A Technique for Concealing Confidential Information inside an Image over an Unsecure Network

تقنية لإخفاء المعلومات السرية داخل صورة

بوجود شبكة غير آمنة

Student Name

Saad Saleh Hassan Al-Dahiry

Supervisor

Prof. Dr. Alaa Hussein Al-Hamami

A Thesis Submitted in Partial Fulfillment of the Requirement for the Degree of Master of Science in Computer Science

Amman Arab University

College of Computer Sciences and Informatics

October 2012

AUTHORIZATION OF THESIS

I, the Undersigned "Saad Saleh Hassan Al-Dahiry" authorize hereby "Amman Arab University for Graduate Studies" to provide copies of this thesis to libraries, institutions, agencies, and other parties upon their request.

Signature 

APPROVAL

Name: Saad Saleh Hassan Al-Dahiry

Degree: Master of computer science

Title of thesis: A Technique for Concealing Confidential Information inside an Image over Unsecure Network

Examining committee:

Ahmed O. Aljaber

Chair Prof.Dr.Ahmed Al-Jaber

Dr. Firas Al-Mashaqba

Alahamami

Prof. Dr. Alaa Al-Hamami

Dedication

This thesis is dedicated to my father , who taught me that the best kind of knowledge to have is that which is learned for its own sake. It is also dedicated to my mother, who taught me that even the largest task can be accomplished if it is done one step at a time.

Dr.Alaa Al-hamami has been the ideal thesis supervisor , his sage advice , insightful criticisms , and patient encouragement aided the writing of this thesis in innumerable ways.

To Iraq my wounded country that has been always the big encouragement and the motivation.

Finally I wish to express my thanks to my brother and friends who motivated me to finish my thesis.

Acknowledgment

This thesis is the result of almost ten months of full-time study , and during this time I have been supported by many people. I am now delighted to have the opportunity to express my sincere gratitude and appreciation to all of them.

First , I am most grateful for the careful insights of my supervisor prof. Dr.Alaa al-hamami , which contributed to writing , organizing and editing the contents of this thesis as well as his invaluable viewpoints, stimulating suggestions and great patience .His guiding hand and expertise in the field of steganography proved extremely useful to this research .

Also, special thanks go to prof. Dr. muzhir al-ani , Dr. ahmed al-jaber and all faculty members who have encouraged me and helped me during my study in amman arab university .

Finally , I would really like to extend my deep gratitude and sincere thanks to all of my friends and colleagues who were of great help in the completion of this work.

Table of contents

Table of Figures

List of Tables

Abbreviation List

AAC	Advance Audio Coding
AVC	Advance Video Coding
BER	Bit-Error-Rate
BPCS	Bit-Plane Complexity Segmentation
DCT	Discrete Cosine Transform
DPSK	Differential Phase Shift Keying
DWT	Discrete Wavelet Transform
EZW	Embedded Zerotree Wavelet
FLV	Flash Video
GA	Genetic Algorithm
GGD	Generalized Gamma Distribution
GLRT	Generalized Likelihood Ratio Test
GVIP-05	Graphics, Vision and Image Processing
HDC	Hidden Data Capacity
HHK	Hindi Hexadecimal modified Katapayadi
ISH '05	Info. Security & Hiding
IT	Information Technology
JPEG	Joint Photographic Experts Group
LSB	Least Significant Bit
MPEG	Moving Picture Experts Group
MSB	Most Significant Bit
PM1	Plus Minus 1
PSNR	Peak Signal-to-Noise Ratio
PVD	Pixel Value Differencing
QIM	Quantization Index Modulation
STMDF	Steganographic Technique Based on Minimum Deviation of Fidelity
SVM	Support Vector Machine
TTA	Telecom Technology and Applications

Abstract

Recently, the need for new methods that offer more privacy and security during transmitting data has widely increased. In this thesis, a technique that is used in hiding confidential data in image is investigated. Hiding technique or as called also Steganographic will help in the protection of data during the transmission process. It depends on the gaps that exist in the human visual and audio systems in which the Least Significant Bit (LSB) of digital images and sound tracks gray levels is modified.

In this thesis three methods are proposed; the first method is to use the cryptography technique for a text message and then embedding the encrypted message in a cover. The second method is the use of the double hiding. The third method is useing a chaos-based image encryption system by using tent map. The embedding methods are different in new techniques, where the LSB method is used in the first method, the chaos-based is used in the second method and 3D Skew Tent Map in the third method. In the first method, least Significant Bit Replacement Method, image steganography approximately uses all information hiding methods and trys to modify unimportant data in the cover picture. Least significant bit (LSB) addition is a general, easy approach for inserting data in a cover picture. Changing LSB doesn't modify the quality of picture to person observation but this system is sensitive to a selection of picture processing attacks such as compression, cropping and so on. In the second method, Spatial Domain Steganography utilizing 1-Bit Most Significant Bit (MSB) and chaotic method is used, due to that the steganography has a significant position in protected communication. In the third method, the proposed scheme uses the 3D skew

tent map to mix up the plain-image proficiently in the pixel locations combination procedure, while utilizes the joined map lattice scheme to adjust the gray values of the entire picture pixels significantly. The behavior investigation involving key space investigation, statistical investigation, strength adjacent to malevolent attacks like cropping, nosing, JPEG compression, are performed numerically and visually. There is a comparison between the three suggested methods according to some criteria such as: complexity, processing time and security to show their ability in information hiding. Results obtained from the comparison indicate that the third method is the fastest in terms of time, the best in terms of noise and therefore is the best in terms of security.

Arabic summary

تقنية لإخفاء المعلومات السرية داخل صورة بوجود شبكة غير آمنة

الخلاصة

مؤخرا، ازدادت الحاجة لوجود طرق جديدة تتضمن امن و حماية خلال عملية نقل البيانات بشكل أوسع. في الرسالة، تم البحث والشرح عن طريقة لأخفاء بيانات سرية داخل الصور. طريقة الأخفاء او ما تسمى ب (Steganographic) تساعد على حماية البيانات اثناء عملية نقل البيانات. تعتمد هذه الطريقة على الثغرات الموجودة في النظم البشرية البصرية والسمعية التي يتم من خلالها للتعديل استخدام البت الاقل اهمية ((LSB)) و مستويات الرصاصي المسارات الصوتية.

في هذه الرسالة تم اقتراح ثلاثة طرق. الطريقة الأولى هي استخدام طريقة التشفير cryptography للرسائل المكتوبة ثم تضمين هذه الرسائل المشفرة داخل غطاء. الطريقة الثانية هي استخدام الأخفاء المزدوج (double hiding) و الطريقة الثالثة هي استخدام نظام الchaos-based image encryption عن طريق استخدام ال tent map. طرق التضمين في هذه الطرق تختلف من طريقة لأخرى، اذ ان في الطريقة الأولى تم استخدام طريقة البت الاقل اهمية (LSB) و في الطريقة الثانية تم استخدام طريقة الchaos اما في الطريقة الثالثة تم استخدام طريقة الD Skew Tent Map٣ . في الطريقة الأولى (least Significant Bit Replacement) الصورة المستخدمة لأخفاء المعلومات تستخدم تقريبا جميع طرق اخفاء المعلومات و ذلك لتعديل المعلومات الغير مهمة في صورة الغلاف.اضافة البت الاقل اهمية هي (LSB) عبارة عن طريقة سهلة لأدخال العلومات في صورة الغلاف. تغيير ال LSB لا يغير نوعية الصورة بالنسبة لرؤية الشخص ولكن هذا النظام حساس لهجمات عملية تعديل الصورة كضغط الصورة و ازالة اجزاء منها و غيرها من عمليات تعديل الصورة. في الطريقة الثانية (Spatial Domain Steganographyباستخدام (MSB) Bit Most Significant-١) التي تستخدم طريقة ال chaotic ، اخفاء المعلومات له اهمية في عملية حماية الأتصال. في الطريقة الثالثةو تم استخدام ال D٣ skew tent map لمزج الصورة العادية ببراعة في عملية تجميع مواقع البكسل، في حين تستخدم هذه الطريقة نظام map lattice المرتبط لتعديل القيم الرصاصية (gray values) بشكل دقيق لجميع بكسل الصورة. يتضمن بحث السلوك بحث مجال المفتاح و بحث الاحصائي

(statistical) . القوة المرافقة للهجمات الخطيرة (malevolent) كتعديل الصورة و ضغط الصورة و ازالة اجزاء منها و غيرها تتم تنفيذها عدديا و بصريا. في هذه الرسالة سوف نقوم بالمقارنة بين الطرق الثلاثة اعتمادا على مجموعة من المعايير كالتعقيد و المدة الزمنية و الحماية لاظهار قدرتها في اخفاء المعلومات. النتائج التي حصلنا عليها هي في الطريقة الثالثة هي الاسرع من حيث الوقت، وهي الافضل من حيث الضوضاء ،بالتالي هي الافضل من الناحية الامنية.

Chapter One
Introduction

1.1 Introduction

For a long time, using a computer to modify a digital image was something achieved only by a fairly trifling crowd of experts who have admission to costly tools. Typically this mixture of specialists and tools was merely to be established in research labs, and so the turf of digital image processing has its origins in the educational monarchy. Currently, on the other hand, the mixture of a powerful computer on each desktop computer and the point that almost each person has some sort of device for digital image gaining (like a scanner, a digital camera, or a cell phone camera) has caused in an over abundance of digital images as well as many digital image processing has come to be as public as word processing. Today, Information Technology (IT) experts must be more than merely acquainted with digital image processing. They are anticipated to be able to intelligently modify images and associated digital media, which are a gradually vital portion of the workflow not merely to those tangled with media and medicine but all sorts of companies [1].

The need for new proficient, secure and private ways in the protection of secret data is increasing. Secure data are classified into two states in the computer networks, which are: saved or transferred via the network. One of the basic needs during exchanging information is protecting data in a way that it will be seen only by the intended recipient. This can be achieved by using an encryption technique that can obscure the message contents. In this technique, the transmission processes are hidden [2].

1.2 Overview

Hiding technique or as called Steganographic is utilized to hide the transferred information existence with other information. The main data carriers that are used in the hiding technique are images and audio files. This is used if a data transmitter wants to send data to a specific recipient and at the same time does not desire anybody else to know that data and carrier are communicating [3, 4].

Chaos signs are considered to be superior for useful utilization since these signs have significant features like they are greatly perceptive to scheme factors and primary circumstances. They have pseudo-random feature and non-periodicity like the chaotic signs typically noise-like and so on. Therefore, the mixture of chaotic theory and cryptography types is considered to be a significant region of data protection. The features of chaotic signs that formulate chaos scheme are exceptional and strong cryptosystem adjacent to any statistical attacks. The encryption of images is dissimilar from that of contents and thus it is hard to hold them by conventional encryption techniques, as a result of some intrinsic characteristics of images like bulk information capability and high information redundancy [5, 6, 7].

Recently, the chaos based cryptographic algorithms have proposed several latest and proficient techniques to improve protected image encryption methods to meet the need for real-time image transmission above the communication channels. Thus, chaos based image encryption which is provided much concentration in the research of data protection and several

mage encryption algorithms based on chaotic schemes have been suggested. There have been various image encryption algorithms based on chaotic maps such as the Logistic map, the Standard map, the Baker map, the PWNLCM , the Cat map, the Chen map and so on. In order to enhance the protection behavior of the image encryption algorithm, the idea of shuffling the locations of pixels in the plain-image and then modifying the gray values of the shuffled image pixels is utilized. Recently, a new block based image shuffling is suggested to accomplish superior shuffling result utilizing two chaotic maps and the encryption of the shuffled image is executed utilizing a third chaotic map to impose the protection of the suggested encryption procedure [8, 9].

Nowadays, the most common used data transmitters in the hiding of secret messages are digital images, videos and audios. Hiding techniques depend on the gaps that are present in the visual and audio systems of humans in which the Least Significant Bit (LSB) of digital images as well as sound tracks gray levels are changed. In these techniques, data bits are added to image transform coefficients in order to offer higher image reliability as well as more robust to manipulation of images. Some of these transform coefficients are: Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) [10, 11].

Hiding techniques work within two domains, which are: Spatial and frequency domains. The spatial domain is used in the applications that need high load and invisibility as well as low robustness. In the spatial domain, images are divided into a specific number of bits.

The first nth bit is used to embed information due to the existence of high interference. Images are divided into several blocks where a specific number of pixels from each one of the resultant blocks are replaced. Techniques that are based on the frequency domain are used in several applications, such as: digital watermarking, broadcast monitoring and fingerprinting. In these techniques, a small amount of data is required to be inserted into the image carrier. The required amount of data causes little distortion as well as offers high invisibility [12, 13].

Digital watermarking submits to definite data hiding methods whose idea is to insert secret data within multimedia content such as video, images, or audio information. The watermark is usually included to a definite region in the novel content to defend its copyright [14].

Several digital watermarking techniques have been suggested in excess of the last years. In accordance with whether or not the novel sign is throughout the watermark recognition procedure, digital watermarking techniques could also be approximately classified within two kinds: non-blind and blind techniques. Non-blind techniques need the novel image at the recognition end, while blind techniques do not need the novel image at the recognition end. Blind techniques are more practical than non-blind techniques since the novel image might not be obtainable in real situations [15].

A significant part of image processing is concealing confidential information inside a cover media, to be able to send it securely over an unsecured network (like the Internet).

This scheme is highly used to send account codes, company's account information, and personal information. In this project, it is expected to study three methods to achieve successful hiding of the information, image steganographic and massage inserted on an encrypted Image Methods [16].

An example of hidden communication using this scheme is described in the problem of the prisoner shown in Figure 1.1, where Fadi and Khalil, are two prison inmates, and they want to communicate in order to build a plan to escape. However, all communications between them are watched and controlled by the warden Mohammad, who will punish them in smallest suspicion of presence of secret contacts between them. Fadi wants to send a secret message (M) to Khalil, and to do that he must impede (M) into a cover object (C), to get the stego-object (S). The stego-object (S) is transmitted via the public network. In an uncontaminated massage concealing structure, the method for implanting the message is unidentified to Mohammad and joint as a secret amongst Fadi and Khalil. Still, it is normally important to rely on the confidentiality of the algorithm itself. Fadi and Khalil share a secret password which is used to implant the message. Mohammad has no awareness about the secret password that Fadi and Khalil share, even though he is conscious of the algorithm that they could be using for implanting messages. The warden Mohammad who is able to inspect all the messages swapped between Fadi and Khalil and attempts to conclude if it possibly holds a concealed message. If it seems that it does, he overturns the message and/or takes proper act; otherwise he lets the message over without any action [16].

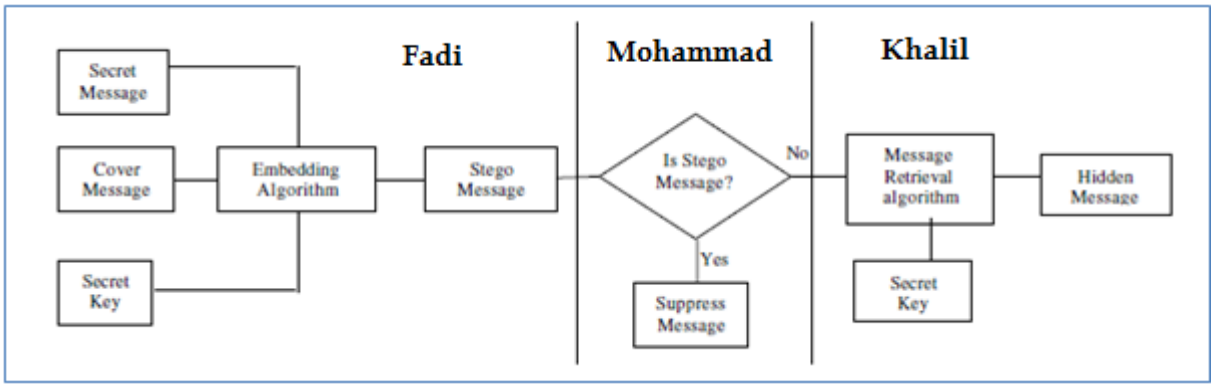

Figure 1.1 Secret key warden massage hiding framework [16]

In this project, three techniques of hiding information will be introduced and explained, which are: the Chaos method, the Least Significant Bit (LSB) method and the 3D Skew Tent Map. Chaos method is used in the image encryption since it is related to several dynamics of its main features. It is very sensitive to both the initial conditions as well as the parameters of the system. The response of the system is random. The main specifications of the chaotic method are: Enhanced flexibility in the encryption of data, good privacy, large, and complicated with many encryption keys and simple design [17].

Least Significant Bit (LSB) is used to hide information in the least significant bits of a carrier. It is one of the simplest methods in hiding data where it offers high data rate. LSB is a simple technique in audio series watermarking, in which the hiding of data into a discrete stream is done by modifying the least significant bits [18].

3D Skew Tent Map is used to create chaotic orbits applied to scuttle the pixel locations while one coupled map lattice is used to surrender random gray value sequences, in order to modify the gray values so as to improve the safety [76].

1.3. The Aim

The aim of this thesis is to describe and developed methods for hiding data within images in order to secure data transmission, to improve the information transmission security during replacing data from a transmitter to a receiver in a way that these data will not be seen by anybody else as well as enhance the image visual properties, decrease the embedding data that causes errors and eliminate the wrong contours. A comparison between the three methods will be implemented according to some criteria to show the strength of the methods and their drawbacks.

These aims can be realized by:

1. Performing an appropriate research as well as analysis of information.
2. Modifying several applications, restrictions and technical problems.
3. Offering several cases and techniques to solve the used issues.

1.4. The Objectives

Several objectives for this project will be achieved, in order to accomplish the aim of the study:

1. Understand the main methods that will be utilized for hiding data within images.
2. Discuss the secure data transmission system and how to improve this system.
3. Describe the main schemes which will be utilized for enhancing the hiding data within images.
4. Understand the three methods of hiding data within images, which are a Least Significant Bit (LSB), a chaos mapping via using one or more methods and a 3D Skew Tent Map.

5. Compare the three methods according to some criteria.

1.5. Problem Statement

In this thesis, three methods will be utilized with known steps for hiding data within images, which are a Least Significant Bit (LSB), a chaos mapping via using one or more methods and a 3D Skew Tent Map. Hiding technique known as Steganographic will help in the protection of data during the transmission process. However, when the hiding data methods will be used during the transmission process, there will be defects within the images, thus different methods will be used to recognize these defects to enhance the information transmission security and this is why the thesis aims to use three different methods for hiding data as well as the three methods will be compared in order to determine the best of these methods.

1.6. Research Importance

Recently, due to the development of the information technology and other technologies which are related to the data domain, people have been created new proficient and surreptitious ways to defend private data. Data safety and privacy are becoming a developing necessary issue due to the fact that electronic communications are widely used and admitted as the main tools of communication. In hiding data technology, some methods use images to protect information, but there are defects within the image, so there are different methods to recognize this defect. Three methods for hiding data will be suggested; the first method is by using encryption on a text and then using the Chaos algorithm to embed the encrypted message. The second method is by using double cover.

The embedding algorithm will be the Least Significant Bit (LSB). The third method is by using encryption on a text and then using the 3D Skew Tent Map algorithm to embed the encrypted message. Finally a comparison will be made between the three methods according to some criteria such as: complexity, processing time, attack and security.

1.7. The proposed solution

Three methods of hiding will be suggested:

1. The first method is by using encryption on a text and then using the Least Significant Bit (LSB) to embed the encrypted message.
2. The second method is by using double cover. The embedding algorithm will be the Chaos algorithm.
3. The third method is by using encryption on a text and then using the 3D Skew Tent Map algorithm to embed the encrypted message. Finally a comparison will be made between the three methods according to some criteria such as: complexity, processing time, attack and security.

In the first method, least Significant Bit Method, all information hiding methods are used by image steganography, in order to modify unimportant data in the cover picture. Least Significant Bit (LSB) is a common, simple approach for inserting data in a cover picture. Changing LSB doesn't alter the quality of image to individual observation but this system is sensitive a selection of image processing attacks such as compression, cropping and so on as in Figure 1.2.

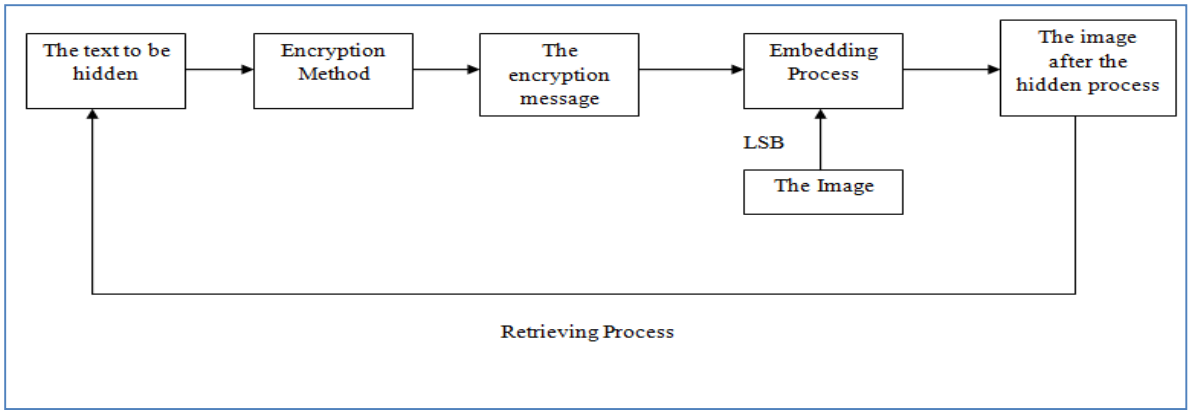

Figure 1.2: First method embedding

LSB method is used in the hiding of messages in an image. It disperses the message bits in a specified image in a random way which prevents unauthorized persons from extracting the message. The digital logarithm calculation method is used in order to discover the bit location into pixel to hide the required message. This method offers a stage key which is utilized throughout the hiding and extracting processes of the message [19].

LSB method is used in the hiding of data in n which is the least significant bits of a specified medium for small value of n. It depends on the replacing of pixel intensity by changing the least significant bits in a way that cannot be noticed by anyone except the specified receiver. The value of n is 1 or 2 [19].

Least Significant Bit (LSB) process is shown in Figure 1.3.

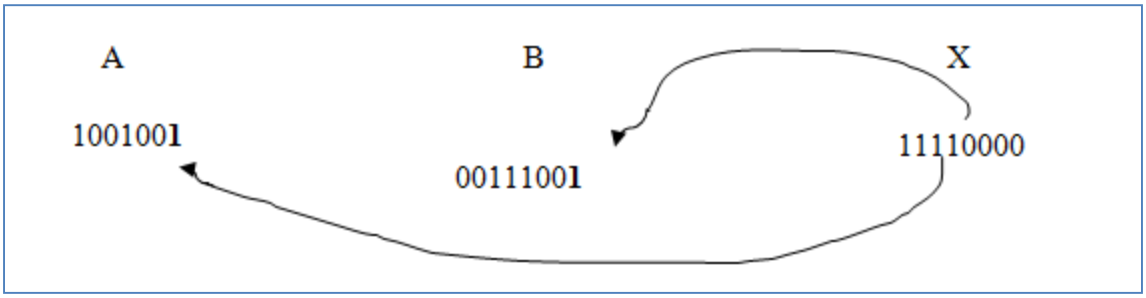

Figure 1.3: Least Significant Bit (LSB) process[20]

As an example, if n equals 1 with a pixel that has intensity equals to 16 which is in the binary code equal 00010000. Then, modifying the least significant bit of the proposed pixel intensity will change the intensity by 2n-1 only, which equals in this case 1. In other words, the proposed pixel will have its original intensity value which is 16= 00010000, or will have the value of 17=00010001 where this value cannot be noticed by anyone [20].

The second method used in this proposed solution include the embedding of message in a cover image by using chaos mapping algorithm , but the message is not encrypted firstly as in the first method mentioned above and then we will embed this cover image in another cover image by using LSB as shown in Figure 1.4.

