A ROBUST ENCRYPTION AND DATA HIDING TECHNIQUE BY USING HYBRID DES AND LSB ALGORITHM

AHMED NASHAAT SHAKIR SHAKIR

AUGUST 2016

A ROBUST ENCRYPTION AND DATA HIDING TECHNIQUE BY USING HYBRID DES AND LSB ALGORITHM

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED
SCIENCES OF
ÇANKAYA UNIVERSITY

BY
AHMED NASHAAT SHAKIR SHAKIR

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE
DEGREE OF
MASTER OF SCIENCE
IN
THE DEPARTMENT OF
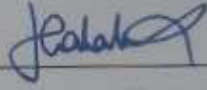COMPUTER ENGINEERING

AUGUST 2016

Title of the Thesis: **A robust Encryption and Data Hiding Technique by using Hybrid DES and LSB Algorithm.**

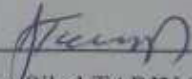Submitted by **Ahmed Nashaat Shakir SHAKIR**

Approval of the Graduate School of Natural and Applied Sciences, Çankaya University.

Prof. Dr. Halil EYYUBOĞLU
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

Prof. Dr. Müslim BOZYİĞİT
Head of Department **Y.**

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

Assist. Prof. Dr. Sibel TARIYAN ÖZYER
Supervisor

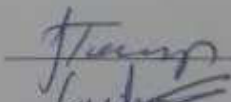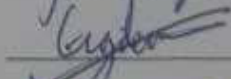**Examination Date:** 18.08.2016

Examining Committee Members

Assist Prof. Dr. Sibel TARIYAN	(Çankaya Univ.)	
Assist. Prof. Dr. Çiğdem DİNÇKAL	(Çankaya Univ.)	
Assoc. Prof. Dr. Hadi Hakan MARAŞ	(Çankaya Univ.)	
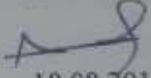
STATEMENT OF NON-PLAGIARISM PAGE

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name :   Ahmed SHAKIR

Signature   :

Date   :   18.08.2016

ABSTRACT

A ROBUST ENCRYPTION AND DATA HIDING TECHNIQUE BY USING HYBRID DES AND LSB ALGORITHM

Ahmed Nashaat SHAKIR SHAKIR

M.Sc., Department of Computer Engineering

Supervisor: Assist Prof. Dr. Sibel TARIYAN ÖZYER

AUGUST 2016, 48 pages

Information hiding is the process of hiding the details of a function, object or both. On the other hand, information hiding represents an important method that is used in data security. Another name of information hiding is the steganography which hides data inside other data, such as embedding text inside an image or an image inside another image. Steganography techniques have been used from ancient times through the use of many different mechanical ways, such as writing in invisible ink in the Greek Testament. On the other hand, Cryptography is the process of hiding information by encrypting data using a complex algorithm. It is used when collaborating over an untrusted intermediary, such as the Internet. Steganography and cryptography work similarly but in different contexts. In this study, we have presented an integration of cryptography and steganography to produce an efficient and robust model. In terms of cryptography, the Data Encryption Standard (DES) algorithm has been implemented, whereas in steganography, the Least Significant Bit (LSB) algorithm has been used. Our results show efficient time implementation and a robust algorithm mechanism in terms of Peak Signal-to-Noise Ratio (PSNR), Signal-to-Noise Ratio (SNR), and Mean Square Error (MSE).

Keywords: Data Hiding, Steganography, Cryptography, Data Encryption Standard (DES), Least Significant Bit (LSB).

ÖZ

HİBRİD DES VE LSB ALGORİTMA KULLANARAK SAĞLAM ŞİFRELEME VE VERİ GİZLEME TEKNİĞİ

Ahmed Nashaat SHAKIR SHAKIR

Yüksek Lisans, Bilgisayar Mühendisliği Anabilim Dalı

Tez Yöneticisi: Yard. Doç. Dr. Sibel TARIYAN ÖZYER

AĞUSTOS 2016, 48 sayfa

Bilgi gizleme bir işlev, bir nesne ya da her ikisinin ayrıntılarını gizleme işlemidir. Diğer taraftan, bilgi gizleme veri güvenliğinde kullanılan önemli bir yöntemi temsil eder. Bilgi gizlemenin diğer adı steganografidir; bir diğer veri içerisinde veriyi gizler, bir görüntü içerisine metin gömme ya da başka bir görüntü içerisinde bir görüntü gizlemek gibi. Steganografi teknikleri, Yunan Ahit'te görünmez mürekkeple yazılı olduğu gibi, birçok farklı mekanik yolların, kullanımı yoluyla, antik çağlardan beri kullanılmaktadır. Diğer taraftan, şifreleme, karmaşık bir algoritma kullanarak veri şifreleyerek bilgiyi saklama işlemidir. Internet gibi, güvenilmeyen bir aracı üzerinde ortak çalışılırken kullanılır. Steganografi ve kriptografi benzer çalışırlar ancak farklı bağlamlarda. Bu çalışmada, biz verimli ve sağlam bir model üretmek için bir kriptografi ve steganografi entegrasyonu sunuyoruz. Kriptografi açısından, Veri Şifreleme Standardı (DES) algoritması uygulanmışken, steganografi de En Az Anlamlı Bit (LSB) algoritması kullanılmıştır. Bizim sonuçlarımız verimli zaman uygulama ve sağlam bir algoritma mekanizmasını; Tepe Sinyal-Gürültü Oranı (PSNR), Sinyal-Gürültü Oranı (SNR) ve Ortalama Kare Hata (MSE) açısından göstermektedir.

Anahtar Kelimeler: Veri Gizleme, Steganografi, Kriptografi, Veri Şifreleme Standardı (DES), En Az Anlamlı Bit (LSB).

ACKNOWLEDGEMENTS

TABLE OF CONTENTS

LIST OF FIGURES

FIGURES

LIST OF TABLES

TABLES

LIST OF ABBREVIATIONS

ANNs	Artificial Neural Networks
AES	Advanced Encryption Standard
AI	Artificial Intelligence
BMP	Bitmap
CL-PKC	Certificateless-Public Key Cryptography
CBC	Cipher Block Chaining
CFB	Cipher Feedback
CA	Cellular Automata
DES	Data Encryption Standard
DSA	Digital Signed Algorithm
DCT	Discrete Cosine Transform
ECB	Electronic Code Block
ECC	Elliptic Curve Cryptography
GA	Genetic Algorithm
HVS	Human Visual System
IDE	ID-based Encryption
IDEA	International Data Encryption Algorithm
JPEG	Joint Photographic Experts Group
LSB	Least Significant Bit
MSE	Mean Square Error
NIST	National Institute for Standards and Technology
OFB	Out Feedback
PNS	Pseudorandom Number Sequences
PP	Pseudorandom Permutation
PKG	Private Key Generator

PINs	Personal Identification Numbers
PKC	Public Key Cryptography
PVD	Pixel Value Differencing
PSNR	Peak Signal-to-Noise Ratio
PNG	Portable Network Graphics
RSA	Rivest Shamir Adleman
SNR	Signal-to-Noise Ratio
SKC	Secret Key Cryptography
SA	Secret Awareness
WT	Wavelet Transform
WSN	Wireless Sensor Network

CHAPTER 1

INTRODUCTION

1.1 Introduction

Julius Caesar had been sending messages that contained important information to his followers, but he did not trust the messengers. Thus, he shifted the positions of the letters in order to make the messages appear meaningless. Only the one who knew the shifting value could reveal the plain message. From here, the story of data security begins. When the data can be understood, they are called plain text; otherwise, they are called cipher text, and changing the state of the text from plain to cipher is called cryptography. Cryptography began thousands of years ago and it was used very much in wars to exchange instructions and war plans. Currently, and along with the vast growth of technology and telecommunications, encryption has become a crucial tool to protect data from being tampered.

Information hiding techniques have freshly become significant in a number of different application areas, such as digital video, audio, images and many other applications. In order to achieve a powerful hiding mechanism, both steganography and cryptography are used to serve these goals. Steganography deals with composing hidden messages so that only the sender and receiver know that the message even exists, while cryptography refers to the practice and study of encryption algorithms or how to secure data transformation between two nodes in order to prevent unauthorized access to these data. This means that cryptography hides the contents of a secret message from malicious and/or unauthorized access, while steganography endeavors to conceal the presence of the message itself. Today, cryptography includes more than encryption and decryption such that encrypted messages are not modified in route paths, also provide more secure identification and authentication of communication partners.

1.2 Research Aims

Our research aims to review and study the most important techniques used in steganography and encryption processes. It covers the following areas:

1. It presents the art and techniques of encryption and steganography that are used in data protection in addition to a review of a number of previous studies;
2. It proposes a new mix of steganography and cryptography algorithms to protect data from disclosure or unauthorized modification;
3. This research focuses on confidentiality and data integrity for multimedia data. (We mainly use images that can be suitably generalized to other media types); and
4. A number of recommendations and future work will be presented.

1.3 Thesis Structure

Our research is composed of five chapters as follows:

Chapter 1: An introduction to the topic of the research;

Chapter 2: In this chapter, a theoretical overview of cryptography, its history, the types of cryptography and the most dominant algorithms that have been implemented in this context. In addition, this chapter will present an overview of steganography and the types of steganography as well as the algorithms inside this type of data protection.

Chapter 3: This chapter discusses the most common research and studies which present cryptography and steganography, followed by reviews of the methods that have adopted a combination of both.

Chapter 4: In this chapter, we will review the proposed algorithm, discuss the implementation process and the results obtained.

Chapter 5: This chapter presents the conclusion and our recommendations for future work.

CHAPTER 2

BACKGROUND

2.1 Introduction

The vast and rapid growth of technology and all of its aspects are affecting our daily life style. Using computers, and more recently mobile devices, has become an essential part of our daily activities. On the other hand, networking, communication and social media applications see our data exposed and prone to being hacked at any time. This begs a very important question: "Are we correctly securing our data, especially the most important data?" If the answer is "yes," then, is the level of security satisfactory? Let us assume we ask paranoid people such questions. In fact, we hear many stories everywhere about hackers and crackers and the many frequent attacks that are being recorded. This justifies the necessity for the adoption of information security with many informational aspects.

The Internet nowadays represents an essential medium that is being used to perform most of our daily tasks in addition to connecting tens of millions of people. Moreover, it is increasingly being used to perform web-based operations and business, such as bank transactions, e-commerce, and online shopping. Such operations totally depend on the Internet in order to be performed; thus, security for such activities is tremendously important and it needs to be heavily embedded when working in an Internet environment.

Information security can be implemented in several ways according to the nature of the task and the level of importance. It may be employed using conventional techniques, such as passwords and Personal Identification Numbers (PINs). It also can be performed using more advanced technologies, such as biometric authentication, which may be implemented in a unimodal or multimodal manner where more than one biometric is used [1,2].

A number of security methods access control, such as authentication; however, it can be used to make any hacked data meaningless even if captured from different media. Cryptography is one of the most effective approaches that have been taken to change plain information into ambiguous meaningless data. It has played a key role in many data security fields even before the invention of technology and the Industrial Revolution.

Another way used to protect information is to hide it in another type of information, which is called data hiding, or steganography. This kind of security contributes to protecting data in a way that masks the information to conceal it and make it difficult to observe. Whether cryptography, steganography, or both are used, the hiding of data should be implemented with a high level of efficiency and accuracy so as to fulfill the required purpose for which it was designed. In the upcoming sections, we present an entry-level view for both techniques and look more deeply at the main characteristics of both approaches.

2.2 Cryptography

Cryptography is a method of sending or receiving secret information in an unknown manner. It is also known as encryption. Cryptography is not a modern technology. In fact, history has recorded many attempts at encryption used in earlier times. The first form of cryptography occurred around 1900 B.C. in ancient Egypt, where an inscription has been discovered written in a nonstandard hieroglyph [3]. Some experts have claimed that the appearance of cryptography techniques dates back to the invention of writing, with different perspectives ranging from diplomatic missives to war plans.

In 400 B.C., it was recorded that the Spartans were writing their messages on leather strips wrapped around a cylinder in a transposition cipher method. They used the cylinder diameter as the secret key [4]. See Figure 1.

```
   ---------------------------------
    /T/H/I/S/I/S/_/          / \
   / /H/O/W/I/T/            |   |
  / /W/O/U/L/D/              \ /
   ---------------------------------
```
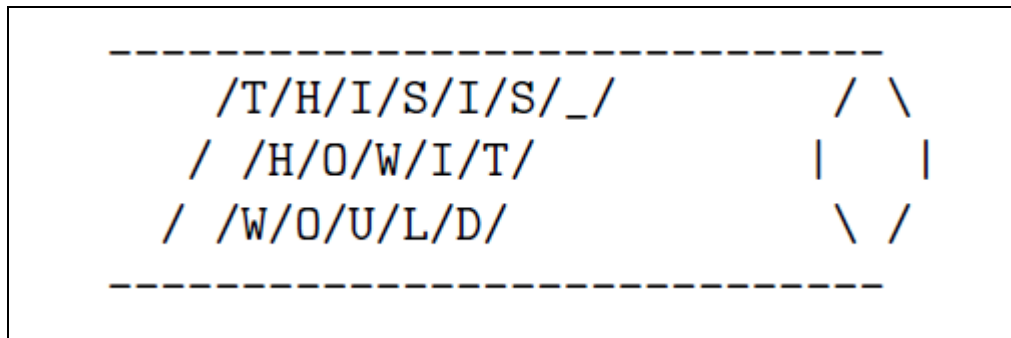
Figure 1 Spartan cryptography method [4]

Julius Caesar used one of the most familiar techniques of cryptography represented by the substitution of letters. The cipher shifts three letters to the right. In the English alphabet, the method would send the letter D instead of A, B for E, and C for Z [5]. British Playfair also was a method of encryption that used the substitution of letters. Charles Wheatstone devised it in 1854, but Lord Playfair, who developed the method, changed the name later on. In a simple technique, it encrypts a pair of letters (a digraph) rather than using a single character. Playfair was hard to break due to the complexity of frequency, which is difficult to specify. This technique was widely used for tactical issues by the British forces during times of war [6].

