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

Video Steganography Algorithm Based On Edge Detection

A Project

Submitted to the Council of the College of Science for Women at University of Babylon in Partial Fulfillment of the Requirements for the Degree of Higher Diploma of Science in Computer Science

By

Iman Khalid Obias Al-jebory

Supervised By

Prof. Dr. Suhad Ahmed Ali

2021 A.D

1443 A.H

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

﴿قَالُوا سُبْحَانَكَ لَا عِلْمَ لَنَا إِلَّا مَا عَلَّمْتَنَا إِنَّكَ أَنْتَ الْعَلِيمُ الْحَكِيمُ﴾

صدق الله العلي العظيم

سورة البقرة: الآية (32)

Supervisor Certification

I certify that project entitled "**Video Steganography algorithm Based on Edge Detection**" was prepared at the Department of computer Sciences/ College of Science for Women/ University of Babylon, by (**Iman khalid Obias**) as partial fulfillment of the requirements for the degree of Higher Diploma of Science in Computer Science.

Signature:

Name: Prof. Dr. Suhad Ahmed Ali

Date: / / 2021

Address: University of Babylon/College of Science for Women

The Head of the Department Certification

In view of the available recommendations, I forward the Project entitled "Video Steganography Algorithm Based On Edge Detection" for debate by the examination committee.

Signature:

Name: Dr. Farah Al-Shareefi

Date: / / 2021

Address: University of Babylon/College of Science for Women

Certification of the examing committee

We, the member of the examing committee, certify that we have read this project entitled (Video Steganography Algorithm Based On Edge Detection)and after examining the higher diploma student (Iman Khalid Obais Al-jebory) in its content in 2\12\2021, and that in our option and it is accepted as a project for the degree of higher diploma in science\computer science with a degree (excellent).

Committee chairman:

Signature:

Name: ***Majid Jabbar Jawad***

Scientific order: Prof. Dr.

Date: \ \2021

Committee member:

Signature:

Name: ***Saher Adel Kadum***

Scientific order: Asst. Prof

Date: \ \2021

Committee member (supervisor):

Signature:

Name: ***Suhad Ahmed Ali***

Scientific order: Prof. Dr.

Date: \ \2021

Date of examination: 2\12\2021

Deanship authentication of collegeof science for women.

Approved for the college committee of grade studies.

Signature:

Name: ***Faez Ali Rashid***

Scientific order: Prof. Dr.

Address: Dean of college science for women

Date: \ \2021

Dedication

Thanks to ALLAH in the first and last place, my Creator, to teacher and messenger, Mohammed (May Allah blesses and grants him), and his progeny, who taught us the purpose of life...

To that who taught me my first words, the joy of the spirit and the essence of life

... My affectionate mother (Allah have mercy on her)

To that who yanked a living from the cruelty of the rocks

... My dear Father (Allah have mercy on him)

To that vast space and land that sprouted from the blood of the martyrs to

... The beloved homeland

To those who bear on them the building of the generation of the future

... Our esteemed teachers

To all those, I dedicate my work

Acknowledgments

Praise and thanks to God who enable me to complete my thesis and facilitated the difficulties for me. Thanks are to all my teachers in the college of science for women; particularly I am highly indebted expressing my thanks to the supervisor in this thesis **Dr. Suhad Ahmed Ali** for his excellent guidance and encouragement to complete my thesis.

I would like to thank my dear brothers, sisters, for their love, patience, and understanding to spend my time on this research. This accomplishment would not have been possible without them.

Finally, I would like to thank all my friends and all the people who helped me during my higher diploma study.

Student Name

Iman khalid obias

Abstract

The most famous researchers' main concern and focus of attention have become information security, 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 Internet attacks, in this research, we attempted to embody one of the security methods in protecting data. Focusing on protecting texts sent from the note or modification by attackers by hiding them inside the video. The proposed method is to hide the Arabic and English texts, both of which are almost equally efficient. Initially, before hiding text in the cover video, the edge is detected by the three most significant bits of the frame pixel by the edge detection filters that it represents (Prewitt, Sobel, krich, Robert, Laplacian), Where the edge is determined by the threshold limit set by the user, and then the pixel in the original video frame is examined to see if it represents an edge point; if it does, four bits of text are concealed, and if it does not, two bits are hidden. This method is safer than hiding all the pixels in a sequence. This project reached the highest PSNR scale (**69.308**) through all edge detection filters when English text was embedding and the obtained PSNR ratio was (**68.4558**) when Arabic text is embedding. The difference between Arabic and English texts for PSNR scale values is because the number of English letters 26 needs 7 bits to represent it, while the number of Arabic letters 28 needs 8 bits to represent it, so the Arabic language needs more bits to embed, which means that it needs more Pixels of the image, thus the PSNR scale is reduced.

List of Publications

1. **Iman khalid obias al-jebory , Suhad A. Ali," Video Steganography algorithm based on edge detection" accepted in Journal of University of Babylon for Pure and Applied Sciences.**

Table of content

List of Tables

List of figures

List of Algorithms

List of Abbreviations

ASCII	**American Standard Code for Information Interchange**
AVI	**Audio Video Interleave**
EI	**Embedded Frame Image.**
ES	**Extract The Message**
HVS	**Human Visual System**
LoG	**Laplacian of Gaussian**
LSB	**Least Significant Bit**
LSBMR	**Least Significant Bit Matching Revisited**
MSE	**Mean Square Error**
NC	**Normalized cross correlation**
OPAP	**Optimal Pixel Adjustment Process**
PSNR	**Peak Signal to Noise Ratio**
RGB	**Red-Green-Blue**

Chapter one

General introduction

Chapter One
General Introduction

1.1 Introduction

In recent times, the digital world has become an unsafe medium due to the hackers and intruders present who are always looking to steal or access the data in an unauthorized way. To avoid the loss of data during transmission, data should be kept safe and transferred in a protected way. This can be done by using a variety of data hiding techniques where the original data is hidden or modified in an unreadable format which seems of negligible importance to the middle party. With the secrecy of data being the main concern, such techniques are well used. Hidden data techniques are not new. Such techniques have been used since medieval times when important data needed to be hidden and sent during times of wars and disputes. One of the classical examples of cryptography techniques is the Ceaser cipher, where the original data is modified in a specific way to make it unintelligible. This data is then sent to other regions and deciphered in the same way to extract the original message. The term "information hiding" refers to the process of embedding a secret message into a digital medium. The hidden message can take any form, including photos, text, movies, files, etc. which can be represented in bits. The cover file is used in steganography techniques to embed secret messages into it. This embedded cover file is called a stego-file[1].

Steganography is a method of concealing data. Its goal is to conceal secret information in a digital cover file (image, audio, video, etc) without being detected. The steganalysis technique, on the other hand, aims to discover the presence of secret data concealed in the cover files. If an attacker was able to reveal a presence or read the hidden message, the steganographic system was considered broken [2].

1.2. Related Works

This section highlights the steganography research that has already been completed using various technologies. Several strategies are linked for secret information communication:

In(2018) M. Aaref proposed that the secret message (English text) is hidden in the edge of the frames of the. AVI video without changing the details of frames. The secret message was embedded frames that have sufficient edge point details in them. The recommended solution was evaluated using both the Peak Signal to Noise Ratio (PSNR) and the Mean Square Error (MSE) since we calculated both PSNR and MSE between the cover frames and the embedded ones. The results obtained were objectively good as the PSNR value ranges from 74.5293dB to 75.9123 dB.[3]

In (2018) Ola presented an image steganography technique dependent on Chaotic-Address Steganography. The first technique is based on the well-known LSB technique, while the second technique is based on a recent approach that searches for the identical bits between the secret message and the cover image. Chaotic-Address (logistic) is employed in this technique to extract the shuffled addresses bits [4].

In 2019, Bannek et al. introduced Image masking technology using the "Kirsch mask", which has special properties for determining the maximum edge strength in various directions Depending on the threshold setting of the "Kirsch operator" and the intensity per pixel of the jacket image, a scale with three bands will be generated. This criterion is used to choose flexible possibilities for coding abbreviation, such as 2, 3, or 4 LSB. As a key, the threshold value can be shared with the target recipient. [5]

In (2019) D. Deshmukha and Dr. Kurundkar. proposed a new algorithm for concealing data in video. Hidden data has been disguised as text and inserted into video frames. Hiding in LSB bits reduces the resolution of pixels, making them more visible to the human eye during detection procedures and making them more vulnerable to attackers. However, unlike the LSB method, their proposed technique can embed a large amount of data. Different edge detectors are used in their approaches to detecting edges.[6]

In (2020) D. Deshmukh and G. Kurundkar proposed a text hiding by video steganography. For hiding data in video, two algorithms are used: random scan and edge detection. For edge detection of chosen frames, five edge operators are used: Sobel, Canny, Prewitt, Log, and Robert. They choose a frame at random to hide the text bits, and then the edge operators use it to find the edge. They discovered that Sobel has a greater number of edges than other operators. Robert operator has a small number of edges. Prewitt's edge map is medium.[7]

In 2020, Ayub and Selwal introduces a new image masking technique that embeds data in the carrier image's edge pixels. Because the edge pixels differ from their neighbors, the attacker is less suspicious of data fragments at the edges, ensuring improved security. Edge detection filters such as "Prewitt, Sobel, Laplacian, and Canny" are used in the proposed technique to mask existing images using edge-based data masking in the DCT field algorithm. Because of image compression, the suggested steganography approach reduces the image size[8].

In 2020, Prasad and Pal proposed a mechanism to increase the cover photo embedding ability, and the Cover Image feature was used to assist the process of masking parts of secret messages, whereby Additional confidential message bits are inserted in the edge region of the cover image rather than the smooth area. Portions of a confidential message are hidden in the cover photo using the parameter-dependent embedding process. The parts of the secret message are embedded in the cover image with the indication of the keys, i.e. what is known as a stego key, to increase the security of the content. The layout is applied to some typical grayscale photos [9].

1.3 Problem Statement

Due to the rapid growth of emergent technologies and information distribution, techniques are presented to protect secret information from plagiarism. A common secure technique is information hiding. The problem addressed in this project is the hiding of secret information inside the video in a way that prevents an adversary from the acquisition of the secret information. In case an adversary detects the presence of embedded information within the cover frame, it is challenging to recover the secret message if he does not have information about the mechanism of the algorithm used.

1.4 project Objective

Design and implement an approach for hiding text that is more secure and efficient. It is difficultly discoverable by using edge detection as an additional security dimension in steganography to realize the aim in keep data privacy, which is embedded.

1.5 project Organization

The remainder of the project is structured into four chapters, the contents of which are listed below:.

- **Chapter two: (Theoretical Background)**

This chapter presents a theoretical background of information hiding, edge detection, and performance evaluation.

- **Chapter three: (Proposed System Design and Implementation)**

This chapter presents a proposed method for protecting private data.

- **Chapter four: (Experimental Work and Discussion of Results)**

This chapter presents the description of the different experiments and discusses the results and evaluations obtained from the implementation of the proposed system.

- **Chapter five: " Conclusions and Future Works"**

Finally, the conclusions and future works will be presented in this chapter. In addition, in this chapter, some proposals are expressed future work Purpose may take.

Chapter two

Theoretical Background

Chapter Two

Theoretical Background

2.1 Introduction

Hiding an exclusive message or specific details through a medium by using a hidden method can be known as Steganography. This has been derived from two different terms steganos, and graphs. The first means to be confidential and not shared with any (individual), the second means to be realized by writing or drawing [1]. The text, image, video, or audio file can simply be the channel's cover medium where the data will be hidden to be private or confidential. The extra bits in the shell media can always be replaced and the secret data is put into space by the stego algorithm. Unnecessary parts with super standards of videos and sounds are available to hide. Moreover, there are many applications of steganography such as the military, industrial, copyright, and intellectual property rights (IPR) sectors. [8]

Due to the higher embed payload of videos compared to digital photos [10][11], and the temporal properties of video enable always redundancy, which is not provided in digital photographs, videos are becoming increasingly popular as a cover object in steganography. Confidential material can be easily buried inside a video with the high number of frames accessible.[11]

This chapter discusses the theoretical background related to the suggested system. In addition, it reviews the meaning of the information hiding, its types, the important component in it, and security requirements and techniques for video steganography.

