# Enhancing Steganography Techniques in Digital Images

**Thesis** · November 2016

DOI: 10.13140/RG.2.2.16678.57925



**1 author:**

Shihab A. Shawkat S. A. Shawkat
University of Samarra Iraq
**4** PUBLICATIONS **44** CITATIONS

SEE PROFILE

**Computer Science Department**

**Faculty of Computers and Information**

**Mansoura University**

# Enhancing Steganography Techniques in Digital Images

***A Thesis***

Submitted to the Faculty of Computers and Information
Computer Science Department, Mansoura University
in Partial Fulfillment of the Requirements for the Degree
of Master of Science in Computer Science

***Submitted by***

**Shihab Ahmed Shawkat**

B.Sc., Dept. of Computer Science, Fac. of Sciences, Tikrit University (2007)
Lecturer at the Ministry of Education, Salah Al-Deen, Iraq

***Under the Supervision of***

**Prof. Dr. Taha Ibrahim Elarif**

Emeritus Professor of Computer Science, Faculty of Computers
and Information, Ain Shams University

**Dr. Osama M. Abu Elnasr**

Lecturer in Computer Science Department, Faculty of Computers
and Information, Mansoura University

**Egypt - 2016**

***Thesis Title***

# Enhancing Steganography Techniques in Digital Images

***Researcher Name***

**Shihab Ahmed Shawkat**

***Supervising Committee:***

| # | Name | Occupation | Signature |
|---|---|---|---|
| 1 | **Prof. Dr.** Taha Ibrahim Elarif | Emeritus Professors of Computer Science Faculty of Computers and Information Ain Shams University | Taha Elarif |
| 2 | **Dr.** Osama M. Abu Elnasr | Lecturer in Computer Science Department Faculty of Computers and Information Mansoura University | |

**Department Chair**

**Assist.Prof.** Samir Eldesoky Elmougy

Samir Elmougy

**Vice Dean for Higher Studies**

**Prof. Dr.** Ahmed Abu-Elfetouh Saleh

**Dean of Faculty**

**Prof. Dr.** Hassan Hussien Soliman

***Thesis Title***

# Enhancing Steganography Techniques in Digital Images

APPROVED Abee GENERAL MANAGER

REVISED Nancy DATE 27/12/2016

***Researcher Name***

**Shihab Ahmed Shawkat**

***Referees and Judging Committee:***

| # | Name | Occupation | Signature |
|---|---|---|---|
| 1 | **Prof. Dr.** Taha Ibrahim Elarif | Emeritus Professors of Computer Science Faculty of Computers and Information Ain Shams University | Taha Elarif |
| 2 | **Prof. Dr.** Mohamed Mohamed Eisa | Dean of the Higher Institute of Management and Computer Port Said University | M. Eisa |
| 3 | **Assist. Prof. Dr.** Samir Eldesoky Elmougy | Chair of the Computer Science Department, Faculty of Computers and Information Mansoura University | Samir Elmougy |

| Department Chair | Vice Dean for Higher Studies | Dean of Faculty |
|---|---|---|
| **Assist. Prof.** Samir Eldesoky Elmougy | **Prof. Dr.** Ahmed Abu-Elfetouh Saleh | **Prof. Dr.** Hassan Hussien Soliman |
| Samir Elmougy | | |

# ACKNOWLEDGMENTS

At first, great thanks to **ALLAH** for his graces on me that enabled me to continue the requirements of my study and overcome the difficulties that have faced me during this work. I'd like to convey my utmost gratitude to all people who have helped me or who have contributed to this project in any way. They have made this a great learning experience.

First and foremost, I would like to express my sincere gratitude to ***Prof. Dr. Taha Elarif*** , for his continuous support of my study, for his patience, motivation, and enthusiasm. His guidance helped me in all the time of research and writing this thesis. I deeply thank ***Dr. Osama M. Abu Elnasr***, for supervising this work, his continuous feedback and encouragement throughout the project. The fruition of my efforts is owing to his guidance and his support, without him this work would have been impossible. Special thanks are to ***Prof. Dr. Abdelhamid Elnaggar*** for his sincere guidance and prove reading this thesis.

Special thanks must be offered to ***Prof. Dr. Mohamed Mohamed Eisa*** and to ***Assist. Prof. Dr. Samir Eldesoky Elmougy*** , for their accepting to referee my thesis.

I extend my thanks and gratitude to my family, for their sincere support and patience during my study abroad. I am also highly grateful to my mother may **ALLAH** prolong her life, and my deceased father may **ALLAH** forgive and have mercy on him. Many thanks also go to my brothers and sisters for their continuous support and encouragement over the years.

I would also like to thank my friends, colleagues and anyone who has helped me with his thoughts and opinions in successfully completing this project. Last but not least, I like to express my grateful thanks to the **Ministry of Education and Scientific Research in Iraq** for their role and financially supporting the accomplishment of this thesis.

***Researcher***
***Shihab Ahmed Shawkat***
***2016***

# Abstract

The marvelous development in data transmission technology has put lots of potential on the process of securing data than before. Lots of methods have last decades for data been developed in the protection such as steganography and cryptography. Steganography refers to the science and art of hiding information inside a carrier, where nobody except the intended recipient, knows about the existence of hidden information. On the other hand, cryptography can be identified as the conversion of data into a secret code for transmission over a public network. The hidden information can existed be in a form of (text, audio, image or video). These approaches used in concealing secret texts are seeking to find a kind of harmony between the secret text and image pixel values.

The main objective of this work is to improve and propose a new hybrid technique for data security through the integration between cryptography and steganography algorithms. This system will be used to embed an encrypted secret message into a cover image to get high imperceptibility and durability with minimal deterioration in the received stego image. The proposed system was developed based on the Least Significant Bit (LSB) approach as a common steganography technique and 2D Discrete Wavelet Transform (DWT). This is in addition to improve the currently methods used in hiding secret messages, through making an integration between steganography techniques and cryptographic algorithms (Advanced Encryption Standard (AES) and Rivest Shamir Adleman (RSA)). In this hybrid approach the secret message is encrypted first before being hidden and that is an image part of the image stego.

# Abstract

In this work, a comparison is carried out between the original image file (cover image) and the stego image coming after performing the proposed techniques. Also, the hidden text is analyzed before being transmitted and after being received by the intended recipient. This is to make sure that less distortion happens to the original cover file after embedding the secret text and were also calculated to evaluate the obtained results from the proposed approaches based on statistical values. The proposed techniques in this work were performed on different message sizes varied between 1 to 256 bytes. These messages were hidden in some grayscale and color (RGB) cover images obtained from http://sipi.usc.edu/database/database.php 2011.

Various parameters were used for evaluating, the proposed techniques the Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE), and Mean Absolute Error (MAE), and Bit Error Ratio (BER), and Signal to Noise Ratio (SNR), and Structural Similarity (SSIM), and Structural Content (SC), and correlation. Experimental results presented at the end of the thesis confirm a relative improvement in the criteria used to measure the efficiency of the system. The PSNR in some extensions came to the limits of 88%. MSE in some extensions has become very low and close to zero. MAE parameter shows very small values with both color and grayscale images. This indicates no significant difference between the cover and stego image. The BER retrieval accuracy examining of the text after the adjustment has become close to 100%. The last three parameters (SSIM, SC and Correlation) take a value of one or very close to one with all the studied images (color and grayscale). This indicates a very high correlation between both the cover and stego image.

## *List of Contents*

# List of Contents

# List of Contents

# List of Contents

# List of Contents

# List of Contents

# List of Contents



-

# List of Figures

## *List of Figures*

# List of Figures

# List of Figures

# List of Figures

# List of Figures

# List of Tables

## *List of Tables*

# List of Abbreviations

## *List of Abbreviation*

| Abbreviation | Definition |
|---|---|
| **AES** | Advanced Encryption Standard (Rijndael) |
| **RSA** | Rivest-Shamir-Adleman Algorithm |
| **LSB** | Least Significant Bit Technique |
| **DWT** | Discrete Wavelet Transform Technique |
| **E** | Message |
| **P** | Plain Text |
| **C** | Cipher Text |
| **D** | Decryption |
| **K** | Secret Key |
| **SKC** | Symmetric Key Cryptography |
| **PKC** | ASymmetric Key Cryptography |
| **NIST** | National Institute For Standards And Technology |
| **PRNG** | Park Miller Random Number Generator |
| **MAC** | Media Access Control Address |
| **MIT** | Massachusetts Institute Of Technology |
| **RGB** | Read, Greed and Blue Colors |
| **DE** | Differential Evolution |
| **LFSR** | Line are Feedback Shift Register |
| **HVS** | Human Visual System |
| **DCT** | Discrete Cosine Transform Technique |
| **H** | High Pass Filter |

# List of Abbreviations

| Abbreviation | Definition |
|---|---|
| **L** | Low pass filter |
| **HWT** | Haar Wavelet Transformation |
| **BMP** | Microsoft Windows Bitmap |
| **TIFF** | Tagged Image File Format |
| **JPEG** | Joint Photographic Experts Group |
| **NHSA** | New Hybrid Security message Allocation Algorithm |
| **BFA** | Blowfish algorithm |
| **PBSA** | pattern based bits shuffling algorithm |
| **HCSSD** | High Capacity and Security Steganography using DWT |
| **ASCII** | stands for American Standard Code for Information Interchange |
| **CODED** | computed using the single-level reconstructed approximation |
| **PSNR** | Peak Signal to Noise Ratio |
| **MSE** | Mean Square Error |
| **MAE** | Mean Absolute Error |
| **BER** | Bit Error Ratio |
| **SNR** | Signal to Noise Ratio |
| **SSIM** | Structural similarity |
| **SC** | Structural Content |

## *List of Publication*

**1.** S. A. Shawkat , O. Abu-Elnasr and T. Elarif. "Evolved Algorithm to Secure Communication with Steganography". *International Journal of Intelligent Computing and Information Science (IJICIS)*, Vol.17 No.1, 1-17, 2017.

**2.** Elhoseny, M., Ramírez-González, G., Abu-Elnasr, O. M., Shawkat, S. A., Arunkumar, N., & Farouk, A. (2018). "Secure medical data transmission model for IoT-based healthcare systems". *IEEE Access*, *6*, 20596-20608.

# CHAPTER 1

# Introduction

## 1.1. Overview

The rapid and continuous development in information technology has forced computer networks to grow tremendously in a very short time. This results in facilitating electronic data transfer and in large amounts. The overwhelming advancement in the electronic ways of data exchange and the widespread of image use have put a huge potential on both security and protection of confidential data from unauthorized admission. Accordingly, development of security systems is very critical to guarantee the security of data during transition through the internet.

Cryptography is considered as one of the most commonly utilized techniques to guarantee data security. In recent years, great development has been achieved in data encryption technology. Many data encryption approaches are currently used especially for digital image security. Random encryption keys are produced in these techniques, whereas the genuine content becomes invisible.

Steganography is the science and art of hiding information within a carrier, where no one, except the intended recipient, has the knowledge of the existence of hidden information. Steganography as a term is derived from the

ancient Greek words "***steganos***", which means covered and "***graphic***" which means writing. In this operation, a secret message is concealed in another piece of normally looking information, which is known as the cover. This process aims to keep the secret information hidden without revealing any kind of suspicion to the viewer's [1].

Currently, there are lots of algorithms used to encrypt data in ways and styles. A hybrid encryption is a protocol using multiple codes of different types together. One of the common approaches is to generate a secret key to encrypt a random symmetric, and then encrypt this key cipher by using asymmetric public key of the recipient. The message is then encrypted using the same symmetric cipher and secret key. Then the secret key and the message are encrypted and sent to the receiver. In this work, an integration of encryption algorithms on the basis of (**AES** and **RSA**) was used to enhance the security of data transfer. It uses the AES algorithm for data transmission due to its high efficiency in the encryption block.

## 1.2. Problem Formulation

The Steganography is used as an approach for hiding digital information in a digital image, therefore it is considered as a means of communication that is used to transfer secret messages. However, transferring large amount of confidential data safely is dependent on the size of the cover image transmitted and used between related parties. In this work, the goal was to secure the transmitted data and prevent it from looking suspicious. This is carried out using steganography techniques and system encryption algorithms together for the purpose of improving these fundamental aspects of hiding digital information in an image. Some digital properties which can be used to determine the ability of Steganography and enhance the image used in the concealment quality were applied to guarantee reliable transition approach of secret data [2].

Generally, the fundamental framework for an image steganography model that could be utilized in copyright protection or concealing communication is demonstrated in Figure (1.1). Two main processes are involved in image steganography model consists, which are the embedding process and the extracting process. The first process is used to hide or embedding the secret message in a certain image, which is known the cover image.

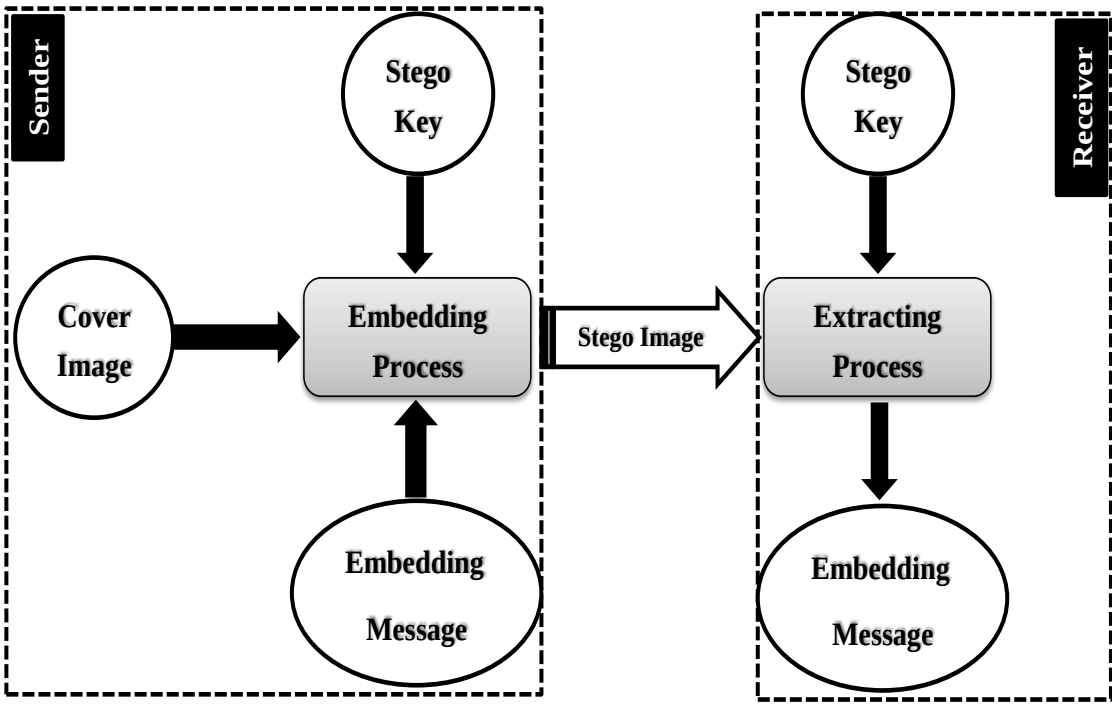



**Figure (1.1):** General framework of the steganography techniques**.**

In hidden communication techniques, the cover image is no more than an innocent piece of information that is used to hide the secret information. whereas in copyright protection techniques, the cover image is the important information that needs protection and the hidden message could be a copyright mark. In the embedding process, a stego key is used to make the embedded message difficult to extract without passing this key. The stego image represents the output of the message embedding process. This image includes the original image holding the hidden secret message. At the recipient side the embedded message is retrieved from the stego image either to verify the image copyright or

to complete the hidden communication process. The stego key is used in the embedding process and it has to be used in the extracting process.

Researchers are still working to find sophisticated techniques for hiding information to keep in track with the rapid evolution and advancement in technologies used in hiding information and networking.

## 1.3. Research Problem and Motivations

The purpose of the steganography is not only preventing others from knowing the hidden information, but also removing the suspicion in having hidden information. The distinctive thing in techniques used in hiding information is to stay in track with modern technologies and their ability to be used in all computer media (texts, image, audio, video and network packets).The message is a confidential document to be transmitted and camouflaged in the carrier so that it becomes difficult to detect.

There are two main aspects in any steganography system, which are steganography capacity and imperceptibility. However, these two properties are confusing with each other. This is because it is very hard to increase capacity while maintaining the steganography imperceptibility of a steganography system. Furthermore, there are still limited methods of concealing information for use with data transfer communication protocols, which can be unconventional but their future is promising.

The major **challenges** of developing an effective steganography system are [3]:

- The size of payload: Steganography aims at hidden communication and therefore usually requires sufficient embedding capacity. Requirements for higher payload and secure communication are often contradictory.
- The security of hidden communication: In order to avoid raising the suspicions of eavesdroppers, while evading the meticulous screening of algorithmic detection, the hidden contents must be invisible both perceptually and statistically.
- One of the most important motivations of our current work is to increase peak signal to noise ratio (**PSNR**), another motivations are to decrease the main squared error (**MSE**), decrease the average difference, and increase the embedding capacity of the stego image.
- The steganographic techniques are very sensitive to any different amendments get on the cover, such as image processing operations (smoothing, filtering , ,image transitions, etc.) and compression techniques, remove and filter the digital noise techniques that these techniques lead to the removal or amendments to the information an integral part of a highly secret . There is also a need to design algorithms steganography able to afford image processing operations.
- One of the important challenges is a must have the message content is safe from both (perceptual attacks or statistical). An important prerequisite for the design of algorithms is to hide information because there is more powerful special interest because of the presence of an active and malicious attack.

## 1.4. Thesis Objectives

The aim of this thesis is to improve and propose a new hybrid technique for data security through integration between cryptography and steganography algorithms. This system is used to embed an encrypted secret message into a cover image to get high imperceptibility and durability with minimal deterioration in the received stego image. The main objectives of this work were to:

- Develop a security system for hiding text data in an image using steganography techniques (**LSB** and **DWT**) individually.
- Develop a hybrid security system which integrates both data encryption (**AES** and **RSA**) and steganography techniques (**LSB** and **DWT**) to increase data imperceptibility, robustness and performance of stego image.
- Evaluate the efficiency of the developed system in securing and retrieving the original data.

## 1.5. Contributions

The main contributions of this thesis could be summarized in the development of an enhanced technique for hiding secret information on the spatial scale of data transformation. This is in addition to giving a new direction on how to improve the existing methods used in hide secret messages, through the integration between Steganography and coding techniques. In the proposed

system the secret message is first encrypted before being embedded in the stego image. This is to achieve the highest level of security and make it very difficult for a stranger to see the hidden message.

## 1.6. Thesis Layout

This thesis consists of six chapters including this chapter. These chapters are structured as follows:

- ✓ **Chapter 2 (*"An Overview on Encryption"*):** This chapter provides an overview of general historical review of information security. It introduced the encryption techniques used in encrypting text in digital images. Then, it provides a detailed explanation about the basic concepts and coding algorithms that were used in terms of advantages and characteristics of each algorithm.
- ✓ **Chapter 3 ("*Background and Previous work in Steganography*"):** This chapter provides an introduction about the related work in the field of steganography. It also provides a general idea about steganography, main data hiding concepts, historical review and then move to more detailed steganography types and examples.
- ✓ **Chapter 4 (*"The Proposed System Model"*):** This chapter illustrates how the proposed security system was development. It also explains the applied algorithms and the different data management and manipulation in that system.

- ✓ **Chapter 5 (*"Experimental Results and their Discussions"*):** This chapter contains the results coming from carrying out the proposed security system, data representations and their discussions.
- ✓ **Chapter 6 (*"Conclusion and Future Work"*):** Summary of the major conclusions and recommendations for the future work are included in this chapter.

# CHAPTER 2

## An Overview of Encryption

Information security has become more important in data storage and transmission. This chapter provides some security backgrounds that apply many encryption algorithms. The rapid development of data exchange in electronic ways and the widespread of image use have put a great potential on data security and safeguard of confidential data from accessible from unauthorized. Encryption is considered as one of the most commonly used approaches for ensuring high data security. In recent years, a great development has occurred in encryption technology, where many encryption methods are used for image security. These methods produce random encryption keys, whereas the actual content is not visible. Both of the encryption and decryption algorithms are designed and implemented to provide secure transfer of image data.

**This chapter includes the follows topics:**

**1 –** Introduction to Information Security,

**2 –** History of Cryptography,

**3 –** Types of Cryptography (Encryption),

**4 –** Image Encryption,

**5 –** Digitai image concept,

**6 –** Major image Encryption Techniques,

**7 –** Summary.

## 2.1. Introduction to Information Security:

Information security is a means to an end and not the end in itself. In business, the existence of an effective information security program is usually secondary to the need to make a profit. In the public sector, information security is secondary to the stability of its services. The must not lose sight of these goals and targets.

The Digital communication is an integral part of life. With the advent of digital technology, This has become more sophisticated than ever. Moreover, information has become the most expensive commodity in the sense of the most sought-after in the world today. In addition, the rapid growth of the age of the computer for all documents and audio and video recordings being digitized. This has increased the need to ensure the security and integrity of any document, audio and video to maintain privacy, piracy and mass reproduction. This condition varies from one individual to another. The different techniques used to ensure that privacy is encryption [4].

The confidential information may be considered such as military secrets, banking transactions, and so on must be guarded against unauthorized access. As a result, developing a new field of study is called "information security". Information security is a science that deals with the secure transfer of critical information from one person to another. This should happen by maintaining the integrity and authentication, confidentiality and non-repudiation, in such a way

that the transmitted information can not be accessed by unauthorized person only the sender and receiver [5]. This is considered the core of information security that provides a structure for all other aspects of information security.

The information security has three primary goals for information security, which are confidentiality, integrity, and availability as illustrated in Figure (2.1) [6]:

- **Confidentiality (secrecy)**: Refers to maintain the restrictions authorized access to information and disclosure, including ways to protect the privacy of personal and confidential information. Loss of confidentiality is the unauthorized disclosure of information.
- **Integrity:** Deals guard against the alteration of the information inappropriately or destruction, including ensuring non repudiation of the information and authenticity. Loss of integrity is the unauthorized modification or destruction of information. Availability of secure access in timely and reliable information on time.
- **Availability:** Disable access to or use of information or information system. When they put these three principles together and the information we have and will be well protected. In addition to multiple sources of information security attacks, there are also many types of information security attacks.


**Figure (2.1):** The security requirements triad [6].

Every data communication transaction must met some of the goals related to information security. Most of these goals include the common security of information in addition to the three mentioned before [7]:

1. **Identification (Entity authentication):** It the identity of the entity (person, credit card, etc.).
2. **Authorization:** Is the transportation to another entity, with official approval to do to be a certain thing.
3. **Message authentication:** Is backing a source of information, which is also known known as the origin of the data authentication.
4. **Validation of information:** It is a way to provide a timely authorization of the use or manipulation of information.
5. **Time-stamping:** Is the record time of creation or existence of information.
6. **Signature:** Is a way to link the information to the entity.

### 2.1.1. Security Implementation:

Four complementary courses of action are involved in security implementation [8]:

- **Prevention:** An ideal security system aims to prevent unauthorithed attacks. However, this is not practical in most cases, because there are many threats that prevention is a reasonable goal.
- **Detection:** The absolute protection in some cases, are not possible, while it is possible to detect security attacks. For example, there is intrusion detection systems are designed for the purpose of detecting the presence of an individual or unauthorized individuals register to enter the system.
- **Response:** It refers to the system in response to stop the attack and prevent further damage. This is in case if security mechanisms detect an ongoing attack.
- **Recovery:** It referes to the backup of the security system in case if it is compromising the integrity of the data. As in the former case, you can restore the correct copy of the data that can be recharged.

## 2.2. Cryptography

### 2.2.1. History of Cryptography:

Cryptography is a rather old business; however it seems closely connected with modern electronic communication. Possible to give an early example and return to about (2000 BC), when it was used non standard hieroglyphs "secret" in the civilization of ancient Egypt. The Egyptian days ago, it has been the use of encryption in one form or the other in a lot sometimes, if not more, and that the cultures that developed a written language. For example, there are no documented cases of secret writing in the civilization of ancient Greece, a Skital of Sparta, Figure (2.2), or that you know the famous blades Caesar. This work focuses on modern cryptographic approaches in issues related to data security and their relationship with cryptography [9].

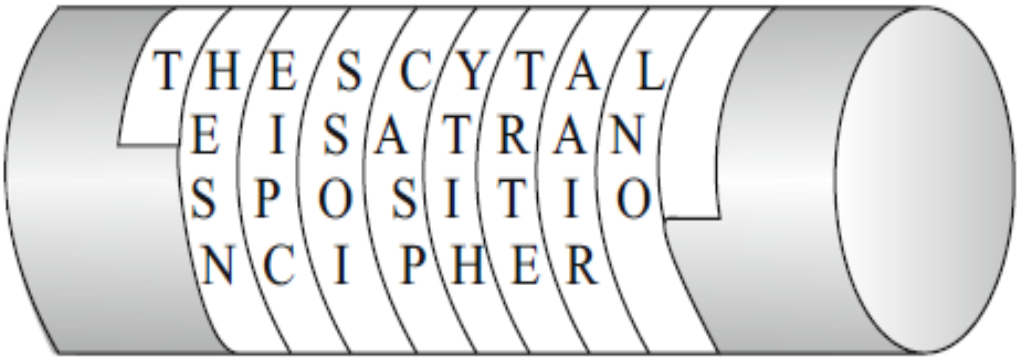



**Figure (2.2):** Scytale of Sparta [9].

Figure (2.3) provides an overview to the field of cryptography. The first thing that we notice is that the most general term is cryptology and not cryptography.

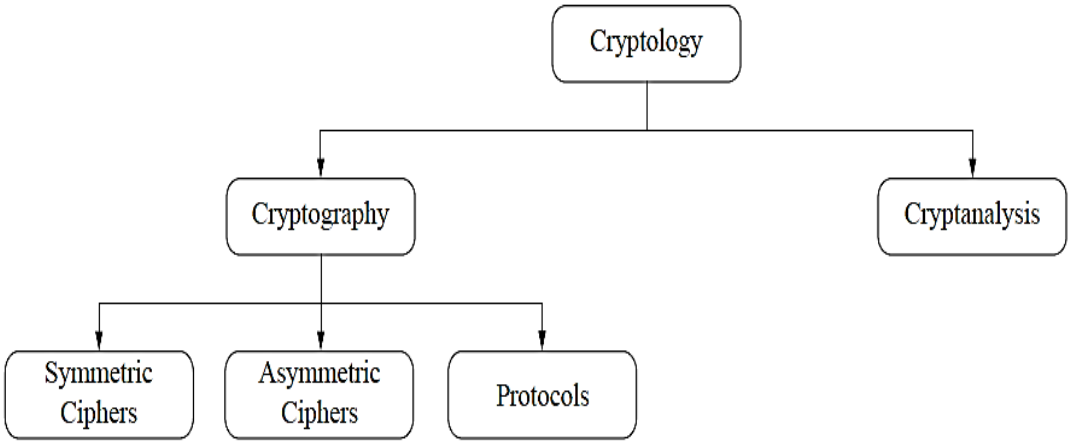



**Figure (2.3):** Overview of the field of cryptology [9].

Cryptology is divided into two main sections, namely:

- **Cryptography**: It the science of secret writing the main goal is to hide the true meaning of the message used.
- **Cryptanalysis**: It is a science or art of coding systems break down. Sometimes you might think that the break be available and should not be included in the classification of a serious scientific discipline. Although these days most of cryptanalysis by researchers in academia and of central importance to modern coding systems. We will never know whether they are safe or not [9].

The Cryptanalysis is considered as an integral part of cryptology, because it is the only way to assure that a cryptosystem is secure. Cryptography is a general word, which has sub-categories, as illustrated in Figure (2.4).

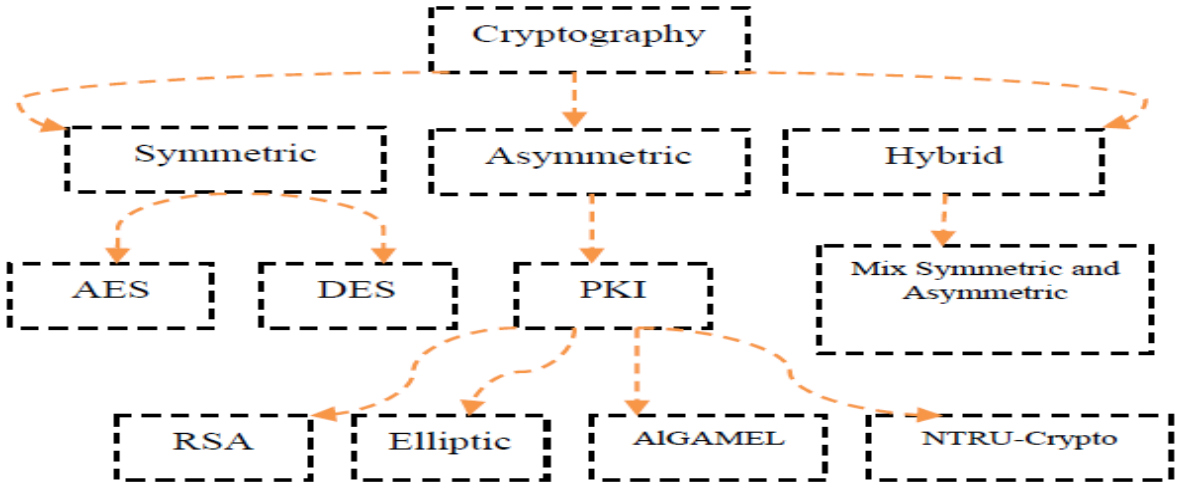



**Figure (2.4):** Shows Cryptography Tree**.**

Cryptography can be defined as working to transform the data into a secret code to carry more than the public network. Therefore, the sender was able to secure sensitive information and mission or to transmit it through non secure networks or non protected storage, so the data will not be available to only one recipient.

### 2.2.2. Cryptography Main Concepts:

A large number of technical and legal skills are requires to achieve information security in an electronic society. The provision of technical means is through encryption. Since the Cryptography or (Cryptology) is considered the practice and study techniques for secure communication, in the presence of third parties, it called the (adversaries). More generally, it is about building and analysis protocols that overcome the influence of adversaries. The encryption modem intersects the disciplines of mathematics, computer science, and electricalengineering. Cryptography is not the only means by which the provision of information security, but it is one set of technologies [10].

### 2.2.2.1. Cryptography Goals:

One of the things it offers Cryptography, which is the number of security objectives and to ensure data privacy, and do not change the data and so on. Because of the advantages of a major security coding and it is used widely today. Among all targets the security of the information listed above, the following four objectives are considered the foundation. These objectives are (confidentiality, authentication, integrity and non repudiation) [11].

The primary goal of Cryptography is sufficiently address each of these four areas that have been mentioned in both theory and practice. Encryption is working on the prevention and detection of fraud and other malicious activities.

### 2.2.2.2. Major Concepts:

Encryption cryptography is the process of encoding messages in way hackers can not read it, but that can be authorized pesonnal. In the encryption system (**E** = the message), it is encrypted (**P** = plain text) using the encryption algorithm that transforms them into unreadable (**C** = cipher text). This is done using the encryption key, which explains how the message to be encrypted. Only authorized party, is able to decode text using symbols and codes (**D** = decryption algorithm), which usually requires (**K** = secret decryption key). Usually it needs to generate key encryption algorithm system for technical reasons, to produce random keys [12].

The role of cryptography can be illustrated as a simple model of cryptography as demonstrated in Figure (2.5). The basic idea of encryption is to modify the content of the message in a certain way only allow the legal recipient can rebuild its content. The discrete valued cryptosystem can be described by:

- **P**: It is a symbol a set of possible plain texts.
- **C**: It is a symbol a set of possible cipher texts.
- **K**: It is a symbol a set of possible cipher keys.
- **E,D**: It is a symbol a set of possible encryption and decryption transformations.

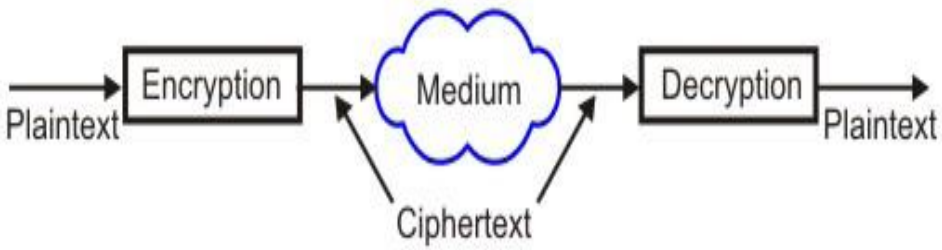



**Figure (2.5):** Asimple cryptography model [12].

### 2.2.3. The Basic Terminology in Cryptography:

- **Plain Text:** It refers to the original message sender that the wants to communicate with another person.
- **Cipher Text:** It to the message that cannot be understood by anyone. In other words it is a meaningless message, where the original message (plain text) you will turn to the message unreadable and incomprehensible through an encoder before the actual message transfer.

- **Encryption:** It explans is the process used to convert (plain text) into (cipher text), which is called as Encryption. Encryption technique are used to send secret messages and encoded through a private and secure channel. The encryption process will need two main things, which are the basics of each algorithm encryption algorithm and key.
- **Decryption:** It reverses the encryption process. In other words, any process to convert (cipher text) to (plain text).We use the decryption technique side in the second technique (receiver) so as to obtain the support of the original (cipher text message). Here, the process also needs to decryption algorithm and key to make sure the message is sent.
- **Key:** It refers to a numerical or alpha numeric text or a special character. And this key is used on the first two phases as encryption (plain text) and the second time decryption of (cipher text) the selection is very important in the cryptography key to the security of the encryption algorithm mainly depends directly on it. When the same key is used for encryption and decryption it is called as symmetric key cryptography. On the other hand, when it is the use of different keys in the cryptographic mechanism, Where it is to use a special encryption key one, and another, and the second is used is different from the decryption key. Where this mechanism is called as Asymmetric Cryptography Key as illustrated in Figure (2.6) [13].

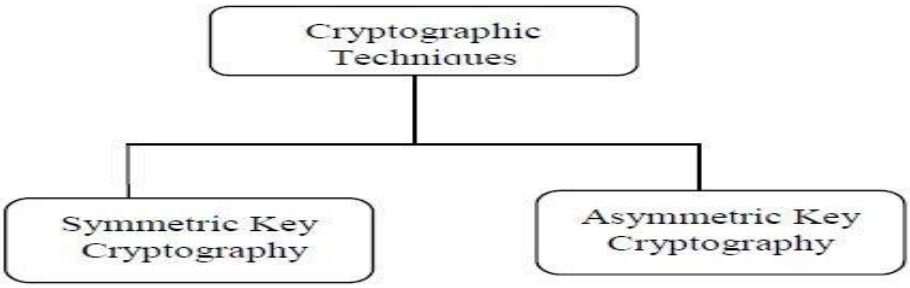



**Figure (2.6):** The Cryptographic techniques [13].

## 2.3. Types of Cryptography (Encryption):

Basically there are many ideas of categorized cryptograph techniques. According to cryptography techniques are divided on the bases of no of the key used for encoding and decoding the message information and also define the use and applications of these types of cryptography [14]. The two types of cryptography techniques are given below:

- Symmetric Key (Private or Secret Key Cryptography (**SKC**)).
- Asymmetric Key (Public Key Cryptography (**PKC**)).

### 2.3.1. Symmetric Key (Private or Secret Key Cryptography (SKC)):

In private key crypto system, one key is used for both the time i.e. encryption and decryption at sender and receiver side respectively. The sender has some key or some predefined set of rules to encode the plain message into cipher text to transmit cipher data to the receiver using any channel. The receiver receives cipher text and applies the same key or set of rule to decrypt the cipher text into the plaintext.

As a single key is used for both encryption and decryption, it is also known as symmetric encryption or symmetric cryptography as shown in Figure (2.7).

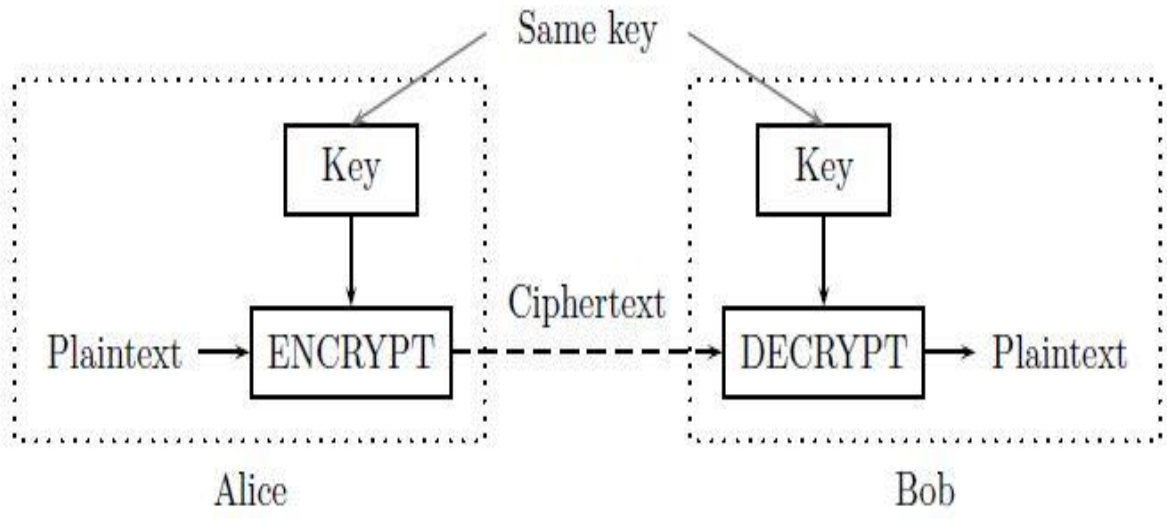



**Figure (2.7):** A two party communication using encryption (**SKC**) [14].
(Ciphertext = encrypt (plaintext, key) , Plaintext = decrypt (ciphertext, key)).

In this type of cryptosystem, It must be the key to know that all of the (sender and receiver), and it should be secure.The biggest problem with this type of method is how the key distribution between two parties. Private Key cryptography techniques are normally classified as stream ciphers or block ciphers. The stream ciphers apply on a byte or word at a same time and implement a kind of function by which complete plain text message will encrypt and converts into cipher text. The other type of cipher encodes one block of data message at a time by using the same key on every block of data as it is called as

block cipher. Some most common types of private key cryptography schemes are DES and AES [15].

#### 2.3.1.1. Advantages of Private Key Symmetric Cryptography:

A private key symmetric cryptosystem is faster than public key cryptosystem. In symmetric cryptosystems, encrypted data can be transferred on any channel because the key is not transmitted with the data so there is not a possibility that the data will be intercepted:

1. A symmetric cryptosystem also uses password authentication to prove the identity of receiver.
2. A user only having the secret key can decrypt a message.

#### 2.3.1.2 Disadvantages of Private Key Symmetric Cryptography:

Disadvantages of private key symmetric cryptosystems can be summarized as:

1. It has a big problem of key transportation. It requires transmitting the key before the message is being transmitted to the receiving system. In the digital world of electronic communications is not secure as it is impossible to ensure that the message will transmitted securely or no one will be able to tap communication channels. This is because insurance contact is the only way for the exchange of keys, which will exchange them personally.
2. Symmetric key cryptography can not provide digital signatures, which in turn can not be repudiated.

**There are two types of symmetric key algorithms:**

- **First is Block cipher:** which processes the input one block of elements at a time, producing an output block for each input block. The basic encryption code depends on the size of the fixed used data block. It must be added to it, if data is not on the length of the block size limit, it must be added to it.
- **Second is Stream cipher:** the kind who does not work on the basis of the block, but is working to convert all (1 bit) or (1 byte) of data used in only one time. It processes input elements, continuously, producing output one element at a time, as it goes along. The other one, the simple transposition cipher, simply permutes the Symbols in a block. Simple substitution and transposition ciphers individually do not provide a very high level of security. However, by combining these transformations it is possible to obtain strong ciphers [16].

### 2.3.1.3. Advanced Encryption Standard (AES) Algorithm:

The Advanced Encryption Standard (AES) is a crypto standard defined by the National Institute for Standards and Technology (NIST) in the United States. It is a result of a contest organized in 1997. NIST has encouraged existing parties all over the world to submit proposals for new standards. He was required of the proposals submitted to support block size of (128) bits, at least, as well as the three main volumes consist of (128 192 and 256) bits. Three years later, the Rijndael Algorithm, designed by Joan Daemen and Vincent Rijmen, was announced as winner. The final standard AES was presented in 2001.

Figure (2.8) demonstrates the Block Cipher Operation. The important reason behind the success of the Rijndael algorithm was its simpilisity and easy to implement at both software and hardware levels.

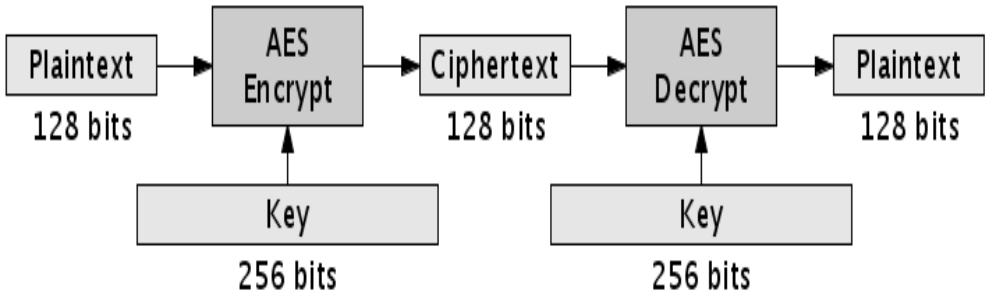



**Figure (2.8):** Block Cipher Operation [17].

Encryption with AES (Rijndael) algorithm consists of adding the initial round key. This is followed then by this application function round of the function (*Nr* - 1) times and (*a* = Nal) round with *a* a little (mod *i*) and the round function [17].

The round suction consists of the (subbytes, shiftrows and mixcolumns) steps and an addition of the round key. The Mix Columns step is careless in the (Nal) round. The following give rise to describe a high level of AES (Rijndael) algorithm:

```
By testring Rijndael (byteString plaintextBlock; key)
 1  InitState (plaintextBlock; state)
 2  AddKey (state; key0)
 3  for  i ⇐ 1 to Nr - 1 do
 4       - SubBytes (state)
 5       - ShiftRows (sate)
 6       - MixColumns (state)
 7       - AddKey (state; keyi)
 8  SubBytes (state)
 9  ShiftRows (state)
10  AddKey (state; keyNr )
11  return state;
```

Both that hat each one of the inputs and outputs of the blocks AES (Rijndael) algorithm is to be in chains in the form of bytes. First, the state will be creating a matrix with a plain text block, and then work on the matrix filled (column by column). Then it is taken cipher text of the matrix state after the last round.

At this time, the note will be read matrix (column by column). All the steps function round of (subbytes, shiftrows, mixcolumns and Add key). It is invertible in the opposite direction [18]. The following are the steps of of the AES (Rijndael) algorithm and the type of output layers:

- **Subbytes** (nonlinear layer) .
- **Shif trow** (linear mixing layer) .
- **Mixcolumn** (nonlinear layer).
- **Addroundkey** (key addition layer).