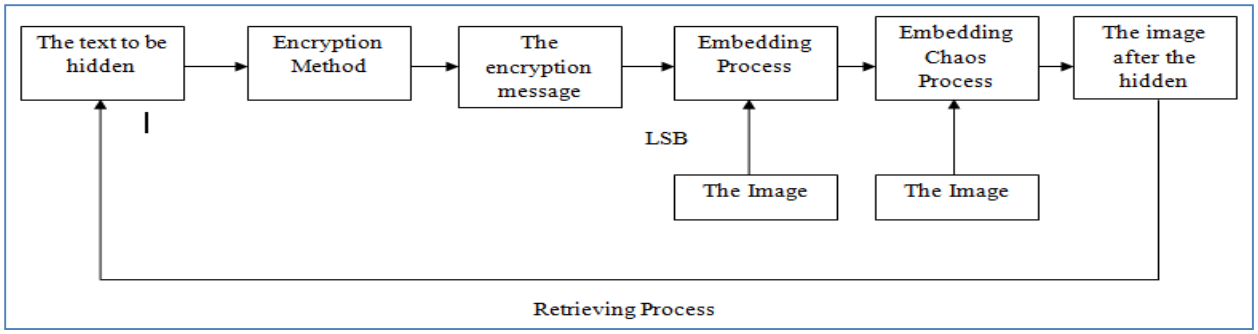

Figure 1.4: Second method embedding

Chaos mapping is a non linear, deterministic and stochastic method. It is very sensitive to the initial conditions as well as the orbits expanding in the whole space. Chaos mapping method is used in several applications, such as in the hiding of data in order to enhance security [16, 17].

The simplest type of the chaotic maps is the logistic map that is given by the following equation:

$$x_{n+1} = \mu x_n (1 - x_n) \quad \ldots\ldots\ldots (1)$$

Where: $0 \leq \mu \leq 4, x_n \in (0,1)$

Several researchers found that the logistic map is in the chaotic state if $3.5699456 < \mu \leq 4$. That is to say, the series that are produced by the logistic map is non-convergent as well as non-periodic. The resultant series from the logistic map are very sensitive to the initial conditions, where any two logistic series that are produced by two dissimilar initial conditions are uncorrelated. The logistic map is applied in several applications, such as the generation of a series like the information hiding and the encryption of embedded position [17, 18].

The third method involves the insertion of encrypted message that is encrypted by using LSB encryption algorithm and then the encrypted message will be embedded in a cover image by using chaos mapping algorithm, after that, also the encrypted message for the third time will be embedded in a cover image by using the 3D Skew Tent Map algorithm as shown in Figure 1.5.

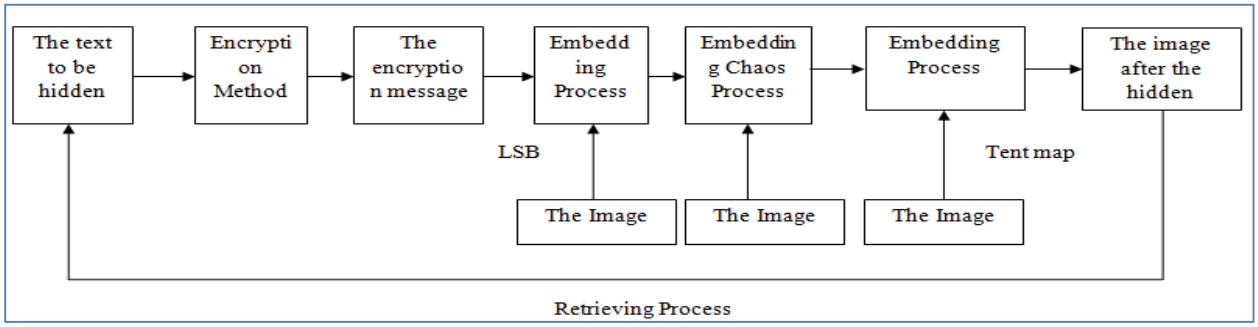

Figure 1.3 Third method embedding

Digital images have some fundamental characteristics like redundancy of information, being less responsive as compared to the content information, bulk information ability and strong connection amongst adjoining pixels. Conventional encryption algorithms like RSA and DES (Data Encryption Standard) are not appropriate for realistic digital picture encryption owing to the limitation of low-stage efficiency although encrypting pictures. Chaos has been established to cryptography as its periodicity, pseudo-randomness and understanding to primary circumstances and manage factors are about to uncertainty and dispersion in cryptography. These properties create chaotic schemes a probable selection for building cryptosystems [6, 7, 8].

The unimodal skew tent map $T_0: [0,1] \rightarrow [0,1]$ is given by:

$$T_0(x) = \begin{cases} x/a & ,if\ x \in [0,a] \\ (1-x)/(1-a) & ,if\ x \in [a,1] \end{cases} \quad (11)$$

Where, $x \in [0,1]$, is the condition of the scheme, and $a \in [0,1]$ is the control factor. It is a noninvertible conversion of the unit period against itself. As $= 0.5$, then T_0 is a regular tent map.

In the three methods mentioned above the specified receiver will open the embedding that is included in the pictures by using the same algorithm but in reverse way.

1.8. Contribution

The proposed techniques will enhance the image visual properties, decrease the embedding that causes errors and eliminate the wrong contours. In addition, it enhances the information transmission security during exchanging data from a transmitter to a receiver in a way that thesis data will not be seen by anybody else.

1.9 Thesis Outline

The content of this thesis is divided into five chapters which are combined with each other, and in addition to chapter one, it contains the following:

- Chapter two reviews a literature of recent research works that describes hiding data technologies.
- Chapter three explores the methodology including resources, requirements, and methods to perform steganography, theories and concepts and risk and cost management issues.

- Chapter four discusses the work done along with the results achieved. Testing and evaluation of the performance will be also included.
- Chapter five explores the conclusion and suggestions and/or recommendations for future work.

CHAPTER TWO
LITERATURE REVIEW

2.1. Introduction

There are two common types for data hiding, which are the recognition methods (steganalysis) and the embedding methods (steganography). The first type aims to raise the load, enhance the sturdiness and investigate the features of the stego image within embedding operations. There are several methods of steganalysis technique that regard the performance of the recognition operation as one of the significant aspects. Many steps are involved within the data hiding system, in order to accomplish the embedding operation of the private note within the precise image. The technique is the most significant step within the operation, such that it will be utilized for embedding information, also the nature of the image is one of the significant steps that must be investigated. The LSB embedding is used within the steganographic method, to illustrate the number of palette images and the pixel values, or to quantize the coefficients within the image layout. Recently, many investigations proposed new methods for raising the ability as well as discussed the nature of the stego images. Steganographic techniques may get benefit due to the redundancy, since the image is accumulated within the image layout. These techniques substitute insignificant bit planes within the spatial domain; also these techniques are simply noticeable from arithmetical analysis [19, 20].

2.2. Related Works

Marvel, et al [21, 22] suggested easy tools for saving one bit per block within the JPEG coefficients. This allows several exterior similarities.

The embedded data is saved inside the JPEG coefficients as well as the receiver includes them in order to remove the embedded data. Many studies provide a technique that depends on arithmetical investigation of couples of values that are replaced throughout message embedding. In addition, this technique supplies consistent outcomes, if the position of the message is known.

Alkhrais,h [23], suggested a developed technique for hiding private image within a container image. In this technique, each pixel is fabricated with a sequence of bits in an image. By basically overwriting the information, which it was already in the image, the 4-least significant bit of 8-bit right color image to grasp 4-bit of the private message. The investigational outcomes of this technique view the effect of altering the 4-least significant bits which it is almost completely unnoticeable.
Hasanien,a.e [24], initiated a proficient approach, which it depends on the hypothesis of wavelets, to defend a possession by hiding iris information within a digital image .

Fridrich, et al [25] introduced that for steganographic techniques which operate in the spatial domain, the cover images accumulated within the JPEG layout, are very pitiable options. Due to that the quantization initiated by JPEG density is able to have an exceptional fingerprint which is also able to be utilized for recognition of very tiny alterations of a cover image through examining the matching of the stego image within the JPEG layout. Also, Fridrich initiated an influential steganalysis technique (RS steganalysis) for recognition of LSB embedding. This technique uses susceptible double statistics based on spatial connections in images [25].

One of the most used techniques for hiding sensitive or secret information is Steganography technique. It stores the information into something that appears to be nothing out of the ordinary. In defending significant data, Steganography and cryptology techniques are identical to each other in ways that are utilized. The Steganography technique includes hiding data such that it shows that there is no hidden data at all, which it is different from cryptology technique. Recently, steganography and watermarking techniques are related to the hiding data technology. One of the methods that are used to cover the data in digital object such as image, video or audio, is watermarking techniques, in such that the data are tough to modifications or variations. The mark in the watermarking technique is undetectable or imperceptible for the human visualization system; also it is not allowed to extract the watermark without mortifying superiority for the data of a digital object [26, 27, 28].

In the watermarking technique, the significant function is to guarantee safety schemes, which these schemes are proposed in order to avoid illegal copying of digital multimedia. So when the digital sign such as audio, pictures or video, is copied also the data will be copied. In steganography technique, the major purpose is to cover private data in the other hiding multimedia such as video, audio or image, thus the existence of the data will not be detected by the others. There is a main difference between steganography technique and others techniques for the secret replace of data, due to the fact that in the cryptography technique, the data will be observed by persons, by viewing the coded data, while the persons are not able to realize data. But in steganography technique, the existence of data will not be observed by persons at all.

The steganography and cryptography techniques are both utilized in hiding precious data, although there is a difference between them [27, 28].

New alternative arrangement techniques are suggested to defeat these drawbacks, to increase the efficiency of the hiding data technology. These methods depend on a different theory to the idea of arrangement in such a way that the data are embedded within another multimedia as well as construct the data in the way that the hackers cannot notice them. Recently, the hiding data technology is categorized into more precise such as encryption data (Cryptography), hiding data (Steganography) or a mixture between them [29].

Recently, security has been developed to be one of the most significant factors in all domains, such as video observation, secret communication and medical and armed forces purposes. For thousands of years, hiding data technology has been utilized in order to protect data during the transmission operation without penetration of the hackers. As a result of the increasing in the use of digital images on the Internet, images are able to be utilized in for hiding data. Images that include secure information are very sufficient for several purposes that require safety transmission of the data [30].

One of the most proficient techniques is encryption technique that is utilized widely to transfer images including secure information throughout networks. This technique gets the information and combines them with a key and an algorithm to obtain secure and unreadable information. Key must be placed at the receiver in order to decrypt the information and read it.

There are several algorithms for encryption technique or data hiding technology that are utilized to guarantee the security of the multimedia information. On the safety transmission of information, a drawback is noticed, which it is to try to mix the data hiding technology and encryption technique in one step. There is another technique for hiding data, which is steganography technique. This technique protects data by hiding information within other data [31].

The most domains which the steganography technique used are computers domain. Information is one of the important elements in the computer communication world; also lots of techniques have been established to achieve the main aim, to utilize steganography technique for hiding data. For hiding data within images, the hidden data is embedded within a huge object, so the alteration will not be viewed by the human eye. Digital images have the advantage of involving large amount of bytes to choose pixel color for the picture. It is necessary to ensure that the cover image is big enough in order to hold the byte manipulation [32, 33].

2.3. Information Hiding Techniques

One of the very common techniques for hiding data by embedding secret notes with simplicity is Least Significant Bit (LSB) technique. This technique is able to add the secret note in the least significant bits of images. The human illustration system is not responsive enough to identify alterations in color, thus the (LSB) technique is operated to insert the secret note in the least significant bits of images. The alterations in luminance are much better identified.

The necessary algorithm for the (LSB) technique is to get the primary N cover pixels where N is the whole length of the secret note that is to be included in bits, and then each pixel's end bit will be substituted by one of the note bits [34, 35].

Figure 2.1 shows the necessary algorithm for the (LSB) technique.

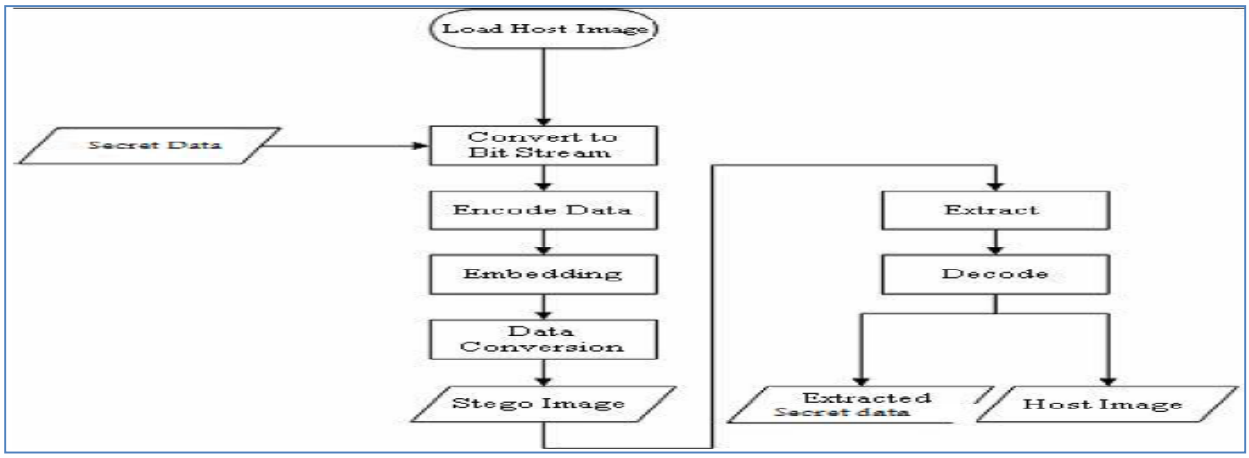

Figure 2.1: Least Significant Bit (LSB) procedures [30]

Nowadays, in the communication domain, the penetration of data has increased, due to the fact that the security of the transmission data has also increased. Security in the transmission data has become one of the most important characteristics for prosperous networks. There are two methods that are extensively utilized in hiding data technology, Steganography and Cryptography methods. They are able to control data to cipher as well as to cover their presence. Also, these methods are utilized in several applications and domains such as communication, computer technology fields and so on. In addition they are utilized to defend army messages, credit card data, E-mails, individual folders, commercial information and so on [36].

2.4. Cryptographic Method

Cryptography means the study of means of exchanging data from its ordinary, understandable shape into an inconceivable shape. Coded text is the way to defend data by converting it into an incomprehensible shape. An encrypted note is able to be damaged by cryptanalysis, which is known as code breaking. The new cryptography methods are almost indestructible. The security methods of the transmission data utilize mathematical systems and algorithms, in order to transform information into an incomprehensible message. The message can be coded by the related key [37].

Figure 2.2 shows the general form of cryptographic system.

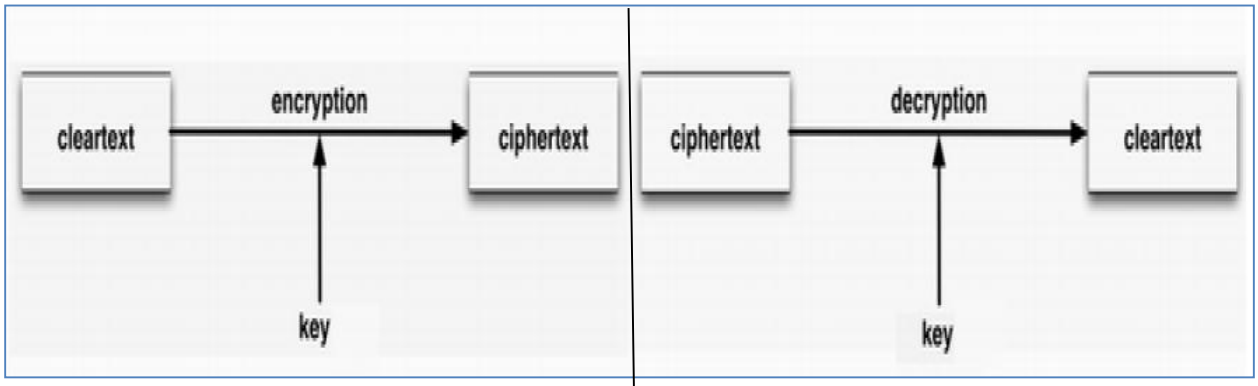

Figure 2.2: Cryptographic flow [36]

2.5. Steganographic Method

Steganography means the knowledge of communicating in such a way that hides the presence of communication. Steganography method detects the presence of the note by including it within a transporter folder of several kinds. An eavesdropper is able to interrupt the cryptographic note, at that time the steganographic note cannot be noticed if it exists. Cryptography and

Steganography methods have the same aim in hiding data technology but each one has different way to secure data. Encryption encodes the information in such a way that an unintentional receiver cannot decide its proposed denotation, but the Steganography method tries to avoid an unintentional receiver from predicting that the information is there. To have an improved confidential communication, it is better to combine between the encryption with Steganography. Steganography method aims to avoid drawing doubt in order to transfer the secret note. Steganalysis is a technique of noticing probable private communication by utilizing text to steganography; also it tries to overcome steganography methods [38, 39].

Figure 2.3 shows the general form of Steganographic method.

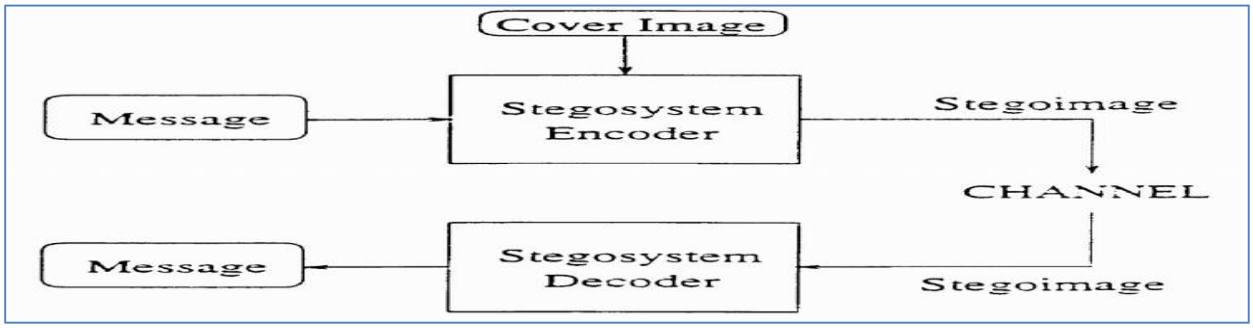

Figure 2.3: Steganographic flow [36]

Depending on deceiving algorithm called x^2 , a new steganography technique was proposed by Famili, Z., et al [58]. Based on statistical properties, considerable differences are present between coefficients histograms of stego image and cover image, and x^2-test shows that stego image includes hidden messages. They provided the idea of using cover image in order to hide messages. They used 16 images in order to apply their suggested algorithm, and the results is shown in Table 2.1, where the

value of x^2 for cover image was obtained as illustrated in the first column, by using JSTEG technique. The value of x^2 was calculated and put in the second column, and it could be easily observed that the first column is highly different than the second one so it could be clearly realized that the stego image includes a hidden message by applying x^2-test, for the suggested method the value of x^2 was estimated as shown in the third column, and a comparison between first and third columns reveals that the values of x^2 were not nearly changed [40].

Table (2. 1): Results of applying x^2-test [40]

cover image x^2	stego image x^2 (JSteg method)	stego image x^2 (proposed method)
245	14	223
227	14	197
511	14	463
360	11	340
611	11	508
329	10	316
140	10	136

After applying algorithm, it was noted that after embedding message there are no striking changes in the coefficient histogram of DCT in comparison with the original message, and based on that it could be concluded that through x^2- test, eavesdroppers will not be able to identify hidden message

within the image. Although the suggested technique decreases embedding message capacity, it improves the ability of steganography to withstand x^2-test and so it increases the security of steganography [40].

The steganography technique, known as embedding capacity, is very important. and Sajedi,h. and Jamzad,m. [41], introduced it as an images' property with existence of several steganalyzers, and provide a technique for calculating cover image capacity of impeding. The actual capacity of embedding may vary from image to image even when "number of non-zero DCT coefficients" are identical because when the contents of images are not similar then the distribution of coefficient of non-zero DCT will not be equal. If the capacity of image to hide data is known, the embedding process will be applied more securely.

They suggested an approach to specify the embedding security limits through a system which uses several units of steganalyzer. In the suggested system, a number of steganalyzers, which are distinguished by its sensitivity to variant payloads and having identical type, are combined together in order to form steganalyzer unit. For an image, the embedding rate's upper limit could be exactly determined based on each steganalyzer confidence, so based on the capacity of embedding, the person who makes embedding will be able to choose the more suitable cover image. Based on the capacity of embedding, choosing the most suitable and secure cover image will decrease the possibility of detection risk [41].

The connection between image embedding capacity and image complexity was also analyzed, as shown in Figure 2.4.

The capacity of embedding for simple and very complex image is lower than high and middle complex one. The results of experiment show that stego image security is improved by applying the suggested approach [42].

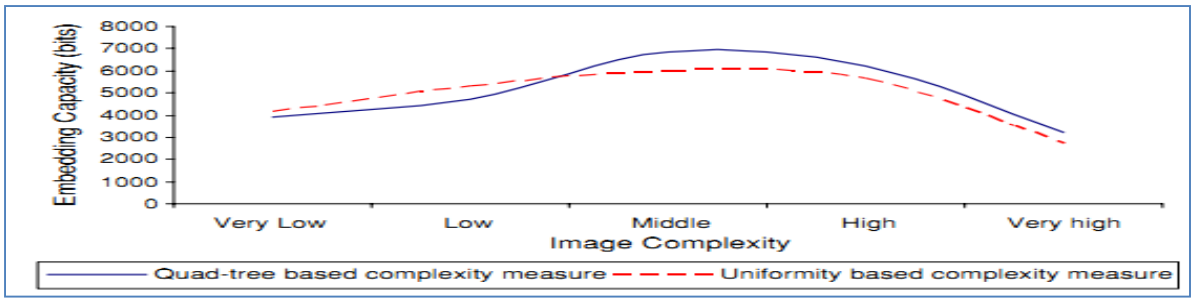

Figure 2.4: Image complexity [42]

2.6. Algorithms of Steganography That Use both Different and Identical Histograms of What is Called "Raw Digital Video Streams"

One of the very important data-embedding techniques is steganography which uses unsuspected media to embed secret data within it. Although images were widely used previously in steganography, video stream has been also used nowadays. As Cetin and Ozcerit said, in case when digital video stream is used, the most important thing that controls the successful and efficiency of embedding data is to choose pixels where the cover data required to be hidden inside, these pixels are called "target pixels", the stego-video will be affected by the two problems which are unwanted "temporal and spatial perception" if the selecting process of pixels was not performed accurately [43].

Chang,c. and tseng,h. [44] suggested two novel algorithms of steganography using both different and identical histograms of what is called “raw digital video streams”. The format of files which contain the data required to be hidden could be ‘xls’, ‘pdf’, ‘html’, ‘doc’, ‘mp3’, or ‘rar’. Choosing the most suitable pixel is the main point which the two novel algorithms are built on, and the selection process is done by giving a large attention to the cover video capacity and perceptibility variables. In order to understand the influence of other very important variables such as amount of corrupt bits and Hidden Data Capacity (HDC), another two processes are provided to the study which are block-based and frame approaches. After applying block-based and frame-based approaches, it is shown that for identical histogram approaches, frame-based technique provides better output than block one, and vice versa when different histogram approach is used. Enhancing stego-video “temporal and spatial perception” degree and providing more capacity for data-embedding than provided by ordinary used steganography method are results of applying the suggested steganographic technique.