After that, and according to the new technology represented by the invention of computers, mobile devices and telecommunications, there is no doubt that the science and techniques of cryptography have developed accordingly. In spite of the variety of cryptography techniques, cryptography itself represents the science of transforming plain (clear) text into cipher (cryptogram) text. This process of changing text, or messages, is also known as encryption. The process of reversing an encrypted text to its original state (plain text) is called decryption. Both of these processes are controlled by a single key or multiple keys [7]. Figure 2 shows the basic encryption diagram.
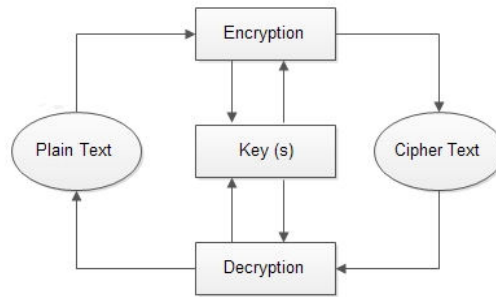
Figure 2 Basic encryption diagram

Working in an application-to-application environment, there are a number of security requirements that have to be taken into consideration, such as:

- **Authentication**: This is the technique that is used by any system or application to verify and specify identity, and determine the level of access for the identity. A well-known form of authentication is normally based on something we know (knowledge-based), such as passwords, or something we have (token-based), such as ID cards, or something inside our body (biometric), such as fingerprints [8]. When these kinds of authentications are spoofed, information can be easily captured.

- **Privacy**: This ensures that no one can view the information except the intended receiver.

- **Integrity:** This is the process of ensuring that an intended message should arrive at the desired entity in a form that is identical to the original message.

- **Non-repudiation**: This is the process which is used to prove that the message was really sent by the valid sender.

Generally, cryptography not only protects our data from spoofing or alteration, it is also a method of authentication. It especially provides a means to convert any important information such that it is useless even when the data is captured. There are various methods and algorithms to implement cryptography, ranging from simple techniques to complex ones. In the following sections, the most predominant cryptography algorithms are presented.

2.3 Cryptography Algorithms

Cryptography is divided into two main approaches which are typically employed to perform different types of cryptography:

- Secret/Private Key Cryptography (SKC), also known as symmetric cryptography; and
- Public Key Cryptography (PKC), also known as asymmetric cryptography.

Despite the variety of cryptography algorithms, they all share the same principle for every case. Encryption means converting plain text into cipher text, and decryption means converting the cipher (encrypted) text into plain text.

2.3.1   Secret Key Cryptography (SKC)

This approach uses a single key for both operations (encryption and decryption). Where the sender of the message uses a key or a rule set to encrypt a specific plain text, the sender then sends the encrypted message (cipher text) to the intended receiver, after which the receiver uses the same key (rule set) to transform the cipher text into plain text. Since the same key is used in this method, it is called symmetric encryption [3]. With this method, the essential issue is that, the key should know for both of encryption parts (sender and receiver); accordingly, a challenge occurs in such cases, which is the difficulty and the risk of keys distribution.

There are a number of characteristics which clearly describe symmetric cryptography as:

- The performance of the approach that is faster in comparison to other encryption techniques.
- The encrypted message (cipher text) that can be sent onto a stream or link with no concern for the transferred data if they are interrupted or captured since the key can be transmitted separately with different links. Hence, the low possibility of data being decrypted, and in some cases no possibility of decryption.
- SKC can be compounded with other conventional security authentication techniques, such as passwords to ensure the reliability of transmission.

- In systems that rely on symmetric encryption, only the key owners can obtain the plain information. This enhances the process of reliability.

In spite of the aforementioned advantages of the symmetric approach, it also comes with some limitations which sometimes hinder the usability of this method [9]. As mentioned before, the main challenge of the SKC approach is related to the process of key distribution. As commonly known, every communication medium is considered to be an insecure environment since the transmitted data are always prone to being interrupted. To overcome such problems, the keys are exchanged personally or by using a different medium of communication.

SKC comes with a variety of schemes which are commonly categorized as either stream ciphers or block ciphers. The first type is a crucial class of SKC [10], since they simultaneously encrypt characters individually using the binary digits of the plain message. On the other hand, block ciphers encrypt a set of characters in the plain text using constant encryption transformation. If a comparison between the two types is made, stream ciphers are found to be faster and have less complexity than block ciphers. In addition, stream ciphers are a more suitable form for some telecommunication applications. Furthermore, and due to the buffering processing of data transmission; stream ciphers become more appropriate, especially when dealing with limited buffer ability, so that the characters can be individually sent and received, such as when using mobile devices [11].

The common stream cipher form is known as a self-synchronizing stream cipher. This term comes from the behavior of this mode, such that the encryption process continues to remain in a synchronized case simply by knowing how far the n-bit key stream is. Self-synchronizing produces a key stream in the form of an independent message stream such that it uses the same function to generate a key stream on both sides (sender and receiver). Since self-synchronizing does not result in a propagation error, it repeats the key stream to ensure that the process is completed. Block ciphers, on the other hand, can run in one of many forms, which are described as follows:

- Electronic Code Block (ECB): This is the mode that can be represented as the process where each block of plain text has a specific and corresponding block value in the encrypted text (cipher text) and vice versa (i.e. the value of the plain text block will definitely come out with the same value for the cipher text). ECB

is commonly used when the plain text is divided into a number of blocks; in other words, ECB has the capability of supporting a separated key for each block of plain text. ECB is considered to be a less efficient technique when dealing with small blocks as well as for identical encryption mode. This is due to the nature of language in which some words or phrases are at times being reused. That which produces a duplication of block parts, and accordingly the cipher text, can easily be attacked.

- Cipher Block Chaining (CBC): According to its name, CBC is performed with a chaining mechanism so that the decryption process of any encrypted block depends on preceding cipher text blocks. According to the validity of the blocks, which proceeds to the current block, it is contained in the instantly previous block. The main challenge of this mode is that when a bit error occurs, all blocks in the same process will be affected since each block in the CBC is XORed with the previous cipher text block and it will be encrypted [12].

- Cipher Feedback (CFB): This mode implements the encryption operation by dividing the data to be encrypted into units with sizes smaller than the block size. The CFB mode works similarly to CBC since it follows a chaining mechanism where the block sequence plays a key role in the overall encryption process [13].

- Out Feedback (OFB): This mode works in a way that is similar to a synchronized stream cipher. The mechanism of OFB is represented by the prevention of the same plain text block from producing a same cipher text throughout the mechanism of internal feedback, which works independently for both plain and cipher blocks. Figure 3 represents the encryption in different cipher modes.
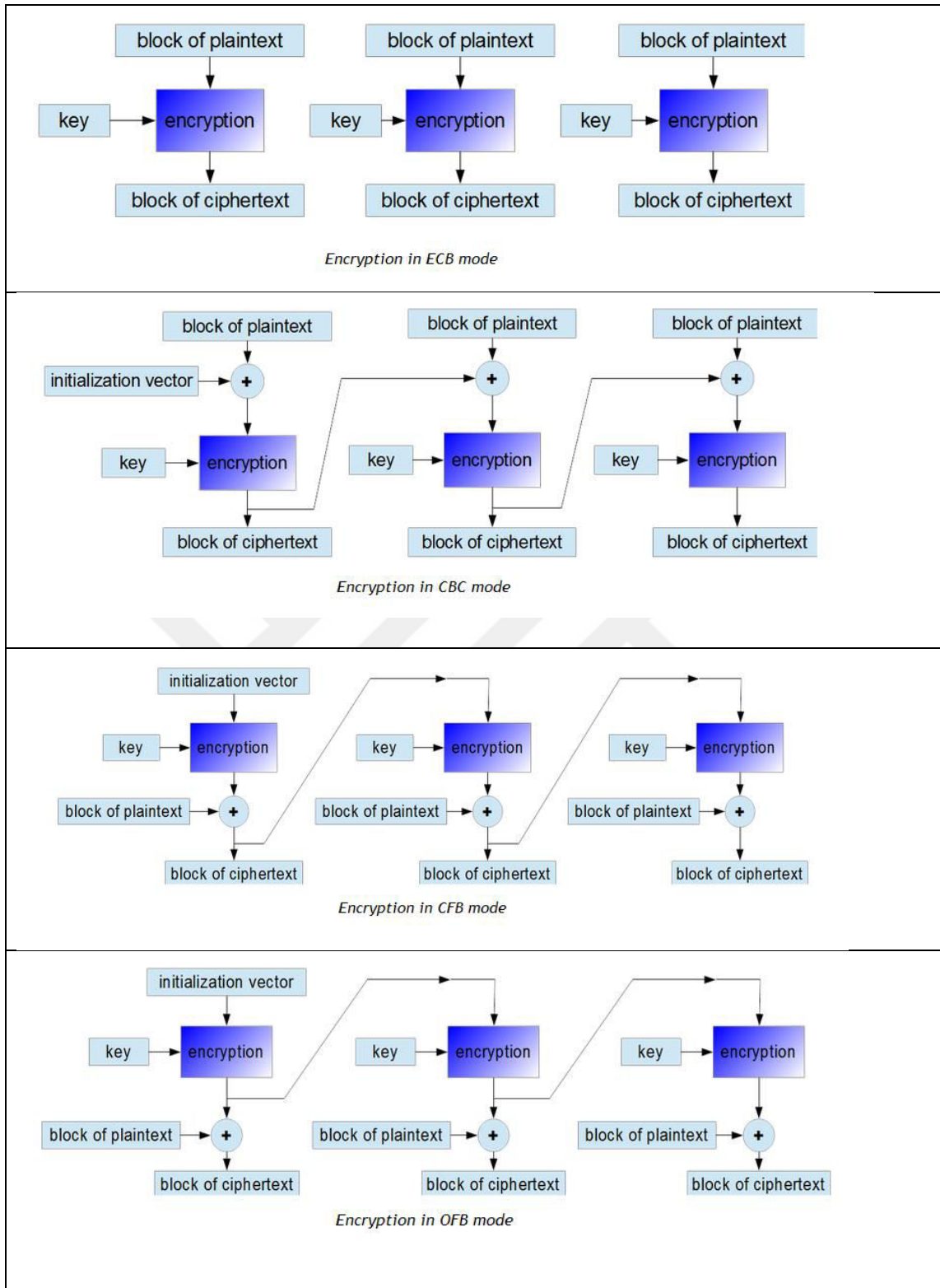
Figure 3 Different cipher encryptions [13]

2.3.2   SKC Algorithms

Today, there are number of algorithms that have been invented and implemented under the context of SKC. In the following sections, the most well-known algorithms will be illustrated in addition to the main characteristics of each algorithm.

2.3.2.1 Data Encryption Standard (DES)

IBM developed this method in the 1970s. It was adopted by the National Institute for Standards and Technology (NIST) in 1977 for commercial applications. DES was the very first encryption algorithm approved by the US Government, Therefore, DES was rapidly used by many industries, including financial services since financial data require efficient encryption. In addition, DES was employed and embedded with various systems due to its simplicity, including with smart cards, SIM cards, and many network-based applications and devices, such as routers, switches and modems.

DES follows the block cipher mechanism to perform encryption; hence, it applies the keys to blocks rather than bits at a time. It also employs a 56-bit key that runs on 64-bit blocks. In addition, DES involves a set of complex rules and operations which are designed to produce fast hardware performance. However, software implementation of DES is considered slow; therefore, and due to today's need for applications to be fast, especially in real time applications, DES has become a less desired encryption algorithm.

- **DES Operation Structure**

As mentioned previously, DES uses a 56-bit key, which is separated into eight blocks with 7 bits per block. The last bit for each block is assigned to an equity bit (0 or 1). In spite of DES using 64 bits for encryption, only 56 bits are actually used. This is for computational purposes and to ease the randomness process. Figure 4 shows DES structure.
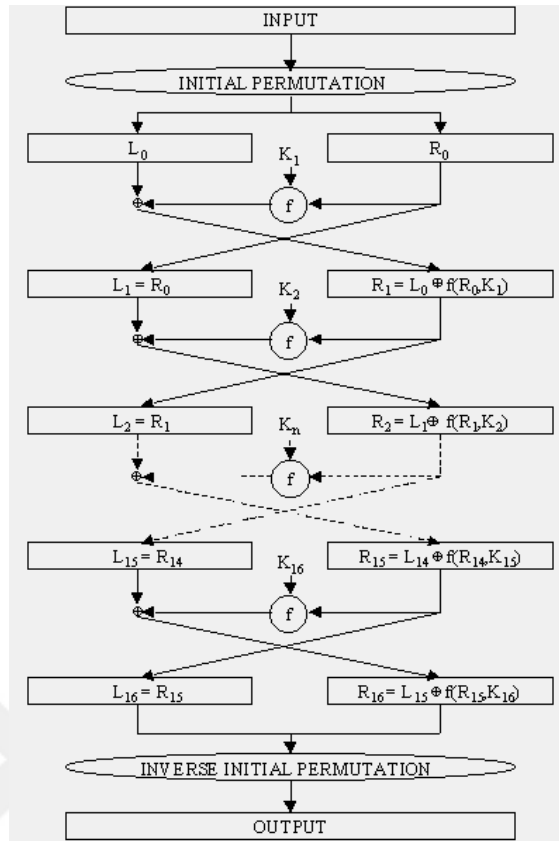
Figure 4 DES structure

After this, DES assigns 64 bits for the plain text with 16 rounds of replacements (permutation) steps, and substitution. The overall initial steps of DES are as follows:

A. To encrypt a 64-bit block, it should be assigned to an initial permutation (IP). In this step, each bit is transferred to a new position; for instance, moving the sixth, seventh and eighth bits to the 55th, 56th and 48th positions respectively.

B. All 64 bits, which are produced from the previous step, are divided into two blocks of 32 bits, known as left and right, each of which are assigned to an initial value, namely L_0 and R_0.

