Ministry of Higher Education and
Scientific Research
University of Babylon
College of Science for Women
Department of Computer Science

Image Blocks Features Based Coverless Steganography

A Thesis

Submitted to the Council of College of Science for
Women, the University of Babylon in a Partial
Fulfillment of the Requirements for theDegree of Master
in Science\ Computer Sciences

By
Hadeel Talib Mangi

Supervised By
Prof. Dr. Suhad Ahmed Ali
Prof. Dr. Majid Jabbar Jawad

2023 A. D. **1444 A. H.**

بسم الله الرحمن الرحيم

" قالُوا سُبحانَك لا عِلمَ لنَا

إلا ما عَلمتَنا إنكَ أنتَ العَليمُ الحكيمُ "

صدق الله العظيم

(سورة البقرة: آية 32)

Supervisors Certification

We certify that this thesis entitled "***Image Blocks Features Based Coverless Steganography***" was done by (Hadeel Talib Mangi) under our supervision.

Signature:
Name: Prof. Dr. Suhad Ahmed Ali
Date: / / 2023
Address: University of Babylon/College of Science for Women

Signature:
Name: Prof. Dr. Majid Jabbar Jawad
Date: / / 2023
Address: University of Babylon/College of Science for Women

The Head of the Department Certification

In view of the available recommendations, I forward the dissertation entitled “***Image Blocks Features Based Coverless Steganography***” for examining committee.

Signature:
Name: Dr. Saif M. Kh. Al-Alak
Date: / / 2023
Address: University of Babylon/College of Science for Women

Dedications

To my family especially my great parents…

To my husband, children, and my brothers…

To my teachers and friends,

I dedicate this work.

Hadeel

Acknowledgments

All thanks and praise to Allah, the Lord of the world, who gave me courage and enabled me to achieve this work.

My thanks and gratitude go to my supervisors Prof. Dr. Suhad Ahmed Ali and Prof. Dr. Majid Jabbar Jawad for the support and guidance they have given me and the effort and time to complete this research.

Thanks and Gratitude to all my Professors and all the staff of the Department of Computer Sciences \ College of Sciences for Women \University of Babylon for their help.

All Thanks and Gratitude are due to all my family for their support andencouragement.

I would like to thank my friends for helping me.

Hadeel (2023)

Abstract

Ensuring the confidentiality of the information when it is transmitted through public channels is always needed. The steganography technique is one of the possible solutions to achieve this goal. Most of the existing image Steganographic approaches embed the secret information imperceptibly into a cover image by modifying its content. This modification causes some distortion in the stego image. In addition, these modifications caused by the embedding will be left in the cover image, which will make the detection technology for hidden information successful, this detection technology is called steganalysis. In order to overcome the modification of the cover during the embedding process, a coverless image steganography (CIS) technique is proposed.

However, the CIS faces several challenges namely, capacity, robustness, and security.

This thesis proposed a CIS method that explores the effectiveness to enhance capacity and embedding in a single cover image only as well as enhancing the robustness against attacks. The proposed approach performs coverless information hiding by establishing mapping relationships between the hash codes of the image blocks and each segment of the secret message. To compute the hash codes for an image, a powerful hashing algorithm based on scrambling and Discrete Wavelet Transform (DWT) is proposed. A hash sequence table is built using a proposed hashing algorithm. To reduce the searching time, an indexing table is built based on the generated hash sequence table. Each segment of the secret message is mapped with the generated hash sequences and save the auxiliary information for each matched segment in a file which is encrypted using proposed encryption method.

According to the experimental results, the proposed hashing method can gain all of the hash codes that equal to 256 hash codes in a single image and for the significant number of images that outcomes the previous methods that couldn’t gain or gained hash codes for a limited number of images only. The experimental findings also show that the proposed system obtain a higher hiding capacity that equal to 261,888 bits in single image that outcomes all the previous methods. The experimental findings also proved the system's resilience against a variety of attacks that the value of BER is close to zero and also outcomes the previous methods in robustness criteria that gain higher RC value than them. Since the stego-image is natural one without any modification traces, the approach can resist all of the existing steganalysis tools. Experimental results and analysis prove that the approach also have higher level of security that entropy value close to 1,and correlation value close to zero, as well as the proposed system proved that it has short execution time.

List of Contents

Content No.	Title	Page No.
Chapter One: Genaral Introduction		
1.1	Introduction	1
1.2	Related Works	2
1.3	Problem Statement	9
1.4	Aims of the Thesis	10
1.5	Thesis Contributions	10
1.6	Organization of Thesis	11
Chapter Two: Theoretical Background		
2.1	Introduction	12
2.2	Information Hiding	12
2.2.1	Watermarking	12
2.2.2	Steganography	13
2.3	Image Steganography	14
2.3.1	Traditional Image Steganography	15
2.3.2	Coverless Image Steganography	16
2.3.2.1	Based on Robust Hashing	18
2.3.2.2	Based on BOW Algorithm	18
2.3.2.3	Based on Generative Model	18
2.3.2.4	Based on Partial Duplicates of a Given Secret Image as Stego-Images	18
2.4	Embedding Domain of Image Steganography	19
2.4.1	Special Domain of Image Steganography	19
2.4.2	Transform Domain of Image Steganography	20

2.5	Requirements of Image Steganography	21
2.6	Coverless VS Traditional Image Steganography	23
2.7	Block Dividing Based Coverless Image Steganography	24
2.8	Applications of Image Steganography	25
2.9	Attacks on coverless Image Steganography	26
2.10	Evaluation Metrics of Coverless Image Steganography algorithm	27
2.10.1	Capacity Measures	27
2.10.2	Robustness Measures	27
2.11	Encryption	28
2.11.1	Chaotic Encryption	28
2.11.2	Encryption Evaluation Metrics	30
2.11.2.1	Entropy	30
2.11.2.2	Correlation Coefficient	30
2.11.2.3	Avalanche Effect	30
2.11.2.4	National Institute of Standards and Technology Tests	31
Chapter Three: The proposed Image Blocks Features Based Coverless Steganography System(IBFBCSS)		
3.1	Introduction	33
3.2	The Proposed Image Blocks Features Based Coverless Steganography(IBFBCS)	33
3.2.1	Processes on the Sender Side	34
3.2.1.1	Secret Data Splitting	35
3.2.1.2	Embedding with Image Blocks Features Based Coverless Steganography(IBFBCS)	35
3.2.1.3	Auxiliary Information File Encryption Process	44
3.2.2	processes on the Receiver Side	47

Chapter four: Experimental Results and Discussion

4.1	Introduction	50
4.2	Data Set	50
4.3	Experimental Results of the Proposed System	52
4.3.1	Tests on the Generated Hash Codes	52
4.3.2	Testing the Embedding Procedure	54
4.3.3	Testing the Extracting Procedure	57
4.3.4	The Information Hiding Capacity	58
4.3.5	Execution Time Analysis	59
4.3.6	Experimental Results Related to System Robustness	60
4.3.1	Experimental Results related to Security Analysis	72

Chapter five: Conclusions and Ideas for Future Works

5.1	Introduction	77
5.2	Conclusions	77
5.3	Future Works	78
	References	80

List of Figures

Figure No.	Title	Page No.
Chapter Two: Theoretical Background		
2.1	Classification of image Steganography	14
2.2	General block diagram of traditional image steganography system	15
2.3	Block diagram of coverless image steganography	17
2.4	DWT's Image Analysis	21
2.5	Trade-off Triangle between Basic Requirements	22
2.6	Extracting the final feature from an image patch	24
Chapter Three: The proposed Image Blocks Features Based Coverless Steganography System(IBFBCSS)		
3.1	Block diagram of the proposed system	34
3.2	Diagram of Hash Sequence Generation	37
3.3	Image scrambling	39
3.4	Hash Sequence Generation	41
3.5	indexing process	42
3.6	Embedding process	43
3.7	Auxiliary information file encryption process	44
3.8	Auxiliary Information Scrambling process	45
3.9	Auxiliary Information file decryption process	47
3.10	Extraction process	49
Chapter four: Experimental Results and Discussion		
4.1	Sample of collected cover images	51
4.2	Secret data	52
4.3	The splitting of secret data	54
4.4	The result of generated hash sequences	55

4.5	The hash Table	56
4.6	The auxiliary information file	56
4.7	The encrypted Auxiliary information file	57
4.8	The decrypted auxiliary information file	57
4.9	The segmented extracted data	58
4.10	The extracted secret data	58
4.11	key influencing on encryption and decryption process	73

List of Tables

Table No.	Title	Page No.
Chapter One: Genaral Introduction		
Table (1.1)	Summary of previous CIS methods	7
Chapter four: Experimental Results and Discussion		
Table (4.1)	The relationship between block size and generated hash code	52
Table (4.2)	The robustness versus block sizes	53
Table (4.3)	Comparison of the various hashing algorithms and the numbers for secret data not found	54
Table (4.4)	The hiding capacity of different information hiding approaches	59
Table (4.5)	Execution time of hashing, embedding and extracting operations	59
Table (4.6)	The results of the compression attack	61
Table (4.7)	The results of the noise attacks	62
Table (4.8)	The results of the filtering attacks	65
Table (4.9)	The results of the geometrics attacks	68
Table (4.10)	The results of brightness and sharpening attacks	70
Table (4.11)	Comparison of Robustness with Two CIS methods	71
Table (4.12)	security measurements values	74
Table (4.13)	NIST tests values	75
Table (4.14)	Security analysis for tested images	76

List of Algorithms

Algorithms No.	Title	Page No.
Algorithm (3.1)	Embedding Process	35
Algorithm (3.2)	Hash Sequence Generation	37
Algorithm (3.3)	Image Scrambling	38
Algorithm (3.4)	Encryption Process	46
Algorithm (3.5)	Extracting Process	47
Algorithm (3.6)	Decryption Process	48

List of Abbreviations

Term	**Meaning**
AE	Avalanche effect
BOW	Bag-of-words
BER	Bit Error Rate
CC	Correlation coefficient
DC	Direct Current
DCT	Discrete Cosine Transform
DFT	Discrete Fourier Transform
DWT	Discrete Wavelet Transform
RC	Extraction Accuracy
HOGS	histograms of oriented gradients
HVS	human visual system
IC	Identity card
LDA	latent Dirichlet allocation
MIS	medical information systems
MSB	Most Significant Bit
NIST	National Institute of Standards and Technology
LFSR	the linear feedback shift register's
VoIP	Voice over IP

List of Publications

This work has resulted in the following publication:

[1] H. T. Mangi, S. A. Ali, and M. J. Jawad, "Enhancing of Coverless Image Steganography Capacity Based on Image Block Features",Accepted for publication in TELKOMNIKA Telecommunication Computing Electronics and Control, Vol.99, No.1, 2023.

[2] H. T. Mangi, S. A. Ali, and M. J. Jawad, “Encrypting of Text Based on Chaotic Map”, JOURNAL of UNIVERSITY of BABYLON for Pure and Applied Sciences, vol. 31, no. 1, 2023.

Chapter One

General Introduction

Chapter One
General Introduction

1.1 Introduction

Due to the widespread use of multimedia data and technological improvements in the areas of image, audio, and video transmission, secret communication between a sender and a receiver has taken place on a significant amount of significance in order that the third parties(attackers) cannot access critical or confidential information [1]. So in the modern world, security issues related to information transit have grown to be a major concern. As long as this information is kept safe, individuals will be satisfied [2]. To prevent unanticipated outcomes, information security is essential for any firm [3]. Therefore, it is suggested that information hiding be used that hide the information in a cover file[2][3]. Steganography and watermarking are two widely used techniques for information hiding [6]. They both directly alter the media file's content (such as images, videos, and music), providing copyright protection and covert communication or sender identification [7]. Steganography is a process for hiding secret information by enclosing it in a regular, non-secret file or communication; the information is subsequently extracted at the designated place [8]. Many works have been done in image steganography because images are one of the crucial carriers utilized in multimedia communication [9].

Image Steganography is the technique of hiding the existence of the communicated information within images [10]. There are two types of steganography techniques for images, according to the documentation: Traditional image steganography with data embedding and coverless image steganography [11]. The Traditional methods of image steganography typically change the image just enough to disguise the information. Traditional information hiding techniques include spatial domain techniques like histogram modification least significant bit substitution [12] and transform domain techniques like Discrete Fourier Transform (DFT)[13], discrete cosine transform [14] and discrete wavelet transform [15].These steganography techniques can be used for clandestine communication, but the content on the cover is changed. On the stego cover, there will unavoidably be a mark of modification. Consequently, the stego cover is equally challenging to avoid being discovered by steganalysis techniques that are already in use. For the purpose of avoiding being discovered, the "coverless image steganography" is a newest filed of image steganography than traditional image steganography that produced in May 2014 [16] [17]. The objective behind coverless information concealment is to choose cover images that have stego-images of features that indicate secret information [18]. A suitable hashing method can be used to map associations between visual features and hidden message parts [19]. However, there are a number of significant challenges of coverless image steganography to overcome such as [20]:

Capacity: Where the length of the image hash determines how effective coverless steganography will be, as it is based on the mapping links between secret information and natural images, resulting necessary to compile an image data set made up of a large number of natural images, which come from a variety of sources and cannot accurately meet the requirements in order to transmit messages accurately.

Robustness: Coverless image steganography needs to be resistant to both attackers and steganalysis tools.

Security: Coverless image steganography also needs to have a higher security due to using mapping relationships for saving the exchanged information.

1.2 Related Works

Many works have been done in Coverless image steganography. This section briefly discusses some of the coverless image steganography methods that have been previously suggested.

In 2015, Zhou Z. and his research team proposed one of the first methods of coverless image steganography, which uses an image to represent 8 bits. This method consists of building an image database containing at least 256 different images collected from the internet, then indexing the database according to the 8-bit binary sequence generated by the hashing algorithm., The secret data is converted to a bit string, split up into several segments and the cover images whose hash sequences are the same as the segments are used to implement the information concealing. picked as the stego-images from the database. however, each cover image can hide only 8 bits [24].

In 2016, Z. Zhou and his research team suggested coverless steganography based on BOW (Bag-of-words). Information the text is concealed using the BOW idea. Visual words are recovered to represent text information in order to conceal text information in an image. Using a BOW model, visual words are extracted from an image set by creating a mapping between text information's keywords and visual words. The next stage is to split each image up into a number of smaller versions. For each sub-image, a histogram of visual words is constructed, and the visual words with the highest values in the histogram are chosen to represent the sub-image. Finding a collection of sub-images with visual words connected to text data is done via the mapping relation. Stego images, which incorporate various sub-images, are images used for covert communication [25].

In 2017, Z. Zhou and his research team proposed a method for coverless image steganography based on histograms of oriented gradients (HOGS) and hashing. The original images with hash sequences matching the secret information are extracted directly from a large database and used as stego images for secret communication instead of choosing a cover image for secret information embedding. This method uses the HOGs-based hashing technique to generate hash sequences. Three parts make up the hash sequence creation procedure. Before being separated into 4 separate, non-overlapping blocks, each database image is converted to a gray level. Each image block contains the HOGs features, which are extracted. The mean value of all entries is compared to each item's value in the HOGs histogram to construct the block's hash sequence. The value is 1 if the block's HOGs are higher than the mean value; otherwise, it is 0 [26].

In 2018, X. Zhang and his research team was proposed a coverless image steganography method utilizing the discrete cosine transform and the latent Dirichlet allocation (LDA) topic model. The classification of the image database is done in the first using the latent dirichlet allocation topic model. The second stage involves selecting the images associated with one topic and performing an 8× 8 block discrete cosine transform(DCT) on them. The relationship between direct current coefficients in the subsequent blocks thus creates a robust feature sequence. The feature sequence, DC, position coordinates, and image path are then combined to form an inverted index. [27].

In 2019, Chen, X., Qiu and his research team suggested a high-capacity coverless information steganography technology. By dividing the cover image into various image blocks, each of which can hold one bit of hidden information, the capacity is substantially increased. Then, using secret information, extracting the image blocks needed for replacement from the image block database and combine them to create the stego image. The required image blocks are comparable to cover image blocks and all come from natural images, which contributes to the great quality of the stego image. Additionally, they created a two-level index structure. The findings demonstrate the bigger capacity and improved visual quality of the suggested strategy [28].

In 2020, X. Zhang and his research team presented a generative coverless image information hiding technique based on fractal theory to increase the robustness and imperceptibility of the current coverless image information hiding. Firstly, four methods for creating fractal images are examined. The relationship between the coverless information concealment and the first four fractal image-creation approaches is then discussed. secondly using fractal image generation algorithm for creating fractal images that regulates pixel rendering during the production process in order to hide sensitive information [29].

In 2020, Yang, L. and her research team proposed for the goal of increasing the capacity a coverless information hiding approach based on the Most Significant Bit (MSB) of the cover image (CIHMSB). The cover image is first divided into a number of pieces. Second, to symbolize using the MSB of the cover image Calculated is each fragment's average intensity, which is the secret information. Third, a mapping that is one-to-one employing the mapping, the relationship between the secret information and the MSB of the image fragment is established. the mapping order (designated as Km), chosen previously by the sender and the receiver. This method providing a mapping flag (abbreviated as Kf) by the sender along with the stego image to the receiver, when the stego image is delivered through regular channels, the channel noise may distort it, making it difficult for the recipient to precisely decode the secret data. Therefore, the technology is required to choose more ideal image features and to increase the robustness [30].

In 2021, Abdulsattar, F. S. proposed a method for coverless image steganography based on Eigen decomposition, the study investigates the efficacy of coverless information hiding, which transmits secret information using one cover image. By creating mapping relationships between the characters of the secret message and the hash codes of the image blocks, the method provides coverless information concealing. The block is divided into nine smaller blocks, and the greatest eigenvalues of the smaller blocks are compared using four different configurations to get the hash code. The method creates a lookup table to contain the previously computed hash codes along with the corresponding block positions in order to accelerate the embedding procedure. Block sizes, sub-block configurations, and overlapping blocks are three crucial factors in the method. The results indicate that overlapping is required to produce a large enough number of distinct hash codes, and the suggested strategy has a larger concealing capacity [31].

In 2021, Q. Liu and his research team suggested a technique for coverless image steganography to increase robustness against geometric attacks; the suggested solution offers a deep learning-based coverless information hiding strategy with no change traces. The method is tested against a number of frequently used image attacks, including JPEG, contrast, and particularly the robustness of geometric attacks [32].

In 2022, X. Liu and his research team proposed a robust coverless steganography using limited mapping images. To ensure the distinctability and robustness of the mapping features in this approach, The method combining geometrically invariant features and exploiting ResNet101 for the classification of candidate images for reducing the suspicion of the attackers; that adopt a well-trained residual neural network with a depth of 101 layers so that users can select a category of the image dataset and search for a suitable cover image[33].

In 2022, J. Pan and his research team introduced a coverless image steganography based on the two-level approach and unique arrangements are introduced in the study for generating a sufficient diversity of features while also improving overall capacity and image quality. Additionally, the work develops a new encryption model for secret message security based on the logical mapping. This technique uses a look-up table and a two-level mechanism to deliver a secret message using a single carrier image with coverless information concealment. The created location table is embedded on the original image using reversible information hiding to ensure storage and security [34].

In 2023, R. Campbell and his research team suggested an improvement in terms on capacity on the LINA YANG work in [20]. In this study, a coverless information-hiding technique based on the cover image's lowest and highest values of the fragment (CIHLHF) is proposed. The most Significant bit of the lowest and highest binary forms are transferred to the secret data binary form. Using predetermined keys, the mapping is arranged. Its results prove that the suggested strategy has a greater concealment capacity than similar techniques [35]. Table (1.1) summarized the literature mentioned in this section.

