Republic of Iraq

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

A Coverless Image Steganography Based on Secured Image Wavelet Hashing

A Thesis

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

By

Nadia Abud Al-Karim

Supervised By

Prof. Dr. Suhad Ahmed Ali

Prof. Dr. Majid Jabbar Jawad

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

بسم الله الرحمن الرحيم

ٱقۡرَأۡ بِٱسۡمِ رَبِّكَ ٱلَّذِى خَلَقَ ١
خَلَقَ ٱلۡإِنسَٰنَ مِنۡ عَلَقٍ
٢ ٱقۡرَأۡ وَرَبُّكَ ٱلۡأَكۡرَمُ ٣
ٱلَّذِى عَلَّمَ بِٱلۡقَلَمِ ٤
عَلَّمَ ٱلۡإِنسَٰنَ مَا لَمۡ يَعۡلَمۡ ٥

صَدقَ الله العَظيمْ

سُورَةُ العَلَقِ

الآيات (١-٥)

Supervisor Certification

I certify that this thesis entitled

Coverless Image Steganography Technique Based Hiding Secret Data in Image

written by

Nadia Abud Al-Karim

was prepared under my supervision at College of Science for Women
a partial fulfillment of the requirements for the degree of a Master's in Computer Science.

Signature:
Name: Prof. Dr. Suhad Ahmed Ali

Date: / / 2022

Signature:
Name: Prof. Dr. Majid Jabbar Jawad

Date: / / 2022

Head of the Department Certification

In view of the available recommendations, I forward the thesis entitled "**A Coverless Image Steganography Based on Secured Image Wavelet Hashing*****" for debate by the examining committee.***

Signature:
Name:
Date: /   / 2022
Address: University of Babylon/College of Science for Women

Acknowledgements

First of all, I thank God who inspired me with patience and strength to complete this study.

It is not easy except what God makes easy.

I would like to express my sincere thanks and appreciation to Supervisor

Prof. Dr. Suhad Ahmed Ali and Prof. Dr. Majid Jabbar Jawad

To direct and follow up on it and provide important advice and suggestions for improving this study

My sincere thanks and appreciation to the Dean of the University of Babylon and to the academic and administrative faculty.

I would like to thank the Head of the Department of Computer Science and her academic and staff colleagues.

In the end, I thank everyone who wished me success.

Finally, I apologize to those whose names were not mentioned. .But I am grateful to all of them for their help

Dedication

Praise be to Allh always and forever..Praise be to Allh who we think is good and he honors us with something better than him..Thank Allh for my success in every step of my life and passing my studies with success and excellence...Thank Allh for achieving one of the goals of my father, who was and still is the light of my path and my eyes, may Allh have mercy on you A piece of my heart..my thanks to the first supporter and the true supporter of the human being. If I gave my soul to her, I would not reward a little for a little

My thanks to my dear husband, if it were not for him, I would not have reached this stage. My thanks to my beloved sisters and everyone who stood and supported. My thanks for the gift of studying, my beloved friends.

Abstract

Information security has become the main concern of the most famous researchers and the focus of their attention, as they are constantly trying to find the best and safest ways to transfer information through a secure tunnel to protect it from hacking attempts and common attacks on the Internet and in this research. Steganography is a system for hiding information. It aims to hide secret information into a digital cover file such as image without being suspicious. On the other hand, steganalysis technique aims to detect the existence of secret data that hidden in the cover files. A steganographic system is considered broken if the attacker was able to reveal a presence or read the concealed message.

Using typical image steganography techniques, a cover image is chosen, and secret data is then inserted into it to create the stego-image. However, the embedding will leave modification traces in the cover image, making successful steganalysis easy. So, how to successfully hide information without changing the carrier are a breakthrough and a challenge. The coverless image steganography framework is a new field of research when compared to previous methods of image steganography. Coverless image steganography attempts to conceal secret information, however there are several major challenges to overcome: To hide the data, no changes to the image are required. In other words, secret information cannot be transported without a carrier, but it can be hidden by creating a carrier image that is visually identical to the original or by establishing mapping rules between carrier image and secret information. Finding relevant images that already contain the information of the secret data is one technique to conceal a secret data in coverless image steganography. Stego images are used to communicate sensitive information and are categorized as such. The biggest issue is locating photos that already contain the required information.

In this thesis; a new coverless steganography is presented to hide the secret data in a more secure way and to enhance the robustness against attacks. This method depends on frequency domain. The embedding process consists of several steps. Firstly, the secret data is encrypted by proposed encryption method based on chaotic then the encrypted data is divided into non overlapping segments. Secondly, a set of images is collected to find appropriate images to be stego images. Thirdly, to build a hash value for an image, a powerful hashing algorithm is used. Fourthly, for each image hash sequence, the inverted index structure is created. Fifthly, choose the image which its hash equivalent to the encrypted secret data. Several tests are done to measure the robustness of the proposed method.

According to the experimental results, the suggested method satisfies two requirements security and robustness. Where, the system was implemented by Matlab2020 language. Also, the experimental results illustrate the durability of the system and its resistance to a range of attacks such as noise, compression of JPG, cropping, rotation, histograms, and filters, and the values of NC and BER equal 1 and 0 respectively for types of the tested images. Also, the proposed method compare with other recent coverless method based on hashing method and the results outperform other methods in most attacks.

List of Contents

List of Figures

List of Table

List of Algorithms

List of Abbreviations

AE	Avalanche effect
BER	Bit Error Rate
BOW	Bag-of-words
CC	Correlation coefficient
CNNs	convolutional Neural Networks
DC	Direct Current
DCT	Discrete Cosine Transform
DFT	Discrete Fourier Transform
DL	deep learning
DWT	Discrete Wavelet Transform
GANs	generative adversarial networks
HOGS	on histograms of oriented gradients
HUGO	Highly Undetectable Steganography
HVS	human visual system
IWT	Integer Wavelet Transform
LDA	latent Dirichlet allocation
LSB	Least Significant Bit
MIS	medical information systems
NC	Normalized correlation
VoIP	Voice over IP
WOW	Wavelet Obtained Weights

List of Publications

This work has resulted in the following publication:

[1] N. A. Al_karim, S. A. Ali, and M. J. Jawad, "Text Hiding In Image Based On Robust Spatial Hashing Algorithm”, Journal of Positive School Psychology, pp. 2566-2576, 2022.

[2] N. A. Al_karim, S. A. Ali, and M. J. Jawad, " A Coverless Image Steganography based on Robust Image Wavelet Hashing”, Accepted in TELKOMNIKA Telecommunication Computing Electronics and Control, Vol. 99, No. 1, 2022.

Chapter One

General Introduction

Chapter One
General Introduction

1.1 Introduction

Secret communication between a sender and a receiver has become very important due to the extensive usage of multimedia data and advancements in telecommunications such as: image, audio and video. So that information that is sensitive or confidential cannot be accessed by third parties. Information hiding is normally accomplished performed using two well-known methods, steganography and watermarks, both methods directly modify the content of the media file (image, video, audio, etc.) for copyright protection and covert communication or identification of the sender. There are three basic objectives of covert communication: The message cannot be seen by anybody else while it is being transmitted; it is not modified while it is being transmitted; and the sender is who he claims to be. The science of concealing and transferring hidden information is known as steganography[1],[2]. It is a set of techniques for concealing information through the use of multimedia data, such as image, text, audio, video, video, etc.[3],[4],[5].Because people utilization of images since they are one of the most widely used media, Image steganography has attracted a lot of interest. Today, steganographic communication is a key technological advancement in the domain of information security [6], [7].

1.2 Image Steganography

Image steganography is a component of data security, where images contain sensitive or secret data, such that it is not visible and cannot be identified by the human visual system (HVS) [5]. According to the documentation available, there are two types of steganography techniques for images: image steganography with data embedding and coverless image steganography. In addition, there are two types of data embedding methods: spatial domain and frequency domain[8]. Although the human visual system does not detect the modification in the carrier image induced by data embed, the disadvantage of spatial domain approaches such as Least Significant Bit(LSB)[5],[9], Highly Undetectable Steganography (HUGO)[1] and Wavelet Obtained Weights(WOW)[10] are that they are not resistant to normal image and steganalysis attacks[11]. As a result, frequency domain algorithms such as the Discrete Fourier Transform (DFT)[12], Discrete Wavelet Transform (DWT)[13], Discrete Cosine Transform (DCT)[14],and Integer Wavelet Transform(IWT)[15] have been presented that use modified coefficients for data embedding. These methods are more resistant to image attacks, but they are more computationally complexity.

The coverless image steganography framework is a new field of research when compared to previous methods of image steganography. Coverless image steganography attempts to conceal secret information, however there are several major challenges to overcome:-

- To hide the data, no changes to the image are required. In other words, secret information cannot be transported without a carrier, but it can be hidden by creating a carrier image that is visually identical to the original or by establishing mapping rules between carrier image and secret information[15].
- Finding relevant images that already contain the information of the secret data is one technique to conceal a secret data in coverless image steganography. Stego images are used to communicate sensitive information and are categorized as such. The biggest issue is locating photos that already contain the required information[16].

- The coverless image steganography strategies can resistance image steganalysis tools and considerably increase image security since hiding critical or confidential information does not modify the image and can resist attacks such as contrast change, brightness, noise addition, and rescaling[17], rotation[18], JPEG compression[19] etc.

1.3 Related Works

Briefly, this section reviews some of previously proposed methods related to coverless image steganography.

Zhou et al. proposed a coverless image steganography method in 2015, based on the spatial domain, in which an image can be represented by 8 bits of information using a hashing algorithm to generate hash sequences. For all hash sequences, including lookup tables, an inverted index structure is created. The approach is tested against several image attacks that are common such as JPEG, contrast, and scaling attack[20].

In 2016, a coverless steganography based on BOW (Bag-of-words) was proposed by Z. L. Zhou et al. The BOW concept is used for hiding text information. To hide text information in an image, visual words are recovered to represent text information. To extract visual words from an image set, a BOW model is utilized, and a mapping connection is established between keywords in text information and visual words. The following step is the division of each image into several sub-images .A histogram of visual words is created for each sub-image, and visual words having the largest values in the histogram selected to represent the sub-image. The mapping relation is used to find a group of sub-images with visual words related with text information. For secret communication, Stego images are images that include these sub-images [21].

In 2017, Z. L. Zhou et.al. A method for coverless image steganography is proposed based on histograms of oriented gradients (HOGS) and Hashing. Instead of selecting a cover image for secret information embedding, the original images with hash sequences matching the secret information are extracted direct from a huge database and utilized as stego images for secret communication, using the HOGs-based hashing technique to generate hash sequences. The process of creating hash sequences is split into three phases. Each database image is converted to a gray_level before being divided into 4 non-overlapping blocks. The HOGs features are extracted from each image blocks. To create the block's hash sequence the mean value of all entries is compared to each item's value in the HOGs histogram; if the block's HOGs are larger than the mean value, the value is 1, otherwise it is 0)[22].

In 2018, Xiang Zhang et al. proposed a coverless image steganography technique that makes use of the discrete cosine transform and the latent Dirichlet allocation (LDA) topic model. In First, latent dirichlet allocation topic model is used for classifying the image database. Second step, the images belonging to one topic are choosed, and 8 × 8 block discrete cosine transform is performed to these images. Then robust feature sequence is generated through the relation between direct current coefficients in the adjacent blocks. Finally, an inverted index which contains the feature sequence, dc , location coordinates, and image path is created[23].

In 2019, Liming Zou et.al proposed a method generates a set of hash sequences for the Chinese dictionary. The the secret information is divided into four segments, the a hash sequences that are corresponding to these segments are generated depending on hashing algorithm. This method then maps the dictionary and the array through a mapping relationship. It can be efficiently used to retrieve the hidden information from the image and it achieve the aim of concealing information using the Chinese language[24].

In 2020, Y. Luo et al. proposed coverless image steganography method based on image block matching and dense convolutional network. This approach transfers a set of stego-images instead of the chosen image for embedding the secret data, which share one or more visually similar blocks with the given secret image. The DCT coefficient and supervised deep learning improve retrieval accuracy and robustness, this method provides a deep learning-based coverless information hiding technique. The proposed method with no change traces try to improve the robustness, and retrieval accuracy according to experimental data[25].

In 2020, Xiang Zhang et al. proposed a fractal-based generative coverless image information hiding approach to improve and make more imperceptible the existing coverless image information hiding. First, four methods for creating fractal images are examined, and the connection between the coverless information hiding and these techniques is explained. The second method is based on the fractal image generating algorithm, which controls pixel rendering during the generation process to conceal secret information [26].

In 2020 Yi Cao et al. proposed a coverless information hiding method based on the generation of anime characters. It first transforms the secret data into a set of the characters' attribute labels, and then it uses the label set as a driver to create anime characters directly using generative adversarial networks (GANs) [8].

QiLi et. al. proposed an encrypted coverless information hiding method based on generative models. The encryption and decryption stages of this process involve sending secret images between two image domains. The hidden image is initially integrated into a public image during the encryption step. After that, the image is input to a generative model, which then produces an encrypted image. An extraction module and an adversarial loss algorithm are then used to enhance the quality of the images generated during the encryption stage. A second generative model is created in the decryption stage to recreate the synthetic images from the encrypted images. Lastly, The synthetic image that was constructed is isolated from the hidden image[27].

In 2020, a CIS algorithm based on DenseNet feature mapping is proposed. One uses deep learning obtaining hash sequences that map high-dimensional CNN features. A binary tree hash index is built to accelerate the search for hidden information and the DenseNet hash sequence for the sender, and all matching pictures are then provided. Calculating the cover image's DenseNet hash sequence enables the recipient to successfully retrieve the secret information. The cover images are unchanged during the whole steganography process [28].

In 2021, Qiang et. al. proposed a method for coverless image steganography. The proposed method provides a deep learning-based coverless information hiding technique with no change traces try to improve the robustness against geometric attacks. The approach is tested against several image attacks that are common such as JPEG, contrast, and especially in the robustness of geometric attacks[29].

1.4 Problem Statement

Techniques to secure sensitive information from plagiarism are offered as a result of the rapid growth of emerging technologies and information distribution. Information hiding is a popular security strategy. Traditional image steganography techniques generate a stego-image by producing a cover image and putting concealed data inside it. The modification indications created by the embedding, on the other hand, will be left in the cover image, allowing for successful steganalysis. So, how to successfully hide information without changing the carrier are a breakthrough and a challenge. Coverless image steganography is a technique for embedding secret data that differs from ordinary image steganography. coverless steganography still has several chanllanges such as low robustness and security. T, this thesis addressed the following problems:

- The concealment of secret information within digital images in such a way that an opponent is unable to obtain the secret information. The hiding method focus on how to represent image features and establish a map relationship between image feature and the secret information.
- In this thesis, two of the key challenges of coverless steganography will be considered which include accuracy and security. The accuracy aspect focuses on finding a set of images that already contain the required information while the security can verify by finding a good mapping between secret information and selected image. Two factors of steganography's security are its resistance to steganalysis tools and its protection against attackers.