### 2.3.1.3.1. AES as Hardwired Electronics:

AES is a symmetric cipher where the same key is used on both sides. It has a fixed message block size of 128 bits of text (plain or cipher), and keys of length 128,192, or 256 bits. When longer messages are sent, they are divided into 128 bit blocks. Obviously, longer keys make the cipher more difficult to break, but also enforce a longer encrypt and decrypt process. A 128 bit message block can be thought of as organized in a two dimensional 4×4 byte array. AES encryption has four main operations that are repeated multiple times, and work on bytes, rows, and columns of this array. Figure (2.9) illustrates the AES encryption and decryption processes [19].

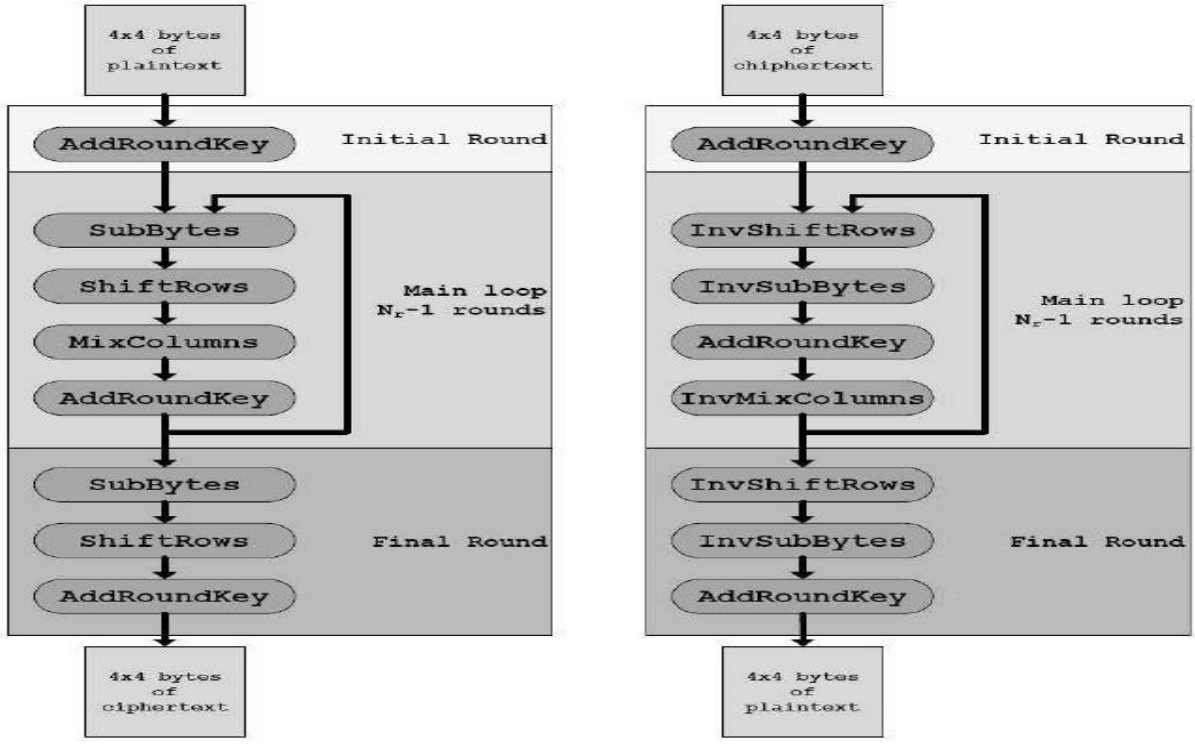



**Figure (2.9):** AES encryption and decryption processes [19].

### 2.3.1.3.2. Evaluation Criteria for AES:

The main demand of the AES algorithm submission is requir you must be a block cipher, which supports the length of the block consists of a 128 bit key lengths are: (128, 192, and 256) bits. The following evaluation criteria were used in evaluating the call for proposals [20]:

1. **Security:** Is one of the most important factors in the evaluation in terms of**:**

- Are compared to the actual security algorithm for other algorithms provided.
- It is important to ensure the integrity of the foundation of mathematics used to maintain the security of the algorithm.
- The other security factors that are by the public and that are discovered during the evaluation process.

2. **Cost:** This section includes the following**:**

- The licensing requirements, as the AES algorithm should be available and not exclusive.
- Must be Are available as well (Excellent computational efficiency, memory capacity) requirements.

3. **The algorithm and implementation of characteristics:** This includes the following**:**

- Flexibility, which are intended to provide the key tools such as: (PRNG, MAC generator, retail, stream cipher).
- Must provide a suitable environment between (Hardware and software) used and also provides (The ease and simplicity).

The following Table (2.1) summarizes the performance analysis and comparison AES algorithms.

**Table (2.1):** Performance analysis and comparison such as AES.

| No. | Features | Advantages |
|---|---|---|
| **1** | Encryption | Fast |
| **2** | Decryption | Fast |
| **3** | Key size (length) | 128 bits. 192 bits. 256 bits |
| **4** | The block size | 128 bits |
| **5** | Rounds | 10. 12 or 14 |
| **6** | Speed depends on Key | Fast |
| **7** | Security | Excellent security (Insecure ) |
| **8** | Cost | Cheaper |
| **9** | Implementation | Simple |
| **10** | Power consumption | Low |

### 2.3.2. Asymmetric or Public Key Cryptography (PKC):

Public Key is the mostly used cryptography in the last few decades worldwide. It was first developed by both Martin Hellman, a professor at (Stanford University) and Whitfield Diffie in the (University of Washington) and that in 1976. They proposed a couple key cryptograph system in which a two communicating side could exchange of message In a safeness Way through the communications channel is not safe without the need for the exchange of the secret key one is for sender and other for receiver Figure(2.10). Shows a two party communication using a PKC encryption.

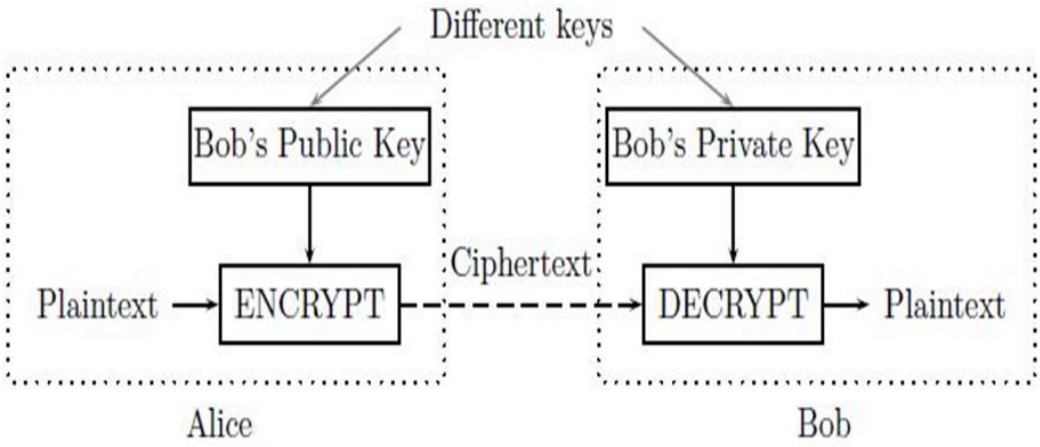



**Figure (2.10):** A two party communication using encryption (PKC) [21].
(Ciphertext = encrypt (plaintext, key) , Plaintext = decrypt (ciphertext, key)

PKC employs two keys one is encryption key and another is decryption key and that are mathematically related to each other but information of one key from the two does not allow anyone to easily find the other key [21].

Encryption key will be used to encrypt the plain message into cipher message and the decryption key is used to decrypt the cipher text message to again plain text. The main thing here is that we can apply any key first, it does not matter that which key was applied first and which is second, but the main point is, both are the keys are required for the process the encryption completely. This approach is required a pair of keys so it also called as asymmetric cryptography.

### 2.3.2.1. Advantages of Asymmetric Key:

Asymmetric Key cryptography has the following advantages:

1. In PKC will note there is no need to be the exchange of keys, which will remove the key distribution problem.
2. In order to increase the key PKC security feature, which the private keys do not ever need to be transmitted or disclosed any person who handles them.
3. It can also be told to PKC that is working to provide digital signatures, which can be repudiated.

### 2.3.2.2. Disadvantages of Asymmetric Key:

The main disadvantage of using PKC is the time complexity for encryption. Nowadays, and note that there are some methods of the secret encryption key to be local or popular, and that the advantage of being much faster than PKC method [21].

### 2.3.2.3. Rivest-Shamir-Adleman (RSA) Algorithm:

The origin is called asymmetric cipher and public key is the Rivest-Shamir-Adelman (RSA) and that of its founders. Because they all were members of the (Massachusetts Institute of Technology (MIT)) and RSA has been selected and that because of its popularity and has also been analyzed extensively. It is commercial, the public key algorithm to be advertised widely and used in each of the sector (business and personal communications). In current applications, RSA the advantage that it has a variable key size ranges (2-2048) bit. The security of this algorithm depends mainly on the key size of the user or the programmer chooses. This algorithm is used and the length of the key size (1024) bit representation despite still being worked with many of the applications with the key (512) bits [22].

A symmetric key is often referred to private or secret key encryption. In general, it is a category of algorithms that use a single key purpose is to (encrypt or decrypt) messages. The key is the way to confidential information that is used, so the parties involved want to communicate with each other and with all confidential. The forms of security optimium are to have each pair of correspondents has a separate key. Therefore, it is important for both parties is to maintain the confidentiality of the user key.

First, working on encrypt the message sent by the sender and using the secret key and this is before it is transmitted to the recipient of the message. On the other hand, that the recipient will use the same key to encrypt the message received by him. This is where he works as a service secret key ratification of the message. It also distinguishes the missionaries from other malicious sources.

### 2.3.2.3.1. Requirements for public key cryptography.

The send message integrity is compromised, in case if the key is known. Accordingly, The Necessary to find a safe manner used to exchange key be established between the correspondents. Encryption of a Private Key, depend solely on the protection key to success in his mission as illustrated in Figure (2.11).

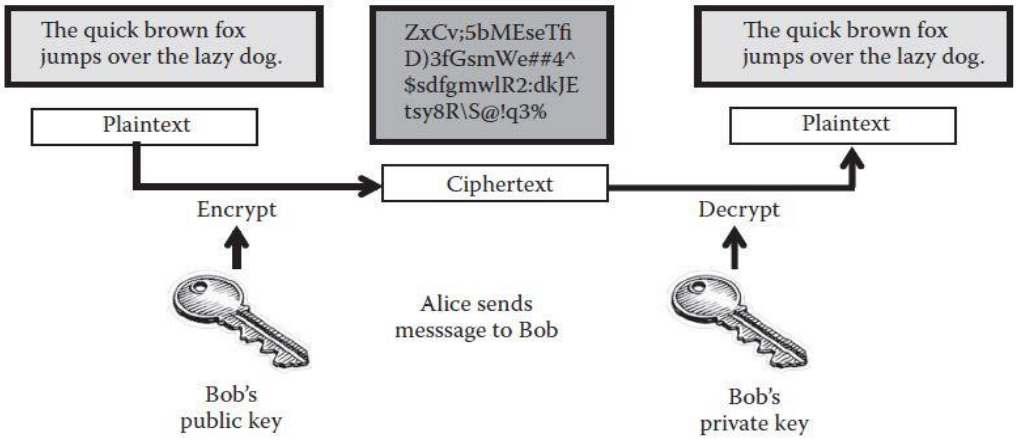



**Figure (2.11):** The public key encryption Bob receives the encrypted message Alice uses her public key for decryption [22].

Public key encryption enables secure electronic business communication through keys and certificates as illustrated in Figure (2.12). It shows how a message is encrypted, therefore only the intended recipient can decrypt it. Consequently, Alice encrypts a message for Bob to receive by encrypting it using Bob's public key. Bob decrypts the ciphertext using his private key [22].

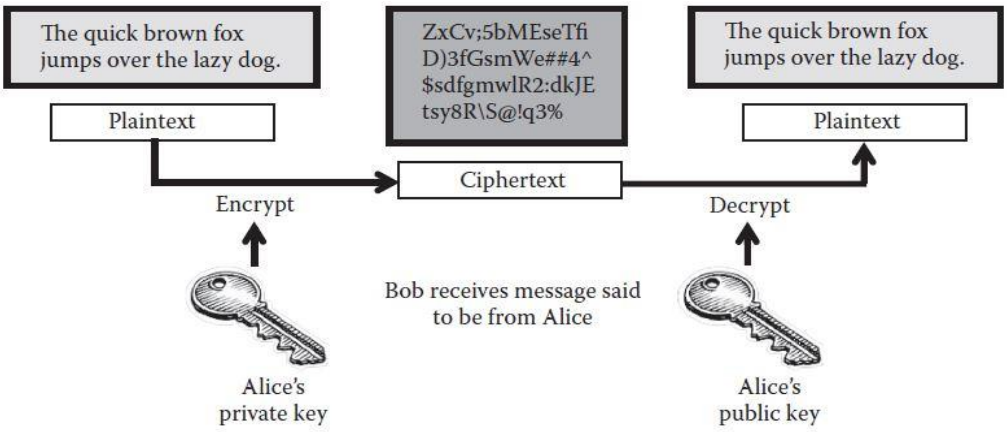



**Figure (2.12):** Alice message encryption for Bob using his public key and its decryption using his private key [22].

### 2.3.2.3.2. Practical Implementation of RSA Algorithm:

To implement the RSA, one has to focus on three parts which are: **a)** key generation. **b)** Encryption process. **c)** Decryption process.

Both sender (**Bob**) and receiver (**Alice**) must know the value of **n**. The sender knows the value of **e**, and only the receiver knows the value of **d**. Thus, this is shown in Figure (2.13) [23].

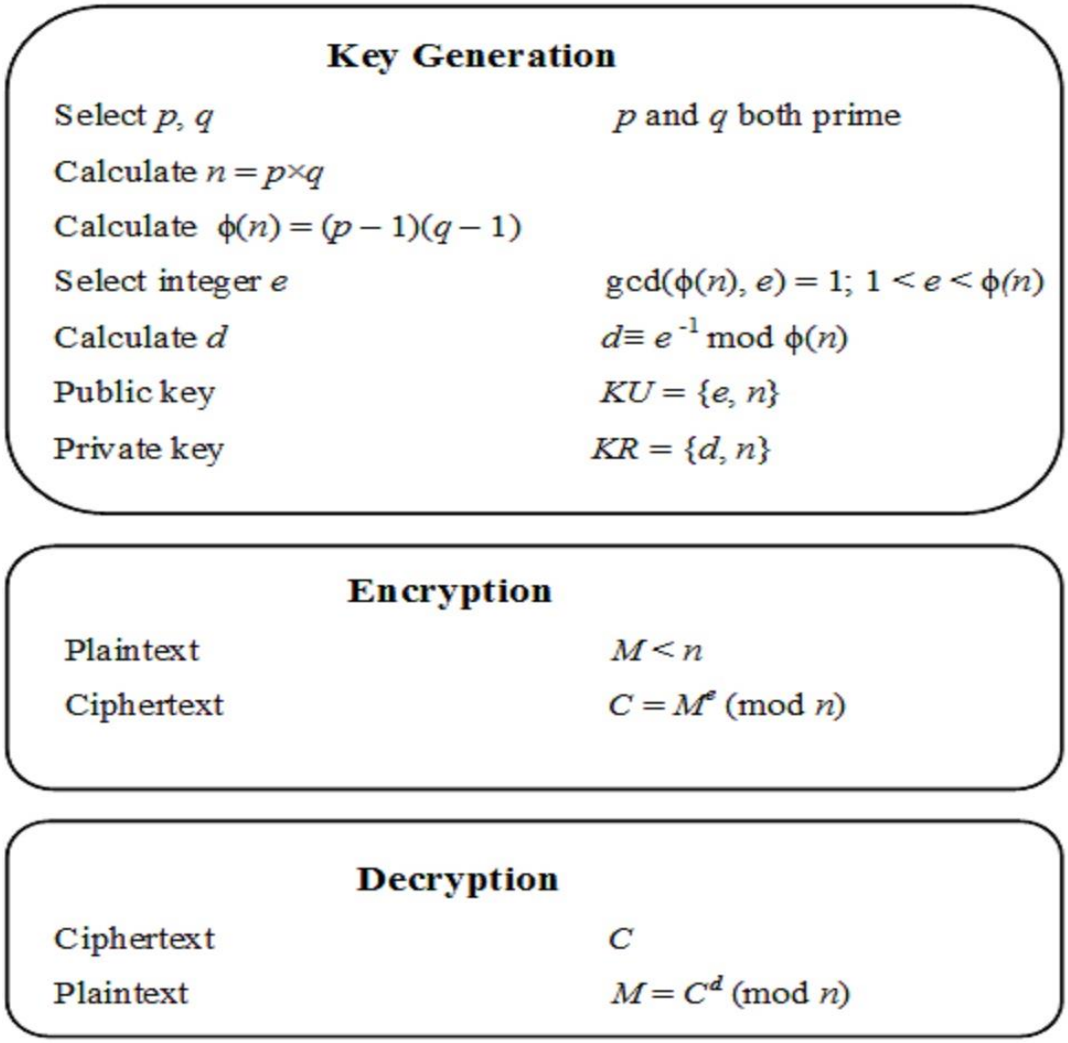



**Figure (2.13):** The RSA Algorithm**.**

**Key Generation Algorithm:**

There are two types of keys in RSA; public key and private key. Table (2.2) represents the feautes in the RSA and their advantages.The steps for key generation are given as follow:

1. Generate two large prime numbers **p** and **q**.
2. Compute **n = p×q.**
3. Compute **ϕ (*n*) = (p-1)(q-1) .**
4. Choose a number relatively prime to **z** and call it **d**.
5. Find e such that e*d=1 mod **ϕ (*n*).**
6. Public key is (**n, e**).
7. Private Key is (**n, d**).

**Table (2.2): Performance analysis and comparison such as RSA**

| No. | Features | Advantages |
|---|---|---|
| **1** | Encryption | Fast |
| **2** | Decryption | Fast |
| **3** | Key size (length) | Be different key during the (encryption and decryption) |
| **4** | The block size | 1024 bits |
| **5** | Rounds | 128 bits |
| **6** | Speed depends on Key | Not applicable |
| **7** | Security | Fast |
| **8** | Cost | Least secure |
| **9** | Implementation | Costly |
| **10** | Power consumption | Complex |

## 2.4. Image Encryption:

In these days when more and more critical information is stored on computers and transmitted over the Internet, we want to include information security and safety. Image is also a substantial part of our information. Then, it's very significant to protect our image from unauthorized access. Accordingly, developing especial and consistent security in stock pilling and transmission of digital images is critical in several applications. Image encryption is to convert an image into another one that is hard to understand as in Figure (2.14), without knowing the key for decryption.

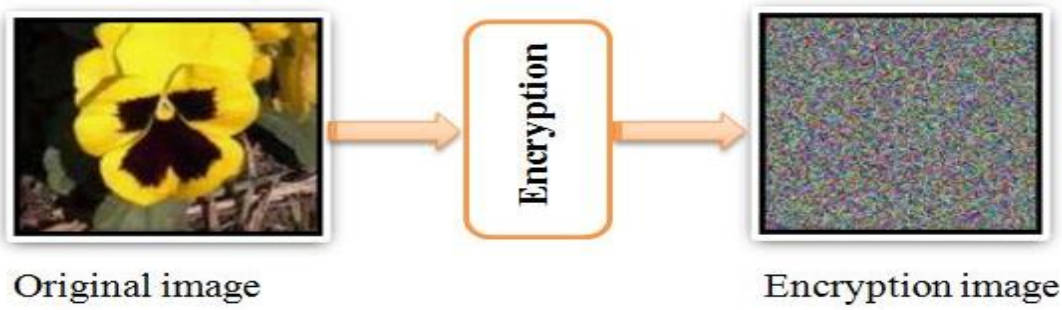



**Figure (2.14):** Image Encryption examples.

Digital imaging has an essential role in various applications such as biomedical, video conference and remote sensing. The interest in the methods of digital image processing comes from these primary applications that deal with the enhancement of pictorial information for human interpretation and storage and transmission of image data. Accordingly, two significant issues are needed to be addressed in image transmition, which are image compression and encryption.

### 2.4.1 Image Encryption is Different from Text Encryption.

Because the image size is much greater than that of text, algorithms of text encryption are not immediately inserted to images [24]. Consequently, the conventional cryptosystems require longer timeing to encrypt the image information. The other issue is that the decrypted texts have to be similar to the original text, while this demand is not basic for image data. Because of the characteristically of humane ideation, a decrypted image comprise small deformity is generally acceptable.

### 2.4.2 What is Image Encryption

Image Encryption refers to the process of converting an image into un readable form. This can be carried out through switch the image pixels in terms of its place and value) in order to secure the information. Many techniques can be used in image encryption, which may involve key charting or hiding or fusibility of image. In general, the image is varied at the pixel level (i.e., value of the pixels or its attitude in authentic array) [25]:

- **Place:** This includes the different steps used in image encryption based on changing the image places only. This operation may involve some approaches such as chaotic mapping, scrambling, and inversion. These processes can be following by group of keys, which can identify the request of the algorithms that could be follow for encryption. Because a pixel residue in the image herself, it may be susceptible to be attacked. However, using variable key length can improve the image

security. The correlation between the pixels in the original image and the encrypted image is reduced.

- **Value**: This process includes the image encryption based on changing the image pixel values only. These methods may include: multiplexing, bit plane mixing, and compressing. The correlation between both of the original images and the encrypted image is much reduced in this process.

### 2.4.3 Why there is a Need for New Image Encryption Methods

There is a critical need for new image Encryption methods for the following reasons [25]:

- The fat development in the internet and information technology resulted in more and more images transmition. Accordingly, protecting these images has increasingly become a critical issue. As a result, encryption becomes an important tool in protecting and securing important information from attack.
- Either the (DES or AES) technique require big number of computational cost and display poor analyses due to main image characteristics such as large data capacity and high correlations among pixels. Therefore there is a need for developing more advanced algorithms.

## 2.5 Digital Image Concepts

### 2.5.1. Digital image

Digital Image is a matrix, or an array, of square pixels (image elements) coordinated in (rows and columns). A massive two dimensional matrix of picture elements called pixels. The pixel is the smallest unit of an image. In a digital image, each pixel represents a different level of color intensity. Image resolution reference to the numbers of pixels available in a digital image (higher resolution alway yield better quality).

Thre are three main types of images (binary, grayscale, and True color (RGB) images) [26,27]. These image formats are explained below and represented in Figure (2.15):

1. **Binary image:** In binary images, all pixels is stored as a single bit (1 or 0), therefore it is called as a binary image or a 1 bit monochrome image, where it has no colour.
2. **Grayscale image:** In grayscale image (8 bit), all pixels have a value, which ranges between (0 and 255). Lower values (zero or closer) look darker in color and higher values (255 and closer) look brighter in color.
3. **RGB color image:** This is the most common data type for graphics and image format, where all pixel is exemplify by using (24 or 32) bits. In color images, each pixel is displayed by using 3 bytes (Read, Greed and Blue colors). This format supports 256 x 256 x 256 possible color combinations (a total of 16,777,216 possibe colors).


**Figure (2.15):** The Main three Types of images [27].

A digital image can be described depending on the number of bits used for pixel representation as follow**:**

**Table (2.3):** The colored area of the image corresponds to the depth a little bit.

| NO. | Image properties | Bits resolution | Color space |
|---|---|---|---|
| **1** | Binary image (black and white) | 1 | 2 colors |
| **2** | Gray scale (monochrome) | 8 | 256 gray levels |
| **3** | Colored image | 8 | 256 colors |
| **4** | Colored image | 16 | 65536 colors |
| **5** | True color (RGB) | 24 | 16,777,216 colors |

### 2.5.2. The Characteristics of the Human Eye:

Two types of cells are found in humans's eye: elongated (rods) and cone like (cones). The number of or rods is about 125 millions, whereas the number of cones is about 5 millions. The rods only reveal the amounts of the light, whereas the etcher reveals the colours. In general, an eye does not have an evenly sensitivity to three essential colours (Red, Green, and Blue). The comparative rate of these allergy is as follow: (red = 30%), (green = 59%), (blue= 11%).

A typical eye has the ablility to recognize approximate amid (40 and 80) shadow of gray, where as it ability recognize amidst (15 and 80) million colours. Both of the cones and rods detect the light entering the eye. The image formed in the brain is obtained as the total of images in three essential colours. Monitors, tv sets, video projectors follow a similar mode as that of the human's eye (three colors model) [28].

### 2.5.3. Color Models

A greyscale image is what people normally call it panchromatic or a (black and white) image. Figure (2.16) illustrates a normal greyscale image with 8 bit colour depth (256 greyscales). On the other hand a true color image with 24 bit colour depth has (8x8x8 bits = 256x256x256 colours = ~16 million colours). Some greyscale images may have more gray scales (e.g., 16 bit = 65536 grey scales). In general, three greyscale images can be common together to form an image to (281,474,976,710,656) grey scales [28].

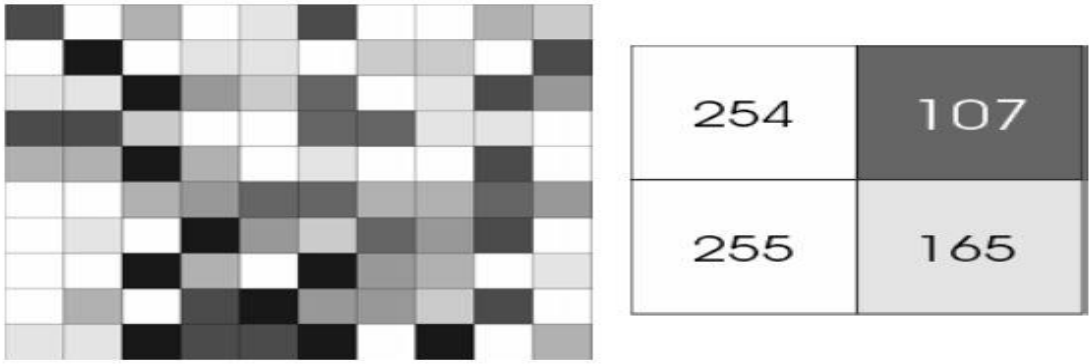



**Figure (2.16):** A 8 bit grayscale image **(**pixel value ranges between 0 (black) and 255 (white)) [29].

The RGB can be represented by the color cube as illustrated in Figure (2.17). The grayscale is represented by the line R = G = B. The RGB model is based on the human sensitivity of colors. This is used for displaying images in monitors, TV sets and other color systems.

The size of an RGB digital image is invariant and depends on the number of bits use for quantization. An 8 bit image for instance has pixel values between (0 and 255), where in the value 0 (coordinate = 0) in the RGB model, means the obscurity of colour, whereas the value (255 coordinate = 1) represents. The colour with extreme density accordingly, the values (0, 0, 0) represent a black color and the values (1, 1, 1) represent a white color.

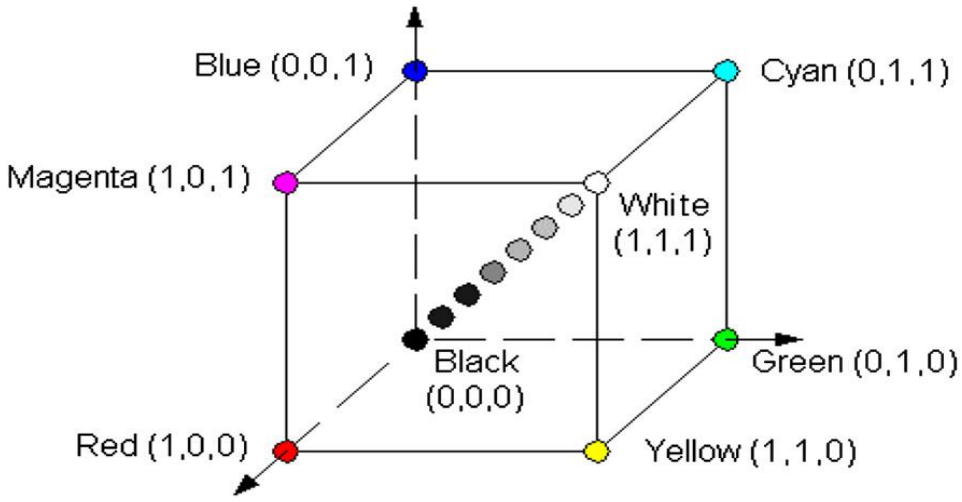



**Figure (2.17):** Color cube used for representing ture color images (RGB) [28].

By merging two of the three main colours (RGB), we obtain the colours use in the CMY colour pattern. Merging both the G and B colors gives the cyan, merging the R and gives maganta, and merging R+G gives the yellow color. The white color is the sum of all three colors as illustrated in Figure (2.18) [29]:

- C (cyan) = G + B.
- M (magenta) = R + B.
- Y(yellow) = R + G.
- W (white) = R + G + B.

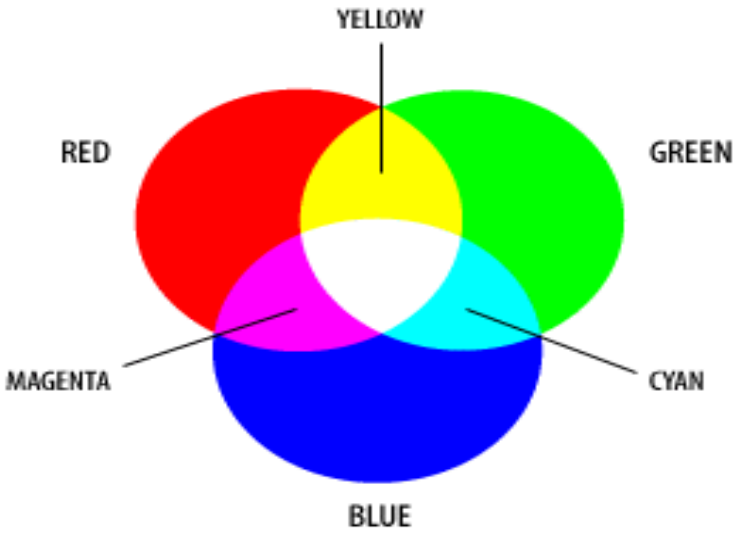



**Figure (2.18):** Merging the three primary colors in the RGB color model to obtain the colors used in the CMY color model [29].

## 2.6. The Major Images Encryption Techniques:

The images encryption techniques can be classified into (3) principle categories as follow [30]:

1. **The Position permutation:** in this algorithm the command of the pixels of a image is a change so that the datum becomes hidden .
2. **The Value transformation:** in this algorithm the biases and weights of the web are assigned accordingly to a binary series, which is produced from a messy system. This system is used for the encryption and/or decryption of each signal element.
3. **Visual transformation:** this algorithm gets benefit from the fact that the extreme substantial visible advantage of the image are position in the low frequencies, whereas the details are palsed in the higher frequencies. Generally, the human visual system (HVS) is very sensitively to lower frequencies than the higher ones .

### 2.6.1. Encryption Techniques: Background and Related Work:

Panduranga and naveens (2010) [31] proposed a hybrid technique for image Encryption. This technique utilizes the concept of carner-image and SCAN patterns generated by SCAN methods. Even though it includes existing method like SCAN methodology, the SCAN is a formal language based 2D spatial accessing methodology. It can efficiently specify and generate a wide range of scanning paths or space filling curves. The innovation of their work is represented in hybridizing and carrier-image creation for encryption.

This recently generated carrier-image is added with original image to get the encrypted image. The scanning method is applied to either original image or carrier image. This is after the addition of original image and carrier image to obtain a highly distorted encrypted image. The diagram of the technique is illustrated in Figure (2.19). On the other hand, applying the reverse process produces the original decrypted image.

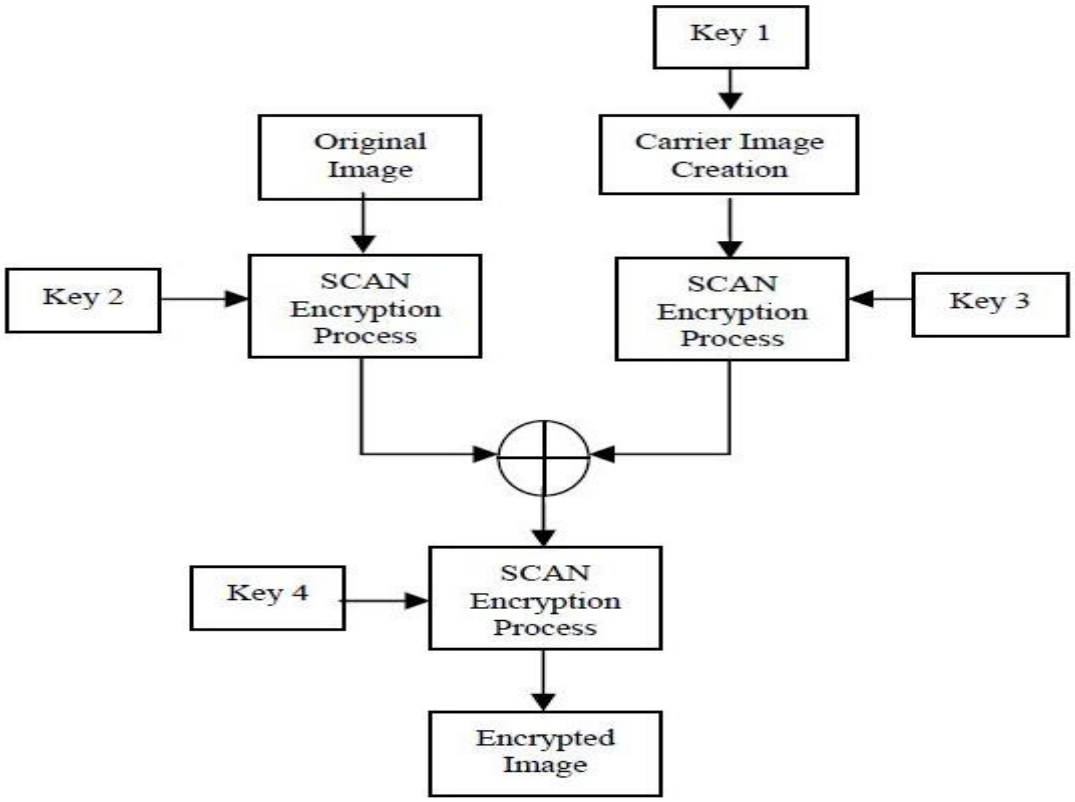



**Figure (2.19):** Diagram of the proposed image encryption approach using SCAN [31].

Abuhaiba et al. (2011) [32] provided a new effective method for image encryption which employs magnitude and phase manipulation using Differential Evolution (DE) approach. The main idea of that approach is to firstly carry out the 2D keyed discrete Fourier transform on the original image. This results in the first level of image encryption by the use of the secret key. Secondly, cros sover operation is performed on two components of the encrypted image, which are selected based on Line ar Feedback Shift Register (LFSR) index generator. Consequently they made more shuffling to the positions of image pixels leading to fully distorted encrypted image. A flowchat of the proposed cryptosystem is illustrated in Figure (2.20). The advantage of this technique is that it reduces the complexity and increases the reliability of the corresponding optical color image encryption systems

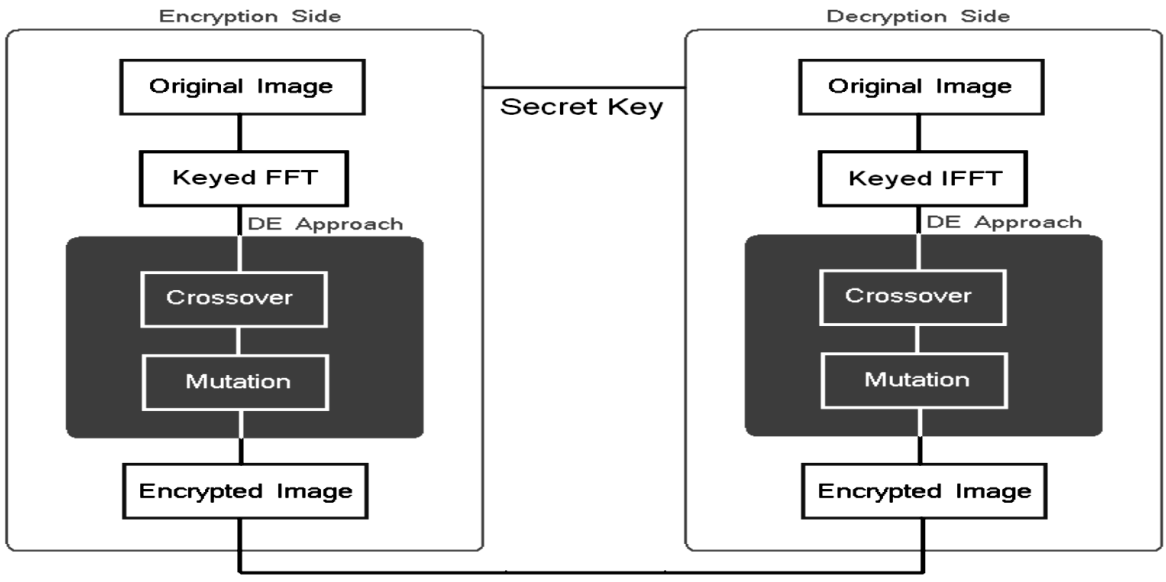



**Figure (2.20):** A flowchart of the differential evolution technique [32].

Bashir et al. (2012) [33] proposed an image encryption technique based on the integration of shifted image blocks and basic Advanced Encryption Standard (AES). The shifted algorithm technique is used to divide the image into blocks. Each block consists of number o f pixels, and these blocks are shuffled by using a shift technique that moves the rows and columns o f the original image in such a way to produce a shifted image. This shifted image is then used as an input image to the AES algorithm to encrypt the pixels of the shifted image. In order to evaluate its performance, the proposed integration technique and AES algorithm were measured through a series of tests. These tests included a correlation analysis, histogram analysis, information entropy, and differential analysis. A model of the technique is shown in Figure (2.21). The obtained results showed that the newly integrated technique had acceptable security and was more proficient than using the AES algorithm alone without the shifting algorithm. This makes it a good technique for the encryption of multimedia data. The results showed the advantage that the histogram of an encrypted image produces a uniform distribution, which is very different from the histogram of the plain image. Moreover, the correlation among image pixels was significantly decreased by using the integration technique and higher entropy was achieved.

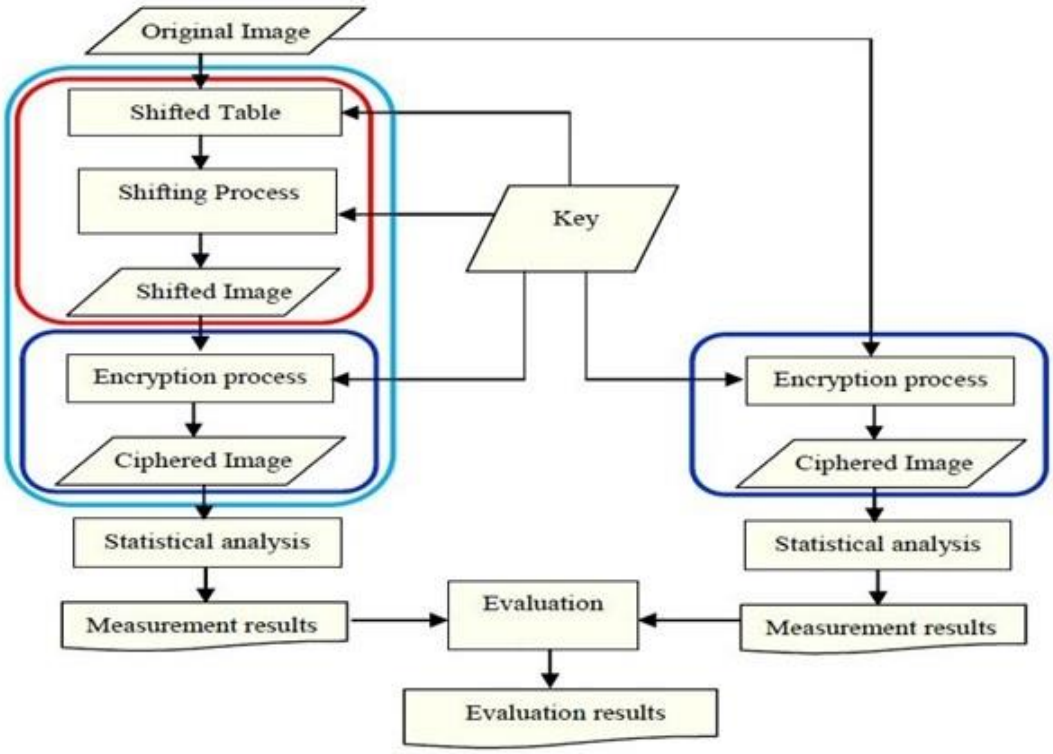



**Figure (2.21):** The Bashir et al proposed technique [33].

Kumara (2013) [34] developed a new approach of image steganography to provide more security to data and data hiding method. That approach employs a hash function to produce a pattern for hiding data bits into LSB of RGB pixel values of the cover image. The approach ensures that the message was encrypted before hiding it into a cover image. Therefore, if the cipher text got revealed from the cover image, the intermediate person other than receiver can't access the message because it is in an encrypted form. Both of the RSA was used with Hash-LSB in order that the original text will be embedded into cover image in the form of cipher-text technique as shown in Figure (2.22).

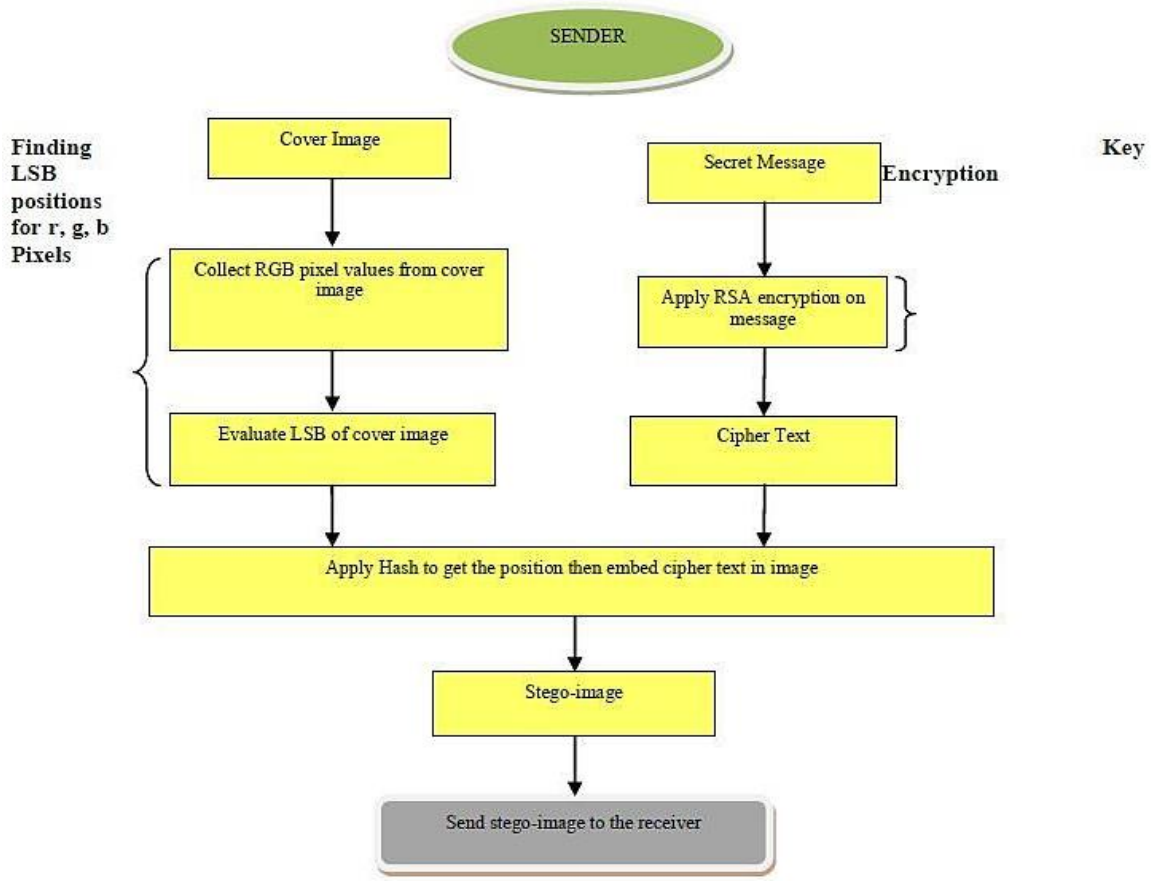



**Figure (2.22):** Flowchart of embedding secret-data in the cover image [34].

Malini et al. (2014) [35] they made a combination of both cryptography and steganography to secure the data during their transmition in the network. The first method was used to encrypt the data whereas the second method was used to embed the encrypted data into grayscale image. The data is encrypted using AES technique and a key is used for encryption and decryption technique is shown in Figure (2.23). After the encryption, the encrypted data is embedded into image. The technique Discrete Wavelet Transform (DWT) is used to store

the secret data in the least important coefficients of each 4X4 Haar transformed blocks. The proposed method possed with very good visual quality of the stego-image and also the algorithm allow variety in implementation to acquire desired robustness and fault tolerance.

