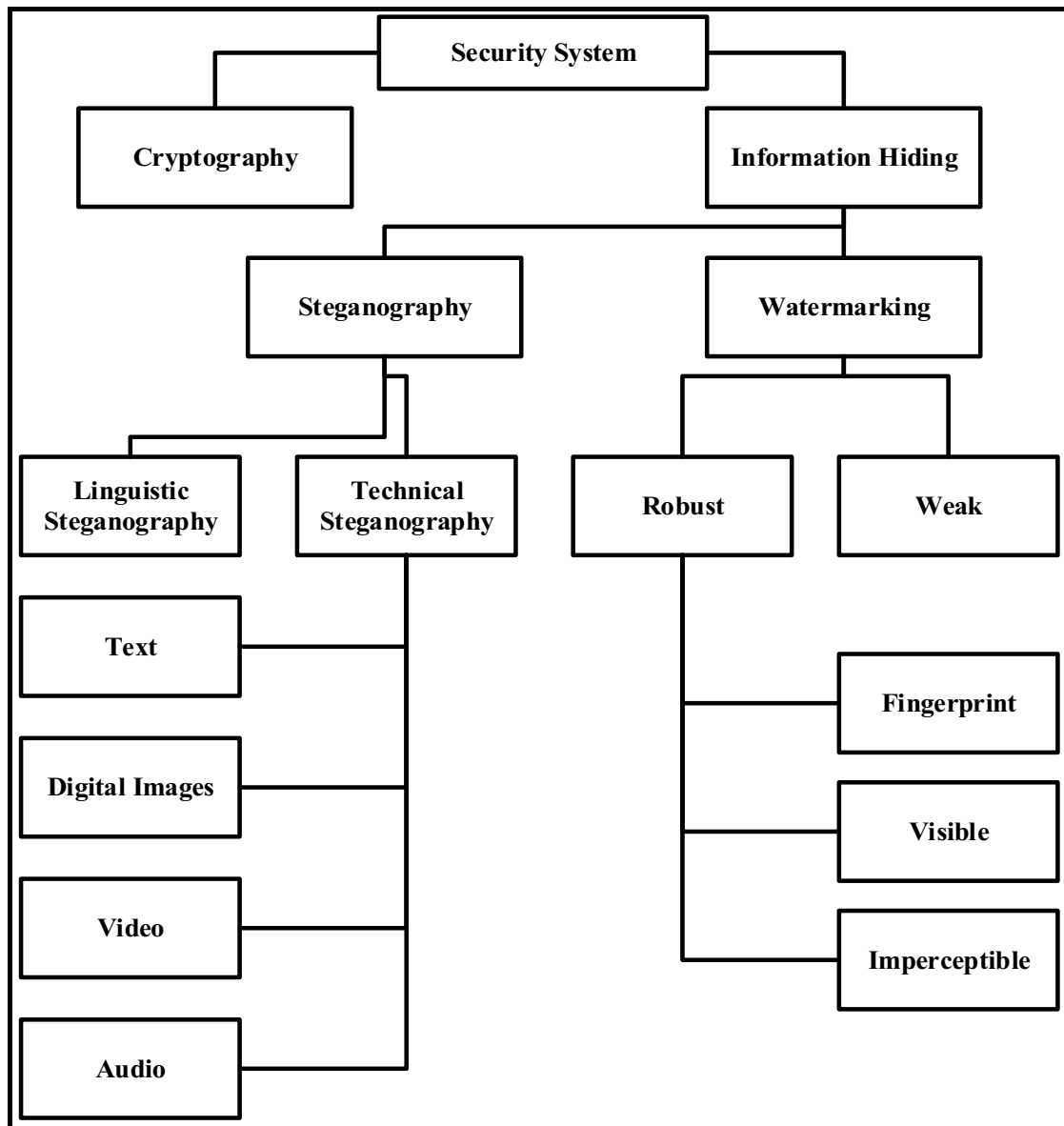


Figure 1-1 The techniques of security system [12]

## 1.2 Steganography

Steganography is an art, technique or science of hiding information inside the cover message or other information. This is the technology of the secret communication and it using a public message as a cover to hide the secret message. [5] [14] [15]

In recent decades, with the large development in the field of the digital information and communication, a huge development in our world have been done, also, it becomes easier to send and share images or other information through the internet which allow persons to exchange sensitive or public information between any two people or more in the world . [11] [16]

Moreover, there are many images which being exchanged daily on the internet. This number of images is continuously increase due to the fact that the digital images taken by people which reach to millions, whether images of personal, scientific, economic, etc. Using the images that are exchanging on internet (sending and receiving) is very useful as a safe environment to exchange and sharing the very sensitive information. This is meets the need of people to protect their images, their secret data or intellectual property. [17] [18]

Steganography technique aims to hide the secret information inside various carrier's media, which may be (image, text, audio, or video files) [19]. Images are more commonly used on the internet and has small size and transmit in less time in comparison with other types covers, so it's often be used as a cover to hide the secret information [20] [21]. The main objective of steganography to hide the existence of sensitive information being sent their originally. [22] [23] [24] [25]

Many algorithms proposed for embedding of the sensitive information in cover image in spatial and frequency domain, but most algorithms caused some changes in image quality and statistical properties. Based on the changes of statistical occurring in the cover image, steganalysis can benefit from these changes to detect the existence of sensitive information inside image as well as may decode the message or disable it using some steganalysis tools. A technique or science the attack on the hidden information in order to extract the content of the secret

information or destroyed called steganalysis [26]. A good method of hiding information must that the distortion resulting from the embedding process is difficult to detect by the human eye and analysis tools (steganalysis). [10]

The origin of the steganography word historically in the Greek language means "covered writing" or "hidden writing". Where the word (steganos) meaning (cover or hidden and secret) and the word (graphic) meaning (writing or drawing) [27] [28] [29]. This science or art used in different forms since hundreds of years (since 440 B.C), where the message send by a human in spatially forms using the skull. where the carrier shaves his head then writes the message and send after his hair grew back. [3] [12] [30]

There are many differences between the steganography and encryption, but the most important difference between them is a fact of existence a secret message being exchanged, where, encryption focused on maintaining the content of the secret message without hiding existence a secret communicating, on other hand, steganography technique is focused on maintaining both the content and existence of a secret message. This difference makes steganography suitable for use to hide the sensitive information, where the existence of a secret message that being exchanged without drawn the attention of observer (enemy). [4] [31] [32]

Methods of steganography and encryption are aims to protect sensitive information from anyone wants to know what content of information which being secretly exchanged [33]. In image steganography, only images been used to hide the sensitive information. With digital images information can be hidden in different methods based on (type format, used technique and a method of embedding). The two methods (cryptography and steganography) can be mixed in order to increase the

protection and the security information especially with great advances in digital information and advanced computing. [4] [10] [34]

There are several reasons for hiding the secret information steganography, the enemy (who want to know the important information) such as security, economic, defensive and scientific. Where starting the attacking on the send message in order to detect the content the message or disable or destroy it. [12]

The field of hiding the sensitive information is developed significantly after the September 2001 attacks in the United States. Where increased focus on electronic multimedia that are sent daily on the web. In addition, was developed a new system or science to analysis the multimedia that raises attention in order to extract the secret information or destruction it [35].

### 1.3 Literature Survey

- ❖ In 1996, Currie, III, and Irvine [36], studied the impact of the JPEG algorithm on the LSB technique to hide the secret information (ASCII type). Moreover, they calculated the error percent in the retrieved message when used the color bitmap image as cover to hide the secret message.
- ❖ In 2003, Al-Towayjri [31], propose a new approach to a novel coding technology to control on the errors that result from the JPEG algorithm when embedding the message (ASCII and image) by the (LSB) method. The coding method was proposed on view the pixel in space as a point with the spatial domain as three color channel values. Then a comparison is done between the different types of stego-cover before and after JPEG compression.
- ❖ In 2010, Cm olcay [37], studied the embedding methods by using Least Significant Bit (LSB), such as LSB replacement, matching. In

addition, the studied and survey the steganalysis such as visual attack, JPEG attack, etc. Then a comparison was made between the embedding methods and steganalysis methods.

- ❖ In 2011, Yadav and et al. [38], a propose a new algorithm to hide the message inside the cover image (grayscale), the cover image is divided into uniform blocks, using the cyclic combination of last three bits (6th, 7th & 8th) the message's bits are embedded into the central pixel of the block, then using the Pseudo Random Generator seeded with a secret key for select the image's blocks, this method provides Distribute the message equally within the image (i.e. the message's bits are embedded inside the last three bits equally), also provides high quality of the image (undetected)
- ❖ In 2012, Sravanthi and et al. [23], studied and proposed a new approach to hide the data in digital image by using plane bit substitution method (PBSM) technology that message bits are embedding to image in each pixel. They suggested a steganography transformation machine (STM) for solution binary operation to the processing of the original image with assists LSB.
- ❖ In 2016, Al-Farraji [39], proposed a method of steganography using adding operation between the value of pixel image (LSB) and value of character ASCII (secret message), in addition, the author used two keys to extract the secret ASCII (secret message). The aim of this method is to enhance the power of hiding and also the difficulty of destroying it.
- ❖ In 2017, Joshi and Yadav [5], a propose a new method to hide the message inside the cover image, where exploit the last three bits from the marked pixel, then performs XOR operation with the three bits (1st,2nd and 3rd) the message's bits are embedded one by one inside the selected bits in cover image, the change in the quality of

stego-image equal to (+1 or -1), due to +1 or -1 modification, the amount of distortion in the Stego image is very slightly. The experimental results showed increases in both the image quality (undetectable) and capacity of the hidden information (storage).

#### 1.4 The Aim of Thesis

The aim of the present work is to study the effect attack of lossy compression (JPEG) on the hidden information (ASCII and text-image) in image steganography, which embedded by the Least Significant Bit (LSB) technique. In addition, to propose a new method (a statistical method) as a new method for certain compression JPEG quality can overcome or reduce the JPEG attack.

#### 1.5 Thesis Layout:

The content of the chapters of the thesis could be briefly review as follows:

- **chapter one:** (General Introduction) represents a general introduction to the system of information security and protection, the difference between encryption and information hiding, as well as what are the techniques of information hiding, in addition, to the survey of some previous studies close to the field of research in this thesis
- **Chapter Two:** (Theoretical Background) represents the theoretical background of the study subject, where it deals with the steganography, steganography terminology, techniques and types of steganography, steganography's media, image compression, compression types (Lossy, lossless) etc.
- **Chapter Three:** (The Proposed System), deals in its two parts with: firstly, describes the algorithm of hiding the secret data (ASCII, text-image) inside the image using the least significant bit (LSB),

secondly, explains the new algorithm (a statistical method) to hide the secret data (ASCII) inside the images

- **Chapter Four:** (Results and Discussions) The experimental results obtain by applying to the Least Significant Bit (LSB) technique and the proposed system are discussed. The quality of image and message before and after the JPEG attack is calculated. The results are discussed to show the amount of damage resulting in the message and the robustness of the message against the attacks with different qualities ranging about (100-50).
- **Chapter Five:** (Conclusions and Recommendations) deals with the conclusions of this study and recommendation for the future works.



*CHAPTER TWO*

*THEORETICAL*

*BACKGROUND*

## Chapter Two: Theoretical Background

### 2.1 Introduction

In the recent years, protection of the privacy and sensitive information of persons, companies, and countries are the important issue and is of great interest to researchers and decision makers. The techniques of hiding information consist of encryption, watermarking and steganography. These techniques are different in their objectives and method of working. [40].

### 2.2 Terminology

The scheme (2-1) represents a general steganography system [41] [42].

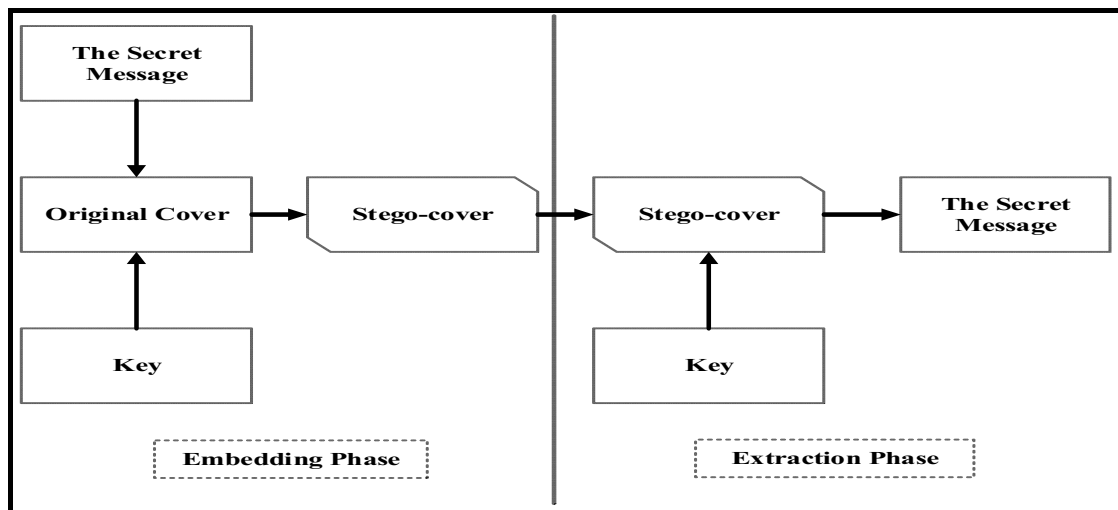


Figure 2-1 General steganography system [42] [43]

- ❖ **Cover:** represents any type of digital formats that use to hide the secret message inside it, such as (image, text, audio, and video) [43].
- ❖ **The secret message:** represent any type of the secret information that must be hidden within another message, such as (image, text, audio, and video). [30] [43]
- ❖ **Key:** represent the secret key to hide and extract the secret message which inside the cover . [43]

- ❖ **Embedding phase:** represent the process of hiding the secret message within the cover. This process is by the sender before sent the message. [30] [43]
- ❖ **Stego-cover:** is the cover after embedded the secret information and is called according to the type of cover. For example, (stego-image) when using an image as the cover. [30] [44]
- ❖ **Extraction phase** is the process of retrieval the secret message using the same Key. Therefore, the extraction process represents inverse the embedding process. [45]

### 2.3 Principles of steganography

Steganography aims to hide the sensitive information inside the host message (cover message). This technique is done by two persons and anyone else cannot know that. Whenever it is difficult to detect the stego-message by the third party (adversary, attacker), the algorithm considered excellent. In addition , the method is considered excellent if the attacker finds it difficult to remove or destroy the secret message [35] [46]. We conclude from all of these that the main objectives of steganography are:

#### 2.3.1 The Storage

The amount of sensitive information that can be hidden inside the cover or host. A large amount of hidden information means the best algorithm [47] [48].

#### 2.3.2 Undetectability

its represents image quality, If the attacker finds it difficult to detect the message present inside the cover or host message, that means the algorithm is excellent. The detection depends on the amount of distortion and degradation generated in the stego-cover. The amount of distortion depending on the amount of the hidden information. Therefore, there is a

direct relationship between the size of hidden information and the detection. Undetectability in stego-image can be measured and calculated by signal-to-noise-ratio (SNR) [47] [48].

### 2.3.3 The Robustness

It means how the stego-cover is robust and resistance against the attacks to remove or destroy the hidden information, considering the high robustness is one of the features of the excellent algorithm [47] [48]. Thus, difficult to obtain the three aims together (Undetectability, Storage, and Robustness). Where it is possible to achieve any two elements together, but on the as expense of the third element. For example, if the algorithm is characterized by high storage quality as well as high image quality (Undetectability) it be end very weak in front of malicious attacks, as in the Least Significant Bit (LSB) technique. [47] [48] [49]

## 2.4 Methods of Hiding

There are mainly three methods to hide data: injection, substitution and generation. [46] [48]

### 2.4.1 Injection

It is one of the embedding techniques, in which the secret information is embed in parts of electronic files (cover) which are avoided the process by the processing application. [46] [48]

### 2.4.2 Substitution

In this method, the substitution (changing) is made in the Least significant bit information of the host file or any selected bits by the bits of the secret information. [46] [48]

### 2.4.3 Generation

This does not require an existing cover file but it generates a cover file for the one aim of substituting the least significant bits. unlike injection and substitution methods. [46] [48]

## 2.5 Steganography's Media

The internet provides a broad range of communication where the information distributes to different styles, such as an image, text, video which are consider as important covers to hidden the sensitive information in various techniques. In steganography techniques, it use the digital formats with a high degree of excess or redundancy. Redundancy represents the bits of the object (cover) that provide the high accuracy of the cover when used and display. [50] [51]

There are four main of file formats used to hiding information [52] [53]

1. Text steganography.
2. Image steganography.
3. Audio/video steganography.
4. Protocol steganography

### 2.5.1 Text Steganography

Embedding the sensitive information in file formats (text) represents the oldest methods used, which hide information inside characters of text. It is difficult to use text that have a weak and simple format as a cover to hide information, where then any slight change occurs, it easily could be detected. While the complex text could easily be used in different techniques. This method not preferable because the text contains of a small amount of excess data compared with image or sound. There are main methods to hiding information inside text (line-shift, word shift, and feature) , after embedded secret information inside a text file, a cover- Text

is gotten. [54] [55]

## 2.6 Image Steganography

Images are more common and popular on the internet [21]. In addition, images have a very high amount of redundant information especially, that have a high contrast between the values of adjacent pixels. Therefore, images are the more used in steganography [30] [56]. The sensitive information are hidden inside the digital image using secret key (algorithm) then a stego-image is obtained [11]. The recipient used the same key to extract the secret message. The gray (8-bit) and color (24-bit) images can be used whenever the images have gradients color, contrast regions and severe or solid colors these consider the best to hide the secret information. these features make the effects of the hidden information (the secret message) imperceptible to the human visual system. [18]

### 2.6.1 Audio Steganography

The sound is used as a cover to hide the secret information in this method. This method is more difficult in comparison to other covers that based on the images. The human ear predicts very sensitive changes, therefore, the points weaknesses of the human ear was to exploit to hide information in form undetectable from the human ear. The human hearing system senses higher frequency sounds than low-frequency sounds, some audible sounds become inaudible if there is higher audible sound than these sounds. According to the above, the best channel is select to hide the secret information . [34] [52]

### 2.6.2 Protocol Steganography

The term protocol steganography is used for embedding information within network protocols such as TCP/IP. The information in this case is

hidden in the header of a TCP/IP packet in some fields that can be either optional or are never used. [52]

## 2.7 Steganography Techniques

There are many methods for classification of the steganographic techniques. It can be classified relative to the type of cover or based on the used method to hide information [57]. In addition, there is a classification based on the type the changes or modifications that occur to the cover image during the embedding information [58]. In this section will focus on the Steganographic techniques. [30] [33]

### 2.7.1 Spatial Domain Method

There are different techniques depending on the spatial domain. In this technique, the message bits is hidden inside the cover bits (color image, gray image), and message bits are replaced with the unneeded or redundant bits of cover. [46] [59]

The technique that depends on the spatial domain is considered as the simplest techniques of steganography. The disadvantage of the technique is the amount of noise and damage additive to the cover image, therefore affect directly on the statistical properties of the image. These techniques using with the uncompressed images such as (TIFF and BMP). The most popular method in the spatial domain is the least significant bit (LSB) [1] [60], where the pixel's values of both the image and message is converted to the binary representation then used the image bits to hiding the message bits. [61] [62] [63]

The embedded data accompanied often with some distortion in the image, but often it is undetectable by the human eye. The images with a large size when the compressed by the JPEG algorithm the amount of information will reduce, this reduction leads to destroy or damage the secret message. [50]

Some techniques depend on the spatial domain: [10]

- Least Significant Bit (LSB)
- Pixel value differences (PVD)
- Gray Level Modifications (GLM)

### 2.7.2 Transform Domain Method

Due to weak resistance and robustness in spatial domain algorithms and the fast development of computing devices, to achieve more secure information, a new algorithm is emerged which are more robust and resistance against attacks. In this technique the secret information is embedded using the frequency domain [46]. The algorithms that work, based on the transform domain, are more robust and resistance than those depending on the spatial domain. The message information is hidden in the (transform space) of a signal, where used the high difference regions to hide information. In addition, it hide information in regions that are least exposure to operations (compression, image processing, cropping, etc.), therefore, it is undetectable and more robustness and resistance against attacks than the spatial domain. [64] [65]

The following types depend on the transform domain technique: [66]

- Discrete Cosine Transform (DCT)
- Discrete Wavelet Transform (DWT)
- Discrete Furrier Transform (DFT)

### 2.7.3 Statistical Method

In this method, modulation and modification are done on some of the statistical features of the cover image. Where the amount of modification and manipulation are very small and able to take advantage of the weakness of the human visual system to detect luminance differences. In this method, a small message can be hidden many times in the cover, and, the presence of (1-bit) is exploit from the cover image to



hiding the secret information inside it. Thereby in order to be embedding (1-bit), simple modification must be done on the cover image imperceptible. Another technique is by processing the message signal and comparison it with the cover signal, this method called "masking" which characterized by the high robustness against the image processing operations such as compression, cropping. [12] [46]

#### **2.7.4 Distortion Method**

Knowing the details of the original image before the process embedding of the secret information is very important. The encoder adds a series of changes to the cover to hide the secret information. On the other hand, the decoder makes a comparison between the cover image and the noise image to extracted in hidden information. Where, the cover-image will subject to a sequence of modifications, which selected based on the secret message required to transmit and get on the stego-cover. The sender did these modifications. The recipient measures the difference between two images to restore the secret message. For example, the modification of the value of the cover pixel to hide the message bit. [46] [67]

#### **2.7.5 Spread Spectrum Techniques**

The message is transferred under the noise level for any specified frequency, when this used with the steganography. The spread spectrum either adds a random noise to the cover image or work as noise with the cover image. [33]

#### **2.7.6 Cover Generation Techniques**

This type is unique when compared with the rest in which the cover image is chosen to hide the sensitive information inside it. Where a cover can be created for the purpose of mainly is hiding the secret information [46].

