Republic of Iraq

Ministry of Higher Education

and Scientific Research

Babylon University

College of Engineering

Multi -Level Steganography Technique for Digital Multimedia Files based on Hybrid Transform

A Thesis

Submitted to the Department of Electrical Engineering / Faculty

of Engineering / University of Babylon in Partial Fulfillment

of the Requirements for the Degree of Master of Science (M.Sc.) in Electrical Engineering.

By

Rafal Fadhil Jabbar

Supervised by

Prof. Dr. Osama Qasim Jumah Althahab

2021/2022 A.D. *1444 A.H.*

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

(وَهُوَ الَّذِي أَنشَأَ لَكُمُ السَّمْعَ وَالْأَبْصَارَ وَالْأَفْئِدَةَ قَلِيلاً مَّا تَشْكُرُون)

(صَدَقَ اللَّهُ الْعَلِيّ الْعَظِيم)

سورة المؤمنون/ الآية (87)

جمهورية العـراق

وزارة التعليم العالي والبحث العلمي

جامعــة بابـل

كليـــــة الهندســـة

التضمين متعدد المستويات لملفات الوسائط الرقمية المتعددة باستخدام التحويل الهجين

قـدمت هـذا الرسالة إلى قسم الهندسة الكهربائية – كلية الهندسة – جامعة بابل كجزء من متطلبات الحصول على درجـة الماجستير في الهندسة الكهربائية

قـــدمت من قبـل :

رفل فاضل جبار

إشــراف

أ.م.د أسامه قاسم جمعه

2022 ***A.D.*** ***1444 A.H.***

CERTIFICATE

The thesis entitled:

Multi -Level Steganography Techqnique for Digital Multimedia Files based on Hybrid Transform

Which is being submitted by

Rafal Fadhil jabbar

In the fulfillment of requirement for the award of the M.Sc. degree in Electrical Engineering. This has been carried out under my supervision and accepted for presentation & examination.

Signature:

Supervisor's name:

Date: / / 2022

This project entitled

Multi -Level Steganography Technique for Digital Multimedia Files based on Hybrid Transform

Which is being submitted by

Rafal Fadhil jabbar

In the partial fulfillment of requirement for the award of the M.Sc. degree in Electrical Engineering has been discussed by us and all the suggested recommendations during the discussion are carried out.

1st Examiner

Signature:

Name :

Date: / / 2022

2nd Examiner

Signature :

Name :

Date: / / 2022

3rd Examiner supervisor)

Signature:

Name :

Date: / / 2022

4th Examiner (The

signature:

Name :

Date : / / 2022

5th Examiner (The second supervisor)

Signature:

Name :

Date : / / 2022

الخلاصة :

تم اقتراح طرق عديدة ، مثل التكامل بين إخفاء المعلومات والتشفير ، لحماية خصوصية المعلومات المتبادلة. تم التعرف على أنظمة إخفاء المعلومات متعددة المستويات كطريقة حاسمة لتعزيز أمن المعلومات باستخدام الوسائط المتعددة للتستر على المعلومات الحساسة التي تشمل المعلومات غير المرئية للعين البشرية.
في هذه الأطروحة ، تم إخفاء النص داخل صورة رقمية باستخدام خوارزمية Turbo code ، وتم تضمين الصورة الأخيرة داخل صورة غلاف أخرى (تسمى هذه الرسالة متعددة المستويات) من أجل الحصول على شيك مصرفي إلكتروني يحتوي على معلومات الشخص والمبلغ المطلوب يتم صرفها مع صورة هوية الشخص الذي سيحصل على المبلغ بشكل مشفر.
لإتمام عملية إرسال الشيك والحفاظ على سرية المعلومات الموجودة بداخله ، يتم استخدام تحويل الرادون لتشفير صورة الهوية واستخدام كود Hadamard كمستوى أخير للتحكم في تشفير صورة الشيك. تم تنفيذ الخوارزمية باستخدام لغة البرمجة MATLAB. يهدف هذا البحث إلى توفير اتصال سري وآمن بين العميل و البنك للحفاظ على المعلومات المتبادلة بينهما من المتسللين.
تم استخدام معيارين لتقييم الطريقة المقترحة. تمت مقارنة النتائج مع خوارزمية LSB المباشرة وكذلك مع الخوارزمية المقترحة في دراسة مرجعية سابقة. المعيار الأول هو معيار شخصي يعتمد على HVS حيث يتم عرض صورة الغلاف وصورة stego على عدد من الأشخاص. المعيار الثاني هو معيار موضوعي حيث سيتم حساب PSNR و BER و SSIM و MSE. أظهرت النتائج أنه لا يوجد فرق واضح بين صورة الغلاف وصورة Stego التي تم إنشاؤها بالعين المجردة. أنتجت الخوارزمية المقترحة أيضًا قيمًا موجبة لـ PSNR و BER و SSIM و MSE.

Abstract

Numerous methods, such as integration between steganography and cryptography, have been suggested to protect the privacy of information exchanged. Multi-level steganography systems have come to be recognized as a crucial method for enhancing information security by using multimedia to cover up sensitive information which including information that is invisible to the human eye.

In this thesis, text was concealed within a digital image using Turbo code algorithm, which work to preserve the information in the most accurate way, and the strength of the turbo code is that it contains a high rate of correction errors that may accure during the process of transferring information through specific channel. Then the last image was embedded inside another cover image (this called multi-level steganography) in order to result an electronic bank check containing the person's information and the amount to be disbursed with an ID image of the person who will receive the amount in encrypted form.

To complete the process of sending the check and to maintain the confidentiality of the information inside it, radon transformation is used to encrypt the ID image which converts the matrix into a diagonal matrix that contains the extent of error correction , which makes it difficult to make errors and reduce the possibility of discovering the included information beside the radon coefficient which generated with the encryption which is another strong point, as the extraction process cannot be completed without it. And use of the Hadamard code as a last level to control the coding of the image of the check. The algorithm was implemented using the MATLAB programming language. This thesis aims to provide a confidential and

secure communication between the client and the bank to preserve the information exchanged between them from hackers.

Two criteria were used to evaluate the suggested method. The results were compared with the straightforward LSB algorithm as well as with the algorithm suggested in a prior reference study. The first criterion is a subjective one that is dependent on the HVS (human visual system) where the cover image and stego image are displayed on a number of people. The second criterion is an objective one where PSNR(peak signal to noise ratio), BER(bit error rate), SSIM(structural similarity index), and MSE(mean squared error) will be calculated. The findings demonstrated that there was no discernible difference between the cover Image and the generated Stego image to the unaided eye. The suggested algorithm also produced positive values for the PSNR, BER, SSIM, and MSE.

Content

List of Abbreviations

HVS	human visual system
PSNR	peak signal to noise ratio
BER	bit error rate
SSIM	structural similarity index
MSE	mean squared error
LSB	lease significant bit
STEGO	steganography

Chapter One

Introduction

1.1 Background

In the age of computers and quick communication, it's important to keep sent information (whether it is a message or plain text) safe from prying eyes while transmitting it via any electronic medium. Steganography is one such data protection method. Another name for data concealment is steganography (from the Greek words stegano for "covered" and graphos "to write"). Techniques for enabling communication between two people make up steganography. In the view of any observer, it conceals not only the communication's contents but also its very existence. Steganography is the practice of obfuscating the existence of data by transferring it across seemingly innocent carriers. In contrast to cryptography, where the message is visible but scrambled so that only a recipient with the right knowledge (encoding method and a key) can recover the message [1]

Watermarking and steganography are two popular methods of information concealment systems. Watermarking uses an implanted visible or invisible mark, whilst steganography is used for confidential communication. The method of digital watermarking is used to store copyright information. This information can be used to confirm ownership. Any user can identify the copyright ownership by extracting the data and comparing it to the original secret information. Steganography is the concealment of data in a way that makes it impossible to identify the concealment [2].

Users of the public channel employ texts as "objects" in their day-to-day activities. Due of its modest size in comparison to other items, it makes a perfect cover item

for data that is being sent between a sender and a recipient. Additionally, text steganography enhances the hidden capacity by taking use of grammatical or orthographic differences between languages. However, due to the lack of redundant information in text files, text stenography is one of the most difficult subfields in stenography. Text also has a nearly same structure, which makes changes obvious [3].

In this thesis, a brand-new method of mapping cover image pixels is suggested to produce a high-security, multi-level image steganography that may be applied to bank check systems. The name, the money, and the date are embedded in the text file after the RGB Stego image is first converted to three gray scale images using the Radon Transform mapping method. The check owner will then use Hadamard coding to construct a Stego-image using the least significant bit of the check image. To obtain the check information, the extraction operation is carried out on the receiver side.

By calculating the Mean to Square of Error (MSE), Root Mean Square Value (RMS), Rate of Bit Error (BER), Ratio of Signal to Noise (SNR), and Peak of Ratio of Signal to Noise (PSNR) with SSIM technique, the recommended Steganography technique is tested for resistance to a variety of attacks.

1-2 Classification of the Data Protection Systems

There are other ways to safeguard sensitive information, but the three most widely utilized ones at the moment are "Steganography," "Watermarking," and "Cryptography," as shown in Figure (1.1) [4].

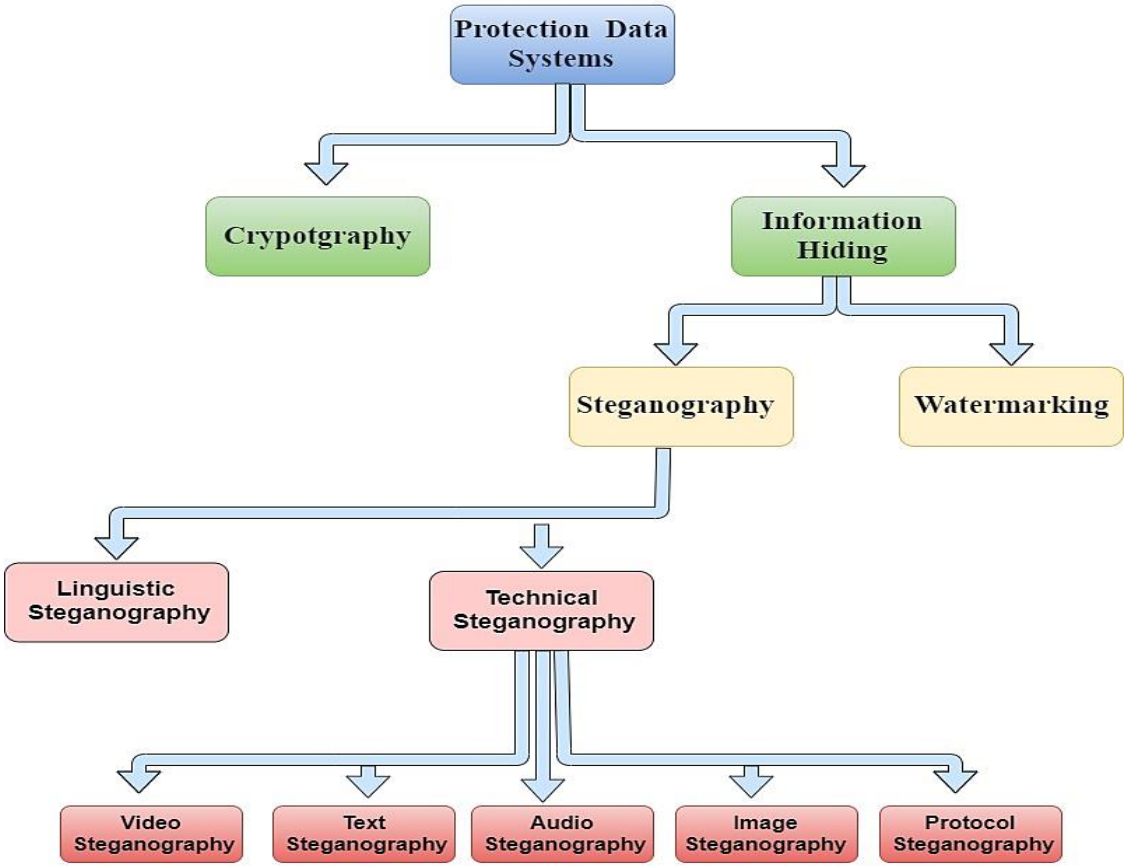


Figure (1.1) Protection types of data systems.

1.3 Digital Steganography Applications

This method has a wide range of uses, which can be distilled into the following[5]:

1_Copyright protection: Determining and ensuring copyright property is the primary effective use of digital steganography. The digital content can be hidden with watermarks that show ownership partner identification info.

2_Data Hiding: The most popular application, data hiding is a mechanism to convey information covertly so that no one who is not authorized can intercept it.

3_Authentication: This process is used to encode the data and determine whether the information is authentic.

4_Application in medicine: The patient's name and other information can be printed on X-ray reports and Magnetic Resonance Imaging (MRI) scans. To avoid any confusion in the reports of two or more patients, this application is crucial in helping the patient receive therapy.

5_Digital finger printing: The ability to identify the owner of digital content by their unique fingerprint and detect the appearance of prohibited copies.

6_Broadcast and publishing monitoring: Here, a signature technique is employed to identify the content's owner, but other distribution routes, such as computer networks, television and radio broadcasts, are also available. This program allows material to be tracked in terms of its appearance and timing. 1.4 Problem Description

7_Without a doubt, the bank procedure requires time for money to be transformed or until it is obtained directly from a particular bank, so the person who needs to transform or write a check to another bank must do a number of tasks to complete the process. In other situations, he may also need to bring the identify of the person who is trying to change the money over to him. In addition to the forging of a bank check, all these procedures could be accompanied by errors in the worth of money or the person's name, which could cause both the individual and the bank to lose money.

8_The forger can use a fake identity to pay the bank check or get the transformation, or he can copy the person's signature. A bank check that you write for someone can be cashed without any fees or for a very small amount, but the money transformation company charges a percentage as transformation fees.

1.4 Problem Statement

1_ Its too hard to deal with text in steganography system because text is more sensitive than other multimedia files .

2_ Difficulty retrieving the Text after the steganography without errors.

3_ when using bank check as an application, the information embedded must be preserved completely in order not to cause money losses.

4_ Building a system with automatic error correction rates to increase the strength of information preservation.

1.5 Literature Review

Many researches have been proposed on various issues around Image steganography because of its growing significance and utilize as depicted in the following survey:

S. Bhattacharyya etal (2013) [6], Here, a new transform domain image steganography technique is presented where Hadamard Transform is performed on each 4 X 4 block of the cover image and the secret data is embedded in the transform coefficients. Extraction is carried out from the same coefficients used during embedding stages, results an efficient and robust stenographic technique which can avoid various image attacks and works perfectly well for both uncompressed and compressed domain. Experimental results demonstrate the effectiveness and accuracy of the proposed technique in terms of security of hidden data and various image similarity metrics.

H. Abdul- Jaleel Alasadi and O. Qasim Jumah Al-Thahab (2014) [7] produce a thesis that developed a new algorithm for audio watermarking technique which based on hybrid transform (discrete wavelet transform and radon transform). This study considers two types of encryption: linear feedback shift register sequence and

Gold sequence. Three images are taken as a test image with an average PSNR 125 dB.

S. Thenmozhi and M. Chandrasekaran (2014) [8] stated a novel image steganography technique in his paper for embedding secret image into the digital images. Stego image is obtained by combining discrete wavelet transform, neural network and radon transform. It consists of three phases. In phase one, host image is decomposed into four parts by applying discrete wavelet transform and optimal sub band is selected for embedding. Radon transform is applied on payload for encryption in phase two. Finally, Back propagation neural network is employed to conceal the encrypted secret information in selected sub band coefficients of the host image. From the experimental results, it can be shown that the proposed image steganography embeds information effectively, better secrecy and a better visual display.

S. Uma Maheswari and D. Jude Hemanth (2015) [9], presented in their paper a frequency domain steganography method that operating in the Ridgelet transform. In the embedding phase, the proposed hybrid edge detector acts as a preprocessing step to obtain the edge image from the cover image, then the edge image is partitioned into several blocks to operate with straight edges and Ridgelet transform is applied to each block. Then, the most significant gradient vectors (or significant edges) are selected to embed the secret data. Authors employed the hybrid edge detector to obtain the edge image, which increases the embedding capacity. Here PSNR is above 49 dB.

Y. E. A. AL-SALHI and S. LU (2015) [10], combined among Hadamard transformation and Absolute Moment Block Truncation Coding to make a new concept called (H-AMBTC), this concept used for compressing the cover file and conceal the secret data into the cover file. In this paper, the comparison process of

the H-AMBTC technique is done for 2x2, 4x4, 8x8 and 16x16 block sizes. The technique recovered the cover image and the secret image completely.

In the same year, H. ABDELLATIEF HUSSEIN [11], prosed a new concept for performing hidden secret data, called MultiLevel Steganography technique. Here, two-levels of stenography have been applied; The first level is called (the upper-level), and it has been applied using enhance LSB image steganography, the secret data in this level is English text, and the cover is gray scale or RGB image, the output is a stego_image. The second level is called (the lower-level); it has been applied using pixel intensity based image steganography. In this level another RGB image has been used as a cover image, embeds as a secure data, and generates the new RGB image as stego image.

A. Amsaveni and P.T Vanathi (2017) [12], proposed a reverse data hiding techniques based on Radon and discrete wavelet transform. The technique is based on three criteria: invisibility, robustness and reversibility. A based strategy is used frequency because it is ahead of the spatial technique in the key points of robustness and reversibility of signal and image processing. Radon transform performs rotation, scaling and translation and changes the location of the secret bits. Proposed method contains blue, green and red channels, so it is useful for many images.

B. Abd-El-Atty, etal (2018) [13] proposed a Hadamard transformation and the novel enhanced quantum representation for quantum images (NEQR). Here a quantum image steganography scheme is embed a quantum text message into a quantum image. The extraction process can recover the text message with the stego image only. The simulation results demonstrated that the proposed scheme has high-capacity, good invisibility, and high security.