2.2 Fundamental of Digital Video

Scenes make up the video. A scene is a series of pictures that depict a logical event. A shot is a collection of interconnected frames captured from a single camera, and it represents a continuous set of actions in place and time. A shot is a collection of images called frames [12]. The typical video structure is shown in Figure 2.1. A video includes a series of frames cascading at the speed of around 20 to 30 fps to view movement [13].

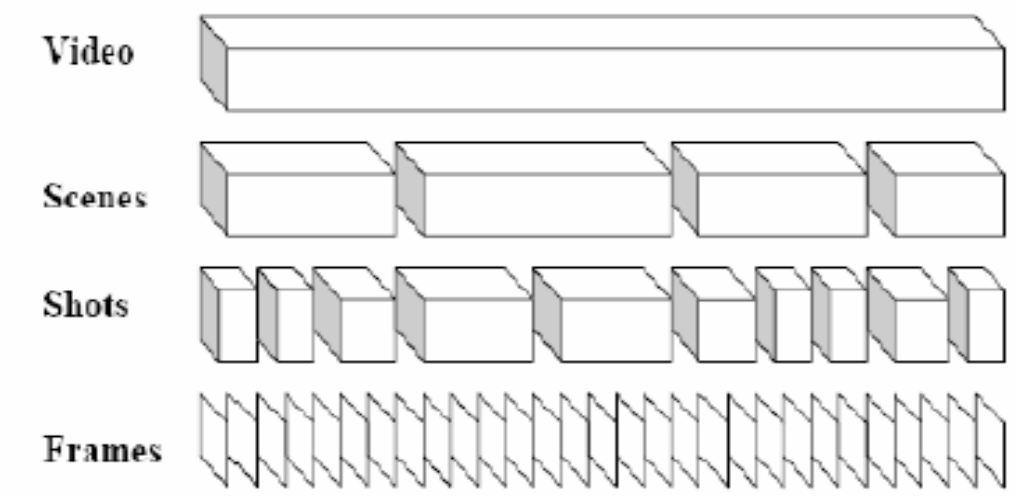


Figure (2.1): Typical Video Structure [19]

2.3 Information security system

Information security (also known as InfoSec) has been defined as "The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability".

2.4 Data hiding or (information hiding)

The early steganography of information was simple methods, before the phones and the mail, whereby the messages were sent by people in secret ways. If you want to hide a message, you have two options: the first is saved by the sender, or the second is to hide it. Whereas, masking data is the technology to include secret information in digital data so that it cannot be seen with the naked eye or audible. In many fields of use, Hide has recently become important. Digital audio, video, and images have become increasingly necessary but unnoticeable, which may include hidden notification of copyright or serial number, which can contain hidden copyright or serial number notification or maybe help to stop unauthorized copying directly. Information hiding techniques are often divided into two parts, such as hiding information/watermark, as shown in Figure (2.2).

Steganography techniques have recently become relevant in a variety of applications. Digital audio, pictures, and video clips are increasingly being packaged with distinct but undetectable tags that may include a serial number or a concealed copyright notice, as well as aid, prevent unauthorized direct copying. [14].

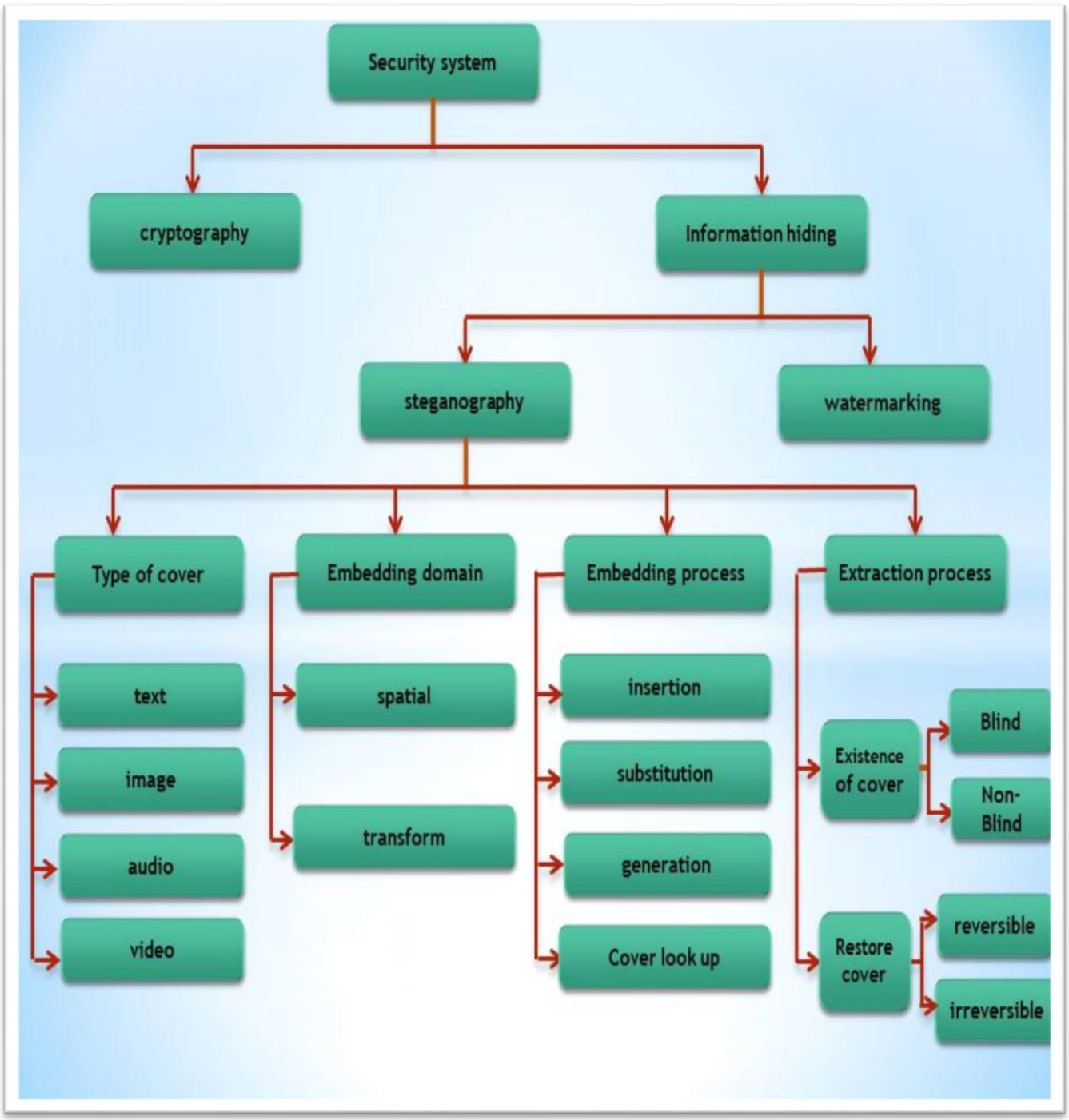


Figure (2.2): Information security system classifications[13]

2.4.1 Steganography

Steganography, which plays a fundamental role in information security, is the art of communicating using information that can not be seen. The word "steganography" comes from the Greek "covered writing". Steganography is used in three components: the “Cover Image” consoles a hidden message, the “Secret Message”, and the “Stego Image” (a cover element with an embedded message). For information steganography purposes, the image (stego image) used must be the same. The image (stego image) used to hide the information must be the same as the original image, of the Stego image, to avoid raising suspicion about the "Stego image" Data masking and the ability to embed a picture are the two basic requirements that are widely considered in many steganography techniques. Steganography is the method that hides data most simply so that no one other than the recipient knows that there is a secret message hidden within the information that is being sent. Also, the main advantage of this method is that no one else except the recipient is supposed to receive the data, so there may be suspicion of hidden information within the message that is being ignored as a channel [15].

Steganography technique has been used in ancient years traced back to 440 B.C. to transfer secret messages. The most famous example, Histaeus king in old Greece utilized it to shave the slave’s head and tattooed some secret information on it. The objective was to ire an insurgency against the Persians. When the slave’s hair grown again sent to dispense the message. Then, the receiver shaved the slave’s hair and get the key messages. In the modern era, steganography is utilization on computers with digital data that is utilized for several purposes like embedding copyright, embedding an individual’s detail in smart IDs, and entering patient detail during a medical imaging system [16].

The applications of steganography are secret Communication, military, medical imaging, internet banking, intelligence agencies, and others [17]. The factors used to determine the effectiveness of any steganography technique are imperceptibility (in which a person should be unable to distinguish the cover object and the secret message), robustness (indicates to the degree of difficulty required to devastate a secret message without destroying the cover object), and payload capacity (denotes to the message size) [18].

Steganography is done by changing bits of redundant information in uniform files like (texts, audio, or image) with bits of secret data [19].

Figure (2.3) shows a graphical representation of steganography. A typical steganography system contains two main steps, one for embedding and one for extraction. The embedding algorithm is used to insert the message within a carrier medium such as an image, audio, and video, where the extraction method extracts the embedded message from the cover. The embedding algorithm is more difficult than the extraction algorithm. The embedding algorithm is used to embed the message within a carrier media such as an image, audio, or video, and the extraction method is used to extract the embedded message from the cover. The embedding algorithm is more difficult than the extraction algorithm. Using the stego key, which is necessary to begin the embedding or extraction process, is one technique to improve steganography security. It is utilized to make the extraction process computationally infeasible for unauthorized users. The steganography terminology is listed.

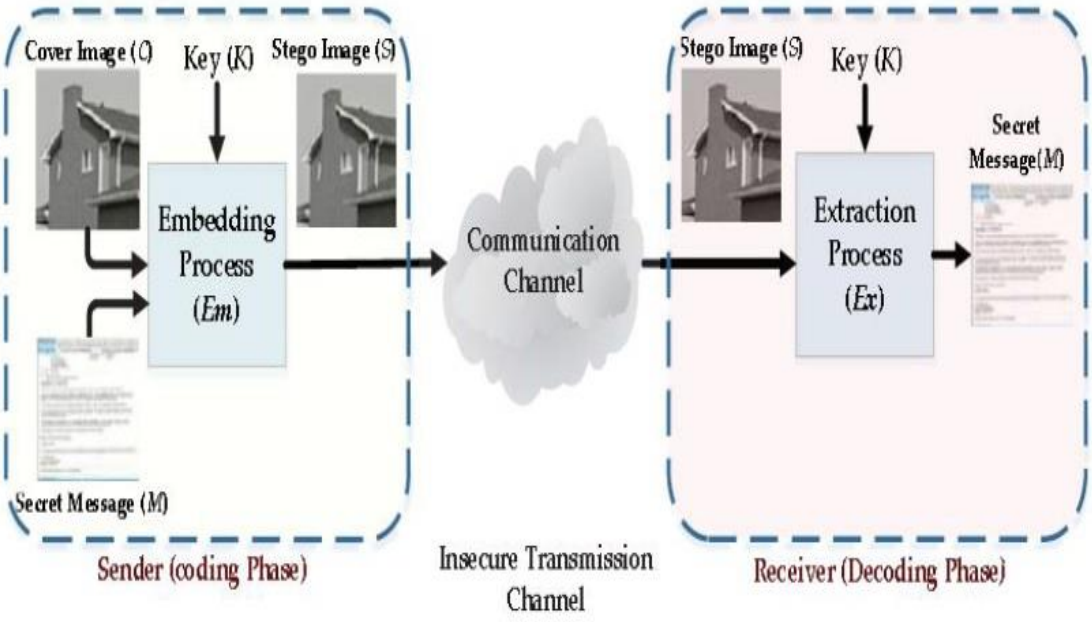


Figure (2.3): Steganography Structure

2.4.2 Steganography Types

The type of cover data is also the type of steganography. today, steganography is examined as a text, audio, video, image, and protocol steganography [20].

1. Text Steganography

Confidential data is hidden in text files. Different methods can be used to hide the data in the text file. These methods include;

• "**Format Based Method"**: Confidential data is hidden inside cover data with methods such as adding text spaces, deliberate typing errors, sizes of writing types. This method is easily detectable by computer software, hence, it is a less preferred method.