## 2.8 Types of Steganography

There are three types of Steganography as shown in figure (2-3) [48]

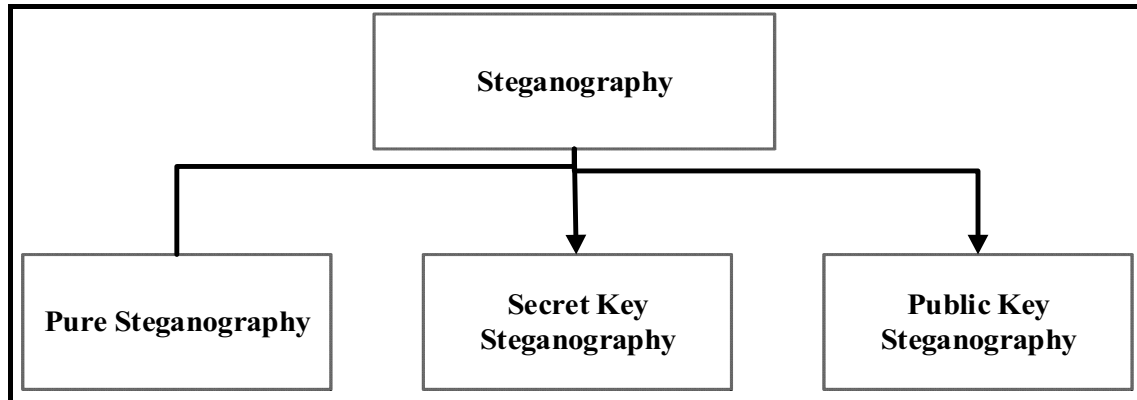


Figure 2-2 The types of steganography [49]

### 2.8.1 Pure Steganography

In this type, the system of steganography does not need to a secret key to exchange some of the secret data. The equation (2.1) shows the process of embedding. [48]

$$E = C \times M \rightarrow S \quad (2.1)$$

Where

- $E$  Encoding algorithm (embedding phase)
- $C$  represent the groups of possible carriers (Covers)
- $M$  represent the groups of the possible message (secret information)
- $S$  represent the Stego-cover (cover+message)

The process of extraction should be followed The relationship shows (  $D: S \rightarrow M$  ) . **Where**,  $D$  = decoding algorithm, in this step the extracting of secret information (message) from the stego- cover ( $S$ ) is done. The size of cover (  $C$  ) must be greater than or equal the size of the message ( $M$ ) as in the relation (  $C \geq M$  ) . Moreover, both sender and recipient must access to the embedding and extraction method (algorithm). The algorithms must be secret not public. [2] [10] [48]

### 2.8.2 Secret key steganography

A secret key is used to hide the secret information. The first party (sender) select a cover (C) to hiding the secret message (M) inside it by using the secret key (K), i.e. the proposed algorithm. The second party (recipient) use the same secret key (K) to reverse the embedding process and extract the secret message (M) from the cover (C). In this type, anyone else except the sender and recipient must not know the secret key used to hide the information. [2] [31] [48]

Equations (2.2) and (2.3) show the process of embedding and extracting respectively

$$E_K = C \times M \times K \rightarrow S \quad (2.2)$$

$$D_K = S \times K \rightarrow M \quad (2.3)$$

### 2.8.3 Public key steganography

Two keys are used, one is special (private) and the other is general (public). The public key stored with the general information base. The public key(general) used to hide information in embedding process, either the special key (secret) used to retrieval the message from the cover in the extraction process. This type utilizes, in fact, in the steganographic system can be used or apply the extraction function (decoding) on any cover whether it contains hidden secret information or not. [2] [31] [48]

## 2.9 Digital Images

The image is a two-dimensional (2D) matrix, composed of small elements called pixels, digital images are images that can be stored, modified and sent in an electronic file, which can be modified using a computer or intelligent device such as mobile phone. each pixel is composed of smaller units called byte, in addition, the byte may consist of

other smaller units called bit. Typically, the digital images classified according to the colour, number of bits (start depth) required to represent the specified pixel and even according to the image features format .for example (2 bit ,8 bit and 24 bit) (colour and gray) ,(BMP and JPEG) [31] [68]. **Digital images** are divided into types as described in the following points:

### 2.9.1 Binary Images

Binary Images are the simplest type of the images. This type takes one (1) bit to represent each pixel. where the value of pixel takes of either (0) or (1), the value (0) represent the black colour, either (1) represent the white colour [30]. This type of images used in X-ray imaging, optical character recognition (OCR). [31] [68]

### 2.9.2 Gray-Scale Images

One pixel contains on one byte, each bit contains on 8bit, 8bit/pixel (8 BPP) In this types, the number of bits used for each pixel represents the gray level available. These means exist 256 gray level (0-255) to represent an image, where (0=black, 1= white), thus it contains grayscale information, no colour information. Can has derived the binary image from the grayscale image by determining the threshold, where any value greater than the threshold to (255) white (1), either less than the threshold to (0) (black). This types used in many fields such as medical, astronomy application [31] [68].

### 2.9.3 Colour images

Types of images contain main colour bands three (Red, Green and Blue), others colours result from mix any two colour from these colour (RGB) in percent different. In a computer, being storing three values for each pixel (RGB) after display this values on monitor generate the colours.

Each colour band represent by 8-bit, 1 pixel =3byte=24bit 24bpp (8R, 8G, 8B) =  $256 \times 256 \times 256 = 16777216$  L. That means in each pixel contains on (16777216 levels colour available). This system is called RGB system. [31] [68]

#### 2.9.4 Multi-spectral Images:

Types of images often contain information outside the Human Visual System (HVS) range, such as Ultraviolet, Infrared, Acoustic, Radar images. This types from the image can sense it and displayed as visual by covert the spectral bands to RGB system. [31] [68]

#### 2.10 Least Significant Bit (LSB)

The least significant bit (LSB) is one of the most common and easiest methods of sensitive information hiding in the spatial domain (steganography) [5] [8] [35]. This method can be applied to different image formats such as (BMP and TIFF) to convert both of the cover image and the secret message to the binary form. The binary form is representing by a series of numbers of zeros and ones. Hiding the sensitive information must determine the place of the specified bit hide the message bits inside it, the gray image consisting of one byte per pixel (BPP) that means the pixel equal to byte. [4] [10] [46] [69]

**Start Depth (SD):** Represents the number of positions that can be exploited to insert the secret messages bits inside it, therefore, it represents the number of bits per byte of the cover's bytes (image, voice or text). in case using a gray image (8 bit) that means, the series (SD) starting from (0 to 7), where start depth (SD=0) corresponds to the first bit (1) and (SD=1) corresponds to the second bit (2) and continue to the last bit (8), where corresponds to the start depth (SD=7).

More Distortion				Less Distortion				
More Robustness				Less Robustness				
								
8	7	6	5	4	3	2	1	No. Bits
7	6	5	4	3	2	1	0	Start depth (SD)
$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$	Decimal conversion
128	64	32	16	8	4	2	1	Decimal weight
MSBs				LSBs				

Figure 2-3 Distribution the bits within the byte [10]

It could be noticed in the figure (2 4), that the rightest bits have less size and caused less distortion in the cover image, undetectable by the human eye. But at the same time have less robustness and the resistance against the attacks or operations (cropping, compression, and an image processing operation) [70]. Either (most-left), bits have more size and more robustness against the attacks or image processing operations but result in a large amount of distortion and damage in cover image detectable by the human visual system. In color image, that contain three compounds basic: (Red, Green, and Blue) and called (RGB), each of these colors is one byte = 8bit, RGB =3byte =24bit [10] [71] [72]

RED	8	7	6	5	4	3	2	1
	$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$
GREEN	8	7	6	5	4	3	2	1
	$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$
BLUE	8	7	6	5	4	3	2	1
	$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$

Figure 2-4 Bitmap distribution inside pixel in color image (RGB)

Using 8-bit grayscale images is the best option, due to fact that their palette is less varied than the 24-bit color images, therefore, it is very difficult to detect the hiding secret information by the LSB insertion from the human visual system (HVS). [46]

Using Least Significant Bit (LSB) to hide the secret message, each bit of the message can be hide inside one pixel of the cover image. This process produces a simple change in the cover image and is able to hide a large amount of the sensitive information inside the image in form that is undetectable by the human eye. [10] [25]

The information can be hide using deferent start depth (SD=0 to SD=7). Where, whenever moved towards (Most-Left) the amount of distortion increases and the image quality is affected this due to the bit's weight [29]. The distortion in the image quality is very low when used the first bit due the weight's bit is small (1), either with use bit that has a larger weight as in the case of the (SD =8,7 – 128,64), it could be note that the amount of deformation in the picture is easily detectability by the human eye. [71] [72]

The advantage of LSB method is high capacity to hide information and undetectability by the human visual system (HVS), either disadvantage is less robustness (the weakness) against the attacks of lossy operations such as (cropping ). [71] [72] [73]

### **2.10.1 Embedding methods of LSB Steganography**

Two methods are the embedding of the secret information in LSB method are: [35] [46] [48]

#### **2.10.1.1 Sequential Method**

In this scheme, the algorithm start encodes at the first pixel of the host file (cover) at point (0,0), and continues the embedded process to last bit of the secret information. [46] [48]

### 2.10.1.2 Randomized method

The specified regions of the cover file are select in order hide the secret information, these regions have good properties that help to hide the message in form undetectable by the attacker. [35] [46]

## 2.11 Image Compression

The time and cost of sending different data are very important in our time, with existence, a large and different amount of data files which being exchanged on the internet in these days. The time and cost of sending data correlate to their size, i.e. small size data file sent very quickly and with a low cost compared to the same file but with larger size, therefore, image compression become more important than anything else. Image compression process is applied to reduce the size of data required to represents the digital images, this data is strongly related with the visual information, and requires a large capacity to save them. In this process, data is compressed, therefore reduce the requirements of storage capacity and also reduces the transmission time. Image compression may result some degradations in image quality because of removal of some important data, so, image compression used to reduce file size by eliminating some unnecessary information in the image and maintaining the necessary information [31] [74]. The main idea of the image compression is finding redundancy of an image pixel which has weakly correlated with neighboring pixels, so the main aim of the image compression removes redundancy in the images(pixels). Image compression is one of the different methods in the digital images processing, which use different mathematics formulas to analyze and determine the repetition regions of information to produce files with smaller sizes [75] [76].



### 2.11.1 The main Aims of Image Compression

1. Reduce the amount of data required to represent image information such as (color, intensity). [76]
2. Reduce memory required to save images and time required to send them. [76]
3. Reduce the cost of sending of images.
4. Reducing the numbers of bits required to represent the image information. [74] [76]

### 2.11.2 Image compression Methods

#### 2.11.2.1 Lossy compression

The small image data (small detail) are removed in this method, and the image details are similar to that undetectable by the human visual system. Therefore, producing a small size file, results in an image which is very close to the original image, but is not similar to it completely. The original uncompressed image cannot retrieve from the compressed image. The best model and more common that used is the lossy compression technique of the JPEG (Joint Photographic Experts Group). In this type, the produces degrade and decrease the image quality. [76] [77]

#### 2.11.2.2 Lossless compression

The lossless compression is completely different from the first type (lossy compression). In this type image information represented in mathematical formats and any data does not remove from the original image, therefore, a matched image is produced which quite similar to the original image. The original image uncompressed can retrieve from the compressed image. This technique of compression known also as noiseless, since it never adds noise to the image. It's also used with some applications such as medical imaging (BMP and GIF) formats represent examples for this type. Often the standard compression of images is JPEG,

which gives greater compression but with a loss in image quality. JPEG is unsuitable for most applications especially, those which required high storage space. [74] [76]

### 2.11.3 JPEG Compression

Joint Photographic Experts Group created the JPEG standard in 1980, where considered as one of the most popular compression standards. JPEG has been developed to provide the compression tools of efficient and flexible, and aims to reduce the file size of the image but leads to decreases in image quality by eliminating the least important or unnecessary of information. The reduction of the size of the information become very necessary to send it in less time and cost. JPEG has four modes of operation namely baseline, hierarchical, lossless and progressive which are designed to support various image applications. Many applications use the Baseline series coder/decoder compression. In addition, there are some applications don't used this mode from JPEG. JPEG compression is a technique for lossy compression, the original image and the image resulting after applying JPEG algorithm are not similar completely. In addition, the image quality is different [78] [79]

### 2.11.4 JPEG Algorithm Steps

JPEG algorithm is work in several steps:

- ❖ First step: convert the pixels of the image (RGB) into color space (luminance Y-chrominance  $C_b$   $C_r$ ), (i.e. Y U V). [31]
- ❖ The chrominance component is down sampled in order to reduce the image size, where the human visual system (HVS) is more sensitive to small changes occurs in luminance than chrominance changes. [31]

- ❖ The pixels of an image are divided into blocks, each block contain a (8×8) pixel. Then a Discrete Cosine Transform (DCT) is used to convert the values of the block from spatially into (8×8) frequency, which consists of coefficients, representing the mean of value for all block individually and have different values some high frequency or low frequency [31]. as in figure (2-5)

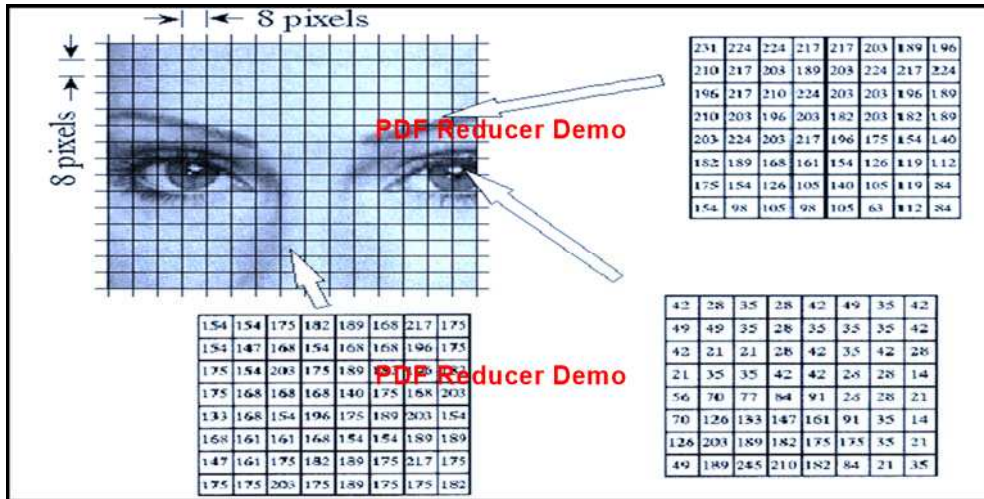


Figure 2-5 The block (8×8) pixel

- ❖ All blocks are individually quantized then; the result value is rounded from table of quantization to an integer. In this step most of the coefficients which are representing the higher frequency are reduced to zero. This process is acceptable when the higher-frequency information is deleted and not result in large changes in the image. On the contrary, a small change visually detectable will produced. Most data reduced through the steps of JPEG algorithm, especially in the quantization process. [31] [74]
  - ❖ After reducing the coefficients in the quantization process, Huffman coding is used to reduce the size of the image significantly. [31] [74]
- Figure (2-6) illustrates the encoding (compressed) and decodes (uncompressed) steps for images using JPEG algorithm: [76]

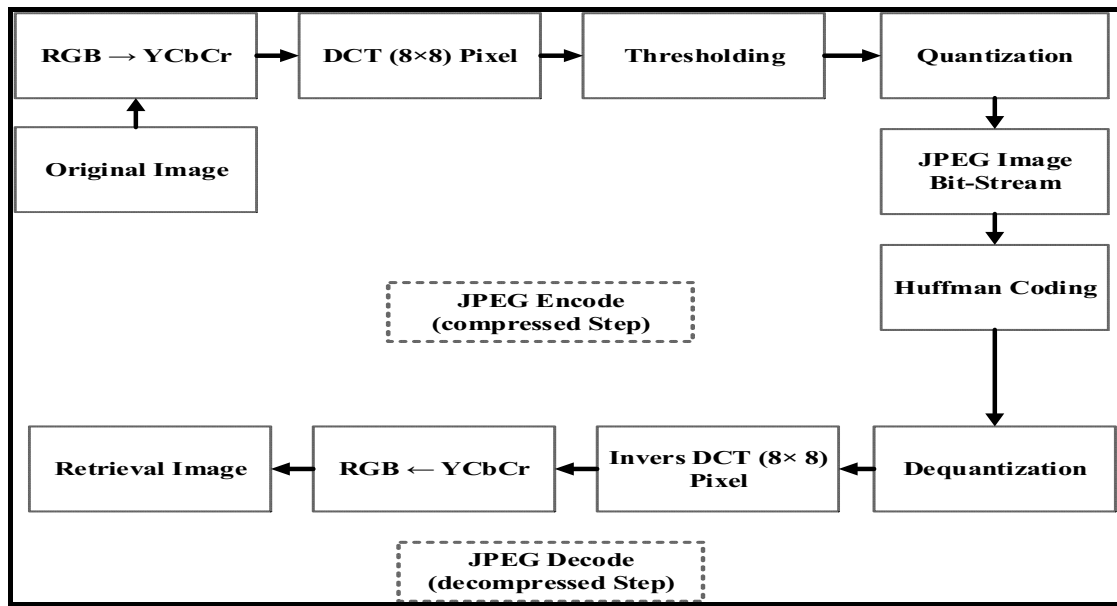


Figure 2-6 The JPEG Compression Scheme [76]

## 2.12 Statistical Measurements

In this thesis, some statistical measurements will be used to calculate the cover-image quality, to measure the amount of the difference between the original image and Stego-image, to measure of the amount brightness of the image and to calculate the amount of contrast between the values of images. These measurements are made before and after the embedding phase, in addition, before and after the implementation of JPEG attacks.[2]

### 2.12.1 Mean:

Mean is represent a brightness average value of image ,measure the general brightness of the image, where the sum of all values of the image is divided by the size of the image (m×n) [2].

$$mean = \frac{1}{mn} \sum_{x,y} (f_{x,y}) \quad (2.4)$$

where

- $f_{x,y}$  Original image
- $mn$  The size of image (No. of rows and columns)
- $x, y$  The coordinates of the pixel in rows (x-axis) and columns (y-axis)

### 2.12.2 Standard Deviation ( $\sigma$ ):

a scale which represent the square root of variance and used to measure the value of image pixels relative to the image mean (i.e. higher and lower the image mean). [80] [81]

$$\sigma = \sqrt{\frac{1}{mn} \sum_{x,y} (f_{x,y} - mean)^2} \quad (2.5)$$

### 2.12.3 Variance:

A parameter or scale that give information about the contrast of the value of image, where the higher contrast image indicates the existence of a high variance between the values of images, and the smaller contrast image indicates to lower variance between the values of images. The relationship between variance and contrast is linear. [80] [81]

$$variance (v) = \frac{1}{mn} \sum_{x,y} (f_{x,y} - mean)^2 \quad (2.6)$$

### 2.12.4 Mean Squared Error (MSE):

The scale used to calculate the difference between the pixel color of the original image and noise image (stego-image) [82] [83].

$$MSE = \frac{1}{mn} \sum_{x,y} (f_{x,y} - f'_{x,y})^2 \quad (2.7)$$

Where  $f'_{x,y}$  Noise image (stego-image)

### 2.12.5 Signal-to-Noise-Ratio (SNR)

The scale used to calculate the image quality, by is calculating the ratio between the mean of original image and the mean of noise image (Stego-

image), therefore it measures how the original image is affected by the added noise (secret information) [2] [82].

$$SNR = 10 \log_{10} \frac{\text{mean}(f_{x,y})^2}{\text{mean}(f'_{x,y})^2} \quad (2.8)$$

# *CHAPTER THREE*

## *THE PROPOSED*

### *SYSTEM*

## Chapter Three: The Proposed system

### 3.1 Introduction

In this chapter, the methods of hiding information (steganography) will be suggested, where the standard Least Significant Bit (LSB) technique will use to hide the secret message in two form (ASCII, Text-image) inside the gray image as a cover. The bits are embedded at average bit per pixel (bpp) of the cover with the use of all eight image bits (SD=0 to SD=7). Then the quality of the image after the embedding using the statistical measures (Mean Square Error (MSE), signal-to-noise ratio (SNR)), are calculated. The image is then attacked using a lossy compression algorithm (JPEG) with a different compression quality ranging between (100-50). After the attack the quality of the cover as well as the quality of the message are calculated to know how the message is resistance and robust against the attack (which represents the aim of the thesis).

To overcome the effect of JPEG attack on the secret message which is embedded by LSB technique, we will propose a new algorithm to hide the secret message (ASCII) inside the gray image as a cover. The aim of the new technique is to overcome of the damage caused by the attack via JPEG algorithm, where we noticed that the least significant bit technique is not robust against the attack, therefore the hidden message suffers from disastrous and devastating deterioration after the attack. A new algorithm is designed in a smart way to be compatible with the JPEG algorithm, where the image is divided into blocks, each block consists of (8×8) pixels, as in the case of JPEG algorithm. The JPEG algorithm maintains on the image mean, therefore, we will use this feature to create and design a new algorithm (new statistical steganography method).



The results of the proposed new method (a new statistical steganography method) are assessed using several tests, statistical measurements like Image Mean, Standard Deviation ( $\sigma$ ), variance, mean square error (MSE) and Signal to Noise Ratio (SNR), were done to calculate the quality of the cover image after JPEG attack. Moreover, the percentage of the affected bits (error percent in the retrieved message) was estimated by calculation of the quality of the retrieved message after the JPEG attack.

In this work, we will use two algorithms to hide the information (steganography), the first is standard (LSB) technique and the second is a new proposed method (new statistical steganography method), which will be more robust and resistant against JPEG attacks as will be seen in chapter 4 (Results and Discussion). These algorithms are as follows:

1. Standard LSB technique to hide secret information (ASCII & Text-image) within the cover (image) using Least Significant Bit (LSB) Steganography.
2. The new Proposed algorithm (statistical method steganography) to hide secret information (ASCII) inside cover (image).