C. After block division is completed, a specific formula is implemented in 16 rounds, for both L an R. The formula can be seen as follows:

$$L_n = R_n - 1 \quad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots(2.1)$$

$$R_n = L_n - 1 \; XOR \; f(R_{n-1}, K_n) \dots\dots\dots\dots\dots\dots\dots(2.2)$$

12

Where *n* represents the number of rounds (i.e. 1 to 16). For each step in the process, each L block is simply taken from the previous block (R block). Then, the new value of R is calculated by applying a bit-by-bit XOR of the L block within the outputs of applying the DES algorithm (f) to the prior R and K_n, where K_n represents a value of 48 bits derived from the 64-bit DES key. For each round, every K_n differs from the other according to the standard key schedule algorithm.

D. The output of the last round (L_{16}, R_{16}) is merged to produce 64 bits and is reproduced in an inverse IP to be (IP-1). After that, the position of the bits is reordered to the original values. In order to do that, the 55th, 56th and 48th are set back to the values of 6th, 7th, and 8th respectively [11,14 and 15] .

DES is considered to be more vulnerable because it is widely used to encrypt texts; therefore, it is most vulnerable to so-called "brute-force" attacks, which are implemented by repeating a large number of keys to break the cipher text. Nevertheless, the DES effectively resists such attacks since it implements 64-bit encryption. In addition to that, and for text messages, there is a variety of letters and punctuation to be used, thereby adding more complexity to the encrypted message to be broken? Thus, for 64-bit blocks, there are approximately 2^{64} values, which is a very huge number of characters to be correlated. In our study, we will employ the DES algorithm due to its simplicity and effectiveness.

2.3.2.2 Advanced Encryption Standard (AES)

AES was founded in 1997, and in 2001, it was announced by NIST as an enhanced algorithm. After DES, AES is considered to be one of the most suitable symmetric algorithms. In addition, it is fast for both software and hardware [16]. The process of AES has a fixed size of blocks with 128 bits or 256 bits. AES runs on a 4×4 array of bytes called as a state. The cipher of AES is determined as a number of rounds similar to DES. Inside these rounds, the plain text is converted to cipher text. For each round, there are a number of processes, including key generation and position changes. AES also applies a number of reverse rounds to return a block to the plain text by using specified keys.

2.3.2.3 International Data Encryption Algorithm (IDEA)

IDEA was developed in 1992 in Switzerland. It follows the block-cipher mechanism within a key of 128 bits. It comes with a high level of security and is known as one of the best encryption methods. IDEA shows good resistance against several attacks. A few modifications have been applied to the original algorithm. IDEA can work with all forms of encryption as listed under NIST. A block cipher encrypts and decrypts plain text in fixed-size bit blocks. When the message exceeds the block size, the algorithm divides the message into blocks of the same size and processes each block individually. The implementation of the IDEA algorithm has a number of characteristics listed below [17]:

- IDEA produces a high level of security.
- The process of IDEA is simple and easy to trace.
- It can be used with a variety of applications.
- Implementing this algorithm on hardware incurs a lower cost.
- It can be use efficiently in terms of protecting privacy and authentication.

2.3.2.4 Blowfish Algorithm

Blowfish was developed in 1993. It follows the block encryption method. The algorithm uses the key of variable length starting from 32 bits and continuing to 448 bits, which is what makes it suitable for various encryption purposes. In addition, this algorithm is considered to be one of the fastest block cipher algorithms. The main drawback of the Blowfish algorithm is the key changing mechanism, where generating a new key needs a number of pre-processing steps which cost about 4 kb of memory for the needs to be specific to each key. This is considered to be slow in performance in comparison with other algorithms [18 and 19]. In the context of SKC, there are other algorithms that have been developed and implemented. Each algorithm has its own advantages and drawbacks which are determined according to the type of application. We mentioned the above methods to highlight the overall

14

encryption behavior which is almost similar in its principles. Thus, we focused on the most related algorithms to the method that is being implemented in this research.

2.3.3   Public Key Cryptography (PKC)

It is also known as an asymmetric encryption approach. It was developed by Martin Helman and his student, and officially declared by Stanford University in 1976 [20]. PKC was first implemented with a two-key cryptography system where two parties connect to each other in a secure manner through a non-secured communication channel with no key sharing. This kind of encryption relies on what is commonly known as a one-way function, where the encryption functions are easily implemented; the decryption process is also very easy. To understand the idea of the last statement, we can assume that to find the product of two prime numbers, such as 7 and 3, there would be almost no time and it will be 21. Another way to the same problem may be what prime numbers result in 21 when they are multiplied by each other? In this situation, in order to find the result, there are more processes and trials to be done, especially when there are more complex numbers.

Generally, PKC implements two keys which are not identical. However, they are mathematically related. Nevertheless, knowing one key does not mean that the other key can be easily determined. In other words, to encrypt plain text, there is a specific private key and to decrypt a cipher text, there is another key. It is not necessary to determine which key is applied first. The crucial point is that both keys are necessarily required to complete the whole process.

With PKC, one key is created as a public key since it can be publicly shared between the two encryption parties. Another key is created as a secret key, which is never uncovered to the other party. To clarify this idea, let us assume that someone (party A) wants to send a message to another person (party B), then party A encrypts a part of the information using party B's public key; party B decrypts the encrypted information using his own private key. One of the main features of this method is that it can easily know and prove the sender of the message since a part of his public key was employed. Figure 5 describes the PKC structure.
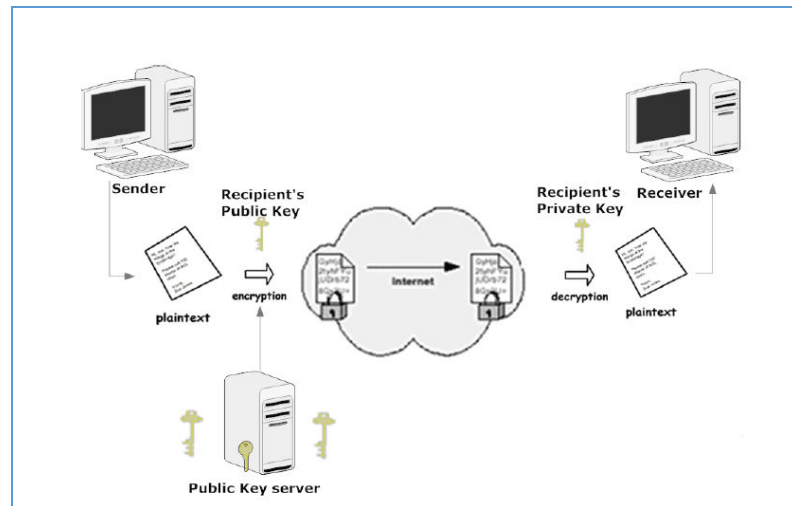
Figure 5 Public key cryptography (PKC) approach

The PKC algorithm can be efficiently used to implement applications that require a high level of confidentiality, such as authentication. This has a number of advantages:

- It produces a better mechanism for the keys distribution in comparison to SKC.
- PKC produces a good level of confidentiality and can be implemented to develop authentication-based applications.

Even though PKC can perform well, it works more slowly than the symmetric approach due to the complexity of mathematical operations and calculations that are used inside the text conversion functions, thereby necessitating more time for processing for PKC [21].

One of the most well-known algorithms that fall under the PKC approach is Rivest-Shamir Adleman (RSA). This algorithm was presented in 1977. It uses the mechanism of factorization of integer numbers into their prime factors. It also uses a variable sized encryption block, as well as variable sized keys. The keys are created from a very large number since the public key of this algorithm has a large number of digits. Attackers will face difficulties when specifying the prime number that is to be used to generate the key. This is what makes RSA a very secure algorithm [21 and 22]. There are more algorithms that adopt the PKC style, such as Diff-Hellman [23], the Digital Signed Algorithm (DSA) [24 and 25], and so on. In this research, the SKC method is used to produce simplicity and quick implementation since it

combines cryptography with steganography using images. Hence, the speed of the technique plays a key role in this context.

2.4 Steganography

The term *steganography* comes from the Greek roots *stegano* (covered) and *graphos* (to write). It is, therefore, the science of hiding information in other information. Steganography is implemented in a manner that makes the information unseen but existent [26]. The various uses of steganography were recorded for thousands of years. In the 5th century B.C., Histaiacus used the first form of information hiding by shaving a slave's head, then writing a message on the slave's skull in a manner similar to tattoos nowadays. He then sent the slave on his way after the slave's hair had regrown [27].

Some Arabic manuscripts, dating back approximately 1200 years and written in a secret manner [28], were found in Turkey and Germany. Five-hundred years ago, the invention of an ancient Chinese secret writing method involved using masking paper with holes in it, where when the mask was placed over another paper, a secret message would be revealed [27]. Figure 6 shows an example if this kind of steganography.
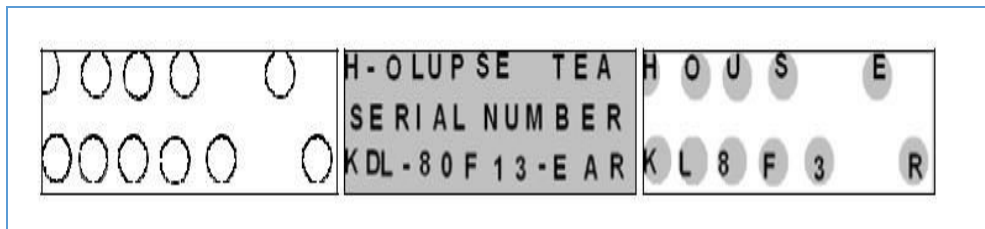
Figure 6 Ancient Chinese steganography [27]

It also has been reported that the Nazis developed many information-hiding techniques during World War II, including invisible ink, null ciphers, and microdots [29 and 30]. Morse code is one of the most common methods of steganography that have been employed, especially in wars. For example, in 1945, Morse code was concealed in a drawing as in Figure 7, where the long blades of grass refer to Morse dashes and the short blades of grass refer to Morse dots [27].
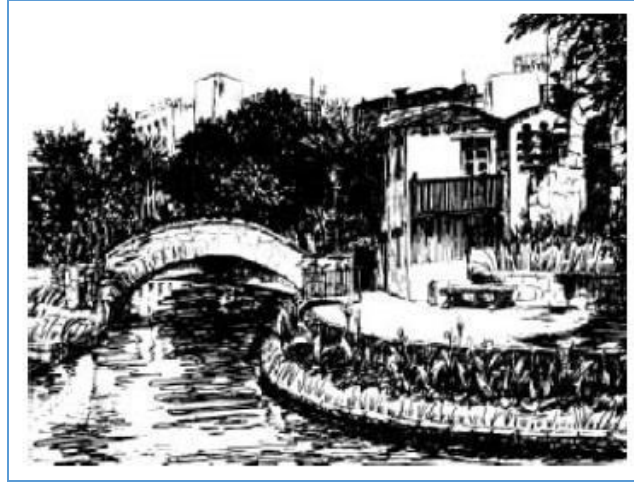
Figure 7 Morse code hidden inside a drawing [27]

Steganography works similarly to cryptography in terms of data protection. Steganography hides information by making it invisible inside other data so that eventually it cannot be understood. Cryptography converts the message such that it is not useful until the message is revealed again through decryption.

Nowadays, steganography plays a key role in many applications, such as audio, video and images. In addition, the concealment of information is increasingly being used with pictures in the manner of hidden serials, signatures and invisible cryptography, which can be used to prevent unauthorized use for different purposes. Furthermore, steganography is being used widely in military communications to insure the security of traffic such that it is considered to be more secure rather than depending on encryption only. Despite the increasing development of modern encryption technologies, many studies and applications prefer information hiding to cryptography and this is due to the suspicion reduction. For example, the text messages are always prone to being attacked because they arouse suspicion in contrast to an image, which seems normal; in fact, the image may include hidden information inside it [31].

To sum up, encryption is about protecting messages by changing the context of the message, whereas steganography is about covering the information so as to be concealed inside other information. It is the same idea of using invisible ink or adding echo noise an audio file. Initially, steganography drew less attention than cryptography; however, nowadays this field of study has become more desirable in

the research community. As a result, steganography has been adopted in various applications. Some of these fields include the following:

- Military field: In spite of the encryption being used, a message is still under threat of being attacked, and once the message is interrupted, there is the possibility of revealing information using different methods, as mentioned previously. Hence, hiding messages inside other data (an image for instance) will hinder an attacker from acquiring any original information.

- Law and Intelligent Agencies: Steganography in this context has intense interest since it can be used to determine the strengths and weaknesses of many methods to trace and reveal hidden information and messages. It has applications in fraud data detection.

- Digital Elections: Sending Emails, tracing anonymous communication, and marketing: All of these areas urgently require a robust and efficient method of steganography.

In the aforementioned paragraphs, we stated that steganography is an information hiding technique. This is the main idea; however, hiding plain information inside an image, for instance, will put the information at risk despite the data being invisible. The modern trend of digital steganography is to mix information hiding with a specific cryptography technique. This approach can produce more efficient and robust applications. Where insert encrypted data in other bit will defiantly enforce security performance [32].

Currently, it is obvious that most applications and data run through the Internet. In addition, using multimedia data over the Internet has been growing rapidly. Multimedia data includes images, videos, audio, and so on.

2.4.1 Types of Steganography

In general, there are two types of steganography [32], namely *fragile* and *robust*. The former embeds information directly into the file. If the file is adjusted, it will be destroyed. This technique is inconvenient in general since the modification process is complex. However, it is useful for low-level evidence due to the fact that fragile steganography is considered to be a simple and easy method.

Robust steganography, on the other hand, tends to embed data into a specific file such that it makes the file difficult to destroy, thereby deeming this type of steganography robust. In this type of steganography, the modifications that are required to remove a specific mark would fail since the hidden part is difficult to specify.

2.4.2 Steganography Algorithms

There are a number of algorithms that have been presented in the context of steganography in the following sections, and since this research focuses on crypto-stegano methods for images, image-based steganography methods are presented in the following sections.