M. O. Espina, etal (2019) [14] presented a multiple tier information security through image steganography technique using a novel puzzle in YCbCr color space, and digitally signed stego image for authentication. Experimental results show that

the resemblance between the stego-images and cover images is high. The recognition of the stego image is small, with the use of the Human Visual System (HVS) having an average PSNR value of 47.72db.

A. Salem Ali, etal (2020) [15] stated the that the current techniques have not been successful in attaining more improved security caused by the non-encrypted data that only underwent the first layer of concealment through merely a straightforward embedment process of the secret data, thus allowing the extraction of the concealed data to be quite simple for hostile entities. Hence, in this study the Bit Inverting Map method is improved so that it narrows the gap of existing work. The experimental results indicate that the proposed framework maintains a better balance between image visual quality and security, with relatively less computational and complexity.

A. Ali Husain and O. Qasim Jumah Al-Thahab (2020) [16], proposed a way of both steganography and watermarking technique to maintain the video copyright by hiding publisher logo image inside the digital video. Here, an optimized technique is proposed by utilizing the advantages of Turbo code to encrypt the logo image bits and using a least significant bit (LSB) for embedding the encoded logo pixels inside the frames of the cover video. The system proved a high quality in result Stegovideo by relative rate reach to 98% from the quality of the original video and PSNR equal about (57 dB) with high robustness against noise like salt and pepper and Gaussian noise.

H. Kweon etal (2021) [17], proposed a deep multi-image steganography with private keys. Here deep CNN-based algorithms have been proposed to hide multiple secret images in a single cover image. In addition, the concept of private keys for secret images is introduced. This method conceals multiple secret images in a single cover image and generates a visually similar container image containing encrypted secret information inside. In addition, private keys corresponding to each secret

image are generated simultaneously. Experimental results demonstrate that the proposed algorithm effectively hides and reveals multiple secret images while achieving high security.

A. A. Mohammed etal (2021) [18], presented a novel watermarking way, which employs hybrid Multiscale/Multiresolution frequency coefficients selection using the Fast Discrete Curvelet Transform (FDCT) in conjunction with Singular Value Decomposition (SVD). In order to add an extra layer of security, the Radon Transform (RT) is applied on the watermarks before embedding process. The proposed method attained promising results and has shown that the imperceptibility of watermarked medical images is higher than 55 dB.

F. Haojun etal (2021) [19] presented a multi-level digital watermarking algorithm that suitable for raster geographic data. Here the multi-level watermark embedding strategy is established on this basis, thereby the proposed system based on the watermark segmentation mechanism with the traditional robust digital watermarking algorithm as the prototype. The results show that the proposed algorithm maintains the performance of the prototype algorithm, and solves new problems caused by the multi-level circulation of raster geographic data, such as multi-copyright protection and multi-user tracking and has high practical values.

Y. Qian Zhang etal (2022) [20] used in their paper a lightweight transform Discrete Hadamard Transform (DHT) with a simple but high-performance image steganographic model. In the case of only stego-image passed, the experiment results demonstrate that the proposed scheme achieves high imperceptibility and security even in the dense embedding of 8 BPP (Bits Per Pixel). Furthermore, the proposed scheme shows desirable robustness and it is efficient.

1.6 The Main Contributions and Objectives

The main aim of this thesis can be depicted as follows:

1) Proposed a new way for the bank check cashing that minimize the time in the process of bank system, so that the bank does not need the identity or signature.

2) Increase the security of the bank check system.

3) Make a Bank check system have little no. of processes so that minimizing the process will in turns minimize the error that may happened.

4) Develop a steganography system that face the counterfeiters and the hackers, which work under different image noise level by using a multi-level steganography process for first time in this application.

5) Improve the Performance Parameters of the proposed multi-level Stego-system like BER, SNR, SSIM, MSE and RMSE.

1.7 Outline of The thesis

This dissertation consists of five chapters, and a list of references. The first one is introduction.

Chapter 2: In this chapter explains the requirements and theories of a digital image multi-level steganography technique, and the performance evaluation of it.

Chapter 3: Introduces the proposed multi-level steganography system and then explain each part widely.

Chapter 4: Explains the different types of attacks studies with the results and discussions for each one, in addition testing the system with the use of social media applications.

Chapter 5: Which contains the conclusions and future works of this thesis.

CHAPTER TWO

BACKGROUND THEORY

2.1 Introduction

The concept of WYSIWYG (What You See Is What You Get) is no longer correct. It would not trick a Steganography person as it was previously, because of the development in the computer systems and steganalysis tools. So, there is a need for new algorithm more that must be secure and reliable and enable entirely hiding the presence of data and deceive various steganalysis systems. In this, the role of the text Steganography emerged as a new secret algorithm used to hide the data in a way cannot be detect easily [21].Text steganography system nowadays is seen as a solution to securing problems [22]. Covering information in an image file can be seen as an extension of hiding data in an image file [23].

In this chapter, the theories of LSB, Radon transform and Turbo Code and Hadamard code are explained briefly with their mathematical expression. At the end of the chapter, evaluation of the Performance of steganography system by many tests like BER, SSIM, PSNR, etc. are studied.

2.2History of Steganography

A simplified representation of Steganography theory is the prisoner's problem where Alice and Bob are in jail locked up in different cells. Where they want to communicate in order to plot an escape plan But any connection between them is checked by a warden named Wendy, who will put them in individual jail at any slight-doubt of trouble. In order to solve this problem, Alice will use the global

standard of Steganography, where Bob wishes to send a secret letter M to Alice. In order to do this he" embeds" M inside a cover-object "letter", to get the Stego-letter S, then sent the Stego-letter through a public channel. The warden Wendy who is free to review all messages transferred among Alice and Bob and decide whether the message is positive or negative. He checks the message and tries to determine if it possibly includes a hidden letter. If it appears that it does, then she takes suitable action else she allows the letter to pass without any modification [24].

In the present day, as a result of growth in inter-linked multimedia systems, electronic digital camera, wireless networks and digitalisation, therefore vastly increased the possibility of distribution and regenerating of information. Steganography procedures had been transferred into digital processing. Currently, research, study and development in the area of digital signal processing, information theory and encoding techniques are supporting in getting stable and robust steganography systems [24].

The general steganography algorithm can be described in figure (2.1) where the secret data type may take different binary bits formats like digital text data, digital image file and digital video file. The digital cover file can take all digital media formats like video, image, etc. The data covered inside a host media (cover) is named as 'Secret information', while the output embedded digital cover media after hiding data in it is termed as 'Stego- file'. The stego- file is shared within an open channel or unsecured communication channel. At the reception, a reverse embedding and decryption algorithm is assumed to use on the stego-file in order to extract on secret data [25].

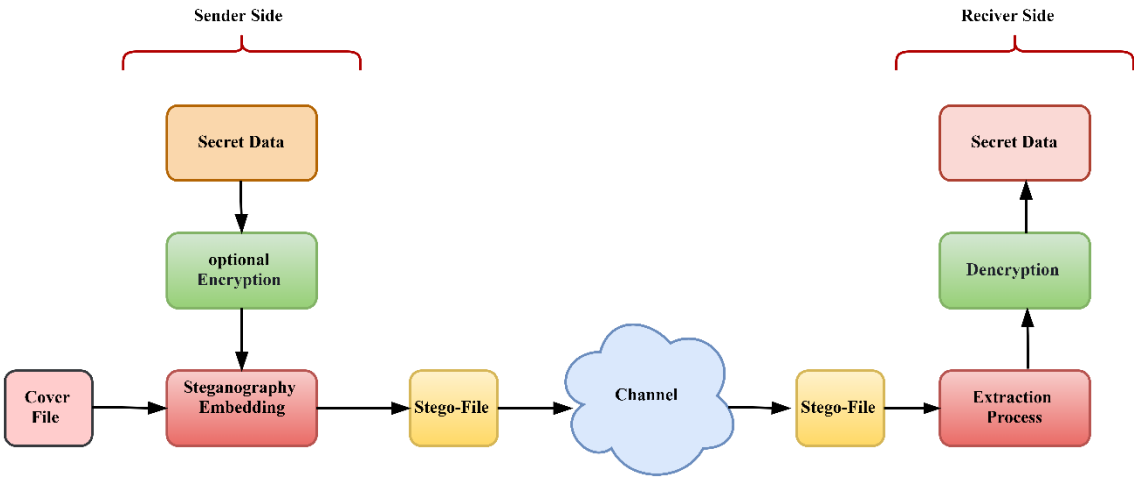


Figure (2.1) General Block diagram of the Steganographic system algorithm.

In every steganographic system, there are three essential properties used to experiment the effectiveness of a steganographic system, namely capacity, security and robustness. As explained in figure (2.2), while some researcher considered that there are four properties, namely imperceptibility.[26]

- Capacity: the capacity defined as the quantity of the secret data bits that can be embedded in the bits of the cover-file. The efficient steganographic system aims to achieve maximum information hiding inside a minimum cover file in a way that maintaining the satisfactory quality of the stego-file. It is also known as embedding capacity or hiding capacity and is measured in terms of bits per transform [27].
- Security: In the system steganographic, the security word indirectly refers to undetectability or unnoticeability. So, any steganography technique considers as a secure system if the secret information is not noticeable or removable by statistical means or by an attacker after being detected. [28].
- Robustness: it represents the ability of a Steganography algorithm to embed and extract the secret data from the cover file after corrupted inside noise channel by using computer processing or any other method [28].

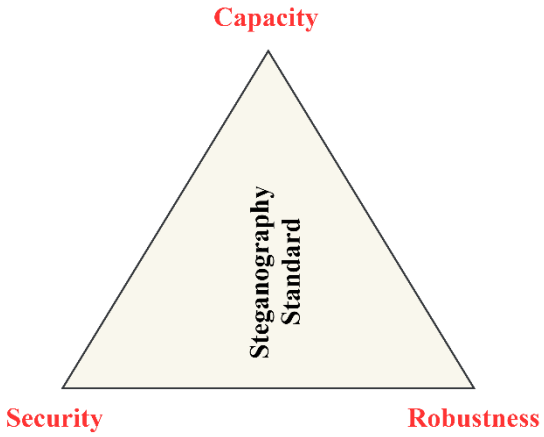


Figure (2.2). The main properties of the data hiding

2.3 (LSB) Least Significant Bits

LSB is the most straightforward method to hide a secret data inside the cover media(embed data in an image file) in a way that cannot be distinguishing the variation in the cover image by the abstract human eyes [29].

In computing, the cover image can represent as a matrix of pixels so that each pixel can represent by 1byte consist of 8 bits which represent 256 gray coolers between the black and white, while for the color image there are 256 shades for each red, green and blue image. The LSB, which determines whether a number is odd or even, is the position of the bit that contains the units value in a binary integer. Figure (2.3) describe of the decimal no.149 in binary format with an LSB that highlighted by a square and its value is 1. the LSB decimal expression value in the 8-bit binary digit is "1" while the MSB Represents a value of "128" [30,31].

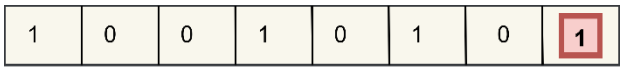


Figure (2.3) Binary representation of pixel 149

The LSB aims to replace the minimum weighting value of pixel bits by message bits. So, when the color image is using as a cover image, the bits of each of the red, green and blue (RGB) color elements can be used. In other words, one can store 3 bits in each color pixel (since each color pixel is the result of combine three pixels (red, green and blue) and each one of these pixels is represented by 8-bits. So, for example, if an image that has dimension 1280 × 720-pixel image, can thus hide a total amount of 2,764,800 bits or 354,600 bytes of embedded data. The main principle of LSB can be shown in the following example.

If you want to embed a pixel with an intensity value of (200) in the matrix below, then:

255	1	10
181	228	128
25	15	12

- Convert each byte matrix to 8 bits binary

11111111	00000001	00001010
10110100	11100100	10000000
00011001	00001111	00001100

- Convert the pixel (that have intensity value) to binary

200= 1 1 0 0 1 0 0 0

- Replace LSB of the matrix in pixel bit data

1111111**1**	0000000**1**	0000101**0**
1011010**0**	1110010**1**	1000000**0**
0001100**0**	0000111**0**	00001100

- Finally, convert the result matrix to decimal

255	1	10
180	229	128
24	14	12

Figure (2.4) displays a basic summary of the phenomenon. It is clear from the sample that there is a very small amount of change—only 4 bytes—and that change. In light of this, it can be said that the LSB approach is highly effective at concealing data that a human eye cannot see [31].

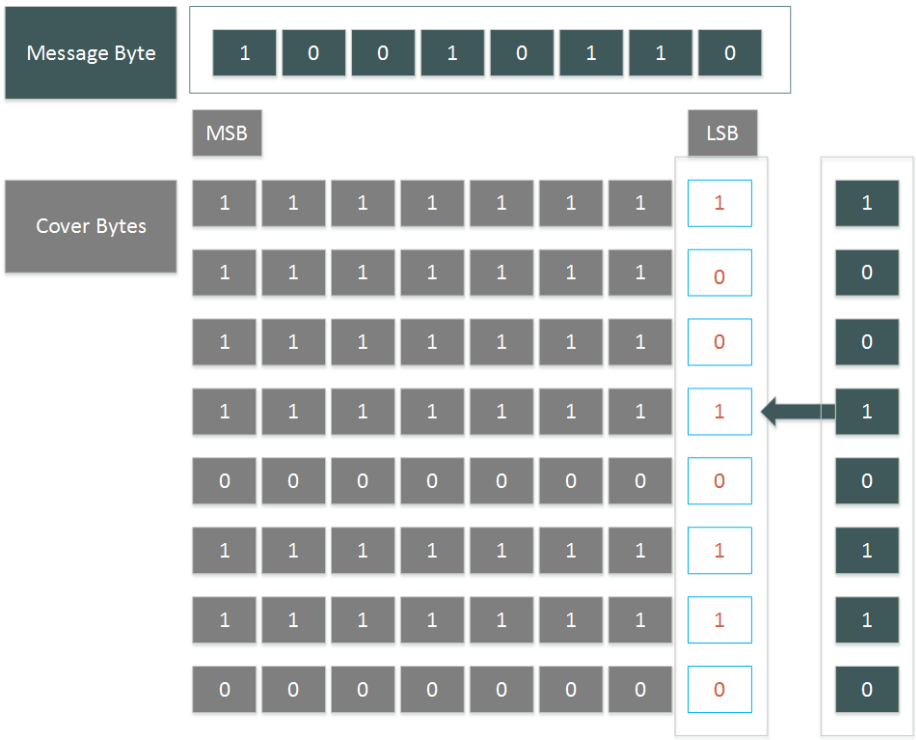


Figure (2.4) . The binary description of LSB replacement

2.4 Pseudorandom sequence.

The most well-known category of digital sequences is pseudorandom (PR) or pseudonoise (PN) sequences. In the 1950s, interest in pseudorandom sequences and their applications started to grow [32].

They are now often employed in current cellular communication systems for practical purposes. Binary, non-binary, and other types are the three basic classifications used for digital sequences. The most often utilized class of sequences can be considered to be binary sequences. Embedding non-binary sequences in potent digital signal processing hardware made them usable implementations. They have numerous qualities that are better than those of binary sequences, with quaternary sequences serving as an example [33].

Sequences are included in the third category of other types because they have been thought to satisfy particular application needs. For instance, in frequency-hopping spread-spectrum systems, radar and pulse compression waveforms, image processing systems, etc. [34].

2.4.1 Binary PN Sequences.

Maximal length binary sequences (m sequences), Other names for these sequences are linear feedback shift register (LFSR) sequences and pseudo random binary sequences (PRBSs) [1].

The majority of PR's attributes are illustrated as follows [35].

A. Balance Property.

The number of 1s in a whole period of a PN sequence differs from the number of 0s by no more than 1. There is always one more 1 than 0 than there are.

B. **Run Property.**

As long as these fractions reflect significant numbers of runs, one-half of the runs of each kind in each period of a maximum length sequence are of length 1, one-fourth are of length 2, one-eighth are of length 3, and so on.

C. Correlation Property.

Correlation is a measure of how similar two sequences are. When two sequences are being compared, it is referred to as a "cross correlation" and as a

"autocorrelation" when they are the same. The relationship between the two sequences, x and y, with regard to the time delay m is expressed mathematically in equation (2.1) as follows:

$$R(m)_{xy} = \sum_{k=0}^{L-1} x(k)y(k+m) \qquad (2.1)$$

Where R(m) is the autocorrelation equation for the digital bit sequence can thus be written in equation (2.1):

R (m) is equal to the sum of all "1" bits.

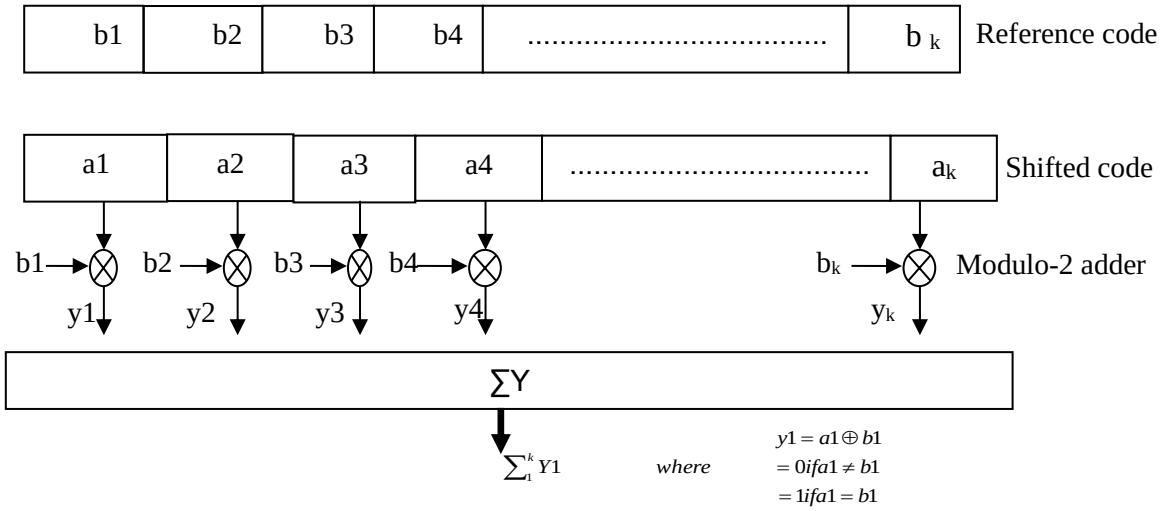


Figure (2.5): a K-length correlator the output of each stage of shifting one sequence ai via a K bit shift register is then utilized for a series compare K XOR gates.