Steganographic technique which is based on Pixel Value Differencing (PVD) was taken into consideration and studied deeply by Ji. et al. since it is distinguished by providing high visual imperceptibility and increasing the capacity of data embedding. The study includes two parts: in the first part, an enough extraction and embedding data circumstances were derived, where there is a broad range to select parameters of embedding, and they prove that the PVD technique could be more widely applicable. In the second part, they analyze the security of steganography which is based on PVD, where the steganalyzer of the mentioned technique is founded and applied

on it. Although this technique gives high visual imperceptibility and high capacity, the outcomes reveal that the new steganography which is based on PVD is not able to withstand statistical detection and has low security, and they suggested that more research must be done regarding steganography based on PVD in order to improve its security [45, 46].

Steganography is the process of hiding data within media and steganalysis is the inverse process of it. In this survey a video bit-stream motion vectors are used to hide data where Su. et. al. suggested Steganography technique to identify presence of hidden data inside motion vectors. In order to specify presence of hidden data and depending on analysis of statistics of 12 extracted characteristics which have both domains temporal and spatial. Feature classification approach was suggested by Su. et al. The machine which is utilized to discriminate is Support Vector Machine (SVM). The outcomes of applying the suggested methods on several motion activity videos reveal that the suggested technique gives high performance in detecting data presence within steganography algorithms based on motion vectors. Swanson. et al, suggested a method which uses stream of digital video as a primary video to hide secondary video or auxiliary data which have high rate of bits. In order to transfer ancillary data using the suggested technique, there is no need to present bit interleaving or separate channel [47, 48, 49].

By utilizing quantization algorithm and projection that is based on perception, the information could be inserted in the primary source invisibly

The security and accessibility levels, which could be defined by users, are supported by the algorithm. Swanson, et al [49] used “real time video-in-video and speech-in-video” examples to demonstrate their algorithm. The size of block which is used by them, is 8X8 where two bits were embedded in each block, so in each frame, 2400 bits could be embedded in case a video of size 240X320 is used, and thus 9000 bytes/s could be embedded in 30 frames/s. a sequence of equal length of “broadcast News” movie, which has 240X360 size of frame, is used to embed “Madonna Video”. MPEG is used in order to encode “Madonna Video” at 294 bytes/frame rate of bit, Figure 2.5 demonstrates that after embedding data there are no observable distortion in the sequences of video.

Figure 2.5: Application video-in-video, a) “Broadcast News” Primary movie, b) Primary and embedded movies, c) “Madonna Movie” [49]

In addition they used classroom video, where the set of frames that it is composed of are 250 and with 360X240 in size for each one, to embed 4 speech streams and Figure 2.6 shows some of these video frames.

Furthermore, they show the embedding data robustness and the effect on the distortion and degradation of video, where in the setting of free distortion, there was not any bit error that takes place when they used lossy environment to test the algorithm robustness. They exposed host video to several Gaussian noise levels, and the “Bit-Error-Rate” (BER) was 1.2 percent and 0.2 percent respectively when the Peak Signal-to-Noise Ratio (PSNR) was 28.1 dB and 30.0 dB respectively. Futere, BER was 1 percent and 0.1 percent respectively when the hosted video is exposed to Joint Photographic Experts Group (JPEG) coding of motion with 7:1 and 3:1 ratio of compression respectively [49].

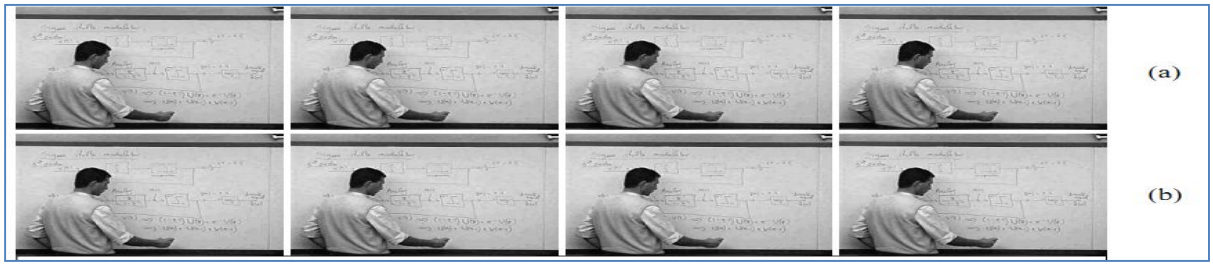

Figure 2.6: Application of speech in video, a) primary classroom video b) Primary with embedded data [49]

A compressed Moving Picture Experts Group (MPEG) video is used to embed data within it through an effective algorithm suggested by Zheng, et al [50] Under compression of MPEG-2, a content of digital video could be hidden by using the algorithm, where the information is hidden inside sub-blocks of medium frequency after dividing block coefficients of 8X8 Discrete Cosine Transform (DCT) into it. Compressed coefficients are allowed to be

immediately used to embed data through the algorithm, which decrease the time consumed in hiding process and enable more video streams amount to be used. The reason behind that is that there are several strategies of coding associated with several frame types, such as B-frame, P-frame and I-frame, the degree of robustness vary, but generally it could be clearly concluded that in countering MPEG-2 compression, the suggested technique shows excellent degree of robustness.

Ability to utilize DCT coefficient with no need to compress and decompress it is considered as one of the important benefits of the suggested technique. Video-in-video, captioning and delivery of secret data are some of practical fields where the suggested algorithm could be applied successfully. Zheng, et al, have tested their algorithm and the outcomes reveal that it has high performance efficiency [50].

A novel technique to embed data with spatial domain inside digital image was discussed by Daneshkhah. et al [51]. Unlike other methods, a specific coding is used to enable plane of forth and second bits in addition to less important pixel bit to be controlled and used to hide data. On the other hand, for one plane of bit, one alternation could take place for each process of embedding. The suggested algorithm reveals that it has high robustness and could not be detected easily. Furthermore, the embedding capacity of proposed method is acceptable comparing with Least Significant Bit (LSB)-Matching method as shown in Figure 2.7.

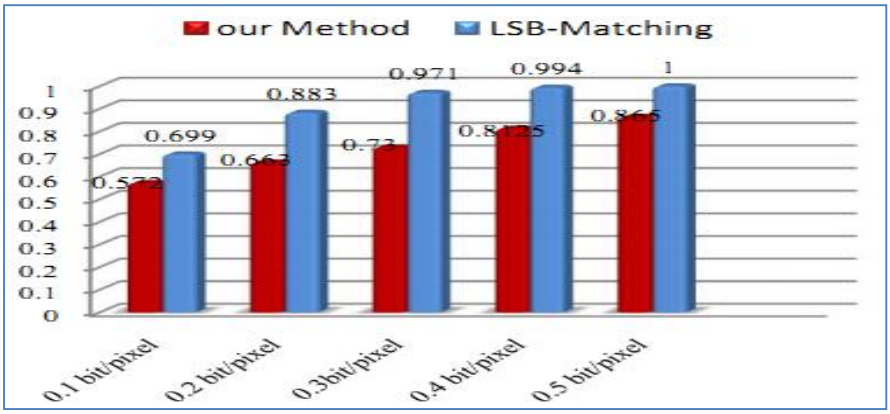

Figure 2.7: Rate of correct detection vs. rate of embedding of 0.1, 0.2, 0.3, 0.4 and 0.5 bit/pixel [51]

As shown in Figure 2.7, the rate of correct detection of LSB-Matching method is higher than the rate of correct detection of the suggested method. Thus, at 0.3 bit/pixel the rate of detection of LSB-Matching method is 24% higher than for the suggested method and so it gives higher security level.

A new scheme of steganography is presented by Lou. et al, [52] depending on sensitivity of human vision, where it distinguishes by providing a high capacity for embedding data and its ability to obstruct visual degradation. The cover image local complexity determines the pixel capacity of embedding, which increases the quantity of data required to be embedded and allow keeping high visual quality. According to local complexity differences, pixels could be grouped into 3 levels, taking into consideration sensitivity of human vision. Depending on human vision, it is so difficult to distinguish the variation between stego and original image.

Capacity of embedding of classified three levels, which are separated by two - threshold boundary limit, pounds the allowable cover image capacity of embedding. So for each level, they create a relation or “compensation ratio” associated with maximum capacity of embedding. As a result, based on the required capacity of embedding, the two threshold limits could be specified by the suggested scheme. After applying the suggested algorithm, the outcomes reveal that the technique is feasible, efficient and simple. In addition, as the algorithm is statistically concealed, it is able to withstand attacks done by RS steganalysis. In addition, comparing with other schemes, the suggested one grants more capacity for embedding data. Furthermore, the visual distortion produced from applying the scheme is minor [53].

A novel steganographic method using side information was used and presented in this paper which is Malik.h [53], in order to minimize the distortion of the stego-image and provide larger embedding capacity. In order to estimate the degree of smoothness or contrast of pixels the method exploits the correlation between neighboring pixels. The edge area may tolerate larger changes than those in smooth areas if the pixel is located in it. The two-sided, three-sided, and four-sided side match methods are employed in the scheme. A novel and efficient steganographic method has been proposed in order to embed secret information into images without producing perceptible distortions.

When the embedded data is extracted from a stego-image there is no need to refer the original image. In order to estimate the amount of data that can

be embedded into an input pixel of cover image the method utilizes the side information. The pixels in edge areas may embed more data than those in non-edge areas. It was clear that this method is better than conventional LSBs substitution method in both security and visual effect. The experimental results have shown that the proposed method provides a better way for embedding large amount of data into cover images without making noticeable distortions. Furthermore, the embedded data can be extracted from the stego-image without referring to the original image [54].

In order to hide information within compressed MPEG stream of video, an algorithm was suggested by Xu et al [55] where I frame is used to embed control data inside in order to make process of extraction data easier, and B and P frames are used to embed redundant data. As a result, although a portion of capacity of embedding was lost, the suggested technique shows an acceptable compromise between security and capacity of embedding; also it shows a good ability to resist processing of video like dropping or adding frame. With no need to primary video, the extraction process could be implemented, where extraction data embedded in B and P frames is done after extracting control data from I frame.

2.7. Compressed Video Secure Steganography

A novel algorithm which is called “Compressed Video Secure Steganography” is presented by Liu, et al [56]. In order to obtain requirements of real time without requiring decompression and within compressed domain; both detection and embedding could be completely implemented. In order to modify the capacity and strategy of embedding, a novel standard applying adjacent frames statistical invisibility is utilized, and

that improves security level and achieves properties of connivance resistance. Also a tester called video steganalysis is created in order to test the suggested algorithm and discover errors. The outcomes reveal that the suggested technique shows high security level when it is implemented on "compressed video steganography" without perceptible degradation.

One of the techniques which are used to hide highly sensitive or secret data within a media in a way that is difficult to be detected is steganography. Elsadig, et al [57] in their study used digital video to hide the required data, this method based on using the data, required to be hidden, to modify the image shown in each frame of video.They Also demonstrated enhancing the capacity of embedding data in streaming of digital video and using insertion technique called "Least Significant Bit (LSB)" on frames and images of video. The outcomes reveal that the extraction process for frames of video was done successfully, and data of 500 pages might be included within 5 images.

From Figure 2.8 and Figure 2.9 it could be seen that according to human vision, the dissimilarity between original and result frame are small. Consequently, the suggested technique could be satisfyingly implemented in frames of video. Presence dissimilarity in original and result frames histogram considered evidence of occurring embedding process without happening and visible dissimilarity [58].

Figure 2.8: Original Frame [58]

Figure 2.9: Resulted Frame [58]

Yu. et al [59] investigated the steganography method of “Plus minus 1 (PM1)”. This technique was built on the least significant bits as an improved method which provides relative high capacity in addition to least significant bit based technique typical attacks foiling. However, they did not present the application of this technique on JPEG images. They proposed a generic algorithm (GA) to perform the JPEG images using PM1 steganography and their GAs were used to minimize blackness as an enhanced feature of performance optimization.

They discussed in details the steganography histogram characteristics by theoretical analysis and they could justify that the preservations of the “first-order-statistical properties” can be achieved for JPEG images based on PM1. They proposed technique could overcome the other method related to securitization and capacity. They performed their objectives by decreasing the blackness ratio between the steganography image and the related estimated image. The modification of each coefficient as decrement or increment could be done with the aid of GA for the PM1. In some methods of steganography like JSTEG, MB2, MB1, Outguess, and F5 capacity was less than their proposed method and provides enhanced security features even if the same secrete message is loaded. They got many experimental results to prove the improved capacity and security characteristics. They used the grayscale images to do the experiments but there are no constraints to implement the colored images for the GA-PM1 technique. Figure 2.10 shows a comparison between the various methods of steganography compared to the PM1 technique related to the security [59].

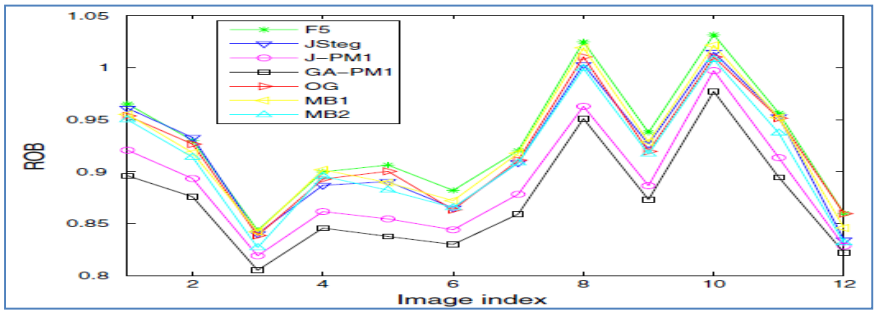

Figure 2.10: ROB of different steganographic techniques at 0.1 BPC [59]

And the same comparison was actuated but for the capacity as shown in the following figure.

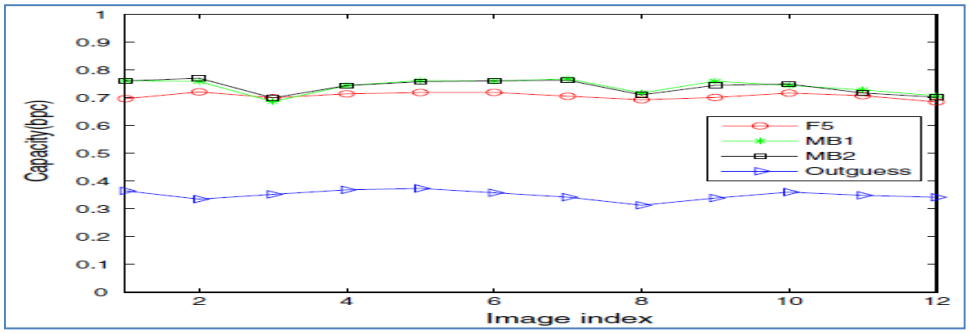

Figure 2.11: Capacity of each technique [59]

Hopper. et al [60] presented the Provably Secure Steganography. They defined the steganography as “the problem of hiding secret messages in innocent-looking public communication so that the presence of the secret messages cannot be detected”. Their paper introduced the steganographic security cryptographic formalization from a channel based on computational approach. This approach is an index of probability distributions upon covered message.

They stated that to constitute a secure steganography, it is necessary to sample from the channel and the functions must be existed as one way using what is called “cryptographic and complexity-theoretic proof techniques”. Depending on rejection sampling, they made a steganographic protocol from the channel as a second step and their model was provably secure within the mentioned conditions for an optimal bandwidth. This can be considered the new secure steganographic protocol proved “example [60].

They also gave the first formalization of “robust” steganography, where an adversary attempts to remove any hidden messages without unduly disrupting the cover channel.

They gave a necessary condition on the amount of disruption the adversary is allowed in terms of a worst case measure of mutual information. They provided a construction that is provably secure and computationally efficient and has nearly optimal bandwidth, assuming repeatable access to the channel" distribution.

Liu. et al [61] Said that their studies are obtained to find a new hiding methods depend on a relation of equivalence that will enhance stego image quality in remarkable way without sacrificing the capacity and security of original scheme of steganography. This will be achieved by using equivalence relation depending on hiding units capacity, all these units can be divided into similarity classes.

Thus, the procedure of hiding is done in equivalence classes, as mentioned, in schemes of traditional steganography. Taking into account the relation between the capacity and length of message, they found that the hiding method performance when using suggested strategy of hiding outperforms the same approaches when implementing messages with the same lengths. To overcome any type of distortion that may be caused by hiding secret data of small size, they suggested to hide the important data (secret data) from similarity class with least capacity of hiding to the similarity classes with largest capacity of hiding. In reality, the main idea not only gives them ability to enhance the stego image quality, but it may also give them ability to utilize different and more significant hiding methods for several equivalence classes to enhance the effectiveness and the security [52].

The requirement of safety during the digital messages transmission over a media of digital communication is adopted by Tripathi [62]. He found that steganography is a very important technique in hiding data and information. A discussion of two level steganography has been obtained by Tripathi.

This discussion involved image based and audio based encoding. Image based stage of steganography uses a methodology of heuristic to involve the algorithm based on the stream of message. For this reason, he suggested anew secure and robust steganographic system for hidden communication. This suggestion involved two stages and leads to a double security level [62].

The use of audio steganography with low bits coding is done by Wakiyama. et al [63]. This technique depends on replacing lower bit data in a cover up audio data by a secret data. To apply this technique, they used wave file like a data of audio. The format of wave file is a Microsoft's RIFF specification subset for the multimedia files storage. An eight bits mono-audio-data were used by them. They suggest two types of novel techniques of coding of extended low bits.

A program and an experiment were made to confirm the method. Also a new secret data were embedded by using novel technique that depends on coding of extended low-bit. A future work is planned to maximize the capacity as well as enhance the audio steganography confidentiality [63].

2.8. Related Works of Several Hiding Data Systems Using Different Algorithms

Bhowal et al [64, 65] defined steganography of Audio method as a technique to ensure transferring data in a secured way between different locations normally in internet community. They offer a new. Principled technique to solve the other problems of substitution method of steganography of audio. They used (RSA) as one of the most powerful encryption algorithm, to encode message in the security level that is too complicated to break. At the second level, they used a greater powerful technique Genetic Algorithm (GA), which depends on Least Significant Bit (LSB) Algorithm to encrypt the encoded message into audio data. Bits of the encrypted message are implanted into higher and random LSB layers, causing an increase in robustness versus addition of the noise. This method introduce some benefits like if anyone knows that there is hidden data in it, but it is so difficult to obtain the hidden data from host audio. But this method faced a problem caused by the difficulty created as a result of flipping of bits.

Another method in steganography is depending on scheme of embedded zero-tree wavelet and steganographic of bit-plane segmentation. This technique is founded by Spaulding. et al [66, 67] The suggested method of steganography permits them to utilize loss compressed figures as fake files in steganographic algorithms of bit plane based. They achieved large rates of embedding around 25 percent of image in the compressed size were got with minimum visible degradation in quality of image. i.e compression of Bit-Plane Complexity Segmentation (BPCS) combined with Embedded Zerotree Wavelet (EZW) was presented to achieve their aim from this method. If another lossy compression is done in the dummy file that already has a

compression of lossy image this will destroy the embedded information in a very easy way see Figure 2.12.

Figure 2.12: a) Original image. b) Compression with EZW. c) Show the effect of another compression in an already compressed image [66].

Chen, W-Y [54] made a research based on the DPSK (Differential Phase Shift Keying) technique that is used in systems of digital communication. To enhance a scheme of steganography, his main aim to disappear a confidential image into a same size image for covering. This will result in an image with no noticeable dilapidation. He employed three strategies to obtain his main goal: 1) NBSPC (A Neighbor Block Signal Phase Comparison) mechanism is used to give the position for embedding secret data. 2) FPDPSK (A Fold Phase Distribution Differential Comparison) is used to enhance cover page quality. 3) Reduction of secret bits number was done by compressing the secret image. The SPIHT (Set Partitioning in Hierarchical Trees) codes were utilized to get an image compression with a low bit rate and high quality of reconstructed image.

Where, Chiang, Y.K [68] had developed the DPSK of distribution of the fold phase to achieve more than 1.5 dB enhancement and twice margin of the noise than the standard set of DPSK method on the identical test circumstances.

These methods have several advantages. One of which is the ability to hide secret images with the same size of cover image, also by using the SPIHT codec the reconstruction operation can be achieved with high value of quality. See Figure 2.13.

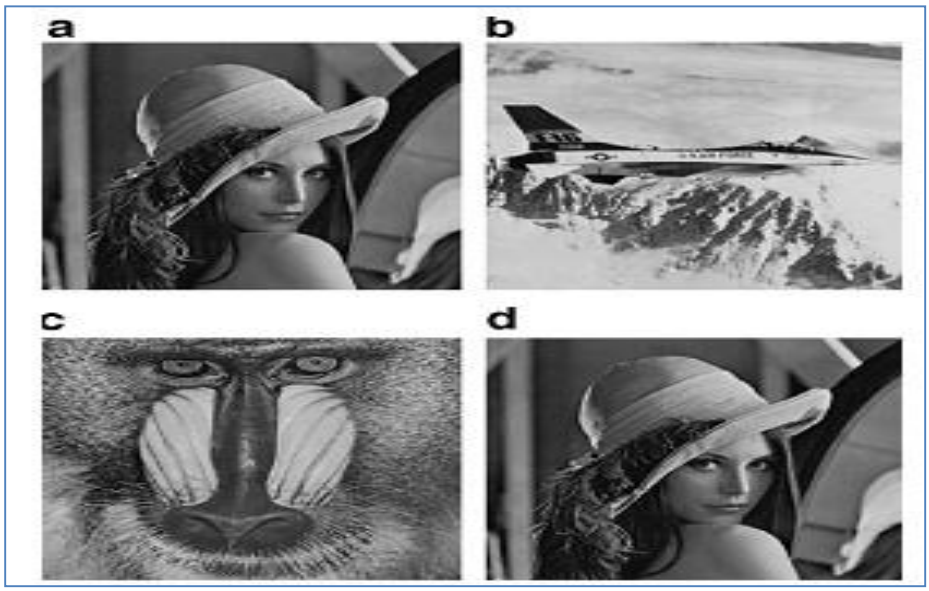

Figure 2.13: a) The stego-image ‘‘Lena’’; (b) The reconstructed secret image ‘‘F16’’ extracted from (a); (c) The ‘‘Baboon’’ stego-image; (d) The reconstructed secret image ‘‘Lena’’ extracted [68]

Arena et al [70] they presented new methods for MPEG-2 coded video sequences. They have selected to work in the domain of the bit stream. This is done to make the embedding process of data simpler in the way that where the original data in a compressed shape. Depending on the advantages of an interleaved encoding exploitation technique and consideration of frequency masking and some space, they had been capable to minimize the original algorithm BER.

Noda et al [71] presented two methods in JPEG steganographic. This is done by using QIM (Quantization Index Modulation) in DCT (The Discrete Cosine Transform) domain. The two techniques approximately protect the quantized DCT histogram coefficients, planning to safe.

2.9. Summary

In this project three techniques are initiated, Cryptography and Steganography techniques and the mixture of three methods. These methods are a Least Significant Bit (LSB), a chaos mapping via using one or more methods and a 3D Skew Tent Map. The first method is to use the cryptography technique for a text message and then embedding the encrypted message in a cover. The second method is by using the double hiding. The third method is used a chaos-based image encryption system by using tent map. The embedding methods are different in new techniques, where the LSB method is used in the first method, the chaos procedure is used in the second method and 3D Skew Tent Map in the third method. New algorithms are proposed to overcome steganalysis. These techniques supply an advanced likeness between the stego and cover images, which results in an improved imperceptibility. The combination between Cryptography and Steganography techniques supply protected means of private communication between two techniques. In the future, these methods can be expanded, in order to organize the message that is attained by the encryption of images to create meaningful words. These techniques avoid steganalysis, which is done by the other techniques.

A significant part of image processing is concealing confidential information inside a cover media, to be able to send it securely over an unsecured network (like the Internet).

This scheme is highly used to send account codes, corporation account information, and personal information. In this project, two methods are used to achieve successful hiding data, which are image steganographic and massage inserted to an encrypted Image Method

CHAPTER THREE
DESIGN AND ANALYSIS

3.1. Overview

In this thesis, three methods are utilized for hiding data within images in order to secure data transmission. The security of the transmitted information will be improved during replacing data from a transmitter to a receiver in a way that these data will not be seen by anybody else as well as enhance the image visual properties, decrease the embedding data that causes errors and eliminate the wrong contours.

