Republic of Iraq
Ministry of Higher Education
and Scientific Research
University of Babylon
College of Engineering

Simulation and Analysis of Multi-Level Security Scheme By Using Chaos Algorithms Based On Encryption and Steganography Techniques.

A Thesis
Submitted to the Department of Electrical Engineering Faculty of Engineering University of Babylon in Partial Fulfillment of the Requirements for the Degree of Master in Engineering / Electrical Engineering /Communications.

By

Aliaa Sadoon Abd Al-Daami

(B.Sc.2017)

Supervised by

Prof. Dr. Ehab AbdulRazzaq Hussein

2022 A.D. 1443 A.H.

بِسْمِ اللَّـهِ الرَّحْمَـٰنِ الرَّحِيمِ

(يَرْفَعِ اللَّهُ الَّذِينَ آمَنـــــُوا مِنكُمْ
وَالَّذِينَ أُوتـُـــــوا الْعِلْمَ دَرَجَاتٍ)

صدق الله العظيم

سورة المجادلة : 11

Supervisors Certification

I certify that this thesis titled **"Simulation and Analysis of Multi-Level Security Scheme By Using Chaos Algorithms Based On Encryption and Steganography Techniques."** was prepared by **Aliaa Sadoon Abd** under my supervision at the Electrical Engineering Department, College of Engineering Babylon University, in a partial fulfillment of the requirements for the degree of Master of Science in Electrical Engineering.

Supervisors

Signature:

Name*: Prof. Dr. Ehab A. Hussein*

Date: / / 2022

In view of the available recommendation, we forward this thesis for debate by the examining committee.

Head of the Electrical Engineering Department

Signature: ***Assist. Prof.Dr. Shamam Alwash***

Name:

Date: / / 2022

Acknowledgements

Thanks be to God for the insight that inspired me, and praise be to Him for the blessings He has bestowed upon me, and to Him is the credit for achieving what I aspire to in this research. Praise be to God, who by His praise opens every book and by His remembrance every speech is issued, and by His praise the people of blessings enjoy the abode of reward.

*It gives me great pleasure to extend my thanks and gratitude to (**Prof. Dr. Ehab AbdulRazzaq Hussein**), who provided me with the information I needed in my research*

And for the great efforts he made for me since he proposed the subject of the research and his continuous supervision, and for his advice that helped me a lot in overcoming the difficulties I faced, calling from God success and brilliance in the scientific career.

I would like to extend my thanks and gratitude to the Deanship of the College of Engineering and the Presidency of the Electrical Engineering Department for the facilities and administrative procedures they provided me, which effectively contributed to the completion of the requirements of this research.

.

Researcher

Dedication

To my kind father.... who taught me how to stand firmly above the earth, my role model, and my ideal in life; He is the one who taught me how to live with dignity and honor.

To my tender mother... the source of love, altruism and generosity, I cannot find words that can give her her due, for she is the epic of love and the joy of a lifetime, and an example of dedication and giving.

To my brothers... my support and I share my joys and sorrows.

To all my friends and to all those from
whom I received advice and support;

I dedicate to you the summary of my scientific effort.

Abstract

This work aims to design a hybrid method that should be more stable and robust than the existing methods to enhance the security of data that represented a primary issue nowadays. One of these rapidly evolving methods is steganography and Encryption by using chaos. Furthermore, the work combines the encryption and steganography to preserve confidential information and at the same time keeping of the fundamental properties of the original data. The proposed system carefully presents the specific design of a multi-level security system so that, sound and image are used as secret messages that are undoubtedly intended to be properly preserved from probable hackers and brute force attacks.

Two algorithms are presented in order to implement the required system. Each of them is based on employing chaotic systems to encrypt secret data and then hide them inside a colored image. The first one is Duffing chaotic map which is used to encode the pixels of the image and hide them inside the Least Significant Bit (LSB) of the red color from the cover image, while, modify Arnold cat map is fraudulently used to encode the audio data and insert them inside the least significant bit of the blue color for the cover image. The second algorithm uses encryption interchangeably and is used the same hidden way, as proposed in the first algorithm. The aim of proposing this is to evaluate their quality and efficiency and adopt it as a multi-level security system.

The proposed system is tested practically using Peak Signal-to-Noise Ratio, Bit Error Rate, Structural Similarity Index, and Mean Squared Error. The followed approach objectively compares the extracted cyphered data as well as between Steganographic and secret information. The results of the proposed systems scientifically proved a high capacity, security, robustness and produce many performance enhancements than the existing known techniques with extremely tiny distortions in the good quality of the desired result Stego-image with the original cover image. The obtained result shows PSNR range (57-59)dB, SSIM(99.98-99.99)% and MSE (0.008-0.0203) compared with the original cover image; also, the extracted secret data SSIM (100%), PSNR(∞), and MSE(0) as compare with an original secret data. All simulations are done with MATLAB 2014b program of 2.3Ghz, Core i5. Another test is done by sending the stego-image though the social media program (Messenger, WhatsApp, Email, Telegram and Viber), and it is found from the results that WhatsApp, Telegram and Email Succeed in reconstructing the secret data while the others failed in this mission.

.

List of Contents

List of Contents

List of Contents

List of Tables

List of Figures

List of Figures

List of Figures

List of Abbreviations

Abbreviation	Definition
1-D	One Dimension.
2-D	Two Dimension.
ACM	Arnold Cat Map.
AES	Advanced Encryption Standard.
AT	Arnold transform.
AWGN	Additive white Gaussian Noise.
BER	Bit Error Rate.
BMP	Bit map.
CRN	Chaotic Random Numbers.
CT	Contourlet Transform.
DCT	Discrete Cosine Transform.
DES	Data Encryption Standard.
DFT	Discrete Fourier Transform.
DWT	Discrete Wavelet Transform.
GIF	Graphical Interchange Format.
HVS	Human Visual System.
IP	Internet Protocol.
JPEG	Joint Photographic Experts Group.
LBM	Length of Binary Message.
LCA	Advanced Computing Laboratory.
LRP	Length of Row Pic.
LSB	Least Significant Bit.
MACM	Modified Arnold Cat Map.
MD	Multi-Dimensional.
MSB	Most Significant Bit.
MSE	Mean Square Error.
Org	Original image.
PSNR	Peak-Signal-to-Noise-Ratio.

List of Abbreviations

Abbreviation	Definition
RGB	Red–Green–Blue.
RIV	Random Index Vector.
RSA	Rivest-Shamir-Adleman.
SSIM	Structural Similarity Index.
SSSNR	Segmental Spectral Signal to Noise Ratio.
Steg	The stego image.
TCP	Transmission Control Protocol.
US	United State.
XOR	Exclusive OR.
NC	Normalized Correlation.
N\A	Not Available.

List of Symbols

Symbol	Definition
$\dot{x}$	The state vector of the system at a time (t)
Xo	Initial condition for chaotic flow system
Z	Differential equations that govern the chaotic flow system
σ, β, ρ	Lorenz System parameters
a, b, c	Rössler System parameters
m ,n, l	Initial condition of Rössler System
f(x)	The electrical response of the nonlinear resistor.
a, b, c, m0, m1	Chua System parameters
a, b, c, I0	Nien System parameters
r ,b	Henon Map parameters
$r.X_n$	Logistic map system parameters
$Y_n.X_n$	Initial condition for duffing map
γ, δ	Duffing system parameters
A,B,C	Arnold Cat map system parameters
B_{err}	The number of error bits in the image
M,N	The dimensions of the duplicate.
$Pic1$	Original image
$Pic2$	Stego image
Xi (k)	The DFT of the individual text patterns' frames
x ,y	Dimensions of image
p	The maximum possible pixel value of the image
μx, μy	The local means
σx, σy	The standard deviations
σxy	The cross-covariance
$C_x(n)$	The cpestral coefficients of original voice.
a(n)	The number of LPC operations
r ,c , d	r: num of rows, c: num of column, d: dimensions of pixel

Chapter One

General Introduction

CHAPTER ONE

GENERAL INTRODUCTION

1.1 Brief Consideration

Sending and receiving data has become very comfortable and accurate as a result of the modern digital revolution, but as a result of the tremendous development in means and hacking programs, it has become difficult to maintain the confidentiality of the information sent from manipulation by hackers. After the development that took place in digital applications and programs that enabled hackers to penetrate copyright and modify any file easily, preserving the copyright of data such as videos, pictures, documents, articles, etc. has become a concern for many institutions such as publishing , universities, television stations, government institutions and many more. other institution [1].

Over the past years, the international community has been aware of the role of the internet in many terrorist attacks . Where most of government confidential information when it's transmitted over the internet is depending on the encryption process as a defence way against penetration, so the confidentiality of information depends on the strength of the encryption system that used, which often easily be broken with due to the advances in decoding technologies and breaking encryption algorithm. Therefore, many researchers and institutions have turned to ways of concealing information in a way that cannot be easily detected (hide the presence of information) [2].

1.2 Literature Review

Boulebtateche et al, (2011) [3], proposed multimedia data such as (audio and images) were presented in different sizes from 1-D logistic maps based on an encryption algorithm. Experimental results show the proposed approach is really effective, The most prominent results were CC=(0.013- 0.004). works with higher security, and is very useful for transferring critical data over unsecured open network media.

Karim et.al,(2011)[4] ,presented a new approach to enhance the security of existing LSB substitution method by adding one extra barrier of secret key. In the said method, secret key and red channel are used as an indicator while green and blue channels are data channels. On the basis of secret key bits and red channel LSBs, the secret data bits are embedded either in green channel or in blue channel. If either the bit of red channel LSB or secret key bit is 1, then the LSB of green channel is replaced with secret message bit, otherwise LSB of blue channel is replaced with secret bit. Although, this approach possesses the same payload as LSB based approaches but it increases the security by making use of secret key. An intruder cannot easily extract the secret information without the correct secret key. The most prominent results were PSNR=53.7%.

Ali Kanso et al, (2012) [5], a new algorithm based on a single 2-D chaotic map was proposed (Arnold Cat map). The proposed approach employs a single chaotic map to determine the pixel position of the host color image and the relevant channel (red, green, or blue), as well as the bit position of the target value where the sensitive information bit can be buried, using a single chaotic map. Some characteristics of the proposed method it included a bigger key space and a high level of security against external attacks. In this work PSNR= 43.95%.

Hemalatha et al.(2013)[6], proposed a novel image steganography technique to hide multiple secret images and keys in color cover image using Integer Wavelet Transform (IWT). This approach results in high quality of the stego image having high PSNR values , but in this work the secret image is decomposed by IWT and hiding only its LL coefficients on the cover image. In this work PSNR= 44.7%.

Zaynab Najeeb et al,(2014)[7], steganography algorithm based on controlute transform by using (MACM) was suggested. The proposed method has proven its efficiency in retrieving confidential data, in addition to achieving high capacity as a result of using the on controlute transform compared to the traditional methods. This result represented by PSNR=44.7%,CC=0.9997.

Rotray et al, (2014) [8], suggested inclusion of confidential data in digital form in the spatial domain by using the (AT) Arnold transform and using least significant bits(LSB).The application is used twice in two different phases.in this work PSNR=(30-51)%.

J. K. Mandal et al, (2014) [9], suggested encrypting the secret parts of the message based on chaos theory before including them in the cover image. A 3-3-2 LSB insertion method has been used for image steganography. The results of this method proved its ability to maintain the stego-image quality in addition to a significant improvement in the value of the peak signal-to-noise (PSNR=50-58)%.

A. Jawahir, et al, (2015)[10], Suggested conversion technology that is compatible with the WAV file extension. The original sounds can be encrypted in different combinations with a password, and the results of random sounds can be restored to the original sounds with the correct password. It is recommended that users need to use a complex password, such as long or mixed-character passwords. In other words, the conversion technology is able to ensure the security of audio data files. In this work MSE=0.0000004.

A. K. Jawad, et al, (2015)[11], Introduced a chaotic system, used to encrypt the message which is a voice signal, and transmit the encrypted message over the AWGN channel. The research focuses on two significant things (information security and noise). The proposed system was maintained two-stage encryption based on chaotic systems. The first stage is chaotic scrambling, and the second one is chaotic masking. These two stages instantly make the encrypted message is too secured during possible transmission through the proper channel because the key space is extremely large. Also proposed three methods to decrease noise in the secure channel.

Muhammad K., et al, (2015)[12], Proposed a new Steganography technology based on secret key, encryption and image switching is proposed to perform gray-level adjustment of true color images. Here, encryption algorithms are used where the secret information and secret key are first encrypted and then included in the cover image. In addition, the input image is changed before the embedding process. The proposed method provides five levels of security through image switching, bit-XOR loop, bit shuffling, stego key-based encryption, and gray-level modulation. This makes data recovery a difficult task for attackers. The result of this work represented by PSNR=40.5% and MSE=0.6823.

B. Mondal et al, (2016)[13], proposed a cryptographic algorithm based on the fundamental principle of random behavior. Encryption was done and then tested with the toughest tests. The experimental results of this efficient algorithm prove the apparent effectiveness of the proposed system in carefully preserving accurate information and resisting attacks against the proposed system. In this work PSNR=39.8%,and MSE=0.03.

Sherif et al. (2017) [14], based on chaos theory, proposed a modern method for image steganography The suggested technique typically includes a new 3-D chaotic map (LCA Map) with a maximum Lyapunov exponent of 20.58, which is used to construct three chaotic sequences effectively.

Chung F., et al, (2018) [15], proposed a new coding system for a color image. The proposed system is traditionally based on chaos theory with an efficient key generation method. Hyper and Logistic Map was properly used to efficiently generate key flow and scramble images. In this effective method, the repeat times are reduced about 3 times compared to other used methods and in the scrambling stage; the location of the pixel is mixed in the input image. The results show the proposal has a high level of safety.

Chunhu Li et al, (2019) [16], designed photo encryption based on the three dimensions Chaotic Logistic Map. At first, the secret key is generated by using a 3D logistic map. This naturally has better randomness properties and a high-security level. The simulation results show that this algorithm, for example, positively has intense security, long keyspace, and high encryption speed.

Kanso, et al, (2020)[17]*,* proposed algorithm for the image steganography by instantly following LSB and secret map, through the confined use of chaotic 3-D maps, which are 3-D Chebyshev maps and 3-D logistic maps. This effective method is typically characterized by a significant degree of comparative safety and considerable resistance to external attacks.Here in the work PSNR=45.8andMSE=3%.

.

Shehab, Jinan, et al (2021)[18], proposed a new steganography algorithm based on 5-D chaotic map. Use the images as confidential information that has been included within the video frames that represent the carrier. The results demonstrate both of the secret color image and cover video, where retaining its explicitness and properties after reconstruction in the receiver. However, the results prove stability and reliability of the proposed system under several conditions and can avoid attacks. PSNR in this work 54.8db.

The proposed system is characterized by strong points compared to previous studies. Most of these studies are represented by security systems of one or two levels as a maximum, which makes the protection of confidential data within the scope of concern. The proposed system is characterized by increased levels of security compared to the previous studies. The proposed system here includes four levels of security. The first level is to encrypt confidential data through chaotic functions. The second level of security is represented by the parameters used, such as secret keys known to the sender and recipient. The third level is to hide the secret data inside the cover image by following the generation of random location and the least significant bit-work of the level. The fourth is to occupy the color levels of the cover image, and therefore it is difficult to retrieve confidential data. In addition to these levels, the system is characterized by synchronization between the sender and receiver and retrieve confidential information at the receiving side with a very low error rate. This proves the efficiency of the proposed work compared to previous studies.

1.3 Aims of the Thesis

In the current technological development, there is a massive increase in the amount of data that is sent and shared over the different types of the communication channel, especially the data that exchanges in the various internet platforms. The maintaining of data, especially the image file and audio file is one of the critical things that make the people worry. The main goals of this thesis are :-

1. Increase the security by designing a multi-level security system that is properly used to effectively protect the secret hidden data from manipulating by mixing between Steganography and cryptography principles.
2. Intentionally hide confidential data inside the RGB scale cover image without causing distinct suspicion, by generating random locations from the cover for the specific purpose of masking.
3. Efficiently implement and scientifically test the proposed chaotic systems.
4. Obtaining highly embedding system through:
    - Provide a high similarity between original image and Stego-image

- Extracting a high quality hidden data from the received Stego-image when sending it through different communication channel under the effect of various noise type.

1.4 Thesis Outline

This thesis is presented into five chapters. Among these chapters the first chapter which generously provides a brief introduction to steganography adequately explains the keywords and familiar phrases that were used in the thesis

Chapter Two: This chapter explains the requirements and theories of the image Steganography technique.

Chapter Three: Introduce the proposed system.

Chapter Four: Introduce the results and discussions.

Chapter Five: Contain the conclusions and future works.

Chapter Two

Theoretical Background

CHAPTER TWO
THEORETICAL BACKGROUND

2.1 Introduction

The concept of WYSIWYG (What You See Is What You Get) is no longer correct. It would not trick a Steganographer person as it was previously, because of the development in the computer systems and steganalysis tools. So, there is a need for new algorithm more secure and reliable enable entirely hide the presence of data and deceive various steganalysis systems. For decades, people have sought to develop innovative methods of covert communication so that ,three interconnected technologies are depicted steganography, watermarks and encryption. It is very difficult to separate the first two matters, especially for those from different disciplines [19].

In this chapter, the most important theories taken within this thesis are: encrypted, the reasons for encryption, image steganography, the necessity of chaos and the LSB principle. At the end of the chapter, evaluation of the Performance of steganography system by many tests like BER, SSIM, PSNR, etc. are studied.

2.2 Theory of Steganography

In 1983 the study of information concealment began [20]. A simplified representation of Steganography theory is the prisoner's problem where Alice and Bob are in jail locked up in different cells. Where they want to communicate in order to plot an escape plan But any connection between them is checked by a warden named Wendy, who will put them in individual jail at any slight-doubt of trouble. In order to solve this problem, Alice will use the global standard of Steganography, where Bob wishes to send a secret letter M to Alice. In order to do this he ”embeds” M inside a cover-object "letter", to get the Stego-letter S, then sent the Stego-letter through a public channel. The warden Wendy who is free to review all messages transferred among Alice and Bob and decide whether the message is positive or negative. He checks the message and tries to determine if it possibly includes a hidden letter. If it appears that it does, then she takes suitable action else she allows the letter to pass without any modification [21].

In recent years, as a result of the development that took place in computer association, the study of the science of concealment has been developed, and several algorithms have emerged to hide messages with high reliability and the difficulty of detection. The measures of steganography have been transferred to digital processing. At present, research, study and development is underway in the field of digital signal processing, information theory, and encryption techniques support to have stable and strong steganography systems[22]. The “Steganography” is the technique of hiding secret messages (text, image, video, sound, etc.) inside the carrier medium (cover) in a way can’t be detected and recognized it by Unauthorized person to view it. Steganography word is the mixing of “Steganos” and “Graphy” Greeks words that exactly means “covered writing”.

For deeper understand the process of Steganography, it must first understand the “Cryptography” process. The Cryptography is the technique of transformer a secret message (information) into another format named “ciphertext” which can’t be readable by an unauthorised person [23].

So that, it can be considered the cryptography as a complementary to Steganography where the secret message is encrypted before concealment it in cover medium, this adds a high degree of security and hardiness. The fundamental concept of data hiding can be sufficiently shown in Figure (2.1)[24].

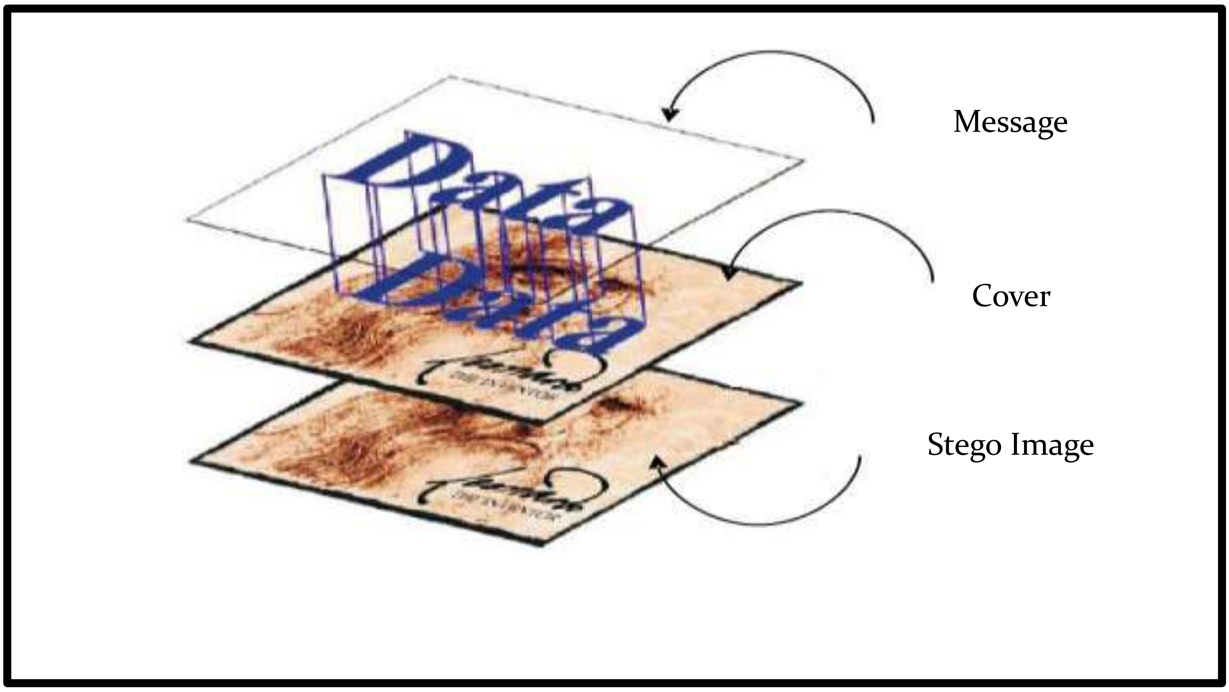


Figure (2.1): Example of hiding data [24].

The secret information which is represented as audio, image, etc. Can be hidden inside another piece of information called the cover media, and it is represented also by an image, audio, or video. After carefully inserting the raw information in the cover, it is referred to as Stego-medium. The Stego key is properly used to naturally restrict direct detection or successful extraction of the embedded data [25].

In the process of steganography, before the embedding process can be carried out correctly, the sender must arbitrarily select some basic tasks, choose the appropriate cover (i.e. picture, video, audio, text) of the confidential information, also select the secret message to be included and sent in addition to creating a word Strong passage (supposed to be known only to the recipient).

The general steganography algorithm can be explained in Figure (2.2). Where the secret data to be hidden is in different digital forms, which may be image text, audio, video, etc. The cover can be one of the digital file formats such as audio, video image, etc. The information hidden inside the cover is known as "secret information". But the information after hiding it is known as 'Stego-file' [26].

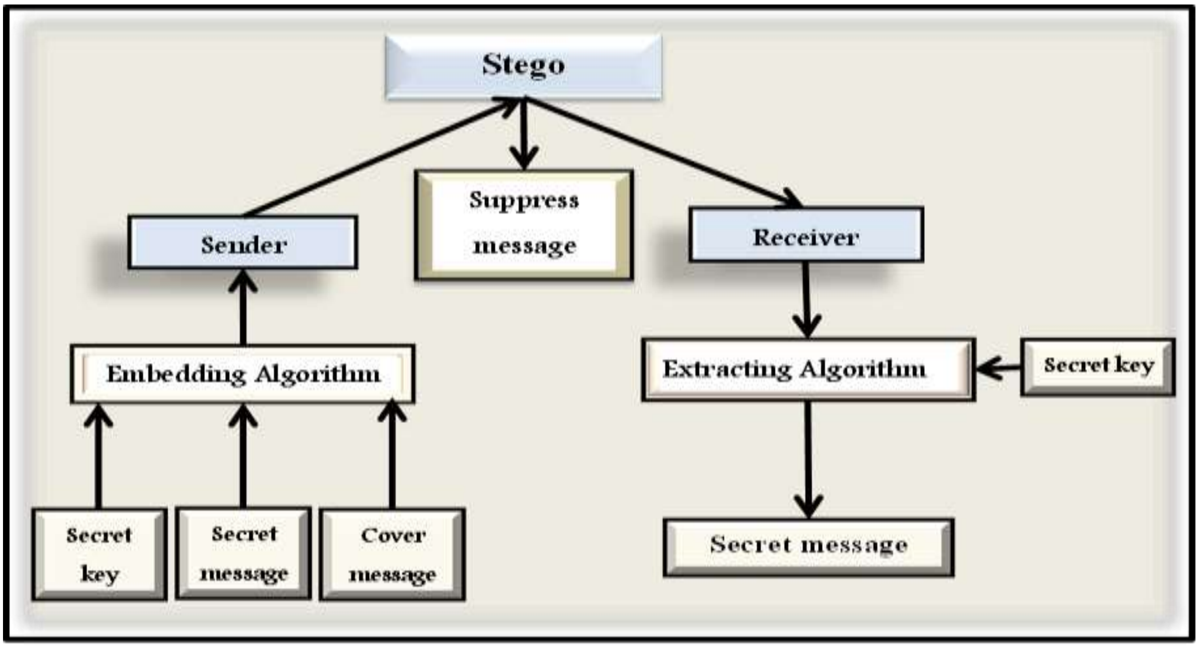


Figure (2.2): Steganography System Scenario [26].

Hiding information is an ancient art of apparently embedding a secret message. This art, unlike cryptography, does not use zeros or symbols for jostling a message and thus they are not clear. United State (US) officials and foreigners suspected that Osama bin Laden was using the flag of stealth to pass the embedded maps and pictures of terrorist targets through chat rooms and other sites [27].

2.3 Classification of Data Protection Systems

There are many ways to protect the secret data, but the most prominent methods currently used are *"Steganography" ,"Watermarking" and "Cryptography*" as shown in Figure (2.3)**.** And the difference between them is shown in Table (1.1) [28].

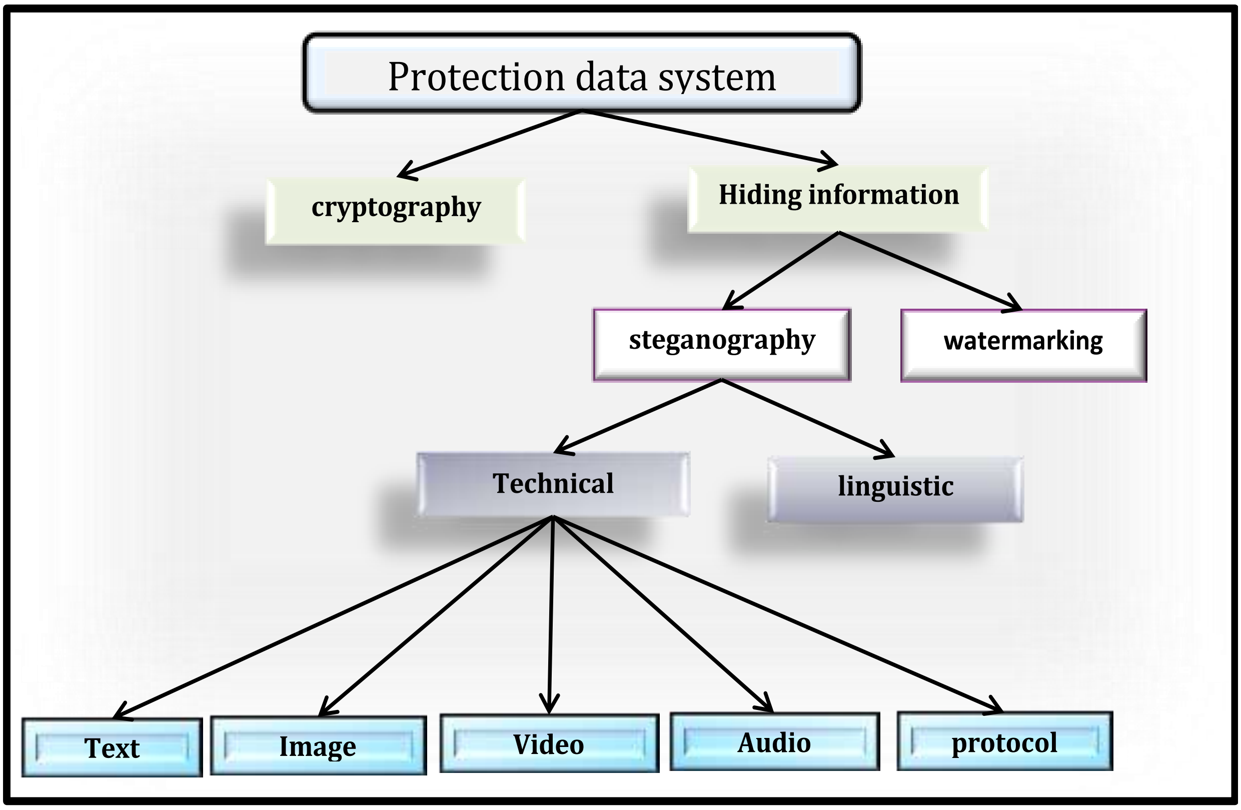


Figure (2.3): Types of protection in data systems [28].

Table (2.1): Comparison between "Steganography", "Watermarking", and "Cryptography" [29].

Criterion	Steganography	Watermarking	Cryptography
Carrier	All digital media	Often audio, image, video files	Ordinarily text files, or images
Secret information	Any digital file	Watermark	Ordinary text
Output-file	Stego-file	Watermarked-file	Cipher-file
Protection Key	Optional	Necessary	Necessary
Fails when	When it is discovered	It is raised/changed	Deciphered
Distinctness	Never	Depends on application	Always
Attack Types	Steganalysis	Image processing	Cryptanalysis

2.4 Data types of steganography

There are several types of date can be used in steganography technique, as shown in the Figure (2.4).

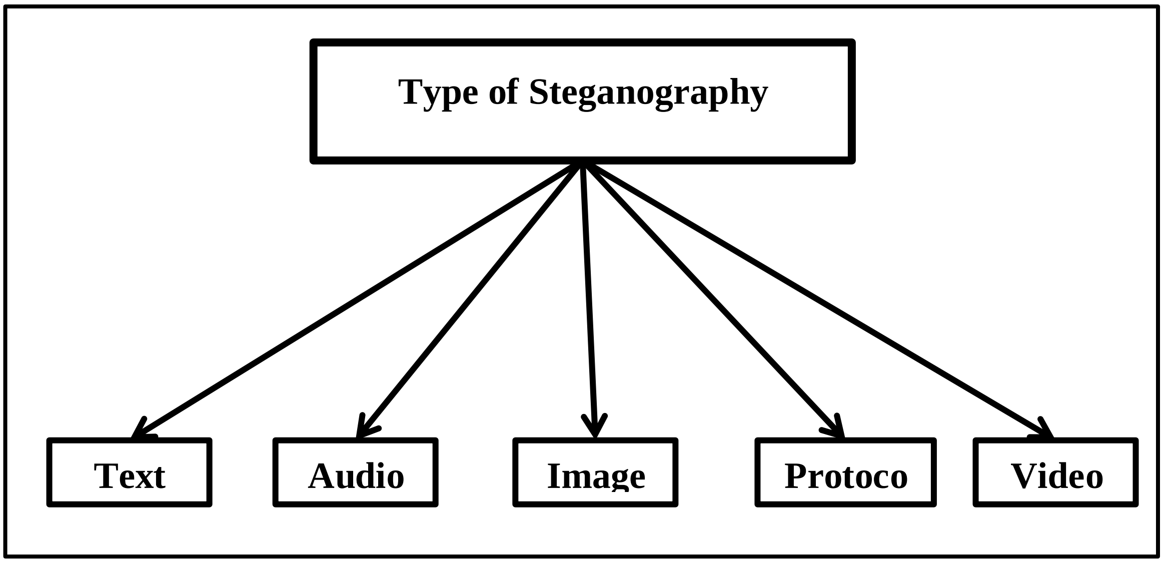


Figure (2.4): Data types of steganography [30].

A. Text steganography

It is a process of changing the format of a text file or changing characteristics of textual elements for hiding a secret data inside the cover text. In which, the change in the text cannot be discerned by readers [31].

B. Audio steganography

It is precisely a process of embedding classified information inside the digital audio file which results in a little modify in the binary sequence of the original audio file. While the listeners must be incapable to properly recognize the necessary change in the audio file. There in common are many efficient ways to hide data within an audio file, for example, Phase Coding, Least Significant Bits (LSB) , etc. [32].

C. Image steganography

It is a process of using an image to hide the bits of secret information, where these bits are embedded inside the cover image in a way not recognised by the human naked eye. There are many ways to hide data within an image file, for example (Least Significant Bits) [33].

D. Protocol steganography

It is a process of using network protocols such as TCP/IP as a carrier to embed specific bits of secret information [34].

E. Video Steganography

It is a process of using a Video for hiding bits of secret information. It is developing as a study area, by using a video file as a cover gives diverse advantages that are unavailable in another digital files format. At this place, the considerable change that typically happens in the original file can't be recognized by the human eyes, because the active frames are visible on-screen for tiny periods of considerable time. Moreover, the video containers are exceedingly greater than images and audio files [35].

2.5 Steganography Application

There are many applications for Steganography techniques, but the most famous one can be summarized as follows: [36]:

- *Copyright protection.*
- *Hiding Information.*
- *Secret Communication System.*
- *Protection of data alteration.*
- *Access control system for digital content distribution.*
- *Media Database systems.*
- *Medical uses.*
- *Remote sensing.*
- *Digital elections and electronic money.*
- *Radar systems.*

2.6 Existing Steganography Methods

Digital steganography techniques are often divided into two categories based on the embedding domain: (I) The spatial domain and (II) The transformation domain. There are many versions of spatial steganography, all directly change some bits in the image pixel values in hiding data. Least significant bit (LSB)-based steganography is one of the simplest techniques that hides a secret message in the LSBs of pixel values without introducing many perceptible distortions. Changes in the value of the LSB are imperceptible for human eyes. Transform Domain Technique: This is a more complex way of hiding information in an image. Various algorithms and transformations are used on the image to hide information in it.