Table (1.1): Summary of previous CIS methods

#	Ref.	Technique	Advantage	Disadvantage	Capacity (Bit for carrier)
1	24	Hashing algorithm	have desirable robustness to the typical image attacks	Limited in capacity	8
2	25	Utilizing the Bag of Words (BOW) paradigm.	The model Reduce the attacker's suspicions by sending images from nearby topics	the retrieval efficiency is limited, when searching for an image in a very large image database	16
3	26	Histograms of oriented gradients (HOGs)-based hashing algorithm.	has good security and strong robustness to the common attacks	It still suffers from a low payload.	8
4	27	Latent Dirichlet allocation and discrete cosine transform	has better robustness against common image processing especially geometric attacks	Little amount of information can be concealed in a single image.	1-15
5	28	Double-level index and block matching	Gained embedding capacity higher than the previous coverless image steganography methods	The cover image was described by a single type of feature.	10000
6	29	Four fractal image-generating techniques are examined, and the connection between CIS and these techniques is explained.	improved the robustness and imperceptibility of the existing coverless image information hiding methods	Require additional work on the ongoing analysis of the relationships between generating parameters and information concealment in coverless images	10000

7	30	The MSB of the image fragments and the binary form secret information are mapped in accordance with the mapping sequence Km, resulting in a mapping flag.	the method increased has hiding capacity than the previous coverless information hiding methods.	Compared to conventional steganography, it has a smaller capacity.	1296
8	31	‘ Eigen decomposition	the approach has a higher hiding capacity than the existing coverless image information hiding methods and attempt to gaining most of hash codes in single image	It cannot generate all the possible hash codes. Require a more devintisy of generated hash code.	55,112
9	32	Deep learning-based coverless information hiding strategy	Has better robustness against geometric attacks	Need a large dataset of images to express the complete secret information because a little bits can be hidden in a single image.	1-15
10	33	ResNet101 deep learning	The scheme has superior performance in terms of Distinguishability, the required number of mapping images, and mapping completeness	Has a little amount of hidden capacity.	32

11	34	Two-level mechanism and a look-up	the model achieves high capacity and perfect hiding rate under the premise of ensuring image quality	If an attacker has complete control over the model, hidden information may be recovered or even altered.	84,005
12	35	Lowest and highest values of the fragment (CIHLHF) of the cover image.	The model increase the Capacity than the existing coverless image information hiding methods	The proposed CIHLHF has a huge mapping flag.	49,152

1.3 Problem Statement

Coverless image steganography has the following challenges:

1. It has less capacity than traditional image steganography and the capacity considered is the biggest challenge for any concealment work, at the same time, there are additional challenges that must be taken into account when making any proposed work. These are robustness and security.

2. Coverless image steganography uses mapping relationships between the secret data and the cover images that are collected in a huge dataset due to cannot finding all the possible hash codes in single image for an enough number of images and the number of mapping relationships increases with the extension of secret information, resulting in a high cost in terms of time and storage for collecting and perhaps being impracticable.

3. The transmission of the set of images increases the overhead time.

Therefore, a system must be proposed that solves the above problems, that increases the capacity of the coverless image steganography that uses only a single image for transmission of all the secret data as well as maintaining the other characteristics.

1.4 Aims of the Thesis

The objectives of thesis include several aspects such as:

1. Proposing an efficient method for increasing the capacity of coverless steganography that guaranty generate diverse hash codes for large number based on image scrambling and block dividing.

2. Proposing a method for increasing the robustness against attacks working in the transform domain.

3. Proposing a method for increasing the security by using symmetric encryption for axillary information file.

4. Finding only the sufficient set of images that contain all the possible hash sequences in order to employ one of them for sending the complete secret message instead of creating a huge dataset so decreasing the cost of time and storage and minimize the overhead time for the transmission of the secret data..

1.5 Thesis Contributions

The contributions in in this thesis can be explained as follows: -

- The proposed system of embedding and extracting procedures, is try to obtain all three challenges of coverless image steganography, which can be listed as follows:

1. Capacity: Instead of creating a huge database for sending the complete secret data using a coverless information hiding strategy, the proposed system investigates the effectiveness of employing a single image for conveying a full secret message by increasing the hiding capacity of the cover image and obtaining all the possible hash codes in a number of images after applying the proposed hiding based on block portioning and image scrambling.

2. Robustness: After employing well-known attacks, the image will have retrieved with a tolerable degree of error. The suggested approach should be able to withstand attacks from changes in brightness, contrast, noise addition, and rescaling.

3. Security: In the proposed system, the symmetric encryption method based on chaotic map encryption is used for encrypting the auxiliary information file, this technique adds a level of security to the system that can be used for preserving the confidentiality of the auxiliary information file.

1.6 Organization of Thesis

The rest chapters of this thesis are divided as follows:

- Chapter two: Theoretical Background

This chapter will give a background overview about information hiding theory, steganography techniques, coverless image steganography, block dividing based coverless image steganography, and potential Steganographic system attacks.

-Chapter three: The proposed Image Blocks Features Based Coverless Steganography System(IBFBCSS)

This chapter explains The proposed system that based on Image Blocks Features Based Coverless Steganography System(IBFBCSS).The algorithms of the proposed system are also covered in this chapter.

- Chapter four: Experimental Results and Discussions

This chapter will present the proposed system's experimental results.

-Chapter five: Conclusions and Ideas for Future Works

This chapter presents the key conclusions and ideas for future work from the results of the proposed system.

Chapter Two

Theoretical Background

Chapter Two
Theoretical Background

2.1 Introduction

The internet takes up a significant amount of space in people's lives today who are interested in securely and digitally sharing a variety of media. Sadly, free access to digital multimedia communication also offers practically unheard-of opportunity to pirate protected works. Therefore, it is imperative to develop security methods that establish covert links and enable users to safely share their digital media and preserving confidentiality in personal communications [36]. Image steganography that hides the information inside an image consider one of the important aspects of information security. Coverless image steganography has emerged as one of the most important methods for preserving this information. This chapter covers the theoretical background of the proposed system. The chapter examines coverless image steganography's basic idea, block-based coverless image steganography, possible attacks on steganography algorithm, and evaluation metrics that are used for evaluating the proposed system. Additionally, it discusses information-hiding strategies, which can be divided into two categories: steganography and digital watermarking.

2.2 Information Hiding

It is a technique of concealing secret information that makes use of cover media, such as images, audios, videos, documents, etc. for hiding the sensitive information within it [37]. The goal of information hiding is to prevent the unauthorized users from seeing or changing the privacy information [38]. Information hiding can be classified into two technique Steganography and watermarking techniques.

2.2.1 Watermarking

Watermarking is a set of technologies employed in digital media copyright protection systems It refers to including sensitive data in digital files that can be used to verify the owner's identity. The art of watermarking is hiding extra information (which could be an image logo, text message, and raw watermark bits) inside the content of the host objects such as images, audio signals, speech signals, 3D graphical objects, videos, texts, software codes, network streams, XML data, and ontologies without serious degradation on the quality of the objects. The watermark must be detectable from the watermarked content even when intentional and unintentional manipulations have been conducted on the digital watermarked content. the digital watermarking takes full use of data redundancy, visual redundancy, or other characteristics that are ubiquitous in digital multimedia works and uses a certain embedding method to directly embed the significant tag information(digital watermark) into the digital multimedia content; as the watermarked digital multimedia work, its intrinsic value or use is not affected in any way, and the human perceptual system can’t detect the embedded digital watermark information [39].

2.2.2 Steganography

Steganography is the science of communication hiding that is concealed to prevent the detection of hidden data which the hidden data are another medium. Steganography allows for the embedding and extraction of confidential information from media. Steganography's objective is to prevent suspicion from being raised about the transmission of a secret message[40]. The stego-object (i.e., the item containing hidden messages) must be perceptually indistinguishable to the extent that suspicion is not aroused, according to the fundamental premise of this system. Steganalysis uses the fact that concealing information in digital media modifies the carrier's properties and applies some sort of distortion to it as the basis for finding the hidden message [41]. A steganalysis system is created to detect hidden data by examining the various aspects of stego-images and cover images (i.e., the images with no hidden messages) [42]. Steganography is a collection of techniques for embedding information using multimedia data, including image, text, audio, video, etc. [43]. Image steganography has sparked a lot of attention since people use images so frequently and because they are one of the most popular forms of media [44].

2.3 Image Steganography

Image steganography is a method for communication that involves concealing information in an image [45]. Secret message insertion could be used to conceal data by encoding it for each bit in the image or primarily inserting it as a message in the noisy parts that reflect places with less observation, such as those where there is a lot of natural color variation. Additionally, because covert data may disperse randomly throughout an entire cover, images have grown to be the most frequent Steganography cover objects. The present research's subsequent sections will therefore concentrate on concealing information in images[46].

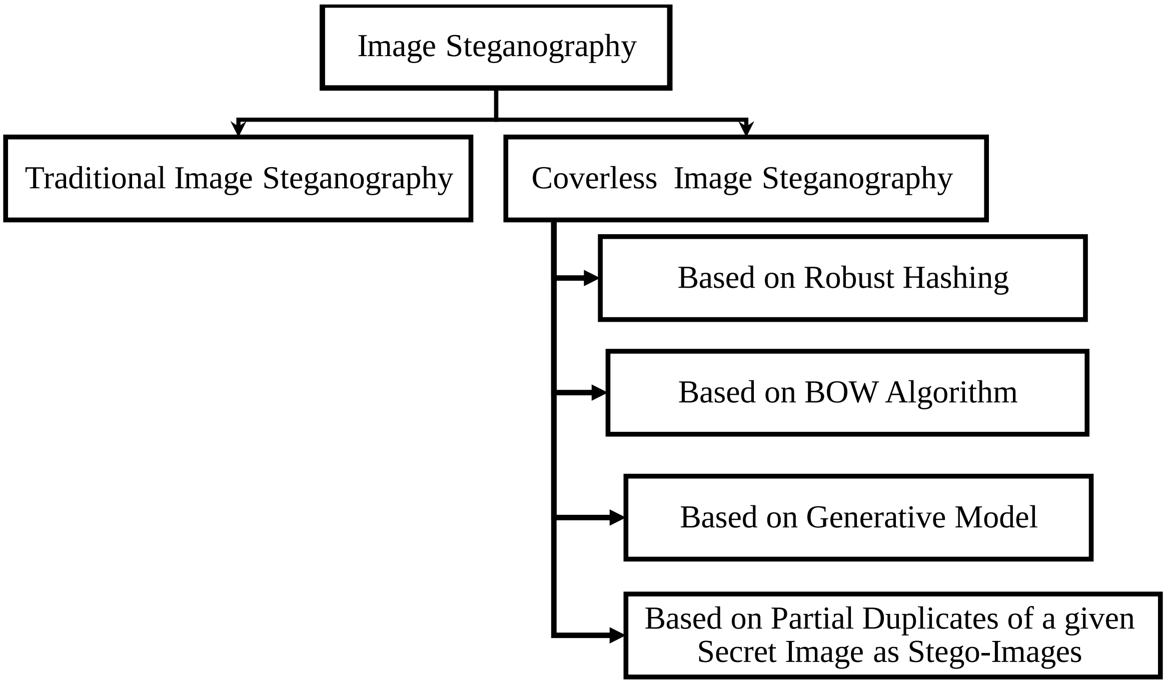


Image Steganography
Traditional Image Steganography
Coverless Image Steganography
Based on Robust Hashing
Based on BOW Algorithm
Based on Generative Model
Based on Partial Duplicates of a given Secret Image as Stego-Images

Figure (2.1): Classification of image Steganography

As shown in Figure (2.1), image steganography can be classified based on cover into two categories namely traditional image steganography and coverless image steganography.

2.3.1 Traditional Image Steganography

In this type, the secret information is concealed inside the digital images which are used to conceal the other information. The block diagram of the general traditional image steganography is shown in Figure (2.2). The approach that is frequently employed in this procedure entails directly encoding the secret data into the carriers. The term "secret data" refers to information where the sender's messages were kept private). The term ‘cover image’ refers to the image that is used to convey the secret message. The term "stego image" refers to the image with hidden data. Additionally, messages can be generated from the images themselves or put in cover images and stego-images. The decoder often in the other side uses the extracting algorithm for extracting the secret data from the stego image [47].

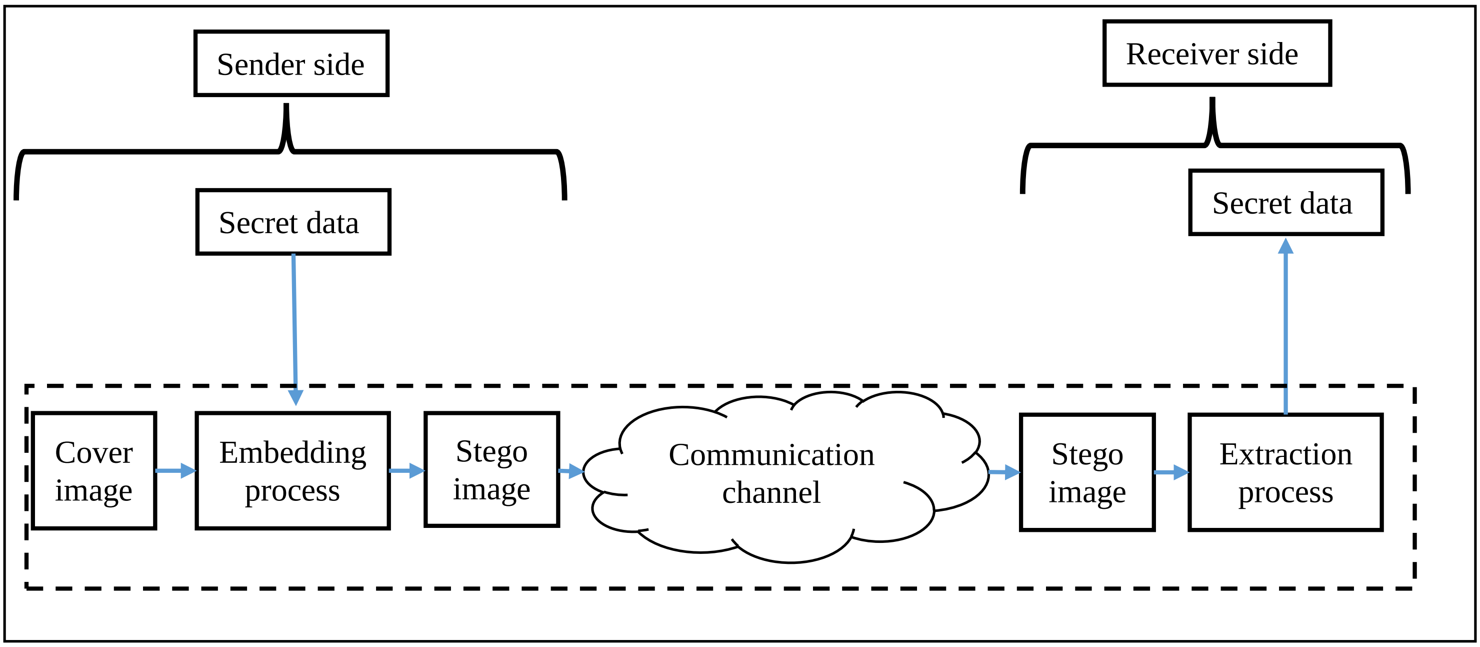


Figure (2.2): General block diagram of traditional image steganography system [47]

Traditional image steganography, however, suffers from a serious weakness in that the cover image retains the modification traces made by embedding, which renders successful steganalysis impossible [48].

2.3.2 Coverless Image Steganography

Coverless steganography is an image steganography framework for hiding the secret data by searching acceptable images which contain these data. These images are considered as stego-images. While the carrier is still utilized in coverless image steganography, it is not altered. The hidden information is represented by its own attributes, including pixel brightness value, color, texture, edge, contour, and high-level semantics. The carrier is passed without going through the standard steganography method's construction of the camouflage carrier (the secret information) [48], In terms of resistance to well-known attacks including brightness change, rescaling, JPEG compression, and contrast enhancement, enhancing the privacy of information's security of the CIS framework outperforms earlier steganography techniques. Due to the fact that it is invisible and it cannot be read. The CIS has a lot of development potential. The fundamental concept of coverless image steganography is to examine the carrier's qualities and map them to the secret information in accordance with predetermined rules based on the attributes' properties. The secret information can be directly represented by the carrier in this way. The stego cover is directly generated or acquired using the secret information. Despite the fact that an image just consists of pixels, the information they hold is very different. The image can express more than the image itself, which is not available in the text, according to previous research on the subject[49].Figure (2.3) describes the block diagram of the technique.

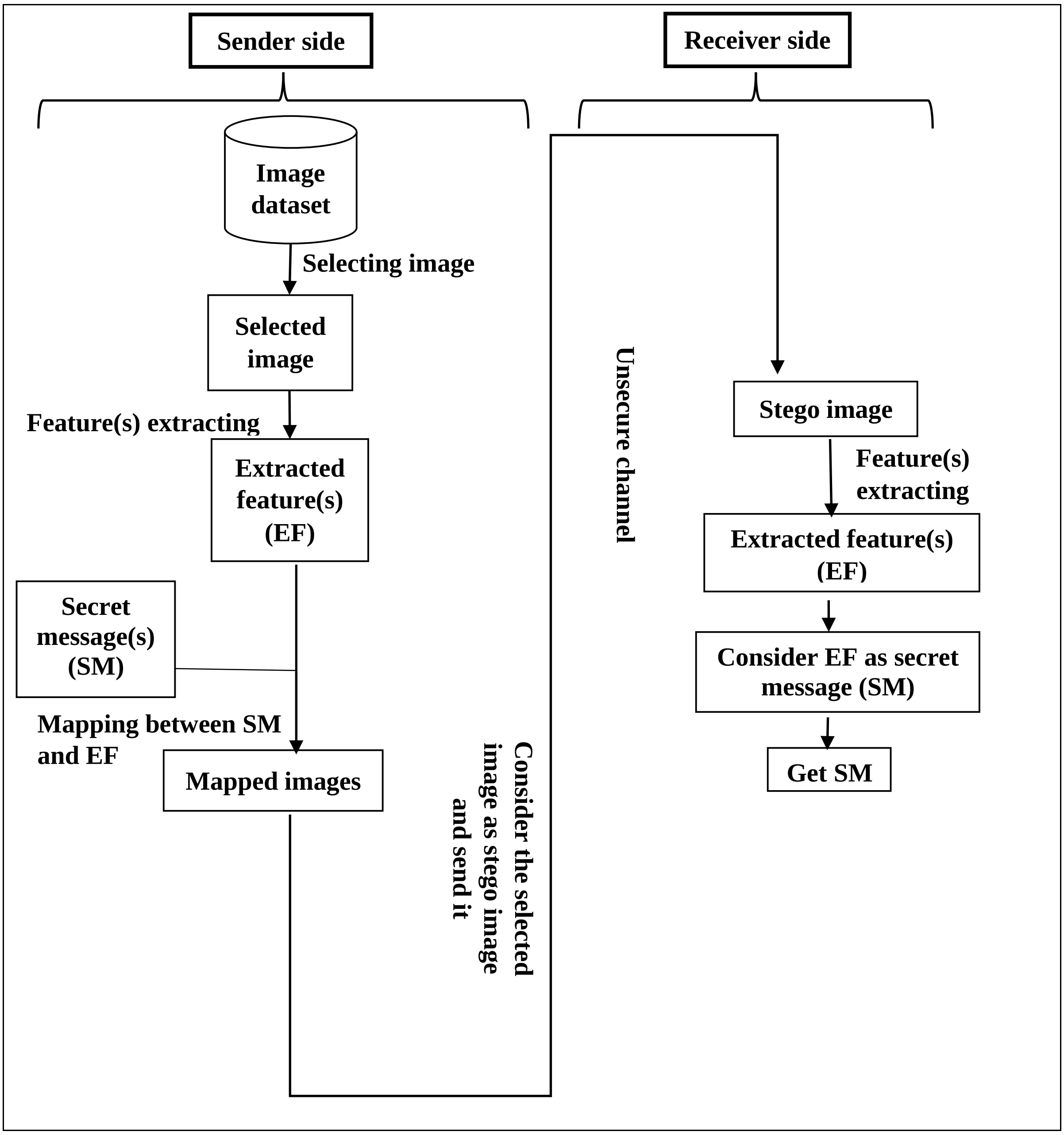


Figure (2.3): Block diagram of coverless image steganography

The major concern of coverless image steganography is how to find the cover images which already contain the secret data.

However, the major contributions of coverless image steganography are:

1) The covert communication can be realized without modifying the stego-image.

2) Because the stego-image has not been altered, the existing steganalysis tools cannot detect secret information.

The coverless image steganography is divided to several categorizes as follows:

2.3.2.1 Based on Robust Hashing

These methods produce a string of numbers for each image in the database using a powerful hashing algorithm. The robust technique is used to construct the sequence for each image in the set. A segment of the secret message is compared to the hash sequence. If they are equal, the part that was chosen serves as the secret message. The hash algorithm must produce a strong hash sequence that can withstand various attacks.

2.3.2.2 Based on BOW Algorithm

The bag-of-words model is used to extract the visual words from the image set, which are then utilized to conceal the textual information in the image. Additionally, established is the mapping between the keywords in the image and the visual words [53]. Then, each image is separated into several images. The values of the visual words are then determined in the histogram to represent the sub-image. Additionally, a relationship is established between the keywords in the image and the visual words. The text content in the image is then concealed using these sub-images.

2.3.2.3 Based on Generative Model

A framework for a coverless image information hiding strategy based on generative models is introduced for the first time in the method in [54]. The generative model database's hidden image is utilized to generate regular, independent images with a range of associations. The produced image is then delivered to the receiver and entered into the model database to produce a second image that is identical to the secret image. The parameters and data set are the same for the sender and the receiver. Transmit the typical standard image, which has no relation to the secret image, to achieve the same outcome as the secret image transmission.