2.4.2.1 Least Significant Bit (LSB)

This is one of the most popular techniques used to hide information. LSB is a simple method to perform steganography [33], that is similar to every other steganography method. LSB embeds data into an image so that the data cannot be detected or observed by a normal observer. This technique replaces some of the image pixels with hidden information inside an image. Although other techniques embed data inside images, LSB does the same work with least significant bits. This process contributes to reducing color variation such that it makes the changes almost undetectable. Such as change is a color numeric value by one and the second change by two and so on.

Since steganography in general endeavors to hide information at a minimum level of variation, LSB specifically performs well in this context. Additionally, LSB provides a mechanism that embeds lossless data to be hidden and keeps all information about the data with less space taken.

2.4.2.2 Pseudorandom Permutation (PP)

This is considered to be a more complex steganography technique since all the bits on the cover image can be accessed through the process of embedding. The bits, which are inside the hidden message, are randomly distributed within the cover image. In addition, there is a random number being generated to act as an index that is used inside the encoding process.

PP mainly works to ensure that the-hidden information is not embedded inside an image with the same order, thereby making the PP difficult to attack. Nevertheless, the PP mechanism's distributing the bits randomly may produce a high-noise image when there is a large amount of embedded hidden data [34].

2.4.2.3 Cover Regions and Parity Bits

In this technique, the cover image is divided into a number of separated regions. Then, each region is used to store bits of information to be hidden instead of using an element. During the encoding process, each region of the cover encodes one key for the steganography process. When decoding the message; all the bits are reconstructed to reveal the hidden message as plain information [35].

2.4.2.4 Quantization and Dithering

The difference between the adjacent pixels is calculated and quantized. In this method, the difference between the quantized signals is calculated to generate the secret key [36].

2.4.2.5 Information Hiding in a Binary Image

A high level of redundancy in the binary images is produced. In the composed form of black and white, it is produces the binary image, this method considered as simple, but it does not present robust results due to the limited variety of binary images [37]. In summary, several techniques have been employed in information hiding with images. In this research, the LSB algorithm will be presented due to the simplicity and efficiency of this algorithm.

2.5 Chapter Summary

From all aforementioned sections, there is no doubt that the growth in Internet-based applications and business has come out with a number of threats, which may put data at risk. Therefore, there should be a mechanism that provides convenient protection to overcome such threats. In addition, the security should not only protect the data themselves, it should also provide a secure medium for data exchange. A number of security procedures have been developed to enhance information exchange reliability. Some of these are based on developing authentication systems, which can range from conventional tools to biometrics. There is also a trend to secure data and online transactions, which is changing the appearance of data. This trend is known as encryption or cryptography. Furthermore, an enhanced method of data protection has been developed, which comprises information hiding techniques or steganography. This approach hides data inside other data. Either cryptography or steganography can be implanted with good performance when a good algorithm is involved. Advanced data protection can be obtained by combining both cryptography and steganography into one model. This can produce a sophisticated framework when depending on the advantages of both approaches.

CHAPTER 3

REVIEW OF LITERATURE

3.1 Introduction

In this chapter, the studies and research that have been presented in the context of cryptography and steganography will be illustrated. The chapter is divided into three main sections. The first section is an overview of the studies of cryptography and how it has developed and implemented. The second section presents the research on steganography. Finally, yet still importantly, the third section will discuss the combination of cryptography and steganography and how they are combined in one model.

3.2 Cryptography

In this section, a number of studies which have been conducted on cryptography will be shown. There will be two sub sections, the first of which presents the works that have been implemented under SKC, and the second of which will discuss the works on PKC.

3.2.1 Secret Key Cryptography (SKC)

With the growth of Internet-based applications and communications, much business is conducted over the Internet. Therefore, working in such an environment is critical due to threats of attack and hacking. Providing secure media in such areas plays a key role. Accordingly, there are several studies that have been implemented in terms of communication security. In [38], the authors proposed a Cellular Automata (CA) encryption method. This method relies on SKC outlines. CA is considered to be a generator of Pseudorandom Number Sequences (PNS). According to the rules of CA,

the performance was good which then led to good enhancement in cellular applications development since CA makes applications more resistant to different attacks.

A security approach depending on SKC has been presented in [39]. The main idea of this method is that the key is embedded inside the source code of encryption at every node of the process in order to protect the other keys. In cases of the specified node number being physically captured, the plain data cannot be revealed, thereby remaining protected. The key selection in this method is generated using the ID of the node and other information, and then a manipulation function is applied to generate the encryption key. The grouping nodes can produce minimum memory, which is taken by the overhead case. The presented method performs well against different types of attacks.

A new security encryption method has been produced in [40], (which is known as Secret Awareness (SA)), in the form of certificate less cryptography. In this method, the method showed that the security presented is better than that presented by public key certificate less encryption. In addition, it makes the certificate less scheme perform more efficiently.

A content-based algorithm has been presented in [41], which implements a bit-wise circular shift process. Since the SKC approach relies on the confidentiality of keys exchange, a high level of secrecy is used. The encryption key is generated by separating each single digit of the key from which a digit is selected randomly and then converted to its corresponding binary number.

After that, a left-wise rotation is performed for each digit performed to the corresponding binary number; then it is stored in a matrix. The decryption process of this algorithm represents the absolute reverse process. This algorithm provides a simple encryption technique by applying the process on the binary numbers. In addition, it produces efficient encryption with a high level of resistance towards any variety of attack.

3.2.2 Public Key Cryptography (PKC)

PKC has also been implemented in many studies due to its efficiency and confidentiality. The algorithms produce sophisticated performance, but they are slow techniques due to their computational complexity. This brings different challenges when adopting such algorithms in specific applications and devices with limited hardware capacity, such as mobile devices. However, such devices are widely used to perform our daily activities, including various communications. In cases of developing an application to work on mobile devices, it is highly recommended to use a robust encryption technique. Applying PKC outlines in applications and methods that run on such devices will come with high-energy consumption due to the complexity of PKC.

A study of quantifying the cost of energy for the authentication and key exchange is presented in [42]. The method produces a comparison between the Rivest-Sahmir and Adlemen (RSA) algorithm and the Elliptic Curve Cryptography (ECC) algorithm. The outcomes of the study proved that the ECC performed better in comparison to RSA.

Many devices nowadays work in an environment of so-called Wireless Sensor Network (WSN). The messages which go back and forth through such media are required to be private and secured. Working with WSN is wrought with a number of limitations, especially when using mobile devices due to the limited capacity of such devices regarding processing and storage. In addition, messages are sent using sensor nodes. In order to establish a secure channel, the sensor must acknowledge the keys. With WSN, performing this task is not easy due to the limitations of the devices.

To overcome such problems, a study presented in [43], proposed a new key distribution scheme for PK algorithms within WSN transmission nodes. The method took into consideration different types of parameters to be evaluated, such as energy consumption, memory, processing, scalability, and so on. The outcomes of the study showed that the proposed method mitigated the memory usage. Moreover, it provided good security performance against attacks. Additionally, the scheme provided node-to-node authentication, which ensures the prevention of node duplication.

Cryptography in general includes two main sections, namely certificate-based and ID-Based. Both sections have their respective advantages and limitations. However, there have been a number of studies that have produced a combination of the two approaches. In [44], the authors presented a hybrid scheme of PK structure. In ID-based encryption (IDE), generating the private key is the most crucial stage. In [45 and 46], the authors proposed a unique private key issuing protocol in the Single Authority Multiple Observer (SAMO) model. This model reduces the load of user authentication significantly, but it is prone to attacks because of the lack of variable authentications.

A study was presented in [47] to overcome the aforementioned problem. It uses a combination of a public key and secret key using the ID-based concept. The method presented an efficient implementation by considering the advantages of both SKC and PKC.

In the concept of PKC, the public key should be transferred securely. In other words, combining the key with the sender or receiver identity should be digitally certificated. At this stage, the overhead problem arises along with digital certificate generation. ID-based structure overcomes such difficulty. The Private Key Generator (PKG) is responsible of generating secret keys derived from user identity. According to the behavior of PKG represented by putting some user information as a part of the encryption key, this technique is highly prone to a large number of attacks, which attempts to recover user identity. To overcome this problem, a new mechanism is presented in [48].

The method is called Certificateless-Public Key Cryptography (CL-PKC). In this method, the certificate of the key is avoided. Additionally, many public keys are linked to an identity, which helps in cases of losing some of the private key.

With PKC, there are a number of mathematical operations that are applied during the encryption process. These operations include data decompositions and discrete logarithm problems. With the growth of computers and applications, common PKC algorithms encounter a number of limitations and difficulties. Those difficulties can be overcome with a method presented in [49]. The presented algorithm is based on the Elliptic Curve Discrete Algorithm problem. The method resulted in a short public key and hence less bandwidth required. This helps to enforce resistance to attack.

26

In addition to the common methods that are used for different cryptography purposes, cryptography can be reinforced with the adoption of Artificial Intelligence (AI) techniques. It obvious that the AI trend can present high and sophisticated performance of computer related activities. In the same context, Artificial Neural Networks (ANNs) plays a crucial role it is adopted in different types of research forms [50].

A study presented in [51], was based on the Hebbian learning rules in order to present ANN training for both sender and receiver parties. In the proposed method, the public key generation is performed using the Genetic Algorithm (GA). The method presented showed good performance and opened the doors toward further implementation possibilities for ANN with cryptography.

3.3 Steganography

In Chapter 2, deep insight is given to highlight the main characteristics of steganography and how it has developed along with the growth of the technology. In the upcoming sections, an overview of the most significant studies and research are illustrated, most notably for image steganography since it is more germane to our study.

The aim of using steganography is to prevent any suspicious intrusion into the private message data. If an attacker can access the hidden information, the steganography fails. The success of steganography, or information hiding, depends on the level of secrecy. Even if the steganography is discovered, there should be a robust algorithm that makes the revealed data useless. In [32], a method was presented to provide secret message compression. The method embeds data in BMP and PNG images. The reason for using such image formats is due to the fact that they are lossless, which means that the information can be preserved during the processing. The method presented a proper mechanism to perform the steganography wherein more information is put inside an image according to the data compression.

One of the most common approaches of steganography is Pixel Value Differencing (PVD), which is generally used in data hiding in images. A study was presented in [52], to analyze the main characteristics of a PVD-based algorithm, in addition to

proposing an enhanced algorithm for steganography depending on the content adaptive scheme. In this method, the image is divided into small squares, after which the squares are rotated 0º, 90º, 180º or 270º. Then, the image is divided into embedding units. The method keeps statistical features by storing the bits in a certain order. As a result, the method showed better security performance in comparison with previous PVD-based methods.

A new algorithm was presented in [53]. The proposed method embedded binary codes and data into an image. The authors used a zipped file before converting it to binary. This provides more storage for the data to be inserted inside the image. The new algorithm is tested with a variety of data sizes stored in an image. The proposed algorithm was efficient and performed well.

Steganography can also be implemented on communication security. A channel encoding security model was presented in [54]. The model achieved an embedment, extraction and steganography mutually according to the pseudorandom sequence to improve performance security. By implanting the model, the outcomes showed that the security performance improved.

In the same context, a new method for steganography in data communication was presented in [55]. The method used halftone images to enhance security performance as well as storage capacity. The method also computed the complexity of every pixel in the image. The result was a high level of quality and a significant reduction of errors.

A new method of steganography was presented in [56]. The authors proposed a combination of a secret sharing mechanism as well as a novel steganography method using the Wavelet Transform (WT). The secret image was encoded using a secret sharing technique. In addition, the cover image was hidden using specific techniques. The outcomes of the study stated a high level of security and robust performance.

A new LSB-based method was presented in [57]. The proposed method was in the form of software detection. The system implements three LSB algorithms to analyze the performance and then generate a finite automation description for the behavior of data hiding. The system produced a reliable detection of LSB steganography in different implementations.

A novel universal steganalyzer for compressed JPEG images was proposed in [58]. The method produces a new steganalytic feature, which represents the ratio between multiple ranges of a normalized coefficient histogram. After that, a strong blind detector was constructed with a one-dimensional feature. The method implements a number of experiments with a significant performance. It can also detect the additive noise of steganography. Furthermore, the method can specify the JPEG compression, which brings many promises in applications development. A new system of information transfer was presented in [59]. The system used JPEG images, which were previously processed with a data hiding tool named (Steg App1.1.0), which was also created by the authors. The method uses information created by an MS Word document. This tool is based on the transformation of the selected picture with a specific technique. The performance of the system was evaluated and worked properly, similarly to the commercial SteganPEG tool.

A novel image for color image steganography was proposed in [60]. The algorithm was implemented with three-phase of intelligent techniques to produce more sophisticated steganography for color images. The first phase was devoted to implement the learning, where the number of bits to be embedded inside the image is estimated. This process was performed using ANN combined with the genetic algorithm. The remaining phases were assigned to implement the steganography processes. The performance was evaluated and compared with other similar methods. The system was immune against three different types of attacks. In addition, the performance showed a high level of efficiency in terms of embedding large amounts of data with 12 bits per pixel.

A new method based on a combination of the strength edges detection with XOR coding was presented in [61]. The encoded image was concealed with a private message using the Wavelet Transform. The edge detection was used to identify the sharp edge in the cover image since the embedding process causes less degradation of the quality of the image compared with other pixel-based techniques although it is difficult to differentiate between sharp and smooth edges. This behavior is similar to the Human Visual System (HVS), which has less sensitivity towards the changes of image states regarding sharpness, edges and contrast.

The proposed algorithm processes the sharp edges of the image first, and then moves to the less sharp areas. The results demonstrated better performance for the steganography in comparison with other methods in addition to demonstrating a higher level of security.

To sum up, steganography techniques have developed increasingly due to the vast growth of technology. People nowadays are using Internet-based applications and methods almost daily. With this growth of data transmission over the Internet and through communication channels, the need to provide a secure environment is urgently required. Steganography can meet this requirement; however, it needs more sophisticated trends to perform any information security perfectly. By combining steganography with cryptography, we can come out with enhanced performance since protection will increase.