In steganography, the image compression methods are widely utilized. There are two kinds of image compressions, which are lossless compression and lossy compression.Loss less compression arrangements provide more guarantees. There are characteristic examples of lossless compression arrangements, which are Microsoft's BMP (Bitmap) and CompuServe's GIF (Graphics Interchange Format).

An 8-bit picture size for execution of the steganography is utilized. Several steganography professionals propose utilizing pictures featuring 256 shadows of gray as the palette, when an 8-bit picture is utilized as the cover-picture. Since the shadows alter very slowly between palettes admissions, the grey-scale pictures are chosen, and this raises the picture's capability to conceal data. A picture encoding method is selected, when an appropriate cover picture has been chosen.

Recently, there are several redoubtable challenges that are created throughout digital content to content improvers, dispensers, aggregators. To improve more tough schemes, the obliteration, removal or alteration of the embedded text is needed. Thus, that the digital content processing and association develop into simplicity [72].

Hiding the picture existence as stego-pictures allows embedding the secret text to cover up pictures, as a result of the change from cryptography to steganography. Steganography theoretically involves that the text to be spread is not observable to the familiar eye. For many years, Steganography has been utilized, in order to spread information without being interrupted by unneeded observers. The major purpose of Steganography is essentially concerned with the security of contents of the concealed data, which that what is called the art of hiding data in data [72].

Since, a great quantity of unnecessary space is produced in the accumulating of pictures, pictures are considered to be a perfect for data. Steganography includes of techniques of spreading secret texts. Indefinite cover transporters transport these secret texts in such a way that the very reality of the embedded texts is unnoticeable. Transporters contain pictures, content, video, audio or any other digitally signified code or spreading. The concealed text might be code text, simple text or something that could be signified as a bit stream [73, 74].

3.2. Evaluation of Image Quality

For comparing stego picture with cover outcomes needs a calculation of image quality, generally the utilized measures are Mean-Squared Error, Peak Signal-to-Noise Ratio and histogram.

3.2.1. Mean-Squared Error

The mean-squared error (MSE) between two images $I_1(m,n)$ and $I_2(m,n)$ is: [72]

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

Where M and N are the number of rows and columns in the input pictures, respectively. Mean-squared error is based on strongly on the picture concentration scaling. A mean-squared error of 100.0 for an 8-bit picture with pixel values in the range 0-255 seems terrible; but a MSE of 100.0 for a 10-bit picture with pixel values in [0, 1023] is hardly perceptible.

3.2.2. Peak Signal-to-Noise Ratio

Peak Signal-to-Noise Ratio (PSNR) prevents this difficulty by scaling the MSE in accordance with the picture range: [72]

$$PSNR = 10\log_{10}\left(\frac{R^2}{MSE}\right) \qquad (3)$$

Where R is the maximum possible pixel value of the image, PSNR is measured in decibels (dB). PSNR is a fine measure for comparing restitution outcomes for the similar picture, but comparisons between pictures of PSNR are insignificant.

3.2.3. Histogram

The number of components inside a range is count up by the histogram functions and these functions demonstrate each range as a rectangular bin. The number of values that drop inside each range is signified by the height or length when utilizing rose of the bins. A picture histogram is a diagram that illustrates the allocation of concentrations in an indexed or concentration picture. Histograms for all the three color parts are computed, as color pictures are considered for testing.

3.3. Encryption Method

It is one of the methods that are used in hiding data technique, which it is applied for content and pictures. The image is encrypted in such a way that the entire pixels in the picture is multiplied with definite key which has similar size of the picture. At the recipient part it multiplied with the opposite of that key to supply the novel picture. In the case of content, each letter is translated to its ascii code and change it by definite number.

In the subsequent code, it signifies how to create encryption for definite text. The letters are translated to ascii code by utilizing “double”, then restructured and multiplied with definite key “m” and lastly subtract 32 to formulate encryption part. In case of decryption it is multiplied with opposite 3 key and adds 32 to obtain the novel text. To explain the method, see Figures 3.1 and 3.2.

```
s = 'This is a test!'
y=double(s)
z = reshape (y, 3, 5);
m = [1 5 3; 2 11 8; 4 24 21];
k=inv(m);
zz=z-32
d=m*(z-32)
ncode = mod (m*(z-32), 95) + 32
scode = reshape (char(ncode), 1, 15)
ncode = reshape (double(scode), 3, 5)
nnumb = mod (inv(m)*(ncode-32), 95) + 32
sorig = reshape (char(nnumb), 1, 15)
```

Figure 3.1: Encryption method/code test

The output of the code in each major step is demonstrated as in Figure 3.2

```
s =This is a test!

y=  84  104  105  115   32  105  115   32   97   32  116  101  115  116   33

zz =
  52   83   83    0   83
  72    0    0   84   84
  73   73   65   69    1

d =
    631    302    278    627    506
   1480    750    686   1476   1098
   3469   1865   1697   3465   2369

ncode =
  93   49  120   89   63
  87  117   53   83   85
  81   92  114   77  121

scode =
]WQ1u\x5rYSM?Uy

ncode =

  93   49  120   89   63
  87  117   53   83   85
  81   92  114   77  121


nnumb =
  84  115  115   32  115
 104   32   32  116  116
 105  105   97  101   33

sorig =
This is a test!
```

Figure 3.2: Output of the code

3.4. Image Analysis

There are several types for analyzing the image in LSB such as LSB in BMP, LSB in PNG and LSB in GIF. LSB formulates the use of BMP picture, because BMP utilizes lossless compression. A very great cover picture will be needed, in order to be able to conceal a secret text within a BMP file. BMP pictures of 800 × 600 pixels were found to have less web purposes. Furthermore, such uses are not recognized as suitable. Thus, LSB Steganography has been improved for use with other picture file arrangements. Some of the major picture steganographic methods were suggested, where there are a great variety of approaches to conceal data in pictures. LSB in GIF pictures has the probability of concealing a big text, but just when the most appropriate cover picture has been selected. Table 3.1 shows a comparison of LSB techniques for various file formats.

Table (3.1): A comparison of LSB techniques for various file formats [72]

	Lsb In BMP	LSB in GIF	LSB in PNG
Percentage Distortion less resultant image	High	Medium	High
Amount of embedded data	High	Medium	Medium
Steganalysis detection	Low	Low	Low
Image manipulation	Low	Low	low

3.5. The proposed Methods

There will be a comparison between the three suggested methods according to some criteria such as: complexity, processing time and security.

- Complexity: in this work, the complexity is related to the strength of the algorithm for embedding the data.
- Processing time: in this work, processing time is related to the time required for the algorithm to be done for whole the image.
- Security: in this work, security issue is related to the hiding the data in high level of encryption.

3.5.1. LSB Steganography Method (First Method)

The identification LSB of Steganography in Color and Gray- Scale pictures could be concerned throughout the enhancement in steganographic methods, and these pictures were detained to gray scale pictures in the primary levels. There are several solutions to solve the complexity in color pictures managing, such as color pictures and the length of the inserted text that it is approximated, the analysis of the difference of the gradient energy and the secret text inserted in the objective picture which is noticed in both gray and color pictures.

Investigators study the Image Steganography extensively. There are several selections of techniques that are utilized for which data could be concealed in pictures such as:

- In Least Significant Bit Replacement Method, image steganography approximately all information hiding methods try to modify unimportant

- data in the cover picture. Least Significant Bit (LSB) addition is a general easy approach for inserting data in a cover picture. An easy system is suggested, in order to put the inserted information at the Least Significant Bit (LSB) of each pixel in the cover picture. The modified picture is named stego-image. Changing LSB doesn't modify the quality of picture to person observation but this system is sensitive to the selection of picture processing attacks such as compression, cropping and so on.

- Moderate Significant Bit Replacement method: in this method to a secret text, the moderate significant bits of each pixel in the cover picture could be utilized. This technique enhances sensitivity to alteration, except that it mortifies the quality of stego-image.

The least significant bit means that the eighth bit within a picture is modified to a bit of the secret text. When utilizing a 24-bit picture, one could accumulate 3 bits in each pixel by altering a bit of each of the red, green and blue color elements, given that they are each signified by a byte. An 800 × 600 pixel picture could be able to accumulate a whole quantity of 1,440,000 bits or 180,000 bytes of inserted information. A grid of a 24-bit for 3 pixels picture could be as follows:

(01010101 01011100 11011000)
(10110110 11111100 00110100)
(11011110 101100101 01101011)

When the number 300, which binary illustration is:

101101100 is inserted within the least significant bits of this fraction of the picture, the resultant grid is as follows:

(00101101 00011100 11011101)
(10100111 11000100 00001101)
(11010011 10101100 01100010)

The number 300 was inserted within the first 8 bytes of the grid, just the 5 bits required to be modified in accordance with the inserted text. Generally, just half of the bits in a picture would require to be changed to conceal a secret text utilizing the highest cover size. Altering the LSB of a pixel results in small alterations in the concentration of the colors, given that there are 256 probable concentrations of each main color. The person eye could not recognize these alterations, so the text is effectively concealed. One could even conceal the text in the LSB without detecting the variation, with a well-selected picture.

A. Design Details

1. Read the novel picture and the picture which is to be concealed in the novel picture.
2. Change the picture to conceal in the cover picture by X bits.
3. As well as the novel picture or cover picture with 240 that is 11110000, thus four MSb's set to 0.
4. The changed concealed picture and the outcome of step 3 are battered. This creates alterations only in the X LSB bits, thus that the picture is concealed in the novel picture.

The picture could be transformed to uint8 format in MATLAB, which this picture is named the stego image. Figure 3.3 shows the block diagram for implemented logic of LSB embedding.

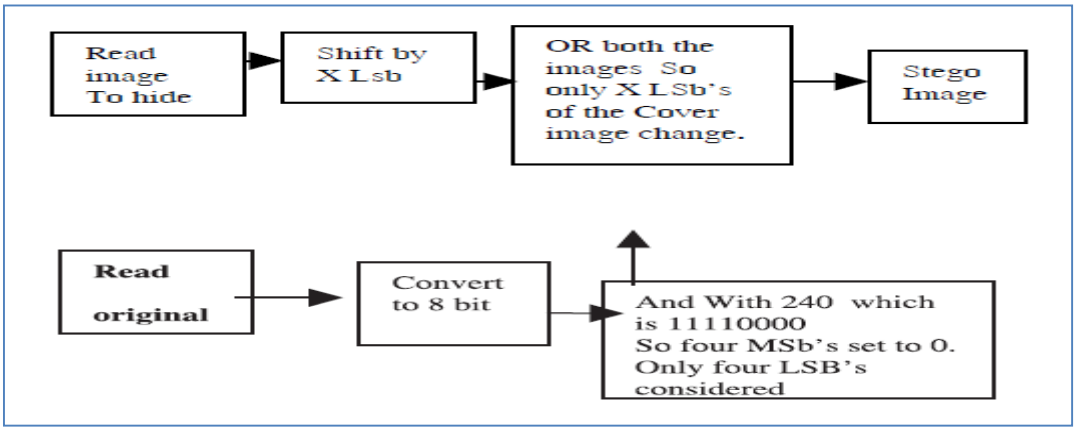

Figure 3.3: The block diagram for implemented logic of LSB embedding [72]

B. Algorithm for Steganalysis

1. The stego picture is bit changed by 4 bits, because it was changed by 4 bits to be embedded within the novel picture.
2. Then, this picture ANDED with 255, which means 11111111 that, provides the novel picture.
3. Primarily all the LSB's were made 0, since it is ANDED with 255. But now, it is improved.
4. To obtain it to Uint8 format, it is transformed back to uint8 that is the removed picture.

Figure 3.4 shows the block diagram for Steganalysis.

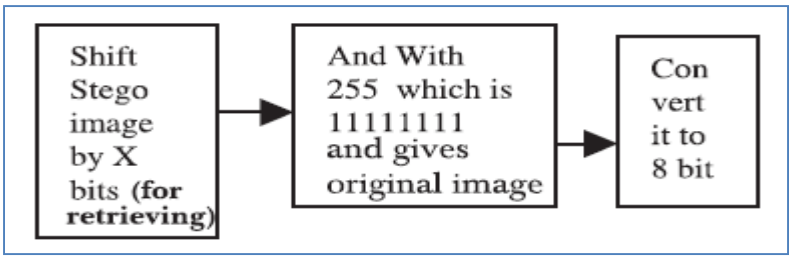

Figure 3.4: The block diagram for Steganalysis [72]

In general the flow chart of this method is illustrated as in Figure 3.5:

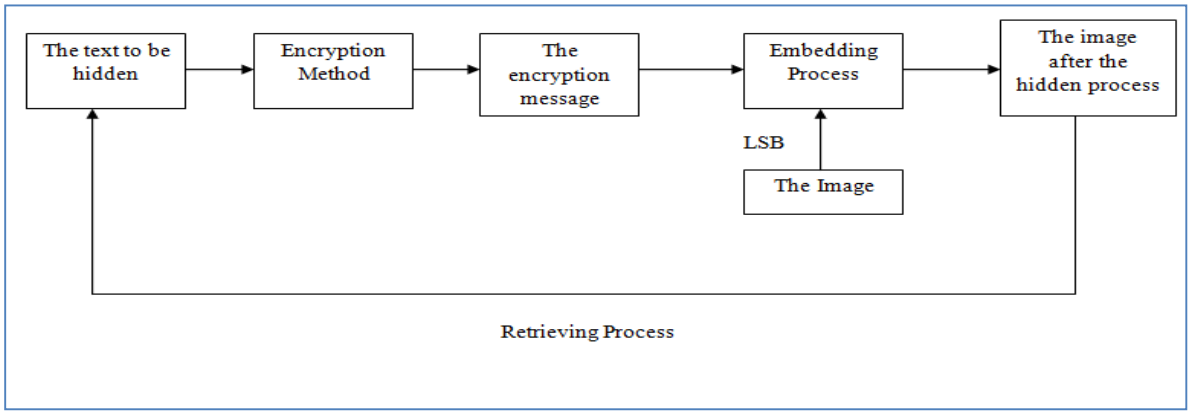

Figure 3.5: Flow Chart of first method

3.5.2. Chaos based Spatial Domain Steganography Method (Second Method)

Recently, Steganography has a significant position in protected communication. Steganography is defined as a method of inserting secret data within cover media such as audio, picture, video and content. Thus the sender and the certified receiver could notice the existence of secret data. Spatial Domain Steganography utilizing 1-Bit Most Significant Bit (MSB) with chaotic method is suggested in this project

A. Design Details

The cover picture is decayed within blocks of 3*3 matrix of identical size. The first block of cover picture is inserted with 8 bits of higher bound and lower bound values which are needed for recovering load at the end. To insert load in 3bits of Least Significant Bit (LSB) as well as one bit of MSB in chaotic method, the means of centre values and variation between uninterrupted pixels is verified. In recent days, the capability and safety is developed compared to the presented techniques with practical PSNR.

The flow chart of Chaos based Spatial Domain Steganography using MSB (CSSM) algorithm is illustrated in Figure 20, which consists of:

1. Cover Image Partition: To confirm the algorithm, the cover image of JPG, BMP, TIF, PNG formats with dissimilar dimensions are taken into account. To raise safety and capability of load, the cover image is separated within 3*3 blocks.
2. Upper and Lower Bound: To obtain best $PSNR$, locate the Upper Bound (UB) and Lower Bound (LB) values with highest Range (R) of 200. Insert pixel (1,1) and (3,3) and embed using chaos algorithm.

Upper Bound Embedding Position (UBEP)

$$UBEP = p_{(n,1)} \qquad (4)$$

Lower Bound Embedding Position (LBEP)

$$\mathrm{LBEP} = p_{(n,5)} \qquad (5)$$

$n = 1,2,\ldots,8$ (X-coordinate in 3*3 matrix block)

p is the pixel concentration magnitude in the cover picture.

Range: $R = UB - LB$ (6)

3. Mean of Median (Me): Think about second block and forwards. Compute the median magnitude of all columns in each block utilizing equation 7.

$M = \frac{1}{2}\{p_{(4,n)} + p_{(5,n)}\}$ (7)

$n = 1,2, \ldots ,8$ (Y-coordinate in 3*3 matrix block)

Mean of median magnitude s in each block is computed utilizing the Equation 8.

$M_e = \frac{1}{8}\{\sum_{i=1}^{8} M(i)\}$ (8)

4. The difference between the consecutive pixels (di): Compute the difference between consecutive pixels from second block of cover picture for inserting load utilizing equation 9.

   $\mathrm{di} = |p_i - p_{i+1}|$ (9)

   i is the index of pixels in 3*3 matrix block

5. $di \leq M_e$: Compare di and M_e, if the di is lower than M_e, so insert the load in both pixels p_i, p_{i+1} in the block of cover image.

6. Embed Payload: Divide each pixel within two identical fractions; most fraction and slightest fraction are illustrated in Figure 3.6.

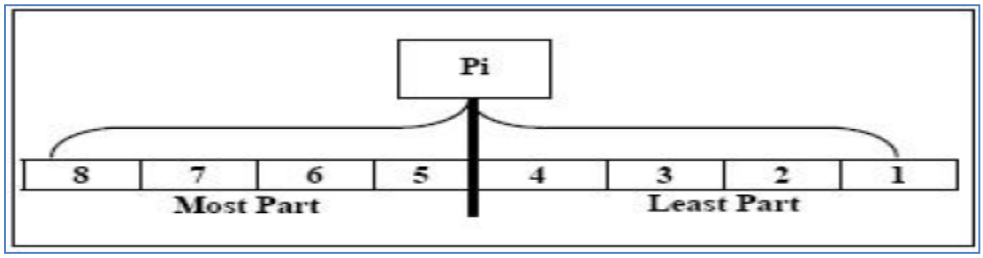

Figure 3.6: Splitting of pixel [75]

Count up the number of ones in the first three bits of most fractions, $8^{th}, 7^{th}$ and 6^{th} locations in the pixel and insert a load in the pixel as shown in Table 3.2.

Table (2.2): Inserting load case [75]

Number of ones in the three bits of most part	Case	Number of bits to embed
0	Case 0	1 bit
1	Case 1	3 bits
2	Case 2	2 bits
3	Case 3	3 bits

- Counter A: Whole number of bits inserted in the 1^{st} location of cover picture pixel in case 2 and case 3.
- Counter B: Whole number of bits inserted in the 5^{th} location of cover picture pixel in case 2 and case 3.
- Counter C: Number of bits inserted in the 2^{nd} location of cover picture pixel in case 2.
- Counter D: Number of bits inserted in the 3^{rd} location of cover picture pixel in case 3.

Case 0: Insert 1 bit of load pixel in the 5^{th} location of the cover picture pixel.

Case 1: Insert 3 bits of load pixel in the 1^{st}, 2^{nd} and 3^{rd} locations of the cover picture pixel.

Case 2: Load inserting in 5^{th} or 2^{nd} location together with 1^{st}location in a chaotic approach.

i. Insert 1^{st} bit of load in the 1^{st} location of cover picture pixel. Increase counter A.
ii. Insert 2^{nd} bit of load in both 2^{nd} or 5^{th} location of cover picture pixel.

- If counter A > LB and counter C > 5, then increase counter B, and if counter B < R, then insert in 5^{th} location of cover picture pixel. Reset counter C to 0.
- Else insert in 2^{nd} location of the cover picture pixel. Increase counter C.

Case 3: Load inserting in 5^{th} or 3^{rd} location together with 1^{st} and 2^{nd} location in a chaotic approach.

i. Insert 2^{nd} bits of load in the $1^{st}$and 2^{nd}location of cover picture pixel. Increase counter A and counter C.
ii. Insert 3^{rd} bit of load in both 2^{nd} or 5^{th} location of cover picture pixel.
   - If counter A > LB and counter D > 5, then increase counter B, and if counter B < R, then insert in 5^{th} location of cover picture pixel. Reset counter D to 0.
   - Else insert in 3^{rd} location of the cover picture pixel. Increase counter D.

B. Evaluation parameters:

a. Mean Square Error(MSE): It is described as the square of error between cover picture and stego-picture. The alteration in the picture could be calculated utilizing MSE. It is computed utilizing equation 10.

$$MSE = \left[\frac{1}{N*N}\right]^2 \sum_{i=1}^{N} \sum_{j=1}^{N} (X_{ij} - \bar{X}_{ij})^2 \qquad (10)$$

X_{ij}: The magnitude of the pixel in the cover picture.

$\bar{X}_{ij}$: The magnitude of the pixel in the stego picture.

N: Size of picture.

b. Peak Signal to Noise Ratio ($PSNR$): It is described as the measure of quality of the picture through comparing the cover picture with the stego-picture, i.e. it computes the fraction of the stego information to the picture fraction. $PSNR$ is computed by equation 11.

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} db \qquad (11)$$

c. Capacity: It is refers to the size of the information in a cover picture, in such a way that it could be adjusted without worsening the reliability of the cover picture. The steganographic inserting process requires protecting the statistical features of the cover picture also its perceptual quality. Capability is signified by bits per pixel (bpp).

d. Entropy: it is a calculation of safety for a steganography scheme. A scheme is completely protected when the Relative Entropy (RE) becomes Zero.

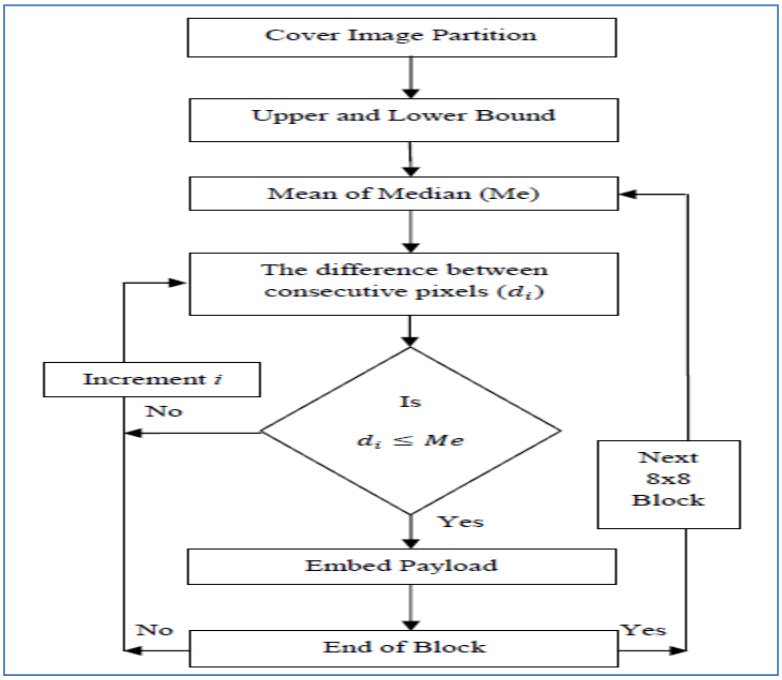

Figure 3.7: CSSM flow chart [75]

C. Algorithm

In this project, a cover picture and payload are considered in such a way that the payload is to be inserted within the cover picture to obtain stego-image utilizing LSB and 1 bit of MSB. So, there are some suppositions to achieve this, which are the stego-image is spread above an ideal channel as well as the cover and payload items are grayscale pictures with dissimilar dimensions.

Table 3.3 and Table 3.4 provide the payload inserting in a chaotic approach and recovery of payload from cover picture at the end respectively

Table (3.3): Embedding algorithm of CSSM [75]

Input: Cover image Output: Stego-image 1. Divide the cover image into blocks of 3*3. 2. Set lower bound and upper bound with max range of 200 to use fifth bit for embedding. 3. Embed lower bound and upper bound values in the first block of the cover image. 4. Determine Median (M) values for each block from second block and onwards. 5. Determine the Mean of Median values in each block. 6. Calculate the difference between consecutive pixel values in each block (di $= \|p_i - p_{i+1}\|$). 7. If $di \leq M_e$, then embed payload in the pixels p_i, p_{i+1} .