• **Random and Statistical Method:** Hidden data is stored inside character strings. Places, where confidential data are hidden, must be reported to the extractor.

• **Linguistics Method**: Hidden data is stored in the syntactic structure.

2. Audio Steganography

This method hides data inside sound files. In this method, audio file formats such as WAV, AU, and MP3 are used as cover data. Audio steganography has different methods [21]. These methods include;

- **Least Significant Bit (LSB)**
- **Parity coding**
- **Phase coding**
- **Spread spectrum**
- **Echo hiding**

3. "Video Steganography"

It's a method for concealing any type of information or data within a digital video format file. H.264, Mp4, MPEG, and AVI video codecs are commonly used as cover data in video steganography. A video file is a file that contains both audio and image at the same time. So almost all of the steganography techniques that can be applied to image and audio files can be applied to video files. Video steganography provides less perceptibility because the video is the fast flow of images and sounds [21]. Due to the large size of video files, the payload capacities of video steganography is quite large [21].

Video steganography techniques are divided into several categories. The embedding approach, i.e. spatial or substitution-based techniques and transform-based techniques, is one way to categorize video steganography techniques. Compressed [22] and Uncompressed Video methods [23, 24] can also be used to classify videos, as Fig (2.4) illustrates. An approach that is based on the classification to identify video steganography approaches, such as Format-based and Video Codec Methods, is another option. [15].

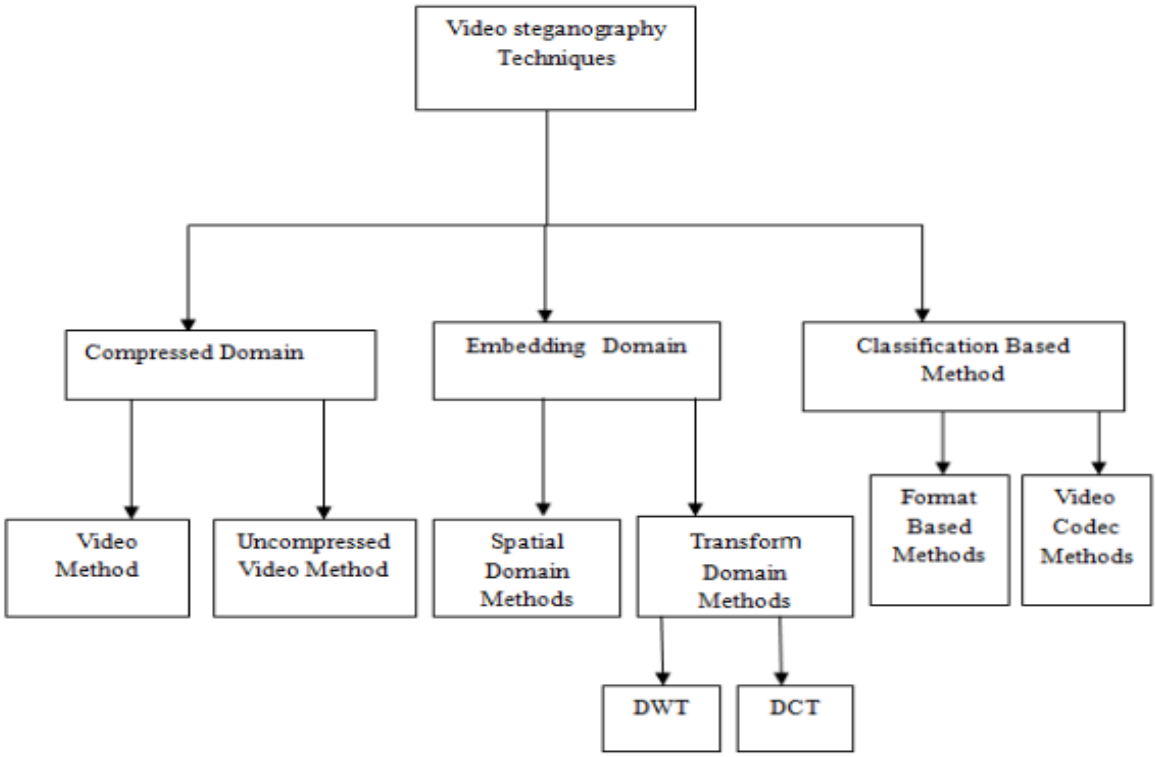


Fig 2.4 Video Steganography Techniques Classification

4. Image Steganography

Today, “hiding information” within images is a common practice. On the "World Wide Web" or in newsgroups, an image with a hidden message can be easily posted. and is difficult for the human eye to detect [16]. Many different image file formats exist in the digital image domain, most of them for particular applications. There are distinct steganographic algorithms for these various image file formats[14].

Usually, two elements are discussed when information is hidden. First, in all potential statistical attacks, the cover media and the media must appear to be identical. Second, the accuracy of the media must not be decreased by the process of inclusion, The difference between the Stego and cover media, in other words, must be unnoticeable to the human visual apparatus. With the help of the key and embedding algorithm, which is shared by the sender and the receiver, a message is embedded in

the cover object, resulting in a matching Stego object that is sent over a communication channel and the extraction algorithm extracts a secret message with the help of the Stego-Media key.

While some progresses have been made in masking information for binary images [25, 13] and 3D images [26], studies mainly suggest masking data in grayscale and color images. As the luminance element, the color image is grayscale, we specialize in making images in grayscale images. In addition, it is commonly considered that gray-scale images are better suited to mask data than color images [27] because the imbalance of correlations between color components can easily reveal the effect of inclusion.

In "noisy" locations with many color variations, a cover source can be adjusted to hide a message within an image without changing its apparent qualities, thus adjustments will be drawn less notice. The most popular methods for creating these modifications include the use of less significant bits or "LSB on the cover image, masking, filtering, and transformations" These methods are frequently utilized in various types of image files, with differing degrees of effectiveness [28].

Steganography consist of basic components: "secret message," "cover message", "secret key," and an "embedding algorithm"

2.5 Spatial domain

The easiest and the simplest way of data embedding in digital images is to modify the cover image pixel values in the spatial domain itself. These techniques use the cover image pixel intensity value levels directly or indirectly to embed the secret message bits. Herein some of the steganographic schemes come under the spatial domain technique includes. Least Significant Bit (LSB), Pixel Value Differencing (PVD) and Texture based[29].

- **Least Significant Bit (LSB) steganography:** Least Significant Bit (LSB) technique is one of the easiest and hence popular spatial image steganographic approaches. The idea behind this method is that, in an image, the least

significant bits represent only feeble information and small changes in those bits cannot get detected by human eyes. In LSB-based spatial domain techniques, the secret data get embedded directly in the host image by altering the least significant bits of selected pixels without distorting the visual quality of the original cover image. This technique yields when it is used in communication channels with only human attacks, where the intruders cannot find visual quality degradation.[29]

- **Pixel value differencing (PVD)** This technique subdivides the cover image into non overlapping blocks consisting of two connecting pixels. It hides the data by altering the difference between these two pixels. The area of the pixel decides the hiding capacity of this technique. For example, if the edge area is chosen, then the difference is high in between the connected pixels, whereas in smooth areas the difference Lecture 6 (Steganography) 4 is low. Thus, the best choice is to select edge areas to embed the secret message that is having more embedding capacity.[29]

- **Texture based:** In this technique the secret and host images are divided into blocks of specific size and each block in secret image is taken as a texture pattern for which the most similar block is found among the blocks of the host image. The embedding procedure is carried on by replacing these small blocks of the secret image with blocks in host image in such a way that least distortion would be imposed on it.[29]

2.6 Edge Detection

Edge is the basic feature of an image[30]. Border pixels connecting two separate regions are known as the edge. Edges can be defined as image pixels changes. Edges distinguish boundaries and are therefore a major problem in image processing. [31].

Edge detection lets users look at those features of an image where there's a more or less sudden alteration in gray level or texture refer to the top of 1 region at the image and therefore the beginning of another[32]. Edge detection within image processing is a well-developed self-domain. key features can be extracted from the image edges, lowering the amount of data to process while maintaining the image's critical structural features [31].

Figure (2.5) and Figure (2.6) below [31] show two images example (original image and an image after edge detection).

Figure (2.4)

Figure (2.5)

Edge detection can be done in various methods. However, the majority of the processes may be classified into two parts: Laplacian and Gradient[33].

1. Gradient: - The edges are detected by the gradient methodology which is one of searching for the minimum and the maximum within the initial derivative of the image.

2. Laplacian:- The Laplacian method looks for zero crossings in the image's "second derivative" to check for edges. The position of the image can be highlighted by measuring the derivative of an Edge, which contains the 1D shape of a ramp. There are

many techniques for detecting edges, such as Sobel, Prewitt, Robert, Kirch, Laplacian, Canny, Fuzzy logic.

2.6.1 Sobel Edge Detection

In 1970, Sobel submitted this method (Rafael C.Gonzalez's (2004) "Sobel edge detection" [31]. In image processing techniques, "Sobel edge detection" is used. Edge detection using the horizontal (180 degrees) as well as the vertical axis is better with Sobel kernels (90 degrees). The detachable Sobel operator is based on a convolving image with an integer-valued filter [34].

The average kernel and differentiation products of the Sobel nucleus can be deconstructed. It will calculate the color gamut by homogenization. The "x-coordinate" is defined as a "right direction" increase, while the "Y-coordinate" is defined as a "down direction" increase. The generated gradient approximation can be merged for each point of the image to give the gradient size and direction. [32]. And Sobel masks as shown in Figure (2.7) [33]:

-1	0	+1
-2	0	+2
-1	0	+1

Gx

+1	+2	+1
0	0	0
-1	-2	-1

Gy

Figure (2.7): 3x3 masks of Sobel edge detection[32]

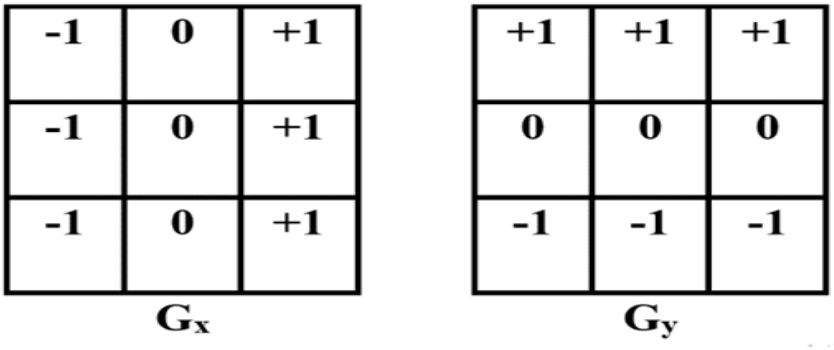
The resulting gradient approximations can be blended at every point on the image. to give the “gradient” magnitude and direction of the gradient by utilizing Equation (2.1) and Equation (2.2) [32,33].

$$Edge\ Magnitude = \sqrt{Gx^2 + Gy^2} \ldots\ldots\ldots\ldots\ldots (2.1)$$

$$Edge\ Direction = \left(\frac{Gy}{Gx}\right) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2.2)$$

2.6.2 Prewitt Edge Detection

The Prewitt edge detection was proposed by "Prewitt" in 1970. [31]. This operator is identical to “Sobel,” but the mask coefficients are different[30]. Prewitt edge detection represents a simple way to estimate the size and direction of edges. A time-consuming mathematical technique is required for edge detection of a differential gradient. The compass's edge detection method determines the direction directly from the core with the largest reaction, rather than using magnitudes in the "x and y directions" [34].



Figure(2.8)3x3 prewitt edge detection masks[33]

The edge magnitude and its orientation as defined in the following Equation (2.3) and Equation(2.4) [33] :

$$Edge\ Magnitude = \sqrt{P1^2 + P2^2} \quad \text{(2.3)}$$

$$Edge\ Direction = \left(\frac{P1}{P2}\right) \quad \text{(2.4)}$$

2.6.3 Robert Edge Detection

The Edge of Roberts was revealed by Lawrence Roberts (1965) [31]. Robert Roberts very accurately locates the edges but it is unable to remove noise. As employing the Gradient Detection method, edges form when brightness varies and have complex shapes. [33], edges can be detected more accurately. The following is a description of the Roberts mask: Figure (2.9).