A linear feedback shift register is the most crucial tool for creating pseudorandom binary sequences (LFSR). An LFSR sequence generator with m stages will always produce a periodic output sequence. A maximal length sequence, or M-sequence, is an output sequence from a shift register with a maximum period of N = 2m-1. The generator polynomial of the m-sequence is a primitive polynomial, where m is the degree of the generator polynomial [36].

g(x) is a primitive polynomial of degree m if the smallest integer n for which g(x) divides $x^n + 1$ is $n = 2^m - 1$.

$g(x) = x^5 + x^4 + x^2 + x + 1$ is a primitive. On the other hand,

$g(x) = x^5 + x^4 + x^3 + x^2 + x + 1$ is not primitive since

$x^6 + 1 = (x + 1)(x^5 + x^4 + x^3 + x^2 + x + 1)$, so the smallest n is 6.

The number of primitive polynomial of degree m is equal to

$$\frac{1}{m}\phi(2^m - 1) \tag{2.2}$$

where $\phi(n) = n\prod_{p|n}\left(1 - \frac{1}{p}\right)$, P| n denotes "all distinct prime divisors of n", f(n) is the quantity of positive integers that are relatively prime to n and less than n. For example, if m=4, then

$\frac{1}{4}\phi(2^4 - 1) = \frac{1}{4}(1 - \frac{1}{3})(1 - \frac{1}{5}) = 2$. Then there are two polynomials:

100011 and 11001.

2.5 Hadamard Code

It is an error correction code that is used for error detection and correction when transmitting massage over a very noisy or unreliable channel, Due to their unique form and the multiple characteristics that define them, Hadamard matrices have numerous applications in many different mathematical fields. This study illustrates a recently discovered relation between minors of Hadamard matrices based on calculus and basic number theory techniques. A straightforward method to determine whether or not a Hadamard matrix of order n k can be embedded in an n-dimensional Hadamard matrix. The outcomes also offer solutions to the issue of calculating the values of the determinant function's spectrum for specific Hadamard minor orders by including an analytical formula in matrices [37,38].

The following formula creates a Hadamard matrix of order n.:

$$H = [1] \equiv [0]$$

$$H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \equiv \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, H_n = H_2 \otimes H_{n|_2}$$

when the kronecker product is indicated by⊗ two matrices A and B's direct product is known as the kronecker product and is also known as the tensor product.

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B \dots \dots a_{1n}B \\ a_{21}B & a_{22}B \dots \dots a_{2n}B \\ & \cdot \\ & \cdot \\ & \cdot \\ a_{m1}B & a_{m2}B \dots \dots a_{mn}B \end{bmatrix} \quad (2.3)$$

For example :

$$H_4 = H_2 \otimes H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \quad (2.4)$$

2.5.1 Hadamard Decoding methods :

Two techniques for deciphering Hadamard codwords will be introduced in this section:

Let w be the word that is heard:

Technique 1:

Find the closest codeword $\boldsymbol{n} \in \boldsymbol{H}_{(\boldsymbol{n},\boldsymbol{p})}$ such that

$$d(w,u) \leq d(w,v), \forall v \in H_{(n,p)}$$

where d is the distance between codwords. (2.5)

Technique 2: This method composed of two steps:

Step 1:

Compute $S = H_{(n,P)} * w^t$ (2.6)

Step 2: The received word is a codeword in the Hadamard code H ((n,p)) if S=, where (is a zero vector, but if S the received word w has been delivered wrongly. as well as each Hadamard code column, which gives the position of the error in w, in order to ascertain where the error in w was[38].

As an example, if the original message is (1,1,0) and the Hadamard code is used with order n = 8, the encoded message is H6=. (0,1,1,0,0,1,1,0). Let w = be the updated version of the message H6 that was encoded (0,1,0,0,0,1,1,0). How can we interpret it? the following

By 1st Technique :

$d(\omega, H_0) = 3, d(w, H_3) = 5, d(w, H_6) = 1$
$d(\omega, H_1) = 3, d(w, H_4) = 3, d(w, H_7) = 5$
$d(\omega, H_2) = 5, d(w, H_5) = 5$

seen that $d(w_y H_6) \leq d(\omega, H_i), \forall i, i = 0,1, \ldots\ldots,7$ and thus H_6 is the The most likely communicated codeword.

By 2nd Technique :

$$S = H_{(8,3)} * w^t = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} * \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} \quad (2.7)$$

Since S is similar to the third column of the Hadamard code with order n=8, we can determine that the error was in the third position of w. Therefore, we write w = (0,1,1,0,0,1,1,0) . Since , $w \in H_{(8,3)}$code,therefore we can see that the original message was (1,1,0).

2.6 Radon transforms

Johann Karl August Radon, an Austrian mathematician, is remembered via the name Radon transform [39]. In image processing, the radon function computes projections of an image matrix along predetermined axes. A collection of line integrals makes up a projection of the two-dimensional function f(x,y). The radon function calculates the line integrals from many sources along parallel beams or routes that point in a specific direction [40].

This has given rise to numerous line detection applications in seismic, computer vision, and image processing. In many different applications, including radar imaging, geophysical imaging, nondestructive testing, and medical imaging in CT scans, the radon transformation is a crucial tool [41]. In that location, the inverse Radon transform is used [39].

The distance between the beams is 1 pixel unit. The radon function rotates the source around the center of the image, taking several parallel-beam projections of the image from various angles. A single projection at a given rotational angle is shown in the following figure (2.6) [40].

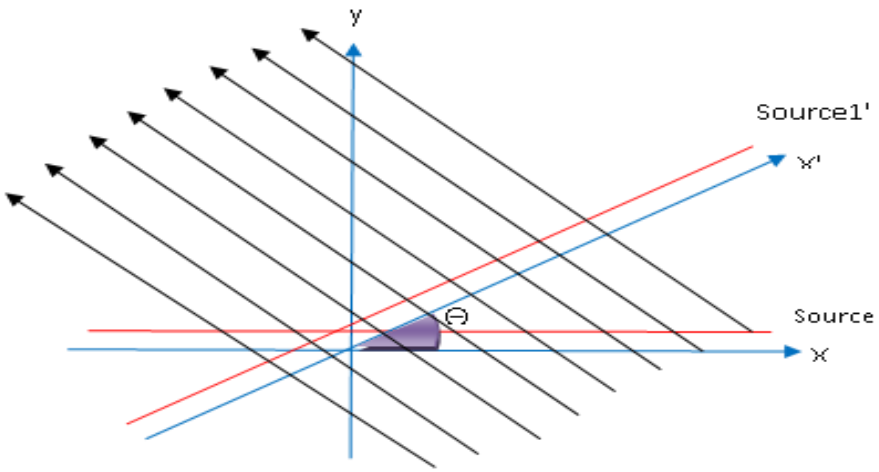


Figure (2.6): Parallel-beam projection at angle theta.

For instance, the line integral of f(x,y) in the vertical direction is the projection of f(x,y) onto the x-axis, and the line integral in the horizontal direction is the projection of f(x,y) onto the y-axis. Figure (2.7) [41] depicts the horizontal and vertical projections of a simple two-dimensional function.

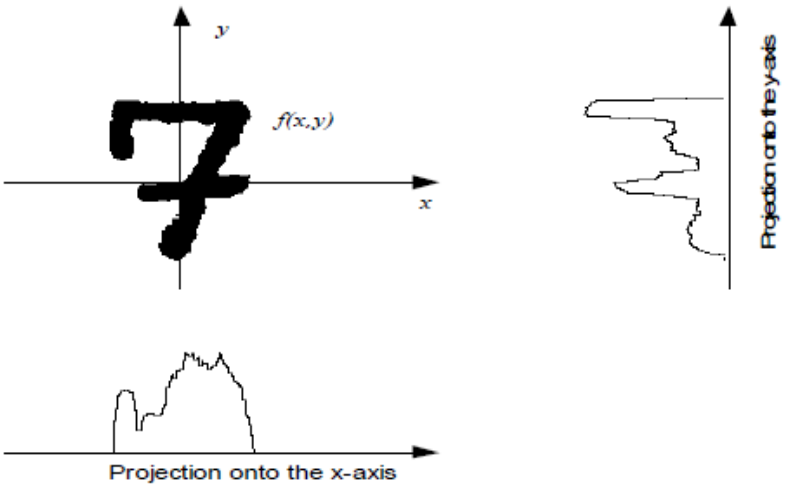


Figure (2.7): Horizontal and vertical projections of simple function.

The Radon transform is an angle-dependent projection of the picture intensity down a radial line. The values along the x'-axis, which is rotated degrees counterclockwise from the x-axis, make up the radial coordinates. The middle pixel of the image presented in figure (2.8) [41] serves as the origin for both axes.

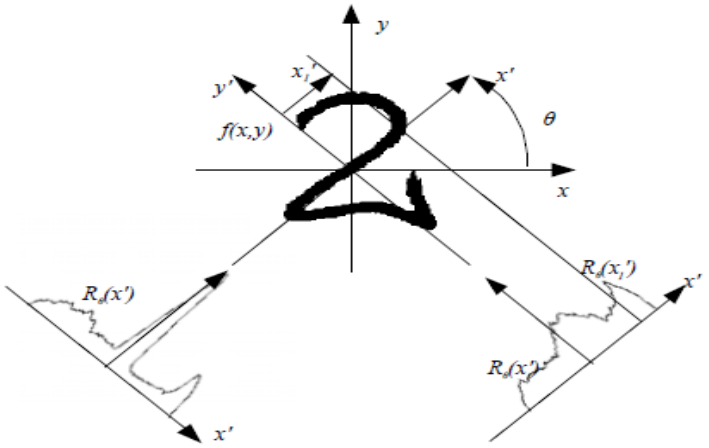


Figure (2.8): Geometry of the Radon Transform.

Correlation is a measure of how similar two sequences are. When two sequences are being compared, it is referred to as a "cross correlation" and as a "autocorrelation" when they are the same. The relationship between the two sequences, x and y, with regard to the time delay m is expressed mathematically in equation (2.1) as follows:

This can be written mathematically by defining:

$$x' = x\cos\theta + y\sin\theta \qquad (2.8)$$

After which the Radon transform can be written in equation (2.9):

$$R_\theta(x') = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f(x,y)\delta(x\cos\theta + y\sin\theta - x')dxdy \qquad (2.9)$$

Where $\delta(\cdot)$ is the delta function with value not equal zero only for argument equal 0, x' is the perpendicular distance of the beam from the origin and θ is the angle of incidence of the beams.

2.6.1 The Finite Radon Transform:

Toft [42] and Abbas Kattoush [43] defined briefly the Finite Radon Transform (FRAT) for two dimensional signals. For simplicity the following steps can be done as**:**

Step 1: Assume the serial data stream is d(k). The data symbols to be transferred are created as a one-dimensional vector by changing the form of d (k) from serial to parallel:

$$d(k)= (d_0\ d_1\ d_2\ \ldots\ldots d_n)^T \tag{2.10}$$

where the time index (k) and the vector length (n) are the appropriate values.

Step 2: Transform the one-dimensional vector d(k) encoding the data packet as a two-dimensional matrix D(k), where the matrix resize process specifies that p should be a prime value.

Step 3: For getting a matrix F(r, s), do a (2-D)FFT for a matrix D(k). It shall be referred to simply as F.

$$F(r,s) = \sum_{m=0}^{p-1}\sum_{n=0}^{p-1} D(m,n) e^{-j(2\pi/p)rm} e^{-j(2\pi/p)ns} \tag{2.11}$$

Step4: Rearrange the matrix F's elements in accordance with the optimum ordering procedure. Therefore, the size of the resulting matrix, which will be represented by the symbol Fopt, will be p(p+1). For window = 7 of FRAT, the two matrices are provided by:

$$F = \begin{bmatrix} F1 & F8 & F15 & F22 & F29 & F36 & F43 \\ F2 & F9 & F16 & F23 & F30 & F37 & F44 \\ F3 & F10 & F17 & F24 & F31 & F38 & F45 \\ F4 & F11 & F18 & F25 & F32 & F39 & F46 \\ F5 & F12 & F19 & F26 & F33 & F40 & F47 \\ F6 & F13 & F20 & F27 & F34 & F41 & F48 \\ F7 & F14 & F21 & F28 & F35 & F42 & F49 \end{bmatrix} \tag{2.12}$$

$$F_{opt} = \begin{bmatrix} F1 & F1 & F1 & F1 & F1 & F1 & F1 & F1 \\ F2 & F0 & F9 & F6 & F8 & F21 & F14 & F13 \\ F3 & F9 & F7 & F31 & F15 & F34 & F20 & F18 \\ F4 & F28 & F25 & F46 & F22 & F47 & F26 & F23 \\ F5 & F30 & F33 & F12 & F29 & F11 & F32 & F35 \\ F6 & F39 & F41 & F27 & F36 & F24 & F38 & F40 \\ F7 & F48 & F49 & F42 & F43 & F37 & F44 & F45 \end{bmatrix} \quad (2.13)$$

Step 5: To get the Radon coefficients matrix R, take the 1D-IFFT for each column of the matrix Fopt.

$$\boldsymbol{R} = \frac{1}{p}\sum_{k=0}^{N-1} \boldsymbol{F}_{opt} \boldsymbol{e}^{\frac{j2\pi kn}{p}} \quad (2.14)$$

Where N=p*(p+1).

Step 6: Create the complex matrix from the real matrix R so that it has dimensions of p (p + 1) / 2 as follows:

$$\overline{r_{l,m}} = r_{i,j} + jr_{i,j+1}, 0 \le i \le p, 0 \le j \le p \quad (2.15)$$

where, $\overline{r_{l,m}}$, refers to the elements of the matrix $\overline{R}$, while $r_{i,j}$, refers to the elements of the matrix R. matrixes R and $\overline{R}$ are given by:

$$R = \begin{bmatrix} r_{1,1} & r_{1,2} & r_{1,3} & \ldots\ldots & r_{1,p+1} \\ r_{2,1} & r_{2,2} & r_{2,3} & \ldots\ldots & r_{2,p+2} \\ \vdots & \vdots & \vdots & \ldots\ldots & \vdots \\ \vdots & \vdots & \vdots & \ldots\ldots & \vdots \\ r_{p-1,1} & r_{p-1,2} & r_{p-1,3} & \ldots\ldots & r_{p-1,p+1} \\ r_{p,1} & r_{p,2} & r_{p,3} & \ldots\ldots & r_{p,p+1} \end{bmatrix} \quad (2.16)$$

$$\overline{R}=\begin{bmatrix} r_{1,1}+jr_{1,2} & r_{1,3}+jr_{1,4} & \ldots\ldots & r_{1,p}+jr_{1,p+1} \\ r_{2,1}+jr_{2,2} & r_{2,3}+jr_{2,4} & \ldots\ldots & r_{2,p}+jr_{2,p+1} \\ \vdots & \vdots & \ldots\ldots & \vdots \\ \vdots & \vdots & \ldots\ldots & \vdots \\ r_{p-1,1}+jr_{p-1,2} & r_{p-1,3}+jr_{p-1,4} & \ldots\ldots & r_{p-1,p}+jr_{p-1,p+1} \\ r_{p,1}+jr_{p,2} & r_{p,3}+jr_{p,4} & \ldots\ldots & r_{p,p}+jr_{p,p+1} \end{bmatrix} \quad (2.17)$$

Prior to downscaling mapped data, complex matrix construction is used to increase bit per Hertz of mapping.

Step 7: The matrix should be shrunk to a one-dimensional vector r(k) of length. $p\times(p+1)/2$.

$$r(k) = (r_0\ r_1\ r_3\ \ldots\ldots\ r_{p(p+1)/2})^T \quad (2.18)$$

Step 8: Take the vector r's 1D-IFFT (k).

$$s(k)=\frac{1}{p(p+1)/2}\sum_{k=0}^{N_C-1} r(k)e^{\frac{j2\pi kn}{p(p+1)/2}} \quad (2.19)$$

Where Nc= p*(p+1)/2.

2.6.2 The Inverse Finite Radon Transform:

To compute the inverse finite radon transform (IFRAT), the steps of computing the FRAT must be done but in a reverse fashion starting with step (8) to step (1).

Step 1: Take the 1D-FFT for the vector s(k).

$$r(k)=\sum_{k=0}^{N_c-1} s(k)e^{-\frac{j2\pi kn}{p(p+1)/2}} \quad (2.20)$$

Where Nc=p*(p+1)/2.

Step 2: convert a vector in one dimension r(k) of length p×(p +1) /2 to the matrix $\overline{R}$ which is complex value.

Step 3: Construct the real matrix R from the complex matrix $\overline{R}$ such that its dimensions will be p × (p +1).

Step 4: The 1D-FFT for each column of the matrix R is taken to obtain the matrix coefficients F_{opt}:

$$F_{opt} = \frac{1}{p}\sum_{k=0}^{N-1} Re^{-\frac{j2\pi kn}{p}} \qquad (2.21)$$

Where N=p*(p+1)

Step5: Redistribute the matrix Fopt's entries in accordance with the optimum ordering procedure. The dimensions of the resulting matrix will therefore be pp, and they will be represented by the letter F.