3.4 Combining Steganography with Cryptography

Encryption and data hiding can be combined into one model to enhance the performance of data security. In the following section, a number of studies, and research that deals with a crypto-stegano approach, will be demonstrated.

Using cryptography or steganography separately can be combined with some issues. A study presented in [62], implemented both steganography and cryptography. The method evolved and iterative process design. In addition, the encoding properties were tested to ensure its functionality and performance. A number of breaking methods were applied to the proposed method and the method presented good performance in terms of security.

A method of merging the encryption within the data hiding was proposed in [63], in the context of image processing. The proposed system performed cryptography and steganography simultaneously by using the image firstly as a cover to perform the steganography, and the same image again used to generate the encryption keys. The system performed efficiently for the steganography as well as the unbreakable cryptography.

A lossless synthetic model was proposed in [64]. This method combines encryption and data hiding to protect medical records from being altered. The method showed a

new trend in protecting multimedia information found in medical record documents. For information hiding, the method adopts the LSB algorithm.

The method outcomes showed a good performance regarding the security. In addition, the output image was smaller than the original image, which facilitates the process when working with communication channels. A new project of integrating cryptography and steganography was developed in [65]. The developed system employed the AES algorithm for cryptography to encrypt the data to be inserted inside an image. In addition, for steganography, the system adopted the Discrete Cosine Transform (DCT) algorithm. The proposed system showed a high level of security and reliability since it depends on high-performance algorithms.

A new method to secure the data from tampering was presented in [66]. The method used Unicode symbols to send the message through a communication channel. Those symbols had been hidden inside the image before they were sent. The system proposed a new method for data security with a more efficient mechanism in comparison to traditional methods.

CHAPTER 4

IMPLEMENTATION AND DISCUSSION

4.1 Introduction

In order to produce an efficient and robust mechanism model, we will propose a mechanism that suggests integration between the improved Data Encryption Standard (DES) cryptography algorithm by using an irrational number (to increase the randomness of the sub key generation used in the DES algorithm), and a data hiding technique by using the Least Significant Bit (LSB) steganography algorithm. First, we will encrypt the data with the key using the improved Data Encryption Standard (DES). We then take this encrypted data and put them into the host image by using the Least Significant Bit (LSB) steganography algorithm. In addition, our proposed mechanism covers both the encryption and decryption algorithm for both the Data Encryption Standard (DES) and the Least Significant Bit (LSB).

4.2 Proposed Algorithm

In this section, we will discuss both the Data Encryption Standard (DES) and the Least Significant Bit (LSB), and how our mechanism works along with implementations and the test part for each algorithm.

### 4.2.1 Improved DES Cryptography Algorithm By Using Irrational Number

As discussed in Chapter 2, DES Operation Structure (DES) normally uses a 64-bit structure distributed as follows: a 56-bit key, which is separated into 8 blocks with 7 bits per block. This means that DES actually uses only 56 bits with 8 bits being used in randomness processes. Overall, DES assigns a 64-bit key for the plain text with 16

rounds of replacement (permutation) steps and substitution. It is clear that this method is not practical or efficient in the present day. In classic DES work, the sub keys used are identical in a group and the key space is slightly smaller. Today, information and communication technology have reached an advanced stage of development, and this has led to the emergence of a new generation of malware. Therefore, the use and adoption of relatively old technologies now could lead to great harm at any work level. It is worth mentioning here that by using the classic DES method, it takes 20 minutes on today's computers to decode them.

To solve this problem, we suggest using the improved data encryption standard (DES) 64-bit key cryptography algorithm with an irrational number. An irrational number is used here for two reasons. First, it extends the key space in the DES algorithm and increases the probabilities of the sub-keys in each group. A normal DES algorithm is shown in Figure 8. Figure 9 shows the DES algorithm based on an irrational number.
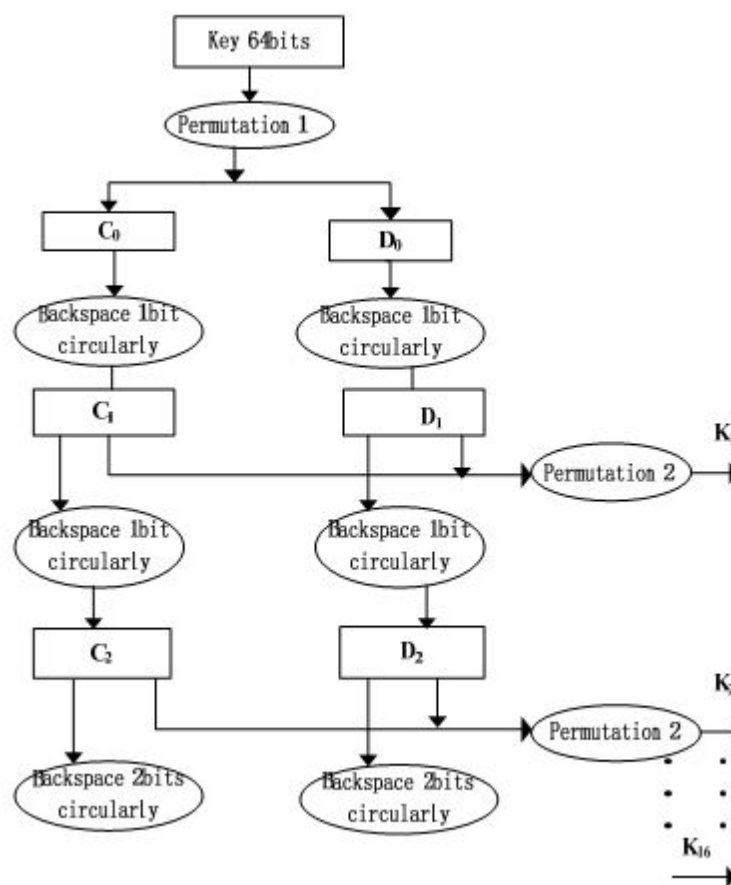
Figure 8 Normal DES algorithm sub-key generation
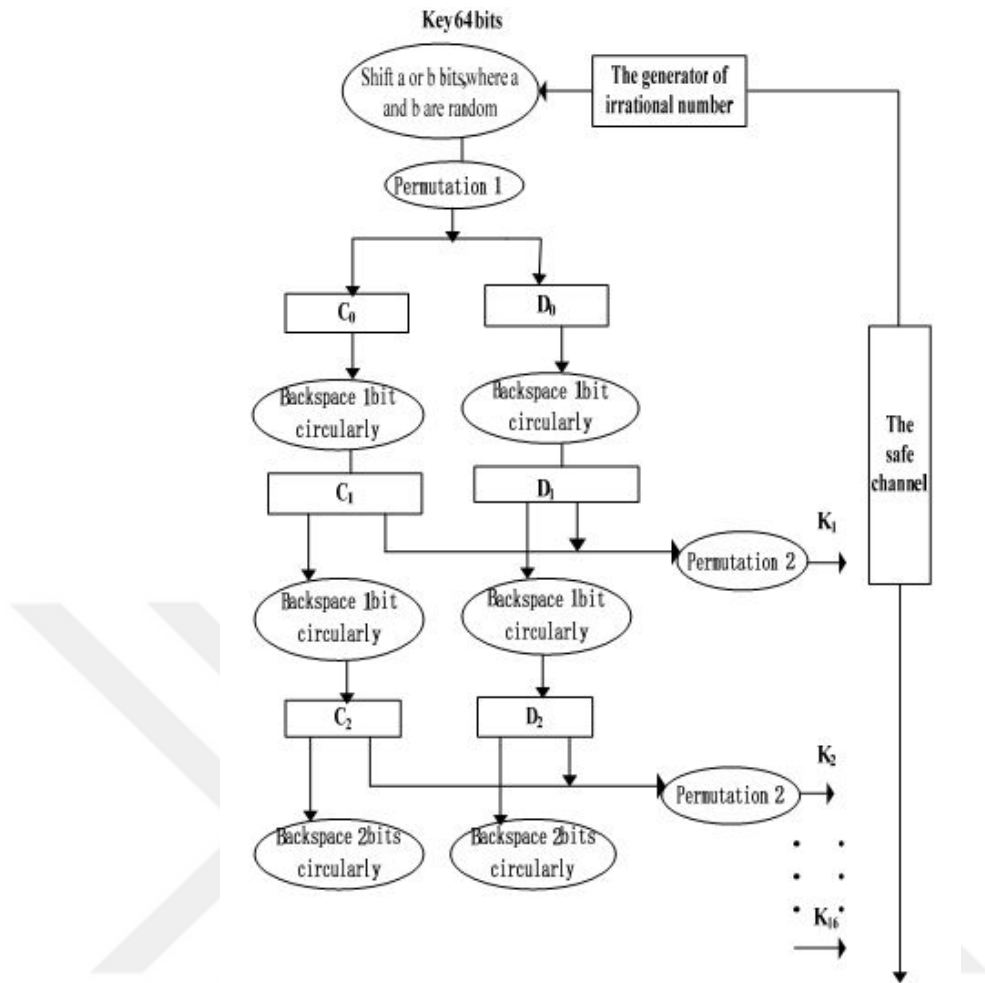
Figure 9 DES algorithm based on an irrational number

As shown in the figure above, 'a' and 'b' are measured based on an irrational number. This information of 'a' and 'b' is used in the shifting process of the production key. The irrational number will be part of this key, which will increase the arbitrariness in the DES sub key, and consequently, increase the robustness of the DES algorithm. Our sub key operates as follows: when two-digit numbers are nominated after two irrational number points in π arbitrarily, 'a' and 'b' will be measured based on the following: if 'a' is equivalent to the first irrational number selected, and 'b' is equivalent to the other irrational number, this will allow an exclusive-or (X-OR) circuit (it means Exclusive disjunction or exclusive or is a logical operation that outputs true only when inputs differ (one is true, the other is false)), to produce an (X-OR) between these two numbers and another two numbers selected in the same way. If we obtain an odd result, it means it will shift 'a' bits; if

34

we obtain an even result, 'b' bits will be shifted. We used MATLAB to implement our code and for the generation of the irrational number. Figure 10 shows our work diagrams for the DES algorithm.

4.2.1.1 DES Encryption Process

Inputs: Plain Text Message 256 bit, Key 64-bit, Irrational number.
Output: Cipher Text Message

- Read the plain text message from the input window
- Read the host key from the input window
- Read the irrational number generated by the code
- Process of the DES rounds and initial permutation
- Process of the cipher function, E-XOR operation with the round key data (E-XOR operation is fed into an S-Box array)
- E-XOR operation between the key data and round data
- Inverse initial permutation
- Cipher text message is produced
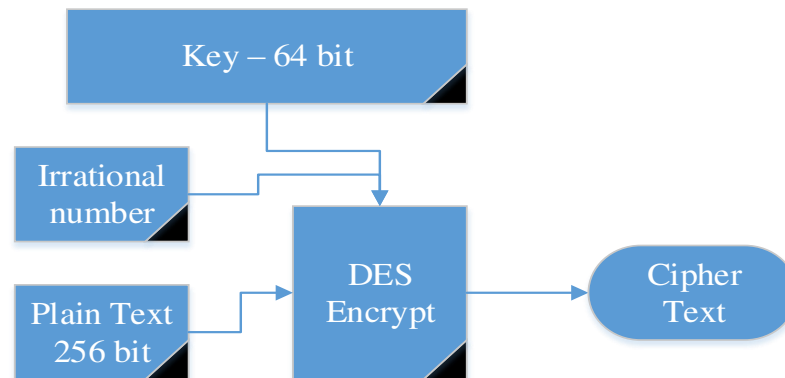
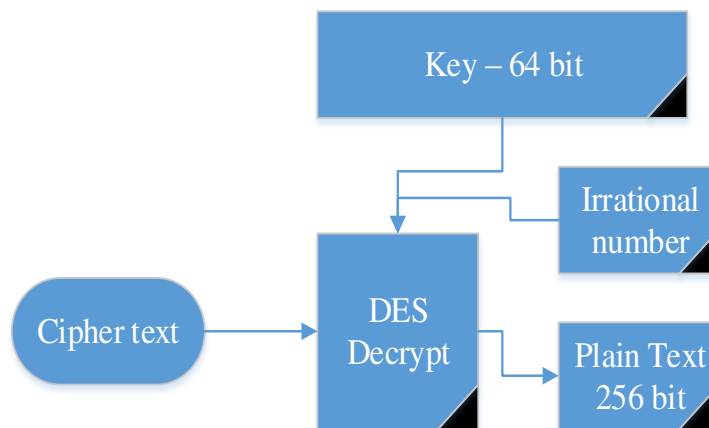**Figure 10** DES encryption process

4.2.1.2 DES Decryption Process

Inputs: Cipher Text Message, Key 64-bit, Irrational number.

Output: Plain Text Message 256 bit

- Read the Cipher Text Message from the input window
- Read the host key from input window
- Read the irrational number generated by the code
- Reverse the process of the DES Rounds and the initial permutation
- Process of Cipher Function, E-XOR operation with the round key data (E-XOR operation fed into an S-Box array)
- E-XOR operation between the key data and the round data
- Inverse initial permutation
- Plain text message is produced

Figure 11 shows the DES decryption process; Figure 12 shows the overall DES encryption and decryption process.



