Libyan Academy-Misurata

School of Applied Science and Engineering

Department of Information Technology

Development of Hiding a Secret Message in an Image by Encryption Using Fuzzy Logic

Thesis Submitted in Partial Fulfilment of the Requirement for the Degree of Master in Information Technology

Submitted by

Aisha Hassan Haweel

Supervised by

Prof. Ahmed Yousef Ben Sasi

Misurata - Libya

Autumn 2018

دولـــــــة ليبيــــا
الأكاديمية الليبية / فرع مصراتة

مصــراتة – ليبيـــا

الأكاديمية الليبية
The Libyan Academy

قـــــرار لجنة المناقشة للطالبة

عائشة حسن علي حويل

للحصول على درجة الإجازة العالية (الماجستير) في قسم (تقنية المعلومات)

قـــامت اللجنة المشكلة بقرار السيد/ رئيس الأكاديمية الليبية/ فـــرع مصراتة رقم **(345) لسنة 2018م** الصـــادر بتاريخ **2018/10/20م** بمناقشة الرسالة المقدمة من الطالبة: **عائشة حسن علي حويل** لنيل درجة الإجازة العالية (الماجستير) في قسم **تقنية المعلومات** وعنوانهـــا:

Development of Hiding a secret message in an Image by Encryption Using fuzzy logic

وبعد مناقشة الرســـالة علنياً على تمام الساعة **(12:00 صباحاً)** يوم **الثلاثاء** المــوافــق **2018/11/27م** بقاعــة المناقشات بالأكاديمية وتقــويم مســتوى الرسالة العلمي والمنـهج الـذي اتبعته الطالبة في بحثها قررت اللجنة ما يلي : قبـول الرسالة ومنح الطالبة: **عائشة حسن علي حويل** درجة الإجازة العالية (الماجستير) في قسم **تقنية المعلومات**

أعضاء اللجنة المناقشــــــة	الصفــــــــــة	التوقيـــــع
السيد/ أ.د. أحمد يوسف بن ساسي	أستـــاذ	
السيد/ د. أحمد محمد ابوشعالة	أستاذ مشارك	
السيد/ د. محمد أحمد الصلابي	أستاذ مشارك	

****

يعتمـــــــــــــد

د. محمد مصباح الشح
رئيس قسم تقنية المعلومات بالأكاديمية
التوقيع:.................................
التـــــاريخ: 18/12/2018م

د. محمد مصباح الشح
عميد مدرسة العلوم التطبيقية والهندسية
التوقيع:.................................
التـــــاريخ: 18/ 12/ 2018م

وزارة التعليم العالي والبحث العلمي
عميد مدرسة العلوم الهندسية والتطبيقية
الأكاديمية الليبية فرع مصراتة

وزارة التعليم العالي والبحث العلمي
قسم تقنية المعلومات
الأكاديمية الليبية - فرع مصراتة

أ.د. علي محمد رمضان
رئيس الأكاديمية الليبية / فرع مصراتة
التوقيع:.................................
التـــــاريخ: 31 / 12/ 2018م

وزارة التعليم العالي والبحث العلمي
رئيس الفرع
الأكاديمية الليبية فرع مصراتة

إقـــرار الأمـــانة العلمية

أنا الطالبة **عـائـشـة حسن علـي حـويـل** المسجلة بالأكاديمية الليبية / فرع مصراتة بقسم **تـقـنـيـة المعلومات** تحت رقم قيد (**31457009**) أقر بأنني التزمت بكل إخلاص بالأمانة العلمية المتعارف عليها لإنجاز رسالتي المعنونة بـــ **(Development of Hiding a Secret Message in an Image by Encryption Using Fuzzy Logic)** لنيل الدرجة العلمية الماجستير وأنني لم أقم بالنقل أو الترجمة من أية أبحاث أو كتب أو وسائل علمية تمَّ نشرها داخل ليبيا أو خارجها إلا بالطريقة القانونية وباتباع الأساليب العلمية في عملية النقل أو الترجمة وإسناد الأعمال لأصحابها، كما أنني أقر بعدم قيامي بنسخ هذا البحث من غيري وتكراره عنواناً أو مضموناً.

وعلى ذلك فأنني أتحمل كامل المسؤولية القانونية المترتبة علي مخالفتي لذلك إن حدثت هذه المخالفة حالياً أو مستقبلاً بما في ذلك سحب الدرجة العلمية الممنوحة لي.

والـــلــه علــى ما أقول شهيد

الاسم: عائشة حسن علي حويل

التوقيع: Aishe

التاريخ: 2018 /12/25

Dedication

I dedicate this thesis to my father and my mother, my husband AbdAlbaset, my brothers, my sisters, and all my friends.

To my supervisor and all people who helped me in this thesis.

Aisha Hassan Haweel

Acknowledgments

First and foremost, all praise and deep thanks are due to Allah, who helps and guided me through the challenges of my study. Glory is Allah who has given me the strength, patience and knowledge to continue and finish this thesis.

I would like to express my deep appreciation to the supervisor of the thesis, **Prof. Ahmed Yousef Ben Sasi** for his patience and unwavering willingness to provide direction, encouragement, support, assistance and feedback during supervising this thesis.

I give heartfelt thanks to **my dear father Dr. Hassan** and **my dear mother** for their understanding and encouragement. Their unconditional love has provide great support to me emotionally during my study, and to **my husband AbdAlbaset** for his understanding, encouragement and endless support to complete this thesis.

In addition, I give heartfelt thanks to **my dear brother Ali**, **my brothers**, **my sisters** and all **my friends** for their encouragement to achieve this research.

Table of Contents

Page

Dedication ii
Acknowledgments iii
List of Contents iv
List of Tables vii
List of Figures viii
List of Equation x
List of Abbreviations xi
Abstract (Arabic) xii
Abstract (English) xiii

CHAPTER 1
INTRODUCTION **1**
1.1 Background 2
1.2 Steganography 3
1.3 Cryptography 4
1.3.1 Purpose of Cryptography 5
1.4 Fuzzy Logic 6
1.4.1 Fuzzy Logic Benefits 7
1.4.2 Fuzzy Logic Applications 7
1.5 Problem Statement 8
1.6 Research Aim and Objectives 8
1.7 Thesis organization 9

CHAPTER 2
LITERATURE SURVEY **11**
2.1 Introduction 12
2.2 Steganography 12
2.2.1 Classification of Steganography 12
2.2.2 Spatial and Transform Domain Steganography 14
2.2.2.1 Transform Domain 14
2.2.2.2 Spatial Domain 15
2.2.2.2.1 Predicted-Based Data Hiding 15
2.2.2.2.2 Histogram-Based Data Hiding 15
2.2.2.2.3 Difference Expansion 15
2.2.2.2.4 Least Significant Bit / Most Significant Bit 16

2.3 Cryptography 17
2.3.1 Types of Cryptography Algorithms 17
2.3.2 Cryptography Techniques 17
2.3.2.1 Data Encryption Standard 17
2.3.2.2 Rivest-Shamir-Adleman 19
2.3.2.3 Advanced Encryption Standard 21
2.4 Fuzzy Logic 23
2.5 Related Works 31
2.5.1 Steganography 31
2.5.2 Cryptography 34

CHAPTER 3
ALGORITHM IMPLEMENTATION **37**
3.1 Introduction 38
3.2 The Proposed System 38
3.2.1 Encryption Process 41
3.2.2 Hiding Process 42
3.2.3 Extraction the Secret Message 42
3.3 Algorithms Performance Measures 43
3.3.1 Mean-Squared Error 43
3.3.2 Peak Signal-to-Noise Ratio 43
3.4 Steganography Attacks 43
3.5 Implemented System 44
3.5.1 Graphical User Interfaces 44

CHAPTER 4
RESULTS AND DISCUSSION **48**
4.1 Introduction 49
4.2 Results and Discussion 49
4.2.1 Comparison of the hiding algorithms 49
4.2.2 Comparison of the cryptography algorithms 54
4.2.3 Comparison of the fuzzy logic functions 56
4.2.4 Comparison of the fuzzy logic and AES algorithm under no attack condition 61
4.2.5 Comparison of the fuzzy logic and AES algorithm under attack condition (salt and pepper) 66

CHAPTER 5 **68**
CONCLUSIONS AND Recommendations
5.1 Conclusion 69
5.2 Recommendations 71

REFERENCES **72**

List of Tables

Page

Table 4.1 MSE measure of the hiding methods 50

Table 4.2 PSNR measure of the hiding methods 50

Table 4.3 Time measure of the hiding methods in offline mode 51

Table 4.4 Time measure of the hiding methods in online mode 51

Table 4.5 Scores of the hiding methods in offline mode 53

Table 4.6 Scores of the hiding methods in online mode 53

Table 4.7 Time measure of the encryption algorithms in offline mode 54

Table 4.8 Time measure of the encryption algorithms in online mode 55

Table 4.9 MSE measure of the FL functions 56

Table 4.10 PSNR measure of the FL functions 57

Table 4.11 Time measure of the FL functions in offline mode 58

Table 4.12 Time measure of the FL functions in online mode 59

Table 4.13 Scores of the FL functions in offline mode 60

Table 4.14 Scores of the FL functions in online mode 60

Table 4.15 MSE measure of the FL and AES algorithm 61

Table 4.16 PSNR measure of the FL and AES algorithm 62

Table 4.17 Time measure of the FL and AES algorithm in offline mode 63

Table 4.18 Time measure of the FL and AES algorithm in online mode 63

Table 4.19 Scores of the FL and AES algorithm in offline mode 64

Table 4.20 Scores of the FL and AES algorithm in online mode 64

Table 4.21 Attack (noise) on the images (Lena, Crowded and Camera man) 66

List of Figures

			Page
Figure	1.1	Generic schematic view of image steganography	4
Figure	1.2	Overview of a simple cryptography system	5
Figure	1.3	Basic structure of fuzzy logic system	6
Figure	2.1	Classification of image steganography	12
Figure	2.2	Data encryption standard (DES) algorithm	19
Figure	2.3	RSA encryption and decryption algorithm	21
Figure	2.4	AES encryption and decryption algorithm	23
Figure	2.5	Intuitionistic fuzzy triangular functions	25
Figure	2.6	Intuitionistic fuzzy trapezoidal functions	26
Figure	2.7	Intuitionistic fuzzy gaussian function	27
Figure	2.8	Intuitionistic fuzzy bell-shaped functions	28
Figure	2.9	Intuitionistic fuzzy sigmoidal function	29
Figure	2.10	Intuitionistic fuzzy S-shaped function	30
Figure	2.11	Intuitionistic fuzzy Z-shaped function	31
Figure	3.1	The proposed system	39
Figure	3.2	Flow chart diagram of the proposed system	41
Figure	3.3	Main interface of hiding a secret message in an image	44
Figure	3.4	Hiding a secret message in an image	45
Figure	3.5	Development of hiding a secret message in an image	46
Figure	3.6	Information about of the research	47
Figure	4.1	MSE performance of the hiding methods	50
Figure	4.2	PSNR performance of the hiding methods	51
Figure	4.3	Time computation of the hiding methods	52

Figure 4.4 Performance of the hiding methods 52
Figure 4.5 Scores of the hiding methods 53
Figure 4.6 Scores of the hiding methods in offline and online mode 54
Figure 4.7 Time computation of the encryption algorithms 55
Figure 4.8 MSE performance of fuzzy logic functions 57
Figure 4.9 PSNR performance of fuzzy logic functions 58
Figure 4.10 Time computation of fuzzy logic functions 59
Figure 4.11 Performance of the fuzzy logic functions 60
Figure 4.12 Scores of fuzzy logic functions 61
Figure 4.13 MSE performance of FL and AES algorithm 62
Figure 4.14 PSNR performance of FL and AES algorithm 62
Figure 4.15 Time computation of FL and AES algorithm 63
Figure 4.16 Performance of the FL 64
Figure 4.17 Performance of the AES algorithm 64
Figure 4.18 Scores of FL and AES algorithm 65
Figure 4.19 Scores of the FL and AES algorithm in offline and online mode 65

List of Equations

Page

Equation 2.1 Triangular functions 25

Equation 2.2 Trapezoidal functions 26

Equation 2.3 Gaussian function 27

Equation 2.4 Bell-shaped function 28

Equation 2.5 Sigmoidal functions 29

Equation 2.6 S-shaped functions 30

Equation 2.7 Z-shaped functions 31

Equation 3.1 Mean-Squared Error 43

Equation 3.2 Peak Signal-to-Noise Ratio 43

List of Abbreviations

AES	Advanced Encryption Standard
DCT	Discrete Cosine Transform
DE	Difference Expansion
DES	Data Encryption Standard
DFT	Discrete Fourier Transform
DWT	Discrete Wavelet Transform
FL	Fuzzy Logic
FLS	Fuzzy logic system
IFS	Intuitionistic Fuzzification Functions
LSB	Least Significant Bit
MF	Membership Function
MSB	Most Significant Bit
MSE	Mean-Squared Error
NIST	National Institute of Standards and Technology
PSNR	Peak Signal-to-Noise Ratio
PVD	Pixel-value differencing
RGB	Red-Green-Blue
RSA	Rivest-Shamir-Adleman
3DES	Triple Data Encryption Standard

الملخص

تعد تقنية الإخفاء والتشفير طريقتين شائعتين لإرسال المعلومات بطريقة سرية. الإخفاء يخفي وجود الرسالة والتشفير يشوه الرسالة. إن استخدام التشفير مع الإخفاء يجعل من الاتصال أكثر تأمينا. ولذلك اقترحنا نظام يجمع بين التشفير والإخفاء لتوفير طريقة فعالة لحماية الرسالة النصية السرية من المستخدمين غير المصرح لهم بالاطلاع عليها. في هذه البحث قمنا باقتراح استخدام خوارزمية المنطق الضبابي لتشفير الرسالة النصية السرية. وقمنا أيضا باقتراح استخدام تقنية البتات الأقل أهمية (LSB) لإخفاء الرسالة النصية السرية المشفرة في البتات الأقل أهمية للصورة الرمادية. إن مدى كفاءة ودقة خوارزمية المنطق الضبابي معتمدة على بعض المقاييس. ومن هذه المقاييس قمنا باستخدام مقياسين لقياس جودة الصورة: متوسط مربع الخطأ (MSE) ونسبة الإشارة إلى الضوضاء (PSNR)، وقمنا أيضا بقياس الوقت المطلوب لتنفيذ هذه الخوارزمية (execution time). النتائج التي تم الحصول عليها من خوارزمية المنطق الضبابي تمت مقارنتها مع خوارزمية تشفير تقليدية (AES). هذه النتائج كانت مرضية، حيث كانت تقدير القياسات لخوارزمية المنطق الضبابي التي طبقت على إحدى الصور المستخدمة بنسبة 0.097، بينما كانت تقدير القياسات لخوارزمية التشفير (AES) بنسبة 0.13، وطبقا لهذه النتائج فإن خوارزمية المنطق الضبابي أعطت أفضل جودة للصورة (stego-image). لذلك فإن خوارزمية المنطق الضبابي أفضل أداء من الخوارزمية الأخرى. كذلك تم اختبار الصورة (stego-image) ضد بعض المخاطر منها: الضوضاء، كانت النتائج معتمدة على نسبة التماثل بين الرسالة النصية السرية الأصلية والرسالة النصية السرية المستخرجة من الصورة (stego-image)، حيث تتراوح نسبة التماثل لخوارزمية المنطق الضبابي التي طبقت على الصور المستخدمة بين 62.5% و 100%، بينما تتراوح نسبة التماثل لخوارزمية التشفير (AES) بين 0% و 100%. هذه النتائج أثبتت قوة الصورة (stego-image) لخوارزمية المنطق الضبابي ضد بعض المخاطر.

Abstract

Steganography and Cryptography are two popular ways of sending information in a secret way. One hides the existence of the message and the other distorts the message itself. Cryptography used with steganography to make its security more robust. Furthermore, we propose a system that combined cryptography and steganography to provide an effective way to protect the secret text messages from unauthorized users. In this thesis, we proposed using of the fuzzy logic (FL) algorithm to encrypt the secret text message. Also, we proposed using the least significant bit (LSB) technique to hide the encrypted secret text message in the least significant bits of the gray image. The efficiency and accuracy of the FL algorithm based on some measurements. Two of these measures used to measure the image quality: Mean-Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR), also, we measured the required time to execute this algorithm (execution time). The results obtained from the FL algorithm were compared with the classical encryption algorithm (AES). The results were satisfactory, the metrics scoring of FL algorithm that applied to one of the used image rated 0.097, while the metrics scoring of AES algorithm rated 0.13. According to these results, the FL algorithm gave the best image quality (stego-image). Therefore, FL algorithm was better in performance than the other algorithm. In addition, stego-image has been tested against some attacks such as noise (salt and pepper). The results based on the ratio of similarity between the original secret text message and the extracted secret text message from the stego-image, where the range of the similarity ratio for the FL algorithm that applied to the used images between 62.5% and 100%, while the range of the similarity ratio for the AES algorithm between 0% and 100%. Those results demonstrated strength of the image (stego-image) of the FL algorithm against some attacks.

Chapter 1

Introduction

1.1 Background

Nowadays the use of computers has become the most important and common means in information storing and retrieving. It also helps in trading information through the local and global networks, e-mail and mobile phones by digital media such as text, audio, image and animation. It has become easy to intercept the sent information via different communication networks or access to those computers, whether independent or linked with the network, to view its contents, steal or tampered the important information.

In result of this, the protection, reliability and credibility of the information should be ensured, so many protection means has appeared, such as password setting, cryptography, and hiding techniques (steganography).

The cryptography converts messages and confidential information to a format that cannot be read unless by using a secret key, then the information is retrieved by the same key. The form of encrypted message and information raises doubts for revealing their content untidily, which attract the hackers to tamper the message that they could not decrypt [1].

Steganography combines the Greek words, that are stegano and graphy. Stegano meaning "protected or covered" and graphe meaning "writing" [2].

The steganography is about inputting the information into media files where it is neither observed nor detected and its existence cannot be recognized, but it seems as ordinary files where the overall form of the carrier file is maintain. The steganography has two categories; watermarking and image hiding. In watermarking little information, such as the signature, a sign the company or institution seal is hidden to authenticate the sent documents. This includes a method that is difficult to be manipulated or erased through image processing operations, such as filtering, engineering transfers and addition of noise [3][4].

The other category includes hiding large amount of important information (documents, messages, diagrams and images) within text or images files, by method that do not raise doubt, but looks as images, declaration or plain text. Steganography is often used together with cryptography to enhance information protecting and obscuring [5].

1.2 Steganography

Steganography is the science and art of hiding information. It embeds the secret information in a cover media in an unnoticeable manner so as not to raise doubts [6][7].

In the past, it was believed that the Greeks were the first to practice the steganography. They used wax tablets for hidden writing, where they were writing the secret messages on a wooden board and then cover it with a wax, so as not to raise doubts about having a secret message below the wax. Later, the microdots technique was developed by the Germans, where the FBI director J. Edgar Hoover described it as "the enemy's masterpiece of espionage". They are photographs, were discovered disguised on a printed envelope carried by a German agent in 1941. The secret message was too small to draw attention, they were neither encrypted nor hidden. Microdots technique allowed to transfer a large amounts of the secret data such as photographs and graphics. Other forms of the hidden writing such as the use of hidden tattoos or invisible ink [6][7].