Step 6: Take the 2-D IFFT of the matrix F(r, s) to obtain the matrix D(k) . For simplicity it will be labeled by F.

$$D(m,n) = \sum_{r=0}^{p-1}\sum_{s=0}^{p-1} F(r,s)e^{-j(2\pi/p)rm}e^{-j(2\pi/p)ns} \qquad (2.22)$$

Step 7: Convert the data packet represented by matrix D(k) two-dimensional matrix to the one-dimensional vector d(k).

Step 8: Suppose d(k) is the serial data stream and convert d (k) from parallel form to serial form.

2.7 Turbo code

The term "Turbo-codes" refers to a novel class of convolutional codes that was suggested by Claude Berrou and a team of academics in 1993. [44]. Today, despite

the fact that the turbo code system has been around for more than 20 years, it is still employed in many communication systems due to its effectiveness and dependability in bit encryption, error correction, and other aspects. According to figure (2.9) [45], the overall design of the turbo code comprises of two or more corresponding Recursive Systematic Convolutional encoders (RSC).

Systematic codes make up most turbo encoders. Thus, to create an encoded output, the product codeword combines the sequence of input message bits and the parity sequence of bits generated from encoding the input message bit-stream with the same encoders. [46,47].

2.7.1 Turbo Code Encoder (TCE)

The most famous turbo code encoder uses two or more RSC encoders connecting in parallel and separated 1 by 1 interleaver part, as displayed in Figure (2.10). The first RSC encoder immediately encrypts the length-K of the input message m., to produce the first parity bits $p^{(1)}$; however, it is interleaved before encoding it by the second RSC encoder to produce the 2nd parity bits $p^{(2)}$. Turbo codes are systematic codes such that the product codeword consists the input bits at the first followed by parity check bits of all RSC encoder m, $p^{(1)}$ and $p^{(2)}$ to parity check $p^{(n)}$ and transmitted all. The number of party bit that follows each input bits depends on the number of Recursive Systematic Convolutional that connected in parallel in the turbo encoder system [48]. The turbo codeword is seen in equation (2.23).

$$C = [m_1\, p_1{}^{(1)}\, p_1{}^{(2)}\, \ldots . p_1{}^{(n)},\, \ldots \ldots , m_k{}^{(1)}\, p_k{}^{(1)}\, p_k{}^{(2)}\, \ldots . . p_k{}^{(n)}] \qquad (2.23)$$

Often, to increase the code rates, the filter outputs are punctured before multiplexing, as shown in Figure (2.10). The Puncturing is the process of systematically removing bits from one or more of the encoder output sequence,

and it acts only on the parity sequences where the systematic bits are not punctured [49].

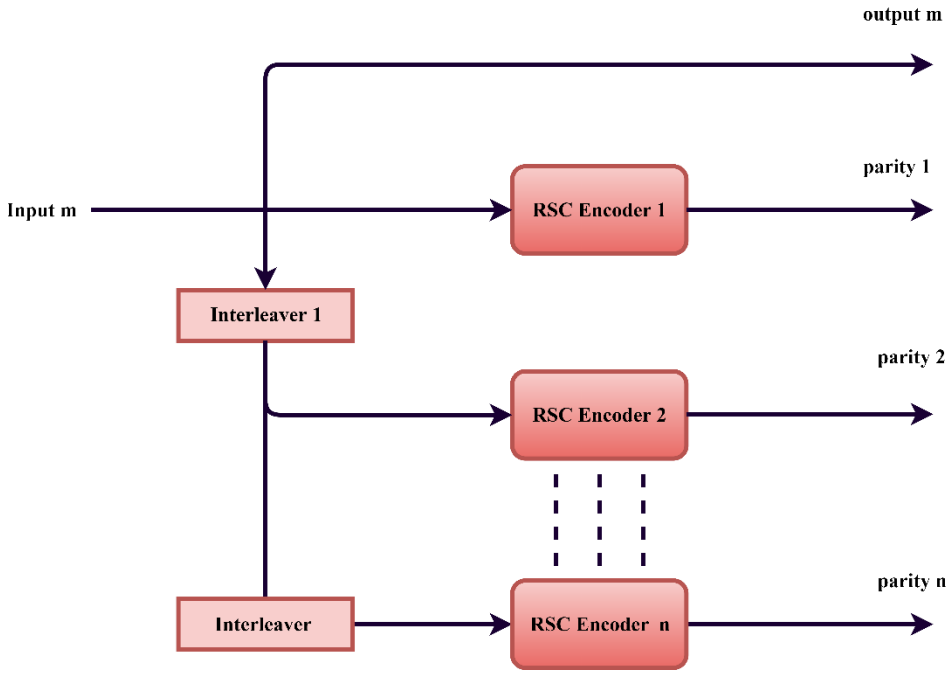


Figure (2.9).The fundamental turbo code with rate 1/n

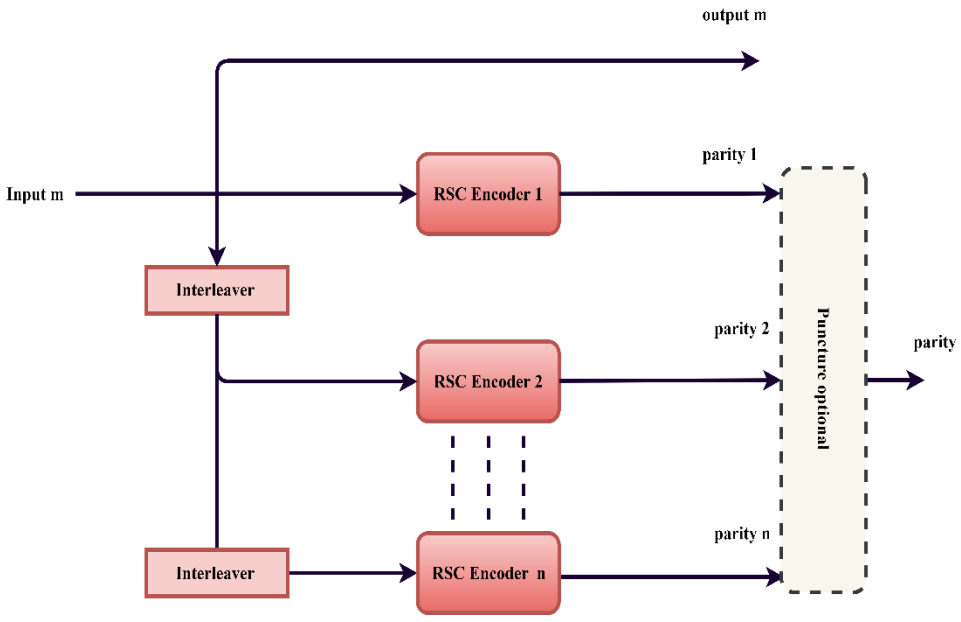


Figure (2.10).The Fundamental Turbo Code With Puncture

Figure (2.11) show example of turbo cod with rate 1/3 and RSC encoder transfer function $\boldsymbol{G(x)} = 1/1 + \boldsymbol{x^2}$ [68].

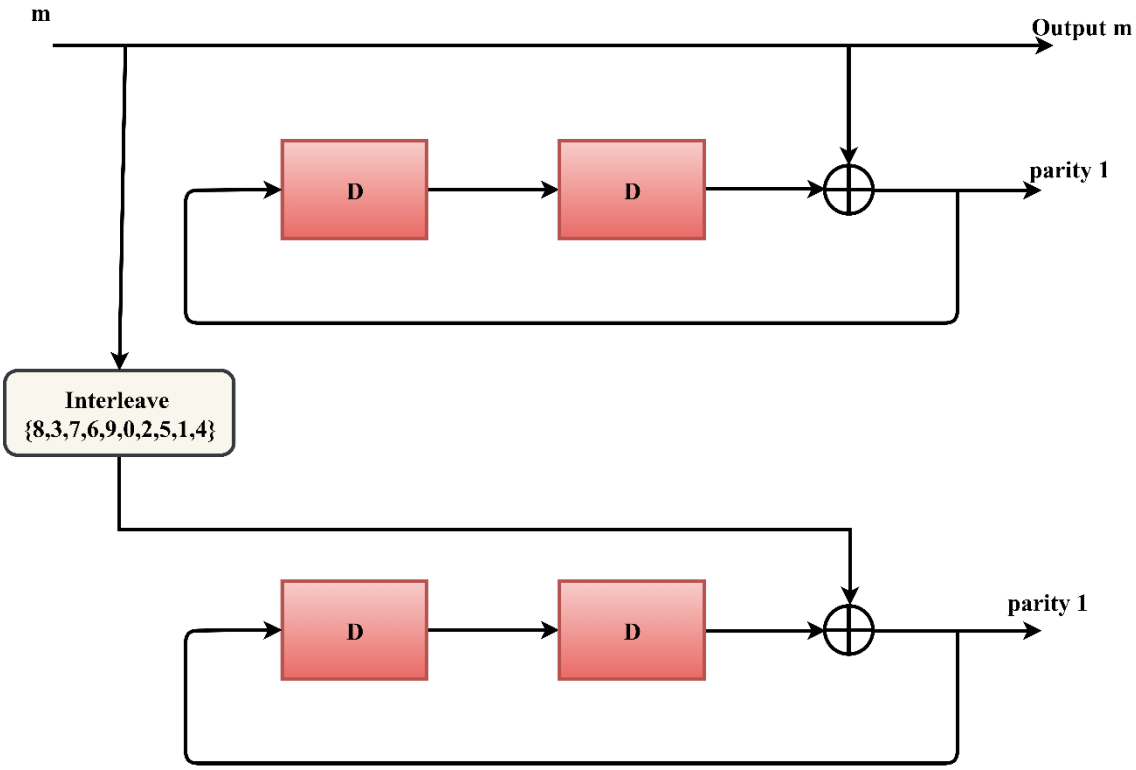


Figure (2.11). Example turbo encoder at rate 1/3.

2.7.2 Interleaving

A method known as interleaving often involves permuting the symbols in an input sequence. De-interleaving, the opposite of this technique, returns the received sequence to its original order. To lessen the effects of burst errors and impulsive noise in bursty channels, it is primarily used in forwarding error correction (FEC) coding [50].

In order to lessen the effects of bursts of errors that can be higher than those that the code can properly handle, interleaving is traditionally used to the codeword. The decoder is aware of the manner the channel interleaver uses to "scramble" the bits of

the codeword, thus any significant bursts of mistakes in the transmitted data stream are broken up on the decoding system by the d__Interleaver at the channel point in the receiver [51].

The main goal of an Interleaver in the turbo system is to improve (increase) the output codeword's weight. In essence, the interleaver does not change the weight of the input dataword; instead, it rearranges the bits to produce a codeword with a higher weight than one would otherwise have [52]. The details of a few Interleaver types are provided in [53,54].

There are some interleaver types and can be stated as follows:

1- **Row–Column Interleaver**

It considers as one of the simplest interleaver types in which input is written row-wise and read column-wise. This interleaver belongs to the group of "block or matrix" interleaves. Such that the data are written, as explained in Table (2.1) and read like in table (2.2).

Table 2.1 Row–Column Interleaver writing data process

X_0	X_1	X_2
X_3	X_4	X_5
X_6	X_7	X_8
X_9	X_{10}	X_{11}
X_{12}	X_{13}	X_{14}

Table 2.2 -Row–Column Interleaver reading data process

X_0	X_3	X_6	X_9	X_{12}	X_1	X_4	X_7	X_{10}	X_{13}	X_2	X_5	X_8	X_{11}	X_{14}

2- Pseudo-Random Interleaver

3- Circular-Shifting Interleaver (CSI)

2.7.3 Turbo Decoding

At the receiver end, the information is de-multiplexed to generate the received data vector. This signal data which usually have an amount of distortion when transitioning through a noisy channel. At the receiver, the data is decoding to obtain only estimates bit from the systematic bit and two groups of parity bits. The general structure of turbo decoder consists of a couple of decoders which connected by interleaver in a structure similar to that of the encoder, which works cooperatively in order to develop the estimation of the original bits as shown in Figure (2.12).

The decoding algorithm is an iterative decoding procedure ,so that every constituent decoder produces a soft decisions or estimates of the information bits. The estimates values are determined utilizing the channel information that received from the sampled amounts of the received sequence, besides the priori information that provides by another decoder in the past iteration. As shown in the figure (2.12), there are three inputs enter to each decoder, the first input is the systematically encoded output bits, while the second input is the parity bits that transmitted from the related encoder, and the third input is a sequence from the other decoder that gives the possible amounts of the bits concerned which named as a-priori information [55,56].

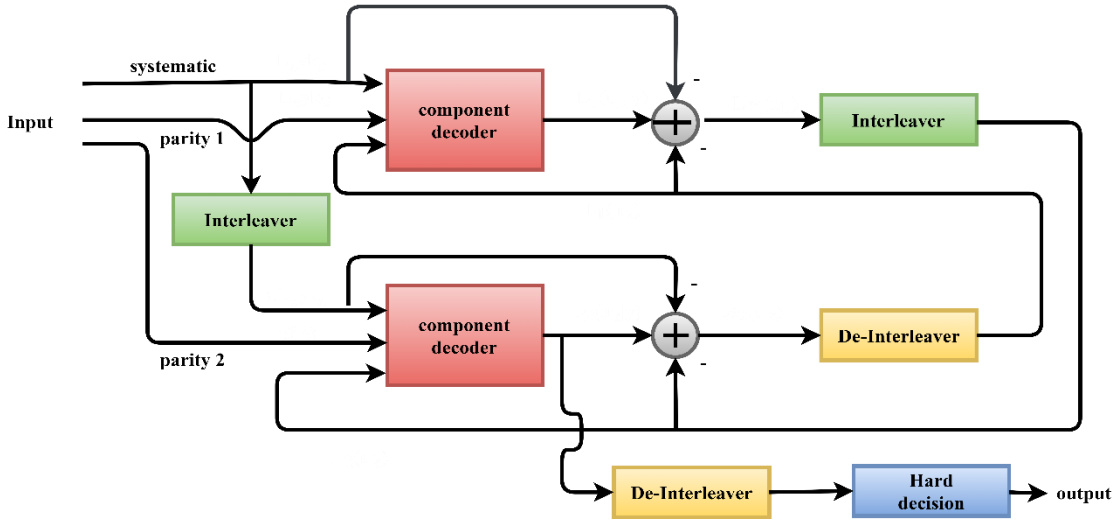


Figure (2.12). The general construction of turbo decoder

The decoding component generates what are referred to as soft outputs for the decoded bits using both the priori knowledge and the inputs from the channel. The magnitude of the designated LLRs (Log-Likelihood Ratios), whose name provides the sign of the bit and the probability of a correct decision, is commonly used to define the soft outputs [57]. The LLR of an information bit is calculated using the log of the ratio of the bit's two potential values and takings, which is denoted as L(u"k").

$$L(u_k) = ln\frac{p(u_k=+1)}{p(u_k=-1)} \tag{2.24}$$

If the $LLRs$ based on conditional probabilities, then the conditional $LLR\ L(u_k|y_k)$ Can be written as Equation (2.24).

$$L(u_k|y_k) = \text{In}\ (\frac{P(u_k=+1|y_k)}{p(u_k=-1|y_k)}) \tag{2.25}$$
$$= L(y_k|u_k) + L(u_k)$$

$$L(u_k|y_k) = L_{C.}y_k + L(u_k) \quad (2.26)$$

The channel dependability value, or Lc, is determined by.

$$L_c = \frac{E_b}{2\sigma^2}4a \quad (2.27)$$

Where E_b=energy/bit, a= the fading amplitude, σ^2=noise variance, (a=1 for non-fading AWGN channel).

2.8 Performance Evaluation

The primary purpose of the steganography systems is to hide the secret data inside the cover file (image or video or any other cover type) in a way cannot be recognized by the human visual system. So, to decide whether the effected of hiding data on video quality is in the acceptable range or not, there are various statistically tests that has been employed to make the decision. In this chapter several parameters will be discuss like (MSE) Mean Squared Error, (SSIM) Structural similarity index and Peak Signal to Noise Ratio (PSNR)

2.8.1 BER (Bit Error Rate)

It is the proportion of bits that are corrupted during transmission across a noisy channel, which causes interference and message bit distortion. As an illustration, the received bits are 00111100 and the broadcast bits are 11001100. Thus, four bits are impacted by transmission when comparing the number of bits sent and received. Therefore, in this example, the BER is 4/8*100 = 50%. Typically, the equation (2.31) [58] is used to calculate the BER of a binary image.

$$BER = \frac{B_{err}}{M*N*8} * 100\% \quad (2.28)$$

were

- B_{err} is the number of error bits in the image.

- M & N are the dimensions of the image and multiply by 8 because of each pixel represents by 8 binary bits.

2.8.2 MSE Mean Square Error

One statistical technique used to establish correspondence between stego image and original image is MSE. The similarity calculation Calculate the mean energy of the error signal by measuring it and subtracting it from the checked signal and the referred signal, respectively. Equation (2.29) can be used to represent the computation of (MSE) [59,60].

.

$$\text{MSE} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}[x(i,j)-x`(i,j)]}{M*N} \quad . \quad (2.29)$$

Where

- M &N symbol represent video resolution.
- x represent the original image.
- $x`$ represent a stego image.

2.8.3 PSNR Peak Signal to Noise Ratio

PSNR is defined as the ratio between the maximum power of a signal and the power of corrupting noise. PSNR is usually expressed as a decibel scale. The PSNR is commonly used as a measure of a quality reconstruction of an image. The signal, in this case, is original data, and the noise is the error introduced. The high value of PSNR indicates the high quality of the image; it can be calculated by equation (2.33)[61,62].

$$PSNR = 10log_{10}(P^2/MSE) \quad (2.30)$$

- P is the maximum intensity value and here it is 255.