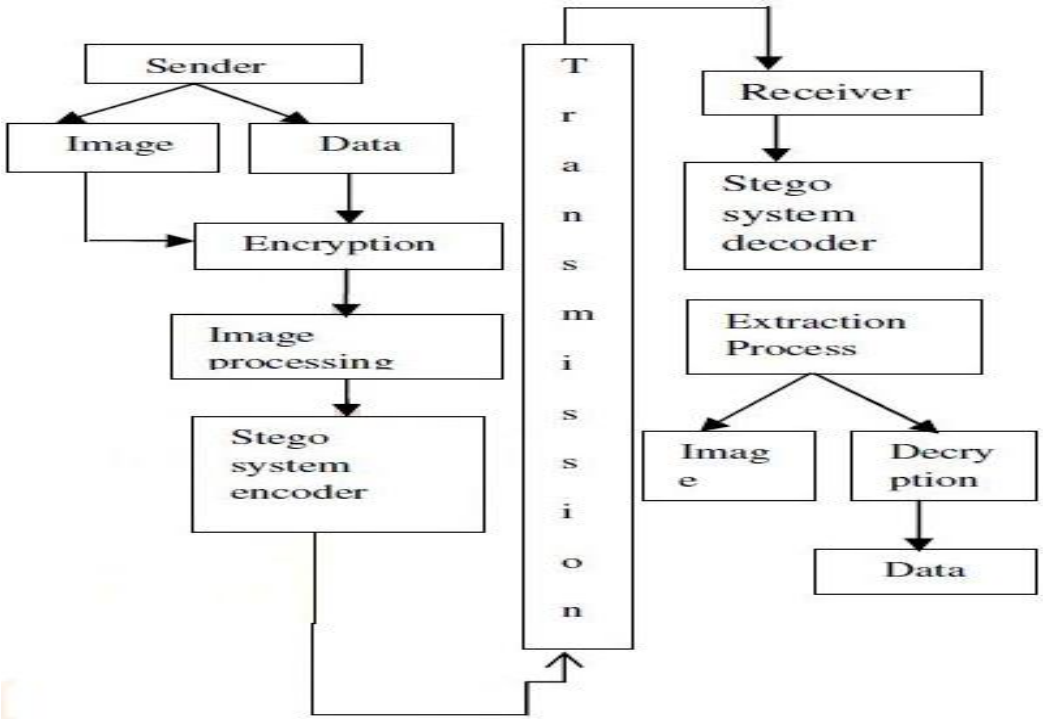



**Figure (2.23):** The method of decryption using the AES algorithm [35].

Zawa (2015) [36] this algorithm provides transformation based on the block on the basis of a combination of image transformation and well-known (encryption and decryption) and this algorithm called Blowfish. In that technique the idea of working is to divide the original image to the group of blocks, where these blocks are arranged in the form of turns using a

transformation algorithm as illustrated in Figure (2.24). After that the the transforms image is encryption using the Blowfish algorithm. Here it was found that the relationship between the elements of the picture and have fallen significantly. It was also found that the correlation decreased and the entropy increased by increasing the number of blocks through using smaller block sizes.

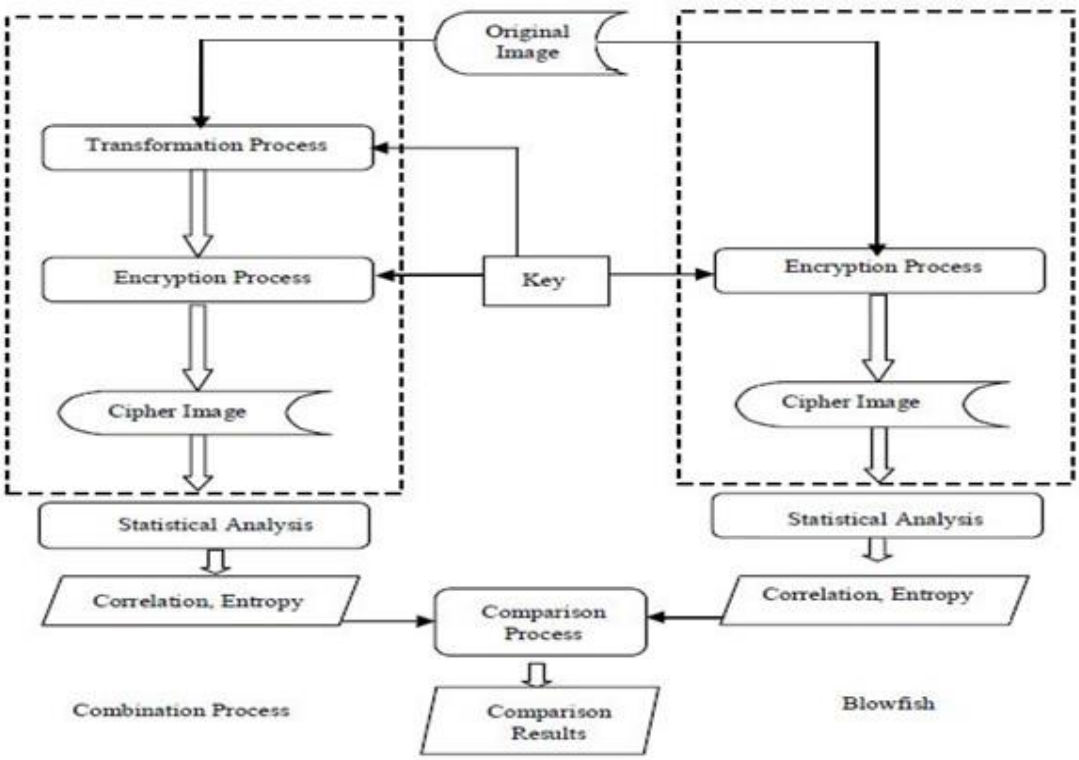



**Figure (2.24):** Block diagram of performance comparison process [36].

Anwar et al.,(2015) [37] developed a technique to secure any type of images especially medical images. They aimed to maintain the integrity of electronic medical information, ensuring availability to that information,

authentication of that information to ensure that authorize people only can access the information. First, the DWT was applied to decompose the image into 4 parts LL, LH, HL and HH as illustrated in Figure (2.25). The AES encryption technique was applied on the first part. The ear print was also embedding in this work, where seven values were extracted as feature vector from the ear image. The proposed techniqued improved the security of medical images through sending them via internet and secured these images from being accessed via any unauthorized person.

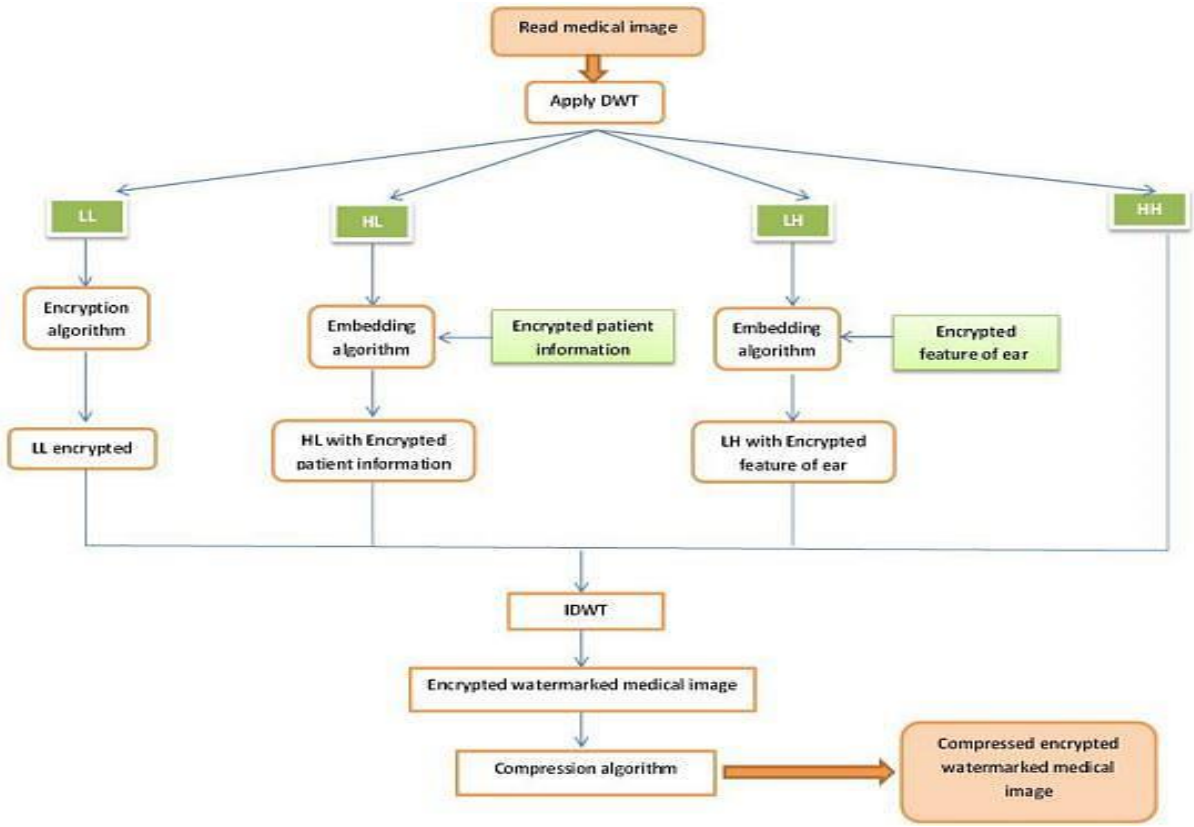



**Figure (2.25):** Model to get compressed encrypted watermarked medical [37].

**Table (2.4)** representas a comparison between the previously developed encryption techniques and the advantages and the disadvantages of each technique.

**Table (2.4):** Image Encryption Techniques: a critical comparison [38].

| No. | Techniquc | Advantages | Disadvantages |
|---|---|---|---|
| **1** | A novel image encryption Algorithm based on hash Function, **2010.** | Because of encryption done in two phases chances of mistakes is low. | Encryption done in two phases so will be increased |
| **2** | A digital image encryption Algorithm based composition of two chaotic logistic maps، **2010**. | Better than all above because of two logistics maps, Uses external sacred keys and Strong security. | Lot of confusion in process. |
| **3** | New modified version of Advance encryption standard based algorithm for image encryption, **2010.** | Higher security. | The algorithm and the secret key, consequently a same data will be ciphered to the same value; which is the main security weakness. |
| **4** | Image encryption using affine transform and XOR Operation, **2011.** | Better Solution and Correlation between pixels values significantly decreases. | Lengthy, complicated and chances of mistakes is high. |
| **5** | Permutation based image Encryption technique, **2011.** | Three phases, casy to be processed. | High chances of error in key Generation. |
| **6** | Permutation Based Image Encryption Technique, **2011**. | Three phases, easy to be processed. | High chances of error in key Generation. |
| **7** | The integration of a shifting technique and the aes algorithm march **2012**. | Improved and effective method. | Possibility of mistakes while preparing shifting table, it is lengthy and difficult process. |
| **8** | Design and analysis of a Novel digital image encryption scheme march **2012**. | Simple, fast and secured against Any attack. | Large, complicated and very Difficult performance and Security analysis. |
| **9** | Secret key encryption Algorithm using genetic Algorithm april **2012.** | Encryption method satisfies the Goal of encrypting the images. | Complicated and algorithm is Too lengthy |
| **10** | New advance image Encryption to enhance Security of multimedia Concept july **2012**. | Best performance, the lowest Correlation and the highest Entropy. | Three phase process and every Image is very complicated. |

### 2.6.2. Measurement and Evaluation of Encryption Quality:

There are many common evaluation parameters to evaluate the efficiency of encryption techniques. Some of these measurements are [39]:

- **Visual Degradation:** defined as working to measure the perceptual distortion of the image data and based on the clear image.
- **Cryptographic Security:** defined as working the encryption system is safe against various Attack (plain text, cipher text).
- **Speed:** defined as working to carry out the (encryption and decryption) algorithms as fast as possible to be more Process.
- **Encryption Ratio:** defined as working to measure the amount of data to be encrypted. This works to increase the computational complexity, but the reduction of the proportion of encryption.

Image encryption quality measures are figures of merit used for the Evaluation Of image encryption techniques. These measures are classified into three Categories [40]; Methods based on the pixel value; position changing, methods based on the pixel's value changing and methods based on both pixel's value and position changing.

## 2.7. Summary

Digital Images paly an important role in our world today. Accordingly, securing the transformation of these images through the network is very critical. As result, several techniques have been developed over last years, which can be used in securing images. This chapter provided a survey over the different image encryption techniques from different research papers. It started with general guidelines about security and cryptography, and then it moved forward toward the challenges and security requirements in image encryption. The techniques described in this chapter can be examined for robustness and efficiency in the evaluation subsection.

This chapter provided a conclusion that all of the image encryption techniques are good and each one has its own advantages and disadvantages. These techniques can also give better security at their scale so that no unauthorized access can be done to images. Each technique has its own suitability and its own limitations; therefore there is a still lot of work to do in this field.

In the next chapter, the will review overview of background and previous work in steganography.

# CHAPTER 3

## Background and Previous Work in Steganography

Information hiding techniques (steganography and watermarking) have recently received quite a bit of attention. At least one reason for this is the desire to protect copyrights of digital (audio, image and video). Other applications include intelligence communication, covert criminal communication, and the protection of various types of communication against illegal spy. Along with new and improved techniques for hiding information, techniques for detecting and (possibly removing) such information will appear in the scene. Hiding data refers to the process of secretly inserting information within a data source without changing its quality. It is the science and art of writing hidden messages in a way that either the sender or expected recipient doesn't realize that the message is hidden. In data hiding process the actual information is not kept in its original format but it is transformed into another equivalent multimedia file such as images, videos or audios. **This chapter includes the follows topics:**

**1 –** Overview of Steganography.

**2 –** Steganography main concepts.

**3 –** Types of domain in Image Steganography Techniques.

**4 –** Steganography Techniques: Background and Related Work.

**5 –** Steganalysis.

**6 –** Summary.

## 3.1. Overview of Steganography:

### 3.1.1. Steganography Defined:

Steganography is the science and art of hiding information within a carrier, where no one, except the intended recipient, has knowledge of the existence of hidden information. The word originates from the ancient Greek words "steganos" (covered) and "graphic" (writing), literally meaning "covered writing" .a process of secret communication where a piece of information (a secret message) is hidden into another piece of innocent looking information, popularly called a cover, in such a way that the existence of the secret information remains concealed without raising any suspicion in the minds of the viewer's [41].

### 3.1.2. The Element S of Steganography:

Two pieces of data are required in steganography, which are the cover and the data to be hidden [42]:

**1. The Cover**

The cover refers to the medium into which the data we will be embedded. The effectiveness of the steganography technique is dependent up on selecting the most appropriate cover. The cover also works as a container for the given message. Steganography is based on hiding the data behind the cover to protect it from being known as secure, dislike encryption. Therefore the embedded data can be retrieved once the embedding is suspected. Image, video, audio and other file formats can be used to embed secret messages.

## 2. The Data

The data that are required to be hidden should be serializable in order to be embedded bit by bit in the cover. The size of data shouldn't exceed the cover size in order to contain all the data. In case of images, both the cover and the data may have the same number of pixels; however the cover will have more color information for each pixel than the hidden data. Figure (3.1) shows the fundamental approach of steganography process [43].

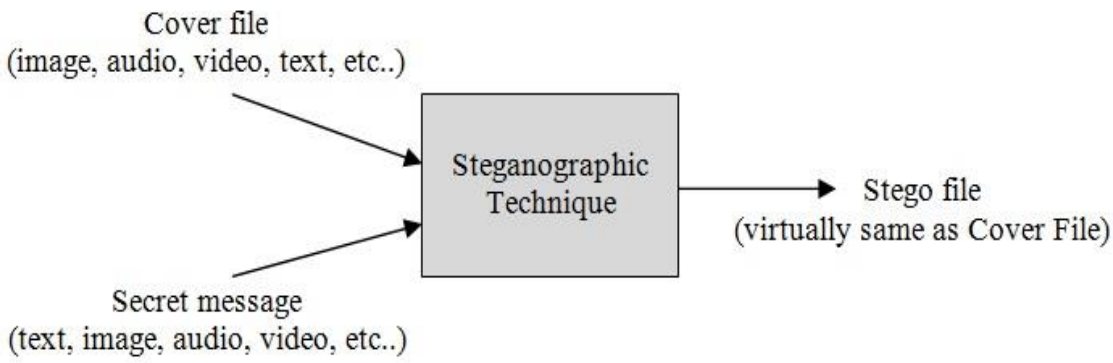



**Figure (3.1)**: Fundamental approach of steganography process [43].

Generally, any steganography system consists of two phases encoding or embedding phase and decoding or extracting phase. A stego key is used to encode or embed the secret message into a covert innocent message as illustrated in Figure (3.2), which shows a general steganography Model [43].
The secret key steganography can be defined as the quintuple (**C, M, K, DK, and EK**) where:

- **C**: the set of possible covers.
- **M**: the set of secret message.
- **K**: the set of secret keys.
- **Ek** : C ×M×K→C

With the property that **DK (EK(c, m, k), k) = m** for all **m Є M, c Є C** and k **Є K.** The items above are described in the following [43]:

- **Emb (m):** refers to data or signal to be hidden in another media.
- **Stego (s):** refers to the object which is carrying a hidden message.
- **Cover (c):** The input to the information hiding process which represents the innocent carrier signal or file.
- **Stego key (k):** This is additional unimpeded secret data which may be required in the information hiding process. This key is required to retrieve the embedded message in its final target.

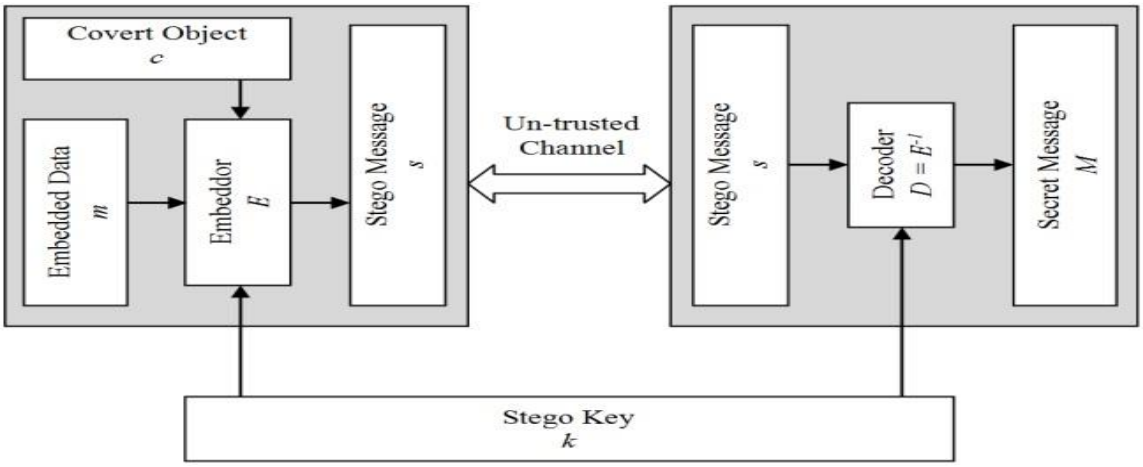



**Figure (3.2):** Fundamental approach of Steganography terminology [43].

Figure (3.3) shows the main functions of steganography. The secret information is hidden in an image (known as cover image) with the stego key by the sender. This image is transmitted over a communication channel. The stego key is used to extract the hidden secret information at the other end. The medium used in this case is a digital JPEG image, however other formats such as audio, and video can be used. A possible formula of the process may be represented as [44]:

***Cover (image, audio, video) + embedded message + stego key = stego- message***

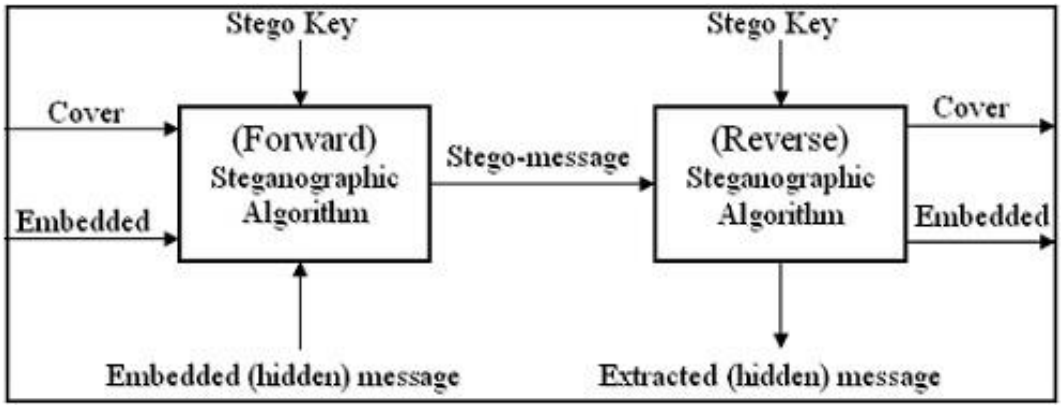



**Figure (3.3):** General Steganography System [44].

Some terminology has been used such as 'cover', 'embedded', and 'stego'. The term "cover" refers to description of an original, innocent massage, data, audio, video, and so on. The sender of a message has to embed hidden information in a cover, called stego. Steganography is an alternative tool for privacy and security [45].

### 3.1.3. Cover Generation Steganography Techniques:

There are two general ways in which you can categorize steganography techniques by: 1- Type of host file, and by 2-How the data has been hidden [46]:

**1. File Type**

File type categorization breaks down steganography based on the type of host or overt file in which the data is hidden. Different file formats have different properties that control how the data can be hidden in the file. For example, most techniques for hiding data in .bmp images place the information in the least significant bits of each pixel. How you pick the bits to use varies somewhat, but most techniques work in a very similar manner. Because of this, knowing the host file type can give you an idea of where the data might be hidden**.**

**2. Method of Hiding**

Breaking down stego techniques based on hiding method is the preferred approach. When it is all said and done, there are only three ways to hide a digital message in a digital cover of new files. There are types of embedding techniques an essentially **three** ways to hide data:

- **Injection***:* finds areas in a file that will be ignored and puts your cover message in those areas. For example, most files contain an **EOF** or (***end-of-file***) marker. When playing an audio file, the application that is playing the file will stop playing when it reaches the EOF because it thinks it is the end of the file. You can inject data after the EOF marker that does not have an effect on the sound of the file.

- **Substitution***:* finds insignificant information in the host file and replaces it with your covert data. For example, with sound files each unit of sound you hear is composed of several bytes. If you modify the LSB technique it will slightly modify the sound, but so slightly that the human ear cannot tell the difference.
- **Generation***:* creates a new overt file based on the information that is contained in the covert message. For example, one generation technique will take your covert file and produce a picture that resembles a modern painting. This is done by substituting a patch of green for every 0 and substituting a patch of yellow for everyone. The picture is created solely based on the bit sequence of the covert file.

There are several approaches in classifying steganography systems. One could categorize them according to the type of covers used for secret communication or according to the cover modifications applied in the embedding process. From the second approach, the steganography methods are grouped in five categories, although in some cases an exact classification is not possible. See Figure (3.4).

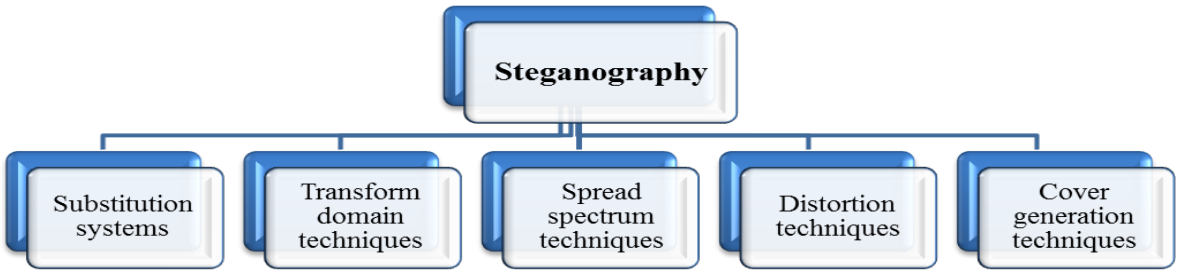



**Figure (3.4):** classification of steganography methods [46].

The most suitable cover media for Steganography is image on which numerous methods have been designed. The main reason is the large redundant space and the possibility of hiding information in the image without attracting attention to human visual system (HVS).

There have been many techniques for hiding information or messages in images in such a manner that the alterations made to the image are perceptually indiscernible. Common approaches are included in this respect, a number of techniques have been developed [47], using features like [48]:

- **Substitution**: The method of substitution generally does not increase the size of the file. Depending on the size of the hidden image, it can eventually cause a noticeable change from the unmodified version of the image Least Significant Bit (LSB) insertion technique is an approach for embedding information in a cover image. In this case, every least significant bit of some or all of the bytes inside an image is changed to a bit of the sink image. When using a 24-bit image, one bit of each of the primary color components can be used for the above purpose.
- **Masking and Filtering**: The masking and filtering techniques starts with the analysis of the image. Next, we find the significant areas, where the hidden message will be more integrated to cover the image and lastly we embed the data in that particular area. In addition to the above two techniques for message hiding.

- **Transform Technique**: transform a technique has also been employed in embedding the message by modulating coefficients in a transform domain. As an example, we may mention here that Discrete Cosine Transform works by using quantization on the least important parts of the image in respect to the human visual capabilities.

### 3.1.4. The Uses of Steganography:

Steganography is applicable to, but not limited to the area differs in what feature of the steganography is utilized in each system. Though steganography's most obvious goal is to hide data, however there are several other related goals used to judge a method's steganography strength as follow [49]:

**1.** It can be used as a solution to make it possible to send information without the fear of the messages being intercepted and traced back to us.

**2.** It also can be used to store information on a certain location.

**3.** Watermarking can also be implemented in data; however it is not necessarily steganography.

**4.** Steganography is critically used in e-commerce, where the majority of users are protected by a username and password with no real method of verifying if the user is the actual card holder.

**5.** Steganography can be integrated with current communication methods to be used in carrying out hidden exchanges.

**6.** Steganography help in transporting sensitive data to pass eavesdroppers without knowing that any sensitive data has passed them.

### 3.1.5. Steganography and Cryptography:

Fundamentally, the main purpose of Cryptography and Steganography is to provide secret communication, however Steganography is quiet different than cryptography. Cryptography is used to hide the contents of a secret message from a malicious people, whereas Steganography hide the existence of the message. Steganography does not change the structure of the secret message, but it hides the message inside a cover message therefore it cannot be seen. Steganography prevents an unintended recipient from suspecting that the data exists. Moreover, the security of traditional Steganography system depends on secrecy of the data encoding system. The Steganography system is directly defeated once the encoding system is known [50].

### 3.1.6. Steganography and Watermarking:

The main objective of steganography is to embed messages inside other cover objects, whereas watermarking aims to protect the owner rights of digital media. Therefore, even if the watermarked file is copied or minor changes were made to the owner can still prove it is his file. Accordingly, both steganography and watermarking are two forms of data hiding and therefore they have some common characteristics [51].

Steganography, watermarking and cryptography are three interlinked techniques [11, 12]. The first two are quite difficult, especially for those who are coming from different disciplines. Figures (3.5-3.6) illustrates the different disciplines of information hiding and the relationships between them.

Tables (3.1) show a comparison between the three data hiding techniques (steganography, watermarking and encryption).

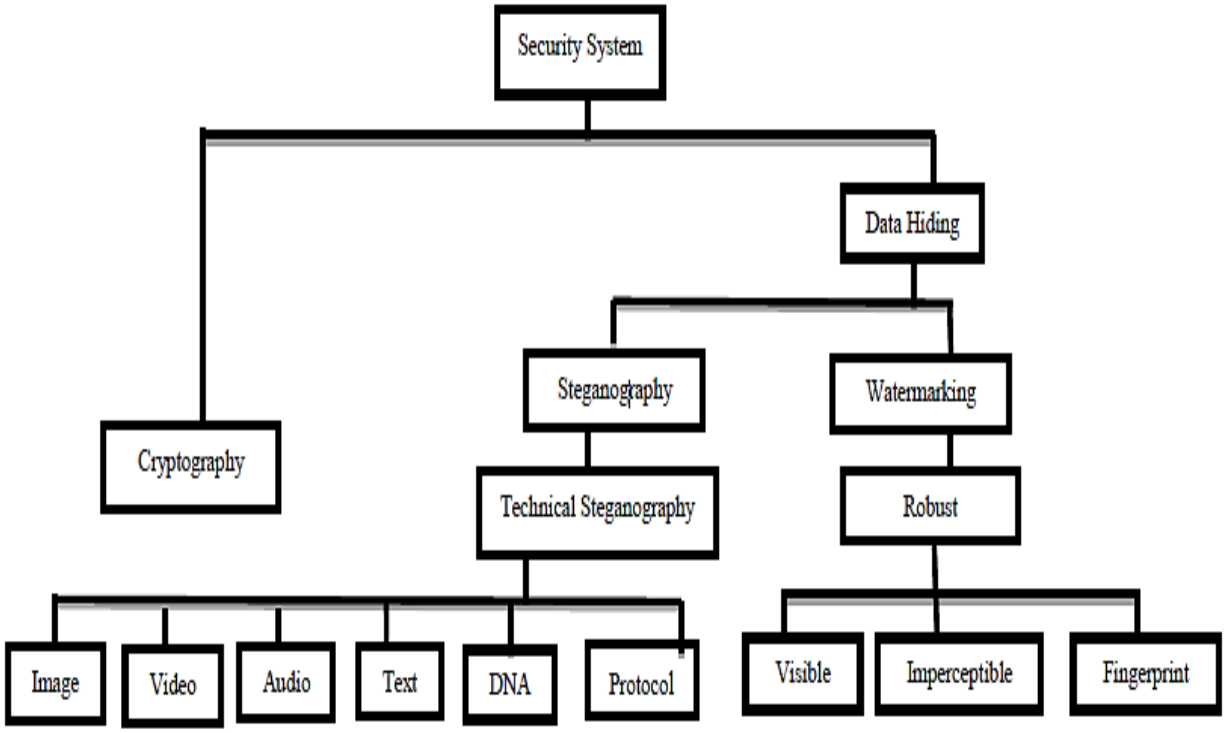



**Figure (3.5):** The different disciplines of information hiding [51].

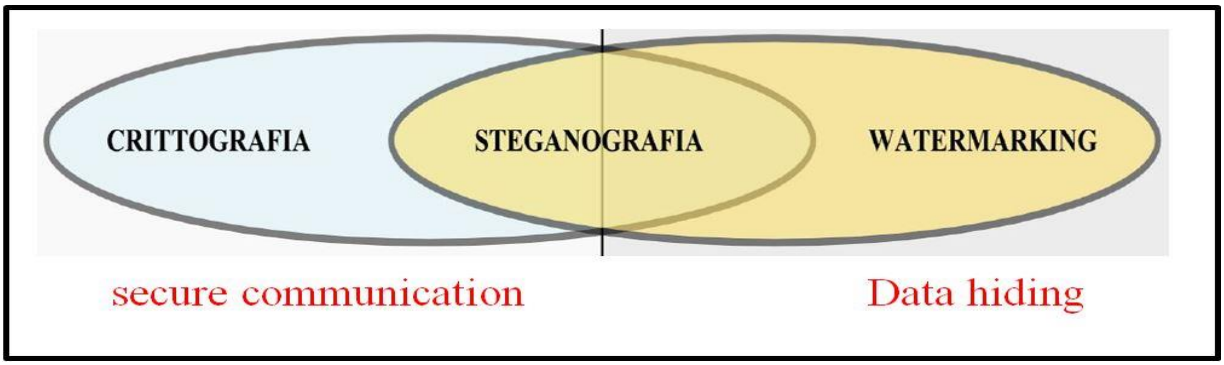



**Figure (3.6):** Relationship of cryptography, steganography and watermarking [52].

**Table (3.1)**: Comparison of (steganography, watermarking and encryption).

| Method / Criterion | Steganography | Watermarking | Encryption |
|---|---|---|---|
| **Carrier** | Any digital media (Text ,Image, Audio ,Video) Files | Mostly ( Image , Audio) files | Usually text based, with some extensions to image files |
| **Secret data** | Hidden | Watermark | Cipher text |
| **Key** | Optional | | Necessary |
| **Input files** | At least two | | One |
| **Authentication** | Full retrieval of data | Usually achieved by cross correlation | Full retrieval of data |
| **Objective** | Secrete communication | Copyright preserving | Data protection |
| **Result** | Stego-file | Watermarked-file | Cipher-text |
| **Concern** | Detectability / capacity | Robustness | Robustness |
| **Type of attacks** | Steganalysis | Image processing | Cryptanalysis |
| **Fails when** | It is detected | It is removed / replaced | De-ciphered |
| **Visibility** | Never | Sometimes | Always |
| **Flexibility** | Free to choose any suitable cover | Cover choice is restricted | There is no cover |
| **Relation to cover** | Not necessarily related to the cover. The message is more important than the cover. | Usually becomes an attribute of the cover image. The cover is more important than the message. | There is no cover |
| **History** | Very ancient except its digital version. | Modern | Modern |

## 3.2. Steganography Main Concepts:

### 3.2.1. The Main Goal of a Steganography System

The main goal of a steganography system is to escape the detection and hide the presence of the secret message from any external follower and keep the confidentiality of embedded data. The steganography process can be summarized in Figure (3.7). For the cover media, the most common attractive media to be used are (image, audio and video) files. The embedding function embeds the secret message into the cover image. The new media object that comes from embedding our secret message into the cover is known as the stego. The extraction function does the inverse of the process done by the embedding function to get the secret message out of the stego. A typical steganography technique basically includes the following steps:

- Providing a file or a cover image to embed the secret information in it.
- Providing a stego in order to get the output file the stego media.
- Embedding the secret message file inside the cover-media.

The embedding Key is chosen in advance by the two parties communicating. This key is needed to both (embed and extract) the hidden information, and if the proper key is not used, it cannot be possible to extract the hidden data from a given cover object [53].

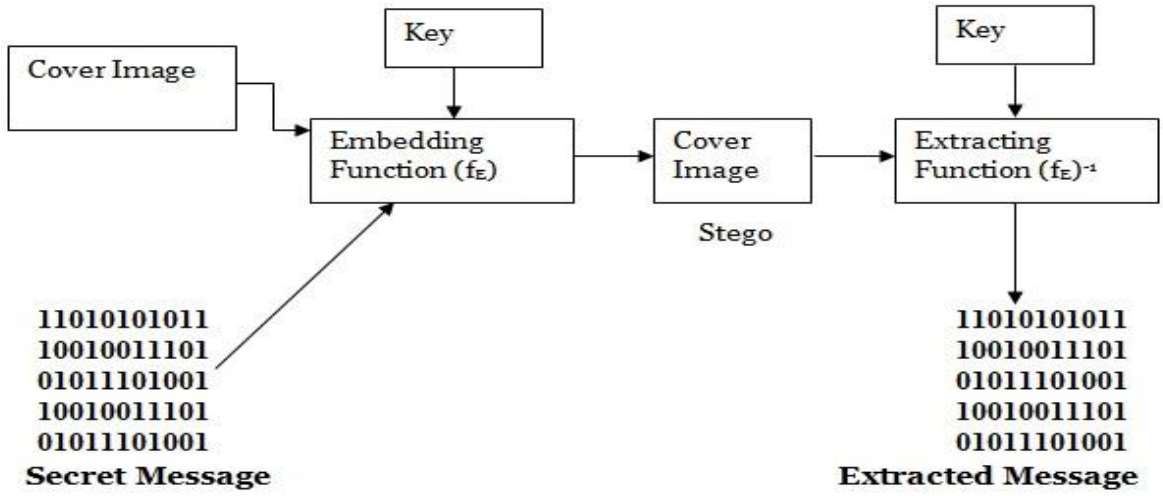



**Figure (3.7):** The steganography process [53].

### 3.2.2. The Basic Requirements of a Steganography System

The previously mentioned algorithms that are for image steganography vary in their advantages, disadvantages and efficiency. Therefore, it is very important to select the most suitable algorithm for an application. All steganography algorithms have to fulfill with some fundamental requirements. The most important requirements are as follows [54]:

- **Imperceptibility** (Invisibility)**:** The stego object and original cover object should be perceptually identical. This is because the strength of steganography lies in its ability to be unobserved by the human eye. The algorithm is compromised, once the image that hides the message has been seen by someone.
- **Load Capacity:** Stenographic capacity means the amount of bits that can be hidden in a cover object without causing statistically significant modifications. Steganography aims at hidden communication therefore it requires sufficient embedding capacity.

- **Robustness:** Statistical analysis is the practice of detecting hidden information through applying statistical tests on image data. As a result, the embedded-data should go on any processing operation and should protect its fidelity.
- **Independency of file format:** there are several types of image file formats that are commonly used on the Internet; therefore it will seem suspicious when only one type of file format is always used in communication between two entities. Consequently the steganography algorithms that have the ability to embed information in any type of file formats are the most powerful and applicable.
- **Security:** Security is in the key goal of any steganography system.

### 3.2.3. Classification of Steganography on The Basis of Digital Medium

Steganography embeds secret data into digital carriers like (text, image, audio, video etc.), such that it cannot be easily detected by the Human Visual System (HVS). There are five types of steganography on the basis of carrier object that is used for embedding the secret data**.** There are following classification of Steganography in Figure (3.8) [55]:

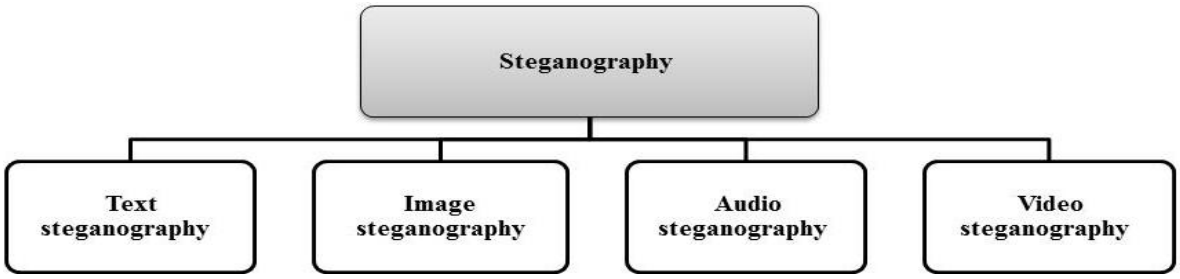



**Figure (3.8)**: Classification Steganography embeds secret data [55].

The following section will discuss the different steganography techniques which are commonly based on the type of the cover object:

**3.2.3.1. Text Based System or Text Steganography:** The procedure of hiding a text inside text can be accomplished by changing the text format or by changing certain properties in text elements such as letters. It is considered as one of the most difficult types of the steganography techniques, where the text files contain very small amount of redundant data in order to hide a secret message. Furthermore, one of the disadvantages is ability to easily changing the text based Steganography by an unwanted parties either by changing the text itself or its format. Adding white-space and tabs to the ends of lines in a document represents an effective type of Steganography. This is because they occur naturally in any document, therefore using them won't seem suspicious to someone [56].

**3.2.3.2. Image Based Steganography System or Image Steganography:** In this system pixel intensity is generally used for hiding the intonation. Image steganography is the most common form of steganography and most widely used in various fields for hiding text in image, audio in image, video in image. It is the most popular medium on internet due to its high frequency of usage. There are different forms for coding in image commonly used method are least significant bit insertion, in which hiding any type of data in only least significant two or three bits of a byte. The secret data bits are embedded in the cover image by modifying the rightmost bit of the pixel value. So, the image is slightly

modified but with no visible changes. Other way of hiding is using masking and filtering techniques. Some algorithms and transformation are also used for hiding image within image or other mediums [57].

**3.2.3.3. Audio Based Steganography System or Audio Steganography:** In this system, secret messages are embedded in digital sounds, where the secret message is embedded by slightly changing the binary sequence of an audio file. This process is more difficult than embedding messages in other media. A variety of methods for embedding information in digital audio have been introduced. Here a message is hidden in the mode of a simple change in the binary sequence of an audio file. The existing system can hide messages in form of many files like (AU, Wav, Mp3, etc.). Concealing the message using this process is relatively harder than hiding the message using other media such as a digital image. There are several techniques and methods that are used for the very purpose of hiding information in this method, these methods come in the range from simple to most difficult that simply hide information in a pattern of a noise in audio file but also there is sophisticated methods more accurate working on advanced signal processing for concealing information technologies [58].

**3.2.3.4. Video Based Steganography System or Video Steganography:** this system hides information in video files, therefore Steganography techniques that work with sounds and images are also applicable to video files. This system has the ability to hide large amounts of data can with less distortion. Also, the use

of video files as a carrier is more eligible when compared with the other approaches [59].

Information hiding systems are compared based on the following characteristics: capacity, security, integrity, robustness, transparency and temper resistance as represented in Table (3.2). Capacity indicates the amount of information that can be hidden in the cover medium. Security refers to the inability of an eavesdropper's to see hidden information. Robustness refers to the amount of modification that the steganography carrier can withstand before an adversary can destroy hidden information [60].