1.5 Aim of Thesis

The aim of thesis includes several aspects such as:

- Building a large dataset for the purpose of coverless steganography.
- Proposing an efficient and secure method for hiding information. It is difficultly discoverable by using coverless steganography. This method depends on finding the good image features that corresponding with secret information.
- Proposing a method for secret data encryption based on chaotic concept that ensures that the data privacy is protected.

1.6 Thesis Contributions

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

- The proposed embedding and extracting procedures, approximately, met most requirements of coverless information hiding, which can be listed as follows: -
    - Robustness: After applying some known attacks, the image extracted with acceptable error. The proposed method should have the ability to be resist against attacks such as contrast change, luminance, noise addition, rescaling.

- Security: In the proposed system, the chaotic based encryption technique is proposed for encrypting of the embedded process. This procedure adds another layer of security that can be used for preserving the confidentiality of secret message.

1.7 Organization of Thesis

The remaining of this thesis is organized in the following chapters:

- **Chapter two: Theoretical Background**

  This chapter will provide the background overview about coverless information hiding science, fundamental of digital image, coverless image steganography, and possible attacks on steganographic system.

- **Chapter three: Proposed Coverless Image Steganography System (CISS)**

  This chapter explains the Proposed Coverless Image Steganography System (CISS). In addition, this chapter discusses the algorithms of the proposed system.

- **Chapter four: The Experimental Results**

  The experimental results of the proposed system will be presented in this chapter.

- **Chapter five: Conclusions & Suggestions of Future Works**

This chapter shows the major conclusions and suggestions for future action from the results of the proposed system.

Chapter Two

Theoretical Background

Chapter Two
Theoretical Background

2.1 Introduction

Due to the increasing number of digital information, the security of this data has become a major concern. Image steganography, which tries to communicate hidden information through cover images, where has appeared recently as one of the most difficult and important areas of information security. So the Coverless image steganography has become one of the most crucial techniques in protecting this data. This chapter discusses the theoretical background related to the suggested system. In addition, it reviews the information hiding techniques which can be classified into two techniques namely, digital watermarking and steganography. Also, this chapter discusses the principle of the coverless image steganography, its challenges, classification and possible attacks on stenographic algorithm.

Information Hiding

The art and science of concealing confidential data so that its presence is undetected is known as information hiding [30]. Information hiding refers to the process of hiding information into a server to achieve a certain goal[31]. It classified into two branches namely digital steganography and watermarking as shown in Figure (2.1).

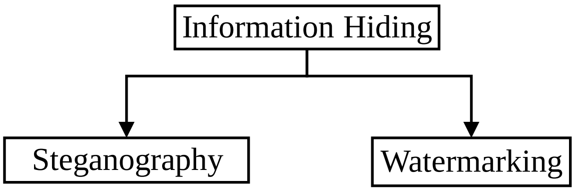


Figure (2.1): Classification of security system

2.2 Steganography

Steganography is different from other data hiding techniques in that it allows an organization or individual to conceal a secret message without revealing by the attacker or the intruder. It's a method of transmitting secret information without raising suspicions about its presence. Steganography tries to conceal information in original – cover – data in such a way that a third party studying the information contains stego data is unable to determine its presence[32]. Steganography is a type of information hiding that tries to hide the embedded data in a message. It is a more secure method of protecting messages than encryption [33]. Steganography methods can be classified according to following:

- The cover in which the secret message is embedded.
- The domain in which the secret message is embedded.

2.2.1 Steganography Based on the Cover Type

Figure (2.2) shows the classifications of steganography method according to the cover type.

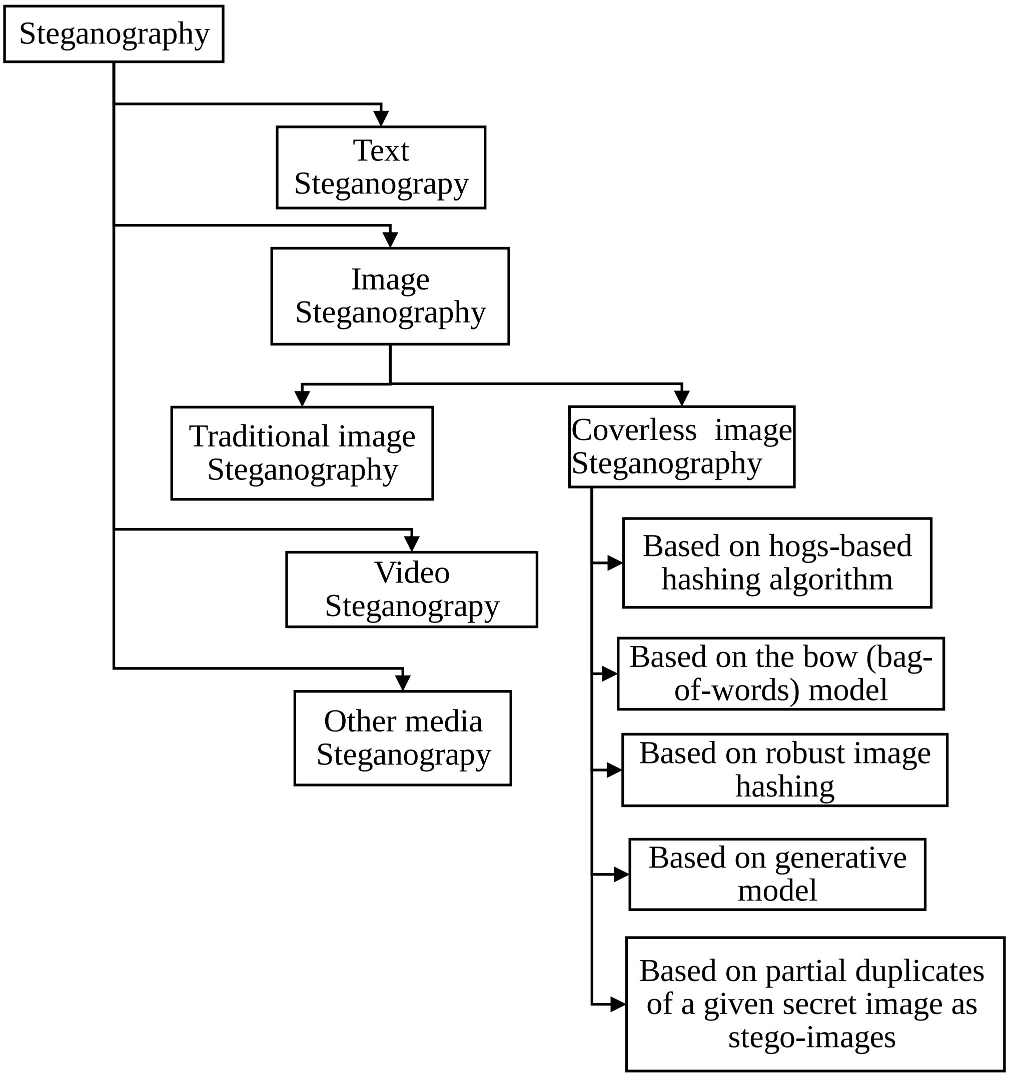

Steganography
Text Steganograpy
Image Steganography
Traditional image Steganography
Coverless image Steganography
Video Steganograpy
Other media Steganograpy
Based on hogs-based hashing algorithm
Based on the bow (bag-of-words) model
Based on robust image hashing
Based on generative model
Based on partial duplicates of a given secret image as stego-images

Figure (2.2): Classification of the Steganography according to the cover

2.2.1.1 Text steganograohy

There are three major categories for this technique. The first one involves hiding the secret message inside a text file [34], which include: (i) Format-Based Methods - This method can be achieved by adding spaces between words and non-displayed letters.(ii) Linguistic Methods: This method includes linguistic analysis. (iii) Random and Statistical generation method:is generating cover text according to the statistical properties. This method is based on character sequences and words sequences. Text steganography is the most difficult kind of steganography since text files lack the same redundancy as other digital media like image, audio and video [35].

2.2.1.2 Video Steganograpy

This method of steganography involves hiding the secret message within a video file. Video steganography is a technique for concealing data or information within video frames. A video is composed of a series of frames or images that are used to conceal text messages. There are a variety of strategies for hiding data in different frames of video that are invisible to the human eye. Several approaches directly inserted data in the cover frame with no modifications and excellent quality. Nowadays, steganography works heavily on data concealing in video frames [36].

2.2.1.3 Image Steganogeaphy

This type of steganography means embeddig the secret message into image file[37]. This type can be classified into two types namely Traditional Image Steganography and Coverless Image Steganography as shown in Figure(2.2).

A. **Traditional Image Steganography**: The standard image steganography method creates a cover image and then stores the secret information in the carrier data With a simple adjustment. Figure(2.3) illustrates the general block diagram of traditional image steganograpy.

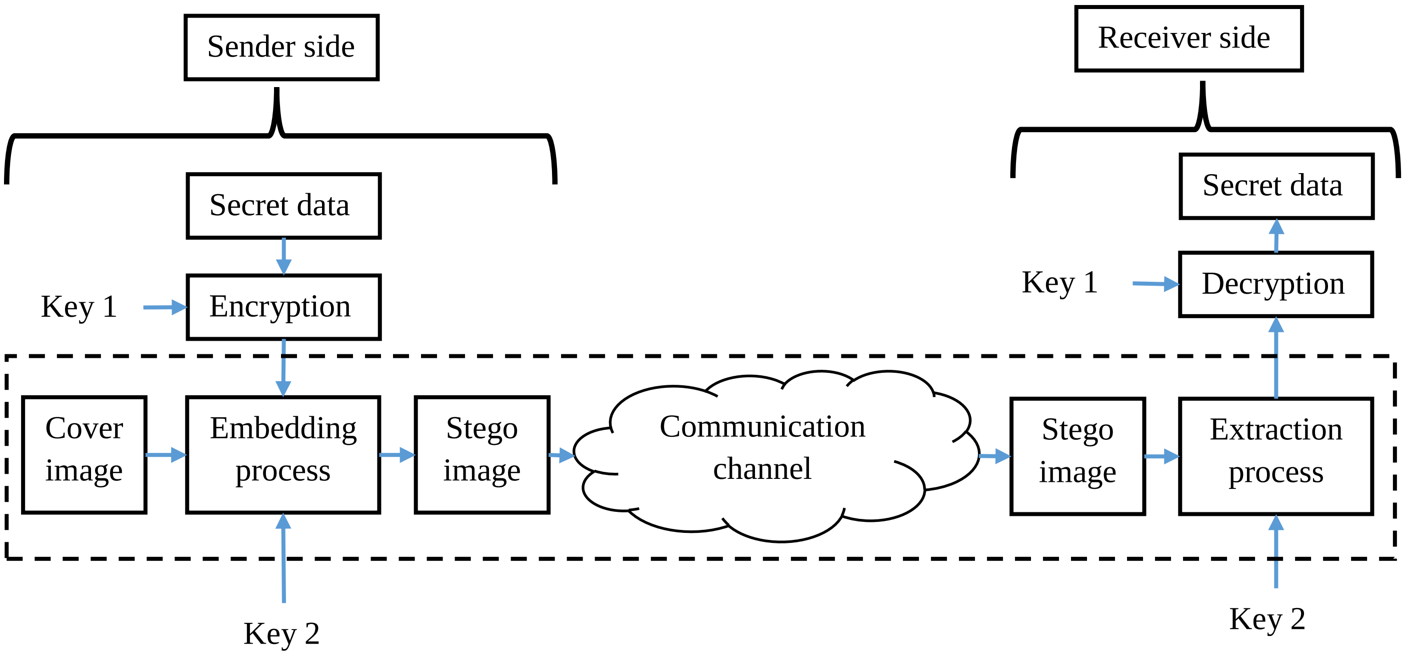


Figure (2.3) : General block diagram of traditional image steganography system [38]

In particular, the equation can be used to represent an embedding system can be represented as follows:

$$C' = Em (C, En (S, k 1) , k 2) \qquad ... (2.1)$$

The secret data and the cover image are represented by the symbols S and C respectively, C' represents stego-image. The keys to the secret data are also shown k1 and k2 for the encryption and embedding functions. The image is then delivered to a channel, where a decryption algorithm is used to decrypt it ,which represent as follow:

$$S r = D (Ex (C^*, k 2) , k 1) \qquad …(2.2)$$

The function D(.) is used to decrypt the data, while the function Sr is the retrieved secret data. The symbol C* is used to represent the deformed (due to channel noise or intruder’s attacks)stego-media, which is caused by an intrusion attack or channel noise. Ex(.)is the extraction function, while the function D(.)is the decryption function. However, traditional image steganography has a critical flaw in that the modification traces created by embedding are left in the cover image, making successful steganalysis impossible[39].

B. Coverless Image Steganography

Several years ago, the concept of coverless image steganography was proposed. This method has a lot of potential due to the lack of readable and invisible text [40]. Coverless image Steganography does not imply non-use of the carrier, but it does imply non-change of the carrier. Its own attributes are used to express the secret information, including pixel brightness value, color, texture, edge, contour, and high-level semantics. The main idea of coverless image steganographic is to map the secret information to the carrier's characteristics. This method can be performed by analyzing the characteristics of the carrier[39].

Figure(2.4) illustrates the general block diagram of coverless image steganograpy.