2.8.4 SSIM Structural Similarity Index

Image processing is subject to a variety of distortions, which may result in deterioration in image accuracy before and after a steganography operation, The pixels that were changed after Steganography must be compared to the pixels before the change. The similarity assessment index bases on the computation of 3-terms, namely the structural term, luminance term and the contract term. The equation of SSIM can be seen in equation (2.31) [63,64].

$$SSIM = \frac{\left((2UxUy+T1)(2\sigma xy+T2)\right)}{(U2x+U2y+T1)(\sigma 2x+\sigma 2y+T2)} \quad (2.31)$$

.

Where U_x& U_y, represent the local mean, σ_x & σ_y, represent the standard deviations, σ_{xy} represent the cross-covariance for images x, y..

CHAPTER THREE
PROPOSED TEXT STEGANOGRAPHY ALGORITHMS

3.1 Introduction

In the previous chapter, many techniques were discussed, so that the general idea of each method was explained in terms of their work and its mathematical representation. In this chapter, all of these technologies will be used to generate a highly secret and robust hybrid system that is used to preserve the customer privacy. This system provides advanced options for the customer that gives him more privacy in disposing of his money and facilitates the process of receiving and delivery as well as avoiding the process of theft and forgery.

This hybrid method works to hide a text file (recipient information and amount released) and an image (picture of recipient) inside the image file in a way that does not affect the image resolution. The suggested advanced hybrid system in this chapter provides a solution for many issues like low embedding capacity, less imperceptibility, less robustness against attacks, and less security, which exist in many traditional steganographic algorithms. The implementation and the design of this steganography system are done by using MATLAB program.

There are numerous papers available today that advocate using the Internet to transmit various types of information using different methods (including e-mail, chat room, bulletin boards and other web sites). There is also a lot of conjecture that some groups may use data-hiding tactics to facilitate communication.

3.2 The Proposed text Steganography System

In the present day, the most famous text steganography algorithm is considered a traditional topic to attackers because of the development of the method and programs that used to break and analyze the text file. That is why there is a need to develop a new technology completely different from the previous methods in terms of coding the text file and location of the hidden information in the image.

Each steganography system consists of two central parts. The first partition is deal with hiding secret data inside the cover file with a high degree of security and robustness. While the second part is deal with recovering these confidential data by using the inverse processes which are used to embed them in the cover file. The general structure of the proposed system can be shown in figure (3.1).The embedding block consists of the text file, original image (or cover object) and the other cover image, and turbo code which is used as a random key to select the embedding position also it is used here in this research for the first time to encrypt the text file pixels.

The embedded /extracted way vary from one system to another according to the applications, complexity, and cost etc. To test the performance of the suggested image steganography algorithm, different types of attacks are applied on the stego-image to simulate passes through a noisy channel. So, there are many calculations must be taken into account, like MSE, PSNR, BER and SSIM.

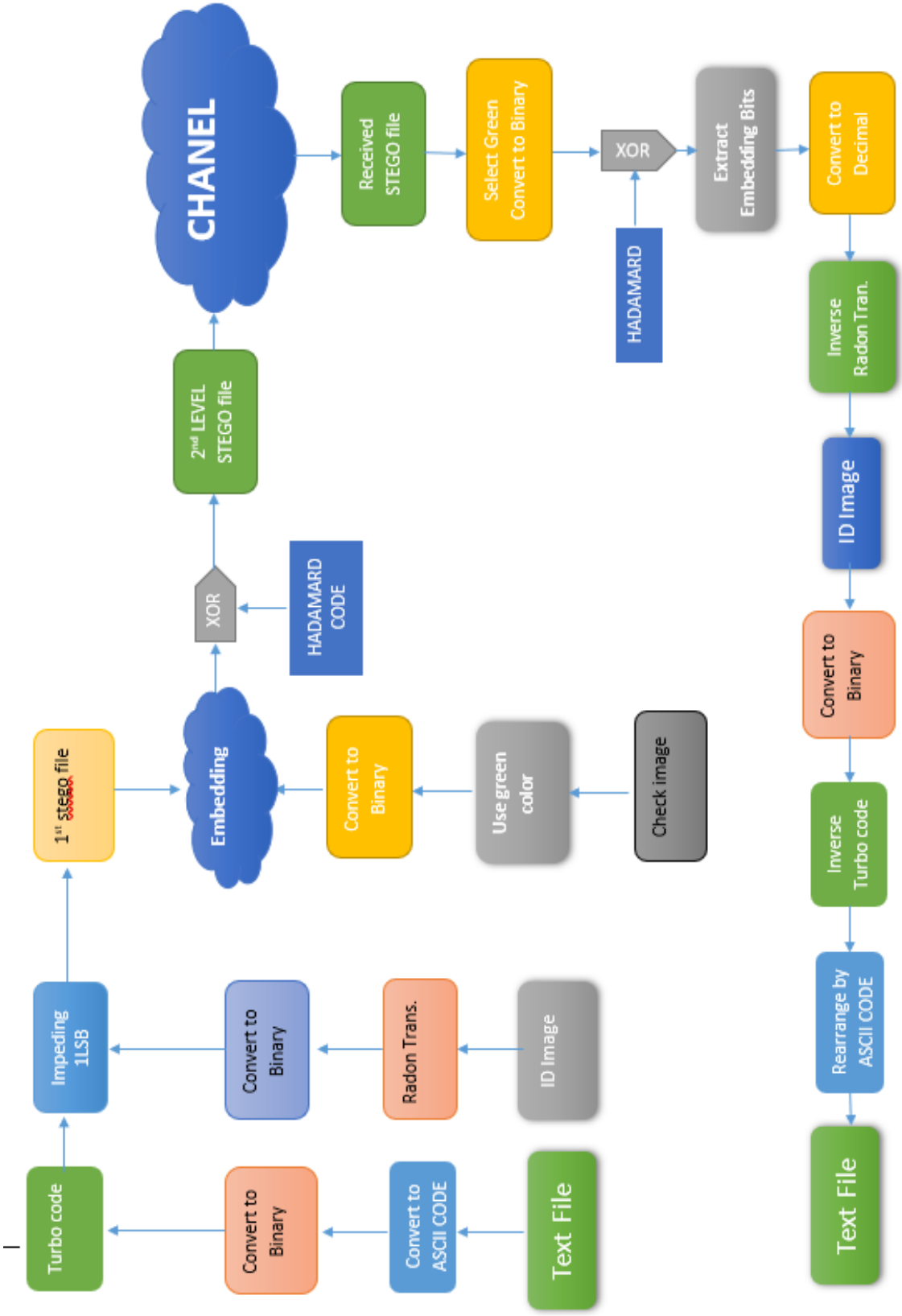


Figure (3.1): Proposed multi level Text Steganography System.

3.2. 1 Analyzing The Text

By all encryption methods, there remains a text for the data when it is intercepted by the enemy, doubting that it is an encrypted message and trying to decipher it by all encryption methods. What wanted here is that the message interceptor (the enemy) does not even suspect the existence of an encrypted message, because it will hide inside an image, so it does not even think about the existence of an encrypted text.

The system will detect the text to be hidden and determine the number of rows and columns for it so that the bytes of each character may be transferred to the inside of the LSB bit in the image. The text to be hidden is read and converted to ASCII Code, then to the binary system. A specified position in the image's left eighth bit will be used to store each character's byte.

3.2. 2 First Security Level (Turbo Code Encryption)

To increase the robustness and the security of the proposed system the system will have a strong error-correcting capability while keeping a manageable level of complexity and coding rate flexibility. Turbo code is used here to get a reliable system to encrypt the information data. After analyzing the text file and converting it to ASCII codes, each one of those codes is passed to the first secret level, which used the turbo code to encrypt it.

Each code is converted into binary block consist of eight binary bits. Then each block is encoded by using turbo code (with rate 1/3). In this case, the outcome of turbo encoding system to each code is 24 bits (8 bit is a code bit, 16 bit is a parity check bits). The parity bits are used to detect and correct the errors that may happen when the text is transferred through a noisy channel. besides that, it is essential role in the encryption domain. As explain in figure (3.2).

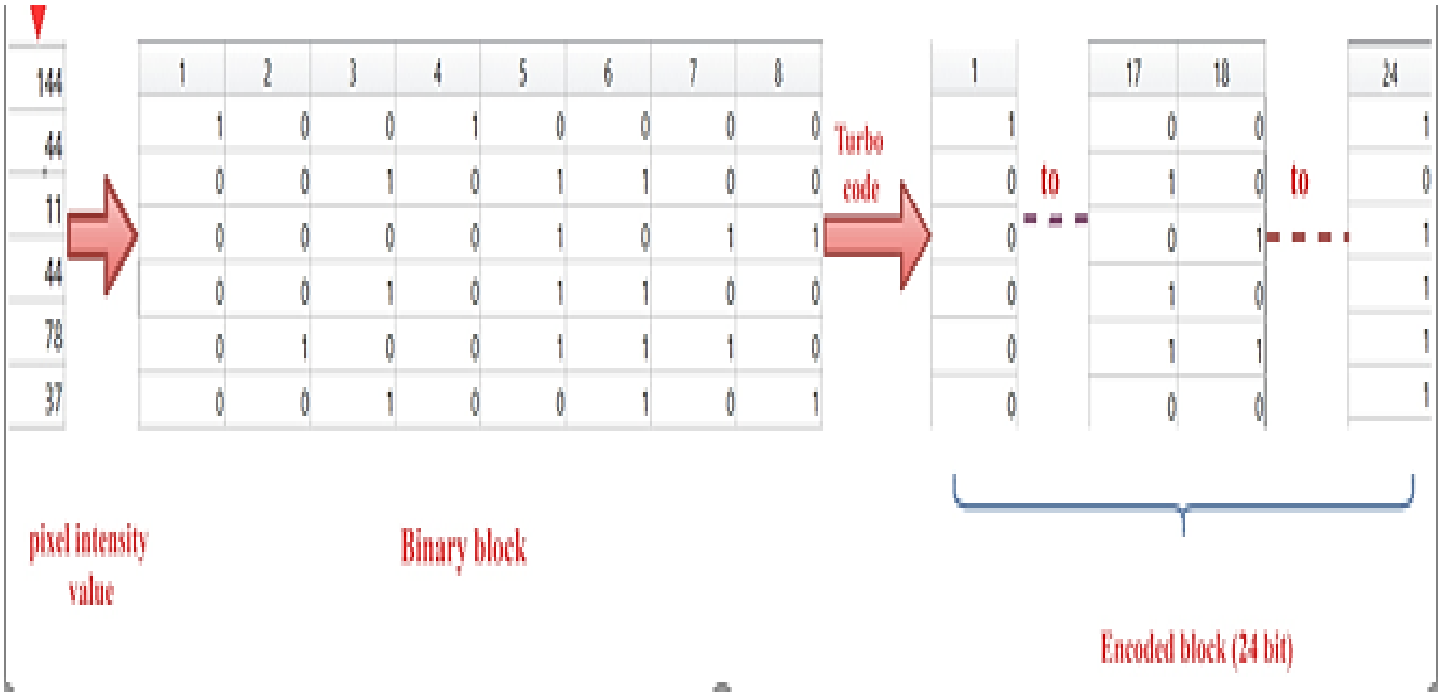


Figure (3.2). Explanation of using turbo code to encrypt the text pixels

3.2. 3 Analyzing The Cover image

This proposed system work to hide the text file (which described in section 3.3.2) inside the input cover image.

Also, this system is considered a flexible system because it can be dealing with any format type of the input image. As displayed in Figure (3.1), the image read in MATLAB as pixels Those pixels are used as a cover to hide the codes of text file in them.

3.2. 4 Second Secret Level by Using Radon Transform

Digital steganography has been widely used for ownership identification and copyright protection.

Here in this work, as shown in Figure (3.1) a new way is suggested to embed (hide) the pixels of the text file inside the image by using the Radon Transform

idea, so that it is utilized to spread the encryption bits of the text pixels inside the cover image in a way that is closest to a random distribution.

So, in this context, it is used to identify the locations of the pixels in the cover frame so that the location represents the positions of the frame pixels which is used to hide logo data bits.

The Radon transformations are applied to the image file once it has been read. The Radon transform is an angular projection of the intensity of an image file along a radial line. The values along the x'-axis, which is rotated degrees counterclockwise from the x-axis, make up the radial coordinates. The application of Radon transforms is briefly covered in chapter two.

3.3The Proposed image Steganography System (multi-level stegano)

Frequent transmission of encrypted messages will attract the attention of outsiders, crackers, and hackers, possibly leading to attempts to decrypt and divulge the original messages. Steganography is used in the digital age to conceal communications by enclosing a secret message inside another seemingly unimportant message. This study aims to develop a multi-level steganography system that may be used to cover data in a color photo with a high level of security. Due to the two levels of embedding that were used in this system's implementation and the high level of security that resulted, two levels of extraction were necessary in order to access the hidden data. Figure (3.1) depicts the multi-level proposed steganography procedure .

3.3.1 Analyzing the check image (main cover image)

The final step is to hide the last stegano-image inside the main cover image which is fulfills the theory of multi-level steganography. This cover image must

contain all the secret information of the check After impeding, it can be sent in any of social media without any change of its properties.

3.3.2 Third Secret Level by Using Hadamard code

The Hadamard matrix is a square array of positive and negative ones with orthogonal rows and columns. In this thesis, the Hadamard transformation is carried out using a rapid computer approach, comparable to the fast Fourier transform algorithm. Since the Hadamard transform just requires additions and subtraction of real numbers. Instead of sending the spatial representation of an image, the Hadamard transform can potentially tolerate channel failures and potentially lessen the noise effect.

3.3.3Embedding Process, (stego_process).

An image embedding is a lower-dimensional representation of the image. In other words, it is a dense vector representation of the image which can be used for many tasks such as classification.

Steganography is embedded by converting the data to the binary strings and distributing the encrypted data on this binary stream after that it will convert back to the decimal values.

As shown in Figure (3.1), the embedding work is to swap the LSB of the image pixel by the bit of the text code. The pixel value of the image is represented by a block of 8 binary bit. In this work, each text code pixel is represented by 24 bits as a result of encrypting it by the turbo code. In this case, each text pixel is hidden by 24 image pixels. The embedding position is controlled by a radon transform. Figure (3.3) is descripting how the embedding process work.

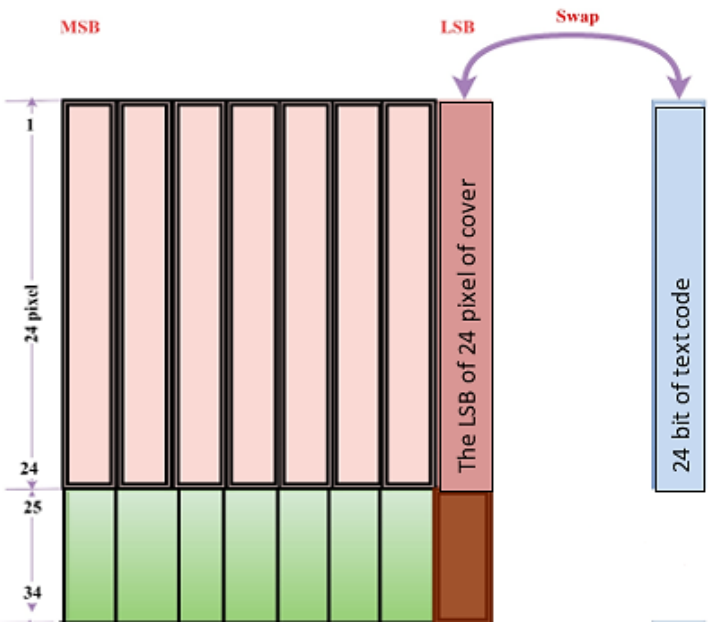


Figure (3.3): embedding processes to three encryption text pixels

So, multi-level steganography in this research can be described in the following steps:

1_ read the ID image (N*N).

2_ read the text file and convert it to ASCII code.

3_apply turbo code to the text.

4_apply radon transform to the ID image.

5_ embedding the text code inside the image code to obtain the first level steganography.

6_ read the main image (check image) in MATLAB.

7_apply Hadamard code to the main image (XOR).

8_embedding the code of the first image inside the coded main image.

9_apply inverse Hadamard code to the main image to obtain the multi-level steganography image and return the main image to its first look.

3.4 Extraction Process.

The extraction process is illustrated in Figure (3.5) the extraction process can be described in the following steps:

a) Read the stego. image of size N*N and extract each color of the image alone.

b) Apply the Hadamard code on each color of the steganography image.

c) apply the inverse LSB to extract imbedded data

d) collect the imbedded data and applying inverse radon transform to extract the ID image.

e) apply the inverse turbo code to extract the ASCII code of the text file

e) decoded the ASCII code to recover the text.

3.4.1 Inverse Turbo Code

Inverse bit plane decoding order for Turbo Code is suggested. Investigations have revealed that while the influence of LSBs on MSBs tends to be greater, the influence of LSBs on LSBs, which can be considered noise, is relatively minimal.

Here, fewer turbo decoding loops are necessary since the decoder can request several puncturing levels for LSBs in a single step. As a result, by broadcasting the LSBs first, a decoding speedup of a factor 2 can be achieved while maintaining or increasing the coding efficiency.

The extraction system used the inverse turbo code (turbo decoding) to decrypt of the encoded image pixel data. Also, this system detects and correct the error in image bits that may happen when passing through a noise channel. After that, the output of the turbo decoding system is reordering as a block of 8 bits so that each block when converting to decimal represent one image pixel.