**Table (3.2):** Comparison between different steganography techniques.

| Technique / Features | Text-Steganography | Image-Steganography | Audio-Steganography | Video-Steganography |
|---|---|---|---|---|
| **Security** | **High** | **High** | Low | **High** |
| **Capacity** | Low | **High** | Low | **High** |
| **Transparency** | Low | Low | Low | **High** |
| **Integrity** | Low | **High** | Low | Low |
| **Temper resistance** | **High** | **High** | **High** | **High** |
| **Robustness** | Low | **High** | Low | Low |

### 3.3. Types of Domain in Image Steganography Techniques

Image steganography techniques can be classified into two types: image steganography in the image domain and in the transform domain. Image domain techniques are also referred as spatial domain technique. Messages in this technique are directly embedded in the intensity of the pixels. The comparison of the various techniques in terms of generic steganography parameters are given in Table (3.3 a-b) [61].

**Table (3.3-a)**: Performance Comparison (Spatial domain).

| No. | Technique | Domain | Capacity | Visibility | Detectability | Robustness | Complexity | Comment |
|---|---|---|---|---|---|---|---|---|
| **1** | LSB | **Spatial** | **H** | L | **H** | L | L | Independent of image format and texture |
| **2** | PVP | | M | L | M | L | L | Suitable for high contrast image |
| **3** | EBE | | L | L | M | L | L | Preferred for image with objects |
| **4** | RPE | | **H** | M | L | L | L | Provides better security of information leakage |
| **5** | PMM | | M | L | L | M | M | N / A |
| **6** | CONNECT | | M | L | L | M | M | Preferred for mosaic image |
| **7** | PL(GLV) | | M | L | L | L | L | Robust hiding for noisy image |

Spatial domain techniques are broadly classified into, Least significant bit **(LSB**), Pixel value differencing **(PVD),:** Edges based data imbedding (**EBE),** Random pixel embedding method **(RPE)**, Pixel Mapping Method **(PMM)** , Labeling or connectivity method **(CONNECT)**, and Gray level value based method **(GLV)**.

**Table (3.3-b):** Performance Comparison (Transform domain).

| No. | Technique | Domain | Capacity | Visibility | Detectability | Robustness | Complexity | Comment |
|---|---|---|---|---|---|---|---|---|
| **8** | DCT | **Transform** | M | L | L | M | M | Simplest in the transform domain |
| **9** | DFT | | M | L | L | M | M | Involves the complex calculations |
| **10** | DWT | | M | L | L | **H** | **H** | Closely matches with human visual perception |
| **11** | IWT | | M | L | L | **H** | **H** | Overcomes the rounding off losses |
| **12** | DCVT | | M | L | L | **H** | **H** | Improves the degradations at edge areas |

Transform domain techniques are broadly classified into,

Discrete Cosine transform technique **(DCT)**, Discrete Fourier transform technique **(DFT)**, Discrete Wavelet transform technique **(DWT)**, Integer Wavelet Transform techniques **(IWT)**, and Discrete Curvelet Transform techniques **(DCVT)**.

### 3.3.1. Spatial Domain Techniques:

Spatial Domain techniques embed secret data pixel directly into cover image. The most popular data hiding method is changing pixels right most digits or last two, known as Least Significant Bit (LSB). Lossless image formats like Image.bmp, image.png, and 8-bit grayscale image.gif are usable for LSB methods. The spatial domain steganography technique relates to the approaches in which data hiding is directly carried out on the pixel values of the cover image. This result in making the effect of the message on the cover image is not visible for the human's eye. Several techniques are used for carrying out this

process. They all utilize the direct pixel embedding; however the pixel selection criterion varies among them. The popular approaches that are commonly used in this domain are represented in Table (3.3) [62]. In this work, the Least Significant Bit (LSB) technique was used.

### 3.3.1.1. Least Significant Bit (LSB) Technique:

The least significant bit of some or all of the bytes inside an image is changed to a bit of the secret message. This technique modifies the last significant bit (right most bit) of the RGB values of the pixel data image based on it its binary coding. Replacing Least Significant Bit is simple. It exploits the fact that the level of precision in many image formats is far greater than that perceivable by normal human vision [63]. This method makes it difficult for the human eye to discern hidden data, therefore it is quite effective. Moreover, the modifications that are made could be attributed to the noise that may already exist in the image. Digital images are mainly of two types:

1. **8 bit images**: In 8 bit images, one bit of information can be hidden.
2. **24 bit images**: In 24 bit images, three bits of information can embedded in each pixel, one in each LSB position of the three eight bit values. Changing the LSB does not change the appearance of the image. Therefore the resultant stego image appears almost the same as the cover image.

Figure (3.9) shows the diagram of applying LSB algorithm on both the cover and hidden images

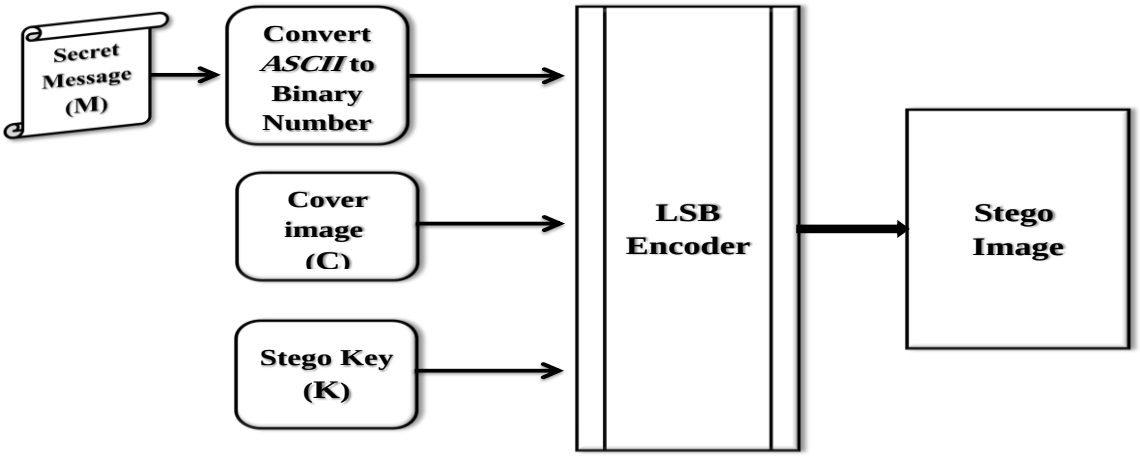



**Figure (3.9):** LSB insertion Mechanism [63].

In this work, we have use two techniques for detection, the first one is the detection with the color images, and the second is the statistical detections when the original images are available in the web secure database. The LSB Encoding Detection in Color Images is illustrated in Figure (3.10):

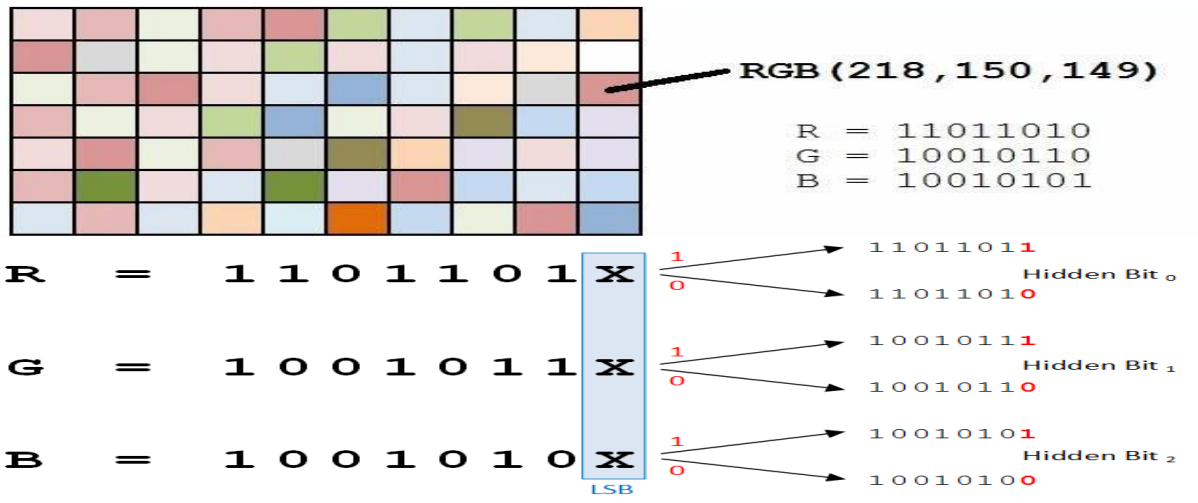



**Figure (3.10):** Two techniques used for detection based on the color images and statistical detections [64].

It could be noticed from the above image that the LSB of the pixel value in the cover image C(i,j) is equal to the message bit m of secret massage to be embedded, C(i,j) remains unchanged; if not, set the LSB of C(i, j) to m. the S(i,j) is the stego image. The procedures used in message embedding are described as follow [44]:

- S(i,j) = C(i,j) - 1**,** if LSB (C(i,j)) = 1 and m = 0 .
- S(i.j) = C(i,j), if LSB (C(i,j)) = m .
- S(i,j) = C(i,j) + 1**,** if LSB (C(i,j)) = 0 and m = 1 .

Where, LSB (C(i, j)) refers to the LSB of cover image C(i,j) and m is the next message bit to be embedded.

The following example, illustrates how the LSB modification was used in the proposed embedding technique. Suppose we would like to embed the message letter "**C**" in the LSBs of an image. The process is performed as follows [65]:

**Inputs:** Text file, cover image and secret key.

**Output:** Stego image.

1. Convert the message data from decimal to binary (C = 10000011)
2. Read the cover image pixels values.
3. Convert the cover image pixels values from decimal to binary.
4. Break the message to be hidden into single bits and take a number of bytes equal to it from the cover image.
5. Replace the LSB of cover data by one bit of the data to be hidden. So the Bit (1) is inserted into LSB of (11010010) to become (00010101). This step is repeated for all the bits of the Message to be embedded.

Consider an 8 bit gray scale bitmap image, where each pixel is stored as a byte representing a grayscale value. Suppose the first eight pixels of the original image have the following gray scale values:

**Before Hiding (grayscale images values):**

| 8-bitgrayscale bitmap image | Byte representing |
|---|---|
| **Bit 1** | 1101001**0** |
| **Bit 2** | 0100101**0** |
| **Bit 3** | 1001011**1** |
| **Bit 4** | 1000110**0** |
| **Bit 5** | 0001010**1** |
| **Bit 6** | 0101011**1** |
| **Bit 7** | 0010011**0** |
| **Bit 8** | 0100001**1** |

To hide the letter **"C"** whose binary value is **(**10000011), we would replace the LSBs of these pixels to have the following:

**After Hiding (New grayscale images values)**:

| 8-bitgrayscale bitmap image | Byte representing |
|---|---|
| **Bit 1** | 1101001**1** |
| **Bit 2** | 0100101**0** |
| **Bit 3** | 1001011**0** |
| **Bit 4** | 1000110**0** |
| **Bit 5** | 0001010**0** |
| **Bit 6** | 0101011**0** |
| **Bit 7** | 0010011**1** |
| **Bit 8** | 0100001**1** |

In the case of still grayscale images of type bitmap, every pixel is represented using 8 bits، with (11111111 = 255) representing white and (00000000 = 0) representing black. Thus, there are 256 different grayscale shades between black and white which are used in grayscale bitmap images. In LSB steganography, the LSB's of the cover image is to be changed. As the message bit to be substituted in the LSB position of the cover image is either 0 or 1, one can state without any loss of generality that the LSB's of about 50 percent pixel changes.There are two possibilities [66]:

1. Intensity value of any pixel remains unchanged.
2. Even value can change to next higher odd value Odd Value change to previous lower even value.

Techniques implemented to 24 bit formats are difficult to detect contrary to 8 bit format. Another example of LSB technique is: Consider a grid for 3 pixels of a 24 bit image and the number 300 is to be embedded using LSB technique. We know that ASCII value of "C" is (67) i.e. (10000011) in binary. Now this secret data is going to hide in LSB of RGB. The resulting grid is as follows [67]:

**Before Hiding (color images values):**

| color / Pixel | Red | Green | Blue |
|---|---|---|---|
| **Pixel 1** | **01010101** | **01011100** | **11011000** |
| **Pixel 2** | **10110110** | **11111100** | **00110100** |
| **Pixel 3** | **11011110** | **10110010** | **10110101** |

Take one 3 pixel set of the RGB channel at a time. This set contains total 9 values, three values from each RGB channel. Index these values from 0 to 8 as shown in Figure (3.11-a,b):

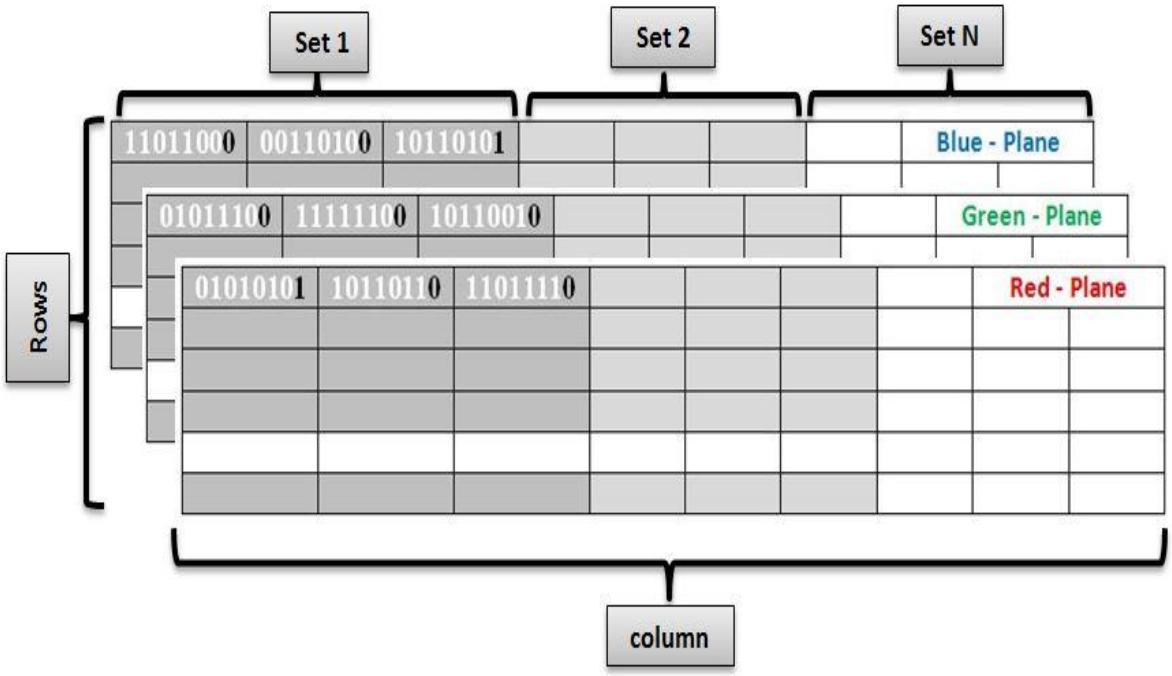



**Figure (3.11-a):** Initial 9 values in binary of cover mage**.**

**After Hiding 'C: 10000011' in LSB of RGB:**

| color / Pixel | Red | Green | Blue |
|---|---|---|---|
| **Pixel 1** | **01010101** | **01011100** | **11011000** |
| **Pixel 2** | **10110110** | **11111100** | **00110100** |
| **Pixel 3** | **11011111** | **10110011** | **10110101** |

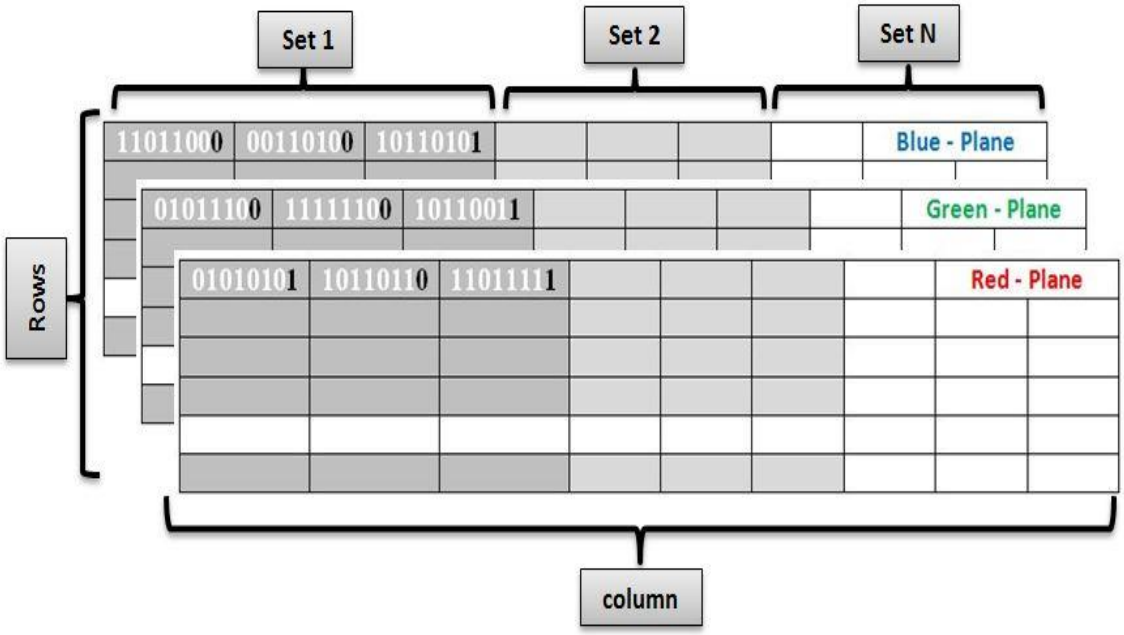
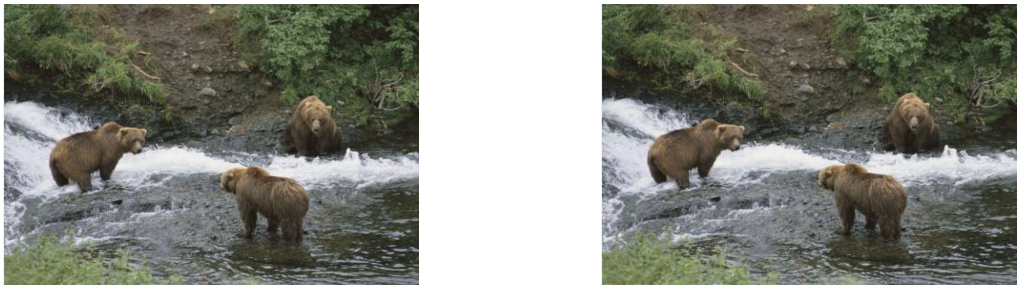



**Figure (3.11-b):** Embedding of "C" with Cover Image.

The difference between the cover (i.e. original) image and the stego image will be hardly noticeable to the human eye. Figure (3.12) that show a cover image and a stego image (with data is embedded); there is no visible difference between the two images.



(**a**) Original image (**b**) Stego image

**Figure (3.12):** The original image before and after the message is stored in the cover image.

Here the number "C" was embedded into the first 8 bytes of the grid, only the 2 bits needed to be changed according to the embedded message .On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size. As described above, LSB is simple technique of data hiding but it is predictable and hidden information can be retrieved easily. So, an efficient technique is required which is secure as well as efficient.

#### 3.3.1.1.1. The Advantages and Disadvantages.

The LSB is characterized by its simplicity in embedding the bits of the message directly into the LSB plane of cover image [68]. Working with the LSB does not result in a human perceptible difference. This is because the amount of the change is small. Consequently, the obtained stego image will look typical to the cover image and it will not be visible to the human eye. The **advantages** of LSB can be summarized in its popularity, easy to understand, high perceptual transparency, and low degradation in image quality. On the other hand, the **disadvantages** are low robustness to malicious attacks, vulnerability to accidental noise, and low temper resistance.

### 3.3.2. Transform Domain Techniques:

Wavelet transform (WT) The first recorded mention of what we now call a "wavelet" seems to be in 1909, is one of important and useful computation tools for a variety of signal and image processing applications. Wavelet transform has the advantage of being able to separate the fine details in a signal. Very large wavelets can be used to identify coarse details, whereas very small wavelets can be used to isolate very fine details in a signal. Conversion of spatial domain information into frequency domain information wavelet is commonly used in image steganography model. This is because the wavelet transform partitions the high frequency and low frequency information on a pixel by pixel basis. The wavelet transform domain is proposed for many steganography applications because of the many advantages it has [69].

**Some Application of Wavelets:**

**Wavelets** are used as a powerful statistical tool that can be used for a wide variety of applications such as: data compression, signal processing, smoothing and image denoizing, computer graphics, fingerprint verification, and multiracial analysis.

The transform based techniques use the domain specific characteristics of image to embed data in it and for carrying it out. Firstly, the image is transformed to that domain such as wavelet domain (DWT), frequency domain (DCT, DFT), wavelet domain etc. The data in these techniques are embedded in the transformed image instead of direct pixels. After that, the image is

retransformed to spatial domain. This algorithm has the advantage of embedding the information in the image that is less exposed to compression, image processing, and cropping. Moreover, the information spreads over a larger number of pixels or the whole image [70].

### 3.3.2.1. Discrete Wavelet Transform (DWT) Technique:

A discrete wavelet transform (DWT) is any wavelet transform for which the wavelets are discretely sampled. It represents one of the frequency domains in which steganography can be applied. A Discrete Cosine Transform (DCT) technique is calculated on blocks of independent pixels, accordingly a coding error causes discontinuity between blocks resulting in unpleasant blocking artifacts. This drawback of DCT is reduced using DWT because DWT is applied on whole image. DWT also provides better energy compaction than the DCT without any blocking artifacts. Two types of filters are used to filter signal of image in the DWT. These filters are [71]:

1. **High pass filter (H)**: in which pixels with high frequency information are kept, whereas pixels with low frequency information are lost.
2. **Low pass filter (L)**: is opposite to the high pass filter, where pixels with low frequency information are kept.

Accordingly, signal is efficiently decomposed into two parts: a detailed part (high frequency) and approximation part (low frequency) as represented in Figure (3.13). In Level 1 detail, the image signals are separates into four sub band images (LL, LH, HL and HH), which indicate the average horizontal and

vertical information [72]. In level 2 each sub band is consequently divided into four more sub bands.

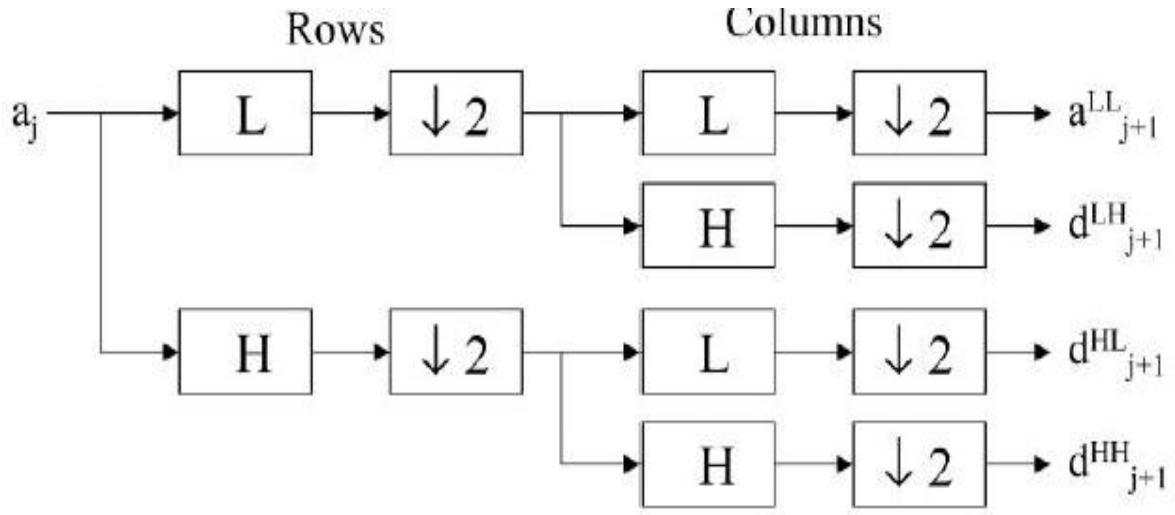



**Figure (3.13):** Discrete Wavelet Transform tree for 2D image [72].

Because human eyes are more sensitive to the low frequency part (LL sub band); the secret message can be hidden in other three parts without making any changes in LL sub band. Since, the other three sub bands are high frequency sub bands they contain unimportant data, therefore hiding secret data in them doesn't cause much degradation in image quality. Consequently, it is possible to use different approaches for enhancing the details in different frequency domain computed with a cascade of filters followed by a factor 2 sub sampling [73].

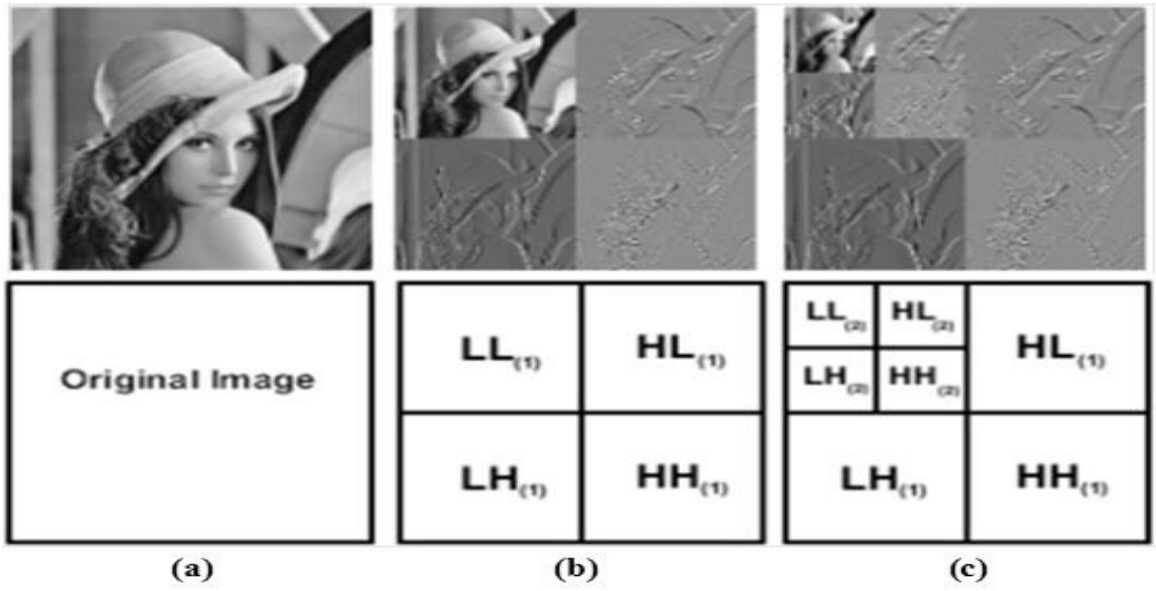
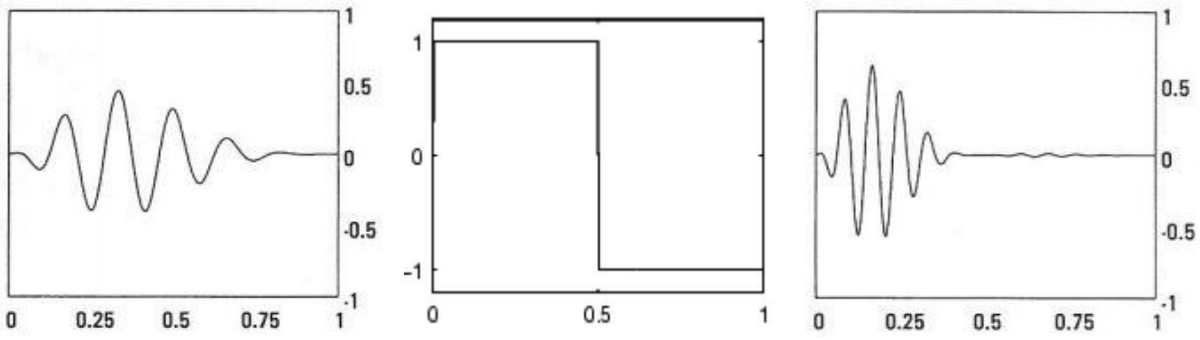



**Figure (3.14):** An example of DWT for Lena image: **a)** original image, **b)** 2D at level-1, and **c)** 2D at level-2 [73].

### 3.3.2.1.1. Haar Wavelet Transformation (HWT):

HWT has been used since it was first introduced by the Hungarian mathematician Alfred in 1910. The Haar Wavelet Transformation (HWT) is a simple form of data compression which includes averaging and differencing terms, eliminating data, storing detail coefficients, and reconstructing the matrix. The HWT is used to simply pair up input values, storing the difference and passing the sum.This process is recursively repeated, pairing up the sums to provide the next scale, finally resulting in differences and one final sum. Figure (3.15) illustrates an example of the Haar functions [74].




**(a)** **(b)** **(c)**

**Figure (3.15):** shapes of: **a)** Signal image, **b)** Haar Wavelet, and **c)** Haar transforms (1-level) [74].

### 3.3.2.1.1.1. The Haar function:

Wavelets are mathematical functions, which were developed for sorting data by frequencies. The word "wavelet" refers to an orthogonal basis of a certain vector space. A Wavelet transformation transfers data from the spatial domain into the frequency domain and subsequently stores each component with a matching resolution-scale.

$$\psi(t) = \begin{cases} 1 \ , & t \in [0, 1/2) \\ -1 \ , & t \in [1/2, 0) \\ 0 \ , & t \notin [0, 1) \end{cases} \qquad t = 2, 3, \ldots \qquad (1)$$

In 2D wavelet transformation, structures are defined in 2D and the transformation algorithm is applied first on rows and on columns [35]. Figure (3.16) illustrates a simple example of the Haar DWT. The Haar DWT works very well to detect the characteristics like edges and corners.

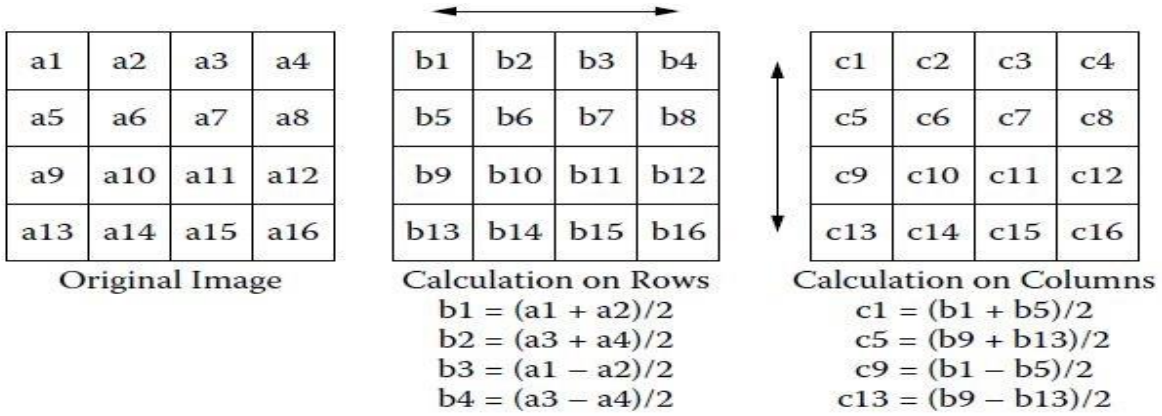



**Figure (3.16):** An example of DWT of size 4 × 4 [75].

Once the embedding process is completed, the inverse Haar DWT is applied in order to create the stego image. The vertical and horizontal operations are carried out as follows [76]:

- **Horizontal Operation:** In this operation, an image will be divided into two bands that are low and high frequencies. Pixels are scanned from left to right in the horizontal direction. Both of addition and subtraction operations are performed on the neighboring pixels. The results of the addition operation are stored on the left side that represents the low frequency band.
- **Vertical Operation:** Low and high frequencies obtained from the horizontal operation are further subdivided into low low (LL), low high (LH), high low (HL), and high high (HH) frequencies. All pixels will be scanned over for the addition and subtraction operations, but in the vertical direction. The addition of the neighboring pixels will be held in the top. Both of the horizontal and vertical operations are represented in Figure (3.17):

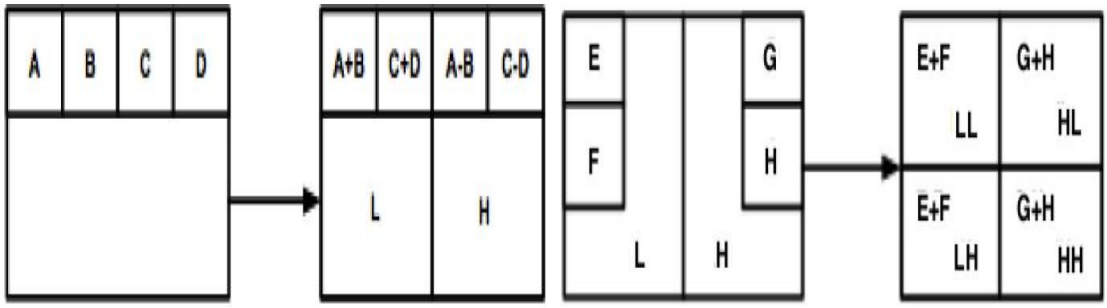



**Figure (3.17): a)** The horizontal operation on the first row and **b)** vertical operation [76].

### 3.3.2.1.1.2. Properties and Advantages of Haar Wavelet Transform:

The Properties of the Haar Transform can be summarized as follow [77]:

1. **Orthogonally:** The original signal is divided into low and high frequencies. These filters that enable the splitting without duplicating redundant information are called orthogonal.
2. **Compact support**: The magnitude response of the filter should be zero outside the transform frequency range. When this property is satisfied, the transform is energy invariant.
3. **Linear Phase**: symmetric filters should be used in order to obtain a linear phase.
4. Haar Transform has poor energy compaction for images.
5. Haar Transform is a very fast, real and orthogonal transform.
6. The basis vectors of the Haar matrix are in a sequential order.

The **advantages** of Haar Wavelet transform are as follows [78]:

1. Computation speed is high.
2. HWT is efficient compression method.
3. Simplicity.
4. Best performance in terms of computation time.
5. It is memory efficient, since it can be calculated in place without a temporary array.

### 3.3.2.1.2. The Advantages and Disadvantages of the DWT Technique.

The advantages and disadvantages of the DWT technique can be summarized in the following points [79]:

The **advantages** of DWT techniques are:

1. With the DWT, there is less chance for loss or removal of the hidden data,
2. Information is distributed all over the whole image,
3. DWT provides higher flexibility in data hiding.
4. DWT is generally independent of image formats.

The **disadvantages** of DWT are:

1. It requires much more understanding of the embedding domain.
2. It also needs careful selection of embedding coefficients in order not to cause image degradation.
3. It has higher mathematical robustness.
4. It has a comparatively low embedding capacity.

### 3.3.3. Cover Image Formats:

Various image file formats can be used for cover images, which reside under to main categories (lossless and loss formats). The following is a summary of the main types of image file formats under these two categories [80, 81]:

#### 3.3.3.1. Lossless image representation formats:

1. **Microsoft Windows Bitmap (BMP):** This image format was developed by Microsoft Corporation. BMP stands for bitmap or bump file. It may contain images with 1, 4, 8, or 24 bits per pixel and it is stored by scan line, bottom to top.
2. **Tagged Image File Format (TIFF):** The TIFF format was created in 1986 by an industry committee chaired by the Aldus Corporation. It handles monochrome; grayscale, 8 and 24 bit color. TIFF files can be saved in a variety of color formats and in different forms of compression. Most graphics programs that use TIFF do not compress files so that file sizes are quite big.
3. **Portable Network Graphic (PNG):** PNG was created as a more powerful alternative to the GIF file format. This format supports an alpha channel, or the "RGB" color space. The alpha channel is added to the three standard color channels (red, green, and blue, or RGB) the PNG is saved with 256 colors maximum but it saves the color information more efficiently. It also supports an 8 bit transparency. PNG supports palette based, grayscale and RGB images.

### 3.3.3.2. Lossy Image Compression Formats:

1. **Joint Photographic Experts Group (JPEG)**: a lossy compression algorithm was developed to compress images with 24 bits depth or grayscale images. This is a very flexible algorithm, where the compression rate can be adjusted. Image compression generally results in loss of more information but the size of the result image will be smaller. JPEG standard has two basic methods for the compression and that meet the unique needs of every application.

**Table (3.4):** Summary of image file formats.

| Format | Name | Characteristics |
|---|---|---|
| **BMP** | Windows bitmap | Uncompressed format. |
| **TIFF** | Tagged Image File Format | **Lossless:** Document scanning and imaging format. Flexible: LZW, CCITT, RLE. |
| **PNG** | Portable Network Graphics | **Lossless:** improves and replaces GIF. Based on the DEFLATE algorithm. |
| **JPEG** | Joint Photographic Experts Group | **Lossless:** big compression ratio, good for photographic images. |

## 3.4. Steganography Techniques: Background and Related Work:

Jain and Ahirwal (2010) [82] have proposed an adaptive least significant bit (LSB) spatial domain approach for data embedding as represented in Figure (3.18). This approach splits the image pixels and creates a stego key. It embeds binary bit stream in 24 bits color image (Blue channel) or in 8 bits grayscale image. This obtained private stego key has five different ranges of gray level

image and each range was subject to substitution of a fixed number of bits to be embedded in the LSB image. The integrity of both secret hidden information in stego image and high hidden capacity represent the strongest point in this. However, the limitation was to hide more bits of signature within the hidden message. This approach also provides a method for color image through modifying the blue-channel with the same method for hiding information. Keeping the integrity of secret hidden information with High capacity was strongest point in this approach, whereas hiding extra bits of signature with hidden message represented its weak point.

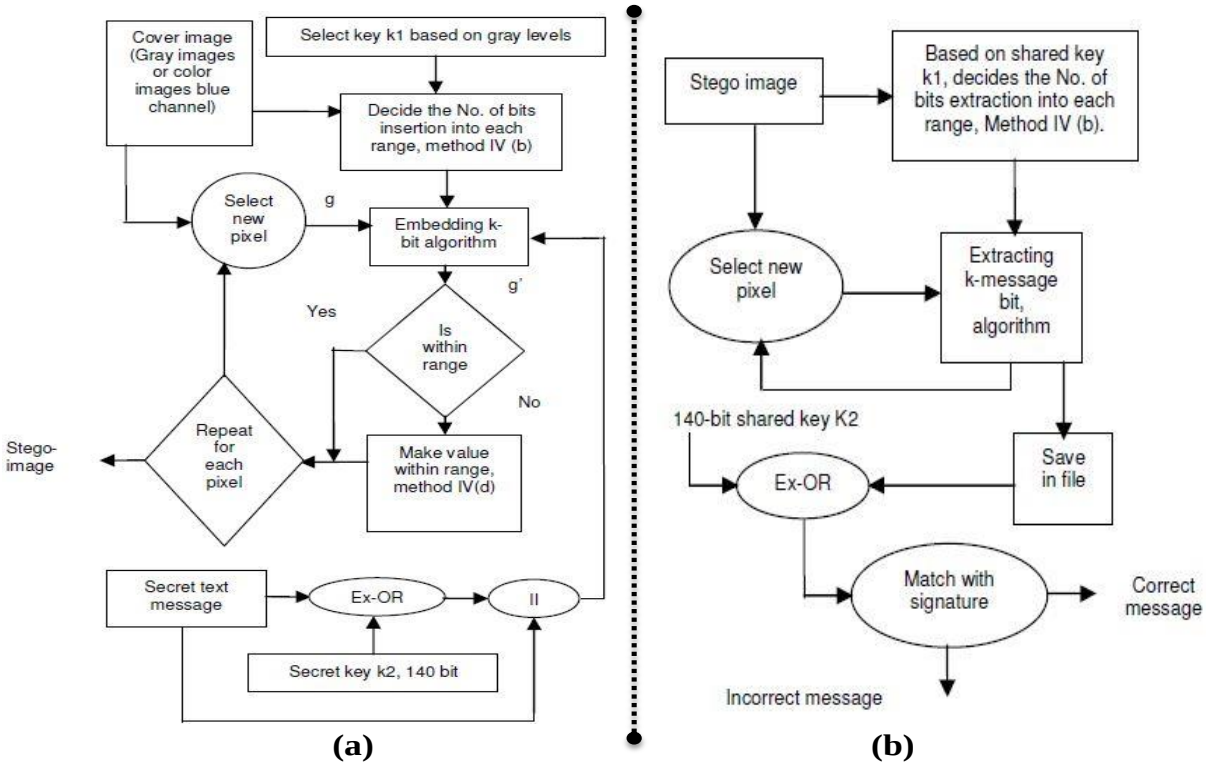



**Figure (3.18):** Block diagram of whole process is message: a) Embedding. b) Extraction and Integrity check [82].

Karim (2011) [83] has proposed a new approach for hiding secret information within the LSB of image as illustrated in Figure (3.19). In this approach a secret key was used to encrypt the hidden information to insure its protection from unlawful users. This approach was based on image steganography, where it enhances the current LSB substitution techniques to maximize the security level of hidden data. This approach was used to substitute LSB of RGB true color image. His obtained results indicated that the proposed approach has provided high level of security and the PSNR value was higher than that obtained from the general LSB based image steganography methods.

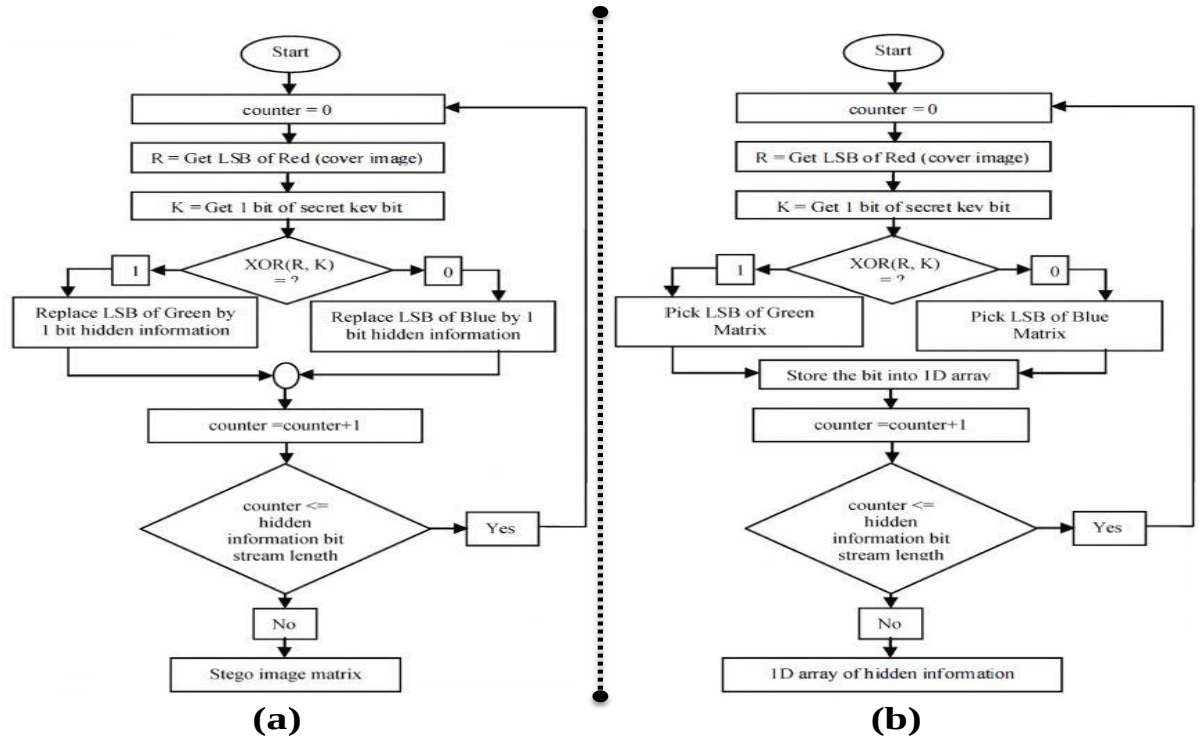



**Figure (3.19):** The flowchart of: a) Hiding information in cover-image and b) Recovering hidden information from stego-image [83].