Table (3.4): Retrieving algorithm of CSSM [75]

Input: Stego-image

Output: Payload

1. Divide the stego-image into blocks of 3*3.
2. Retrieve the lower bound and upper bound values from the first block.
3. Determine Median (M) values for each block from second block and onwards.
4. Determine the Mean of Median values in each block.
5. Calculate the difference between consecutive pixel values in each block (di $= |p_i - p_{i+1}|$).
6. If $di \leq M_e$, then retrieve payload from the pixels p_i, p_{i+1} .

In general the flow chart of this method is illustrated in Figure 3.8:

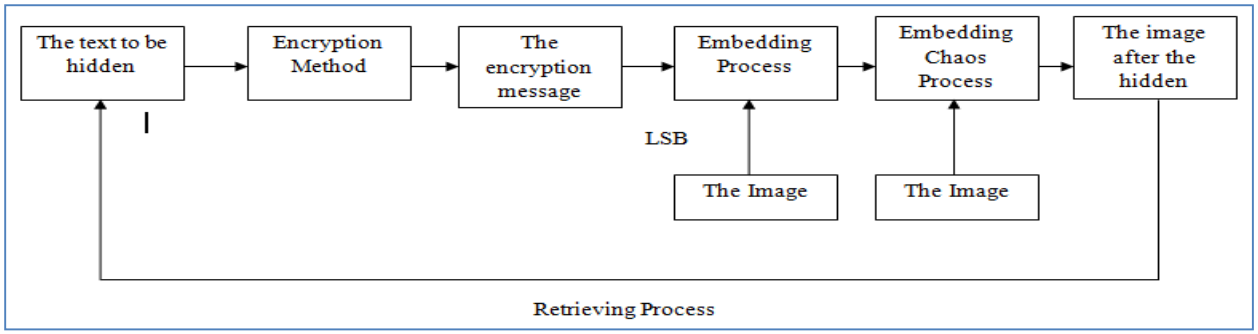

Figure 3.8: Flow chart of second method

A Chaos-based Image Encryption Scheme using 3D Skew Tent Map (Third Method)

Recently, due to the quick improvements in network communication and digital picture, extensive-spread distribution and electronic distribution of digital multimedia information have been communed over the wireless

networks and Internet. Thus, it has developed into imperative in order to avoid them from fails. Several applications need consistent, tough and quick protected scheme in order to accumulate and send out digital pictures. These applications are online confidential photograph album, military picture databases, medical imaging scheme and private video convention. The conditions to accomplish the required safety of digital pictures have led to the improvement of efficient picture encryption algorithms.

Digital images have some fundamental characteristics like redundancy of information, being less responsive as compared to the content information, bulk information ability and strong connection amongst adjoining pixels. Conventional encryption algorithms like RSA and DES (Data Encryption Standard) are not appropriate for realistic digital picture encryption owing to the limitation of low-stage efficiency in spite of encrypting pictures. Opportunely, chaos-based picture encryption algorithms have illustrated their higher behavior. Chaos has been established to cryptography as its periodicity, pseudo-randomness and understanding to primary circumstances and manage factors are about to uncertainty and dispersion in cryptography. These properties create chaotic schemes a probable selection for building cryptosystems.

The unimodal skew tent map $T_0: [0,1] \rightarrow [0,1]$ is given by:

$$T_0(x) = \begin{cases} x/a & ,if\ x \in [0,a] \\ (1-x)/(1-a) & ,if\ x \in [a,1] \end{cases} \quad (12)$$

Where, $x \in [0,1]$, is the condition of the scheme, and $a \in [0,1]$ is the control factor. It is a noninvertible conversion of the unit period against itself. As $= 0.5$, then T_0 is a regular tent map. See Figure 3.9.

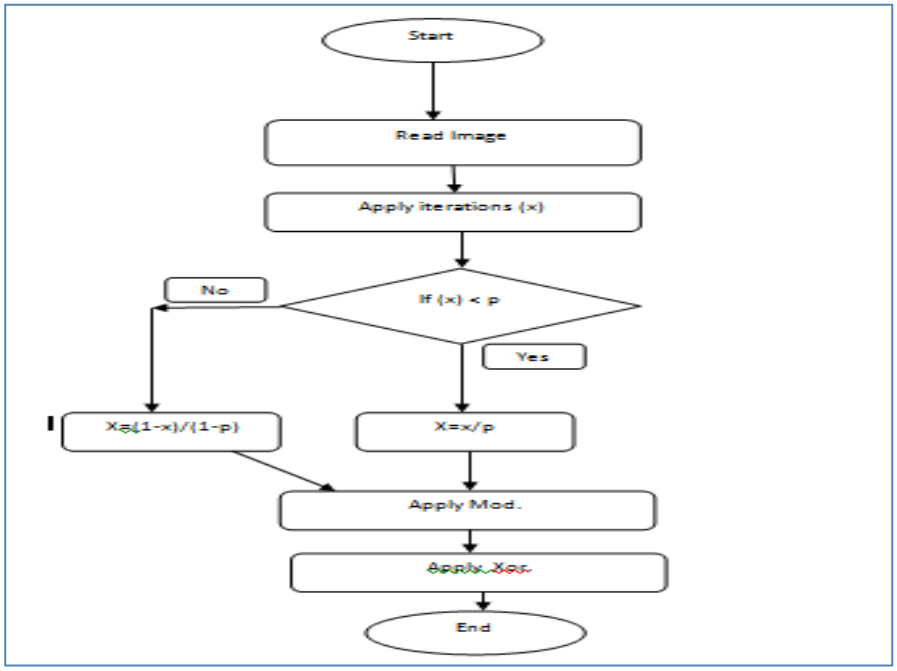

Figure 3.9: Third method

In general the flow chart of this method is illustrated as in Figure 3.10:

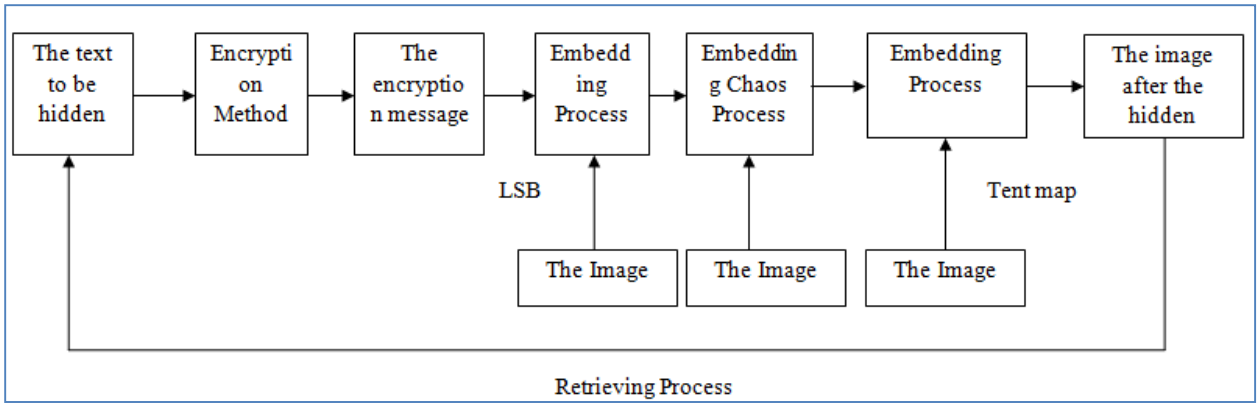

Figure 3.10 Flow chart of third method

3.5.3. Comparison

There will be a comparison between the three suggested methods according to some criteria such as: complexity, processing time and security, as mentioned previously in detailed.

In this project three methods are proposed; the first method is to use the cryptography technique for a text message and then embedding the encrypted message in a cover. The second method is by using the double hiding. The third method used a chaos-based image encryption system by using tent map. The embedding methods are different in new techniques, where the LSB method is used in the first method, the chaos procedure is used in the second method and 3D Skew Tent Map in the third method. After the execution MATLAB cods for the three algorithms. From the results, it is shown that the third algorithm took less time than the others and the first one took most time than the other, thus the third one could be better than the others in hiding data.

CHAPTER FOUR
IMPLEMENTATION AND TESTING

4.1. Introduction

Lately, people have been created new proficient and surreptitious ways to defend private data attributable to the development of the information technology and other technologies which are related to the data domain. Data safety and privacy become a developing necessary issue due to the fact that electronic communications are widely used and admitted as the main tools of communication. In hiding data technology, some methods use images to protect information, but there are defects within the image, so there are different methods to recognize this defect.

In this thesis, three methods for hiding data are suggested; the first method is by using encryption on a text and then using the Least Significant Bit (LSB) to embed the encrypted message. The second method is by using double cover. The embedding algorithm will be the Chaos algorithm. The third method is by using encryption on a text and then using the 3D Skew Tent Map algorithm to embed the encrypted message. In addition some of the characteristics of the MATLAB/SIIMULINK Software will be more efficient, proficient and easier to utilize. The aims and objectives of the project were determined to keep focusing with the research. The project includes all the principles and ideas of the main methods that are utilized for hiding data within images with their factors that have effects on the simulation and estimating the behavior of the proposed methods.

4.2. LSB Steganography Method (First Method)

In the first method, least Significant Bit Method, all information hiding methods are used by image steganography, in order to modify unimportant data in the cover picture. Least Significant Bit (LSB) is a common and simple approach for inserting data in a cover picture. Changing LSB doesn't alter the quality of image to individual observation but this system is sensitive to the selection of image processing attacks such as compression, cropping and so on.

4.2.1. Design and simulation

To evaluate and implement the performance of the system, the code for the first algorithm in the following figure is used.

The following code includes (imread) function that reads image (t.bmp) from graphics file, then convert RGB image or color-map to grayscale by using (rgb2gray) function. The image is displayed by (imshow) function as input image. The input image is titled with the name (orginal image) by (title) function. The input image is resized by (imresize) function. This function returns input image which is scale times to the size of [120,120].

```
RGB=imread('t.bmp');
XX=rgb2gray(RGB);
imshow(XX)
title('orginal image')
RGB=imresize(RGB,[120,120]);%%% dynamic any image can be input
```

The following code includes converting to double precision by (double) function that returns the double-precision value for ((YY)/255).

The histogram of image data is displayed by (imhist) function which displays a histogram for the image YY above, a grayscalecolorbar. The input image is titled with the name (histogram for orginal image) by (title) function. Then, the function (mat2cell) divides the two-dimensional matrix YY into adjacent sub-matrices, each contained in a cell of the returned cell array ms.

```
YY=rgb2gray(RGB);
imshow(YY)


YY=double(YY)/255;
figure
imhist(YY); %%%%  histogram
title('histogram for orginal image')

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%


% %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
ms=mat2cell(YY,[3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 ]...
    ,[3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3   ]);
```

The following code includes (fopen) that opens the file codee.txt for binary read access with the specified permission (r). Then (fread) function reads data in binary format from the file specified by fid into matrix c. after that, new matrix xtot is created using For loop. Finally, the matrix xt using For loop.

```
fid = fopen('codee.txt','r');
c = fread(fid, '*char')'

xtot=[];
for ii=1:length(c)
ee=double(c(ii));
x11=dec2bin(ee);
xtot=[xtot,x11];
end
XT=[];
 xtot_vec=double(xtot);%%%%%%%% 49 is 1, 48 is 0
 g=size(xtot_vec);
 for i=1:g(1)
     xt=CONVERTT(xtot_vec(i,:));
     XT=[XT;xt];
 end

 XBACK=XT;
```

The following code includes reshaping array Rtots by using (reshape) function that returns the 40-by-40 matrix Rtots whose elements are taken column-wise from ms. Then, it displays the maximum value of size for the matrix Rtots with sentence(size of the data in bits is). The (alpha) variable is set to 0.5. The matrix Iw uses For loop. In For loop, variable is defined and is equal to Rtots{1,i}and variable (b) is defined and is equal to XT(1,I) and iw value is equal to built function which is(make_water_mark(a,b,alpha)).

```
Rtots=reshape(ms,[1,40*40]);
BACKUP=Rtots;

disp('size of the data in bits is')
R=max(size(Rtots));
disp(R)


 alpha=0.5;
 IW=[];
 for i=1:length(c)

     a=Rtots{1,i};
     b=XT(1,i);
     iw=make_water_mark(a,b,alpha);

     iw={iw};
     IW=[IW,iw];
 end
 %

for i=1:length(c)
Rtots{1,i}=IW{1,i};
end
```

The function (make_water_mark(a,b,alpha)) includes matrix iw, pii variable is equal to a(2,2) and gc is equal to (1-alpha).*(pii)+(alpha.*b)

```
function [iw]=make_water_mark(a,b,alpha)



pii=a(2,2);

gc=(1-alpha).*(pii)+(alpha.*b);


iw=[a(1,1), a(1,2), a(1,3); a(2,1), gc, a(2,3); a(3,1), a(3,2), a(3,3)];
```

The following code includes reshaping array (cover) by using (reshape) function that returns the 40-by-40 matrix (cover) whose elements are taken column-wise from Rtots. Then, cell2mat (cover) function converts a multidimensional cell array cover with contents of the same data type into a single matrix cover. Then the matrix cover is multiplied by 255. The matrix Yout is displayed and then the histogram of image data is displayed by (imhist) function which function displays a histogram for the image Yout above a grayscalecolorbar. The input image is titled with the name (histogram for image with hidden data) by (title) function. Then, peak signal-to-noise ratio (PSNR) between images A and B is computed.

```
coverr=reshape(Rtots,[40,40]);
coverr=cell2mat(coverr);


Yout=(coverr)*255;

figure
imshow(uint8(Yout))

figure
imhist(double(coverr)); %%%%  histogram
title('histogram for image with hidden data')


YY=double(YY);
A=(YY);
out=double(Yout);
B=(out)./max(max(out));
SNR=PSNR(A,B)

toc
```

4.2.2. Results

The results for the first algorithm are shown as follows, there are four cases; two images and two texts are used in these cases:

For case 1 and case 2, image t1 is used with two different texts. The image t1 and the histogram of the image t1 (input image) before embedding process are shown as follows in Figures (4.1&4.2):

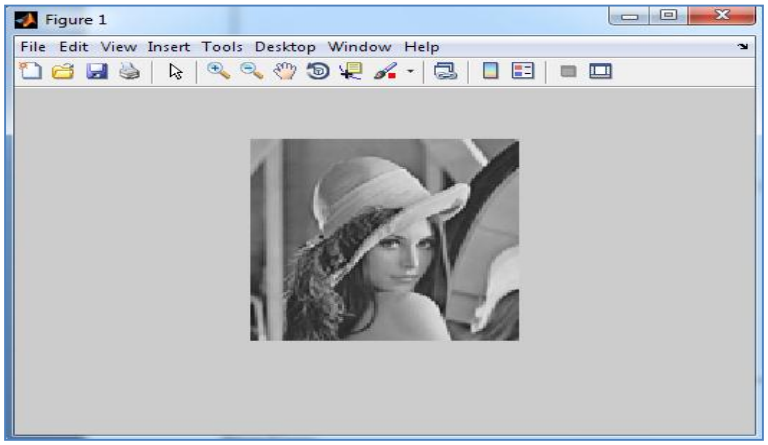

Figure 4.1 : Image (t1) before embedding

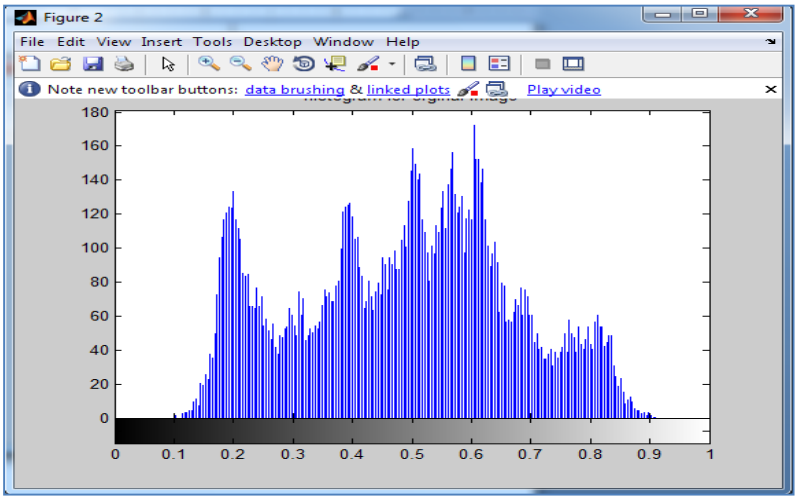

Figure 4.2 : The histogram for image (t1) before embedding

Case 1 (image t1):

For case 1, image t1 is used with (this is test) text. The Size of the data in bits is 1600. From the results of the embedding process throughout the execution of the MATLAB code of the first algorithm, it is found that the value of SNR is 25.6486 and the elapsed time that is needed for the first algorithm to be executed is 7.509200 (in seconds). The image t1 and the histogram of the image t1 after embedding process are shown as follows in Figures (4.3&4.4):

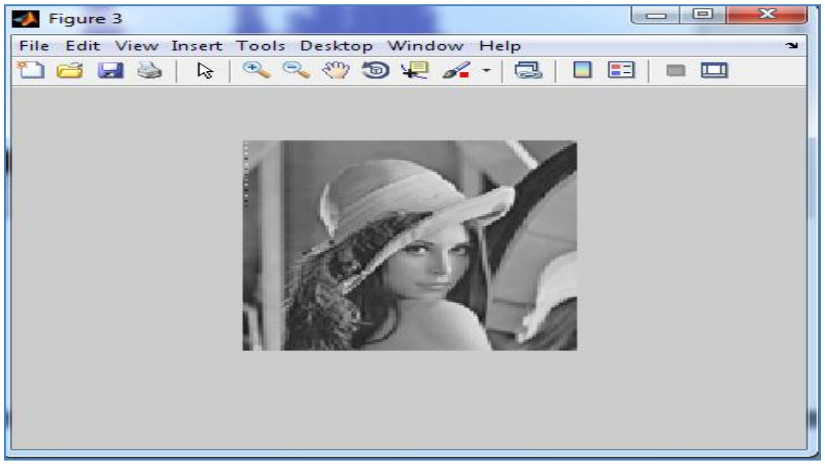

Figure 4.3 : Case 1: Image (t1) after embedding

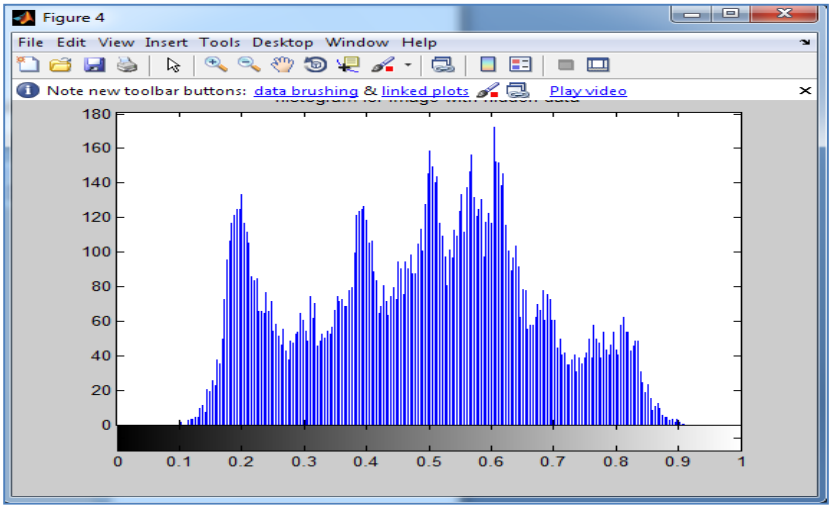

Figure 4.4 : Case 1: The histogram for Image (t1) after embedding

In this case, there is no difference between the input image and the image after embedding process in terms of intensity and clarity of the image. Also the histogram does not change after the embedding process.

Case 2 (image t1):

For case 2, image t1 is used with (this is test file for first algorithm) text. The Size of the data in bits is 1600. From the results of the embedding process throughout the execution of the MATLAB code of the first algorithm, it is

found that the value of SNR is 25.3981 and the elapsed time that is needed for the first algorithm to be executed is 5.526542 (in seconds). The image t1 and the histogram of the image t1 after embedding process are shown as follows:

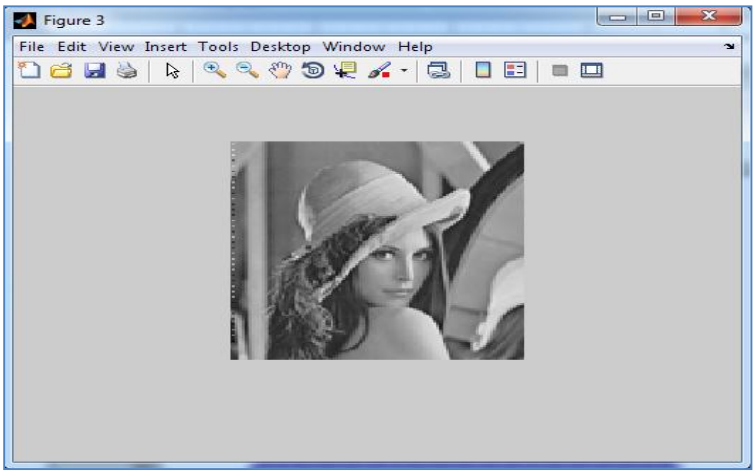

Figure 4.5 : Case 2: Image (t1) after embedding

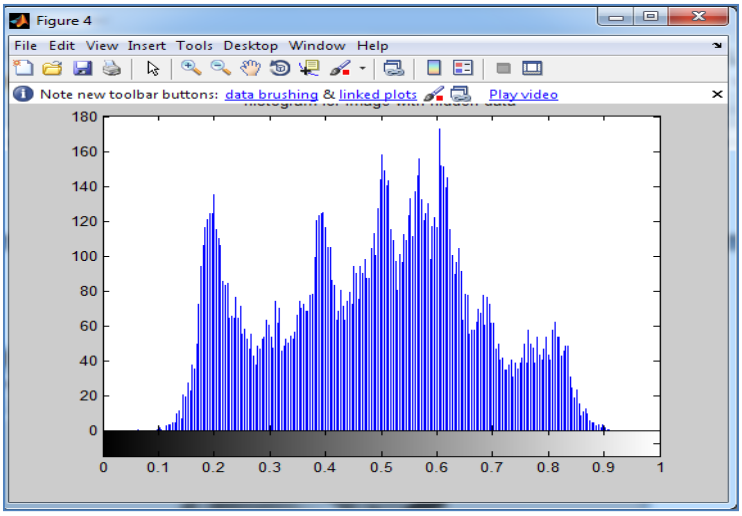

Figure 4.6 : Case 2: The histogram for image (t1) after embedding

Similarly in case 2 there is no difference between the input image and the image after embedding process in terms of intensity and clarity of the image. In addition the histogram does not change after the embedding process.