3.4.2 Inverse Radon Transform (stego_image)

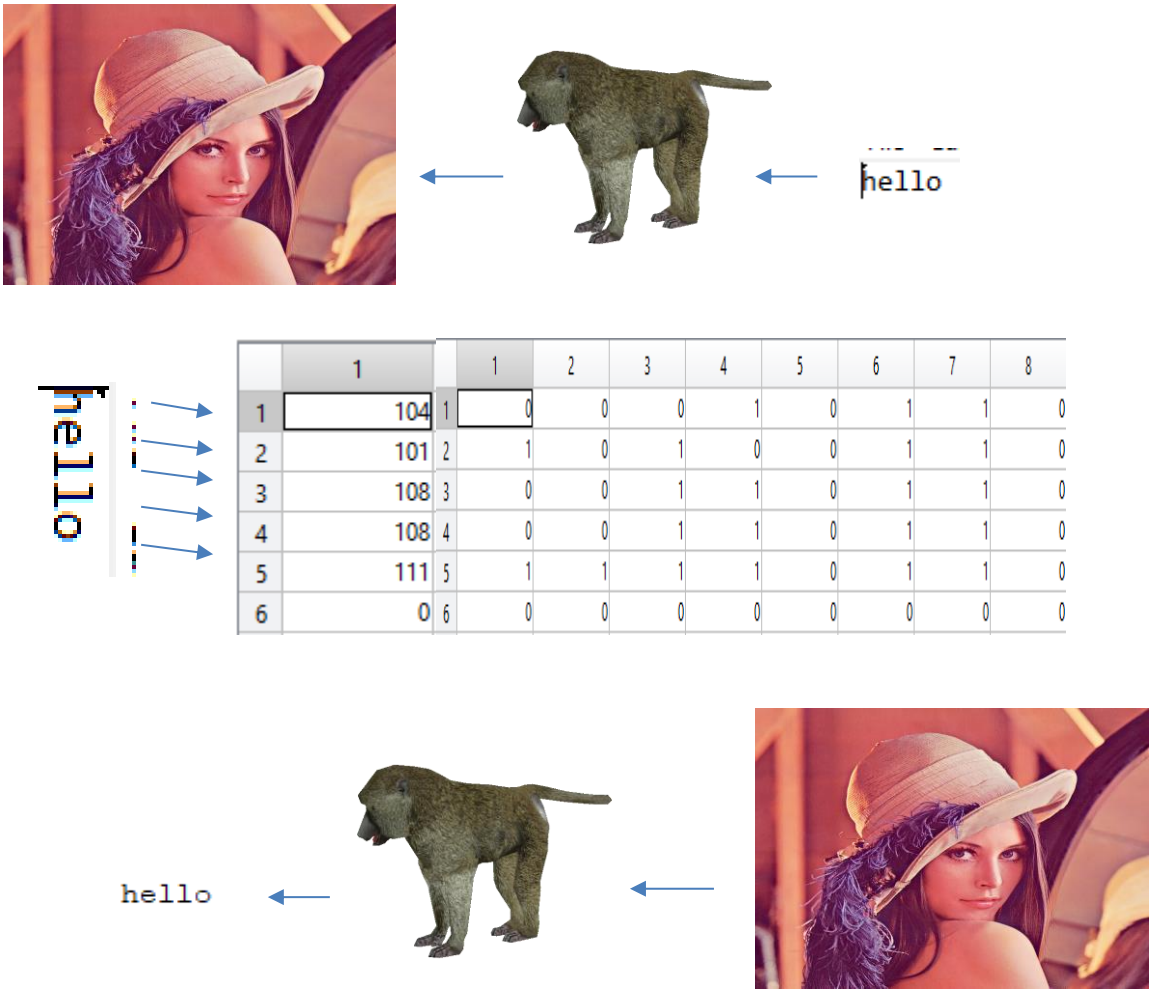
After decrypted the data, is extracted by converting the data from binary strings to the decimal values and the inverse Radon transforms is applied on it to extract the image. The inverse Radon transform consist of many steps. These

steps for applying inverse Radon transforms are explained briefly in the chapter two.

3.5 The practical part:

3.5.1 Test example:

The figure (3.7) shows a simple example for multi_level text steganography which clearly shows the process of converting text into numbers and the process of extracting them with the same numbers without ant change :



	1
1	104
2	101
3	108
4	108
5	111
6	0

	1	2	3	4	5	6	7	8
1	0	0	0	1	0	1	1	0
2	1	0	1	0	0	1	1	0
3	0	0	1	1	0	1	1	0
4	0	0	1	1	0	1	1	0
5	1	1	1	1	0	1	1	0
6	0	0	0	0	0	0	0	0

Figure (3.4): Multi level stegano test example

3.5.2 Embedding Process

The figure (3.5) shows a detailed explanation in numbers for the multilevel steganography embedding process of data within the check image.

As first the text file will be read, then converted to ASCII code then to binary as seen in figure (3.5: a, b)

rafal fadhil jabbr, 45643000, just fourty five milion and six handreds and thirty four iraqi dinar

140x1 double

	1
1	97
2	104
3	109
4	101
5	100
6	32
7	97
8	98
9	100
10	108
11	107
12	97
13	114
14	101
15	101
16	109
17	32
18	97
19	108
20	122

(a) : The ASCII code of text

	1	2	3	4	5	6	7	8
1	0	1	0	0	1	1	1	0
2	1	0	0	0	0	1	1	0
3	0	1	1	0	0	1	1	0
4	1	0	0	0	0	1	1	0
5	0	0	1	1	0	1	1	0
6	0	0	0	0	0	1	0	0
7	0	1	1	0	0	1	1	0
8	1	0	0	0	0	1	1	0
9	0	0	1	0	0	1	1	0
10	0	0	0	1	0	1	1	0
11	1	0	0	1	0	1	1	0
12	0	0	1	1	0	1	1	0
13	0	0	0	0	0	1	0	0
14	0	1	0	1	0	1	1	0

(b): The binary numbers of text ASCII code

Figure (3.5 c) shows the applying of turbo code to the resulted binary of text file.

	1	2	3	4	5	6	7	8
1	0	1	0	0	1	1	1	0
2	1	0	0	0	0	1	1	0
3	0	1	1	0	0	1	1	0
4	1	0	0	0	0	1	1	0
5	0	0	1	1	0	1	1	0
6	0	0	0	0	0	1	0	0
7	0	1	1	0	0	1	1	0
8	1	0	0	0	0	1	1	0
9	0	0	1	0	0	1	1	0
10	0	0	0	1	0	1	1	0
11	1	0	0	1	0	1	1	0
12	0	0	1	1	0	1	1	0
13	0	0	0	0	0	1	0	0
14	0	1	0	1	0	1	1	0
15	1	0	0	0	0	1	1	0
16	0	1	0	0	0	1	1	0
17	0	1	0	0	0	1	1	0
18	0	1	0	0	1	1	1	0
19	0	0	1	1	0	1	0	0
20	0	0	0	0	0	1	0	0
21	0	0	1	0	1	1	0	0
22	1	0	1	0	1	1	0	0

(c)

The second step is reading the ID image then converted it to 2D-image .After that applying the radon transform to it then converted the result image to binary as seen in figure (3.5:d,e,f)

(d)

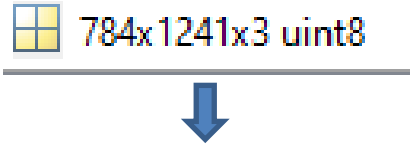
	1
1	8402
2	6311
3	5301
4	5625
5	6776
6	6521
7	5832
8	6182
9	6814
10	6552
11	5880
12	6238
13	6162
14	4638
15	2475
16	5315
17	5324
18	3875
19	3552
20	4041
21	2550
22	3149

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	0	1	0	0	1	0	1	1	0	0	0	0	0	1	0
2	1	1	1	0	0	1	0	1	0	0	0	1	1	0	0
3	1	0	1	0	1	1	0	1	0	0	1	0	1	0	0
4	1	0	0	1	1	1	1	1	1	0	1	0	1	0	0
5	0	0	0	1	1	1	1	0	0	1	0	1	1	0	0
6	1	0	0	1	1	1	1	0	1	0	0	1	1	0	0
7	0	0	0	1	0	0	1	1	0	1	1	0	1	0	0
8	0	1	1	0	0	1	0	0	0	0	0	1	1	0	0
9	0	1	1	1	1	0	0	1	0	1	0	1	1	0	0
10	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0
11	0	0	0	1	1	1	1	1	0	1	1	0	1	0	0
12	0	1	1	1	1	0	1	0	0	0	0	1	1	0	0
13	0	1	0	0	1	0	0	0	0	0	0	1	1	0	0
14	0	1	1	1	1	0	0	0	0	1	0	0	1	0	0
15	1	1	0	1	0	1	0	1	1	0	0	1	0	0	0
16	1	1	0	0	0	0	1	1	0	0	1	0	1	0	0
17	0	0	1	1	0	0	1	1	0	0	1	0	1	0	0
18	1	1	0	0	0	1	0	0	1	1	1	1	0	0	0
19	0	0	0	0	0	1	1	1	1	0	1	1	0	0	0
20	1	0	0	1	0	0	1	1	1	1	1	1	0	0	0
21	0	1	1	0	1	1	1	1	1	0	0	1	0	0	0
22	1	0	1	1	0	0	1	0	0	0	1	1	0	0	1

(e,f): The ASCII code of the image and the binary od it

The final step is considered by the check image, so that it will be read by MATLAB program, then converted to a vector then to binary NO. so that each pixel represented by 8bit. In the same step the resulted binary matrix will XOR ed with the Hadamard code (8bit) to prepares the image for embedding process. This step is show in figure (3.6: g, h).

(g)



	1	2	3	4	5	6	7	8
1	1	0	0	0	1	1	1	1
2	1	0	0	0	1	1	1	1
3	1	0	0	0	1	1	1	1
4	1	0	0	0	1	1	1	1
5	1	0	0	0	1	1	1	1
6	1	0	0	0	1	1	1	1
7	1	0	0	0	1	1	1	1
8	1	0	0	0	1	1	1	1
9	1	0	0	0	1	1	1	1
10	1	0	0	0	1	1	1	1
11	1	0	0	0	1	1	1	1
12	1	0	0	0	1	1	1	1
13	1	0	0	0	1	1	1	1
14	1	0	0	0	1	1	1	1
15	1	0	0	0	1	1	1	1
16	1	0	0	0	1	1	1	1
17	1	0	0	0	1	1	1	1
18	1	0	0	0	1	1	1	1
19	1	0	0	0	1	1	1	1
20	1	0	0	0	1	1	1	1
21	1	0	0	0	1	1	1	1
22	1	0	0	0	1	1	1	1

(h): Convert check image to binary

After that the embedding process is done by hiding the radon-ID-image encoded inside with turbo code for text inside the check-coded image, Then XOR the results with Hadamard code and return the image to 2D-decimal values as seen in figure (3.5: I, j, k).

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	0	1	0	0	1	0	1	1	0	0	0	0	0	1	0
2	1	1	1	0	0	1	0	1	0	0	0	1	1	0	0
3	0	0	1	0	1	1	0	1	0	0	1	0	1	0	0
4	0	0	0	1	1	1	1	1	1	0	1	0	1	0	0
5	1	0	0	1	1	1	1	0	0	1	0	1	1	0	0
6	1	0	0	1	1	1	1	0	1	0	0	1	1	0	0
7	1	0	0	1	0	0	1	1	0	1	1	0	1	0	0
8	0	1	1	0	0	1	0	0	0	0	0	1	1	0	0
9	1	1	1	1	1	0	0	1	0	1	0	1	1	0	0
10	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0
11	0	0	0	1	1	1	1	1	0	1	1	0	1	0	0
12	0	1	1	1	1	0	1	0	0	0	0	1	1	0	0
13	0	1	0	0	1	0	0	0	0	0	0	1	1	0	0
14	1	1	1	1	1	0	0	0	0	1	0	0	1	0	0
15	1	1	0	1	0	1	0	1	1	0	0	1	0	0	0
16	0	1	0	0	0	0	1	1	0	0	1	0	1	0	0
17	0	0	1	1	0	0	1	1	0	0	1	0	1	0	0
18	1	1	0	0	0	1	0	0	1	1	1	1	0	0	0
19	1	0	0	0	0	1	1	1	1	0	1	1	0	0	0
20	0	0	0	1	0	0	1	1	1	1	1	1	0	0	0
21	0	1	1	0	1	1	1	1	1	0	0	1	0	0	0
22	1	0	1	1	0	0	1	0	0	0	1	1	0	0	1

(i): The binary code of check image after embedding

288800x1 double

	1
1	252
2	254
3	254
4	254
5	254
6	252
7	252
8	254
9	252
10	254
11	254
12	254
13	254
14	254
15	254
16	254
17	254
18	254
19	254
20	254
21	252
22	254

(j): Converted to ASCII code

(k)

Figure (3.5): The proposed multi-level steganography process

3.5.3 Extracting Process

The figure (3.6) shows a detailed explanation in numbers for the multilevel steganography extracting process of data from the check image.

At first the 2nd level stego-image (check image) read in MATLAB program and converted to binary to extract the code of ID image and Text information, after converting to binary start to collect the hiding information code as seen in (E) ,from the collected code extract the Text and ID image as seen in (F) and converted it to 2D to show the final result.

288800x1 double

	1
1	252
2	254
3	254
4	254
5	254
6	252
7	252
8	254
9	252
10	254
11	254
12	254
13	254
14	254
15	254
16	254
17	254
18	254
19	254
20	254
21	252
22	254

(B): ASCII ode of multi level stego_image

288800x8 logical

	1	2	3	4	5	6	7	8
1	0	0	1	1	1	1	1	1
2	0	0	1	1	1	1	1	1
3	0	1	1	1	1	1	1	1
4	0	1	1	1	1	1	1	1
5	0	0	1	1	1	1	1	1
6	0	1	1	1	1	1	1	1
7	0	0	1	1	1	1	1	1
8	0	0	1	1	1	1	1	1
9	0	1	1	1	1	1	1	1
10	0	1	1	1	1	1	1	1
11	0	1	1	1	1	1	1	1
12	0	1	1	1	1	1	1	1
13	0	1	1	1	1	1	1	1
14	0	0	1	1	1	1	1	1
15	0	1	1	1	1	1	1	1
16	0	1	1	1	1	1	1	1
17	0	0	1	1	1	1	1	1
18	0	0	1	1	1	1	1	1
19	0	1	1	1	1	1	1	1
20	0	1	1	1	1	1	1	1

(c): Binary code of stego_ image

57360x15 logical

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	1	0	0	1	0	1	1	0	0	0	0	0	1	0
2	0	1	1	0	0	1	0	1	0	0	0	1	1	0	0
3	0	0	1	0	1	1	0	1	0	0	1	0	1	0	0
4	0	0	0	1	1	1	1	1	1	0	1	0	1	0	0
5	0	0	0	1	1	1	1	0	0	1	0	1	1	0	0
6	1	0	0	1	1	1	1	0	1	0	0	1	1	0	0
7	1	0	0	1	0	0	1	1	0	1	1	0	1	0	0
8	0	1	1	0	0	1	0	0	0	0	0	1	1	0	0
9	0	1	1	1	1	0	0	1	0	1	0	1	1	0	0
10	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0
11	0	0	0	1	1	1	1	1	0	1	1	0	1	0	0
12	1	1	1	1	1	0	1	0	0	0	0	1	1	0	0
13	0	1	0	0	1	0	0	0	0	0	0	1	1	0	0
14	1	1	1	1	1	0	0	0	0	1	0	0	1	0	0
15	1	1	0	1	0	1	0	1	1	0	0	1	0	0	0
16	0	1	0	0	0	0	1	1	0	0	1	0	1	0	0
17	1	0	1	1	0	0	1	1	0	0	1	0	1	0	0
18	0	1	0	0	0	1	0	0	1	1	1	1	0	0	0
19	1	0	0	0	0	1	1	1	1	0	1	1	0	0	0
20	1	0	0	1	0	0	1	1	1	1	1	1	0	0	0

(E): extracted code of ID image

140x1 double

	1
1	97
2	104
3	109
4	101
5	100
6	32
7	97
8	98
9	100
10	108
11	107
12	97
13	114
14	101
15	101
16	109
17	32
18	97
19	108
20	122

(F)

57360x1 double

	1
1	8403
2	6310
3	5300
4	5624
5	6776
6	6521
7	5833
8	6182
9	6814
10	6552
11	5880
12	6239
13	6162
14	4639
15	2475
16	5314
17	5325
18	3874
19	3553
20	4041

(F):The ASCII code of extracted TEXT and ID image

```
ans =

rafal fadhil jabbr, 45643000, just fourty five milion and six handreds and thirty four iraqi dinar
```

(G): Extracted Text and ID image

Figure (3.6) : (A,B,C,D,E,F,G) multilevel extracting process

CHAPTER FOUR

SIMULATION RESULTS AND DISCUSSION

The simulation and implementation of the suggested system, together with a discussion of its key components, are presented in this chapter. Here, the multidisciplinary elements of cryptography and steganography are combined. As shown and explained in the chapter three, the Turbo code was used to encrypt the text pixels, and the encoded pixels were then spread throughout the cover image in accordance with the Radon Transform and LSB.

This chapter also demonstrates the user interface design and the effectiveness of the system in preserving quality of the image after embedding of data in an appropriate value. This is done by using performances such as PSNR, MSE, BER, and SSIM between identical pixels in the original image and the final product image. In order to demonstrate the system's effectiveness, the system will also be tested when applied various image noises like gaussian, salt and paper … etc. to the stego_image, These tests will be conducted on image files of various resolutions. The system was put into use with the help of Matlab 2016 program.

Text-Steganography Desktop APP

By using Matlab App Designer, the enabled creation of a professional apps without needing to a professional software developer is implemented. This app can be given

to other users without needing for installing any extra software (Matlab or any program). Figure (4.1) shows the master-Steganography desktop app.

Figure (4.1). master-Steganography desktop app

Figure (4.2) displays the home screen when running the App. Where the home page displays the different app processes, like embedding , extracting, help, etc.