Tayel el at., (2013) [84] have developed an approach to benefit from the advantages of cryptography and steganography together in image processing as demonstrated in Figure (3.20). Cryptography was used to hide the existence of the message and steganography was used to convert the message into an invisible format. The New Hybrid Security message Allocation Algorithm (NHSA) was performed to accomplish a higher security level by adding eight zeroes as LSBs to the cover image pixels. Blowfish algorithm (BFA) was used as an effective encryption algorithm to encrypt the hidden message. A block size of 64 bits was used and the key can be any length from 32 to 448 bits. Their obtained results revealed that the proposed NHSA algorithm worked as a robust method for hiding data in images with high degree of security based on the PSNR and MSE values. This is when the stegnoanalysis is performed on the cover image. It can be used to hiding a wide variety of multimedia data, text, image, audio and video.

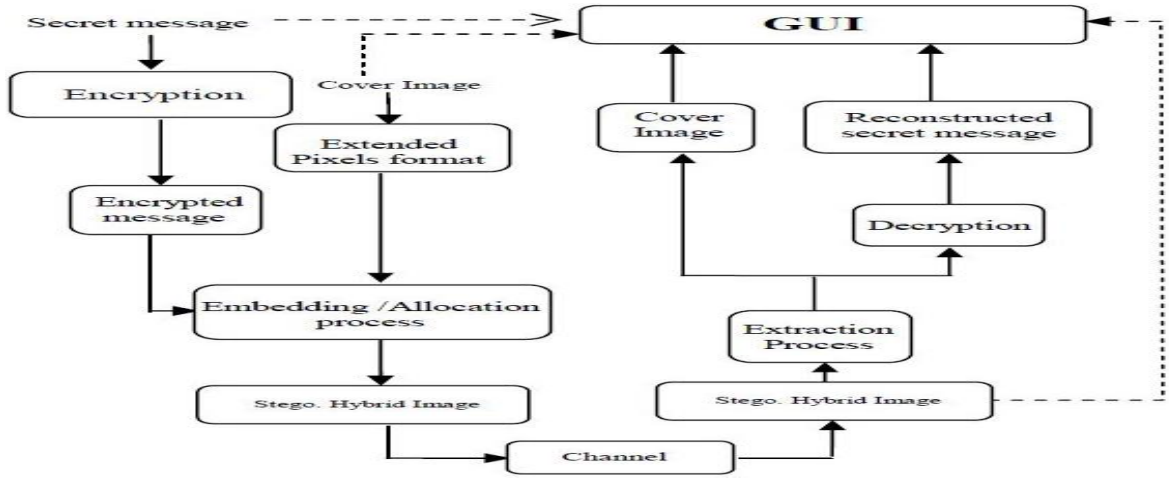



**Figure (3.20):** Block diagram of a New Hybrid Security Allocation Algorithm [84].

Rajkamal and Zoraida (2014) [85] have developed a new approach of image steganography inside the embedded and encrypted data file using Hash LSB with RSA algorithm. This approach uses the Hash function to create a pattern for hiding data bits into LSB of RGB pixel values within the cover image as illustrated in Figure (3.21). In this approach the data have been encrypted first before being embedded into the cover image to protect it against intruders. In the second stage encryption and decryption steganography image was carried out using blowfish algorithm. This technique has proved it efficiency in hiding secret data.

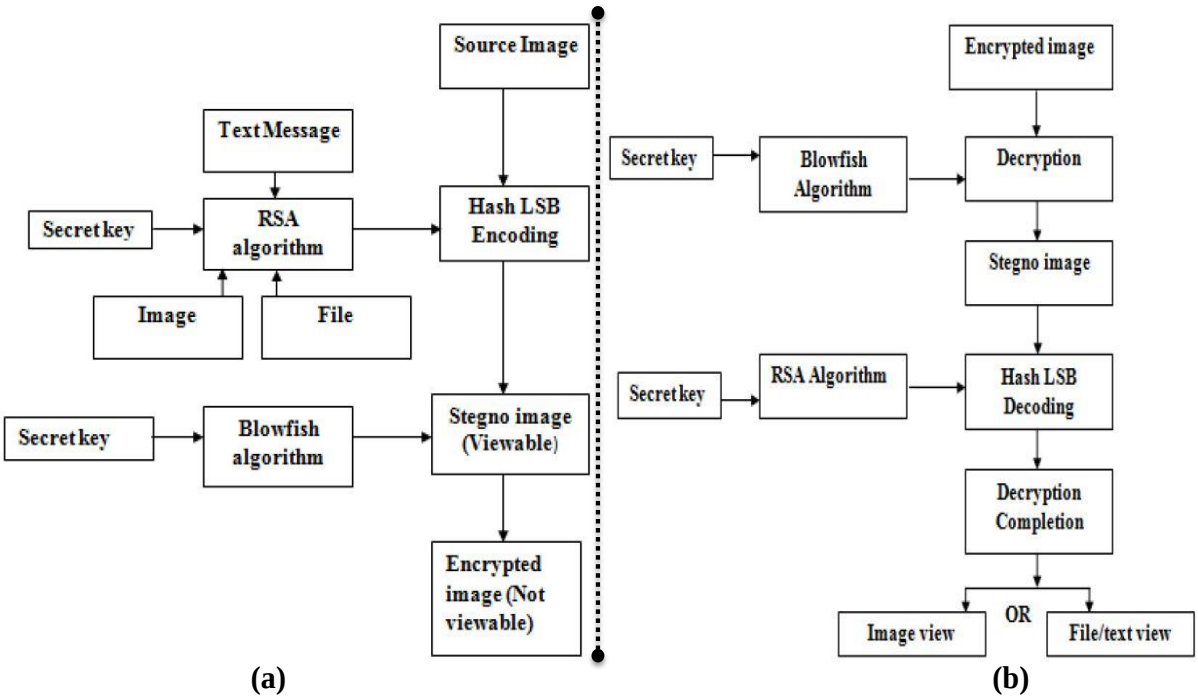



**Figure (3.21):** Block diagram of implementing the Blowfish and H-LSB, RSA algorithm: a) Sender process. b) Receiver process [85].

Muhammad el at., (2015) [86] developed an image steganography technique for grayscale images in spatial domain. In this approach the secret data is encrypted and shuffled using pattern based bits shuffling algorithm (PBSA) and a secret key. The encrypted data are then embedded in the cover image using magic least significant bit (M-LSB) method. The detailed novelty of the proposed technique is illustrated as a block diagram Figure (3.22). The experimental results indicating the high quality of stego images based on PSNR and embedding capacity. This approach could be nominated as a candidate technology for securing communication over the Internet, where it maintains the image quality and assures security of the built in data within the used cover image.

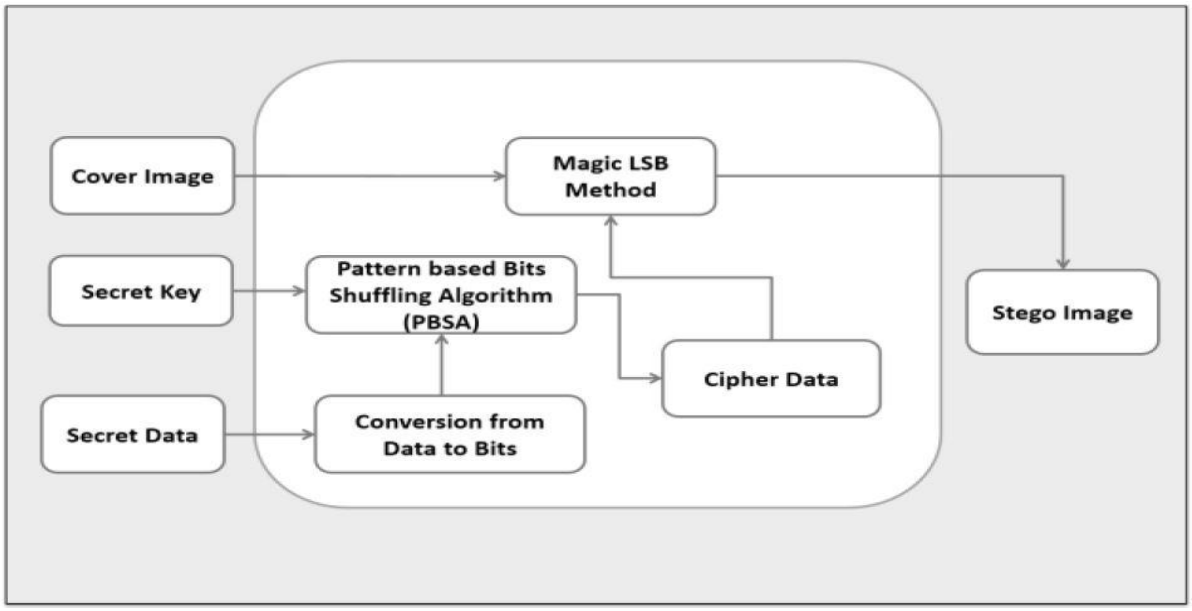



**Figure (3.22):** Block diagram of data hiding based on bits shuffling algorithm (PBSA) [86].

Manjunatha Reddy and Raja., (2009) [87] developed a hybrid approach for hiding data based on fusion of wavelet coefficients for both the cover and payload images into a single image using embedding strength parameters alpha and beta Figure (3.23). The cover and payload were preprocessed to minimize the pixel range to make sure that the payload is recovered accurately at the expected destination. In this approach, the High Capacity and Security Steganography using DWT (HCSSD) was applied with the two level wavelet transform on both the cover and payload images. The payload wavelet coefficients were encrypted and fused with wavelet coefficients of cover image to generate stego coefficients based on the embedding strength parameters alpha and beta. The capacity of the proposed algorithm was increased as the only approximation band of payload was considered. It was found that the Entropy, MSE and capacity were significantly improved with acceptable PSNR when compared with the existing algorithms. This algorithm can be tested in the future with the curvelet transform and other transform techniques.

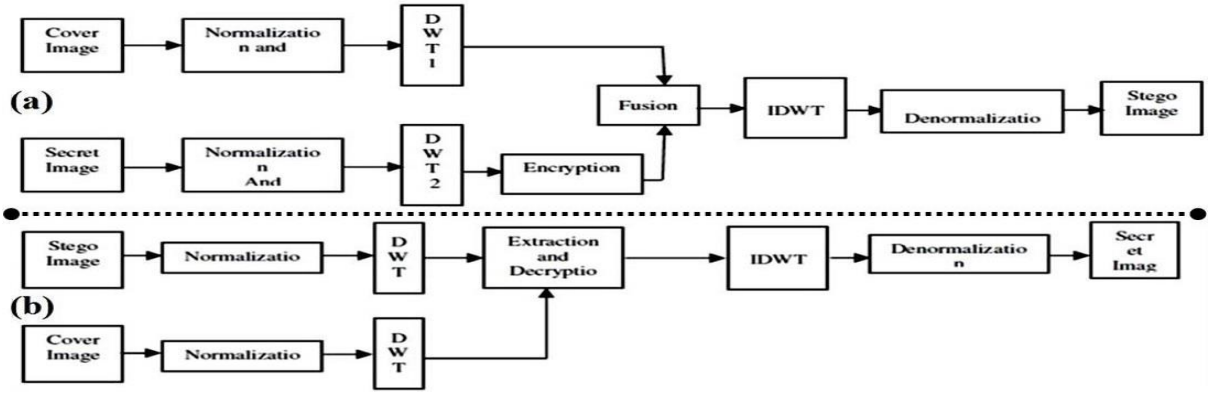



**Figure (3.23):** The block diagram of a hybrid approach for data: a) Embedding, and b) Extraction [87].

Sarkar el at., (2011) [88] proposed a novel technique for Image steganography based on DWT as demonstrated in Figure (2.24). DWT was used to transform original image from spatial domain to frequency domain. First, the 2D DWT was applied on grayscale cover image of size MxN. Second, the Huffman encoding was carried out on the secret messages and image before embedding of secret message. The image was embedded in the high frequency coefficients coming from DWT. It was found the proposed technique has the ability of hiding large amounts of data with high security, good invisibility and without loss in secret data.

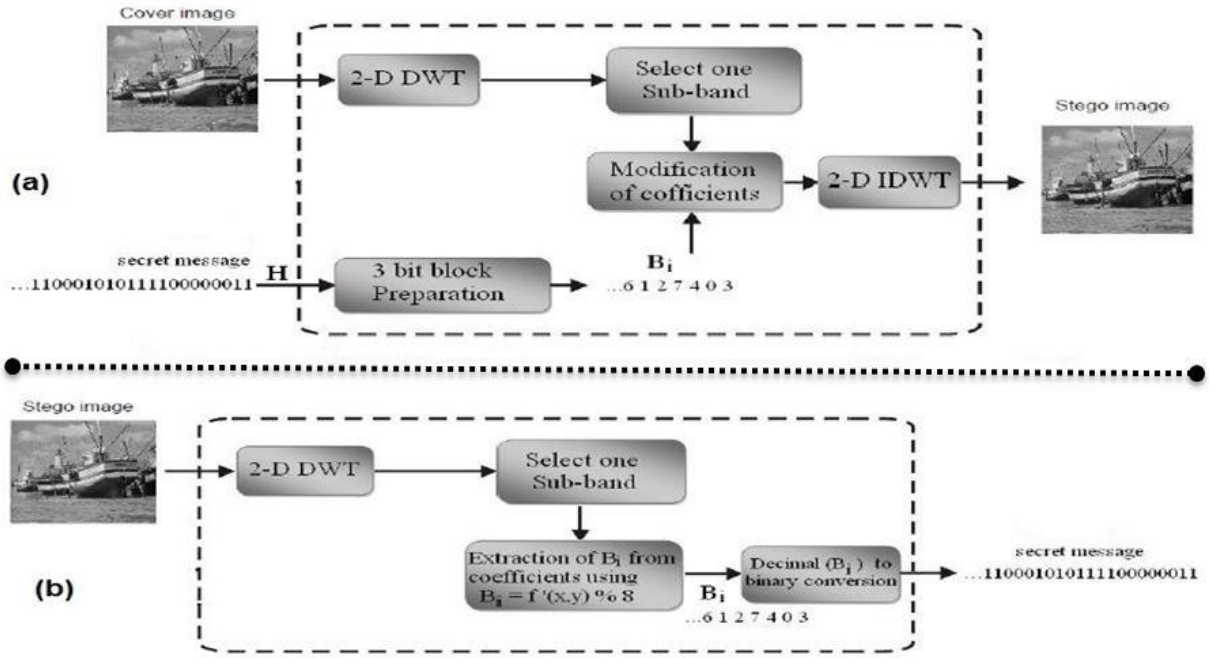



**Figure (3.24):** The block diagram of data: a) embedding a secret message into a cover-image and b) Extraction of secret-message [88].

Prabhakaran et al., (2012) [89] have proposed a new and secure steganography approach based on DWT for embedding a secret image into a cover-image without any major change. In this approach both encoding and decoding processes were used. The flowchart of the proposed technique is illustrated in Figure (3.25). In the encoding stage, Arnold transform was applied with key on the secret message. Then, the DWT was applied on the cover and secret images. In the second stage, the Alpha blender matrix was obtained through adding the wavelet coefficients for respective sub bands of both the cover and secret images. Finally, the inverse DWT was applied to get the stego image. The obtained results have indicated that the proposed technique was high efficient in securing data with high perceptual invisibility.

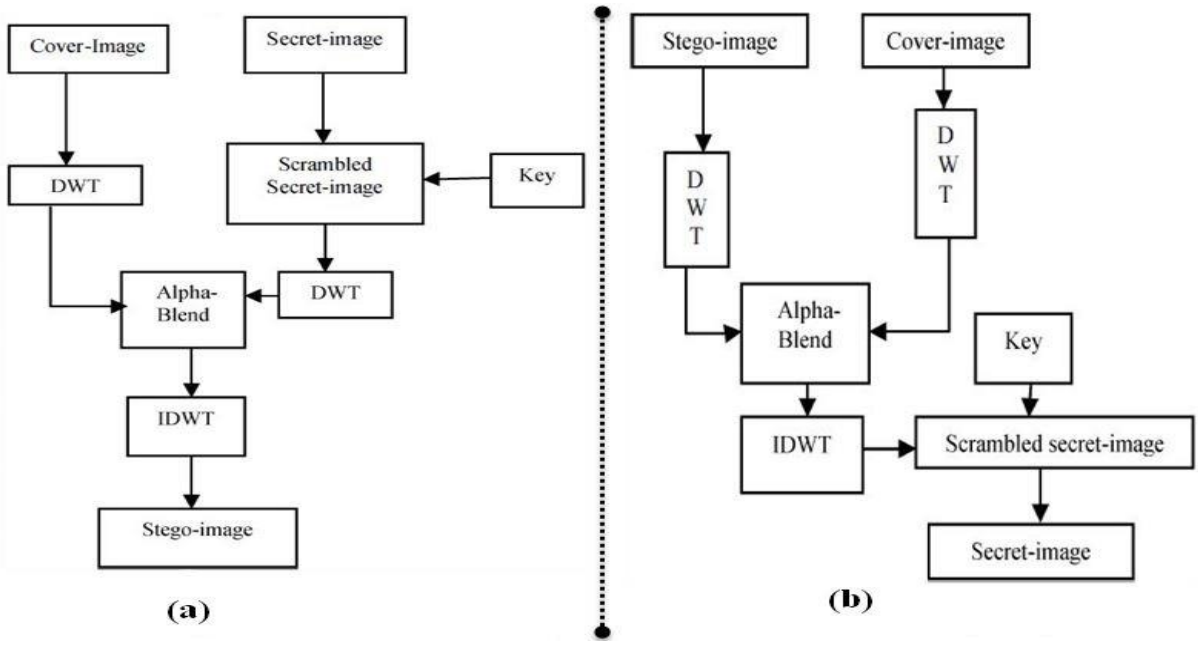



**Figure (3.25):** Flowchart of the proposed modified secure steganography approach for data: a) Encoding, and b) Decoding [89].

Ravi and Mahalakshmi (2014) [90] have developed a secure image coding scheme with multi-level of security based on DWT and AES algorithm as represented in Figure (3.26). The AES algorithm was used for the encryption of consistent image information and two dimensional DWT was used for image decomposition. Image size of 1024x1024 was used considered for encryption and unscrambling. In order to reduce the computation time, the input images were transformed into sub bands using the DWT, and then each one sub band was quantized and encoded utilizing AES. The experimental results exhibited that the proposed secure image encoding scheme was quick and appropriate for giving high security provisions.

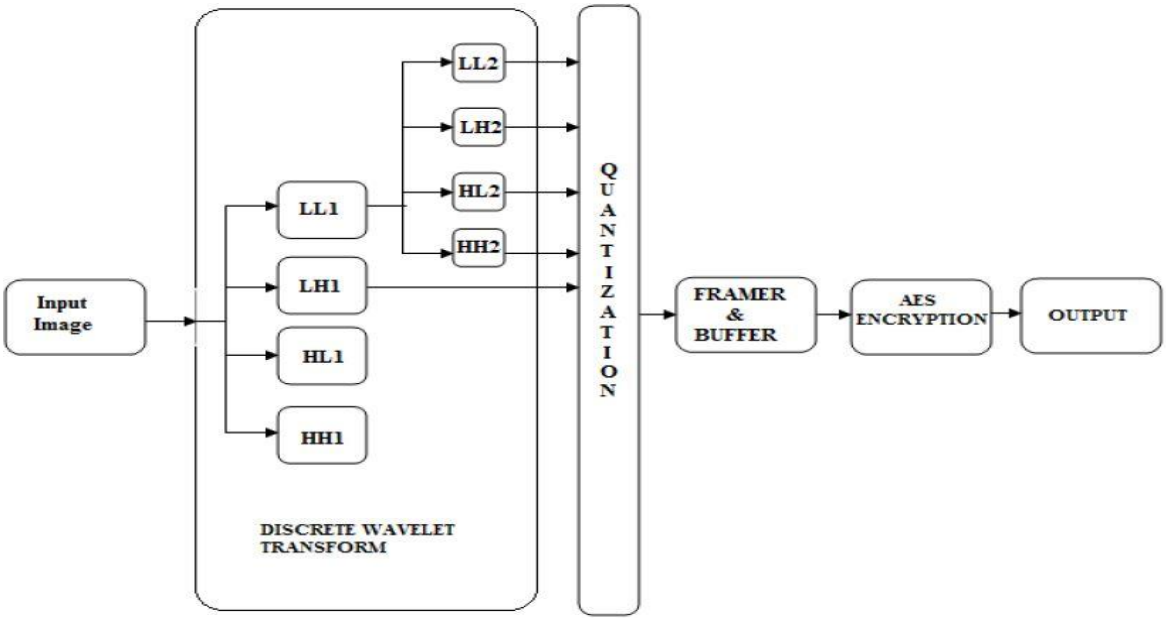



**Figure (3.26):** Modified Secure Image Encoding, Transmitter and Receiver [90].

Podder et al., (2015) [91] have proposed a unique mapping approach to hide secret messages in an image based on (DWT) domain Figure (3.27). DWT was applied on the RGB channels of the cover image. The secret message was only hidden in the vertical and diagonal coefficients of the cover channel, where these coefficients are less sensitive to human eyes. The proposed algorithm has provided higher level of security, good image quality image, good PSNR and low MSE.

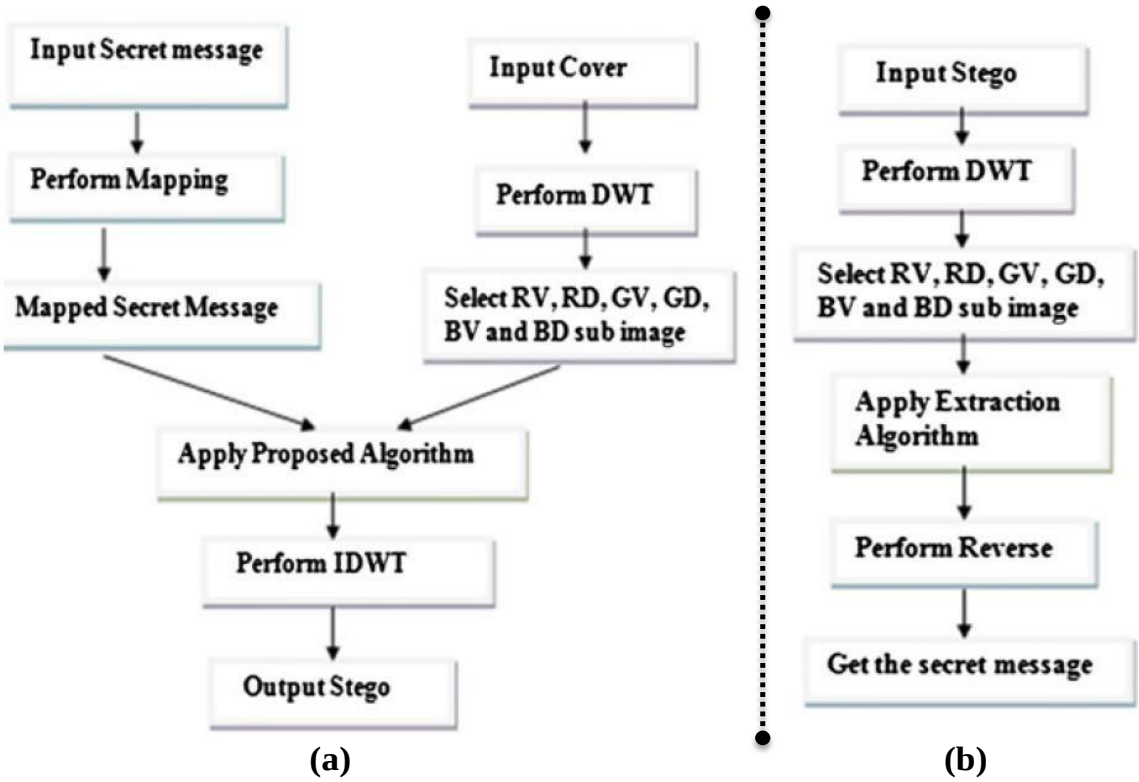



**Figure (3.27):** Block diagram of Proposed Method for data: a) Embedding, and b) Extraction [91].

**Table (3.5):** shows some of the previous proposed methods for image Steganography, particularly spatial Domain and Transform Domain in terms of their chronological order as well as their main characteristics [92]:

**Table (3.5-a):** Chronological order of spatial domain steganography approaches.

| No. | Author | Method used | Advantage | Other parameters |
|---|---|---|---|---|
| **1** | Jasvinder Kaur et.al., **2009** | Embedding using digital operations are compared | More embedding capacity | Embedding capacity 1165084 bits .Image size (512 x 512). |
| **2** | C.-H.Yang et.al. **2010** | Improving histogram based reversible data hiding by interleaving predictions | Larger embedding capacity & better image quality. | PSNR = 48.82 dB, 99947 bits embedding Capacity (512x512) Image. |
| **3** | Fahim Irfan Alam et al. **2011** | Noise filtering before embedding combined with encryption. | Error detection& Noise free transmission. | Success rate of %83< with different types of images. |
| **4** | S.Shanmuga Priya et. al. **2012** | Embedding done in the sharper edge regions using a threshold | Better performance in terms of distortion and resistance against existing steganalysis. | Non adaptive technique has more PSNR& less MSE than adaptive technique. |
| **5** | Shamim Ahmed Laskar et.al.**2013**. | Data embedding in the red plane of the image selected using PRNG | Increases security with reduced distortion rate | PSNR = 58.8 db. MSE = 0.0854 %. |

**Table (3.5-b):** Chronological order of transform domain steganography approaches.

| NO. | Author | Method used | Advantage | Other parameters |
|---|---|---|---|---|
| **1** | Prosanta Gope et. al., **2010** . | Enhanced JPEG steganography with suitable encryption. | Added security using encryption. | Bit Error Rate، MSE and PSNR values are computed |
| **2** | Keith.L. Haynes et. al.**, 2011** . | Using Image Steganography to Establish Covert Communication Channels | Covert communication Security by added encryption | Min. Image Size (128x128)10 Haar features depicted Final class recognition 11.5% . |
| **3** | Anastasia Ioannidou et al., **2012** . | Based on the edges present in an image. A hybrid edge detector is used for this purpose for color images is exploited. | advantages of sharp area of the image is used to hide large amount of data using hybrid edge detector and a high payload technique | It increase imperceptibility، provides higher PSNR for embedded image. |
| **4** | Hemalatha.S et.al., **2013** | Integer Wavelet Transform is used to compare embedding in two different domains. | Quality of image is compared by embedding in RGB and YCbCr domains. | PSNR in RGB = 47. PSNR in YCbCr = 41. |

## 3.5. Steganalysis.

Steganalysis is the art of discovering and rendering such covert messages. steganalysis needs to be done without any knowledge about the key used in embedding or even the algorithm. steganalysis is a process in which a stego analyzer cracks the cover object to get the hidden data. A steganalysis technique is considered successful if it could detect the presence of a secret message.

This could be document (text, image, audio or video). And concealment cover analysis algorithm based on the method of building information hiding

and to analyze the cover trim. And that cover analysis techniques hide images depends on the type of classification form, image form, and focusing on the most important and most widespread (JPEG, BMP, GIF and PNG). the concealment cover analysis techniques that take into account the form most commonly used images (e.g. JPEG, BMP, GIF and PNG) [93].where the frequency range is more powerful compared to the spatial domain.

The different types of cover image in steganography techniques and steganalysis techniques for the detection of secret message in the image [94]:

1. **In gray scale images:** hide information which is undetectable by the human visual system, but concealment cover analysis techniques that are easier to hide cover analysis techniques for color images and gray scale images that give the highest accuracy rate detection of color images .
2. **In JPEG images:** for this genre, most photo techniques is a concealment cover analysis frequency range, due to its loose compression technique to hide information that is in the frequency range to avoid data loss and image analysis cover trim is more complex than other image format for work in the frequency domain is not trivial, so it needs more statistical analysis .
3. **In BMP, TIFF, and PNG images:** most trim cover analysis techniques are spatial analysis cover trim area. Frequency range is more powerful compared to the spatial domain, so you should give more attention and effort to BMP, TIFF images, PNG concealment cover analysis .

The analysis of the trim cover needs more effort in the way of a fling. Did most of the trim cover BMP analysis techniques lack fling database experiences, they create their own database. It has been little effort to analyze the cover trim for GIF and PNG images. Finding a steganography message is the main objective of steganalysis. The following is a summary of possible attacks on a steganography system [95]:

1. **Traffic analysis:** is used to monitor the information send from one source to another.
2. **Detection:** both visual and/or statistical attacks can be used to detect stego data. Visual attacks are used in case if the embedding algorithm causes obvious artifacts in the stego data, whereas the statistical attacks are used to compare the frequencies of a potential stego file with the theoretically expected frequencies of the file. Although the last ones are effective in recognizing stego, they cannot recover the hidden message.
3. **Manipulation:** an attacker could be able to destroy the message by just altering the stego data. Data manipulations include: cropping, rotating, lossy compression, and scaling.
4. **Brute force:** in case if an attacker has received some stego data and is trying to recover the hidden message. This attack can be very difficult unless the sender of the stego data used the same cover data twice and the attacker has a copy of the cover data and the key.

Overall, we note that the main idea behind the analysis of concealment cover is that the existence of confidential data we will cover medium to amend and change the statistical properties, so it can detect these abnormalities in the middle of the statistical properties of the resulting stego. And that this process is called in to find these anomalies (statistical analysis of concealment cover).

### 3.6. Summary:

This chapter provides an introduction about steganography. It started with having a look at steganography main concepts, goals and major types. This is followed describing the most common and recent steganography techniques for image and the advantages and disadvantages of each technique. These techniques seemed to be unbreakable but as natural images were better understood and newer models need to be created and more powerful algorithms which try to minimize changes to image statistics need to be developed. Further improvement in understanding of the statistical regularities and redundancies of natural images helps in analyzing these algorithms. In conclusion, this chapter provided a look at the main idea of steganalysis and common attacks aiming to defeating steganography hidden data in cover files.

In the next chapter, the will review overview of the proposed system model.

# CHAPTER 4

## The Proposed System Model

Steganography and Cryptography are widely used techniques for information manipulation to conceal its existence. Cryptography intentionally messes up a message to make it understood. On the other hand, steganography hides or conceals the message and make it unseen. Actually, steganography can be very valuable when the use of cryptography is prohibited, where strong encryption is generally forbidden. For that reason, steganography can avoid these policies and secretly pass a message. Our research focuses on how to build a strong defensive system. A great effort has been spent in the fields of cryptanalysis and steganalysis to overcome the hiding abilities, so our role is to develop a new technique that is harder to discover or defeat.

This chapter is organized in four sections. The first section is an overview, Section 2 introduces the design of the first proposed system (only steganography technologies) and design of the second proposed system (only hybrid encryption algorithm); Section 3 introduces the evaluation parameters; Section 4 the summary.

## 4.1. Overview

Most of the techniques that use steganography and cryptography concentrate on either encrypting the secret message or hiding its existence in a cover object. In this chapter, a security system is developed based on using steganography and cryptography for better confidentiality and security. Three different aspects were addressed in information hiding systems that compete with each other. These three aspects are: capacity, security, and robustness. Capacity indicates the amount of information that can be concealed in the cover medium. Security reveals the inability of unlawful person to detect the hidden information. Robustness refers to the amount of alterations the stego image or medium can withstand before an unlawful person can damage concealed information.

**The aims of this chapter are to:**

1. Give a new direction on how to improve existing methods for hiding secret messages. The proposed approach evolves both the LSB and 2D-DWT-2 Level separately in embedding and extracting hidden data.
2. Apply both encryption and steganography together with more security levels to gel a very highly secured system for data hiding. In this system, a message is first encrypted before being hidden in a cover image in order to achieve a better level of secrecy.

Although steganography and cryptography provide security by adding multiple layers of security, it is good to make a combination of both cryptography and Steganography. In this case, the data encryption can be carried out using a software and after that the encrypted message is embedded in the cipher text in a digital image or another type of media with the use of stego key. The integration between these two techniques could improve the security of the embedded data. This approach also satisfies the requirements such as capacity, security and robustness for securing data transmission over an open channel. The resulting stego image can be transmitted without revealing that secret information is being exchanged. Furthermore, even if an attacker was able to defeat the steganography technique, he would still require the cryptographic decoding key to decipher the encrypted message.

The proposed scheme is a data hiding technique that uses an image cover (color and grayscale). The proposed recipient needs only to process the required steps in order to reveal the message; otherwise the existence of the hidden information is virtually undetectable. The proposed scheme provides the ability to hide a significant quality of information making it different from common data hiding mechanisms. Figures (4.1 and 4.2) illustrate the general framework of the proposed systems for hiding secret data. These Figures the main performed steps at both the sender's side and the receiver's side.

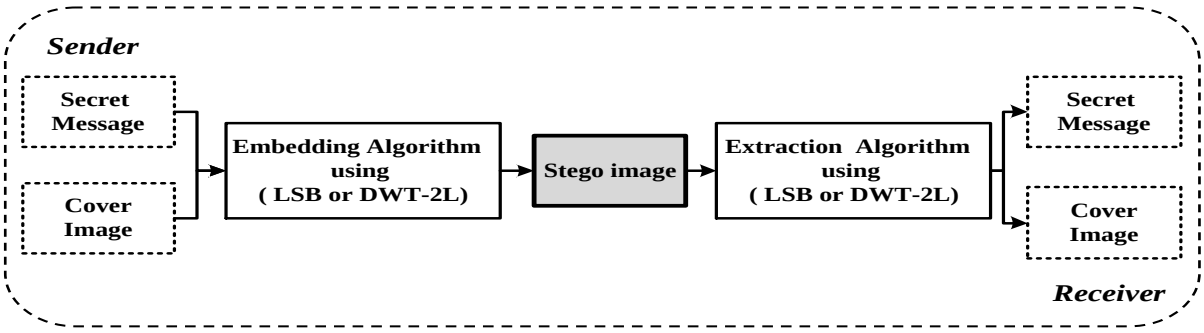



**Figure (4.1):** The proposed framework for hiding information using steganography technologies only.

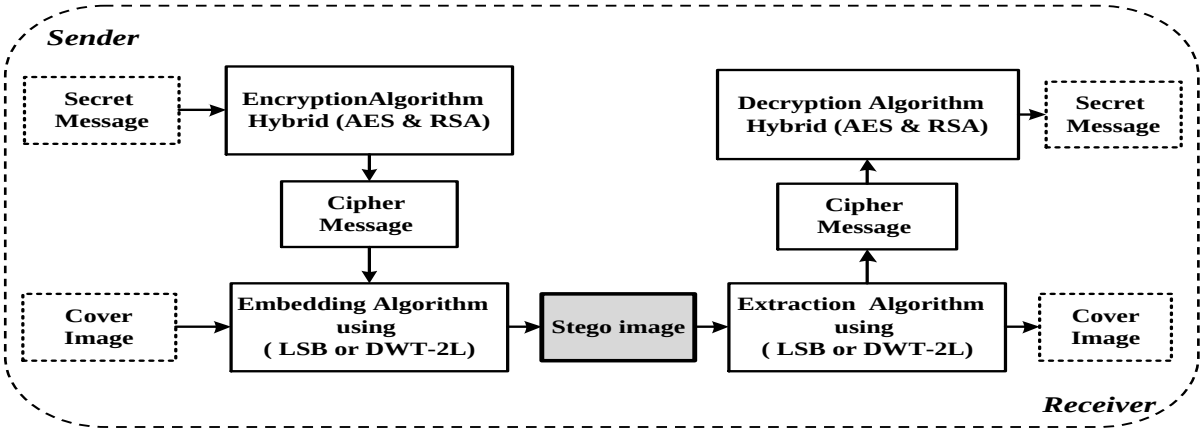



**Figure (4.2):** The proposed framework for hiding information using both steganography and hybrid encryption algorithms.

## 4.2. The Proposed Approach

### 4.2.1. Design the First Proposed System (*Only Steganography Technologies*)

The LSB is a commonly used technique for embedding information in a cover file. The LSB represents the lowest order bit in a binary value which is an essential concept in digital data programming and storage. Hiding text in the

cover image without leaving any visible signs in it to indicate any embedded text, is called the stego cover. The cover after hiding data in it should look the same as the original cover to a third party when displaying on the screen. The proposed approach was intended to evolve both the LSB and 2D-DWT-2L separately in embedding and extracting hidden data. In this work the 2D-DWT schema is developed by 2D-DWT-2L was used to get to the point of being able to perform quite robust embedding, which is very difficult to break or decipher. The proposed system utilizes the least significant bit of binary changes and 2D-DWT-2L to optimize the ASCII embedding layout.

#### 4.2.1.1. Incorporation Process and Recovery Process by Evolved LSB

The LSB data embedded mechanism was improved through making a harmony between the number of bits used in embedding the concealed text and the number of bits used in embedding the cover file. The pixel is randomly selected in the cover image and accordingly the binary value to be concealable is embedded in the bits of the cover image. In this work, the secret text is transformed into an ASCII format, which subsequently is transformed into a binary format. In the extraction process to retrieve the secret text, the pixel location, number bits, and dimensions of the original image are needed to be known. Finally, the binary matrix is created from converting the cover file into binary values as a result of matching the secret text with the cover file and encoding the differences between them to obtain the stego file.

## a. Text Incorporation Procedure Evolving LSB

This algorithm is divided into two parts. The first part (i) is for encoding a secret text, and the second part (ii) is for embedding the encoded message in the cover image. The algorithm used in carrying out these two parts is described below.

***Embedding Algorithm (1): Least Significant Bit Hiding Algorithm (LSB):***

**Inputs**: cover image, secret message. **Output**: stego image**. Variables**: binMsg (k) represent binary values of matrix text ; img(i,j) represent stego image ; k represent counter.

**Begin**

**1.** convert the secret message in ASCII Code as asciiMsg
**2.** convert the ASCII Code to Binary Values as binMsg
**3.** read N → length of binMsg
**4.** prepare b as zero vector of N
**5.** for k = 1 to n
**6.** if (binMsg (k) = = '1')
**7.** set b(k) = 1;
**8.** else
**9.** set b(k) = 0;
**10.** end
**11.** end
**12.** scan the image row by row and encode it in binary as img
**13.** read height of img
**14.** read width of img
**15.** Define counter as k = 1;
**16.** for i = 1 to height
**17.** for j = 1 to width
**18.** Define flag as LSB = mod(double(img (i,j)), 2);
**19.** if (k>m || LSB == b(k))
**20.** set img(i,j) = img (i,j);
**21.** elseif (LSB == 1)
**22.** set img(i,j) = (img (i,j) - 1);
**23.** elseif (LSB == 0)
**24.** set img(i,j) = (img (i,j) + 1);
**25.** end
**26.** k = k + 1;
**27.** end
**28.** end
**29.** set the image with the new values and save it as img

**End**

The LSB data embedded mechanism was improved through making a harmony between the number of bits used in embedding the concealed text and the number of bits used in embedding the cover file. The block-schematically of data embedding using the proposed LSB approach is illustrated in Figure (4.3).

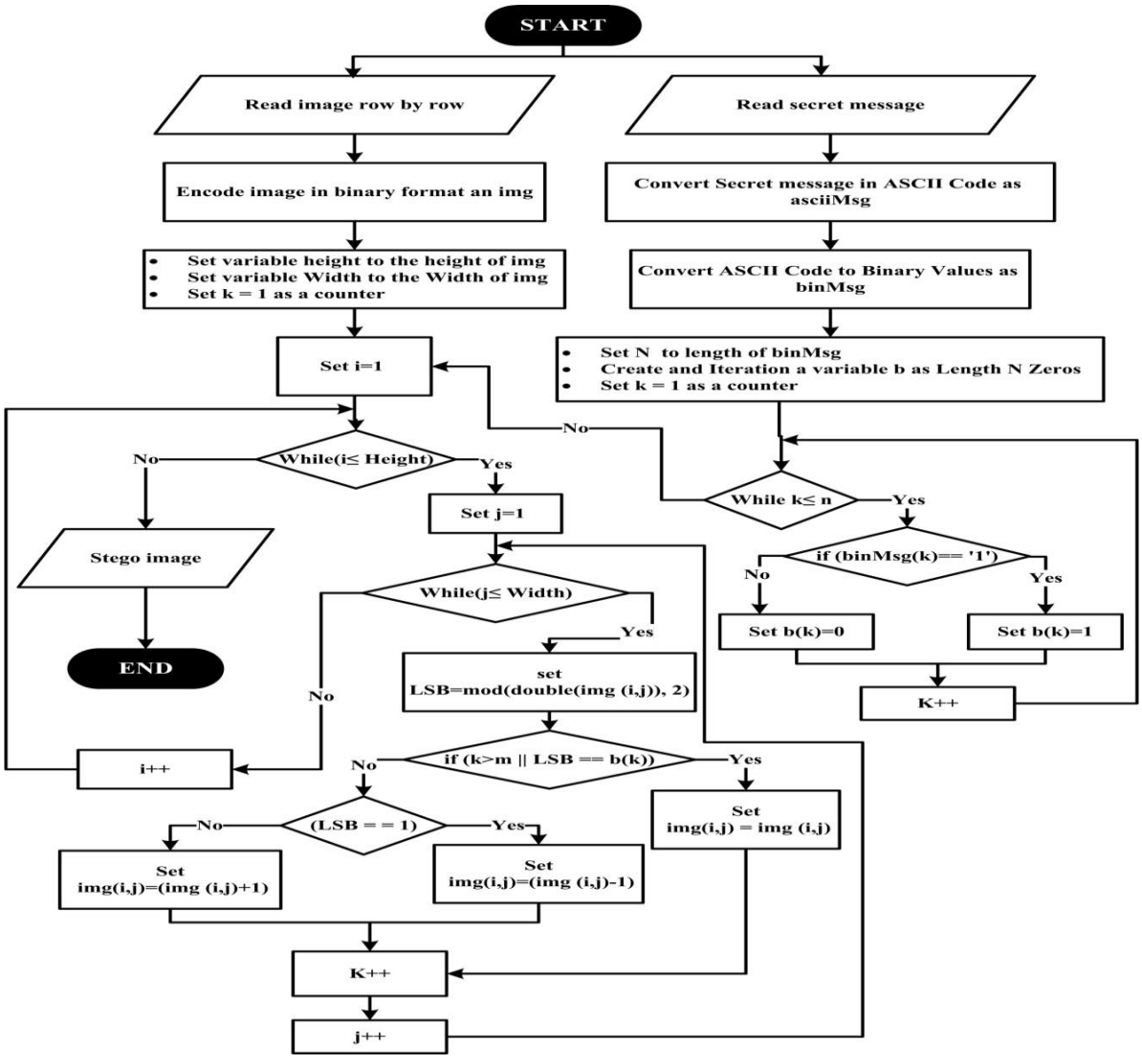



**Figure (4.3):** A block schematically of data embedding using the proposed LSB approach.

### b. Text Recovery Procedure by Evolved LSB

After incorporating the text into the cover file (the stego image), it will be recovered through using the recovery procedures. It is important to identify the stego image to uncover the message bits, rather than the secret text noumenon. In order to generate the text message, the recipient requires getting access to the chain of pattern binary matrix that was used in embedding the procedure. This algorithm used in text recovery based on the LSB is described below. Two parts are involved in that algorithm. In the first part (i) the stego image is scan and row by row and encoded into binary image, and in the second part (ii) the secret message is retrieved. The procedures used in text message recovery is illustrated in Figure (4.4).