2.3.2.4 Based on Partial Duplicates of a given Secret Image as Stego-Images

The secret color image can be sent using this way without any modifications being made [55]. Firstly, the large-scale image database is built by the generated database from this framework. Each image is thereafter divided into a number of independent, non-overlapping patches. The patch that is utilized to conceal the secret information is then identified using the label for each patch produced using the robust hashing algorithm. The hashing algorithm is used to determine the image's position as well. It's crucial to remember that the sender and receiver use the location data as a secret key to communicate. Each image patch's feature is extracted using the hierarchical BOW, and an inverted index structure is produced. The secret image is divided into numerous identical patches as the initial step in concealment. The partial-duplicate image that contains the same patches with the hidden image is then obtained for each patch using the inverted index files. Then, stego-images—a collection of partially duplicate images—is obtained. The receiver receives the images from the framework and extracts the hidden image's position information. The secret image can then be retrieved using the extracted patches.

2.4 Embedding Domain of Image Steganography

With traditional and coverless image steganography, there are two basic domains employed for embedding secret message, namely spatial and frequency domain.

2.4.1 Spatial Domain Image Steganography

Modifying the cover image pixel values in the spatial domain is the quickest and most straightforward method of image steganography. These methods use the cover image pixel intensity value to contain the secret message bits. The quantity of additive noise introduced into the image by these methods, which has a direct impact on the Peak Signal to Noise Ratio and the statistical characteristics of the image, is a severe negative. Although, the spatial-domain embedding techniques are more common due to its simplicity in the embedding and extraction procedures but it is with less strength[50].

2.4.2 Transform Domain Image Steganography

The image is initially converted to its frequency distribution in the frequency domain. In contrast to the spatial domain, where changes are made directly to pixel values, the spatial domain's pixel value changes are dealt with in frequency domain. Whatever needs to be processed is done in the frequency domain, and the resulting image is then given an inverse transform to produce the desired image. The transform domain techniques are considered immune to the operations of image processing and are also considered less vulnerable to steganalysis attacks. Examples of discrete frequency domain transformations include discrete cosine transforms (DCT), discrete Fourier transforms (DFT), discrete wavelet transforms (DWT), etc. [8].

In digital images, discrete wavelet transform utilized many media applications, such as digital image steganography and audio and video compression. The DWT of an image is calculated by passing it through a series of filters. In wavelet transform, the image is analyzed in three spatial directions: horizontal, vertical, and diagonal. The image is divided into four sub bands after us g DWT: LL (Low Low), LH (Low High), HL (High Low), and HH (High High). The output of the low pass filter gives the approximation coefficients; sub-band (LL), which are the high-scale, low frequency components whose content is the most important part of the signal. The output of the high pass filter gives the detail coefficients, sub-bands (LH, HL, and HH), which are the low-scale, high frequency components. This transformation is done using wavelet filters.

Among the characteristics that set DWT-based steganography approaches apart from other transform-based methods are more accurately to reflect the many features of the Human Visual System (HVS), as well as that the wavelet transform is a Multi-resolution method, that can repeat the operation several times on LL sub band in the level based on the application being utilized [52]. Figure (2.4) shows the analysis of DWT for image.

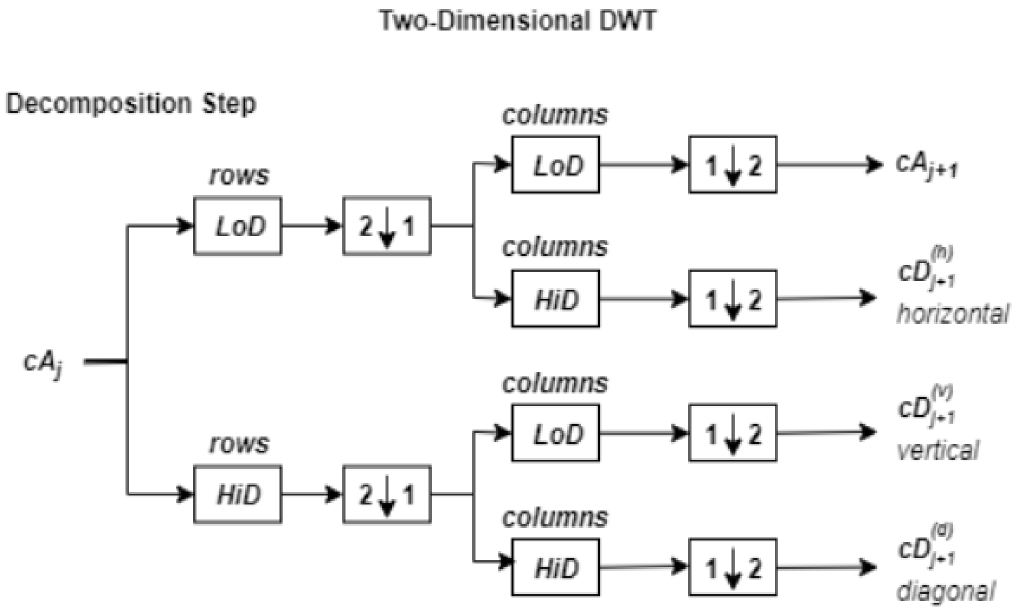


Figure (2.4): DWT's Image Analysis [52]

Where:

- $\boxed{2\downarrow 1}$ — Down sample columns: keep the even-indexed columns.
- $\boxed{1\downarrow 2}$ — Down sample rows: keep the even-indexed rows.
- $\overset{rows}{\boxed{X}}$ — Convolve with filter *X* the rows of the entry.
- $\overset{columns}{\boxed{X}}$— Convolve with filter *X* the columns of the entry.

2.5 Requirements of Image Steganography

Steganography techniques often include embedding and extracting hidden messages. Before applying or carrying out the steganography technique, it's important to keep requirements of image steganography in mind. The strengths and limitations of each technique depend on these requirements. Each requirement in steganography depends on how well it may be applied. They are capacity, robustness, and security. The increasing of one requirement affect other requirements. They tradeoff between them as shown in Figure (2.5).

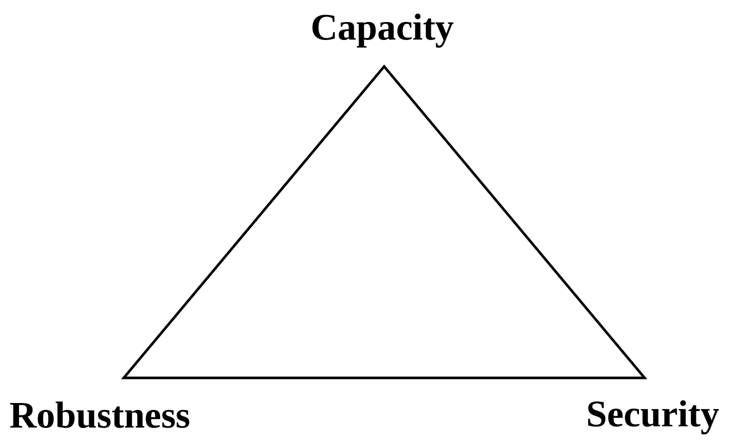


Figure (2.5): Trade-off Triangle between Basic Requirements [56]

1. Capacity

It is the first parameter that reflects the most information that may be effectively buried and retrieved. Compared to watermarking, which just needs a little bit of copyright information embedded, since steganography is used to conceal communication, a high embedding capacity is necessary [57]. Capacity is sometimes expressed in bits per pixel, refers to the typical number of bits hidden inside each pixel of the cover image. The number of hidden messages that can be transmitted through the medium is increased with increasing the amount of bits that can be hidden in the cover image.

2. Robustness

The second parameter assesses the Steganographic technique's is the resistance to attempts for removing or changing the concealed information because when a stego image is connected through reliable systems, an active warden can see and alter the image in an effort to get rid of any hidden information.

Cropping, rotating, data compression and image filtering are an example of image manipulation that may the stego image is exposed before it gets to its destination. These actions can destroy the concealed message depending on how the message is embedded. Therefore, Steganographic techniques should be capable of withstanding both malicious and accidental alterations to the image.

3. **Security**

Security is the third parameter that is seen to be crucial for steganography because the technique should be able to withstand steganalysis tools [58]. A steganography technique is regarded as secure if the classification tool's accuracy value is random guessing, resulting in difficulty for an attacker to decipher the secret message from the cover medium, Security is dependent on the secret key and algorithm knowledge.

2.6 Coverless VS Traditional Image Steganography [48]

In this section, the coverless steganography is contrasted with conventional steganography according to their advantages and disadvantages, focusing mostly on its benefits and drawbacks.

1. Coverless Image Steganography

- **Advantages:** The biggest benefit of coverless images steganography is that can mostly resist the current steganalysis tools and outperforms traditional steganography techniques.
- **Disadvantages:** Since coverless image steganography relies on direct mapping of secret information to hash sequences, one of its biggest drawbacks is that the amount of information that can be concealed depends on the length of the image hash. The image database must also be increased at the same time, even though longer hash sequences can be constructed to conceal more secret information. Otherwise, security decreases as capacity increases.

2. Traditional Image Steganography

- **Advantages:** since the traditional methods of image steganography apply on modification of the image pixels for embedding the sensitive information, its capacity is high compared with coverless image steganography.
- **Disadvantages:** The traditional methods have less security than coverless image steganography because it is exposed to steganalysis tools.

So, the biggest challenge in coverless image steganography is how to increase the capacity of the cover image so it can take the most of secret data because the searching technique about a large number of natural images that contain these data is a hard task and consumption of time, in the meantime it should maintain other requirements as robustness and security for getting the satisfactory result of steganography.

2.7 Block Dividing Based Coverless Image Steganography

Although the fact that coverless steganography is offered numerous benefits over traditional steganography, it still has limited capacity. Meanwhile, capacity has emerged as a crucial evaluation metric. The idea behind dividing the cover image into number of vertical and the horizontal blocks with specific size and extract the feature from each block as described in pervious part for increasing the ability of hiding a large amount of secret data and attempt to hide the complete secret data in one cover image. Figure (2.6) shows that the image is divided into blocks and features which are extracted from each block. The secret message already goes through a partitioning into small segments of specific length and the mapping relationship occur between each segment and each divided block [55].

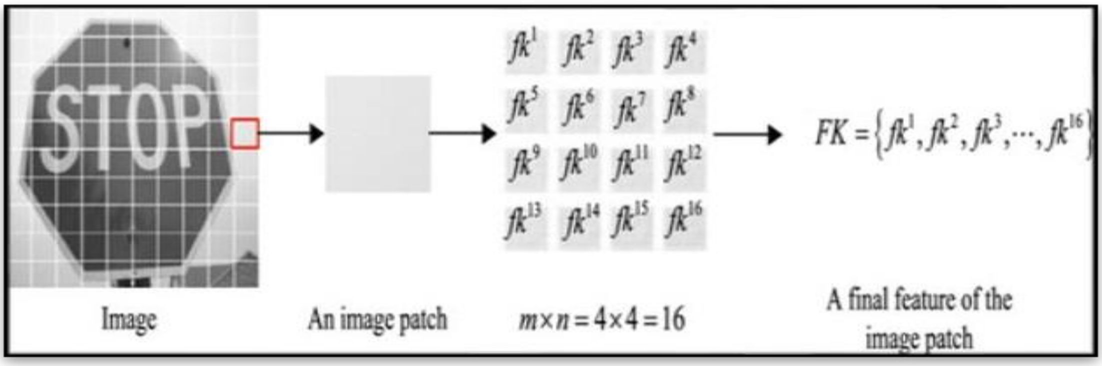

STOP
fk^1 fk^2 fk^3 fk^4
fk^5 fk^6 fk^7 fk^8
fk^9 fk^{10} fk^{11} fk^{12}
fk^{13} fk^{14} fk^{15} fk^{16}
$FK = \{fk^1, fk^2, fk^3, \cdots, fk^{16}\}$
Image
An image patch
$m \times n = 4 \times 4 = 16$
A final feature of the image patch

Figure (2.6): Extracting the final feature from an image patch [55]

But the challenge here is how to find set of images that contain all the features of the secret information. However, the major contributions of block based coverless image steganography are [31]:

1. The hiding capacity will be increased.
2. The bandwidth required to transmit the secret message will be reduced.
3. Avoiding the preprocessing of a large number of images in the same way.

4. The extensive image searching and indexing will be reduced.
5. No large image database is required.

2.8 Applications of Image Steganography

Since data privacy and secrecy become more and more of a concern as Internet communication technologies improve, steganography is employed in a range of fields. In recent years, numerous applications have used steganography to conceal their data.

1. As an illustration, image search engines that examine the network traffic of specific clients in order to insert a unique identifier, smart identity card (ID) applications that turn a number into an image, and smart identity card (ID) applications where personal data is stored on a smart card are all examples. Information is hidden in an image [59].

2. Digital steganography has compelling qualities that make it appropriate for real-time applications. Numerous steganography techniques have been created in order to adapt Voice over IP (VoIP) services. Due to the prevalence of IP telephony, VoIP steganography has grown [60]. Short VoIP talks also don't provide listeners enough time to spot any irregularities because of the message they contain [61]. Using VoIP steganography is different from using a regular file type, such as a text, image, or audio file. It is a real-time tactic that employs VoIP signals to conceal the existence of secret information in real-time communication [59].

3. Using of digital steganography inside medical information systems has been crucial for protecting medical information systems (MIS). The fundamental use of steganography in medical imaging systems was presented as a remedy for the authentication issue, which occurs occasionally when the link between the patient's data and their image is lost[62]. Therefore, steganography is used to hide patient data and diagnosis reports within their medical photographs. You can find a survey on the impact of information security and confidentiality while creating telemedicine applications [63][64].

4.Businesses engage with significant transactions that require confidentiality, hence commercial security has recently become crucial to national security. Using steganography techniques, every company must protect its data from possible attackers[65].

2.9 Attacks on Coverless Image Steganography[66]

Several elements, including a transmission error or noise, can influence the transmission of an image. The destruction of the secret data is one of the most frequent attacks that take place during the transmission of images. Understanding this problem is crucial for creating a more reliable and secure coverless steganography method. There are several kinds of coverless image steganography attacks fall:

1. Noise attacks: refer to deliberate modifications or additions of unwanted disturbances to an image with the intention of compromising its integrity or quality. These attacks aim to disrupt the visual information contained in an image, making it harder to interpret or manipulate accurately. This sort of noise attack uses varied densities of salt-and-pepper, speckle, and Gaussian noises to attack a stego image.

2. Compression attacks: JPEG compression is a widely used method for reducing the file size of images. However, the compression process introduces artifacts that degrade image quality. Deliberately applying JPEG compression with high compression ratios can simulate noise attacks by introducing blocking artifacts, blurring, and loss of fine details

3. Filtering attacks: These attacks typically aim to deceive or manipulate the content of an image for malicious purposes by appling a specific mask filter with specefic window size.For this kind, a Gaussian low pass filter, an averaging filter, and a median filter with diifrent window sizes are used to filter the stego image.

4. Geometic attacks: refer to a class of attacks that exploit vulnerabilities related to geometric properties such as the size or the shape of the image or spatial relationships within a system or algorithm thus it is consider the hardest kinds of attacks.Example of these attacks are rotaion attacks and resizing attacks.

5.Brightness and sharpness attacks: These attacks are typically aimed at deceiving viewers or manipulating the visual content for various purposes. Brightness attacks involve altering the brightness or exposure levels of an image to create misleading or deceptive visual representations while Sharpness attacks involve modifying the sharpness or focus of an image or video to alter its visual quality or impact.

2.10 Evaluation Metrics of coverless Image Steganography Algorithm

The effectiveness and performance of the coverless steganography system must be evaluated throughout the design. Measurement of the extracted secret message's capacity for testing the hiding capacity of the cover image and robustness in order to assess the coverless steganography system are important for proving the effectiveness of the system.

2.10.1 Capacity Measures

To measure the Capacity of the proposed algorithm, the embedding capacity measure is used to calculate according to the number of divided blocks, The Equation (2.1) illustrates the total embedding capability of the hashing method[67].

$$TC = BPB \times EP \qquad ,\ldots. (2.2)$$

Where TC denotes the overall embedding capacity, BPB denotes bit per block and EP is the number of divided blocks.

2.10.2 Robustness Measures

The metrics are utilized to assess the robustness of the suggested methods are: Bit Error Rate(BER) and the Extraction Accuracy(RC) are utilized to assess the robustness of the suggested methods. Bit error rate is used to calculate the error rate between the original and extracted secret information[31] and Extraction Accuracy measures The similarity rate between the retrieved secret information and the original ones.[68].

BER is calculated as follows:

$$BER = \frac{\sum_{i=1}^{n} MS_{cg}(i) \otimes EMS_{cg}(i)}{n} \qquad \dots (2.3)$$

Where MS_{cg} the original secret message,EMS_{cg} is the extracted secret message and n is the number of secret message bits.

While RC is calculated as follows:

$$RC = \frac{\sum_{cg=1}^{n} f(EMS_{cg})}{n} \qquad \dots (2.4)$$

Where

$$f(EMS_{cg}) = \begin{cases} 1 & if\ EMS_{cg} = MS_{cg} \\ 0 & otherwise \end{cases}$$

It is hard to completely prevent content damage during transmission, including image noise, JPEG compression, rescaling, brightness alteration, and contrast shift. so The stego image used to represent the secret data must be robust to these attacks. These variables need to be endure the data gathered from the image. In other words, the hash algorithm is protected against these kinds of attacks.

2.11 Encryption

To preserve the privacy of sensitive data, many companies use encryption. By using an algorithm, this technique modifies data included in a file. The data is shielded from unwanted access [69]. Encrypted text is the end product of a cryptographic algorithm. Different encryption techniques exist, including symmetric and asymmetric encryption. A public key is utilized when using symmetric type [70], but a private key is used when using an asymmetric type.

Many businesses have been employing chaotic encryption as an alternative to the conventional technique despite of to the growing variety of encryption algorithms being introduced [71] [72][73]:

2.11.1 chaotic Encryption

Chaotic encryption is a type of encryption where chaos theory is used as the basis for creating algorithms to encrypt data. In this method of encryption, the plaintext is processed using chaotic pseudo-random sequences and a secret key. These sequences enhance the complexity of the encryption process and make it more resistant to attacks. The use of chaotic theory as a basis of encryption can also provide a high level of randomness and unpredictability, which can further strengthen the security of data.

Properties of Chaotic Encryption

1. Deterministic system: Indicates that some deterministic mathematical formulae control chaotic processes [74].

2. A periodic long-term activity: A chaotic system will not behave properly if its tracks do not follow a stable path. This means that the system tracks will have limited predictability [75].

3. Sensitivity to starting conditions and parameters: Large changes in the input values can be made to chaotic functions without having an impact on the behavior of the system, which is one of their key benefits. This characteristic is frequently applied in information-hiding strategies [76].

Several chaotic maps are used to create the chaos streams. These latter ones are regarded as a nonlinear, dynamic system that produces random sequences employed in several applications. A logistic map, tent map, quadratic map, Bernoulli map, and others are examples of chaotic maps [77]. In general, equation(2.5) can be used to define any chaotic map.

$$x_{n+1} = f(x_n) \quad ,n = 1,2, \quad ....n(2.5)$$

where x_n is referred to as the iteration n's state,The function f maps the state x_{n-1} to the following state x_n.

In this thesis, a chaotic system is used for encrypting the auxiliary information in order to increase the security by encrypting them. The logistic map will be used to create randomized sequential keys for encryption process. Equation (2.6) is used to define the logistic map

$$x_{n+1} = r - (x_n)2 \qquad , \qquad \dots (2.6)$$

Where n is the number of iterations, r denotes the chaos parameter, and xn denotes a number between 0 and 1.

2.11.2 Encryption Evaluation Metrics

The original data's values are altered when an encryption technique is used. The discrepancy between the encrypted and unencrypted data should be minimized as a result of these modifications [71]. A key function of an encryption algorithm is to ensure that the data is independent of the original while also minimizing the difference between the original and encrypted versions. The effectiveness of the encryption algorithm will be evaluated using the metrics listed below:

2.11.2.1 Entropy

The information entropy measures the randomness of a system. With rising entropy, a system's level of unpredictability rises. Equation (2.7) can be used to define the information entropy H of a discrete random variable X with possible values of "x1, x2,..., xn," where p(.) is the X's probability mass function.

$$H(S) = -\sum_{i=0}^{N-1} p(s_i)\ \log_2 p(s_i) \quad \dots\ (2.7)$$

2.11.2.2 Correlation Coefficient (CC)

An essential statistical metric is the correlation coefficient (CC). Its value illustrates how the plain and encrypted texts differ from one another. When the correlation coefficient value is close to 1, it indicates that there is a strong correlation between the two photos. As a result, the encryption system will be subject to attacks [78]. The CC is assessed using equation (2.8).

$$r = \frac{\sum_m \sum_n (A_{mn} - A^{-})(B_{mn} - B^{-})}{\sqrt{(\sum_m \sum_n (A_{mn} - A^{-})^2 (\sum_m \sum_n (B_{mn} - B^{-})^2}} \quad \dots (2.8)$$

Where A' and B' is the average of original data and encryption data respectively.