Today, computers and networks providing communication channels for steganography. Essentially, the process of data hiding is identifying bits of the cover using the hiding technique and replaced these bits with bits of the secret message. Modern steganography's goal is the secret message is kept from unauthorized access [6]. Figure (1.1) shows basic process of steganography:

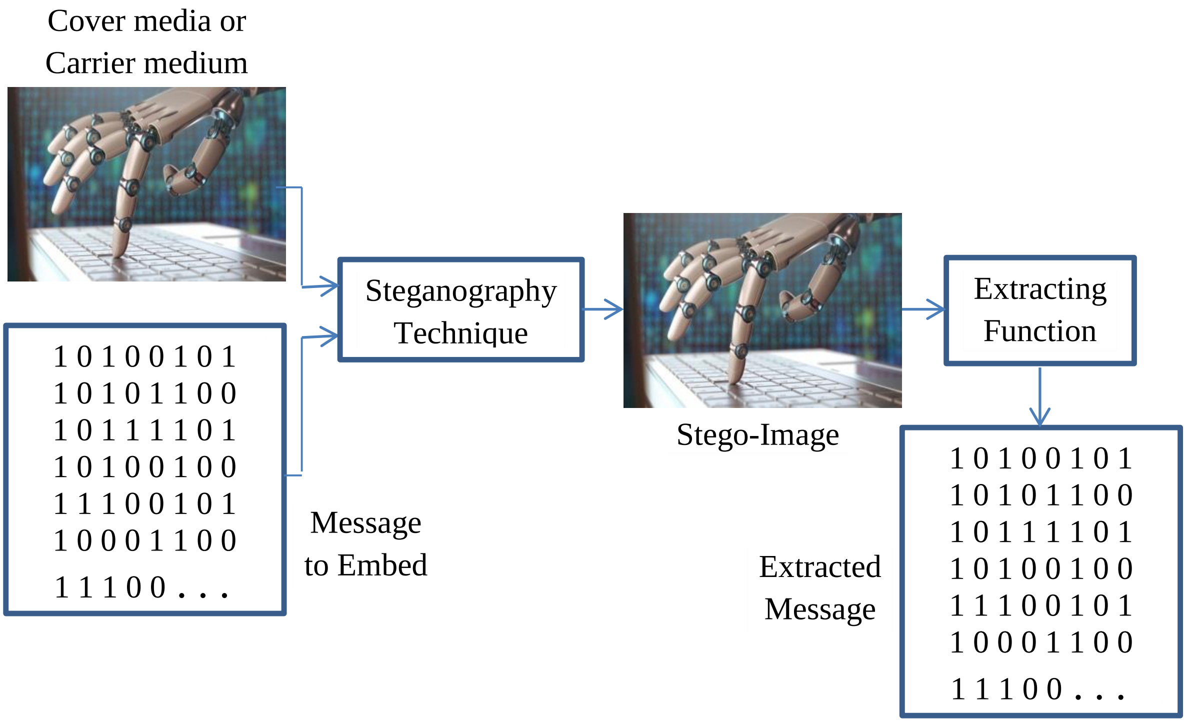


Figure (1.1): Generic schematic view of image steganography

1.3 Cryptography

Cryptography is the mathematical science of symbols, codes and secret messages related to information security aspects such as data safety and privacy. It works to protect information by converting the plaintext to an unreadable format called cipher-text using the encryption algorithm [8].

Cryptography is useful for achieving confidentiality transfer across the networks where the sender sends the cipher-text, and the receiver on the other side receives the cipher-text then decrypt it to plaintext [8][9]. Figure (1.2) shows overview of a simple cryptography system.

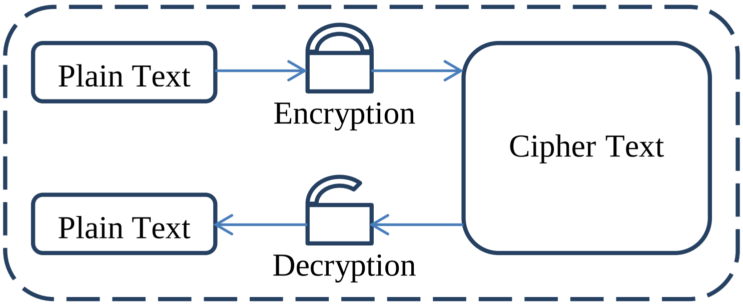


Figure (1.2) Overview of a simple cryptography system

Cryptography and steganography both protect information from illicit parties. Using one of them alone is not perfect to provide confidential information and can be broken. But using both together provides multiple layers of security and confidentiality [10]. Therefore, this research suggests a system to secure the secret message using both steganography and cryptography, which will be detailed in the chapter 3.

There were several techniques for the cryptography. Some of these techniques were; Data Encryption Standard (DES), Rivest-Shamir-Adleman (RSA) and Advanced Encryption Standard (AES). In this research, we will use another method for cryptography. Fuzzy Logic (FL) is the proposed algorithm to encrypt a secret message. In addition, we will give an overview of the fuzzy logic in this chapter.

1.3.1 Purpose of Cryptography

Cryptography provides some of the goals to avoid security problems, which are as follows [11][12]:

1) Confidentiality: the sender and receiver can access the contents of the secret message and cannot be access by an unauthorized person.
2) Authentication: it establishes identity, identifying the sender of the secret message that may be sent by an unauthorized person.

3) Integrity: It maintains the contents of the secret message that sent, and may be only modified by an authorized person.
4) Non- repudiation: It proves that the sender of the secret message has already sent the message and the sender cannot deny sending this message.
5) Access Control: specifies only the authorized parties have access to the secret information.
6) Availability: resources must be available to the authorized parties at any way and any time.

1.4 Fuzzy Logic

Fuzzy logic (FL) is called a fuzzy logic controller, a fuzzy system, etc [13]. Lotfi A. Zadeh proposed fuzzy logic in 1965. FL is a multivalued logic, which specifying intermediate values between evaluations such as fast/slow, tall/short, yes/no, true/false, etc. It means that the concepts like very slow or too short can be formulate mathematically and manipulated by computers to resemble human thinking [14]. Figure (1.3) illustrates the fuzzy logic system (FLS) that contains fuzzification, a knowledge base, a database, inference, and a defuzzification [15].

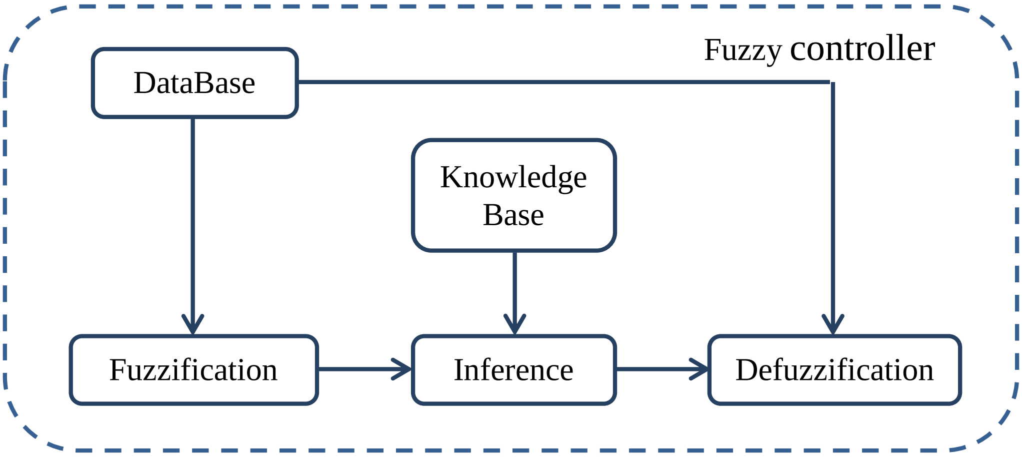


Figure (1.3) Basic structure of fuzzy logic system

The components of FLS briefly as follows [15]:

- Fuzzification: it converts input values into fuzzy values.
- Knowledge base: it includes a rule base that distinguishing control objectives and pattern.
- Database: it provides a fuzzy partition of Membership Function (MF) definitions, input and output spaces, and it provides the needed definitions of discretization and normalization.
- Inference: it is process of formulating the mapping from fuzzy input data to an output and rules to infer fuzzy control actions employing fuzzy implication.
- Defuzzification: converts the values range into output variables and a fuzzy control action inferred transforms into a non-fuzzy control action.

1.4.1 Fuzzy Logic Benefits

Some of the fuzzy logic benefits are briefly as follow [16]:

1) Simplify and reduce the cycle of development.
2) Ease of understanding and implementation.
3) It is flexible.
4) It can be build on the expert's experience.
5) It is permissive with data that is imprecise.
6) It is dependent on the natural language.
7) It can be merged with techniques of the conventional control.
8) It can provide the effective performance.

1.4.2 Fuzzy Logic Applications

Fuzzy logic is one of the artificial intelligence techniques. It has several application domains. Fuzzy logic was proved to be implemented in all scientific scopes nearly, although it has been criticized since its inception will maintain its validity and increases the domains number that attracts the attention to it [17].

Some of the fuzzy logic applications are achieved in the areas such as pattern recognition, control, information systems, and decision support [16].

1.5 Problem Statement

Major constraint of today's for computer communication is to prevent the data to be revealed to the illicit user. Many people try to find a way to hide information especially when it comes to various confidential data such as sensitive documents or files, military maps, and ....,etc.

A person would like to send an email or file with no fear that an illicit person will read the message. Also, with all information that is on the Internet, owners of such information must protect themselves from unwanted spying, copying, theft and false representation.

The most common method for hiding information in the image is Least Significant Bit (LSB) [18][19]. The LSB methods are very sensitive to any kind of image manipulation and can be easily destroyed [20][21].

The method that has been applied in [19], [22] and [23] compares the results of LSB, Most Significant Bit (MSB) and hybrid algorithm of LSB and MSB based on some measurements. Those results focused on the difference between the original image and the stego image, and it has not discussed the level of data protection. Therefore, we suggest a way using fuzzy logic to increase the robustness of an image against some of attacks.

1.6 Research Aim and Objectives

The main aim of research is to hiding a secret message in an image using fuzzy logic to achieve security, privacy, undetectability and to avoid drawing suspicion to transmission of a hidden message. The following objectives are expected to be achieved:

- Surveying of the methods which used in hiding messages and encryption techniques.
- Verifying the comparison of the results of LSB, MSB and hybrid algorithm of LSB and MSB of an image by calculating MSE, PSNR and execution time.
- Verifying the comparison of the results of DES, RSA and AES by calculating the execution time.
- Developing the best method of data hiding by the encryption of the secret text message using fuzzy logic algorithm and the best method of the encryption.
- Execution of hiding operation using the best method of data hiding for an encrypted message.
- Measuring the level of data protection against some attacks of the proposed method.

1.7 Thesis Organization

The thesis is divided into five chapters:

Chapter 1 Introduction: provides a summary of the background to thesis, steganography, cryptography, fuzzy logic, problem statement, research aim and objectives, and the thesis organization are also provided here.

Chapter 2 Literature survey: explains the methods and techniques that were used in the steganography and the cryptography.

Chapter 3 Developed Algorithm Implementation: the developed algorithm is described in detail to clear out how to encrypt and hide the secret text message in an image.

Chapter 4 Results and Discussion: illustrate the results of the developed algorithm and compare them with another encryption algorithm based on some measurements.

Chapter 5 Conclusions and Recommendations: presents conclusions, and recommendations of the future work of this research.

Chapter 2

Literature Survey

2.1 Introduction

In our time, it became necessary to protect the information, because the world became connected across networks. These networks are used to transmit information electronically between private individuals or between private and public organizations, whether they are military or civilians. It is necessary to have ways to keep the information be secret. Great efforts collaborated from around the world to find the best ways to exchange data without being detected such as cryptography and steganography. In this chapter, we will review some techniques for cryptography and Steganography. In addition, some of the previous studies of these techniques will be explained.

2.2 Steganography

2.2.1 Classification of Steganography

All the digital files formats can be used to hide confidential information, but some of these formats are more convenient than others for the hiding. Figure (2.1) shows the main categories of steganography based on nature of file formats as well as the classification of image steganography [24].

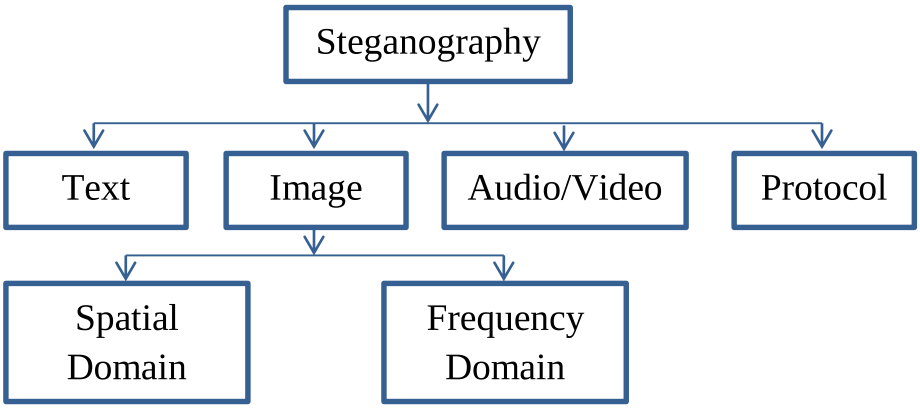


Figure (2.1) Classification of image steganography

Historically, the most important method of steganography is hiding information in text. Text steganography is hiding the secret message in a cover-text using a hiding technique. The cover-text after the hiding process called a stego-text. Then the sender will send a stego-text to the receiver through a communication channel. When the receiver receives a stego-text, will extract the secret message using recovering algorithm of the hiding technique used [24][25].

The audio steganography is hiding the secret message in a cover-file (Audio file). The secret message can be plain text, audio, image, and any file format. The cover-file after a hiding process is known as a stego-file [26]. Audio files when they are large size make it less use than images. In audio steganography, there is one different technique is masking that exploits the human ear properties to data hiding in an unnoticeable way. Sound becomes inaudible when another sound is louder, this creates a channel that hiding the secret data [24].

Protocol steganography is a hiding process the secret message in network control protocols and messages that used in network transmission. There exist secret channels in the OSI network model layers where can be used for the steganography. An example, the secret message can be hidden in some fields of a TCP/IP packet header, which are optional or never used [24].

Image steganography is the most popular for hiding the secret message because it is ease to send through the communication between the sender and receiver, and it consists a large amount of redundant bits that present in the digital representation of an image [24]. The images have three types (binary, Gray scale and Red-Green-Blue) images. Binary image represents by one bit value per pixel where the black pixels is a value "0" and the white pixels is a value "1". Sometimes the gray scale image represents by eight bits per pixel where the black pixels are the values "00000000" and the white pixels are the values "11111111". RGB image represents by 24 bits per pixel where the black pixels are the values "00000000, 00000000, and 00000000" and the white pixels are the values "11111111, 1111111, and 11111111" [27].

In this research, the gray images are used as a carrier message to hide the encrypted secret text message by proposed method which is described in detail in chapter 3.

Image steganography techniques can be divided into: transform domain and spatial domain [27]. Although, transform domain is out of scope. This research will be specific in the area of the spatial domain.

2.2.2 Spatial and Transform Domain Steganography

Image steganography techniques based on the way of embedding data into an image can be divided as follow:

- Transform domain.
- Spatial domain.

2.2.2.1 Transform Domain

It is also called as frequency domain, the image is transformed firstly and then a secret message is hiding in the image [27]. Data hiding in the transform domain is common used for robust watermarking. Similar techniques can also achieve a large-capacity of the data hiding [28].

Transform domain includes transformations such as discrete cosine transform (DCT), discrete wavelet transform (DWT), and discrete Fourier transform (DFT). Data hiding process is hide a secret message in more robust areas of an image where the hidden data spreads across the image and provides the best resistance against signal processing [28].

2.2.2.2 Spatial Domain

It is also called an image domain, the secret message is hidden directly in the pixels intensity [27]. Data hiding in spatial domain is performed based on some of the methods as the following:

2.2.2.2.1 Predicted-Based Data Hiding

Predictive value calculates through using the different predictions. Hiding the secret message in a cover image through using the difference expansion between the pixel and its predictive value. This provides a significant hiding capability without noticeable distortion [29].

2.2.2.2.2 Histogram-Based Data Hiding

Histogram Modification is another commonly used to hiding the information. The secret message is hiding through using the adjacent pixels difference value. It is characterized by restoring the original image from the stego-image, some applications like the medical imaging can be require it. Hiding ability is limited in such methods [30].

2.2.2.2.3 Difference Expansion

Difference-expansion (DE) is embed one layer in a different image. If the current difference image does not have expandable differences, they are embed another layer of the next different image. The drawback of DE is the image quality decreased before the next layer is embedded because the previous layer used all the expandable differences, including a large size of the differences [31].

2.2.2.2.4 Least Significant Bit / Most Significant Bit

Least Significant Bit embedding (LSB) is a commonly technique used in steganography. LSB method is very simple where the secret message bits are hidden in a least significant bits of an image [32][33].

In image steganography, the cover-image after the hiding process called a stego-image. Hiding of a secret message is done in LSB or MSB of an image [22].

LSB is the least significant bits in each pixel of an image, e.g. binary series: 01010011, the least significant bit is far right 1. Hiding process of LSB is hiding the secret message in a least significant bits of each pixel values in a cover-image. E.g. to hiding a character 'A' in a cover-image, the character 'A' will convert into a binary number: 01000001, each bit of a binary number is replaced by the least significant bits of a cover- image to produce a stego-image [22].

Cover-image: 00000011 10000011 10000011 10000011
10000011 01000011 01000011 01000011

Stego-image: 00000010 10000011 10000010 10000010
10000010 01000010 01000010 01000011

Where MSB is the most significant bits in each a pixel, e.g. binary series: 01010011, the most significant bit is far left 0. Hiding process of MSB is hide the secret message in most significant bits of each pixel values in a cover-image. E.g. to hiding a character 'A' in a cover-image, the character 'A' will convert in to a binary number: 01000001, each bit of binary number is replaced by most significant bits of a cover- image to produce a stego-image [22].

Cover-image:	00000011	10000011	10000011	10000011
	10000011	01000011	01000011	01000011
Stego-image:	00000011	10000011	00000011	00000011
	00000011	01000011	01000011	11000011

2.3 Cryptography

2.3.1 Types of Cryptography Algorithms

There are many types of cryptography; two types are the most common of cryptography as follow [11][12]:

- ✓ Symmetric key cryptography (secret key cryptography): the same key is used to encrypt the secret message and to decrypt the encrypted secret message.
- ✓ Asymmetric key cryptography (public key cryptography): two different keys are used. One of them is used to encrypt the secret message and another key is used to decrypt the encrypted secret message.

Some techniques of the cryptography are based on symmetric key algorithm and others are based on an asymmetric key algorithm.

2.3.2 Cryptography Techniques

There are many techniques used to encrypt the information, we will list some of them as follows:

2.3.2.1 Data Encryption Standard

Data Encryption Standard (DES) is a common and widely available encryption system. Developed in the 1970s by IBM, later the National

Institute of Standards and Technology (NIST) adopted it as the Federal Information Processing Standard [34].

DES is a block cipher. It uses a 56-bit key although the DES input key is 64 bits. It is an algorithm that takes plaintext with a fixed length string of bit, and converts it to cipher-text bit string of the same length through a set of complex operations [34] [35].