***"Extraction Algorithm (2): Least Significant Bit Hiding Algorithm (LSB)":***

**Input**: Stego image. **Output**: Retrieved secret message, cover image. **Variables**: s represent binary values of stego image; s(i,j) represent original image ; k represent counter.

**Begin**

```
scan the image (row by row) and encode it in binary as s
read height of s
read width of s
Define flag m = double ( s(1:1:1) ) * 8 ;
Define Counter as k = 1;
for i = 1 to height
for j = 1 to width
if (k <= m)
Set b(k) = mod (double(s(i,j)),2);
    Increase k = k + 1;
        end
   end
end
Define binary Vector = b;
Convert the secret message from binary Vector to ASCII Code as below
    Set defaulte values binValues = [ 128 64 32 16 8 4 2 1 ];
        if mod(length(binaryVector),8) ~= 0
                error ('Length of binary vector must be a multiple of 8.');
```

| | |
|---|---|
| **19.** | end |
| **20.** | bin Matrix = reshape(binaryVector,8,[]); |
| **21.** | Convert the secret message from ASCII Code to text |
| **22.** | Return Retrieved secret message |
| **End** | |

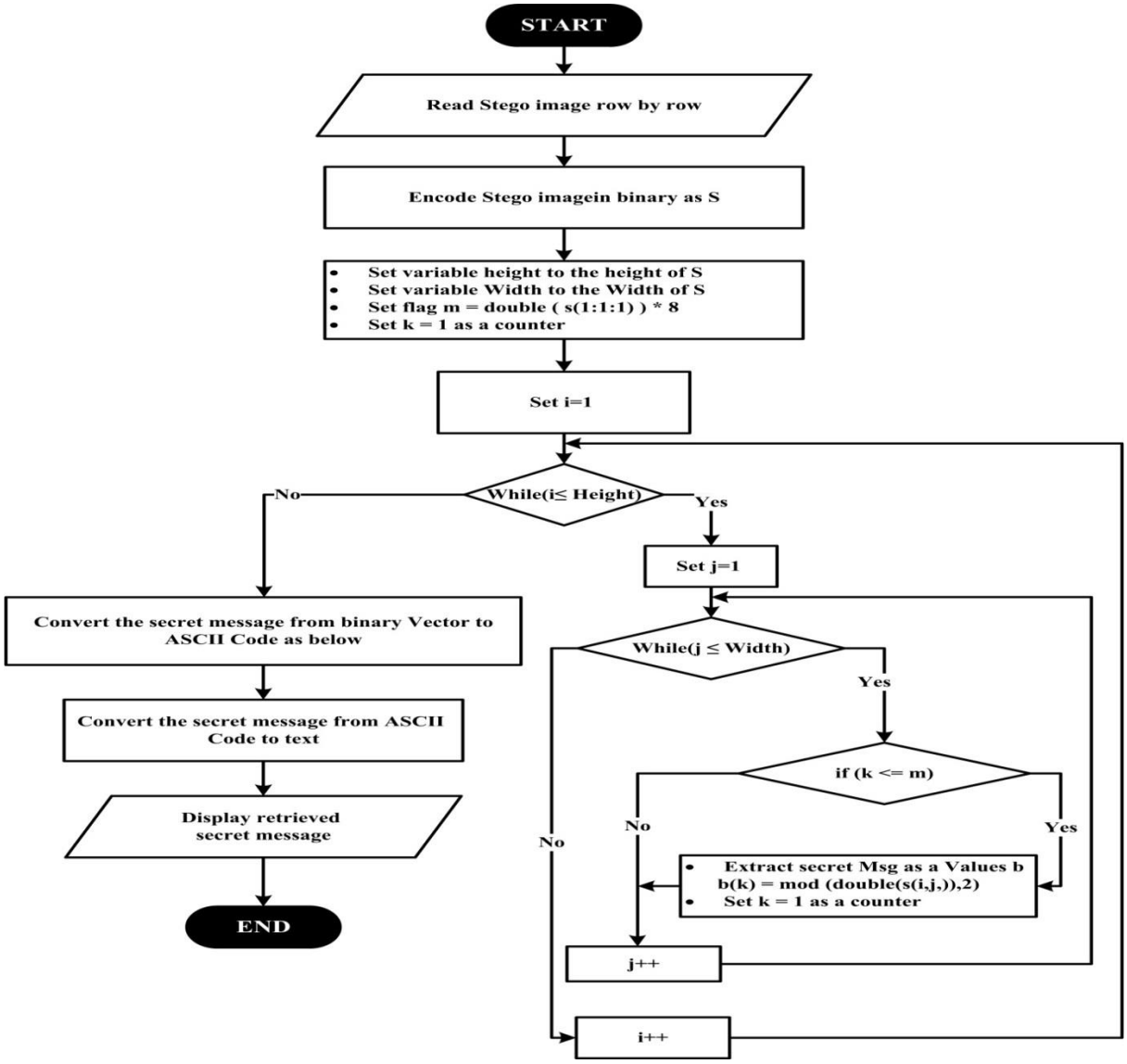



**Figure (4.4)**: A block schematically of procedures used in data recovery with the proposed LSB approach.

### 4.2.1.2. Incorporation Mechanism and Recovery Mechanism by Evolved 2D-DWT-2L

The DWT block fundamentally computes the DWT per column of a frame-based input. Hypothetically, the output is a sample based vector or matrix with the same dimensions as the input. DWT is a mathematical tool that translates an image form the spatial domain to frequency domain. The transformation is developing consequent of small waves, called wavelets, of varying frequency and limited duration. The 1D wavelets transform becomes stretching to a 2D wavelet transform utilizing dissociable wavelet filters. With dissociable filters the 2D transform, becoming calculated by implementing a 1D transform for per the rows of the input, and then redundancies for per the columns. We implemented a Haar DWT, which is the simplest form of DWT. Throughout, Haar DWT the reduced hesitation wavelet coefficient is generated via averaging the two pixel values and the high hesitation coefficients are generated via pick up half of the variance of the analogous two pixels. Our proposed mechanism of a 2D Haar DWT 2level is prescribed in the following:

#### a. Incorporation Mechanism by Evolved 2D-DWT - 2Level

The incorporation mechanism of encoding was improved using 2D-DWT-2L technique as describe in Figure (4.5). In this approach the Haar DWT was implemented. The 2D Haar DWT comprises of two processes: One is horizontal process and the vertical processes. Secret text is transformed into an ASCII format, and then the secret text is divided into even and odd values. The theory

of the odd and the even stenographer (decimation) and up sampling (interpolation) is necessary in handling with finite-length signals. The odd values are concealed in vertical coefficients; therefore, iteration is carried out on odd values with index k (secret message). Consequently, the odd values are set in CV2. The even values are concealed in diagonal coefficients; therefore iteration is performed on even values with index k (secret message). Consequently, the even values are set in CD2. The idwt2 instruction executes a single-level 2D wavelet reconstruction. The CODED is computed using the single level reconstructed approximation by calling the idwt2 for first level and get idec1. Consequently, the CODED is computed for the single level reconstructed approximation by calling idwt2 for second level and get main decoded restore CODED as Stego image. The algorithm used in the incorporation (hiding) mechanism by evolved 2D-DWT-2L is described below.

***"Embedding Algorithm (3): Discrete Wavelets Transform Hiding Algorithm -2Levels (2D- DWT-2L)":***

**Inputs**: cover image, secret message. **Output**: Stego image.

**Begin**

**1.** scan the image row by row as img
**2.** convert the secret message in ASCII Code as asciiMsg
**3.** computes the 2-L wavelet for first level by haar filter
**4.** result of DWT first level coefficients matrix CA1 and details coefficients matrices CH1, CV1, CD1,obtained by a wavelet decomposition of img
**5.** make new matrix of all coefficients dec1
**6.** computes the 2-L wavelet for second level on dec1 by haar filter
**7.** result of DWT first level coefficients matrix CA2 and details coefficients matrices CH2, CV2, CD2, obtained by a wavelet decomposition of img
**8.** Divide asciiMsg to odd and even
- Hide odd values in vertical coefficients
  Iteration on odd values with index k
    Set CV2(i,k) = odd values
  end

- Hide even values in diagonal coefficients
  Iteration on even values with index k
  Set CD2(i,k) = even values
  end

**9.** compute CODED the single level reconstructed approximation by calling idwt2 for first level and get idec1

**10.** compute CODED the single level reconstructed approximation by calling idwt2 for second level and get main decoded

**11.** return CODED as stego image

**End**

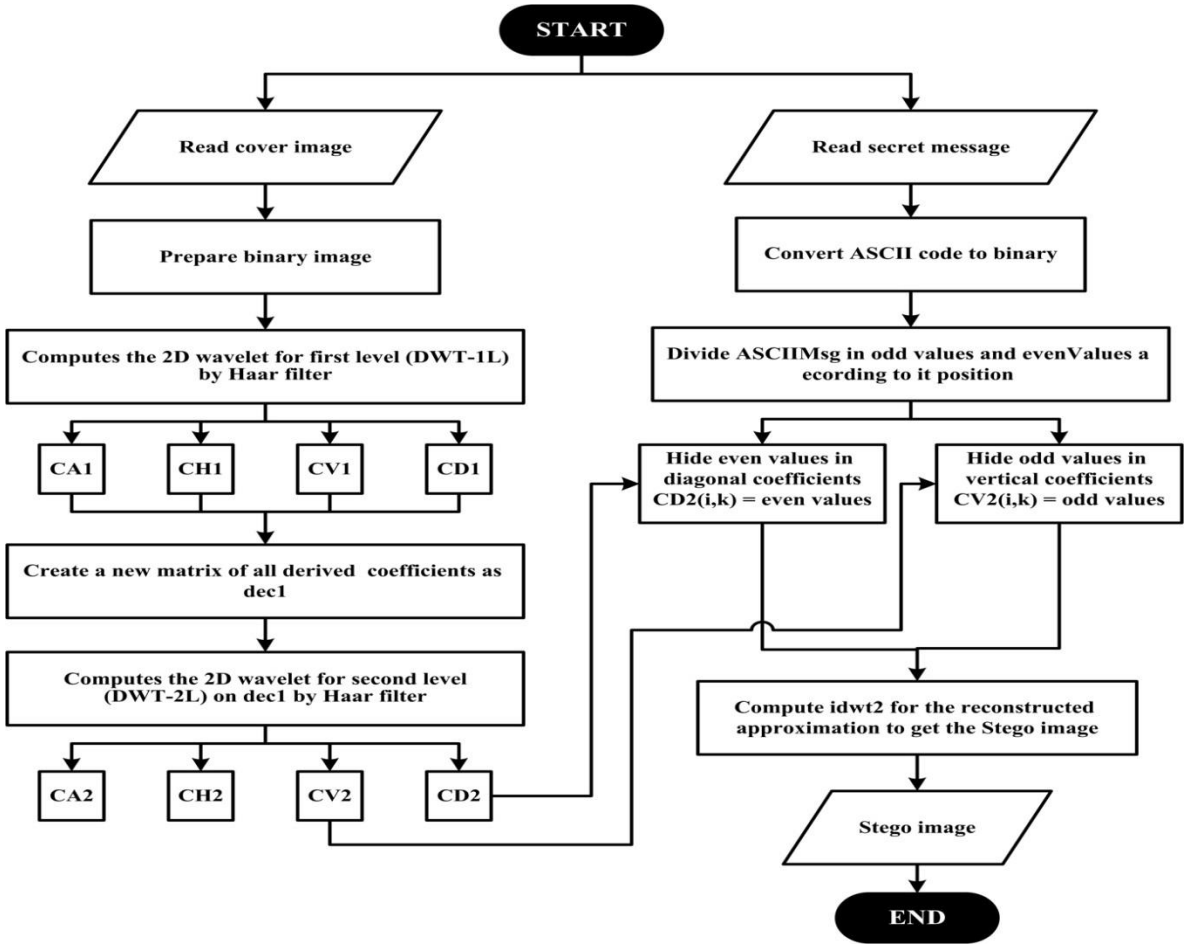



**Figure (4.5):** A block-schematically of data embedding mechanism by evolved 2D-DWT-2Level.

## b. Text Recovery Procedure by Evolved 2D-DWT- 2L

After incorporating the text into the cover file, the procedures described in Figure (4.6) is used to retrieve the embedded secret message. In this process, the recipient has to receive the stego image, that image is scanned as CODED, and then the proposed 2D-DWT-2 level technique is carried on to extract the secret message. The algorithm used in extracting the embedded data is described below.

***"Extraction Algorithm (4): Discrete Wavelets Transform Hiding Algorithm -2Levels (2D-DWT-2L)":***

**Input**: Stego image. **Output**: Retrieved secret message.

**Begin**

**1.** scan the stego image as CODED
**2.** computes the 2-L wavelet for first level by haar filter
**3.** result of DWT first level coefficients matrix CA1 and details coefficients matrices CH1, CV1, CD1, obtained by a wavelet decomposition of img
**4.** make new matrix of all coefficients dec1
**5.** computes the 2-L wavelet for second level on dec1 by haar filter
**6.** result of DWT first level coefficients matrix CA2 and details coefficients matrices CH2, CV2, CD2, obtained by a wavelet decomposition of img
**7.** prepare msg = '';
**8.** Divide asciiMsg to odd and even
- Hide odd values in vertical coefficients
Iteration on odd values with index k
Set msg = CV2(i,k) ;
end
- Hide even values in diagonal coefficients
Iteration on even values with index k
Set msg = CD2 (i,k) ;
end
**9.** decode msg Ascii Code to be text
**10.** return msg as Stego image

**End**

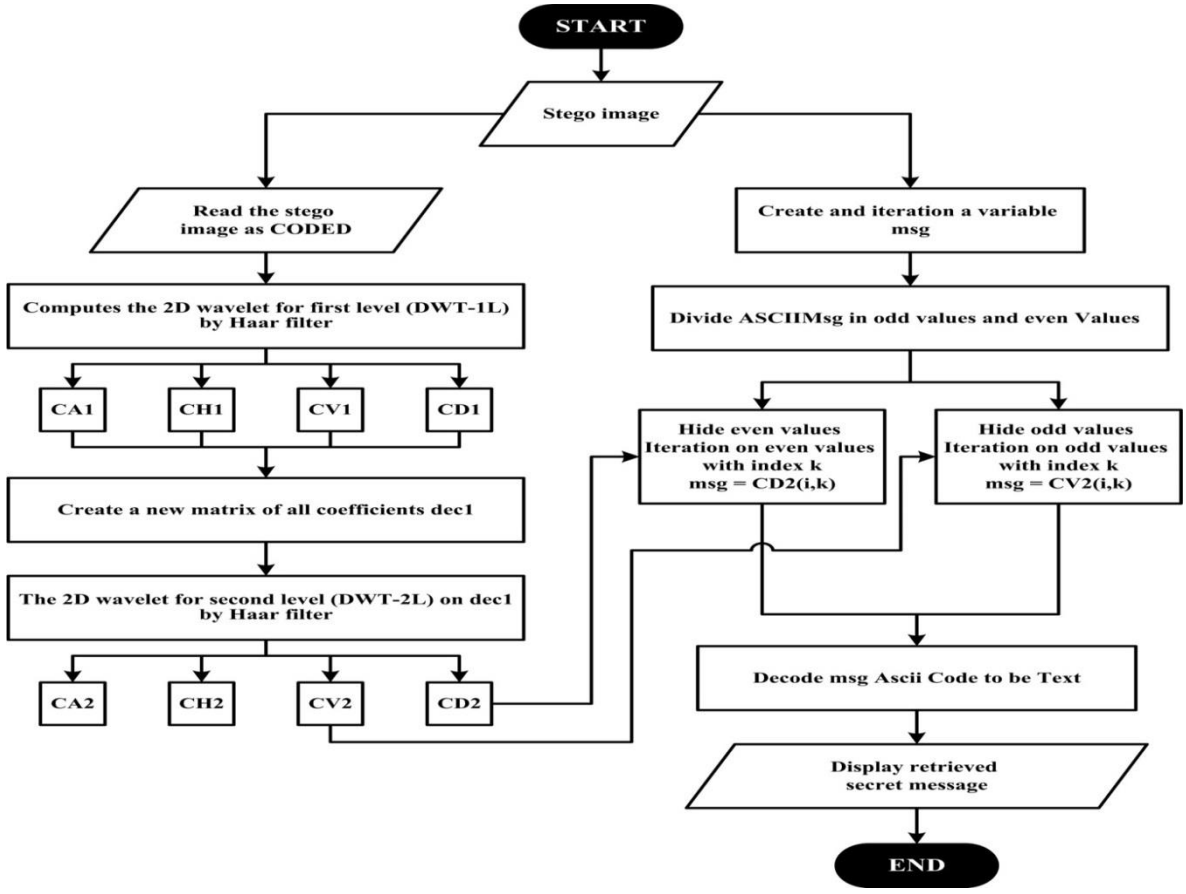



**Figure (4.6):** A block schematically of data recovery mechanism by evolved 2D-DWT-2Level.

### 4.2.2. Design the Proposed System (*Only Hybrid Encryption Algorithm*)

In previously mentioned algorithms, we were dealing with the text as plain text, which will be to be admitted to the concealment techniques to hide it in the selected cover. In this part, we will deal with the text as it will be encrypted using the hybrid (AES and RSA) and then it will be admitted to the

same concealment techniques. In other words, the text will be encrypted first and then it will be hidden. The cryptosystem is originated to shield secret message and image which broadcasted over the channel of broadcast against any assault.

In this section, we propose a substitute transmission system that uses cryptography (symmetric and asymmetric) and steganography to secure and conceal the secret text when transmitted through insecure transmission channels.

#### 4.2.2.1. The Proposed Hybrid Security Algorithm

The asymmetric algorithms are much slower than that the symmetric algorithms, particularly with large amounts of data. In contrast, using the symmetric algorithm as a key distribution is considered a problem because it can't prove the authenticity. Consequently, integrating both the symmetric and asymmetric encryption algorithms eliminates the drawbacks of these algorithms. In this work, a hybrid encryption algorithm was implemented to improve the performance of the (AES and RSA) encryption algorithms to overcome the limitations of each. Also, a hybrid encryption algorithm take an advantage of the strengths of each form of encryption (i.e., the safety of the asymmetric encryption and the speed of the symmetric encryption).

### a. Text Incorporation Procedure Using the Hybrid (AES and RSA) Encryption Algorithm

The proposed Hybrid (AES and RSA) encryption algorithm contains a combination of keys as illustrated in Figure (4.7). The details of that algorithm are described in the following:

***"Encryption Algorithm (5): Hybrid (AES & RSA) Algorithm" .***

**Inputs**: plain (text) message.
**Output**: main_cipher message , key **s**

**Begin**
**1.** Divide plain msg into two parts (Odd_Msg , Even_Msg)
**2.** Generate new AES key s
**3.** Encrypt Odd_Msg by AES-128 using s
**4.** Return Encryption 1
**5.** Print Encryption 1 (The output of the AES-128 algorithm)
**6.** Generate new RSA key (public = m) and (private = x)
**7.** Encrypt Even_Msg by RSA using (public = m)
**8.** Return Encryption 2
**9.** Print Encryption 2 (The output of the RSA key (public = m)algorithm)
**10.** Build Encryption 3 cipher message by (Encryption 1, Encryption 2)
**10.1.** Loop on All Char
**10.2.** If odd
- Get cipher values Encryption 1
- Add to Encryption3
**10.3.** Else then even
- Get cipher values Encryption 2
- Add to Encryption 3
**10.4.** End of Loop
**11.** Print Encryption 3
**12.** Encrypt RSA key (private = x) by AES-128 using s
**13.** Return Encryption4
**14.** Print Encryption 4
**15.** Compress Encryption3 by convert to hashs
**16.** Compress Encryption4 by convert to hashs
**17.** Define message empty main_cipher = ""
**18.** Add Encryption3 to main_cipher
**19.** Add Encryption4 to main_cipher
**20.** Return main_cipher and s
**End**

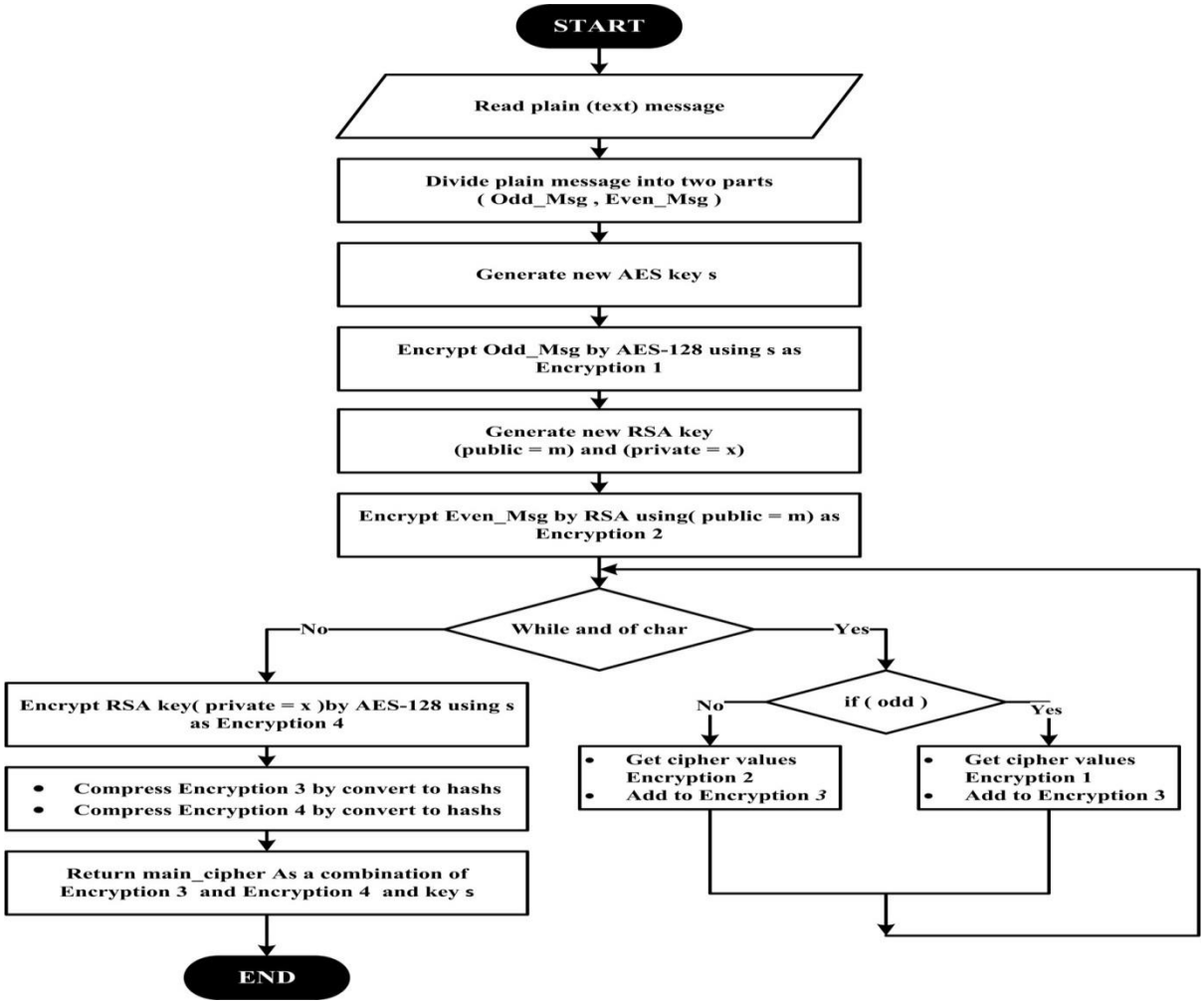



**Figure (4.7):** A block schematically of hybrid (AES and RSA) encryption algorithm.

### b. Text Incorporation Procedure Using the Hybrid (AES and RSA) Decryption Algorithm

Decryption refers to the process of converting the encrypted data back to user well known format, which is reverse of the encryption process. The original data can be retrieved back when the correct key is used during the decryption

process, while using the wrong key results in wrong data. The encryption part is carried out in the opposite direction form a successful decryption. The same key used by the sender has to be used over the cipher text throughout the encryption process. The proposed decryption algorithm is illustrated in Figure (4.8) and described in the following:

***"Decryption Algorithm (6): Hybrid (AES & RSA) Algorithm".***

**Inputs**: main_cipher message , key s
**Output**: plain (text) message.

**Begin**
**1.** Divide plain main_cipher into two parts (Encryptionb 3, Encryption 4)
**2.** Decompress Encryption 3
**3.** Decompress Encryption 4
**4.** Decrypt Encryption 4 by AES-128 using s
**5.** Return RSA key (private = x)
**6.** Define Encryption 1 , Encryption 2
**7.** Loop on All Char in Encryption 3
  **6.1.** If odd
    - Add to *Encryption 1*
  **6.2.** Else then even
    - Add to *Encryption 2*
  **6.3.** End of Loop
**8.** Decrypt Encryption1 by AES-128 using s
**9.** Return Odd_Msg
**10.** Print Decryption1 AES Odd_Msg
**11.** Decrypt Encryption 2 by RSA using (public = m)
**12.** Return Even_Msg
**13.** Print Decryption2 RSA Even_Msg
**14.** Define main_plain message
**15.** Loop on All Char
  **15.1.** If odd
    - Get cipher values Encryption1 and Odd_Msg
    - Add to main_plain
  **15.2.** Else then even
    - Get cipher values Encryption2 and Even_Msg
    - Add to main_plain
  **15.3.** End of Loop
**16.** Return main_plain (text) message
**End**

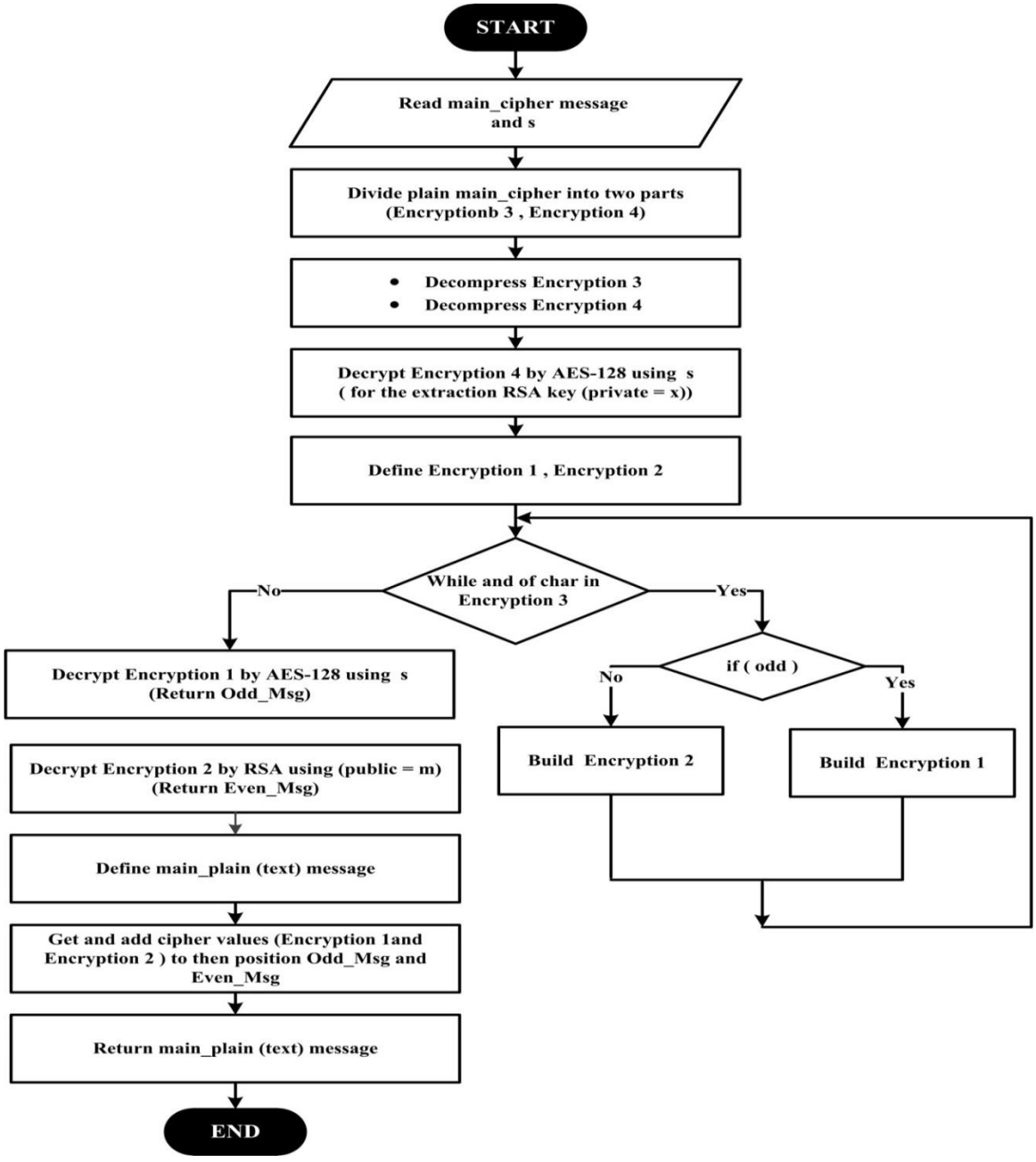



**Figure (4.8):** A block schematically of Hybrid (AES and RSA) Algorithm decryption.

### 4.3. Evaluation Parameters

Eight statistical parameters were used in this work to evaluate the quality of the proposed systems in hiding a secret message. These parameters are described below:

1. **Peak Signal to Noise Ratio (PSNR)**: It used to access the quality of stego image with respect to the original image. It calculates the imperceptibility of the stego image. In other words, it calculates and analyzes the similarity between the two images, where the higher the PSNR value of a stego image, the higher the quality of that image or a higher imperceptibility of the hidden message [96]. The PSNR is calculated according to the following equation:

$$\mathrm{PSNR} = 10 \log_{10} \left[ \frac{\mathrm{I}^2}{\mathrm{MSE}} \right] \qquad (4.1)$$

   where, I represents the maximum possible value of the pixel in the image (e.g., for a gray scale image the maximum value is 255) and MSE is the mean square error.

2. **Mean Square Error (MSE)**: It calculates the magnitude of average error between both the original and the stego images. The difference between the observed values of the original and stego image are squared and then their average is calculated [97]. The RMSE is mainly utilized when large errors exist, where it provides relatively high weight to these errors. The MSE is calculated according to the following equation:

$$MSE = \frac{1}{[R \times C]^2} \sum_{i=0}^{n} \sum_{j=1}^{m} (X_{ij} - Y_{ij})^2 \qquad (4.2)$$

where, R and C are the number of rows and columns in the cover image, $X_{ij}$ is the intensity of the $X_{ij}$ pixel in the cover image, and $Y_{ij}$ is the intensity of the $Y_{ij}$ pixel in stego-image.

3. **Mean Absolute Error (MAE):** It a quantity used to measure how close predictions are to the eventual outcomes. The MAE is on the same scale of data being measured. It measures accuracy of continuous variables. The MAE is the average over the verification sample of the absolute values of the differences between forecast and the corresponding observation. It provides a linear score which means that all the individual differences are weighted equally in the average [98]. The MAE is calculated using the following equation:

$$MAE = \frac{1}{n} \sum_{i=1}^{n} |f_i - y_i| \qquad (4.3)$$

where, $f_i$ is the predicted value and $y_i$ is the true value. Note that alternative formulations may include relative frequencies as weight factors.

4. **Bit Error Ratio (BER)**: It the number of bits received in error divided by the total number of bits transferred. The BER can be estimated by calculating the probability that a bit will be incorrectly received due to noise. The BER is a simple concept its definition can be recognized from the following equation [99]:

$$\text{BER} = \text{Errors} / \text{Total Number of Bits} \qquad (4.4)$$

5. **Signal to Noise Ratio (SNR)**: It defined as the ratio of the power of a signal to that of a background noise or in other words the ratio of the meaningful information to the unwanted signal. The SNR is generally used in engineering and science that make a comparison between the levels of a desired signal to that of a background noise. It is computed according to the following equation [100]:

$$\text{SNR} = \frac{P_{\text{signal}}}{P_{\text{noise}}} \qquad (4.5)$$

where, P is average power.

6. **Structural Similarity (SSIM)**: It an index that measures the structural similarity between two images. Its value ranges between -1 and 1. When two images are nearly identical, their SSIM is close to 1. Accordingly, it is used

as a method for measuring similarity between two images. The following formula is used to compute the SSIM between two sequences seq1 and seq2 at a given pixel P [101]:

$$\text{SSIM} = \frac{2 * mu_1(p) mu_2(p) + c_1}{mu_1(p)^2 + mu_2(p)^2 + c_1} x \frac{2 * cov(p) + c_2}{s_1(p)^2 + s_2(p)^2 + c_2} \quad (4.6)$$

where, $mu_1(P)$ and $mu_2(P)$ are the mean value of seq1 and seq2 computed over a small XY window located around P, $s_1(P)$ and $s_2(P)$ are standard deviation of seq1 and seq2 computed over the same window, cov(P) is the covariance between seq1 and seq2 is computed over the same window, $C_1 = (K1*L)^2$ is a regularization constant (should be as small as possible, $C2 = (K2*L)^2$ is a regularization constant (should be as small as possible), K1 and K2 are regularization parameters (must be >0), and L is a dynamic range of the pixel values (example: L=255 if the sequence is 8 bit encoded). The default window is a Gaussian window with standard deviation of 1.5 along both the X and the Y axis.

7. **Structural Content (SC)**: It a correlation based measure, where it also measures the similarity between two images. It is calculated according to the following equation [102]:

$$sc = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} \left(y(i,j)\right)^2}{\sum_{i=1}^{M} \sum_{j=1}^{N} \left(x(i,j)\right)^2} \qquad (4.7)$$

where, x (i, j) represents the original image and y (i, j) represents the distorted image.

8. **Correlation:** It reaches its maximum when the two signals are similar. It is equivalent to multiplying the complex conjugate of frequency spectrum of one signal by the frequency spectrum of the other. It determines how much two signals or vectors are similar or different in phase and magnitude when two sets of data are strongly linked together. The linearcorrelation coefficient (r) ranges between -1 and 1. It is calculated by using the following equation[103]:

$$\text{Correlation} = \frac{n \sum xy - (\sum x)(\sum y)}{\sqrt{n(\sum x^2) - (\sum x)^2}\ \sqrt{n(\sum y^2) - (\sum y)^2}} \qquad (4.8)$$

where, n is the number of pairs of data, X is the input image and y is the stego image.

## 4.4. Summary

In this chapter, the framework of our proposed data hiding technique was fully described. The layout of the system phases is illustrated in diagrams and the steps of our data hiding algorithm are well described in this chapter. The innovation of our system is in combination of steganography and hybrid encryption algorithm, to ensure highly secured data transition and communication in the near future. The integration between steganography and cryptography provides a very powerful tool which allows people to communicate without possible eavesdroppers. The parameters used in evaluating our proposed system (PSNR, MSE, MAE, BER, SNR, SSIM, SC, and Correlation) are also described in this chapter. The advantages of the proposed system are represented in providing greater embedding capacity, more security, more flexibility and invisibility, based on the studied evaluation parameters.

In the next chapter, the will present and analysis of experimentation results their discussions.

# CHAPTER 5

## Experimental Results and Their Discussions

This chapter presents the results of all the experiments that were carried out in this thesis and their discussions. This chapter is organized in six sections; Section 1 discuss the execution environment; Section 2 introduce the modules of the proposed system; Section 3 presents the experimental results: i - Only steganography technologies (proposed LSB technique and proposed 2D-DWT-2L technique). ii - Steganography and hybrid encryption algorithm: (Proposed LSB technique with hybrid (AES and RSA) and Proposed (2D-DWT-2L) with hybrid (AES and RSA)); Section 4 introduce the comparing of the results of our proposed techniques companied with other results ; Section 5 discuss advantages of the system and Section 6 the Summary.

### 5.1. Execution Environment

In this work, a comparison is carried out between the original image file (cover image) and the stego image coming after performing the proposed techniques. Also, the hidden text is analyzed before being transmitted and after being received by the intended recipient. This is to make sure that less distortion happens to the original cover file after embedding the secret text. Furthermore, eight statistical parameters (PSNR, MSE, MAE, BER, SNR, SSIM, SC, and Correlation), were also calculated to evaluate the obtained results from the

proposed approaches based on statistical values. Our proposed techniques were operated on both color and grayscale images in two images formats (.bmp and .jpeg) as represented in Figure (5.1). The size of the tested cover files varied between 1 to 256 bytes.

The proposed techniques in this work were preformed on different message sizes and lengths. These messages were hidden in some grayscale and color (RGB) cover images obtained from http://sipi.usc.edu/database/database.php .2011 . These methods were implemented using MATLAB (ver. R2015a) software package running on a personal computer with a 2.27 GHz Intel (R) Core (TM) I3 CPU, 8 GB RAM and windows 7 as the operating system.

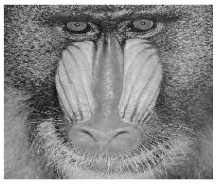
| a - Color image of size dimensions (512*512) and file format (.bmp) | | | | |
|---|---|---|---|---|
|  |  |  |  |  |
| Lana | Baboon | Pepper | Barbara | Jet(f16) |
| b – Gray scale image of size dimensions (256*256) and file format (.jpeg) | | | | |
|  |  |  |  |  |
| Lana | Baboon | Pepper | Barbara | Jet (f16) |

**Figure (5.1):** Specifications of covers files used in the experimental work.

## 5.2. Modules of the Systems

The proposed systems integrate three modules that together constitute the experimental application of our system as follow:

- **The First Frame**: Is text encryption or decoding encryption using encryption algorithms only. This frame is illustrated in Figure (5.2). In this frame, the text is select in the form of .txt file format, then one of the encryption algorithms is selected, the encryption process is executed on the text, and finally, the decryption process is also executed in the same frame to measure the quality and speed of the proposed technique. It is good to mention that the encryption key is saved in a special file that is only used by the recipient person.

- **The Second Frame:** Is embedded or extraction text from the image using Steganography techniques only. This frame is illustrated in Figure (5.3). in this frame, the cover image is selected and the text file is also selected, then one of the stenography techniques is selected and executed on the selected text to embed it in the cover image, the histogram for both the cover image before and after embedding the text file is displayed in fame, the hidden text is retrieved in the same frame to measure the quality and speed of the process, and finally, display the hidden text before and after performing the stenography process. The values of the statistical parameters used in evaluating the quality of the proposed techniques show up in the same frame.

- **The Third Frame:** Is encrypting and embedded, then decoding and extraction text from the image using encryption and steganography techniques together. This frame is represented in Figure (5.4). This frame makes an integration of the first and second frames. However, in this frame the selected text is first encrypted using the hybrid algorithm, and then it is embedded using one of the proposed stenography techniques. It is also good to mention that the final encryption key is saved in a special file that is only used by the recipient person.