Transform domain embedding can be termed as a domain of embedding techniques for which a number of algorithms have been suggested. The process of embedding data in the frequency domain of a signal is much stronger than embedding principles that operate in the time domain. Most of the strong steganographic systems today operate within the transform domain Transform domain techniques have an advantage over spatial domain techniques as they hide information in areas of the image that are less exposed to compression, cropping, and image processing. Some transform domain techniques do not seem dependent on the image format and they may outrun lossless and lossy format conversions.[37,38]

2.7 The Basics of Embedding.

In every steganographic system, there are three essential properties used to experiment the effectiveness of a steganographic system, namely *capacity, security and robustness.* As explained in Figure (2.5), while some researcher considered that there are four properties, namely imperceptibility. [39]:

Capacity: It defined as the quantity of the secret data bits that can be embedded in the bits of the cover-file. The efficient steganographic system aims to achieve maximum information hiding inside a minimum cover file in a way that maintaining the satisfactory quality of the Stego-file. It is also known as embedding capacity or hiding capacity and is measured in terms of bits per transform [40].

Security: In the system steganographic, the security word indirectly refers to detectability or noticeability. So, any steganography technique is considered as a security system if the secret information is noticeable or removable by statistical means or by an attacker after being detected. [41].

Robustness: It represents the ability of a Steganography algorithm to embed and extract the secret data from the cover file after corrupted inside noise channel by using computer processing or any other method [41].

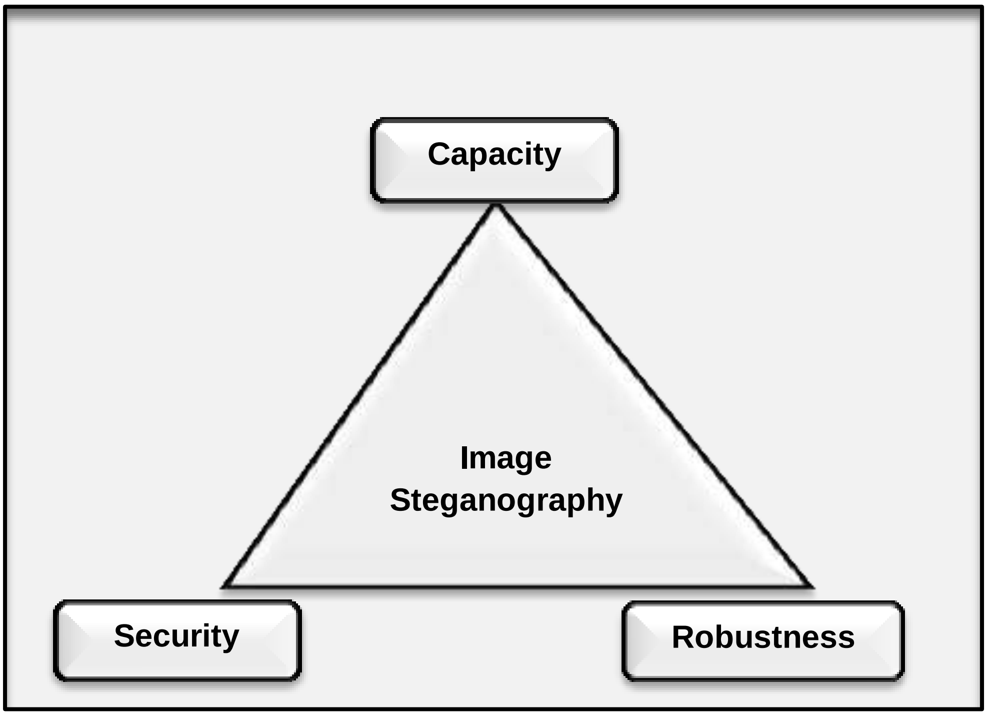


Figure (2.5): The main characteristics of the data hiding [39].

2.8 Speech Encryption

Audio has a lot of repetition compared to text or numeric data. This makes audio encoding with low clarity and high coding analysis strength a difficult task. There are several encryption techniques available to the designer of audio encoders, but the choice of one of these techniques depends on: [42].

1. Bandwidth requirements and usable communication channels.
2. A high level of security is necessary.
3. The needed level of security.
4. The residual intelligibility caused by the encryption system used.

2.9 Digital encryption.

In this type of encryption, the original analog signal is initialy converted to digital form and compressed using any applicable coding algorithm. The digital form is then encrypted using various encryption methods into various forms. The encrypted stream will then be broadcast over the voice channel. The ability of a computerized encryption scheme to compete with well-established basic scramblers is determined by the type of Speech pressure calculations were used are.[43].

There are many types of digital encryption that may be preferred for a variety of applications in today's digital systems. And these characteristics [43]:

a. Technology provides excellent audio discrimination.

b. The encryption equipment and the smartphone can be acoustically connected.

c. Discourse compression is not required by the system.

d. The system is less effect to errors.

2.10 Voice Scrambling

The most standard methods of speech scrambling are divided into three types represented by time domain scrambling, frequency domain scrambling, and the third type that combines the first and second types and is known as two-dimensional scrambling. Speech scrambling algorithms convert the signal of pure speech into an unintelligible signal1. As a result, decryption algorithm with the secret key is tough. [44,45]:

2.11 The Requirements of Voice Encryption.

a. Speech that has been encrypted is unintelligible.

b. The scrambled speech signal's bandwidth should be the same as the original speech signal's bandwidth. This means that the scrambling procedure should not affect bandwidth.

c. The jumbled speech should be difficult to decrypt in the absence of a decryption key. That is to say, the scrambled voice should be cryptographically tough to decipher, robust, and locked. The key space and key sensitivity are considered the two aspects of encryption security[46]:

I. The number of encryption keys, so that if K represents a key and a then a finite grope of potential keys, then (Ks = k1, k2,..., kr) which denotes as the key space, the number of keys is denoted by r.

II. Key sensitivity: The encryption becomes ideal if the voice is very sensitive to the secret key used. This means that any slight change in any of the secret key parameter values produces different results that are not available in the system output.

- Communication delays caused by the scrambling process must be kept as short as possible.
- Assuring the accuracy of the speech recovery procedure, as well as voice intelligibility and speaker characteristics

2.12 Image Definition

An image can be described in terms of vector graphics or bitmap graphics. An image stored in a bitmap is sometimes called a bitmap. An image map is a file containing information that hyperlinks different locations on a given image. The image consists of a group of numbers that form light of different intensity in different places in the image. Grayscale images consist of white, black, and grayscale in between. It is in the form of an array of pixels, each pixel in a gray image consists of 8 bits, and it cans display 256 colors or different shades of gray. A color image is usually made in three RGB color models, red, green and blue [47].

The RGB color model is a collection of red, green and blue light which added together in various ways to reproduce a wide range of colors as shown in Figure (2.6). In a color image, one pixel is 24 bits. The model's name comes from the initials of the three added primary colors, red, green, and blue. The main purpose of the RGB color model is sensing. It uses the RGB model to represent and display images in electronic systems, such as televisions and computers [48].

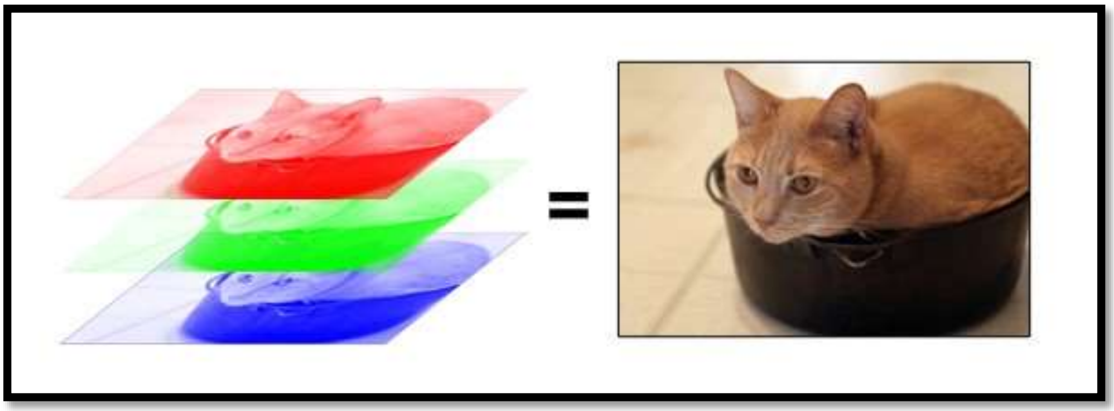


Figure (2.6): RGB image[48].

So, each pixel of the image is composed of 3 values (Red, Green, and Blue) which are values (the range is 0–255) as shown in Figure (2.7)

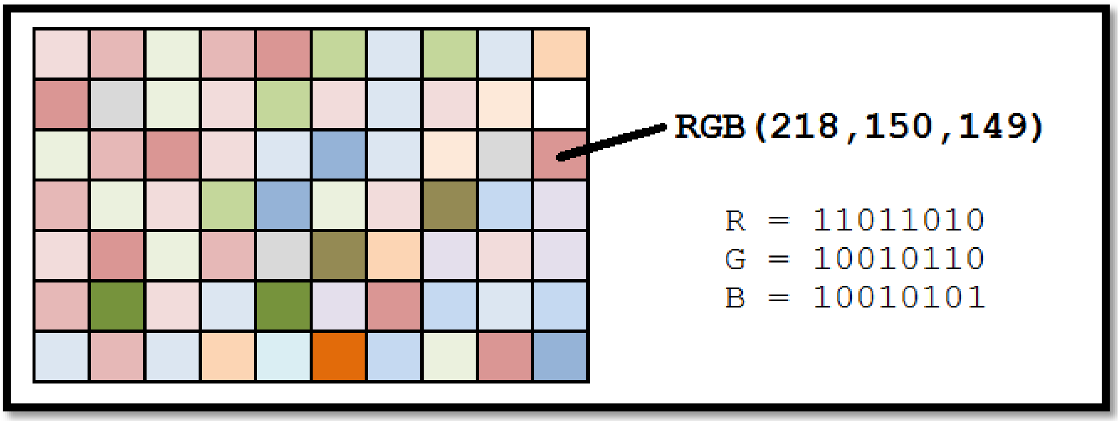


Figure (2.7): The composition of each pixel in the color image[48].

2.13 LSB Algorithm

LSB is the most straightforward method to hide a secret data inside the cover media(embed data in an image file) in a way that cannot be distinguishing the variation in the cover image by the abstract human eyes[49] .

In computing, The cover image can represent as a matrix of pixels so that each pixel can represent by 1byte consist of 8 bits which represent 256 gray colours between the black and white, while for the colour image there are 256 shades for each red, green and blue image. The LSB is the bit location in a binary integer giving the units value, that is, deciding whether the number is odd or even. Table(2.2) describe of the decimal no.149 in binary format with an LSB that highlighted by a square and its value is 1. the LSB decimal expression value in the 8-bit binary digit is “1” while the MSB Represents a value of “128”

Table (2.2): Binary representation of a pixel 149**.**

1	0	0	1	0	1	0	1

The LSB aims to replace the minimum weighting value of pixel bits by message bits. So when the colour image is using as a cover image, the bits of each of the red, green and blue (RGB) colour elements can be used. In other words, one can store 3 bits in each colour pixel(since each colour pixel is the result of combine three pixels (red, green and blue) and each one of these pixels represented by 8-bits The main principle of the LSB can be illustrated in the example below:

If you have the following matrix and you need to hide pixel have an intensity about (201) in it.

1	255	3
25	12	4
181	8	130

- Convert each integer value in a matrix to binary (as 8-bit):

00001011	11111111	00000011
00011001	00001100	00000100
10110101	00001000	10000010

- Convert the pixel have an intensity value (201) to binary: (201=11001001).
- Replace LSB of the matrix in pixel bit data:

0000101**1**	1111111**1**	0000001**0**
0001100**0**	0000110**1**	0000010**0**
1011010**0**	0000100**1**	1000001**0**

- Convert the matrix from binary to the decimal:

11	255	2
24	13	4
180	9	130

The example above shows that 6 bytes have been changed. This change is very simple and cannot be seen in the naked human eye, and this proves that LSB technology has a high efficiency in data embedding. Since it has the following specification[50]:

i. It is proved a high efficiency to hide bits.

ii. Demonstrated flexibility to work with cryptography algorithms such as TURBO or BCH code.

iii. Proven to be highly accurate in data extraction and extraction Bits similar.

2.14 Steganalysis

It is the breaking of steganography and is the science of detecting hidden information . The main objective of steganalysis is to break steganography and the detection of stego image. Almost all steganalysis algorithms depend on steganographic algorithms introducing statistical differences between cover and stego image. Steganalysis are of three different types [51]:

i. Visual attacks.

ii. Statistical attacks.

iii. Structural attacks.

Steganography and cryptography are cousins in the spy craft family. Cryptography scrambles a message by using certain cryptographic algorithms which converted secret data into unintelligible form. On the other hand, Steganography hides the message so that it cannot be seen [51].

2.15 Cryptography

Cryptography is the combination of two Greek words Crypto which means “Secret” and Graphy which means “writing”. So, cryptography is a way to change the message or (information) from one form to another secret form which is differ from the original with the help of a secret key and this process is called Encryption. However, the term cryptography can be used to refer the science and art of transforming messages to make them secure and immune to attacks. The changed value of secret message is called cipher, while getting the original message from cipher is called decryption as shown in Figure (2.8) [52]

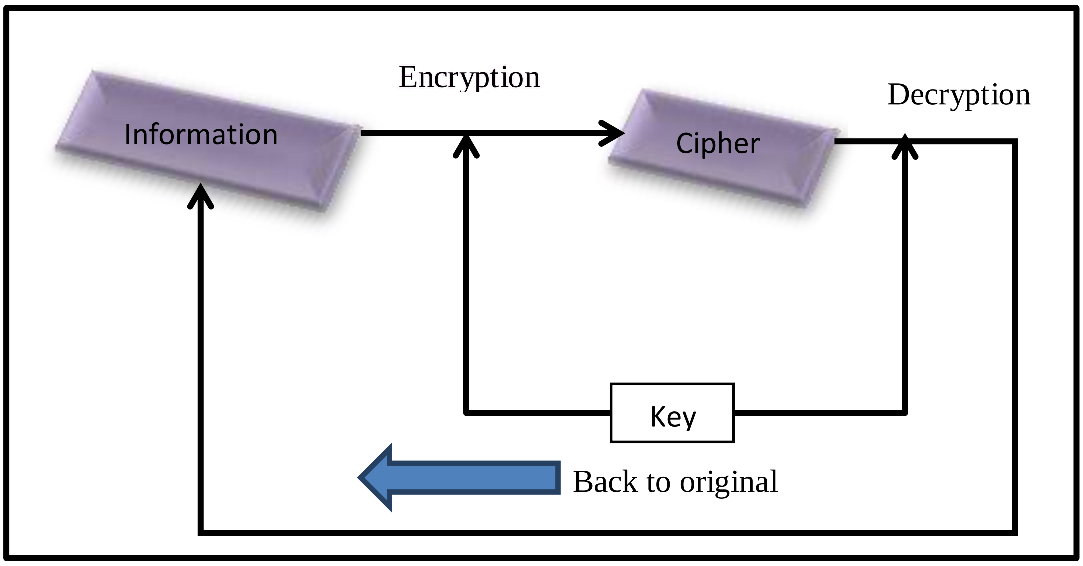


Figure (2.8): Encryption / Decryption process[52].

According to key, cryptographic algorithms can be divided into two types:

A. **Secret Key Cryptography**: The key used for encryption and decryption process is the same. It is also termed as symmetric key cryptography such as AES (Advanced Encryption Standard) and DES (Data Encryption Standard) [53].

B. **Public Key Cryptography**: Two different keys are used, one for encryption and another for decryption. It is also known as asymmetric key cryptography such as RSA (Rivest-Shamir-Adleman) [54].

2.16 Cipher

The intermediate results after encrypting plaintext is called cipher text. It is totally differs from plaintext. It may be in readable form or not. According to the cipher cryptographic algorithms the cipher can be divided into two parts[55]:

- **Stream Cipher-** In stream cipher, encryption and decryption are done typically on one symbol (such as a character or a bit) at a time. In a stream cipher, each binary digit is processed individually one bit at a time with the help of key such as XOR encryption algorithm. It takes less time and space than block cipher, but it is not easy to implement correctly, the stream cipher block diagram can be shown in Figure (2.9) [56].

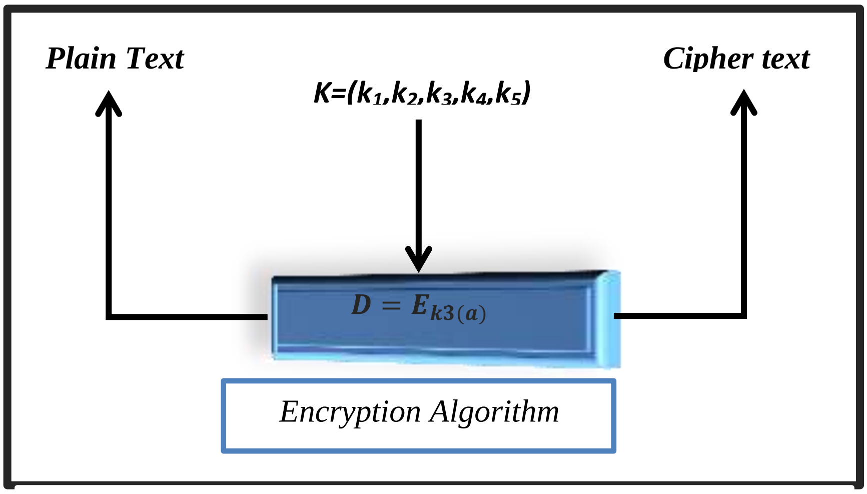


Figure (2.9): Stream Cipher[56].

- **Block Cipher** With the exception of stream cyphers including Blowfish and DES, a piece or block of information is handled at a moment in a block cypher. It needs more effort and storage than stream cypher, but because they are not working on particular elements, block cypher is easier to build. A block cypher encrypts a collection of plaintext characters of length m (m>1) to generate a collection of cypher text of the same length. A block cypher, per the concept, utilizes a single key to encode the whole block, even if the key has numerous possibilities. Figure (2.10) shows the concept of a block cipher [57].

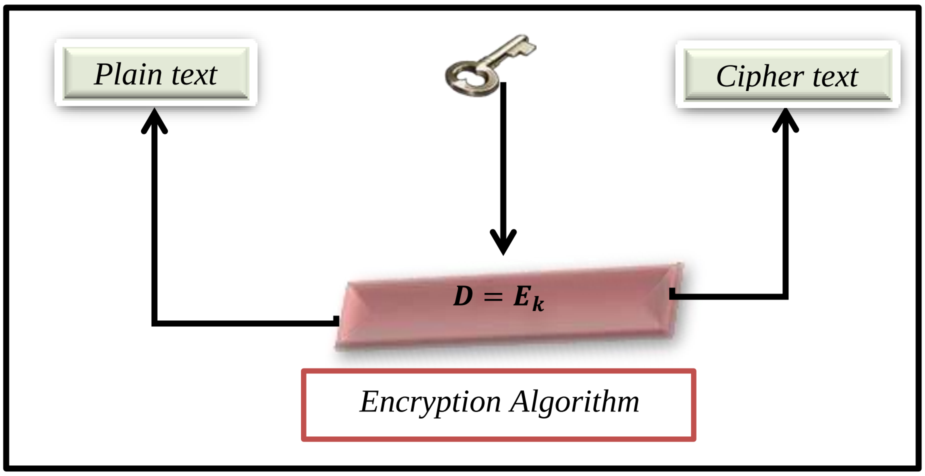


Figure (2.10): Block Cipher[57].

2.17 Types of Cipher

In the past, a simple pen and paper can be used in cipher method which was also known as classical cipher. Also, there are important types of cipher which can be depicted as follows:

A. **Substitution Cipher**: A substitution cipher replaces one symbol with another. If the symbols in the plaintext are alphabetic characters, then replace one character with another. For example, replace letter B with letter E, and letter S with Y. Each unit or group of units is replaced by some other predefined symbol or character such as Caesar cipher and one time pad cipher [57].

B. **Transposition Cipher:** Transposition Cipher does not substitute one symbol for another, instead of that, it changes the location of the symbols. A symbol in the second position of the plaintext may appear in the eighth position of cipher text. A symbol in the seventh position of the plaintext may appear at the first 2 position of cipher text. It is simply a permutation of plaintext, such as Rail fence cipher [57].

C. **Polyalphabetic Substitution Cipher**: In this, each occurrence of a character may have a different substitute. The relationship between characters in a plaintext to a character in the cipher text is a one-to-many, for example "a" could be enciphered as "E" in the beginning of the text, but as "M" in the middle. Substitution methods are used such Vigenere method and Enigma machine [58].

2.18 Cryptanalysis

It is the technique of finding the true meaning of encrypted plaintext. It tries to detect the way of working of the system by using encryption algorithms and a secret key. It can simply be called an attack on cryptography. It can also be termed as code breaking or cracking of the code. It can be of following types [58,59]:

i. ***Cipher text only*:** In this type of attack, the attacker has access to only some cipher text. He tries to find the corresponding key and the plain text.

ii. ***Plain text:*** In this type of attack, the attacker has access to only some plain text/cipher text pairs in addition to the intercepted cipher text that he wants to break

iii. ***Chosen plain text***: : Chosen plain text is similar to the known-plain text attack, but the plain text/cipher text pairs have been chosen by the attacker himself.

iv. ***Chosen cipher text***: Chosen cipher text is similar to the chosen plain text attack, except those attackers chooses some cipher text and decrypts it to form a cipher text/ plain text pair

2.19 Chaos Theory

Chaos is derived from a Greek word ‘Χαos’, meaning a state without order or predictability. A chaotic system is a simple, non-linear, dynamical, and deterministic system that shows a completely unpredictable behaviour and appears random [60, 61]. Moreover, it is a deterministic system with great sensitivity to initial conditions, such that a computer system can give an amazingly different result when the value of an input parameter is changed. On the other hand, in classical science small changes in an initial value might generate small differences in the result [62]. That chaos sensitivity depends on initial conditions and gives unpredictable results [61]

Later on, Edward Lorenz (1963) examined chaos theory and described a simple mathematical model of weather prediction. Lorenz’s model was the first numerical model to detect chaos in a non-linear dynamical system [63]. Lorenz’s finds an interesting behaviour in that some equations which rise to some surprisingly complex behaviour and also find chaos behaviour depend on the initial condition [60, 64]. In 1975, Li and Yorke were the first to introduce the word ‘chaos’ into mathematical literature, where system results appear random [61]. Chaotic maps have been the subject of an extremely active research area due to their characteristics, such as sensitivity to the initial value, complex behaviour, and completely deterministic nature. The chaotic behaviour can be observed in many different systems, such as electronic systems, fluid dynamics, lasers, weather, climate and economics [65, 66].

2.20 Definition of Chaos

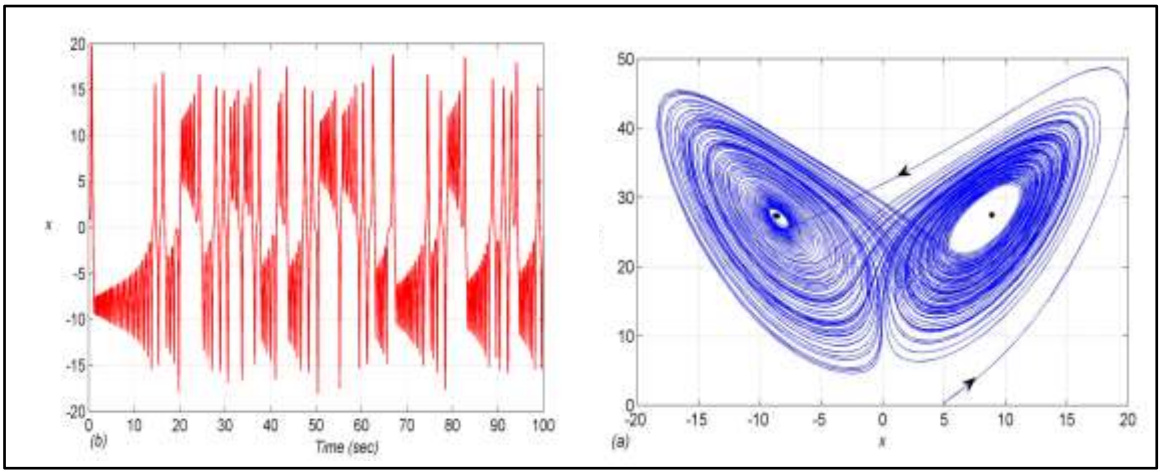
Chaotic Systems are basically nonlinear and exhibit an apparently random behavior for certain range of values of system parameters. However, the solutions or trajectories of the system remain bounded within the phase space. This unstable state is strongly dependent on the values of the parameters and on the initial conditions. This definition has three properties of chaos mentioned in it can be explained as follows [64].

- ***Aperiodic long-term behavior:*** Refers to the system tracks do not stabilize on any stable points, quasiperiodic orbits or periodic orbits. Thus, the track that follows will have limited predictability.
- ***A deterministic system:*** means that the system does not have any stochastic input parameters or it is not random. The irregular behavior of chaotic systems is due to the system's essential nonlinearity rather than the noise.
- ***Sensitivity to initial conditions:*** Refers to the tracks even if they start from very close primary conditions will separate exponentially fast (butterfly effect). This means long-term predictability becomes impossible.

2.21 Types of Chaotic System

Chaotic systems can be divided into those described by differential equations, known as flows, and those described by differential equations, known as maps. Trajectory and orbit describe the evolution of these dynamical systems. The trajectory of a flow is the path the flow takes as time progresses. An orbit is a set of points that a map moves through under iteration. The dynamics of a chaotic system can be represented in the time domain as time series as shown in Figure(2.11a) or in phase space as a strange attractor that seen in Figure (2.11b) [67].

The time series graph is obtained by simply plotting the amplitude of the signal against time. On the other hand, the strange attractor is obtained by plotting two or more of the state variables of the system against each other. The state variables of the system are most often defined as the first or the second derivative of the time series, or a combination of those [67].



(*a*) (*b*)

Figure (2.11): (*a*): Chaotic time series. (*b*): Strange attractor[67].

2.20.1 Chaotic Flow (Autonomous Chaotic System)

These chaotic conjunctions are derived from a set of differential equations, and such systems are continuous time. Most autonomous non-linear dynamic described by differential equations. [66, 67].

The systems are described by a differential equation so; chaotic flow can be represented as follows:

$$\dot{x} = z(x,t). \qquad an\dot{d} \qquad x(t_o) = x_o\cdot. \qquad (2.1)$$

Where: $\dot{\boldsymbol{x}}$: is the state vector of the system at a time (t), ***z:*** refers to a set of differential equations that govern the system, and x_o*:* is the initial condition of the system.

The peculiar attractant of chaotic flow systems is referred to as the pathway which is characterized by a smooth and continuous nature. There are several well- chaotic flow systems such as [68].

I. *Lorenz system.*

II. *Rossler system.*

III. *Chua system.*

IV. *Nien system.*

I. Lorenz System

One of the most known nonlinear continuous chaotic systems is a Lorenz chaotic system which was proposed by the atmospheric scientist E. Lorenz in 1963. The Lorenz system was proposed to describe the fluid circulation in a shallow layer of fluid when high temperature (heating process) is applied equally below and a low temperature (cooling process) is applied equally above. The fluid motion is assumed to be circular in two dimensions which are horizontal and vertical with boundary conditions: [69].

The system is described by a set of three ordinary first order differential equations which are:

$$\frac{dx}{dt} = \sigma(y - x), \qquad (2.2)$$

$$\frac{dy}{dt} = x(\rho - z) - y, \qquad (2.3)$$

$$\frac{dz}{dt} = xy - \beta z. \qquad (2.4)$$

The equation (2.2-2.4) shows the rate of change with respect to time [69].

Where:

The Lorenz system behavior is depending basically on the initial conditions, the initial conditions values set to (*x*=0, *y*=5, *z*=25).

(β, σ, ρ): represent the parameters and are usually imposed positive values. Lorenz used the parameter values, $\beta = \frac{8}{3}, \ \sigma = 10, \ \rho = 28.$ [69,70].

From Figure (2.12), it can be noticed that the system trajectory has the butterfly effect. The butterfly effect, which E. Lorenz named, is a concept which means that large effects come from small causes. This effect describes a phenomenon in Lorenz system which states any tiny difference in the initial conditions causes a large difference in later states in general and in weather, especially you can see the time series waveform of the Lorenz system in

Figure(2.9). Also, from the trajectory of the Lorenz system, important points must be noted.

- ***A.*** No crossing occurs instead it crosses itself repeatedly. So, in 3D surface viewing, there is no cross or merge between orbits.
- ***B.*** It is impossible to predict the next cycle.
- ***C.*** The Lorenz system concluded the term fractal which can be defined as a set of points of the infinite surface area, but with no volume [70].

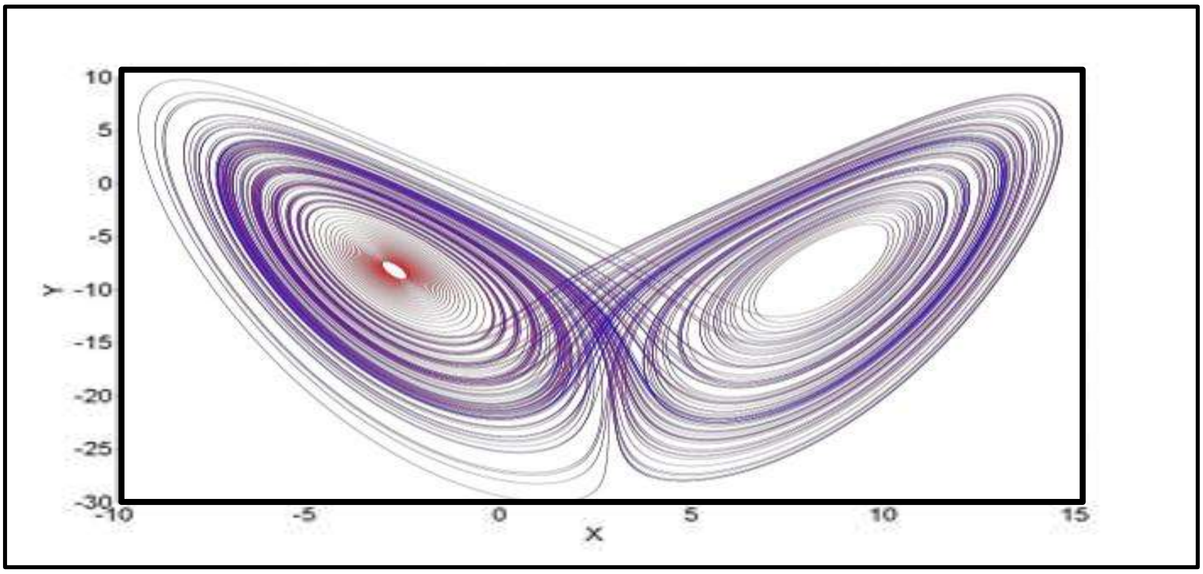
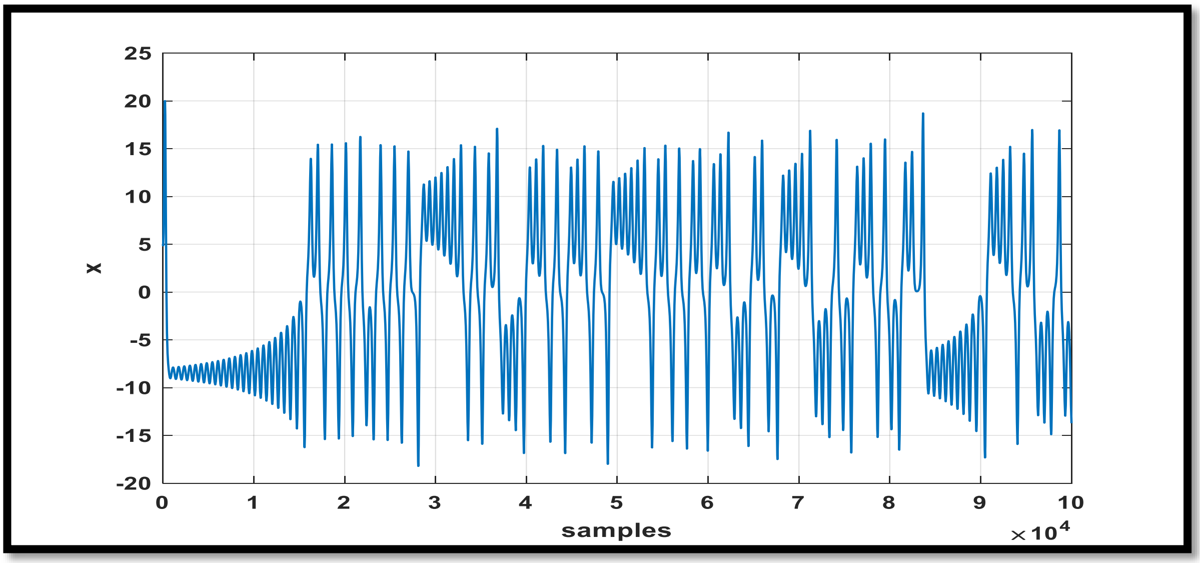
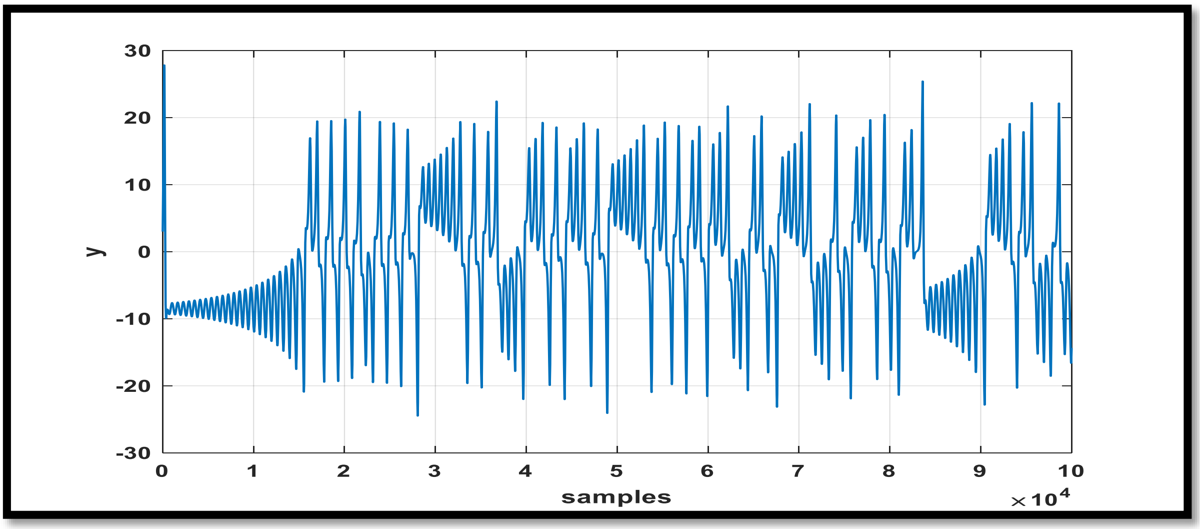


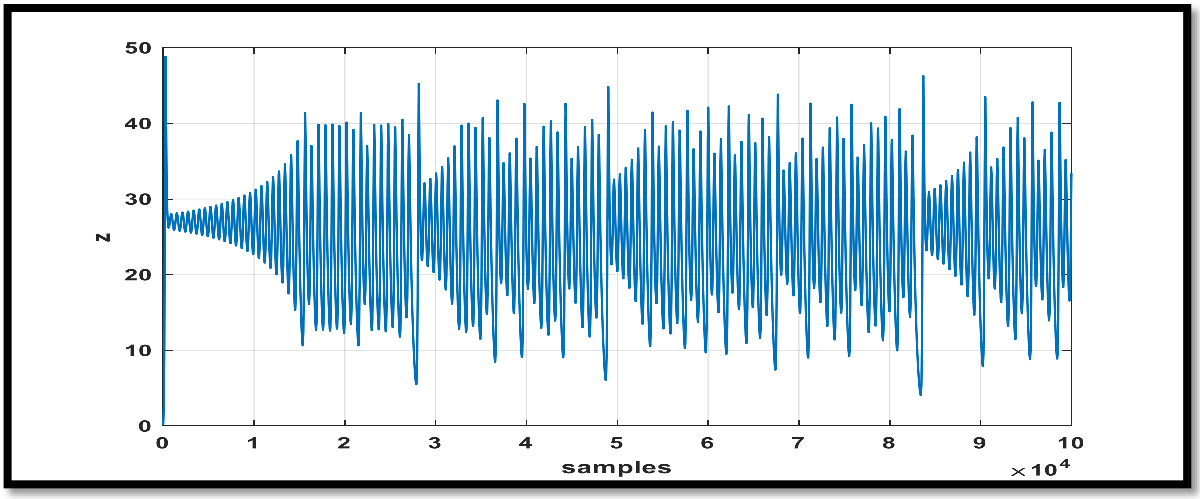
Figure (2.12): Lorenz system trajectory [7].