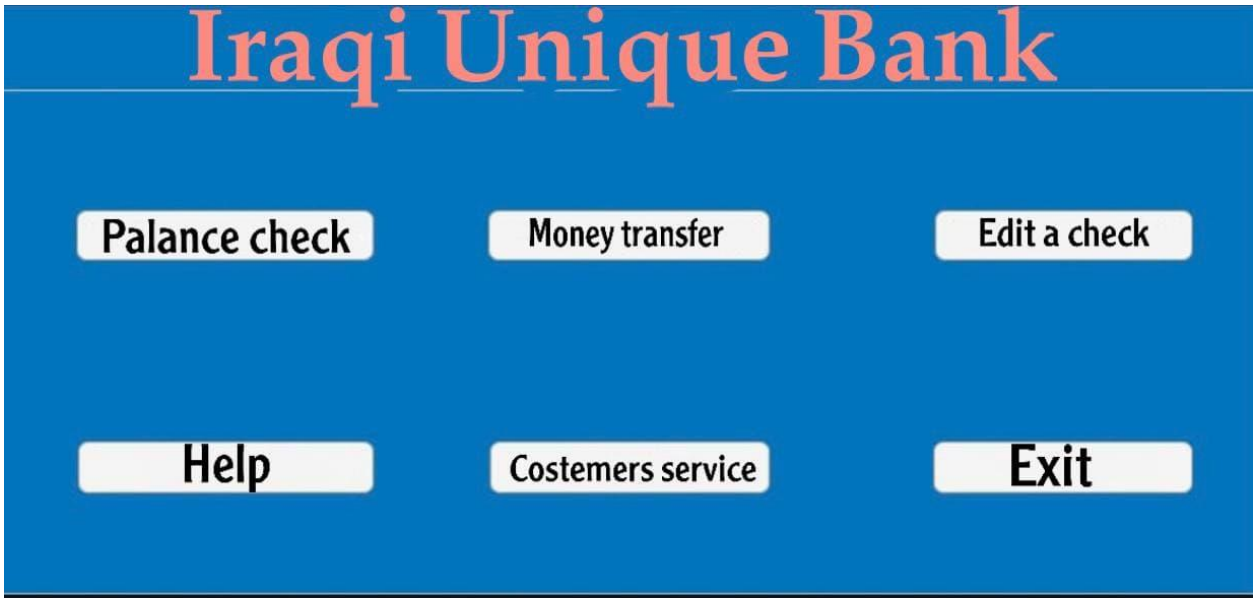


Figure (4.2). App home screen

Figure (4.3,4.4) displays the embedding and extracting pages respectively, which the process of embedding in and extraction the ID image and the text are done.

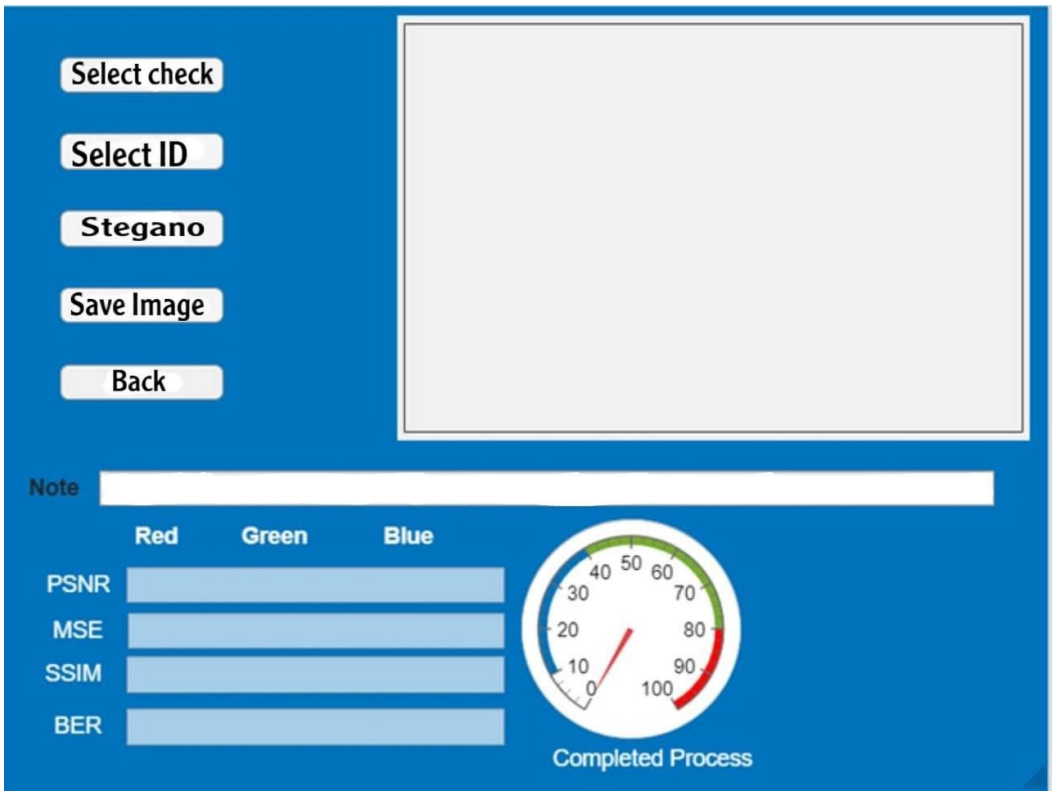


Figure (4.3). Embedding Page

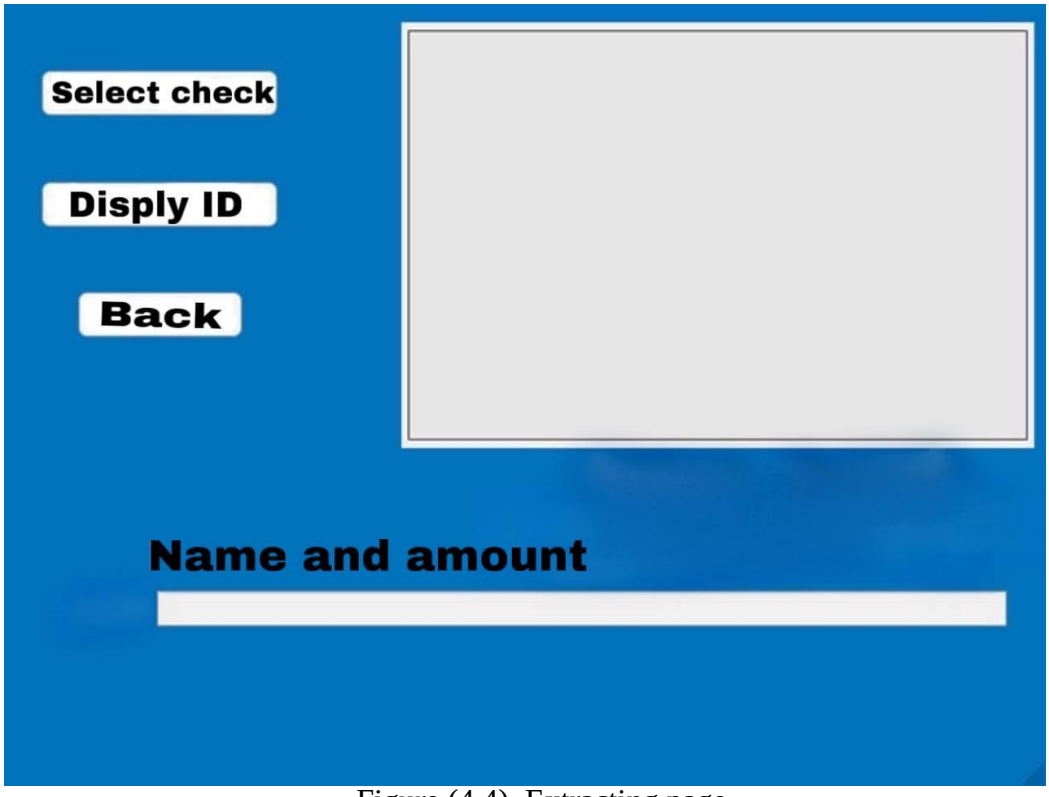


Figure (4.4). Extracting page

❖ The tests in this chapter will focus on three fundamental parts that shows the efficiency and performance of the proposed system.

1) Image quality after Steganography.
2) Quality of extracted ID image and text.
3) Effectiveness of the secret-system to maintain the hidden text under the effect of different noise levels.

4.1. ID & TEXT Quality After Steganography:

In this section a comparison between text and ID before and after data hide will be performed.

4.2.1 TEXT without Turbo Code Usage:

Figure (4.5) show the results after extracting the text without using the turbo code before and after external noises was shed on the image of the check.

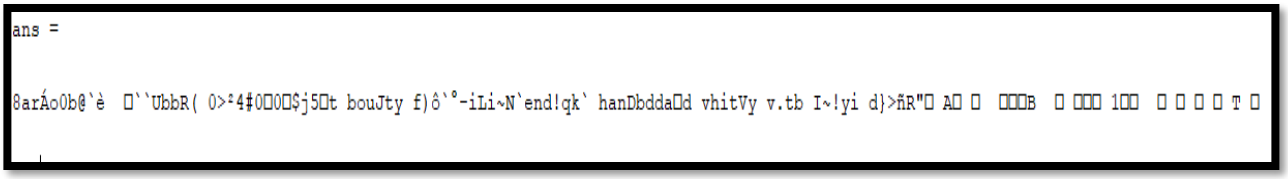
It is clear from the results that all the text bits will not be able to distinguish without using turbo code and this is an indication of the importance and strength of the turbo code in preserving the information.

```
ans =

rafal fadhil jabbr, 45643000, just fourty five milion and six handreds and thirty four iraqi dinar
```

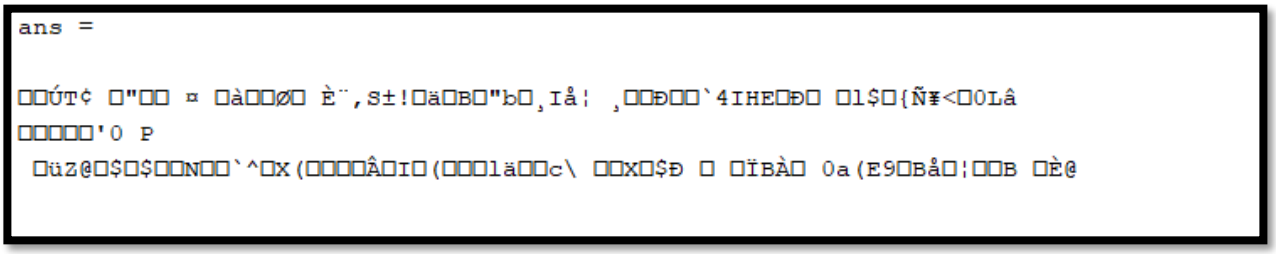
(A)

```
ans =

rafal fadhil jabbr, 45643000, just fourty five milion afd shx handreds and`thirty four`iraqi dinar
```

(B)



(C)



(D)

Figure (4.5): stego_image extraction … a: the extract text without noise ... (b): the extract text with salt and paper noise… (c): the extract text with Gaussian noise noise … (d): the extract text with speckle noise

4.2.2 TEXT with the use of Turbo Code:

When using turbo code, notice that the entire text appears without any damage in the bits, and this shows the power that the turbo code gives in preserving information from external influences.

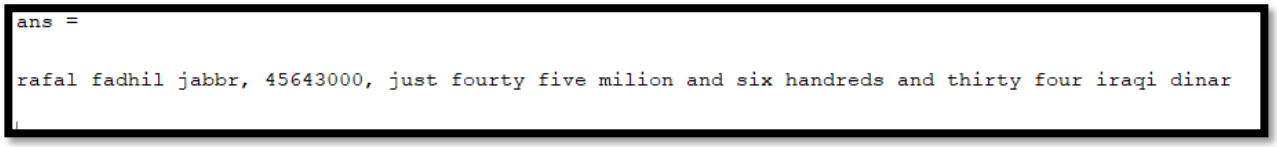


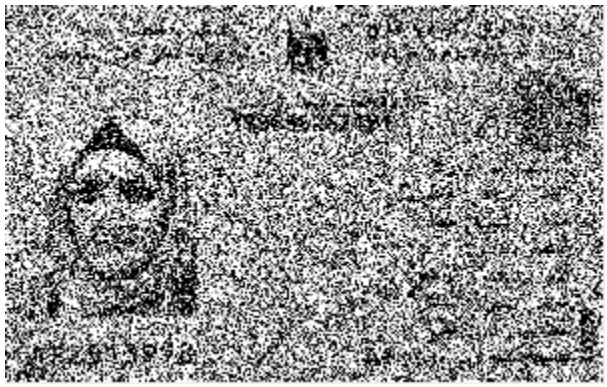
Figure (4.6) extracted text with turbo code

As seen from the figures (4.5,4.6)) that the use of the turbo system to encrypt the Text file has another benefit, it works to increase the similarity (SSIM) between the

original hide text with the extracted text by reducing and correct the error bits that happen in text after applied different noises on stego-Image.

4.2.3 ID without use of Radon transform:

For ID image in the figure (4.7) below, note that the identity image is greatly affected when external disturbances were shed, the ID image cannot be extracted with the same accuracy as it was included, even without the effect of noise when radon is not used, so Radon transform has the great impact in maintaining the internal structure of the ID.



(A.)

(B.)

(C.)

(D.)

Figure (4.7): Test of extract ID image without use of Radon Transform (A.): without any attack. (B.): with salt and paper noise. (C.): with gaussian noise. (D.): with speckle noise.

4.2.4 ID with use of radon transform:

With use of radon transform code, it be notice that the ID image it has almost no effect on shedding noise.

Fig (4.8): ID with use of radon transform

As displayed in figures (4.6, 4.8) the system is efficiently extracting the full quality of embed ID and text with and without existing of noise and working to enhance the quality of extracted hidden data, because the using of turbo code and radon transform besides its general work in improving the system security.

4.3 Study the image of the check after steganography:

4.3.1 Histograms for Proposed Method

Figure (4.9) displays a symbol of a histogram for check image . The figure (4.9) displays the amount of image pixels at each intensity value Figure (4.9-C) displays the histogram of the original image while (4.9-D) shows the histogram of the identical image after hiding data in it. Figure (4.9-E) displays the identically between those two images and the amount of change in pixel. In figure (4.9-E) the brown color shows the identical in amount of pixel between original and stego image while the red and cyan color explains the amount of difference between the two image at each intensity value. From all that it can say that the amount of difference in quality is tiny and can be neglected and HVS cannot recognize that difference.


Iraqi Unique Bank
Customer privacy is our motto
Mr. Osama Qasim Al-Thahab
Signiture

(a)


Iraqi Unique Bank
Customer privacy is our motto
Mr. Osama Qasim Al-Thahab
Signiture

(b)

(C)

Figure (4.9). Histogram of the embedding system . **A**- original Image, **B**- Stego-Image, C- difference between of Stego and original Image at each intensity value

4.3.2 Visual Quality for Check After Noise

The quality of the outcomes image that have been resulted from our suggestion system are very similar to the quality of the original digital image pixels before the embedding process. In generic, the PSNRs value is between (62.62-71.58) dB.

From the result, it can be noted that the value of MSE is very tiny (0.0035-0.039), which is smaller than all the previous steganography systems mentioned early,
In addition to the average SSIM for the Stego Image. It can note that the similarity value range is between (99.75-99.88) % with an amount of differencing range between (0.12-0.25)%. This tiny difference cannot be noted by natural human eyes.

Table 4.1 display the effectiveness of the proposed system to deal with the different resolutions of check and ID image. The tests in that table are applying on the various quality of check image after embedding different size IDs in it. As noted in that Table the similarity (SSIM) is ranging between (99.8-99.99)% and the Visual Quality in db is ranged (69.8-88.6). Also it can be concluded that the proposed system has a tiny effected of Image resolution (can be neglected). In addition of a high capacity for hiding high-resolution ID image.

Table 4.1 .The effectiveness of the proposed system with different ID and Check size.

	CHECK Resolution	ID Resolution	Average SSIM	Average MSE	Average PSNR
	360*640	360*640	99.979	0.0038	70.323
	360*640	480*480	99.978	0.0036	70.32
	480*854	512*512	99.97	0.00367	71.3
	480*854	*854480	99.967	0.00365	70.3
	720*1280	720*1280	99.96	0.0037	70.5
	720*1280	512*512	99.98	0.0035	71.3
	720*1280	400*400	99.99	0.0035	71.85

Figure (4.10) shows the comparison between cases if embedding is performed in the least (one, two, three, five, six or seven) significant bits.

1LSB

2LSB

3LSB

4LSB

5LSB

6LSB

Figure (4.10) : The ability of human visual system to recognize the change in stego_image if more than LSB used

Criterion		Average SSIM	Average MSE	Average PSNR
	1LSB	99.99	0.0035	84.87
	2LSB	99.99	0.0037	84.232
	3LSB	99.8	0.082	78.421
	4LSB	99.78	5.82	67.932
	5LSB	88.96	21.55	59.834
	6LSB	53.4	67.879	56.665
	7LSB	42.37	131.98	44.321

Table (4.2). Summarize of the effects of using more than 1 LSB in result image quality

Table (4.2) shows the results of PSNR ,MSE ,BER amd SSIM for check image when the embedding process states for 1LSB to 7LSB

The ability of the human visual system (HVS) to recognize the difference between the original and Stego image in each LSB case can be shown in Figure (4.10). It can be noted that the HVS can recognize the difference in the image if embedding is performed in the cases (4,5,6,7) LSB. Our system uses 1 LSB to maintain the quality of Stego-Image.

4.4 Calculations With add of Noise

4.4.1 Salt and Pepper noise (Impulse Noise)

Table (4.3). the effect of salt and paper noise on the check image.

Parameters	No attack	Salt &Paper noise
PSNR	84.87	71.6502
SNR	43.7290863538762	9.5004
BER	0.0562	0.00048
RMS	0.5374	0.1972
MSE	0.2888	0.0389
SSIM	0.999	0.958

This type of noise generates sharp and sudden disturbances in stego-Image. Table 4.3 discusses the performance of the proposed system after adding the Salt and Pepper noise on the stego-Image file.

The testing in that Table is calculating for Stego-Image . The tests are taking under noise density (0.001).

2_Gaussian noise

Table (4.4). the effect of Gaussian noise on the check image.