The complex operations transform a plaintext through 16 iterations with values obtained from the key. These values generated from 16 iterations and each iteration contains XOR, replacements and permutations, then resulting 16 sub-keys each of 48-bits. The plain text is 64-bits, DES algorithm divides 64-bits into right and left parts, each part is 32-bits, where passing through the expansion block that increases the number of bits from 32-bits to 48-bits. These 48-bits transform with 48-bits of sub-key into XOR operation to 48-bits, then goes this 48-bits into 8 S-boxes and then permuted of the initial 64-bits, after 32-bits swap is reversed of the permutation [34] [35].

DES algorithm transforms 64-bits input to a 64-bits output into a set of steps. It is dependent on a symmetric-key algorithm, so the same key are used for decryption with the same steps [34] [35].

Many attacks make DES block cipher unsafe, but it still used to protect the sensitive online applications by the financial services and others [34]. The flowchart of DES algorithm is shown in figure (2.2).

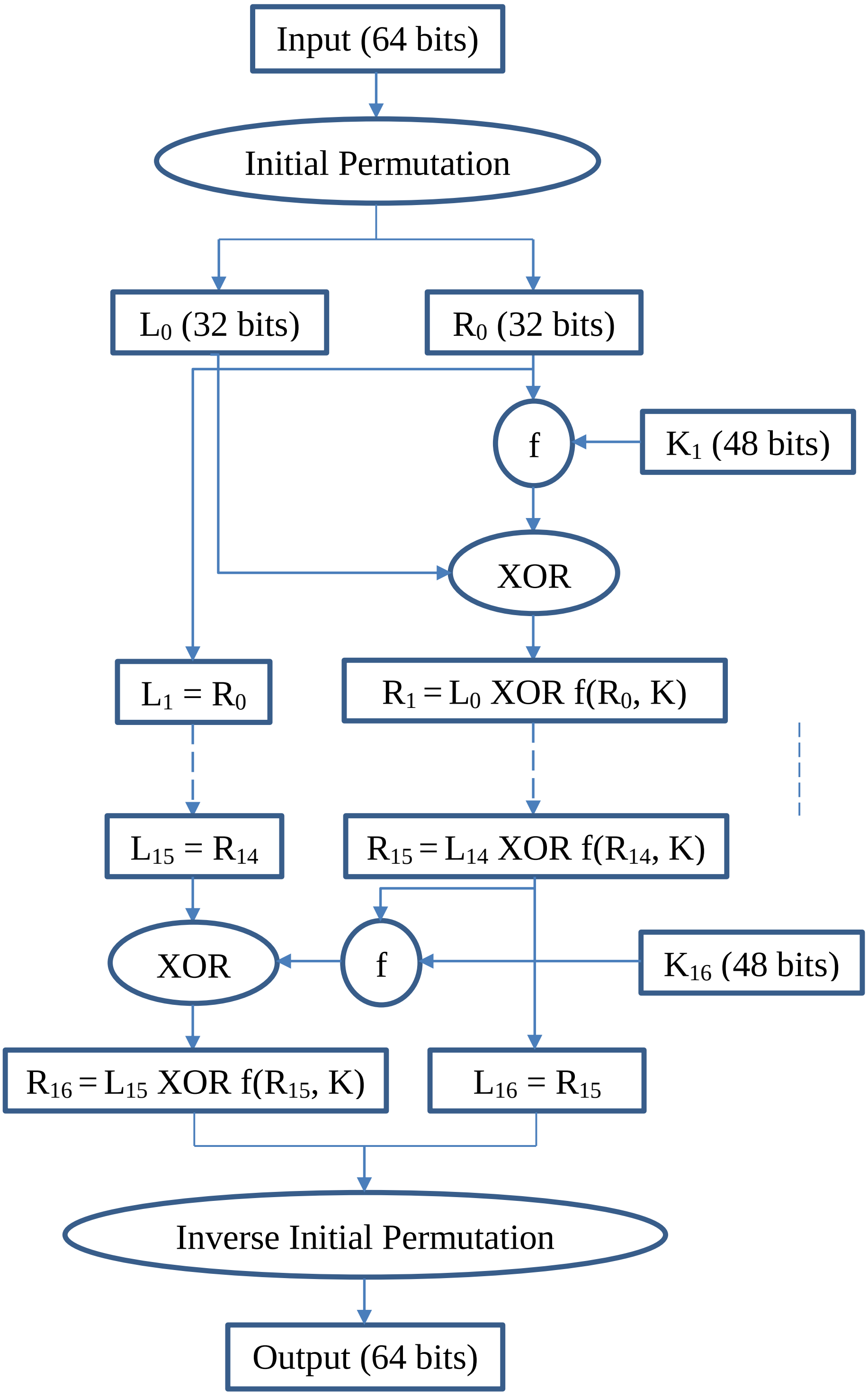


Figure (2.2) Data encryption standard (DES) algorithm

2.3.2.2 Rivest-Shamir-Adleman

Rivest-Shamir-Adleman (RSA) is designed in 1978 by Ron Rivest, Adi Shamir, and Leonard Adleman. It is based on an asymmetric key algorithm, and it uses two different (public and private) keys to encrypt and decrypt the secret messages. These keys are generated using selection two prime numbers, a public key is used to encrypt the secret message and a private key is used to decrypt the encrypted secret message [34].

RSA algorithm operations can be divided into three steps; that are encryption, keys generation and decryption. It has many weaknesses, when select two small values from the prime numbers to generate the keys, the data encryption process becomes weak and encrypted data can be decrypted by attacks. While if select two large values from the prime numbers to generate the keys, it consumes more time and deteriorates the performance of RSA algorithm when compared to DES algorithm. The steps of RSA algorithm as the following [34]:

1) Generation the keys (public and private).
   - Select a large prime numbers p and q and $p \sim= q$
   - Calculate $n = p * q$
   - Calculate $\varphi\ (n) = (p-1) * (q-1)$
   - Select the public key e such that: $gcd\ (\varphi\ (n),\ e) = 1;\ 1<e< \varphi\ (n)$
   - Select the private key d such that: $d*e \bmod \varphi\ (n) =1$
   - The public key is (n, e) and the private key is (n, d), and all the values (d, p, q and phi) keep secret.
2) Encryption: calculate cipher text C from plaintext message M.
   - $C = M^{e} \bmod n$
3) Decryption: calculate plaintext M from cipher text C.
   - $M = C^{d} \bmod n$

Figure (2.3) shows the steps of RSA algorithm.

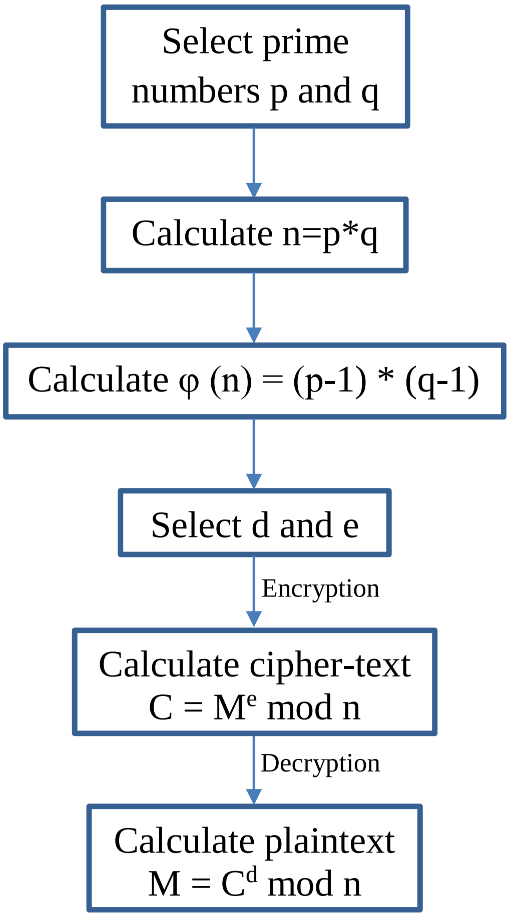

Select prime numbers p and q
Calculate n=p*q
Calculate φ (n) = (p-1) * (q-1)
Select d and e
Encryption
Calculate cipher-text C = M^e mod n
Decryption
Calculate plaintext M = C^d mod n

Figure (2.3) RSA encryption and decryption algorithm

2.3.2.3 Advanced Encryption Standard

Advanced Encryption Standard (AES) is the new encryption standard, where National Institute of Standards and Technology (NIST) recommended replacing DES with AES in 2001. This algorithm is easy to implement on hardware and software, it has a great speed for execution, and ability to secure information against various attack techniques [34][36].

AES algorithm is called as AES-128 when key length of 128, AES-192 when key length of 192, and AES-256 when key length of 256 bits. In addition, it can support any set of data block (128 bits). When encrypting and decrypting an information, the operations of AES algorithm is pass through (10, 12, and 14) rounds depending on key length where 10 rounds for 128-bit, 12 rounds for 192-bit, and 14 rounds for 256-bit [34][36].

In order to encrypt data block (128-bit), AES algorithm divides this data into four blocks. The blocks of data are organized as bytes array (4 × 4), it is called a state. The algorithm operations passes through nine rounds, these operations are as following [34]:

1) Substitute bytes (SubBytes): it converts each byte (8 bits) of data block to another block of data.

2) Shift rows (ShiftRows): the bytes shifted cyclically in the last three rows of the state based on the row location.

3) Mix columns (MixColumns): the matrix is multiplied to each column of the state.

4) Add round key (AddRoundKey): the state (128-bits) is a bitwise XOR with the round key (128-bits).

Mix columns (MixColumns) operation is not passing through the final (10th) round. Decryption reverses all the steps that used in the encryption, which will inverse shift rows (InvShiftRows), inverse substitute bytes (InvSubBytes), add round key (AddRoundKey) and inverse mix columns (InvMixColumns) [34][36].

All of those processes in AES encryption and decryption algorithm shown in figure (2.4).

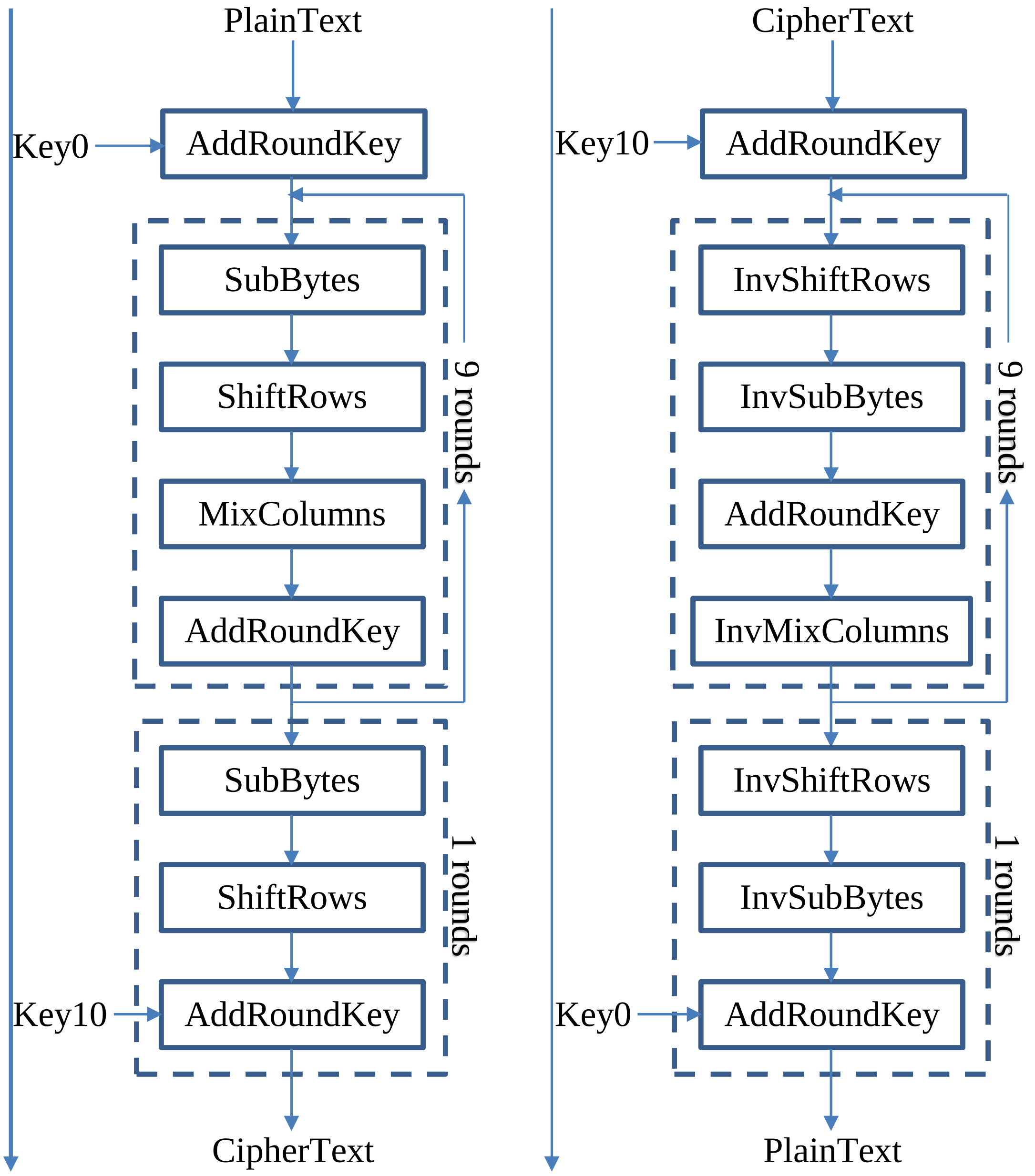


Figure (2.4) AES encryption and decryption algorithm

2.4 Fuzzy Logic

Fuzzy system idea is a fuzzy (sub) set. Membership function (μ_A) is a graphical representation of each input. It operates on a fuzzy set and returns various values between 0.0 and 1.0 [14]. Where a value (0.0) indicates to the complete exclusion and a value (1.0) to the complete membership [15]. Fuzzification in the fuzzy set specify the membership degree, it is formulate membership and non-membership values of an Intuitionistic Fuzzy Set (IFS) [37].

Membership and non-membership function: intuitionistic fuzzy set A on the inputs X. where Membership function is defined as μ_A: X → [0, 1], where the value of each element of X is mapped by $\mu_A(x)$ to a value between 0 and 1. The value of $\mu_A(x)$, $x \in X$ is called a membership degree or a membership value. While non-membership function: intuitionistic fuzzy set A on the inputs X is defined as ν_A: X → [0, 1], where the value of each element of X is mapped by $\nu_A(x)$ to a value between 0 and 1. The value $\nu_A(x)$, $x \in X$ is called a non-membership degree or a non-membership value [37].

The graphical representation of membership and non-membership functions may contain the different shapes that created using simple curves and straight lines. These functions can be graphically represented any shape as long as the shapes represent the information distribution within the system as the following [37]:

- The intuitionistic fuzzy triangular function: it forms a triangle through a set of three points.
- The intuitionistic fuzzy trapezoidal function: it is a truncated triangle curve with a flat top.
- The intuitionistic fuzzy Gaussian and bell-shaped function: it forms the smooth curves that is open right or left.
- Intuitionistic fuzzy S-shaped and Z-shaped function: it forms the curves of polynomial.

In this research, the membership functions were used for the above fuzzy functions in the implementing of the proposed algorithm.
Those functions will follow in detail:

1) *Triangular functions*

The triangular function is specified through the parameters a, b, c. These parameters were determined by ASCII codes as following [37]:

a refer to the start point and ***c*** refer to the end point. Those locates feet of the triangle.

b locates the peak.

x refer to ASCII value of the secret message.

And we will encrypt ***x*** value by triangular functions, which takes the following form [37]:

$$\mu_A(x) = \begin{cases} 0 \quad , & x \leq a \\ \left(\dfrac{x-a}{b-a}\right), & a < x \leq b \\ \left(\dfrac{c-x}{c-b}\right), & b \leq x < c \\ 0 \quad , & x \geq c \end{cases} \qquad \dots (2.1)$$

The graphical representation of intuitionistic fuzzy triangular functions shown in figure (2.5).

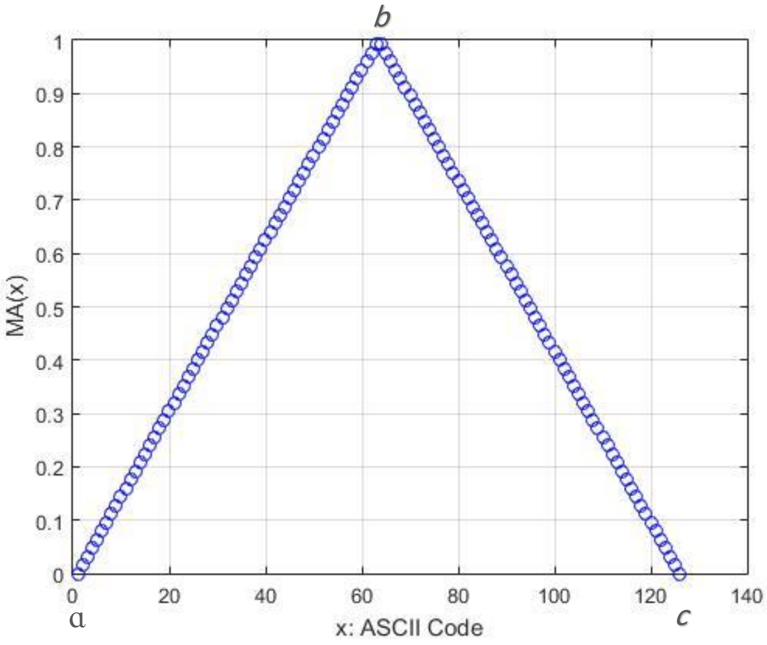


Figure (2.5) Intuitionistic fuzzy triangular functions

2) *Trapezoidal functions*

The trapezoidal function is determined through selection the parameters a, b, c and d which in turn forms a trapezoidal. The parameters is specified by ASCII codes as following [37]:

a refer to the start point and ***d*** refer to the end point. Those locates feet of the trapezium.

b and ***c*** locates the shoulder point.

x refer to ASCII value of the secret message.

And we will encrypt ***x*** value by trapezoidal functions, which takes the following form [37]:

$$\mu_A(x) = \begin{cases} 0 \quad , & x \le a \\ \left(\frac{x-a}{b-a}\right), & a < x < b \\ 1 \quad , & b \le x \le c \\ \left(\frac{d-x}{d-c}\right), & c < x < d \\ 0 \quad , & x \ge d \end{cases} \qquad \ldots (2.2)$$

The graphical representation of intuitionistic fuzzy trapezoidal functions shown in figure (2.6).

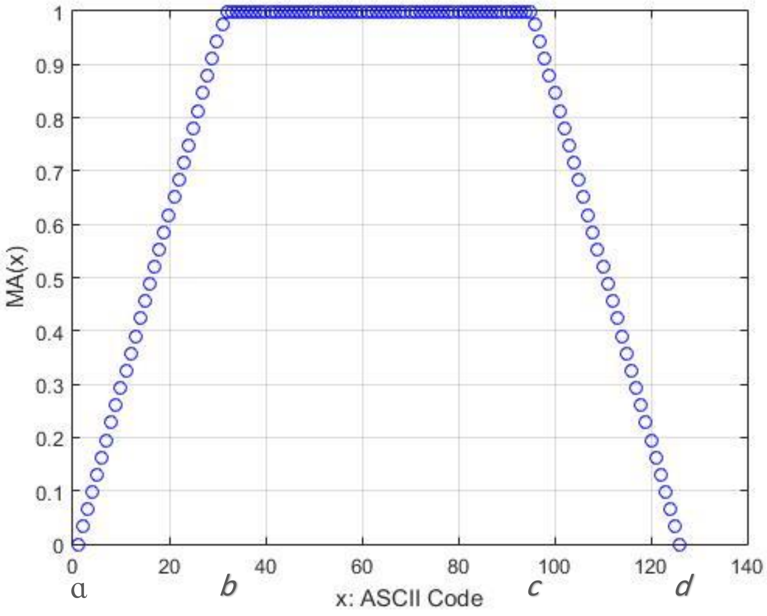


Figure (2.6) Intuitionistic fuzzy trapezoidal functions

3) *Gaussian function*

The gaussian function determined through selection two parameters: k and m, where width k > 0 and m is a central value. The curve is narrower, the value of k will be smaller [37].