For case 3 and case 4, image t3 is used with two different texts. The image t3 and the histogram of the image t3 (input image) before embedding process are shown as follows:

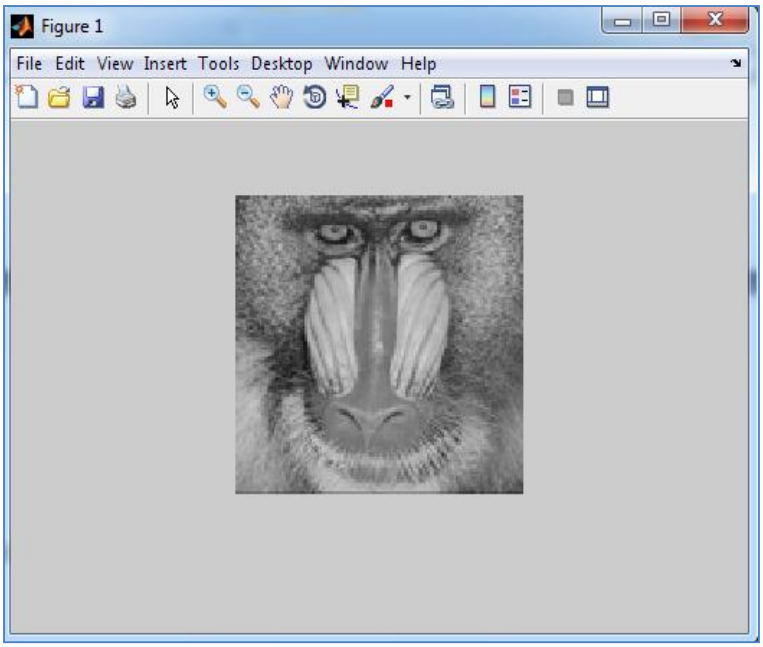

Figure 4.7 : Image (t3) before embedding

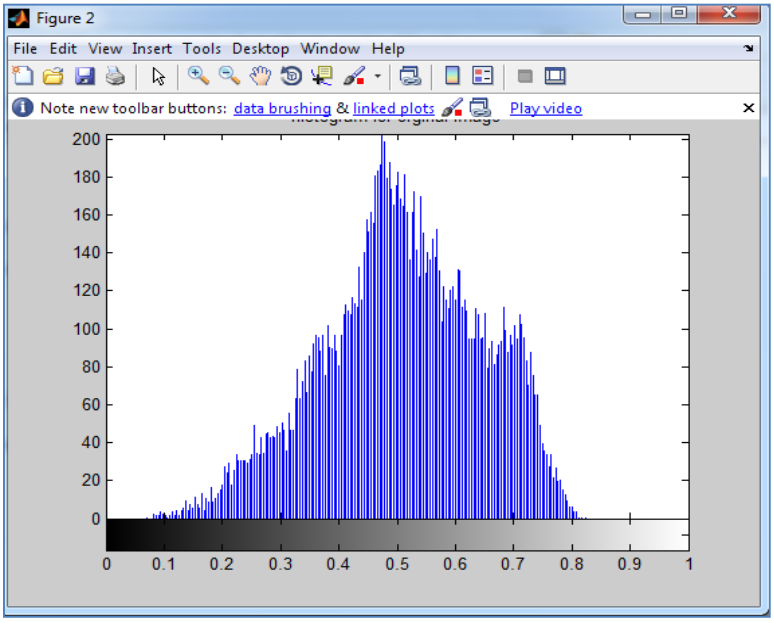

Figure 4.8 : The histogram for image (t3) before embedding

Case 3 (image t3):

For case 3, image t3 is used with (this is test) text. The Size of the data in bits is 1600. From the results of the embedding process throughout the execution of the MATLAB code of the first algorithm, it is found that the value of SNR is 18.9135 and the elapsed time that is needed for the first algorithm to be executed is 1.353972 (in seconds). The image t3 and the histogram of the image t3 after embedding process are shown as follows:

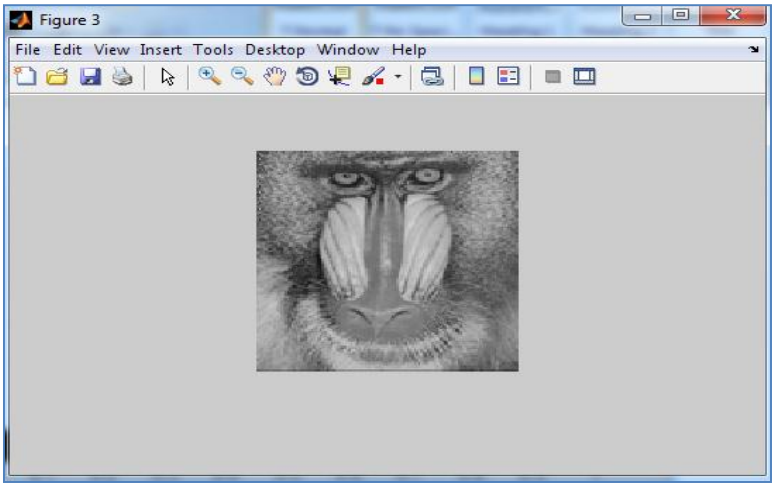

Figure 4.9 : Case 3: Image (t3) after embedding

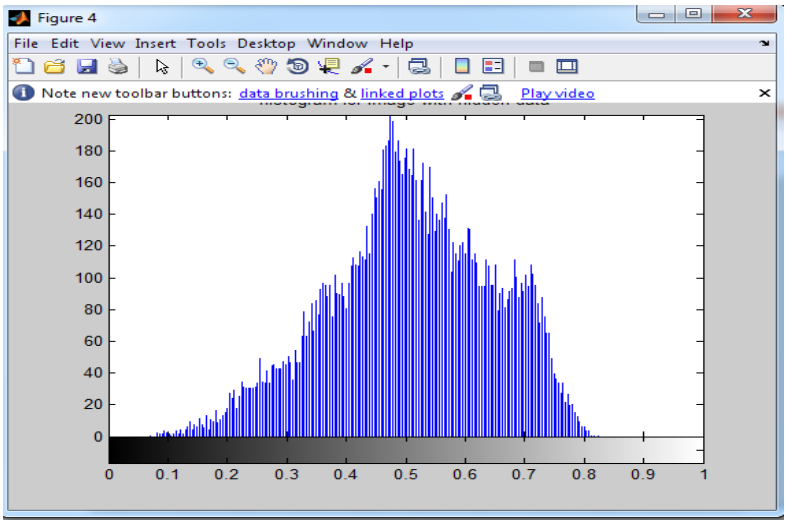

Figure 4.5 : Case 3: The histogram for image (t3) after embedding

In case 3, there is no difference between the input image and the image after embedding process in terms of intensity and clarity of the image. Further more, the histogram does not change after the embedding process.

Case 4 (image t3):

For case 4, image t3 is used with (this is test file for first algorithm) text. The Size of the data in bits is 1600. From the results of the embedding process throughout the execution of the MATLAB code of the first algorithm, it is found that the value of SNR is 21.1251and the elapsed time that is needed for the first algorithm to be executed is 1.400884 (in seconds). The image t3 and the histogram of the image t3 after embedding process are shown as follows:

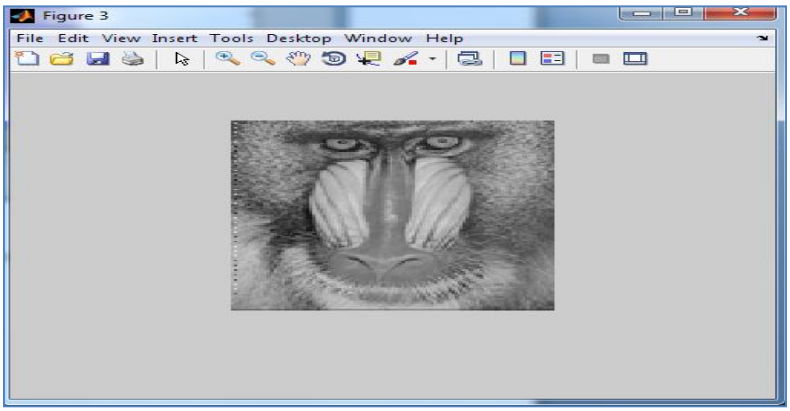

Figure 4.6 : Case 4: Image (t3) after embedding

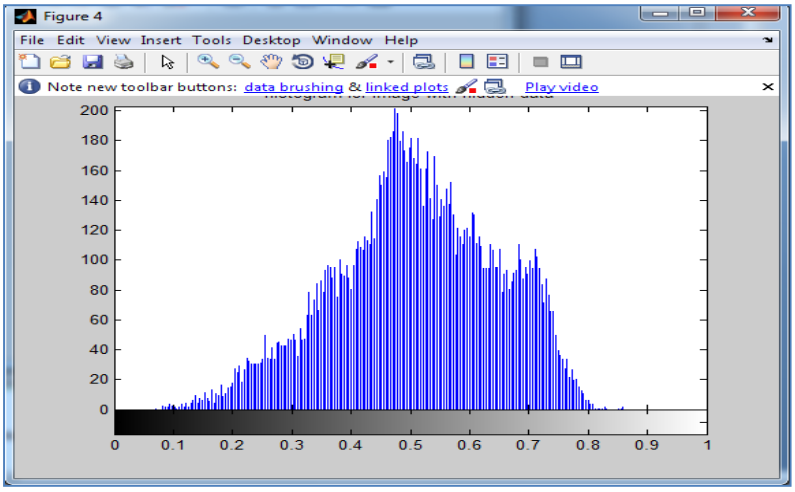

Figure 4.7 : Case 4: The histogram for image (t3) after embedding

As in case 3, in case 4 there is no difference between the input image and the image after embedding process in terms of intensity and clarity of the image. The histogram does not change after the embedding process.

4.3. Chaos based Spatial Domain Steganography Method (Second Method)

In the second method, Spatial Domain Steganography, which uses1-Bit Most Significant Bit (MSB) with chaotic method, attributable to that the steganography has an important role in protected communication. Steganography is a technique of inserting secret data within cover audio, picture, video and content, so the sender and the specialized receiver could detect the existence of secret data.

4.3.1. Design and simulation

The code for the second algorithm is similar to the code for the first algorithm, but it differs in such a way that each algorithm has its for loop which includes

its own built function. In this algorithm, the built function (make_embed_second(a,b,alpha)) includes matrix iw, p1 variable is equal to a(1,1)and p2 is equal to a(3,3) and gc is equal to (1-alpha).*(pii)+(alpha.*b).

```
function [iw]=make_embed_second(a,b,alpha)

p1=a(1,1)
p2=a(3,3)

pii=(p1+p2)/2;

gc=(1-alpha).*(pii)+(alpha.*b);


iw=[a(1,1), a(1,2), a(1,3); a(2,1), gc, a(2,3); a(3,1), a(3,2), a(3,3)];
```

4.3.2. Results

The results for the second algorithm are shown below, there are four cases, two images and two texts are used in these cases:

For case 1 and case 2, image t1 is used with two different texts. The image t1 and the histogram of the image t1 (input image) before embedding process are shown as follows:

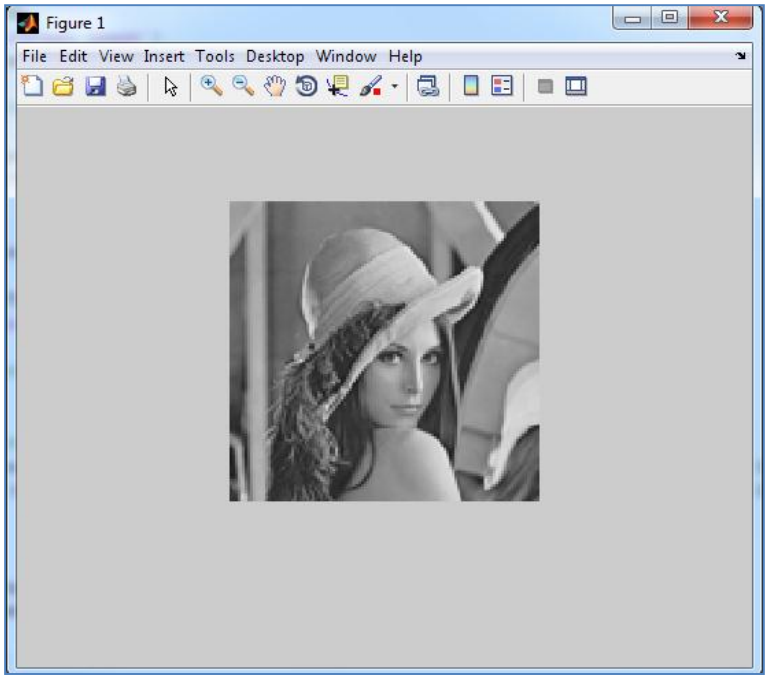

Figure 4.13 : Image (t1) before embedding

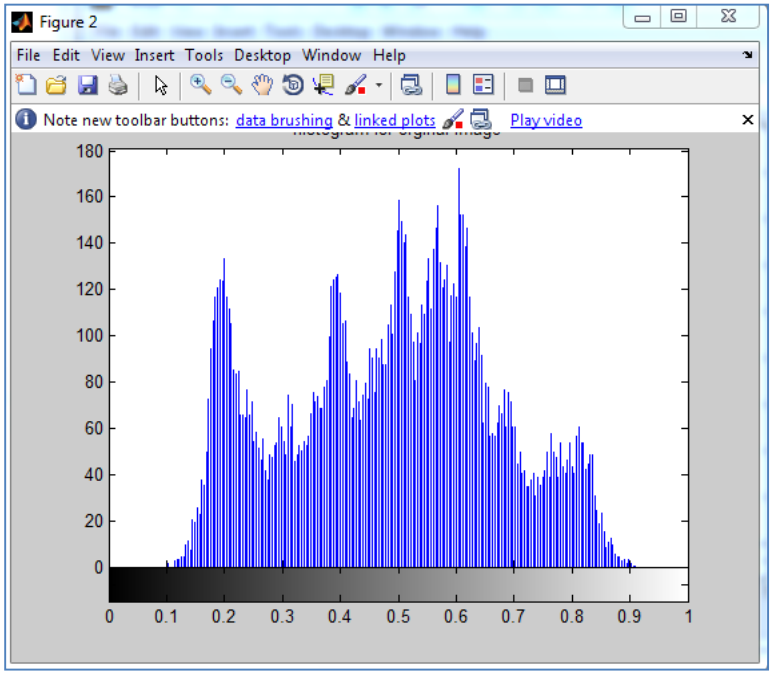

Figure 4.14 : The histogram for image (t1) before embedding

Case 1 (image t1):

For case 1, image t1 is used with (this is test) text. The Size of the data in bits is 1600. From the results of the embedding process throughout the execution of the MATLAB code of the second algorithm, it is found that the value of SNR is 25.6413 and the elapsed time that is needed for the second algorithm to be executed is 4.384285 (in seconds). The image t1 and the histogram of the image t1 after embedding process are shown as follows:

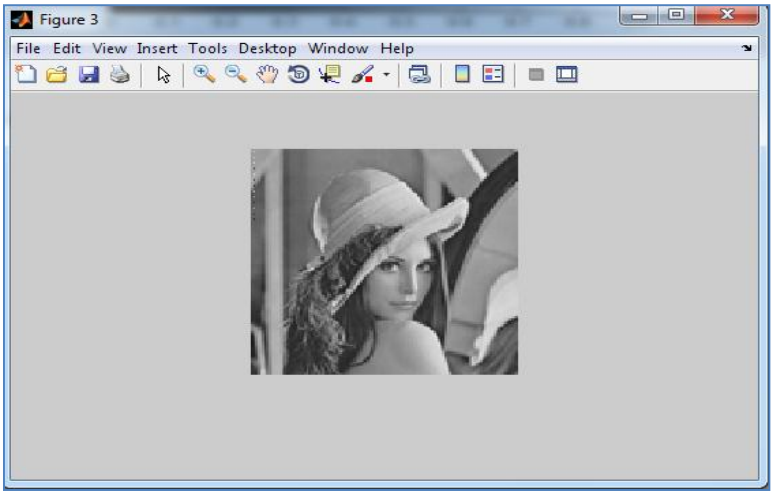

Figure 4.15 : Case 1: Image (t1) after embedding

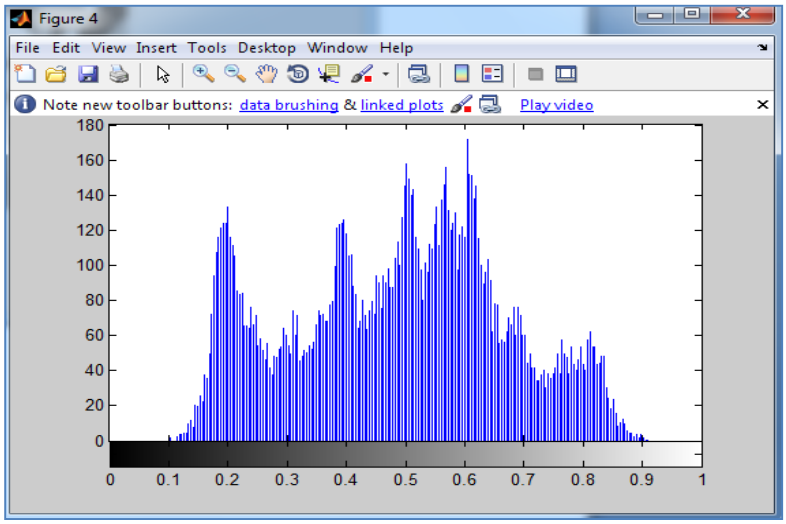

Figure 4.16 : Case 1: The histogram for image (t1) after embedding

In this case, there is no difference between the input image and the image after embedding process in terms of intensity and clarity of the image. In addition the histogram does not change after the embedding process.

Case 2 (image t1):

For case 2, image t1 is used with (this is test file for first algorithm) text. The Size of the data in bits is 1600. From the results of the embedding process throughout the execution of the MATLAB code of the second algorithm, it is found that the value of SNR is 25.3809 and the elapsed time that is needed for the second algorithm to be executed is 1.355209 (in seconds). The image t1 and the histogram of the image t1 after embedding process are shown as follows:

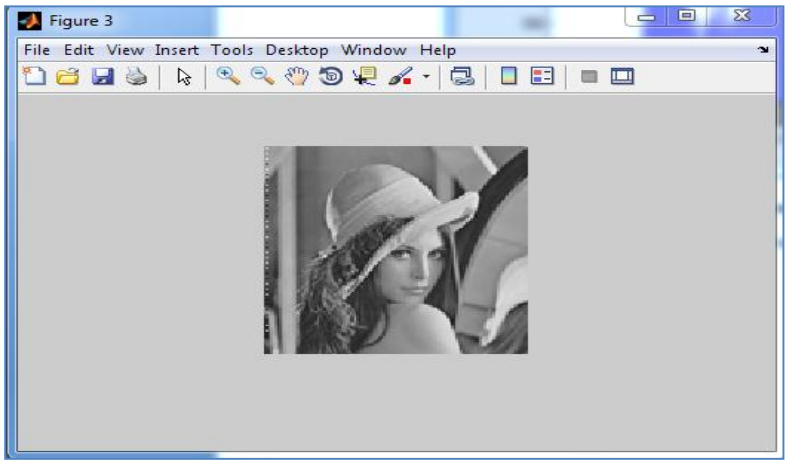

Figure 4.17: Case 2: Image (t1) after embedding

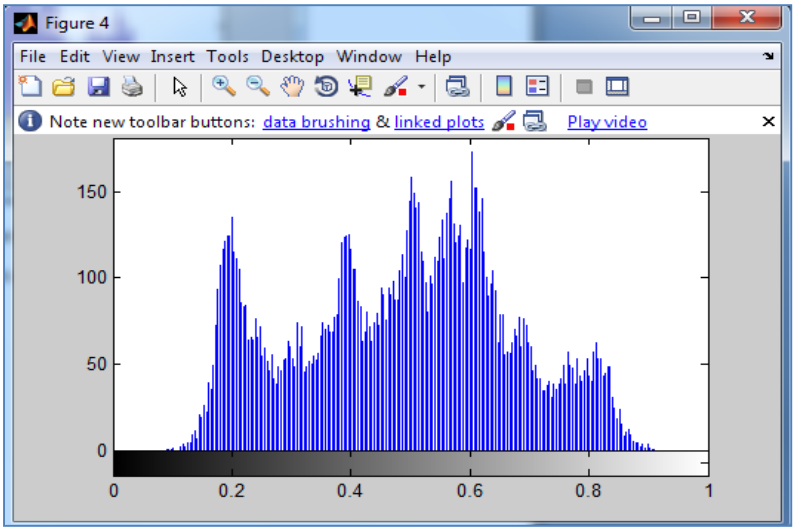

Figure 4.18: Case 2: The histogram for image (t1) after embedding

In case 2, there is no difference between the input image and the image after embedding process in terms of intensity and clarity of the image. Further the histogram does not change after the embedding process.

For case 3 and case 4, image t3 is used with two different texts. The image t3 and the histogram of the image t3 (input image) before embedding process are shown as follows:

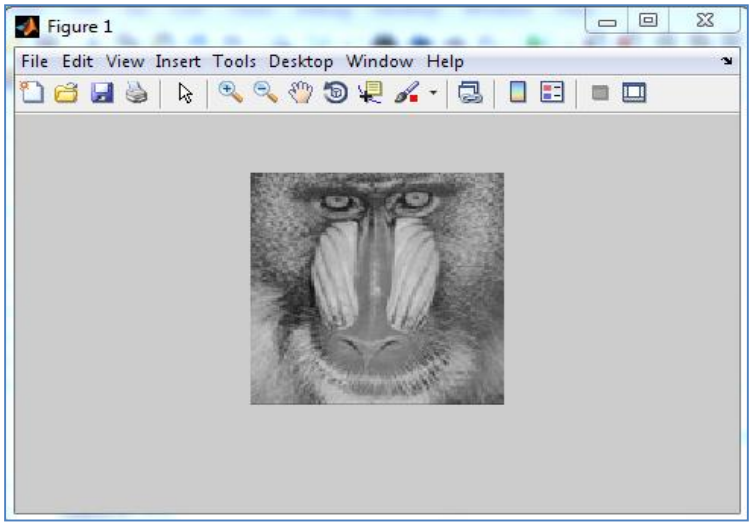

Figure 4.19: Image (t3) before embedding

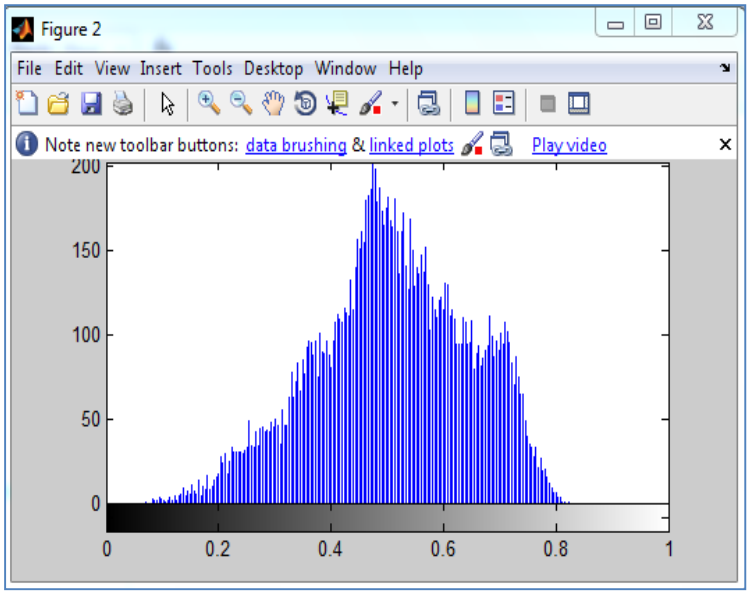

Figure 4.20: The histogram for image (t3) before embedding

Case 3 (image t3):

For case 3, image t3 is used with (this is test) text. The Size of the data in bits is 1600. From the results of the embedding process throughout the execution of the MATLAB code of the second algorithm, it is found that the value of SNR is 18.9105 and the elapsed time that is needed for the second algorithm to be executed is 1.554131 (in seconds). The image t3 and the histogram of the image t3 after embedding process are shown as follows:

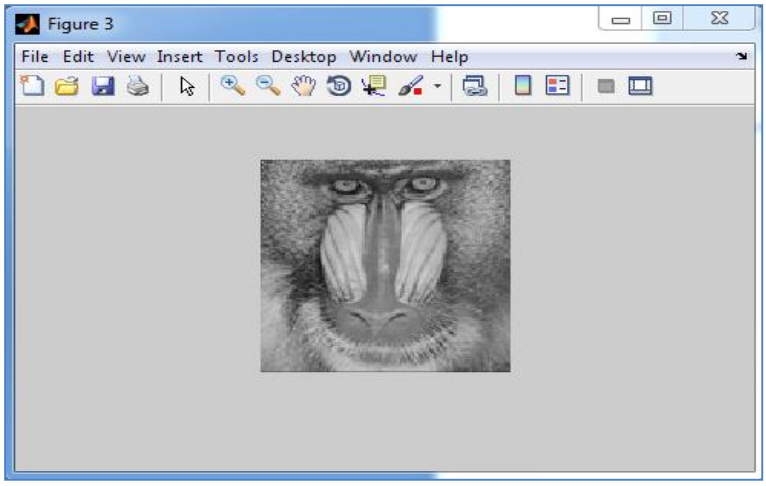

Figure 4.21: Case 3: Image (t3) after embedding

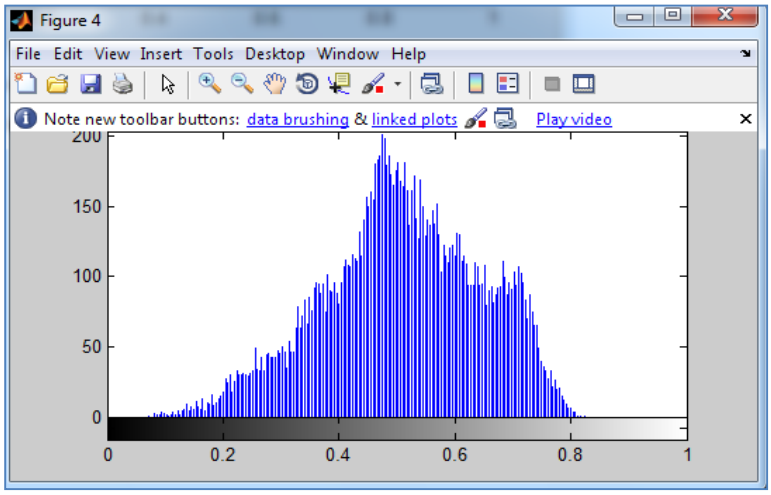

Figure 4.22: Case 3: The histogram for image (t3) after embedding

There is no variation occurs to the image after embedding process in terms of intensity and clarity of the image. In addition the histogram does not change after the embedding process.