(*a*)



(b)



(c)

Figure (2.13): Time series waveforms of Lorenz system: $(a)x(t), (b)y(t),$ and (c) $z(t)$[70].

The Lorenz system has some important features which could be observed from its differential equations such as:

a) The nonlinearity of the system because of the multiplication terms *(xy, xz)*

b) The growth of the system depends only on the system variables at the time because the equations of the system are major instruction differential equations [71].

II. Rössler System

In 1976, Otto Rössler proposed a new nonlinear continuous-time chaotic system. This system differs from the Lorenz system by the number of second order nonlinear terms, where Lorenz has two nonlinear terms which are mn and ml. The differential equations of the system are [72, 73]:

$$\dot{x} = -(y - z).$$
$$\dot{y} = x + ay. \tag{2.5}$$
$$\dot{z} = b + z(x - c).$$

Where: (a, b, & c): represent the system parameters and (x, y, z) are the initial value. The system attractor acts as chaotic when *a = b = 0.2, and c = 5.7*, as shown in Figure (2.14).

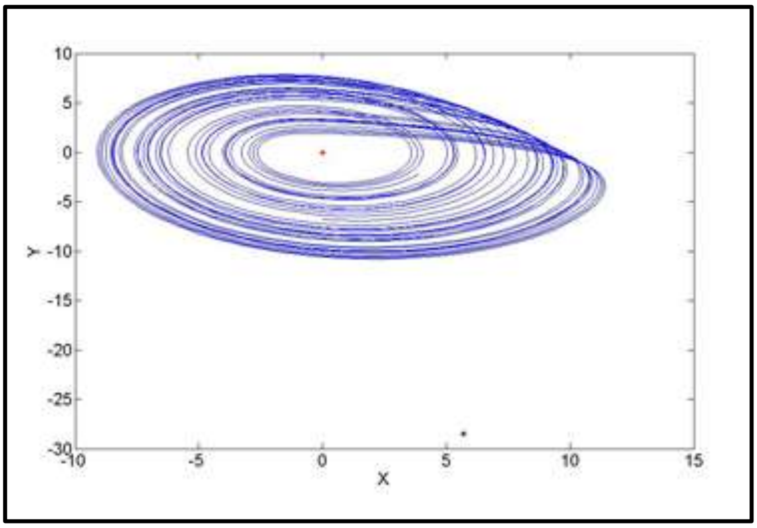


Figure (2.14): Rössler attracter trajectories [73].

The system trajectory has a disk embedded structure, as shown in Figure (2.14), whereas the Lorenz system has a butterfly shape. Rössler shared several chaotic properties with other chaotic systems, including sensitivity to initial conditions, randomness, unpredictability, and aperiodicity

III. Chua System

In 1983, Leon Chua designed an electronic circuit which displays a chaotic behavior with an oscillation that never repeats itself (aperiodic). The circuit shows a simplicity construction and it is a declaration of a real-chaotic system model. Chua system can be expressed by using the following differential equations [74]:

$$\begin{aligned} \dot{x} &= a(y - x - f(x)). \\ \dot{y} &= x - y + z. \qquad (2.6) \\ \dot{z} &= -(bz + cy). \end{aligned}$$

$$f(x) = m_1 + 0.5(m_0 - m_1)(|x + 1| - |x - 1|). \qquad (2.7)$$

Where: *f(x):* represents the electrical response of the nonlinear resistor. a, b and c can be found form the values of the circuit components. The values of the parameters are usually taken as follows: *a = 0, b = 4.78, c = 0.0385,* m_0*= -1.27;* m_1 *= -0.68*. Figure (2.15) shows the Chua system attracter [74].

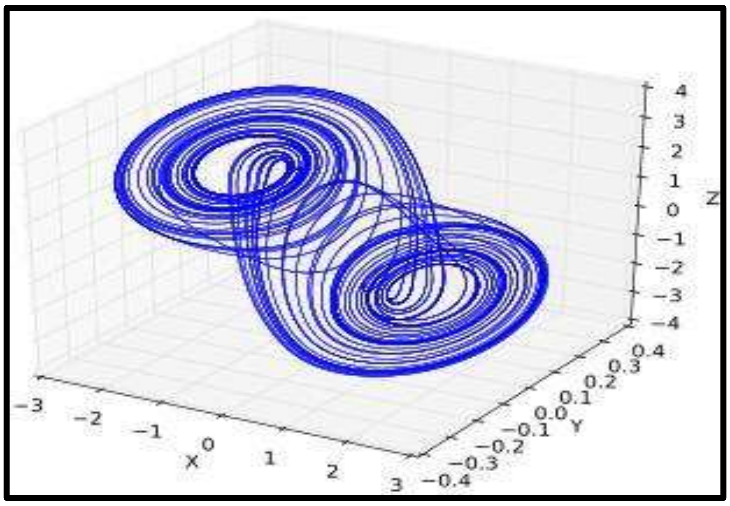


Figure (2.15): Chua system attractors [74].

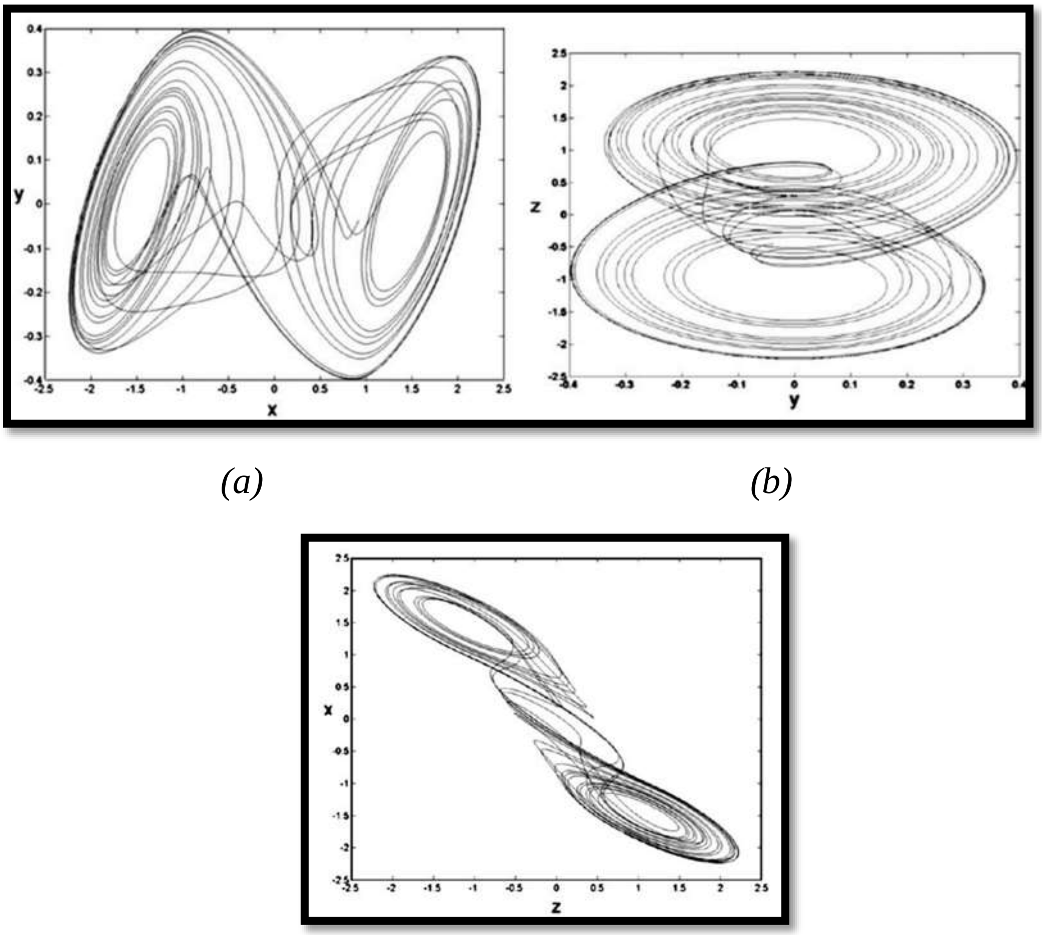
IV. Nien System

In 2007, H.H. Nein proposed a nonlinear random chaotic system which has the same characteristics of any chaotic system. Nien rewrote the equations of the circuit which were proposed by Chua and become [75].

$$\begin{aligned} \dot{x} &= -a(y + x + f(x)). \\ \dot{y} &= -b(x + y). \qquad (2.8) \\ \dot{z} &= y. \end{aligned}$$

$$f(x) = bx + 0.5(x - b)\ (|x - I_0| - |x + I_0|). \qquad (2.9)$$

Where: *(a, b and c)*: are the system's parameters, *f(x)* is the nonlinear function of the system. Figure (2.16) state the 2D trajectories of Nein system .



(a) *(b)*

(c)

Figure (2.16): 2-D trajectories of Nein system: (*a*) *xy trajectory*. (*b*) *yz* trajectory, & (*c*) *xz* trajectory [75]

2.20.2 Chaotic Maps

Chaotic maps are mathematical equations used to generate random sequences that are highly sensitive to their initial conditions and control parameters. Chaotic maps are classified into two categories: one-dimensional (1D) and multi-dimensional (MD) chaotic maps. There are many well-known chaotic maps such as:

A. Logistic map

In 1845, Pierre Verhulst proposed a logistic map, which is a simple nonlinear dynamical map. A logistic map is one of the most popular and simplest chaotic maps [76]. Logistic map became very popular after it was exploited in 1979

by the biologist Robert M. May [77]. The logistic map is a polynomial mapping, in complex chaotic system, the behavior of which can arise from very simple nonlinear dynamical equations. The logistic map equation is written as seen in equation (2.10).

$$X_n + 1 = r.X_n.(1 - X_n). \qquad (2.10)$$

Where: X_n : is a number between [0,1], X_0: represents the initial population, and r : is a positive number between *(0,4)* [78].

The logistic map behavior depends on the bifurcation parameter r, so, when r is equal to:

1- [0 to 1] the system has a stable fixed point near to 0.

2- [1 to 3] the system has a stable fixed point near to (*(r-1)/r*).

3- [3 to 3.57] it will be aperiodic attractor of *2m* where *m =1,2, ….*

4- [3.57 to 4] the system acts as chaotic system.

B. Henon Map

The Henon map is a two-dimensional chaotic map that may be expressed using difference equations:

$$x_{n+1} = 1 - r * (x_n)^2 + y_n. \qquad (2.11)$$

$$y_{n+1} = b * x_n. \qquad (2.12)$$

Where: r and b are system parameters that the system depends on them. Usually, *r=1.4* and *b=0.3* which makes the Henon map act as a chaotic map with range [*1.07 to 1.4*]. For other values, the Henon map will converge to a constant value, and acts as a periodic system or losses randomness (regular system). It is very important to select the values of initial conditions and the value of the parameter r which makes the system have a strange attractor or infinite divergence. Figure (2.17) shows the bifurcation diagram of the system, depending on the value of parameter r. [80]

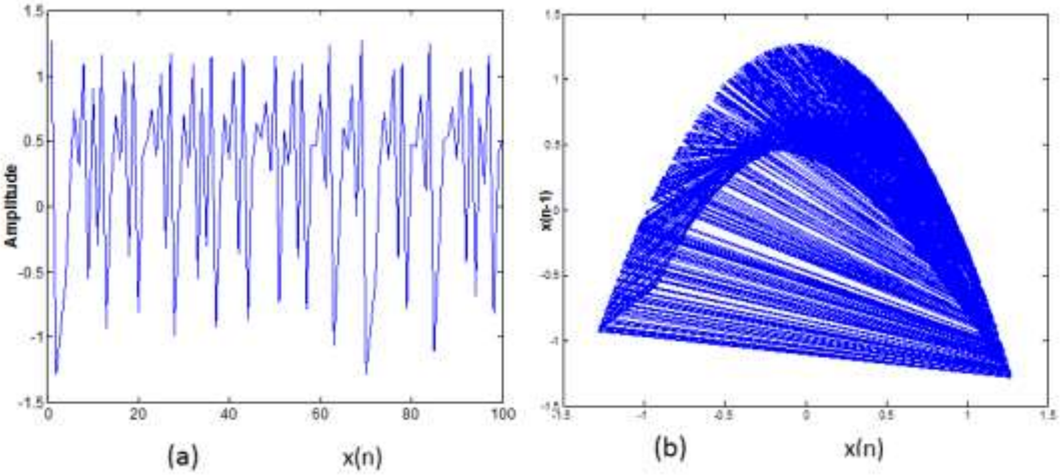


Figure (2.17): The Hénon map (a) Time Series x(n), (b) Strange Attractor.[80]

Also, Henon map's difference equations could be converted into one-dimension difference equation in the form of:

$$x_{n+2} = 1 - r * (x_{n+1})^2 + b * x_n. \qquad (2.13)$$

Here: r *and* b are the system parameters.

So, Henon map could be used for image scrambling when using the two dimensions difference equation forms, and changing the pixel's value when using the 1-D difference equation form [80].

C. Duffing Map

It represents a dynamic logistic system, and shows a chaotic, decreasing behavior with time. Also known as (Holmes map). When pixel coordinates (X,Y) are used as inputs to the Duffing equation, new coordinates (x_{n+1}, y_{n+1}) will be generated depending on the equation*(2.14)*.

$$\begin{aligned} x_{n+1} &= Y_n \\ y_{n+1} &= -\delta X_n + \gamma Y_n + Y^3{}_n \end{aligned} \qquad (2.14)$$

The duffing map depends on two parameters δ and γ, there are usually used δ = 2.75 and γ = 0.2 to produce chaotic behavior. Trajectory and orbit are two terms used to designate the development of these non-static systems. Trajectory regards to the track taken by the flow through time, and a number of points which a map moved over the iteration. The time domain will represented by a strange attractor in the phase space. While the strange attractor represents from the time series of the chaotic system, Figure (2.18a) illustrate the time series of the chaotic system and the changing aspects (dynamics) strange attractor, as shown in Figure. (2.18b) [81].

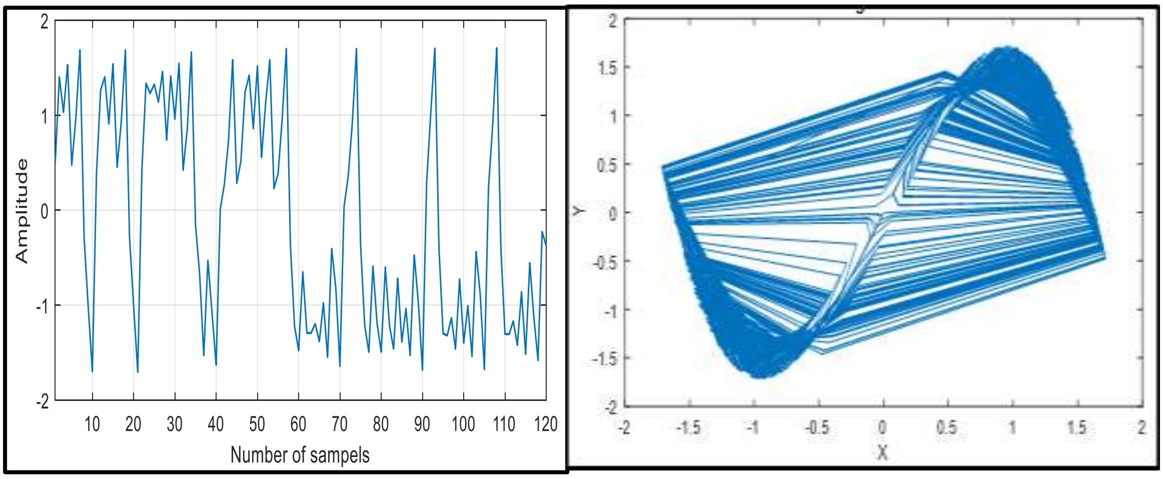


Fig (2.18) :*(a)*Time series for chaotic Duffing map, *(b)* Strange attracter for Duffing map[81].

D. Arnold's Cat Map

Arnold’s cat map (ACM) or Arnold transform (AT), proposed by Vladimir Arnold in 1960, is a chaotic map which when applied to a digital image randomizes the original organization of its pixels and the image becomes imperceptible or noisy. However, it has a period p and if iterated p number of times, the original image reappears. The mathematical formula is shown in equation. (2.15)[82,83]:

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \begin{pmatrix} x \\ y \end{pmatrix} (modN) \qquad (2.15)$$

Where, x, y ∊ {0, 1, 2 … N −1} and N is the size of a digital image . A new image is produced when all the points in an image are manipulated once by equation (2.15). But this system does not have any parameter except the value of the pixel and the size of the image N [84, 85].

It can be easily seen that the origina of Arnold transformations given by equation (2.15) can be modified to produce a sequence of Arnold transformations ,and One way to generalize the above 2-D Arnold cat map can be achieved by introducing new parameters(a_1,b_1,c_1) to increase and ensure high security implementation as in equation (2.16) [86]:

$$\binom{x'}{y'} = \begin{bmatrix} 1 & B_1 + {C_1}^2 \\ A_1 & 1 + A_1 B + AC^2 \end{bmatrix} \binom{x}{y} \pmod N \qquad (2.16)$$

where A,B and C are positive integer value assumed to be as a control parameters and (A, B, C) ∈ R, N is the size of the data after converting it to two dimensions, (x, y) is the original data location, and (x', y') are the values of the shuffled data after applying Modified Arnold cat Map. Parameters are used as a control to increase security. As shown below in Figure (2.18). Any change in one of the variables slightly, the results of x will change.

2.21 Performance Evaluation of image.

The primary purpose of steganography systems is to hide confidential data inside a cover file (photo, video or other cover type) in a way that the human visual system can't recognize. So to determine whether or not the effect of data masking on image quality is in the acceptable range, there are several statistical tests that have been used to make the decision. In this chapter you will discuss several parameters such as Mean Square Error (MSE), Structural Similarity Index (SSIM), Peak Signal to Noise Ratio (PSNR), Cpestral Distance Measure (CD) and others.

2.21.1 MSE (Mean Square Error).

MSE is one of the statistical methods which use to determine the correspondence between the stego image and original image. The computation of the similarity is by measuring of error signal getting from subtracting the checked signal from the referred one, then calculate the mean energy to the error signal. The calculation of (MSE) can be written as in equation.(2.17) [89].

$$MSE = \frac{1}{x*y} \sum_{i=1}^{x} \sum_{j=1}^{y} (Pic1(i,j)_i - Pic2(\mathrm{i},\mathrm{j})_i)^2 \qquad (2.17)$$

In the formula (2.18) $Pic1$ is the original image, $Pic2$ is stego image, $\boldsymbol{m}$ as well as $\boldsymbol{n}$ are image dimension.

2.21.2 PSNR (Peak Signal to Noise Ratio).

It is defined as the ratio between the maximum power of a signal and the power of corrupting noise. PSNR is usually expressed as a decibel scale. The PSNR is commonly used as a measure of a quality reconstruction of an image. The signal, in this case, is original data, and the noise is the error introduced. The high value of PSNR indicates the high quality of the image; it can be calculated by equation. (2.19) [88].

$$PSNR(dB) = 10\log_{10}\left[\frac{p^2}{MSE}\right]. \qquad (2.19)$$

Here, *P* is the maximum possible pixel value of the image. When the pixels are represented using 8 bits per sample, this is 255.

2.21.3 SSIM (Structural Similarity Index).

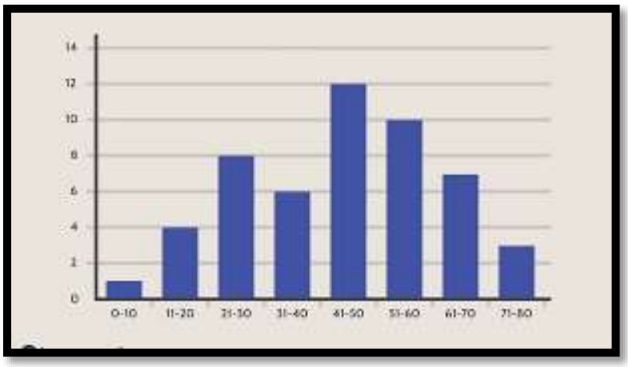
SSIM in image processing is subject to a variety of distortions, which may result in deterioration in image accuracy and to estimate the change of media resolution before and after a steganography operation. The image that was changed after Steganography must be compared to the image before the change. The equation of SSIM can be seen in equation (2.20) [88,89].

$$SSIM(\%) = \frac{(2\mu_x\,\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu^2{}_{x+}\mu^2{}_y + c_1)(\sigma^2{}_x + \sigma^2{}_y + c_2)} \times 100\%. \qquad (2.20)$$

Where μ_x, μ_y represent the local means, σ_x, σ_y represent the standard deviations while σ_{xy} represent the cross-covariance.

2.21.4 Histogram

It is a graphical demonstration which shows a visual impression of the circulation of pixels through scheming the number of pixels at each grayscale level. The histogram of the cover image and the stego image was found to show that the statistical properties of the cover image were not affected by changing some coefficients . So if the histogram of the cover is nearly equal to the histogram of the stego-image, then this means that the proposed system was good enough to avoid the attackers. The histogram is shown in Figure (2.19) [90].



Figure(2.19): Histogram definition[90].

2.21.5 Linear Predicative Code Measure (LPCM):

The difference between the original sound and the encoded or retrieved voice is known as the Linear Predicative Code (LPCM) distance. The equation (2.21) illustrates that [91]:-

$$d_{lpc} = \ln\left(\frac{AVA^T}{BVB^T}\right) \qquad (2.21)$$

where A=(1,a$_1$,a$_2$,…………,a$_p$) is the section of the original speech signal's calculated LPC data vector. While, B=(1,b$_1$,b$_2$,…………,b$_p$) is the vector of the restrained LPC parameter of the frame corresponding to the encoded or retrieved language sign

V = [v(i , j)] i,j = 1,2 ,3,…..p

In which [v (I, j)] are the pretty standard similarity coefficient vectors obtained from A, as well as p is the quality of the linear oratorical strainer. The greater the d$_{lpc}$ importance in encapsulated tone, the greater the spatial frequency deformation in the previous series of words.

2.21.6 Cpestral Distance Measure (CD)

It is described by equation (2.22) [92]:-

$$C = 10log_{10}\left[2\sum_{n=1}^{p}\left\{C_x(n) - C_y(n)\right\}^2\right]^{\frac{1}{2}} \qquad (2.22)$$

Where $C_x(n)$ are the cpestral coefficients of the *nth* frame's original speech, $C_y(n)$ are the corresponding recovered or encrypted speech frame's cpestral coefficients, and p is the total number of frames. The polished LPC spectrum is used to obtain the cpestral parameters for any frame. The cpestral coefficients are then calculated using recursion from the LPC coefficients:

$$C_x(n) = a(n) + \sum_{k=1}^{n-1}\left(\frac{k}{n}\right)C_x(k)a(n-k) \quad n \geq 1 \qquad (2.23)$$

In which a(n) is *nth* is the number of LPC operations, it is established that C_x *(1) = a(1)* the aforementioned based on wavelet transform separation In which Xi (k) is the DFT of the individual text patterns' frames as well as Yi (k) is the DFT of the encryption or restored speech specimens' frames. Because auditory systems are frequently hypersensitive to timing inaccuracies, the measurement in equation. (2.23) is represented in terms of the volume of time-frequency observations..

2.21.7 Segmental Spectral Signal to Noise Ratio (SSSNR)

In the frequency domain, it is determined as in equation (2.24) [93]:

$$(SSSNR_i)_{dB} = 10log \frac{\sum_{k=1}^{N} |X_i(k)|}{\sum_{k=1}^{N} [|X_i(k)| - |Y_i(k)|]} \qquad (2.24)$$

In which Xi (k) is the DFT of the individual text patterns' frames as well as Yi (k) is the DFT of the encryption or restored speech specimens' frames. Because auditory systems are frequently hypersensitive to timing inaccuracies, the measurement in equation (2.25) is represented in terms of the volume of time-frequency observations.

Chapter Three

Research Methodology

CHAPTER THREE
RESEARCH METHODOLOGY

3.1 Introduction

In the previous chapter, many techniques were discussed, so that the general idea of each method was explained in terms of their work and its mathematical representation. In this chapter, all of these technologies used to design multi-Level security scheme. This chapter is presented in three main sections. After the introduction, in the first main section. The second main section refers to the first algorithm, which proposed. This section consists of three general parts. Introduction of algorithm, in the first part .The general block diagram of the first algorithm explained in the second part. This diagram which contain the transmission end, namely the clarification of the encryption and steganography of secret messages, the channel model is briefly described and the details of the receiving end that are contrary to the transmission steps, decryption, and steganalysis have already clarified the audio and image messages. The third main section of this chapter includes the second algorithm. The workflow of this chapter is shown in the Figure (3.1). The implementation and design of this system are done by using MATLAB 2014b program.

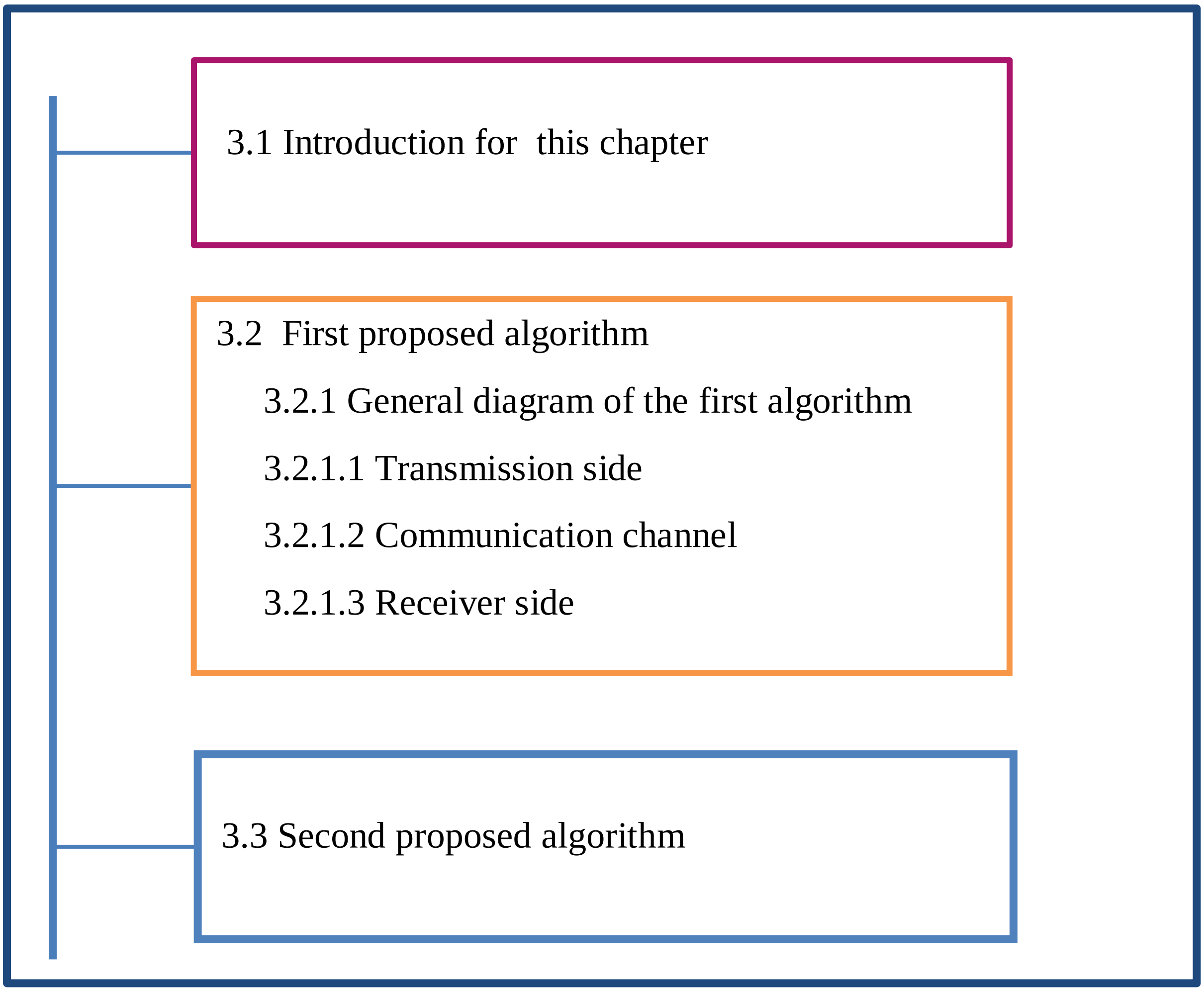

3.1 Introduction for this chapter
3.2 First proposed algorithm
3.2.1 General diagram of the first algorithm
3.2.1.1 Transmission side
3.2.1.2 Communication channel
3.2.1.3 Receiver side
3.3 Second proposed algorithm

Figure (3.1): The workflow of chapter three**.**

3.2 First Proposed Method

In the present day, the most famous steganography algorithm is considered a traditional topic to attackers because of the development of the method and programs that used to break and analyses the stego-file. That is why there is a need to develop a new technology completely different from the previous methods in terms of coding and locating of the hidden information. The algorithm here involves the design of a multi-level security system. Initially, secret messages are encrypted using (Duffing chaotic map, Modify Arnold Cat Map). After the encryption process, the encoded bits are embedded within the cover image in a way that does not allow HVS identify the presence of that data. The algorithm scenario is illustrated by the general diagram which included in section 3.2.1.

3.2.1 General Block Diagram of First Algorithm

The mechanism of the first proposed algorithm is illustrated through the general diagram shown in Figure (3.2). This figure shows that the algorithm includes several levels of confidential data protection. These levels are represented by encryption, steganography, and the use of secret keys. The primary motive of most research in encryption and steganography era is to increase speed and resistance to various security assaults. one of the maximum broadly used systems in encryption methods is chaotic structures. In general the particular functions of chaotic systems is excessive dependence and sensitivity to initial conditions and parametrs. For some makes use of, excessive sensitivity to initial condition and complex chaotic dynamics make chaotic structures very beneficial. consequently, the use of chaos in encryption strategies affords high complexity, diffusion and safety. so a Multi-level security Scheme is proposed by using Chaos based totally on Encryption and Steganography for safety verbal exchange system. Here, the properties of Duffing chaotic map is used in the encryption of the secret image and MACM is used for encrypting the voice. The encryption represents the first security level in this algorithm.