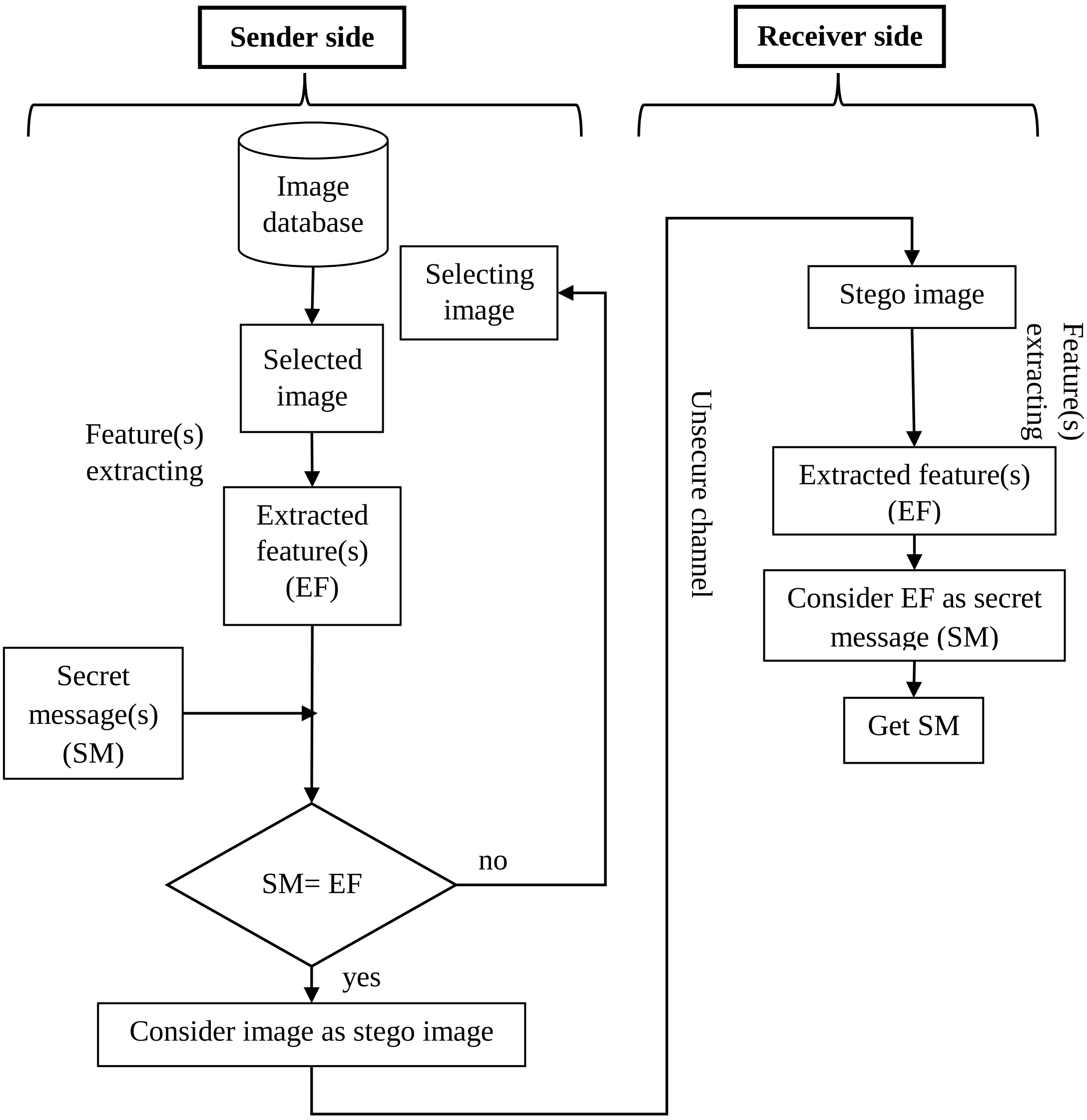


Figure (2.4): General block diagram of coverless

The following are the important contributions of coverless image steganography**-:.**

- Secret communication is possible without changing the stego-image**.**
- This Existing steganalysis tools cannot detect hidden information since the stego-image has not been changed.

2.2.2 Steganography Methods Based on the Embedding Domain

In these methods, the embedding process is done either in spatial domain or in frequency domain. Although spatial domain techniques can allow for imperceptibility and concealment of more information, they are not as effective as other data hiding techniques due to their lack of resistance to attacks. For this reason, frequency domain techniques are proposed that use transformed coefficients for data embedding, such as the Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT).

2.2.2.1 Discrete Wavelet Transform

It is utilized in a variety of media applications, including audio and video compression and digital image watermarking. A sequence of filters are used to calculate an image's DWT. The samples are passed through a low pass filter, L, and a high pass filter, H. The signal that results out of each filter has the same number of samples as the original signal. This means that the signal with double the number of particles is a double-sampler signal. This is done through a method called down sampling. In this case, half of the samples are discarded. The output of a low pass filter is used to give the approximation coefficients(LL), which are the high-scale, low frequency components. while the output of a high pass filter is used to give the detail coefficients, which are the low-scale, high frequency components. The sub-bands of the signal are the high-scale components that are most important to the signal. This transformation is done using wavelet filters.

The wavelet transform is a multi-resolution technique that can be used to analyze the image in three spatial directions: vertical, horizontal, and diagonal. The DWT division of the image (I) into four bands is performed at each level as shown in Figure (2.5). The lowest level of the division divides the image into a single band called the LL,and it The most significant band coefficients are those with low frequencies, while the lowest significant band coefficients are those with high frequencies (LH, HL, HH). This process can be repeated several times depending on which application is used [41].

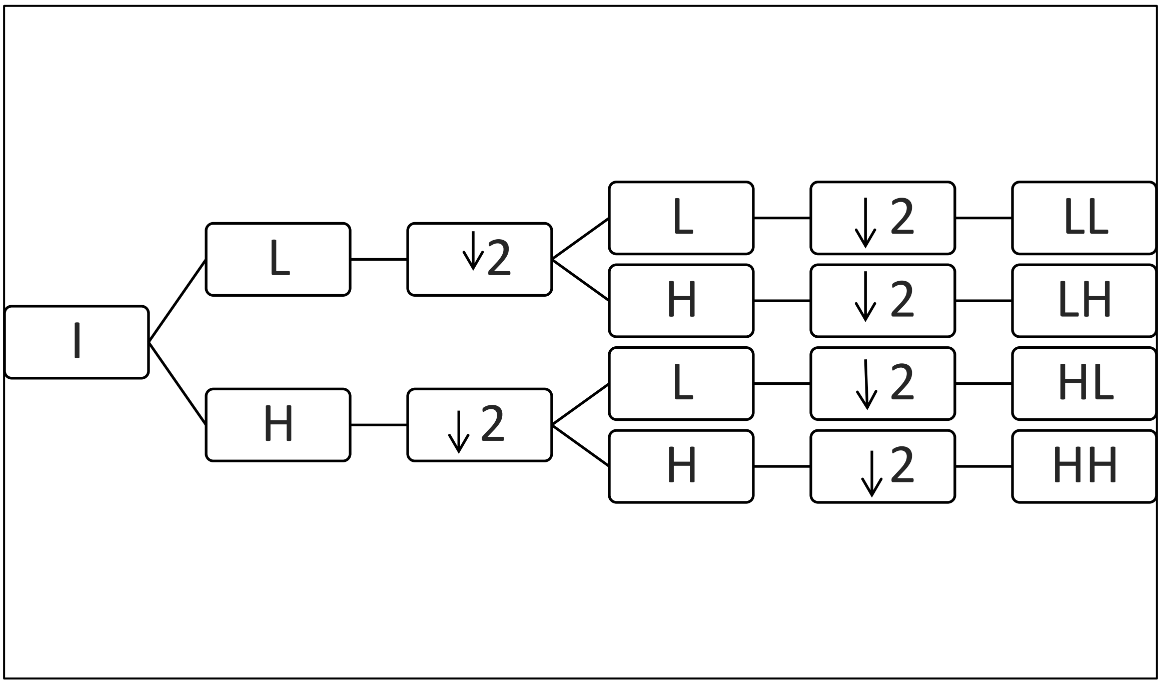


Figure (2.5): Analyzing an Image by DWT[41]

2.3 Challenges of Coverless Image Steganography

Coverless image steganography seeks to conceal secret information, but there are a few things to keep in mind: Firstly, A single feature cannot be used. Data transmission capacity and efficiency will be insufficient anyway. Secondly, To effectively transmit a message, the sender usually provides a large number of nature images in advance. These images come from various sources, which makes it difficult to accurately match the ideal situation. Thirdly, the approach must be resistant to steganalysis tools as well as attackers. To summary, The various challenges that coverless image steganography has to overcome include high accuracy, security, and capacity [39].

1. **Capacity**

Due to the various attributes of the image, the current image processing tools are not able to detect hidden information. These include its pixel brightness, texture, and edge. The old methods of information concealing involves using SIFT to produce a strong image hash in order to conceal the secret data[42]. The length of the picture's image hash sequence determines the capability of coverless image steganography. CIS method maps the relationship between the nature images and the secret information.As a result, coverless steganography is much smaller than traditional image steganography. The average amount of bits concealed inside each pixel of the cover image is referred to as the capacity, which is commonly represented in bits per pixel.

2. **Accuracy**

The entire image steganography procedure must be able to communicate complete and correct information in order to achieve high accuracy. Coverless image steganography can be used to communicate information hidden in secret images using natural images. To send messages accurately,the amount of nature images that the sender collects for sending messages is very large. Incorrect or incomplete information transmission can result in errors or even lead to the creation of an inverted index structure. Due to the nature of the image, deviations in its selection or the creation of an inverted index structure can affect the transmission of the image, At the same time, if the image is attacked in the process of transmission the image's accuracy will be decreased [39].

3. **Security**

The resistance to steganography tools and the security against attackers are two aspects of steganography security. The most common data hiding tools are working on the modication traces and the perfect image steganography method has complete resistance to all types of steganalysis tools. Moreover, because coverless image steganography relies on secret information to "generate/acquire" carriers. Most coverless image steganography techniques map the relationship between the nature images and the secret information using a mapping relationship. They then retrieve the corresponding image from the image set. If attackers can find the mapping and image data sets used by coverless image steganography techniques, they can quickly obtain the necessary details to perform their operations. Securing the secrets of your data is very important [39].

2.4 Classifications of Coverless Image Steganography Methods

There are various types of coverless image steganography techniques that can be used as follows [39]:

2.4.1 Methods based on Robust Hashing Algorithm

These techniques use a robust hashing algorithm to generate a sequence of numbers for each image in the database. For each image in the set, the sequence is generated according to the robust method. Hash sequence is compared with a segment of secret message. If they equal then the selected image represent the secret message segment. The hash algorithm must generate a robust hash sequence which can stay against different attacks.

2.4.2 Methods Based on the BOW (Bag-of-Words) model

To extract the visual words from the image set, the bag-of-words model is applied, which are then used to hide the text information in the image. The mapping relationship between the visual words and the keywords in the image is also established[43]. Each image is then subdivided into many images.To represent the sub-image, the values of the visual words are then calculated in the histogram. Additionally, a relationship is built between the visual words and the image's keywords. These sub-images are then used to hide the text information in the image.

2.4.3 Method Based on Generative Model

The method in [44] is the first one to introduce a framework of a generative model-based coverless image information hiding approach. The hidden image in the generative model database is used to create regular and independent images with a variety of meanings. The receiver then receives the created image, which is then inserted into the model database to create another image that is identical to the secret image. Both the sender and the receiver use the identical data set and parameters. To have the same result as the secret image transmission, transimt the average standard image, which is unrelated to the secret image.

2.4.4. Method Based on partial duplicates of a given secret image as stego-images

This method does not require any changes in order to communicate the secret color imag[45]. Firstly, The database generated by this framework is then used to construct a large-scale image database. Then, each image is separated into number of non-overlapping patches. The label for each patch computed using the robust hashing algorithm is then used to identify the patch that is used to hide the secret information. The location of the image is also computed using the hashing algorithm. It's important to note that the sender and receiver share the location information as a secret key. Using the hierarchical BOW, each image patch's feature is extracted, and an inverted index structure is created. The first stage in concealing the secret image is to divide it into multiple identical patches. Then, using the inverted index files, the partial-duplicate image that contains the same patches with the hidden image is retrieved for each patch. Following that, a number of partly duplicate images, known as stego-images, are obtained.The framework then sends the images to the receiver, where the position information of the hidden image is extracted. The extracted patches can then be used to retrieve the hidden image.

2.5 Applications of image Steganography

Steganography is used in a variety of fields because data privacy and secrecy are becoming increasingly important challenges as Internet communication technologies advance. Steganography have been used in many applications to hide their data in recent years.

For example ,image search engines that analyze the network traffic of individual clients in order to insert a unique identifier smart identity card (ID) applications, which convert a number into an image, and smart identity card (ID) applications, where personal information is stored on a smart card A photograph conceals information[46].

Digital steganography also offers appealing properties that make it suitable for real-time applications. To adapt Voice over IP (VoIP) services, a large range of steganography techniques have been developed. Because IP telephony is so widespread, VoIP steganography has gained in popularity[47] . Furthermore, because of the contained message, short VoIP conversations do not provide eavesdroppers enough time to detect any anomalies[48].The use of VoIP steganography differs from the use of a standard file type like text, image, or audio. It's a real-time strategy that hides the existence of secret material in real-time communication by using VoIP signals[47].

In [49], Some modern domains that use the method of hiding messages are mentioned in this article. In terms of preserving electronic patient data, the digital steganography approach has played a critical role inside medical information systems (MIS).

The basic application of steganography in medical imaging systems was proposed to provide a solution for the authentication problem, where sometimes the relation between the patient' s information and their image is lost. Therefore, steganography is employed to embed patients' information and diagnosis reports inside their medical images. A survey of the effect of information security and confidentiality on designing telemedicine application is accessible[50],[51,[52].

In recent years, business security has become essential to the security of countries, as they deal with large transactions that need to be confidential. Each organization must preserve data from potential attackers with the aid of steganography methods.

2.6 Attacks on Image Steganography[53]

The transmission process of an image can be affected by various factors such as a transmission error or noise. One of the most common attacks that occur during the process of image transmission is destruction of the secret data. This issue is important to know in order to develop a more robust and secure coverless steganography technique. The attacks on image steganography can be classified into two categories as follows:

1. Passive Attack: The attacker aims at knowing the details and information of the embedded information without compromising the image quality. In other words, an attacker does not try to remove or destroy the secret information and this directly affects confidentiality of the digital image.

2. Active Attack: In this attack, the hacker attempts to make some changes on the data. Salt **&** pepper, Gaussian and speckle noise attacks, JPEG compression are examples of this type of attacks.

2.7 Evaluation Metrics of Coverless Image Steganography Algorithm

The design of coverless steganography system needs to assess the efficiency and performance of the system. To evaluate the coverless steganography system, it is necessary to measure robustness of extracted secret message.

- **Robustness measures**

To measure the robustness of the proposed algorithms two measures are used these are normalized correlation (NC) and bit error rate (BER). Normalized correlation is used to measure the resemblance among the extracted secret information and the original ones and Bit error rate is used for measuring the error rate between the extracted secret information and the original [54]. NC is calculated as follows:

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

While BER is calculated as follows:

$$BER = \frac{\sum_{i=1}^{n} MS_{cg}\,(i) \otimes EMS_{cg}\,(i)}{n} \qquad \dots (2.4)$$

Where MS_{cg} the original secret message and EMS_{cg} is the extracted secret message.

Another measurement for robustness is Extraction Accuracy (RC) which can be defined as the following:

$$RC = \frac{\sum_{cg=1}^{n} f(EMS_{cg})}{n} \qquad \ldots (2.5)$$

Where

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

During the transmission process, it is impossible to avoid any kind of content degradation, including image noise. Each stego image selected from the database to represent the secret data segment is subject to these attacks. These variables must be able to withstand the information collected from the image. To put it another way, the hash algorithm is resistant to these types of attacks.

2.8 Chaotic Encryption

In order to protect the privacy of secret information, many organizations have been using encryption. This method involves changing the information in a file through an algorithm. It prevents unauthorized access to the data[55]. The result of an encryption algorithm is called encrypted text. There are various types of encryptions, such as asymmetric and symmetric. In asymmetric type, a public key is used while in the case of asymmetric, a private key is used[56].