Those parameters are specified by ASCII codes. We will encrypt ***x*** (value of the secret message) by gaussian function, which takes the following form [37]:

$$\mu_A\ (x) = \exp\left(-\frac{(x-m)^2}{2(k)^2}\right) \qquad \ldots (2.3)$$

The graphical representation of intuitionistic fuzzy gaussian function shown in figure (2.7).

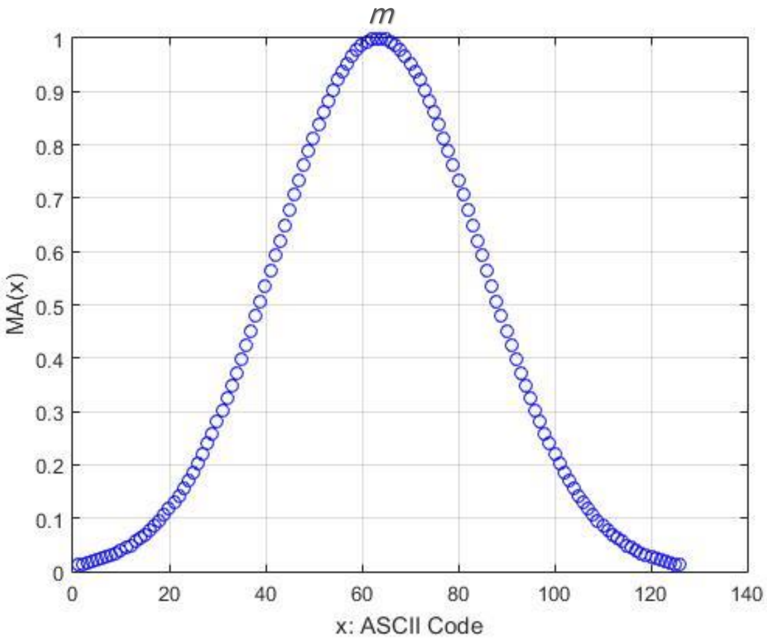


Figure (2.7) Intuitionistic fuzzy gaussian function

4) *Bell-shaped function*

The bell-shaped function is determined through the parameters a, b (positive) and c. The parameters is described by ASCII codes as following [37]:

a refer to the width and ***b*** controls the slopes at the points of the crossing.

c locates the curve center.

x refer to ASCII value of the secret message.

And we will encrypt ***x*** value by the bell-shaped function, which takes the form as the following [37]:

$$\mu_A\,(x) = \left(\frac{1}{1 + \left|\frac{x-c}{a}\right|^{2b}}\right) \qquad \ldots(2.4)$$

The graphical representation of intuitionistic fuzzy bell-shaped function shown in figure (2.8).

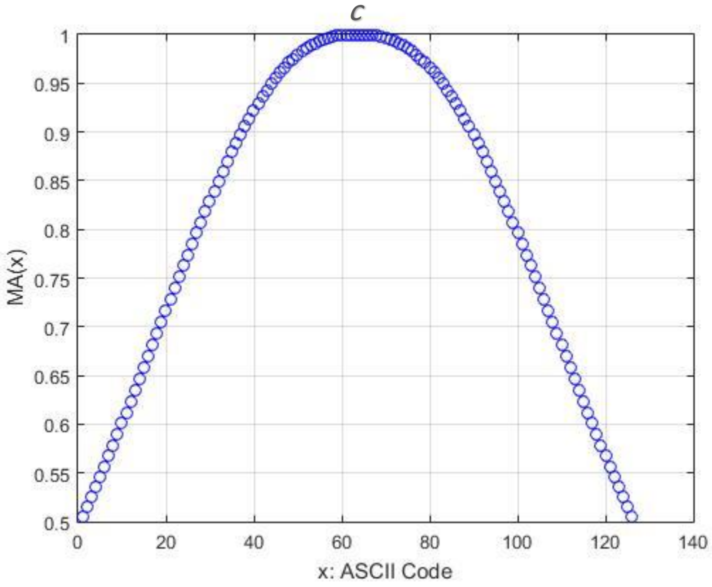


Figure (2.8) Intuitionistic fuzzy bell-shaped functions

5) *Sigmoidal function*

The sigmoidal function is based on the selection of the two parameters *a* and *c*. The function is open to the left or to the right based on the parameter *a* sign, it is open to the left, If the parameter *a* is negative, whereas it is open to the right, If the parameter *a* is positive. The parameters is specified by ASCII codes as following [37]:

c locates the distance from the origin.

a specifies the function steepness.

x refer to ASCII value of the secret message.

And we will encrypt ***x*** value by the sigmoidal function, which takes the form as the following [37]:

$$\mu_A\,(x) = \left(\frac{1}{1+\exp\big(-a(x-c)\big)}\right) \qquad \ldots (2.5)$$

The graphical representation of intuitionistic fuzzy sigmoidal function shown in figure (2.9).

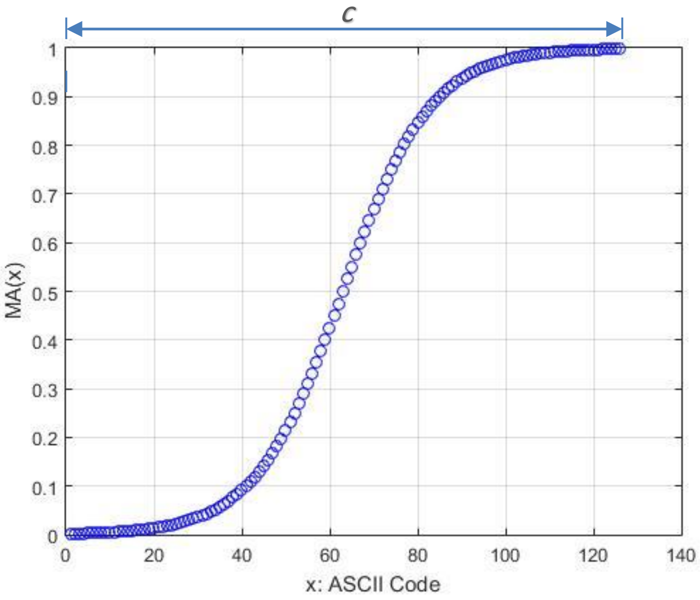


Figure (2.9) Intuitionistic fuzzy sigmoidal function

6) *S-shaped functions*

The s-shaped function is specified through the parameters *a* and *b*, these parameters determine the extremes of the curve sloped portion. The parameters is specified by ASCII codes as following [37]:

a refer to the start point and ***b*** refer to the end point.

x refer to ASCII value of the secret message.

And we will encrypt ***x*** value by the S-shaped functions, which takes the form as the following [37]:

$$\mu_A(x) = \begin{cases} 0 & , \quad x \le a \\ 2\left(\frac{x-a}{b-a}\right)^2 & , \quad a < x \le \frac{a+b}{2} \\ 1-2\left(\frac{x-b}{b-a}\right)^2 & , \quad \frac{a+b}{2} \le x < b \\ 1 & , \quad x \ge b \end{cases} \qquad \ldots (2.6)$$

The graphical representation of intuitionistic fuzzy S-shaped function shown in figure (2.10).

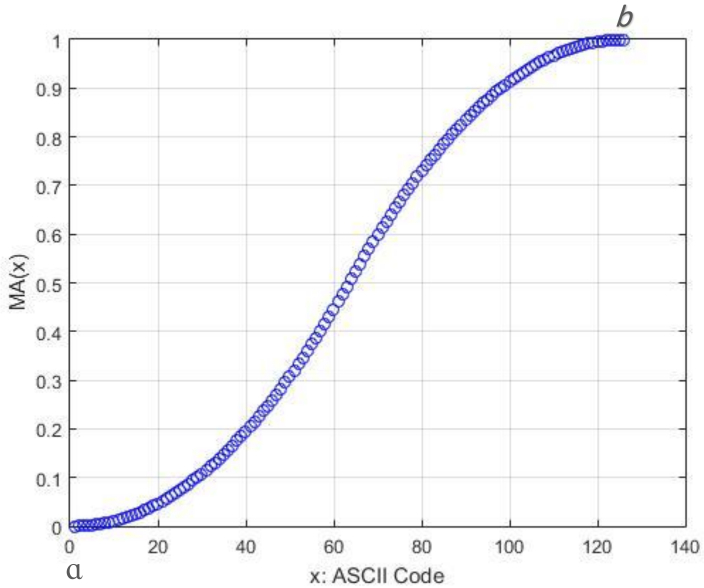


Figure (2.10) Intuitionistic fuzzy S-shaped function

7) *Z-shaped functions*

The z-shaped function is determined through two parameters *a* and *b*, these parameters specify the extremes of the curve sloped portion. The parameters is specified by ASCII codes as following [37]:

a refer to the start point and ***b*** refer to the end point.

x refer to ASCII value of the secret message.

And we will encrypt ***x*** value by the Z-shaped functions, which takes the form as follow [37]:

$$\mu_A(x) = \begin{cases} 1 & , \quad x \le a \\ 1 - 2\left(\frac{x-a}{b-a}\right)^2 & , \quad a < x \le \frac{a+b}{2} \\ 2\left(\frac{x-b}{b-a}\right)^2 & , \quad \frac{a+b}{2} \le x < b \\ 0 & , \quad x \ge b \end{cases} \qquad \dots (2.7)$$

The graphical representation of intuitionistic fuzzy Z-shaped function shown in figure (2.11).

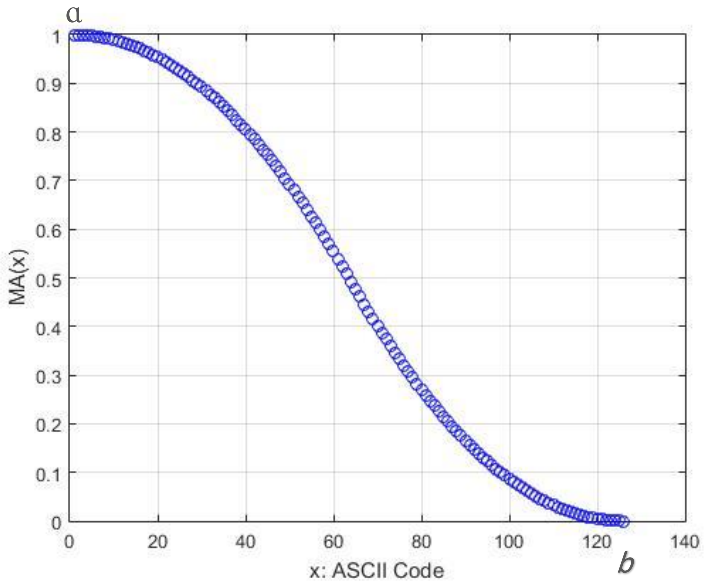


Figure (2.11) Intuitionistic fuzzy Z-shaped function

2.5 Related Works

There are some related works of this research have given experimental results. We will introduce some of them as the following:

2.5.1 Steganography

Several data hiding schemes have been implemented for different applications. Some schemes used an image as a cover media to carry secret data (e.g., audio, image, and text).

Lande et al [38] proposed Fuzzy logic approach to concealment the encrypted watermark in the wavelet domain. Techniques of digital watermarking and cryptography need to be inserted in digital rights management. They are encrypted the content into an incomprehensible format and with leaves water object markup in order distinguishable. The objective of their study is to develop a strong water system so that it can be used easily and safely on the devices. The results show that the proposed system has strength and robustness against different attacks like noise additions and filtering.

LSB classical method hiding information directly in the least significant bit without any change. Al-Rubbaiy [20] proposed a method by enhanced the classical LSB method by split cover-image into sub-images (10×10 pixels) and select only even sub-images to hide data. Also suggested encrypted secret message by using standard fuzzy functions before embedded process to increasing hidden robustness. This proposed system is useful when attacker try to find the plaintext but it's not useful when attacker try to distortion this text without knowing this text.

The secret data can be hidden in the edge areas of the image versus the smooth areas, without the alterations in the image to be visible. To improve the hiding capacity and provide an undetectable visual quality. Liao, Wen, and Zhang [39] proposed a novel steganographic method based on modified LSB substitution and four-pixel differencing. Hiding of the secret information is into each pixel by the k-bit modified LSB substitution method, where k is specified by the average difference value of a four-pixel block. The average difference value is utilized to classify the block as an edge area or a smooth area. Their experimental results have shown better image quality and a large concealment capacity.

LSB embeds secret data by replacing LSBs of a pixel with secret bits directly. However, not all pixels can tolerate an equal amount of change. As a result, many new sophisticated LSB approaches have been proposed to improve this drawback. Yang et al [40] proposed a new adaptive LSB steganographic method. They used Pixel-Value Differencing (PVD) to differentiate between the smooth areas and the edge areas. The difference value level is known by the user. To estimate how many bits of secret data that will be hidden into the pixels, they used the difference value of two consecutive pixels. Pixels that located in the edge areas are hidden by a k-bit LSB method with a larger value more than that of the pixels which located in the smooth areas. The results show that method gives a high image quality and a large hiding capacity.

Khurana and Mehta [22] proposed using two ways to hiding data in an image that are LSB and MSB of an image. LSB of each pixel in cover image is used to embedding message. MSB of each pixel in cover image is used to embedding message. The results were based on measuring an image quality of both LSB and MSB. Where Mean Square Error (MSE) are used to measure difference between the original image and the stego-image. If MSE value is low that means the difference between the original image and the stego-image is low, then the image quality is better.

Garg [23] proposed using two techniques to hiding information in an image, which are LSB and MSB of an image. Their results based on two measures to compute the image quality of LSB and MSB which are MSE and Peak Signal-to-Noise Ratio (PSNR). Where LSB based steganography gave a better results of the image quality than MSB based steganography.

Sabokdast and Mohammadi [41] proposed a new method to hide information in the cover image; where the information is embedding in LSB of an image. Also, LSB is modified by using a fuzzy system. The input of the fuzzy system is the average difference value of the four-pixel block and the output is the bits number that are hiding in each pixel of the block. There is another a fuzzy readjustment that modifies the gray pixels of the block. Fuzzy readjustment ensures that the bits number generated by fuzzy system before hiding are similar of the bits number after hiding and the modifications are little. Their experimental results show improve of an image quality and good hiding capacity.

Akinola and Olatidoye [19] proposed a hybrid approach and compared its efficiency with LSB and MSB algorithms. The LSB and MSB techniques were combined in the hybrid algorithm. The secret message replaced with Two bits (the least significant bit and the most significant bit) of the cover. Comparisons were made based on MSE, PSNR and the encoding time between the hybrid algorithm, LSB and MSB. LSB algorithm produced the best stego-image quality. The combined algorithm had lesser time of image and text encoding.

2.5.2 Cryptography

To give more prospective about the performance of the encryption algorithms. There are some previous works done in field of data encryption and the results expressed for some of used algorithms.

Alanazi et al [42] has done a comparative study of three Encryption Algorithms that are Data Encryption Standard (DES), Triple Data Encryption Standard (3DES) and Advanced Encryption Standard (AES) which presented in to nine factors namely key length, cipher type, block size, security, possible keys, possible ASCII printable character keys and the time required to check all possible keys at 50 billion per second. This study shows that AES is better than DES and 3DES.

Mandal et al [43] introduces comparison between two most widely used symmetric encryption techniques i.e. DES and AES. Their results explain memory required for implementation of AES is 10.2 KB and for DES 43.3

KB. AES is a better option in case of less memory is required, as well as simulation time is less for AES and greater for DES.

Kumar et al [44] introduce comparison between DES and Rivest-Shamir-Adleman (RSA). DES is a secret key based algorithm and RSA is a public key based algorithm. There are two features that specify the difference from one algorithm to another, which are protection of encrypted data against attacks and the required time for encryption and decryption. Their results shown DES algorithm is much better than RSA algorithm where the required time to encryption and decryption RSA algorithm is large.

Singh [34] introduced a detailed study of the encryption algorithms such as RSA, DES, 3DES and AES. These algorithms are different in terms of speed, time and throughput. Each algorithm is distinguished in its own way that might be suitable for different applications. Their Comparative study shows AES algorithm is most efficient from RSA, DES and 3DES where RSA are slower and least security from other algorithms.

Mahajan and Sachdeva [36] introduce a survey of three encryption techniques such as AES, DES and RSA algorithms. Their experiments results show AES algorithm requires a least encryption time from DES and RSA algorithms where RSA algorithm requires a longest encryption time from DES and AES algorithms. Also, decryption of AES algorithm is better than other algorithms. Therefore, the evaluation of AES algorithm is much better than DES and RSA algorithms.

The methods in [19], [22] and [23] proposed hiding a secret text message in a LSB, MSB and hybrid approach of LSB and MSB of an image. In this research, we will hide the secret text message in the best algorithm of LSB, MSB and hybrid algorithm of LSB and MSB of an image by calculating MSE, PSNR and execution time. Before the hiding of a secret text message, we will encrypt this message using the better encryption technique of DES, RSA and AES which are in [36] against the proposed algorithm, which described in chapter 3.

Chapter 3

Algorithm Implementation

3.1 Introduction

This thesis explains in detail implementing the proposed system. The fuzzy logic functions and encryption techniques are used to build this system. The structure of the final software application was illustrated.

3.2 The Proposed System

The proposed system used a gray image as a cover to embed a secret text message. The message is the information which supposed to be secretly stored for transferring to another person so that any illicit person cannot read it. The length of the secret message depends on the length of the image, where the length of a secret message must be less than the length of the image to procedure hiding process as correctly.

In this research, we encrypted the secret text message before hiding it in the image to provide higher security of the message.

Encryption process is used to encrypt the secret text message. The encrypted message is converted in a binary form. At the same time the image was converted into a binary form for hiding the encrypted message. The processed image is now termed as stego-image. To get the secret text message that was hidden in the stego-image. Stego-image will be converted to binary form and extract a binary stream of encrypted message, then decrypt it. Also, some of the attacks are used on stego-image to test and verify the robustness of the algorithm that used to encrypt the secret message. Figure (3.1) shows the proposed system and figure (3.2) shows the flowchart of the proposed system.