0	0	0
0	−1	0
0	0	1

0	0	0
0	0	−1
0	1	0

Figure(2.9) : The Roberts operators[32].

Roberts Cross factor performs an easy and fast measurement of a two-dimensional spatial scale on the image. This detector uses much less than other devices due to its limited functions like it is asymmetric and cannot be generalized to detect edges that multiply from 45 ° C. The parameter used for this function is the same as the Sobel operator[30].

2.6.4" Kirch Edge Detection"

The method of Kirsch for edge detection was proposed by Kirsch in 1971 [36]. Kirsch's method for Edge Detection locates all eight edge responses in predetermined directions "East (E)", "Southeast (SE), South (S), Southwest (SW), West (W), Northwest (NW), North (N), and Northeast (NE)" are examples of predefined edge replies. In This algorithm, each core mask rotates at a 45-degree angle before incrementing through the compass's eight directions. The maximum size for each pixel of the image in all directions to form the warp is used to determine edge responsiveness. In most cases, To determine kirsch edge reactions, the following eight masks are used. To render warping, the edge reaction to each pixel of the image is determined, such as maximum size in all directions. Figure 1 shows the eight masks used to measure Kirsh edge responses (2.10) [37] :

$$k_0: E=\begin{bmatrix}-3 & -3 & 5\\ -3 & 0 & 5\\ -3 & -3 & 5\end{bmatrix} \quad k_1: NE=\begin{bmatrix}-3 & 5 & 5\\ -3 & 0 & 5\\ -3 & -3 & -3\end{bmatrix} \quad k_2: N=\begin{bmatrix}5 & 5 & 5\\ -3 & 0 & -3\\ -3 & -3 & -3\end{bmatrix} \quad k_3: NW=\begin{bmatrix}5 & 5 & -3\\ 5 & 0 & -3\\ -3 & -3 & -3\end{bmatrix}$$

$$k_4: W=\begin{bmatrix}5 & -3 & -3\\ 5 & 0 & -3\\ 5 & -3 & -3\end{bmatrix} \quad k_5: SW=\begin{bmatrix}-3 & -3 & -3\\ 5 & 0 & -3\\ 5 & 5 & -3\end{bmatrix} \quad k_6: S=\begin{bmatrix}-3 & -3 & -3\\ -3 & 0 & -3\\ 5 & 5 & 5\end{bmatrix} \quad k_7: SE=\begin{bmatrix}-3 & -3 & 5\\ -3 & 0 & 5\\ -3 & 5 & 5\end{bmatrix}$$

Figure(2.10) : Kirsch masks[36]

the largest value found when rotating each mask with the image is used to define the size of the edge. The direction is determined by the mask having a maximum volume [36].

2.6.5 Laplacian Edge Detection

The "Gaussian Laplacian (LoG)" was proposed by Marr (1982). The Laplacian edge detector calculates a second-order derivative, which represents the LoG of an image f(x, y), as well as the 2D function derivative. The term is commonly referred to as an equation (2.5) [35]:

$$"\nabla^2 f(x,y) = \frac{d^2 f(x,y)}{dx} + \frac{d^2 f(x,y)}{dy}" \quad \ldots\ldots(2.5)$$

Which has two effects: The image is smoothed and the Laplacian is calculated., resulting in a “double-edged image”. Then find zero intersections between double edges to define the edges. The mask is occasionally used to implement the Laplacian function numerically below [36] :

0	-1	0
-1	4	-1
0	-1	0

G_x

-1	-1	-1
-1	8	-1
-1	-1	-1

G_y

Figure(2.11): Mask Laplacian[36]

The Laplacian Operator is sensitive to fine lines and independent points and measures edges from all directions. it's a passive effect on noise, though, and generates dual pixel edges[35].

2.6.6 Canny Edge Detection

"Canny Edge Detection technology" is one of the most common edge detection methods in image processing since its development. In 1983, John Kanye introduced it in his master's thesis at the Massachusetts Institute of Technology. It still outperforms many of the modern algorithms that have been developed [31]. Canny is a highly significant method for detecting edges since it separates the noise from the image before locating edges. The Canny method is preferable since it preserves the image's edge features and relies on the direction to identify the edges and threshold value. [36].

The discovery of the optimum edge detection algorithm was canny's goal. Within these criteria, the "optimal" edge detector is[33, 31]:

i. "Good discovery": Within the original image, the approach should define as many real edges as possible.
ii. "Good localization": The various edges of the image should be as close to the sides as possible.
iii. " Minimum response": This condition indicates that the edge of a picture should only be differentiated once, and noise should not cause any false edges. To apply this algorithm or technique[31, 32], Canny suggested a sequence of steps(5 steps).

Step1(Noise reduction): - Edge detection results are extremely sensitive to image noise. Applying Gaussian blur to the image to smooth it out is one technique to get rid of the noise. To accomplish so, a Gaussian Kernel (3x3, 5x5, 7x7, etc...) is used in conjunction with picture convolution. The kernel size depends on the expected blurring effect".

Step 2 (Gradient calculation): - The gradient computing stage calculates the image's gradient by detecting the edge strength and direction using edge detection operators. A change in the intensity of pixels is represented by edges. Using filters that highlight the intensity shift in both horizontal (x) and vertical (y) directions is the simplest way to notice it (y) When the image is smoothed, the derivatives Ix and Iy w.r.t. x and y are found. By convolving I with the Gx and Gy Sobel kernels, respectively, it can be realized.[32]:

$$Gx=\begin{bmatrix}-1 & 0 & 1\\ -2 & 0 & 2\\ -1 & 0 & 1\end{bmatrix} \qquad Gy=\begin{bmatrix}-1 & -2 & -1\\ 0 & 0 & 0\\ 1 & 2 & 1\end{bmatrix}$$

:

The gradient's magnitude G and slope are then determined as follows:

$$|G| = \sqrt{Gx^2 + Gy^2} \approx |Gx| + |Gy| \text{.....(2.6)}$$

$$"\theta(x,y) = \left(\frac{Gy}{Gx}\right)" \text{.....(2.7)}$$

Step 3(Edge Linking): This step shows that until the edge direction obtained in Step 2 above is identified, we will link it to a controllable direction inside the image. “Canny” proposed that four essential rules be followed for this purpose:

If Theta is in the range of 0 to 245(0)OR 15750 to 1800, it is set to 0

If Theta is in the range of 2450-0675(0), it is set to 450.

If Theta is in the range of 675(0) to 112.5(0), it is set to 900.

If Theta is between 122,560 and 157,560, it is set to 1350.

Step 4(“Non-maximum suppression”): This step indicates that after selecting any of the four directions of the edge, the non-maximum for repression should now not be applied. “Non-maximum” repression is utilized to trace along an edge in the direction of the edge and suppress any pixel value (make it equal to 0) that is not considered an edge. The "no maximum repression" step will only preserve those pixels that are at an

edge with a higher gradient size. This will result in a very fine line in the resulting image. Three pixels at 3 x 3 about pixels (x, y) are check-up so that.

"If Θ = , then the pixels (x + 1, y), (x, y), and (x − 1, y) are check up"

"If Θ = , then the pixels (x + 1, y + 1), (x, y), and (x − 1, y − 1) are check up".

"If Θ = , then the pixels (x, y + 1), (x, y), and (x, y − 1) are check up

"If Θ = , then the pixels (x + 1, y − 1), (x, y), and (x − 1, y + 1) are check up".

"If the pixel (x, y) has the biggest gradient magnitude of the three examined pixels, very importantly saying it's preserved as an edge".

"If one of the other two pixels has a higher gradient magnitude, then pixel (x, y) should not be preserved as an edge".

Step 5 (double threshold): This stage, which comes at the end of "Canny," suggests that we should decelerate. This step shows that there are still local noise-induced maximum limitations after step 4. Therefore, we use thresholds and not one, but two thighs and thresholds are used. Therefore, for a single pixel considered to have a G scaled to size, To create the single-pixel edge, the rules of thumb must be followed.

"If G < Tlow discard the edge". "If G > Thigh keeps the edge".

If G is between Thigh and Tlow and any of its neighbors during a 3 ×3 region around it have gradient magnitudes greater than Thigh keep the edge.

If none of the pixel's neighbors have large gradient magnitudes, but there is at least one pixel between Thigh and Tlow, scan the 5*5 regions to see if any of them have a magnitude greater than Thigh. If that's the case, preserve the edge but discarded it.

2.7 Methodology

Ineffective knowledge, noise, and frequencies are filtered out in edge detection while keeping the necessary structural properties in the image. One of the favored ways to represent input images and their features is edge maps. The process of measuring the quality of the image is of great importance, especially in medical images because it is related to human life and their health, so the quality of the image is very important[33].

2.7. 1 "Mean Square Error (MSE)"

The mean squared error of an estimator, which is the difference between the estimator and what is estimated, is used to compute the average of the squares of the "errors." The contrast occurs due to chance or because the estimator fails to calculate information that would allow for a more accurate estimate. The PSNR has differed inversely from the MSE. The M.S.E can be found from the following Equation (2.8) [33]:

$$“MSE = \frac{1}{mn} \Sigma_{1=0}^{m-1} \Sigma_{j=0}^{n-1} \left(p_1(i,j) - p_2(i,j)\right)^2 \text{ …….(2.8)”}$$

Where I (i, j) and K (i, j) are the edge detected image and ground truth image respectively and m, n are the dimensions of the image.

2.7.2.” Peak Signal to Noise Ratio”

PSNR is the ratio of corrupting noise power to the signal's maximum potential power, which determines the sincerity of its depiction. PSNR refers to the ratio of the edge detected images to the ground truth image, which is also known as the estimated image. also known as estimator output PSNR can be rated by the following Equation (2.9) [33]:

$$PSNR = 10\, log10\, (MAXi^{\,2} / MSE) \text{ …..(2.9)}$$

MAXi is the maximal variation in the input image data. If it has an 8-bit unsigned integer datatype, MAXiis255.

2.7.3 YCbCr color space

To ensure a robust watermark an alteration in one color component from the host image must not affect the other color components. [18]

The color space YCbCr divides a color image into three components (Y represents the luminance component; Cb and Cr represent the chrominance components). To make the watermark imperceptible, the luminance's of key frames are used to embed the watermark and the chrominance is left

unchanged. The equations (2.10) and (2.11) show transformation from RGB to YCbCr and YCbCr to RGB respectively [19].

$$\begin{bmatrix} Y \\ Cb \\ Cr \end{bmatrix} = \begin{bmatrix} 16 \\ 128 \\ 128 \end{bmatrix} + \begin{bmatrix} 0.257 & 0.504 & 0.098 \\ -0.148 & -0.291 & 0.439 \\ 0.439 & -0.368 & -0.071 \end{bmatrix} \cdot \begin{bmatrix} R \\ G \\ B \end{bmatrix} \quad \dots (2.10)$$

$$\begin{bmatrix} R \\ G \\ B \end{bmatrix} = \begin{bmatrix} 1.164 & 0.000 & 1.596 \\ 1.164 & -0.392 & -0.813 \\ 1.164 & 2.017 & 0.000 \end{bmatrix} \cdot \begin{bmatrix} (Y-16) \\ (Cb-128) \\ (Cr-128) \end{bmatrix} \quad \dots (2.11)$$

When JPEG compression tolerance and noise addition are important, the Y-component in YCbCr is best for hiding data, the Cr-compone nt in color space is best for resisting scaling and rotating attacks, and the Cb-component is best for cropping resistance. To achieve maximum robustness against the majority of attacks YCbCr color space is used for watermarking [20].

2.7.4 Edge Entropy

It is a metric that gives some information about the texture of an image as edges of the image. This metric is used in some hidding techniques to determine the appropriate location for embedding a watermark in an image. The points edge is not suitable for embedding and can cause destroying the host image,

so using this metric is used to determine which block of the image is good for the embedding process, in other words, this metric preserve provides a good level of imperceptibility[20] .Edge entropy is calculated according to the equation (2.12).

$$E = \sum_{i-1}^{n} \quad P_i^{exp(1-P_i)} \qquad \dots (2.12)$$

Where P_i represents the probability of the pixel value i.