2.11.2.3 Avalanche Effect (AE)

The Avalanche Effect explains how changes to the plaintext affect the cipher text for a strong cipher. The method produces a completely different output when the input is merely slightly changed. The effectiveness of diffusion is evaluated using this metric. A strong encryption algorithm should be capable of causing the output bits to change significantly following a modest change in the key or the plaintext should cause the cipher text to change significantly (approximately half of the output bits must fluctuate) [79]. Determining the value of the (AE) is done According to equation (2.9).

$$AE = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}[(C(i,j) * C'(i,j)^2]}{M * N} \qquad \ldots.(2.9)$$

2.11.2.4 National Institute of Standards and Technology (NIST) Tests

The NIST tests describe the quality of random number generators that assessed. These tests examine different byte sequence structure elements. These evaluations are frequently used as a standard for identifying compressed and encrypted information for evaluating the randomness of the encryption algorithm[12]. Each test examines a single aspect of the sequence and then uses a test-specific decision rule to decide if the analysis's findings support randomness or not [81].

Due to their widespread acceptance and application in the field of randomization testing[82], so these tests are used in the evaluation.

- **Longest Run of Ones in a Block:** Check to see if the length of the longest run of ones in the sequence under test is in line with the length of the longest run of ones that would be predicted in a random sequence.

- **Binary Matrix Rank Test:** Verify the original sequence's fixed-length substrings for linear dependencies. Keep in mind that this test is part of the DIEHARD suite of tests as well.

- **Non-Overlapping Template Matching Test:** Determine how frequently a specific non-periodic (aperiodic) pattern appears by counting the occurrences of predetermined target strings. The 68-bit aperiodic pattern 0 1 1 1 1 1 is an example.

- **Overlapping Template Matching Test:** This test, like the last one, checks for instances of pre-defined target strings. This test shifts the test window by one byte when a match is made, whereas the prior test moved the test window to the end of the matching sequence.

- **Linear Complexity Test:** This measures the linear feedback shift register's length (LFSR). A sequence's linear complexity is determined by how long the smallest linear feedback shift register (LFSR) produces the sequence. Longer LFSR's are a characteristic of random sequences. A too-short LFSR suggests non-randomness.

- **Random Excursions Test:** Test the number of cycles in a cumulative sum random walk that contains exactly K visits. The goal of this test is to ascertain whether the amount of trips to a specific state during a cycle differs from what would be predicted by a random sequence.

- **Random Excursions Variant:** determine how many times a specific state is visited overall in a cumulative sum random walk. This test looks for variations from the predicted frequency of visits to different states in a random walk.

Chapter Three

The proposed Image Blocks Features Based Coverless Steganography System(IBFBCSS)

Chapter Three
The proposed Image Blocks Features Based Coverless Steganography System(IBFBCSS)

3.1 Introduction

The objective behind coverless steganography is to choose cover images with features that convey secret information as stego-images, in contrast to typical steganography procedures. By splitting an image into many blocks and employing a strong hashing technique, it is possible to map relationships between visual attributes and secret message segments. This chapter explains the proposed coverless image steganography technique based on block division for achieving better capacity; this chapter will provide several of the algorithms, procedures, and diagrams that are employed in the proposed system.

3.2 The proposed Image Blocks Features Based Coverless Steganography System(IBFBCSS*)*

This section provides a detailed explanation of the proposed coverless image approach. Figure (3.1) shows the main block diagram of the proposed Image Blocks Features Based Coverless Steganography System(IBFBCSS)**.**Two procedures include the embedding procedure in the sender side and the extracting procedure in the receiver side up the proposed methodology.

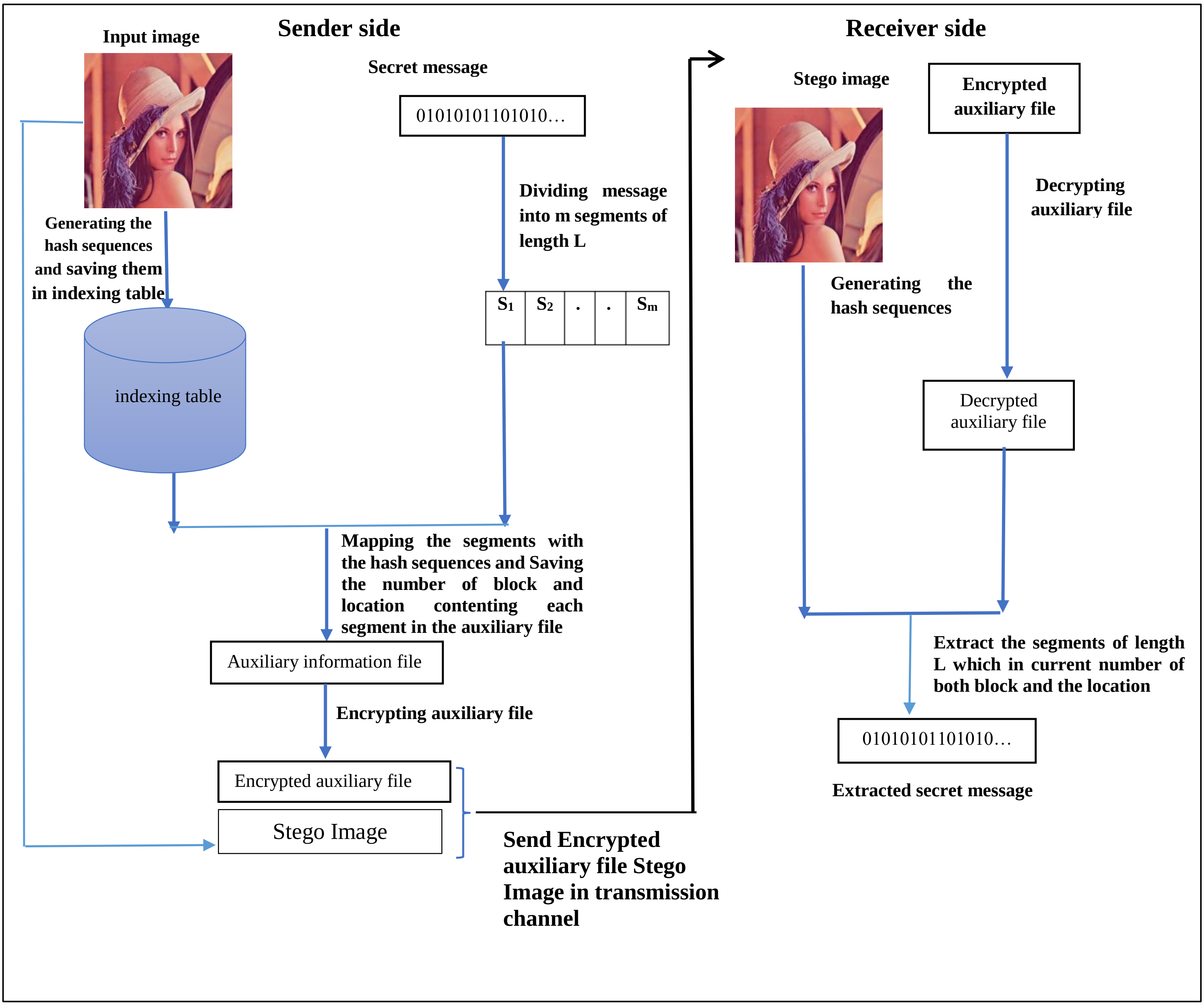

Sender side
Input image
Secret message
01010101101010…
Dividing message into m segments of length L
S1 S2 . . Sm
Generating the hash sequences and saving them in indexing table
indexing table
Mapping the segments with the hash sequences and Saving the number of block and location contenting each segment in the auxiliary file
Auxiliary information file
Encrypting auxiliary file
Encrypted auxiliary file
Stego Image
Send Encrypted auxiliary file Stego Image in transmission channel
Receiver side
Stego image
Encrypted auxiliary file
Decrypting auxiliary file
Generating the hash sequences
Decrypted auxiliary file
Extract the segments of length L which in current number of both block and the location
01010101101010…
Extracted secret message

Figure (3.1): Block diagram of the proposed system

3.2.1 Processes on the Sender Side

On the sender's side, a number of processes are carried out as described in Algorithm (3.1):

Algorithm (3.1): Embedding Process

```
  Input: Cover Image (CI), Secret Data (SD)
 Output: Stego Image (SI), Encrypted Auxiliary File (EAF)
Begin
    1. Split SD into segments with length 8bits.
    2. Divide CI into non overlapping blocks.
    3. Generate Hash sequences of CI blocks and save in dataset.
    4. Build Hash Table of hash sequences for all blocks of CI
    5. For i=1, i<length (SD /8)
    6. Map secret data segment SD(i) with sequence of index Hash Table (i)
    7. Save matched block number, location number in Auxiliary file
    8.  End For
    9. Encrypt Auxiliary file using algorithm (3.4).
    10.Get EAF
    11.Send SI, EAF
End
```

Each process's specifics are described in the sections that follow:

3.2.1.1 Secret Data Splitting

A given secret data (SD) that needs to be hidden should be divided into *Em* segments as follows:

$$Em = \begin{cases} \frac{N}{Nseg} & if\ N\%Nseg = 0 \\ \frac{N+Coz}{Nseg} & otherwise \end{cases} \qquad (3.1)$$

Where (N) denotes the total length of the secret data, (Nseg) denotes the total length of the segment. If N does not multiple Nseg; Zeroes are added to the final piece of secret information and *Coz* denote the total number of zeroes that added to the length of the secret data.

3.2.1.2 Embedding with a Image Blocks Features Based Coverless Steganography(IBFBCS)

As shown in Figure (3.1), the embedding process consists of several stages.

The following sections go into detail about each stage:

A. Hash Sequence Generation

This stage consists of three steps that include choosing cover image, binary hash sequences calculation, and building an indexing table.

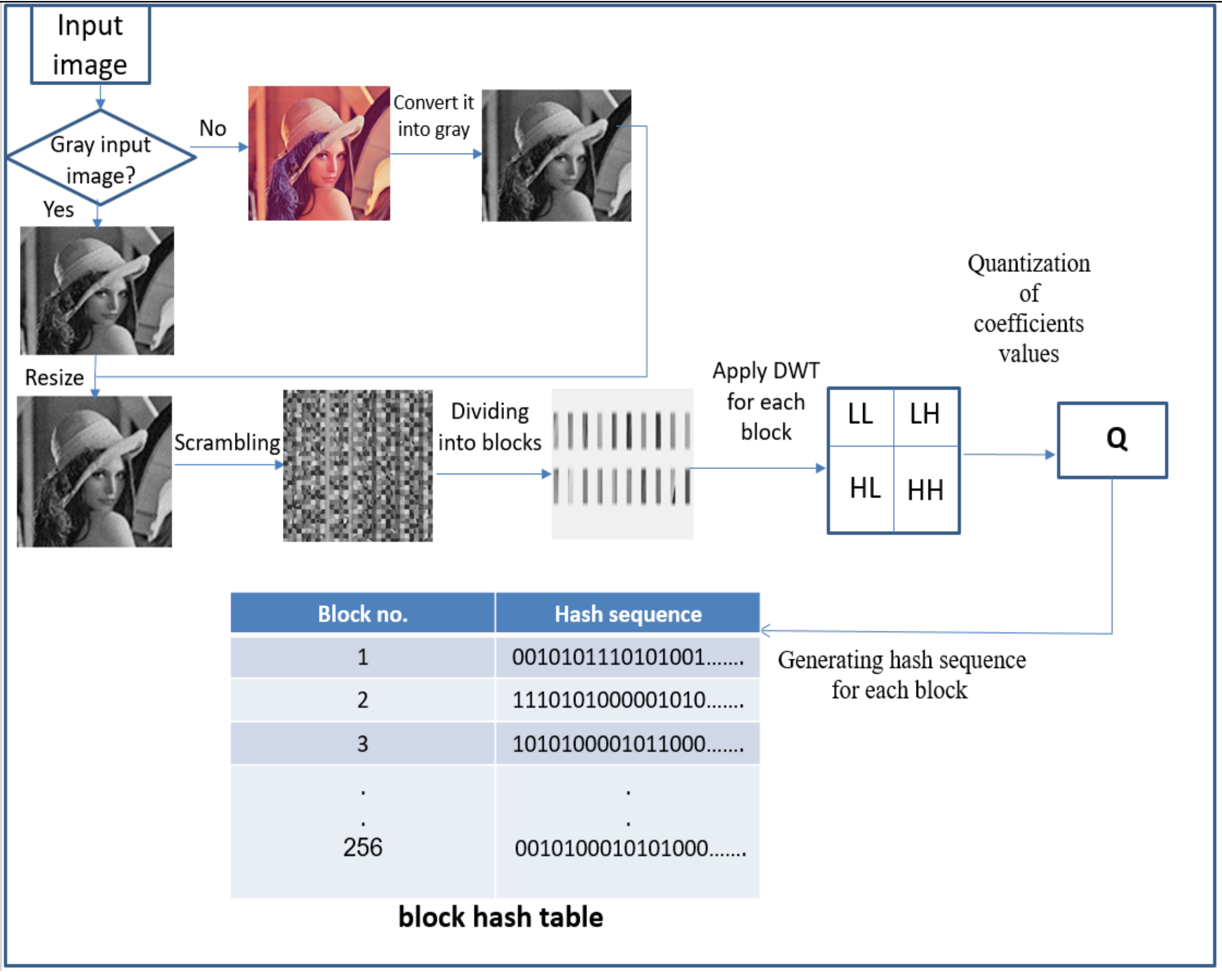
1- Choosing the Cover Image

To embed the secret data using the proposed coverless image steganography, one way is to search for image that already have all the information, such that any secret data can embed on it, which is used for sending the private data. Divide the selected image into blocks and the features of these blocks are extracted and generate hash sequences from them by using an efficient hash algorithm that can resist image processing attacks. The input image to the system may be gray or color image.

2- Binary Hash Sequence Calculation

Hash code is a fixed-length binary sequence, which is calculated from an image block based on its local content. Each image block can be expressed by a hash code, which can then be mapped to a specific part in the secret information. In this work, a hash sequence is generated from gray scale image.Therefore, if the input image is color it will converted to gray scale image.Also, the input image is normalize to size (512×512) pixels to guarantee that the images of different sizes share the same feature length. The hash generating process is done in the frequency domain. When creating a hash sequence in this domain, several steps are performed as shown in Algorithm (3.2). Using this domain, the Haar wavelet transform is used to construct hashes from the image coefficient.

The hash generating steps are illustrated in the Figure (3.2).



Block no.	Hash sequence
1	0010101110101001…….
2	1110101000001010…….
3	1010100001011000…….
.	.
.	.
256	0010100010101000…….

block hash table

Figure (3.2): Diagram of Hash Sequence Generation

Algorithm (3.2): Hash Sequence Generation

```
Input: Cover Image (CI)
Output: Hash Sequences (SigmHash)
 Begin:
    1. Convert CI to gray scale if it is color scale.
    2. Resize CI to 512×512
    3. Scrambling CI using Algorithm (3.3)
    4. Divide the scrambled CI into non-overlapping blocks of (32×32) pixels.
    5. Perform Hear wavelet transform on all blocks.
    6. Quantize coefficients values for four sub bands(LL,LH,HL,HH) of all
       blocks according to equation (3.3).
    7. For i=1, i<Bno          // Bno is the number of blocks
    8. Generate SigmHash using equation (3.4).
    9. Save the number of block, location with its hash sequence in lookup table
    10. End For
   End
```

The cover image is scrambled to reduce the relationship between pixels, increasing the cover image's randomness and robustness. This procedure is carried out by employing a key (position key) to build a scrambled image based on the following one to- one mapping equation:

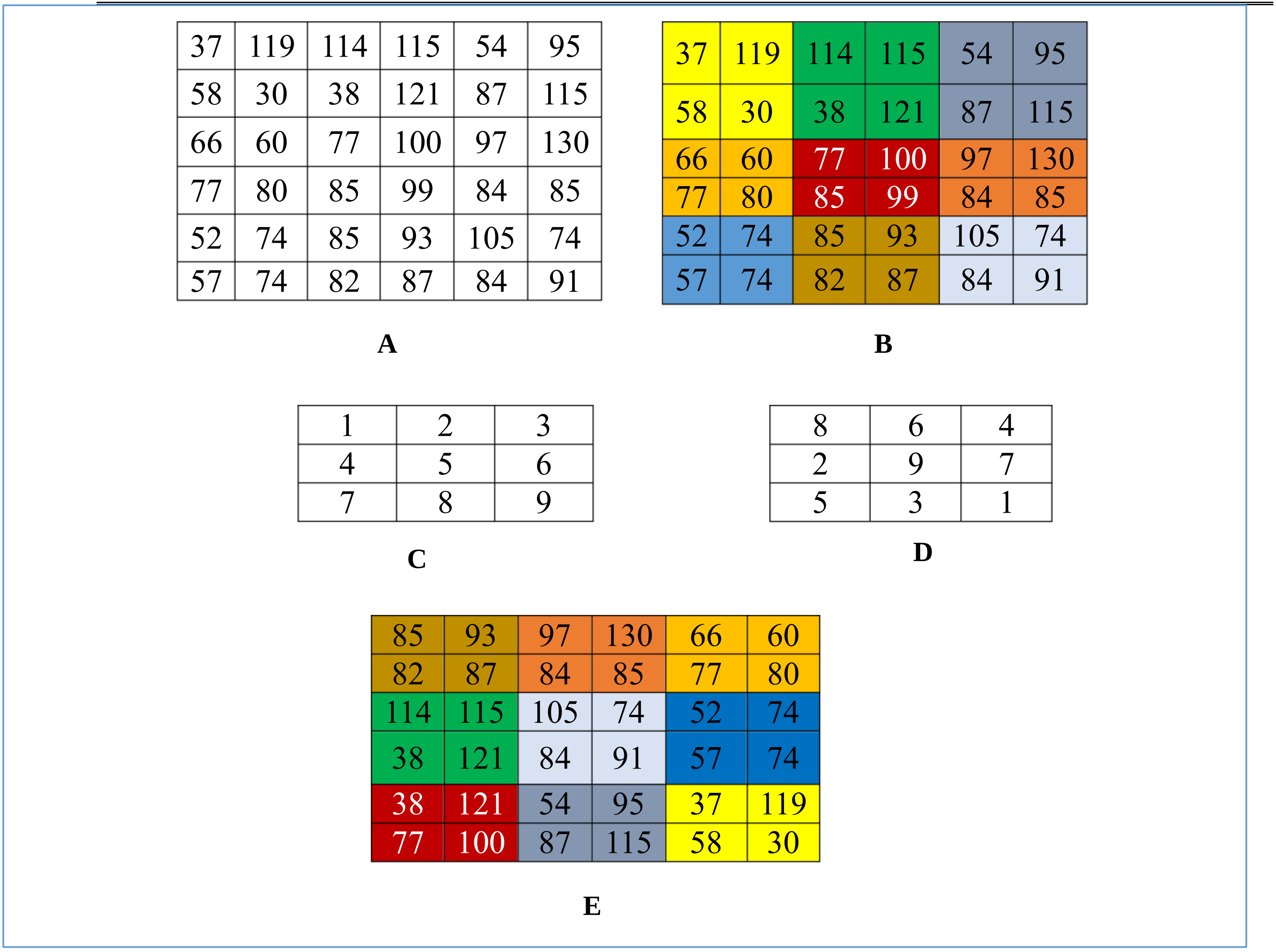
$$\mathrm{X}' = [\mathrm{F}(\mathrm{X}) = (\mathrm{K} * \mathrm{X}) mod\ N] + 1 \qquad \ldots (3.2)$$

Where: X, X' (∈[0, N -1]) is the block number, k (a prime number and K ∈ Z – { factors of N }),it is a secret key, and N(∈ Z– {0}) is the total number of blocks in the image of size N =$2^n \times 2^n$, and n ∈ N. A lookup table is formed by using the following Algorithm (3.3) to register the mapping address of each block in the image for using it in changing the positions of the blocks.

Algorithm (3.3): Image Scrambling

```
Input: Cover Image (CI)
Output: Scrambled- Image (SI)
Begin
   1. Partition CI into non-overlapping blocks of 16 × 16 pixels.
   2. Allocate a unique nonnegative integer X ∈ {0, 1, 2, . . . N -1}to each
      block from the top left in row major order, N = $2^{n-1} \times 2^{n-1}$.
   3. Select a prime number k ∈ [1, N – 1].
   4. For each block number X, obtain $\mathrm{X}'$ and it's mapping block by using
      equation (3.2). All the $\mathrm{X}'$ s formed the SI.
   5. Return SI
End
```

For example, a sub image of size 6× 6 is suggested as the original image. The original image along with its suggesting block index matrix, lookup table generated using equation (3.2) and key value equal to (7). This operation is shown in Figure (3.3).