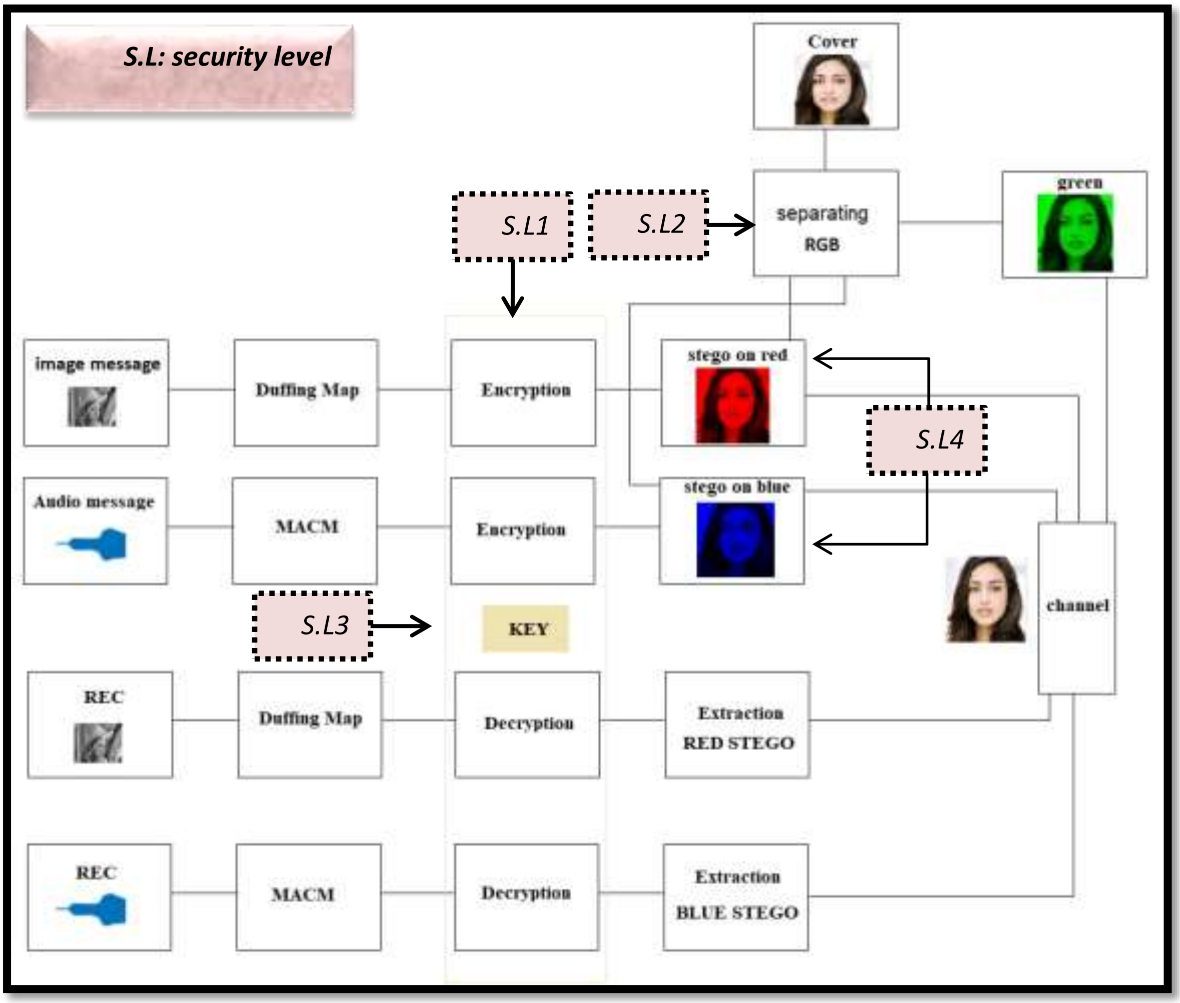


Figure (3.2): First proposed method block diagram.

Another level of security of this algorithm lies in the type of cover which used to transmit confidential information. In this proposed method the color image is used as cover media . In other phrases, the color image contains an RGB coloring model. Each RGB image can be represented by a three-dimensional array. The first plane of the three-dimension represents the pixel intensities of red color space, the next plane represents the pixel intensities of green color space, and the third plane represents pixel intensities of blue color space, In this proposed work, as shown in Figure(3.3), the color cover image is analysed and converted into three color space(three-dimensional array Red & Green & Blue). The intensity of each pixel in each array is ranged between zero (black) and 255 (white).

The motivation behind segmenting the cover image into its primary colors is to hide the encrypted bits of the secret image inside the red color. Also, the secret audio bits which hidden inside the blue color of the cover image. After segmenting the cover into its basic colors and embedding the secret message bits within each color, those layers are grouped and retrieved as a color image called stego-image, so as not to arouse the suspicion of hackers. The depth of detail for this algorithm is explained in Subsequent paragraphs of this chapter.

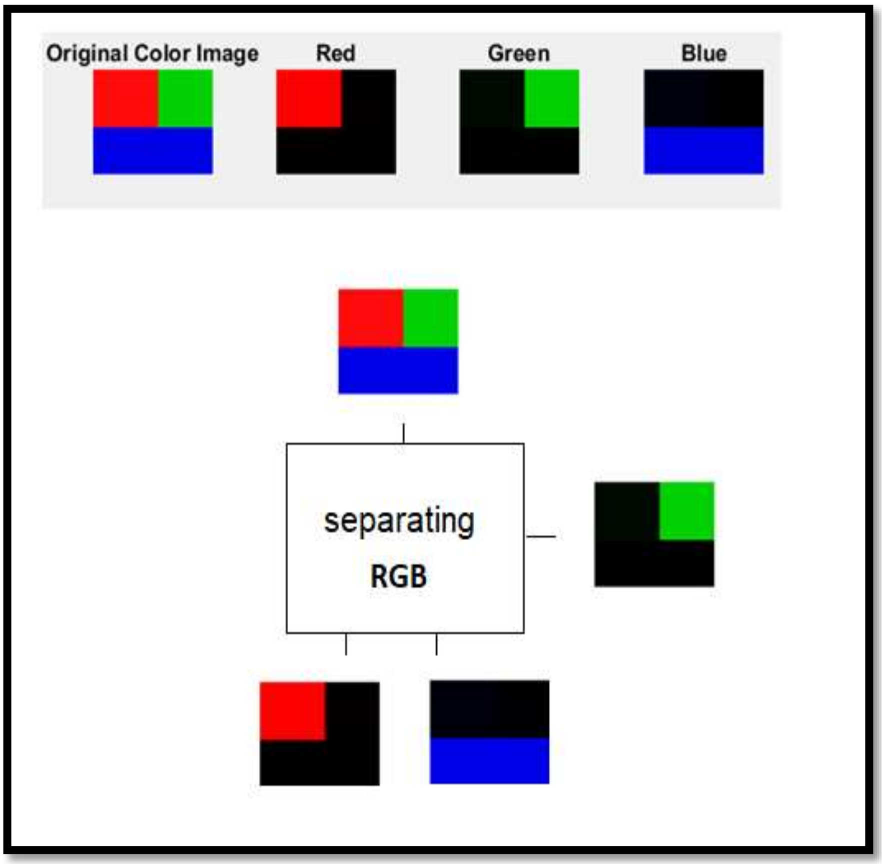


Figure (3.3): Separator block of the original image.

3.2.1.1 Transmission Side

In this section, the transmitter side is explained. The block diagram of this section is shown in Figure(3.4). Through the illustration of this algorithm, the sending side represents the procedures that must be configured by the sender, which are the secret information to be sent within the proposed protection system. The confidential information in this research is an image file and an audio file. Before sending these secret messages, they are subjected to security levels represented in encrypting and steganography way. Encryption is done by using the chaotic algorithm that represented by (Duffing chaotic map and MACM). After encrypting these data, they are subjected to the process of hiding information specifically within the color layers (R,B) that make up the cover image.

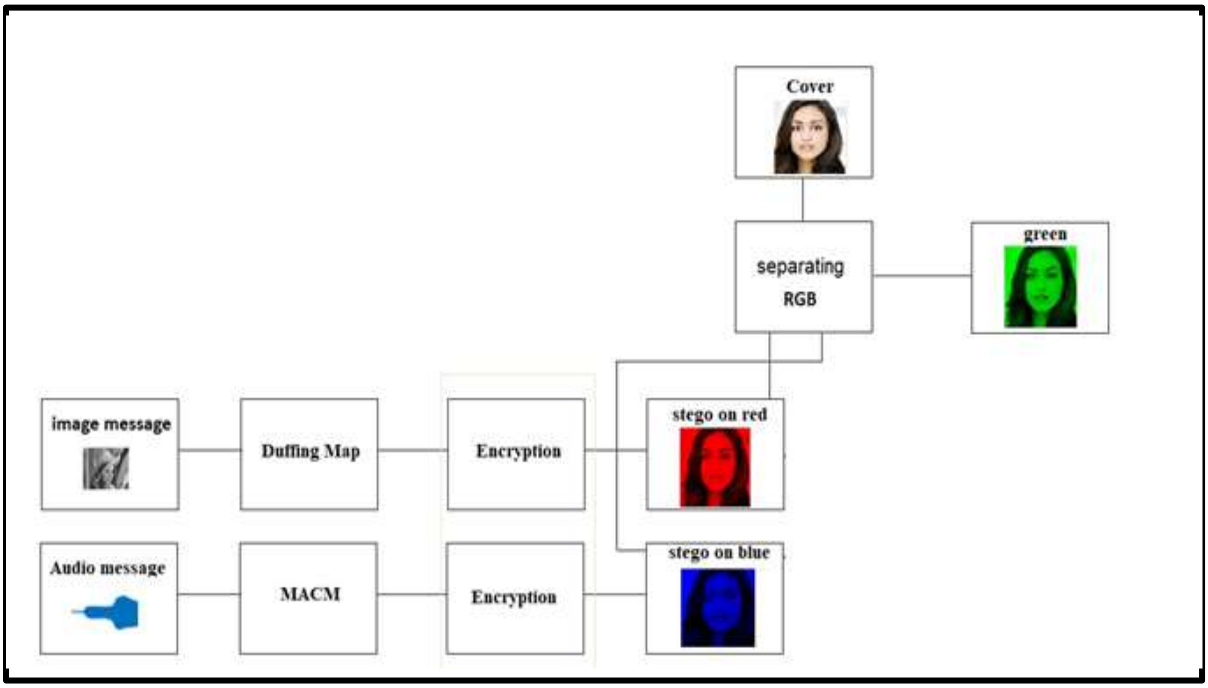


Figure (3.4): Transmission side.

After clarifying the general form of the proposed algorithm and the types of confidential information used.The security levels are explained in this algorithm. To increase the robustness and the security of the proposed system. Encryption based on chaos was used here to obtain a reliable system to protect confidential information represented by audio and video as shown in Figure (3.2). Here in this work, a new way is suggested to embed (hide) the encoded pixels of the secret message inside the cover image.

The transmission side includes two basic parts:

A. Encryption and steganography for image.
B. Encryption and steganography for audio.

Encryption was clarified as a first security level, then the second level, which is steganography, was clarified. This was done in every main part of the transmitter side.

A. Encryption And Steganography For Image

Here in this work, as shown in Figure(3.5).In the mechanism of encrypting and hiding the image, as mentioned earlier, is explained steganography here is based on chaotic cryptography.

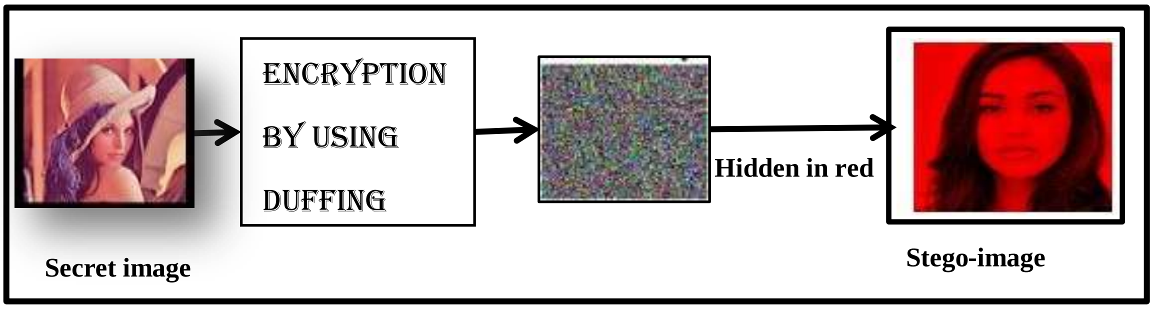


Figure (3.5): Encryption and steganography process.

The encryption of the secret image in the proposed work was done by using Duffing map. For i mage part, takes a point (X_n, Y_n) in the plane and maps it to a new point given by equations (2.14).

These parameters $(\delta, \gamma.)$ and its values add a level of security to the proposed system. Because used they as keys for the cryptosystem in this study. Note that according to the chaos theory used in the proposed method, slight changes to these parameters will change the behavior of the entire system which lead to a high sensitivity system. This structure and operation helps to make the system more secure. The initial conditions and parameters for encryption image are:(**Initial condition** :X=-1 **;***Y=0.5); (***parameter** $\delta = 2.75$, γ =2;*)*. The image encryption algorithm is show in Figure (3.6).

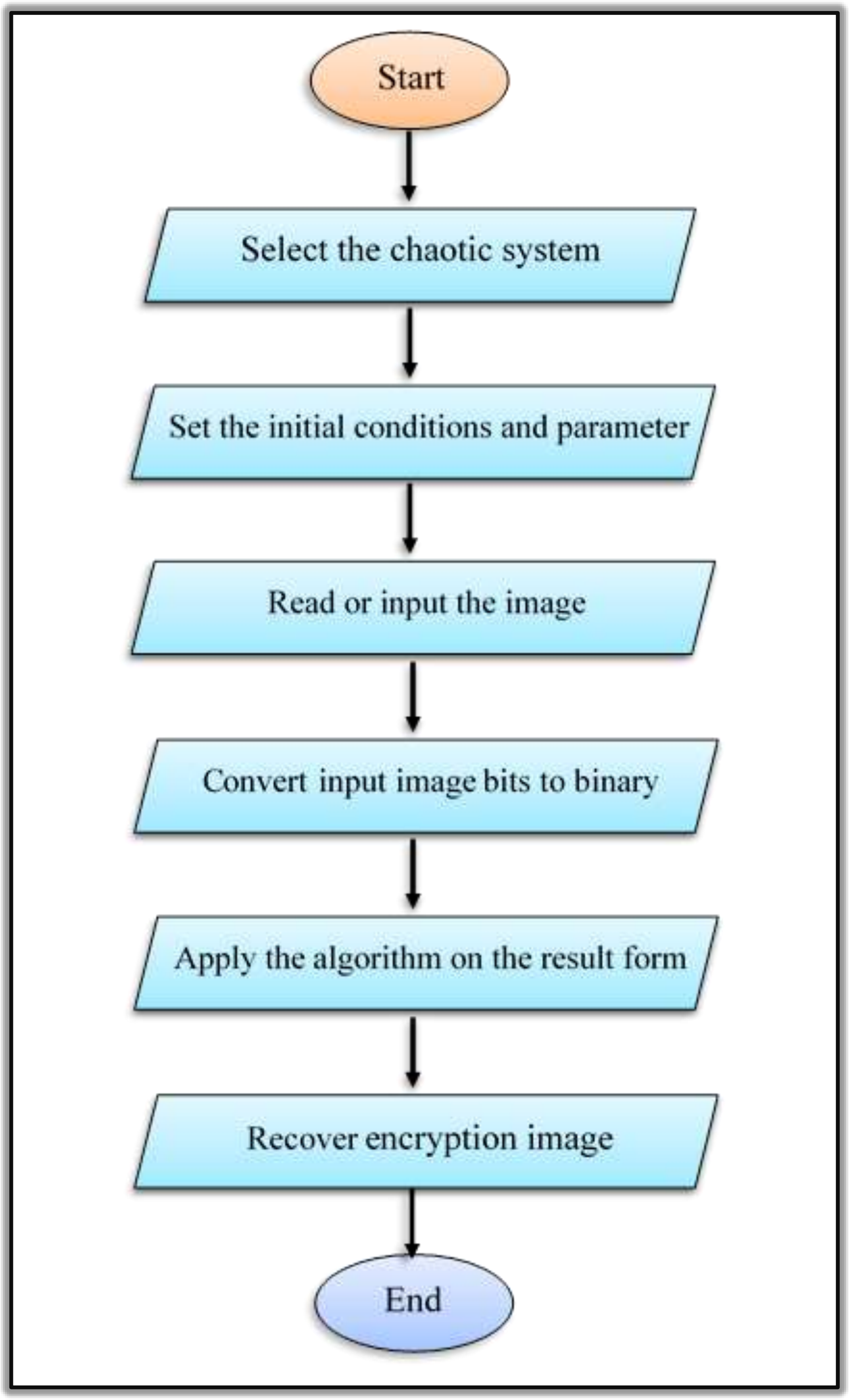

Start
Select the chaotic system
Set the initial conditions and parameter
Read or input the image
Convert input image bits to binary
Apply the algorithm on the result form
Recover encryption image
End

Figure (3.6) : Flowchart of encryption image.

The image encryption in the first algorithm involved first reading the secret image. Then converting the image to binary. The other encryption step is in the chaos function, where the Duffing map it taken that generates random numbers of the same size as the image to be encrypted it . Enter the parameters of this function, which represent secret keys that cannot be retrieved information without knowing it. Duffing Map also used for diffusion and confusion for the data. After a random number is generated through the chaos function, (XOR) is performed between the bits of the secret image and the random numbers which generated by the chaos. After this process, an encryption image is generated that has different pixels than the original image, but has the same size.

After encrypting the image, it will be hidden as shown in Figure (3.5). But as a result of the development of technology the process of hiding data is not sufficient to protect the data against attacks. because just to know that the eavesdropper image sent information can be retrieved in a simple way. To get a very high level of hidden information, we propose a new method based on the chaos system by generating a random index vector (RIV) for the hidden data in the LSB of the image pixels is proposed. To generate an RIV, all three conditions must be met:

1. The length of the generated RIV should be equal to the length of the data you want to hide.
2. The RIV value must be true values and the range of RIV starts at 1 to multiply the image dimensions (r * c * d).
3. Do not duplicate the RIV .

When an RIV is generated with these specifications, it is used to hide the data inside the LSB of the cover image pixels

Now clarify the proposed chaotic steganography algorithm, the following algorithm is used to produce RIV based on chaotic Duffing map.

- Load the cover picture and the secret message.
- Converting the cover picture with dimensions (r*c*d) to one vector.

Where: r: No. of rows, c: No. of column, d: Dimensions of pixel.

- Converting the secrete message to binary data.
- Generating Chaotic Random Numbers (CRN) and multiplied by large number like (10^{12}).

$$CRN = round(X * 10^{12}). \qquad (3.1)$$

- Obtained the random index to embed binary data by using the equation(3.2):

New Index=mod[CRN,(r*c*d)]. (3.2)

- Repeating the process from step 4 and check if the new index is used before, and must be changed otherwise. It completes the repeating process entail reach to the total length of binary message.
- Embedding each bit form binary message in the LSB of the cover picture vector based on random chaotic location.
- Finally reconstructed the Stego. picture with the original dimension.

Based on Figure (3.7) flowchart; initially, the cover image, the secret message, and the chaos parameters are loaded. Obviously these are raw inputs. Then the initial values for n and k are equal to one selected and the RIV is empty and ready to be filled.

$$n = 1 \qquad k = 1 \qquad RIV = []$$

In the next step, the cover image becomes a vector., The secret message is converted to binary data. Then the CRN numbers are generated. To do this, multiply the output by a large number (for example: 100,000,000,000,000) as in equation (3.3). Then, again using the following equation (3.4), obtain index.

$$CRN = round(X * 1000000000000) \qquad (3.3)$$

$$New\ Index = mod[CRN\ , (r * c * d)] \qquad (3.2)$$

Then repeat the process in step 4 to see if the new index was previously used, should be need to change it. If you do not change it, the full length of the binary message is required to complete the iterative process. Includes each bit type binary message in the cover image vector LSB based on a random chaos index. RIV is made after dividing the image cover into its primary colors, which mean it is done inside pixels (R,G & B).Eventually, it reconstructed the Stego-image with the original dimensions.

It should be noted that the length of RIV generated by the algorithm is equal to the hidden data. Also, the value of RIV is numerically greater than one and its maximum is equal to $r * c * d$.(r: number of rows, c: number of columns, d: dimensions of pixel) . Thus the range of RIV changes is shown in equation (3.4)

$$1 \leq \text{RIV} \leq r * c * d \qquad (3.4)$$

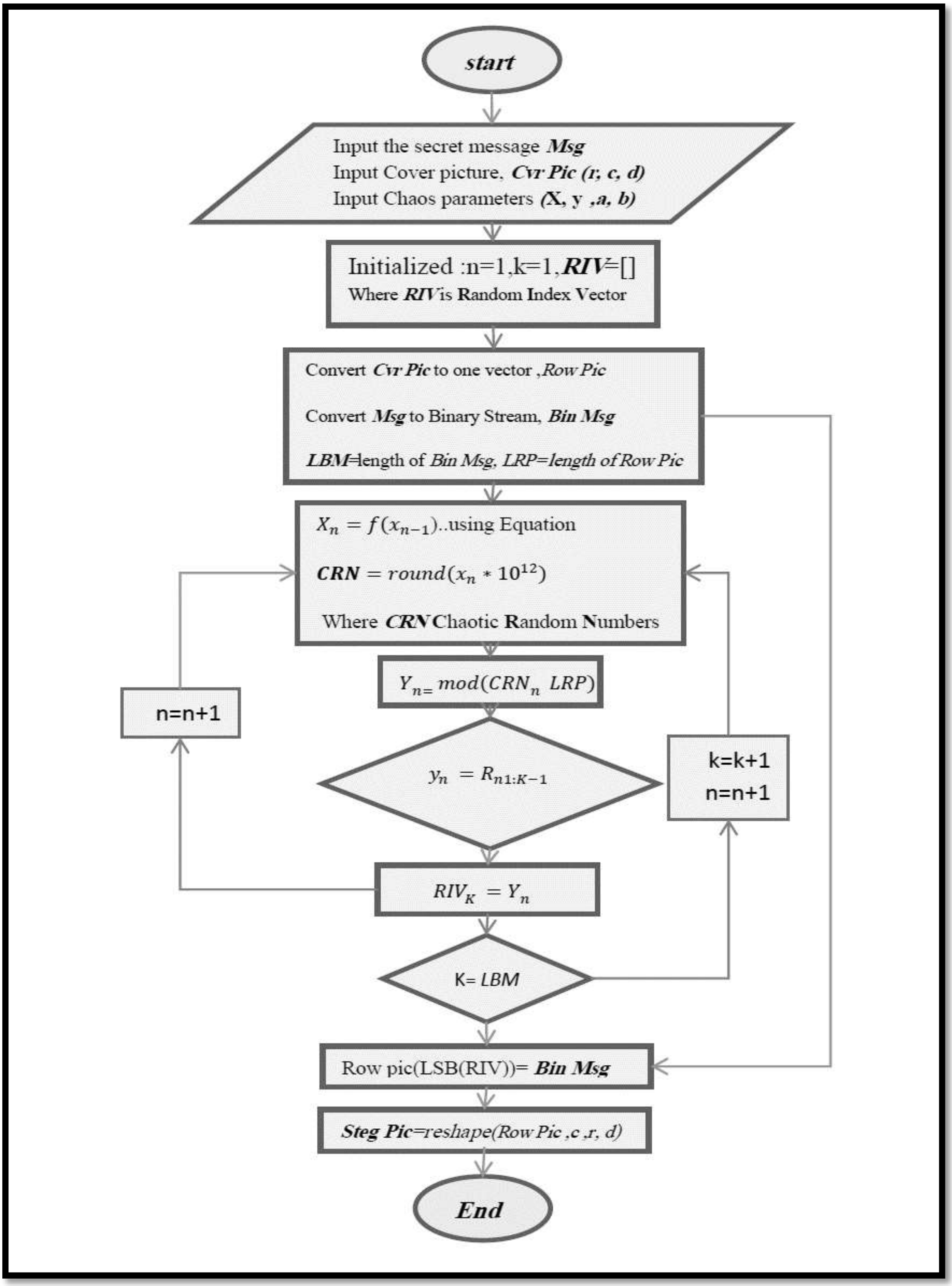

start
Input the secret message Msg
Input Cover picture, Cvr Pic (r, c, d)
Input Chaos parameters (X, y ,a, b)
Initialized :n=1,k=1,RIV=[]
Where RIV is Random Index Vector
Convert Cvr Pic to one vector ,Row Pic
Convert Msg to Binary Stream, Bin Msg
LBM=length of Bin Msg, LRP=length of Row Pic
$X_n = f(x_{n-1})$..using Equation
$CRN = round(x_n * 10^{12})$
Where CRN Chaotic Random Numbers
$Y_{n=} mod(CRN_n\ LRP)$
n=n+1
$y_n = R_{n1:K-1}$
k=k+1
n=n+1
$RIV_K = Y_n$
K= LBM
Row pic(LSB(RIV))= Bin Msg
Steg Pic=reshape(Row Pic ,c ,r, d)
End

Figure (3.7): Flowchart of the image encryption and steganography.

B. Encryption and steganography for audio

The second path from the transmitter side shown in Figure(3.4) illustrates the application of the proposed algorithm on the voice message. This message is also subject to the same security levels that were applied to the picture message. Encrypted over secret audio message by using Modify Arnold's cat Map. In the proposed system model the voice signal is scrambling encrypted by using an algorithm based on chaotic map sequence known on both the transmitter and the receiver. Then the scrambled voice signal is hidding in blue color for cover image. Scrambling process performance usually depends on three important factors, security, band width and delay. While the security of scrambled voice depends on two factors, scrambled voice unintelligible and the cryptanalysis (key space and sensitivity).Figure (3.8) shows the flowchart of the algorithm that used for encryption and then audio steganography.

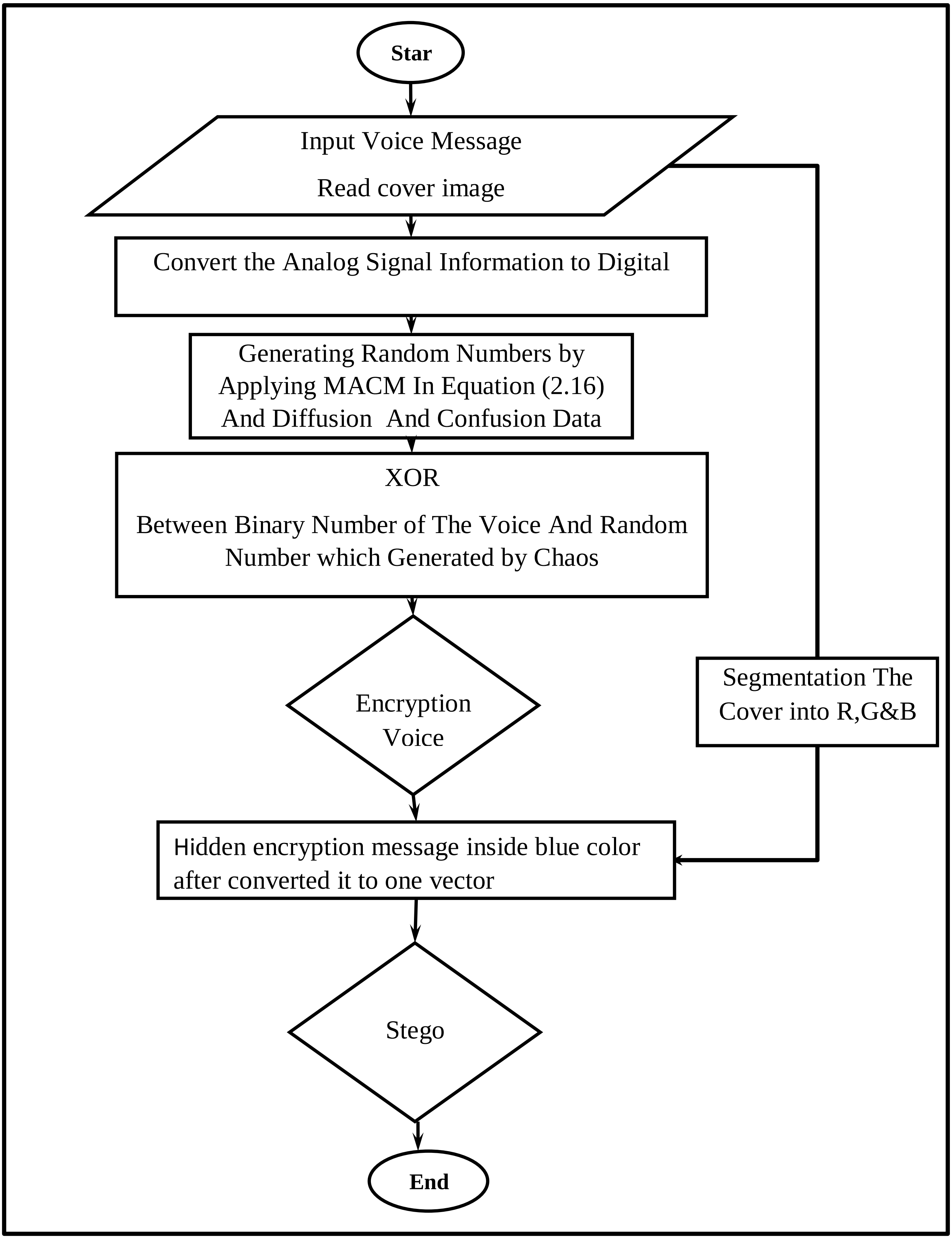

Star
Input Voice Message
Read cover image
Convert the Analog Signal Information to Digital
Generating Random Numbers by Applying MACM In Equation (2.16) And Diffusion And Confusion Data
XOR
Between Binary Number of The Voice And Random Number which Generated by Chaos
Encryption Voice
Segmentation The Cover into R,G&B
Hidden encryption message inside blue color after converted it to one vector
Stego
End

Figure (3.8): Encryption and steganography for audio.

The inputs of this algorithm are the cover image and audio (message). The size of the audio message should be clearly smaller than the size of the cover image. The audio messages are converted to binary signals in the next step. After converting the audio to Binary, (MACM) is used for the purpose of generating random numbers with the same size as the data used. It also used for diffusion and confusion the data, and this represents another level of security in the encryption stage. This was also done in the image encoding stage.

- **Diffusion:** This step is actually a kind of rearrangement or changing the position. In this case, using MACM, the original data locations are changed randomly. The Figure(3.9) shows an example of the effect of this step.
- **Confusion**: In this case, the values of the data that had changed position in the previous step are also changed. This is done with MACM. In fact, the random values generated by MACM are xored) with the values of the data that have been moved to execute the encrypted message. This is one of the most important steps and another level of security. An example of this is shown in Figure(3.10)

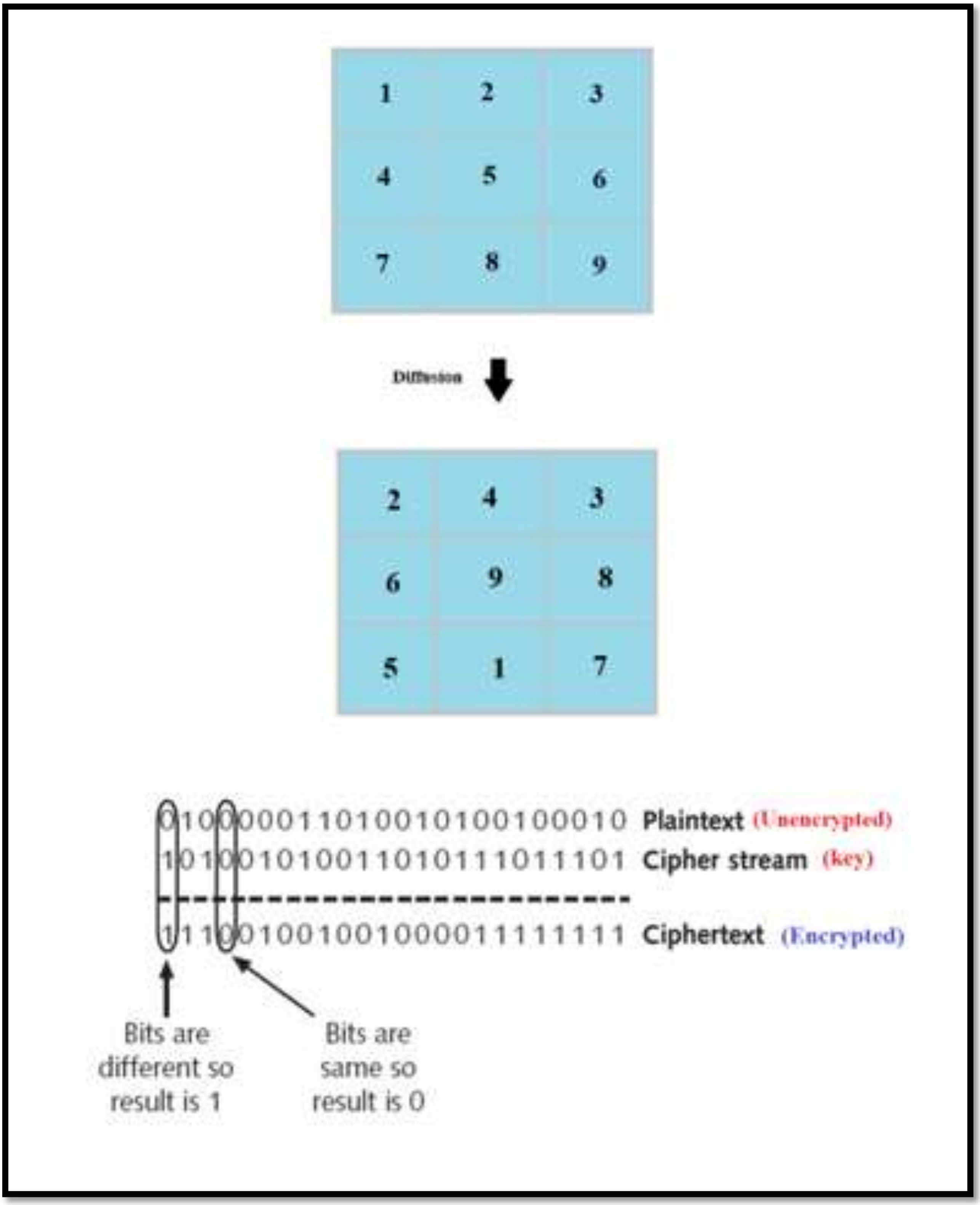

1
2
3
4
5
6
7
8
9
Diffusion
2
4
3
6
9
8
5
1
7
010000011010010100100010 Plaintext (Unencrypted)
101001010011010111011101 Cipher stream (key)
111001001001000011111111 Ciphertext (Encrypted)
Bits are different so result is 1
Bits are same so result is 0

Figure (3.9): Example of Diffusion and XOR.