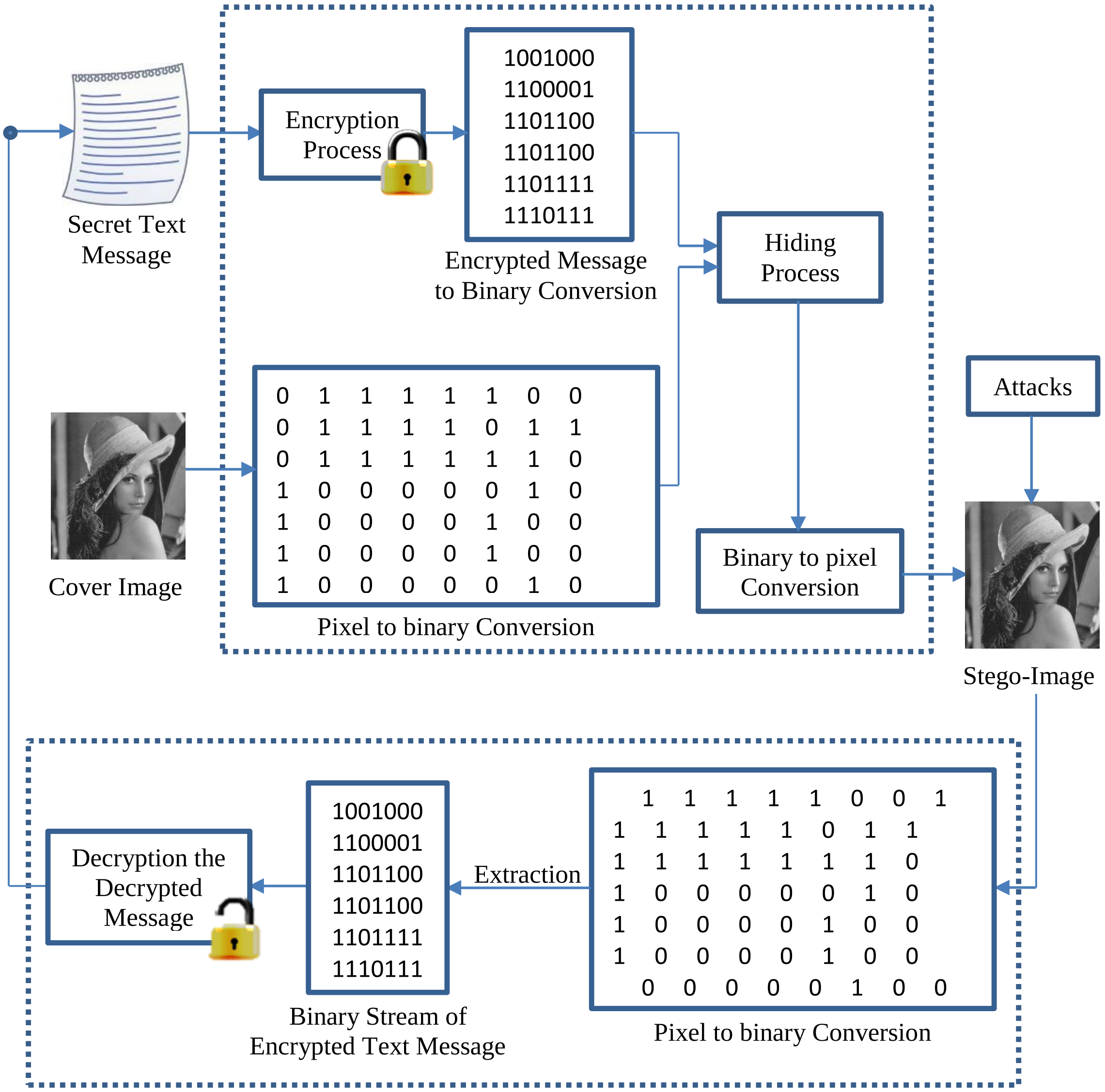
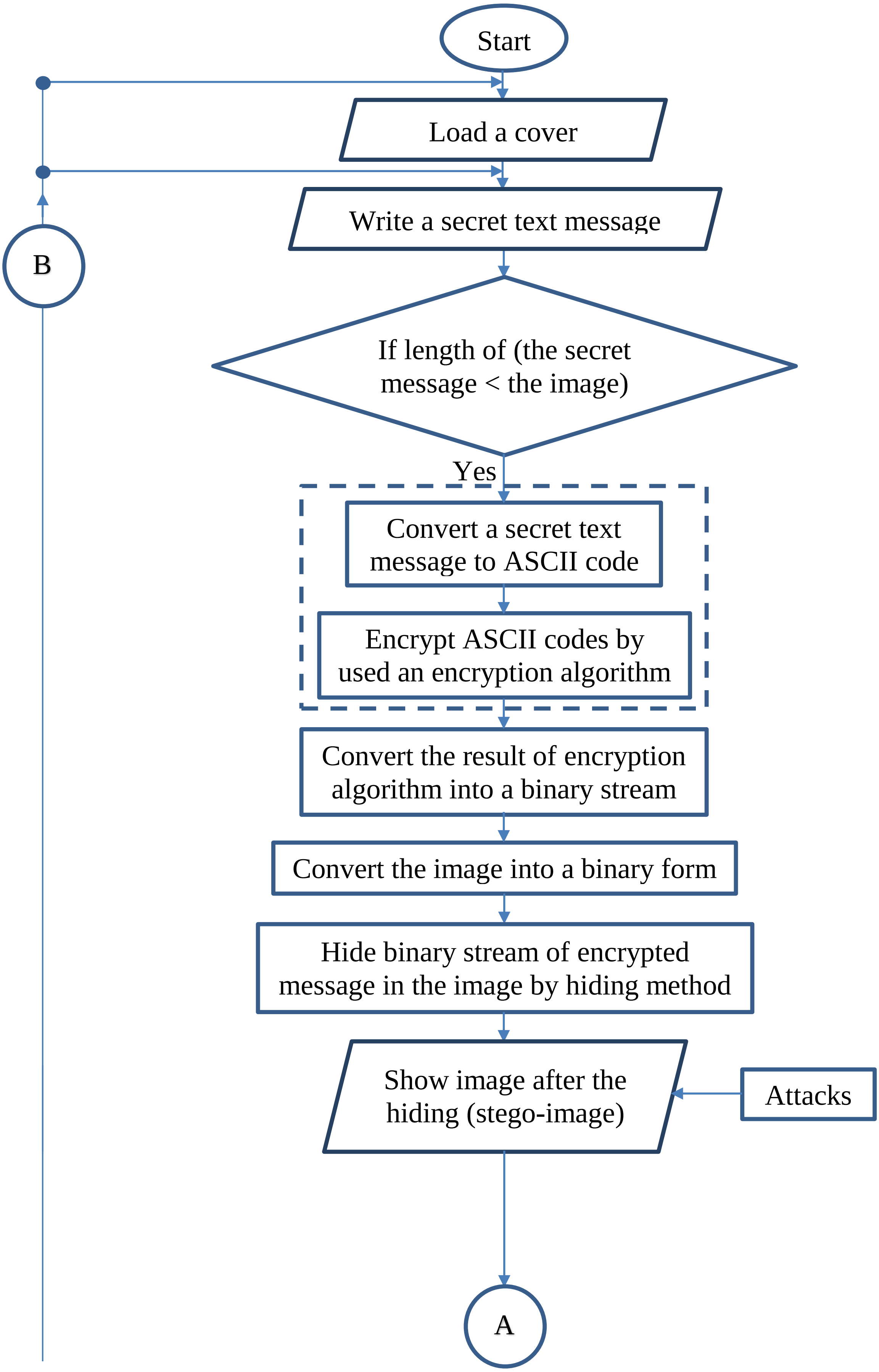


Figure (3.1) The proposed system


Start
Load a cover
Write a secret text message
B
If length of (the secret message < the image)
Yes
Convert a secret text message to ASCII code
Encrypt ASCII codes by used an encryption algorithm
Convert the result of encryption algorithm into a binary stream
Convert the image into a binary form
Hide binary stream of encrypted message in the image by hiding method
Show image after the hiding (stego-image)
Attacks
A

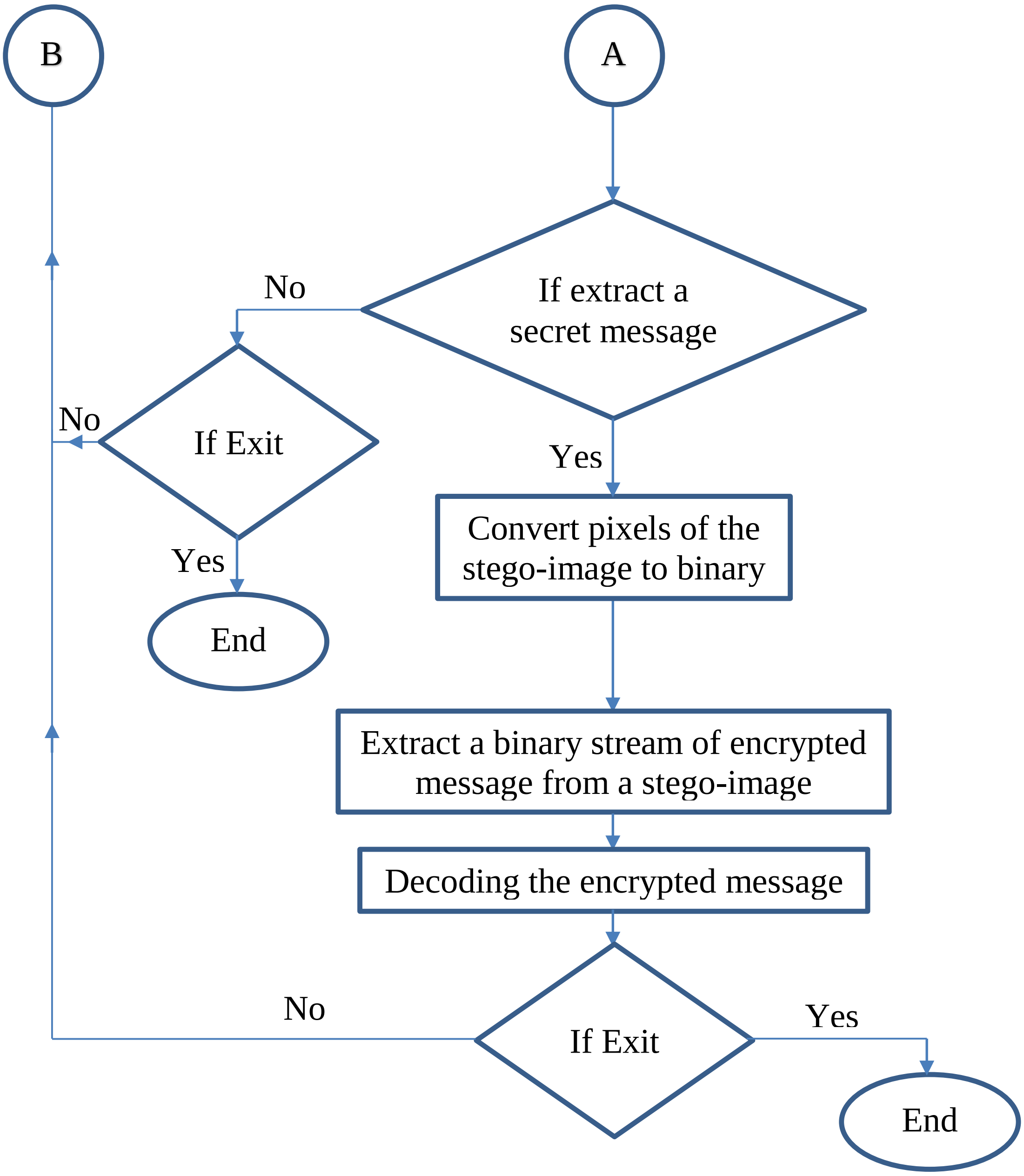

B
A
If extract a secret message
No
Yes
If Exit
No
Yes
End
Convert pixels of the stego-image to binary
Extract a binary stream of encrypted message from a stego-image
Decoding the encrypted message
If Exit
No
Yes
End

Figure (3.2) Flow chart diagram of the proposed system

3.2.1 Encryption Process

In this research, we will use two algorithms in the encryption process of the secret text message, which are fuzzy logic and classical encryption algorithm. To achieve that we will convert the secret text message to ASCII codes, then use the algorithms as follows:

1) *Fuzzy logic algorithm*

   In this algorithm, there are many various functions of the fuzzification that are explained in chapter 2. We will use these functions that converts the ASCII codes into fuzzy values. After that, the fuzzy values converts into binary stream to hiding process.

2) *Encryption algorithm*

   Encryption techniques are DES, RSA and AES, we will using the best of them to encrypt the ASCII codes, then converts into binary stream to hiding process.

3.2.2 Hiding Process

To hide the secret text message, we use of LSB, MSB and a hybrid approach of LSB and MSB. The bits of an image replaced with the bits of secret text message based on hiding method.

3.2.3 Extraction the Secret Message

The extraction part will be reversing the process; extracting secret text message from the image, with decryption of an algorithm.

To extract this message from the stego-image on the receiver side. These steps will be followed:

- Convert pixels of the stego-image to binary, then extract a binary stream of encrypted secret text message from an image. The extraction based on number of rows and columns of the secret text message.
- The secret text message obtained by decryption algorithm operations of the encrypted secret text message. Decryption algorithms are FL and AES algorithm.

Those steps of extraction the secret text message from the stego-image are showing in figure (3.1) and figure (3.2).

3.3 Algorithms Performance Measures

There are commonly used metrics for measuring the image quality which are MSE and PSNR [45].

In this research, we will use those metrics of the image quality of the stego-image. In addition to the execution time.

3.3.1 Mean-Squared Error

MSE represents the cumulative squared error between the cover image and the stego-image. To calculate the MSE between two images I1 (M, N) and I2 (m, n). The equation is as follows [45][46]:

$$MSE = \frac{\sum_{M,N}[I_1(M,N) - I_2(M,N)]^2}{M * N} \qquad \ldots (3.1)$$

M and N are the number of rows and columns in the cover image.

3.3.2 Peak Signal-to-Noise Ratio

PSNR measures the statistical difference between the cover and stego image. The mean-squared error value is needed to compute the PSNR. The equation is as follows [45][46]:

$$PSNR = 10 \ \log_{10} \frac{(255)^2}{MSE} \qquad \ldots (3.2)$$

The MSE and PSNR describe an image quality. The image is better quality whenever the value of the MSE is low or the value of the PSNR is high.

3.4 Steganography Attacks

To verify the robustness of the implemented algorithm, steganography attacks are used on stego-image as explain in figure (3.1) and figure (3.2). These attacks consist of detecting, extracting and destroying hidden information in the stego-image. There are several types of attacks. Some of them are used such as noise (salt and pepper) [47].

3.5 Implemented System

This part describes the implementation of study proposed system. The current study implies images and secret text message in the application of the system. Three standard images are used; Lena, Crowd, and Cameraman, were the format of the used images is JPEG.

The implemented system is conducted on a laptop computer with Intel® Core™ i7-6700HQ CPU@2.60GHz, 32.0GB of RAM memory, Microsoft windows 2010.

3.5.1 Graphical User Interfaces

The Graphical User Interface was constructed using MATLAB GUIDE (Graphical User Interface Design Environment). Using the layout tools provided by GUIDE, designed the graphical user interface shown in figure (3.3).

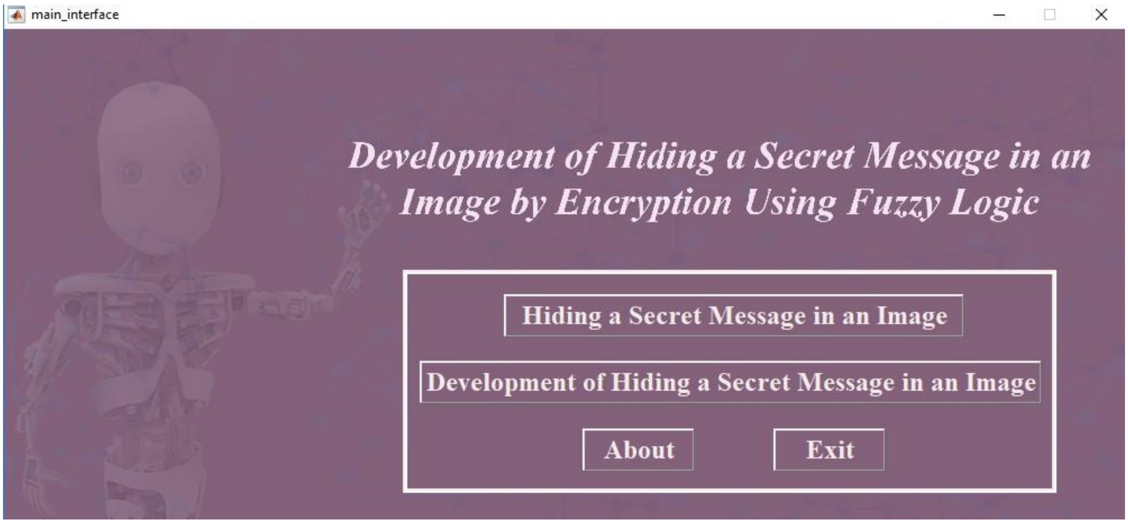
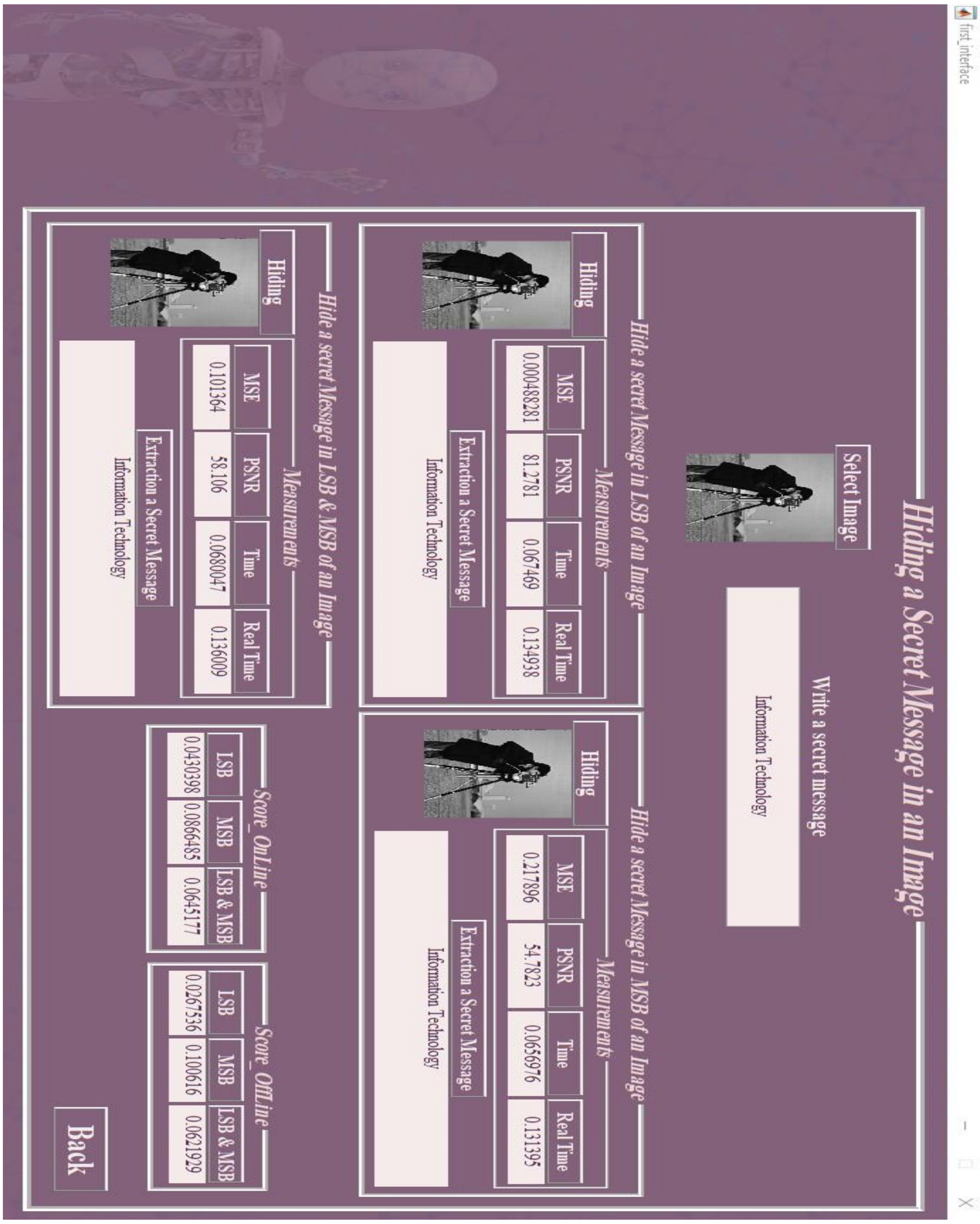

main_interface
Development of Hiding a Secret Message in an Image by Encryption Using Fuzzy Logic
Hiding a Secret Message in an Image
Development of Hiding a Secret Message in an Image
About
Exit