Due to the increasing number of encryption algorithms being introduced, many companies have started using chaotic encryption as an alternative to the traditional method[57] [58] [59] [60]:

✓ **Deterministic system:** means that chaotic systems are governed by some deterministic mathematical formulae.

✓ ***A periodic long-term behavio***r: 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.

✓ **Sensitivity towards initial conditions and parameters**

One of the main advantages of chaotic functions is their ability to perform large changes in the input values without affecting the system's behavior. This feature is commonly used in information hiding techniques [61] [62].

The chaos streams are generated by using several chaotic maps. The latter are considered as a non-linear, dynamic system used to generate random sequences that are used in many applications. There are several types of chaotic maps such as a logistic map, tent map, quadratic map, Bernoulli map, and others [63]. In general, any chaotic map can be defined according to equation (2.6)

$$x_{n+1} = f(x_n) \quad , n = 1,2, \quad ...\text{n} \qquad \ldots(2.6)$$

Where x_n is called the state of iteration n, the function f is mapping the state x_n to the next state $x_{\text{n+1}}$.

In this study, the logistic map is used to generate randomize sequential keys to encrypt secret information. The logistic map is defined according to equation (2.7) [64].

$$x_{n+1} = r - (x_n)2 \qquad , \qquad \ldots(2.7)$$

Where n represents the iterations number, r is the parameter of chaos, and x_n is a number between zero and one.

2.8.1 Encryption Evaluation Metrics

When implementing an encryption algorithm, the values of the original data are changed. A good algorithm should make these changes in a way that reduces the difference between the encrypted and the original data [57].

The importance of an encryption algorithm is not only to reduce the difference between the original and encrypted data, but also to ensure that the data is independent of the original. The following metrics will be used to measure the performance of the encryption algorithm:

- **Correlation coefficient Test**: - One of the most crucial statistical metrics is it. The amount of difference between the original data and the encrypted data is represented by the value of it. It highlights the amount of dependence between the original data and the coded one. When the correlation coefficient value is close to 1, it means that there is a great correlation between the two images. Therefore, the encryption system is weak when the value of (CC) high. If the value approaches to 0, then this indicates to efficiency and strength of the coding system [64]. The correlation coefficient has the formula shown in equation (2.8) below:
  - $$r = \frac{\sum_m \sum_n (A_{mn} - A^-)(B_{mn} - B^-)}{\sqrt{(\sum_m \sum_n (A_{mn} - A^-)^2 (\sum_m \sum_n (B_{mn} - B^-)^2}} \qquad \ldots (2.8)$$

Where A and B represent the original and the encrypted data respectively, A' and B' represent the average of the original data and encrypted data respectively.

- **Entropy:** A system's randomness is measured by the information entropy. The amount of randomness in a system increases with increasing entropy. Information entropy H of a discrete random variable X with possible values of {x1, x2, ... , xn} can be defmed as equation (2.9) , where p(.) denotes the probability mass function of X .

$$H(S) = -\sum_{i=0}^{N-1} p(s_i) \log_2 p(s_i) \qquad \ldots (2.9)$$

- **Avalanche effect:** The Avalanche Effect describes how modifications to the plaintext have an impact on the ciphertext for a good cipher. When the input is only slightly altered, the algorithm generates an entirely different result. This metric is used to test the efficiency of diffusion. A good encryption algorithm should be able to produce significant changes in the output bits after a small change in the key or the plaintext should produce a significant change in the cipher text (about half of the output bits must vary) [65]. The Avalanche effect (AE) can be calculated according to the equation (2.10):

$$AE = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} [(C(i,j) * C\prime(i,j)^2]}{M * N} \qquad \ldots \quad (2.10)$$

2.9 Color Image to Gray Scale Conversion

The RGB color image is converted to grayscale (G) by forming a weighted sum of the R, G, and B components as follows:

G=0.2989 * R + 0.5870 * G + 0.1140 * B ,… (2.11)

Chapter Three

Coverless Image Steganography System (CISS)

Chapter Three

Coverless Image Steganography System (CISS)

3.1 Introduction

Due to the advancement in telecommunications and the widespread use of multimedia data such as image, audio and video, secret communication between a sender and a receiver is necessary so that third parties cannot access sensitive or confidential information. This chapter describes the proposed system which is based coverless image steganography technique is used for embedding the secret data, when compared to traditional methods of image steganography, does not require modifications to the image to hide the data, this does not mean that secret information can be transferred without a carrier. Some algorithms, procedures, and figures are used in the proposed system will be illustrated in this chapter.

3.2 The Proposed Coverless Image Steganography System (CISS)

In this section, the proposed coverless image method is explained in details. Figure (3.1) displays the suggested general block diagram of Coverless Image Steganography System (CISS). The proposed method consists of two procedures, namely embedding procedure and extracting procedure.

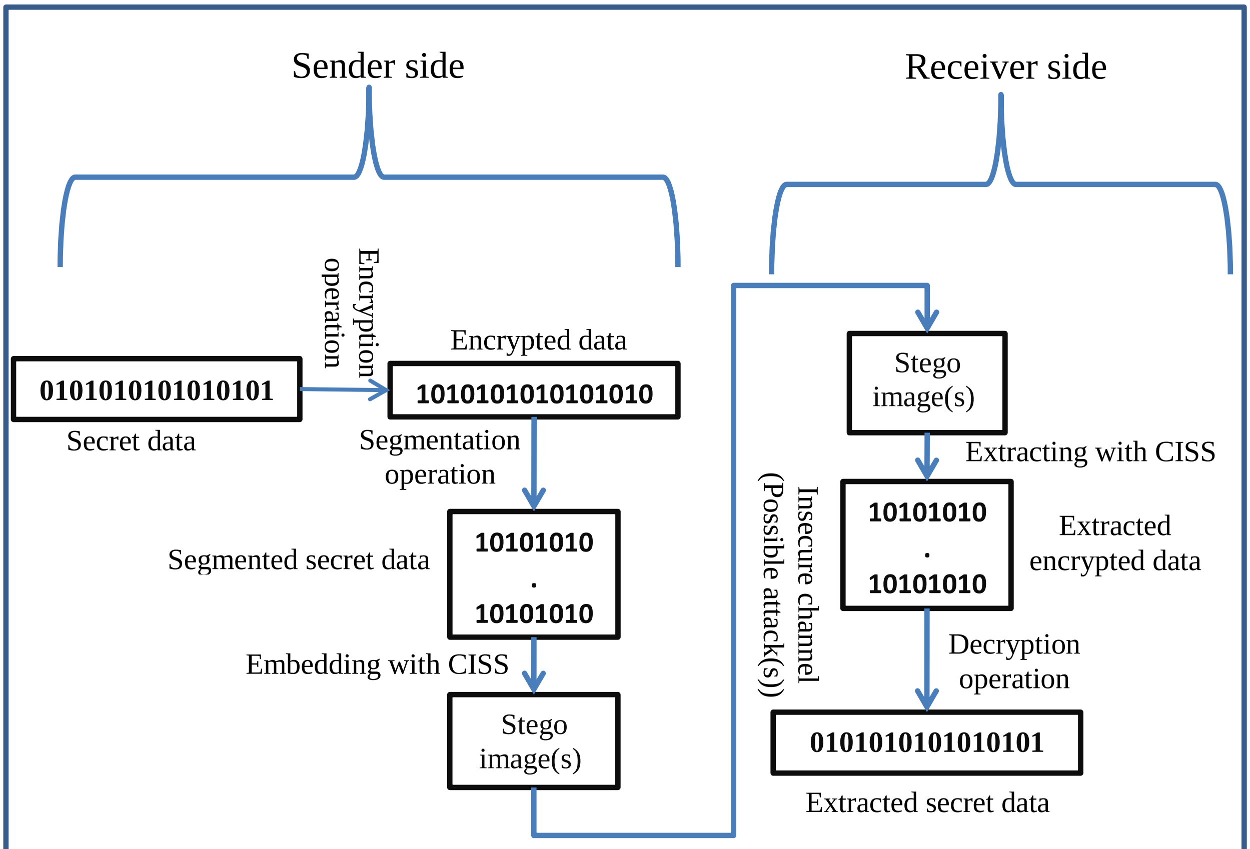


Figure (3.1): General block diagram of general CISS system

3.2.1 Activities at the Sender Side

At the sender side, several activities are being done as described in Algorithm (3.1):

Algorithm (3.1): Sender Activities

Input: SD //secret data
{pic_1,pic_2,....,pic_n } //Images in database
Outputs: {Pc1,Pc2,…,PcMsegment} //Cover Images corresponding to secret data

Begin
Step1: First, Chaotic-based encryption is used to encrypt secret data (SD) to obtain encrypted secret data (EM).
Step2: Then, encrypted secret data (EM) is split into 8-bit-long pieces. Specifically, EM = EM_1, EM_2, ...,EMn When this segment ends, zeros will be added to the end of M_i if it is less than 8 bits.
Step3: Bulding Hash table for all images in the dataset by calculating the hash sequence of all images . The details of hash sequence are described

```
in 3.2.3.1.
Step4:Do for all message segments
  Step4-1: According to the mapping relationship between Hash table and segment sequence , choose the appropriate image $Pic_i$ from the images database for the 8-bit-length segment to obtain cover image $Pc_i$.
    Step 4-2: Continue until each segment has been produced.
Step 5: All cover images $\{pc_i\}$ are sent to the receiver in order.
End
```

The following sections describe the details of each activity.

3.2.1.1 Secret Data Encryption

In this activity, the secret data is encrypted. This activity improves the security of CISS. Figure (3.2) illustrates the encryption procedure. The following steps describe the encryption procedure:

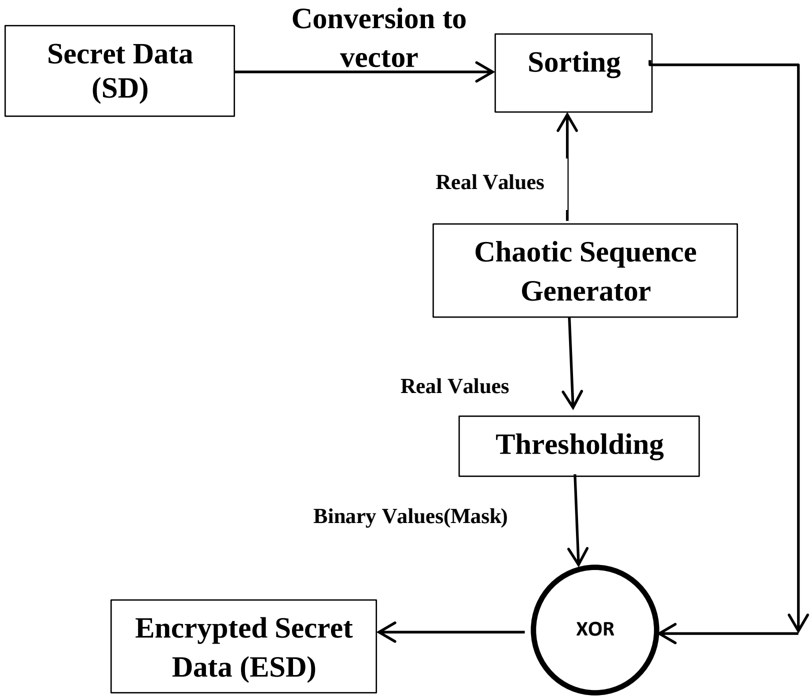


Figure (3.2): Secret data encryption

A. Scrambling the Secret Data

The following steps is used for scrambling the secret data:

- Converting the input secret data into a 1D vector (v- Data)
- Creating a chaotic sequence (Chaotic_ Seq) with length equal to (v- Data) using the logistic chaotic system equation (2.7). The result of equation (2.7) is real numbers between [0, 1]
- Sorting the result of equation (2.7).
- Rearrange the positions of the secret data according to the results of the sorted data. Figure (3.3) shows the steps of scrambling of secret data.

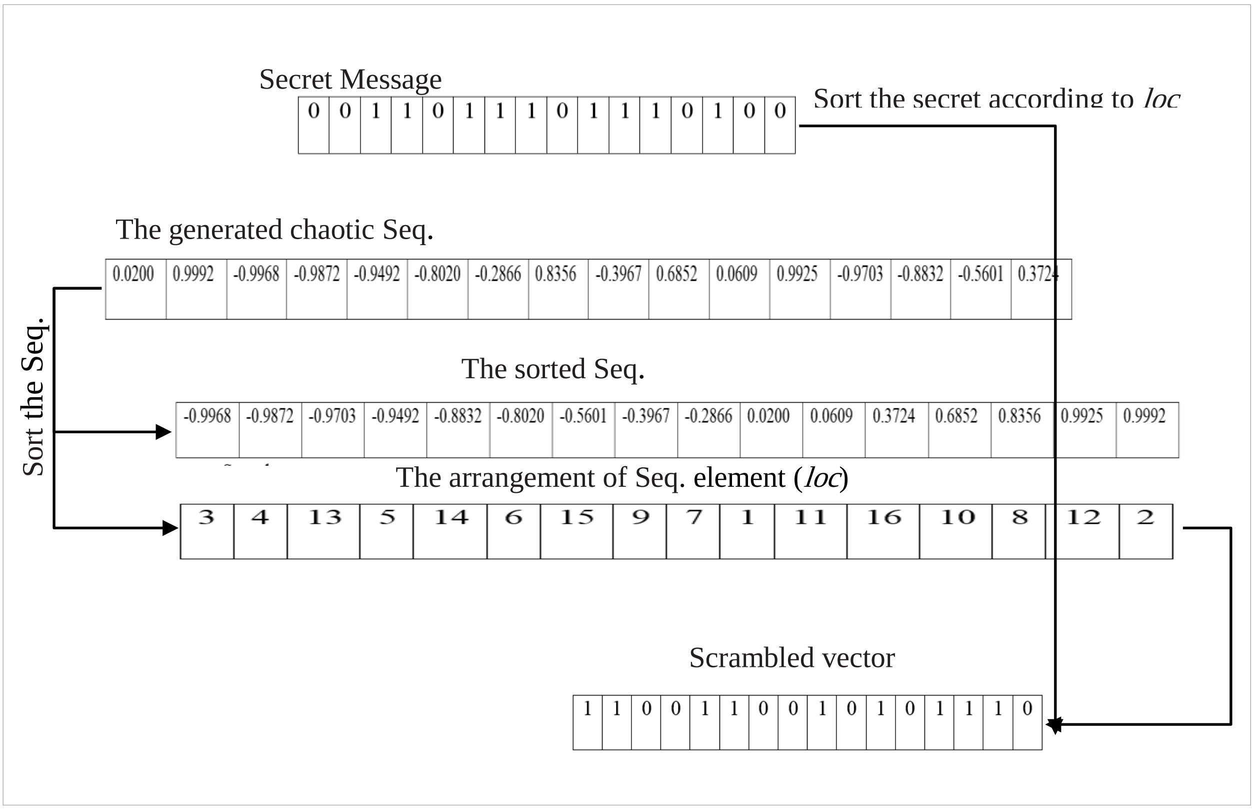


Figure (3.3): Binary image scrambling by chaotic system

B. Chaotic Sequence Thresholding

The binary mask that will be utilized later in the encryption procedure is constructed using the chaotic sequence that was created (Chaotic_ Seq).