Chapter three

Proposed System Design and Implementation

Chapter Three
Proposed System Design and Implementation

3.1 Introduction

The Internet has now become a major channel for delivering information from one place to another such as text, image, sound, and video data. Information security is one of the most important factors of information and communication technology. For security purposes, the concept of steganography is used. video steganography is a technique by which information can be secretly included by hiding through the video.where The edges of candidate frame were used to include the secret message, so that the effect on the frame is less than the inclusion in the direct least important bit. The edges represent the most powerful areas in the image, the inclusion in them is not noticeable due to the intensity of the coloration in those areas.

This chapter describes a proposed system, based on steganography technique and edge detection , for preserving the security of the data. In this chapter, the proposed system used Figures, procedures, and algorithms that explain the method of hiding the proposed information . The suggested method hiding Arabic and English texts with video.

3.2 The Suggested System The suggested method aims to protect the text by hiding it in the cover video as shown in Figure (3.1).

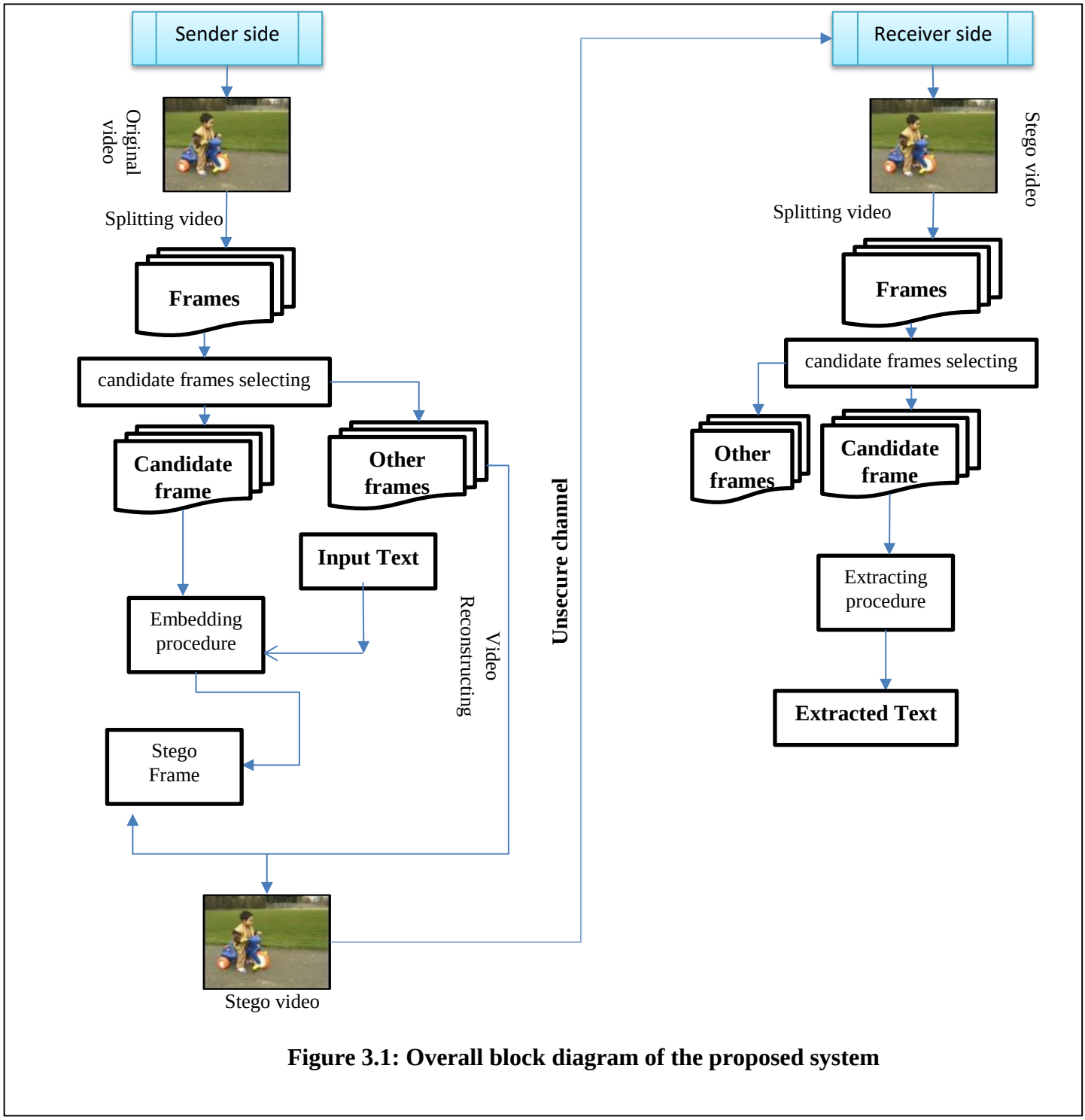


Figure 3.1: Overall block diagram of the proposed system

Algorithm (3.1) illustrates the overall steps that are done on the sender side.

Algorithm (3.1): General Steps of the Sender
Input: - *Org_v* // Input Original Video. - *Org_Txt* // Input Text. **Output:** - *S_v* // Stego video.
Step 1: Split the original video (*Org_v*) into frames. **Step 2:** Read the original text (*Org_Txt)* **Step 2.1:** Obtain the ASCII code for each character in the input text. **Step 2.2:** Convert each ASCII code for each character into binary code. **Step 3**: Extract a candidate frame (*Cframe*) using algorithm (3.2). **Step 4**: Embed *text bits* in candidate frame image to form the Stego frame (*Sframe*) by applying embedding process. **Step 6:** Combine other video frames with stego frame to get Stego video (*S_v*).

The scheme proposed consists of two procedures.

- procedure at (sender side)
- Procedure at (receiver side).

3.1.1 **Procedure at Sender Side**

This procedure is done on the sender's side. This procedure consists of several steps. These steps are listed as follows:

Step 1: Splitting the Input Video into Frames

In this step, the video is decomposed into frames. These frames will be used in the next step.

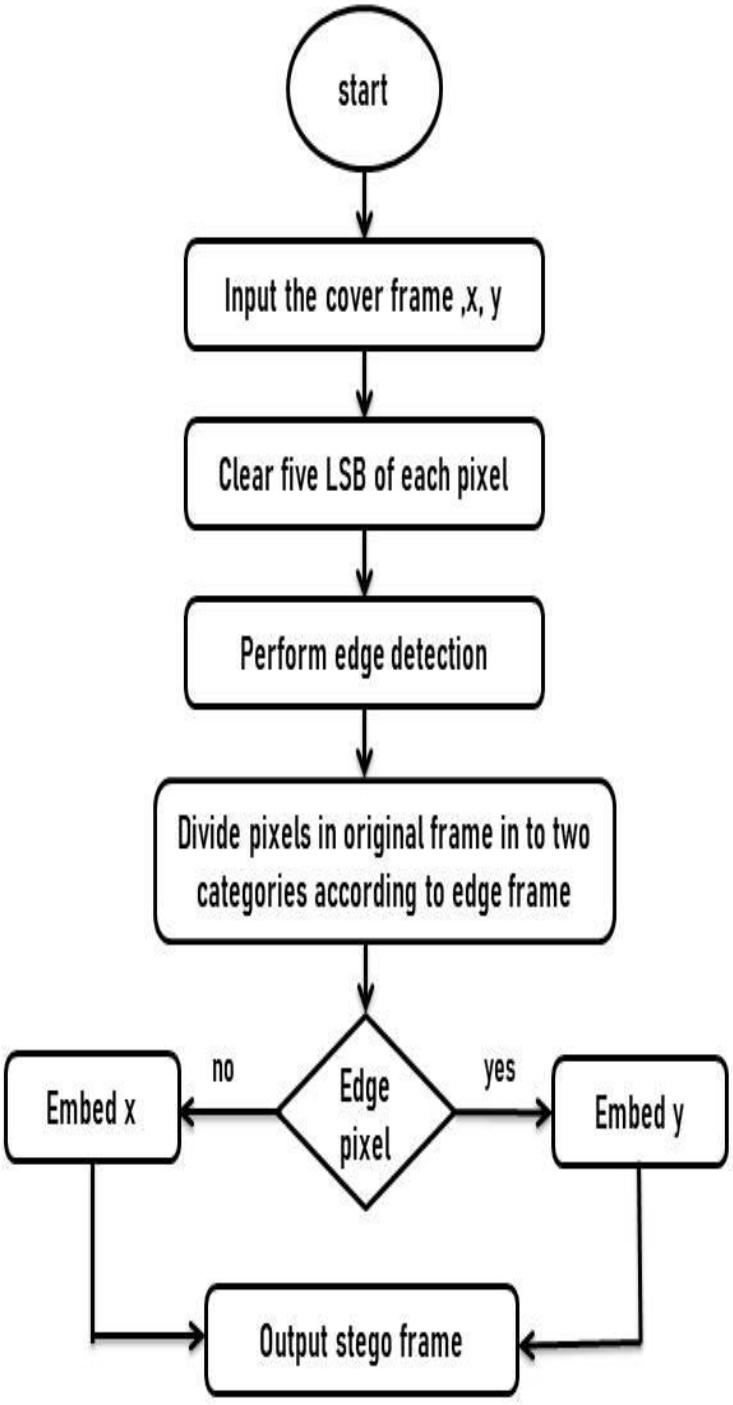
Step2: Selecting the Candidate Frame for Embedding Procedure

After decomposing the video into frames, a candidate frame is extracted to be as a cover for embedding the input text. The extracting procedure is done by applying algorithm (3.2)

Algorithm (3.2): Candidate frame extraction
Input : - Video Frames. - N //number of frames **Output:** - (*Cframe*) Candidate frame. - (Findex) index of Candidate frame.
Step 1: For each frame I from 1 to N do **Step 1.1:** Convert RGB color frame into grayscale color using equation (2.7) **Step 1.2:** Calculate the edge entropy of each frame using equation (2.12) and save the results on (Eframes) array. **End For** **Step 3: Sort** (Eframes) array in ascending order. **Step 4:** Find the frame with less edge entropy and save as candidate frame (*Cframe*) with it's index (Findex). **End**

Step3: Embedding Process

An embedding process is done on the sender side. It includes many steps, which depict in Figure (3.2).



Figure(3.2): Embedding Procedure Flowchart

A. Clear Pixel

A frame is a group of pixels that represent color values, or what is known as the image's density. Each pixel in the image consists of 8 bits, so at this stage clear the five least important bits of each pixel will be by substituting the value zero instead of the value of that bit. The following example depicts the clearing process to get the most significant bits frame.

Table (3.1): example depicts the clearing process

Pixels	Clearing five LSB	New Pixels
155=10011011	10000000	128
126=01111110	01100000	96
88=01011000	01000000	64
156=10011100	10000000	128

B. Edge Detection

This step is based on the previous stage, where the edge of the top three bits of importance is revealed by using a set of filters for detecting edges, including Sobel, Robert, Krich, laplacian, and Prewitt. The following example shows how to detect the pixels in the most significant bits frame in the previous step as edge pixel by assign the value (1) and non-edge pixel by assigning the value (0).

Table(3.2): example shows how to detect the pixels in the most significant bits

New pixels	**128**	**96**	**64**	**128**
Edge Pixels	1	0	0	1

Algorithm (3.3) shows the edge detection process using a set of filters for detecting edges, including Sobel, Robert, Krich, and Prewitt.