Figure (3.3): Main interface of hiding a secret message in an image

The handlers for clicking on the buttons are coded using MATLAB code to perform the necessary operations. At the main interface window, there are main menu that contain a set of selections as the following:

- Hiding a secret message in an image: this interface as shown in figure (3.4) contains hiding a secret text message in an image by using LSB, MSB and hybrid algorithm of LSB and MSB. In addition, quality measurements of an image and extraction the secret text message from stego-image.


first_interface
Hiding a Secret Message in an Image
Select Image
Hiding
Extraction a Secret Message
Back

Write a secret message: Information Technology

Hide a secret Message in LSB of an Image — Measurements

MSE	PSNR	Time	Real Time
0.000488281	81.2781	0.067469	0.134938

Information Technology

Hide a secret Message in MSB of an Image — Measurements

MSE	PSNR	Time	Real Time
0.217896	54.7823	0.0656976	0.131395

Information Technology

Hide a secret Message in LSB & MSB of an Image — Measurements

MSE	PSNR	Time	Real Time
0.101364	58.106	0.0680047	0.136009

Information Technology

Score_OnLine

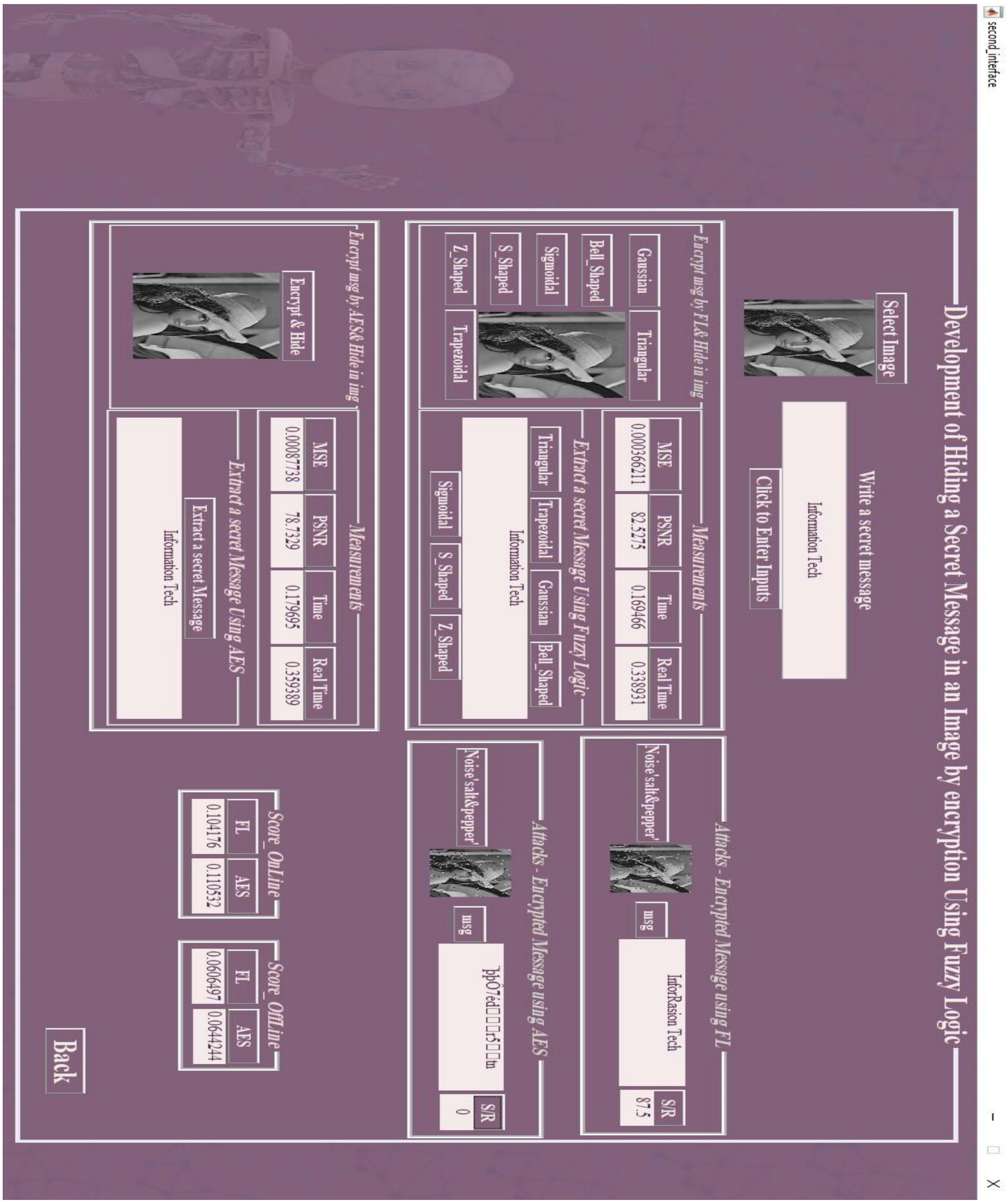
LSB	MSB	LSB & MSB
0.0430398	0.0866485	0.0645177

Score_OffLine

LSB	MSB	LSB & MSB
0.0267536	0.100616	0.0621929

Figure (3.4) Hiding a secret message in an image

- Development of hiding a secret message in an image: This interface contains encryption the secret text message by using two algorithms that are FL functions and AES algorithm and hiding a secret text message in LSB of an image. Also, quality measurements of an image and extraction the secret text message from the stego-image. In addition, some attacks are used on the stego-image. Furthermore, those are shown in figure (3.5) and sigmoidal function was used.



second_interface

Development of Hiding a Secret Message in an Image by encryption Using Fuzzy Logic

Information Tech

MSE	PSNR	Time	Real Time
0.000366211	82.5275	0.169466	0.338931

Information Tech

MSE	PSNR	Time	Real Time
0.00087738	78.7329	0.179695	0.359389

Information Tech

InforRasion Tech

S/R
87.5

þþ07ed□□r5□□m

S/R
0

Score_OnLine

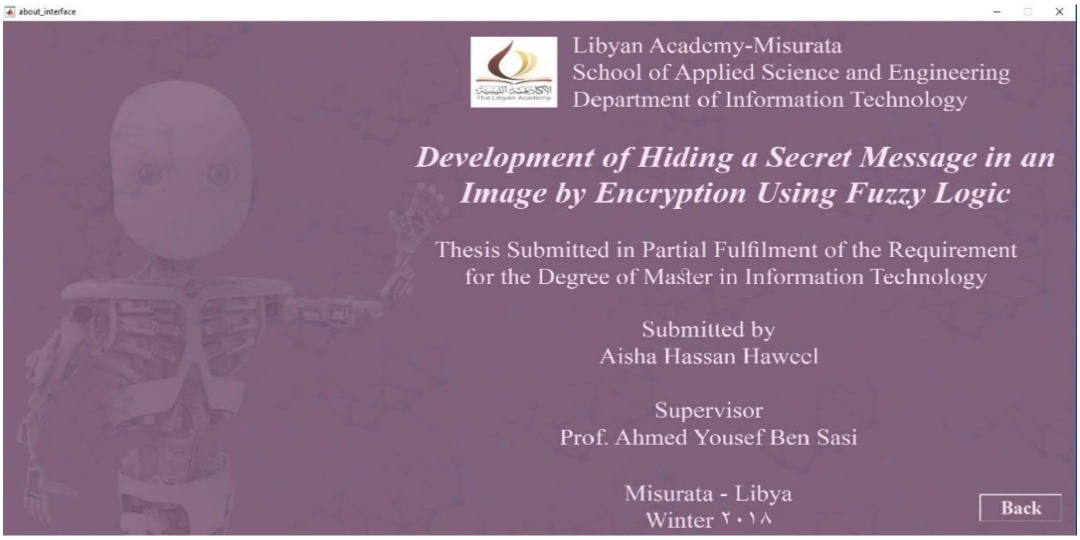
FL	AES
0.104176	0.110532

Score_OffLine

FL	AES
0.0600497	0.0644244

Figure (3.5) Development of hiding a secret message in an image

- The information about this research are shown in figure (3.6).



Libyan Academy-Misurata
School of Applied Science and Engineering
Department of Information Technology

Development of Hiding a Secret Message in an Image by Encryption Using Fuzzy Logic

Thesis Submitted in Partial Fulfilment of the Requirement for the Degree of Master in Information Technology

Submitted by
Aisha Hassan Haweel

Supervisor
Prof. Ahmed Yousef Ben Sasi

Misurata - Libya
Winter ٢٠١٨

Figure (3.6) Information about of the research

Chapter 4

Results and Discussion

4.1 Introduction

This chapter shows the experimental results of the implemented system. Several experiments procedures on some standard images: Lena, Crowd and Cameraman, with different sizes for these images.

4.2 Results and Discussion

Several experiments were performed to evaluate the implemented system. The results of this system were evaluated based on some measurements of an image quality such as MSE and PSNR, and time required for execution of the algorithm. In addition, the robustness of an image against some attacks.

Three standard gray images with different sizes were used in the experiments as cover images. They are Lena, Crowd, and Cameraman. These images were used as a cover image to hide the secret text message in an image, and adopted to comparison the obtained results.

In this research, the results are evaluated based on some the measurements as the following:

4.2.1 Comparison of the hiding algorithms

Hiding of the secret text message in an image using LSB, MSB and hybrid algorithm of LSB and MSB to select the best method of hiding.

In table (4.1) a comparison of the hiding methods has been done on mean-squared error (MSE) to evaluate the quality of the stego-image.

Table (4.1) MSE measure of the hiding methods

Algorithm	*Lena*	*Crowd*	*Cameraman*
LSB	9.53674e-05	0.000305176	0.000488281
MSB	0.0301552	0.0661469	0.217896
Hybrid algorithm	0.0253181	0.0312195	0.101364

The results viewed in the table above give a lower MSE value of the images (Lena, Crowd, and Cameraman) for the LSB algorithm as compared to MSB and hybrid algorithm. Figure (4.1) shows MSE performance by using linear equation of the LSB, MSB and hybrid algorithm of LSB and MSB. Lower MSE values indicates better quality of the stego-image.

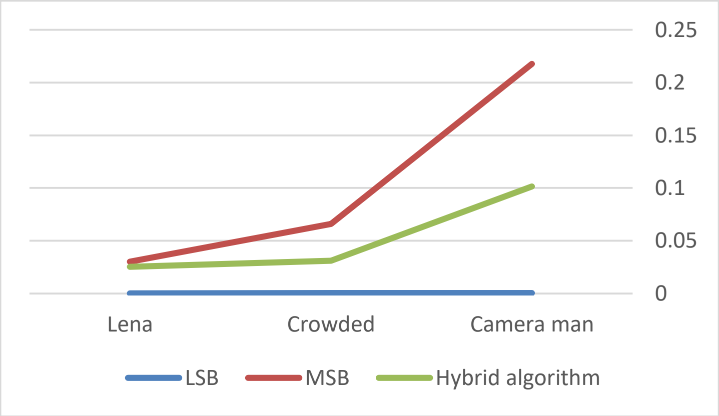


Figure (4.1) MSE performance of the hiding methods

In table (4.2) the comparison of the hiding methods based on basic of peak signal to noise ratio (PSNR) to evaluate the stego-image quality.

Table (4.2) PSNR measure of the hiding methods

Algorithm	*Lena*	*Crowd*	*Cameraman*
LSB	88.3708	83.3193	81.2781
MSB	63.3712	59.9597	54.7823
Hybrid algorithm	64.1305	63.2205	58.106

The results viewed in table (4.2) give a higher PSNR value of the images (Lena, Crowd, and Cameraman) for LSB algorithm as compared to MSB and hybrid algorithm. PSNR performance by using linear equation is shown in figure (4.2) of LSB, MSB and hybrid algorithm of LSB and MSB. Higher PSNR values indicates better quality of the stego-image.

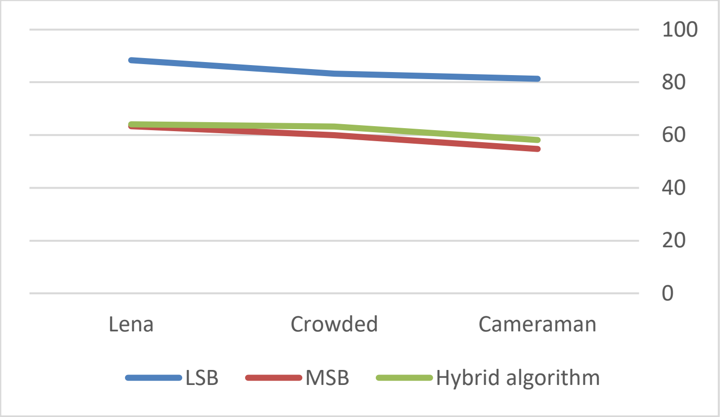


Figure (4.2) PSNR performance of the hiding methods

Execution time is an important measure. So, the time of computation has be computed in offline and online mode. Table (4.3) and table (4.4) show the required time for hiding algorithms execution per second in offline and online mode.

Table (4.3) Time measure of the hiding methods at offline mode

Algorithm	*Lena*	*Crowd*	*Cameraman*
LSB	0.138242	0.0677669	0.067469
MSB	0.139878	0.0678941	0.0656976
Hybrid algorithm	0.13716	0.0680442	0.0680047

Table (4.4) Time measure of the hiding methods at online mode

Algorithm	*Lena*	*Crowd*	*Cameraman*
LSB	0.276483	0.135534	0.134938
MSB	0.279755	0.135788	0.131395
Hybrid algorithm	0.274321	0.136088	0.136009

The results shown in table (4.3) and table (4.4) view execution time of LSB, MSB and hybrid algorithm of LSB and MSB. LSB algorithm requires a lower time for the execution of the images (Crowd) as compared to MSB and hybrid algorithm. MSB algorithm requires a lower time for the execution of the images (Cameraman) as compared to LSB and hybrid algorithm. Hybrid algorithm requires a lower time for the execution of the images (Lena) as compared to LSB and MSB. Time computation by using linear equation of LSB, MSB and hybrid algorithm of LSB and MSB is shown in figure (4.3).

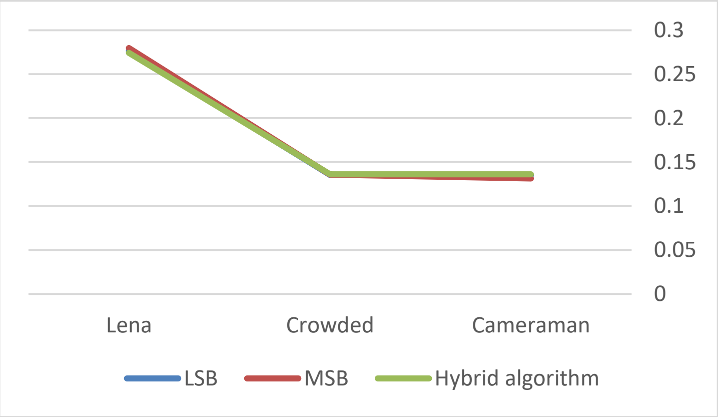
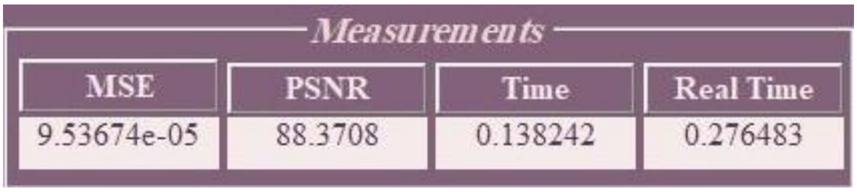


Figure (4.3) Time computation of the hiding methods

Figure (4.4) shows snapshot from the implemented system, which performs some measurements of the hiding process in LSB of a Lena image that are MSE as shown in table (4.1), PSNR as shown in table (4.2) and execution time as shown in table (4.3)(4.4).



Measurements

MSE	PSNR	Time	Real Time
9.53674e-05	88.3708	0.138242	0.276483

Figure (4.4) Performance of the hiding methods

Scores that shown in table (4.5) and table (4.6) in offline and online mode is the average of measurements values (MSE, PSNR and execution time) where the relationship is positive between them.

Table (4.5) Scores of the hiding methods at offline mode

Algorithm	*Lena*	*Crowd*	*Cameraman*
LSB	0.0498843	0.0266914	0.0267536
MSB	0.0619376	0.0502396	0.100616
Hybrid algorithm	0.0593572	0.0383605	0.0621929

Table (4.6) Scores of the hiding methods at online mode

Algorithm	*Lena*	*Crowd*	*Cameraman*
LSB	0.0852272	0.0431216	0.0430398
MSB	0.931136	0.0573014	0.866485
Hybrid algorithm	0.0904784	0.050234	0.0645177

The experimental results shown in table (4.5) and table (4.6) view the scores for the images (Lena, Crowd and Cameraman) and the lower value of the scores was the best algorithm according to average of measurements values and the positive relationship was established between them. Above-all, LSB algorithm gives the best performance where the metrics scoring applied to a (Lena) image rated 0.085, (Crowd) image is 0.0431 and (Cameraman) image is 0.0430. The scores by using linear equation of LSB, MSB and hybrid algorithm of LSB and MSB is shown in figure (4.5).

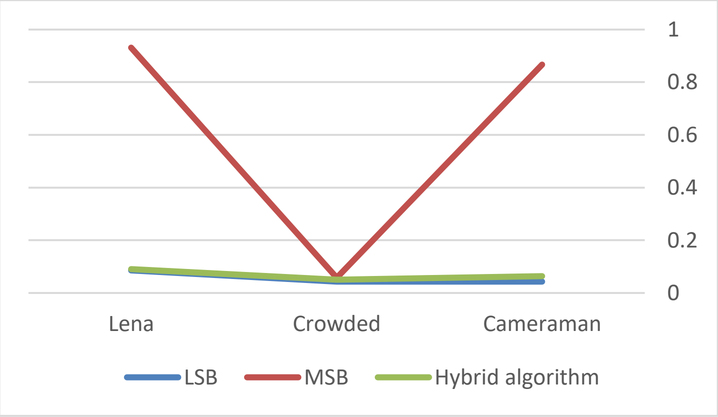
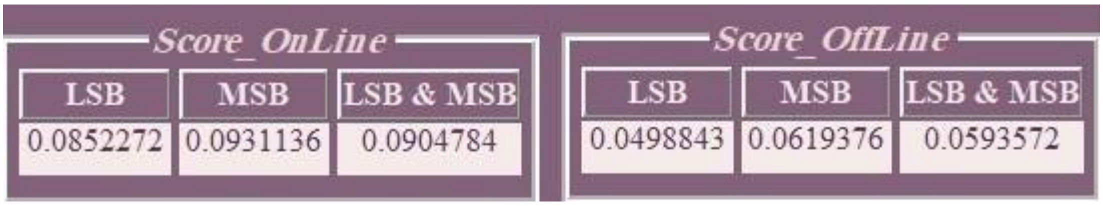


Figure (4.5) Scores of the hiding methods

Figure (4.6) shows snapshot of the implemented system that were some scores of the hiding methods (LSB, MSB and hybrid algorithm of LSB and MSB) of a Lena image in offline mode as shown in table (4.5) and online mode as shown in table (4.6).