First, each secret data element's mask sequence (Mask_{Seq}) is created using the following equation.:

$$Mask_{Seq(i)} = \|\lfloor \text{Chaotic\_Seq (i)} \times 255 \rfloor\|$$

$$\text{for i=1…length (image)} \quad ,\ldots(3.1)$$

where i represents a current index of Seq, $\|.\|$ represents absolute value, $\lfloor . \rfloor$ represents rounding opeartion, and Chaotic_Seq represents created chaotic sequence.

Secondly, The next stages require the binary mask (Mask), which is obtained by thresholding the elements of the Mask_ seq sequence into the binary range (0,1) in accordance with equation (3.2).

$$\text{Mask(i)} = \begin{cases} 1 \quad \text{if} \quad \text{Mask}_{\text{seq(i)}} \geq \text{T} \\ 0 \qquad\qquad\quad \text{oterwise} \end{cases}, \qquad \ldots(3.2)$$

where T is a threshold that the user sets.

C. Encrypted Secret Data(ESD)

Finaly, the *xor* operation is applied between Scrambled_ vec_Data obtain from (step 2) and mask to get encrypted secret data (ESD).

Algorithm (3.2) depicts the encryption process.

```
Algorithm (3.2): Encryption process
Input:  SD   // secret data
Output: ESD  // Encrypted secret data
Step1: Generating chaotic sequence using the same steps in section 3.2.1.1 for Chaotic Sequence Generator
Step2: Sorting the extracted secret data according to the generated chaotic sequence in step1.
Step3: Generate a binary sequence by applying equation (3.2) on the generated chaotic sequence in step1.
Step4: applying XOR operation between the sorting secret data from step 2 and generated bits sequence from step 3 to obtain the secret data.
End
```

3.2.1.2 Splitting of ESD

For a given encrypted encrypted secret data (ESD) needed to be hidden, it should divide into Em segments according to the following:

$$\boldsymbol{Em = \frac{N}{Nseg} + 1} \qquad ,\dots \quad (3.3)$$

Where (Nseg) is the length of hash sequence(Nseg=8) and (N) is the length of secret information. If N is not a multiple of Nseg, 0 is added in the last image and the number of 0 is recorded in added image.

3.2.1.3 Embedding Using Coverless Image Steganography System (CISS)

The frame diagram of the proposed coverless method is illustrated in Figure (3.4) which consists of several stages. The specifics of each stage are described in the following sections.

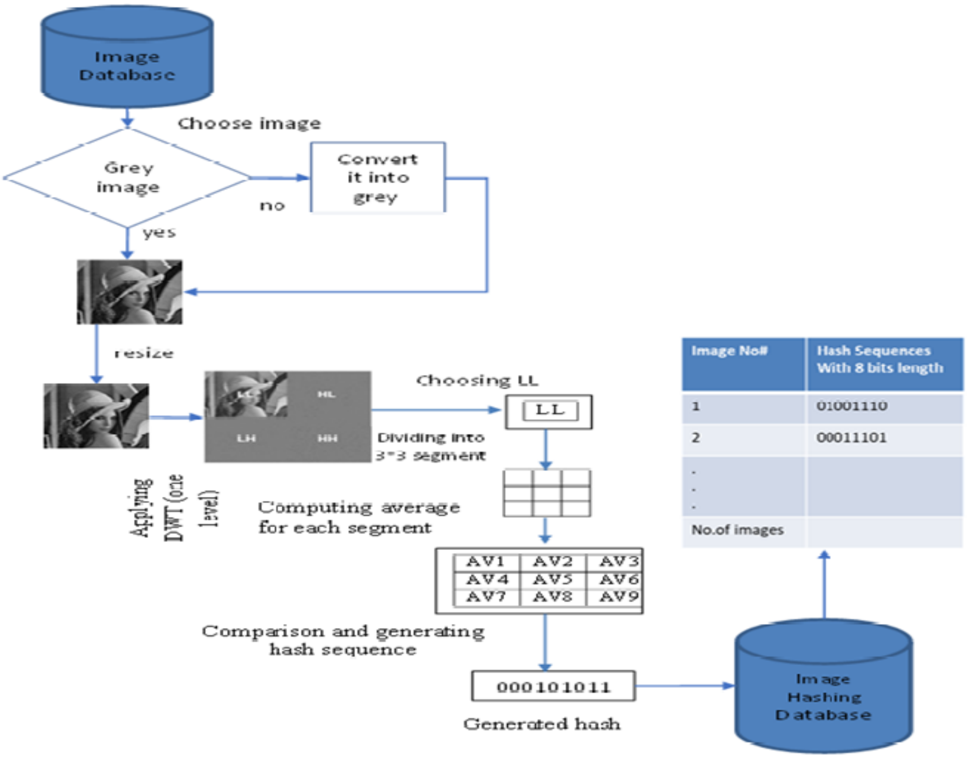


Image No#	Hash Sequences With 8 bits length
1	01001110
2	00011101
. . .	
No.of images	

Figure(3.4):Hash sequence generation with frequency domain

A. Hash generation stage

This stage consists of three steps include building images database, hash sequences generation, and building a hash indexing table.

a:Building images database

To conceal secret data in coverless image steganography, one way is to find suitable images that already contain the information. Such images are classified as stego images, which are used to communicate sensitive data. The robust hashing sequence of an image is used in this procedure to carry out the image feature coding, creating a complete image database. Web images that were crawled by the authors. This dataset contains 7741 images that were randomly crawled from the internet. The resolutions of the internet images are different, and there are no fixed categories.

b:Hash code production by robust hashing algorithm

Hash generation is done in frequency domain. With this domain, several phases can be completed during the production of a hash sequence using Algorithm (3.3). With this domain, hashing is created from the coefficient of image by implementing the discrete wavelet transform (DWT).

```
Algorithm (3.3): Hash sequence generation using frequency domain
Input:
   Pci                    //original cover image i
Output:
   ImgHash                //sequence of bits
Begin
Step 1:Read image data $Pc_i$
Step 2: Each image data $Pc_i$ is normalized to a size of $N \times N$ pixels using nearest interpolation to guarantee that images of different sizes share the same feature length.
Step 3: if the image data $Pc_i$ is color image
            Convert the normalized image from the RGB to gray scale image, and the
             gray component is selected for representation.
Step 4: Applying DWT on ($Pc_i$) to obtain four subbands (LL, LH, HL, HH).
 Step 5: Dividing the LL subband into $3 \times 3$ non-overlapping segment.
 Step 6: Computing the average intensity of each segment to obtain $3\times3$ block
            average   array (BAvg).
 Step 7: Converting (BAvg) into vector (VAvg) by scanning the array row by row.
 Step 6: Converting VAvg into binary by comparing every two adjacent elements
         according to equation (3.4) to obtain binary hash image sequence (ImgHash)
         with length 8 bits.
End
```

The above steps are shown in the Figure (3.5)

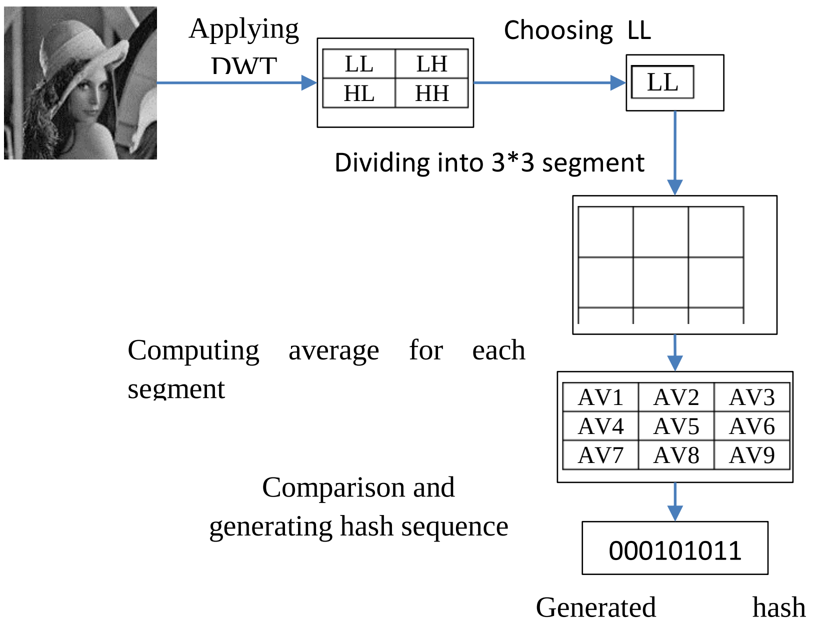

Applying DWT
LL LH
HL HH
Choosing LL
LL
Dividing into 3*3 segment
Computing average for each segment
AV1 AV2 AV3
AV4 AV5 AV6
AV7 AV8 AV9
Comparison and generating hash sequence
000101011
Generated hash

Figure (3.5): Hash sequence generation with frequency domain

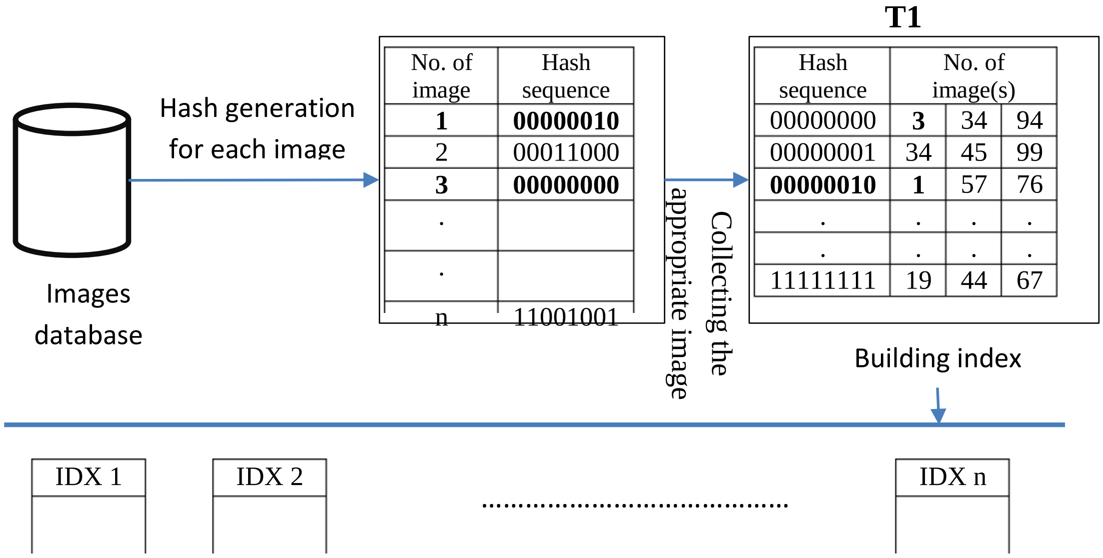
The selected color image is converted to grayscale (G) applying equation (2.11). Then, the DWT is applied on the grayscale image (G). With frequency domain, the following equation is used to generate the binary hash sequence {H1, H2, . . ., Hn} from LL subband as follows:

$$\begin{cases} H(ii)= 1;\ \text{if } Av(ii) > Av(ii+1) \\ \quad , \text{where } 1 < ii < 8 \\ H(ii) = 0;\ \text{otherwise} \end{cases} \qquad \dots (3.4)$$

c:Building the inverted index structural by image indexing

To use a secret message with a binary hash as the query, it will take a long time to look for all images with hash sequences that match the query in the database if we do an extensive search. To speed up the search, all of the images in the database are indexing according to their hash sequence. Then, for all of the hash sequences, a query table T1 is design, which is an inverted index structure. T1 is a lookup table that contains entries to the greatest extent possible Hash sequences of 8 bits. Each value leads to a set of the entire image IXDs that share the same hash sequence. Assume that image A's hash sequence is [

1,1,1,0,0,1,1,1] and that its IXD is IXD(A), and that IXD(A) belongs to the list pointed by the entry 1,1,1,0,0,1,1,1,1 as shown in Figure (3.6)



No. of image	Hash sequence
1	**00000010**
2	00011000
3	**00000000**
.	
.	
n	11001001

Hash sequence	No. of image(s)		
00000000	**3**	34	94
00000001	34	45	99
00000010	**1**	57	76
.	.	.	.
.	.	.	.
11111111	19	44	67

Figure (3.6): Building index hash table

B. Embedding stage

In this stage, the index structure is used to find suitable images with hash sequences those are the same with the secret data segments. Finally, the acquired images are referred of as stego images and they are sent one by one to the receiver.

3.2.2 Activities at the Receiver Side

At the receiver side, several activities are being done as describe in algorithm (3.4):

```
Algorithm (3.4): Receiver Activities
Input: {$Pc_1$,$Pc_2$,…,$Pc_{Msegment}$} //Stego Images corresponding to secret data
Outputs: ESD                          //Extracted secret data
Step1:  For i=1 to number of received stego images do
   Step1.1: Read image data of stego image $Pc_i$
   Step1.2: Call Algorithm (3.3) to  generate the hash sequence for the
            image data. The generated hash sequence represent the
            extracted secret data segment.
  End for
Step2: The extracted secret data (ESD) is represented by the combination
```

of all extracted secret data segment.
End

The following sections describe the details of each activity.

A. Extraction Procedure

This section describes extraction the secret message in the receiver side. The secret data can be recovered without disorder if all stego images are received correctly. For each receiving image, its hash sequence is generated that using the same proposed method for generating hash sequence that used by sender.

C: Extracted Secret Data Decryption

In this activity, the extracted secret data is decrypted. Figure (3.7) and Algorithm (3.5) illustrate the decryption procedure.