Figure 11 DES decryption process
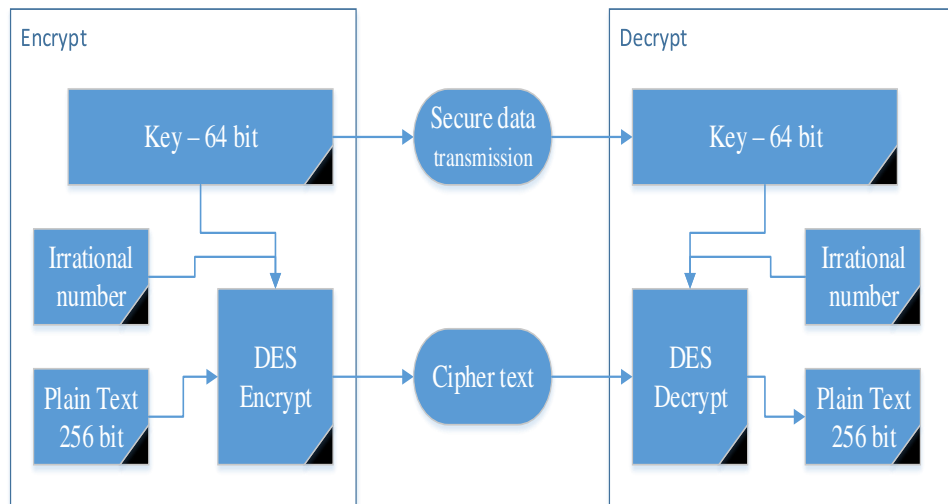
Figure 12 DES algorithm

4.2.2 Least Significant Bit (LSB) Steganography Algorithm

As explained above, in our proposed algorithm, we used both cryptography and steganography. Cryptography was implemented by using the improved DES, and in steganography, we used the least significant bit algorithm. We used a 256×256 bitmap as a cover image RGB (it means color model is an additive color model in which red, green and blue light are added together in various ways to reproduce a broad array of colors), component and hid the 256-bit cipher text in a mutable location within a cover image. The main purpose of using both techniques is to increase the robustness of our algorithm. Figures 13 and 14 show the working mechanism of the least significant bit algorithm.
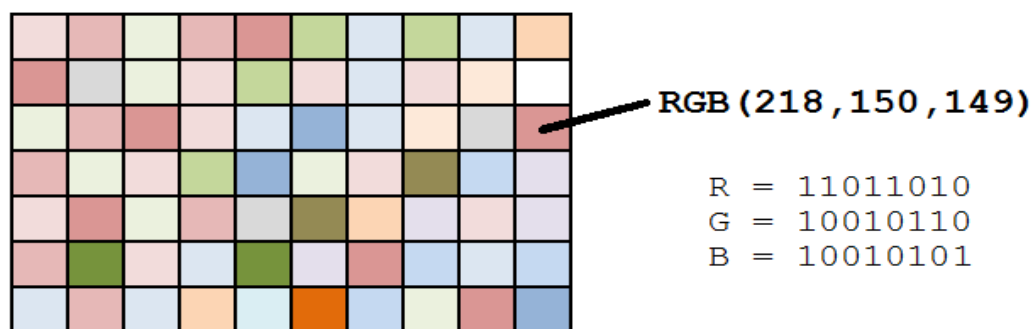
Figure 13 Working mechanism of least significant bit algorithm
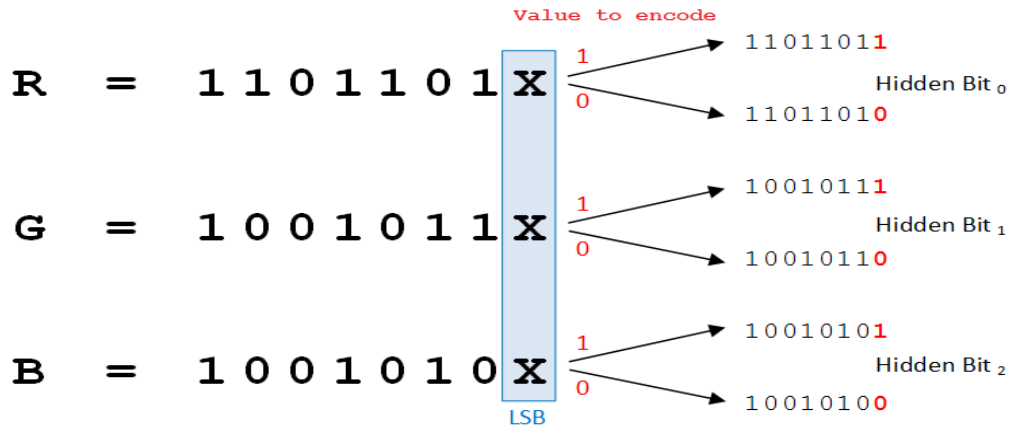
Figure 14 Selection mechanism of the least significant bit algorithm.

We assume that we have cover image "I (i, j)" and we want to create a steganography image "IS (i, j)" and our message bit will be "Mb" Then the message embedding process is as follows:

IS (i, j) = I (i, j) - 1, if LSB (I (i, j)) = 1 and Mb = 0 …………………….……….(4.1)

IS (i, j) = I (i, j), if LSB (I (i, j)) = Mb …………………………………………..(4.2)

IS (i, j) = I (i, j) + 1, if LSB (I (i, j)) = 0 and Mb = 1 ……………….……………(4.3)

The result will produce a steganography image "IS (i, j)." The extraction process of the message is the reverse process of the above equation, as follows:

IS (i, j) = I (i, j) +1, if LSB (I (i, j)) = 1 and Mb = 0 ………………………………..(4.4)

IS (i, j) = I (i, j), if LSB (I (i, j)) = Mb ………………………………………… (4.5)

IS (i, j) = I (i, j) - 1, if LSB (I (i, j)) = 0 and Mb = 1 ………………………………..(4.6)

4.2.2.1 LSB Embedding Algorithm

Inputs: Host image (256×256), and Cipher Text Message

Output: Steganography image (256×256)

- Read cipher text message from text file that results from the previous encryption process by the improved DES algorithm
- Read host cover image
- Read the RGB component from the host cover image where the message should be embedded
- Read the last bit in each pixel of the host cover image in order to embed our cipher text message
- Embed the cipher message bits into the LSB location of each host cover message pixel
- Production of the steganography image

The LSB embedding process is shown in Figure 15 below.
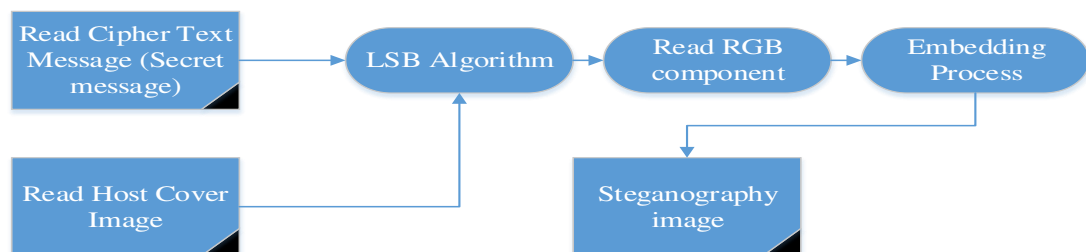


Figure 15 LSB embedding process

4.2.2.2 LSB Extraction Algorithm

Input: Steganography image (256×256)

Output: Cipher Text Message (Secret message)

- Read steganography image (256×256)
- Read the RGB component for each pixel in the steganography image
- Extract the last bit of each pixel in the steganography image
- Convert each pixel bit into a decimal value
- Extract message value to the secret message text file

The LSB extraction process is shown in Figure 16 below, While Figure 17 shows the overall Embedded and Extraction Process
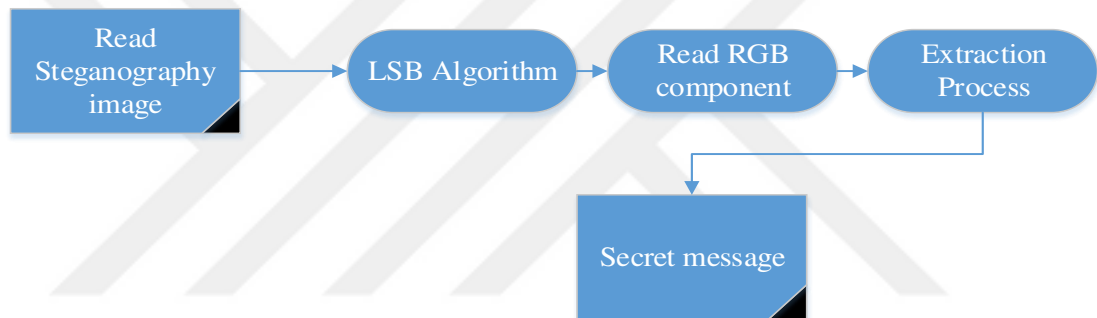
Figure 16 LSB extraction process
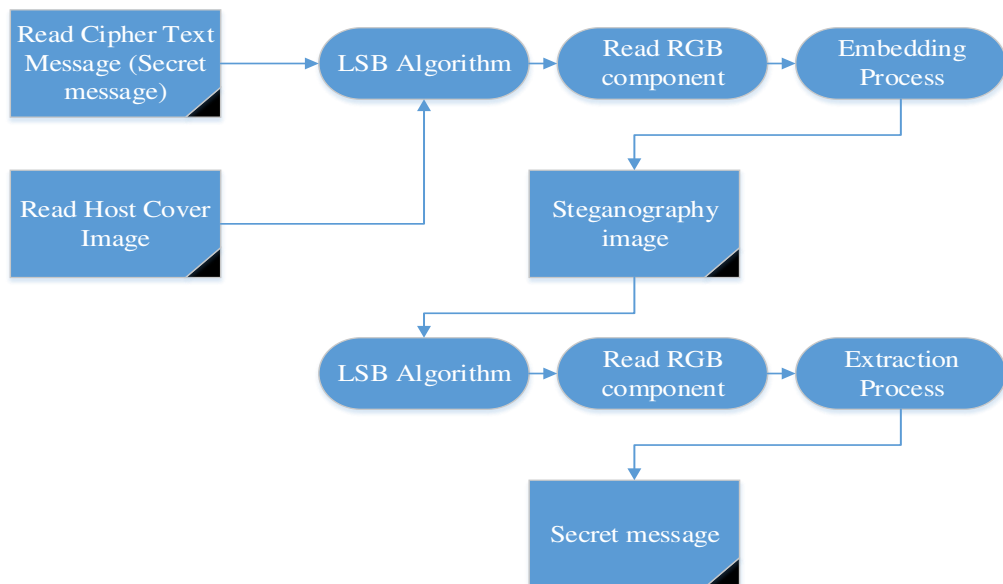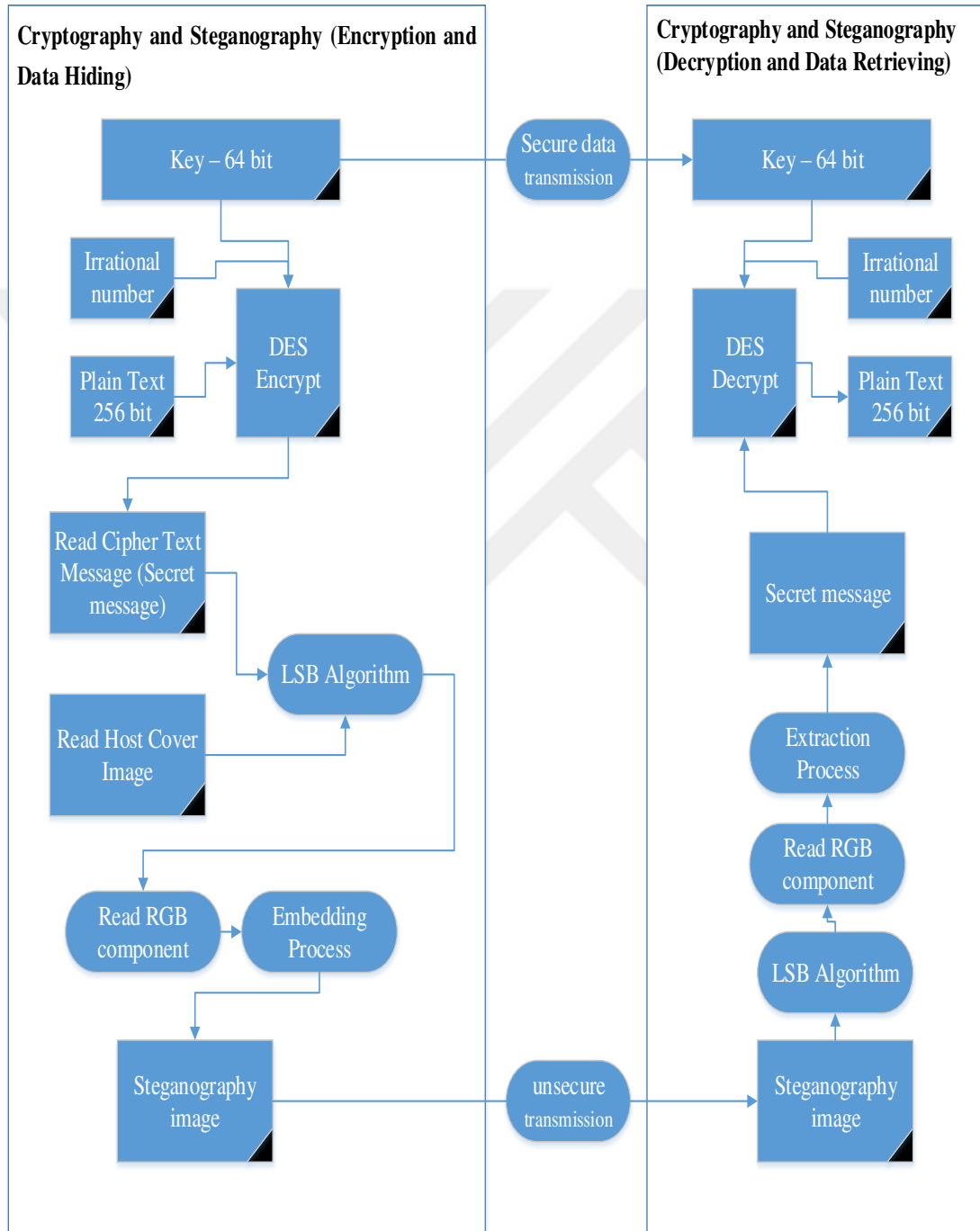

Figure 17 LSB embedded and extraction process

4.2.3 Overall Workbench

The integration between the improved Data Encryption Standard (DES) cryptography algorithm by using an irrational number, and the data hiding technique by using the Least Significant Bit (LSB) steganography algorithm are shown in Figure 18.