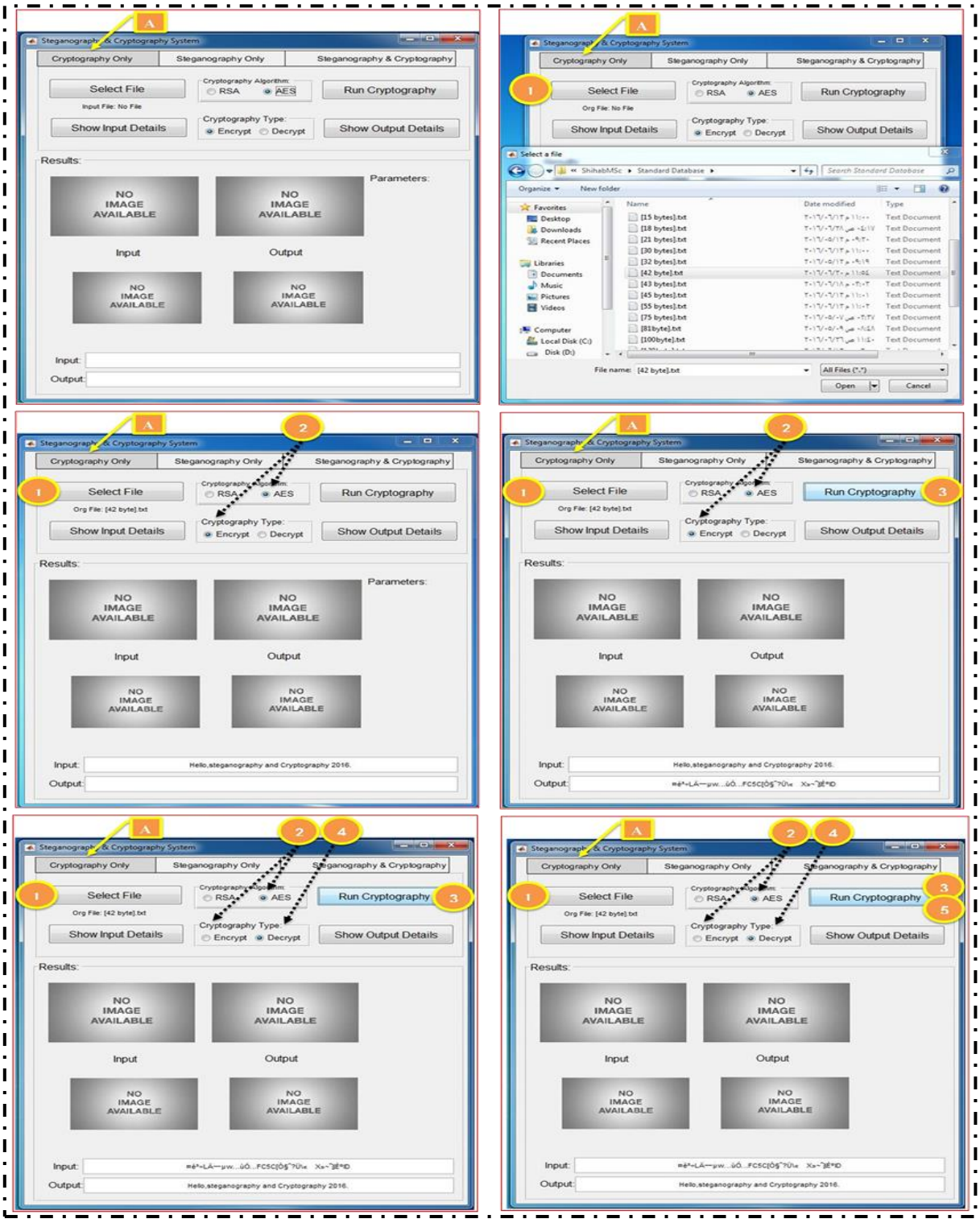



**Figure (5.2):** First frame for text encryption or decoding encryption with encryption algorithms only.

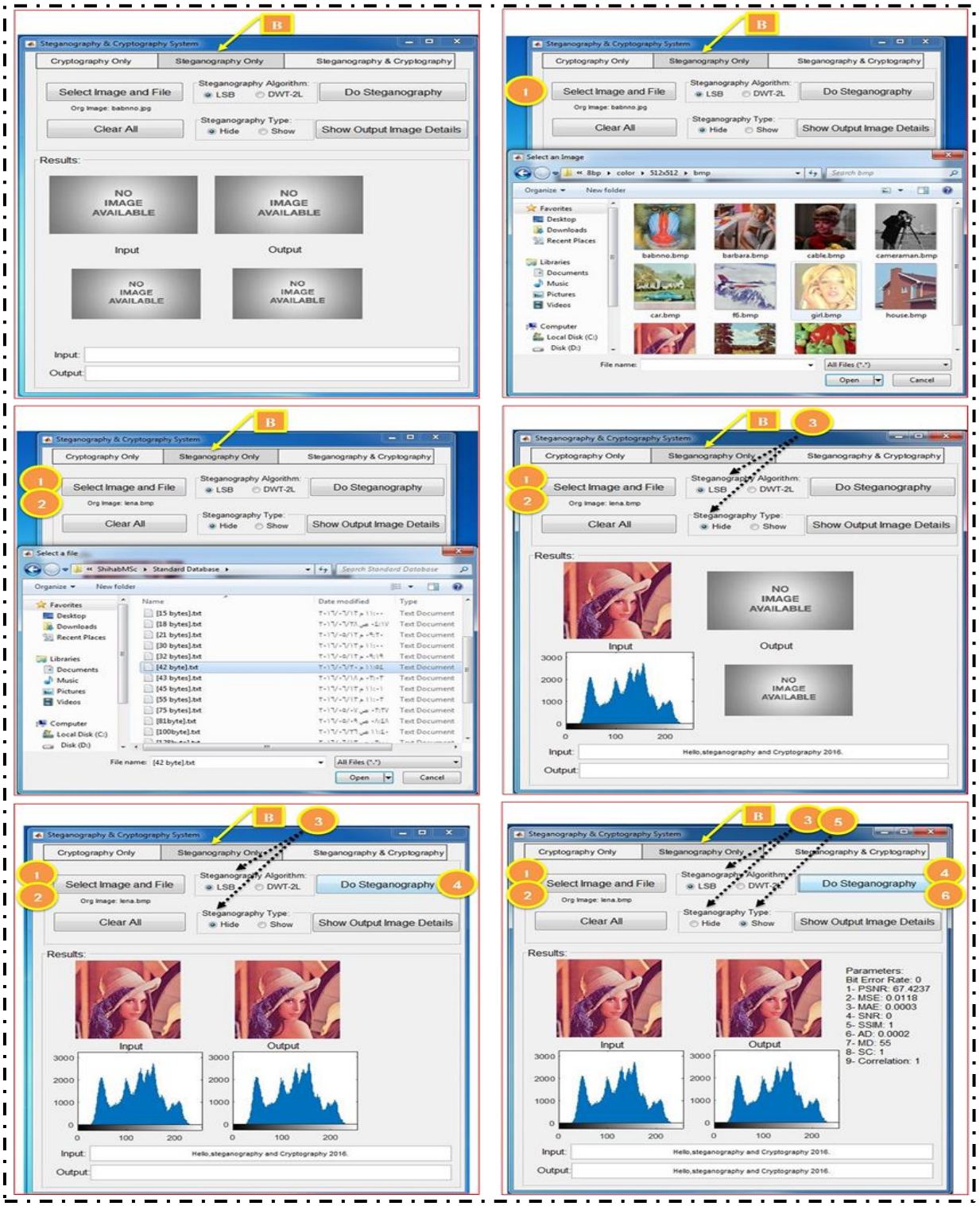



**Figure (5.3):** Second frame for text embedding or extraction using Steganography techniques only.

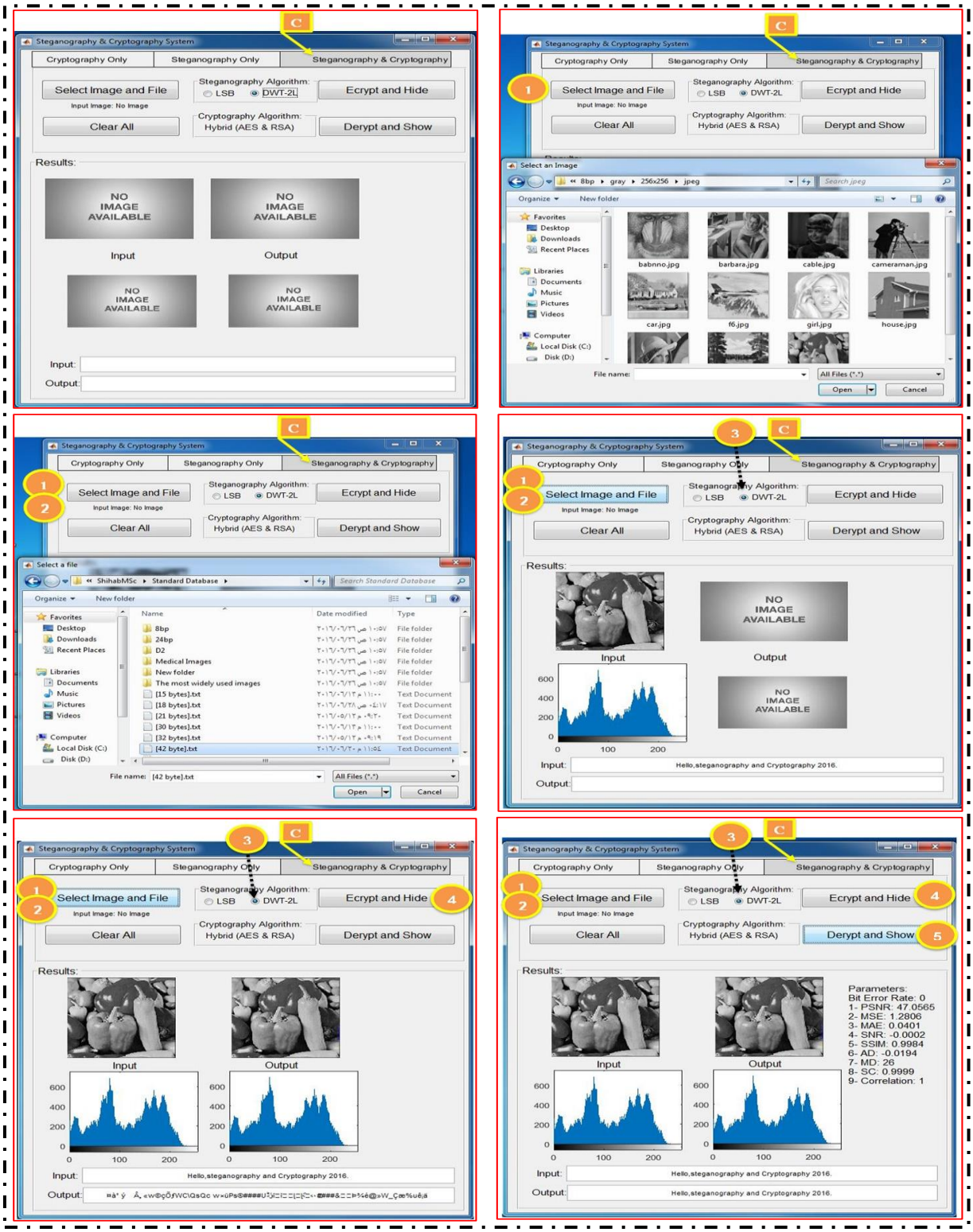



**Figure (5.4):** Third frame for text encryption and embedding then decoding and extraction using both encryption and steganography techniques.

## 5.3. Experimental Results

### 5.3.1. Experimental Results of the Proposed LSB Technique

Table (5.1) shows the obtained results from implementing the proposed LSB technique on the tested color and grayscale images using different text sizes. It was noticed that both the BER and SNR give the value of zero with all the studied images (color and grayscale), which indicates that the number of bits received in error is zero. It was observed that the PSNR values were increased by increasing the text size with each of the tested color images except with pepper image. The obtained PSNR values for color images varied from 66.29 to 88.33. This reveals a higher quality of stego image, where the similarity between the original image and the stego image decreases by increasing the text size. This is generally true when there is lots of a color variation in the cover image, but when the numbers of colors are limited as in the pepper image the PSNR values decrease by increasing the text size. The PSNR values took an opposite trend with the grayscale images, were the values decreased by increasing the text size with the all the tested images except with the pepper image. This agrees with the previously mentioned notation. The obtained PSNR values for grayscale images varied from 65.92 to 86.75.

On the other hand, it was found that values of MSE are decreased by increasing the text size for all the studied color images except the pepper image. In general, the smaller the value of the MSE the higher the quality of the steganography technique. The obtained MSE values for the color images ranged between 0.0001 and 0.0153. It could also be concluded that the MSE is also

correlated with the number of color variations in the cover image, where the larger the color variations the smaller the MSE value. With the grayscale images, there wasn't a general trend with the MSE values. These values varied from one image to another. For both Lena and Barbara images the lowest MSE values were obtained when a 128 byte text size was used, whereas the highest values were obtained when a 256 byte text size was used. In contrast, both of the Baboon and Jet (f16) images the lowest MSE values were obtained when a 100 byte text size was used, whereas the highest values were obtained when a 256 byte text size was used. The pepper images took another trend, where the lowest MSE values were obtained when a 256 byte text size was used, whereas the highest values were obtained when a 128 byte text size was used. Accordingly, it could be concluded that the MSE values for the grayscale images vary for one image to another based on the histogram of pixel values in each image, either they equally distribution along the grayscale or they are not.

MAE parameter shows very small values; which ranged between 0 and 0.0008 with both color and grayscale images. This indicates no significant difference between the cover and stego image. The last three parameters (SSIM, SC and Correlation) take a value of one or very close to one with all the studied images (color and grayscale). This indicates a very high correlation between both the cover and stego image.

**Table (5.1):** Results of statistical parameters obtained from applying the LSB approach on both color and grayscale images with different text sizes.

| **Color Images (512*512), .bmp** | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Image Name** | **Text Size (byte)** | **PSNR** | **MSE** | **MAE** | **BER** | **SNR** | **SSIM** | **SC** | **Correlation** |
| **Lena** | 15 | **66.29** | **0.0153** | **0.0003** | **0** | **0** | **1** | **1** | **1** |
| | 30 | 66.98 | 0.0130 | 0.0003 | 0 | 0 | 1 | 1 | 1 |
| | 45 | 67.56 | 0.0114 | 0.0003 | 0 | 0 | 1 | 1 | 1 |
| | 55 | 68.05 | 0.0102 | 0.0003 | 0 | 0 | 1 | 1 | 1 |
| **Baboon** | 15 | 69.40 | 0.0075 | 0.0002 | 0 | 0 | 1 | 1 | 1 |
| | 30 | 70.17 | 0.0062 | 0.0002 | 0 | 0 | 1 | 1 | 1 |
| | 45 | 71.24 | 0.0049 | 0.0003 | 0 | 0 | 1 | 1 | 1 |
| | 55 | 71.97 | 0.0041 | 0.0002 | 0 | 0 | 1 | 1 | 1 |
| **pepper** | 15 | **88.33** | **0.0001** | **0** | **0** | **0** | **1** | **1** | **1** |
| | 30 | 83.23 | 0.0003 | 0 | 0 | 0 | 1 | 1 | 1 |
| | 45 | 79.39 | 0.0007 | 0 | 0 | 0 | 1 | 1 | 1 |
| | 55 | 77.70 | 0.0011 | 0 | 0 | 0 | 1 | 1 | 1 |
| **Barbara** | 15 | 68.31 | 0.0096 | 0.0002 | 0 | 0 | 1 | 1 | 1 |
| | 30 | 69.00 | 0.0082 | 0.0002 | 0 | 0 | 1 | 1 | 1 |
| | 45 | 69.97 | 0.0065 | 0.0002 | 0 | 0 | 1 | 1 | 1 |
| | 55 | 70.57 | 0.0057 | 0.0002 | 0 | 0 | 1 | 1 | 1 |
| **Jet(f16)** | 15 | 68.48 | 0.0092 | 0.0002 | 0 | 0 | 1 | 1 | 1 |
| | 30 | 69.17 | 0.0079 | 0.0003 | 0 | 0 | 1 | 1 | 1 |
| | 45 | 70.11 | 0.0063 | 0.0003 | 0 | 0 | 1 | 1 | 1 |
| | 55 | 70.77 | 0.0054 | 0.0003 | 0 | 0 | 1 | 1 | 1 |
| **Grayscale Images (256*256), . jpeg** | | | | | | | | | |
| **Image Name** | **Text Size (byte)** | **PSNR** | **MSE** | **MAE** | **BER** | **SNR** | **SSIM** | **SC** | **Correlation** |
| **Lena** | 100 | 72.21 | 0.0039 | 0.0002 | 0 | 0 | 1 | 1 | 1 |
| | 128 | 78.23 | 0.0001 | 0.0001 | 0 | 0 | 1 | 1 | 1 |
| | 256 | 63.23 | 0.0309 | 0.0007 | 0 | 0 | 0.9999 | 1 | 1 |
| **Baboon** | 100 | 84.25 | 0.0002 | 0.0001 | 0 | 0 | 1 | 1 | 1 |
| | 128 | 82.31 | 0.0004 | 0 | 0 | 0 | 1 | 1 | 1 |
| | 256 | 65.92 | 0.0166 | 0.0005 | 0 | 0 | 1 | 1 | 1 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **pepper** | 100 | 71.19 | 0.0049 | 0 | 0 | 0 | 1 | 1 | 1 |
| | 128 | 67.99 | 0.0103 | 0 | 0 | 0 | 1 | 1 | 1 |
| | 256 | 74.71 | 0.0022 | 0.0002 | 0 | 0 | 1 | 1 | 1 |
| **Barbara** | 100 | 67.99 | 0.0103 | 0.0004 | 0 | 0 | 1 | 1 | 1 |
| | 128 | 71.68 | 0.0044 | 0.0003 | 0 | 0 | 1 | 1 | 1 |
| | 256 | **61.48** | **0.0462** | **0.0008** | **0** | **0** | **0.9999** | **1** | **1** |
| **Jet(f16)** | 100 | **86.75** | **0.0001** | **0** | **0** | **0** | **1** | **1** | **1** |
| | 128 | 80.73 | 0.0005 | 0 | 0 | 0 | 1 | 1 | 1 |
| | 256 | 66.19 | 0.0156 | 0.0005 | 0 | 0 | 1 | 1 | 1 |

### 5.3.2. Experimental Results of the Proposed 2D-DWT-2L Technique.

Table (5.2) shows the obtained results from carrying out the proposed 2D-DWT-2L technique on the tested color and grayscale images using different text sizes. Similar to the obtained results with the LSB both of the BER and SNR give the same value of zero with all the studied images (color and grayscale. However, it was noticed that the PSNR values were decreased by increasing the text size with each of the tested color images. The obtained PSNR values for color images varied from 69.12 to 62.54. This indicates that the quality of stego image is impaired by increasing the text size. In other words the similarity between the original image and the stego image increases by increasing the text size. This could be attributed to the segmentation of the original image into four parts and each part is also divided into four more parts. This could limit the variability of pixel values within each part and consequently increase the similarity between the cover image and the stego image. The PSNR values took the same trend as the color images with the 2D-DWT-2L technique, were the PSNR values decreased by increasing the text size with the all the tested images.

The obtained PSNR values for grayscale images varied from 64.90 to 55.97. It was found that MSE values were increased by increasing the text size for all of the studied images (color images and grayscale). This indicates that the image distortion is increased by increasing the text size. The obtained MSE values for the color images ranged between 0.0079 and 0.0362; whereas the MSE values for the grayscale images ranged between 0.0211 and 0.1643.

The values of MAE with the color images were smaller than those obtained with the grayscale images, which could be attributed the relatively high color variability between color and grayscale images. In general, these values were higher than those obtained with the LSB approach. Also, the values of SSIM, SC and Correlation were almost equal to one with all the studied images (color and grayscale), indicating a very high correlation between the cover and stego image.

**Table (5.2):** Results of statistical parameters obtained from performing the (2D-DWT-2L) approach on color and grayscale images with different text sizes.

| **Color Images (512*512), .bmp** | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Image Name** | **Text Size (byte)** | **PSNR** | **MSE** | **MAE** | **BER** | **SNR** | **SSIM** | **SC** | **Correlation** |
| **Lena** | 15 | **69.12** | **0.0079** | **0.0014** | **0** | **0** | **0.9999** | **1** | **1** |
| | 30 | 65.79 | 0.0171 | 0.0028 | 0 | 0 | 0.9998 | 1 | 1 |
| | 45 | 63.89 | 0.0265 | 0.0042 | 0 | 0 | 0.9997 | 1 | 1 |
| | 55 | 63.19 | 0.0312 | 0.0051 | 0 | 0 | 0.9997 | 1 | 1 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Baboon** | 15 | 68.46 | 0.0093 | 0.0014 | 0 | 0 | 1 | 1 | 1 |
| | 30 | 65.17 | 0.0197 | 0.0029 | 0 | 0 | 1 | 1 | 1 |
| | 45 | 63.82 | 0.0270 | 0.0041 | 0 | 0 | 1 | 1 | 1 |
| | 55 | 63.41 | 0.0296 | 0.0048 | 0 | 0 | 1 | 1 | 1 |
| **Pepper** | 15 | 66.77 | 0.0137 | 0.0013 | 0 | 0 | 1 | 1 | 1 |
| | 30 | 64.53 | 0.0229 | 0.0025 | 0 | 0 | 1 | 1 | 1 |
| | 45 | 63.08 | 0.0319 | 0.0036 | 0 | 0 | 1 | 1 | 1 |
| | 55 | **62.54** | **0.0362** | **0.0040** | **0** | **0** | **1** | **1** | **1** |
| **Barbara** | 15 | 68.88 | 0.0084 | 0.0014 | 0 | 0 | 1 | 1 | 1 |
| | 30 | 65.83 | 0.0170 | 0.0028 | 0 | 0 | 0.9999 | 1 | 1 |
| | 45 | 64.07 | 0.0254 | 0.0041 | 0 | 0 | 0.9999 | 1 | 1 |
| | 55 | 63.24 | 0.0308 | 0.0051 | 0 | 0 | 0.9998 | 1 | 1 |
| **Jet(f16)** | 15 | 68.87 | 0.0084 | 0.0014 | 0 | 0 | 0.9999 | 1 | 1 |
| | 30 | 65.61 | 0.0179 | 0.0028 | 0 | 0 | 0.9998 | 1 | 1 |
| | 45 | 63.82 | 0.0269 | 0.0043 | 0 | 0 | 0.9997 | 1 | 1 |
| | 55 | 63.15 | 0.0315 | 0.0051 | 0 | 0 | 0.9996 | 1 | 1 |
| **Grayscale Images (256*256), . jpeg** | | | | | | | | | |
| **Image Name** | **Text Size (byte)** | **PSNR** | **MSE** | **MAE** | **BER** | **SNR** | **SSIM** | **SC** | **Correlation** |
| **Lena** | 75 | 64.44 | 0.0233 | 0.0040 | 0 | 0 | 0.9999 | 1 | 1 |
| | 100 | 59.20 | 0.0782 | 0.0130 | 0 | 0 | 0.9994 | 1 | 1 |
| | 128 | 56.53 | 0.1443 | 0.0236 | 0 | 0 | 0.9990 | 1 | 1 |
| **Baboon** | 75 | 61.79 | 0.0430 | 0.0050 | 0 | 0 | 1 | 1 | 1 |
| | 100 | 57.62 | 0.1124 | 0.0150 | 0 | 0 | 0.9999 | 1 | 1 |
| | 128 | **55.97** | **0.1643** | **0.0242** | **0** | **0** | **0.9997** | **1** | **1** |
| **pepper** | 75 | 62.80 | 0.0341 | 0.0046 | 0 | 0 | 1 | 1 | 1 |
| | 100 | 58.32 | 0.0956 | 0.0140 | 0 | 0 | 0.9999 | 1 | 1 |
| | 128 | 56.05 | 0.1613 | 0.0237 | 0 | 0 | 0.9998 | 1 | 1 |
| **Barbara** | 75 | **64.90** | **0.0210** | **0.0037** | **0** | **0** | **1** | **1** | **1** |
| | 100 | 58.98 | 0.0822 | 0.0133 | 0 | 0 | 0.9998 | 1 | 1 |
| | 128 | 56.26 | 0.1537 | 0.0242 | 0 | 0 | 0.9995 | 1 | 1 |
| **Jet(f16)** | 75 | 63.72 | 0.0276 | 0.0043 | 0 | 0 | 0.9999 | 1 | 1 |
| | 100 | 59.23 | 0.0776 | 0.0129 | 0 | 0 | 0.9994 | 1 | 1 |
| | 128 | 56.66 | 0.1402 | 0.0233 | 0 | 0 | 0.9989 | 1 | 1 |

### 5.3.3. Experimental Results of the Proposed LSB with Hybrid (AES and RSA).

In this case the same text files, images and criteria were used but with different approach. In this approach the text is encrypted by using encryption algorithms that were previously explained. Then it is being embedded using the LSB stenography techniques. Accordingly, the obtained results in case of using LSB only were very close to that obtained with LSB with hybrid AES and RSA. This indicates that LSB stenography technique in both cases had the same effect on the cover image and with the same performance.

It was found that the PSNR values were relatively high with the color images than those with the grayscale images. They varied from 66.29 to 88.33 in case of color images and from 60.17 to 86.75 with the gray scale images in Table (5.3). However, these values didn't show a general trend with the different text sizes. Both the MSE and MAE were very small and had the same range of values with both type of images, which indicates a very good quality of the stego image. The MSE values varied from 0.0001 to 0.0153, whereas the MAE ranged between 0 and 0.0003. The SSIM, SC and Correlation were almost equal to one with all the studied images (color and grayscale).

**Table (5.3):** Results of statistical parameters obtained from performing the LSB with hybrid (AES and RSA) approach on color and grayscale images with different text sizes.

| **Color Images (512*512), .bmp** | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Image Name** | **Text Size (byte)** | **PSNR** | **MSE** | **MAE** | **BER** | **SNR** | **SSIM** | **SC** | **Correlation** |
| **Lena** | 15 | **66.29** | **0.0153** | **0.0003** | **0** | **0** | **1** | **1** | **1** |
| | 30 | 66.98 | 0.0130 | 0.0003 | 0 | 0 | 1 | 1 | 1 |
| | 45 | 67.56 | 0.0114 | 0.0003 | 0 | 0 | 1 | 1 | 1 |
| | 55 | 68.05 | 0.0102 | 0.0003 | 0 | 0 | 1 | 1 | 1 |
| **Baboon** | 15 | 69.40 | 0.0075 | 0.0002 | 0 | 0 | 1 | 1 | 1 |
| | 30 | 70.17 | 0.0062 | 0.0002 | 0 | 0 | 1 | 1 | 1 |
| | 45 | 71.24 | 0.0049 | 0.0003 | 0 | 0 | 1 | 1 | 1 |
| | 55 | 71.97 | 0.0041 | 0.0002 | 0 | 0 | 1 | 1 | 1 |
| **pepper** | 15 | **88.33** | **0.0001** | **0** | **0** | **0** | **1** | **1** | **1** |
| | 30 | 83.23 | 0.0003 | 0 | 0 | 0 | 1 | 1 | 1 |
| | 45 | 79.39 | 0.0007 | 0 | 0 | 0 | 1 | 1 | 1 |
| | 55 | 77.70 | 0.0011 | 0 | 0 | 0 | 1 | 1 | 1 |
| **Barbara** | 15 | 68.31 | 0.0096 | 0.0002 | 0 | 0 | 1 | 1 | 1 |
| | 30 | 69.00 | 0.0082 | 0.0002 | 0 | 0 | 1 | 1 | 1 |
| | 45 | 69.97 | 0.0065 | 0.0002 | 0 | 0 | 1 | 1 | 1 |
| | 55 | 70.57 | 0.0057 | 0.0002 | 0 | 0 | 1 | 1 | 1 |
| **Jet(f16)** | 15 | 68.48 | 0.0092 | 0.0002 | 0 | 0 | 1 | 1 | 1 |
| | 30 | 69.17 | 0.0079 | 0.0003 | 0 | 0 | 1 | 1 | 1 |
| | 45 | 70.11 | 0.0063 | 0.0003 | 0 | 0 | 1 | 1 | 1 |
| | 55 | 70.77 | 0.0054 | 0.0003 | 0 | 0 | 1 | 1 | 1 |
| **Grayscale Images (256*256) , . jpeg** | | | | | | | | | |
| **Image Name** | **Text Size (byte)** | **PSNR** | **MSE** | **MAE** | **BER** | **SNR** | **SSIM** | **SC** | **Correlation** |
| **Lena** | 100 | 72.21 | 0.0039 | 0.0002 | 0 | 0 | 1 | 1 | 1 |
| | 128 | 78.23 | 0.0010 | 0.0001 | 0 | 0 | 1 | 1 | 1 |
| | 256 | 66.75 | 0.0137 | 0 | 0 | 0 | 0.9999 | 1 | 1 |
| **Baboon** | 100 | 84.25 | 0.0002 | 0.0001 | 0 | 0 | 1 | 1 | 1 |
| | 128 | 82.31 | 0.0004 | 0 | 0 | 0 | 1 | 1 | 1 |
| | 256 | 63.83 | 0.0269 | 0 | 0 | 0 | 1 | 1 | 1 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **pepper** | 100 | 71.19 | 0.0049 | 0 | 0 | 0 | 1 | 1 | 1 |
| | 128 | 67.99 | 0.0103 | 0 | 0 | 0 | 1 | 1 | 1 |
| | 256 | **60.17** | **0.0625** | **0** | **0** | **0** | **1** | **1** | **1** |
| **Barbara** | 100 | 67.99 | 0.0103 | 0.0004 | 0 | 0 | 1 | 1 | 1 |
| | 128 | 71.68 | 0.0044 | 0.0003 | 0 | 0 | 1 | 1 | 1 |
| | 256 | 70.27 | 0.0061 | 0 | 0 | 0 | 1 | 1 | 1 |
| **Jet(f16)** | 100 | **86.75** | **0.0001** | **0** | **0** | **0** | **1** | **1** | **1** |
| | 128 | 80.73 | 0.0005 | 0 | 0 | 0 | 1 | 1 | 1 |
| | 256 | 63.62 | 0.0282 | 0 | 0 | 0 | 1 | 1 | 1 |

### 5.3.4. Experimental Results of the Proposed (2D – DWT – 2L) with Hybrid (AES and RSA).

In this approach, also the same text files, images and criteria were used but with the (2D - DWT - 2L) and hybrid (AES and RSA). In this case the text is encrypted by using encryption algorithms that were previously explained. Then it is being embedded using the (2D - DWT - 2L) stenography techniques. It was found that the obtained results in case of using (2D - DWT - 2L) only were more acceptable than those obtained when it is being integrated with the hybrid (AES and RSA). There was an obvious effect on the visibility of the cover image as a result of encryption process. This also was reflected on the obtained results of the statistical parameters used in evaluating the quality of the proposed method.

The obtained PSNR values were relatively lower than those obtained with the other studied approaches, although the color images still had higher values than the grayscale images. They PSNR values varied from 52.41 to 56.99 with color images and from 45.39 to 47.96 with the gray scale images in Table (5.4).

On the other hand, MSE and MAE values were comparatively higher than those obtained with other studied approaches. These values were generally smaller with the color images than those obtained with the gray scale images. The MSE values varied from 0.1298 to 0.3727 with the color images and from 1.0382 to 1.876 with the grayscale images. MAE values are ranged between 0.0091 and 0.0075 with color images and from 0.0476 to 0.0508 with the grayscale images.

**Table (5.4):** Results of statistical parameters obtained from performing the (2D - DWT - 2L) with hybrid (AES and RSA) approach on color and grayscale images with different text sizes.

| **Color Images (512*512), .bmp** | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Image Name** | **Text Size (byte)** | **PSNR** | **MSE** | **MAE** | **BER** | **SNR** | **SSIM** | **SC** | **Correlation** |
| **Lena** | 15 | **56.99** | **0.1298** | **0.0075** | **0** | **0** | **0.9992** | **1** | **1** |
| | 30 | 54.70 | 0.2199 | 0.0105 | 0 | 0 | 0.9988 | 1 | 1 |
| | 45 | 53.05 | 0.3220 | 0.0150 | 0 | 0 | 0.9981 | 1 | 1 |
| | 55 | 52.97 | 0.3276 | 0.0153 | 0 | 0 | 0.9980 | 1 | 1 |
| **Baboon** | 15 | 56.55 | 0.1438 | 0.0062 | 0 | 0 | 0.9999 | 1 | 1 |
| | 30 | 54.41 | 0.2354 | 0.0080 | 0 | 0 | 0.9999 | 0.9999 | 1 |
| | 45 | 52.66 | 0.3518 | 0.0114 | 0 | 0 | 0.9996 | 0.9999 | 1 |
| | 55 | 52.67 | 0.3511 | 0.0119 | 0 | 0 | 0.9996 | 0.9999 | 1 |
| **pepper** | 15 | 56.54 | 0.1440 | 0.00056 | 0 | 0 | 0.9999 | 1 | 1 |
| | 30 | 54.19 | 0.2477 | 0.0079 | 0 | 0 | 0.9998 | 1 | 1 |
| | 45 | **52.41** | **0.3727** | **0.0091** | **0** | **0** | **0.9997** | **1** | **1** |
| | 55 | 52.55 | 0.3610 | 0.0093 | 0 | 0 | 0.9998 | 0.9999 | 1 |
| **Barbara** | 15 | 56.69 | 0.1393 | 0.0054 | 0 | 0 | 0.9995 | 1 | 1 |
| | 30 | 54.38 | 0.2369 | 0.0078 | 0 | 0 | 0.9992 | 0.9999 | 1 |
| | 45 | 52.81 | 0.3397 | 0.0146 | 0 | 0 | 0.9989 | 1 | 1 |
| | 55 | 52.64 | 0.3534 | 0.0144 | 0 | 0 | 0.9988 | 1 | 1 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Jet(f16)** | 15 | 56.64 | 0.1409 | 0.0090 | 0 | 0 | 0.9991 | 1 | 1 |
| | 30 | 54.15 | 0.2495 | 0.0137 | 0 | 0 | 0.9987 | 1 | 1 |
| | 45 | 52.49 | 0.3660 | 0.0197 | 0 | 0 | 0.9983 | 1 | 1 |
| | 55 | 52.55 | 0.3611 | 0.0199 | 0 | 0 | 0.9983 | 1 | 1 |
| **Grayscale Images (256*256), . jpeg** | | | | | | | | | |
| **Image Name** | **Text Size (byte)** | **PSNR** | **MSE** | **MAE** | **BER** | **SNR** | **SSIM** | **SC** | **Correlation** |
| **Lena** | 100 | 47.60 | 1.1299 | 0.0529 | 0 | 0 | 1.0004 | 1.0004 | 0.9998 |
| | 128 | 45.53 | 1.8174 | 0.0610 | 0 | 0 | 0.9942 | 1.0002 | 0.9998 |
| | 256 | 46.14 | 1.5813 | 0.0562 | 0 | 0 | 0.9947 | 1.0002 | 0.9999 |
| **Baboon** | 100 | **47.96** | **1.0382** | **0.0476** | **0** | **0** | **0.9977** | **0.9999** | **1** |
| | 128 | 45.88 | 1.6757 | 0.0623 | 0 | 0 | 0.9967 | 0.9999 | 1 |
| | 256 | 46.43 | 1.4784 | 0.0576 | 0 | 0 | 0.9970 | 0.9999 | 1 |
| **pepper** | 100 | 47.24 | 1.2254 | 0.0353 | 0 | 0 | 0.9983 | 0.9999 | 1 |
| | 128 | **45.39** | **1.8760** | **0.0508** | **0** | **0** | **0.9979** | **0.9999** | **1** |
| | 256 | 46.03 | 1.6201 | 0.0469 | 0 | 0 | 0.9981 | 0.9999 | 1 |
| **Barbara** | 100 | 47.70 | 1.1028 | 0.0393 | 0 | 0 | 0.9973 | 0.9998 | 1 |
| | 128 | 45.80 | 1.7069 | 0.0527 | 0 | 0 | 0.9965 | 0.9997 | 1 |
| | 256 | 46.42 | 1.4802 | 0.0487 | 0 | 0 | 0.9967 | 0.9998 | 1 |
| **Jet(f16)** | 100 | 47.03 | 1.2875 | 0.0655 | 0 | 0 | 0.9950 | 1.0004 | 0.9998 |
| | 128 | 45.41 | 1.8703 | 0.0878 | 0 | 0 | 0.9940 | 1.0006 | 0.9997 |
| | 256 | 46.22 | 1.1551 | 0.0774 | 0 | 0 | 0.9945 | 1.0005 | 0.9997 |

## 5.4. Comparing the Results of our Proposed Techniques with other Results

### 1. The Propose LSB Technique:

**i.** Emam et al. (2016) [104] developed a system based on LSB approach his approach a color data set images with a size (512x512). Figure (5.5) represents the obtained PSNR values from applying our approach as compared with those obtained from the studied reference on the same dataset. This indicates a higher performance of our approach in hidden the secret data.

Figure (5.6) represents the obtained MSE values from applying our approach as compared with those obtained from the studied reference on the same dataset. Our MSE values for all the tested images and text sizes were smaller than those obtained by [104], which also reveals the higher performance of our approach.

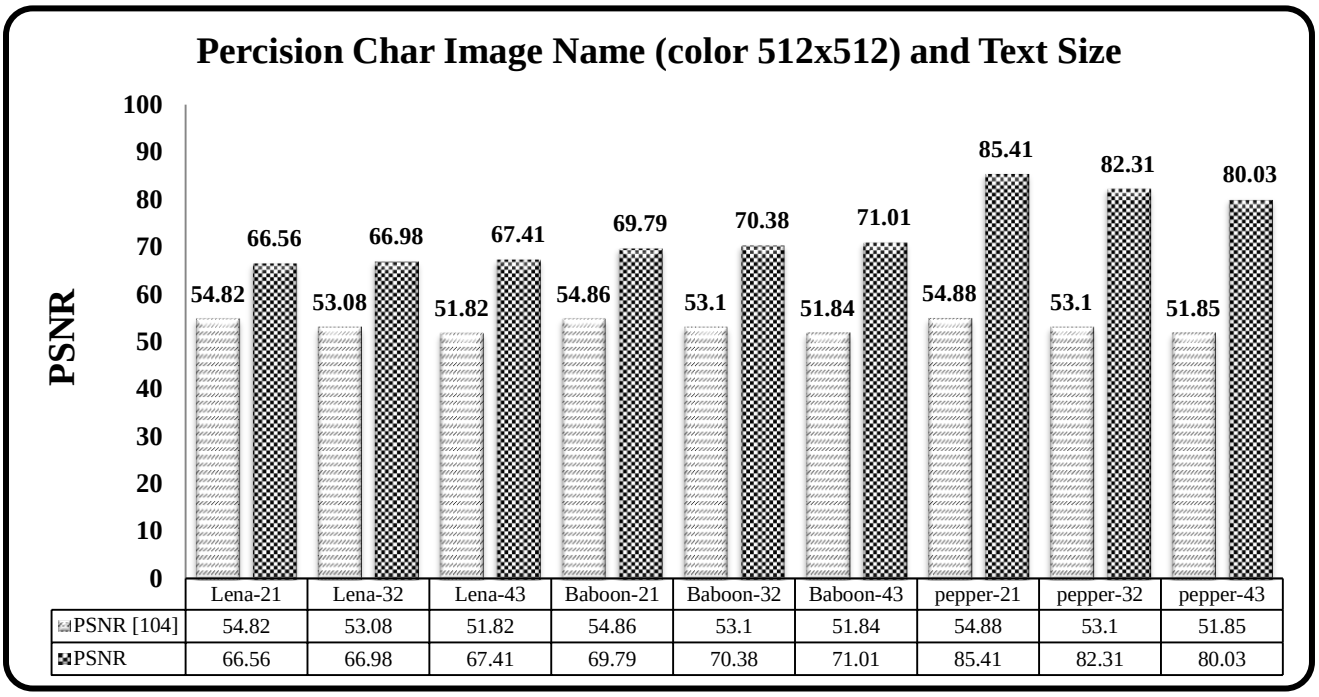
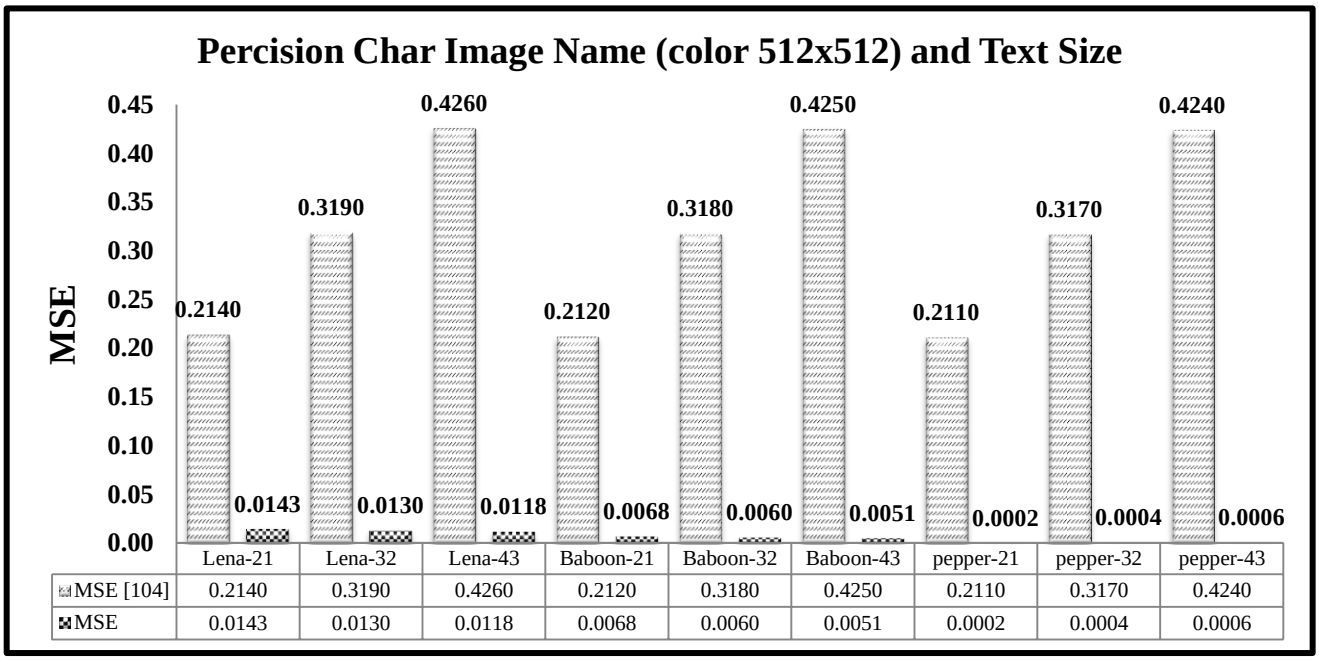


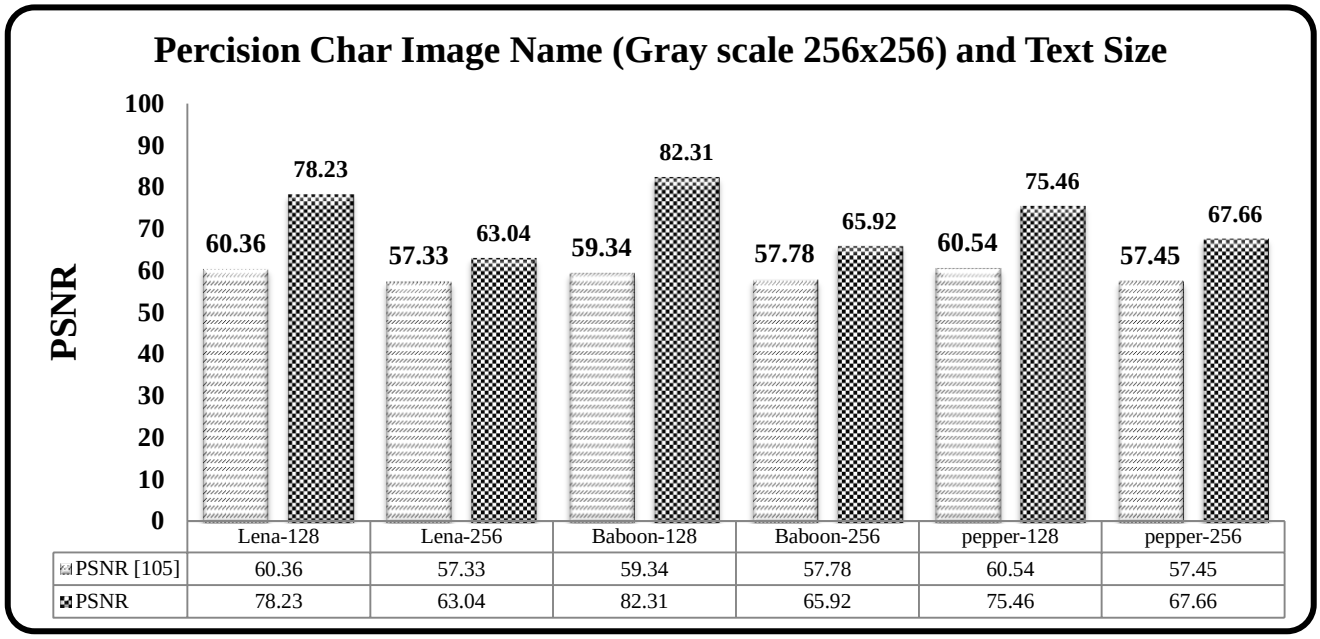

**Figure (5.5):** PSNR values obtained from our LSB approach compared with those obtained by [104] on color images.




| | Lena-21 | Lena-32 | Lena-43 | Baboon-21 | Baboon-32 | Baboon-43 | pepper-21 | pepper-32 | pepper-43 |
|---|---|---|---|---|---|---|---|---|---|
| MSE [104] | 0.2140 | 0.3190 | 0.4260 | 0.2120 | 0.3180 | 0.4250 | 0.2110 | 0.3170 | 0.4240 |
| MSE | 0.0143 | 0.0130 | 0.0118 | 0.0068 | 0.0060 | 0.0051 | 0.0002 | 0.0004 | 0.0006 |

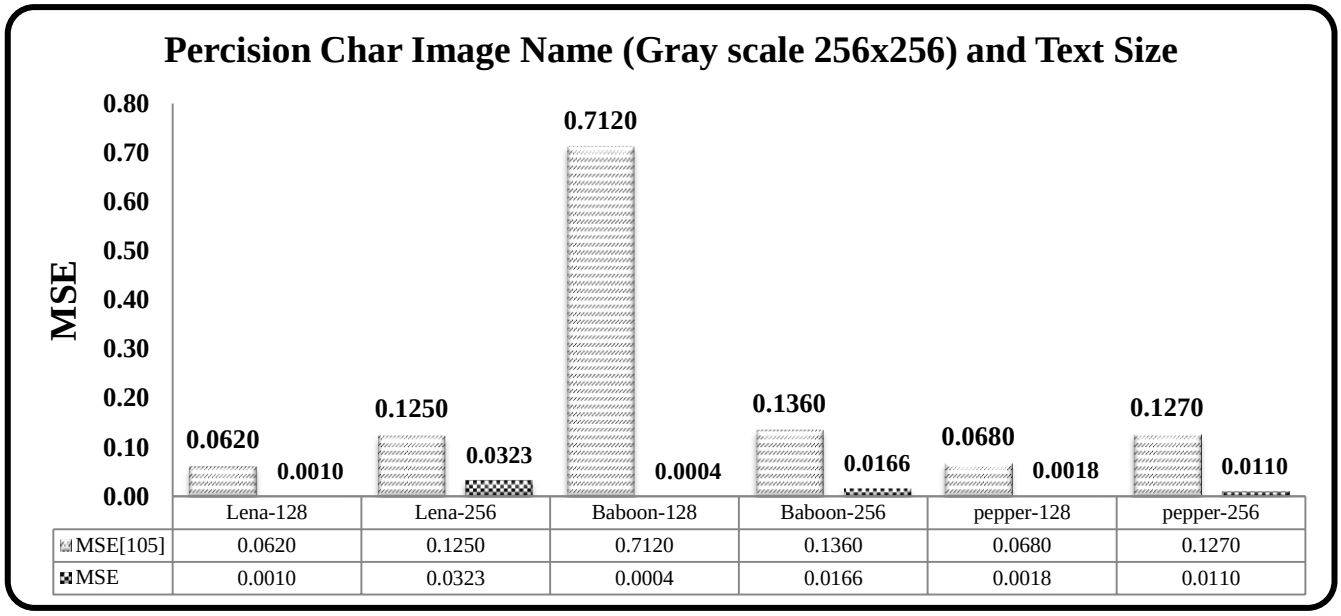
**Figure (5.6):** MSE values obtained from our LSB approach compared with those obtained by [104] on color images.