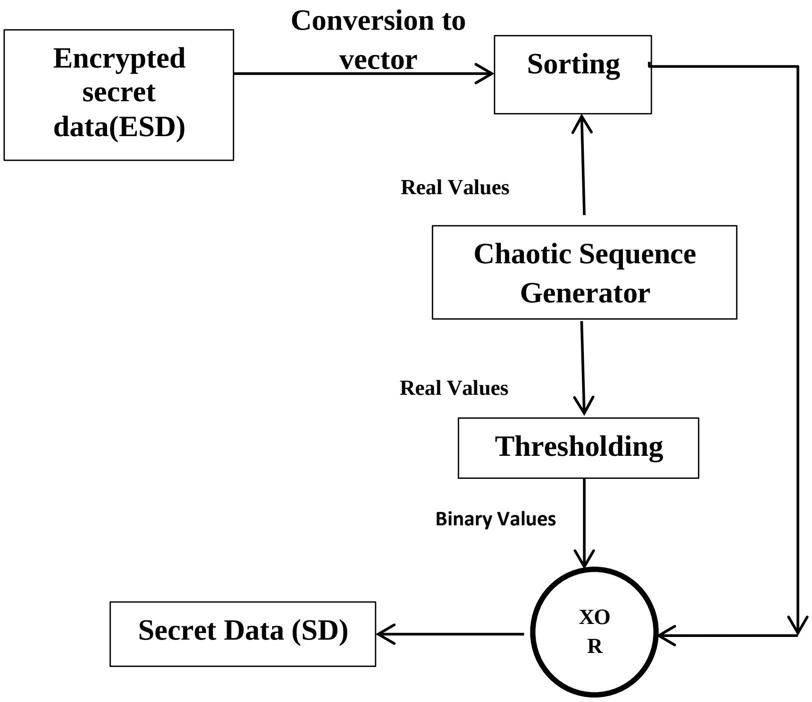


Figure (3.7): Secret data encryption

```
Algorithm (3.5): Decryption Process
Input:    ESD      //extracted secret data
Output: DSD    // decrypted secret data
Step1: Generating chaotic sequence using the same steps in section
           3.2.1.1 for Chaotic Sequence Generator
Step2: Sorting the extracted secret data according to the generated
          chaotic sequence in step1.
Step3: Generating a binary sequence by applying equation (3.2) on the
           generated chaotic sequence in step1.
Step4: Applying XOR operation between the sorting secret data from
        step 2 and generated bits sequence from step 3 to obtain the secret
         data.
End
```

Chapter Four

Performance Evaluation and Results

Chapter Four

Performance Evaluation and Results

4.1 Introduction

This chapter is dedicated to presenting the tests conducted on the proposed system. In addition, it introduces a discussion of the experimental work results for evaluating the performance of the system. The suggested system is implemented with the device that has the following features:

- Intel Core i5 processor running at 1.60 GHz
- RAM 4 GB
- Microsoft Windows 10 Pro

The proposed system is simulated with MATLAB programming language version R2020. To illustrate the influence of various factors involved in the overall system performance, several experiments were run. The experimental results were analyzed to clarify the results by some performance metrics that are discussed in chapter two.

4.2 Data Set

One of the most important steps in implementing a coverless image strategy is to look for images that already have 7741 images. These images are known as stego-images, and they are used to transmit the secret data. Figure (4.1) shows a number of images in the collected dataset.

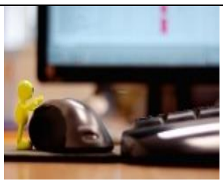
Image1		Image5		Image9	
Image2		Image6		Image10	
Image3		Image7		Image11	
Image4		Image8		Image12	

Figure (4.1): Sample of images dataset

The images in the collectd data set have differnt sizes. Therefore, the image must be normalized and may have set sizes to (228×228) before mapping into hash sequences.

Also, different types of secret messages are tested. Figure (4.2) shows samples of secret message.

Smsg1	0000101101001001001010100000011110101010
Smsg2	0011100001111000010101100001111110101011

Figure (4.2): Sample of secret data

4.3 Experimental Results

The proposed coverless method's efficiency is tested in terms of embedding, security, and robustness.

4.3.1 Experimental Results Related to Encryption

To increase the security of the embedding scheme, the secret messages have been encrypted utilizing a method based on chaotic principle. The encryption procedure is done with several steps as described in the following sections:

4.3.1.1 Chaotic System Parameters Selection

To determine the best values of chaotic system parameters such as (chaotic sequence generation with initial values x_0, control parameter r) several tests are conducted as follows:

A. Chaotic Sequence Generator

The chaotic sequence generated by the logistic map in equation (2 .2) is highly sensitive to any tiny variations in an initial value, therefore any tiny change can lead to different results. Figure (4.3) shows obstetrics of two signals for two different initial values (X0 = 0.5 and X0= 0.5000001) by using logistic chaotic.

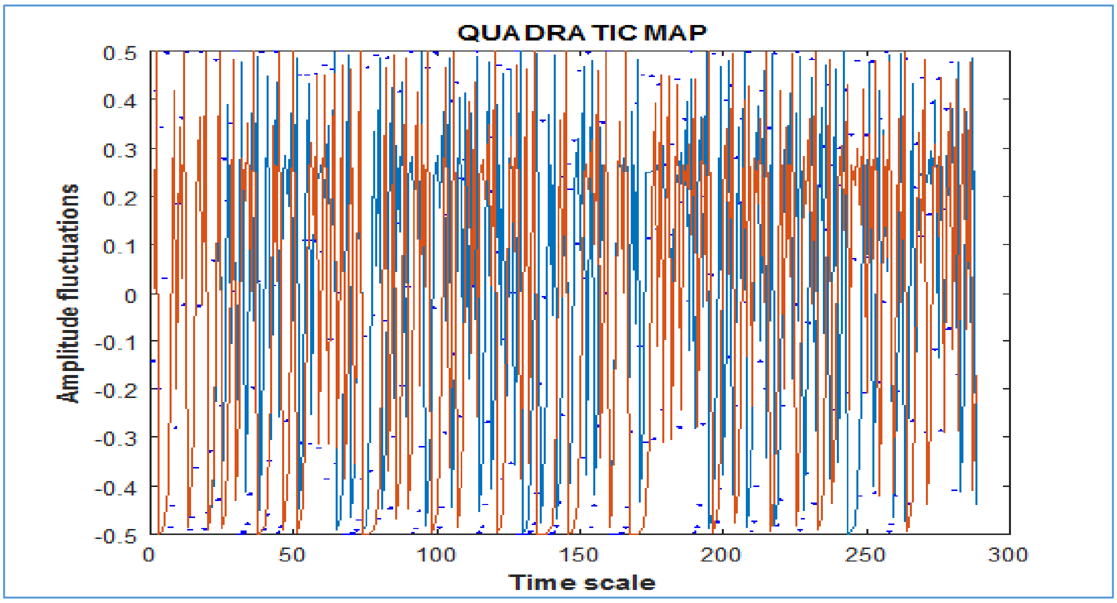


Figure (4.3): **Generation of two signals with different initial values**

Figures ((4.4) and (4.5)) show that the logistic chaos generator has good autocorrelation and cross-correlation characteristics, making it perfect in security applications.

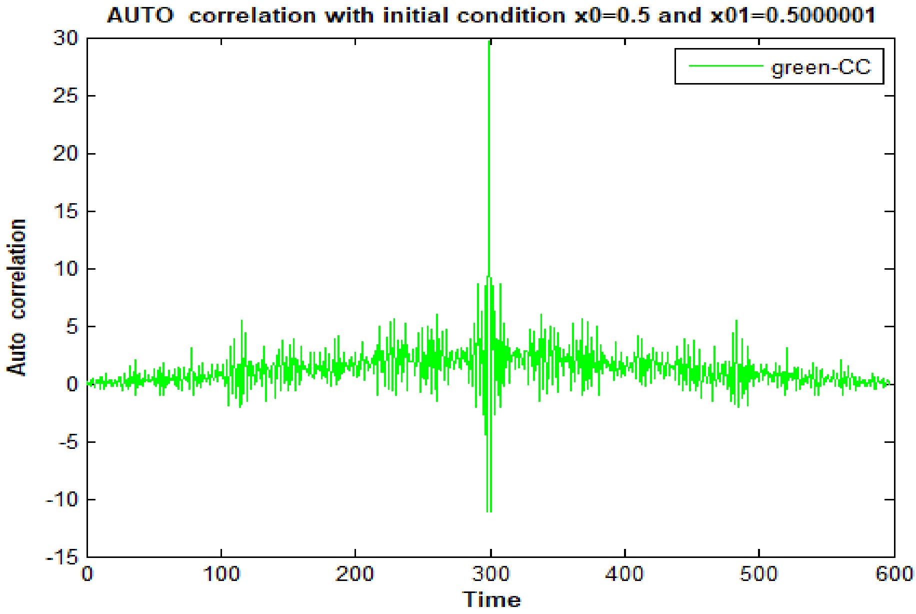


Figure (4.4): Auto correlation execution for quadric chaos Generator

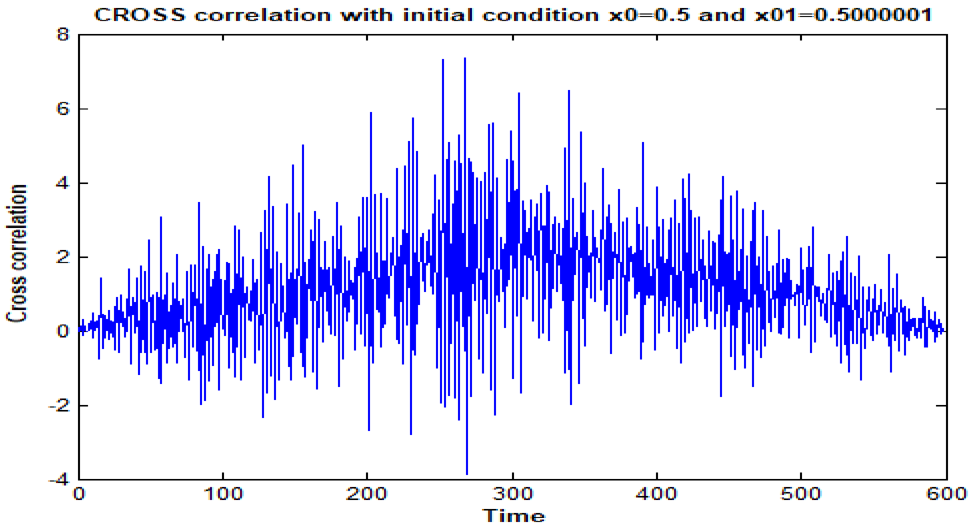


Figure (4.5): Cross correlation execution for logistics chaos generator

B. Effectiveness of Chaotic Parameters System

To select the best chaotic control parameter, it should be determine the regions of the system displaying convergence, bifurcation, and chaos. A full image of the chaotic map behaviors through study of:

- The "bifurcation diagram" is a graphical representation to the relation inter the behavior of the chaotic system and values of certain parameter, then the value of parameter will be measured graphically.
- The magnitude of the "Lyapunov exponent" is an pointer of the behavior of the chaotic system. If the positive value of "Lyapunov exponent" is indicate to the chaotic behavior, while when it is negative is indicate to the stable behavior.

Figure (4.6) shows the bifurcation diagram of the "Logistic map " and the value of "Lyapunov exponent " with regard to bifurcation parameter (*r*).

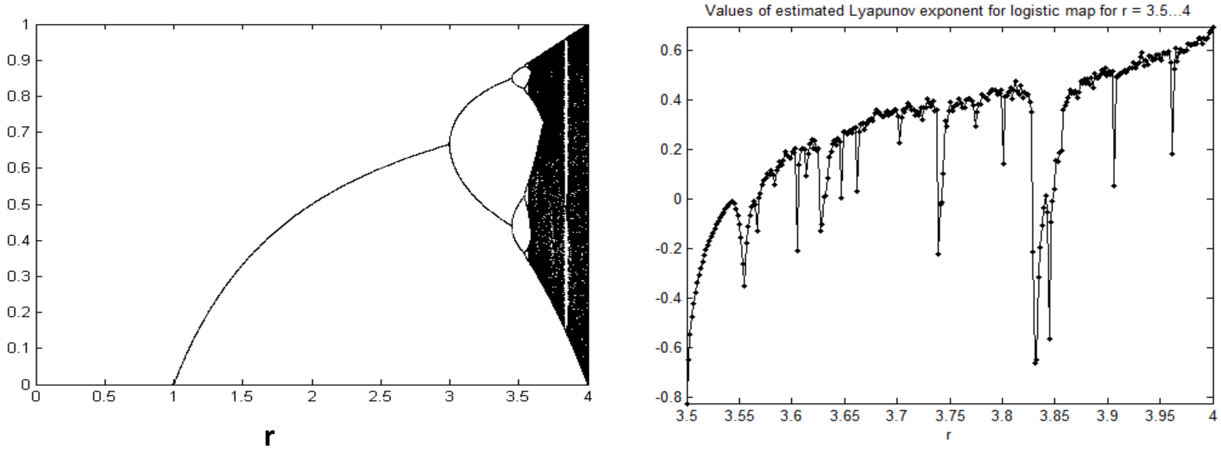


Figure (4.6): **Logistic Chaotic Map (a) Bifurcation diagram of the Logistic map (b) Lyapunov exponent at x_0=0.5**

It shown that from bifurcation diagram the chaotic region locate at r∈ [3.5686,4].

4.3.1.2 Security Analysis

A perfect encryption algorithm has the following characteristics:

1. Sensitivity to the premier value of chaotic (secret key).
2. Very weak relation (correlation) between the original and encrypted data.
3. Good entropy information

A. Key Sensitivity Analysis

It is regarded as one of the crucial metrics used to evaluate encryption systems. It is used to evaluate how sensitive an encryption system is to even the smallest change to the secret key used for encryption and decryption. The suggested system uses the secret key value (x_0=0.5) to encrypt secret messages (Smsg2), as shown in figure (4.7b),), the secret key is changed to (x_0=0.5000001) and applied to the secret's decryption as shown in figure (4.7d). It is clearly the decryption that message was much different from the original message using a secret key that had been slightly modified. That implies that the suggested system is highly sensitive to even the smallest change in the secret key.

0111000011110000101011000	**0 0 01 1 1 1 00 0 0 1 111010 10**
A . Smsg2	B. Encrypted message with *x0*=0.5
011100001111000010101100000	**111001 11000010101011001**
C. Decrypted message with *x0*=0.5	D. Decrypted message with *x0*=0.5000001

] **Figure (4.7): key influencing on encryption and decryption process**

B. Avalanche Effect

The efficiency of the diffusion method can be measured by using the Avalanche Effect metric. If the original secret A is encrypted utilizing the proposed scheme to get the encrypted secret B, then we measured the Avalanche effect between A and B; which indicates the various bits between A and B, then if B and C vary in half of their bits, then that denotes the encryption manner has pretty diffusion properties. The value of AE for (Smsg2) is (1) which means the proposed encryption system has good diffusion.

C. Entropy

The entropy of any encrypted secret is calculated using Equation (2.4), the ideal value for entropy for the encrypted binary secret should be (1) or a value close to (0.989587521222056). It is very close to (1).

D. Correlation coefficient (CC)

The correlation is computed for encrypted data according to the equation (2.3). The correlation coefficient is very small (-1), which points to that the original secret and their corresponding encrypted are entirely uncorrelated with each other. This shows that data encryption method is effective and provides a greater level of security.

4.3.2 Experimental Results Related to CISS

To measure the performance of the proposed system, two measures are used namely, normalized correlation (NC) and bit error rate (BER).