Figure 18 Overall workbench for the proposed algorithm

The proposed algorithm was made using Matlab code and through the use of three interfaces also built using Matlab code, as shown in Figures 19, 20 and 21 below.

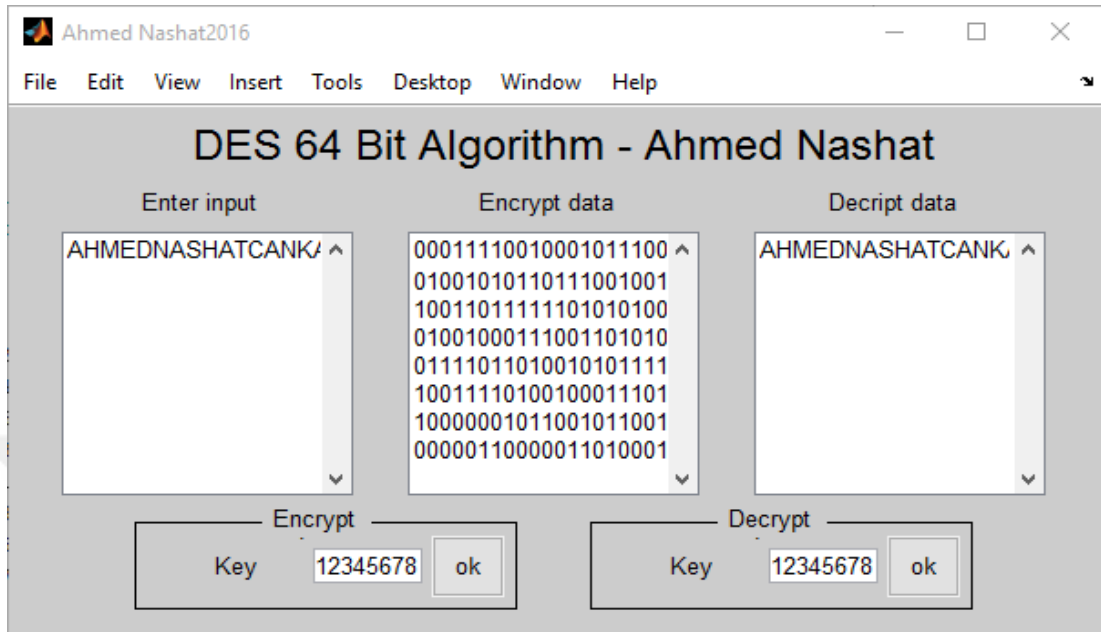
Figure 19 DES algorithm interface

Program code windows above show, our main DES application, include following box windows, first input (the text message along with key box entry), second is encryption data box (text message after DES apply) , third is decrypt data box (present the original text message after decrypt DES apply along with key box).
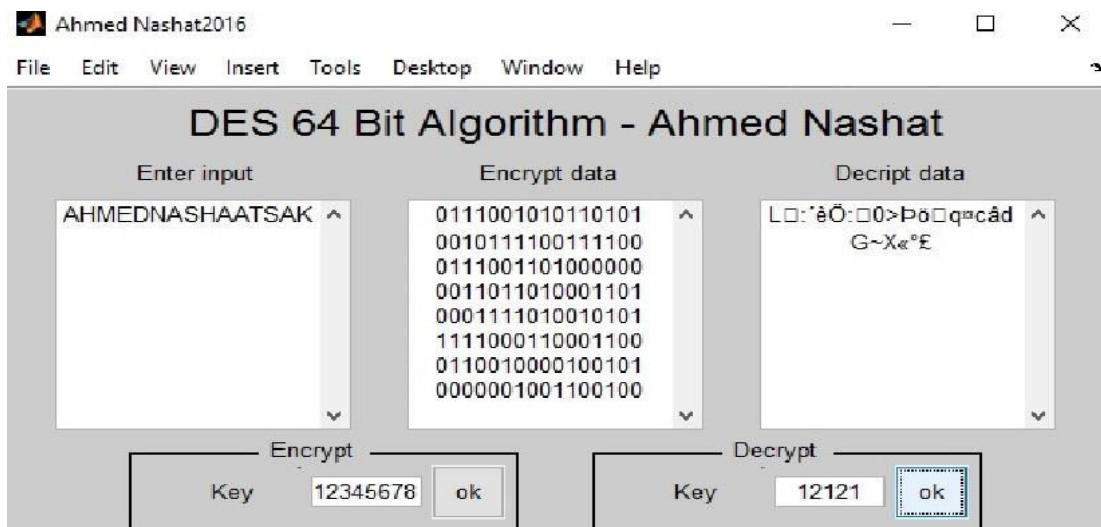

Figure 20 Examination placebo key

Program code windows above show, our main DES application, when try to enter incorrect key in decrypt key box, her we use key (12345678), while we inter incorrect key for decrypt process (12121), the result show we cannot read the encrypt message without having the right key.
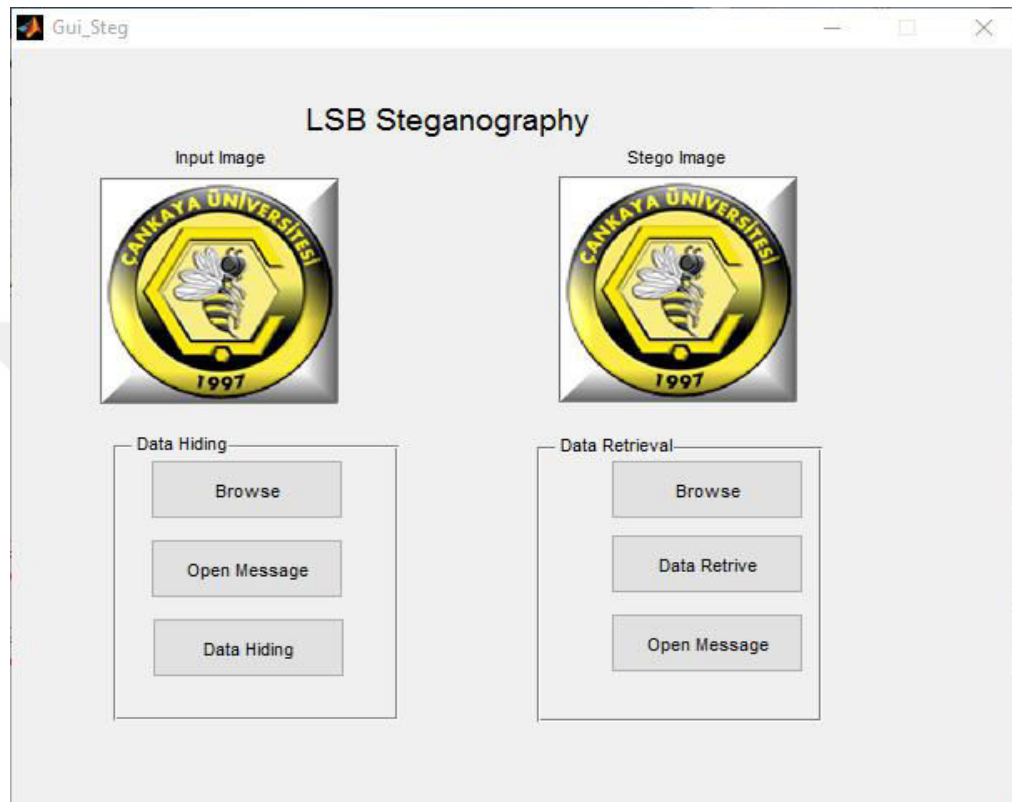
Figure 21 LSB algorithm interface

Program interface above show our LSB algorithm interface, include two part , the first part is input image, her we should select host image and encrypted message come from applying DES algorithm and finally applying our LSB algorithm. While the second part is concerning with message data retrieve, here we should select our steganography image and applying invers LSB algorithm to get our data retrieved.

4.2.4 Performance Test

In our proposed algorithm, the initial input is plain text and our final output is a steganography image. In this case, we should use many concepts to test our proposed algorithm, such as testing the performance of the improved DES algorithm by comparing it with normal DES implantation, Peak Signal-to-Noise Ratio (PSNR), Signal-to-Noise Ratio (SNR), and Mean Square Error (MSE) used to test the quality of the steganography image. Table 1 shows the comparison made between the time implementation of the normal DES algorithm and the improved DES algorithm for both the encryption and decryption processes. The results were obtained by applying mutable time implementations in the same plain text and with the same key for each initial round.

Table 1 DES encryption and decryption performance test

Encryption in Second time	Encryption in Second time	Decryption in Second time	Decryption in Second Time
DES	Improved DES	DES	Improved DES
0.7809	0.7805	0.7784	0.7779
0.7730	0.7720	0.7423	0.7329
0.7730	0.7073	0.7820	0.7817
0.7847	0.7077	0.7742	0.7732
0.7382	0.7330	0.7771	0.7708
0.7927	0.7907	0.7741	0.7737
0.7474	0.7350	0.7421	0.7332
0.7844	0.7840	0.7738	0.7639
0.7733	0.7710	0.7703	0.7307
0.7321	0.7290	0.7778	0.7739
0.7877	0.7007	0.7713	0.7701

The Peak Signal-to-Noise Ratio (PSNR), Signal-to-Noise Ratio (SNR), and Mean Square Error (MSE) were used to test the quality of the image. A high quality image should go over more than 30 dB [67,68 and 69]; this means a higher value for PSNR and SNR mean high quality for the image and quality algorithm, as we assume we have host image "I (i,j)", and a steganography image " IS (i,j)", where "i" and "j" are the dimensions of the image. Then the PSNR, SNR and MSE can be calculated from the following:

$$\text{PSNR} = 10\log_{10} (I_{signal})^2/\text{MSE} \quad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots(4.7)$$

$$\text{SNR} = 10\log_{10} (I_{signal}/I_{noise}) \quad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots(4.8)$$

In addition, the mean square error (MSE) can be calculated from the following:
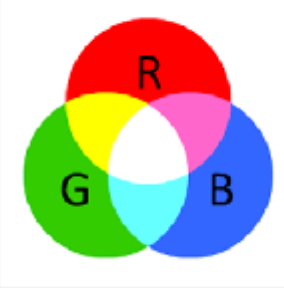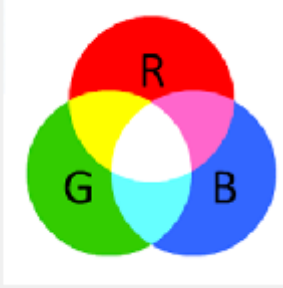
$$\text{MSE} = 1/I*J ((IS-I)^2) \quad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots(4.9)$$

Table 2 shows the PSNR and SNR test value obtained from different test images, i.e., after applying the above equation to calculate the differences between the host image and the final steganography image. Table 3 shows the visual image test for both the host image and the steganography image.

Table 2 PSNR and SNR (differences between the host image and the steganography image)

No.	Cover Image	Secret Message	Steganography Image	SNR(dB)	PSNR(dB)	MSE
1	RBG	Text	Çankaya Logo	47.40	48.56	0.036
2	RBG	Text	RBG pixel	46.01	47.34	0.045
3	RBG	Text	RBG circle	46.67	48.99	0.027
4	RBG	Text	Microsoft Logo	45.98	46.02	0.023

Table 3 Visual image test

Image	Result Image
Cankaya Logo	
RBG pixel	
RBG circle	
Microsoft Logo	

CHAPTER 5

CONCLUSION AND RECOMMENDATIONS

5.1 Conclusion

In order to support and improve the security model of information mobility, which moves through an insecure channel, we proposed a new algorithm schema that suggests integration between an improved Data Encryption Standard (DES) cryptography algorithm by using an irrational number and a data hiding technique by using the Least Significant Bit (LSB) steganography algorithm.

Moreover, we discussed the most important types and methods of encryption techniques used in the present day in addition to effective steganography techniques. We reviewed previous work and the literature related to our subject and implemented the proposed algorithm using the Matlab platform and examined the effectiveness of the algorithm through several stages, including the DES Encryption and Decryption Performance Test. Peak Signal-to-Noise Ratio (PSNR), Signal-to-Noise Ratio (SNR), and Mean Square Error (MSE) were used to test the quality of steganography images in addition to visual test images.

Our test lab showed the following results: the average time in the implementation for both the encryption and decryption process of the improved DES algorithm is better than the implementation of the normal DES. In addition, the suggestion of using an irrational number along with the DES algorithm provided us with improved security and advanced encrypting efficiency. In addition, it extended the key space without any extra running time, which can be considered to be promising in the field of information and communication technology today.

Although the Least Significant Bit (LSB) steganography algorithm uses a part of the host cover image information which is changed slightly in an attempt to conceal

information inside it, our lab visual image results show that both images (i.e. host image and steganography image) cannot be visually differentiated.

In addition, the integration between the improved Data Encryption Standard (DES) and the Least Significant Bit (LSB) steganography algorithm provides us with two layers of protection, the first of which is the encryption with an improved DES algorithm and the second being the hiding of this cipher text in multiple locations in the cover host image. Therefore, even if an attacker succeeds in finding hidden information, he will find encrypted information which cannot be deciphered without the use of a key. In addition, in the reverse situation, if an attacker was to steal, or successfully sniff, the secret key, he would not be able to know the location of the message due the use of the Least Significant Bit (LSB) steganography algorithm.

5.2 Recommendations for Future Work

Work on encryption and on data masking is not easy because of the rapid development that occurs in the field of information technology, and with the development of an attacker's skills, it is very important to continue to work on the development of new algorithms in order to face these daily challenges. Some recommendations for future work include the following:

- Continue to work on the development of new bilateral algorithms that represent more than one layer of information security;
- Reduce the time taken to process encryption and decryption;
- Work on the development of new algorithms that provide more space for data transmitted and increase the key space by proposing a new mechanism;
- Propose new ways to hide data in new unpredictable locations within the host cover image; and
- Propose means that are more efficient for data transfer through the unsafe intermediate.