Algorithm (3.3): Edge detection

Steps for the method to detect edges
Input: Candidate Frame

Output: Detected Edges

Begin
Step 1: frame Image entry to read
Step 2: stratify Mx "horizontal mask" and My "vertical mask" to the input image
Step 3: Apply various "edge detection algorithms" and get a gradient
Step 4: Create a separate image for both Mx and M_y
Step 5: Results are combined to find the absolute gradient magnitude as per equation (3.1).

$$G[f(x,y)] = \sqrt{M_x^2 + M_y^2} \ldots\ldots\ldots\ldots\ldots\ldots (3.1)$$

Step 6: The absolute magnitude is the image of the magnitude of the resulting slope
Step7: if G[f(x,y)]>T, then possible edge point

End

C. Embedding Process

Depending on the previous stage, the cover frame original pixels are classified into two categories, "non-edge pixels", and "edge pixels", respectively. Where "x and y" are used, where "x" means the number of secret bits to be included in 'non-edge pixels' and corresponding"y" means the"number of secret bits" to be included in "edge Pixels" are included for these two categories by replacing "k-LSB," where "k" is equal to either "x or y" which is determined by "edge information". Finally, I get a "stego-frame". Figure (3.3) shows an example where (x=2) and (y=4). Assume the “secret message (S=101001111110)".

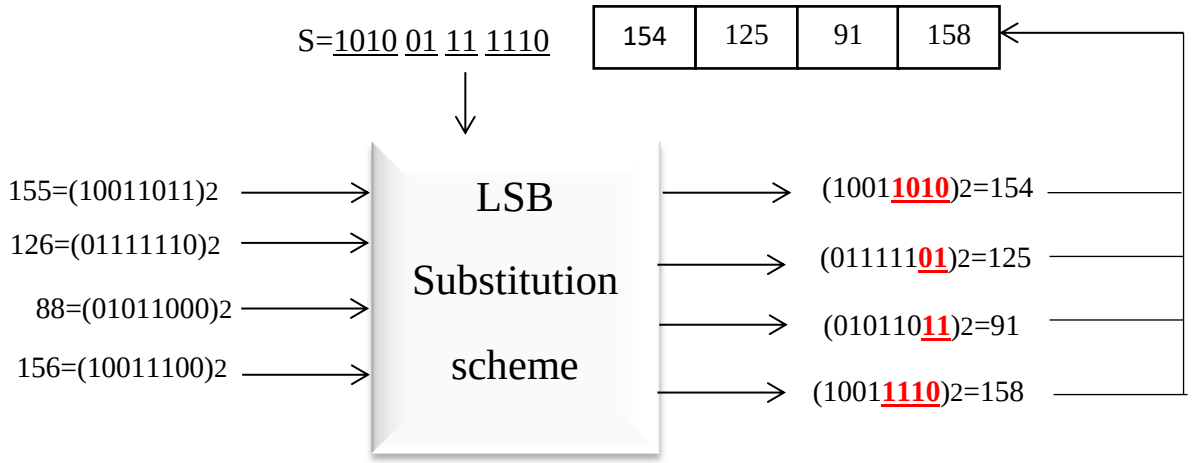


Figure (3.3) Example on the Embedding Process

Algorithm (3.4): demonstration of the embedding process.

Algorithm (3.4): **The Embedding Procedure**

input: I Cover Frame
x "number of bits that can be hidden in one pixel" if it is not an edge.
y "number of bits that can be hidden in one pixel" if it is an edge.
S secret text message

output: Embedded Frame image.

Begin
Step 1. read the cover frame image
Step 2. read the text to be hidden (message).
Step 3. Enter a value (process number) representing the filter selection used for edge detection. We use five types of edge detection filters (Sobel, Prewitt, Kirch, Robert, and Laplacian).
Step 4. Next, the edge reveals the five least significant bits of each pixel according to the specific filter type, i.e. if we enter zero (process number) zero, the edge is detected using the Sobel filter and if we enter 1, the edge is with the Prewitt filter and if 2 Kirch and if 3 Robert 4 If Laplacian.
Step 5. Convert text to bits. Then we compare each pixel in the original image with a pixel that corresponds to it in the Edge Detection image. If the pixel is an edge, the bits will be hidden by the number y, and if the edge is not we hide the number x.

Step 6. Apply the PSNR scale between the original image and the image after hiding to find the similarity between the two pictures according to equation(3.3):

$$MSE = \sum_{i=1}^{M} \sum_{j=1}^{N} \left(I(i,j) - C(i,j)\right)^2 / M * N \text{……/……..(3.2)}$$

$$PSNR = 10\, log10\, (255^{\,2} / MSE) \text{ ……(3.3)}$$

End

Finally, a stego frame is combined with other frames to get the stego video.

3.2.2 Procedure at Receiver Side

A stego video is sent to the receiver side. Algorithm (3.5) describes the general steps that are done by the receiver side.

Algorithm (3.5): General Steps of the receiver side

Input:

- *S_v* // stego video.

Output:

- *Extr_Txt* // Extracted text.

Step1: Splitting the stego video (*S_v*) into a number of frames.

Step2: Extract candidate frame image (*Cframe)* using the algorithm (3.2)

Step3: Extract the embedding text bits from the candidate frames image (*Cframe*) by applying the extraction process.

Step4: Convert the extracted text bits into SACII code to obtain the extracted text *(Extr_Txt*)

End

3.2.2 Extracting Procedure

The embedded frame will go through the clear pixel stage and edge detection stage. at the "extraction phase", the recipient first extracts two "parameters x and y from the pixels of the image". Also, "edge information" is set identical within the embedding phase. Therefore, the key data are extracted exactly. Figure (3.4) shows the extraction process.

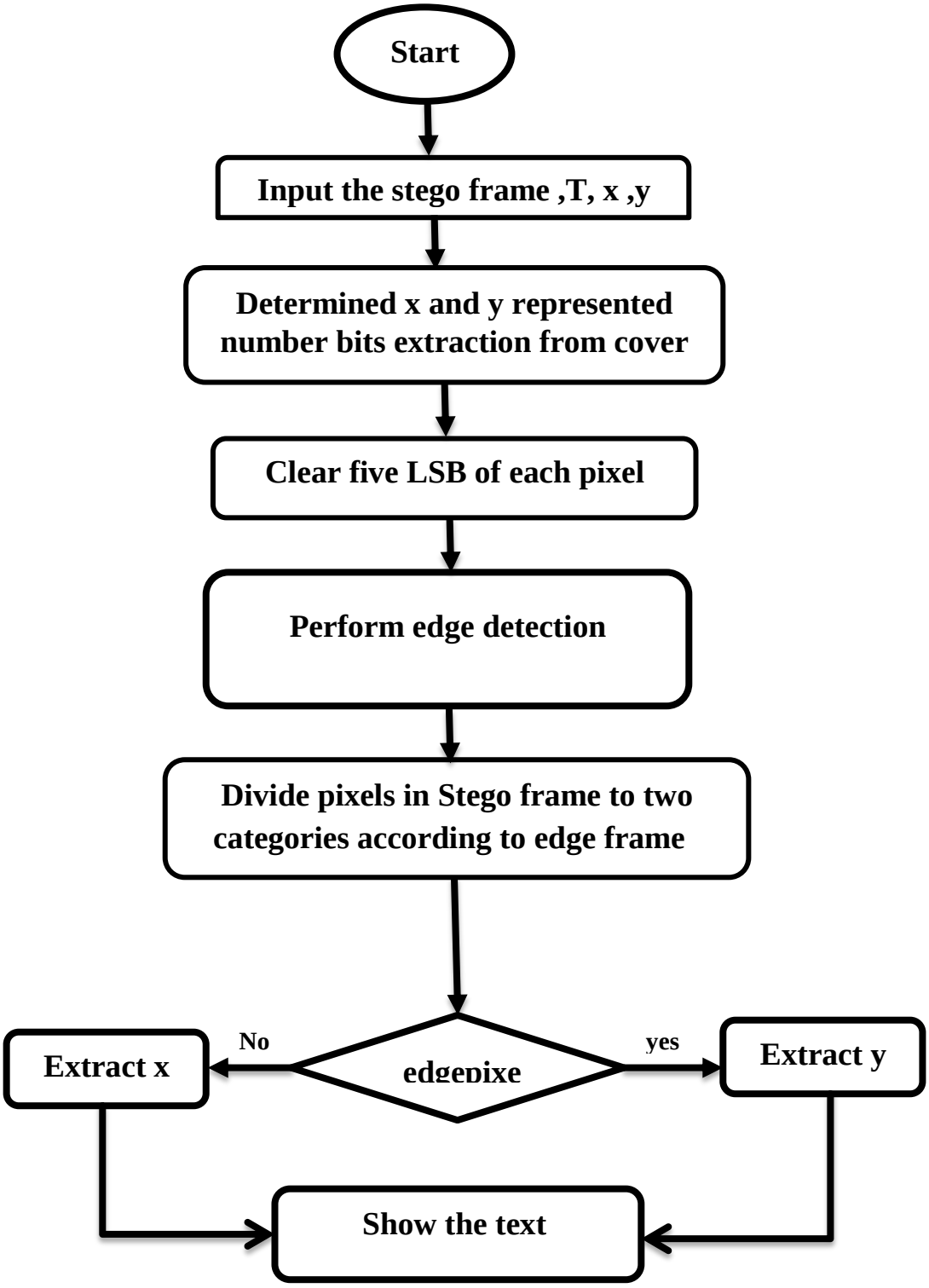


Figure (3.4): The flowchart of the Extraction Phase.

The extraction process is depicted in the algorithm (3.6).

Algorithm (3.6): extraction procedure

Input: EI Embedded Frame Image.

Output: ES Extract The Message.

Begin

Step 1. Enter a value (process number) representing the filter selection used for edge detection. We use five types of edge detection filters (Sobel, Prewitt, Kirch, Robert, and Laplacian)

Step 2. Next, the edge reveals the five least significant bits of each pixel according to the specific filter type, i.e. if we enter zero (process number) zero, the edge is detected using the Sobel filter and if we enter 1, the edge is with the Prewitt filter and if 2 Kirch and if 3 Robert 4 If Laplacian.

Step3. Extract x "secret bits" of "non-edge pixels" while y of "edge pixels".

Step4. Convert the extracted bits into text and save them in the (ES).

Step 5. find similarities between the original text and the extracted text by using NC according to the following equation:

$$\text{Normalized Cross Correlation} = \frac{\sum A*B}{\sqrt{\sum A^2 * \sum B^2}} \ldots\ldots\ldots\ldots (3.4)$$

End

Chapter four

Experimental Work and Discussion of Result

Chapter Four

Experimental Work and Discussion of Results

4.1 Introduction

This chapter introduces a discussion of the experimental work results and comparison with prior works. The proposed system techniques and existing techniques have been simulated using MATLAB programs. The proposed system and existing techniques applied to hide a secret message (text) inside grayscale, and the proposed system is implemented with the following characteristics:

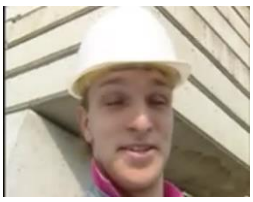
- AMD A8-4500M APU with Radeon (TM) HD Graphics 1.90 GHz
- 4GB RAM
- Microsoft Windows 10 pro
- The proposed system is simulated with the MATLAB R2019a programming language version .

The experimental results were analyzed to clarify the results by some performance metrics discussed in chapter two; these metrics are Quality metrics (PSNR). The results of the secret message also measured before and after embedding by a metric NormalizedCross-Correlation.

4.2 Data Set

The proposed method is tested on the several videos; some of these are standard [https://media.xiph.org/video/derf/]. The tested videos are with format (avi) of different sizes. Table (4.1) shows details of some videos that applied in our system.

Table (4. 1): Some videos used in the experiments

Video Name	First frame	Number of frames	Size of each frame
Standard v108		1206	320*214
Rhinos		114	452*223
foreman		250	320*240
Ali		53	120*90

4.3 Experimental Results Related to the Data Hiding System

The experimental results can be discussed in two views. The first view is related to the candidate frame extraction operation. While the second view related to the video steganography system.

4.3.1 Experimental Results Related to the candidate Frame Extraction

The tests that are done in this stage are related to extract candidate frame for preparing to next stage which is embedding. At first, the candidate frames are extracted based on their edge entropies. Figure (4.1) shows examples of candidate frame (frame

index =31) for standard video (ali.avi), (frame index =168) for standard video (foreman.avi), (frame index =89) for standard video (**Rhinos**.avi).