37	119	114	115	54	95
58	30	38	121	87	115
66	60	77	100	97	130
77	80	85	99	84	85
52	74	85	93	105	74
57	74	82	87	84	91

A

37	119	114	115	54	95
58	30	38	121	87	115
66	60	77	100	97	130
77	80	85	99	84	85
52	74	85	93	105	74
57	74	82	87	84	91

B

1	2	3
4	5	6
7	8	9

C

8	6	4
2	9	7
5	3	1

D

85	93	97	130	66	60
82	87	84	85	77	80
114	115	105	74	52	74
38	121	84	91	57	74
38	121	54	95	37	119
77	100	87	115	58	30

E

Figure (3.3): Image scrambling
A) The sub image matrix B) Non overlapping blocks of (2x2) pixels C) The sub image block matrix D) Lookup table E) Scrambled image

Hash generation is done frequency domain. With this domain, several phases can be completed during the production of a hash sequence. The scrambled image is divided into Bw ×Bh non-overlapping segment. Two levels Discrete Haar wavelet transform is applied on each segment (Seg) to obtain two dimensional array (Seg_T) contains approximation and details four sub bands (LL, LH, HL, HH). Suppose a scrambled image is divided into segment with size 4 ×4 as shown in Figure (3.4a) and the obtained transform array (Seg_T) will be taken in the hash sequence generating as shown in Figure (3.4b). To increase the robustness of the generated hash, each coefficient in (Seg_T) is quantize according to the following:

$\text{Seg}_{Tq}(i,j) = \frac{\text{Seg}_{T}(i,j)}{2}$,… (3.3) 1 =< i<(B$_w$, 1 =<j<B$_h$)

Where Seg $_{Tq}$ represent the quantized segment array.

The result of applying equation (3.3) on Seg $_{Tq}$ in the Figure (3.4a) is depicted in Figure (3.4c). The two dimensions 2D Seg $_{Tq}$ with size (B$_w$ ×B$_h$) is converted to 1D vector V_Seg $_{Tq}$with length (B$_w$ ×B$_{h)}$ as shown in Figure (3.5d). Finally, a binary hash sequence with length ((B$_w$ ×B$_h$)-1) is generated for each block by using the following equation:

$$H_{(I)}= \begin{cases} 1 \text{ if } V\_\text{Seg}_{Tq}\text{ (I)}> V\_\text{Seg}_{Tq}\text{ (i+1) where } 1 =< i<(B_w\times B_h) \\ 0 \quad \text{otherwise} \end{cases} \quad , \dots (3.4)$$

The generated hash sequence for this example according to the equation (3.4) by overlapping way is shown in Figure (3.4E).

Figure (3.4) clarify an example for generating a hash sequences.

85	93	97	130
82	87	84	85
114	115	105	74
38	121	84	91

A

371.2500	4.5000	-6.5000	-1.5000
0.2500	35.0000	-42.0000	41.0000
-3.7500	29.0000	-17.0000	-16.0000
-20.7500	2.0000	12.0000	19.0000

B

185.625	2.25	-3.25	-0.75
0.125	17.5	-21	20.5
-1.875	14.5	-8.5	-8
-10.375	1	6	9.5

C

185.625	0.125	-1.875	-10.375	2.25	17.5	14.5	1	-3.25	-21

-8.5	6	-0.75	20.5	-8	9.5

D

111001111001010

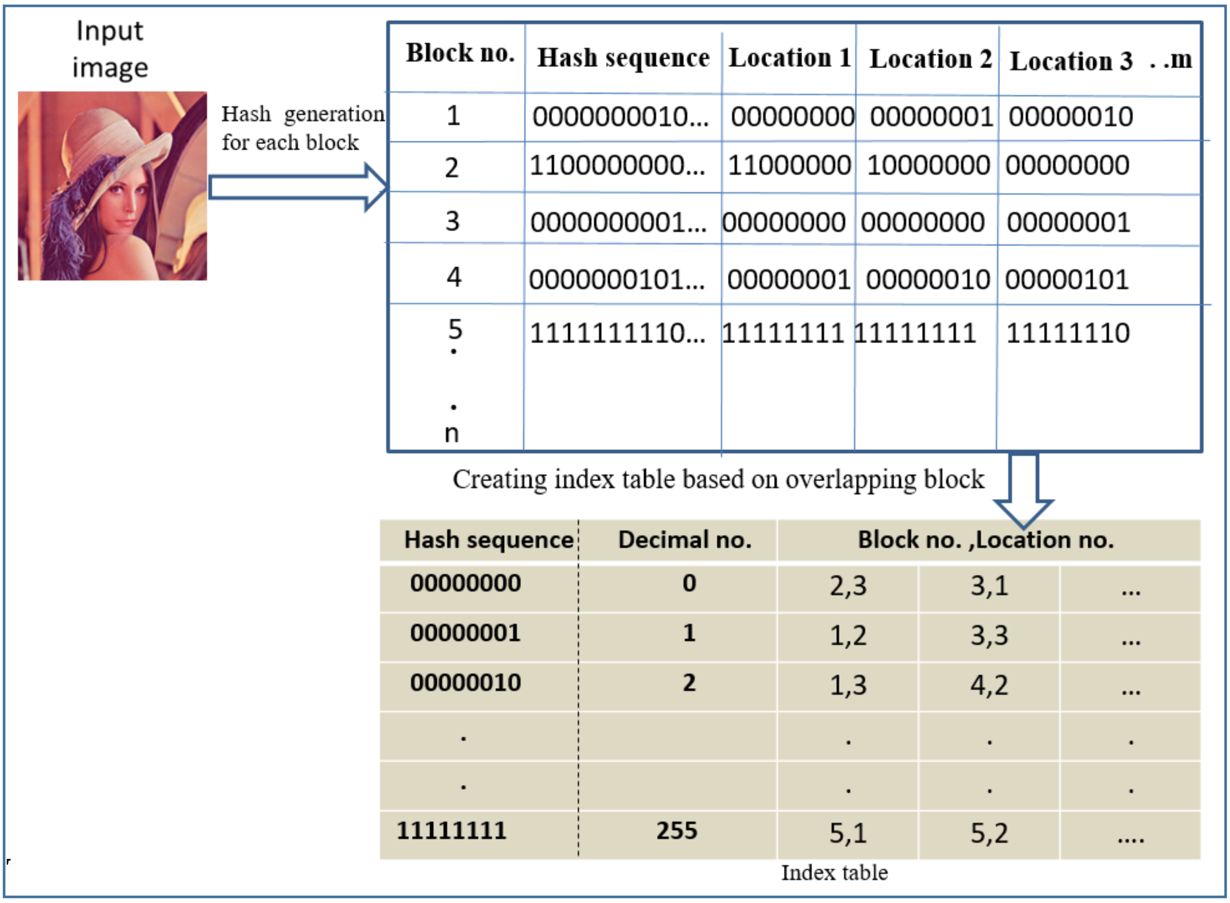
E

Figure (3.4): Hash sequence generation:
A) Image segment B) Transformed image segment C) Quantized transformed image segment (Seg$_{Tq}$)
D) Conversion 2D quantized segment into 1D V_Seg $_{Tq}$ E) Generated Hash sequence

All generated hash sequence for all blocks is saved in a block hash table (BHT) its row represents block number while its columns represent the hash sequence bits for specific block number as shown in Figure (3.2).

B. Building the Index Table using Block Indexing

Each block in the cover image have nonspecific number of bits depending on the block size, the searching operation for each segment in a block hash table (BHT) about the matched sequence take a long time, for speeding up the time, an inverted table has been building for each sequence that have the corresponding block and location number that matched for it. All of the blocks are indexed in the database according to their hash sequence. Then, for all of the hash sequences, make a query table, which is an inverted index structure that contains entries to the greatest extent possible Hash sequences of 8 bits. Each value leads to a set of the entire blocks IXDs that share the same hash sequence. Assume that block A's hash sequence is [0,0,0,0,0,0,0,1] and that its IXD is IXD(A), and that IXD(A) belongs to the list pointed by the entry 0,0,0,0,0,0,0,1as shown in Figure (3.5).


Input image
Hash generation for each block
Creating index table based on overlapping block
Index table

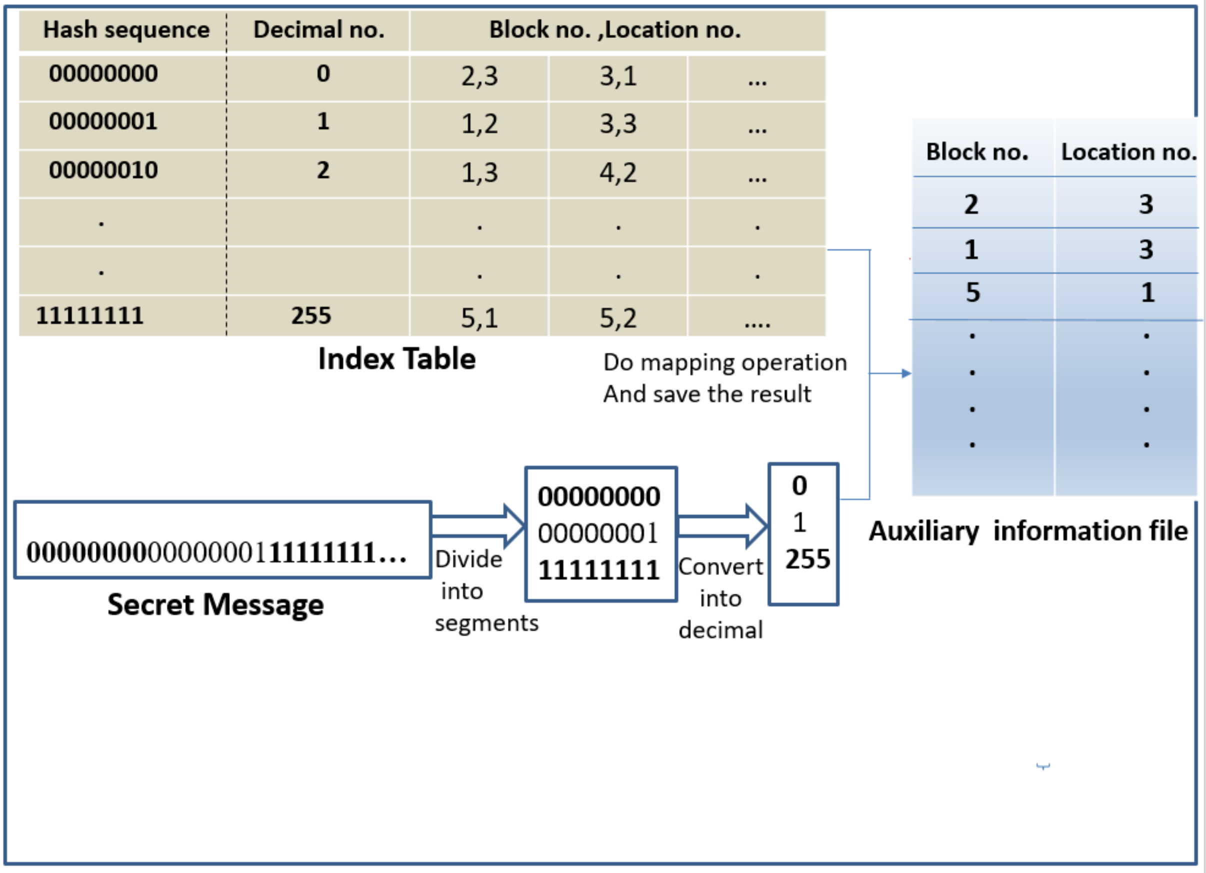
Block no.	Hash sequence	Location 1	Location 2	Location 3 . .m
1	0000000010...	00000000	00000001	00000010
2	1100000000...	11000000	10000000	00000000
3	0000000001...	00000000	00000000	00000001
4	0000000101...	00000001	00000010	00000101
5	1111111110...	11111111	11111111	11111110
.				
.				
n				

Hash sequence	Decimal no.	Block no. ,Location no.		
00000000	0	2,3	3,1	...
00000001	1	1,2	3,3	...
00000010	2	1,3	4,2	...
.		.	.	.
.		.	.	.
11111111	255	5,1	5,2	....

Figure (3.5): Indexing process

C. Embedding procedure

In this step, the secret message is splitting into segments with length (n bits) which mean that hash sequences from $(0\ldots2^{n})$ must be found in the cover image. Then, each segment is converted to decimal format to speed up the searching process. The decimal number will be matched with an indexed hash table to find the block that its sequence matched to the sequence of the segment. While the matching process is done, the block number and the location of the matching for each segment are saved in the auxiliary information file. This file is a 2D array the row dimension of it is the number of segments and the column dimension of it is 2 (block number and location number). This file will be encrypted and send with a stego image to the receiver. Figure (3.6) shows the embedding process with segment length (n=8).



Hash sequence	Decimal no.	Block no. ,Location no.		
00000000	0	2,3	3,1	...
00000001	1	1,2	3,3	...
00000010	2	1,3	4,2	...
.		.	.	.
.		.	.	.
11111111	255	5,1	5,2	....

Block no.	Location no.
2	3
1	3
5	1
.	.
.	.
.	.
.	.

Figure (3.6): Embedding process

D. The Capacity of Information Hiding

The proposed approach can store non-specific bits of information in each image block depending on the size of the cover image and the size of the blocks. The mapping process is an overlapping way that increases the hiding capacity. The hiding capacity (B_C) in each block with size ($B_w \times B_h$) is calculated as follows:

$$B_c = B_w \times B_h - 1 \quad ,\ldots (3.5)$$

For an image of size (M×N) that divides into a block of size ($B_w \times B_h$) the capacity (C) can be calculated as follows:

$$C = \frac{M}{B_h} \times \frac{N}{B_w} \times B_c \qquad , \ldots (3.6)$$

3.2.1.3 Auxiliary Information File Encryption Process

Auxiliary information file is encrypted in this process. This action strengthens CISS's security. The encryption process is demonstrated in Figure (3.7).

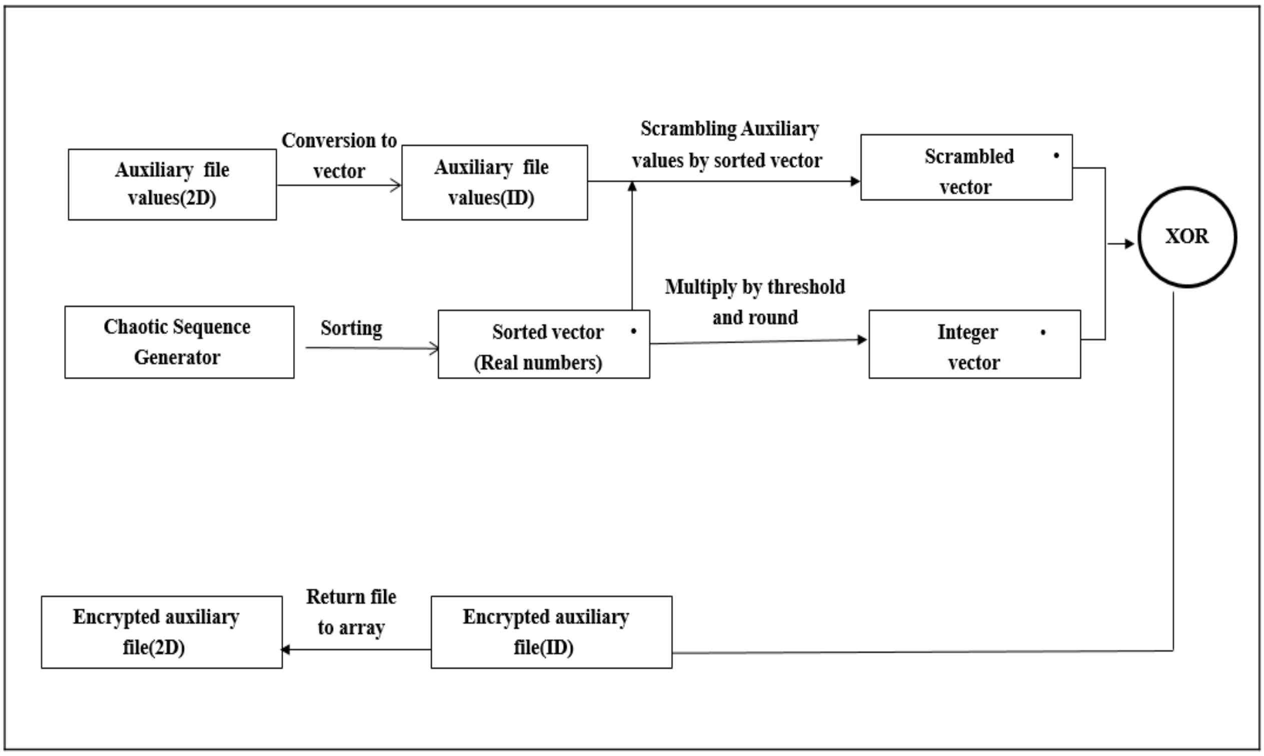

Auxiliary file values(2D)
Conversion to vector
Auxiliary file values(ID)
Scrambling Auxiliary values by sorted vector
Scrambled vector
XOR
Chaotic Sequence Generator
Sorting
Sorted vector (Real numbers)
Multiply by threshold and round
Integer vector
Encrypted auxiliary file(2D)
Return file to array
Encrypted auxiliary file(ID)

Figure (3.7): Auxiliary information file encryption process

The encryption process is described in the steps below:

A. Scrambling the Auxiliary Information File Values

The processes involved in scrambling auxiliary values are shown in Figure (3.8). The auxiliary information file values are scrambled using the steps below:

- Converting the auxiliary values into a 1D vector (v- Data).
- Using the logistic chaotic equation (2.5), generate a chaotic sequence (Chaotic_ Seq) of length (v-Data) (). Real numbers between [0, 1] are the result of equation.
- Sorting the created Chaotic Seq in ascending (or descending) order.
- And then altering the bit position of auxiliary information values according to the results of the sorted Chaotic Sequence.

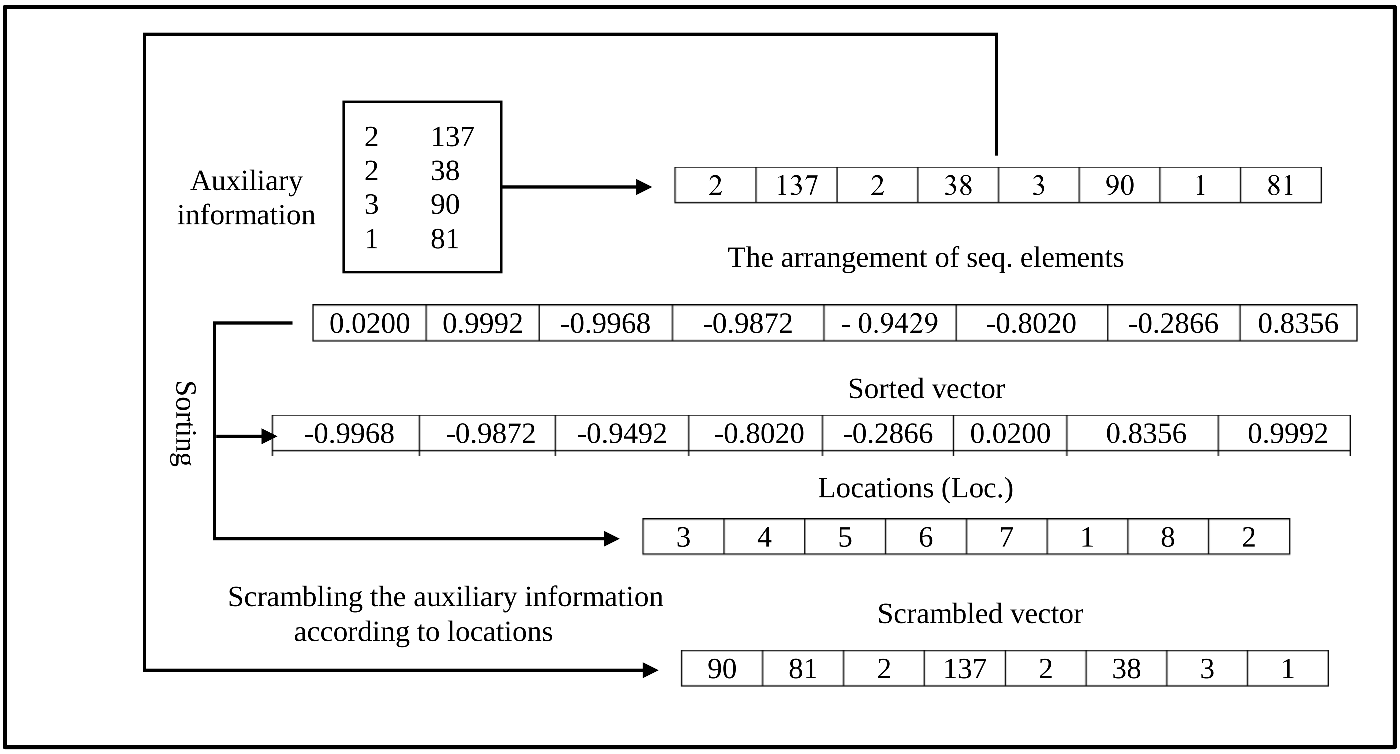


Figure (3.8): Auxiliary information scrambling process

B. Encryption

The chaotic sequence that was formed is employed utilized in the encryption method.