REFERENCES

1. **Ibrahim., F., (2014),** *"Multi-Modal Assoclation Learning Using Spike-Timing Dependent Plasticity (STDP)",* (MSc), Universiti Utara Malaysia (UUM).

2. **Yusoff N., and Ibrahim F., (2015),** "*Face-Voice Assoclation Towards Multimodal-Based Authentication Using Modulated Spike-Time Dependent Learning",* Paper presented at the 5th International Conference on Computing and Informatics, ICOCI 2015, Istanbul, Turkey.

3. **Kessler C., (2003),** *"An Overview of Cryptography",* Gary C. Kessler.

4. **Schaefer E., (2009),** *"An Introduction to Cryptography and Cryptanalysis",* California's Silicon Valley: Santa Clara University.

5. **Luciano D., and Prichett G., (1987),** *"Cryptology: from Caesar Ciphers to Public-Key Cryptosystems",* The College Mathematics Journal, 18(1), 2-17.

6. **Singh S., (2011),** *"The Science of Secrecy from Ancient Egypt to Quantum Cryptography"*,Anchor.

7. **Robling E., (1982),** *"Cryptography and Data Security",* Addison-Wesley Longman Publishing Co., Inc.

8. **Bhattacharyya D., Ranjan R., Farkhod A., and Choi M., (2009),** *"Biometric Authentication: A review",* International Journal of U-and E-Service, Science and Technology, 2(3), 13-28.

9. **Biham E., and Shamir A., (1997),** *"Differential Fault Analysis of Secret Key Cryptosystems Advances in Cryptology"*, CRYPTO'97 (pp. 513-525): Springer.

10. **Rueppel A., (2012),** *"Analysis and Design of Stream Ciphers",* Springer Science & Business Media.

11. **Menezes J., Van C., and Vanstone A., (1996),** *"Handbook of Applied Cryptography"*, CRC press.

12. **Bellare M., Kilian J., and Rogaway P., (1994),** *"The Security of Cipher Block Chaining",* Paper presented at the Advances in Cryptology—CRYPTO'94.

13. **Xiao Y., Chen H., Du X., and Guizani M., (2009),** *"Stream-Based Cipher Feedback Mode in Wireless Error Channel",* Wireless Communications, IEEE Transactions on, 8(2), 622-626.

14. **Grabbe O., (1992),** *"The DES Algorithm Illustrated",* Laissez Faire City Times, 2(28), 12-15.

15. **Russell D., and Gangemi G., (1991),** "*Computer Security Basics ",* O'Reilly Media, Inc..

16. **Schneier B., Kelsey J., Whiting D., Wagner D., Hall C., Ferguson N., and Stay M., (2000),** *"The Twofish Team's Final Comments on AES Selection",* AES round, 2.

17. **Chang S., (2004),** *"International Data Encryption Algorithm",* jmu. edu, googleusercontent. com, Fall.

18. **Schneier B., (1994),** *"Description of A new Variable-Length Key, 64-bit Block Cipher (Blowfish)",* Paper presented at the Fast Software Encryption.

19. **Thakur J., and Kumar N., (2011),** *"DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis",* International journal of emerging.

20. **Odlyzko M., (1994),** *"Public Key Cryptography",* AT&T Technical Journal, 73(5), 17-23. doi: 10.1002/j.1538-7305.1994.tb00606.

21. **Blakley G., and Borosh I., (1979),** *"Public Key Cryptosystems do not Always Conceal Messages",* Computers & Mathematics with Applications, 5(3), 169

22. **Barrett P., (1986),** "*Implementing The Rivest Shamir and Adleman Public Key Encryption Algorithm on A standard Digital Signal Processor",* Paper presented at the Crypto.pp 160-178.

23. **Steiner M., Tsudik G., and Waidner M., (1996),** "*Diffie-Hellman Key Distribution Extended to Group Communication",* Paper presented at the Proceedings of the 3rd ACM.

24. **Hardy N., Vetter L., and Tribble D., (2000),** *"System and Method for Generating Unique Secure Values for Digitally Signing Documents",* Google Patents.

25. **El Gamal A., and Kim H., (2011),** *"Network Information Theory",* Cambridge university press.

26. **Lu S., (2004),** *"Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property",* Steganography and Digital Watermarking Techniques for Protection of Intellectual Property: Igi Global.

27. **Cheddad A., Condell J., Curran K., and Mc Kevitt P., (2010),** "*Digital Image Steganography: Survey and Analysis of Current Methods",* Signal processing, 90(3), 727-752.

28. **Sadkhan B., (2004),** "*Cryptography: Current Status and Future Trends",* Paper presented at the Information and Communication Technologies: From Theory to Applications, International Conference.

29. **Kahn D., (1996***),"The Comprehensive History of Secret Communication from Ancient Times to The Internet",* Simon and Schuster.

30. **Westfeld A., (2006),** "*Steganalysis in The Presence of Weak Cryptography and Encoding",* Paper presented at the IWDW.

31. **Petitcolas A., Anderson J., and Kuhn G., (1999),** "*Information Hiding-A survey",* Proceedings of the IEEE, 87(7), 1062-1078.

32. **Umamaheswari M., Sivasubramanian S., and Pandiarajan S., (2010),** "*Analysis of Different Steganographic Algorithms for Secured Data Hiding",* IJCSNS International Journal of Computer Science and Network Security, 10(8), 154-160.

33. **Subhedar S., and Mankar H., (2014),** "*Current Status and Key Issues in Image Steganography: A survey*", Computer Science Review, 13–14, 95-113.

34. **Even S., and Mansour Y., (1997),** "*A construction of A cipher from A single Pseudorandom Permutation",* Journal of Cryptology, 10(3), 151-161.

35. **Johnson F., and Katzenbeisser S., (2000),** "*A survey of Steganographic Techniques",* Paper presented at the Information hiding.

36. **Fridrich J., (1999),** "*A new Steganographic Method for Palette-Based Images",* Paper presented at the PICS.

37. **Wu M., and Liu B., (2004),** "*Data Hiding in Binary Image for Authentication and Annotation",* Multimedia, IEEE Transactions on, 6(4), 528-538.

38. **Zomaya Y., Seredynski F., and Bouvry P., (2003),** "*Secret Key Cryptography With Cellular Automata*", Paper presented at the Computer Systems and Applications, Book of Abstracts. ACS/IEEE International Conference on.

39. **Thiruppathy V., and Radhakrishnan S., (2012, 25-27 April 2012),** "*Secret Key Cryptography Based Security Approach for Wireless Sensor Networks*", Paper presented at the Recent Advances in Computing and Software Systems (RACSS), 2012 International Conference on.

40. **Zhang G., (2011),** "*Secret Key-Awareness Secure in Certificateless Cryptograph",* Procedia Environmental Sciences, 10, Part A, 633-639.

41. **Chandra S., Mandal B., Alam S., and Bhattacharyya S., (2015),** "*Content Based Double Encryption Algorithm Using Symmetric Key Cryptography",* Procedia Computer Science, 57, 1228-1234.

42. **Wander S., Gura N., Eberle H., Gupta V., and Shantz C., (2005, 8-12 March 2005),** "*Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks",* Paper presented at the Pervasive Computing and Communications, 2005. PerCom 2005. Third IEEE International Conference on.

43. **Salam I., Kumar P., and HoonJae L., (2010, 16-18 Aug. 2010),** "*An Efficient Key Pre-distribution Scheme for Wireless Sensor Network Using Public Key Cryptography",* Paper Presented at the Networked Computing and Advanced Information Management (NCM), 2010 Sixth International Conference on.

44. **Chen L., Harrison K., Moss A., Soldera D., and Smart P., (2002),** "*Certification of Public Keys Within an Identity Based System*", Information Security Springer, pp. 322-333.

45. **Lee B., Boyd C., Dawson E., Kim K., Yang J., and Yoo S., (2004),** "*Secure Key Issuing in ID-based Cryptography",* Paper presented at the Proceedings of the Second Workshop on Australasian Information Security, Data Mining and Web Intelligence, and Software Internationalisation-Volume 32.

46. **Lee B., Dawson E., and Moon S., (2005),** "*Efficient and Robust Secure Key Issuing Protocol in ID-based Cryptography",* Paper Presented at the Preproceedings of the 6-th International Workshop on Information Security Applications.

47. **Lee B., (2010),** "*Unified Public Key Infrastructure Supporting Both Certificate-based and Id-based Cryptography*", Paper Presented at the Availability, Reliability, and Security, ARES'10 International Conference.

48. **Hajer Y., (2011),** "*Survey on Certificateless Public Key Cryptography",* Paper Presented at the 6th International Conference on Internet Technology and Secured Transactions, Abu Dhabi, United Arab Emirates.

49. **Bai Q., Zhang W., Jiang P., and Lu X., (2012, 11-13 Aug. 2012)**, *"Research on Design Principles of Elliptic Curve Public Key Cryptography and its Implementatio",* Paper Presented at the Computer Science and Service System (CSSS), 2012 International Conference on.

50. **Al-Taei A., (2015)**, *"Automated Classification of Game Players Among The Participant Profiles"* in Massive Open Online Courses.

51. **Jhajharia S., Mishra S., and Bali S., (2013, 8-10 Aug. 2013),** "*Public Key Cryptography Using Neural Networks and Genetic Algorithms",* Paper Presented at the Contemporary Computing (IC3), Sixth International Conference.

52. **Luo W., Huang F., and Huang J., (2011),** "*A more Secure Steganography Based on Adaptive Pixel-value Differencing Scheme",* Multimedia Tools and Applications, 52(2-3), 407-430.

53. **Ibrahim R., and Kuan S., (2011),** "*Steganography Algorithm to Hide Secret Message Inside an Image",* arXiv Preprint arXiv:1112.2809.

54. **Sun X., and Wang X., (2012)**, *"A Information Steganography System Based on Channel Encoding Emerging Computation and Information",* Chnologies for Education (pp. 131-137): Springer.

55. **Pour H., and Payandeh A., (2012).,** "*A new Steganography Method Based on The Complex Pixels",* Journal of Information Security, 3(3), 202.

56. **Khosravi J., and Naghsh R., (2014),** "*A novel Joint Secret Image Sharing and Robust Steganography Method Using Wavelet*", Multimedia systems, 20(2), 215-226.

57. **Zhao Z., Liu F., Luo X., Xie X., and Yu L., (2013),** *"LSB Replacement Steganography Software Detection Based on Model Checking Digital Forensics and Watermaking",* Springer, (pp. 54-68).

58. **Li X., Zhang T., Zhang Y., Li W., and Li K., (2014),** "*A novel Blind Detector for Additive Noise Steganography in JPEG Decompressed Images*", Multimedia Tools and Applications, 68(3), 1051-1068.

59. **Uljarević D., Veinović M., Kunjadić G., and Tepšić D., (2015),** "*A new Way of Covert Communication by Steganography Via JPEG Images Within A microsoft Word Document*", Multimedia Systems, 1-9.

60. **El-Emam N., and Al-Diabat M., (2015),** "*A novel Algorithm for Colour Image Steganography Using A new Intelligent Technique Based on Three Phases*", Applied Soft Computing, 37, 830-846.

61. **Al-Dmour H., and Al-Ani A., (2016),** "*A steganography Embedding Method Based on Edge Identification and XOR Coding*", Expert Systems with Applications, 46, 293-306.

62. **Lyu S., and Farid H., (2006),** "*Steganalysis Using Higher-order Image Statistics*", Information Forensics and Security, IEEE Transactions on, 1(1), 111-119.

63. **Bloisi D., and Iocchi L., (2007),** "*Image Based Steganography and Cryptography*", Paper Presented at the VISAPP (1).

64. **Bourbakis N., Rwabutaza A., Yang M., Skodras A., and Ewing R., (2009),** "*A synthetic Stegano-crypto Scheme for Securing Multimedia*", Medical Records . , Applied Soft Computing.

65. **Narayana S., and Prasad G., (2010),** "*Two New Approaches for Secured Image Steganography Using Cryptographic Techniques and Type Conversions*", Signal and Image Processing: An International Journal (SIPIJ) Vol, 1.

66. **Raphael J., and Sundaram V., (2011),** "*Secured Crypto-stegano Communication Through Unicode*", World of Computer Science and Information Technology Journal, 1(4,138-143), 2221-0741.

67. **Ammar H., Seda Y., and Ersin E., (2015),** "*Dynamic Binary Location Based Multi-watermark Embedding Algorithm in DWT*", (Improved) , Journal of Theoretical and Applied Information Technology, Vol. 78. No. 2.

68. **Ammar H., Et al., (2014),** *"SVD and DWT Techniques for Copyright Protection",* 3rd Global Conference On Computer Science, Software, Istanbul, Turkey.

69. **Hussein J., Hu F., and RAHEM T., (2016),** *"IR and Multi Scale Retinex Image Enhancement for Concealed Weapon Detection,"* , Indonesian Journal of Electrical Engineering and Computer Science, vol. 1, no. 2.

APPENDIX

CURRICULUM VITAE

PERSONAL INFORMATION

Surname, Name: SHAKIR, Ahmed

Date and Place of Birth: 03 November 1982, Kirkuk

Marital Status: Married

Phone: +90 537 270 3972

mail: ahna2005@yahoo.com

EDUCATION

Degree	Institution	Graduation
M.Sc.	Çankaya Univ., Computer Engineering	2016
B.Sc.	Technical College Kirkuk, Software Eng.	2005
High School	Al Tameem High Schools, Kirkuk	2000

WORK EXPERIENCE

Year	Place	Enrollment
2006 - 2007	Channel Turkmeneli	Technical Administrator
2007 - 2009	Computer Center / Kirkuk University	Technician
2009 - 2010	CISCO Academy / Kirkuk University	Technician
2010 - 2011	Video Conference / Kirkuk Univ.	Technician
2011 - 2013	Internet and Computing Core Certification / Kirkuk University	Center Manager

LANGUAGES

Arabic, Turkmen, Turkish, Kurdish , English, Azerbaycan.

HOBBIES

Hiking and travel around the world.