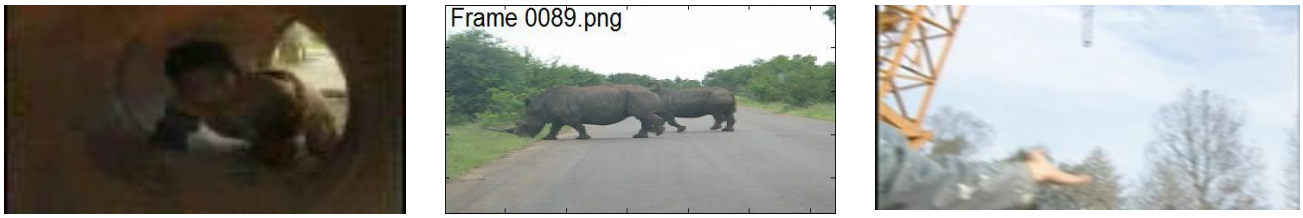


Figure (4. 1): Candidate Frame Extraction

4.3.2 Experimental Results Related to the Video steganography System

This section includes the results of the embedding system that consists of the following steps:

Step 1: Clear First Five Bits (Least Significant Bits)

The frame consists of a set of pixels. Each pixel converted into eight bits. The bits divided into two parts, the first part is the "most significant" and the second part is the "least significant". Usually, the first bit is the" least significant bit" and the last bit is the" most significant bit". At this stage, the first five least significant bits cleared. Where, the first, second, third, fourth, and fifth bits are replaced with a zero value. The remaining sixth, seventh and eighth values remain the same and then convert these bits into a numerical value and put in the same location in the frame.

1. We take a portion of a 3 * 3 frame.

112	**150**	**200**
50	**73**	**255**
0	**210**	**20**

2. Convert each pixel to binary (8-bit).

Table(4.2): Explain Convert each pixel to binary (8-bit).

eighth bit	seventh bit	sixth bit	fifth bit	fourth bit	Third bit	Second bit	First bit	Value
0	1	1	1	0	0	0	0	112
1	0	0	1	0	1	1	0	150
1	1	0	0	1	0	0	0	200
0	0	1	1	0	0	1	0	50
0	1	0	0	1	0	0	1	73
1	1	1	1	1	1	1	1	255
0	0	0	0	0	0	0	0	0
1	1	0	1	0	0	1	0	210
0	0	0	1	0	1	0	0	20

3. Clear the Five bits (the bit whose value is zero remains zero. The bit whose value is one becomes zero).

Table (4.3):Explain Clear the Five bits

eighth bit	seventh bit	sixth bit	fifth bit	fourth bit	Third bit	Second bit	First bit	Value
0	1	1	0	0	0	0	0	112
1	0	0	0	0	0	0	0	150
1	1	0	0	0	0	0	0	200
0	0	1	0	0	0	0	0	50
0	1	0	0	0	0	0	0	73
1	1	1	0	0	0	0	0	255
0	0	0	0	0	0	0	0	0
1	1	0	0	0	0	0	0	210
0	0	0	0	0	0	0	0	20

4. Convert bits to numeric value.

Table (4.4) : Convert bits to numeric value		
96	128	192
32	**64**	**224**
0	**192**	**0**

Figure (4.2) shows the original frames and the frames after clear five bits.




Figure (4.2): Left frame is the origin and right frame after cleared five bits.

Step2: The Edge Detection

In this stage, the edge detects the three most significant bits from the previous step. The reason behind this is because these bits contain the most important frame image information by which it is determined whether this pixel is an edge. Detect using five filters (Sobel, Prewitt, Kirch, Robert, and Laplacian).

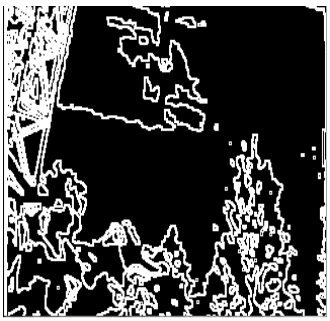
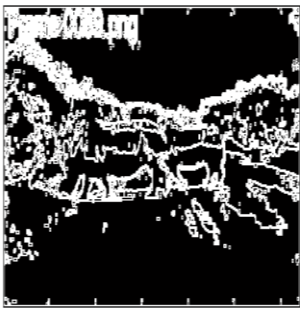
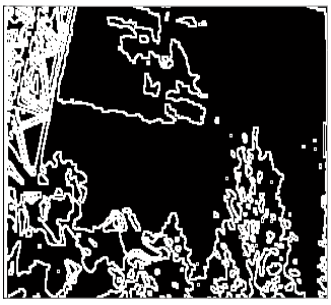
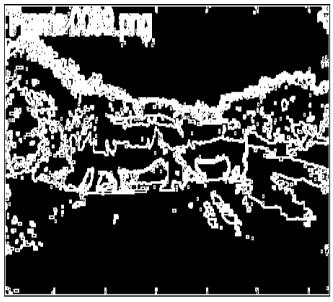
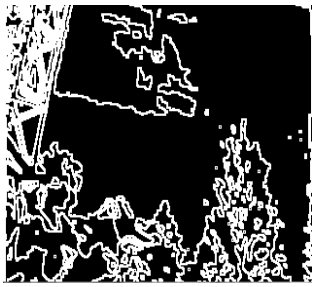
(Sobel, Prewitt) for each of these filters, there are special values with a filter size of 3 * 3 and some with a size of 2 *2 (Robert). Some of them consist of two filters, one towards the x-axis and the other towards the y-axis, as shown in chapter two. Both filters applied to the image after taking a 3 * 3 window. Then the gradient magnitude is applied.

Krich filter consists of eight filters each of 3 * 3 size applied to the frame and then took the largest value to compensate in the center of the frame.

As for the Laplacian, it consists of one filter applied directly to the frame, and the result placed in the center of the frame.

Figure (4.3) shows the original frame and the edge detection of the frame after scanning the five least important bits. The filters used were applied and the number of edges was calculated for each frame. There are clear differences between the edge detection filters, some of which show the smallest details in the frame as an edge, and some of them are limited to the clear objects in the frame. The greater the number of edges in the frame, the better the more data is included in the frame.

Edge detection	I_{org}			
	$I_{clear\ 5bit}$			

Sobel	Edge frame of I_{clear}	 Edge count=2372	 Edge count=18164	 Edge count=24879
Prewitt	Edge frame of I_{clear}	 Edge count=2371	 Edge count=18164	 Edge count=24899
Kirch	Edge frame of I_{clear}	 Edge count=2406	 Edge count=2406	 Edge count=25498

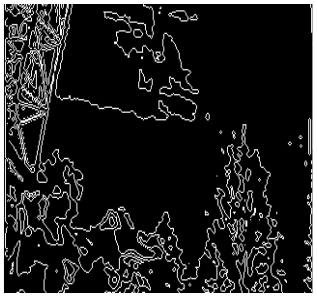
Robert	Edge frame of I_{clear}	 Edge count= 1517	 Edge count=10446	 Edge count=16303
Laplacian	Edge frame of I_{clear}	 Edge count=911	 Edge count= 6654	 Edge count=9462

Figure (4.3): The number of edge pixels detected by Sobel, Prwitt, Krich,Robert,Laplacian

4.3.3 Hidden Data

In this section, the mechanism for" embedding data" within the "cover frame" are explained within the following steps.

1. The "cover frame" and hidden text are read. For example, a secret message (*A word is enough to the wise*) will be hidden in grayscale frame (frame index =31) for standard video (ali.avi)

Cover frame	The text to be hidden
	***A word is enough to the wise***

Figure (4.4): "cover frame" and hidden text are read

2.After reading the frame, the cover and text to hide, the text converted from letters to a numerical value. Then convert it to bits. Converts each letter to 7 bits in English and 8 bits in Arabic. The proposed system receives Arabic and English texts.

Table (4.5) :convert each letter to numerical value in text English.

Text with characters	Text with value
A word is enough to the wise	**65 32 119 111 114 100 32 105 115 32 101 110 111 117 103 104 32 116 111 32 116 104 101 32 119 105 115 101**
كلمة تكفي للحكماء	**1603 1604 1605 1577 32 1578 1603 1601 1610 32 1604 1604 1581 1603 1605 1575 1569**

Table (4.6) :convert numerical value to bit.

Text with characters	Text with value
65	**1 0 0 0 0 0 1**
32	**0 1 0 0 0 0 0**
119	**1 1 1 0 1 1 1**
111	**1 1 0 1 1 1 1**

1. The first five bits of each pixel in the frame cleared, then the edge detected in one of the ways we touched on it.

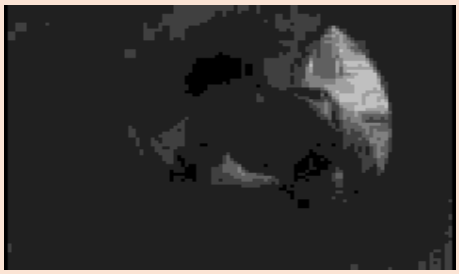
frame cover	**Detection by Sobel Threshold =129**
	

Figure (4.5): After scanning five bits, the edge is detected by one of the suggested methods

2. After revealing the edge of the cover frame, the text inside the frame hidden depending on the edge values. If "pixel value" in "edge frame " is 255, four bits of text will be hidden in the corresponding pixel in an "original frame ". If the "pixel value" in the "edge detection frame " is zero, two bits of text hidden in the original frame.

We take a portion of the frame and apply to it what mentioned, where every pixel is converted to bits in case of hidden.

Origin frame	Detection frame	Text in binary
11 160 11 11 130 11 11 12 15 14 130 15 190 17 14 17	0 255 0 0 255 0 0 0 0 0 255 0 255 0 0 0	65: 1 0 0 0 0 0 1 32: 0 1 0 0 0 0 0 119: 1 1 1 0 1 1 1

Table(4.7): Blue represents an edge, and orange is a non-edge

eighth bit	seventh bit	sixth bit	fifth bit	fourth bit	Third bit	Second bit	First bit	Value
0	0	0	0	1	0	1	1	11
1	0	1	0	0	0	0	0	160
0	0	0	0	1	0	1	1	11
0	0	0	0	1	0	1	1	11
1	0	0	0	0	0	1	0	130
0	0	0	0	1	0	1	1	11
0	0	0	0	1	0	1	1	11
0	0	0	0	1	1	0	0	12
0	0	0	0	1	1	1	1	15

Here the pixel bits are replaced by the text bits.

Table(4.8): Pixel Bits are replaced by the text bits.

eighth bit	seventh bit	sixth bit	fifth bit	fourth bit	Third bit	Second bit	First bit	Value
0	0	0	0	1	0	0	1	11
1	0	1	0	0	0	0	0	160
0	0	0	0	1	0	0	1	11
0	0	0	0	1	0	0	0	11
1	0	0	0	0	1	0	0	130
0	0	0	0	1	0	1	1	11
0	0	0	0	1	0	0	1	11
0	0	0	0	1	1	1	1	12
0	0	0	0	1	1	1	1	15

Table (4.9): convert Pixel Bits are replaced by the text bits to numeric value.			
9	160	9	8
132	**11**	**9**	**15**
15	**14**	**130**	**15**

The PSNR scale is calculated to measure the variation between the" original frame "and the frame after hiding as shown in Figure (4.4) using different edge detector methods.

Filters	**Origin image**	**Stego image**	**PSNR**
Sobel			**69.308**
Prewitt			**69.308**
Kirch			**69.308**
Robert			**63.420**

Laplacian			**69.308**

(a) "original image" **(b) "stego image"**

Figure (4.6): steganography of the proposed method (a) "original frame" **(b)" stego** frame"

Another example: If the texts are Arabic: "كلمة تكفي للحكماء". Figure (4.5) shows the original and stego frames.

Filters	**Origin frame**	**Stego frame**	**PSNR**
Sobel			**68.4558**
Prewitt			**68.4558**
Kirch			**68.4558**

Robert			**62.8014**
Laplacian			**68.4558**

(a) original frame **(b) stego** frame

Figure (4.7): steganography of the proposed method (a) original frame **(b) stego** frame

Another example of the proposed method is applied to (frame index =31) for standard video (ali.avi), in which the English text, "Iraq is a country of civilizations and glories" is included. The PSNR scale found to measure the similarity between the frames before and after the inclusion, as well as the NC scale, which measures the percentage of similarity between the original and the text after extraction as shown in Table (4.10) and Table (4.11) shows the scales results for the Arabic text "العراق بلد الحضارات والامجاد".