All types of content damage, such as image noise, JPEG compression, rescaling, brightness change, and contrast shift, are unavoidable during the transmission process and so on. Each stego image selected from the database to represent the secret data segment is subject to these attacks. These variables must be able to withstand the information collected from the image. To put it another way, the hash algorithm is resistant to these types of attacks. The secret data that will be tested in the embedding process is “0000101101001001001010100000011110101010”. Firstly, the secret data is encrypted and splitting into segments with 8-length for each one. The encrypted data is “1111010010110110110101011111100001010101”.Then, the image in the data set that match its hash sequence with secret data segment will be selected as stego image. Finally, each stego image will go with different attacks to measure the robustness.

A) Test the Robustness of the proposed system against JPEG compression

Each stego image selected from the database to represent the encrypted secret data segment subject to JPEG compression with various quality factors. According to the Table (4.1), the proposed system gives a good robustness against JPEG compression attack, where the value of NC and BER is of acceptable.

Table (4.1): Results after applying compression attacks

Secret data	Orignal image	Quality factors (Q)	BER	NC	Extracted Secret data	Sample of image after attack
11110100		10	0	1	11110100	
		30	0	1	11110100	
		40	0	1	11110100	
		50	0	1	11110100	
10110110		10	0	1	10110110	
		30	0	1	10110110	
		40	0	1	10110110	
		50	0	1	10110110	
11010101		10	0	1	11010101	
		30	0	1	11010101	
		40	0	1	11010101	
		50	0	1	11010101	
11111000		10	0	1	11111000	
		30	0	1	11111000	
		40	0	1	11111000	
		50	0	1	11111000	
01010101		10	0	1	01010101	
		30	0	1	01010101	
		40	0	1	01010101	
		50	0	1	01010101	
00000000		10	0	1	00000000	
		30	0	1	00000000	
		40	0	1	00000000	
		50	0	1	00000000	
		Average	0	1		

To obtain the original secret message, all extracted segments are combined and the decryption process is applied on the extracted data to obtain the original confidential data, which are (00001011011010010010010010101000000111110101010).

B) Test the Robustness of the proposed system against noise attacks

In noise attack test, a stego image is attacked with several noise attacks namely, salt &pepper, speckle and Gaussian noises with different noise density. Table (4.2) through Table (4.5) shows the results under noise attack.

Table (4.2): Results after applying Salt & Pepper noise attack

Secret data	Original image	Noise Type (Salt & Pepper)	BER	NC	Extracted Secret data	Sample of image after attack
11110100		0.01	0	1	11110100	
		0.001	0	1	11110100	
		0.02	0	1	11110100	
		0.03	0	1	11110100	
10110110		0.01	0	1	10110110	
		0.001	0	1	10110110	
		0.02	0	1	10110110	
		0.03	0	1	10110110	
11010101		0.01	0	1	11010101	
		0.001	0	1	11010101	
		0.02	0	1	11010101	
		0.03	0	1	11010101	
11111000		0.01	0	1	11111000	
		0.001	0	1	11111000	
		0.02	0	1	11111000	
		0.03	0	1	11111000	
01010101		0.01	0	1	01010101	
		0.001	0	1	01010101	
		0.02	0	1	01010101	
		0.03	0	1	01010101	
00000000		0.01	0	1	00000000	
		0.001	0	1	00000000	
		0.02	0	1	00000000	
		0.03	0	1	00000000	
		Average	0	1		

Table (4.3): Results after applying Speckle noise attack

Secret data	Original image	Noise Type (Speckle)	BER	NC	Extracted Secret data	Sample of image after attack
11110100		0.01	0	1	11110100	
		0.001	0	1	11110100	
		0.02	0	1	11110100	
		0.03	0	1	11110100	
10110110		0.01	0	1	10110110	
		0.001	0	1	10110110	
		0.02	0	1	10110110	
		0.03	0	1	10110110	
11010101		0.01	0	1	11010101	
		0.001	0	1	11010101	
		0.02	0	1	11010101	
		0.03	0	1	11010101	
11111000		0.01	0	1	11111000	
		0.001	0	1	11111000	
		0.02	0	1	11111000	
		0.03	0	1	11111000	
01010101		0.01	0	1	01010101	
		0.001	0	1	01010101	
		0.02	0	1	01010101	
		0.03	0	1	01010101	
00000000		0.01	0	1	00000000	
		0.001	0	1	00000000	
		0.02	0	1	00000000	
		0.03	0	1	00000000	
		Average	0	1		

Table (4.4): Results after applying Gaussian noise attack

Secret data	Original image	Noise Type (Gaussian Noise)	BER	NC	Extracted Secret data	Sample of image after attack
11110100		0.01	0	1	11110100	
		0.001	0	1	11110100	
		0.02	0	1	11110100	
		0.4	0	1	11110100	
10110110		0.01	0	1	10110110	
		0.001	0	1	10110110	
		0.02	0	1	10110110	
		0.4	0	1	10110110	
11010101		0.01	0	1	11010101	
		0.001	0	1	11010101	
		0.02	0	1	11010101	
		0.4	0	1	11010101	
11111000		0.01	0	1	11111000	
		0.001	0	1	11111000	
		0.02	0	1	11111000	
		0.4	0	1	11111000	
01010101		0.01	0	1	01010101	
		0.001	0	1	01010101	
		0.02	0	1	01010101	
		0.4	0	1	01010101	
00000000		0.01	0	1	00000000	
		0.001	0	1	00000000	
		0.02	0	1	00000000	
		0.4	0	1	00000000	
		Average	0	1		

Table (4.5): Results under possion noise attack

Secret data	Original image	Extracted Secret data	BER	NC	Sample of image after attack
11110100		11110100	0	1	
10110110		10110110	0	1	
11010101		11010101	0	1	
11111000		11111000	0	1	
01001001		01001001	0	1	
00000000		00000000	**0**	**1**	
		Average	0	1	

In all obtained results under different attacks the decryption process is applied on the extracted data to obtain the original confidential data, which is (0000101101001001001010100000011110101010).

C: Robustness against Filtering Attack

Each stego image selected from the database to represent the encrypted secret data segment is subject to many filter attack with various filter size. According Table (4.6), the proposed system gives a good robustness against medain attack, where the value of NC and BER is of acceptable. Also, the stego images were filtered with a low pass filtering (Gaussian filter)and mean filter with different sizes of filter kernal. Table (4.6),table(4.7)and table (4.8) illustrates NC and BER values under filtering attack .

Table (4.6): Results under medain filtering attack

Secret data	Original image	Filter size	BER	NC	Extracted Secret data	Sample of image after attack
11110100		1*1	0	1	11110100	
		2*2	0	1	11110100	
		3*3	0	1	11110100	
10110110		1*1	0	1	10110110	
		2*2	0	1	10110110	
		3*3	0	1	10110110	
11010101		1*1	0	1	11010101	
		2*2	0	1	11010101	
		3*3	0	1	11010101	
11111000		1*1	0	1	11111000	
		2*2	0	1	11111000	
		3*3	0	1	11111000	
01001001		1*1	0	1	01001001	
		2*2	0	1	01001001	
		3*3	0	1	01001001	
00000000		1*1	0	1	00000000	
		2*2	0	**1**	00000000	
		3*3	0	**1**	00000000	
		Average	0	1		

Table (4.7): Results under mean filtering attack

Secret data	Original image	Filter size	BER	NC	Extracted Secret data	Sample of image after attack
11110100		1*1	0	1	11110100	
		2*2	0	1	11110100	
		3*3	0	1	11110100	
10110110		1*1	0	1	10110110	
		2*2	0	1	10110110	
		3*3	0	1	10110110	
11010101		1*1	0	1	11010101	
		2*2	0	1	11010101	
		3*3	0	1	11010101	
11111000		1*1	0	1	11111000	
		2*2	0	1	11111000	
		3*3	0	1	11111000	
01001001		1*1	0	1	01001001	
		2*2	0	1	01001001	
		3*3	0	1	01001001	
00000000		1*1	0	1	00000000	
		2*2	0	1	00000000	
		3*3	0	1	00000000	
		Average	0	1		

Table (4.8): Results under Gussein filtering attack

Secret data	Original image	Filter size	BER	NC	Extracted Secret data	Sample of image after attack
11110100		1*1	0	1	11110100	
		2*2	0	1	11110100	
		3*3	0	1	11110100	
10110110		1*1	0	1	10110110	
		2*2	0	1	10110110	
		3*3	0	1	10110110	
11010101		1*1	0	1	11010101	
		2*2	0	1	11010101	
		3*3	0	1	11010101	
11111000		1*1	0	1	11111000	
		2*2	0	1	11111000	
		3*3	0	1	11111000	
01001001		1*1	0	1	01001001	
		2*2	0	1	01001001	
		3*3	0	1	01001001	
00000000		1*1	0	1	00000000	
		2*2	0	1	00000000	
		3*3	0	1	00000000	
		Average	0	1		

D. Robustness against geometric attacks

In this expermint, robustness against rotation attack is tesed .Each stego image selected from the database to represent the secret data segment is subject to rotation attack with various factors. The proposed method achieved acceptable results in rotation attack with different rotation degrees as shown in Table (4.9).

Table (4.9): Result after applying rotation attack

Secret data	Original image	Factor	NC	BER	Extracted Secret data	Sample of image after attack
11110100		0.180	1	0	11110100	
		10	1	0	11110100	
		45	0.60	0.5	11010111	
		90	0. 8	0.25	11010110	
10110110		0.180	1	0	10110110	
		10	0.6	0.37	01110100	
		45	0.40	0.62	01010111	
		90	0.8	0.25	01000100	
11010101		0.180	1	0	11010101	
		10	0.6	0.37	01010111	
		45	0.60	0.37	01010011	
		90	0.6	0.37	10010110	
11111000		0.180	1	0	11111000	
		10	0.4	0.37	01010000	
		45	0.40	0.37	01010000	
		90	0.4	0.37	01001000	
01010101		0.180	1	0	01010101	
		10	0.5	0.5	01101100	
		45	0.25	0.62	01000011	
		90	0.5	0.62	11001101	
00000000		0.180	1	0	00000000	
		10	1	0.37	01000011	
		45	1	0.37	01000011	
		90	1	0.25	00000011	

In rotation attack ,both NC avg and BER avg differint in variance angle. Table (4.10) shows the average values of NC and BER against rotation attack with different rotation angles.

Table (4.10): The NC avg and BER avg values under rotation attack

Angle	BER avg	NC avg
0.180	0	1
10	0.33	0.68
45	0.47	0.54
90	0.35	0.68

Another geometric attack is resizing. Each stego image selected from the database to represent the secret data segment. The proposed method achieved good results with size (1024*1024)according to Table (4.11).

Table (4.11): Results after applying resize attack(1024*1024)

Secret data	Original image	Extracted Secret data	BER	NC	Sample of image after attack
11110100		11110100	0	1	
10110110		10110110	0	1	
11010101		11010101	0	1	
11111000		11111000	0	1	
01010101		01010101	0	1	
00000000		00000000	**0**	**1**	
		Average	0	1	

E. Robustness against brightness and sharpening attacks

The stego images were tested against increasing the brightness image with factor for example its values (10, 20). The proposed method achieved good results in both brightness and sharpening attacks. Also, the stego images attack with the sharpening of image as shown in table (4.12) and (4.13)

Table (4.12): Results after applying brightness attack

Secret data	Original image	Ratio	Extracted Secret data	BER	NC	Extracted Secret data	Sample of image after attack
11110100		+10	11110100	0	1	01000011	
		+20	11110100	0	1	01000011	
10110110		+10	10110110	0	1	11010110	
		+20	10110110	0	1	11010110	
11010101		+10	11010101	0	1	01010011	
		+20	11010101	0	1	01010011	
11111000		+10	11111000	0	1	00010010	
		+20	11111000	0	1	00010010	
01010101		+10	01010101	0	1	00110010	
		+20	01010101	0	1	00110010	
00000000		+10	00000000	**0**	**1**	00000000	
		+20	00000000	**0**	**1**	00000000	
			Average	**0**	**1**		

Table (4.13): Results after applying sharping attack

Secret data	Original image	Extracted Secret data	BER	NC	Sample of image after attack
11110100		11110100	0	1	
10110110		10110110	0	1	
11010101		11010101	0	1	
11111000		11111000	0	1	
01010101		01010101	0	1	
00000000		00000000	0	1	
		Average	0	1	

4.4 Comparison with Exsting Methods

To verify the effectiveness of the proposed method, the performance of our presented technique is compared with other existing state-of-the-art CIS method [28] [29] under robustness. For the purpose of comparing the (Caltech-101) database [66] has been uploaded and tested by our method. The Caltech-101 dataset, created by Caltech, contains 9145 images of 102 object categories. This step can be carried out by implementing the image without cover strategy in searching for images in the dataset. These images are known as stego-images, and they are used to transmit the secret data. In the experiment, we randomly selected 100 sequences and calculated the recovery rate of the secret information, namely the robustness, without considering the order. Figure (4.8) shows a number of images in the collected dataset.