Type of gray image can be used in this work is bitmap (BMP) as a cover image to hide and carry the secret information. Two images were used, first: is standard Lena image, and the second: is standard Baboon image. Each image has certain advantages so in the work we use more than one image to show the importance of the image used in the process of hiding information (Steganography). The dimensions of the image used in this work are (512×512), in both Lena or Baboon image. as shown in figure (3-1) a and b.

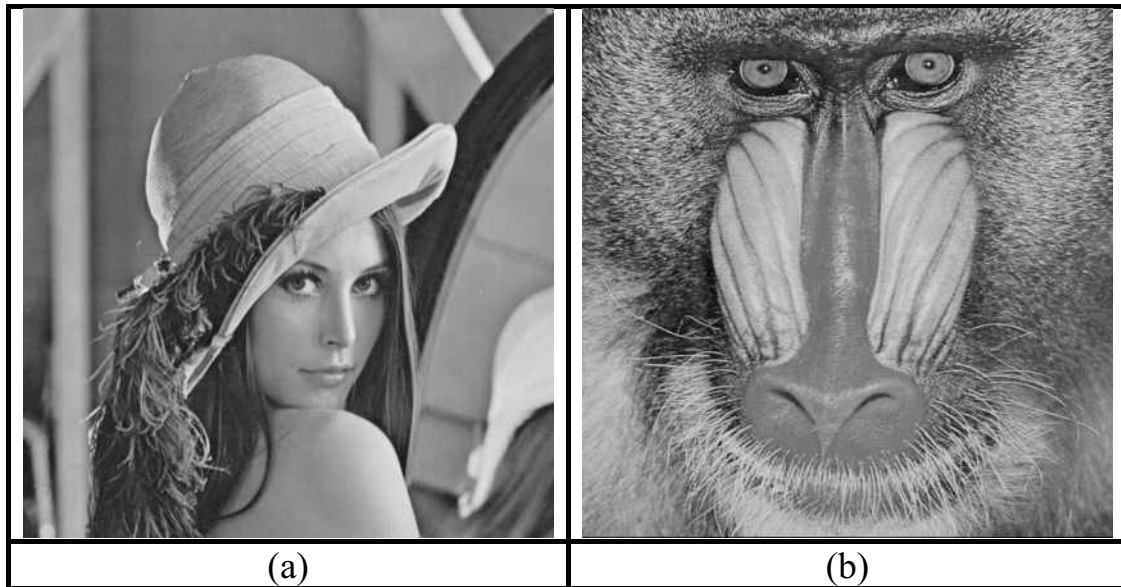


Figure 3-1 Sample images (a) Lena and (b) Baboon (size 512×512 pixel)

### 3.2 The Standard least significant bit (LSB) technique

The standard LSB steganography technique is used to hide the secret message within the cover image. One byte of the cover image was used to embed one bit of the secret message, and the embedding process done by different starting depth (SD) ranging about (0-7).

Two different formats of The secret message (ASCII and text-image) were used. The cover image used is a grayscale image of type BMP (8 bit), which contains a lot of features that make it distinctive and also important in the field of information hiding, as in the case of Lena and Baboon images. The standard Lena gray image contains different regions (smooths & variance), while, the Baboon gray image is characterized by the high variance between the values of adjacent pixels, which make these images very suitable for use in information hiding (steganography). This is because it is difficult to detect the existence of hidden data by the human visual system (HVS). In LSB method we used the sequential scheme to embed the message's bits within the cover's bits without selected some specified bytes as the random scheme.

**LSB Technique steps:**

The work steps of LSB technique works based on the following steps:

1. Selection of the cover-image (Grayscale BMP (512×512)).
2. Selection of the secret message in two different formats (ASCII and text-image).
3. The relationship between the size of cover image and secret message represents as the equations (3-1 a) and (3-1 b):

$$\textit{Size of Secret Message} \leq \textit{size of cover-image} / 8 \quad (3-1 a)$$

$$\textit{No. of message's bits} \leq \textit{No. of cover's bits} / 8 \quad (3-1 b)$$

4. Determine of the starting depth (SD) ranging from (0-7).
5. In Encode Phase: starting the embedded process where embed one bit of a secret message within one byte of the cover image. (the Sender)
6. After the embedding process, obtain on the stego-image. (cover image + secret message).
7. Performing the JPEG attack using its standard algorithm (by Irfan view Program) on the stego-image with compression quality ranging between (100-50).
8. In Decode phase, apply the LSB technique to extract the retrieved secret message after the JPEG attack. (the recipient).

In order study and know the effect of the JPEG algorithm attack on the Least Significant Bit (LSB) steganography, steps were suggested:

1. Using only one bit of the cover's bits to embed the secret message's bits with a starting depth (SD) ranging about (0-7).
2. Using two different formats of secret message (ASCII and text-image).

3. After applying the LSB technique, we perform JPEG attack on the stego-image using the standard JPEG algorithm (this attack is done by Irfan view Program) with the quality compression different from (100-50).
4. Measuring the quality of stego-image after the embedding phase and after the attacking by the JPEG algorithm.
5. Finally, calculation of the error percent in the retrieved message to find message quality after the JPEG attack.

The quality of the image before embedding and after the attack is measured using some statistical measurements, i.e. Image Mean as in the equation (2-4), Standard Deviation ( $\sigma$ ) as in the equation (2-5), Mean Square Error (MSE) as in the equation (2-7) and Signal-to-Noise Ratio (SNR) as in the equation (2-8).

Figure (3-2) Block diagram shows the standard least significant bit (LSB) algorithm works in both cases, encryption (embedding) and decryption (extraction).

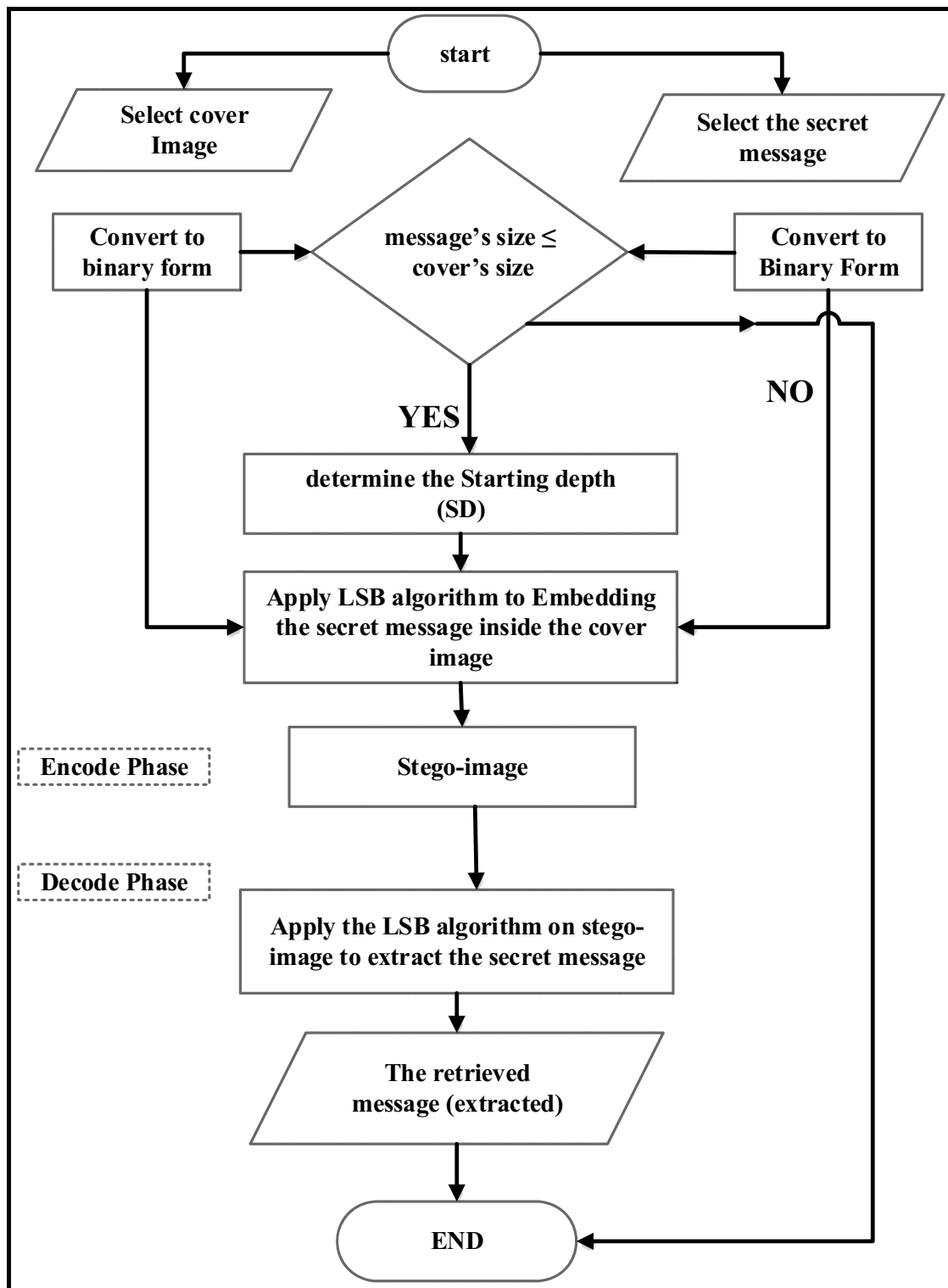


Figure 3-2 Block diagram of the standard Least Significant Bit (LSB) steganography

The figure (3-3) illustrate how to calculate the quality of both stego-image and the retrieved message after JPEG attack on the hidden message using (LSB) technique with compression quality ranging between (100-50).

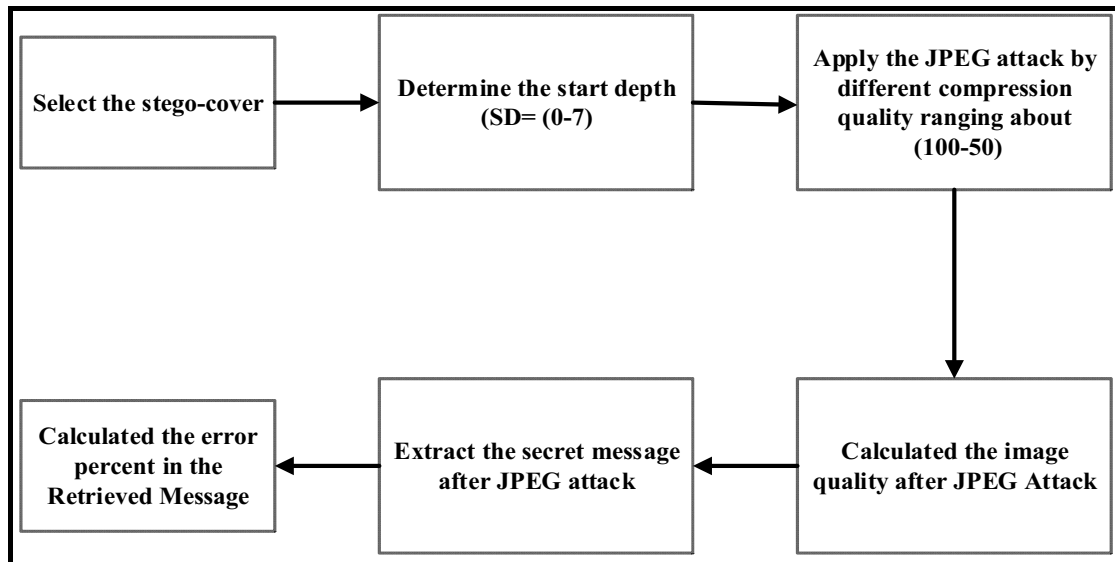


Figure 3-3 scheme the quality Calculation image and message after JPEG attack on the hidden message using (LSB) steganography.

### 3.3 The Proposed Algorithm (NSSM)

A new method was proposed in this thesis to hide the secret information (ASCII) within the carrier image (Grayscale, BMP). The proposed algorithm is called (A New Statistical Steganography Method). The new method is designed in a form that is similar and compatible with the JPEG algorithm, in which the image is divided into blocks, each block contains on  $(8 \times 8)$  pixel. The secret message's bits are embedded into the blocks of the cover image. Only one pixel of the block  $(8 \times 8)$  pixel is assigned to embed the message, while the mean and standard deviation ( $\sigma$ ) are calculated to remaining (63) pixels. In this method, the secret message' bits are embedded inside the cover image using value of ( $\sigma$ ) ranging about (1 to 25). A single bit of message bits is embedding within each block  $(8 \times 8)$  pixel of image's blocks.

#### The proposed algorithm steps:

The proposed algorithm designed and works as follow:

1. The cover-image is divided into blocks.

2. Each block consists of (8×8) pixel as shown in figure (2-5) compatible with the JPEG algorithm. In the JPEG algorithm all blocks containing (8×8) pixel.
3. One pixel of all block (8×8) pixels is selected which is the center pixel.
4. The mean and The standard deviation ( $\sigma$ ) values of each block (8×8) pixel are calculated without the contribution of the center pixel.
5. The threshold value is determined for the ( $\sigma$ ) to choose the block as a valid location to embed the secret message's bit.
6. The marked pixel is replaced by the modified mean value ( $V_n$ ) based on the value of the planted message's bit, as in equation (3.2).
7. The standard deviation value was adding or subtract from the block's mean after multiplying it by the difference's value to block's mean, if the bit's value is equal one otherwise, we subtract standard deviation value multiplied by the difference's value from image's mean. Shown in equation (3.2)

$$V_n = \begin{pmatrix} \mu + \omega\sigma & \text{if message bit} = 1 \\ \mu - \omega\sigma & \text{otherwise} \end{pmatrix} \quad (3.2)$$

Where:

- $V_n$       The new value for the centered block pixel
- $\omega$         The difference factor ( $\omega > 0$ )
- $\mu, \sigma$     the value of mean and standard deviation ( $\sigma$ ) of each block (8×8) pixel in the cover image without the contribution of the centered pixel

Each block (64) pixel can hide one bit from the secret message. So must be find the size of the cover image and size of the secret message, according to the equations (3.3 a) and (3.3 b):

$$\text{No. of blocks} = \text{the size of cover image} / 64 \quad (3.3) \text{ a}$$

$$\text{The size of secret image} \leq \text{No. of blocks} / 8 \quad (3.3) \text{ b}$$

Starting embedding the secret message's bits within the blocks of the cover image from the left corner at the top to the right corner at bottom. After complete embedding all bits of the secret message inside the cover image, we get on the Stego-Image.

In order to study the effect of JPEG attack on the embedded message in the stego-image, the following steps were suggested:

1. Selecting the cover image (Grayscale Bmp).
2. Selecting the secret message (ASCII).
3. Embedding one bit of the secret message within one block of the cover-image with various difference value (DIF=1 to 25).
4. Performing JPEG attack on stego-image (by using Irfan view program) with compression quality ranging between (100-50).
5. Calculating the cover-image quality after applying the proposed algorithm and after the JPEG attack.
6. Calculating the retrieved message's quality after JPEG attack, by finding the error percent of the affected bytes.

The (NSSM) proposed algorithm works in the two cases, encoding (embedding) and decoding (extraction), as shown in figure (3.4):



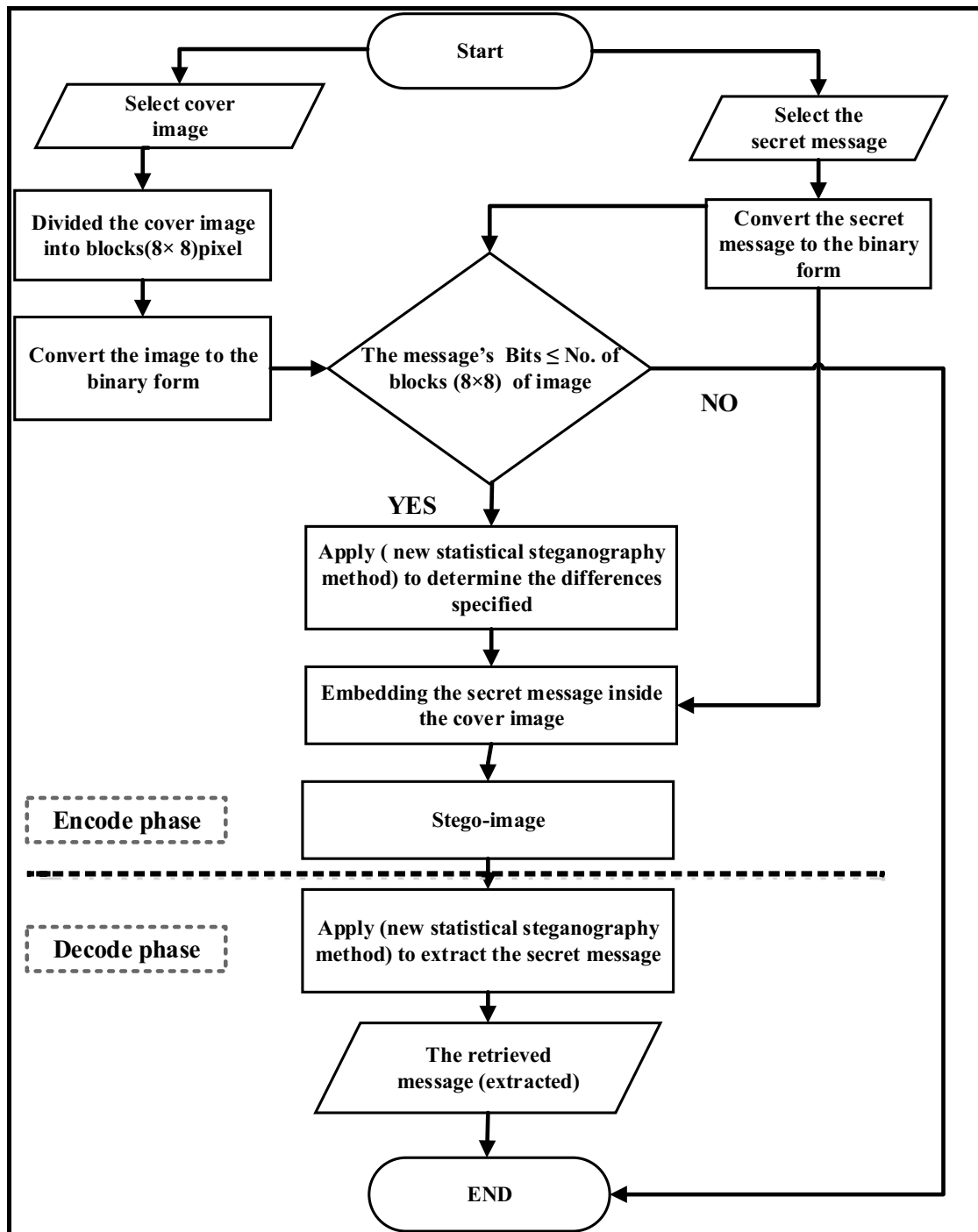


Figure 3-4 Block diagram of new Statistical Steganography Method (NSSM)

Figure (3.5) illustrate the hidden message using the (NSSM) and the quality calculation for both cover image and the message using a different compression quality range between (100-50) after the JPEG attack.

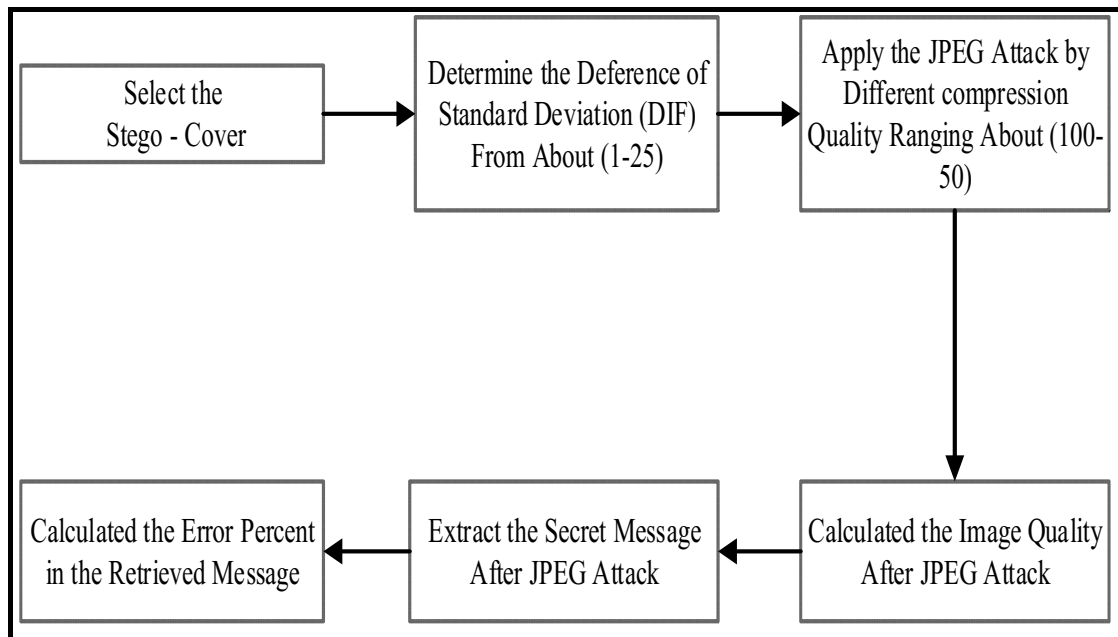


Figure 3-5 Scheme the quality calculation of image and message after JPEG attack using the (NSSM) steganography

*CHAPTER FOUR*

*RESULTS*

*&*

*DISCUSSIONS*

## Chapter Four: Results and Discussions

### 4.1 Introduction

The experimental results of the least significant bit (LSB) and the new adopted (NSSM) methods involved in this work are demonstrated in this chapter. The obtained results were also discussed in order to know the extent of their robustness and resistance to attacks using JPEG algorithm for different compression quality ranging from (100-50). Moreover, the amount of damage on both the cover-image and the hidden message were calculated using two grayscale (BMP) standard images (Lena and Baboon) with size (512×512) pixel. The standard JPEG algorithm adopted in the (Irfan View program) version 4.5 is used to perform the attack.