First, each auxiliary file element's mask sequence ($Mask_{Seq}$) is created by utilizing the following equation:

$$Mask_{Seq(i)} = \|\lfloor \text{Chaotic\_Seq (i)} \times B_{no} \rceil\| \quad \text{for i=1…length (auxiliary file)} \qquad , \ldots(3.7)$$

Where i is the current index of the sequence, $\|.\|$ is the absolute value, $\lfloor . \rceil$ is the rounding operation, and Chaotic_Seq represents generated chaotic sequence. B_{no} is number of bits in each block.

Secondly, for encrypting the auxiliary values, a mathematical operation is performed; the XOR operator is used between the Scrambled vector and Mask for getting encrypted secret Message (ESM).

Algorithm (3.4) describes the encryption process.

Algorithm (3.4): Encryption Process

```
Input:    Auxiliary File (AF)
Output: Encrypted Auxiliary File (EAF)
Begin
  for n=1,n<s-1                //s is the size of AF
      Generate: A 1D chaotic Sequence as equation (2.5).
  end for
  Sort: the generated chaotic Sequence and get its indices of it.
  for m=1,m<s
      Scramble: AF values using indices of sorted chaotic sequence as described in
      section (3.2.1.3, A)
  End for
  for m=1, m<s
      multiply: chaotic Sequence by threshold and rounding(IS) as equation (3.7)
  End for
  BIS=Dec2Bin(IS)
  BAF=Dec2Bin (scrambled Af values)
  for m = 1,m<s
      Perform XOR operation between BIS and BAF to produce EAF
  End for
End
```

3.2.2 Processes on the Receiver Side

On the receiver’s side, a number of processes are carried out as described in Algorithm (3.5).

Algorithm(3.5): Extracting Process

```
Input: Stego Image (SI), Encrypted Auxiliary File (EAF)
Output: Extracted Secret Data (ESD)
Begin
    1. Decrypt: EF using the algorithm (3.6)
    2. Generate: hash sequences for SI using the algorithm (3.2)
    3. For i=1, i<size(EF,1)
    4. Do extraction process
    5. End for
End
```

Each process's specifics are described in the sections that follow:

A. Decryption Process

In this process, the auxiliary information file is decrypted Figure (3.9) and algorithm (3.6) describe the decryption process.

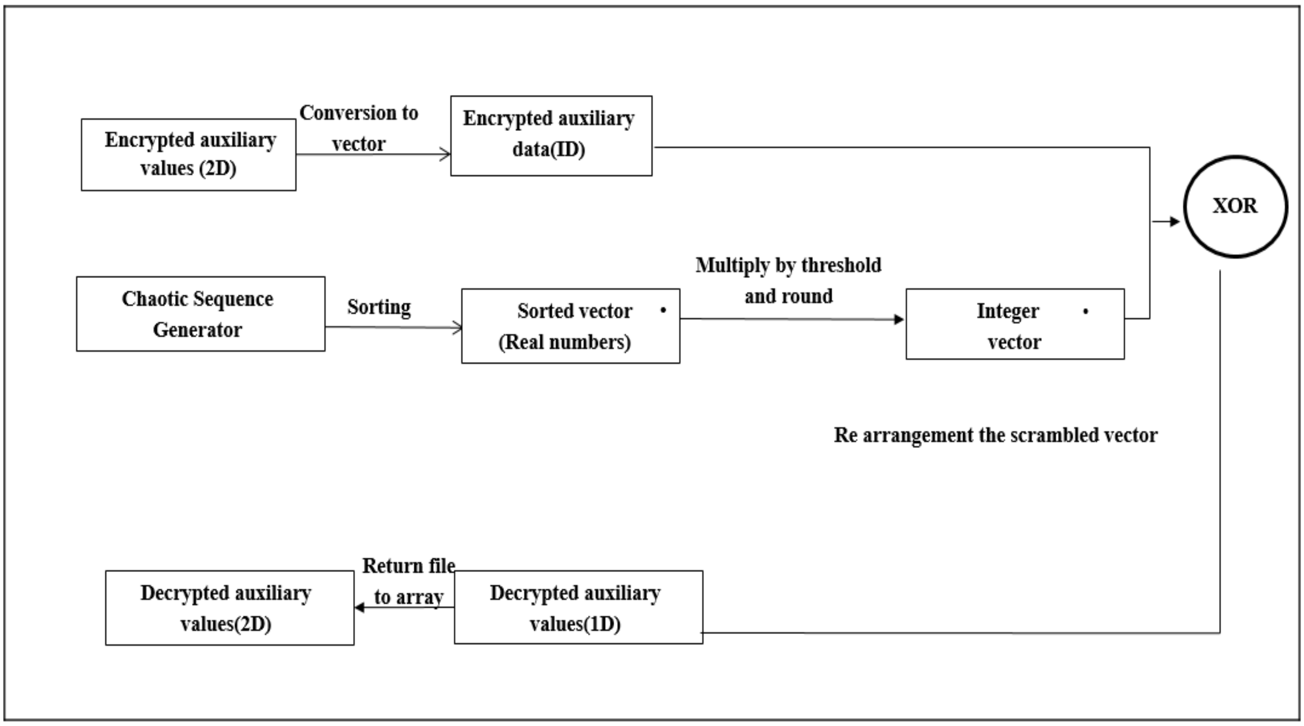

Encrypted auxiliary values (2D)
Conversion to vector
Encrypted auxiliary data(ID)
XOR
Chaotic Sequence Generator
Sorting
Sorted vector (Real numbers)
Multiply by threshold and round
Integer vector
Re arrangement the scrambled vector
Decrypted auxiliary values(2D)
Return file to array
Decrypted auxiliary values(1D)

Figure (3.9): Auxiliary information file decryption

Algorithm (3.6): Decryption Process

```
Input:    Encrypted Auxiliary File (EAF)
Output:   Extracted Auxiliary File (EXAF)
Begin
   1. for n=1,n<s-1            //s is the size of AF
      Generate: A 1D chaotic Sequence as equation (2.5).
   2. end for
   3. Sort: the generated chaotic Sequence and get its indices.
   4. for m=1,m<s
         Multiply: chaotic Sequence by threshold and rounding(IS) as equation (3.7)
   5. end for
   6. BIS=Dec2Bin(IS)
   7. for m = 1,m<s
        Perform XOR operation between BIS and EAF
   8. End For
   9. for m = 1,m<s
      Rearrange: the generated sequence from step 7 to obtain EXAF
   10.End for
End
```

B. Extraction Process

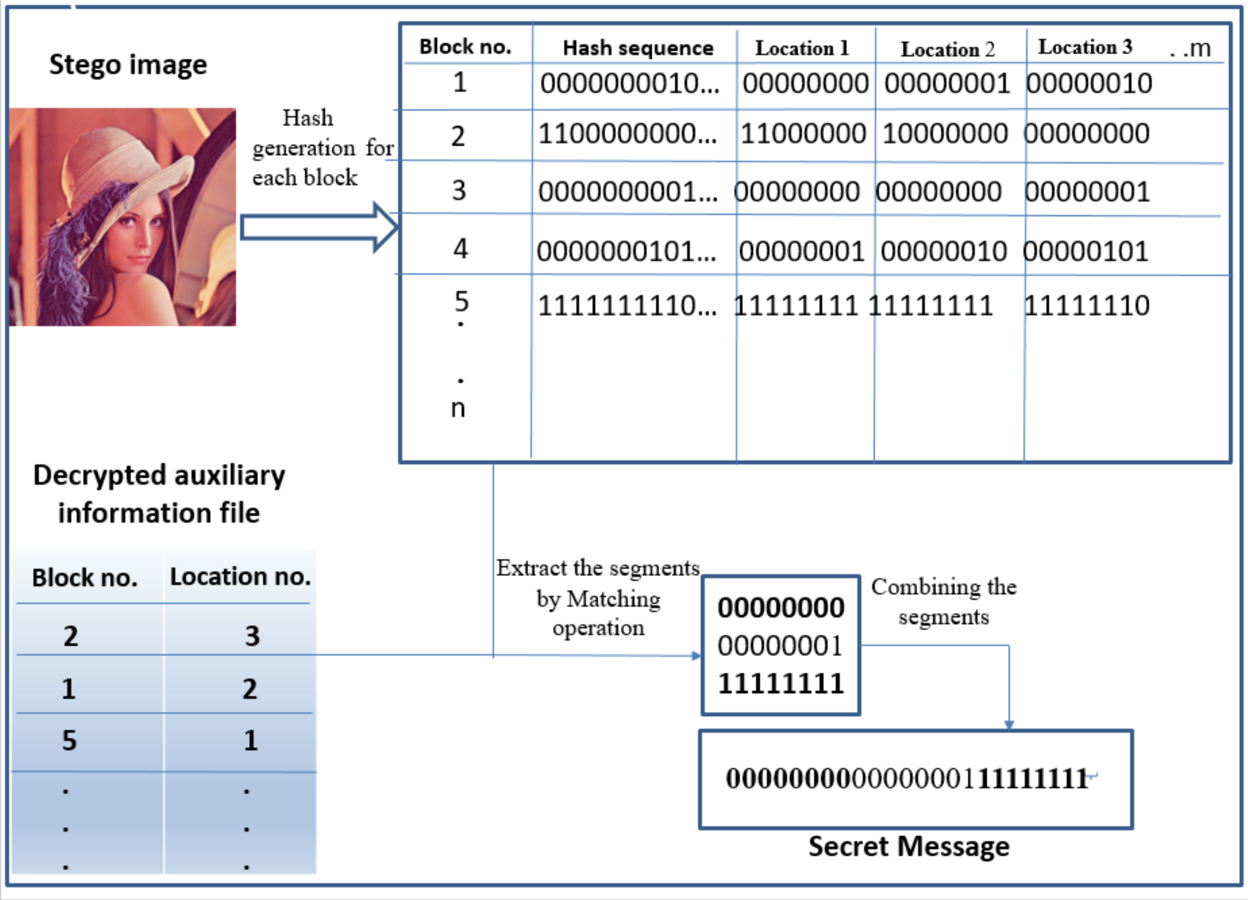
In this section, the hidden message will be retrieved from the receiver side. The following processes are done for this process:

1. By matching the numbers of block, and location in the decrypted auxiliary information file with the generated hash sequences one by one, the system can extract the segments of the secret data with segment length (n=8).

2. Merge the segments and remove the zeroes padded.

3. Show the extracted secret data.

Figure (3.10) shows the extraction procedure.


Stego image
Hash generation for each block
Decrypted auxiliary information file
Extract the segments by Matching operation
Combining the segments
Secret Message

Block no.	Hash sequence	Location 1	Location 2	Location 3	. .m
1	0000000010...	00000000	00000001	00000010	
2	1100000000...	11000000	10000000	00000000	
3	0000000001...	00000000	00000000	00000001	
4	0000000101...	00000001	00000010	00000101	
5	1111111110...	11111111	11111111	11111110	
.					
.					
n					

Block no.	Location no.
2	3
1	2
5	1
.	.
.	.
.	.

00000000
00000001
11111111

0000000000000001**11111111**

Figure (3.10): Extraction process

Chapter Four

Experimental Results and Discussion

Chapter Four

Experimental Results and Discussions

4.1 Introduction

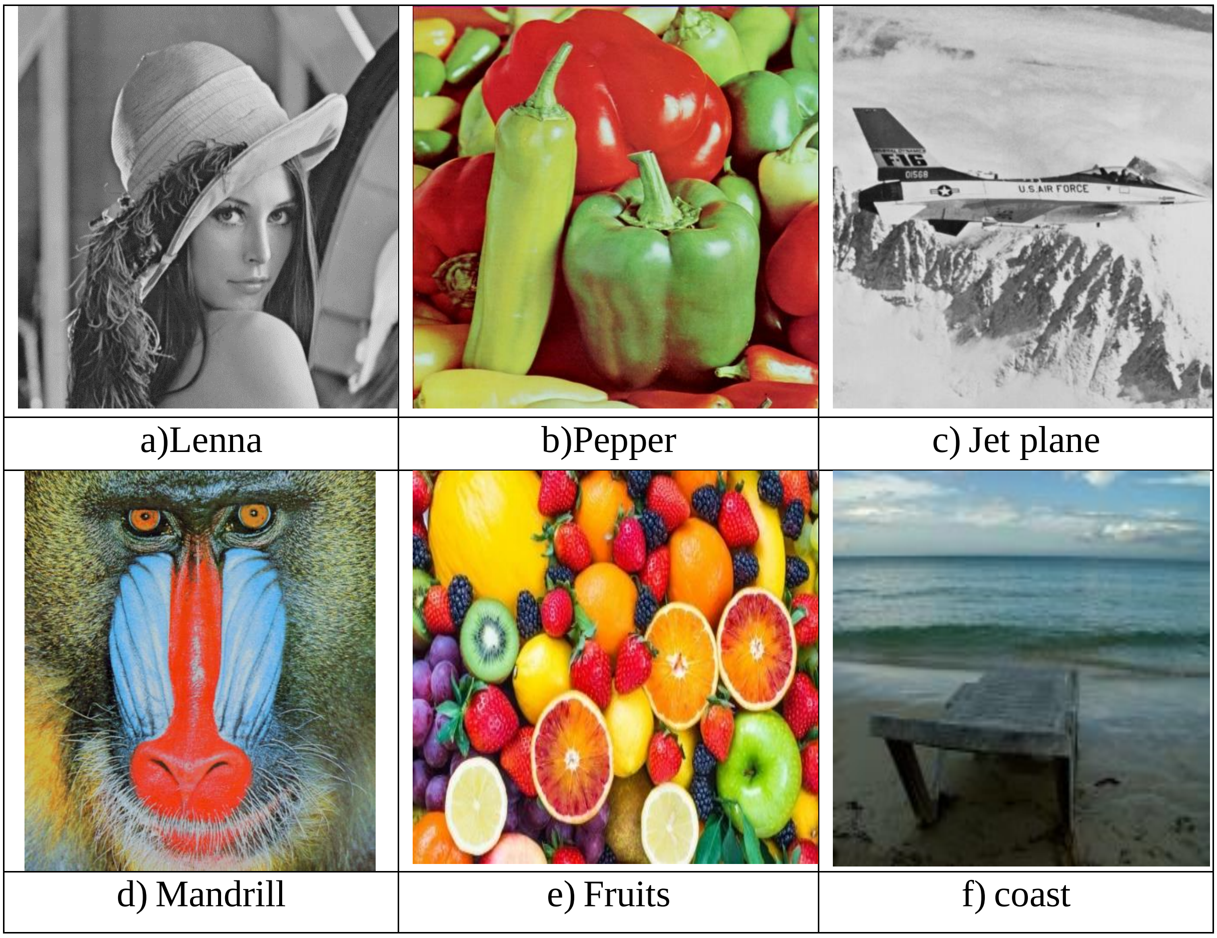
This chapter is devoted to provide the results of the tests performed on the proposed system. It also introduces a discussion of the experimental work's findings for assessing the system's performance. The proposed system is put into use with a device that has the following characteristics:

- Intel Core i7 processor running at 1.60 GHz
- RAM 16 GB
- Microsoft Windows 10 Pro

MATLAB programming language R2020 is used to simulate the proposed system. A number of tests were conducted to demonstrate the impact of different elements on the overall system performance. By using several performance measures that are covered in chapter two, the experimental data were analyzed to provide more explanation.

4.2 Data Set

Finding images that contain all the available sequence is one of the most crucial tasks in putting the proposed coverless image technique into practice. The data set that is used contains 50 images that achieving the purpose of the proposed method, it randomly selected from the internet are included in this dataset. Internet images come in a variety of resolutions, and a variety of categories. These images are known as stego-images. Standard of color and gray images have been used in a variety of experiments as a cover image, Figure (4.1) displays a sample of covered images in the gathered dataset, these are ‘Lena’, ’papper’, ’Jet plane’ ‘Mandrill ‘, ‘Fruits ‘, ‘coast‘. Single image, known as the stego-image, is required to send the secret data.



a)Lenna b)Pepper c) Jet plane

d) Mandrill e) Fruits f) coast

Figure (4.1): Sample of collected cover images

The cover image that is used for transmission is resizing into the resolution of 512×512. The hash codes calculated from a cover image is an important factor in the embedding process. When the calculated hash codes are varied and cover a broad range of different values, the probability of embedding a secret data with different characters in a single image increases. Since the length of a hash code calculated from each block is 8 bits. The size of the secret data file that is used in all experiments is 6245 bits. Figure (4.2) shows samples of the secret data file.

00000000000000010000001000000011000001000000010100000110000………

Figure (4.2): Secret data

4.3 Experimental Results of the Proposed System

The efficiency of the proposed coverless technique is assessed in terms of available hash codes, embedding and extracting processes, capacity, execution time, robustness and security.

4.3.1 Tests on the Generated Hash Codes

Several experiments that analyze the number of unique hash codes with respect to various parameters are conducted. In the beginning, the relationship between the generated hash codes and block size is studied. Also, the robustness toward attacks and its relation with generated hash codes are considered in the experiments.

A. the Effect of the Block Size on the Generated Hash Code and Robustness

One of the key parameters in the proposed technique is the block size. A series of experiments are set up to investigate the connection between the amount of distinct hash codes and the block size. The outcomes of these studies are summarized in Table (4.1).

Table (4.1): The relationship between block size and generated hash code

Image name	Block size		
	8×8	16×16	32×32
Lena	254	256	256
Pepper	250	256	256
Jet plane	253	256	256

As shown in table (4.1), as the block size is increased, the number of distinct hash codes grows. In block size equal to (16×16) and more, the proposed system got all the possible hash codes in single cover image, but, the robustness must be considered against image processing attacks in the same time. So, the proposed system was tested in terms of robustness under the block size (16×16) and (32×32) using Extraction Accuracy as its equation (2.4) for deciding the optimal choice that apply the tradeoff between the ability of gaining all hash codes and robustness in the same time. The result of experiments is shown in table (4.2).

Table (4.2): The robustness versus block sizes

Attack Type	**Factor**	**Block size**	
		(16×16)	**(32×32)**
No attack	-	100%	**100%**
Median filter	3×3	81.45%	**86.09%**
Median filter	5×5	71.07%	**73.83%**
Gaussian low-pass filter	3×3	92.41%	**95.00%**
Gaussian noise	0.001	66.03%	**66.70%**
Salt and pepper noise	0.001	100%	**100%**
Speckle noise	0.001	79.11%	**85.43%**
Sharpening attack	0.05	100%	**100%**
Average filter	3×3	79.56%	**81.93%**
Histogram equalization	**-**	92.33%	**93.30%**
Motion blur	**-**	63.89%	**68.59%**

The results demonstrated that as block size is increased, the resilience against all tested image processing assaults increases. So the optimal choice is the block size (32×32) that achieve a tradeoff between the robustness and the number of distinct hash codes. So, all experiments will apply with block size of (32×32) pixels.

B. The Availability of Hash Codes

Finding all the possible hash codes in the single image such that it can embed any secret data is the most important critera in the proposed method, through the experiential on the collected dataset, all the images contain all the possible hash codes.

C. Comparison with Exiting Hash Generation Methods

A sample of images are taken as shown in Figure (4.1) for comparison with other previous methods that uses the same images, the term "Hash code(types)" refer to the several kinds of hash codes that were generated and The term "No-find(bits)" refers to that the secret data was unable to locate the associated hash code. As a result, the proposed system can hide all secret data when the same number of bits is hidden in the same image as shown in Table (4.3).

Table (4.3): Comparison of the various hashing algorithms and the numbers for secret data not found

Method	Ref.				The proposed system	
	[31]		[34]			
Hiding Capability	Hash Code (Types)	No-Find (Bits)	Hash Code (Types)	No-Find (Bits)	Hash Code (Types)	No-Find (Bits)
Lena	208	156	256	0	256	0
Pepper	188	219	256	0	256	0
Jet Plane	158	305	256	0	256	0

As shown in Table (4.3), the proposed system generates all possible hash codes for 8 bits segments that use for embedding.