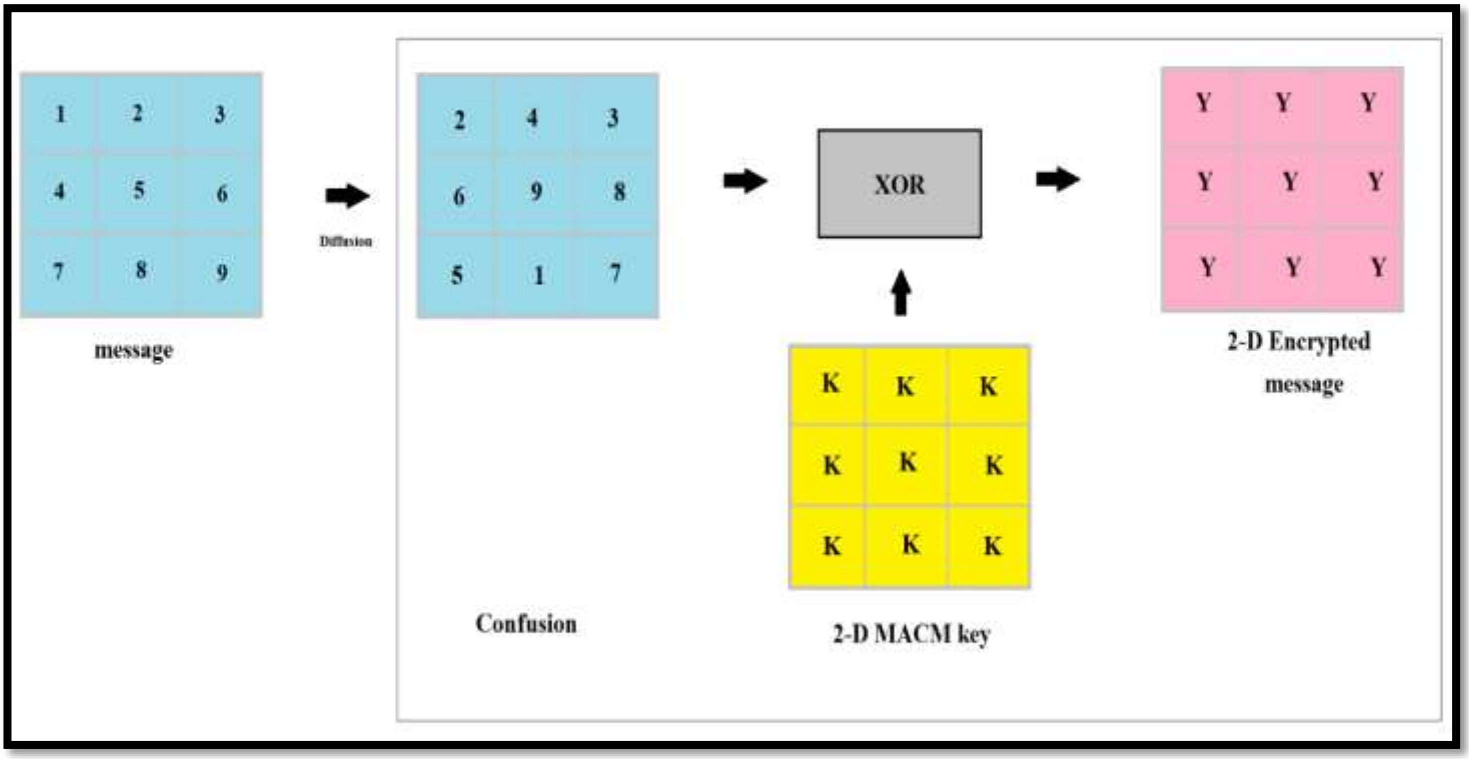


Figure (3.10): Example of Diffusion with Confusion

By following the flow chart in Figure (3.8), when the encoded sound is obtained, it then moves to the other level of security represented by steganography. At this stage, the cover image is read after that its separate to (R,G&B) and this procedure represents an additional level of security, which makes it difficult for the hacker to realize that there is hidden data inside the blue color specifically, and to understand this requires more effort and more time.

The embedding process was performed using the least significant bit method. The encoded message bits are hidden inside the LSB of the blue color of the cover. After embedding the secret data inside cover, a stego image is obtained and sent to the receiver through a communication channel.

3.2.1.2 Communication Channel

One of the most important components in communication systems is called "communication channel". In this method, A communication channel establishes a connection between a "transmitter" or sender and a "receiver" of a communication. In this research,the channel that is used for testing the proposed system is Internet channel(social media programs). Figure(3.11).

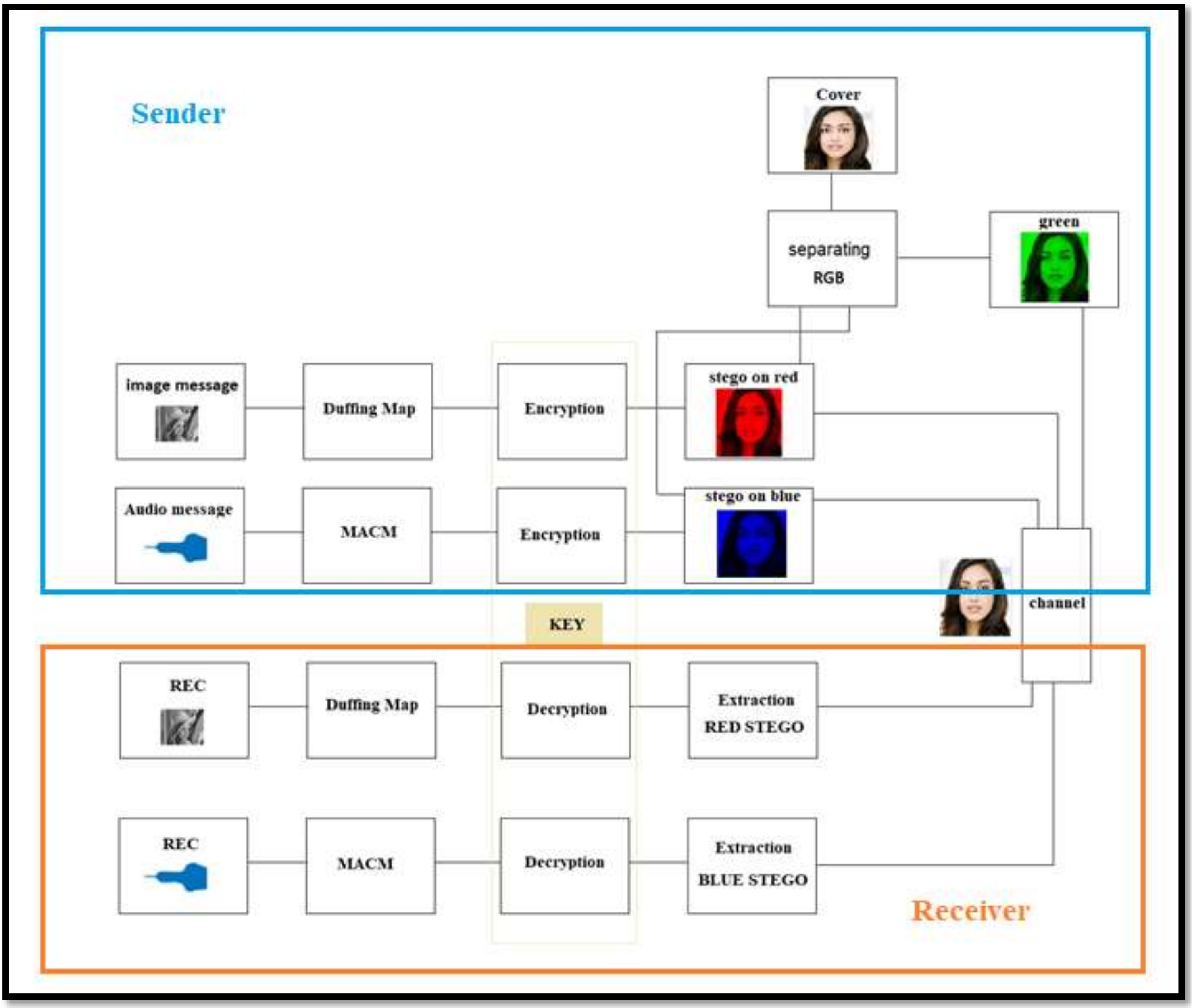
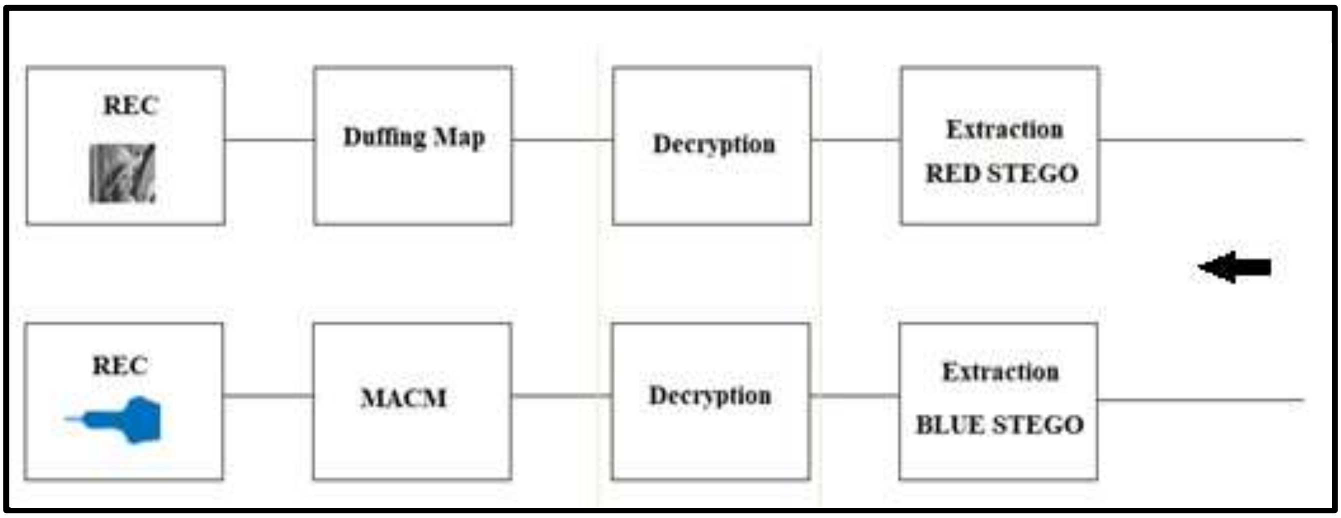


Figure (3.11): Separation of components of the proposed diagram block into three main components of sender, receiver and a communication channel.

3.2.1.3 Receiver Side

In this section, will explain the receiver part will explained. The block diagram of this section is shown in the Figure (3.12).This section consist of :
I. Decryption and Steganalysis of image, II. . Decryption and Steganalysis of



audio.

Figure (3.12): Receiver side.

I. Decryption And Steganalysis of Image.

After sent the information with the communication channel, the recipients of proposed system need to be reversed. In this case, you need to do three important things in sequence.

- *Color image extraction*
- *Extract information from the cover*
- *Decryption*

Obviously, one of the most important features of a chaotic cryptosystem is its sensitivity to initial conditions. In short, the goal is to reconstruct the original signal or message at the receiver (the encrypted and steganographed signal enters the receiver after passing through the noise channel). The first step is to extract the encrypted message from the cover. Defined as the opposite of steganography. The next step is decryption.

The procedure for this purpose is shown in Figure (3.13). First, the original image (red channel) needs to be separated and LSB extracted. As mentioned earlier, the encrypted message is in the LSB. Need to create the array with the key parameters. In the next step with Duffing Map, the main message is encrypted. This message should eventually be converted to a two-dimensional, viewable image. This will be the message(image).

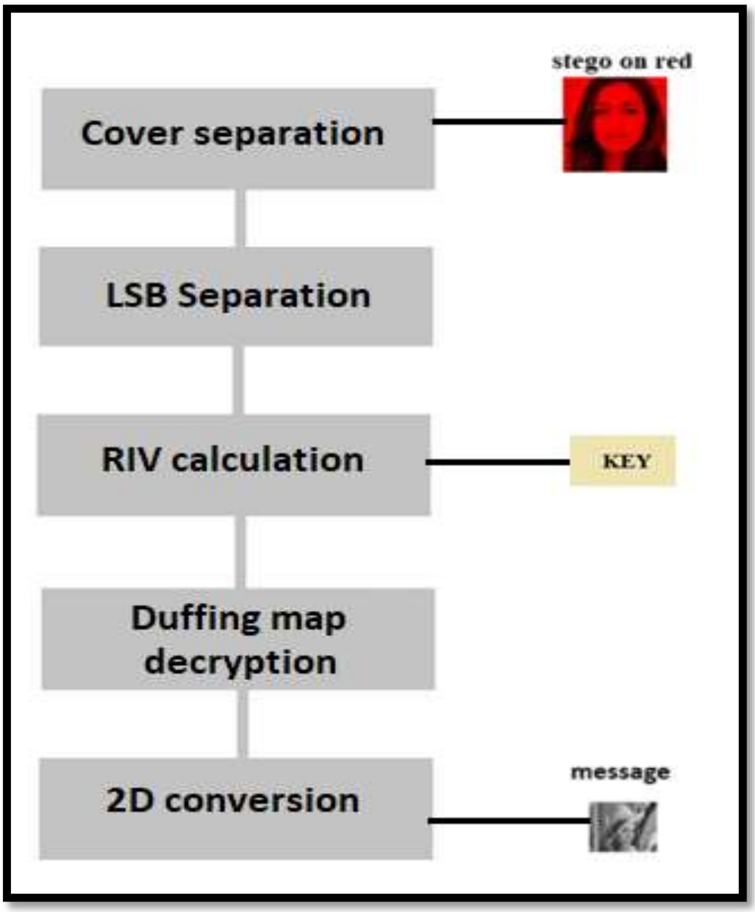


Figure (3.13): Decryption and steganalysis.

II. Decryption And Steganalysis of Audio

As mentioned, the MACM-based encryption algorithm used several levels of security. The first is the initial condition. Initial condition must be available on both the sender and receiver. Another level of security used in the algorithm was the dimensions of the incoming message, which are also key. Also, size A, B and C are another level of security. The same key is using in encryption and decryption system as shown in Figure (3.14).

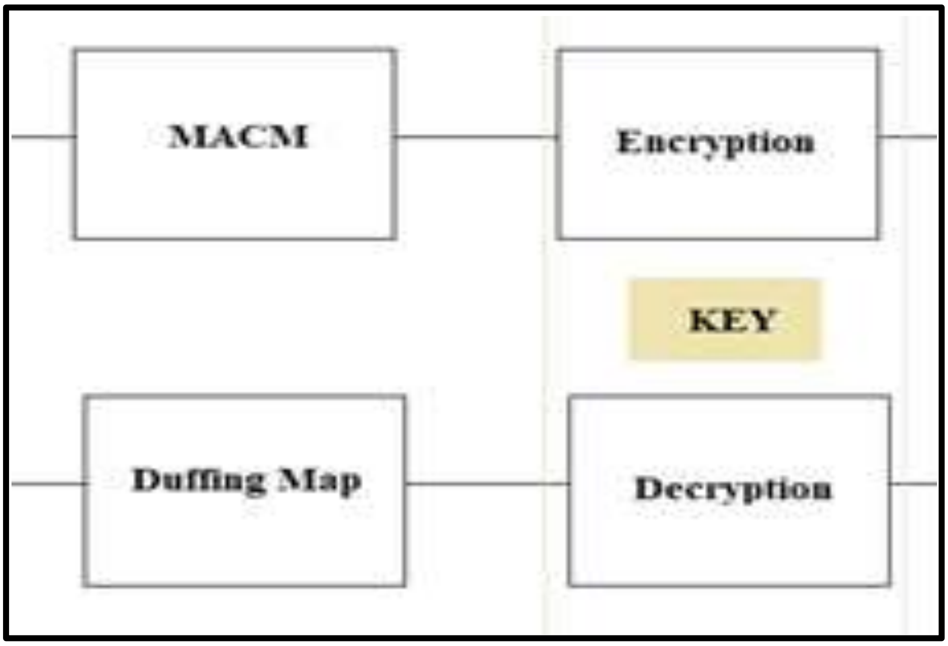


Figure (3.14): Encryption and decryption based on the same key.

Figure (3.15) shows the algorithm of decryption. Given this figure, it is clear that all encryption steps must be performed in reverse. Eventually the original sound will be restored. As know; the most common type of key-based encryption is "private key" encryption. This type of cryptography is called symmetric. In this type of encryption, the sender and receiver are aware of the key used to encrypt the information. Private key encryption is a good option for exchanging information over the Internet or storing sensitive information in a database or file. In this case, there was a similar scheme for encryption and decryption (both for image and audio).

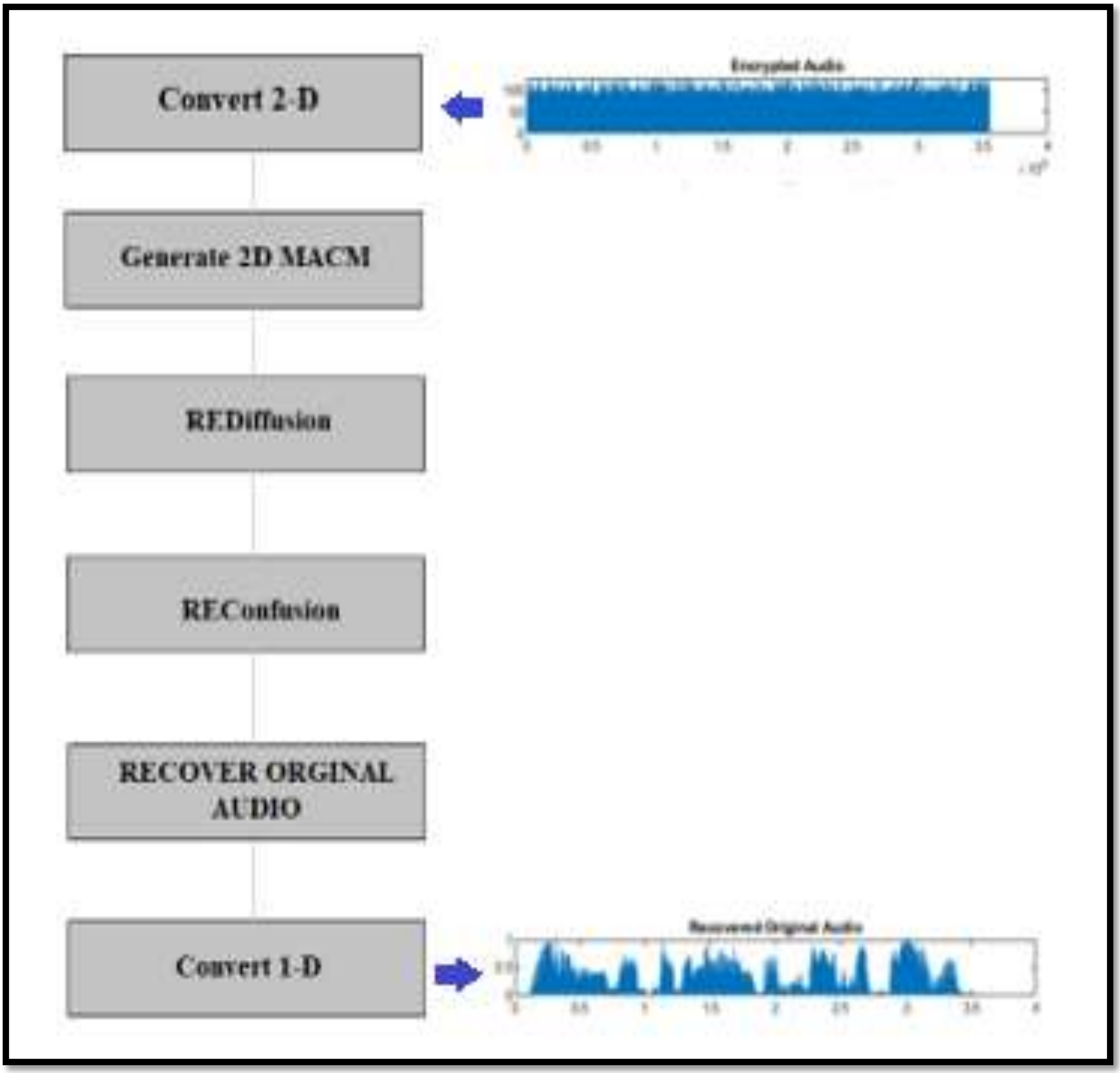


Figure (3.15): Decryption for audio.

3.3 Second Proposed Method

The first section shows a block diagram of the proposed method. The second section provides details on the sender. The sender details are the coding and steganography of audio and image messages. Duffing map are investigated as a chaos scheme for audio messages, and MACM are investigated as a chaos scheme for image messages. The third section briefly describes the channel model.

Finally, in the fourth section, the receiver side details, which are the opposite of the transmission steps, decryption and steganalysis have been clarified for audio.

Figure (3.16) shows the form of this proposed method. It consists of several parts that were clarified in the first proposed method above in section (3.2). The difference is only in the encryption part, and the mechanism of work

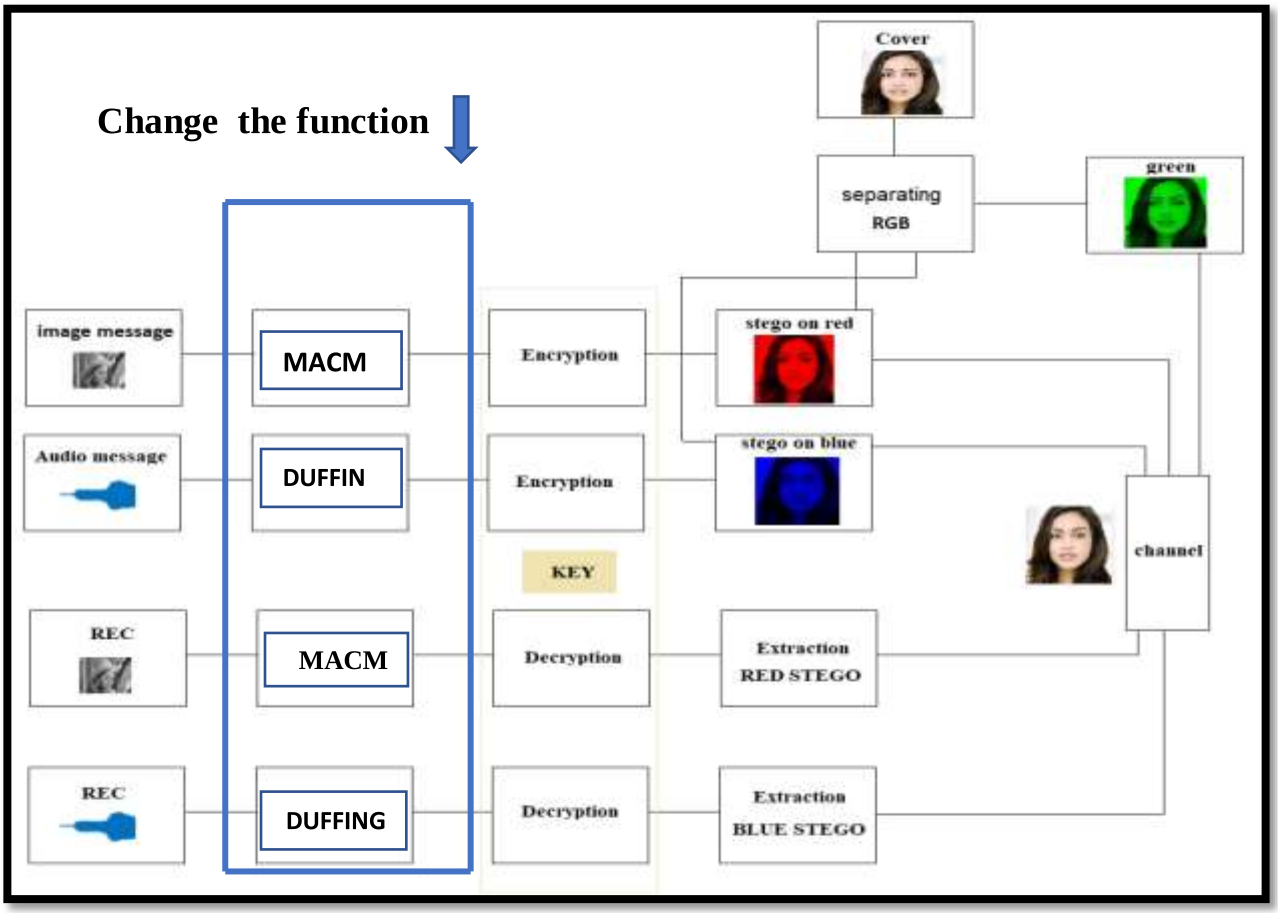


Figure (3.16): The second proposed method block diagram.

This system is design based on MATLAB. The Duffing chaos map is used to encrypt the audio signal, and the Arnold cat map is used to scramble the image signal. After the encryption process, the result value will be hidden on the cover image. At first, the encryption and steganography process for audio will be explained in the steps below:

The first step: Read the voice as one dimension. Each voice consist of number of samples (frequency sample) and each sample consist of 8 bits, in this thesis using voice about (f_s=*8000 sample*) mean about 64k bits.

The second step: Convert the voice to binary.

The third step: Take just the positive value by shifting the negative value.

The fourth step: Generated the chaotic map (Duffing chaotic map) with length equal to audio length. Set the initial value and parameter ((Initial condition: X=-1; Y=0.5) ; (parameter: a = 2.75 ; b = 0.15;)).Random numbers will be generated from the Duffing map (0-255).

The fifth step: Make (XOR), between the result of the second step and fourth step to get encryption voice and generating a secret key that is known only to the sender and recipient, and that key is encrypted by Duffing function. The length of key is equal to the data used.

The six step: After encoding, the audio is hidden inside a colored cover image. Initially the cover image is read. After that separated the cover image in to RGB (red, green, blue) and selector color where (1-R, 2-G, 3-B).

The seventh step: In this way, the sound is hidden inside the blue color, and the color is actually chosen by activating the option from the previous step. The seventh step is performed through MATLAB as shown in the line below.

Cover (Location) = bitset (Cover (Location), 3, BinDataStr)

Where **BinDataStr:** binary data stream, **3**: The color blue.

The eighth step: convert the cover image to binary stream. Embedding each bit from binary message in the LSB of the cover. Figure (3.17) shows the flowchart for audio encryption and steganography.

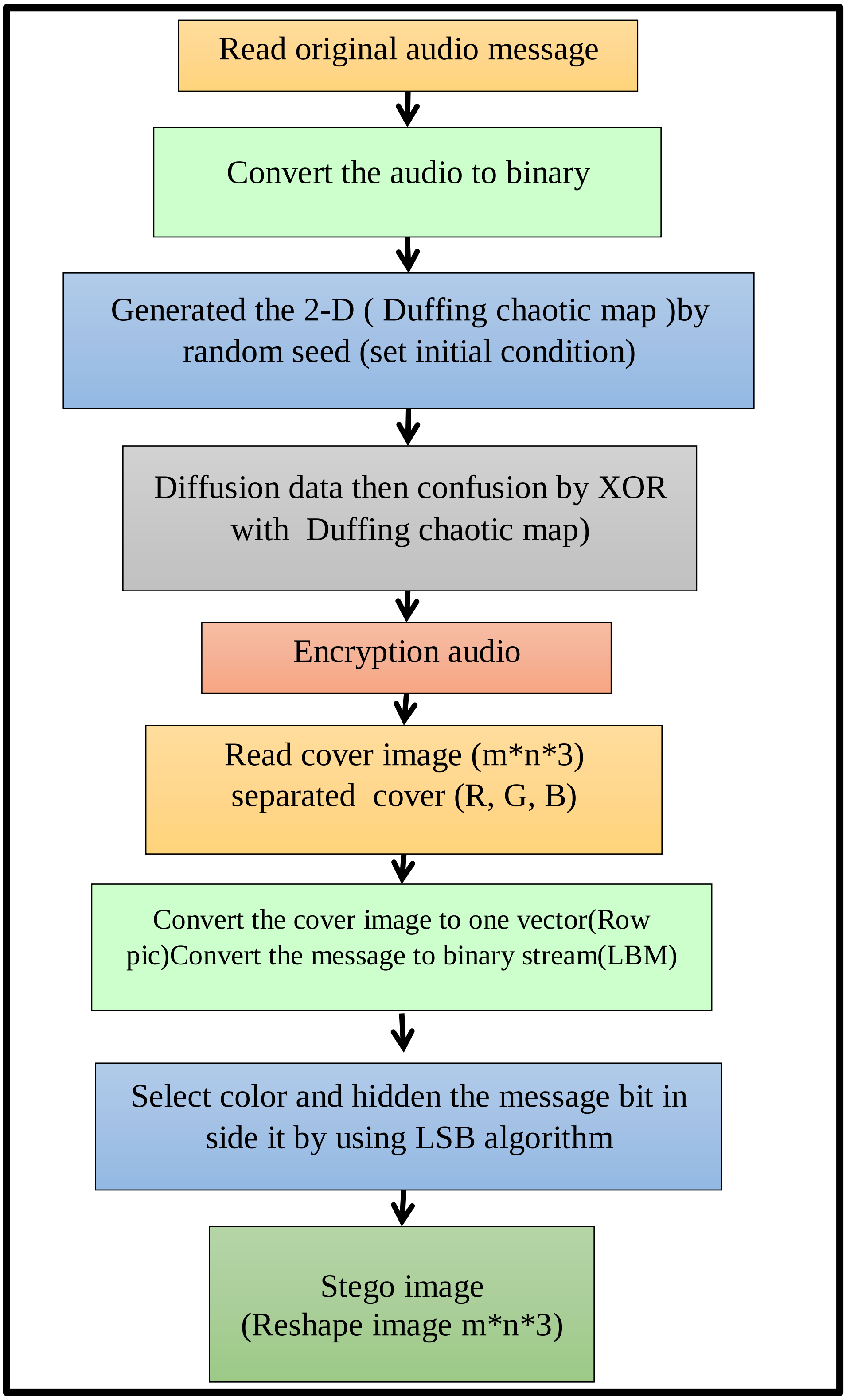

Read original audio message
Convert the audio to binary
Generated the 2-D (Duffing chaotic map)by random seed (set initial condition)
Diffusion data then confusion by XOR with Duffing chaotic map)
Encryption audio
Read cover image (m*n*3) separated cover (R, G, B)
Convert the cover image to one vector(Row pic)Convert the message to binary stream(LBM)
Select color and hidden the message bit in side it by using LSB algorithm
Stego image (Reshape image m*n*3)

Figure (3.17): Encryption and steganography audio by Duffing map

After the audio steganography and encryption process, image encryption is explained using Arnold's cat map and then hiding it in cover image (exactly in red color).

This method is the same as that used in the first algorithm of the image. Only here the image is encrypted using Modify Arnold Cat Map (MACM) instead of Duffing's Chaotic Map. The implications of this difference are discussed in Chapter 4, Contains the result of each method.

Chapter Four

Result and Discussion

CHAPTER FOUR
RESULT AND DISCUSSION

4.1 Introduction

This chapter presents the simulation and implementation with the discussion of the most significant features of the proposed system. A combination of two multidisciplinary components is seen here Encryption and Steganography. As displayed in the previous chapter, have a presentation is done by using the chaos characteristics for encryption the image and audio. Then distributed the encoded pixels inside the cover image frames in a way closer to a random distribution depending on the (R,G,B) and LSB is seen and discussed.

This chapter also displays the user interface design and show the efficiency of the system to maintaining the cover image quality after embedding data in in a suitable value by applying several tests like PSNR, MSE, BER and SSIM among of the original image and the stego image output. Symmetric key coding is used for all simulations. All simulations run in MATLAB 2019. This chapter consists of eight parts. After being introduced in the first part, the second part represents the parameters for assessing the quality and efficiency of the proposed system. In the third part, the effect of the keys explained. The fourth part describes the results of the first algorithm. The fifth part shows the results of the second algorithm, sixth part describes a general comparison of the two algorithms and discussion. The seventh part Perform the proposed system under the effect of the different Internet platforms. last part shows a comparison with related work.

4.2 Evaluation Criteria

Quality evaluation is an important issue. There are various criteria for assessing quality, and these criteria are divided into two types: the first type (subjective view) and the second type (objective). The first and simplest criterion is a subjective perspective. As a result, the observer or listener can comment on the similarities or differences between the two signals (image or sound), paying attention to their quality. However, this is not a quantitative measure. Objective parameters are represented by different types, divided into two groups. The first group is to measure the quality of the stego and received images, and the second group can be used to evaluate the performance of the extracted voice messages, an example of this types (PSNR, MSE, SSSNR, CC ,etc.). All the parameters used to measure the efficiency of the proposed system are explained in the second chapter precisely in terms of equations and graphs for each type. Here it is implemented in order to evaluate the efficiency of the system.