Case 4 (image t3):

For case 4, image t3 is used with (this is test file for first algorithm) text. The Size of the data in bits is 1600. From the results of the embedding process throughout the execution of the MATLAB code of the second algorithm, it is found that the value of SNR is 20.7870 and the elapsed time that is needed for the second algorithm to be executed is 1.460030 (in seconds). The image t3 and the histogram of the image t3 after embedding process are shown as follows:

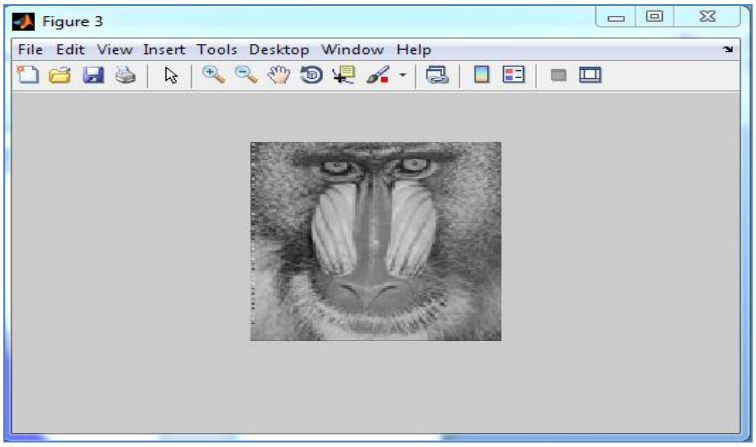

Figure 4.23: Case 4: Image (t3) after embedding

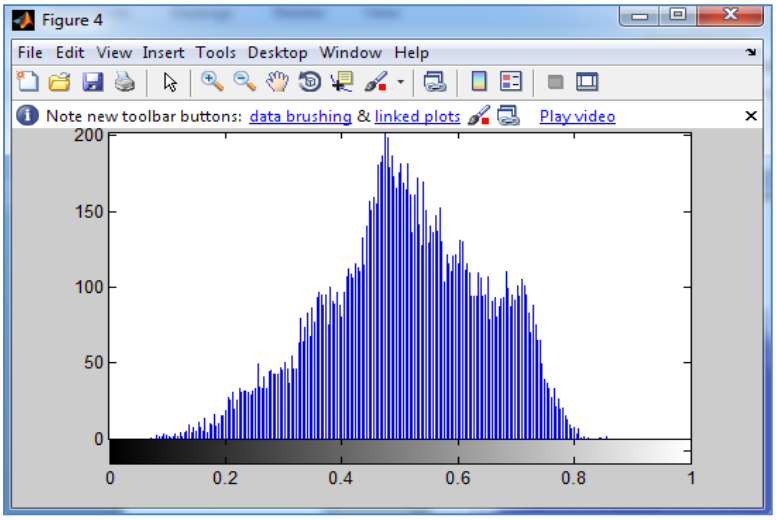

Figure 4.24: Case 4: The histogram for image (t3) after embedding

As in case 3, there is no difference between the input image and the image after embedding process in terms of intensity and clarity of the image. Further the histogram does not change after the embedding process.

The Outcomes:

After resizing the input image, the system divides the overall image into blocks, each block sized by 3x3, the chaos method in this case can be obtained by taking first bit with address (1,1) and third bit with address (3,3), and then an average is made between them and the embedding procedure is applied. Finally, the output from the embedding will be replaced by the centre of the block (2,2). P1 refers to the first index of the 3*3 matrix and the range of values of P1 is between 0 and 1, also P2 refers to the final index of the 3*3 matrix and the range of values of P2 is between 0 and 1. Each time the average of P1 and P2 is computed to determine the centre of the 3*3 matrix.

Table (4.1): Pixel values

Case no.	P1	P2
Case1	0.6314	0.6157
	0.6627	0.5569
	0.6431	0.3255
	0.4941	0.3569
	0.3373	0.3569
	0.3529	0.3686
Case2	0.6314	0.6157
	0.6627	0.5569
	0.4941	0.3569
	0.3373	0.3569
	0.3529	0.3686
	0.4196	0.4078
	0.2431	0.2392
Case 3	0.3373	0.5333
	0.3608	0.3451
	0.4706	0.4667
	0.4275	0.3882
	0.4392	0.4078
	0.4275	0.3882
Case 4	0.6667	0.6784
	0.7373	0.6745
	0.3373	0.5333
	0.3608	0.3451
	0.6431	0.3804
	0.4706	0.4667

4.4. A Chaos-based Image Encryption Scheme using 3D Skew Tent Map (Third Method)

In the third method, the proposed system utilizes the 3D skew tent map to mix up the plain-image proficiently in the pixel locations combination process, while utilizeing the joined map lattice system to alter the gray values of the whole image pixels significantly.

4.4.1. Design and simulation

The code for the third algorithm is similar to the code for the first algorithm, but it differs in such a way that each algorithm has its For loop which includes its own built function. In the third algorithm, the built function (make_embed_third(a,b)) includes if statement that if $a < b$ then iw is equal to a/b, else iw is equal to $(1-a)/(1-b)$.

```
function [iw]=make_embed_third(a,b)



        if(a<b)
            iw=a/b;
        else
            iw=(1-a)/(1-b);
        end
```

4.4.2. Results

The results for the third algorithm are shown below, there are four cases, two images and two texts are used in these cases:

For case 1 and case 2, image t1 is used with two different texts. The image t1 and the histogram of the image t1 (input image) before embedding process are shown as follows:

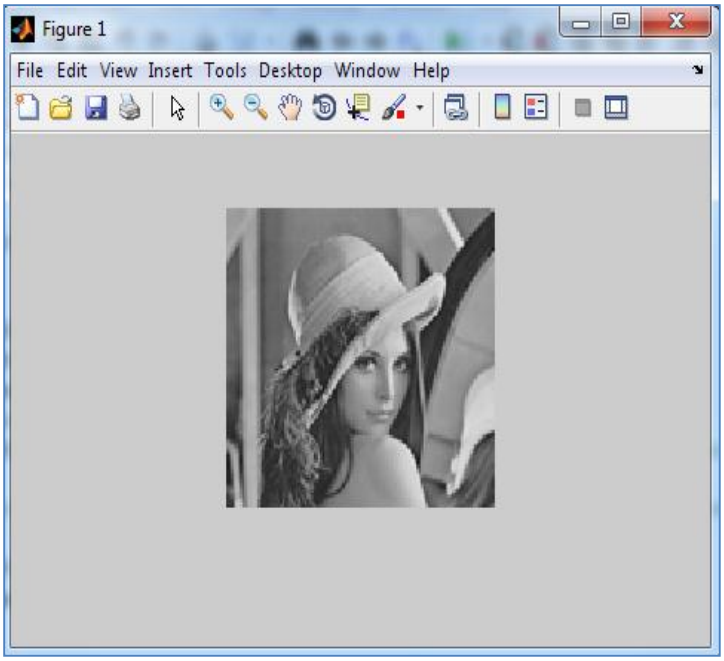

Figure 4.25: Image (t1) before embedding

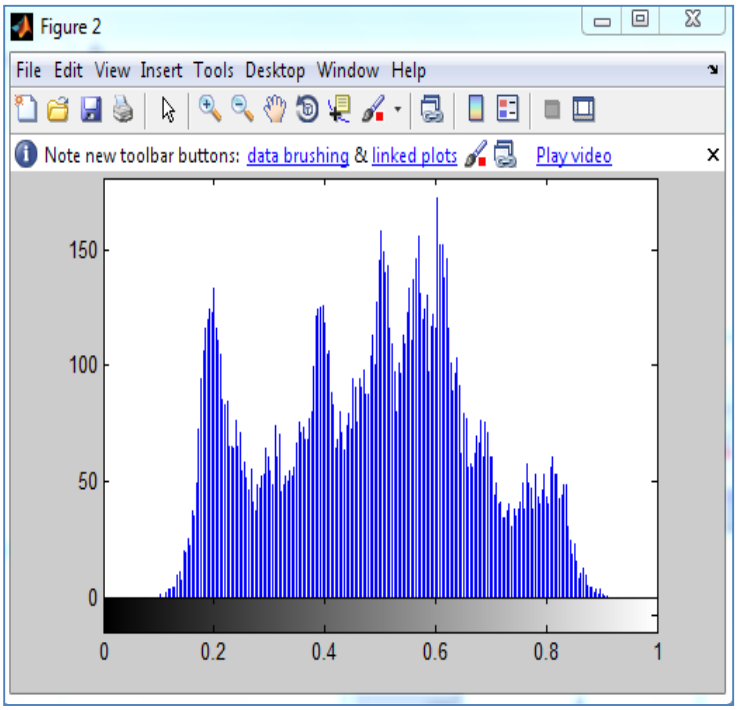

Figure 4.26: The histogram for image (t1) after embedding

Case 1 (image t1):

For case 1, image t1 is used with (this is test) text. The Size of the data in bits is 1600. From the results of the embedding process throughout the execution of the MATLAB code of the third algorithm, it is found that the value of SNR is 25.4145 and the elapsed time that is needed for the third algorithm to be executed is 1.862472 (in seconds). The image t1 and the histogram of the image t1 after embedding process are shown as follows:

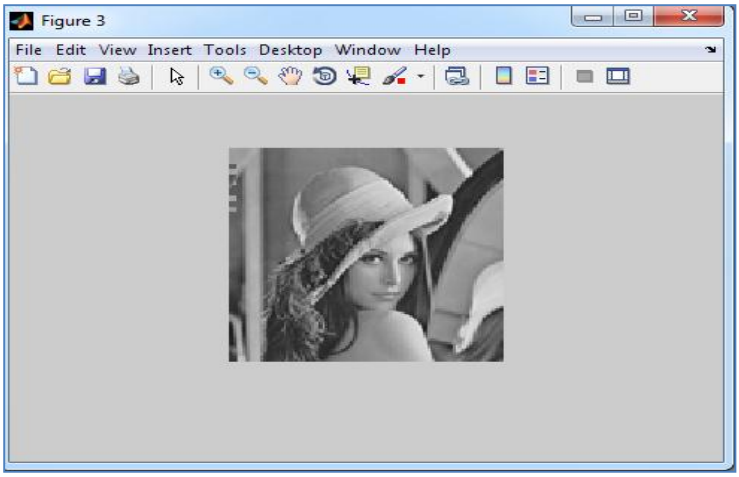

Figure 4.27: Case 1: Image (t1) after embedding

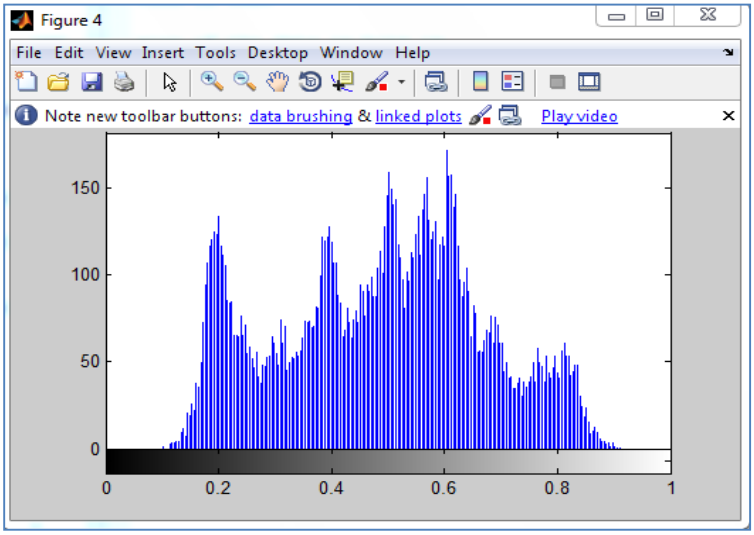

Figure 4.28: Case 1: The histogram for image (t1) after embedding

In case 1, the image after embedding process does not differ in terms of intensity and clarity of the image. In addition, the histogram does not change after the embedding process.

Case 2 (image t1):

For case 2, image t1 is used with (this is test file for first algorithm) text. The Size of the data in bits is 1600. From the results of the embedding process throughout the execution of the MATLAB code of the third algorithm, it is found that the value of SNR is 23.4055 and the elapsed time that is needed for the third algorithm to be executed is 1.467712 (in seconds). The image t1 and the histogram of the image t1 after embedding process are shown as follows:

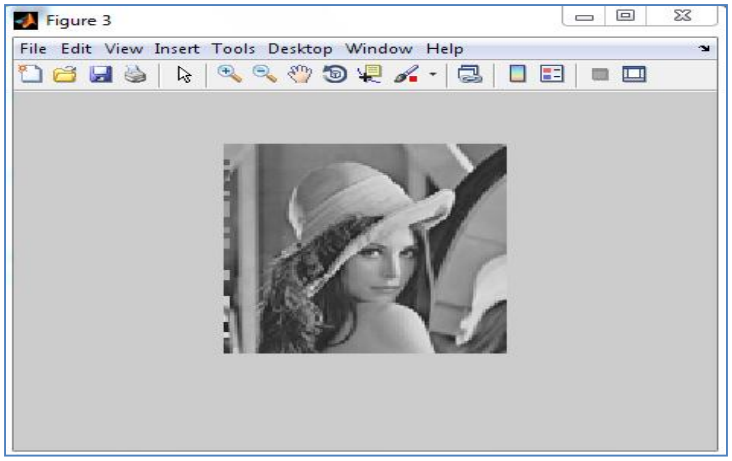

Figure 4.29: Case 2: Image (t1) after embedding

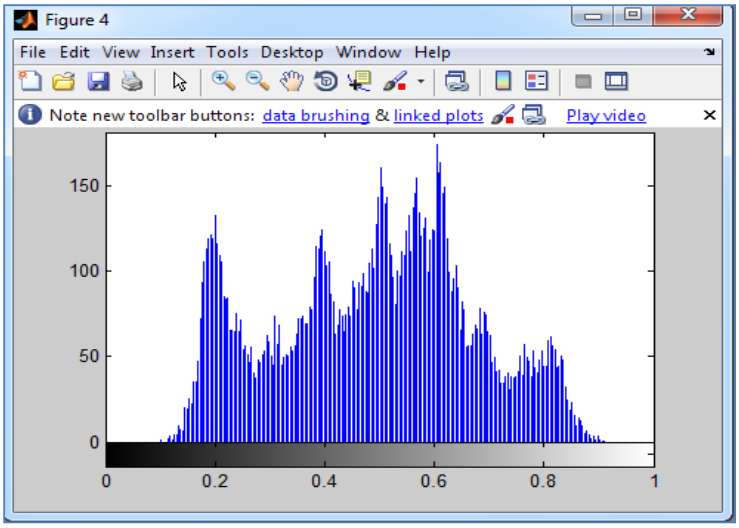

Figure4.30: Case 2: The histogram for image (t1) after embedding

Also in case 2, there is no difference between the input image and the image after embedding process in terms of intensity and clarity of the image. Further more the histogram does not change after the embedding process.

For case 3 and case 4, image t3 is used with two different texts. The image t3 and the histogram of the image t3 (input image) before embedding process are shown as follows:

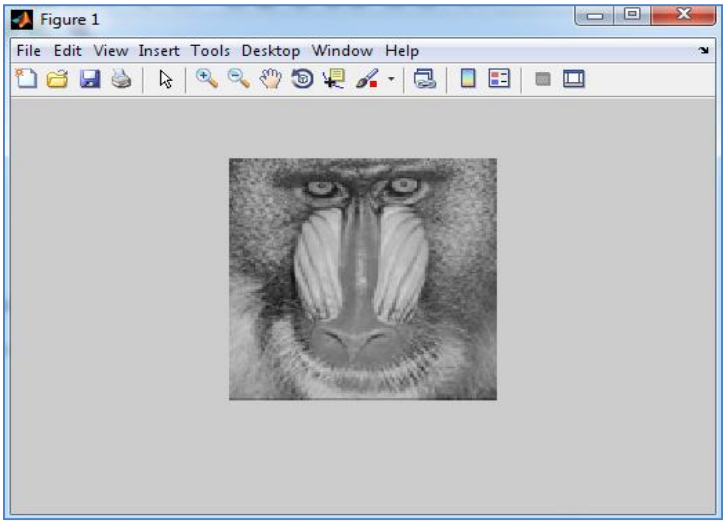

Figure 4.31: Image (t3) before embedding

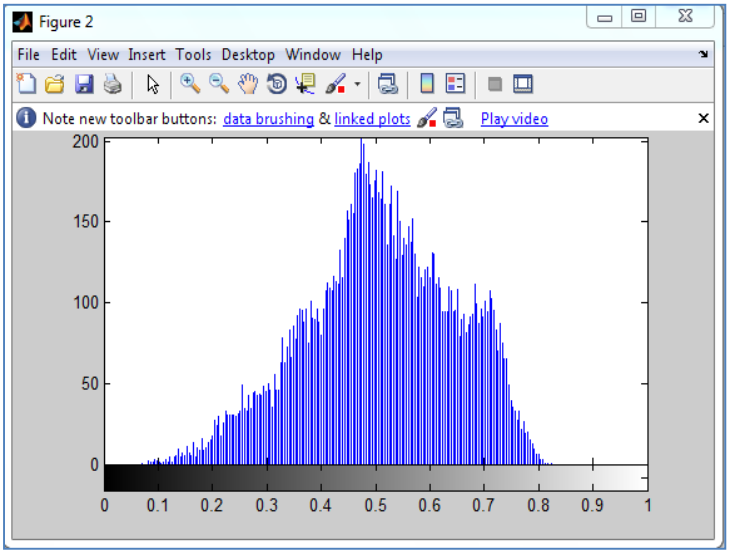

Figure 4.32: The histogram for image (t3) before embedding

Case 3 (image t3):

For case 3, image t3 is used with (this is test) text. The Size of the data in bits is 1600. From the results of the embedding process throughout the execution of the MATLAB code of the third algorithm, it is found that the value

of SNR is 18.8482 and the elapsed time that is needed for the third algorithm to be executed is 1.378212 (in seconds). The image t3 and the histogram of the image t3 after embedding process are shown as follows:

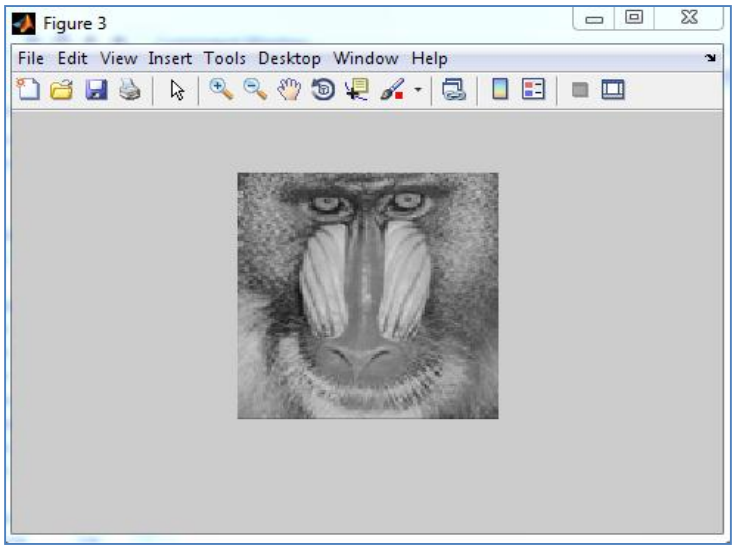

Figure 4.33: Case 3: Image (t3) after embedding

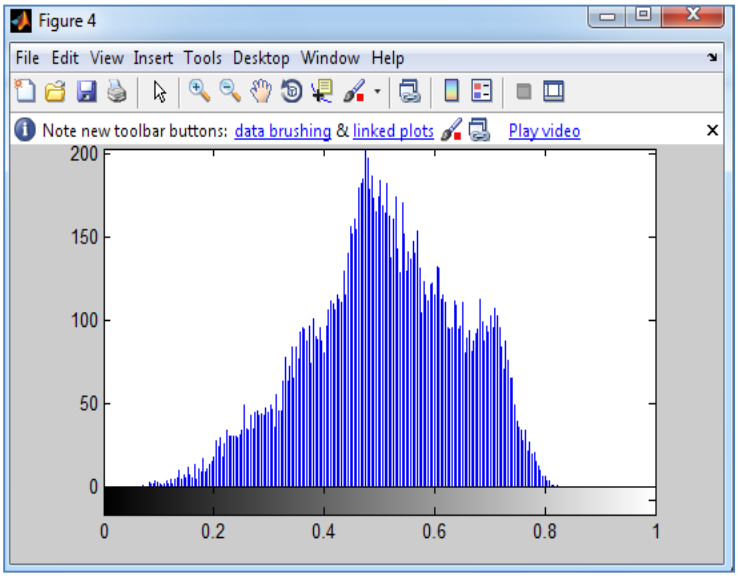

Figure 4.34: Case 3: The histogram for image (t3) after embedding

Case 4 (image t3):

For case 4, image t3 is used with (this is test file for first algorithm) text. The Size of the data in bits is 1600. From the results of the embedding process throughout the execution of the MATLAB code of the second algorithm, it is found that the value of SNR is 18.6397 and the elapsed time that is needed for the second algorithm to be executed is 1.338551 (in seconds). The image t3 and the histogram of the image t3 after embedding process are shown as follows:

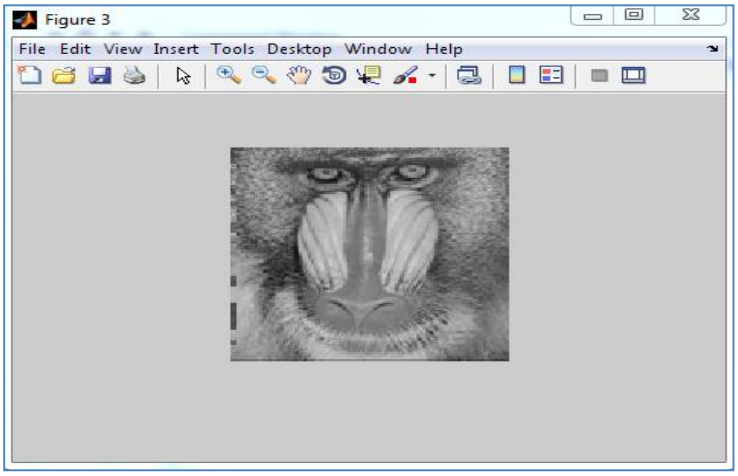

Figure 4.35: Case 4: Image (t3) after embedding

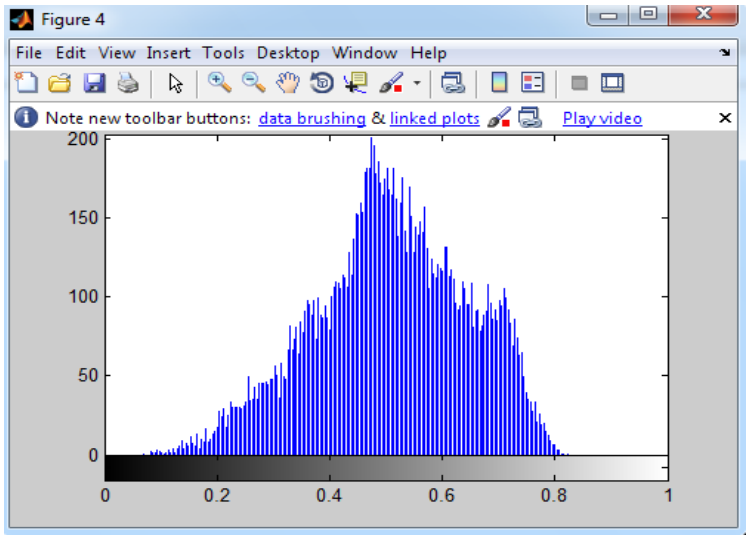

Figure 4.36: Case 4: The histogram for image (t3) after embedding

In case 4, there is no difference happens between the input image and the image after embedding process in terms of intensity and clarity of the image. Further the histogram does not change after the embedding process.