**ii.** Chandran et al. (2015) [105] developed a system based on LSB approach his approach a grayscale data set images with a size (256x256). Figure (5.7) represents the obtained PSNR values from applying our approach as compared with those obtained from the studied reference on the same dataset. This indicates a higher performance of our approach in hidden the secret data. Figure (5.8) represents the obtained MSE values from applying our approach as compared with those obtained from the studied reference on the same dataset. Our MSE values for all the tested images and text sizes were smaller than those obtained by [105], which also reveals the higher performance of our approach.




| | Lena-128 | Lena-256 | Baboon-128 | Baboon-256 | pepper-128 | pepper-256 |
|---|---|---|---|---|---|---|
| PSNR [105] | 60.36 | 57.33 | 59.34 | 57.78 | 60.54 | 57.45 |
| PSNR | 78.23 | 63.04 | 82.31 | 65.92 | 75.46 | 67.66 |

**Figure (5.7):** PSNR values obtained from our LSB approach compared with those obtained by [105] on grayscale images.




| | Lena-128 | Lena-256 | Baboon-128 | Baboon-256 | pepper-128 | pepper-256 |
|---|---|---|---|---|---|---|
| MSE[105] | 0.0620 | 0.1250 | 0.7120 | 0.1360 | 0.0680 | 0.1270 |
| MSE | 0.0010 | 0.0323 | 0.0004 | 0.0166 | 0.0018 | 0.0110 |

**Figure (5.8):** MSE values obtained from our LSB approach compared with those obtained by [105] on grayscale images.

**2. The Performance of our Proposed (2D-DWT-2L) Technique:**

**i.** Was also compared with another approach developed by reference [106] on two color images using one text size. Figures (9 and 10) illustrates the obtained PSNR and MSE values from applying our approach as compared with those obtained by the studied reference. It was also found that our proposed approach had the higher PSNR values and the smaller MSE values when compared with those values derived by the reference approach. This also indicates the higher performance of our 2D-DWT-2L approach.

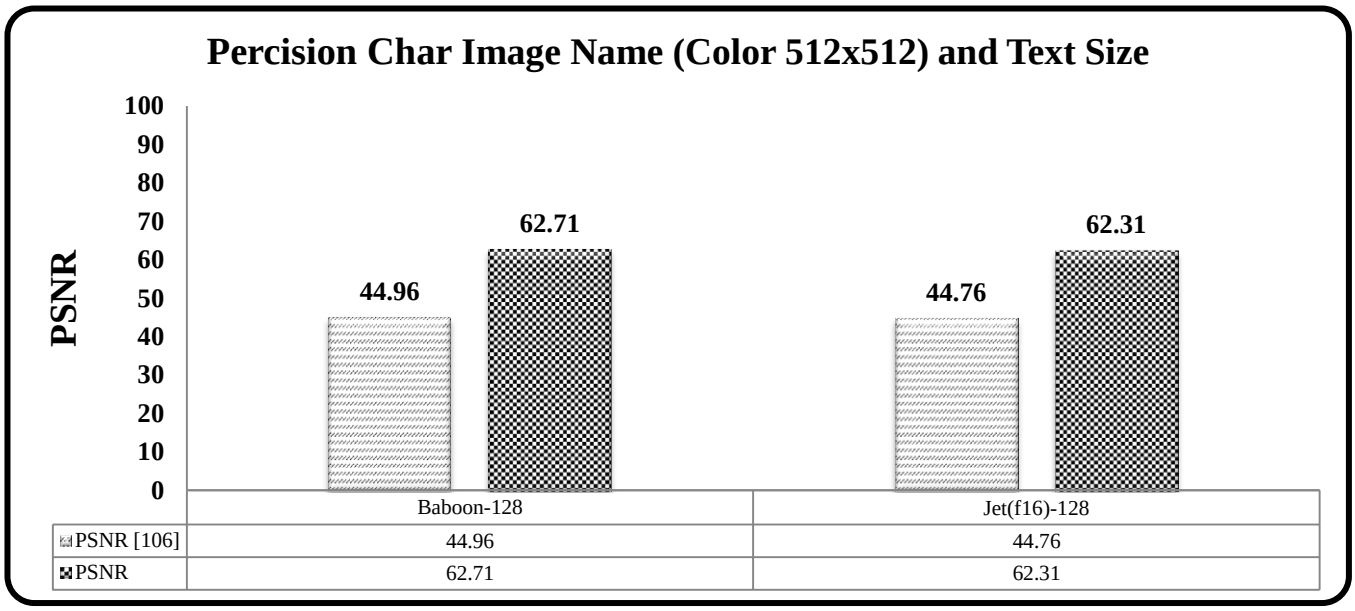



**Figure (5.9):** PSNR values obtained from our (2D-DWT-2L) approach compared with those obtained by [106] on two color images.

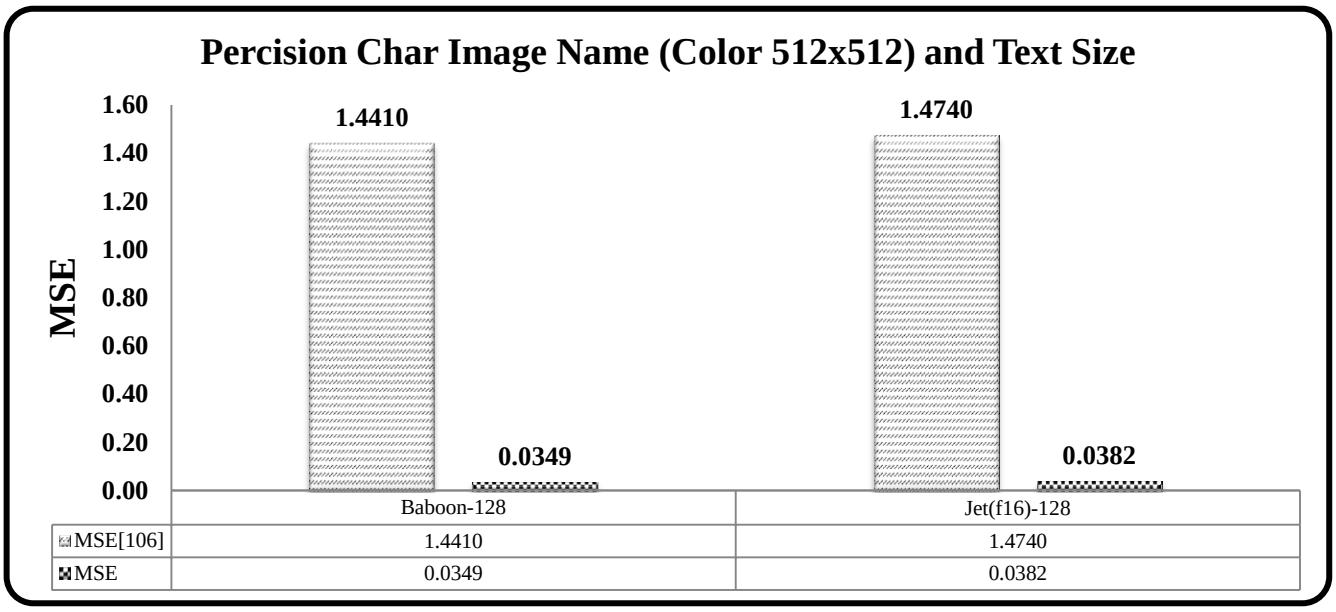



**Figure (5.10):** MSE values obtained from our (2D-DWT-2L) approach compared with those obtained by [106] on two color images.

**ii.** Our proposed (2D-DWT-2L) approach was also evaluated by comparing its results with those obtained from applying that approach developed by [107] on two color images using one text size. Figures (11 and 12) show the obtained PSNR and MSE values from applying our approach as compared with those obtained by the mentioned reference. Our PSNR values were higher for the two studied color images when compared with the reference values. On the other hand, our MSE values were smaller than those obtained by the reference approach on the same images. All of these results indicate that our proposed 2D-DWT-2L approach had higher performance than the reference approach used in this study.

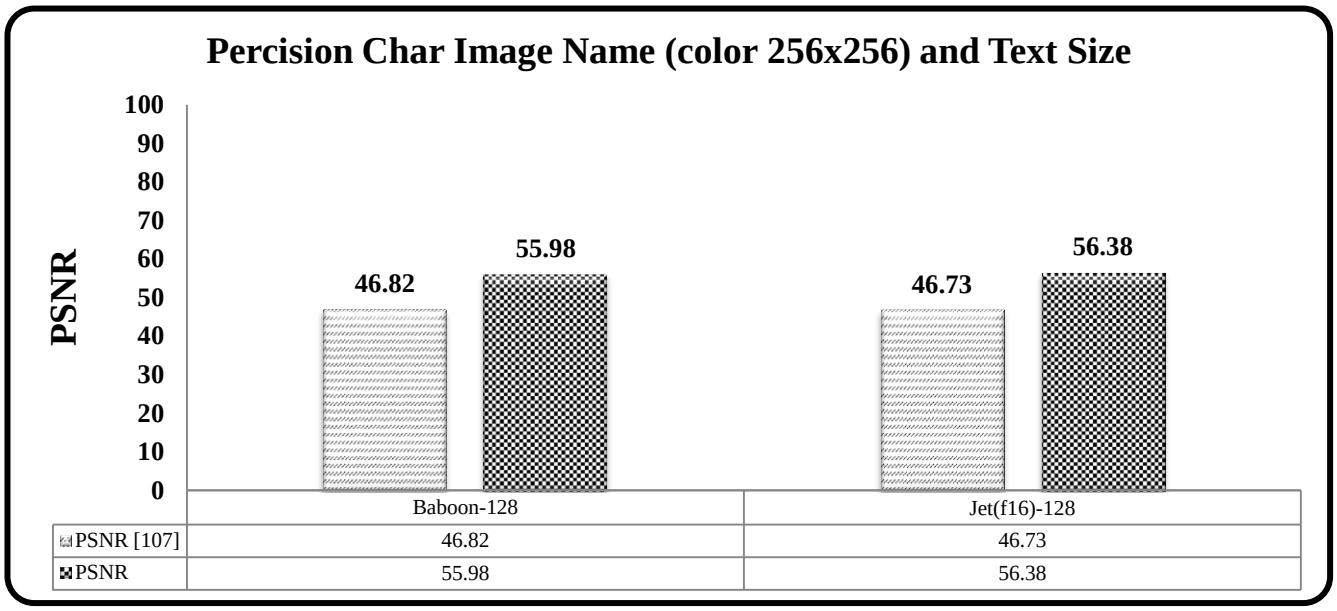



**Figure (5.11):** PSNR values obtained from our (2D-DWT-2L) approach compared with those obtained by [107] on two color images.

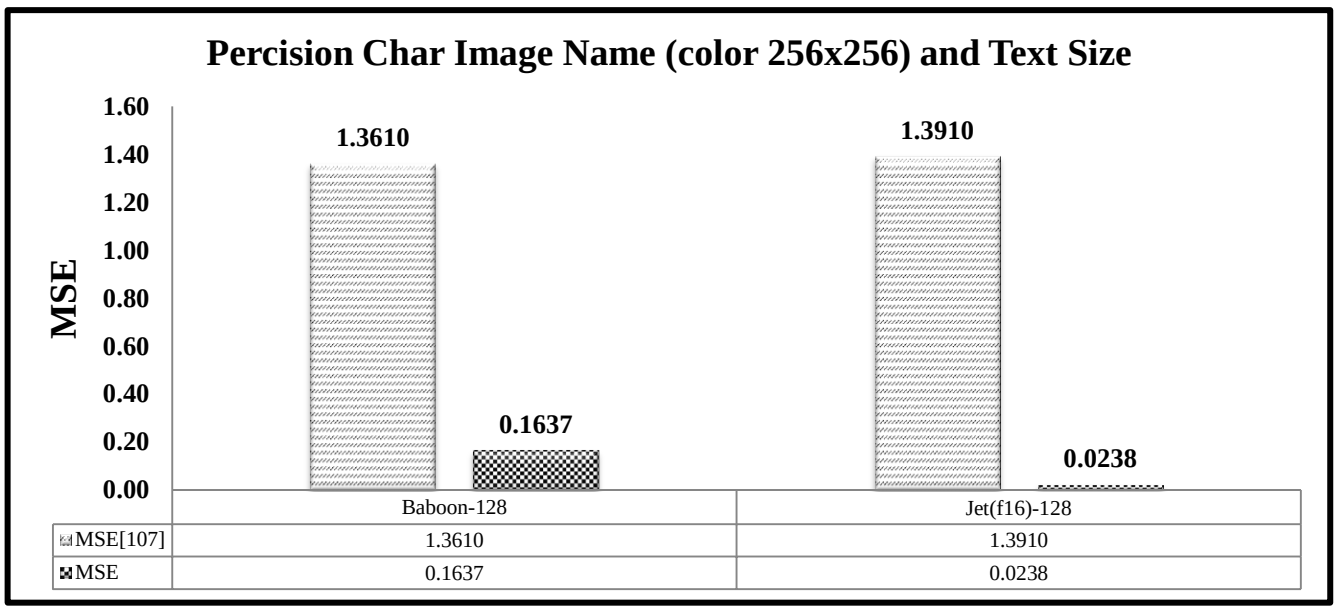



**Figure (5.12):** MSE values obtained from our (2D-DWT-2L) approach compared with those obtained by [107] on two color images.

### 3. LSB and 2D-DWT-2L Technique with Hybrid (AES and RSA):

**i.** Our proposed LSB and hybrid (AES and RSA) technique was also compared with another approach developed by reference [108]. However, this reference doesn't include any representation of its results in a form of table or figures. Table (5.6) represent the obtained PSNR and MSE values from applying our approach on 512x512 pixel color images with 126 and 256 byte text sizes.

**Table (5.5):** Comparing the results of our propose LSB with hybrid (AES and RSA) based on [108] approch with referece PSNR and MSE values.

| **LSB and hybrid (AES and RSA)** | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **No.** | **Comparison between other Method** | **Image Name Used** | **Text Size (byte)** | **Image Type** | **File Format** | **Parameter** | | | |
| | | | | | | **PSNR** | | **MSE** | |
| **5** | Approach In [108] | …….. | …….. | …….. | …….. | …….. | | …….. | |
| **#** | Proposed method | Lena<br>Baboon<br>Pepper | (128.256)<br>(128.256)<br>(128.256) | Color 512 * 512 | .bmp | **72.20**<br>**77.67**<br>**70.44** | **76.01**<br>**72.15**<br>**64.51** | **0.0039**<br>**0.0011**<br>**0.0059** | **0.0016**<br>**0.0040**<br>**0.0230** |

**ii.** The performance of our proposed 2D-DWT-2L with hybrid (AES and RSA) technique was also compared with another technique developed by reference [109] on 256x256 pixel medical color image using 18 byte text size. Table (5.7) shows the obtained PSNR and MSE values from applying our approach as compared with those obtained by the studied reference. It was also found that our proposed approach had a higher PSNR value and a smaller MSE value than that obtained in the reference approach. This also reveals the higher performance of our proposed approach.

**Table (5.6):** Comparing the results of our propose (2D-DWT-2L) with hybrid (AES and RSA) based on [109] approch with referece PSNR and MSE values.

| **2D-DWT-2L with hybrid (AES and RSA)** | | | | | | | |
|---|---|---|---|---|---|---|---|
| **No.** | **Comparison between other Method** | **Image Name Used** | **Text Size (byte)** | **Image Type** | **File Format** | **Parameter** | |
| | | | | | | **PSNR** | **MSE** |
| **6** | Approach In [109] | Medical Images | ( 18 ) | Color 256 * 256 | .jpg | 56.76 | 0.1338 |
| **#** | Proposed method | Medical Images | ( 18 ) | Color 256 * 256 | .jpg | **57.03** | **0.1286** |

## 5.5. Advantages of the Proposed System

The proposed steganography technologies and hybrid encryption algorithm have many operational advantages, which can be summarized in the following:

1. Great storage capacity, where adding data to an image file may make an observable increase in its storage size, especially when hiding large amount of data. With our proposed techniques, no significant difference was observed between the cover image before and after embedding the secret message.
2. Flexibility and low computation complexity are also ensured in our proposed techniques.
3. More security is also guaranteed in our system, where all people can used or download the image but only the intended person can get access to the hidden message.
4. A combination of public and private keys is used in our system to ensure a very high security of the proposed scheme. Also, in order to maintain the security of the extracted text from any unauthorized access, the text was encrypted with a hybrid technique. The proposed encryption method also provides a higher speed in term of both encryption and decryption times.

## 5.6. Summary

This chapter started with describing the execution environment and then the user interface of our proposed techniques. The types of images and the text sizes that were used in executing the studied technique were introduced after that. The obtained results from performing our proposed data hiding techniques (LSB , 2D-DWT-2L , LSB with hybrid (AES and RSA) and 2D-DWT-2L) with hybrid (AES and RSA) were represented and discussed in details. Also, the performance of these techniques was compared with previously obtained results from other references. Performance evaluation was based on eight statistical parameters, However only PSNR and MSE distinguished the variations among the proposed techniques. There were no significant variations among the other studied parameters with the proposed techniques. Our proposed techniques showed higher quality when compared with previous results. However, the 2D-DWT-2L with hybrid (AES and RSA), showed the lowest the other techniques performance when compared with it was noticed that although text encryption increases the text security, it decreases the invisibility of the cover image. In other words, text encryption to some extent increases covers image distortion, which makes it visible to unwanted personals.

# CHAPTER 6

## Conclusion and Future Work

### 6.1. Conclusion

The main advantages of our system are providing greater embedding capacity, more security, more flexibility and more invisibility. Also, an adopted hybrid encryption algorithm was used in this work. This hybrid system is considered as an amalgamation of AES and RSA algorithms. It could be concluded that both of two proposed steganography techniques (LSB and 2D-DWT-2L) and their integration with encryption (AES and RSA) algorithms had higher performance when applied on color and grayscale images with different text sizes. This is based on the eight studied statistical parameters (PSNR, MSE, MAE, BER, SNR, SSIM, SC, and Correlation). However, only the PSNR and MSE distinguished the variations among the proposed techniques.

There were no significant variations among the other statistical parameters with the proposed techniques. It was found that the PSNR values were increased by increasing the text size with the tested color images except with pepper image. This reveals that the similarity between the original image and the stego image decreases by increasing the text size, which is generally true when there is lots of a color variation in the cover image. However, when the numbers of colors are limited as in the pepper image the PSNR values decrease by increasing the text size.

The PSNR values took an opposite trend with the grayscale images, were the values decreased by increasing the text size. On the other hand, the MSE were decreased by increasing the text size for all the studied color images, except the pepper image, which is also correlated with the number of color variations in the cover image, where the larger the color variations the smaller the MSE value. However, there wasn't a general trend in the MSE values with the grayscale images, where the values varied from one image to another. This could be attributed the histogram of pixel values in each image, either they equally distribution along the grayscale or they are not.

The performance of the four proposed approaches was further evaluated by comparing their results with those obtained from other approach on both color and grayscale images with different text sizes. Our approaches had higher PSNR values and lower MSE values than those obtained by the reference results. However, the (2D-DWT-2L) with hybrid (AES and RSA), showed the slowest performance when compared with other technique it was noticed that although text encryption increases the text security, it decreases the invisibility of the cover image. In other words, text encryptions to some extent increases cover image distortion, which makes it visible to unwanted personals. In conclusion, our proposed approaches had higher performance in hiding secret data when compared with the reference approaches used in this study.

## 6.2. Future Work

In the future work, we can further enhance information security techniques develop an avenue for secure data transmission. This work can be developed to be applied on other data file formats such as, video, audio. Also it is possible to build a strong method for hiding Arabic text in a cover media by using each Arabic text in the cover media. On a large scale implementation we will try to simulate multiple communicating parties (normal and covert communication). We are looking forward to enhance the method proposed in use quantum steganography can be stronger than classical steganography, by introducing a quantum steganography system that cannot be imitated by one.

# List of References

**[1]** Shanableh, Tamer. "Data hiding in MPEG video files using multivariate regression and flexible macroblock ordering." *IEEE Transactions on Information Forensics and Security* 7.2, 455-464, 2012.

**[2]** Yalman, Yildiray, and Ismail Erturk. "A new histogram modification based robust image data hiding technique." *Computer and Information Sciences, 2009. ISCIS 2009. 24th International Symposium on*. IEEE, 2009.

**[3]** Andrews, Chinchu Elza, and Iwin Thanakumar Joseph. "An Analysis of Various Stegonographic Algorithms." *International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)* 2.2.116-123, 2013.

**[4]** R.Amirtharajan and John Bosco Balaguru Rayappan ."An Intelligent Chaotic Embedding Approach to Enhance the Quality of Stego-Image", *Information Sciences*, 193, 115-124, 2012.

**[5]** Amirtharajan, Rengarajan, Jiaohua Qin, and John Bosco Balaguru Rayappan. "Random image steganography and steganalysis: Present status and future directions." *Information Technology Journal* 11.5, 566. 2012.

**[6]** Peltier, Thomas R. I*nformation security fundamentals-Auerbach Publications*. CRC Press, 2005.

**[7]** Peltier, Thomas R. *Information security fundamentals*. CRC Press, 2013. available o at:http://www.slideshare.net/duskydawn/infomation-system-security-67432011 . last accessed on [access 23-02-2014] .

**[8]** William, Stallings. *Computer Security: Principles And Practice*. Pearson Education India, 2012.

**[9]** Paar, Christof, and Jan Pelzl. *Understanding cryptography: a textbook for students and practitioners*. Springer Science & Business Media, 2009.

**[10]** Chuchra, Rimmy, and R. K. Seth. "Modeling Implementation of TESA-Three Step Encryption Algorithm for enhancing Password Security." *International Journal of Computer Applications* 126.13. .2015.

**[11]** Sheth, Ravi K. "Analysis of Cryptography Techniques." *international journal of research in advance engineering* 1.2 .1-6, 2015.

**[12]** Rivest, Ronald L., Adi Shamir, and Leonard Adleman. "A method for obtaining digital signatures and public-key cryptosystems." *Communications of the ACM* 21.2, 2000.

**[13]** Ayushi, A. "Symmetric Key Cryptographic Algorithm." *International Journal of Computer Applications* 1.15, 2010.

**[14]** Mandal, Akash Kumar, Chandra Parakash, and Archana Tiwari. "Performance evaluation of cryptographic algorithms: DES and AES." *Electrical, Electronics and Computer Science (SCEECS), IEEE Students' Conference on*. IEEE, 2012.

**[15]** Stanoyevitch, Alexander. *Introduction to Cryptography with mathematical foundations and computer implementations*. CRC , 2010.

**[16]** Goldreich, Oded. *Foundations of cryptography: volume 2, basic applications*. Cambridge university press, 2009.

**[17]** available o at: https://www.cs.rit.edu/~ark/462/module03/notes.shtml , [access at 18 November 2015].

**[18]** Delfs, Hans, Helmut Knebl, and Helmut Knebl. Introduction to cryptography. Vol. 2. Berlin etc.: Springer-*New York*, (pp.19 -26), 2007.

**[19]** Mjolsnes, Stig F., ed. *A Multidisciplinary Introduction to Information Security*. CRC Press, (pp. 26-28) , 2011.

**[20]** Available o at: http://competitions.cr.yp.to/aes.html , [access at 18 November 2015].

**[21]** Watson, David Lilburn, Gianluigi Me, and Frank Leonhardt. *Handbook of electronic security and digital forensics*. Ed. Hamid Jahankhani. World Scientific, 2010.

**[22]** Peltier, Thomas R. *Information security fundamentals*. CRC Press,.pp. 32-41, 2013.

**[23]** Stallings, William. *Cryptography and network security: principles and practices.* Pearson Education India, 2006.

**[24]** Payal Sharma, Manju Godara, Ramanpreet Singh. "Digital Image Encryption Techniques: A Review." International Journal of Computing & Business Research: 2229-6166, 2012.

**[25]** Majhi, B. *High Security Image Encryption By 3 Stage Process*. Diss. PhD Thesis. National Institute Of Technology Rourkela, 2014.

**[26]** Battiato, Sebastiano, and Marco Moltisanti. " Tecniche di steganografia su immagini digitali",http://docplayer.it/3228702-steganografia-su-immagini-digitali.htm1 ,(online), [access at 2/3/2016].

**[27]** Poynton, Charles. *Digital video and HD: Algorithms and Interfaces*. Elsevier, 2012.

**[28]** Srdjan Stankovic,Irena Orovic, Ervin Sejdic ."Multimedia Signals and Systems ", Vol. 716. *Springer Science & Business Media*, pp133-139, 2012.

**[29]** Availableoat:https://www.spacetelescope.org/static/projects/fits_liberator/image_processing.pdf ,(online), [access at 27/12/2015].

**[30]** Chowdhury, Mahfuzulhoq, Md Moniruzzaman, and Parijat Prashun Purohit. "Multiple Selective Regions Image Cryptography on Modified RC4 Stream Cipher." *International Journal of Grid and Distributed Computing* 7.3, 189-198, 2014 .

**[31]** Panduranga, Naveen Kumar. "Hybrid approach for image encryption using SCAN patterns and Carrier images." *International Journal on Computer Science and Engineering* 2.02, 297-300, 2010.

**[32]** Hassan, Maaly Awad S., and Ibrahim Soliman I. Abuhaiba. "Image encryption using differential evolution approach in frequency domain." *arXiv preprint arXiv: 1103.5783*, 2011.

**[33]** Bashir, Ahmed, Abd Samad Bin Hasan, and Hamida Almangush ." A New Image Encryption Approach using The Integration of A Shifting Technique and The Aes Algorithm ", *International Journal of Computer Applications (0975 – 8887)*, V42.no.9, pp.36-45, 2012.

**[34]** Kumar, Anil, and Rohini Sharma. "A secure image steganography based on RSA algorithm and hash-LSB Technique." *International Journal of Advanced Research in Computer Science and Software Engineering* 3.7, 363-372, 2013.

**[35]** G.Malini , G.Manisha , S.Subbulakshmi ." Double-Stegging the Image in Dwt Domain with AES Encryption", *International Journal of Emerging Technology & Research (IJETR)*, V1. 4, 2014.

**[36]** Zaw, Zin May, and Su Wai Phyo. "Security Enhancement System Based on the Integration of Cryptography and Steganography." *International Journal of Computer (*IJC), v19, no.1, pp.26-39, 2015.

**[37]** Anwar, Asmaa Sabet, Kareem Kamal A. Ghany, and Hesham El Mahdy. "Improving the security of images transmission." *International Journal* 3.4, 2015.

**[38]** Yadav, Ravi Shankar, M. H. D. R. Beg, and Manish Madhava Tripathi. "Image encryption techniques: A critical comparison." *International Journal of Computer Science Engineering and Information Technology Research* 3.1, 67-74, 2013.

**[39]** Sharma, Godara, and Singh. "Digital Image Encryption Techniques: A Review." *International Journal of Computing & Business Research* 2229-6166, 2012.

**[40]** Jolfaei, Alireza, and Abdolrasoul Mirghadri. "Image encryption using chaos and block cipher." *Computer and Information Science* 4.1, 172, 2010.

**[41]** Sravanthi, Devi, Riyazoddin, and Reddy "A spatial domain image steganography technique based on plane bit substitution method." *Global Journal of Computer Science and Technology Graphics & Vision*, 12.15, 2012.

**[42]** Rocha, Scheirer, Boult, and Goldenstein. "Vision of the unseen: Current trends and challenges in digital image and video forensics." *ACM Computing Surveys (CSUR)* 43.4 .26, 2011.

**[43]** Al-Othmani, Abdulaleem Z., A. Abdul Manaf, and Akram M. Zeki. "A survey on steganography techniques in real time audio signals and evaluation." *International Journal of Computer Science Issues (IJCSI)* 9, 2012.

**[44]** Al-Ani, Zaidoon, Zaidan, and Alanazi ."Overview: Main fundamentals for steganography". *arXiv preprint arXiv*:1003.4086, 2010.

**[45]** Goswami, Sudhir, Jyoti Goswami, and Rajesh Mehra. "An efficient algorithm of steganography using JPEG colored image." *Recent Advances and Innovations in Engineering (ICRAIE)*, IEEE, 2014.

**[46]** Eric, Cole. "Hiding in plain sight, Stegnography and the art of Covert Communication." *Wiley, Indianapolis, Indiana, ISBN* 10, 2003.

**[47]** Sahoo, G., and R. K. Tiwari. "Designing an embedded algorithm for data hiding using steganographic technique by file hybridization." *International Journal of Computer Science and Network Security (IJCSNS),* 8.1, 228-233, 2008.

**[48]** Tiwari, Rajesh Kumar, and Gadadhar Sahoo. "Some New Methodologies for Image Hiding using Steganographic Techniques." *arXiv preprint arXiv*: 1211.0377, 2012.

**[49]** Kumar, Arvind, and Km Pooja. "Steganography-A data hiding technique." *International Journal of Computer Applications* 9.7, 19-23, 2010.

**[50]** Lecturer, Ayushi, and Haryana Sonipat. "A Symmetric Key Cryptographic Algorithm."*Hindu College of Engineering*, V1 .15, 2010.

**[51]** Cheddad, Abbas, Condell, Curran, and Mc Kevitt."Digital image steganography: Survey and analysis of current methods." *Signal processing* 90.3, 727-752, 2010.

**[52]** Singh, Kamred Udham. "A Survey on Image Steganography Techniques." *International Journal of Computer Applications* 97.18 , 2014.

**[53]** Mehta, Uma, and Mr Daulat Sihag. "Multi-Part Data Hiding in Audio Steganography." *International Journal of Advanced Research in Computer and Communication Engineering (ijarcce),* 3.10, 2014.

**[54]** Reddy, Velagalapalli Lokeswara, Arige Subramanyam, and Pakanati Chenna Reddy. "A least significant bit embedding technique of digital image steganography." *Atti della Fondazione Giorgio Ronchi* , 66.4 577-588, 2011.

**[55]** Gupta, Sumeet, and Dr Namrata Dhanda. "Audio Steganography Using Discrete Wavelet Transformation (DWT) & Discrete Cosine Transformation (DCT)." *IOSR Journal of Computer Engineering* 17.2, 32-44, 2015.

**[56]** Saha, Babloo, and Shuchi Sharma. "Steganographic Techniques of Data Hiding Using Digital Images (Review Paper)." Defence Science Journal 62.1, 11-18, 2012.

**[57]** Gupta, Shashank, and Rachit Jain. "An innovative method of Text Steganography." *Third International Conference on Image Information Processing (ICIIP).* IEEE, 2015.

**[58]** Jayaram, P., H. R. Ranganatha, and H. S. Anupama. "Information hiding using audio steganography–a survey." *The International Journal of Multimedia & Its Applications (IJMA)* Vol 3, 86-96, 2011.

**[59]** Bhaumik, A. K., Choi, Robles, and Balitanas. "Data hiding in video." *International Journal of database theory and Application* 2.2, 2009.

**[60]** Rajesh, Singh." Understanding Steganography over Cryptography and Various Steganography Techniques", *International Journal of Computer Science and Mobile Computing*, Vol.4.3, 2015.

**[61]** Tiwari, Anjali, Seema Rani Yadav, and N. K. Mittal. "A review on different image steganography techniques." *International Journal of Engineering and Innovative Technology (IJEIT)* 3.7, 121-124, 2014.

**[62]** Hussain, Mehdi, and Mureed Hussain. "A Survey of Image Steganography Techniques", *International Journal of Advanced Science and Technology*, Val 54, 2013.

**[63]** Al-Shatnawi, Atallah M. "A new method in image steganography with improved image quality." *Applied Mathematical Sciences* 6.79, 3907-3915, 2012.

**[64]** Sonu Rana." special cryptography using ecc technique for rfid communication *", International Journal of Science And Higher Engineering Research (IJSHER)*, 2347-4890, 2015.

**[65]** Sharma, Vijay Kumar, and Vishal Shrivastava. "A steganography algorithm for hiding image in image by improved LSB substitution by minimize detection." *Journal of Theoretical and Applied Information Technology* 36.1, 1-8, 2012.

**[66]** Sharma, Vijay Kumar, and Vishal Shrivastava. "Improving the performance of least significant bit substitution steganography against rs steganalysis by minimizing detection probability.*" International Journal of Information and Communication Technology Research* 1.4, 2011.

**[67]** Mehboob, Beenish, and Rashid Aziz Faruqui. "A stegnography implementation." *Biometrics and Security Technologies, ISBAST International Symposium on*. *IEEE*, 2008.

**[68]** Pavani, M., S. Naganjaneyulu, and C. Nagaraju. "A survey on LSB based steganography methods." *International Journal Of Engineering And Computer Science*, 2319-7242, 2013.

**[69]** Sifuzzaman, M., M. R. Islam, and M. Z. Ali."Application of wavelet transform and its advantages compared to Fourier transform*," Journal of Physical Sciences*, vol. 13, pp. 121-134, 2009.

**[70]** Thakare, Swapnil and Bhale. "A review of digital Image Steganography Techniques." *International Journal of Advanced Research in Computer Science and Software Engineering* 4.6, 465-471 , 2014.

**[71]** Katharotiya, Anil Kumar, Swati Patel, and Mahesh Goyani. "Comparative analysis between DCT & DWT techniques of image compression." *Journal of information engineering and applications* 1.2, 9-17, 2011.

**[72]** Shejul, Anjali and Kulkarni. "A DWT based approach for steganography using biometrics." *Data Storage and Data Engineering (DSDE), 2010 International Conference on. IEEE*, 2010.

**[73]** Hou, Yuanyuan, and Ping Zhou. "Approach on digital radiographs enhancement based on wavelet transform." *Image and Signal Processing (CISP), International Congress on. IEEE*, Vol. 2, 654-568, 2010.

**[74]** Gupta, Dipalee, and Siddhartha Choubey. "Discrete wavelet transform for image processing." *International Journal of Emerging Technology and Advanced Engineering* 4.3, 598-602, 2015.

**[75]** Nidhi Sethi, Ram Krishna, R.P. Arora." Image Compression Using Haar Wavelet Transform", *Computer Engineering and Intelligent Systems*, Vol 2.3, 2011.

**[76]** Goel, Stuti, Arun Rana, and Manpreet Kaur. "ADCT-based robust methodology for image steganography." *International Journal of Image, Graphics and Signal Processing* 5.11, 23, 2013.

**[77]** Raviraj, Sanavullah. "The modified 2D-Haar Wavelet Transformation in image compression." *Middle-East Journal of Scientific Research* 2.2, 73-78, 2007.

**[78]** Mahmoud,Mohamed, Dessouky,Deyab, Salah, and Elfouly." Comparison between Haar and Daubechies Wavelet Transformions on FPGA Technology ", *World Academy of Science, Engineering and Technology* 26, 68-72, 2007.

**[79]** Singh, Prabhishek, and Chadha. "A survey of digital watermarking techniques, applications and attacks." *International Journal of Engineering and Innovative Technology (IJEIT)* 2.9, 165-175, 2013.

**[80]** Paula Aguilera," Comparison of different image compression formats", www.homepages.cae.wisc.edu .pdf (Online):[ access at 1/3/2016].

**[81]** Hamid, Yahya, Ahmad, Al-Qershi. "Image steganography techniques: an overview." *International Journal of Computer Science and Security (IJCSS)* 6.3, 168-187, 2012.

**[82]** Jain, Yogendra Kumar, and R. R. Ahirwal. "A novel image steganography method with adaptive number of least significant bits modification based on private stego keys." *International Journal of Computer Science and Security*4.1, 40-49, 2010.

**[83]** Karim, SM Masud, Md Saifur Rahman, and Md Ismail Hossain. "A new approach for LSB based image steganography using secret key." *Computer and Information Technology (ICCIT), International Conference on. IEEE*, 286-291, 2011.

**[84]** Tayel, Mazhar B., Alaa El-Din Sayed Hafez, and Hamed Shawky Zied. "A new hybrid security allocation steganography algorithm." *Computer Engineering & Systems (ICCES), on. IEEE*, 217-220, 2013.

**[85]** Ajkamalpa, Zoraidap." Image and Text Hiding using RSA & Blowfish Algorithms with Hash-Lsb Technique", *International Journal of Innovative Science, Engineering & Technology,* Vol. 1.6,81-89, 2014.

**[86]** Muhammad, Ahmad, Farman and Jan. "A new image steganographic technique using pattern based bits shuffling and magic LSB for grayscale images." *arXiv preprint arXiv*: 1601.01386, 2016.

**[87]** Reddy, HS Manjunatha, and Raja. "High capacity and security steganography using discrete wavelet transform." *International Journal of Computer Science and Security (IJCSS)* 3.6, 462-472, 2009.

**[88]** Nag, Biswas, Sarkar, and Sarkar. "A novel technique for image steganography based on DWT and Huffman encoding." *International Journal of Computer Science and Security,(IJCSS)* 4.6, 561 - 570 ,2011.

**[89]** Prabakaran, G., and R. Bhavani. "A modified secure digital image steganography based on Discrete Wavelet Transform." *Computing, Electronics and Electrical Technologies (ICCEET), International Conference on. IEEE*, 2012.

**[90]** Renjith and Mahalakshmi. "DWT-AES based information security system for unmanned vehicles." *American Journal of Engineering Research (AJER)*, Val 3. 8, 101-112, 2014.

**[91]** Podder ,Majumdar, Kumari and Biswas. "A Wavelet-Based Text-Hiding Method Using Novel Mapping Technique." *Intelligent Computing, Communication and Devices. Springer India*, 309-318, 2015.

**[92]** Sumathi, Santanam, and Umamaheswari. "A Study of Various Steganographic Techniques Used for Information Hiding." *arXiv preprint arXiv*: 1401.5561, 9-25, 2014.

**[93]** Badr, Sherif ,Ismaial, and Khalil. "A Review on Steganalysis Techniques: From Image Format Point of View." *International Journal of Computer Applications* 102.4, 11-19, 2014.

**[94]** Chanu, Yambem Jina, Themrichon Tuithung, and Kh Manglem Singh. "A short survey on image steganography and steganalysis techniques." *Emerging Trends and Applications in Computer Science (NCETACS), National Conference on. IEEE*, 2012.

**[95]** Böhme, Rainer. *Advanced statistical steganalysis*. Springer Science & Business Media, 2010.

**[96]** Johnson, Neil F., and Sushil Jajodia. "Exploring steganography: Seeing the unseen." *Computer*, 31.2, 26-34, 1998.

**[97]** Jassim, Firas A. "A novel steganography algorithm for hiding text in image using five modulus method." *arXiv preprint arXiv:* 72 (17), 39-44, 2013.

**[98]** Akhtar, Nadeem, Shahbaaz Khan, and Pragati Johri. "An improved inverted LSB image steganography." *Issues and Challenges in Intelligent Computing Techniques (ICICT), International Conference on*. IEEE, 2014.

**[99]** Wikipedia contributors. "Mean absolute error." *Wikipedia, The Free Encyclopedia. Wikipedia*, The Free Encyclopedia, 2 Jun. 2016. Web. 8 Sep. 2016.

**[100]** Wikipedia contributors. "Signal-to-noise ratio." *Wikipedia, The Free Encyclopedia*. Wikipedia, The Free Encyclopedia, 24 Aug. 2016. Web. 8 Sep. 2016.

**[101]** Z. Wang, A. C. Bovik, H. R. Sheikh, E. P. Simoncelli ."Image quality assessment: from error visibility to structural similarity",*IEEE Transactions on Image Processing*, 13(4), 600-612, 2004.

**[102]** ECE, CSE, and M. M.U. Mullana."Image quality assessment techniques pn spatial domain." *Int. J. Comput. Sci. Technol* 2.3, 177-184, 2011.

**[103]** Silva, Karen Panetta, and Agaian. "Quantifying image similarity using measure of enhancement by entropy." *Defense and Security Symposium. International Society for Optics and Photonics*, 2007.

http://mathbits.com/MathBits/TISection/Statistics2/correlation.htm

**[104]** Emam, Marwa M., Abdelmgeid A. Aly, and Fatma A. Omara. "An Improved Image Steganography Method Based on LSB Technique with Random Pixel Selection." *International Journal of Advanced Computer Science & Applications* 1.7: 361-366, 2016.

**[105]** Joshi, Kamaldeep, and Rajkumar Yadav. "A new LSB-S image steganography method blend with Cryptography for secret communication." *Third International Conference on Image Information Processing (ICIIP)*. IEEE, 2015.

**[106]** Chandran, Saravanan, and Koushik Bhattacharyya. "Performance analysis of LSB, DCT, and DWT for digital watermarking application using steganography." *Electrical, Electronics, Signals, Communication and Optimization (EESCO), International Conference on*. IEEE, 2015.

**[107]** Vanitha, T., Souza, Rashmi, and Dsouza. "A review on steganography-least significant bit algorithm and discrete wavelet transform algorithm." International Journal of Innovative Research in Computer and Communication Engineering 2.5, pp89-95, 2014.

**[108]** Mare, Septimiu Fabian, Mircea Vladutiu, and Lucian Prodan. "Secret data communication system using Steganography, AES and RSA." *Design and Technology in Electronic Packaging (SIITME), IEEE 17th International Symposium for*. IEEE, 2011.

**[109]** Anwar, Asmaa Sabet, Kareem Kamal A. Ghany, and Hesham El Mahdy. "Improving the security of images transmission." *International Journal* 3.4, 2015.