4.3 Key Space and Key Sensitivity

For secure system ,the key space should be large enough to make sure that the brute force attack is infeasible. Increasing the key length exponentially. increases the time that it takes an attacker to perform a brute force attack ,when the attacker trying all possible key combinations to break the system. In the proposed system, parameters (a1, b1 ,c1) of MACM also(δ, γ)can be used as Duffing parameters and sub-band dimensions X, Y as switches, so if the combination of all of these keys (Y, X, a1, b1, c1, δ, γ) was calculated, then it is large and hence, any exhaustive search through all possible keys is impractical to get the secret data .

Figure(4.1) the permutation of the secret image over the subband of the cover image as an example .Ablock of (4×4) will be taken, according to different groups of keys.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

a

16	2	8	10
9	15	1	7
6	12	14	4
3	5	11	13

b

16	10	8	2
11	5	3	13
6	4	14	12
1	15	9	7

c

Figure(4.1):-Permutation by MACM a:The original position b: a_1=2,b_1=3,c_1=4 c: a_1=3,b_1=3,c_1=4

So, it can be concluded that the proposed algorithm is sensitive to the key; any change of the key will generate a completely different results and cannot get the correct secret data. Chaotic permutation makes proposed system more secure because the steganography techniques reduce the chance of detection of the secret message , but if an attacker discovers the existence of the message then he could very easily extract it out of the cover just by decomposed it . So this permutation adds another layer of protection which increases the security ,and if the attacker determined the level and the subband that the secret data was embedded on , then only the noisy data he can get without the correct keys.

4.4 The Results of the First Proposed Algorithm.

The first proposed algorithm included coding and steganography of audio and image messages. This algorithm uses a duffing chaotic map to encrypt the image and a Modify Arnold Cat Map to encrypt the audio. After that, the encrypted data is hidden inside the cover image, especially use the blue color to hide the audio and the red color to hide the message image.

4.4.1 Encryption Result.

Test measurements are performed on all simulation results. Also the histograms are used to analyze the performance of un encoded images(the original image), the image after encryption (encryption image image) and the image after decryption (the recovered image), and is also used to analyze the performance of the audio in the same way used for image analysis. The encoding results include two parts: A. The audio encoding results, B. The image encoding results.

A. Audio Encryption Results

This section contains the results of the encryption effect on secret audio. The result of the audio encoding is displayed. Here the voice clip used for testing purpose has 8 KHz sampling frequency and 05:68 seconds length (45440 samples), as is shown in Figure (4.2).

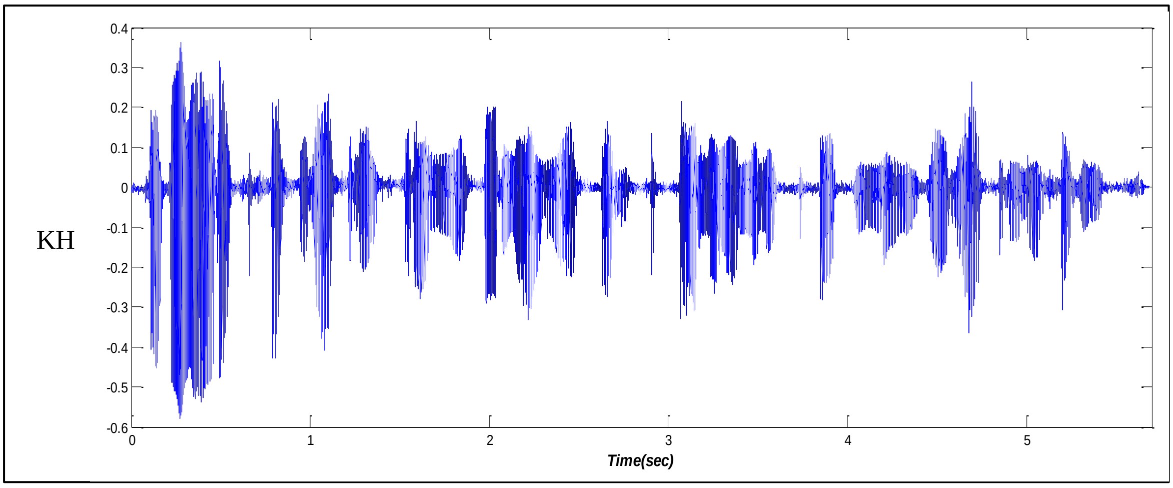


Figure (4.2): Original voice signal.

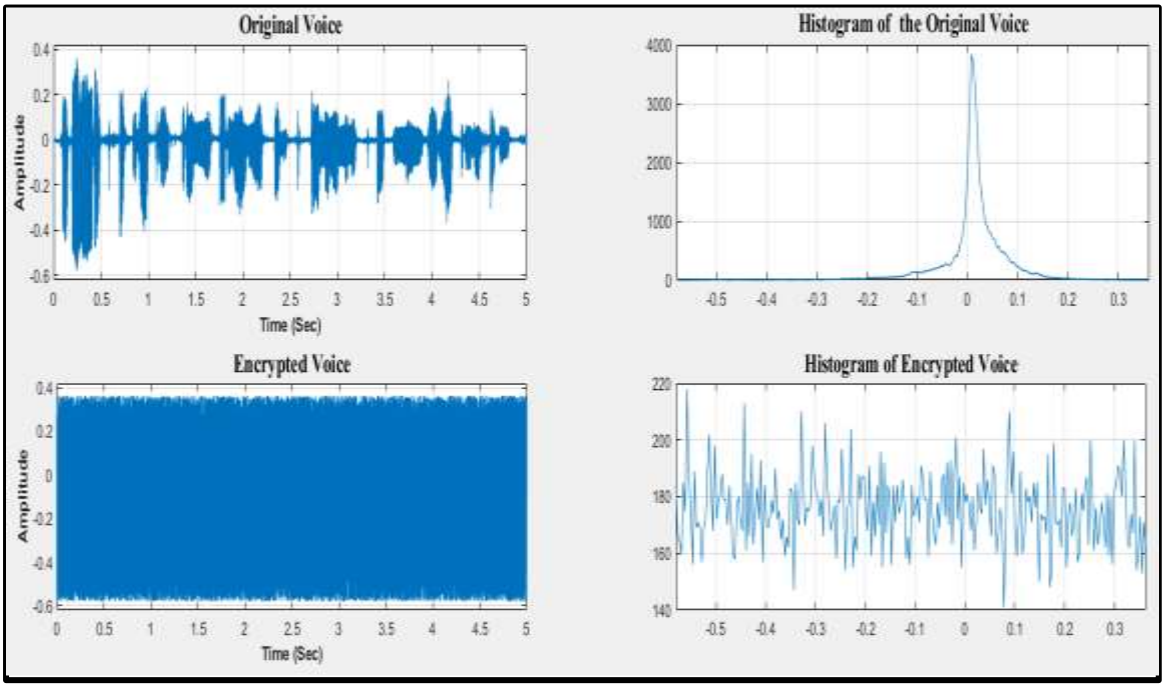
Here, in this part, the most prominent results obtained when applying the MACM encoding process to the secret audio are explained. The results were presented in two ways as mentioned in paragraph (4.2). So that, the tables represent the result of the object as clarified in Table (4.1),while the figure refer to the subjective view as shown in Figure (4.3).

Table (4.1):Result of encryption voice.

SSSNR(dB)	LPC	CD	MSE
-12.07	16.14	7.61	0.21

The results presented in Table (4.1) show the effectiveness of the acoustic coding mechanism used. Through the displayed parameter values, it can be shown that the parameters of the original secret sound are almost non-existent to the listener after this encoding mechanism, and the obtained sound cannot be understood. Where the LPC value is greater than 1 it means that the original values of the sound are completely scattered, as well as the CD where whenever If its values are higher than 1, it means that the encryption mechanism is efficient.

In addition to what is presented in Table (4.1), the effectiveness of the algorithm on the secret voice can be understood by looking at the figure. (4.3) This figure shows the original audio diagram and its graph also shows the sound of the encoder after applying MACM and its histogram.In addition to what is presented in Table(4.1), the effectiveness of the algorithm on the secret sound can be understood by looking at the Figure(4.3) . This figure shows the plot of the original audio and its histogram also shows the encoder audio after applying the MACM and its histogram.



Figure(4.3): Audio encryption results.

Figure (4.3) proves that the histogram resulting from the encryption process is completely different from the original histogram. This proves that the encryption used in this step doesn’t leave a trace of the original voice. Rather, it shuffles the audio sample in such a way that it is difficult to understand what has been encoded. This proves the strength of the method used to encrypt the voice and make it incomprehensible to the hacker. This encryption method represents the first level of the proposed algorithm.

The proposed encryption algorithm was tested on more than one voice message of different sizes. The results of this procedure are shown in Table(4.2).

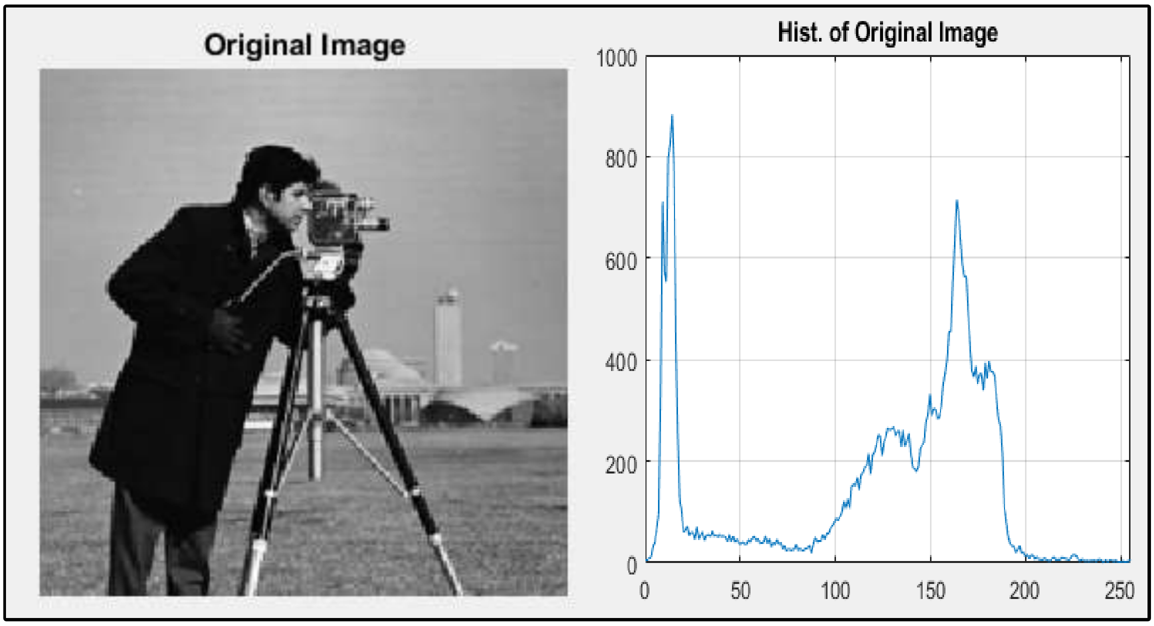
Table (4.2): Result of encryption algorithm for different size audio.

File size (wav)KB	ENCRYPTION AUDIO			
	SSSNR	LPC	CD	MSE
8KB	-12.069	16.144	7.6078	0.206
10KB	-12.0671	16.154	7.6016	0.2033
16kB	-12.0072	16.1455	7.5993	0.203

The results presented in Table (4.2) prove the success of the first voice coding algorithm in encoding voice messages of different sizes. Where it can be concluded that this method has proven its effectiveness in encrypting all voice messages, regardless of their size. Where the LPC values are very high, CD is greater than the negative values, and the error rate is close to one. This proves that the encryption mechanism is very effective..

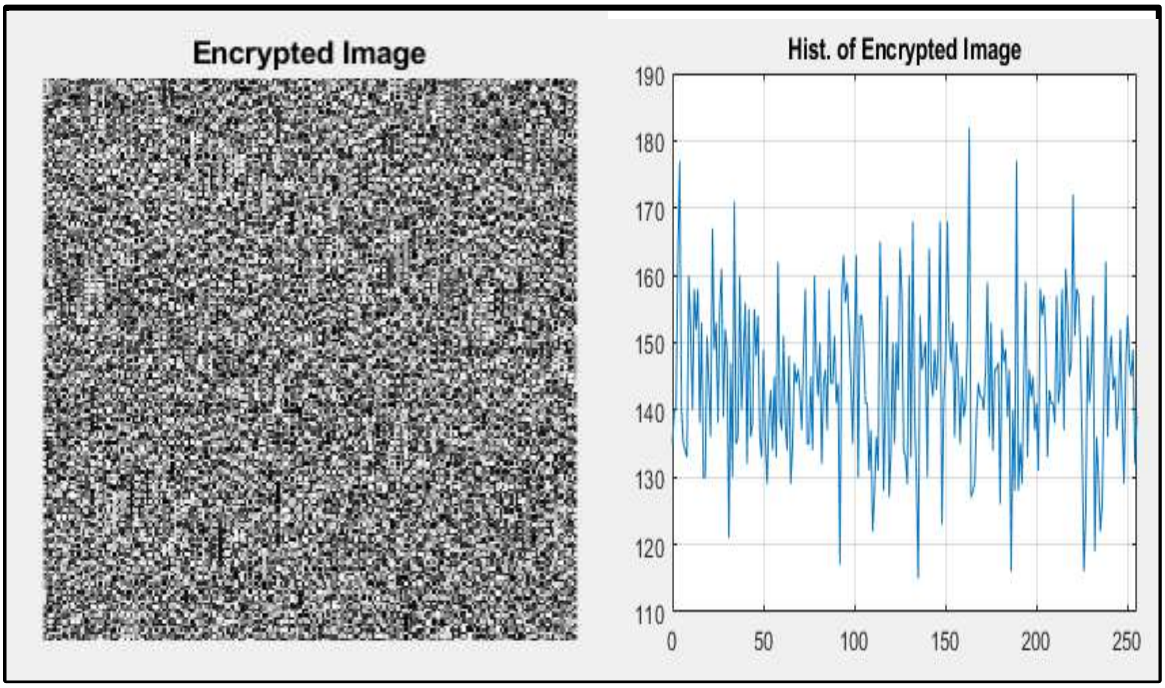
B. Image Encryption Results.

After displaying the results related to audio encoding, the results of image encoding are shown in this section, in this algorithm a gray image of size(192*192) was used as a secret image to test the proposed encoding algorithm. Figure (4.4) shows the original image and its histogram.



Figure(4.4):Secret image and its histogram.

The encryption algorithm represented by duffing map was applied to the image shown in Figure (4.4). The most prominent results that were obtained from this encryption process are illustrated by the same mechanism that was presented in the audio results. Figure (4.5) shows the encrypted image and its histogram



Figure(4.5): Encryption image and its histogram.

When the image that was accessed after the encryption process which shown in Figure (4.5) was compared with the original image in Figure (4.4), it was proved that there is a significant difference between them, as there are no clear features of the original image. This makes it difficult for hackers to decrypt and recover data unless the key that was used is identified.

Also, the histogram of the encrypted image is completely different from the graph of the original secret image. This means that the original image are scattered in a way that is difficult to understand. In addition to the subjective part of the results, the object was displayed through Table (4.3), where that table showed the values that were obtained by comparing the encoded image with the original.

Table(4.3): Encoder results for different size images.

Dimension of the secret image	**ENCRYPTION IMAGE**		
	MSE	PSNR	SSIM
32*32	6.432	3.01	8.36 e+03
32*64	8.036	2.98	9.51e+03
192*192	8.4680	3.691	9.25e+03

Table (4.3) proves the effectiveness of duffing map in encoding images of different sizes. Where through the similarity values between the encrypted image and the secret image, find that the similarity amount is around 8.36 e+03, as well as for MSE is >1, which means that the amount of distortion that occurs on the secret image is very high, which means the success of the proposed encryption algorithm.

Thus, it can be concluded that the chaotic functions used in encoding sound and image, represented by (MACM and Duffing map) have the ability to encode any image or audio file without paying attention to its size.

4.4.2 Steganography Results

In the third chapter, it was clarified that the process of hidden confidential data is adopted as a second security level after encryption. Here in this part, the most prominent results of this level will be shown represented in hiding the encoded audio bits within the blue color of the cover image and the encrypted image bits within the red color of the cover image. Cover image size used here about (512*512*3). The results of steganography process are also displayed in two sections:

Figure (4.6) shows the process of hiding a secret image with a size(192 * 192) and a secret audio (16 KB).

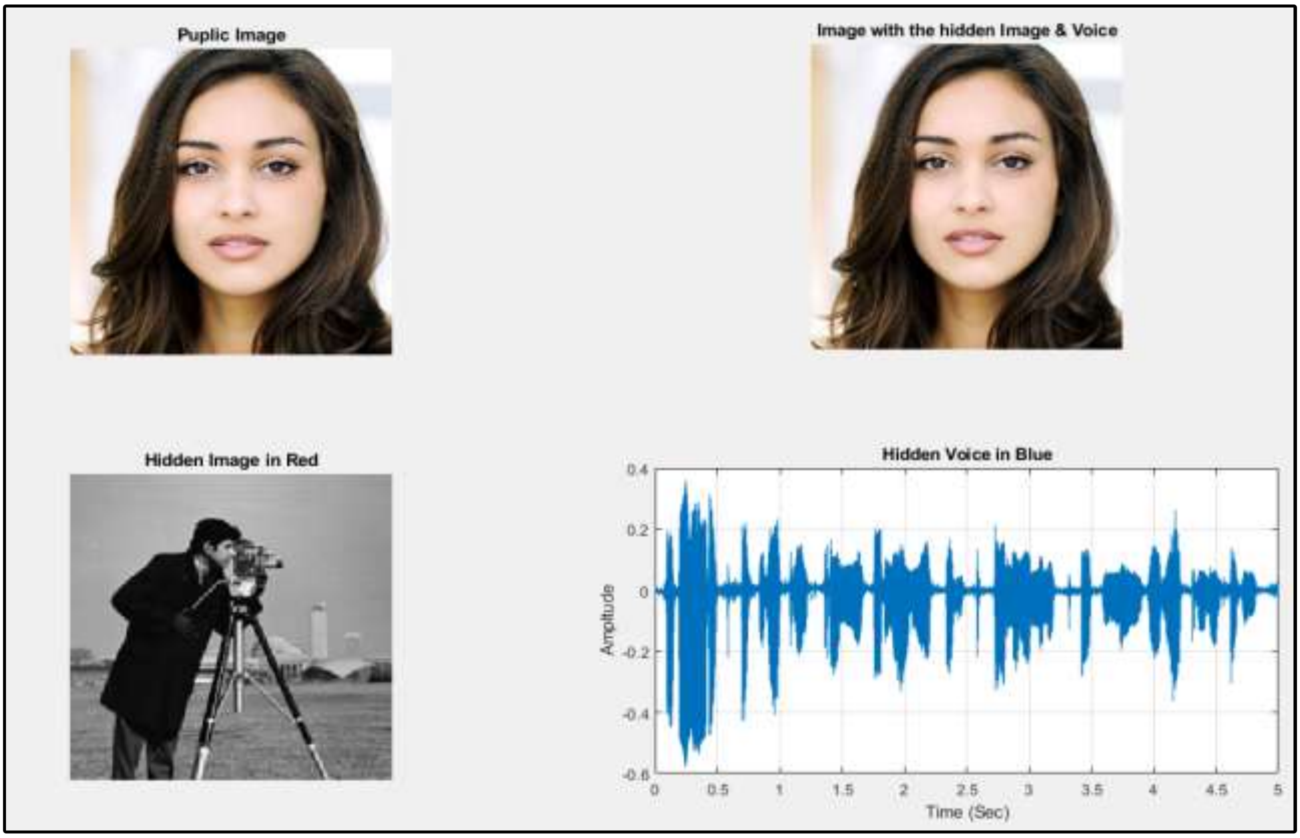
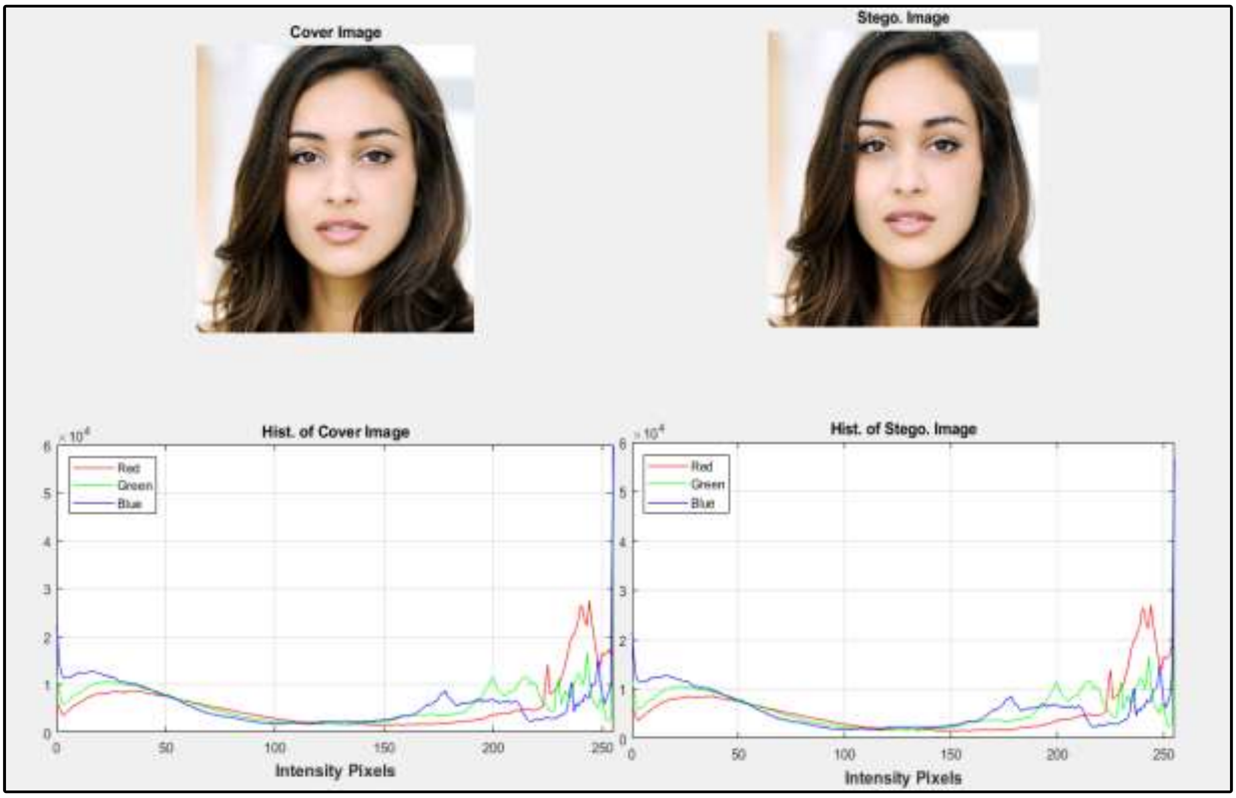


Figure (4.6): Result of steganography

Figure (4.6) shows the extent of the change in the cover image after hiding the data. Changes in the cover are imperceptible and invisible to the human eye. This indicates that the proposed system is effective and does not arouse the suspicion of hackers that there is data hidden in the available cover image.In addition that, Figure (4.7) proves the amount of congruence between the two images. It also shows that the change in the histogram between the original image and the stego image is indistinguishable.



Figure(4.7): The results of hiding the secret audio and secret image inside the cover image.

It can be concluded that the masking process proposed in this algorithm is very effective and it is difficult for the hacker to sense the presence of hidden data inside the envelope.

After presenting the results that proved the effectiveness of the proposed system in the stage of hiding information. A set of secret images and secret sounds of different sizes will be used and included inside a cover image of size (512 * 512). Table (4.4) shows the most important results obtained.

Table(4.4): Results of stego images

DIMESION OF SECRET IMAGE	SIZE OF AUDIO FILE	STEGO IMAGE		
		MSE	PSNR	SSIM
32*32	8kB	0.0828	58.952	0.99996
32*64	10KB	0.101	57.85	0.99995
192*192	16KB	0.2427	54.43	0.99988

Since (MSE) it has values <1 and values (SSIM) that are very close to 1 it means that the distortion that occurred on the cover image after including confidential data is very little and cannot be easily sensed.

After showing the results of the Stego image in Table (4.4), the Stego image is sent over the public channel and received by the recipient. To stabilize the efficiency of the system, the received data must be similar to the transmitted data. On the receiving side, secret images and secret voices are received only by those who know the key, which only the sender knows. To test the efficiency of the proposed system, the data received should be the same as the data sent, with no distortion or loss. Figure (4.8) shows that the received secret image is the same as the transmitted image and hasn’t any change.

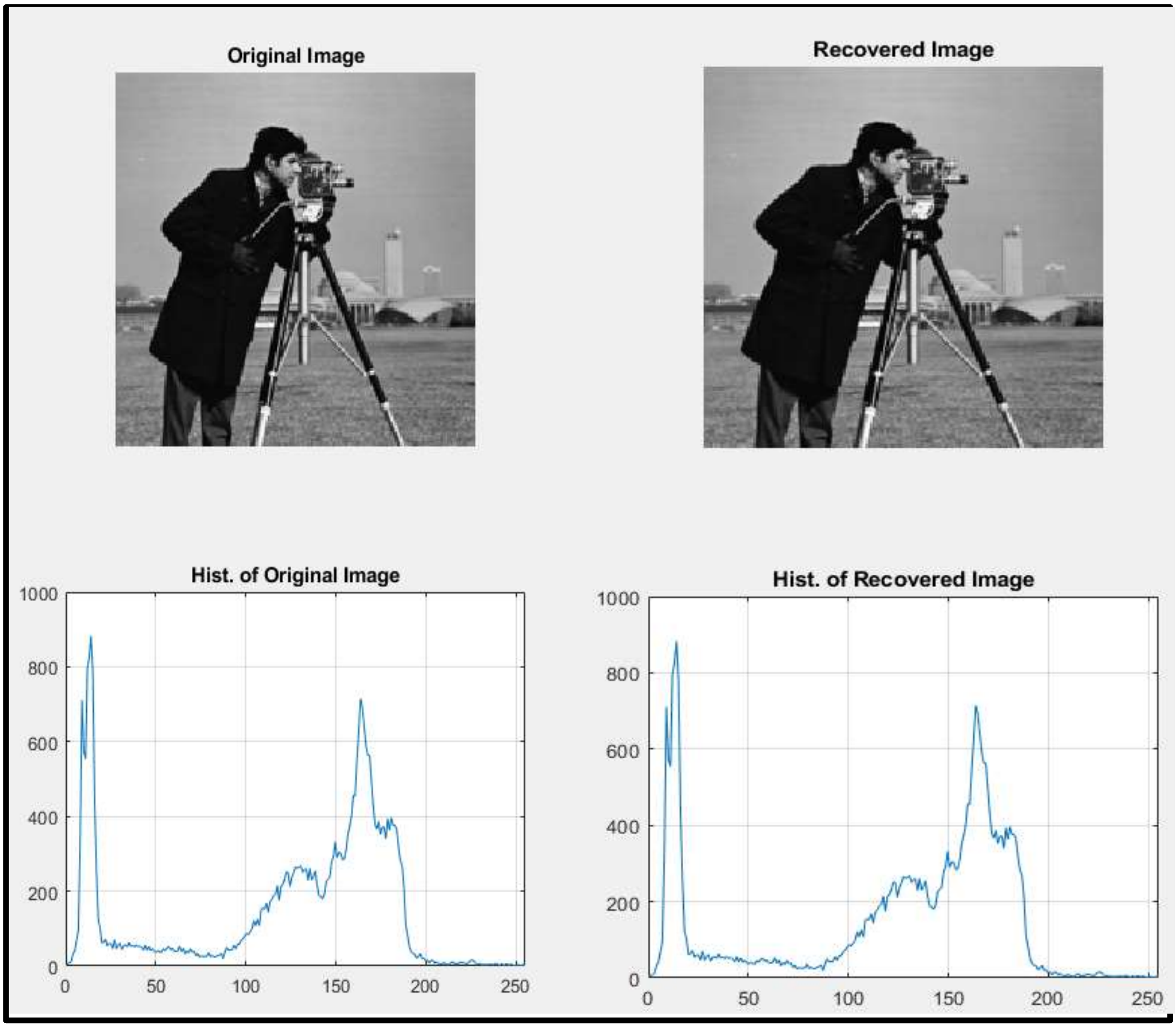


Figure (4.8): The received image histogram compared to the histogram of the original image.

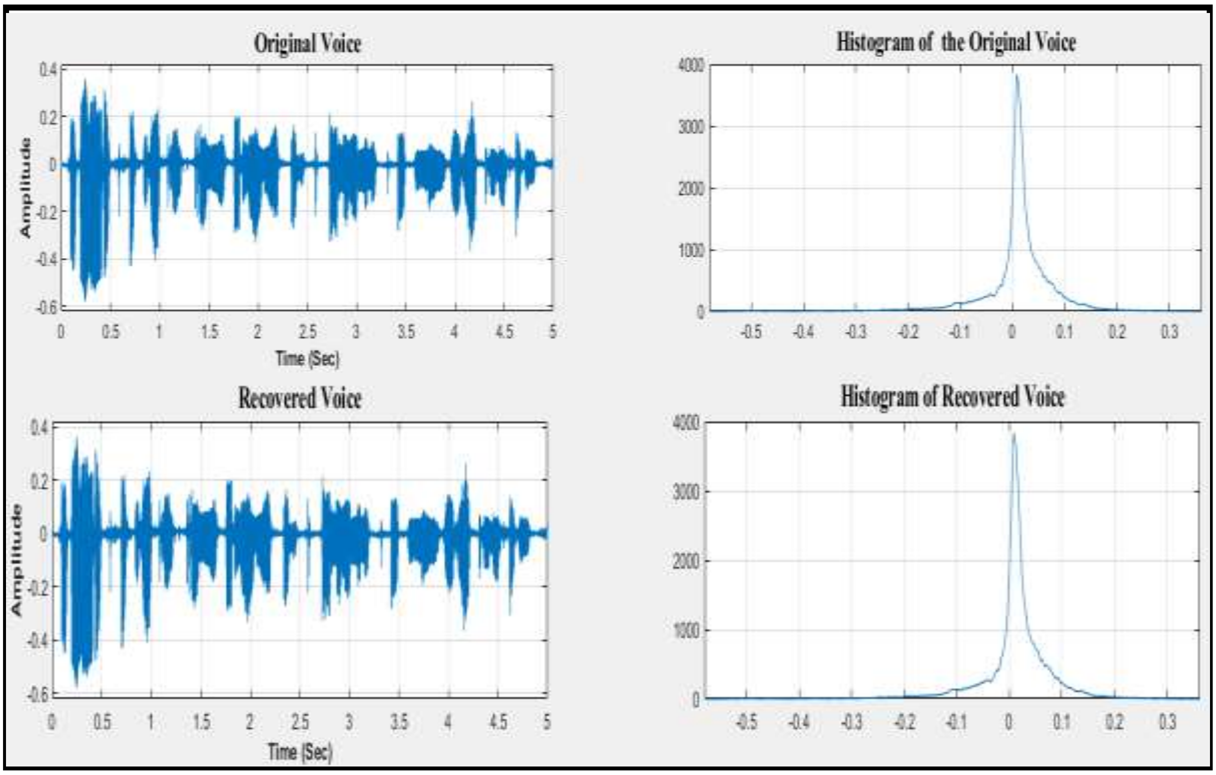
In addition to what was shown in figure which clarify the different between histogram. Table (4.5) presents the results obtained from comparing the sent and received image. The table has proven the effectiveness of the proposed algorithm in maintaining the confidentiality of information when it is sent and received without any loss or distortion, and this is one of the basics that must be available in any approved security system.

Table(4.5) Result of different recover image.

Dimension of the secret image	**RECOVER IMAGE**		
	PSNR	MSR	SSIM
32*32	**inf**	**0**	**1**
32*64	**Inf**	**0**	**1**
192*192	**Inf**	**0**	**1**

The results obtained and shown in Table(4.5) are the result of comparing the sent secret image with the received image. These values proved the effectiveness of the proposed algorithm in maintaining the confidentiality of information when sending and receiving it without any loss or distortion, and this is one of the basic conditions that must be provide in any approved security system.

After the system has proven its effectiveness in preserving the sent secret image and receiving it without any change. Its efficiency must be tested in preserving the sent secret voice and its arrival at the receiving destination without change or loss. The mechanism of testing the system was done by visual comparison, as shown in Figure (4.9). To prove more, this process was carried out through the values presented in Table (4.6) which resulting from the comparison of the sound before sending and the sound received.



Figure(4.9): Histogram of original voice and recovered voice.

Figure (4.9) proves that the transmitted sound reaches the recipient in a clear and understandable way. The change in the sound is almost imperceptible.

Table(4.6): Result of different recover audio.

File size (wav)KB	**RECOVER AUDIO**			
	SSSNR	LPC	CD	MSE
8kB	**51.287**	**-18.82**	**-5.81**	**1.58644e-07**
10kB	**51.3**	**-18.81**	**-5.81**	**1.586424e-07**
16Kb	**72.34**	**-59.14**	**-22.095**	**3.87716e-11**

Through the values presented in Table (4.6) it has been proven that the sound reaches the transmitter with a very small loss, where the displayed values are as close as possible to the standard values and the small difference does not really affect the quality of the received sound and it can be bypassed by adding filters to get rid of the noise that causes this

4.4.3 Keys Used

For secure systems, the key space must be large enough to ensure that brute force attacks are not practical. The longer the key, the longer it takes an attacker to perform a file brute force attack. If an attacker attempts to decrypt the system using all possible key combinations, it will increase dramatically.. Well thought out. Parameters A = 2313, B = 33311 and C = 43312 were used as secret keys when using Modify Arnold Cat Map (MACM) to encrypt the audio. The parameters were used as secret keys for the sender and receiver when encrypting and steganography the audio using the Duffing Map. Table (4.7) shows the response of the system to any change occurs in the key used.

Table(4.7): Result of different recover when change encryption parameter.