4.5. The Comparison

In this project three methods are implemented; the first method is to use the cryptography technique for a text message and then embedding the encrypted message in a cover. The second method is by using the double hiding. The third method used a chaos-based image encryption system by using tent map. The embedding methods are different in new techniques, where the LSB method is used in the first method, the chaos procedure is used in the second method and 3D Skew Tent Map in the third method. After executing MATLAB cods for the three algorithms from the results, it is shown that the third algorithm took less time than the others and the first one took most time than the others. Thus, third one could be better and more secure than the others in hiding data. Also from the results, the first method could be more complex than the other methods, since its cases took more time to be executed. These conclusions were concluded about the three methods from the following tables:

LSB Steganography Method (First Method)

	C=	Size of the data in bits	SNR	Elapsed time (in seconds)
Case 1	this is test	1600	25.6486	7.509200
Case 2	this is test file for first algorithm	1600	25.3981	5.526542
Case 3	this is test	1600	18.9135	1.353972

Case 4	this is test file for first algorithm	1600	21.1251	1.400884

Chaos based Spatial Domain Steganography Method (Second Method)

	C=	Size of the data in bits	SNR	Elapsed time (in seconds)
Case 1	this is test	1600	25.6413	4.384285
Case 2	this is test file for first algorithm	1600	25.3809	1.355209
Case 3	this is test	1600	18.9105	1.554131
Case 4	this is test file for first algorithm	1600	20.7870	1.460030

A Chaos-based Image Encryption Scheme using 3D Skew Tent Map (Third Method)

	C=	Size of the data in bits	SNR	Elapsed time (in seconds)
Case 1	this is test	1600	25.4145	1.862472
Case 2	this is test file for first algorithm	1600	23.4055	1.467712
Case 3	this is test	1600	18.8482	1.378212
Case 4	this is test file for first algorithm	1600	18.6397	1.338551

To compare between the three methods, the average of SNR and the average for the elapsed time to every method were taken, as in the following table:

Method	Size of the data in bit	Average SNR	Average time (in seconds)
LSB (1st method)	1600	22.7713	3.94765
Chaos based spatial domain(2nd method)	1600	22.6800	2.18841
Tent map (3rd method)	1600	21.5770	1.51174

From the above table, LSB method has the longest elapsed time due to the manipulation for each byte in the cover image. The third method has the minimum average SNR value, and the first method has the highest average SNR value. Through the comparison table above, note that the third method is the fastest in terms of time, which is the best in terms of noise and therefore is the best in terms of security.

4.6. Summary

There are three methods suggested in this project, the first method is to use the cryptography technique for a text message and then embedding the encrypted message in a cover. The second method used the double hiding. Finally, the third method is used a chaos-based image encryption system by using tent map. For embedding procedure, there is an embedding technique used for each methods, where the LSB method is used in the first method, the chaos procedure is used in the second method and 3D Skew Tent Map in the third method. Some of the characteristics of the MATLAB/SIIMULINK Software are used to implement these methods, since it is more efficient, proficient and easier to utilize. As a result of the execution the MATLAB

codes for the three algorithms of the methods, it is found that the third method could be better and more secure than the others in hiding data in terms of the elapsed time, since the third algorithm took less time to be executed than the others. Also from the results, the first method could be more complex than the other methods, since its cases took more time to be executed. From these conclusions, in the future the advantages of each method could be used together in one method; this developed method will combine between the advantages of the methods that are used in this project.

CHAPTER FIVE
CONCLUSION AND FUTURE WORK

5.1. Introduction

In the past, a utilized computer to modify a digital image was something achieved only by a fairly trivial crowd of specialists who have permission to costly tools. In general this combination of specialists and tools was simply to be created in research labs, and so the turf of digital image processing has its origins in the educational monarchy. Presently, on the other hand, the combination of a powerful computer on each desktop computer and the point that almost each individual has some kind of apparatus for digital image gaining (like a scanner, a digital camera, or a cell phone camera) has caused in an excess of digital images as well as lots of digital image processing has come to be as public as word processing. Nowadays, Information Technology (IT) specialists must be more than merely familiar with digital image processing. They are expected to be able to intelligently adjust pictures and associated digital media, which are a gradually imperative section of the workflow not merely to those tangled with media and medicine but all sorts of companies.

The requirement for new expert, protected and private methods in the protection of secret information always develops. Secure information is classified into two states in the computer networks, which are: Saved or transferred via the network. One of the basic needs during exchanging data is protecting data in a way that it will be seen only by the intended receiver. This could be achieved by using an encryption method that could obscure the message contents. In this technique, the transmission procedures are hidden.

5.2. Conclusion

In this project, there are several conclusions that were concluded from the three used methods, which are as follows:

1. LSB formulates utilization of BMP picture, because BMP utilizes lossless compression. A very great cover picture is needed, in order to be able to conceal an undisclosed text within a BMP file. BMP pictures of 800 × 600 pixels found to include fewer web purposes. Furthermore such utilizations are not admitted as suitable.

2. LSB Steganography has been improved for utilization with other picture file layouts. There exists a great variety of techniques for hiding data in pictures. All the main picture file layouts have dissimilar techniques of hiding texts, with dissimilar well-built and weak points correspondingly. When the most appropriate cover picture has been selected, LSB in GIF pictures has the probability of hiding a huge text.

3. Chaos based Spatial Domain Steganography using MSB (CSSM) algorithm is suggested in which the load bit stream is inserted in both MSB and LSB of grayscale cover picture. The cover picture is decayed within 3*3 blocks. The key is inserted in the first block which is utilized to recover the load at the destination. The remaining 3*3 blocks are utilized to insert load in a chaotic way to defend the secret data. The suggested algorithm has superior capability and safety with elevated PSNR compared to the existing algorithm.

4. In this project, a proficient image encryption system depends on 3D skew tent map and coupled map lattice are suggested. The 3D skew tent map is used by the suggested system, in order to mix up the plain-picture professionally in the pixel positions permutation procedure. In addition the coupled map lattice scheme is utilized to alter the gray values of the entire picture pixels significantly.

5. In the 3D skew tent map method, the behavior examination involving statistical investigation, key space investigation, toughness adjacent to malicious attacks like JPEG compression, nosing, cropping, are performed numerically and visually. In future the same technique could be expanded to the convert domain and robustness of algorithm.

5.3. Future Work

The objective of data hiding is to prevent peeper from finding out the undisclosed texts embedded in the cover-pictures. In the future, some alterations could occur to some hiding data systems as:

1. In JPEG–JSTEG, only a small number of texts could be embedded in the cover-picture. Thus in the future, the capacity of hidden text could be improved by developing an improved steganographic technique, in order to enhance the text load in every block of the stego-picture while keeping the stego-picture quality acceptable.

2. In JPEG–JSTEG, the steganographic technique may improve in such that the secret text could be embedded in the middle-frequency part of the quantized DCT coefficients. Based on the protection analysis,

3. this method has the similar conceal, thus has the similar security stage as JPEG–JSTEG. In addition, this method matches the need of steganography with a bigger text capacity than that of JPEG–JSTEG.
4. A new conceptual structure for steganographic communication could be used by utilizing cipher-text as a cover intermediate. Utilizing cipher-text as a steganographic carrier could recommend confidentiality that it could be utilized to camouflage the oppositions as well as maintain the hidden communication undisclosed since no one will attempt to search for steganographic message in a cipher text.

5. In cipher-text technique, oppositions would spend exertion to decrypt the cipher-text but would get nothing practical since the basic message won't have any secret data. On the other hand, the future receiver having the suitable stego key could obtain hold of the hidden data.

References

[1] Burger,B. 2008. “Digital Image Processing an Algorithmic Introduction Using Java”. .Springer Science+Business Media, LLC.

[2] Al-Haj,A. 2007. "Combined DWT-DCT Digital Image watermarking", Journal of Computer Science, Vol.3 No. 9, page 740-746.

[3] LUO,X , LIU,B and LIU,F. 2005. "Improved RS Method for Detection of LSB Steganography".Int. Workshop on Info. Security & Hiding (ISH '05).

[4] Lee,Y and Chen,L. 2000." A high capacity image steganographic model". In IEE Vision, Image and Signal Processing.

[5] Luo,X , Liu,B and Liu,F. 2005. " Improved RS Method for Detection of LSB Steganography", Int. Workshop on Info. Security & Hiding (ISH '05),Singapore May 9-12.

[6] Birgit,P. 2001. “Information Hiding Terminology ”, First International Workshop, Cambridge, UK, Proceedings, Computer Science 1174. pp. 347-350, May –June.

[7]Ahmad,M and Shamsher Alam,M. 2009. “A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping”, Musheer Ahmad et al /International Journal on Computer Science and Engineering, Vol. 2(1).

[8] Fridrich,J. 1998. “Symmetric ciphers based on two-dimensional chaotic maps.” International Journal of Bifurcation and Chaos, vol.8, no.6,pp.1259-1284.

[9] Yen,J.C and Guo,J. I. 1999. “A new image encryption algorithm and its VLSI architecture.” in Proceedings of IEEE workshop on signal processing systems,pp. 430-437

[10] Voloshynovskiy,S , herrigel,A , Rytsar,Y and Pun,T. 2002. “Stegowall: Blind statistical detection of hidden data”. Proc. of SPIE Electronic Imaging, Security and Watermarking of Multimedia Contents IV. San Jose, CA, USA.

[11] Bergmair,R and Katzenbeisser,S. 2006. “Content-Aware Steganography: About Lazy Prisoners And Narrow-Minded Wardens”. 8th Information Hiding. Virginia, USA.

[12] Fridrich,J , Golgan,M and Du,R. 2001. “Detecting LSB Steganography in Color and Gray-Scale Images”. Magazine of Multimedia, Special Issue on Security. pp. 22–28.

[13] Provos,N. 2001. “Defending Against Statistical Steganalysis”, 10th USENIX Security Symposium. Washington, DC.

[14] Minamoto,T and Aoki,K. 2010. “A blind digital image watermarking method using interval wavelet decomposition”, International Journal of Signal Processing, Image Processing and Pattern Recognition, Vol. 3(2).

[15] Cox,I.J , Miller,M.L and Bloom,J.A. 2002. “Digital Watermarking. Morgan Kaufmann Publishers”.

[16] Chandramouli,R , et al. 2004. "Image Steganography and Steganalysis: Concepts and Practice”, Springer-Verlag Berlin Heidelberg.

[17] Grigoras1,V and Grigoras,C. 2006. “Chaos Encryption Method Based on Large Signal Modulation in Additive Nonlinear Discrete-Time Systems” Proc. of the 5th WSEAS Int. Conf. on Non-Linear Analysis, Non-Linear Systems and Chaos, Bucharest, Romania, October 16-18.

[18] Cvejic,N and Seppänen,T. 2004. " Increasing Robustness of LSB Audio Steganography Using a Novel Embedding Method", Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC’04).

[19] Wu,M.Y and Lee,J.H. 1998. “A Novel Data Embedding Method for Two-Color Facsimile Images. In Proc. of Intl. Symp” on multimedia Information Processing.

[20] Kurak,C and Mchugh,J. 1992.” A cautionary note on image downgrading”. In Computer Security Applications Conference. pp. 153-159. San Antonio.

[21] Marvel,L.M , Hartwig,G.W and Boncelet,C. 2000. “Compression-compatible fragile and semi-fragile tamper detection”. In SPIE EI Photonics West. pp. 131-139. San Jose, CA.

[22] Westfeld,A and Pfitzmann,A. 2000. “Attacks on Steganographic Systems. Notes in Computer Science”. **1768**. pp. 61−75. Springer-Verlag, Berlin.

[23] Alkhrais,H. 2005. "4 least Significant Bits Information Hiding Implementation and Analysis".

[24] Hassanien,A.E. 2005. "Hiding Iris Data for Authentication Of Digital Images using Wavelet".

[25] Fridrich,J , Golgan,M and DU,R. 2001." Steganalysis based on JPEG compatibility". SPIE Multimedia Systems and Applications IV. Denver, CO.

[26] Zaidan,A.A , Zaidan,B.B and Othman,F. 2009. "New Technique of Hidden Data in PE-File with in Unused Area One". International Journal of Computer and Electrical Engineering (IJCEE). **1**(5). pp 669-678.

[27] Abdulrazzaq,M.M , Zaidan,A.A , Zaidan,B.B , Raji,R.Z and Mohammed,S.M. 2009. "Implementation Stage for High Securing Cover-File of Hidden Data Using Computation Between Cryptography and Steganography". International Conference on Computer Engineering and Applications (ICCEA09), Telecom Technology and Applications (TTA). **19**(6). Manila, Philippines. pp 482-489.

[28] Naji,A.W , Hameed,S.A , Zaidan,B.B , Al-khateeb,W.F , Khalifa,O.O , Zaidan,A.A and Gunawwan,T.S. 2009." Novel Framework for Hidden Data in the Image Page within Executable File Using Computation between Advance Encryption Standard and Distortion Techniques". International Journal of Computer Science and Information Security. **3**(1). pp. 73-78.

[29] Taqa,A , Zaidan,A.A and Zaidan,B.B. 2009. "New Framework for High Secure Data Hidden in the MPEG Using AES Encryption Algorithm". International Journal of Computer and Electrical Engineering. **1**(5). pp.589-595.

[30] Alam,F.I , Bappee,F.K and Khondker,F.U.A. 2011. "An Investigation into Encrypted Message Hiding Through Images Using LSB". International Journal of Engineering Science and Technology (IJEST).**3**(2). pp. 948- 960.

[31] Katzenbeisser,S.F and Petitcolas,A.P. 2000. "Information Hiding Techniques for Steganography and Digital Watermarking". Artech House, Norwood.

[32] Amirtharajan,R and Balaguru,R.J.B. 2003. "Constructive Role of SFC & RGB Fusion versus Destructive Intrusionl". International Journal of Computer Applications.**1**(20). pp. 30–36.

[33] Amirtharajan,R and Balaguru,R.J.B. 2009. Tri-Layer Stego for Enhanced Security, A Keyless Random Approach.

[34] Amirtharajan,R , Nathella,K and Harich,J. 2010. "A Cluster Cover Approach". International Journal of Computer Applications. **3**(5). pp. 11–18.

[35] Wang,R.Z , Lin,C.F and Lin,J.C. 2000. "Image hiding by optimal LSB substitution and genetic algorithm", Pattern Recognition. **34** (3). pp. 671–683.

[36] Prasad,G and Narayana,S. 2011. "A novelapproach for concealed datasharing and dataembedding forsecured communication". International Journal of Computer Science, Engineering and Applications (IJCSEA). **1**(1). pp. 1- 10.

[37] Stallings,W. 2003. Cryptography and Network Security, Principles and Practice, Third edition, Pearson Education. Singapore.

[38] Bryan,C. 2001. Steganography: How to Send a Secret Message.

[39] Westfeld,A and Wolf,G. 1998. "Steganography in a Video conferencing system, in proceedings of the second international workshop on information hiding". **1525**. pp. 32-47.

[40] Galand,F and Kabatiansky,G.A. 2009. 'Coverings, Centered Codes, and Combinatorial Steganography', Supported in part by the Russian Foundation for Basic Research, Moscow.

[41] Sajedi,H and Jamzad,M. 2009. 'Secure Steganography Based on Embedding Capacity', Springer-Verlag, Iran.

[42] Shang-Lin Hsieh, I-Ju Tsai, Bin-Yuan Huang and Jh-Jie Jian. 2008. " Protecting Copyrights of Color Images using a Watermarking Scheme Based on Secret Sharing and Wavelet Transform ", Journal of Multimedia, vol. 3, no. 4, October .

[43] Cetin,O and Ozcerit,A. 2009. 'A new Steganography Algorithm Based on Color Histograms for Data Embedding into Raw Video Streams', Elsevier Ltd, Computers & Security, Turkey.

[44] Chang,C and Tseng,H. 2004. 'A steganographic method for digital images using side match', Elsevier, Taiwan.

[45] Ji,L , Li,X , Yang,B and Liu,Z. 2010. 'A Further Study on a PVD-Based Steganography', IEEE, China

[46] Kumar,G , Sasidharan,S , Karthikha,N , Sherly,A and Avani,Y. 2010. "An Efficient Embedding and Restoration Steganographic Scheme for Secure Multimedia Communication", International Conference on Advances in Computer Engineering, India.

[47] Su,Y , Zhang,Che and Zhang,Chu. 2011. 'A video Steganalytic Algorithm Against Motion-Vector-Based Steganography', Elsevier, Signal Processing, China.

[48] Sverdlov,S , Dexter and Eskicioglu,A.M. 2005. "Robust DCT-SVD Domain Image Watermarking for Copyright Protection: Embedding Data in All Frequencies", submitted to Multimedia Computing and Networking Conference, San Jose, CA, January.

[49] Swanson,M , Zhu,B and Tewfik,A. 1997. 'Data Hiding for Video-in-Video', IEEE, Minneapolis.

[50] Zheng,P , Zhao,B and Liu,M. 2009. 'An Effective Method to Hide Information in MPEG Video Sequences', IEEE, China.

[51] Daneshkhah,A , Aghaeinia,H and Seyedi,S. 2011. 'A More Secure Steganography Method in Spatial Domain', IEEE, Iran.

[52] Lou,D , Wu,N , Wang,C , Lin,Z and Tsai,C. 2010. 'A Novel Adaptive Steganography Based on Local Complexity and Human Vision Sensitivity', Elsevier, Taiwan.

[53] Malik,H. 2010. "Statistical modeling of footprints of QIMsteganography",IEEE,USA.

[54] Chen,W-Y. 2008. 'Color image steganography scheme using DFT, Spiht codec, and modified differential phase-shift keying techniques', Elsevier, Taiwan.

[55] Xu,C , Ping,X and Zhange,T. 2006. 'Steganography in Compressed Video Stream', IEEE, China.

[56] Liu,S , Yao,H , Zhang,S and Gao,W. 2010. "A steganography strategy based on equivalence partitions of hiding units", School of Computer Science and Technology, Harbin Institute of Technology, P.R.China.

[57] Elsadig,M , Kiah,M , Zaidan,B and Zaidan,A. 2009. 'High Rate Video Streaming Steganography', IEEE, Malaysia.

[58] Famili,Z , Faez,K and Fadavi,A. 2009. 'A New Steganography Based on x^2 Technic', Springer-Verlag Berlin Heidelberg, Iran.

[59] Yu,L , Zhao,Y , Ni,R and Zhu,Z. 2008. "PM1 steganography in JPEG images using genetic algorithm", Springer-Verlag

[60] Hopper,N , Von ahn,L and Langford,J. 2009. "Provably Secure Steganography", IEEE transactions on computer.

[61] Liu,B , Liu,F , Yang,C and Sun,Y. 2008. 'Secure Steganography in Compressed Video Bitstreams', IEEE, China.

[62] Tripathi,A. 2010. "A Two Level Message Adaptive Steganographic Approach", International Conference on Advances in Computer Engineering, India.

[63] Wakiyama,M , Hidaka,Y and Nozaki,K. 2010. "An audio steganography by a low-bit coding method with wave files", IEEE, Computer Society, USA.

[64] Bhowal,K , Pal,A.J , Tomar,G.S and Sarkar,P.P. 2010. "Audio Steganography using GA", International Conference on Computational Intelligence and Communication Networks, India.

[65] Kung,C.M , Jcng,J.H and Truong,T.K."Watermark Technique using Frequency Domain".

[66] Spaulding. J, Noda , H., Shirazi , M. and Kawaguchi , E., 2002," BPCS steganography using EZW lossy compressed images", ELSEVIER, Japan.

[67] Su,P , Lu,M and Wu,C. 2011. "A practical design of high-volume steganography in digital video files", Springer, Taiwan.

[68] Chiang,Y.K and Tsai,P. 2008. "Steganography using overlapping codebook partition", ELSEVIER, Taiwan.

[69] Bhattacharyya,S , Kshitij,A.P and Sanyal,G. 2010. "A Novel Approach to Develop a Secure Image based Steganographic Model using Integer Wavelet Transform", International Conference on Recent Trends in Information, Telecommunication and Computing, India.

[70] Arena,S , Caramma,M and Lancini,R. 2008. "data hiding in the bit streamdomain for MPEG-2 codedvideo sequences exploiting space and frequencymasking"cefriel, Italy.

[71] Noda,H , Niimi,M and Kawaguchi,E. 2006. "High-performance JPEG steganography using quantization index modulation in DCT domain", ELSEVIER, Japan.

[72] Neeta,D and Snehal,K. 2004. “Implementation of LSB Steganography and Its Evaluation for Various Bits”. pp. 173-178

[73] Birgit,P. "Information Hiding Terminology". First International Workshop, Cambridge, UK, Proceedings, Computer Science 1174. pp. 347-350, May - June

[74] Andreas,W and Pfitzmann,A. 1999. "Attacks on Steganographic Systems". Third International Workshop, IH'99 Dresden Germany, October Proceedings, Computer Science1768. pp. 61- 76

[75] Sathisha,N , Madhusudan,G.N , Bharathesh,S,K , Babu,S , Raja,K.B and Venugopal,K.R. 2010. "Chaos based Spatial Domain Steganography using MSB". 2010 5th International Conference on Industrial and Information Systems. pp. 177-182

[76] Ruisong,Y.E and Zhou,W. 2012. "A Chaos-based Image Encryption Scheme Using 3D Skew Tent Map and Coupled Map Lattice". I. J. Computer Network and Information Security. pp. 38-44.

[77] Schneier,B.1995. Cryptography: Theory and Practice, CRC Press, Boca Raton.

[78] Fridrich,J. 1998. Symmetric ciphers based on two-dimensional chaotic maps. International Journal of Bifurcation and Chaos, 1259-1284.

[79] Chen,G.R. , Mao,Y.B , Chui,C.K. 2004. " A symmetric image encryption scheme based on 3D chaotic cat maps". Chaos, Solitons & Fractals, 749-761.