### 4.2 The Standard Least Significant Bit (LSB) Technique

The LSB steganography technique is a simple and popular method to hide (embed) the secret message within the cover image with two different formats (ASCII and text-image) using start depth ranging between (0-7) in case used Lena and Baboon image. Table (4-1) & Figure (4-1) show the stego image quality after embedding.

Table 4-1 The Stego-image quality (SNR &MSE) after LSB by using (ASCII & Text-image) messages, for Lena image

SD	SNR (ASCII) (dB)	MSE (ASCII)	SNR (Text-image) (dB)	MSE (Text-Image)
0	43.3746	0.495	43.3813	0.4942
1	37.3595	1.9774	37.3635	1.9756
2	31.3246	7.9355	31.3452	7.898
3	25.3258	31.5835	25.3105	31.6948
4	19.3306	125.5977	19.0706	133.3457
5	13.2129	513.7461	13.8165	447.0781
6	7.1986	2052.0156	7.6338	1856.2381
7	1.4452	7718.125	-0.032	10845.25

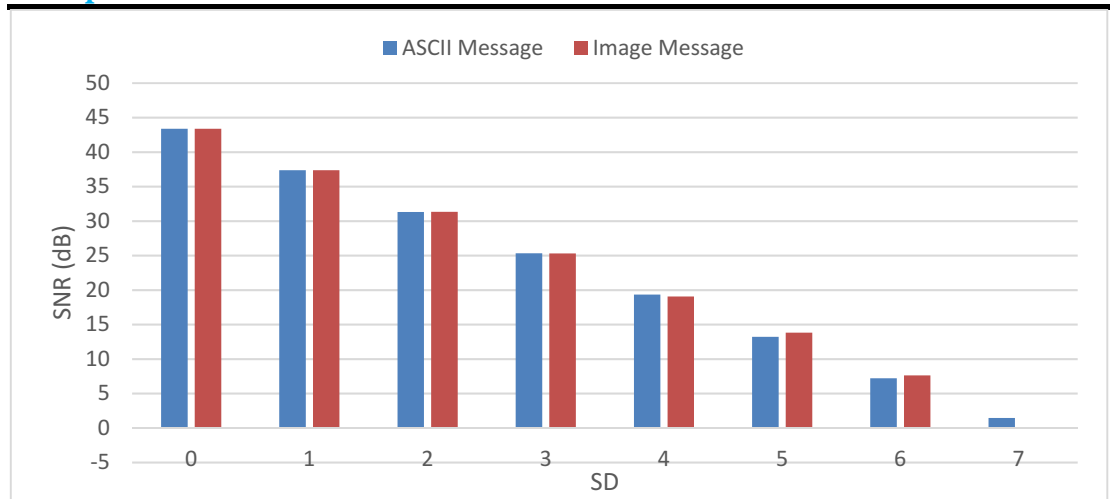


Figure 4-1 Stego-image quality (SNR) after LSB by using (ASCII & Text-image) messages for Lena image.

Table 4-2 The Stego-image quality (SNR &MSE) after LSB by using (ASCII & Text-image) messages, for Baboon image

SD	SNR (ASCII) (dB)	MSE(ASCII)	SNR(text image) (dB)	MSE (text image)
0	45.7676	0.4931	45.7546	0.4946
1	39.7367	1.9772	39.726	1.9821
2	33.724	7.8944	33.7072	7.925
3	27.6941	31.645	27.6915	31.6643
4	21.6523	127.2012	21.792	123.1748
5	15.6034	512.125	15.9782	469.7852
6	9.66811	2002.6563	9.34431	2164.7656
7	3.5843	8152.5	3.7904	7774.5625

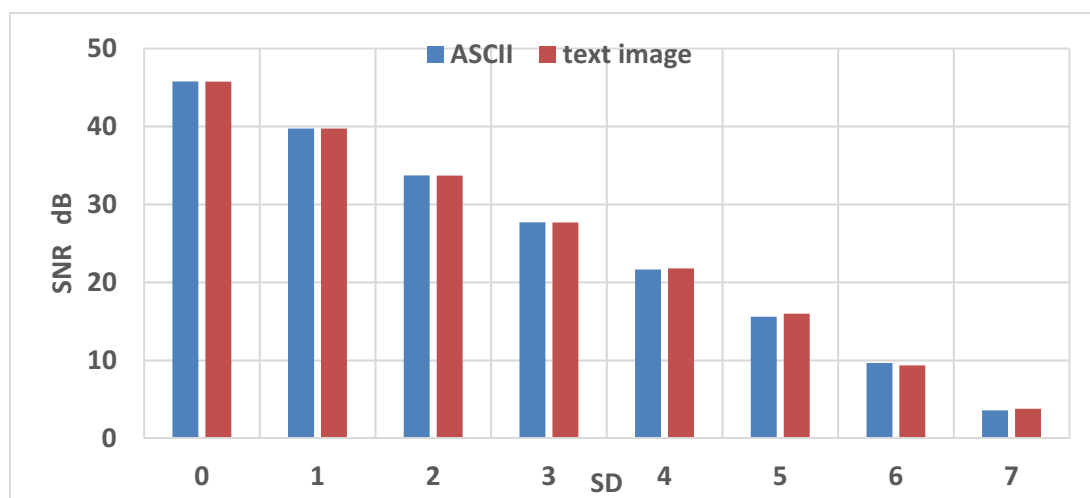
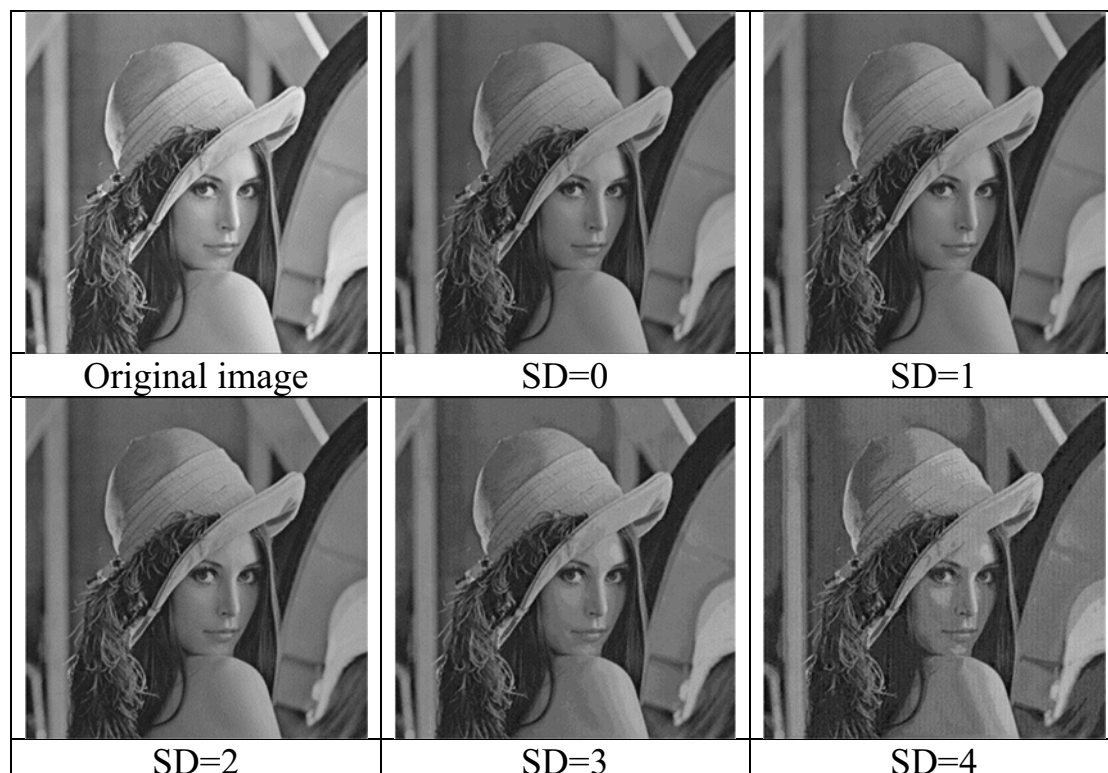


Figure 4-2 Stego-image quality (SNR) after LSB by using (ASCII and text-image) messages for Baboon image.

As shown in tables (4-1) and (4-2) and figures (4-1) and (4-2), the change in the stego-image quality after embedding the secret message's bits using LSB technique is very little also it is imperceptible to the human visual system (HVS). This is because LSB technique alters the value of a certain bit such (1st, 2nd, ... 8th). The amount of distortion is directly relating to the location of the used bit (weight).

Baboon image was used as cover-image, we noticed that the amount of damage that resulting embedding of the message's bits is slightly less than the amount of damage resulting when using the Lena-gray image is used as its cover image. This behavior applies to the message in (ASCII, Text-image) format. This is due to the Baboon image has a significant variance between the values of neighboring pixels, making it the best option for hiding information inside it.

Generally, the stego-image quality is decreasing and degrade with increases the bit's weight and become highly distortion after used the bit number 5 (SD=4) to embedding the message's bits. Where the value of (SNR) become under (19 dB) for Lena image. as shown in figure (4-3)



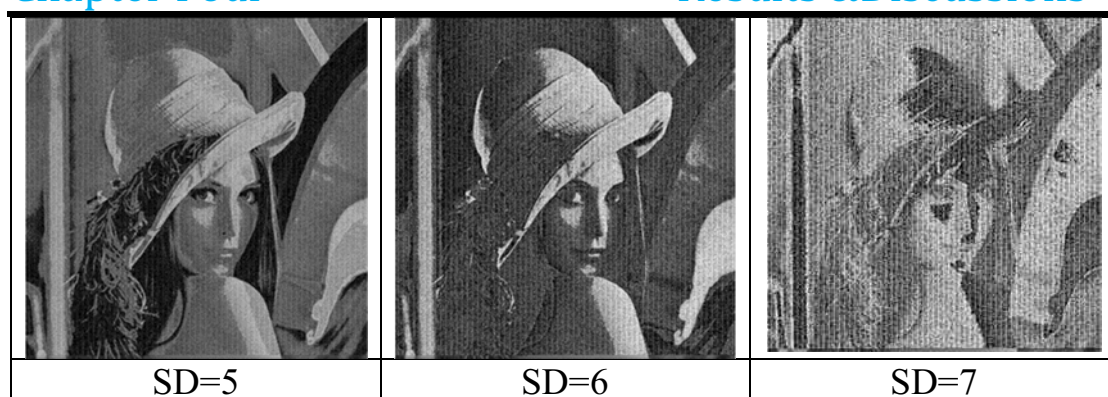


Figure 4-3 The amount of distortion in stego-image Lena after embedding using LSB technique.

After performing the attack on the stego-image (Baboon and Lena) using the standard JPEG algorithm, the amount of damage and the effect produced by comparing the quality of the image after the embedding and quality after the attack were calculated, as shown in Tables (4-3) to (4-10) & Figure (4-4) to (4-7).

Table 4-3 The cover quality (SNR (dB)) after JPEG attack with compression ratio ranging from (100-50) (ASCII) for Lena image.

SD	Q=100	Q=90	Q=80	Q=70	Q=60	Q=50
0	50.6733	33.9988	31.8647	30.7095	29.8752	29.2406
1	50.6425	33.4007	31.3529	30.2518	29.462	28.864
2	50.5981	31.8997	29.9443	28.9756	28.2508	27.7067
3	50.606	30.0218	27.545	26.6225	25.9996	25.5177
4	50.6615	28.8123	24.8096	23.538	22.8866	22.4576
5	50.5798	28.4994	22.8685	20.4461	19.2653	18.6062
6	50.8417	28.7063	22.7755	19.4102	17.2698	15.897
7	53.8097	31.7799	25.817	22.4165	19.9931	18.1753

Table 4-4 The cover quality (MSE) after JPEG attack with compression ratio ranging from (100-50) (ASCII) for Lena image

SD	Q=100	Q=90	Q=80	Q=70	Q=60	Q=50
0	0.0921	4.2843	7.0031	9.1371	11.0725	12.8145
1	0.0927	4.9141	7.8745	10.1469	12.1705	13.9673
2	0.0936	6.937	10.882	13.6015	16.0719	18.2169
3	0.0934	10.686	18.9017	23.3747	26.9794	30.1458
4	0.0931	14.2461	35.8067	47.987	55.7526	61.5411
5	0.0922	14.8898	54.4477	95.1069	124.8227	145.2789
6	0.0924	15.1006	59.1657	128.4094	210.2021	288.353
7	0.0924	14.7415	58.1875	127.3158	22.4442	338.0691

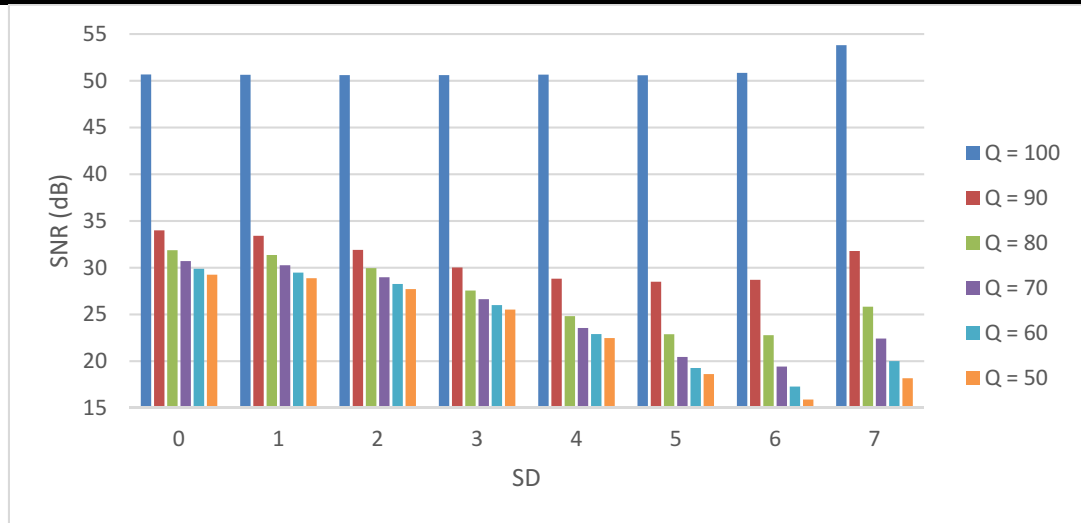


Figure 4-4 The cover quality (SNR) after JPEG attack with compression ratio ranging from (100-50) (ASCII) for Lena image

Table 4-5 The stego-image quality(SNR (dB)) after JPEG attack with compression ratio ranging from (100-50) (Text-image) for Lena image

SD	Q=100	Q=90	Q=80	Q=70	Q=60	Q=50
0	50.6788	34.0295	31.9094	30.756	29.9154	29.2862
1	50.6953	33.4906	31.4553	30.3719	29.5801	28.9866
2	50.7267	32.1428	30.1434	29.2068	28.52	27.9994
3	50.8279	30.5137	27.988	27.0316	26.4306	25.9971
4	51.0621	29.3957	25.6818	24.369	23.6392	23.1795
5	51.3054	29.2449	23.9007	21.7605	20.6497	19.9655
6	52.0982	29.9985	24.0786	20.829	18.9068	17.7345
7	55.5779	33.5563	27.654	24.2673	21.9072	20.139

Table 4-6 The cover quality (MSE) after JPEG attack with compression ratio ranging from (100-50) (Text-image) for Lena image

SD	Q=100	Q=90	Q=80	Q=70	Q=60	Q=50
0	0.0926	4.2787	6.9715	9.0923	11.0339	12.754
1	0.0927	4.8692	7.7801	9.9844	11.9812	13.7357
2	0.093	6.7113	10.6353	13.1949	15.4558	17.4242
3	0.0929	9.9841	17.8602	22.26	25.5633	28.2468
4	0.0927	13.6087	32.0042	43.2994	51.2229	56.9425
5	0.0923	14.8313	50.7696	83.1046	107.3251	125.6368
6	0.0925	15.0029	58.6365	123.9152	192.9092	252.6869
7	0.0922	14.6829	57.1529	124.6545	214.6463	322.5102



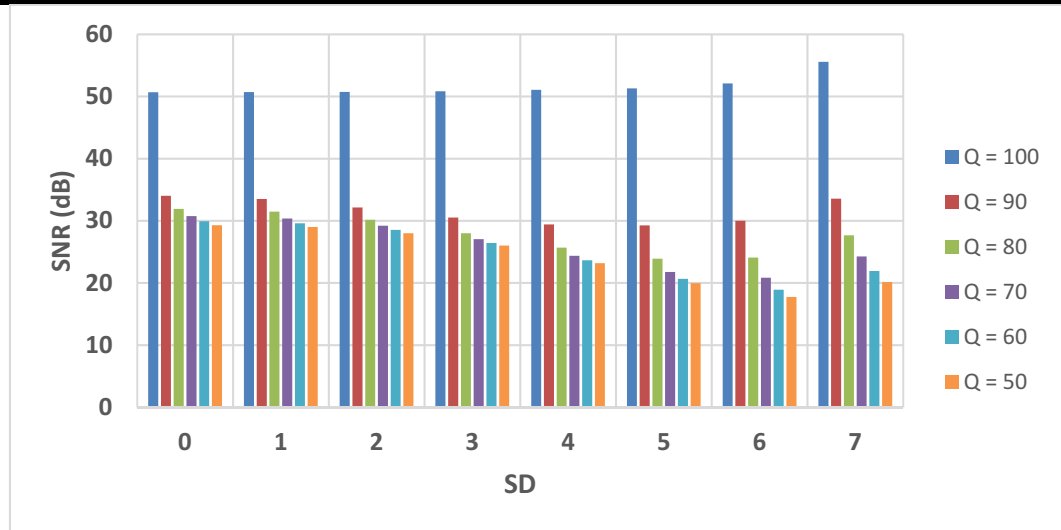


Figure 4-5 The cover quality (SNR) after JPEG attack with compression ratio ranging from (100-50) (Text-image) for Lena image.

Table 4-7 The cover quality (SNR (dB)) after JPEG attack with compression ratio ranging from (100-50) (ASCII) for Baboon image.

SD	Q=100	Q=90	Q=80	Q=70	Q=60	Q=50
0	53.0151	31.448	27.136	25.0202	23.6942	22.7775
1	53.0388	31.6051	27.0947	24.981	23.6569	22.7418
2	53.0134	31.4463	26.9303	24.8283	23.5247	22.6187
3	53.028	31.125	26.4209	24.3343	23.0669	22.1988
4	52.9785	30.9063	25.5506	23.1801	21.8603	21.0166
5	52.9688	30.8341	24.9108	21.8714	20.1193	19.0397
6	53.7581	31.6769	25.7249	22.3032	19.9785	18.3494
7	53.402	31.3629	25.4294	22.0095	19.5757	17.7275

Table 4-8 The cover quality (MSE) after JPEG attack with compression ratio ranging from (100-50) (ASCII) for Baboon image.

SD	Q=100	Q=90	Q=80	Q=70	Q=60	Q=50
0	0.0929	17.7351	35.9691	58.5419	79.4441	98.1143
1	0.0923	12.8466	36.2931	59.0469	80.0946	98.8819
2	0.0928	13.3135	37.6617	61.1069	82.5001	101.6381
3	0.0924	13.3216	42.3061	68.4008	91.5806	111.8184
4	0.093	14.9944	51.4632	88.8278	120.3736	146.185
5	0.0919	15.0216	58.7551	128.301	177.0933	227.0665
6	0.0921	14.8782	58.5793	128.7992	219.9805	320.1097
7	0.0921	14.7297	57.7498	126.9203	222.2894	340.2016

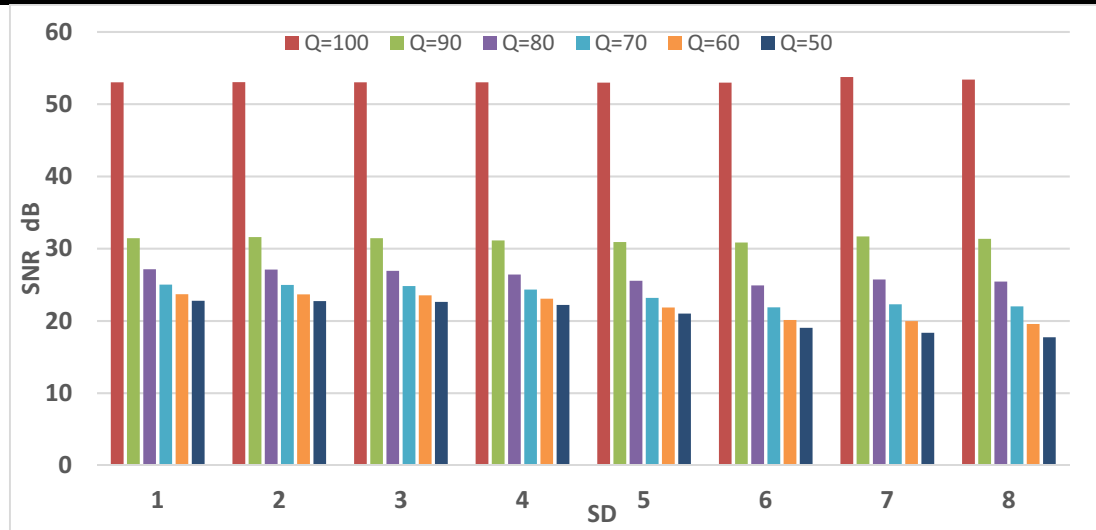


Figure 4-6 The cover quality (SNR) after JPEG attack with compression ratio ranging from (100-50) (ASCII) for Baboon image

Table 4-9 The cover quality (SNR (dB)) after JPEG attack with compression ratio ranging from (100-50) (text image) for Baboon image.