Image1		Image5		Image9	
Image2		Image6		Image10	
Image3		Image7		Image11	
Image4		Image8		Image12	

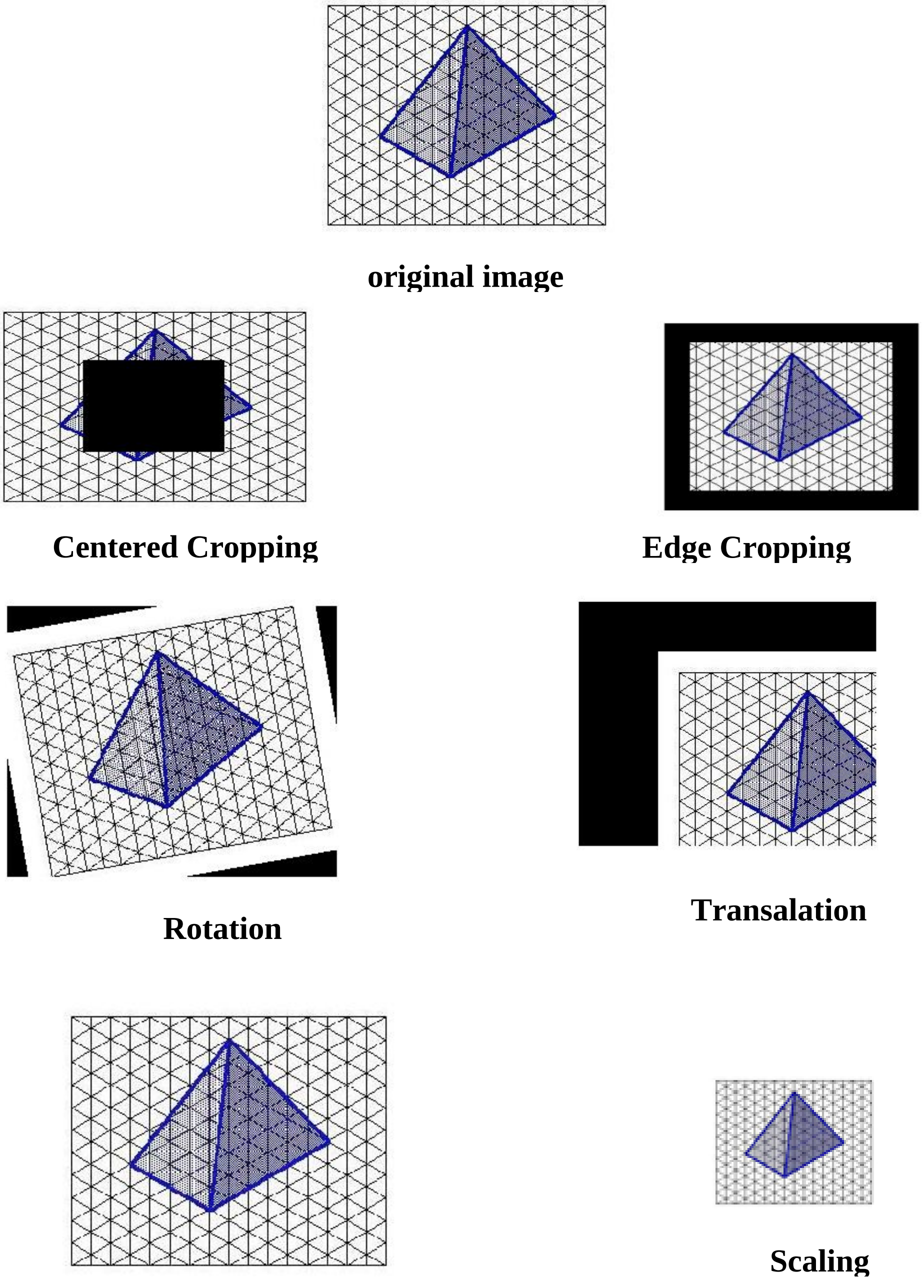
Figure (4.8): Samples of Caltech-101 database

Table (4.14) shows the results of of extracted accuracy (RC) values for both methods in [28] [29] and our proposed method.

Table (4.14): Robustness (%) comparison with Two CIS methods in Caltech-101

Attack Type	Factor	RC		
		Method in Ref.[28]	Method in Ref.[29]	The Proposed method
Compression attack	10	80.59	69.66	**99.2500**
Gaussian attack	σ(0.001)	92.10	-	**99.6250**
rotation attack	10	71.02	63.25	**73.3750**
Gaussian filter	3*3	95.32	80.34	**99.3750**
Salt and Speckle Noise	σ(0.001)	-	78.63	**99.7500**
Centered Cropping	20%	72.88	41.88	**77.5000**
Edge Cropping	20%	**76.98**	73.93	53.2500
Translation	(80,50)	**-**	**55.98**	45.3750
Scaling	3	99.12	82.05	**99.6250**
Gamma	0.8	-	82.05	**99**

Figure (4.9) shows the several kinds of attacked images and the original image coming from the Caltech-101 dataset.



original image

Centered Cropping

Edge Cropping

Rotation

Transalation

Scaling

Gamma

Figure (4.9):The Caltech-101 dataset sample display of attacked images

It shows that proposed method generally outperform other methods in most attacks.

Chapter Five

Conclusions and Future Works

Chapter Five

Conclusions and Future Works

5.1 Introduction

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

5.2 Conclusions

After applying the suggested system, some conclusions can be listed as follows:

1. The suggested approach increases the level of data security by utilizing encryption at the first level and coverless image steganography at the second level to embed data into the container media.
2. The security of secret information. Like the coverless image steganography, the proposed coverless image steganography accomplishes the process of information hiding by establishing the mapping relationship between secret information and carriers.
3. 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 such as pixel brightness value, as contrast to using the given cover image for doing so.
4. As a result of the suggested framework's ability to prevent the traces of modification from leaving in the stego images. Its robust hashing algorithm also ensures that it can be used against various image attacks.
5. The suggested approach cannot be discovered by steganalysis algorithms since carriers have not been modified.
6. The suggested system, which encrypts the secret message using the chaotic encryption method, performs well in testing. The results show

that the encrypted image has entropy information equal to ideal value 1 and correlation coefficients close to ideal value 0.

7. The experimental results show the robustness of the embedding algorithm, its robustness is tested on different types of attacks.

8. Additionally, our image database has a wide range of images, and each hidden piece of information can index several matching stego-images. Also, we could send various stego-images to various recipients. In this instance, even if the attackers succeed in obtaining the stego-images, it will be difficult for them to access the secret data. The coverless information concealing solution that is suggested provides improved security as a result.

5.3 Future Works

The suggestions for future works can be shown as follows:

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

2.Enhance the capacity of steganography while maintaining the typical size of the image database.

3. Due to the three party does not able to discover the secret message, it is possible to implement the proposed system with other types of sensitive images, such as military images.

References

[1] C. Osborne, A. Tirkel, and T. Hall, "Image and Watermark Registration for Monochrome and Coloured Images," *Digital Image Computing, Technology and Applications, Wellington New Zealand,* pp. 59-64, 1997.

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

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

[4] 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.

[5] S. Deepikaa and R. Saravanan, "VoIP steganography methods, a survey," *Cybern. Inf. Technol,* vol. 19, pp. 73-87, 2019.

[6] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal processing,* vol. 90, pp. 727-752, 2010.

[7] A. A. El-latif, B. Abd-El-Atty, and S. E. Venegas-Andraca, "A novel image steganography technique based on quantum substitution boxes," Optics & Laser Technology, 2019.

[8] Y. Cao, Z. Zhou, Q. Wu, C. Yuan, and X. Sun, "Coverless information hiding based on the generation of anime characters," *EURASIP Journal on Image and Video Processing,* vol. 2020, pp. 1-15, 2020.

[9] T. Pevný, T. Filler, and P. Bas, "Using high-dimensional image models to perform highly undetectable steganography," in *International workshop on information hiding*, 2010, pp. 161-177.

[10] V. Holub and J. Fridrich, "Designing steganographic distortion using directional filters," in *2012 IEEE International workshop on information forensics and security (WIFS)*, 2012, pp. 234-239.

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

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

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

[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] 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.

[16] S. Zheng, L. Wang, B. Ling, and D. Hu, "Coverless information hiding based on robust image hashing," in *International conference on intelligent computing*, 2017, pp. 536-547.

[17] 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.

[18] 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*, 2010, pp. 1-19.

[19] 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.

[20] Z. Zhou, H. Sun, R. Harit, X. Chen, and X. Sun, "Coverless image steganography without embedding," in *International Conference on Cloud Computing and Security*, 2015, pp. 123-132.

[21] 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.

[22] 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.

[23] 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.

[24] L. Zou, J. Sun, M. Gao, W. Wan, and B. B. Gupta, "A novel coverless information hiding method based on the average pixel value of the sub-images," *Multimedia tools and applications,* vol. 78, pp. 7965-7980, 2019.

[25] Y. Luo, J. Qin, X. Xiang, Y. Tan, Q. Liu, and L. Xiang, "Coverless real-time image information hiding based on image block matching and dense convolutional network," *Journal of Real-Time Image Processing,* vol. 17, pp. 125-135, 2020.

[26] 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.

[27] Q. Li, X. Wang, X. Wang, B. Ma, C. Wang, and Y. Shi, "An encrypted coverless information hiding method based on generative models," *Information Sciences,* vol. 553, pp. 19-30, 2021.

[28] Q. Liu, X. Xiang, J. Qin, Y. Tan, and Y. Qiu, "Coverless image steganography based on DenseNet feature mapping," *EURASIP Journal on Image and Video Processing,* vol. 2020, pp. 1-18, 2020.

[29] 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.

[30] 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.

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

[32] R. S. HAMEED, B. H. A. ABD RAHIM, M. M. TAHER, and S. S. MOKRI, "A LITERATURE REVIEW OF VARIOUS STEGANOGRAPHY METHODS," *Journal of Theoretical and Applied Information Technology,* vol. 100, 2022.

[33] A. Kumar and K. Pooja, "Steganography-A data hiding technique," *International Journal of Computer Applications,* vol. 9, pp. 19-23, 2010.

[34] K. Bennett, "Linguistic steganography: Survey, analysis, and robustness concerns for hiding information in text," 2004.

[35] S. Sharma, A. Gupta, M. C. Trivedi, and V. K. Yadav, "Analysis of different text steganography techniques: a survey," in *2016 Second International Conference on Computational Intelligence & Communication Technology (CICT),* 2016, pp. 130-133.

[36] G. Nikam, A. Gupta, V. Kalal, and P. Waghmare, "A Survey of Video Steganography Techniques," *Journal of Network Communications and Emerging Technologies (JNCET) www. jncet. org,* vol. 7, 2017.

[37] S. Bhallamudi, "Image Steganography Final project–Report," in *Tech. Rep.*, ed: Wright State University, 2015.

[38] 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.

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

[40] S.-Z. Wang, X.-P. Zhang, and W.-M. Zhang, "Recent advances in image-based steganalysis research," *Chinese journal of computers,* vol. 32, pp. 1247-1263, 2009.

[41] 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.

[42] S.-W. Ha and Y.-H. Moon, "Multiple object tracking using SIFT features and location matching," *International Journal of Smart Home,* vol. 5, pp. 17-26, 2011.

[43] 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,* 2007, pp. 197-206.

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

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

[46] N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," *Computer,* vol. 31, pp. 26-34, 1998.

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

[48] 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.

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

[50] 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.

[51] 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.

[52] 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.

[53] O. Hosam, "Attacking image watermarking and steganography-a survey," *International Journal of Information Technology and Computer Science,* vol. 11, pp. 23-37, 2019.

[54] M. Hussain, A. W. A. Wahab, Y. I. B. Idris, A. T. Ho, and K.-H. Jung, "Image steganography in spatial domain: A survey," *Signal Processing: Image Communication,* vol. 65, pp. 46-66, 2018.

[55] 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.

[56] 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.

[57] 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.

[58] 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.

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

[60] 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.

[61] 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.

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

[63] 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.

[64] 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.

[65] 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.

[66] https://data.caltech.edu/records/20086

المستخلص

أصبح أمن المعلومات الشغل الشاغل لأشهر الباحثين ومحور اهتمامهم ، حيث أنهم يحاولون باستمرار إيجاد أفضل الطرق وأكثرها أمانًا لنقل المعلومات عبر نفق آمن لحمايتها من محاولات القرصنة والهجمات الشائعة على الإنترنت. وفي هذا البحث حاولنا تجسيد إحدى طرق الأمان في حماية البيانات. إخفاء المعلومات هو نظام لإخفاء المعلومات. يهدف إلى إخفاء المعلومات السرية في ملف غلاف رقمي مثل الصورة دون الشك. من ناحية أخرى ، تهدف تقنية **Steganalysis** إلى الكشف عن وجود بيانات سرية مخفية في ملفات الغلاف. يعتبر نظام إخفاء المعلومات مكسورًا إذا تمكن المهاجم من الكشف عن وجود أو قراءة الرسالة المخفية.

باستخدام تقنيات إخفاء الصور النموذجية ، يتم اختيار صورة غلاف ، ثم يتم إدخال البيانات السرية فيها لإنشاء صورة **stego**. ومع ذلك ، فإن التضمين سيترك آثار تعديل في صورة الغلاف ، مما يجعل تحليل الإخفاء الناجح أمرًا سهلاً. لذا ، فإن كيفية إخفاء المعلومات بنجاح دون تغيير الناقل يمثل اختراقًا وتحديًا. يعد إطار إخفاء الصور بدون غطاء مجالًا جديدًا للبحث عند مقارنته بالطرق السابقة لإخفاء الصور. يحاول إخفاء الصور بدون غطاء إخفاء المعلومات السرية ، ولكن هناك العديد من التحديات الرئيسية التي يجب التغلب عليها: لإخفاء البيانات ، لا يلزم إجراء تغييرات على الصورة. بمعنى آخر ، لا يمكن نقل المعلومات السرية بدون ناقل ، ولكن يمكن إخفاؤها عن طريق إنشاء صورة حاملة مطابقة بصريًا للصورة الأصلية أو عن طريق إنشاء قواعد تعيين بين صورة شركة النقل والمعلومات السرية. يعد العثور على الصور ذات الصلة التي تحتوي بالفعل على معلومات البيانات السرية إحدى التقنيات لإخفاء البيانات السرية في إخفاء الصور غير المغطاة. تُستخدم صور **Stego** لتوصيل المعلومات الحساسة ويتم تصنيفها على هذا النحو.

أكبر مشكلة هي تحديد موقع الصور التي تحتوي بالفعل على المعلومات المطلوبة.

في هذه الأطروحة؛ تم تقديم طريقة إخفاء جديدة بدون غطاء لإخفاء البيانات السرية بطريقة أكثر أمانًا ولتعزيز القوة ضد الهجمات. تعتمد هذه الطريقة على مجال التردد. تتكون عملية التضمين من عدة خطوات. أولاً ، يتم تشفير البيانات السرية بطريقة التشفير المقترحة على أساس الفوضى

، ثم يتم تقسيم البيانات المشفرة إلى أجزاء غير متداخلة. ثانيًا ، يتم جمع مجموعة من الصور لإيجاد الصور المناسبة لتكون صورًا مغرورة. ثالثًا ، لبناء تسلسل تجزئة لصورة ما ، يتم استخدام خوارزمية تجزئة قوية. رابعًا ، لكل تسلسل تجزئة للصور ، يتم إنشاء بنية الفهرس المقلوبة. خامسًا ، اختر الصورة التي تعادل تجزئتها مع مقطع البيانات السرية. يتم إجراء العديد من الاختبارات لقياس متانة الطريقة المقترحة.

وفقًا للنتائج التجريبية ، فإن الطريقة المقترحة تفي بمتطلبين من الأمان والمتانة. حيث تم تطبيق النظام بلغة **Matlab2020**. كما توضح النتائج التجريبية متانة النظام ومقاومته لمجموعة من الهجمات مثل الضوضاء وضغط **JPG** والقص والتدوير والرسوم البيانية والمرشحات وقيم **NC** و **BER** تساوي ١ و ٠ على التوالي للأنواع من الصور المختبرة. أيضًا ، تقارن الطريقة المقترحة مع طريقة أخرى غير مغطاة حديثة تعتمد على طريقة التجزئة وتتفوق النتائج على الطرق الأخرى في معظم الهجمات.

وزارة التعليم العالي و البحث العلمي

جامعة بابل كلية العلوم للبنات

قسم علوم الحاسوب

اخفاء الصوره بدون غطاء بالاعتماد على الهاش المويجي الامن للصوره

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

مقدمة من قبل

نادية عبد الكريم عمران

اشراف

الاستاذ الدكتور
سهاد احمد علي

الاستاذ الدكتور
ماجد جبار جواد

١٤٤٤هـ

2022 مـ