Scheme	Encryption parameters	Decryption parameters	Result of recover

Scheme1	a=2.75
	b=-0.15
		a=2.69999
		b=0.15
			fail

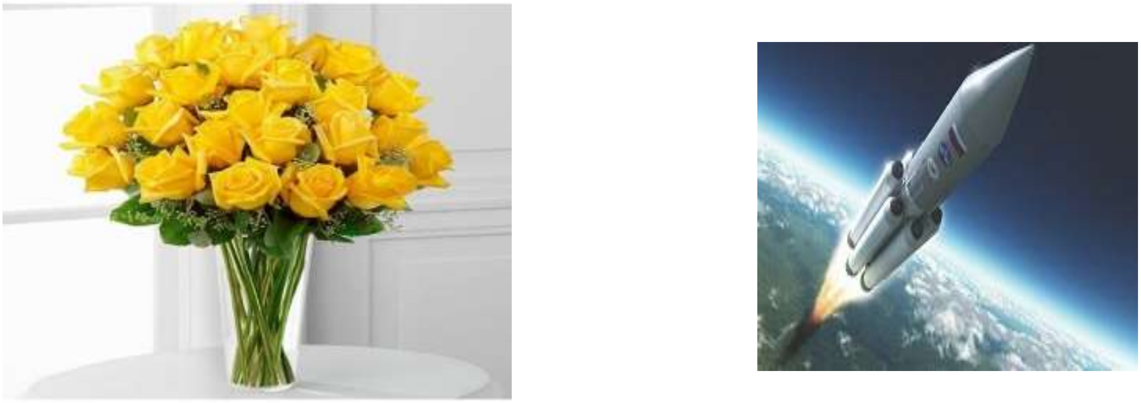
Scheme2	a=2.75
	b=-0.15
		a=2.75
		b=-0.15
			Successful

Scheme3	A=2313,
	B=33311
	C=43312
		A=2312999,
		B=33311
		C=43312
			fail

Scheme4	A=2313,
	B=33311
	C=43312
		A=2313,
		B=33311
		C=43312
			successful

As mentioned, the cryptographic key is very sensitive in a secure multi-level security based on chaos. In other words, if a hacker wants to hack the system and steal data, he must know the exact value of the parameters, and if even a small percentage makes a mistake, the results will be wrong . This means that the attack has failed. Table(4.7) clearly shows that the recovery result is successful only if the password is exactly the same on both sides and even a small change will cause the recovery to fail **.**

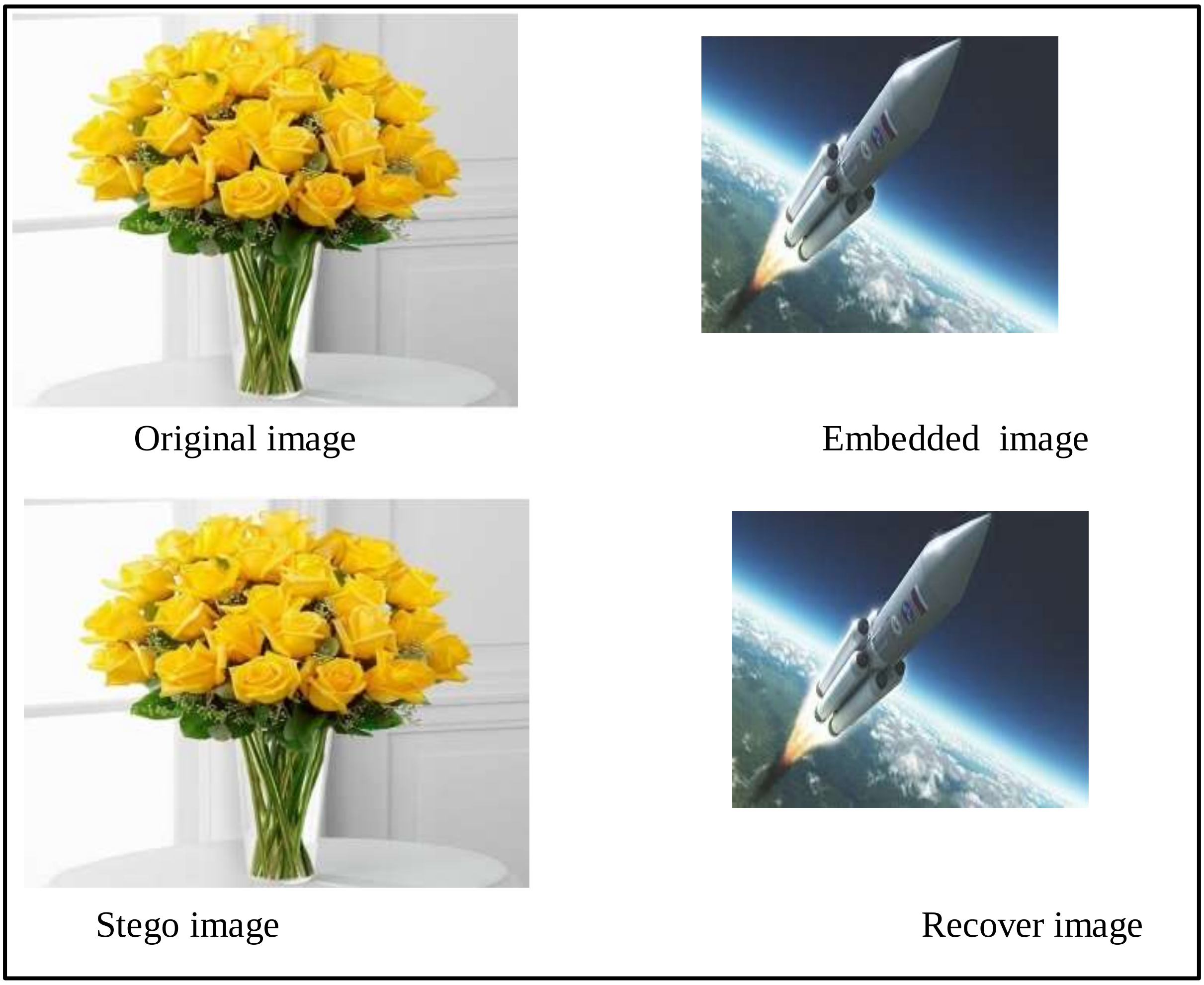
Figure (4.10) is an example to illustrate the effect of the change in the key on the quality of the received information. It displays the cover image and the secret image that is hidden inside the cover



Original image Embedded image

Figure(4.10) : Original image and embedded image.

A secret colored image was used to test the effect of the key upon receipt. Figure(4.11) shows that the sent image can be received when entering the same parameter values used where (**Initial condition** :X=-1 **;***Y=0.5); (**parameter** $\delta =$ 2.75, γ =2;)*was entered upon receipt. They are the same as those set by the sender and represented as secret keys



Original image

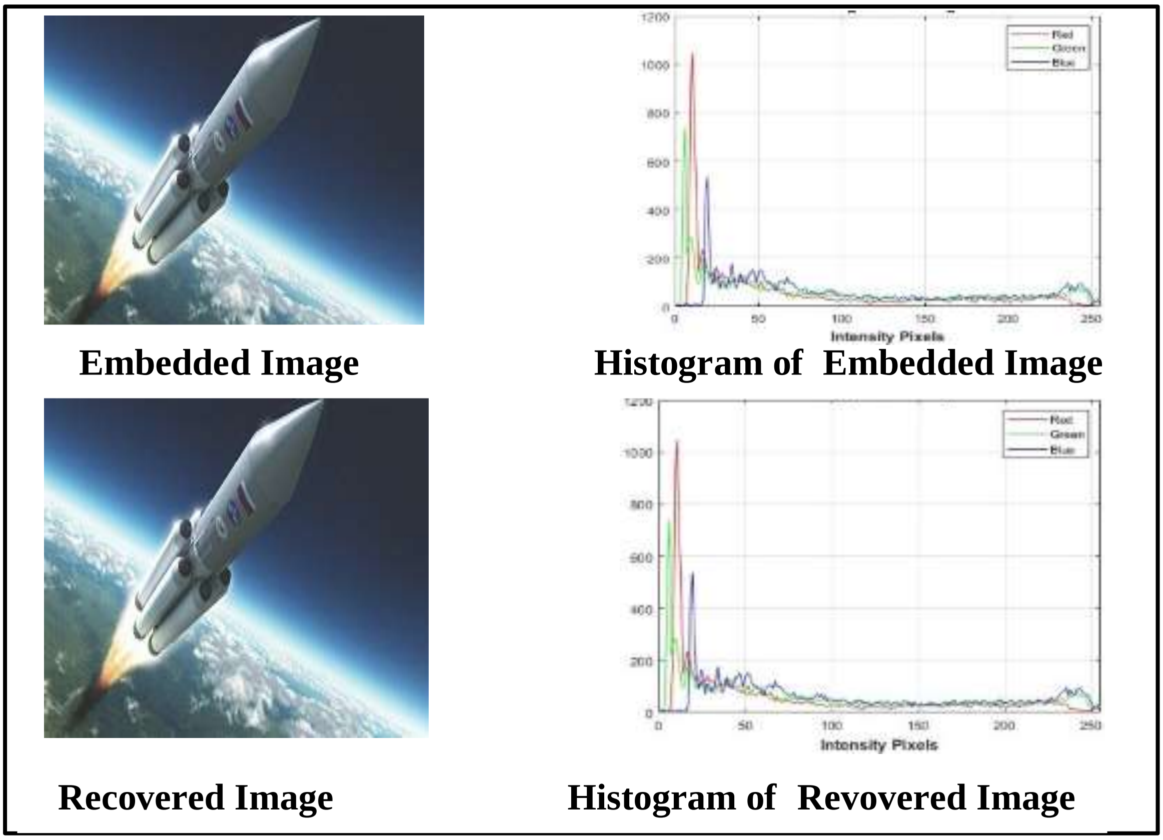
Embedded image

Stego image

Recover image

Figure (4.11): Result of the operation without any change in the parameter values.

In order to ensure that the information sent can be retrieved when using the same secret key, this is done by comparing the histogram of the information sent and received, and this is shown in the Figure(4.12)



Embedded Image **Histogram of Embedded Image**

Recovered Image **Histogram of Revovered Image**

Figure(4.12): Histogram of secret image and recovered image when used the same key in encryption and decryption.

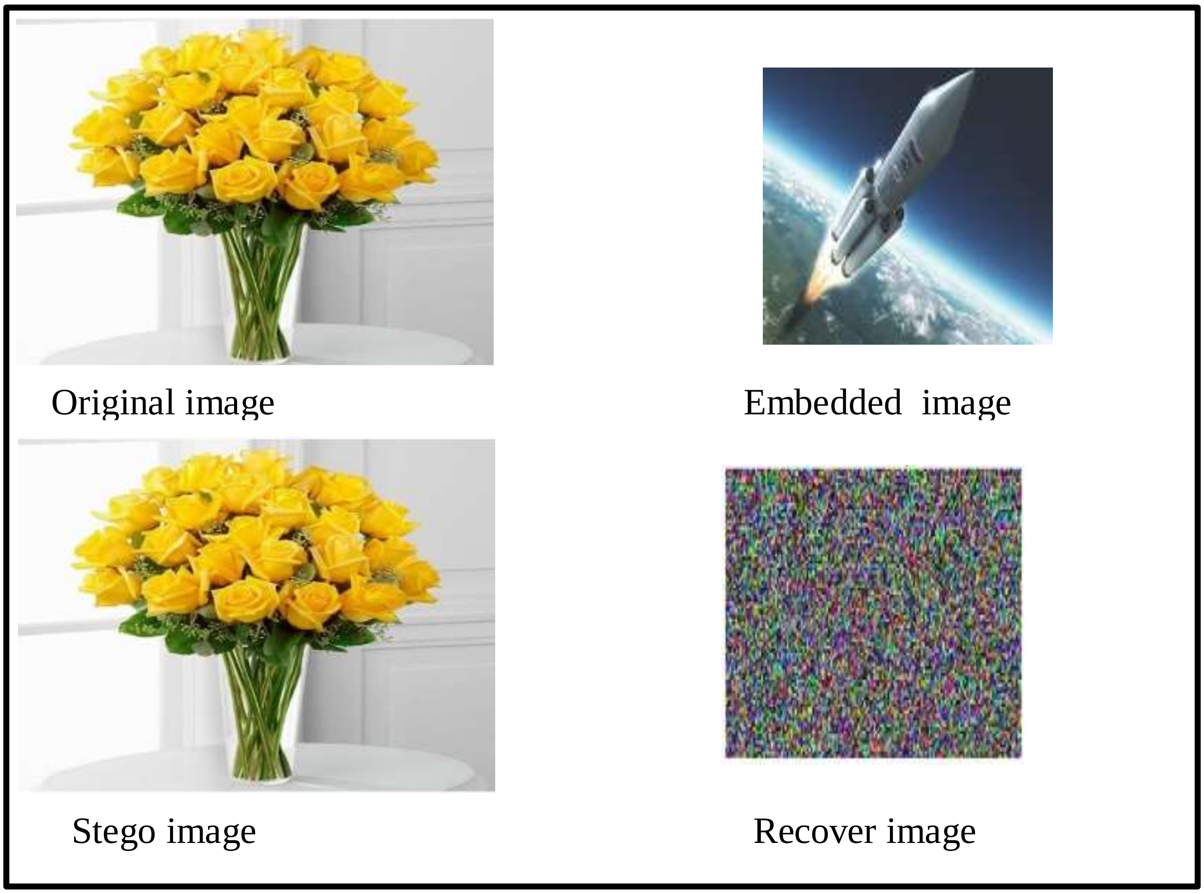
Figure(4.12)proved that the histograms of both images are exactly the same, and the image received is the same as sent

In addition to the above results. Table (4.8) proved the received image is the same as the sent image when the secret key known to the sender is used without any change in it.

Table(4.8): Result of recover image quality.

Parameters measuring of recovered image quality	PSNR	SSIM	MSE
Value	**INF**	**100%**	**0**

In order to prove the sensitivity of the keys to any change, even if it was slight. One of the parameters used has been changed by (0.000001) which is almost very slight and ineffective. But it led to completely different results. Figure (4.13) illustrates the effect of that change that occurred in one of the parameters used as secret keys



Original image

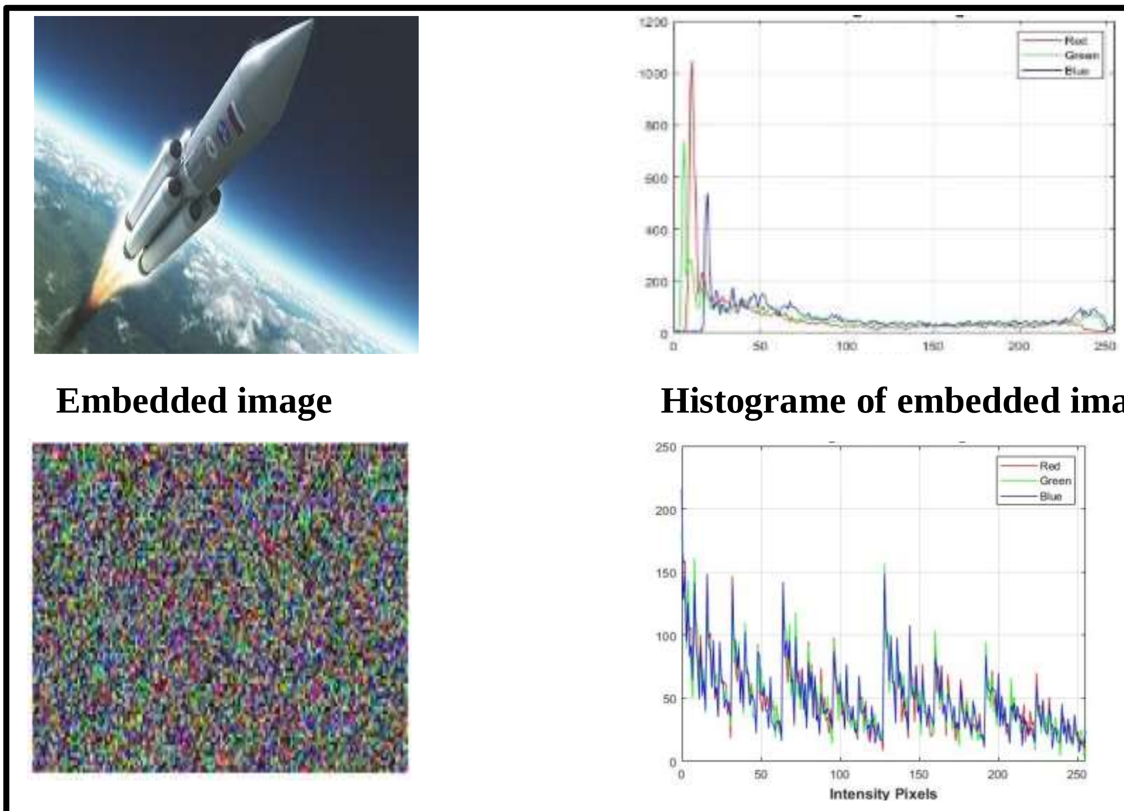
Embedded image

Stego image

Recover image

Figure (4.13) :The difference between the sent image and the received image when changing the values of the secret key at the receiving point

In addition to that, Figure (4.14) shows the extent of the change that occurs in the histogram of the received image, which means that the values of bits change when the values of the key change, even if the change is very small, and this was clarified in paragraph (4.3) of this chapter.



Embedded image **Histograme of embedded image**

Recovered embedded image **Histograme of embedded image**

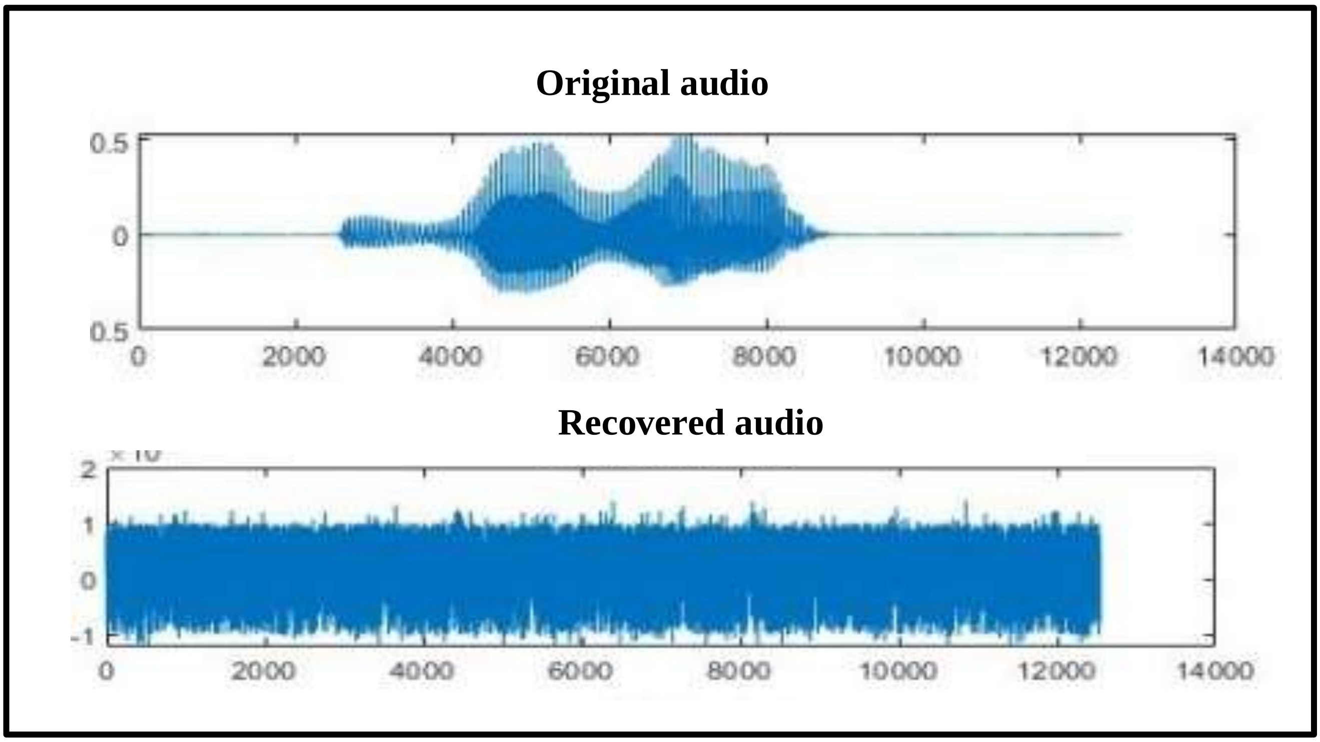
Figure(4.14): Histogram of the secret image after a change in the secret key values

In addition to the results that were explained, which showed the difference between the histogram of the received secret image and the histogram of the sent secret image. Table (4.9) shows the values of the results obtained by comparing the received image with the sent image when a change in the secret key occurred by (0.000001).

Table(4.9): Result of recover image quality when change in the value of secret key

Parameters measuring of recovered image quality	PSNR	SSIM	MSE
value	38.54	20%	0.967

After displaying the images and the effect of the key on obtaining the results, the Figure (4.15) shows the extent of the change that occurs on the sound when the key is changed by (0.000001).


Original audio

Recovered audio

Figure(4.15) : Recover audio when a change in the value of the secret key occurs

It can be concluded that the effectiveness of the chaotic functions that were adopted in maintaining secret messages and their extreme sensitivity to changes in the initial condition and parameters made them add a level of security to the proposed system

4.5 The Results of the Second Proposed Algorithm

The second algorithm, similar to the first algorithm, consists of several levels of security, the main of which are encryption and steganography. The results of this proposed method were presented and detailed in the same way that was followed in the first methodology. In the first, the results of audio coding were clarified when using (Duffing chaotic map) and then followed by those of image coding when applying (MACM).

4.5.1 Encryption Result.

This section contains the coding results of the second algorithm developed. The same confidential data used to test the efficiency of the first algorithm is used. Here, the result of the encoding process is divided into two parts. The first includes the result of encoding a secret sound using (Duffing map). The second part contains the result obtained by encoding the secret image based on the use of (MACM).

The voice here is used within the results display of the first algorithm, As shown in Figure (4.2) .Here the results obtained when encoding the audio by using duffing map will be displayed. Table (4.10) presents the results of audio coding obtained after applying the second proposed algorithm on it.

Table (4.10):Result of voice when encrypted it by using (Duffing map).

SSSNR(dB)	LPC	CD	MSE
-12.347	16.19	7.135	0.21

The results obtained and shown in Table (4.10) also confirm the effectiveness of the second algorithm in the audio encoding process. Here, the amount of MSE is high, which means that the encryption mechanism used is effective. Also, the LPC values through their displayed values prove the efficiency of the proposed algorithm in encryption. As the higher the LPC values, it confirms the extent to which the parameters of the original secret data are hidden, that is, the increased hash resulting from the proposed encryption algorithm. After that, the efficiency of this algorithm is tested in encrypting the secret image. Here the same secret image that was used in the first algorithm shown in Figure (4.4) is used. Table (4.11) shows the results of encryption images which have different size by using MACM.

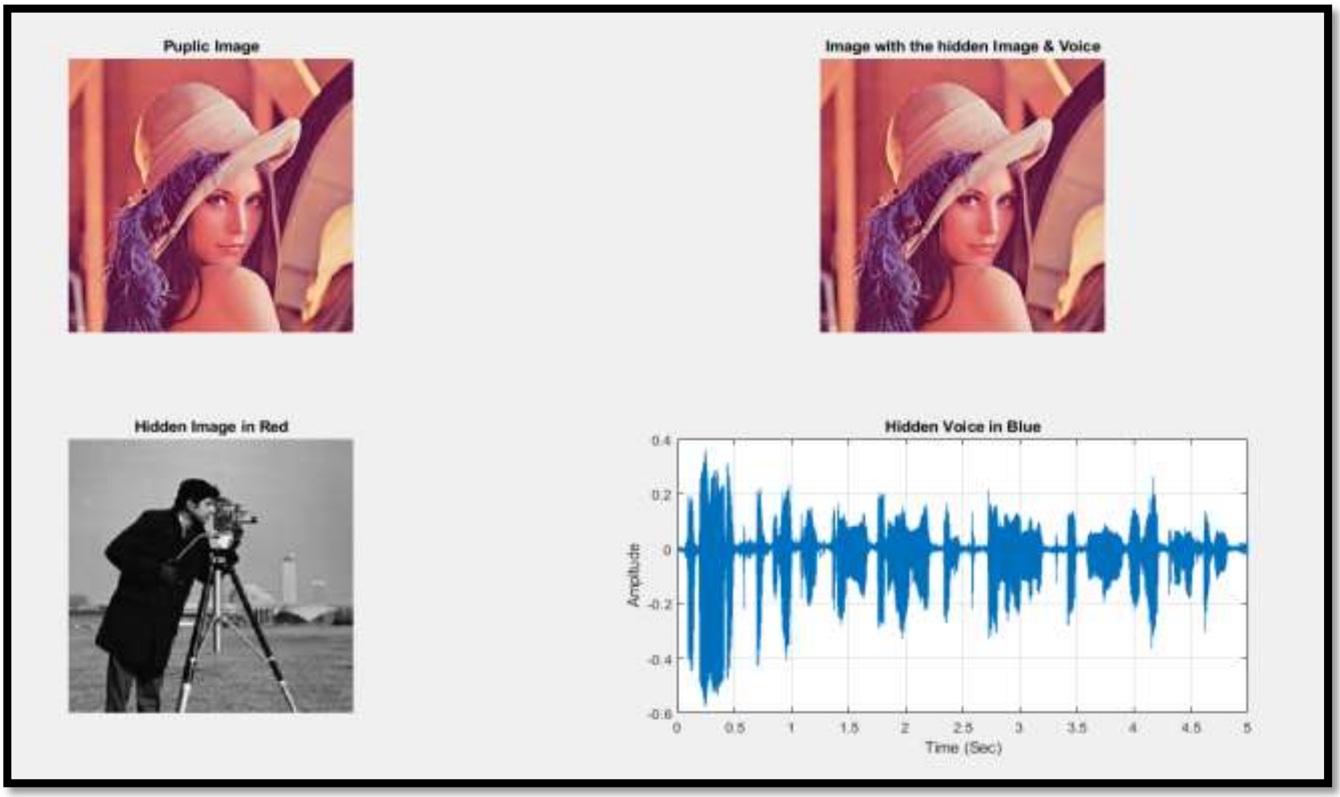
Table(4.11): Results of encryption images by using Duffing chaotic map.

Dimension of the secret image	**ENCRYPTION IMAGE**		
	MSE	PSNR	SSIM
32*32	**6.702**	**3.41**	**8.56 e+03**
32*64	**8.213**	**3.01**	**9.21e+03**
192*192	**8.521**	**3.801**	**9.45e+03**

Table (4.11) proves the success of the second proposed algorithm by encrypting secret images that have different sizes and this is similar to what happened in the first algorithm .Where the amount of similarity between the secret image before encryption and the image generated by the encryption process is very little, < 1. Also, the PSNR values are very few. The MSE is high, meaning the original bits are completely scattered, which proves the success of the proposed encryption mechanism. After completing the presentation of the coding results for the second method, the results for steganography were presented,

4.5.2 Steganography Results

The other security level after encryption is steganography. At the hidden stage, the proposed system should provide the highest similarity between the cover image and the stego image. That is, it shouldn’t carry any alteration or distortion. So as not to arouse the hacker's suspicion of the existence of hidden data and thus attempt to recover it. Figure (4.16) shows the effect of steganography on the cover image when adopting the second algorithm The results of the efficiency test of the second algorithm were done using a cover image that differs from the one that was applied in the first algorithm, and the reason behind this is for the purpose of distinguishing between them, as this



does not affect because the size of the cover in both algorithms is equal.

Figure (4.16) : Steganography result when applying the second algorithm.

Figure (4.16) proves that the Stego image does not differ from the cover image and does not arouse the suspicion of the existence of data hidden by hackers .Since there is no difference in the images displayed using the two algorithms, it is actually necessary to display the parameter values of the second algorithm. To ensure that both methods are effective and adopted as a multi-level security system. Table (4.12) displays the results of masking for a different set of images used as secret message.

Table (4.12) : Result of steog image for second algorithm.

DIMESION OF SECRET IMAGE	SIZE OF AUDIO FILE	STEGO IMAGE		
		PSNR	MSE	SSIM
32*32	**64KB**	**68.97**	**0.0076**	**0.915**
32*64	**44KB**	**59.9796**	**0.0057**	**0.987**
192*192	**25KB**	**63.972**	**0.0203**	**0.996**

Table (4.12) also proves that the second algorithm is efficient, as the similarities between the stego image and the cover image are very large and the change is almost neglected and cannot be seen by the human visual system, which makes it difficult for the hacker to sense the presence of any hidden data. Whereas, the SSIM values, resulting from comparing the original cover image with the stego image, are very high, as close to 1. While the MSE values are very little because the change in bits is very small.

In addition to everything that was mentioned to prove that the cover pictures are not affected much by hiding the data inside them. The Figure (4.17) adds another proof to this, as the histogram of the cover picture is very similar to the histogram of the stego picture and the change is almost indistinguishable.

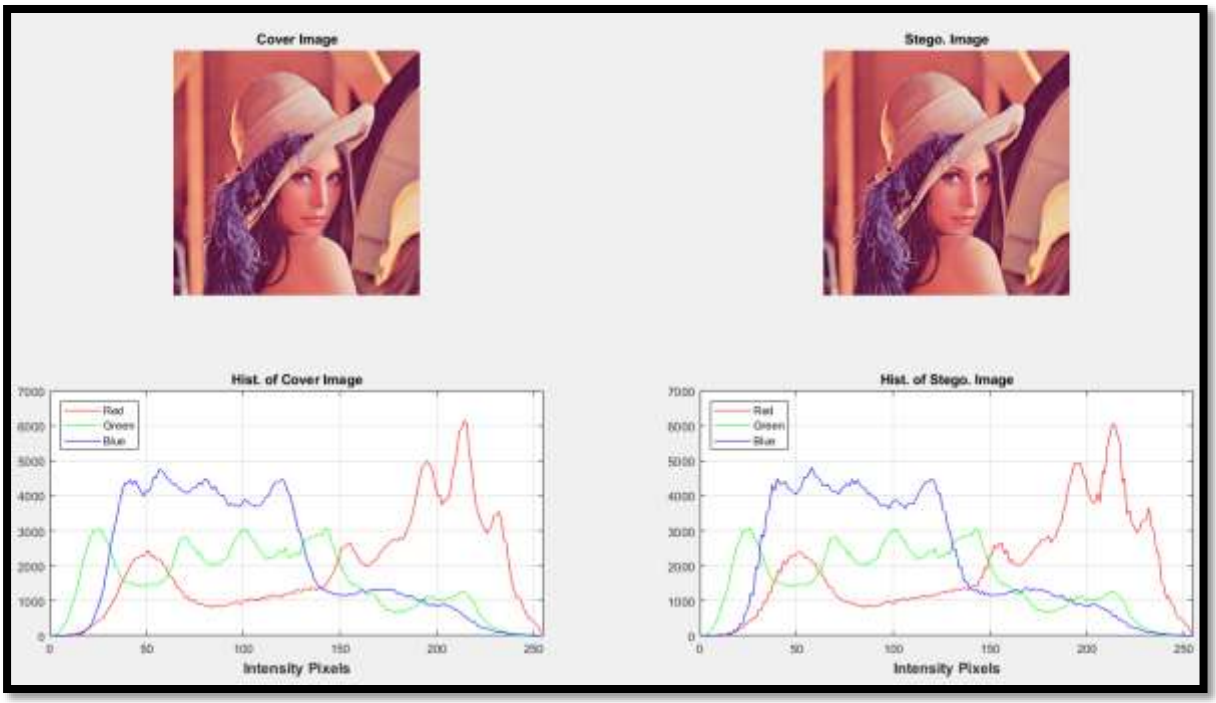
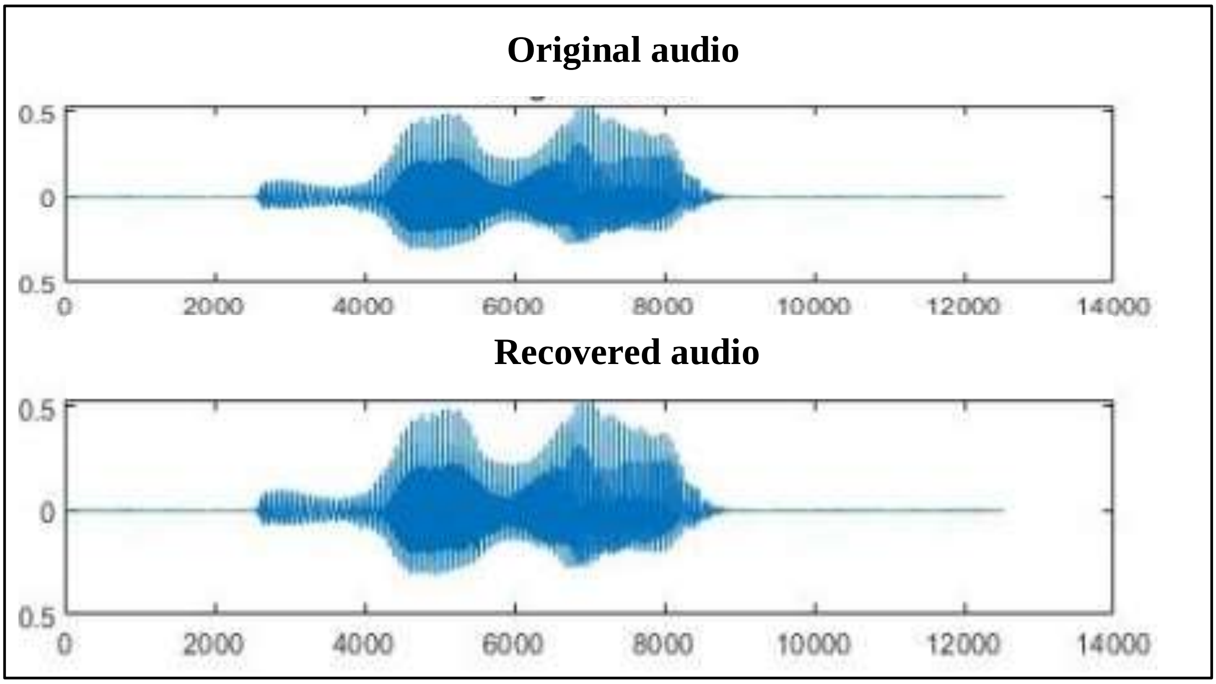


Figure (4.17): The similarity between the histogram of the original image and the Stego image.