SD	Q=100	Q=90	Q=80	Q=70	Q=60	Q=50
0	53.0352	31.647	27.1585	25.0403	23.7156	22.7985
1	53.0678	31.6394	27.1386	25.0253	23.7019	22.7871
2	53.1381	31.5418	27.0294	24.9265	23.623	22.7145
3	53.1625	31.3001	26.6387	24.5555	23.2795	22.4089
4	53.2991	31.2232	25.9565	23.6397	22.3172	21.4651
5	53.5538	31.4073	25.5818	22.6496	20.9778	19.9361
6	54.7376	32.6575	26.7361	23.3755	21.1407	19.6012
7	55.184	33.1716	27.2705	23.8309	21.4357	19.6175

Table 4-10 The cover quality (MSE) after JPEG attack with compression ratio ranging from (100-50) (text image) for Baboon image.

SD	Q=100	Q=90	Q=80	Q=70	Q=60	Q=50
0	0.0929	12.7343	35.9415	58.5348	79.4111	98.0823
1	0.0926	12.8606	36.2533	58.9758	79.986	98.7396
2	0.0918	13.2598	37.478	60.8217	82.1122	101.22
3	0.0928	14.2535	41.6938	67.3577	90.3621	110.4204
4	0.0927	14.4505	50.2721	85.704	116.2116	141.4046
5	0.092	15.0779	57.6619	113.2693	166.4533	211.5728
6	0.0921	14.8734	58.15	126.0671	210.9048	300.6304
7	0.0926	14.7118	57.2494	126.3962	219.4074	333.4826

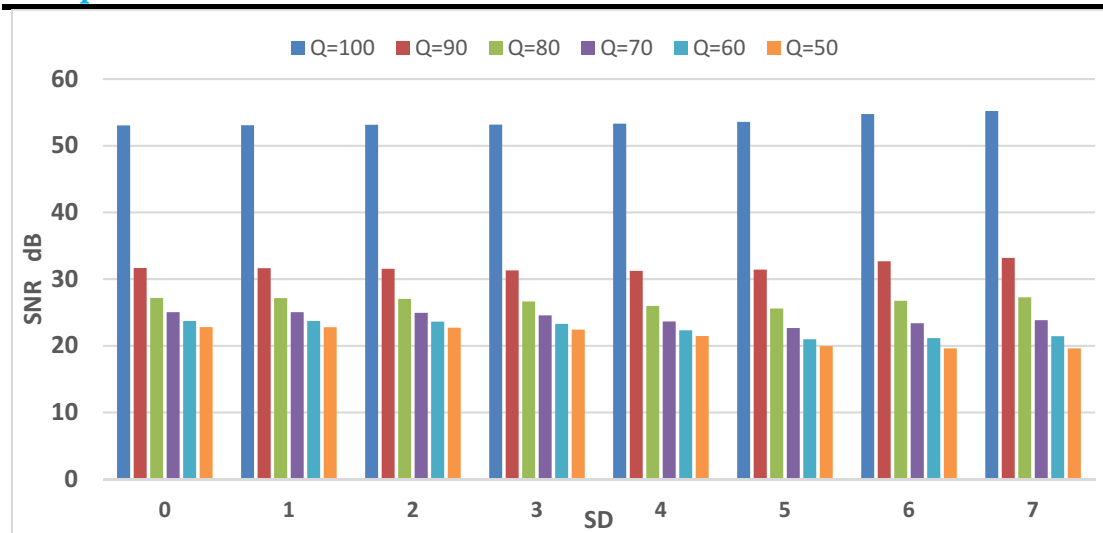


Figure 4-7 The cover quality (SNR) after JPEG attack with compression ratio ranging from (100-50) (text image) for Baboon image

The following behavior in the figures (4-4) and (4-7) can be noticed:

1. The quality of the stego-image gradually decreases as the compression quality is decreasing, where the amount of lost data increases as the compression quality decreases.
2. Reduction of the quality of the stego-image with the increasing of the weight of the bit used to hide the data (start depth) for all values, except the values at the quality (100). This is due to the amount of information in the high frequency of the stego-image increased with the start depth because the image distortion is recorded in the high frequency.
3. The amount of damage in the image quality after JPEG attack (when Baboon image was used as cover-image) is very similar to the amount of damage produced when using the Lena image as cover image. This behavior is applying to message format (ASCII, text-image).

Tables (4-11 to 4-16) and figures (4-8 to 4-11) demonstrate the computing of the JPEG attack on the message (ASCII and text image) which hidden inside Lena and Baboon image.

Table 4-11 The error percent in the ASCII message after JPEG attack for different compression ratio and Start depth for Lena image

SD	Q=100	Q=90	Q=80	Q=70	Q=60	Q=50
0	54.6268	99.6112	99.6262	99.6637	99.602	99.6266
1	31.7072	99.5834	99.5865	99.6698	99.6853	99.6359
2	17.3193	98.451	99.1916	99.3119	99.4909	99.6081
3	9.3061	93.4709	96.9268	97.8679	98.593	98.8429
4	4.6746	77.1236	91.0858	94.1621	95.4149	96.0073
5	2.4222	46.1754	72.9736	83.9767	89.2005	91.9559
6	0.65411	19.1058	34.6941	49.8226	62.6184	71.44
7	0.2684	7.8342	15.0082	12.7224	28.2946	35.0921

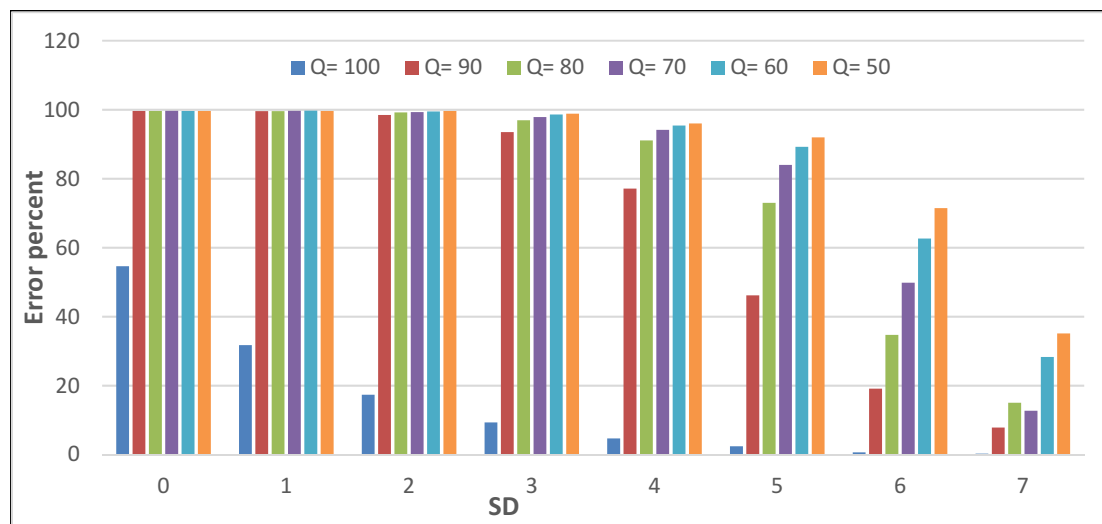


Figure 4-8 The error percent in the ASCII message after JPEG attack for different compression ratio and Start depth for Lena image.

Table 4-12 The (Text-image) message quality(SNR (dB)) for different compression ratio and Start depth for Lena image.

SD	Q=100	Q=90	Q=80	Q=70	Q=60	Q=50
0	13.5562	4.6643	4.6381	4.5252	4.3833	3.4205
1	16.7551	4.7941	4.6162	4.5719	4.4123	4.3323
2	20.175	5.8441	5.3754	5.0486	4.929	4.8166
3	23.0366	8.0673	6.723	6.3572	6.0385	5.8408
4	25.6813	10.5292	8.6445	7.9731	7.4963	7.2235
5	28.7031	13.4686	10.5163	9.5043	8.9648	8.5226
6	33.3234	17.511	14.1923	12.3545	11.3966	10.7618
7	36.3975	23.2326	20.065	18.4788	17.2081	16.1612

Table 4-13 The quality (MSE) of Text-image message for different compression ratio and start depth for Lena image.

SD	Q=100	Q=90	Q=80	Q=70	Q=60	Q=50
0	2225.7195	17247.293	17351.696	17808.667	18400.294	22966.715
1	1065.7097	16739.504	17439.376	17618.416	18277.844	18617.447
2	484.9029	13144.343	14642.361	15786.715	16227.431	16653.206
3	250.8954	7878.1613	10736.345	11679.667	12569.071	13154.542
4	136.4644	4468.9192	6897.744	8050.8032	8985.1037	9567.5545
5	68.0526	2271.4194	4482.5587	5658.7896	6407.2531	7094.1016
6	23.486	895.4815	1922.7378	2935.6244	3660.0819	4236.1637
7	11.5719	239.8267	497.3424	716.6007	960.1552	1221.8901

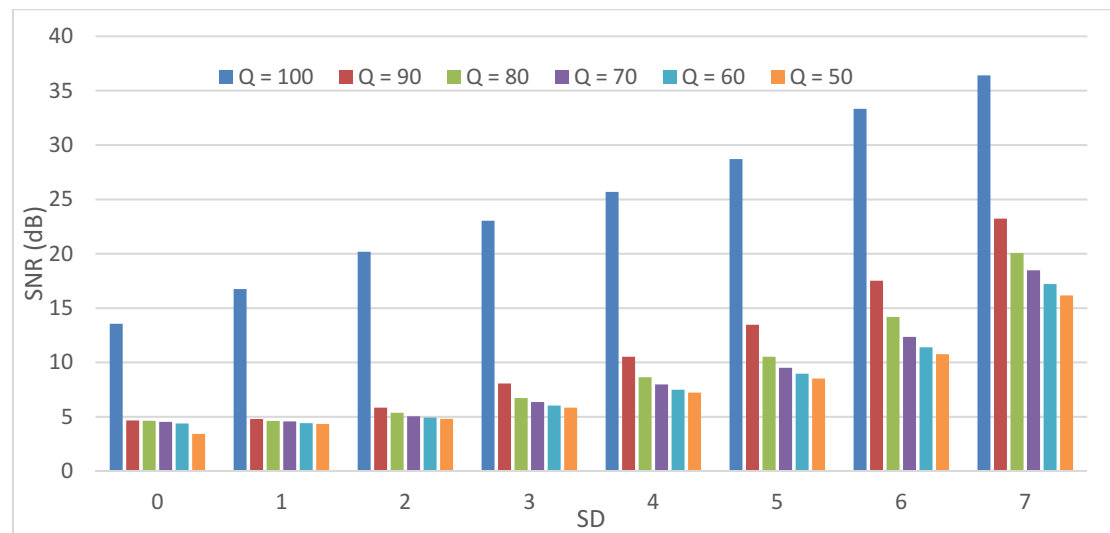


Figure 4-9 The (Text-image) message quality (SNR) for different compression ratio and Start depth for Lena image.

Table 4-14 The error percent in the ASCII message after JPEG attack for different compression ratio(100-50) and Start depth for Baboon image

SD	Q=100	Q=90	Q=80	Q=70	Q=60	Q=50
0	54.7934	99.605	99.5896	99.6513	99.6174	99.6297
1	31.7702	99.6143	99.568	99.6143	99.605	99.6297
2	17.0107	99.4785	99.6328	99.5958	99.5804	99.6236
3	8.8864	96.4022	99.2841	99.5469	99.5094	99.5032
4	4.5944	80.456	95.5475	98.0252	98.593	98.7843
5	2.1229	54.1239	80.2987	90.3206	94.0541	95.9085
6	1.225	30.4483	50.9766	65.3769	75.1859	81.6532
7	0.3394	10.1176	18.2974	25.3541	31.5622	37.3384

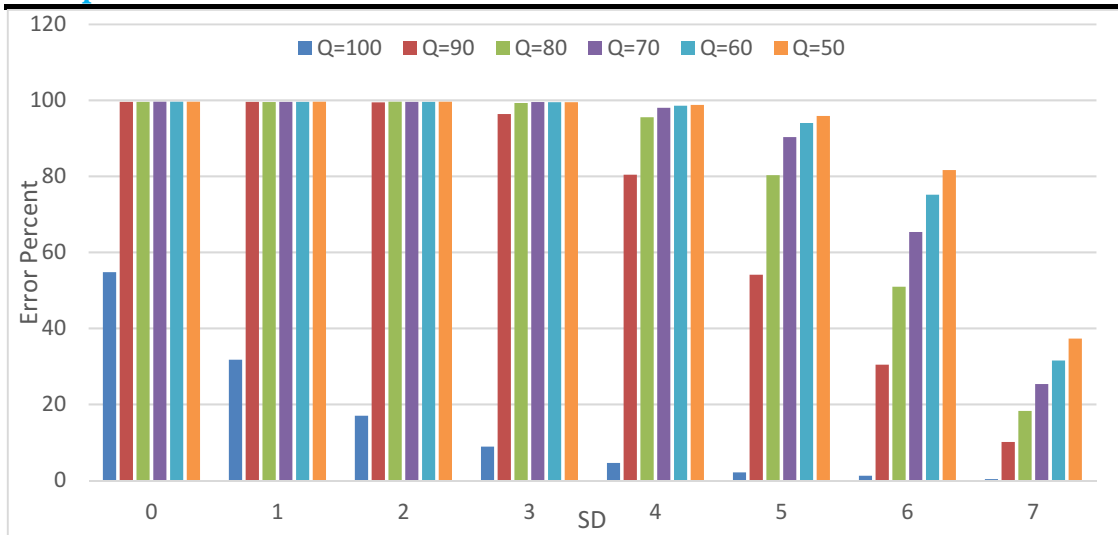


Figure 4-10 The error percent in the ASCII message after JPEG attack for different compression ratio(100-50) and Start depth for Baboon image

Table 4-15 The quality (SNR (dB)) of (text image) message for different compression ratio (100-50) and Start depth for Baboon image.

SD	Q=100	Q=90	Q=80	Q=70	Q=60	Q=50
0	13.5288	4.6755	4.6758	4.6453	4.6158	4.6225
1	16.6757	4.6681	4.6669	4.6385	4.6677	4.636
2	19.971	4.9022	4.6491	4.6665	4.6116	4.6577
3	23.2423	6.8698	5.142	4.9336	4.8168	4.8289
4	26.1962	10.3296	7.1655	6.1035	5.6332	5.4683
5	29.088	13.7658	10.2781	8.6579	7.6592	7.0991
6	32.1913	16.9818	13.8615	12.0171	10.8004	9.9917
7	36.8615	22.3411	19.5225	17.7407	16.4538	15.5934

Table 4-16 The quality (MSE) of (text image) message for different compression ratio (100-50) and Start depth for Baboon image.

SD	Q=100	Q=90	Q=80	Q=70	Q=60	Q=50
0	2240.124	17202.8955	17201.9466	17323.1252	17440.9449	17414.3303
1	1085.3786	17232.2562	17237.1359	17350.1639	17233.8078	17359.9817
2	508.2167	16327.9388	17307.6888	17238.4683	17457.8557	17273.5609
3	239.2868	10.379.3655	15450.8756	16210.3683	16652.3251	16606.0205
4	121.2081	4679.422	9696.1385	12382.3899	13798.6289	14332.4806
5	62.2805	2121.1815	4733.201	6876.4456	8654.3569	9845.6074
6	30.4809	1011.5212	2074.9316	3172.7713	4198.6532	5058.0095
7	10.3994	294.4728	563.5052	849.3394	1142.2822	1392.5515

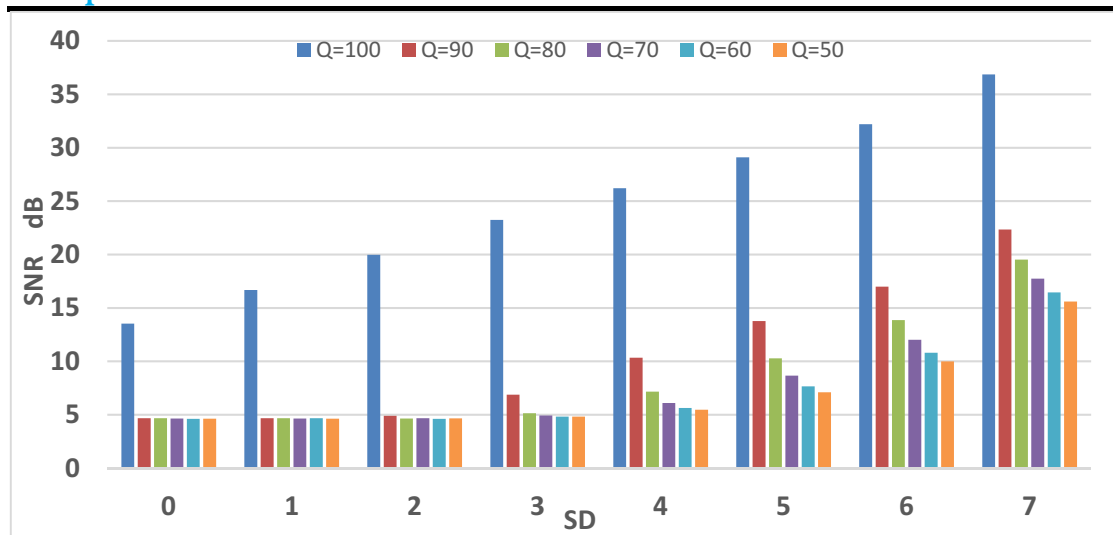


Figure 4-11 The quality (SNR) of (text image) message for different compression ratio (100-50) and Start depth for Baboon image.

The following behavior in the figures (4-8) and (4-11) can be noticed:

1. The retrieved message (text-image) quality increased with increasing the start depth (SD) at compression quality (100)., where the effect of JPEG attack on the Least significant bit is greater than the effect it on a most significant bit.
2. The effect of JPEG attack is devastating on the message from ASCII format for all start depth and all compression ratios, except in compression quality equal (100) (for bits from (5<sup>th</sup>-8<sup>th</sup>) are higher than start depth 4).
3. In case of text-image message, the retrieved message is readable when the message quality is higher than (SNR=13 dB), as shown in the figure (4-12).
4. The retrieved message in text-image format is more robust and immutable than ASCII format against the JPEG attacks
5. In addition, the error percent in the retrieved message after performing the JPEG attack is very similar, whether, using the Baboon or Lena image as cover, this behavior applies to both message formats (ASCII, text-image).





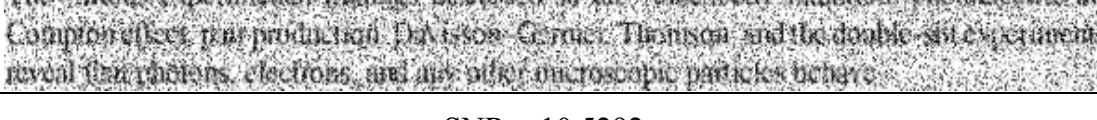
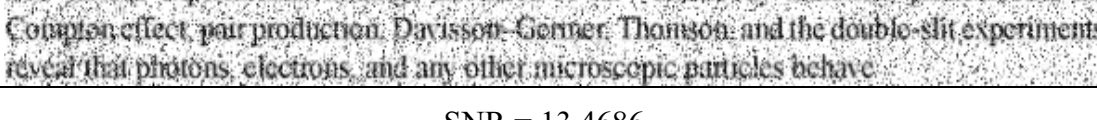
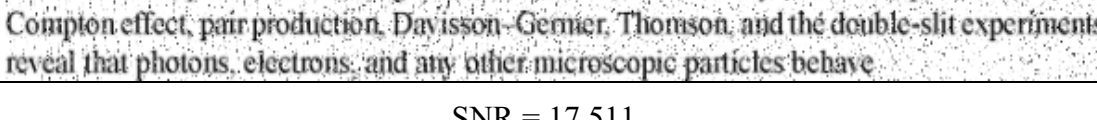
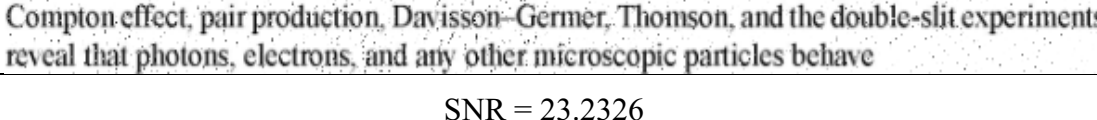
The various experimental findings discussed so far—blackbody radiation, photoelectric and Compton effect, pair production, Davisson–Germer, Thomson, and the double-slit experiments—reveal that photons, electrons, and any other microscopic particles behave
The Original Text-Image

SNR = 4.6643

SNR = 4.7941

SNR = 5.8441

SNR = 8.0673

SNR = 10.5292

SNR = 13.4686

SNR = 17.511

SNR = 23.2326

Figure 4-12 the quality (SNR) of the retrieved message (text-image) after JPEG attack with compression ratio (Q=90) for Lena image.

It could be seen from figure (4-12), the secret message that is embedded using the standard least significant bit algorithm has less resistance and



robustness against attack using the lossy compression JPEG attack. Therefore, we propose in this thesis a new method which is more robust and resistance toward the JPEG attack, and is designed in a way that simulates the JPEG algorithm to overcome the damage and distortion resulting from the JPEG attack. This method is called (A New Statistical Steganography Method) (NSSM).

### 4.3 A New Statistical Steganography Method (NSSM)

The texture factor in cover image is a very important factor and effective on the steganography methods. In this work, two standard grayscale images are considered as a sample image, the first image Lena has a moderate texture with a little variance between the neighboring pixels. The second image represents a high texture and a high variance between the neighboring pixels, this image is Baboon image.

A new statistical steganography method (NSSM) is applied to embed the secret message (ASCII) within the cover image's blocks. Tables (4-17) and (4-18) and figure (4-13) illustrate the quality of the cover image after embedding the secret message bits using ( $\sigma$ ) with two different values as threshold values of (0.5 and 1).