Score_OnLine

LSB	MSB	LSB & MSB
0.0852272	0.0931136	0.0904784

Score_OffLine

LSB	MSB	LSB & MSB
0.0498843	0.0619376	0.0593572

Figure (4.6) Scores of the hiding methods at offline and online mode

The results obtained in this research confirms the submission of Akinola and Olatidoye [19] that LSB is better than MSB and hybrid algorithm for hiding messages. Khurana and Mehta [22] and Garg [23], also compared LSB steganography with MSB steganography and asserted that LSB steganography is much better than MSB steganography.

Therefore, the LSB algorithm will be used to hide the encrypted secret text message later in this research.

4.2.2 Comparison of the cryptography algorithms

The experimental results for encryption algorithms that are DES, RSA and AES are shown in table (4.7) and table (4.8). These results evaluated by time computation per second in offline and online mode of algorithm execution based on block size of data.

Table (4.7) Time measure of the encryption algorithms at offline mode

Algorithm	*Packet Size*			
	(128Bit)	*(256Bit)*	*(384Bit)*	*(512Bit)*
DES	0.0597	0.1179	0.1671	0.2151
RSA	1.8361	2.2479	2.3859	2.6856
AES	0.0230	0.0380	0.0461	0.0653

Table (4.8) Time measure of the encryption algorithms in online mode

Algorithm	*Packet Size*			
	(128Bit)	*(256Bit)*	*(384Bit)*	*(512Bit)*
DES	0.1195	0.2358	0.3343	0.4301
RSA	3.6722	4.4957	4.7718	5.3712
AES	0.0460	0.0761	0.0922	0.1307

The results shown in table (4.7) and table (4.8) view execution time of the encryption algorithms. Time taken by RSA algorithm for encryption process is much higher compared to the time taken by DES and AES algorithm, while AES algorithm consumes a less time as compared to RSA and DES algorithm. The execution time of RSA algorithm rated 3.6722 into packet size (128 bit) while the execution time of AES algorithm rated 0.0460 into packet size (128 bit), and the execution time of RSA algorithm rated 5.3712 into packet size (512 bit) while the execution time of AES algorithm rated 0.1307 into packet size (512 bit). Time computation shown in figure (4.7) by using linear equation of the DES, RSA and AES algorithm.

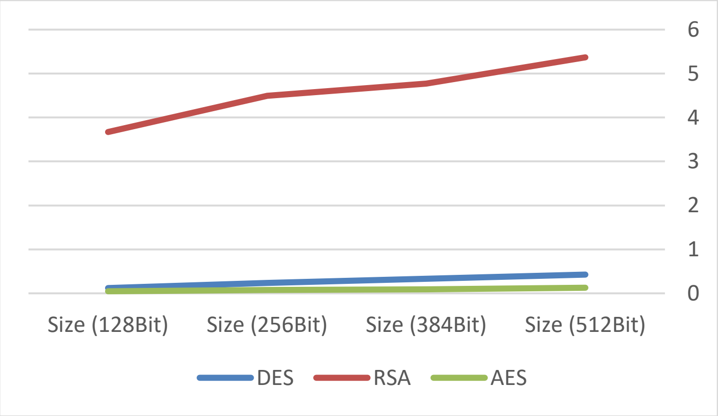


Figure (4.7) Time computation of the encryption algorithms

The results evaluated that AES algorithm is much better than DES and RSA algorithm. These results confirms the submission of Mahajan and Sachdeva [36] that AES algorithm is much better than DES and RSA algorithm. Therefore, AES algorithm is used to encrypt the secret text message for the comparison with fuzzy logic algorithm.

4.2.3 Comparison of the fuzzy logic functions

Fuzzy logic functions was used to encrypt the secret text message then hide this message after the encryption in LSB of an image.

In table (4.9) the comparison of FL functions has been done on basic of parameter Mean-Squared Error (MSE) to evaluate the quality of the stego-image.

Table (4.9) MSE measure of the FL functions

Algorithm	*Lena*	*Crowd*	*Cameraman*
Triangular	0.000453949	0.00175476	0.00186157
Trapezoidal	0.000549316	0.0020752	0.0022583
Gaussian	0.000408173	0.00154114	0.00163269
Bell_Shaped	0.00043869	0.00163269	0.00189209
Sigmoidal	0.000366211	0.00137329	0.0015564
S_Shaped	0.000442505	0.0018158	0.0018158
Z_Shaped	0.000419617	0.00157166	0.00164795

The results viewed in table (4.9) can be seen that a lower MSE value of the images (Lena, Crowd and Cameraman) for the sigmoidal function as compared to other functions of the fuzzy logic. Figure (4.8) shows MSE performance by using linear equation of triangular, trapezoidal, gaussian, bell_shaped, sigmoidal, s_shaped and z_shaped functions. Lower MSE values indicates better quality of the stego-image.

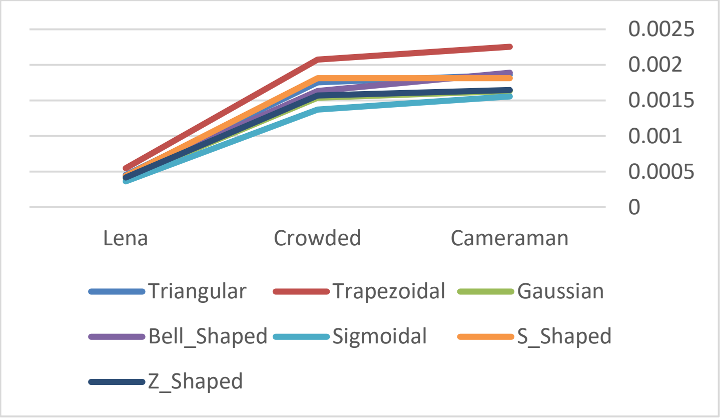


Figure (4.8) MSE performance of fuzzy logic functions

In table (4.10) the results of comparison are shown based on basic of parameter peak signal to noise ratio (PSNR) of an image quality for FL functions.

Table (4.10) PSNR measure of the FL functions

Algorithm	*Lena*	*Crowd*	*Cameraman*
Triangular	81.5947	75.7226	75.466
Trapezoidal	80.7666	74.9942	74.627
Gaussian	82.0564	76.2864	76.0358
Bell_Shaped	81.7432	76.0358	75.3954
Sigmoidal	82.5275	76.7872	76.2436
S_Shaped	81.7056	75.5741	75.5741
Z_Shaped	81.9363	76.2012	75.9954

The results viewed in table (4.10) depict that a higher PSNR value of the images (Lena, Crowd and Cameraman) for the sigmoidal function as compared to other functions of the fuzzy logic. PSNR performance by using linear equation is shown in figure (4.9) of triangular, trapezoidal, gaussian, bell_shaped, sigmoidal, s_shaped and z_shaped functions. Higher PSNR values indicate better quality of the stego-image.

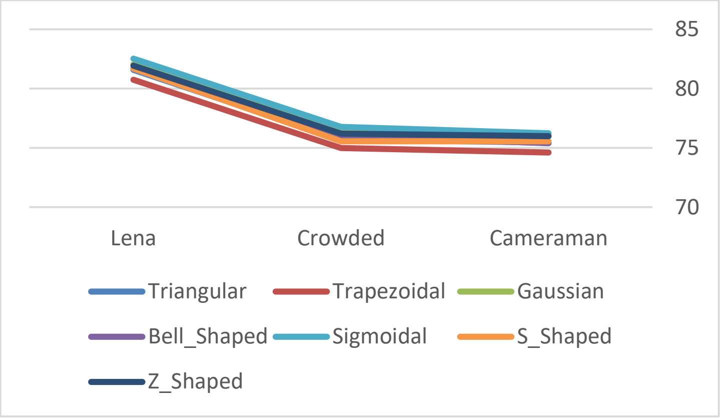


Figure (4.9) PSNR performance of fuzzy logic functions

Execution time is an important measure. So, computed the required time in offline and online mode. Table (4.11) and table (4.12) shows the required time for FL functions execution per second in offline and online mode.

Table (4.11) Time measure of the FL functions at offline mode

Algorithm	*Lena*	*Crowd*	*Cameraman*
Triangular	0.15029	0.0867437	0.0836219
Trapezoidal	0.158468	0.0854767	0.0816735
Gaussian	0.150776	0.0885728	0.08173
Bell_Shaped	0.148359	0.0856897	0.077971
Sigmoidal	0.149294	0.0802359	0.07763
S_Shaped	0.151126	0.0810307	0.0811706
Z_Shaped	0.160464	0.0825967	0.0822858

Table (4.12) Time measure of the FL functions at online mode

Algorithm	*Lena*	*Crowd*	*Cameraman*
Triangular	0.30058	0.173487	0.167244
Trapezoidal	0.316936	0.170953	0.163347
Gaussian	0.301551	0.177146	0.16346
Bell_Shaped	0.296717	0.171379	0.155942
Sigmoidal	0.298588	0.160472	0.15526
S_Shaped	0.302252	0.162061	0.162341
Z_Shaped	0.320928	0.165193	0.164572

The results shown in table (4.11) and table (4.12) view execution time of FL functions is close to each other. Sigmoidal function requires lower time of the image (Lena, Crowd and Cameraman) as compared to other functions of fuzzy logic. Time computation by using linear equation of triangular, trapezoidal, gaussian, bell_shaped, sigmoidal, s_shaped and z_shaped functions are shown in figure (4.10).

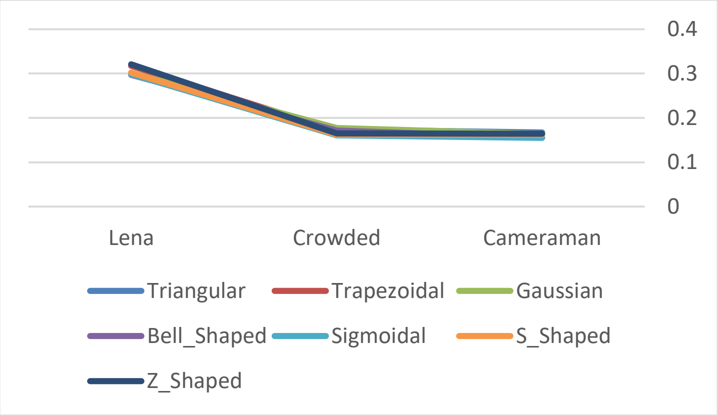
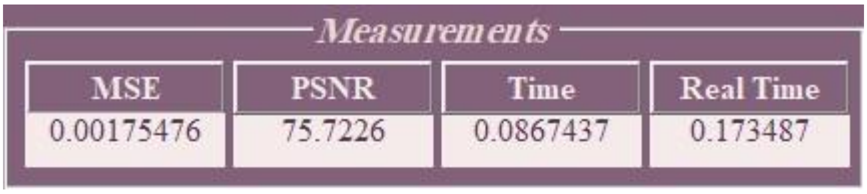


Figure (4.10) Time computation of fuzzy logic functions

Figure (4.11) shows snapshot of the implemented system, which performs some measurements of the fuzzy logic algorithm (triangular function) for a Crowd image that were MSE as shown in table (4.9), PSNR as shown in table (4.10) and execution time as shown in table (4.11)(4.12).



Measurements

MSE	PSNR	Time	Real Time
0.00175476	75.7226	0.0867437	0.173487

Figure (4.11) Performance of the fuzzy logic functions

Table (4.13) and table (4.14) view the scoring of measurements values (MSE, PSNR and execution time) in offline and online mode.

Table (4.13) Scores of the FL functions at offline mode

Algorithm	*Lena*	*Crowd*	*Cameraman*
Triangular	0.0543333	0.0339015	0.0329115
Trapezoidal	0.0571329	0.0336288	0.0324439
Gaussian	0.0544569	0.0344075	0.0321715
Bell_Shaped	0.0542636	0.0334914	0.0310422
Sigmoidal	0.0539257	0.0315441	0.0307674
S_Shaped	0.0546026	0.0320262	0.0320728
Z_Shaped	0.0576961	0.0324305	0.0323642

Table (4.14) Scores of the FL functions at online mode

Algorithm	*Lena*	*Crowd*	*Cameraman*
Triangular	0.092716	0.0550384	0.0531957
Trapezoidal	0.0976669	0.054368	0.0521357
Gaussian	0.0929844	0.0560736	0.0519949
Bell_Shaped	0.0926057	0.0543707	0.0498137
Sigmoidal	0.092073	0.0510208	0.0495125
S_Shaped	0.093212	0.051628	0.0517119
Z_Shaped	0.0988034	0.052497	0.0523328

The experimental results shown in table (4.13) and table (4.14) explained the average of measurements values for the images (Lena, Crowd and Cameraman) where a lower value of the scores is the best algorithm. Sigmoidal function gives a best performance than other functions of fuzzy logic, where the metrics scoring applied to a (Lena) image rated 0.0920, (Crowd) image is 0.0510 and (Cameraman) image is 0.0495. The scores by using linear equation of triangular, trapezoidal, gaussian, bell_shaped, sigmoidal, s_shaped and z_shaped functions are shown in figure (4.12).

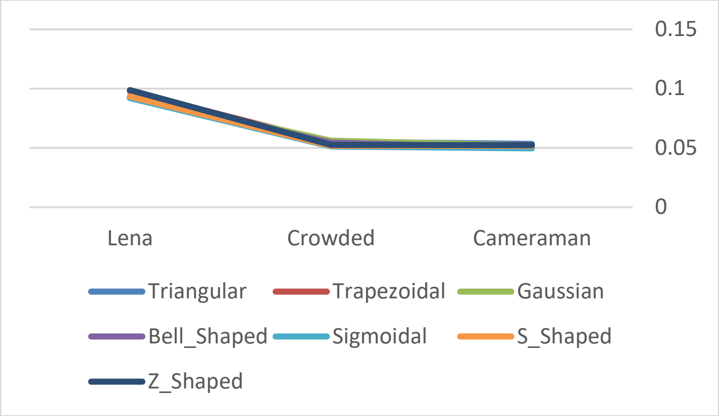


Figure (4.12) Scores of fuzzy logic functions

Overall, sigmoidal function gives a best performance. Therefore, sigmoidal function of fuzzy logic algorithm is used to encrypt the secret text message for the comparison with AES algorithm.

4.2.4 Comparison of the fuzzy logic and AES algorithm under no attack condition

Table (4.15) view comparison between the fuzzy logic (FL) and advanced encryption standard (AES) algorithm based on Mean-Squared Error (MSE).

Table (4.15) MSE measure of the FL and AES algorithm

Algorithm	*Lena*	*Crowd*	*Cameraman*
FL	0.000366211	0.00137329	0.0015564
AES	0.00087738	0.00315857	0.00343323

The experimental results in table (4.15) view a lower MSE value of the fuzzy logic algorithm as compared to AES algorithm. Figure (4.13) shows MSE performance by using linear equation of both algorithms that are FL and AES.

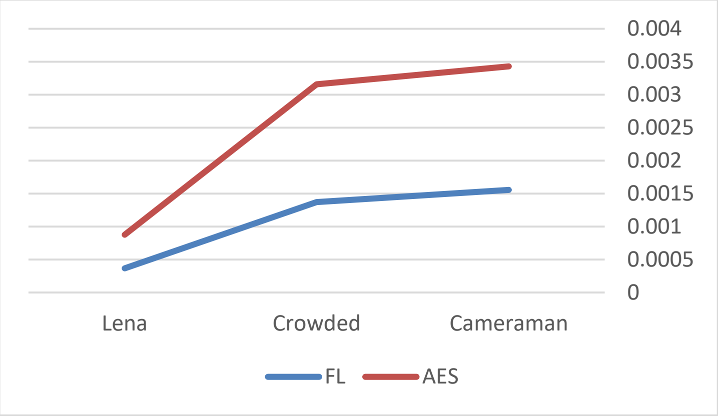


Figure (4.13) MSE performance of FL and AES algorithm

Table (4.16) view comparison between the FL and AES algorithm based on peak signal to noise ratio (PSNR).

Table (4.16) PSNR measure of the FL and AES algorithm

Algorithm	*Lena*	*Crowd*	*Cameraman*
FL	82.5275	76.7872	76.2436
AES	78.7329	73.1699	72.8078

The experimental results in table (4.16) view a higher PSNR value of the fuzzy logic algorithm as compared to AES algorithm. Figure (4.14) shows PSNR performance by using linear equation of both algorithms.

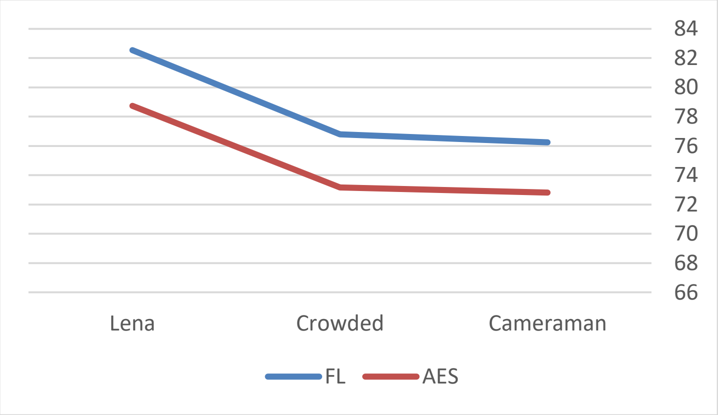


Figure (4.14) PSNR performance of FL and AES algorithm

We also have computed the computation time of FL algorithm and AES algorithm to show how much time is required for the execution in offline and online mode. Table (4.17) and table (4.18) view the execution time of FL and AES algorithm in offline and online mode.

Table (4.17) Time measure of the FL and AES algorithm at offline mode

Algorithm	*Lena*	*Crowd*	*Cameraman*
FL	0.157777	0.0780816	0.0792332
AES	0.215452	0.0912913	0.0861819

Table (4.18) Time measure of the FL and AES algorithm at online mode

Algorithm	*Lena*	*Crowd*	*Cameraman*
FL	0.315554	0.156163	0.158466
AES	0.430903	0.182583	0.172364

The results that view in table (4.17) and table (4.18) explained FL algorithm consumes a lower time as compared AES algorithm. Figure (4.15) view the required time of the execution of both algorithms by using linear equation.