4.3.2 Testing on the Embedding Procedure

For evaluating the effectiveness of the proposed system, the secret data depicted in Figure 4.2 is used and the standard "Lenna" image for embedding. The embedding process is done according to the following steps:

Step1: The secret data is splitting into segments of length 8 after doing zero padding as shown in Figure (4.3).

Segment no.	1	2	3	4	5	6	7	……..
Bits	00000000	00000001	00000010	00000011	00000100	00000101	00000110	……..

Figure (4.3): The splitting secret data

Step2: Several steps are done on the cover image including converting into gray scale if it is a color image, resizing the cover image into 512×512 pixels, scrambling the cover image for decreasing its correlation, and the scrambled cover is divided into non-overlapping blocks of size 32×32 pixels. So, the number of blocks is 256.

Step3: Transforming each divided block in the cover image by using DWT, quantizing it, and converting it into a vector.

Step4: Generating a hash sequence from each block according to section 3.2.1.1. Figure (4.4) illustrates the result of hash sequences of size 256×1023.

Block no.	**Sequence (bit no.)**								
	1	**2**	**3**	**4**	**5**	**6**	**.**	**.**	**1023**
1	0	0	1	1	0	1	.	.	1
2	0	0	1	0	1	1	.	.	0
3	0	0	0	1	0	1	.	.	`1
.	.	.	.	.	.	.	.	.	.
256	0	0	0	0	0	0		.	0

Figure (4.4): The result of generated hash sequences

Step 5: The inverted index table is built for all generated hash sequences according to the overlapping block; the resulting hash table is shown in Figure (4.5).

Hash sequence	Decimal no.	No. of a block, no. of location		
00000000	**0**	3,733	10,633	…
00000001	**1**	1,574	1,657	
00000010	**2**	1,141	1,158	
.				
.				
11111111	**256**	10,552	17,657	

Figure (4.5): The hash Table

Step 6: Mapping each segment of the secret data with a similar hash sequence saved in the hash table, and saving the results of mapping operating in a file. Figure (4.6) illustrates the results of the mapping procedure.

Block no.	Location no.
3	733
1	574
1	141
.	
.	.
3	3

Figure (4.6): The auxiliary information file

Step 7: Encrypting the file by using the proposed chaotic map encryption, the encrypted file is shown in Figure (4.7).

```
0001110100

0001001111

0001001111

0001001111

0101110011

    .

0110000101

1111101010
```

Figure (4.7): The encrypted auxiliary information file

Step 8: Sending the stego image and the encrypted auxiliary information file to the receiver.

4.3.3 Testing the Extracting Procedure

On the Receiver side, the activities were carried out as below:

Step 1: Receiving the stego image and auxiliary information file

Step 2: Decrypting the auxiliary information file. The result of the decryption operation is shown in Figure (4.8).

Block no.	Location no.
3	733
1	574
1	141
.	
.	.
3	3

Figure (4.8): The decrypted auxiliary information file

Step 3: Generating the hash table from the stego image (as described on the sender side).

Step 4: Extracting the segments of the secret data by the auxiliary information file and hash sequence. Figure (4.9) illustrates the segmented extracted data.

Segment no.	1	2	3	4	5	6	7	……..
Bits	00000000	00000001	00000010	00000011	00000100	00000101	00000110	……..

Figure (4.9): The segmented extracted data

Step 5: combine all the segments for the complete secret data and delete all padded zeroes, as shown in figure (4.10).

0000000000000001000000100000001100000100000001010000011 0000.........

Figure (4.10): The extracted secret data

4.3.4 The Information Hiding Capacity

In this section, two subsections will be listed related to the calculated hiding capacity:

A. Hiding Capacity Computation

The mapping process is an overlapping way that increases the hiding capacity. The hiding capacity in each block is calculated as equation (3.5). the block capacity (B_C) using block size (32×32) is equal to :

$$B_c=1023 \text{ bits}$$

Therefore For the whole single image of size (512×512) that divides into a block size (32×32), the capacity (C) can be calculated through equation (3.6).

$$C= 261{,}888 \text{ bits}$$

The proposed system gained a high amount of information capacity at the scale of the block and thus at the scale of the whole image due to use overlapping way for generating the hash sequences.

B. Comparison with Exiting Methods

The performance of the offered strategy is compared with other previous methods in terms of hiding capacity by using the same image, and resolution in order to confirm the efficiency of the proposed method as shown in Table (4.4).

Table (4.4): The hiding capacity of different information hiding approaches

Method	Capacity (bits/image)
HOGs [26]	8
Double-level index[28]	10000
CIHMSB[30]	1296
(non-overlapping)[31]	6272
(overlapping)[31]	55,112
Ring statistic features[33]	32
Two-Level Mechanism[34]	84,005
CIHLHF[35]	49,152
The proposed method	**261,888**

As shown in Table (4.4), the proposed system has a higher capacity than all the previous methods.

4.3.5 Execution Time Analysis

Execution time considers also one of the important factors in the hiding system. This section examines the execution times of hashing, embedding, and extracting operations. Table (4.5) lists the execution time (in seconds) for each process individually.

Table (4.5): Execution time of hashing, embedding and extracting operations

Image name	Hashing generation operation	Embedding operation	Extracting operation
Lena	0.232912	0.002685	0.186504
Jet plane	0.412649	0.002689	0.072796
Pepper	0.225657	0.002556	0.076091

As shown in Table (4.5), the hashing process takes little time, and Due to the embedding process using a lookup table, which contains the pre-generated hash code for each image block, and location, it takes less time than the extracting procedure. The three procedures generally take a short amount of time to complete, therefore the proposed hiding strategy is appropriate for real-time applications.

4.3.6 Experimental Results Related to System Robustness

The proposed approach depends on mapping relationships between the block hash codes and the secret data. No modification has been made to the cover image contents. The transmission of the stego image happens across un secure channel that is vulnerable to image processing attacks such as image noise, rescaling, JPEG compression, contrast shift, brightness change, and so on. which may change the generated hash sequences and fail to extract the secret data from the receiver. Thus The stego image that represents the secret data must be subject to these attacks. To put it another way, the hash algorithm must be resistant to these types of attacks. Thus Bit Error Rate (BER) is used for testing the robustness of the proposed method. The secret data is shown in Figure (4.2) and the ‘Lenna’ image is used for embedding.

A. Robustness Proposed System Against JPEG Compression

The chosen Stego image is compressed using JPEG with different quality levels. Table (4.6) shows that the proposed method provides strong resistance against JPEG compression attacks, with good values for BER.

Table (4.6): The results of the compression attack

Quality factors(Q)	BER	Stego image after attack
30	0.27	
60	0.19	
80	0.15	
90	0.12	

As shown in table(4.6), the proposed method obtained desirable results against compression attack for a various of compression ratios that the value of BER is small.

B. Robustness to Noise Attacks

A stego image is subjected to noise attacks. a noise attack including salt and pepper, speckle, and Gaussian noises with different noise densities. Table (4.7) shows different types of noise attacks.

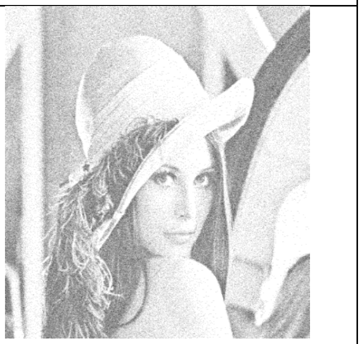
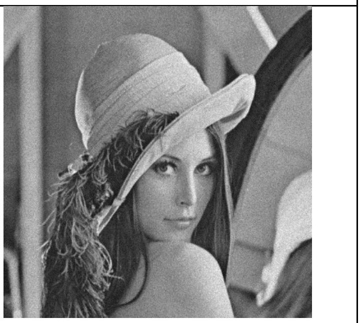
Table (4.7): The results of the noise attacks

Attack type	**Density of noise**	**BER**	**Stego image after attack**
Salt & pepper	0.001	0	
	0.01	0.07	
	0.02	0.10	
	0.03	0.18	

To be continued

Speckle noise	0.001	0.14	
	0.01	0.29	
	0.02	0.32	
	0.03	0.38	
Gaussian noise	0.001	0.33	

To be continued

	0.01	0.34	
	0.02	0.35	
	0.4	0.39	
Poisson noise		0.25	

As shown from Table (4.7) the proposed method obtained desirable results against various of noise attacks and for varied Densities of noise that the value of BER is small.

C. Robustness to Filtering Attacks

Additionally, the stego image was filtered using a low pass (Gaussian) filter, a mean filter, and a median filter with various filter kernel window sizes. BER values under filtering attack are shown in Table (4.8).

Table (4.8): The results of the filtering attacks

Attack type	Density of noise	BER	Stego image after attack
Median filter	1×1	0	
	2×2	0.19	
	3×3	0.13	

To be continued

Mean filter	1×1	0	
	2×2	0.19	
	3×3	0.18	
Gaussian filter	1×1	0	

To be continued

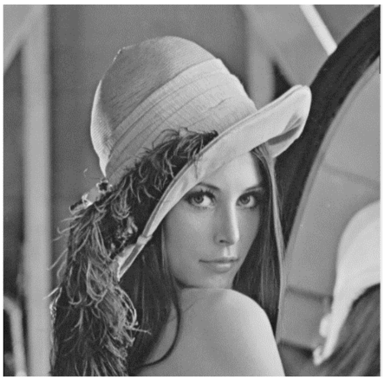
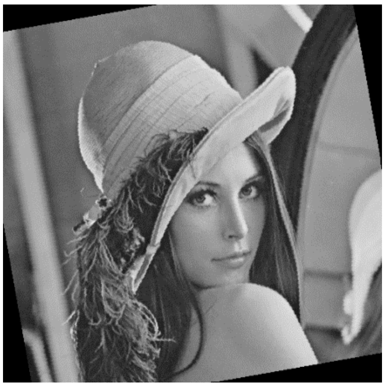
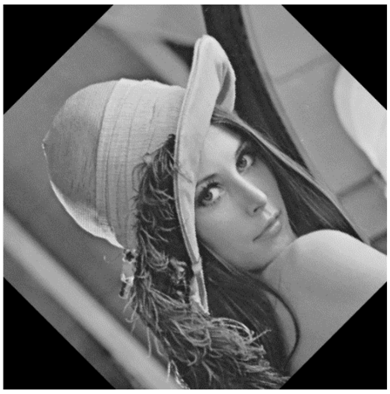
	2×2	0.19	
	3×3	0.04	

As shown from Table (4.8) the proposed method obtained desirable results against various of filtering attacks and for window sizes that the value of BER is small.

D. Robustness to Geometric Attacks

Resize and rotate attacks are Tested as shown in Table (4.9). the proposed approach performs acceptable results in rotate attacks with various rotation degrees which considered hardest kind of attacks. Also, the proposed method is tested against resize attack with different size ratio and the results show that the method performs well against resizing attack.

Table (4.9): The results of the geometrics attacks

Attack type	Angle	BER	Stego image after attack
Rotation	0.180	0.10	
	10	0.48	
	45	0.49	

To be continued

Resize	(1024×1024)	0.06	
	0.3	0.25	

As shown from Table (4.9) the proposed method obtained acceptable results against various of geometric attacks that are rotation attacks for a varied angles and resizing attacks for a varied sizes, that the value of BER is consider small because this type of attacks is the hardest types of attacks that manipulate the structure of the image.

E. Robustness to Brightness and Sharpness Attacks

The brightness attack for the stego image was examined under factor values (10, 20). Additionally, the stego image was examined when subjected to image sharping attack. The results demonstrated in Table (4.10).

Table (4.10): The results of brightness and sharpening attacks

Attack type	Factor	BER	Stego image after attack
Brightness	**+10**	0.01	
	+20	0.01	
Sharpness	**0.05**	0	

As shown from Table (4.10) the proposed method obtained desirable results against brightness attacks and sharpness attacks that the value of BER is small.

Generally, Tables (4.6-4.10) illustrate that the system is robust against several image processing attacks due to hashing generating algorithm depending on image scrambling, wavelet transform, quantization. On the other hand, if an attacker could compromise the channel and obtain the stego image and the locations file and, the value of other parameters (i.e. block size, key of chaotic, etc) should also be known to calculate the hash codes. So, all attempts to discover the secret data are failed.

F. Comparison with Exiting Methods

The performance of the offered strategy is compared with other current state-of-the-art CIS methods [31] [34] under robustness in order to confirm the efficacy of the proposed method using Extraction Accuracy in equation (2.4) .The comparisons with other previous are done on the same image that tested in these methods 'Lenna' image and the same secret data size. The results of the comparisons are shown in Table (4.11).

Table (4.11): Comparison of Robustness with Two CIS methods

Attack Type	Factor	Ref.		The proposed system
		[31]	[34]	
No attack	-	80.10%	100%	**100%**
Median filter	3×3	65.90%	72.60%	**86.09%**
Median filter	5×5	59.60%	68.20%	**73.83%**
Gaussian low-pass filter	3×3	69%	75.80%	**95%**
Gaussian noise	0.001	39.30%	6.90%	**66.70%**
Salt and pepper noise	0.001	3.70%	1%	**100%**
Speckle noise	0.001	39.90%	10.60%	**85.43%**
Sharpening attack	0.05	88.50%	78.80%	**100%**
Average filter	3×3	69%	77.30%	**81.93%**
Histogram equalization	**-**	80%	80%	**93.30%**
Motion blur	**-**	58.50%	59.70%	**68.59%**

As shown in Table (4.11), the proposed strategy consistently outperforms previous methods in all attacks.

4.3.7 Experimental Results Related to Security Analysis

A good encryption algorithm has the following properties:

1. Sensitivity for initial values (secret key).
2. Reliable entropy data.
3. The original and encrypted data have very little correlation with one another.
4. Produce a good amount of randomizing.

A. Key Sensitivity Analysis

It is thought to be one of the most important measures for assessing encryption algorithms. It is employed to gauge an encryption system's sensitivity to even the slightest alteration to the secret key that is utilized for both encryption and decryption. The suggested approach encrypts the auxiliary information file displayed in figure (4.6) using the secret key value (x0=0.6) resulting in the encrypted auxiliary information file shown in figure (4.7). By modifying the secret key to (x0=0.6000001) and applied to the secret's decryption as shown in figure (4.11 D) which differs greatly from the original auxiliary information values (x0=0.6). That suggests that the proposed method is extremely sensitive to even the slightest alteration in the secret key.

Block no.	Location no.
3	733
1	574
1	141
.	
.	.
3	3

A- The auxiliary information file

0001110100
0001001111
0001001111
0001001111
0101110011
.
0110000101
1111101010

B-The encrypted auxiliary information file

Block no.	Location no.
3	733
1	574
1	141
.	
.	.
3	3

C-The decrypted auxiliary information file Using (x=0.6)

Block no.	Location no.
230	20
46	83
21	727
.	
.	.
15	186

D- The decrypted auxiliary information file using (x=0.6000001)

Figure (4.11): Key influencing on encryption and decryption process

B. Avalanche Effect

The Avalanche Effect metric can be used to gauge how effective the diffusion process is. The Avalanche effect is evaluated between the original auxiliary file in binary form and the encrypted auxiliary file, which shows the different bits between the two files according to equation (2. 9).

C. Entropy

The entropy of any encrypted data can be computed according to equation (2.7). The optimum entropy value should be (1) or a value near it.

D. Correlation Coefficient (CC)

The correlation coefficient is used to illustrate how the plain and encrypted texts are uncorrelated from one another, it is calculated according to equation (2.8).

All values of security measurements are described in Table (4.12).

Table (4.12): Security measurements values

Metric name	Value
Entropy	0.9990
Correlation coefficient	-0.0249
Avalanche effect	0.5199

As shown in table (4.12), the proposed encryption algorithm is effective and provides a higher level of security.

D. The NIST Tests

Seven tests of NIST are used for evaluating the proposed system in terms of randomizing including the Frequency test, Non-Overlapping Template Matching Test, Overlapping Template Matching Test, Linear Complexity Test, Cumulative Sums (Forward) Test, Cumulative Sums (Reverse) Test, Random Excursions Test and Random Excursions Variant. The significance value (P) indicate that the default value of the NIST tests indicate that the fraction of the sequence is random or not random based on the default value (0.01). The sequence is regarded as random if the P-value is greater than 0.01. Otherwise, if the P- value is less than 0.01, the sequence is considered not random [15]. Table (4.13) describe the results of tests. The results of NIST experiments are shown in table (4.13).

Table (4.13): NIST tests values

Test Name	p-value	Status
Longest Run of Ones in a Block	0.22174346028425668	Random
Binary Matrix Rank Test	0.1964481854867722	Random
Non-Overlapping Template Matching Test	0.07159678971446465	Random
Overlapping Template Matching Test	0.9773728654483924	Random
Linear Complexity Test	0.3206861205709942	Random
Random Excursions Test(state='+1')	0.7512117103661213	Random
Random Excursions Variant(state='-1.0')	0.4142161782425252	Random

As shown in table (4.13), the results indicate that the generated algorithms successfully passed the tests that NIST has examined, showing that their P-values are higher than the default P-value. As a result, there is a significant amount of randomness in the binary sequence produced by the developed algorithm.

E. Testing the Effectiveness of Chaotic Keys

To ensure the effectiveness of selecting the keys for the proposed encryption system in this work, several images were taken and examined them in terms of security measurements. These are 'Jet plane',' Mandrill',' coast'. The results of experiments shown in table (4.14).

Table (4.14): Security analysis for tested images

Test Name	Jet plane	Mandrill	Coast
Entropy	0.9992	0.9990	0.9988
Correlation coefficient	-0.0140	-0.0082	-0.0056
Avalanche effect	0.5145	0.5123	0.5118
Longest Run of Ones in a Block	0.2923344677208121	0.12097990849603397	0.0026908791992790956
Binary Matrix Rank Test	0.15732903969225756	0.751786089549666	0.6182001828104364
Non-Overlapping Template Matching Test	0.22103800826241338	0.21802200112060988	0.11177230431163789
Overlapping Template Matching Test	0.8422894108271192	0.35368829889182485	0.6797694863885718
Linear Complexity Test	0.2131323100668984	0.7156713409753308	0.6285505816628485
Random Excursions Test(state='+1')	0.5494159513527803	0.6999858358786277	0.8930721407359578
Random Excursions Variant(state='-1.0')	0.24821307898992362	0.6830913983096087	0.10247043485974937

Table (4.14) shows that chosen keys which used for the encryption process are effective regardless of the text.

Chapter Five

Conclusions and Ideas for Future works

Chapter Five

Conclusions and Ideas for Future Works

5.1 Introduction

In this chapter, conclusions and suggestions for future works are illustrated after applying the proposed system.

5.2 Conclusions

The following conclusions can be drawn after using the proposed system:

1. The proposed hashing generation algorithm has proven its effectiveness in providing all hash sequences in single image. In this work, the hash code is calculated using the scrambling process which has great impact since it provide diversity values of hash sequence which increase the possibility of hiding secret message of different strings in single image.
2. All the possibilities of generated hash codes (256 hash codes) can be obtained with increasing the block size.
3. The robustness of the proposed system is increased with increasing the block size.
4. The proposed coverless information hiding with the help of overlapping mapping relationship has high capacity. The mapping process between the secret segment and the generated hash sequence from each block is done in overlapping way. The experimental results show that the proposed system could achieve a high capacity of embedding this increased the possibility of embedding the complete secret data in single image.
5. The proposed framework does not need to employ the designated cover image for embedding the secret data but directly transfers secret information through its own properties. Since carriers have not been altered in coverless image steganography, the proposed method cannot be detected by steganalysis techniques.

6. There is no need for a large database that increases the cost in terms of time and storage. No time is lost in searching process. Almost all earlier methods required searching a database for the necessary image. Depending on the size of the database, searching for images can be a slow process.

7. Due to the embedding process using a lookup table, which contains the pre-generated hash code for each image block, and location, it takes less time than the extracting procedure. The hashing process takes also little time, the three procedures generally take a short amount of time to complete.

8. According to experiment results of embedding robustness, the proposed algorithm is put to the test against several forms of attacks and its robustness is more than the previous methods. The using of scrambling, discrete wavelet transform, and the quantization process in hash generating process made the system more robust against attacks.

9. The proposed system, which uses the chaotic encryption method to encrypt the auxiliary information file, performs well in testing. The results indicate that the encrypted file has correlation coefficients that are very close to the ideal values of 0, with entropy information equal to the ideal value of 1.

10. Additionally, the system is applied on different standard images and other collected images which could allow at every time send different stego-image to the receiver for avoiding attacker suspicions. As well as there are other parameters that must be known for extracting the secret data. In this instance, even if the attackers succeed in obtaining the stego-image, it will be difficult for them to access the secret data. The coverless information concealing solution that is proposed provides improved security as a result.

5.3 Future Works

The suggestions for future works can be demonstrated as follows:

1. The generating hash sequence algorithm can be developed to generate hash codes from multi-channel images RGB (24 bits).