Table 4-17 The cover quality (SNR (dB)) after applying the NSSM for two threshold values (0.5, 1) for Lena and Baboon image

DIF	SNR( Baboon TH=0.5)	SNR( Baboon TH=1)	SNR (Lena TH=0.5)	SNR (Lena TH=1)
1	32.9906	32.9906	38.9813	38.9832
2	32.9764	32.9764	38.8313	38.8343
3	32.9483	32.9483	38.597	38.6012
4	32.9066	32.9066	38.2915	38.2968
5	32.8516	32.8516	37.9296	37.9359
6	32.7838	32.7838	37.5259	37.5331
7	32.7039	32.7039	37.0935	37.1015
8	32.6126	32.6126	36.6463	36.6522
9	32.5105	32.5105	36.1849	36.194
10	32.3985	32.3985	35.7242	35.7337
11	32.2773	32.2773	35.2665	35.2763
12	32.1478	32.1478	34.8152	34.8253

13	32.0109	32.0109	34.373	34.3832
14	31.8672	31.8672	33.9412	33.9516
15	31.7176	31.7176	33.521	33.5315
16	31.5629	31.5629	33.1127	33.1234
17	31.4037	31.4037	32.7167	32.7274
18	31.2408	31.2408	32.3329	32.3436
19	31.0747	31.0747	31.961	31.9717
20	30.906	30.906	31.6007	31.6115
21	30.7352	30.7352	31.2518	31.2626
22	30.5628	30.5628	30.9137	30.9245
23	30.3893	30.3893	30.5861	30.5968
24	30.215	30.215	30.2684	30.2791
25	30.0403	30.0403	29.9603	29.971

Table 4-18 The cover quality (MSE) after applying the NSSM for two threshold values (0.5 and 1) for Lena and Baboon image

DIF	MSE (Baboon TH=0.5)	MSE (Baboon TH=1)	MSE (Lena TH=0.5)	MSE (Lena TH=1)
1	9.3467	9.3467	1.3612	1.3606
2	9.3773	9.3773	1.409	1.408
3	9.4381	9.4381	1.4871	1.4856
4	9.5293	9.5293	1.5955	1.5935
5	9.6507	9.6507	1.7341	1.7316
6	9.8024	9.8024	1.903	1.8999
7	9.9844	9.9844	2.1022	2.0984
8	10.1967	10.1967	2.3317	2.3271
9	10.4392	10.4392	2.5914	2.586
10	10.712	10.712	2.8815	2.8752
11	11.0151	11.0151	3.2018	3.1945
12	11.3484	11.3484	3.5523	3.5441
13	11.712	11.712	3.9332	3.9239
14	12.1059	12.1059	4.3443	4.3338
15	12.5301	12.5301	4.7856	4.774
16	12.9845	12.9845	5.2573	5.2445
17	13.4692	13.4692	5.792	5.7451
18	13.9842	13.9842	6.2914	6.2759
19	14.5295	14.5295	6.8539	6.837
20	15.105	15.105	7.4467	7.4282
21	15.7108	15.7108	8.0697	8.0497
22	16.3469	16.3469	8.723	8.7014
23	17.0132	17.0132	9.4066	9.3833
24	17.7098	17.7098	10.1204	10.0954
25	18.4367	18.4367	10.8645	10.8377

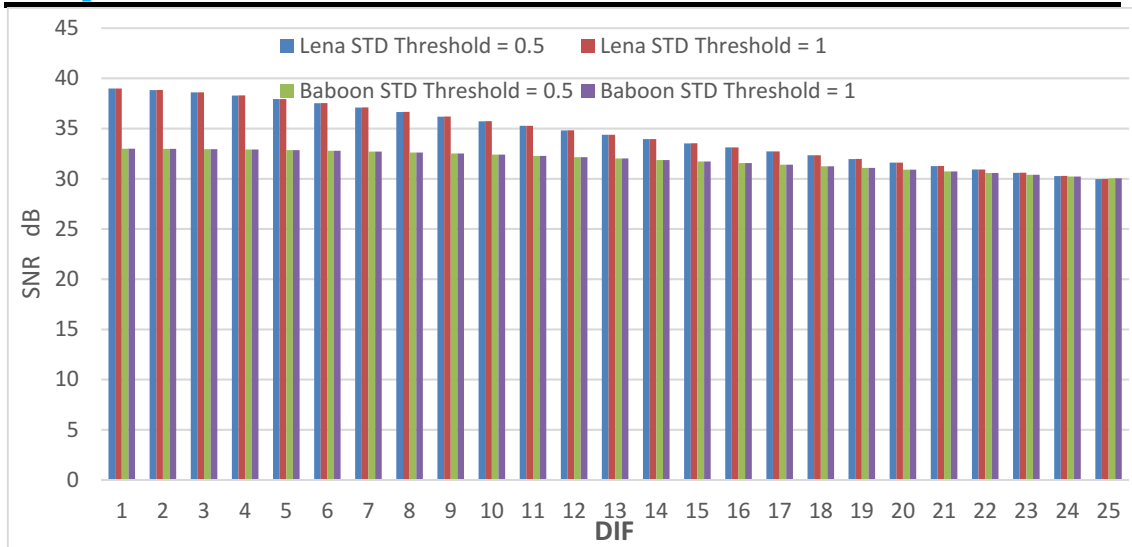


Figure 4-13 The cover quality after applying the NSSM for two threshold values (0.5 and 1) for Lena and Baboon image

We note from the figure (4-13), that the image quality with high variance or high texture as (Baboon image) is less affected and damage by the application of the (NSSM) method for small difference values, and when of the difference factor value is increased , the quality of the two images (Lena & Baboon) is related to in the difference value equal to  $(20 \sigma)$ . On the other hand, the value of threshold does not affect the behavior and result of the cover image after applying the NSSM when all the blocks are selected. A new statistical steganography method (NSSM) is designed based on the fact of the JPEG algorithm maintains the mean value of the image brightness after the attack. This is illustrated in the table (4-19) and figure (4-14):

Table 4-19 The mean value of the Baboon image for different threshold values (0.5 and 1) after JPEG attack for different compression quality

DIF	Stego	Q= 100	Q=90	Q=80	Q=70	Q=60	Q=50
1	129.6895	129.6895	129.6918	129.6874	129.6918	129.6868	129.7014
2	129.6884	129.6888	129.6903	129.6844	129.6897	129.6888	129.7057
3	129.6874	129.6871	129.6888	129.6837	129.6881	129.6848	129.7062
4	129.6863	129.6872	129.6884	129.6803	129.6877	129.6868	129.7038
5	129.6853	129.6859	129.6864	129.6816	129.6865	129.6883	129.7025
6	129.6842	129.6842	129.6841	129.6796	129.6839	129.6873	129.7035
7	129.6831	129.6837	129.6825	129.6785	129.6812	129.6877	129.7055

8	129.6821	129.6816	129.6833	129.6775	129.6814	129.688	129.7072
9	129.681	129.6805	129.6819	129.6799	129.682	129.6866	129.7041
10	129.68	129.6804	129.6822	129.6731	129.6797	129.686	129.706
11	129.6789	129.6784	129.6805	129.6814	129.6742	129.6817	129.7028
12	129.6778	129.6782	129.6801	129.6814	129.676	129.6781	129.7041
13	129.6768	129.677	129.6787	129.6794	129.6735	129.6749	129.7024
14	129.6757	129.6752	129.6755	129.6776	129.6762	129.6785	129.6993
15	129.6746	129.6739	129.6733	129.6772	129.6732	129.6766	129.6987
16	129.6736	129.6733	129.6697	129.6746	129.6728	129.6753	129.6945
17	129.6725	129.6725	129.6702	129.6735	129.67	129.6724	129.6947
18	129.6715	129.6723	129.6705	129.6716	129.6688	129.6719	129.693
19	129.6704	129.6706	129.6696	129.6689	129.6667	129.6708	129.6942
20	129.6693	129.6697	129.668	129.6731	129.663	129.6706	129.6925
21	129.6683	129.6688	129.6687	129.6726	129.6613	129.6696	129.6845
22	129.6672	129.668	129.6706	129.6743	129.6612	129.6691	129.6864
23	129.6662	129.6646	129.6688	129.6693	129.6582	129.6643	129.6831
24	129.6651	129.6645	129.6678	129.6689	129.6592	129.665	129.6786
25	129.664	129.6642	129.666	129.6685	129.66	129.6654	129.6739

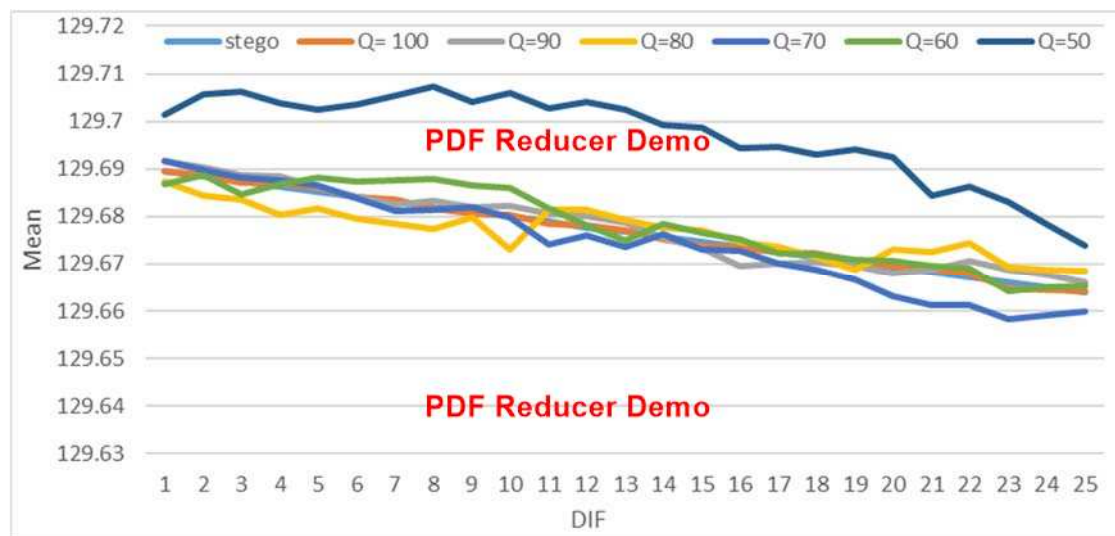


Figure 4-14 The mean value of the Baboon image for different threshold values (0.5,1) after JPEG attack for different compression quality

Figure (4-14) shows, the mean values of the image's brightness and their values a proximally constant are ranging between (129.6592- 129.7057). Therefore, this feature will be used to survive the effect of the JPEG attack.

After embedding of the secret message's bits inside the cover image's blocks (using two types of images, moderate texture (Lena) and high texture (Baboon) by the new statistical steganography method (NSSM), it was noticed that the amount of distortion and degradation in the image is very little and unnoticeable by the human vision system. Therefore, the image quality is very high and acceptable. Figure (4-15), show some stego images using a different standard deviation ( $\sigma$ ).

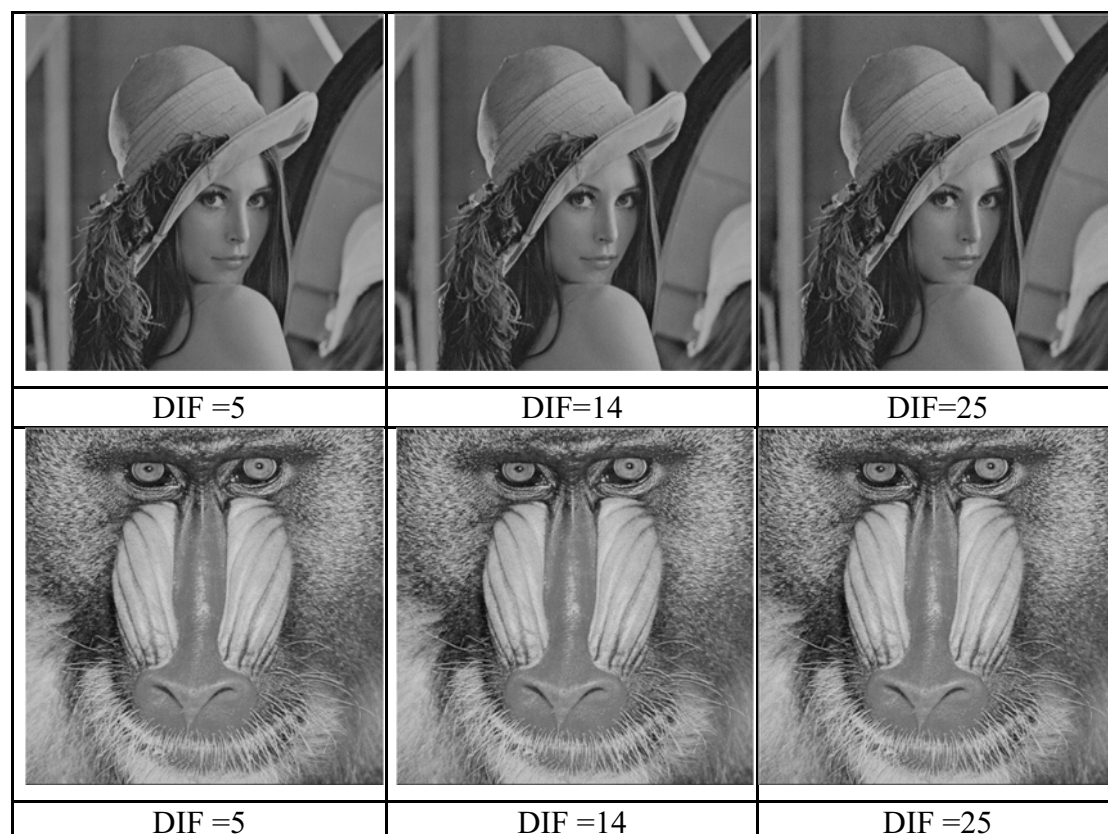


Figure 4-15 The amount of distortion in stego-image using (NSSM).

After embedding the secret message inside the cover image, the JPEG attack was performed on the stego image with different compression ratio ranging from (100- 50). The cover image quality after JPEG attack is very good (i.e. higher than 25 dB). as it is depicted in tables (4-20 to 4-23) and figures (4-16) and (4-17).

Table 4-20 The cover quality (SNR (dB)) after JPEG attack (Lena -TH=0.5 and 1)

DIF	Q= 100	Q= 90	Q= 80	Q= 70	Q= 60	Q= 50
1	50.6314	33.8045	31.6636	30.5359	29.7211	29.1163
2	50.6063	33.7778	31.6431	30.518	29.7046	29.1027
3	50.5923	33.7343	31.6092	30.4889	29.6795	29.0802
4	50.6532	33.6795	31.5598	30.7783	29.6447	29.0498
5	50.6683	33.6086	31.5021	30.3983	29.6001	29.0104
6	50.66	33.5245	31.4303	30.3375	29.5464	28.964
7	50.602	33.4197	31.3483	30.2674	29.4855	28.9089
8	50.6293	33.3088	31.2569	30.1882	29.415	28.8468
9	50.6256	33.1872	31.1558	30.1009	29.339	28.7766
10	50.6201	33.055	31.0442	30.0039	29.254	28.701
11	50.6594	32.9189	30.9263	29.9009	29.1636	28.6187
12	50.6902	32.7698	30.7982	29.7907	29.066	28.5296
13	50.6454	32.6205	30.6621	29.6752	28.9609	28.4346
14	50.6481	32.4644	30.524	29.5532	28.8515	28.3352
15	50.6377	32.3032	30.3802	29.4249	28.7386	28.2302
16	50.6246	32.1364	30.2335	29.2929	28.6221	28.121
17	50.6347	31.9716	30.08	29.1587	28.5015	28.0085
18	50.6634	31.8059	29.9248	29.0204	28.3759	27.8929
19	50.6359	31.6385	29.7673	28.88	28.2467	27.7744
20	50.6732	31.4761	29.6068	28.7356	28.1158	27.6521
21	50.6578	31.3118	29.4468	28.5905	27.9828	27.5276
22	50.6853	31.1468	29.2813	28.4442	27.8488	27.4007
23	50.6972	30.9928	29.1199	28.2964	27.7123	27.2711
24	50.6671	30.8344	28.9572	28.1468	27.5737	27.1406
25	50.6648	30.6779	28.7946	27.9984	27.4349	27.0096

Table 4-21 The cover quality (MSE) after JPEG attack (Lena -TH=0.5 and 1)

DIF	Q= 100	Q= 90	Q= 80	Q= 70	Q= 60	Q= 50
1	0.0931	4.482	7.3377	9.5133	11.4766	13.1915
2	0.0936	4.5096	7.3723	9.5525	11.5201	13.2328
3	0.0939	4.5549	7.43	9.6165	11.5867	13.3013
4	0.0926	4.6127	7.5149	9.7069	11.6798	13.3945
5	0.0923	4.6886	7.6155	9.8191	11.8002	13.5164
6	0.0924	4.7806	7.7422	9.9575	11.9471	13.6616
7	0.0937	4.8971	7.89	10.1195	12.1158	13.8362
8	0.0931	5.237	8.0577	10.3059	12.314	14.0352
9	0.0932	5.1665	8.2475	10.5152	12.5316	14.2639
10	0.0933	5.326	8.4623	10.7526	12.7793	14.5146
11	0.0925	5.4956	8.653	11.0108	13.0483	14.7923
12	0.0918	5.6877	8.9557	11.2941	13.345	15.0992
13	0.0928	5.8867	9.2408	11.5984	13.6721	15.4336
14	0.0927	6.1022	9.5397	11.9293	14.0212	15.7912
15	0.0929	6.3332	9.861	12.2873	14.3907	16.1778

16	0.0932	6.5814	10.2	12.6666	14.7821	16.5902
17	0.093	6.836	10.5673	13.0644	15.1991	17.026
18	0.0924	7.102	10.9521	13.4878	15.6455	17.4857
19	0.093	7.3815	11.3569	13.9313	16.1184	17.9699
20	0.0922	7.6629	11.7823	14.4028	16.6121	18.4841
21	0.0925	7.9588	12.2276	14.8925	17.1293	19.0221
22	0.0919	8.2673	12.7032	15.4035	17.6669	19.587
23	0.0917	8.5659	13.1846	15.9373	18.2319	20.1814
24	0.0923	8.8847	13.6886	16.4968	18.824	20.7978
25	0.0924	9.211	14.2116	17.0709	19.436	21.4358

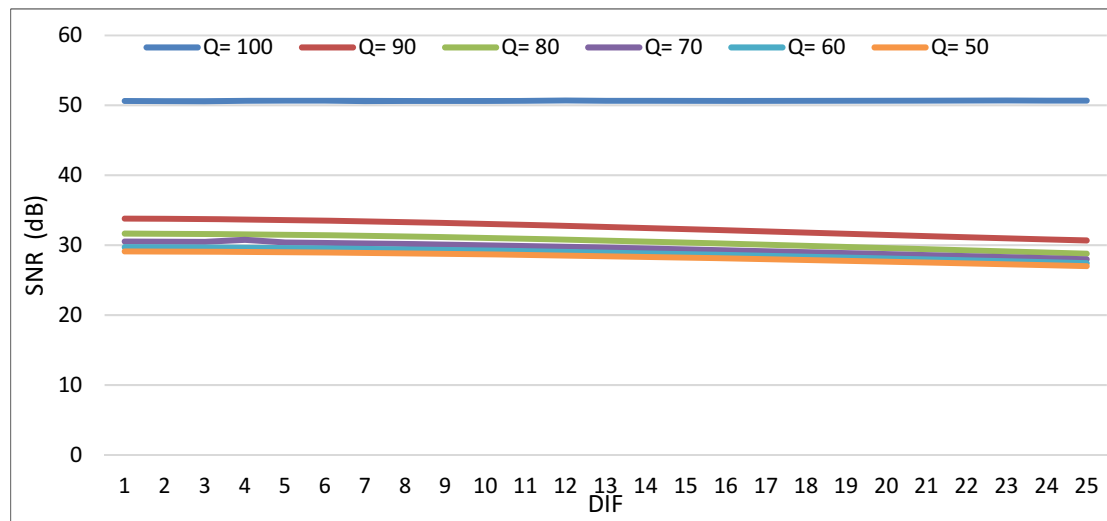


Figure 4-16 The cover quality (SNR) for Lena image after JPEG attack for  $\sigma$  threshold = (0.5 and 1)

Table 4-22 The cover quality (SNR (dB)) after JPEG attack for Baboon image (TH = 0.5 and 1)

DIF	Q= 100	Q= 90	Q= 80	Q= 70	Q= 60	Q= 50
1	53.0276	31.5798	27.0189	24.8797	23.5606	22.6632
2	53.0374	31.5774	27.0179	24.8787	23.5601	22.6625
3	53.0286	31.5745	27.018	24.8766	23.5582	22.6612
4	52.9901	31.5692	27.0152	24.8745	23.5552	22.6587
5	53.0506	31.5662	27.0115	24.8718	23.5516	22.6561
6	52.9966	31.5581	27.0068	24.8664	23.5469	22.6519
7	53.0083	31.5503	27.0012	24.8602	23.5415	22.6474
8	53.0263	31.5423	26.9933	24.8534	23.5351	22.6418
9	53.0335	31.5334	26.9861	24.845	23.5279	22.636
10	53.0099	31.521	26.9753	24.836	23.52	22.6289
11	53.0565	31.5081	26.9639	24.8267	23.5118	22.6209
12	53.0505	31.4968	26.9514	24.8163	23.5019	22.6123
13	53.0289	31.4835	26.9394	24.8045	23.4919	22.6028
14	53.0196	31.4691	26.925	24.7923	23.4806	22.593
15	53.0246	31.456	26.9102	24.7788	23.469	22.5828