In addition, the results will be divided into two parts, one for the secret audio sent and comparing it with the received audio, and another for the images.

Initially, the test will be conducted on the sound. Figure (4.18) shows that the retrieved sound is the same as the transmitted sound.



Figure(4.18): Recover audio for second algorithm**.**

In Figure (4.18) a sound volume (24.5kB) was used for this test. The figure proves that through the human visual system it is not possible to detect any difference between the transmitted sound and the received sound, but to make sure of this, measurements will be made to find the difference between the received and the original sound. Table (4.13) shows the most important results obtained for a group of sounds of different sizes, which are the same ones that were used in the first algorithm and gave specific results that were presented in the Table (4.5)

Table(4.13): Result of different recover audio for second algorithm used.

File size (wav)KB	**RECOVER AUDIO**			
	SSSNR	LPC	CD	MSE
24.5KB	**67.98**	**-67.78**	**-32.412**	**5.5584 e-10**
44KB	**77.914**	**-54.99**	**-27.89**	**4.987 e-12**
8khz	**70.544**	**-53.63**	**-23.919**	**2.57299e-11**

Table (4.13) shows that the retrieved sound is very similar to the transmitted sound with a slight difference that is almost indistinguishable. This is explained in the values presented in the table, where SSNR is within a high range and MSE<1, after the completion of proving the efficiency of the second algorithm in saving and receiving the secret voice without any distortion or loss. Then the same test was applied to the secret image. The table shows the results that were reached after decoding and cryptanalysis as shown in Table (4.14).

Table(4.14) Result of different recover image for the second algorithm

Dimension of the secret image	**RECOVER IMAGE**		
	PSNR	MSR	SSIM
32*32	**inf**	**0**	**1**
32*64	**Inf**	**0**	**1**
192*192	**Inf**	**0**	**1**

Table (4.14) shows that the received images are similar to the sent images without any difference at all. It confirms the effectiveness of the second algorithm in ensuring that the confidential data reaches the receiving side safely and without any loss. This is shown in the results where the ssim values resulting from comparing the secret image with the retrieved image are exactly the same, as well as MSE 0, PSNR is very high, meaning that the values are completely identical between confidentiality and retrieved

4.5.3 Key used

The effect of the key is exactly the same as the effect described in the first algorithm in paragraph (4.6). Therefore, it is not clarified in the result of the second algorithm.

4.6. Comparison of the two algorithms and discussion.

The goal of suggesting two algorithms,. It lies in determining the efficiency of each algorithm and adopting it as a multi-level security system. In addition, the reason behind using chaotic mutual functions in the two algorithms is due to determining the effect of the type of function used on the encryption results.

To determine the efficiency of each algorithm and adopt it as a reliable and developed security system. The three basic conditions must be met in each of them.

I. It must provide capacity to store data inside the cover without distorting the cover image

II. The transmitted data must reach the recipient without any change or loss in its characteristics

III. The stego image should be so similar to the cover image before data is hidden in it so as not to arouse the hacker's suspicion of the existence of secret data.

The results obtained from testing the two algorithms show that each of them achieved the approved conditions. In addition, the amount of difference between the results of the two algorithms is very small. All of this proves that changing the chaotic functions used in encryption does not affect the scattering of the data. The reason is that the process used in encryption is (XOR) between the values to be encrypted and the random values generated by the chaos. Therefore, changing the random values doesn’t effect on the system output, whether those values are the outcome of the MACM or Duffing chaotic map. But the purpose of changing the chaos functions is to achieve greater space key used for encryption. Increasing the number of dimensions and parameters of the chaotic function more leads to a larger key space. This makes it difficult for the hacker to retrieve the encrypted data.

4.7 Performance Of The Proposed System Under The Effect Of The Different Internet Platforms.

In this section, a measure of the efficiency of the proposed system to extract. Secret messages (audio and image) is included when Stego-image is transmitted across various Internet platform. Table (4.15) shows the efficiency of extracting the image and audio after transmitting them via the Internet service platform that used by the common peoples (social media) such as Facebook ,Email, WhatsApp, Viber and Telegram.

Table (4.15):Reliability of the proposed system to extract an embedded message from the Stego-image after transfer in the different internet platform.

Platforms	Recover image	Recover audio
@ ✓	***SUCCESSFUL***	***SUCCESSFUL***
Instagram	***FAIL***	***FAIL***
facebook	***FAIL***	***FAIL***
Viber	***FAIL***	***FAIL***
WhatsApp ✓	***SUCCESSFUL***	***SUCCESSFUL***
Telegram ✓	***SUCCESSFUL***	***SUCCESSFUL***

Table (4.15) shows the efficiency of the system in extracting the secret image and the secret audio after transferring the Stego-image to the Internet service platform. Both Email ,WhatsApp and Telegram succeeded in retrieving confidential information without any loss. The rest of the social media platforms that were clarified in the table have failed in that.

4.8 Comparison with related work

Table(4.16) presents a report of related works that described in chapter one of the security system by using chaos based on encryption and steganography .

That summary highlights each of chaos function used, Embedding technique, Stego-image quality, secret information used, etc. Compared with all techniques as depicts in the table (4.16), the experimental results prove that the suggested algorithm produces a better quality , and the MACM and Duffing map will increase the security .

and robustness in extracting a high-quality secret message , also the chaotic map works at the receiver end to estimate the correct value of secret information by eliminating the error bits that may result in the channel. Furthermore, the steganography proved another secret level to the suggested algorithm.

Table (4. 16): Comparison between related works and the proposed system

Ref	Chaos function	Embed technique	Secret message	PSNR for stego image	CD for encrypted audio-image	MSE for encryption
[3]	Logistic map.	-	Image-Audio	-	0.013-0.004	-
[4]	-	LSB	Image	53.7-53.73	-	-
[18]	Arnold cat map	LSB	Image	(43.95-45)	-	-
[19]	-	LSB	Image	44.7-44.8	-	-
[20]	MACM	Contourlet domain	Image-Text	(44.5-67)	(0.9997-1)	-
[21]	Arnold’s cat map	LSB	Image-Text	(30-51.3)	-	-
[22]	logistic chaotic map	LSB	Image	49.7-58	-	0.08-1.0
[23]	transposition technique	-	Audio	-	-	0.0000036
[24]	Lorenz chaotic	-	Audio	-	-	-
[25]	-	new Steganography technology based on secret key	Image	40.5017	-	0.6829

Ref	Chaos function	Embed technique	Secret message	PSNR for stego image	CD for encrypted audio-image	MSE for encryption
[26]	2D chaotic map known as standard map	-	Image	39.787	0.00296	-
[27]	3-D chaotic map (LCA map)	4LSB AND 4MSB	Text	39.9-48.9	-	0.99970
[28]	Hyper and Logistic Map	-	Image	-	R=−0.032 G=−0.012 B=−0.012	-
[29]	3D Logstic map	-	Image		0.0036	
[30]	3D Chebyshev and 3D logistic maps	LSB	Image	45.866	-	2.9967

Ref	Chaos function	Embed technique	Secret message	PSNR for stego image	CD for encrypted audio-image	MSE for encryption
[31]	3D Chebyshev and 3D logistic maps,	LSB	Image	45.8661	-	R=1.5877 G=1.8215 B=1.6841
[32]	5D hyper-chaotic system	LSB	Image	54.8	-	-
Proposed system	Duffing map MACM	LSB	Image Audio	57-59	0.003	0.004

As shown in Table 4.16, the proposed system succeeded in overcoming the previous systems in terms of the accuracy of the resulting stego image, which ranges between (57-59) decibels.

In addition to the high capacity to include data compared to the previous traditional methods, where each cover image has the ability to include a secret image and a secret audio without distorting the cover image. In addition to the effectiveness of the system in retrieving the secret audio and the secret message while preserving its characteristics. Also, the hiding technology used is highly efficient, as neither hacker nor external force can sense the presence of data hidden inside the cover.

Chapter Five

Conclusion and Future Works

CHAPTER FIVE

CONCLUSION AND FUTURE WORKS

5.1 Conclusions

The private security and excellent reliability of the complex system are examined under various types of direct challenges. In notable addition, from all the output results of successful tests and model simulations, it can be reasonably concluded some of the apparent points sufficiently proved the practical efficiency of the proposed system.

1. The proposed system provide the maximum possible capacity, the raw data included acute observer and the received data itself is typically transmitted without any change as seen from the results.
2. From the desired results properly obtained from cover images and various types of secret messages and secret sounds, the using of Stego image was naturally obtained with closed characteristics of the original cover image and the used correlation was extremely close to that, so it is difficult to distinguish between them.
3. Due to the high quality of the Stego image results the effective range is between (99.998-99.999)%. This is required to the complex embedding in 1 Bit LSB that is properly used in this used system. Therefore, the proposed system has merely proven to be highly efficient in intentionally deceiving the human visual system so that the human eye cannot sufficiently recognize the minor difference between the original image and the Stego-image.
4. Using the Modified Arnold Cat Map (MACM) and Duffing Chaotic Map increases the personal security of the system by operating the model parameters of this chaotic map as a secret key between the used transmitter and intended receiver.

5. The proposed algorithm is public, only the private key is kept secret, so the immune system is unbreakable. System implementation is easy, and it undoubtedly requires a short time, for hiding an image, its takes, barely 0.5 Sec., and for hiding a speech message it takes less than one second.
6. The encryption process using various Chaos functions proved that the type of the Chaotic function doesn’t affect the scattering of the secret data during encryption because the encryption process is done through (XOR) between the secret data and the random values generated by the chaotic system. But the difference lies in the (key space) which depends on the number of parameters and initial value.
7. It can be found when testing the proposed system through the internet channel that WhatsApp, Telegram and Email succeed in reconstructing the secret data while the other program failed in this mission.

5.2 Future Works

1. The effects of channel noise on the systems can be investigated.
2. Implement encryption and steganography by utilizing other distinct types of chaos instead of the (MACM) and (Duffing map), such as Chua, Lü, Logistic , Nien , Henon ,Lorenz and Rössler, etc.
3. Using the adaptive filters to typically decrease the noise effects and meaningfully improve the quality of the recovered messages.
4. After dividing the cover image into its primary colors (R,G,B) it is possible to hide part of the audio bits within the blue color and the other part within the green color and part of the image bits is hidden within the green color and the other part within the red color of the cover image. That is, naturally dividing the cover into the three colors and carefully hiding the choice bits of confidential information inside the colors and thus the private capacity can be typically increased.
5. It is possible to calculate another level of security, which is to hide the stego-image inside another cover image. The stego-image efficiently is the cover image after hiding the confidential data inside it.
6. Using AWGN and other types of channel to test the proposed system under real channel conditions

References

References

[1] W. Easttom, “Steganography,” in Modern Cryptography, Springer, 2021, pp. 337–356.

[2] R. E. Blahut, Cryptography and secure communication. Cambridge university press, 2014.

[3] S. Pramanik, R. Ghosh, D. Pandey, D. Samanta, S. Dutta, and S. Dutta, “Techniques of Steganography and Cryptography in Digital Transformation,” in Emerging Challenges, Solutions, and Best Practices for Digital Enterprise Transformation, IGI Global, 2021, pp. 24–44.

[4] A. A. Al-Ataby and F. M. Al-Naima, “High capacity image steganography based on curvelet transform,” in 2011 Developments in E-systems Engineering, 2011, pp. 191– 196

[5] N. Provos and P. Honeyman, “Hide and seek: An introduction to steganography,” IEEE Secur. Priv., vol. 1, no. 3, pp. 32–44, 2003

[6] M. Shirali-Shahreza, “Mohammad Shirali-Shahreza Computer Science Department, Sharif University of Technology, Azadi Street, Tehran, IRAN shirali@ cs. sharif. edu,” Int. J. Digit. Content Technol. its Appl., vol. 2, no. 1, 2008

[7] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, “A secure and improved selfembedding algorithm to combat digital document forgery,” Signal Processing, vol. 89, no. 12, pp. 2324–2332, 2009.

[8] S. K. Dubey and V. Chandra, “Steganography, cryptography and watermarking: A review,” Int. J. Innov. Res. Sci. Eng. Technol., vol. 6, no. 2, pp. 2595–2599, 2017

[9] K. Alla and R. S. R. Prasad, “An evolution of Hindi text steganography,” in 2009 Sixth International Conference on Information Technology: New Generations, 2009, pp. 1577–1578.

[10] H. Dutta, R. K. Das, S. Nandi, and S. R. M. Prasanna, “An overview of digital audio steganography,” IETE Tech. Rev., vol. 37, no. 6, pp. 632–650, 2020.

[11] M. Hassaballah, M. A. Hameed, and M. H. Alkinani, “Introduction to digital image steganography,” in Digital Media Steganography, Elsevier, 2020, pp. 1–15..

[12] B. Xu, J. Wang, and D. Peng, “Practical protocol steganography: Hiding data in IP header,” in First Asia International Conference on Modelling & Simulation (AMS’07), 2007, pp. 584–588.

[13] Y. Liu, S. Liu, Y. Wang, H. Zhao, and S. Liu, “Video steganography: A review,” Neurocomputing, vol. 335, pp. 238–250, 2019.

[14] H. B. Karaman and S. Sagiroglu, “An application based on steganography,” in 2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, 2012, pp. 839–843.

[15] K. B. Raja, K. R. Venugopal, and L. M. Patnaik, “High capacity lossless secure image steganography using wavelets,” in 2006 International conference on advanced computing and communications, 2006, pp. 230–235.

[16] S. I. Sowan, “Steganography For Embedding Data In Digital Image.” Universiti Putra Malaysia, 2003.

[17] S. Bhavana and K. L. Sudha, “Text Steganography using LSB insertion method along with Chaos Theory,” Int. J. Comput. Sci. Eng. Appl., vol. 2, no. 2, p. 145, 2012.

[18] B. Boulebtateche, M. M. Lafifi, and S. Bensaoula, “A multi media chaos-based encryption algorithm,” in Proc. 12th Int. Arab Conf. Inf. Technol.(ACIT), 2011.

[19] Z. Tang and X. Zhang, “Secure image encryption without size limitation using Arnold transform and random strategies,” J. Multimed., vol. 6, no. 2, p. 202, 2011.

[20] A. Kanso and H. S. Own, “Steganographic algorithm based on a chaotic map,” Commun. Nonlinear Sci. Numer. Simul., vol. 17, no. 8, pp. 3287–3302, 2012.

[21] A. Saravanan, A. Sivabalan, and R. Prabhu, “Information hiding scheme on image using contourlet wavelet transform,” Int. J. Adv. Comput. Theory Eng., vol. 2, no. 2, pp. 67– 70, 2013.

[22] M. Mishra, A. R. Routray, and S. Kumar, “High security image steganography with modified Arnold cat map,” arXiv Prepr. arXiv1408.3838, 2014.

[23] M. Bilal, S. Imtiaz, W. Abdul, S. Ghouzali, and S. Asif, “Chaos based Zerosteganography algorithm,” Multimed. Tools Appl., vol. 72, no. 2, pp. 1073–1092, 2014.

[24] A. Jawahir and H. Haviluddin, “An audio encryption using transposition method,” Int. J. Adv. Intell. Informatics, vol. 1, no. 2, pp. 98–106, 2015.

[25] H. N. Abdullah, S. S. Hreshee, and A. K. Jawad, “Design of Efficient noise reduction scheme for secure speech masked by chaotic signals,” J. Am. Sci., vol. 11, no. 7, pp. 49– 55, 2015.

[26] A. Dhamija and V. Dhaka, “A novel cryptographic and steganographic approach for secure cloud data migration,” in 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), 2015, pp. 346–351.

[27] K. Muhammad, J. Ahmad, M. Sajjad, and M. Zubair, “Secure image steganography using cryptography and image transposition,” arXiv Prepr. arXiv1510.04413, 2015.

[28] B. Mondal and T. Mandal, "A nobel chaos based secure image encryption algorithm," Int. J. Appl. Eng. Res., vol. 11, no. 5, pp. 3120–3127, 2016.

[29] A. Sharif, M. Mollaeefar, and M. Nazari, "A novel method for digital image steganography based on a new three-dimensional chaotic map," Multimed. Tools Appl., vol. 76, no. 6, pp. 7849–7867, 2017.

[30] C. Fu, G. Zhang, M. Zhu, Z. Chen, and W. Lei, "A new chaos-based color image encryption scheme with an efficient substitution keystream generation strategy," Secur. Commun. Networks, vol. 2018, 2018.

[31] C. Li, G. Luo, and C. Li, "An Image Encryption Scheme Based on The Threedimensional Chaotic Logistic Map.," Int. J. Netw. Secur., vol. 21, no. 1, pp. 22–29, 2019.

[32] M. Y. T. Irsan and S. C. Antoro, "Text encryption algorithm based on chaotic map," in Journal of Physics: Conference Series, 2019, vol. 1341, no. 6, p. 62023.

[33] A. ALabaichi, M. A. A. K. Al-Dabbas, and A. Salih, "Image steganography using least significant bit and secret map techniques.," Int. J. Electr. Comput. Eng., vol. 10, no. 1, 2020.

[34] M. Ahmad, B. Alam, and O. Farooq, "Chaos based mixed keystream generation for voice data encryption," arXiv Prepr. arXiv1403.4782, 2014.

[35] A. Yahya, "Steganography techniques," Steganography Tech. Digit. Images, pp. 9–42, 2019.

[36] G. J. Simmons, "The prisoners' problem and the subliminal channel," in Advances in Cryptology, 1984, pp. 51–67.

[37] K. M. Hosny, Multimedia security using chaotic maps: principles and methodologies, vol. 884. Springer Nature, 2020.

[38] M. M. S. Rani, G. G. Mary, and K. R. Euphrasia, “Multilevel multimedia security by integrating visual cryptography and steganography techniques,” in Computational intelligence, cyber security and computational models, Springer, 2016, pp. 403–412.

[39] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran, “Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research,” Neurocomputing, vol. 335, pp. 299–326, 2019.

[40] A. Pradhan, A. K. Sahu, G. Swain, and K. R. Sekhar, “Performance evaluation parameters of image steganography techniques,” in 2016 International Conference on Research Advances in Integrated Navigation Systems (RAINS), 2016, pp. 1–8.

[41] J. Fridrich, P. Lisoněk, and D. Soukal, “On steganographic embedding efficiency,” in International Workshop on Information Hiding, 2006, pp. 282–296.

[42] L. J. Sheu, “A speech encryption using fractional chaotic systems,” Nonlinear Dyn., vol. 65, no. 1, pp. 103–108, 2011.

[43] R. Gnanajeyaraman and K. Prasadh, “Audio encryption using higher dimensional chaotic map,” Int. J. Recent Trends Eng., vol. 1, no. 2, p. 103, 2009.

[44] Z. Su, G. Zhang, and J. Jiang, “Multimedia security: a survey of chaos-based encryption technology,” Mutimedia A Multidisiplinary Approach to Complex Issues, Ed. I. Karydis, InTech, pp. 99–124, 2012.

[45] G. R. Bagwe, D. S. Apsingekar, S. Gandhare, and S. Pawar, “Voice encryption and decryption in telecommunication,” in 2016 International Conference on Communication and Signal Processing (ICCSP), 2016, pp. 1790–1793.

[46] S. Shaerbaf and S. A. Seyedin, “A secure chaos-based communication scheme in multipath fading channels using particle filtering,” Iran. J. Electr. Electron. Eng., vol. 8, no. 1, pp. 1–9, 2012.

[47] H.-N. Wang, W. Zhong, J. Wang, and D. XIA, “Research of measurement for digital image definition,” J. Image Graph., vol. 9, no. 7, pp. 828–831, 2004.

[48] M. T. Parvez and A. A.-A. Gutub, “RGB intensity based variable-bits image steganography,” in 2008 IEEE Asia-Pacific Services Computing Conference, 2008, pp. 1322–1327

[49] D. Neeta, K. Snehal, and D. Jacobs, “Implementation of LSB steganography and its evaluation for various bits,” in 2006 1st international conference on digital information management, 2006, pp. 173–178.

[50] K. Praghash, C. Vidyadhari, G. NirmalaPriya, and R. Cristin, “Secure information hiding using LSB features in an image,” Mater. Today Proc., 2021.

[51] I. Avcibas, N. Memon, and B. Sankur, “Steganalysis using image quality metrics,” IEEE Trans. Image Process., vol. 12, no. 2, pp. 221–229, 2003.

[52] N. Sethi and D. Sharma, “A new cryptology approach for image encryption,” in 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing, 2012, pp. 905–908.

[53] A. K. Mandal and C. Parakash, “Mrs. Archana Tiwari-‘Performance Evaluation of Cryptographic Algorithms: DES and AES’, IEEE Student’s Conference on Electrical,” Electron. Comput. Sci. IEEE, 2012

[54] B. Applebaum, B. Barak, and A. Wigderson, “Public-key cryptography from different assumptions,” in Proceedings of the forty-second ACM symposium on Theory of computing, 2010, pp. 171–180

[55] S. Dhull, S. Beniwal, and P. Kalra, “Polyalphabetic Cipher Techniques Used For Encryption Purpose,” Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 3, no. 2, pp. 64– 66, 2013.

[56] M. Hell, T. Johansson, A. Maximov, and W. Meier, “A stream cipher proposal: Grain128,” in 2006 IEEE International Symposium on Information Theory, 2006, pp. 1614– 1618.

[57] A. J. Abd and S. T. F. Al-Janabi, “Classification and Identification of Classical Cipher Type using,” J. Eng. Appl. Sci., vol. 14, no. 11, pp. 3549–3556, 2019.

[58] A. Kahate, Cryptography and network security. Tata McGraw-Hill Education, 2013.

[59] G. Bard, Algebraic cryptanalysis. Springer Science & Business Media, 2009.

[60] L. Tosi, “‘ Then Rose the Seed of Chaos’: Masque and Antimasque in The Dunciad in Four Books,” Stud. Lit. Imagin., vol. 38, no. 1, p. 197, 2005.

[61] X. Zeng, R. A. Pielke, and R. Eykholt, “Chaos theory and its applications to the atmosphere,” Bull. Am. Meteorol. Soc., vol. 74, no. 4, pp. 631–644, 1993.

[62] A. Atangana and I. Koca, “Chaos in a simple nonlinear system with Atangana–Baleanu derivatives with fractional order,” Chaos, Solitons & Fractals, vol. 89, pp. 447–454, 2016.

[63] G. L. Baker and J. P. Gollub, Chaotic dynamics: an introduction. Cambridge university press, 1996.

[64] A. Serletis and P. Gogas, “Chaos in East European black market exchange rates,” Res. Econ., vol. 51, no. 4, pp. 359–385, 1997.

[65] A. Serletis and P. Gogas, “The North American natural gas liquids markets are chaotic,” energy J., vol. 20, no. 1, 1999.

[66] B. Jovic, Synchronization techniques for chaotic communication systems. Springer Science & Business Media, 2011.

[67] B. Jovic, “Chaotic Synchronization, Conditional Lyapunov Exponents and Lyapunov’s Direct Method,” in Synchronization Techniques for Chaotic Communication Systems, Springer, 2011, pp. 49–78.

[68] J. Hite Jr, Learning in chaos. Routledge, 2009.

[69] E. N. Lorenz, “Deterministic nonperiodic flow,” J. Atmos. Sci., vol. 20, no. 2, pp. 130– 141, 1963.

[70] M. Moghtadaei and M. R. H. Golpayegani, “Complex dynamic behaviors of the complex Lorenz system,” Sci. Iran., vol. 19, no. 3, pp. 733–738, 2012.

[71] M. S. Willsey, K. M. Cuomo, and A. V Oppenheim, “Selecting the Lorenz parameters for wideband radar waveform generation,” Int. J. Bifurc. chaos, vol. 21, no. 09, pp. 2539–2545, 2011.

[72] A. Sambas and M. S. WS, “Halimatussadiyah, Unidirectional chaotic synchronization of Rossler circuit and its application for secure communication,” WSEAS Trans. Syst., vol. 9, no. 11, pp. 506–515, 2012.

[73] O. E. Rössler, “An equation for continuous chaos,” Phys. Lett. A, vol. 57, no. 5, pp. 397– 398, 1976.

[74] L. O. Chua, The genesis of Chua’s circuit. Electronics Research Laboratory, College of Engineering, University of california, 1992

[75] H. H. Nien, C. K. Huang, S. K. Changchien, H. W. Shieh, C. T. Chen, and Y. Y. Tuan, “Digital color image encoding and decoding using a novel chaotic random generator,” Chaos, Solitons & Fractals, vol. 32, no. 3, pp. 1070–1080, 2007.

[76] S. C. Phatak and S. S. Rao, “Logistic map: A possible random-number generator,” Phys. Rev. E, vol. 51, no. 4, p. 3670, 1995.

[77] L. Kocarev and G. Jakimoski, “Logistic map as a block encryption algorithm,” Phys. Lett. A, vol. 289, no. 4–5, pp. 199–206, 2001.

[78] H. Sakaguchi and K. Tomita, “Bifurcations of the coupled logistic map,” Prog. Theor. Phys., vol. 78, no. 2, pp. 305–315, 1987.

[79] M. F. M. Mursi, H. E. H. Ahmed, F. E. Abd El-samie, and A. H. Abd El-aziem, “Image encryption based on development of Hénon chaotic maps using fractional Fourier transform,” Int. J. Strateg. Inf. Technol. Appl., vol. 5, no. 3, pp. 62–77, 2014.

[80] M. M. Hasan, T. M. Faruqi, M. Tazrean, and T. H. Chowdhury, “Biometric encryption using duffing map,” in 2017 4th International Conference on Advances in Electrical Engineering (ICAEE), 2017, pp. 737–742.

[81] P. Gupta, S. Singh, and I. Mangal, “Image encryption based on Arnold cat map and Sbox,” Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 4, no. 8, pp. 807–812,.

[82] M. Ausloos, The logistic map and the route to chaos: From the beginnings to modern applications. Springer Science & Business Media, 2006.

[83] C. Li, K. Tan, B. Feng, and J. Lu, “The Graph Structure of the Generalized Discrete Arnold’s Cat Map,” IEEE Trans. Comput., 2021.

[84] E. Hariyanto and R. Rahim, “Arnold’s cat map algorithm in digital image encryption,” Int. J. Sci. Res., vol. 5, no. 10, pp. 1363–1365, 2016.

[85] M. F. A. Elzaher, M. Shalaby, and S. H. El Ramly, “An Arnold Cat Map-Based Chaotic Approach for Securing Voice Communication,” in Proceedings of the 10th International Conference on Informatics and Systems, 2016, pp. 329–331.

[86] R. K. Sinha, N. San, B. Asha, and S. S. Sahu, “Chaotic image encryption scheme based on modified arnold cat map and henon map,” in 2018

International Conference on Current Trends towards Converging Technologies (ICCTCT), 2018, pp. 1–5.

[87] H. Marmolin, “Subjective MSE measures,” IEEE Trans. Syst. Man. Cybern., vol. 16, no. 3, pp. 486–489, 1986.

[88] A. Hore and D. Ziou, “Image quality metrics: PSNR vs. SSIM,” in 2010 20th international conference on pattern recognition, 2010, pp. 2366–2369.

[89] U. Sara, M. Akter, and M. S. Uddin, “Image quality assessment through FSIM, SSIM, MSE and PSNR—a comparative study,” J. Comput. Commun., vol. 7, no. 3, pp. 8–18, 2019.

[90] J. Chaki and N. Dey, “Histogram-Based Image Color Features,” in Image Color Feature Extraction Techniques, Springer, 2021, pp. 29–41.

[91] D. O’Shaughnessy, “Linear predictive coding,” IEEE potentials, vol. 7, no. 1, pp. 29– 32, 1988.

[92] M. K. Tariq, “Objective Tests of Speech Signal.” M. Sc. Thesis, College of Engineering Al-Mustansiriya University, Department of Electrical Engineering ,2001.

[93] A. M. Raheema, S. B. Sadkhan-SMIEEE, and S. M. A. Satar, “Performance Enhancement of Speech Scrambling Techniques Based on Many Chaotic Signals,” in 2020 International Conference on Computer Science and Software Engineering (CSASE), 2020, pp. 308–313.

الخلاصة

حاضرُنا مليءٌ ببياناتٍ هائلةٍ ، وأمنُها منوطٌ بطريقةِ الحفاظِ عليها. فإنشاؤها ونقلُها عبر الإنترنت ، قد يعرضها لمجموعة تهديدات وإختراقات او سرقات. لذا كان ظروريّاً البحثُ عن أساليب و وسائل وطرق لتأمينها والحفاظ على أمنِها ، لتجنب ما ذكرناه. ولعلّ أنجع هذه الأساليب هي علم إخفاء المعلومات فضلا عن التشفير. في السنوات الماضية كان موضوع اخفاء المعلومات فعّال ، حيث ظهرت العديد من الخوارزميات للعمل على تطوير تقنيات إخفاء المعلومات. إخفاء المعلومات هو العلم الذي يتعامل مع إخفاء البيانات السرية في بعض الوسائل والناقل قد يكون صورة أو صوت أو نص أو فيديو. وسوف يكون التعامل هنا مع إخفاء المعلومات داخل الصورة بطريقة لا يمكن للنظام البصري البشري التعرف عليها. التشفير لايقل اهمية عن اخفاء المعلومات ويمثل أحد اهم طرق حماية المعلومات، ويعمل على تحويل البيانات من تنسيق واضح ومفهوم الى تنسيق مشفر لا يمكن فهمة او قراتئة.

يتطلب الاحتفاظ بالبيانات السرية ابتكار استراتيجيات جديدة معقدة. يُنشئ النظام المقترح في هذا البحث طريقة هجينة تحتاج إلى أن تكون أكثر استقرارًا وقوة من الأساليب والطرق المستخدمة سابقًا ، وتجمع بين التشفير القائم على الفوضى وإخفاء المعلومات . أن السبب وراء استخدام الأنظمة الفوضوية هو أنّها حساسةٌ للغاية بسبب الظروف الأولية. وهذا يجعل من الصعب فهم المفتاح الخاص بكلمة المرور بسهولة. حيث ان أي تغيير طفيف ممكن ان يحدث في الظروف الأولية سوف يؤدي إلى نتائج بعيدة المدى وغير متوقعة في مخرجات النظام ، وهذا هو حجر الزاوية في نظرية الفوضى. وفي النظام المقترح تم استخدام الصوت والصورة كرسائل سرية لحمايتها. يُقدم هذا البحث اقتراح خوارزميتين كلاهما يُمثل نظام امان مقترح ومطوّر .

في الخوارزمية الاولى تم تشفير الصوت باستخدام (Duffing map) وتشفير الصوره باستخدام (MACM)،بعد ذلك تم اخفاء الرسائل المشفرة داخل الالوان الاساسيه المكونه لصورة الغلاف. تم اخفاء بتات الصورة السريه المشفره داخل اللون الاحمر من الغلاف من خلال استغلال البت الاقل أهمية اما الصوت المشفر فتم اخفائة داخل اللون الازرق من صورة الغلاف.

الخوارزميه الثانية على غرار الخوارزميه الاولى تتضمن تشفير البيانات السريه بعد ذلك اخفائها داخل ناقل عملية التشفير . تتضمن عكس الدوال الفوضوية التي تم أستخدامها في الخوارزمية الاولى ، اما طريقه التشفير فلا تحمل اي اختلاف عن تلك المستخدمة في الخوارزميه الاولى

إنّ استخدامَ خوارزميتين بدوال فوضويه متبادله يعود الى سببين :السبب الاول اختبار كفائة كل خوارزمية في أمان المعلومات واعتمادها كنظام أمان موثوق ومطور ، اما السبب الثاني فهو اثبات أنّ

نوعيه الدالة الفوضوية المستخدمه بحد ذاتها لا تؤثر على نتائج التشفير ، لكن عند الابعاد لتلك الدالة الفوضوية المقترحة والبراميترات الخاصة بها يتناسب طرديا مع حجم المفتاح المستخدم للتشفير.

المقاييس المستخدمة في الاختبارات العملية للنظام المقترح هي نسبة الإشارة القصوى إلى الضوضاء(PSNR)، ومؤشر التشابه الهيكلي(SSIM) ، ومتوسط الخطأ التربيعي(MSE). أثبتت النتائج التجريبية للأنظمة المقترحة علميًا أنها عالية السعة والأمان والمتانة وتنتج العديد من تحسينات الأداء مقارنة بالتقنيات المعروفة حالياً ، مع تشوهات صغيرة للغاية في جودة Stego-image .

تظهر النتائج ان Stego image نجحت في تحقيق(99.98-99.99) SSIM, PSNR(57-58).عند مقارنتها مع الصورة الغلاف .بالإضافة الى ذلك البيانات المسترجعة حققت PSNR (∞),SSIM100% مقارنة بالبيانات السرية الاصلية.

وزارة التعليم العالي والبحث العلمي

جامعة بابل / كلية الهندسة

قسم الهندسة الكهربائية

تحليل وتمثيل لنظام حماية متعدد المراحل باستخدام خوارزميات عشوائية معتمدة على تقنيات التشفير والإخفاء

رسالة
مقدمة الى كلية الهندسة في جامعة بابل
كجزء من متطلبات نيل درجة الماجستير في الهندسة / الهندسة الكهربائية / اتصالات

من قبل

علياء سعدون عبد الدعمي

اشراف

الأستاذ الدكتور إيهاب عبدالرزاق حسين

1443هـ **2022م**