Parameters	No attack	Gaussian noise
PSNR	84.87	83.6976
SNR	43.7290863538762	43.7027
'BER'	0.0562	0.0023
RMS	0.5374	0.059
'MSE'	0.2888	0.0035
SSIM	0.999	0.9965

after applying Gaussian noise with variance (0.001), and zero mean. That Table shows the efficiency of the proposed system to save the hidden data user with Gaussian noise .

3_Spekle Noise:

Table (4.5). the effect of spekle noise on the check image.

Parameters	No attack	Spekle noise
PSNR	84.87	70.95
SNR	43.7290863538762	30.079
'BER'	0.0562	0.00044
RMS	0.5374	0.213
'MSE'	0.2888	0.00498
SSIM	0.999	0.9972

The tables (4.3,4.4,4.5) proves that proposed system has a high efficiency to protect the embedded information with high-reliability to extract data as compared with the traditional techniques that used LSB technique only. Also, the proposed system (by turbo system) is worked to estimate a correct value of bits which has been changed by noisy channel. Where the suggested system gives a huge enhancement in SSIM and BER when retrieving the hidden data besides a high level of security due to use turbo code and radon transform.

As noted from the above calculations the system is efficiently extracting the full quality of embed ID and text with and without existing of noise and working to enhance the quality of extracted hidden data, because the using of turbo code and radon transform besides its general work in improving the system security .

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

In this section, a measure of the efficiency of the proposed system to extract the embedded text when the Stego-check is transferred through different internet platforms are tested. Table (4.7) displays some sample of the Popular internet services which common (social media) peoples used it to share and transfer data like Facebook, YouTube, WhatsApp, Viber and Telegram. Table (4.7) shows the efficiency of extracting text after transition check in that internet service platform

Table (4.7). Reliability of the proposed system to extract an embedded text from the Stego-check after transfer in the different internet platform

Platform	Check Image			Extracting Text		
	SSIM	MSE	PSNR	SSIM	MSE	PSNR
E-mail	100%	zero	infinity	100%	zero	infinity
facebook	100%	zero	infinity	100%	zero	infinity
Instagram	100%	zero	infinity	100%	zero	infinity
WhatsApp	100%	zero	infinity	100%	zero	infinity
Telegram	100%	zero	infinity	100%	zero	infinity

4.5 Comparison with related work

Table 4.8 shows the comparison of the proposed system with some related works, and it can be shown that the suggested algorithm (Radon Transform, Hadamard code with the aid of Turbo code) have an experimental result of them with better quality of Stego-Text and image system with the range between (84-96) db also with higher embedding capacity and more security level. The results also stated that the turbo code will increase the security and robustness in extracting the text file.

Table (4.5) Proposed system comparison with some related works

Reference	Algorithm	PSNR No attack	SSIM No attack	MSE No attack	PSNR Gaussian Noise	SSIM Gaussian Noise	PSNR S and P Noise	SSIM S and P Noise
M. O. Espina [14]	Multiple level information security	47.7	-----	1.1	----	-----	-----	-----
A. Salem Ali [15]	Multilevel stego-Security system	66.66	0.98	-----	----	-----	-----	-----
H. Kweon [17]	Multi-level image steganography by using privet key	30	0.8	-----	10	0.3	15	0.58
A. A Mohammed [18]	Radon Transform	55.17	0.9949	-----	-----	-----	-----	------
Proposed method	Multi-level image steganography by Radon-Hadamard-Turbo code	84.87	0.997	0.027	60.6	0.98	68.3	.96

CHAPTER FIVE

Conclusions and Future Works

5.1 conclusion

- The proposed system was done by MATLAB program, and has been converted into a desktop APP.
- The system success with sending and receiving the steganography check image as well as extracting the TEXT and ID image embedded within the check after receiving it.
- Here, the importance of the Turbo code, Radon transform and Hadamard code is shown in preserving information during the embedding process and fully retrieval during the extracting process.
- The system has an MSE value of (0.027) which is indicates that the system has high level of security and has more efficiency when compared with previous researches in this field.
- The check image was sent in most social media sites such as (Email, Facebook, Instagram, WhatsApp, Telegram) and received completely without any change in the general structure of the image, with no effect was observed on the information contained within it .

5.2 Future Work

Developing the application using the Java language and converting it to an application on the mobile phone to facilitate the process of its use and enable the user to use it everywhere and anytime.

It will also explore new possibilities for the application to work on a larger scale and facilitate banking services operations.

Develop the algorithm to become more powerful in preserving the embedded information from hacker confusion.

References

[1] A. Freidoon Fadhil, "IMAGE STEGANOGRAPHY BASED CURVELET TRANSFORM", Al-Rafidain Engineering Vol.18 No.5 October 2010, pp 94-106.

[2] S. A. El_Rahman, "A comparative analysis of image steganography based on DCT algorithm and steganography tool to hide nuclear reactors confidential information", Computers and Electrical Engineering 70 (2018), pp 380–399.

[3] R. Thabit, N. I. Udzir, S. M. Yasin, A. Asmawi, N. Alifah Roslan and R. Din, "A Comparative Analysis of Arabic Text Steganography", Appl. Sci. 2021, 11, 6851, pp.1-32.

[4] A. Ali Husain, "Turbo Code based Video Steganography Technique for Image Hiding", Thesis in Electrical Engineering, University of Babylon, 2020, pp. 3.

[5] H. Adnan Hassan and O. Qasim Jumah Al-Thahab, "DIGITAL WATERMARKING OF MULTIMEDIA BASED HYBRID TRANSFORM", Thesis in Electrical Engineering, University of Babylon, 2019, pp. 4.

[6] S. Bhattacharyya, S. Mondal and G. Sanyal, "A Robust Image Steganography using Hadamard Transform", International Conf. on Information Technology in Signal and Image Processing - ITSIP 2013, Mumbai, India, pp. 132-142.

[7] H. Abdul- Jaleel Alasadi and O. Qasim Jumah Al-Thahab, "Audio Watermarking for medical application", Thesis in Electrical Engineering, University of Babylon, 2014.

[8] S. Thenmozhi and M. Chandrasekaran, "Image Steganography Technique using Radon Transform and Neural Network with the Wavelet Transform", Proceedings of the International Congress 2014, Bangkok, Thailand, pp. 143-49.

[9] S. Uma Maheswari and D. Jude Hemanth, "Image Steganography using Hybrid Edge detector and ridgelet transform", Defense Science Journal, Vol. 65, No. 3, May 2015, pp. 214-219.

[10] Y. E. A. AL-SALHI, S. LU, "Quality Measurements of Lossy Image Steganography Based on H-AMBTC Technique Using Hadamard Transform Domain", International Journal of Innovative Research in Information Security, Issue 9, Volume 2 (November 2015), pp. 1-5.

[11] H. ABDELLATIEF HUSSEIN, "Multi-Level Image Steganography by Using Pixel Intensity", Thesis in COLLEGE OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY, SUDAN UNIVERSITY OF SCIENCE AND TECHNOLOGY, 2015.

[12] A. Amsaveni and P.T Vanathi, "Reversible Data Hiding Based on Radon and Integer Lifting Wavelet Transform", Journal of Microelectronics, Electronic Components and Materials Vol. 47, No. 2, 2017, pp. 91 – 99.

[13] B. Abd-El-Atty, A. A. Abd El-Latif, and Mohamed Amin, "New Quantum Image Steganography Scheme with Hadamard Transformation", Advances in Intelligent Systems and Computing conference, 2018, pp. 342-352.

[14] M. O. Espina, A. C. Fajardo, B. D. Gerardo and R. P. Medina, "Multiple Level Information Security Using Image Steganography and Authentication", International Journal of Advanced Trends in Computer Science and Engineering, Volume 8, No.6, 2019, pp. 3297-3303.

[15] A. Salem Ali, M. Sabbih Hamoud Al-Tamimi, and A. Ahmed Abbood, "Secure Image Steganography Through Multilevel Security", International Journal of Innovation, Creativity and Change, Volume 11, Issue 1, 2020, pp.80-103.

[16] A. Ali Husain and O. Qasim Jumah Al-Thahab, "Implementation Of Stego-Watermarking Technique by Encryption Image Based On Turbo Code For Copyright Application", International Conference of Information Technology to

enhance E-learning and other Application, IEEE conference Baghdad, Iraq, 2020, 149-153.

[17] H. Kweon, J. Park, S. Woo and D. Cho, "Deep Multi-Image Steganography with Private Keys", Electronics 2021, 10, 1906, 2021, pp. 1-10.

[18] A. A. Mohammed, M. M Abdullah, S. R. Awad and F. S. Alghareb, "A Novel FDCT-SVD Based Watermarking with Radon Transform for Telemedicine Applications", International Journal of Intelligent Engineering and Systems, Vol.15, No.1, 2021, pp.64-74.

[19] F. Haojun, K. Yunbo and Li Xiao, "A Multi-level Watermarking Algorithm for RasterGeographic Data Based on Watermark Information Segmentation Mechanism", Journal of Physics: Conference Series, V. 2006, 2021, pp. 1-6.

[20] Y. Qian Zhang, K. Zhong and X. Yuan Wang, "High-Capacity Image Steganography Based on Discrete Hadamard Transform", IEEE Access, V. 10, 2022, pp. 65141 – 65155.

[21] A.Cheddad, “Steganoflage : A New Image Steganography Algorithm,” 2009.

[22] R. Boopathy, R. Dhaya, M. Ramakrishnan, and S. P. Victor, International Journal for Research in Applied Science & Engineering Technology (IJRASET), vol. 3, no. Vi, pp. 46–52, 2015.

[23] J. Kour and D. Verma, “Steganography Techniques –A Review Paper,” International Journal of Emerging Research in Management &Technology, vol. 3, no. 5, pp. 132–135, 2014.

[24] R. Chandramouli and N. Memon, “Analysis of LSB based image steganography techniques,” in IEEE International Conference on Image Processing, 2001, vol. 3, pp. 1019–1022.

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

[26] B. Li, J. He, J. Huang, and Y. Q. Shi, “A survey on image steganography and steganalysis,” Journal of Information Hiding and Multimedia Signal Processing, vol. 2, no. 2, pp. 142–172, 2011.

[27] M. S. Subhedar and V. H. Mankar, “Current status and key issues in image steganography: A survey,” Computer Science Review, vol. 13, pp. 95–113, 2014.

[28] P. Goel and P. Goel, “Data Hiding in Digital Images : A Steganographic Paradigm,” Indian Institute of Technology–Kharagpur, 2010.

[29] P.Jayaram, R.Ranganatha, and S.Anupama, “Information Hiding Using Audio Steganography - A Survey,” The International Journal of Multimedia & Its Applications (IJMA), vol. 3, no. 3, pp. 86–96, 2011.

[30] R. Goyal, N. Kumar, and I. Ntroduction, “LSB Based Digital Watermarking Technique,” International Journal of Application or Innovation in Engineering & Management (IJAIEM), vol. 3, no. 9, pp. 15–18, 2014.

[31] A. Swathi and S. A. K. Jilani, “Video Steganography by LSB Substitution Using Different Polynomial Equations,” International Journal Of Computational Engineering Research, vol. 2, no. 5, pp. 1620–1623, 2012.

[32] A. Kattoush," A Novel Radon-Wavelet-Based Multi-Carrier Code Division Multiple Access Transceiver Design and Simulation under Different Channel Conditions," The International Arab Journal of Information Technology, Vol. 9, No. 3, May 2012.

[33] A. Sawlikar and M. Sharma," Analysis of Different Pseudo Noise Sequences", International Journal of Computer Technology and Electronics Engineering (IJCTEE). Vol. 1, 2009.

[34] R.N. Mutagi," Pseudo Noise Sequences Tor Engineers", Electronics & communication engineering journal, vol. 8, No.2, pp.79-87,1996, April 1996.

[35] R. Vaddiraja," Generalized D-Sequences And Their Application To CDMA

Systems", A Thesis Of M.sc, Faculty of the Louisiana State University, 2003.

[36] M. Lampton, S. Sciences Lab, and U. Berkeley," A Pseudo-Random Number Generator for Spreadsheets", Journal of Statistical Software, Volume VV, Issue II, 2010.

[37] Dimitrios Christou, Marilena Mitrouli*, and Jennifer Seberry “Embedding and extension properties of Hadamard matrices revisited” (IJAIEM), Spec. Matrices 2018.

[38] Ass.Hameed K. Dawiod, and Ass.Khalid H. Hameed, “On representation of Hadamard Codes” AL- Fatih Journal . No . 32 .2008

[39] M. Miciak," Radon Transformation And Principal Component Analysis Method Applied In Postal Address Recognition Task", International Journal Of Computer Science And Applications, Techno-mathematics Research Foundation, Vol. 7 No. 3, pp. 33 - 44, 2010,2010.

[40] F. Matus, and J. Flusser, "Image Representation via Finite Radon Transform", Pattern Analysis and Machine Intelligence, IEEE Transactions on vol. 15, No.10 , pp. 996-1006, October 1993.

[41] L. Granai, "Radon and Ridgelet transforms applied to motion compensated images", In Multimedia and Expo, ICME'03. Proceedings, International Conference on, Vol. 1, pp. I-561, IEEE, 2003.

[42] P. Toft, "The Radon Transform Theory and Implementation", Thesis of Ph. D, Technical University of Denmark, 1996.

[43] A. Kattoush," A Novel Radon-Wavelet-Based Multi-Carrier Code Division Multiple Access Transceiver Design and Simulation under Different Channel Conditions," The International Arab Journal of Information Technology, Vol. 9, No. 3, May 2012.

[44] J. Barbier and E. Filiol, “Overview of Turbo-Code Reconstruction Techniques.,” IACR Cryptology ePrint Archive, vol. 2009, pp. 1–5, 2009.

[45] E. K. Hall, S. G. Wilson, and S. Member, “Stream-Oriented Turbo Codes,” vol. 47, no. 5, pp. 1813–1831, 2001.

[46] C. Berrou and A. Glavieux, “Near optimum error correcting coding and decoding: Turbo-codes,” IEEE Transactions on Communications, vol. 44, no. 9, pp. 1261–1271, 1996.

[47] T. M. Duman and M. Salehi, “New performance bounds for turbo codes,” IEEE Transactions on Communications, vol. 46, no. 6, pp. 717–723, 1998.

[48] C. Berrou, A. Glavieux, and P. Thitimajshima, “Near Shannon limit errorcorrecting coding and decoding: Turbo-codes.,” in In Proceedings of ICC’93-IEEE International Conference on Communications, 1993, vol. 2, no. 1, pp. 1064–1070.

[49] R. Garello, G. Montorsi, S. Benedetto, and G. Cancellieri, “Interleaver properties and their applications to the trellis complexity analysis of turbo codes,” IEEE Transactions on Communications, vol. 49, no. 5, pp. 793–807, 2001.

[50] C. P. Dennett, “an Investigation of Turbo Codes Over Mobile Wireless Channels,” University of Wolverhampton, 2006.

[51] P. Jung and M. Naβhan, “Performance evaluation of turbo codes for short frame transmission systems,” Electronics Letters, vol. 30, no. 2, pp. 111–113, 1994.

[52] S. Rekh, S. S. Rani, and A.Shanmugam, “Optimal choice of interleaver for turbo codes .,” Academic Open Internet Journal, vol. 15, pp. 6–13, 2005.

[53] S. Yang, C. Xu, W. Tan, C. Wu, and Y. X. Lee, “Interleaver and deinterleaver for iterative code systems,” United States Patent, vol. 8, no. 205, pp. 1–13, 2012.

[54] F. Dowla, “turbo code,” in HANDBOOK OF RF AND WIRELESS TECHNOLOGIES, 2004, pp. 375–399.

[55] G. Santosh and S. Rajaram, “DESIGN AND IMPLEMENTATION OF TURBO CODER FOR LTE ON FPGA,” International Journal of Electronics Signals and Systems (IJESS), vol. 3, no. 2, pp. 15–19, 2013.

[56] S. A. Abrantes, “From BCJR to turbo decoding: MAP algorithms made easier,” pp. 1–30, 2004. [77] S. A. Barbulescu, “ITERATIVE DECODING OF TURBO CODES AND OTHER CONCATENATED CODES,” 1996.

[57] S. K. Chronopoulos, G. Tatsis, and P. Kostarakis, “Turbo Codes—A New PCCC Design,” Communications and Network, vol. 03, no. 04, pp. 229–234, 2011.

[58] H. A.-J. Al-Thahab, Osama Q.Alasadi, “audio watermarking for medical application based on hybrid transforma,” University Of Babylon, 2014.

[59] P. R. Deshmukh and B. Rahangdale, “Data Hiding using Video Steganography.,” International Journal of Engineering Research & Technology, vol. 3, no. 4, pp. 856–860, 2014.

[60] R. Paul, A. K. Acharya, V. K. Yadav, and S. Batham, “Hiding large amount of data using a modren approach of video steganography,” in IET Conference Publications, 2014, pp. 337–343.

[61] P. Shinde and T. B. Rehman, “A Novel Video Steganography Technique,” International Journal of Advanced Research in Computer Science and Software Engineering Research, vol. 5, no. 12, pp. 676–684, 2015.

[62] S. A. Naji, H. N. Mohaisen, Q. S. Alsaffar, and H. A. Jalab, “Automatic region selection method to enhance image-based steganography,” Periodicals of Engineering and Natural Sciences, vol. 8, no. 1, pp. 67–78, 2020.

[63] Z. Wang, A.C. Bovik, H. R. Sheikh, and E. P. Simoncelli, “Image quality assessment: From error visibility to structural similarity,” IEEE Transactions on Image Processing, vol. 13, no. 4, pp. 600–612, 2004.

[64] S. I. M. Ali, M. G. Ali, and L. A. Z. Qudr, “PDA: A private domains approach for improved MSB steganography image,” Periodicals of Engineering and Natural Sciences, vol. 7, no. 3, pp. 1405–1411, 2019