<b>16</b>	53.0017	31.4394	26.8934	24.7649	23.4569	22.5716
<b>17</b>	53.0358	31.4207	26.8776	24.7499	23.444	22.5594
<b>18</b>	53.0587	31.4044	26.8594	24.7337	23.4295	22.5466
<b>19</b>	53.0274	31.3862	26.8415	24.7167	23.4146	22.5331
<b>20</b>	53.0221	31.3705	26.8213	24.6988	23.399	22.5192
<b>21</b>	53.0618	31.3471	26.8008	24.6807	23.3825	22.3038
<b>22</b>	53.0358	31.3276	26.7797	24.6614	23.3652	22.4879
<b>23</b>	53.0557	31.3055	26.7566	24.6408	23.3476	22.471
<b>24</b>	53.0328	31.2806	26.7335	24.6199	23.3289	22.4543
<b>25</b>	53.0301	31.2638	26.7077	24.5979	23.3091	22.4361

Table 4-23 The cover quality (MSE) after JPEG for Baboon image (TH = 0.5 and 1)

<b>DIF</b>	<b>Q= 100</b>	<b>Q= 90</b>	<b>Q= 80</b>	<b>Q= 70</b>	<b>Q= 60</b>	<b>Q =50</b>
<b>1</b>	0.0926	12.9268	36.9469	60.4643	81.9239	100.727
<b>2</b>	0.0924	12.9338	36.9551	60.477	81.9323	100.7417
<b>3</b>	0.0926	12.9422	36.954	60.506	81.9678	100.7708
<b>4</b>	0.0934	12.9579	36.9777	60.5342	82.0223	100.8296
<b>5</b>	0.0921	12.9668	37.0082	60.572	82.0897	100.8881
<b>6</b>	0.0933	12.991	37.0488	60.6467	82.1793	100.9864
<b>7</b>	0.093	13.0142	37.0964	60.7337	82.2816	101.0895
<b>8</b>	0.0926	13.0381	37.1636	60.8286	82.4016	101.2197
<b>9</b>	0.0925	13.0648	37.2254	60.9457	82.5376	101.3556
<b>10</b>	0.093	13.1022	37.318	61.073	82.6885	101.5218
<b>11</b>	0.092	13.1413	37.4158	61.2044	82.8454	101.7087
<b>12</b>	0.0921	13.1755	37.5237	61.3501	83.0345	101.9111
<b>13</b>	0.0926	13.2159	37.6279	61.5175	83.2257	102.1342
<b>14</b>	0.0928	13.2602	37.7534	61.6911	83.4432	102.3668
<b>15</b>	0.0927	13.3001	37.8828	61.8835	83.6675	102.607
<b>16</b>	0.0932	13.3512	38.0297	62.0824	83.9026	102.8735
<b>17</b>	0.0924	13.409	38.1686	62.2989	84.1519	103.1629
<b>18</b>	0.092	13.4598	38.3293	62.5319	84.4355	103.47
<b>19</b>	0.0926	13.5163	38.4886	62.7784	84.7271	103.7925
<b>20</b>	0.0927	13.5656	38.6687	63.0387	85.0341	104.1271
<b>21</b>	0.09919	13.639	38.8525	63.3037	85.3582	104.4997
<b>22</b>	0.0925	13.7008	39.0425	63.5863	85.7016	104.8857
<b>23</b>	0.92	13.771	39.2518	63.89	86.0515	105.2962
<b>24</b>	0.925	13.8504	39.4619	64.1994	86.4237	105.7054
<b>25</b>	0.0926	13.9045	39.6982	64.5273	86.8205	106.1486



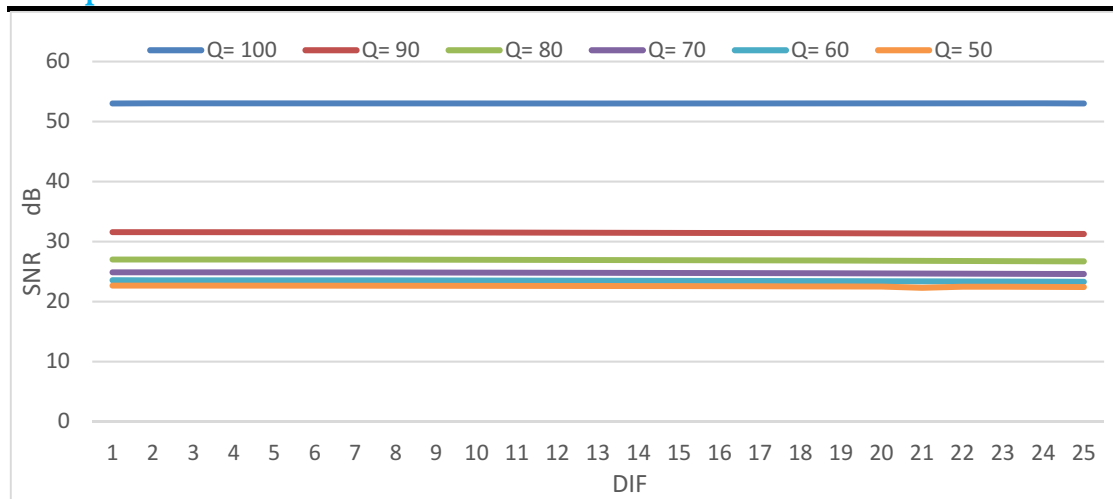


Figure 4-17 The cover quality (SNR) for the Baboon image after JPEG attack for  $\sigma$  threshold = (0.5 and 1)

The aims of the JPEG attack are to compress and decrease the amount of information in image in order to destroy the hidden message inside the cover image. One from operations of JPEG algorithm is the smoothing process, where, it works to smooth the image's surface (i.e. equality between image's pixels). The Baboon image has a high texture and high variance, therefore, it suffers from the smoothing process more than Lena image which has a moderate texture or little variance between the neighboring pixels. We note from figure (4-16) and (4-17), that the image quality after the JPEG attack is very high, especially when the compression ratio was (100), and the quality of the image is higher than (50 dB) in the Lena image and (53 dB) in the Baboon image. Some behavior was noticed even in compression ratio (50) and value of the image quality is ranging from (29 dB) in Lena image to (22 dB) in Baboon image. This quality is considered to be high and good (i.e. there is no noticeable difference between the image after embedding and the image after the JPEG attack) as it is shown in figure (4-18)

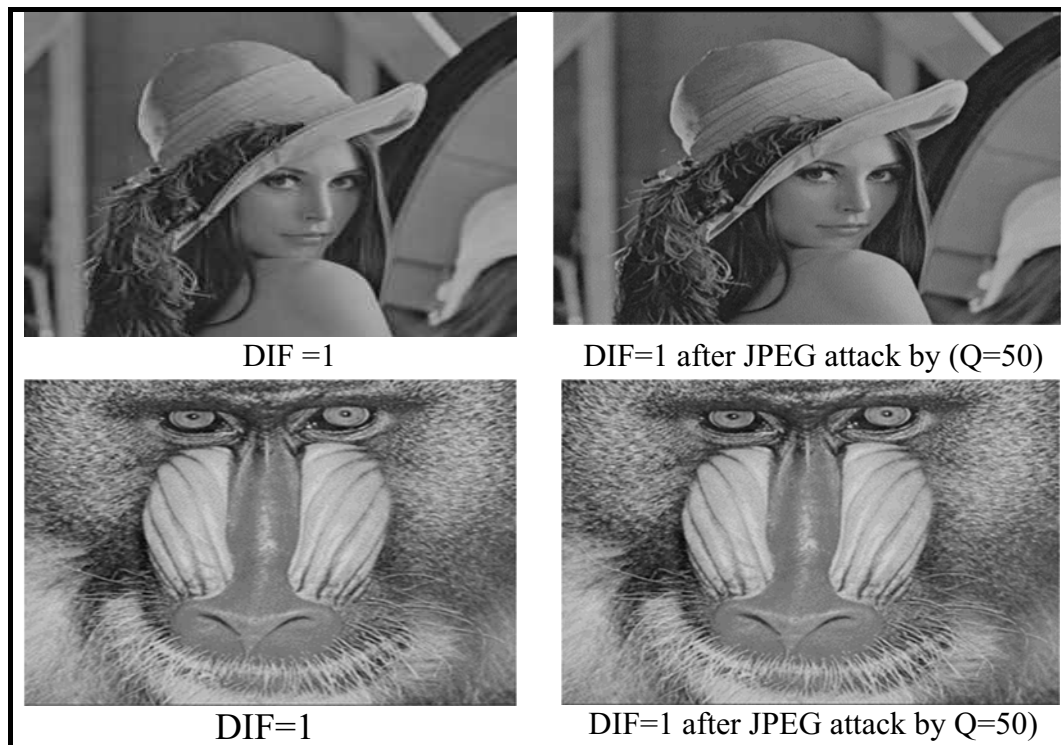


Figure 4-18 Comparison between two images before & after JPEG attack (Q=50)

The error percent in the retrieved message from the cover image after JPEG attack is computed using different compression ratio ranging (100-50), as shown in the table (4-24 to 4-26) and figures (4-19 to 4-21).

Table 4-24 The error percent of retrieved message after JPEG attack for Lena image (TH=0.5)

DIF	Q= 100	Q= 90	Q= 80	Q= 70	Q= 60	Q= 50
1	19.1532	98.1855	99.3952	99.7984	99.5968	100
2	0.2016	96.371	99.3952	100	99.3952	99.3952
3	0	94.3548	98.9919	99.3952	98.9919	99.5968
4	0	90.9274	99.7984	99.5968	100	99.5968
5	0	85.6855	100	99.7984	99.3952	99.5968
6	0	78.4274	99.7984	99.1935	99.7984	100
7	0	71.1694	99.7984	99.5968	100	99.7984
8	0	60.4839	100	99.1935	99.3952	98.9919
9	0	50.6048	98.7903	98.7903	99.7984	99.7984
10	0	39.3145	98.3871	99.1935	99.7984	99.5968
11	0	32.0565	99.1935	99.7984	99.3952	99.1935
12	0	22.9839	99.5968	99.5968	100	99.5968
13	0	15.7258	97.1774	99.3952	99.5968	99.7984
14	0	9.6774	96.371	98.5887	100	99.5968
15	0	5.6452	68.3468	98.5887	99.3952	100
16	0	2.2177	59.0726	98.7903	99.5968	99.7984
17	0	0.8065	54.0323	98.9919	99.5968	98.9919
18	0	0.4032	49.7984	98.3871	99.7984	99.5968

<b>19</b>	0	0.2016	46.1694	98.3871	99.5968	99.1935
<b>20</b>	0	0	42.9435	98.5887	99.3952	99.3952
<b>21</b>	0	0	37.2984	98.5887	99.5968	99.7984
<b>22</b>	0	0	34.0726	97.5806	99.7984	99.7984
<b>23</b>	0	0	30.4435	97.9839	99.1935	99.1935
<b>24</b>	0	0	26.4113	97.7823	99.1935	98.7903
<b>25</b>	0	0	21.5726	97.9839	98.9919	99.3952

Table 4-25 The error percent of retrieved message after JPEG attack for Lena image (TH=1)

<b>DIF</b>	<b>Q= 100</b>	<b>Q= 90</b>	<b>Q= 80</b>	<b>Q= 70</b>	<b>Q= 60</b>	<b>Q= 50</b>
<b>1</b>	44.6465	99.596	99.596	99.596	99.798	100
<b>2</b>	33.3333	98.9899	99.596	99.1919	99.596	99.3939
<b>3</b>	33.3333	99.596	99.798	99.596	99.596	99.596
<b>4</b>	33.3333	99.596	100	99.3939	99.3939	99.3939
<b>5</b>	33.3333	99.798	99.596	99.798	99.3939	99.596
<b>6</b>	33.3333	99.1919	99.596	99.596	99.596	100
<b>7</b>	33.3333	98.5859	99.596	99.798	99.1919	99.596
<b>8</b>	33.3333	97.5758	100	100	99.798	99.1919
<b>9</b>	33.3333	98.5859	99.3939	99.798	99.798	99.798
<b>10</b>	33.3333	98.1818	99.1919	99.798	99.596	99.3939
<b>11</b>	33.3333	97.9798	99.3939	99.596	99.1919	98.9899
<b>12</b>	33.3333	98.9899	99.1919	99.798	99.596	99.3939
<b>13</b>	33.3333	55.1515	98.9899	99.1919	99.798	99.3939
<b>14</b>	33.3333	21.1414	99.596	99.1919	99.596	99.798
<b>15</b>	33.3333	21.8184	99.3939	99.596	100	99.798
<b>16</b>	33.3333	19.1919	99.1919	99.798	98.7879	99.3939
<b>17</b>	33.3333	17.9798	99.1919	99.596	98.9899	99.1919
<b>18</b>	33.3333	17.7778	99.1919	100	100	99.3939
<b>19</b>	33.3333	17.7778	98.9899	99.596	99.3939	99.596
<b>20</b>	33.3333	17.5758	94.9495	99.3939	100	99.798
<b>21</b>	33.3333	17.5758	91.9192	99.1919	99.596	98.9899
<b>22</b>	33.3333	17.5758	91.7172	100	99.3939	99.798
<b>23</b>	33.3333	17.5758	91.7172	98.5859	99.798	99.1919
<b>24</b>	33.3333	17.5758	91.7172	98.9899	100	98.9899
<b>25</b>	33.3333	17.5758	81.8182	99.3939	100	99.596

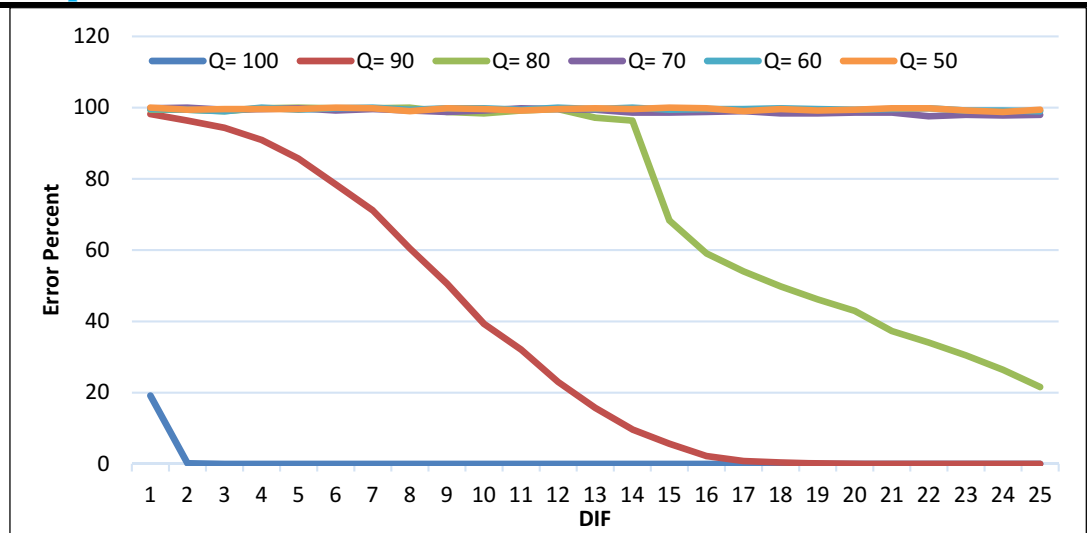


Figure 4-19 The error percent of retrieved message after JPEG attack for Lena image (TH=0.5)

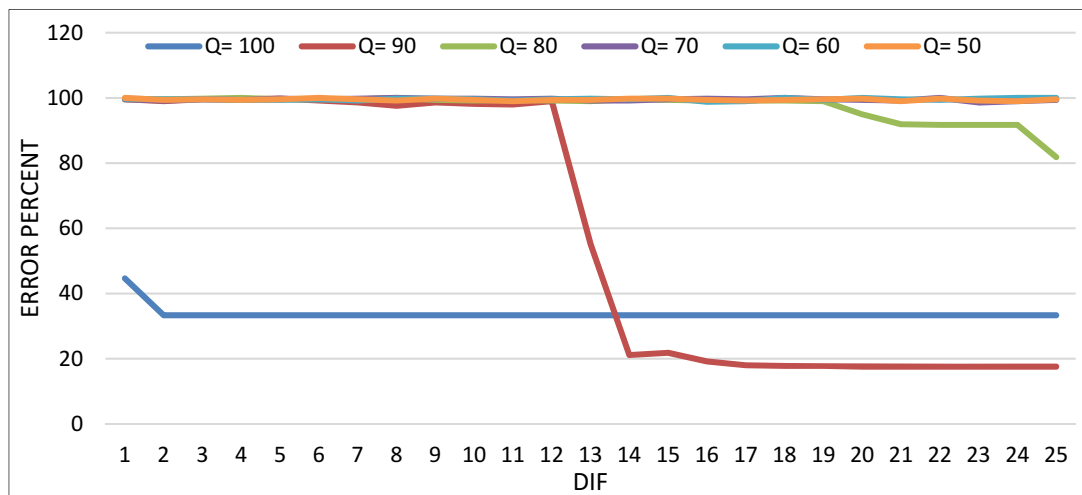


Figure 4-20 The error percent of retrieved message after JPEG attack for Lena image (TH=1)

Table 4-26 The error percent of retrieved message after JPEG attack for Baboon image (TH=0.5 and 1)

DIF	Q =100	Q= 90	Q= 80	Q= 70	Q= 60	Q= 50
1	21.9758	99.3952	99.1935	99.3952	99.5968	99.3952
2	0.2016	96.371	98.9919	98.9919	99.5968	99.1935
3	0	91.5323	98.1855	98.5887	99.5968	98.7903
4	0	82.8629	95.3629	98.3871	99.5968	98.5887
5	0	71.5726	93.9516	97.1774	99.5968	98.5887
6	0	59.879	92.1371	96.9758	98.9703	98.5887
7	0	44.1532	89.5161	96.5726	98.1855	98.3871
8	0	31.25	86.6935	95.9677	98.1855	98.1855
9	0	19.9597	83.2661	94.9597	98.1855	98.5887
10	0	11.2903	78.2258	93.1452	97.5806	98.3871

11	0	6.4516	73.5887	91.9355	97.5806	98.3871
12	0	4.0323	66.9355	90.121	97.379	98.3871
13	0	1.8145	60.8871	88.3065	96.7742	98.1855
14	0	1.2097	55.8468	84.4758	95.7661	97.9839
15	0	0.4032	50.2016	81.6532	94.9597	97.7823
16	0	0.2016	43.5484	79.2339	94.7581	97.379
17	0	0.2016	38.1048	76.2097	94.3548	96.7742
18	0	0.2016	32.6613	73.5887	94.3548	96.371
19	0	0	26.6129	69.7581	94.3548	95.5645
20	0	0	23.1855	65.7258	93.3468	95.3629
21	0	0	18.9516	61.6935	91.3306	95.1613
22	0	0	14.9194	59.6774	80.2419	94.5565
23	0	0	11.6935	56.6532	78.2258	93.5484
24	0	0	9.4758	52.4194	76.2097	93.5484
25	0	0	7.0565	48.9919	73.3871	93.1452

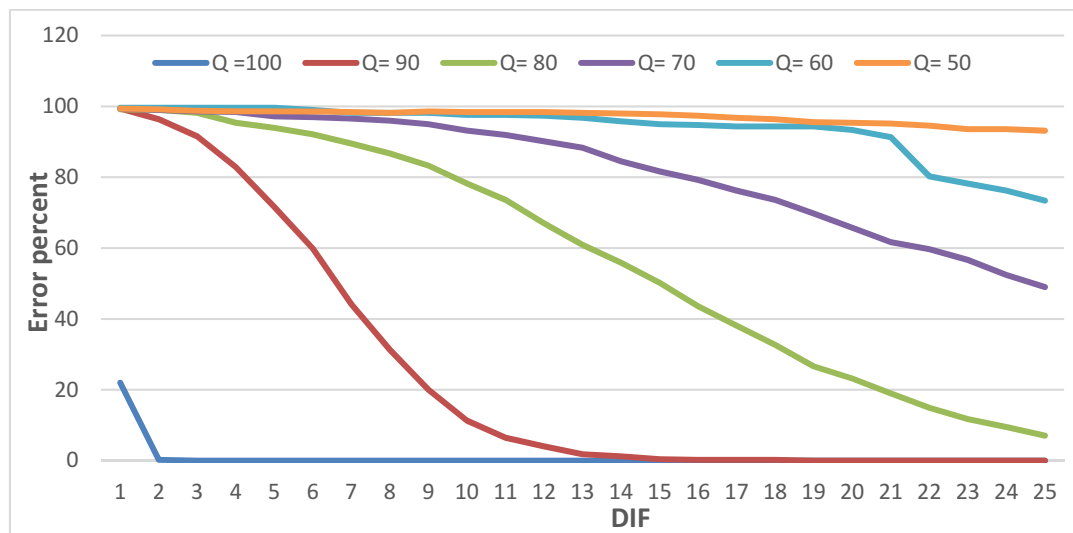


Figure 4-21 The error percent of retrieved message after JPEG attack for Baboon image (TH=0.5 and 1)

The following notes could be drive from the data in table (4-24 to 4-26) and figure (4-19 to 4-21):

1. Using the new statistical steganographic method (NSSM), the secret message which hidden inside Baboon and Lena image respectively, can be override the JPEG attack starting from the difference (DIF=2) when the compression ratio equal to (Q=100), also starting from

difference equal (DIF=14, DIF=17) when the compression ratio equal to (Q=90).

2. Using Lena image in ( $\sigma$ ) threshold value equal (Th=1), failed to retrieved the secret message in compression ratio of (Q=90) and even in compression ratio equal to (Q=100). This failure is because the one block of image blocks failed to override the ( $\sigma$ ) threshold test, where the value of threshold is high. This result in a miss-arranged in the sequence of the retrieved message's bits, which caused to damage and corrupt the retrieved message starting from that bit. with decreasing the value of threshold ( $\sigma$ ) to 0.5, we note all image blocks override the test.
3. Baboon image has a high texture did not affected by the change in the value of threshold ( $\sigma$ ) in contrast to the Lena image. The JPEG attack couldn't reduce the texture to significant value due to the smoothing effect that associate with it.