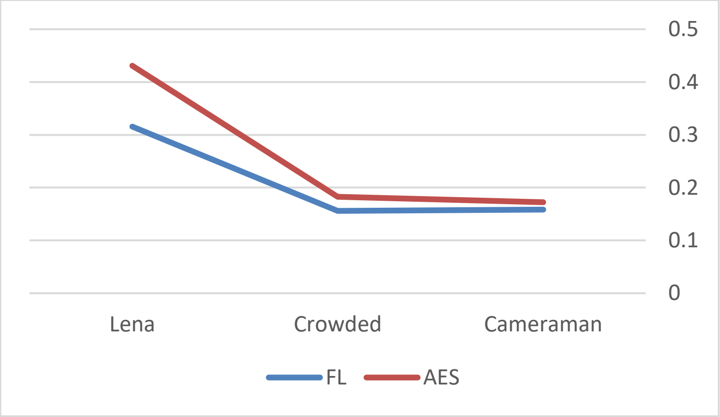
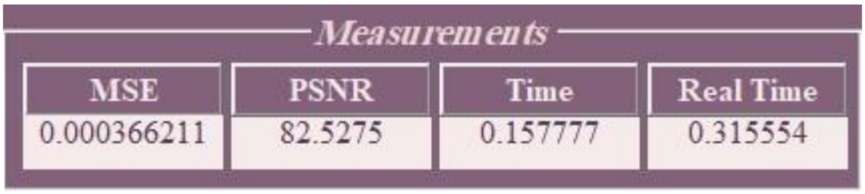


Figure (4.15) Time computation of FL and AES algorithm

Figure (4.16) shows snapshot of the implemented system, which performs some measurements of FL algorithm for Lena image that were MSE as shown in table (4.15), PSNR as shown in table (4.16) and the execution time as shown in table (4.17)(4.18).

Runtime is changing during the run of the program which is not fixed each time, although MSE and PSNR is fixed.

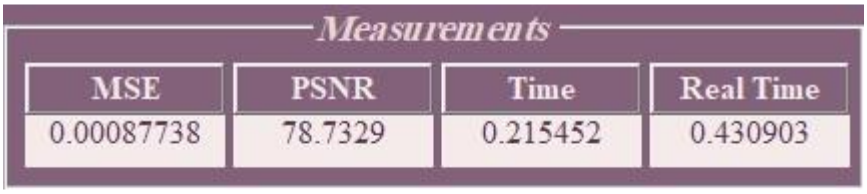


Measurements

MSE	PSNR	Time	Real Time
0.000366211	82.5275	0.157777	0.315554

Figure (4.16) Performance of the FL algorithm

Figure (4.17) shows snapshot of the implemented system, which performs some measurements of AES algorithm for Lena image that were MSE as shown in table (4.15), PSNR as shown in table (4.16) and execution time as shown in table (4.17)(4.18).



Measurements

MSE	PSNR	Time	Real Time
0.00087738	78.7329	0.215452	0.430903

Figure (4.17) Performance of the AES algorithm

Table (4.19) and table (4.20) show the scoring of measurements values (MSE, PSNR and execution time) in offline and online mode.

Table (4.19) Scores of the FL and AES algorithm at offline mode

Algorithm	*Lena*	*Crowd*	*Cameraman*
FL	0.0567535	0.030826	0.0313018
AES	0.0763434	0.0360389	0.03445

Table (4.20) Scores of the FL and AES algorithm at online mode

Algorithm	*Lena*	*Crowd*	*Cameraman*
FL	0.0971629	0.0497282	0.0504744
AES	0.131987	0.0581398	0.0551428

The experimental results shown in table (4.19) and table (4.20) describes the scores for the images (Lena, Crowd and Cameraman) where a lower value of the scores is the best algorithm. FL algorithm gives a best performance than AES algorithm. The metrics scoring of FL algorithm that applied to a (Lena) image rated 0.097, while the metrics scoring of AES algorithm rated 0.13. The metrics scoring of FL algorithm that applied to a (Crowd) image rated 0.049, while the metrics scoring of AES algorithm rated 0.058. The metrics scoring of FL algorithm that applied to a (Cameraman) image rated 0.050, while the metrics scoring of AES algorithm rated 0.055. The scores by using linear equation of FL and AES algorithm is shown in figure (4.18).

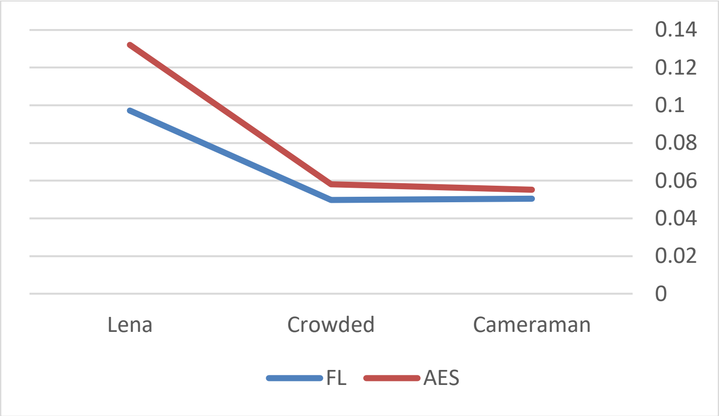
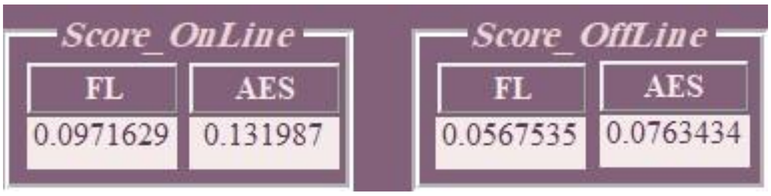


Figure (4.18) Scores of FL and AES algorithm

Figure (4.19) shows snapshot of the implemented system that were some scores of FL and AES algorithm for Lena image in offline mode as shown in table (4.19) and online mode as shown in table (4.20).



Score_OnLine

FL	AES
0.0971629	0.131987

Score_OffLine

FL	AES
0.0567535	0.0763434

Figure (4.19) Scores of the FL and AES algorithm at offline and online mode

All the experimental results proved fuzzy logic algorithm is the best performance against the AES algorithm. These results evaluated based on measurements of quality image that are Mean-Squared Error (MSE) and peak signal to noise ratio (PSNR), in addition, required time of algorithm execution.

4.2.5 Comparison of the fuzzy logic and AES algorithm under attack condition (salt and pepper)

In this research, to verify and test the robustness of the FL algorithm against AES algorithm, we used some attacks such as noise (salt and pepper). Table (4.21) view the attack (noise) on the images (Lena, Crowd and Cameraman). In addition, extraction the secret text message after occurs the attack on the stego-image, and the ratio of similarity between the original secret text message and the secret text message after the extraction from the stego-image of FL and AES algorithm.

Table (4.21) Attack (noise) on the images (Lena, Crowd and Cameraman)

The Secret Text Message	*Attack on stego-image (Noise)*	*Extraction the secret text message of FL*	*similarity Ratio of FL*	*similarity Ratio of AES*
Information Tech	Lena	Idformation Tech	93.75%	0%
	Crowd	InfJrmatio T ch	81.28%	0%
	Cameraman	In orma$jo Tech	75%	0%

The results that view at table (4.21) explain the robustness of the fuzzy logic and AES algorithm. Similarity ratio between the origin secret text message and the extracted secret text message from the stego-image of FL algorithm is a higher than AES algorithm through the attack (noise) that applied on a stego-image (Lena), where similarity ratio of FL algorithm is 93.75%, while similarity ratio of AES algorithm is 0%. Similarity ratio into a stego-image (Crowd) of FL algorithm is 81.28%, while similarity ratio of AES algorithm is 0%. Similarity ratio into a stego-image (Cameraman) of FL algorithm is 75%, while similarity ratio of AES algorithm is 0%.

Overall, the experimental results of the experiments that conducted on a stego-image (Lena, Crowd, and Cameraman) give the robustness of the fuzzy logic algorithm better than AES algorithm.

Chapter 5

Conclusions and Recommendations

5.1 Conclusions

Cryptography and steganography are well known and widely used techniques that manipulate information (messages) in order to encrypt or hide their existence respectively. Steganography is the art and science of communicating in a way which hides the existence of the communication; the steganography hides the message so it cannot be seen, while cryptography scrambles a message so it cannot be understood. The summary can be included in:

1) There are some algorithms to hide a secret text message in an image such as LSB, MSB and hybrid algorithm of LSB and MSB. In this thesis, we choose the best algorithm of these algorithms by the comparison based on the image quality measurement (MSE and PSNR), and calculate the required time to execute the algorithm. The metrics scoring applied to a (Lena) image rated 0.085, (Crowd) image is 0.0431 and (Cameraman) image is 0.0430. These results prove the LSB is the best to hide the secret text message in an image.
2) The robustness and strength of the hiding increased with the encryption. Therefore, we encrypted the secret text message by using fuzzy logic algorithm before hiding it in LSB of an image. There are several functions of the fuzzy logic such as triangular, trapezoidal, gaussian, bell_shaped, sigmoidal, s_shaped and z_shaped functions, and to choose the best function for the encryption, we compared these functions based on the image quality measurement (MSE and PSNR) and the execution time. The metrics scoring applied to a (Lena) image rated 0.0920, (Crowd) image is 0.0510 and (Cameraman) image is 0.0495. These results prove that the sigmoidal function is better than other functions of the fuzzy logic.

3) In this thesis, we compared the results of fuzzy logic algorithm with another encryption algorithm. There are multiple encryption techniques including DES, RSA and AES. These techniques are compared depending on the execution time calculation. The execution time of AES algorithm rated 0.0460 into packet size (128 bit), and of packet size (512 bit) rated 0.1307. These results obtained from the comparison of these techniques based on the execution time demonstrated that AES is the best algorithm. So, we used the AES algorithm to encrypt the secret text message before the hiding process.
4) The results obtained from encrypting the secret text message by using the fuzzy logic algorithm were compared with the results obtained from encrypting the secret text message by using the AES algorithm. The comparison was based on the measurement of an image quality (MSE and PSNR) required time to encrypt and embed a secret message in a cover image. The metrics scoring of FL algorithm that applied to a (Lena) image rated 0.097 while the metrics scoring of AES algorithm rated 0.13, where these metrics in online mode, and the metrics scoring of FL algorithm in offline mode is 0.056 while the metrics scoring of AES algorithm is 0.076. These experimental results presented and analysed show that fuzzy logic algorithm obtains effective time and image quality better than AES algorithm.
5) In addition, some attacks of the steganography has been applied to test the robustness of the image (stego-image) such as noise (salt and paper). The results based on similarity ratio between the origin secret text message and the extracted secret text message from a stego-image. Similarity ratio into a stego-image (Lena) of FL algorithm is 93.75%, while similarity ratio of AES algorithm is 0%. Similarity ratio into a stego-image (Crowd) of FL algorithm is 81.28%, while similarity ratio of AES algorithm is 0%, and similarity ratio into a stego-image

(Cameraman) of FL algorithm is 75%, while similarity ratio of AES algorithm is 0%. These results demonstrate the high robustness of the fuzzy logic algorithm to some attacks like noise.

Therefore, such systems are recommended to be used across networks by users for establishing a more secured communication.

5.2 Recommendations

Although the improvements and developments were introduced in this thesis, we recommend further ways for future work that could be done. The future work should be focused towards optimizing the robustness of the algorithm. This is because the hidden information will be destroyed by some word processing software. Furthermore, it is important to improve the implemented system. There are many suggestion points which can be given to improve the system, these are the followings:

- Using image compression methods to increase robustness against the attacks.
- Dealing with animation images.
- Dealing with audio and video files.
- Use other techniques of the steganography.

References

[1]. Kahate, Atul. Cryptography and network security. Tata McGraw-Hill Education, 2013.

[2]. Siper, Alan, Roger Farley, and Craig Lombardo. "The rise of steganography." Proceedings of Student/Faculty Research Day, CSIS, Pace University (2005).

[3]. Lenti, József. "Steganographic methods." Periodica Polytechnica Electrical Engineering 44.3-4 (2000): 249-258.

[4]. Johnson, Neil F., Zoran Duric, and Sushil Jajodia. Information Hiding: Steganography and Watermarking-Attacks and Countermeasures: Steganography and Watermarking: Attacks and Countermeasures. Vol. 1. Springer Science and Business Media, 2001.

[5]. Habes, Alkhraisat. "Information hiding in BMP image implementation, analysis and evaluation." Saint Petersburg Institute for Informatics and Automation, Russian Academy of Sciences, Saint Petersburg, Russia Received February 26 (2006).

[6]. Abikoye Oluwakemi, C., S. Adewole Kayode, and J. Oladipupo Ayotunde. "Efficient data hiding system using cryptography and steganography." IJAIS 11.4 (2012): 1-6.

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

[8]. Bloisi, Domenico Daniele, and Luca Iocchi. "Image based steganography and cryptography." VISAPP (1). 2007.

[9]. Desai, Hardikkumar V. "Steganography, Cryptography, Watermarking: A Comparitive Study." Journal of Global Research in Computer Science 3.12 (2013): 33-35.

[10]. Fadhil, Mohammed Abbas. "A Novel Steganography-Cryptography System." Proceedings of the World Congress on Engineering and Computer Science. Vol. 1. 2010.

[11]. Mitali, Vijay Kumar, and Arvind Sharma. "A survey on various cryptography techniques." International Journal of Emerging Trends and Technology in Computer Science 3.4 (2014): 6.

[12]. Tripathi, Ritu, and Sanjay Agrawal. "Comparative study of symmetric and asymmetric cryptography techniques." International Journal of Advance Foundation and Research in Computer (IJAFRC) 1.6 (2014): 68-76.

[13]. Liang, Qilian, and Jerry M. Mendel. "Interval type-2 fuzzy logic systems: theory and design." IEEE Transactions on Fuzzy systems 8.5 (2000): 535-550.

[14]. Hellmann, Martin. "Fuzzy logic introduction." Université de Rennes 1 (2001).

[15]. Drir, Nadia, Linda Barazane, and Malik Loudini. "Optimizing the operation of a photovoltaic generator by a genetically tuned fuzzy controller." Archives of Control Sciences 23.2 (2013): 145-167.

[16]. Qasaimeh, Ahmad Raji. Application of the artificial intelligence to the design of constructed wetlands for heavy metal removal. Diss. Concordia University, 2003.

[17]. Prasanna, Mahesh K., and Shantharama C. Rai. "Applications of Fuzzy Logic in Image Processing-A Brief Study." Compusoft 4.3 (2015): 1555.

[18]. Bashardoost, Morteza, Ghazali Bin Sulong, and Parisa Gerami. "Enhanced LSB image Steganography method by using knight Tour algorithm, Vigenere Encryption and LZW compression." IJCSI International Journal of Computer Science Issues 10.2 (2013): 221-227.

[19]. Akinola, Solomon O., and Adebanke A. Olatidoye. "ON THE IMAGE QUALITY AND ENCODING TIMES OF LSB, MSB AND COMBINED LSB-MSB STEGANOGRAPHY ALGORITHMS USING DIGITAL IMAGES." International Journal of Computer Science and Information Technology (IJCSIT) 7.4 (August, 2015), 79-91.

[20]. Al-Rubbaiy, Fatma H. "Concealment of Information and encryption by Using Fuzzy Technique." Journal of the college of basic education in Al-Mustansyriah University, 16.69 (2011), 25-34.

[21]. Sarkar, Tanmoy, and Sugata Sanyal. "Digital Watermarking Techniques in Spatial and Frequency Domain." arXiv preprint arXiv:1406.2146 (2014).

[22]. Khurana, Anil, and B. Mohit Mehta. "Comparison of LSB and MSB based Image Steganography." International Journal of Computer Science and Telecommunications (IJCST) 3.3 (September, 2012), 870-871.

[23]. Garg, Mr Rohit. "Comparison Of Lsb and Msb Based Steganography In Gray-Scale Images Vol. 1, Issue 8, Oct 2012." International Journal of Engineering Research and Technology (IJERT).

[24]. Khare, Pallavi, Jaikaran Singh, and Mukesh Tiwari. "Digital Image Steganography." Journal of Engineering Research and Studies 2.3 (2011): 101-104.

[25]. Por, Lip Yee, and B. Delina. "Information hiding: A new approach in text steganography." WSEAS International Conference. Proceedings. Mathematics and Computers in Science and Engineering. No. 7. World Scientific and Engineering Academy and Society, 2008.

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

[27]. Sheth, Ravi K., and Rashmi M. Tank. "Image Steganography Techniques." International Journal Of Computer Engineering And Sciences 1.2 (2015): 10-15.

[28]. Wang, Huaiqing, and Shuozhong Wang. "Cyber warfare: steganography vs. steganalysis." Communications of the ACM 47.10 (2004): 76-82.

[29]. Tseng, Hsien-Wen, and Chi-Pin Hsieh. "Prediction-based reversible data hiding." Information Sciences 179.14 (2009): 2460-2469.

[30]. Cheddad, Abbas, et al. "Digital image steganography: Survey and analysis of current methods." Signal processing 90.3 (2010): 727-752.

[31]. Hu, Yongjian, et al. "Difference expansion based reversible data hiding using two embedding directions." IEEE Transactions on Multimedia 10.8 (2008): 1500-1512.

[32]. Fridrich, Jessica, and Miroslav Goljan. "On estimation of secret message length in LSB steganography in spatial domain." Proceedings of SPIE. Vol. 5306. 2004.

[33]. Gupta, Shailender, Ankur Goyal, and Bharat Bhushan. "Information hiding using least significant bit steganography and cryptography." International Journal of Modern Education and Computer Science 4.6 (2012): 27.

[34]. Singh, Gurpreet. "A study of encryption algorithms (RSA, DES, 3DES and AES) for information security." International Journal of Computer Applications 67.19 (2013).

[35]. Ramanujam, Sriram, and Marimuthu Karuppiah. "Designing an algorithm with high Avalanche Effect." IJCSNS International Journal of Computer Science and Network Security 11.1 (2011): 106-111.

[36]. Mahajan, Prerna, and Abhishek Sachdeva. "A Study of Encryption Algorithms AES, DES and RSA for security." Global Journal of Computer Science and Technology (2013).

[37]. Radhika, C., and R. Parvathi. "Intuitionistic fuzzification functions." Global Journal of Pure and Applied Mathematics,© Research India Publications 12 (2016): 1211-1227.

[38]. Lande, Pankaj U., et al. "A Fuzzy logic approach to encrypted Watermarking for still Images in Wavelet domain on FPGA." International Journal of Signal Processing, Image Processing and Pattern Recognition 3.2 (2010): 1-10.

[39]. Liao, Xin, Qiao-yan Wen, and Jie Zhang. "A steganographic method for digital images with four-pixel differencing and modified LSB substitution." Journal of Visual Communication and Image Representation 22.1 (2011): 1-8.

[40]. Yang, Cheng-Hsing, et al. "Adaptive data hiding in edge areas of images with spatial LSB domain systems." IEEE Transactions on Information Forensics and Security 3.3 (2008): 488-497.

[41]. Sabokdast, Masume, and Majid Mohammadi. "A fuzzy approach for data hiding in images." Fuzzy Systems (IFSC), 2013 13th Iranian Conference on. IEEE, 2013.

[42]. Alanazi, Hamdan, et al. "New comparative study between DES, 3DES and AES within nine factors." arXiv preprint arXiv:1003.4085 (2010).

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

[44]. Kumar, Aman, Sudesh Jakhar, and Sunil Makkar. "Comparative Analysis between DES and RSA Algorithm’s." International Journal of Advanced Research in Computer Science and Software Engineering 2.7 (2012): 386-391.

[45]. Goel, Stuti, Arun Rana, and Manpreet Kaur. "A review of comparison techniques of image steganography." Global Journal of Computer Science and Technology (2013).

[46]. Kumar, KB Shiva, et al. "Performance comparison of robust steganography based on multiple transformation techniques." Int. J. Comp. Tech. Appl 2.4 (2011): 1035-1047.

[47]. Xing, Yan, and Jieqing Tan. "A color image watermarking scheme resistant against geometrical attacks." Radioengineering 19.1 (2010): 62-67.