2. It is possible to implement the proposed system in video, text, and audio.

3. Studying the ability of applying the proposed system in sensitive image such as medical and military image.

4. It is possible to increase the level of security by encrypting the secret data before the embedding process.

References

Refrences

[1] D. Ashenden, “Information Security management : A human challenge ?,” Inf. Secur. Tech. Rep., vol. 13, no. 4, pp. 195–201, 2008, doi: 10.1016/j.istr.2008.10.006.

[2] A. Shaik, V. Thanikaiselvan, and R. Amitharajan, “Review Article Data Security Through Data Hiding in Images : A Review”, doi: 10.3923/jai.2017.1.21.

[3] B. Madhu, “An Overview of Image Security Techniques,” vol. 154, no. 6, pp. 37–46, 2016.

[4] S. Bansod and G. Bhure, “Data Encryption by Image Steganography,” vol. 4, no. 5, pp. 453–458, 2014.

[5] R. Gupta, S. Gupta, and A. Singhal, “Importance and Techniques of Information Hiding : A Review,” vol. 9, no. 5, pp. 260–265, 2014.

[6] T. Morkel, J. H. Eloff, and M. S. Olivier, "An overview of image steganography," in ISSA, pp. 1-11,2005.

[7] S. M. Thampi, “Information Hiding Techniques : A Tutorial Review 1 . History of Information Hiding 2 . What is Steganography and why is it important ?,” 2004.

[8] A. Arya and S. Soni, "A literature review on various recent steganography techniques," International Journal on Future Revolution in Computer Science & Communication Engineering, vol. 4, pp. 143-149, 2018.

[9] A. A. Abd EL-Latif, B. Abd-El-Atty, and S. E. Venegas-Andraca, "A novel image steganography technique based on quantum substitution boxes," Optics & Laser Technology, vol. 116, pp. 92- 102, 2019.

[10] M. Kharrazi, H. T. Sencar, and N. Memon, “Image Steganography: Concepts and Practice,” 2004.

[11] L. A. Sandoval-Bravo, V. I. Ponomaryov, R. Reyes-Reyes, and C. Cruz-Ramos, “Coverless image steganography framework using distance local binary pattern and convolutional neural network,” no. April 2020, p. 14, 2020, doi: 10.1117/12.2556310.

[12] G. Swain and S. K. Lenka, “Classification of Image Steganography Techniques in Spatial Domain : A Study,” vol. 5, no. 03, pp. 219–232, 2014.

[13] R. T. McKeon, "Strange Fourier steganography in movies," in *2007 IEEE International Conference on Electro/Information Technology,* 2007, pp. 178-182.

[14]T. Rabie and I. Kamel, "On the embedding limits of the discrete cosine transform," *Multimedia Tools and Applications,* vol. 75, pp. 5939-5957, 2016.

[15]P. Tay and J. Havlicek, "Frequency implementation of discrete wavelet transforms," in *6th IEEE Southwest Symposium on Image Analysis and Interpretation,* pp. 167-171, 2004.

[16] Kumar, A. & Pooja, K. Steganography- A Data Hiding Technique. *Int. J. Comput. Appl.* 9, 19–23 ,2010.

[17] Wu, J. *et al.* A Coverless Information Hiding Algorithm Based on Grayscale Gradient Co-occurrence Matrix. *IETE Tech. Rev. (Institution Electron. Telecommun. Eng. India)* 35, 23–33 ,2018.

[18] M. M. Liu, M. Q. Zhang, J. Liu, P. X. Gao, and Y. N. Zhang, “Coverless Information Hiding Based on Generative Adversarial Networks,” *Yingyong Kexue Xuebao/Journal Appl. Sci.*, vol. 36, no. 2, pp. 371–382, 2018, doi: 10.3969/j.issn.0255-8297.2018.02.015.

[19] C. Yuan, Z. Xia, X. Sun , “Coverless image steganography based on sift and bof“Journal of Internet Technology,vol.18,no.2,pp.435–442,2017, doi: 10.6138/JIT.2017.18.2.20160624c.

[20]]A. Qiu, X. Chen, X. Sun, S. Wang, and G. Wei, “Coverless Image Steganography Method Based on Feature Selection,” *J. Inf. Hiding Priv. Prot.*, vol. 1, no. 2, pp. 49–60, 2019, doi: 10.32604/jihpp.2019.05881.

[21]A. Shapi’i, R. Sulaiman, M. K. Hasan, A. Y. M. Kassim, and S. Abdullah, "Scaling technique for digital implant in medical images using pixel density algorithm," *European Journal of Scientific Research,* vol. 47, pp. 24-32, 2010.

[22] D. Khovratovich, I. Nikolić, and C. Rechberger, "Rotational rebound attacks on reduced Skein," in *International Conference on the Theory and Application of Cryptology and Information Security,* pp. 1-19,2010.

[23] J. Wu, Y. Liu, Z. Dai, Z. Kang, S. Rahbar, and Y. Jia, "A coverless information hiding algorithm based on grayscale gradient co-occurrence matrix," *IETE Technical Review,* vol. 35,pp. 23-33, 2018.

[24] Zhou Z., Sun, H., Harit, R., Chen, X., & Sun, X., “Coverless image steganography without embedding,” in International Conference on Cloud Computing and Security, pp.123 –132,2015.

[25] Z. Zhou, Y. Cao, and X. Sun, "Coverless information hiding based on bag-of-words model of image," *J. Appl. Sci,* vol. 34, pp. 527-536, 2016.

[26] Z. Zhou, Q. J. Wu, C.-N. Yang, X. Sun, and Z. Pan, "Coverless image steganography using histograms of oriented gradients-based hashing algorithm,vol. 18, pp. 1177-1184, 2017.

[27] X. Zhang, F. Peng, and M. Long, "Robust coverless image steganography based on DCT and LDA topic classification," *IEEE Transactions on Multimedia,* vol. 20, pp. 3223-3238, 2018.

[28] Chen, X., Qiu, A., Sun, X., Wang, S. & Wei, G. A high-capacity coverless image steganography method based on double-level index and block matching. *Math. Biosci. Eng.* 16, pp.4708–4722 ,2019.

[29] X. Zhang, F. Peng, Z. Lin, and M. Long, "A Coverless Image Information Hiding Algorithm Based on Fractal Theory," *International Journal of Bifurcation and Chaos,* vol. 30, p. 2050062, 2020.

[30] Yang, L., Deng, H., & Dang, X. J. I. A., "A novel coverless information hiding method based on the most significant bit of the cover image ",vol.8, pp.108579-108591,2020.

[31]Abdulsattar, F. S. "Towards a high capacity coverless information hiding approach".,*Multimed. Tools Appl.* ,Vol.80, pp.18821–18837 ,2021.

[32] Q. Liu, X. Xiang, J. Qin, Y. Tan, and Q. Zhang, "Reversible sub-feature retrieval: Toward robust coverless image steganography for geometric attacks resistance," *KSII Transactions on Internet and Information Systems (TIIS),* vol. 15, pp. 1078-1099, 2021.

[33] X. Liu, Z. Li, J. Ma, W. Zhang, J. Zhang, and Y. Ding, “Robust coverless steganography using limited mapping images,” *J. King Saud Univ. - Comput. Inf. Sci.,* vol. 34, no. 7, pp. 4472–4482, 2022, doi: 10.1016/j.jksuci.2022.05.012.

[34] J. Pan, X. Sun, H. Yang, and V. Snášel, “SS symmetry Information Hiding Based on Two-Level Mechanism and Look-Up Table Approach,” pp. 1–17, 2022.

[35] K. Anggriani, S. Chiou, N. Wu, and M. Hwang, “A High-Capacity Coverless Information Hiding Based on the Lowest and Highest Image Fragments,” 2023.

[36] R. Campbell, J. Al-muhtadi, P. Naldurg, G. Sampemane, and M. D. Mickunas, “Towards Security and Privacy for Pervasive Computing *,” pp. 1–15, 2003.

[37] J. Qin, Y. Luo, X. Xiang, Y. Tan, and H. Huang, “Coverless image steganography: A survey,” *IEEE Access*, vol. 7, pp. 171372–171394, 2019, doi: 10.1109/ACCESS.2019.2955452.

[38] [M. Hussain, A. W. Abdul Wahab, N. Javed, and K.-H. Jung, "Hybrid data hiding scheme using right-most digit replacement and adaptive least significant bit for digital images," *Symmetry,* vol. 8, p. 41, 2016.

[39] H. Y. Lee, “Adaptive reversible watermarking for authentication and privacy protection of medical records,” Multimedia Tools and Applications, pp. 1-18,2019.

[40] information security (infosec) https://searchsecurity.techtarget.com/definition/information-security-infosec.

[41] S. Dhawan and R. Gupta, “Analysis of various data security techniques of steganography : A survey “, Information Security Journal A Global Perspective, vol. 9, no. 30, pp. 1–25, 2020, doi: 10.1080/19393555.2020.1801911.

[42] M. Saravanan and A. Priya, “An Algorithm for Security Enhancement in Image Transmission Using Steganography,” pp. 1–8, 2019, doi: 10.33969/JIEC.2019.11001.

[43] M. A. Majeed, R. Sulaiman, Z. Shukur, and M. K. Hasan, "A review on text steganography techniques," *Mathematics,* vol. 9, p. 2829, 2021.

[44] Ritu Sindhu, and Pragati Singh , " Information Hiding using Steganography’, *International Journal of Engineering and Advanced Technology (IJEAT*) , Vol. (9), No 4, April, 2020.

[45] M. Y. Valandar, P. Ayubi, and M. J. Barani, “A new transform domain steganography based on modified logistic chaotic map for color images,” *Journal of Information Security and Applications*, vol. 34, pp. 142–151, 2017.

[46] A. K. Singh, “Steganography in Images Using LSB Technique,” vol. 5, no. 1, pp. 426–430, 2015.

[47] 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.

[48] J. Qin, Y. Luo, X. Xiang, Y. Tan, and H. Huang, "Coverless image steganography: a survey," *IEEE Access*, vol. 7, pp. 171372-171394, 2019.

[49] Z. Zhou, Y. I. Cao, M. Wang, Q. M. J. Wu, S. Member, and E. Fan, “Faster-RCNN Based Robust Coverless Information Hiding System in Cloud Environment,” *IEEE Access*, vol. 7, pp. 179891–179897, 2019, doi: 10.1109/ACCESS.2019.2955990.

[50] G. Swain and S. K. Lenka, “Classification of Image Steganography Techniques in Spatial Domain : A Study,” vol. 5, no. 03, pp. 219–232, 2014.

[51] S. Sharma and U. Kumar, “Review of Transform Domain Techniques for Image Steganography,” no. April, pp. 2–6, 2013, doi: 10.13140/RG.2.1.4797.1928.

[52] Ehab Helmy Mohamed EL-Shazly," Digital Image Watermarking in Transform Domains", *A Thesis Submitted for the Degree of M. Sc., Department of Electronics and Communication Engineering,* Minufiya University ,2012.

[53] J. Yang, Y.-G. Jiang, A. G. Hauptmann, and C.-W. Ngo, "Evaluating bag-of-visual-words representations in scene classification," in *Proceedings of the international workshop on Workshop on multimedia information retrieval*, pp. 197-206, 2007.

[54] X. Duan and H. Song, "Coverless information hiding based on generative model," *arXiv preprint arXiv:1802.03528,* 2018.

[55] [Z. Zhou, Y. Mu, and Q. Wu, "Coverless image steganography using partial-duplicate image retrieval," *Soft Computing*, vol. 23, pp. 4927-4938, 2019.

[56] Z. K. Al-ani, A. A. Zaidan, B. B. Zaidan, and H. O. Alanazi, “Overview : Main Fundamentals for Steganography Overview : Main Fundamentals for Steganography,” no. March, 2010.

[57] J. Ashok, “STEGANOGRAPHY : AN OVERVIEW,” vol. 2, no. 10, pp. 5985–5992, 2010.

[58] C. Applications, “IMAGE STEGANOGRAPHY USING IMPROVED LSB AND EXOR ENCRYPTION ALGORITHM,” no. July, 2014.

[59] T. Morkel, “I MAGE S TEGANOGRAPHY A PPLICATIONS,” no. May, 2012.

[60] W. Mazurczyk, "VoIP steganography and its detection—a survey," *ACM Computing Surveys (CSUR),* vol. 46, pp. 1-21, 2013.

[61] H. Tian, K. Zhou, H. Jiang, Y. Huang, J. Liu, and D. Feng, "An adaptive steganography scheme for voice over IP," in *2009 IEEE International Symposium on Circuits and Systems,* 2009, pp. 2922-2925.

[62] K. Stefan and P. Fabien AP, "Information hiding techniques for steganography and digital watermarking," ed: Artech House, 2000.

[63] B. Zaidan, A. Zaidan, and M. Mat Kiah, "Impact of data privacy and confidentiality on developing telemedicine applications: A review participates opinion and expert concerns," *International Journal of Pharmacology,* vol. 7, pp. 382-387, 2011.

[64] H. N. AlEisa, "Data Confidentiality in Healthcare Monitoring Systems Based on Image Steganography to Improve the Exchange of Patient Information Using the Internet of Things," *Journal of Healthcare Engineering,* vol. 2022, 2022.

[65] N. Subramanian, O. Elharrouss, S. Al-Maadeed, and A. Bouridane, "Image steganography: A review of the recent advances," *IEEE access,* vol. 9, pp. 23409-23423, 2021.

[66] O. Hosam, “Attacking Image Watermarking and Steganography - A Survey,” no. March, pp. 23–37, 2019, doi: 10.5815/ijitcs.2019.03.03.

[67] K. Y. Ng, S. Ong, and K. Wong, “Delving into the Methods of Coverless Image Steganography,” no. November, pp. 1763–1772, 2019.

[68] Q. Liu and X. Xiang, “Coverless image steganography based on DenseNet feature mapping,” EURASIP Journal on Image and Video Processing, vol. 7, 2020.

[69] R. F. Martinez-Gonzalez and J. A. Diaz-Mendez, "Implementation of a Stream Cipher Based on Bernoulli's Map," *arXiv preprint arXiv:1501.01463,* 2015.

[70] C. V. Reddy and P. Siddaiah, "Hybrid LWT-SVD watermarking optimized using metaheuristic algorithms along with encryption for medical image security," *Signal & Image Processing,* vol. 6, p. 75, 2015.

[71] F. E. Abd El-Samie, H. E. H. Ahmed, I. F. Elashry, M. H. Shahieen, O. S. Faragallah, E.-S. M. El-Rabaie, *et al., Image encryption: a communication perspective*: CRC Press, 2013.

[72] S. S. Askar, A. A. Karawia, A. Al-Khedhairi, and F. S. Al-Ammar, "An algorithm of image encryption using logistic and two-dimensional chaotic economic maps," *Entropy,* vol. 21, p. 44, 2019.

[73] R. Kharel, "Design and implementation of secure chaotic communication systems," Northumbria University, 2011.

[74] Y. Sang, J. Sang, and M. S. Alam, "Image encryption based on logistic chaotic systems and deep autoencoder," *Pattern Recognition Letters,* vol. 153, pp. 59-66, 2022.

[75] M. Y. Valandar, P. Ayubi, and M. J. Barani, "A new transform domain steganography based on modified logistic chaotic map for color images," *Journal of Information Security and Applications,* vol. 34, pp. 142-151, 2017.

[76] [G. Sathishkumar and D. N. Sriraam, "Image encryption based on diffusion and multiple chaotic maps," *arXiv preprint arXiv:1103.3792,* 2011.

[77] N. Nesa, T. Ghosh, and I. Banerjee, "Design of a chaos-based encryption scheme for sensor data using a novel logarithmic chaotic map," *Journal of Information Security and Applications,* vol. 47, pp. 320-328, 2019.

[78] N. Ramadan, H. E. H. Ahmed, S. E. Elkhamy, and F. E. A. El- Samie, "Chaos-based image encryption using an improved quadratic chaotic map," *American Journal of Signal Processing,* vol. 6, pp. 1-13, 2016.

[79] M. Sharafi, F. Fotouhi-Ghazvini, M. Shirali, and M. Ghassemian, "A low power cryptography solution based on chaos theory in wireless sensor nodes," *IEEE Access,* vol. 7, pp. 8737-8753, 2019.

[80] S. R. Davies, R. Macfarlane, and W. J. Buchanan, “Comparison of Entropy

Calculation Methods for Ransomware Encrypted File Identification,” 2022.

[81] L. Hao and L. Min, “Statistical tests and chaotic synchronization based pseudorandom number generator for string bit sequences with application to image encryption,” 2014, doi: 10.1140/epjst/e2014-02182-2.

[82] R. Journal and O. F. Information, “On the Interpretation of Results from the NIST Statistical Test Suite,” vol. 18, no. 1, pp. 18–32, 2015.

الخلاصة

هناك حاجة دائما الى ضمان سرية المعلومات عند نقلها عبر قناة عامة. تعد تقنية steganographyأحد الحلول الممكنة لتحقيق هذا الهدف. تتضمن معظم طرق إخفاء الصور الحالية المعلومات السرية بشكل غير محسوس في صورة الغلاف عن طريق تعديل محتواها. لذلك، يتسبب التعديل في بعض التشويه في الصورة الحاوية على الرسالة بالإضافة إلى ذلك، سيتم ترك هذا التعديل الناتج عن التضمين في صورة. الغلاف، مما سيجعل تقنية الكشف عن المعلومات المخفية ناجحة، وتسمى تقنية الكشف هذه أيضًا تحليل إخفاء المعلومات. للتغلب على تعديل الغلاف أثناء عملية التضمين. تم اقتراح تقنيه اخفاء الصور بدون غطاء(CIS).

ومع ذلك، تواجه CIS عدة تحديات وهي السعة العالية والدقة العالية والأمان. اقترحت هذه الأطروحة طريقة إخفاء الصور بدون غطاء. تستكشف الفعالية لتعزيز السعة والتضمين في صورة غلاف واحدة فقط بالإضافة إلى تعزيز المتانة ضد الهجمات. تقوم الطريقة المقترحة بإخفاء المعلومات غير المغطاة عن طريق إنشاء علاقات تعيين بين أكواد التجزئة لكتل الصور وكل جزء من الرسالة السرية. لحساب رمز تجزئة لصورة ما، يُقترح خوارزمية تجزئة قوية تعتمد على التخليط وتحويل المويجات المنفصل (DWT) يتم إنشاء جدول تسلسل التجزئة باستخدام خوارزمية التجزئة المقترحة. لتقليل وقت البحث، يتم إنشاء جدول الفهرسة بناءً على جدول تسلسل التجزئة الذي تم إنشاؤه. يتم تعيين كل جزء من الرسالة السرية مع تسلسل التجزئة الذي تم إنشاؤه وحفظ المعلومات المساعدة لكل مقطع مطابق في ملف يتم تشفيره باستخدام طريقة التشفير المقترحة.

وفقًا للنتائج التجريبية، يمكن لطريقة التجزئة المقترحة الحصول على جميع رموز التجزئة التي تساوي 256 رمز تجزئة في صورة واحدة ولعدد كافي من الصور على عكس الطرق السابقة التي لم تتمكن من الحصول على أكواد التجزئة كلها في صوره واحده أو حصلت عليها في عدد محدود جدا من الصور. تظهر النتائج التجريبية أيضًا أن النظام المقترح يحصل على سعة إخفاء تساوي 261،888 بت في صورة واحدة والتي تفوقت على جميع الطرق السابقة. أثبتت النتائج التجريبية أيضًا مرونة النظام ضد مجموعه متنوعه من الهجمات والتي ظهرت قيمة BER قريبه من الصفر وتفوقت أيضًا على الطرق السابقة في معيار المتانة حيث حصلت على قيمة RC أعلى منها. نظرًا لأن صورة Stego هي صورة طبيعية بدون أي آثار تعديل، يمكن للطريقة مقاومة جميع أدوات تحليل الإخفاء الحالية. أثبتت النتائج والتحليلات التجريبية أن الطريقة تتمتع أيضًا بمستوى أعلى من الأمان حيث ان قيمه إنتروبيا قريبه من 1 ، وقيمة الارتباط قريبة من الصفر ، وكذلك أثبت النظام المقترح أنه يحتوي على وقت تنفيذ قصير

وزارة التعليم العالي والبحث العلمي

جامعة بابل كلية العلوم للبنات

قسم علوم الحاسوب

إخفاء بدون غطاء بالاعتماد على الخصائص المناطقية في الصورة

رسالة مقدمة الى مجلس كلية العلوم للبنات في جامعة بابل وهي جزء من
متطلبات نيل درجة الماجستير في العلوم/ علوم الحاسبات

مقدمة من قبل

هديل طالب منجي

بأشراف

الاستاذ الدكتور
سهاد احمد علي

الاستاذ الدكتور
ماجد جبار جواد

1444 هـ

2023 م