# *CHAPTER FIVE*

## *CONCLUSIONS*

*&*

## *RECOMMENDATIONS*

## Chapter Five: Conclusions & Recommendations

### 5.1 Conclusions

From the work and the previous results in chapter four, depicted in the following paragraph some important remarks.

#### 5.1.1 Standard Least Significant Bit (LSB) Technique

1. Using LSB method, the JPEG attack leads to damage greatly the hidden message.
2. The amount of degradation resulting in the cover image after embedding using the first four bits (less than  $SD = 4$ ) is very small and undetectable by the human visual system.
3. The cover image quality after using the fourth bit (after start depth  $(SD) = 3$ ) is highly affected.
4. We do not recommend using bits after the fourth bit (start depth  $(SD) = 3$ ) to hide the message.
5. The secret message in ASCII format is survive from the JPEG attack in compression quality (100) after a third bit (start depth  $SD = 2$ ), especially with repetition of the writing of the text (ASCII) within the message several times.
6. The secret message in image format is more robust against the JPEG attack than an ASCII format.
7. The secret message in image format is survive from the JPEG attack if the compression ratio more than 80.
8. The retrieved secret message in image format is readable when the quality higher than 13 dB.



### 5.2 A New Statistical Steganographic Method (NSSM)

1. A new statistical steganographic method (NSSM) is succeeded in reducing or overcoming the JPEG attack for low compression ratio (Q=90 and Q=100). This due to the fact the JPEG algorithm maintaining the mean value of the image's brightness.
2. The image quality is very good after embedding and after JPEG attack.
3. Using an image with high texture enhance the results of (NSSM), as in Baboon image, become it reduce the effect of smoothing process resulting from JPEG attack on the cover image.
4. The secret message within a baboon image is survive from the JPEG attack after difference (DIF =1) when the compression quality equal to 100, and after difference (DIF =13) when the compression quality equal to 90.
5. Whenever increasing the value of the difference (DIF) the robustness of the secret message will increase against the JPEG attack.
6. The new statistical steganography method (NSSM) is characterized by the highest robustness and resistance against compression attack JPEG compared with the standard least significant bit (LSB) method.

### 5.3 Recommendations

From this work, the following are remarks and recommendations for future work:

1. To color spaces in the hide of information (steganography).
2. Repetition of the secret message several times to hide inside the cover.
3. Propose or develop a more powerful and robust system against JPEG attacks.

# *REFERENCES*

## References

---

### References

- [1] S. A. Laskar and K. Hemachandran, "High Capacity data hiding using LSB Steganography and Encryption," *International Journal of Database Management Systems ( IJDMS )*, vol. 6, no. 4, pp. 57-68, December 2012.
- [2] I. F. Alsudany, "Analysis and Detection of Information Hiding in Digital Image," *M.Sc. in Data Securty ,Department ofComputer ScienceUniversity of Technology*, 2006.
- [3] R. Ibrahim and . T. S. Kuan, "Steganography Algorithm to Hide Secret Message inside an Image," *Computer Technology and Application*, vol. 2, pp. 102-108, February 2011.
- [4] D. Rawat and V. Bhandari, "Steganography Technique for Hiding Text Information in Color Image using Improved LSB Method," *International Journal of Computer Applications*, vol. 67, no. 1, pp. 22-25, April 2013.
- [5] K. Joshi and R. Yadav, "A New Method of Image Steganography using Last Three Bit Plane of Gray Scale Images," *Indian Journal of Science and Technology*, vol. 10, no. 38, pp. 1-8, October 2017.
- [6] R. Amirtharajan, R. Akila and P. Deepikachowdavarapu, "A Comparative analysis of Image Steganography," *International Journal of Computer Applications*, vol. 2, no. 3, pp. 41-47, 2010.
- [7] F. A. P. Petitcolas, R. J. Anderson and M. G. Kuhn, "Information Hiding—A Survey," *IEEE*, vol. 87, no. 7, pp. 1062-1078, July 1999.
- [8] H. Hazem , K. E. Sabri, M. S. Mohammed and A. Al-Dhamari, "A Hybrid Steganography System based on LSB Matching and Replacement," *International Journal of Advanced Computer*

## References

---

- Science and Applications (IJACSA)*, vol. 7, no. 9, pp. 374-380, 2016.
- [9] P. B. Desai and P. S. Bhendwade, "Image Steganography Using LSB Algorithm," *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (IJAREEIE)*, vol. 5, no. 8, pp. 6883-6890, August 2016.
- [10] A. Cheddad, "Steganoflage : A new image Steganography Algorithm," *PH.D School of computing & Intelligent systems Faculty of Computing & Engineering, University of Ulster*, 2009.
- [11] P. Maniriho and T. Ahmed, "Information hiding scheme for digital images using difference expansion and modulus function," *Journal of King Saud University –Computer and Information Sciences*, pp. 1-13, 2018.
- [12] A. Cheddad, J. Condell, K. Curran and P. M. Kevitt, "Digital Image Steganography : survey and analysis of Current Methods," *signal Processing*, vol. 90, no. 3, pp. 727-752, March 2010.
- [13] C. P. Sumathi, T. Santanam and G. Umamaheswari, "A Study of Various Steganographic Techniques Used for Information Hiding," *International Journal of Computer Science & Engineering Survey (IJCSES)* ,, vol. 6, no. 4, December 2013.
- [14] M. Varsha and K. Wandra, "A Novel Method for Security of Image Base on Image Steganography Using Hybrid Method," *IJARIE*, vol. 3, no. 2, pp. 448-460, 2017.
- [15] B. S. Champakamala , K. Padmini and D. K. Radhika , "Least Significant Bit Algorithm for Image Staganography," *International*

## References

---

- Journal of Advanced Computer Technology (IJACT)*, vol. 3, no. 4, 2012.
- [16] A. Sharma, M. Poriye and V. Kumar, "A Secure Steganography Technique Using MSB," *International Journal of Emerging Research in Management & Technology*, vol. 6, no. 6, pp. 208-214, June 2017.
- [17] M. Ramalingam and N. . A. Mat Isa, "A Steganography Approach over Video Images to Improve Security," *Indian Journal of Science and Technology*, vol. 8, no. 1, pp. 79-86, January 2015.
- [18] N. Jain, S. Meshram and S. Dubey, "Image Steganography Using LSB and Edge-Detection Technique," *International Journal of Soft Computing and Engineering (IJSCE)*, vol. 2, no. 3, pp. 217-222, July 2012.
- [19] S. Kaur, A. Kaur and K. Singh, "A Survey of Image Steganography," *International Journal of Computer Applications Technology and Research*, vol. 3, no. 7, pp. 479-483, 2014.
- [20] M. Rana, B. Sangwan and J. Jangir, "ART of Hiding : An Introduction to Steganography," *International Journal of Engineering and Computer Science(IJECS)*, vol. 1, no. 1, pp. 11-22, ctober 2012.
- [21] F. M. Shelke , A. A. Dongre and P. D. Soni, "Comparison of different techniques for Steganography in images," *International Journal of Application or Innovation in Engineering & Management (IJAEM)*, vol. 3, no. 2, pp. 171-176, February 2014.
- [22] K. . S. Shete, M. Patil and J. S. Chitode, "Least Significant Bit and Discrete Wavelet Transform Algorithm Realization for Image

## References

---

- Steganography Employing FPGA," *I.J. Image, Graphics and Signal Processing*, vol. 6, pp. 48-56, 2016.
- [23] G. S. Sravanthi, B. S. Devi, S. M. Riyazoddin and M. J. Reddy, "A spatial Domain Image Steganography Technique Based on Plane Bit Substitution Method," *Global Journal of Computer Science and Technology Graphics & Vision*, vol. 12, no. 15, 2012.
- [24] S. Areepongsa, Y. F. Syed, N. Kaewamnerd and K. R. Rao, "Steganography for A low-Rate Wavelet Based Image Coder," *IEEE*, vol. 1, pp. 597-600, 2000.
- [25] H. Elkamchouchi, W. M. Salama and Y. Abouelseoud, "Data Hiding in a Digital Cover Image using Chaotic Maps and LSB Technique," *IEEE*, pp. 198-203, 2017.
- [26] T. Morkel, J. Eloff and M. S. Olivier, "AN overview of image steganography," *In/SSA*, pp. 1-11, 2005.
- [27] K. H. Jung and K. Y. Yoo, "Data hiding method using image interpolation," *Computer Standards & Interfaces*, vol. 31, p. 465–470, 2009.
- [28] K. P. Adhiya and S. A. Patil, "Hiding Text in Audio Using LSB Based Steganography," *Information and Knowledge Management*, vol. 2, no. 3, p. 2012, 8-14.
- [29] M. Juneja, P. S. Sandhu and E. Walia, "Application of LSB Based Steganographic Technique for 8-bit Color Images," *World Academy of Science, Engineering and Technology*, vol. 3, no. 2, pp. 297-299, 2009.

## References

---

- [30] R. K. Shath and R. M. Tank, "Image Steganography Techniques," *International Journal of Computer Engineering and Sciences(IJCES)*, vol. 1, no. 1, pp. 10-15, 2015.
- [31] J. M. A. Al-Towayjri, "Overcoming The Effect of JPEG Compression on Steganography," *M.Sc. in computer Science,Universtiy of Technology*, October 2003.
- [32] B. Katre and Bharti, "Dynamic Key based LSB Technique for Steganography," *International Journal of Computer Applications*, vol. 167, no. 13, pp. 9-14, June 2017.
- [33] N. Hamid, A. Yahya, R. B. Ahmed and O. m. Al-Qershi, "Image Steganography Techniques : An Overview," *International Journal of Computer Science and Security (IJCSS)*, vol. 6, no. 3, pp. 168-187, 2012.
- [34] H. B. Kekre, A. Athawale, S. Rao and U. Athawale, "Information Hiding in Audio Signals," *International Journal of Computer Applications*, vol. 7, no. 9, pp. 14-19, October 2010.
- [35] I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich and T. Kalker, *Digital Watermarking and Steganography*, Morgan Kaufmann Elsevier, 2008.
- [36] D. Currie III and C. C. Irvine, "Sumounting the effects of lossy Compression on Steganography," *Proceedings of th19 National In formation System security Conference*, pp. 194-201, October 1996.
- [37] C. Olcay, " LSB Embedding on Still Images," *M.SC. in Computer Engeneering,Department of Computer Engineering, Cankaya University*, April 2010.

## References

---

- [38] R. Yadav, R. Saini and Kamaldeep, "Cyclic Combination Method for Digital Image Steganography with Uniform Image Steganography with Uniform," *Advanced Computing: An International Journal (ACIJ)*, vol. 2, no. 6, pp. 29-43, November 2011.
- [39] O. I. I. Al-Farraji, "Steganography By Use Binary Operations," *International Journal of Engineering Research and General Science*, vol. 4, no. 6, pp. 179-187, December 2016.
- [40] F. Hartung and M. Kutter, "Multimedia Watermarking Techniques," *Proceedings of the IEEE*, vol. 87, no. 7, July 1999.
- [41] S. M. Thampi, "Information Hiding Techniques: A Tutorial Review," *ISTE-STTP on Network Security & Cryptography, LBSCE*, 2004.
- [42] R. Yadav, R. i Saini and Gaurav, "SSB-7: A New Image Steganography System for Messsage Insertion Chance Enhancement using Bit 7," *International Journal of Computer Applications*, vol. 24, no. 4, pp. 7-14, June 2011.
- [43] Y. Garg and A. Kaur, "A Case study on Steganography and its Attacks," *International Journal of Engineering Trends and Technology (IJETT)*, vol. 47, no. 8, pp. 453-457, May 2017.
- [44] C. K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," *Elsevier*, vol. 37, p. 469 – 474, 2004.
- [45] A. Kumar and K. Pooja, "Steganography- A Data Hiding Technique," *International Journal of Computer Applications*, vol. 9, no. 7, pp. 19-23, 2010.



## References

---

- [46] K. Gregory, *Investigator's Guide to Steganography*, U.S.A, 2004.
- [47] A. Febryan , T. W. Purboyo and R. E. Saputra, "Steganography Methods on Text, Audio, Image and Video: A Survey," *International Journal of Applied Engineering Research*, vol. 12, no. 21, pp. 10485-10490, 2017.
- [48] R. D. Krutz, *Hiding Plain sight: Steganography and the Art of covert Communication*, Wiley, 2003.
- [49] S. K. Sabnis and R. N. Awale, "Statistical Steganalysis of High Capacity Image Steganography with Cryptography," *7th International Conference on Communication, Computing and Virtualization, ScienceDirect*, vol. 79, pp. 321-327, 2016.
- [50] W. Bender, D. Gruhl, N. Morimoto and A. Lu, "Techniques for Data Hiding," *IBM System Journal*, vol. 35, no. 3&4, 1996.
- [51] N. F. Johnson and S. Jajodia, "Exploring Steganography:seeing the Unseen," *IEEE computer*, pp. 26-34, February 1998.
- [52] P. c. Mandal, "modern steganographic Technique : A survey," *International Journal of Computer Science & Engineering Technology (IJCSET)*, vol. 3, no. 9, septemper 2012.
- [53] N. F. Johnson, Z. Duric and S. Jajodia, *Information Hiding Steganography and Watermarking - Attacks and countermeasures*, Springer Science & Business Media, 2001.
- [54] K. Munesh, G. Yadav, A. . K. Keshari and S. Katiyar, "Image Processing Using Steganography," *International Journal of Engineering Science and Computing IJESC*, vol. 7, no. 4, pp. 10619-10624, April 2017.

## References

---

- [55] V. Kalpana and C. Gayathri , "Study on Image Steganography Techniques," *International Journal of Engineering and Technology (IJET)*, vol. 5, no. 2, pp. 572-577, Apr-May 2013.
- [56] S. Manaseer, . A. Aljawawdeh and D. Alsoud, "A New Image Steganography Depending On Reference & LSB," *International Journal of Applied Engineering Research*, vol. 12, no. 9, pp. 1950-1955, 2017.
- [57] Deepika and J. . S. Mann, "Steganography System for Hiding Text and Images Using Improved LSB Method," *International Research Journal of Engineering and Technology (IRJET)*, vol. 4, no. 2, pp. 1249-1252, February-2017.
- [58] M. J. Bawaneh and A. A. Obeidat, "A Secure Robust Gray Scale Image Steganography Using Image Segmentation," *Journal of Information Security*, vol. 7, pp. 152-164, 2016.
- [59] S. A. El\_Rahman, "A comparative analysis of image steganography based on DCT algorithm and steganography tool to hide nuclear reactors confidential information," *Computers and Electrical Engineering*, pp. 1-20, 2016.
- [60] D. Singla and . R. Syal, "Data Security Using LSB & DCT Steganography In Images," *International Journal Of Computational Engineering Research (IJCER)*, vol. 2, no. 2, pp. 359-364, 2012.
- [61] P. Goel, "Data Hiding in Digital Images : A Steganographic Paradigm," *M.SC in Computer Science & Engineering, Indian Institute of Technology–Kharagpur*, May 2008.

## References

---

- [62] J. Mielikainen, "LSB Matching Revisited," *IEEE*, vol. 5, no. 13, MAY 2006.
- [63] B. Li, J. He, J. Huang and Y. Q. Shi, "A Survey on Image Steganography and Steganalysis," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 2, no. 2, April 2011.
- [64] K. Peter, C. Scace, M. Heyman and M. Mundy, "A survey of steganography techniques for image files," *Advanced Security Research Journal*, no. 1, pp. 41-52, 2003.
- [65] K. B. S. Kumar, K. B. Raja, R. K. Chhotaray and S. Pattanaik, "Bit Length Replacement Steganography Based on DCT Coefficients," / *International Journal of Engineering Science and Technology*, vol. 2(8), pp. 3561-3570, 2010.
- [66] K. Shete, . M. Patil and J. S. Morbale, "FPGA Implementation of Image Steganography Using LSB and DWT," *IJCSN International Journal of Computer Science and Network*, vol. 4, no. 6, pp. 847-853, December 2015.
- [67] H. S. M. Reddy and K. B. Raja, "High Capacity and Security Steganography Using Discrete Wevelet Transform," *International Journal of Computer Science and Security (IJCSS)*, vol. 3, no. 6, 2009.
- [68] S. E. Umbaugh, *Computer vision and image processing, a practical approach using cviptools with cdrom*. Prentice Hall PTR, 1997.
- [69] M. S. Atoum and M. M. Abu Shquier, "A Various Issues in Image Steganography that Using LSB Technique," *International Journal of Computer Networks and Communications Security*, vol. 3, no. 9, p. 363–366, September 2015.

## References

---

- [70] S. Balbhadra, J. Shrivastava and R. Miri, "A Novel Technique for Secure, Lossless Steganography with Unlimited Payload," *International Research Journal of Engineering and Technology (IRJET)*, vol. 2, no. 3, pp. 1166-1171, June-2015.
- [71] M. Spisak, "An analysis of perturbed quantization steganography in the spatial domain," *M.Sc., Department of Electrical and Computer Engineering, Graduate School Engineering and Management, Air Force Institute of Technology, Wright-Patterson Air Force Base*, 2005.
- [72] M. J. Mohsin, "A new algorithm for a steganography system," *Electrical Engineering Department, University of Technology*, September/ 2014.
- [73] A. Jafar, "Image steganography algorithm based on DWT and Turbo coding," *M.Sc thesis Submitted to the Electrical Engineering Department College of Engineering Al-Mustansiriya University*, 2008.
- [74] V. Singh, O. P. Singh and G. R. Mishra, "A Brief Introduction on Image Compression Techniques and Standards," *International Journal of Technology and Research Advances*, no. 11, pp. 15-21, 2013.
- [75] B. Dunbar, "A Detailed look at Steganographic Techniques and Their use in an open system environment," *SANS Institute*, August 2002.
- [76] M. Singh, S. Kumar, S. Singh and Manish, "Various Image Compression Techniques: Lossy and Lossless," *International*

## References

---

- Journal of Computer Applications*, vol. 142, no. 6, pp. 23-26, May 2016.
- [77] A. Katharotiya, S. Patel and M. Goyani, "Comparative Analysis between DCT & DWT Techniques of Image Compression," *Journal of Information Engineering and Applications*, vol. 1, no. 2, 2011.
- [78] F. Douak, R. Benzid and N. Benoudjit, "Color image compression algorithm based on the DCT transform combined to an Adaptive Block Scanning," *International Journal of Electronics and Communications (AEU) Elsevier*, vol. 65, pp. 16-26, 2011.
- [79] A. M. Raid, W. M. Khedr, M. A. El-dosuky and W. Ahmed, "JPEG Image Compression Using Discrete Cosine Transform - A survey," *International Journal of Computer Science & Engineering Survey (IJCSSES)*, vol. 5, no. 2, pp. 39-47, April 2014.
- [80] R. C. Gonzalez and R. E. Woods, *Digital Image Processing*, 3rd Ed, Prentice Hall, 2008.
- [81] H. R. Wu and K. R. Rao, *Digital Video Image Quality and Perceptual coding*, CRC Press, 2005.
- [82] A. M. Kadhim, "Audio Steganography of Multimedia Files Using Wavelet Transform," *PhD of Science in Physics, The University of Mustansiriyah, College of Science*, 2016.
- [83] M. A. Razzaq, M. A. Baig, R. A. Shaikh and A. A. Memon, "Digital Image Security: Fusion of Encryption, Steganography and Watermarking," *(IJACSA) International Journal of Advanced Computer Science and Applications*, vol. 8, no. 5, pp. 224-228, 2017.

# الخلاصة

في هذه الرسالة تم تبني منهجين لدراسة حالة هجوم JPEG على رسالة مخفية يتم زرعها باستخدام أساليب إخفاء المعلومات. في النهج الأولي، حيث يتم تقديم تحليل إحصائي لتأثير هجوم JPEG على رسالة مخفية مزروعة باستخدام طريقة البت الأقل الأهمية (LSB). يتم تحليل الرسالة في شكل ASCII وصورة النص بعد هجوم JPEG للجودة 50-100 لكل عمق بدء (Start Depth) محتمل باستخدام بت واحدة. من النتائج، تكون الرسالة المستردة في شكل الصورة أكثر قدرة على البقاء بعد هجوم JPEG مقارنة بنموذج ASCII ويمكن قراءتها إذا كانت جودة صورته أعلى من 13 dB. تم عرض مناقشة كاملة للنتائج التي تم الحصول عليها من الغلاف والرسالة المستردة بعد إجراء عملية الزرع بطريقة البت الأقل الأهمية وبعد إجراء هجوم الـ JPEG. في النهج الثاني، تم تقديم طريقة إحصائية جديدة لإخفاء المعلومات (NSSM) لتجاوز أو تقليل تأثير هجوم JPEG على صورة الغطاء (Cover Image). تعتمد الطريقة الجديدة على تحليل خوارزمية JPEG، التي فيها يتم استعمال قيمة الوسط والانحراف المعياري لكل كتلة (Block) للغطاء لتضمين الرسالة السرية، حيث يتم حساب كتل (Blocks) صورة الغلاف بنفس طريقة خوارزمية JPEG. تم استخدام صورتين قياسييتين مختلفتان في قوام نسيجهما لاختبار الطريقة الجديدة، ويتم تقديم تحليل ومناقشة لنتائج تطبيق هذه الطريقة التي أثبتت صحتها لتقليل أو تجاوز هجوم JPEG.



جمهورية العراق  
وزارة التعليم العالي والبحث العلمي  
جامعة بغداد  
كلية التربية للعلوم الصرفة - ابن الهيثم  
قسم الفيزياء

# طريقة جديدة مقترحة لإخفاء المعلومات لتقليل هجوم الضغط الأتلافي

رسالة مقدمة إلى

مجلس كلية التربية للعلوم الصرفة/ ابن الهيثم، جامعة بغداد

وهي جزء من متطلبات نيل درجة الماجستير في علوم الفيزياء

تقدم بها

**محمد كمال صالح**

(بكالوريوس علوم في الفيزياء 2007)

بإشراف

**أ.م. د. حميد مجيد عبد الجبار**

أيلول 2018م

محرم 1440هـ