Table (4.10): Experimental results of the proposed scheme using various values of x and y on (frame index =31) for standard video (ali.avi)

Edge detection Schemes		Sobel		Prewitt		Krich		Robert		Laplacian	
x	**y**	**PSNR**	**NC**	**PSNR**	**NC**	**PSNR**	**NC**	**PSNR**	**NC**	**PSNR**	**NC**
1	**2**	70.414	1	70.414	1	70.482	1	70.089	1	70.741	1
1	**3**	67.529	1	67.529	1	67.731	1	67.623	1	68.892	1
1	**4**	62.464	1	62.464	1	62.100	1	58.850	1	64.531	1
2	**3**	66.786	1	66.786	1	66.786	1	65.042	1	66.586	1
2	**4**	66.211	1	66.211	1	66.211	1	62.332	1	66.586	1
3	**4**	62.350	1	62.350	1	62.350	1	60.121	1	62.350	1

Table(4.11): Experimental results of the proposed scheme using various values of x and y on (frame index =31) of standard video (ali.avi)

Edge detection Schemes		Sobel		Prewitt		Krich		Robert		Laplacian	
x	**y**	**PSNR**	**NC**	**PSNR**	**NC**	**PSNR**	**NC**	**PSNR**	**NC**	**PSNR**	**NC**
1	**2**	70.741	1	70.741	1	70.528	1	69.885	1	71.148	1
1	**3**	66.915	1	66.915	1	66.835	1	67.058	1	67.058	1
1	**4**	61.339	1	61.339	1	61.056	1	60.591	1	62.215	1
2	**3**	66.011	1	66.011	1	66.011	1	66.324	1	66.315	1
2	**4**	65.954	1	65.954	1	65.954	1	62.618	1	66.315	1
3	**4**	61.278	1	61.278	1	61.278	1	59.911	1	61.278	1

4.3.4 Extract Confidential Data

A frame taken after hiding and passed through the previous slices explained in hiding were the first five bits detected. Edge detection is applied for remaining bits. Where is compared if the pixel in the frame after masking is offset by a value of 255, we extract four bits from the frame and if it corresponds to 0 it extracts two bits from the frame.

Table(4.12):frame after hiding and detection frame

frame after hiding				Detection frame			
9	**160**	**9**	**8**	0	255	0	0
132	**11**	**9**	**15**	255	0	0	0
15	**14**	**130**	**15**	0	0	255	0
190	**17**	**14**	**17**	255	0	0	0

1. **Convert pixel to binary:**

Table(4.13): Convert pixel to binary

eighth bit	seventh bit	sixth bit	fifth bit	fourth bit	Third bit	Second bit	First bit	Value
0	**0**	**0**	**0**	**1**	**0**	**0**	**1**	**11**
1	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**160**
0	**0**	**0**	**0**	**1**	**0**	**0**	**1**	**11**
0	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**11**
0	**1**	**1**	**0**	**0**	**1**	**0**	**0**	**130**
0	**0**	**0**	**0**	**1**	**0**	**1**	**1**	**11**
0	**0**	**0**	**0**	**1**	**0**	**0**	**1**	**11**
0	**0**	**0**	**0**	**1**	**1**	**1**	**1**	**12**
0	**0**	**0**	**0**	**1**	**1**	**1**	**1**	**15**

Extract the secret message.

Text in binary	**Text in numeric**	**Text in character**
1 0 0 0 0 0 1	**65**	**A**
0 1 0 0 0 0 0	**32**	**Space**
1 1 1 0 1 1 1	**119**	**W**

The NC scale value is calculated which Measure the similarities between the original and extracted text as shown in Figure (4.8).

Stego frame	**text**	**NC**
	**A *word is enough to the wise***	**1**

	كلمة تكفي للحكماء	1

(a) stego frame **(b) extract secret message**

Figure (4.8): steganography of the proposed method (a) stego frame (b) extract secret message

Chapter five

Conclusion 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

The conclusions can be listed as follows:

1. The " peak noise signal (PSNR) is shown to be the best indicator of optimization efficiency" in a proposed strategy for hiding process implementation; the greater the PSNR quality, the closer the "stego frame" is to the "original frame."In Chapter 4, a PSNR benchmark score when the English text was hidden was(**69.308)**. As for the Arabic language, it is (**68.4558)**, which is a high percentage that shows high image quality due to the use of the method used in the masking process.
2. One of the suggested ways for edge detection is the "Kirch" approach, This includes criteria and uses "the direction" to discover "the edges" as well as "threshold value". Furthermore, a single frame edge should be identified once only, and "noise should not produce any false edges".
3. A frame that has many objects is preferable to one with few objects. since it can be hidden and yet be seen by the Human Visual System (HVS). Because complicated frames may generate more pixel edges than simple frames, they are more efficient. As the texture of the frame becomes more complicated, the embedding capacity increases.

4. The proposed method for the text embedding process is better in terms of security and robustness, capacity, and imperceptibility, and it provides higher performance and low computational complexity than the regular modulation methods.

5.3 Future Works

The suggestions for future works can be summarized as follows:

1. In the suggested method, encrypt the text before hiding it in a video.
2. The suggested method can be applied to hide an image within a video.
3. Voice within the video can be hidden.

References

References

[1] Sharmila K. Wagh, Gaurav Upadhyay, Usha Bakan, Nikita Shinde, Shivani Nimbalkar, “Cryptography and Steganography Techniques in Video”. International Journal of Recent Technology and Engineering (IJRTE), ISSN: 2277-3878, Volume-9, Issue-2, July 2020.

[2] N. koduri, "Information security through image steganography using least significant bit algorithm," MSc. Thesis, Information Security and Computer Forensics University of East London, 2011.

[3] Ashty M. Aaref,” Video Steganography Using LSB Substitution and Sobel Edge Detection”, Diyala Journal of Engineering Sciences, Vol. 11, No. 2, June 2018, pages 67-73.

[4] O. N. Kadhim, "A Chaos-Based Steganographic Approach for Information Hiding," Master, Faculty of Computer Science and Mathematics / University of Kufa, 2018.

[5] Banik, B. G., Poddar, M. K., & Bandyopadhyay, S. K. "Image Steganography Using Edge Detection by Kirsch Operator and Flexible Replacement Technique". In Emerging Technologies in Data Mining and Information Security, Springer, Singapore, pp. 175-187,2019.

[6] Dipika Deshmukha ,Dr.Gajanan Kurundkar b,” Video Steganography using Edge Detection Techniques”, International Conference on Communication and Information Processing (ICCIP-2019),p.p 2-4,2019.

[7] Dipika Deshmukh, Gajanan Kurundkar,”Video Steganography using Sobel Edge Detection Technique”, International Journal of Innovative Technology and Exploring Engineering (IJITEE), pp. 1735-1738 , Volume-9 Issue-5, March 2020.

[8] Ayub, N, & Selwal, A.,"An improved image steganography technique using edge-based data hiding in DCT domain". Journal of Interdisciplinary Mathematics, vol. 23, no.(2), pp.357-366, 2020.

References

[9] Prasad, S., & Pal, A. K."Stego-key-based image steganography scheme using edge detector and modulus function". International Journal of Computational Vision and Robotics, vol. 10,No.(3), pp. 223-24, 2020.

[10] M. Jafar, K. Morteza, An adaptive scheme for compressed video steganography using temporal and spatial features of the video signal, International Journal of Imaging System and Technology,19, December 2009,306-315.

[11] M.M. Sadek, A.S. Khalifa, G. M. Mostafa, Video Steganography: A Comprehensive Review, Multimedia Tools Applications, 74, March 2014, 7063-7094.

[12] Bharti Chandel1 , Dr.Shaily Jain2," Video Steganography: A Survey", IOSR Journal of Computer Engineering (IOSR-JCE), , Volume 18, Issue 1 (Jan – Feb. 2016), PP 11-17.

[13] G. Liang, S. Wang, and X. Zhang. "Steganography in the binary image by checking data-carrying eligibility of boundary pixels". Journal of Shanghai University, vol. 11, no. 3, pp. 272-277, 2007.

[14] Morkel, Tayana, Jan HP Eloff, and Martin S. Olivier. "An overview of image steganography" Conference: Proceedings of the ISSA 2005 New Knowledge Today Conference, 29 June - 1 July 2005.

[15] Fabien A. P. Petitcolas, Ross J. Anderson, et al. "Information Hiding" Proceedings of the IEEE, special issue on the protection of multimedia content", vol.87, no.(7), July 1999.

[16] Naga Ranjith Kumar Kesa, "Steganography A Data Hiding Technique", Master of Science in Information Assurance & St. Cloud State University 12-2018.

[17] Z. Fouroozesh, "Image Steganography based on LSB in Spatial Domain," Master Thesis, Department of Computer Science & Engineering, Qatar University, 2014.

References

[18] P. Goel, "Data Hiding in Digital Images : A Steganographic Paradigm," Master Thesis, Department of Computer Science & Engineering, Indian Institute of Technology–Kharagpur, 2008.

[19] H. Almara'beh, "Steganography Techniques-Data Security Using Audio, Video and Image," International Journal Of Emerging Technology and Computer Science, vol. 6, No. 2, pp. 45-50, 2017.

[20] V. Mahavidyalaya, "Information Hiding Technology- A Watermarking," Advances in Computational Research, vol. 3, No. 3, pp. 37-41, 2011.

[21] Hüseyin Bilal Macit ,Orhan Güngör ,Arif Koyun "A Review And Comparison of Steganography Techniques", Mehmet Akif Ersoy University ,05 January 2019, Antalya, Turkey.

[22] Abhijeet Harihar Khire, Shweta Sanjay Mahadik, Suraj Shivaji Panavkar, "STEGANOGRAPHY", India Department Of Information Technology, 2018.

[23] Utathya Chatterjee, "Image Steganography and Its Application", Msc Computer Science Department College, Dinabandhu Andrews Institute of Technology and Management University Maulana Abul Kalam Ajad University of Technology 28.08.2017.

[24] B.Chitra Devi, N.Thinaharan and M.Vasanthi, "Data Hiding Using Least Significant Bit Steganography in Digital Images ", Statistical Approaches on Multidisciplinary Research,Volume I, Statistical Approaches on Multidisciplinary Research,Volume I, 2017.

[25] Özcan Çataltaş, Kemal Tütüncü Selcuk",Improvement Of Lsb Based Image Steganography". University Faculty of Technology Konya, Turkey,2018.

[26] M. Wu, E. Tang, and B. Lin," Data hiding in digital binary image, Proc". of 2000 IEEE International Conference on Multimedia and Expo, vol. 1, pp. 393-396, 2000.

[27] F. Cayre and B. Macq, Data hiding on 3-d triangle meshes, IEEE Trans. Signal Processing, vol. 51, no. 4, pp. 939-949, 2003.

References

[28] Jessica Fridrich, Miroslav Goljan, and Rui Du. "Reliable detection of LSB steganography in color and grayscale images". Proc. of 2001 ACM workshop on Multimedia and security: new challenges, pp. 27-30, ACM Press, 2001.

[29] Hayat Shahir Al-Dmour, Enhancing Information Hiding and Segmentation for Medical Images using Novel Steganography and Clustering Fusion Techniques, Ph.D. thesis, University of Technology Sydney, 2018.

[30] Hariri, Mehdi, Ronak Karimi, and Masoud Nosrati. "An introduction to steganography methods." World Applied Programming 1.3 (2011): 191-195.

[31] Sujeet Das "Comparison of Various Edge Detection Technique".International Journal of Signal Processing, Image Processing, and Pattern Recognition Vol.9, No.2, 2016.

[32] Deepak Mathur, Dr. Prabhat Mathur "Edge Detection Techniques In Image Processing With Elaborative Approach Towards Canny" Computer Science Department, Lachoo Memorial College Of Science & Technology,2016.

[33] Mrs.Anandhi,Dr.M.S.Josephine,Dr.V.Jeyabalaraja,S.Satthiyaraj,St.Peter‟s "Comparison Of Canny And Sobel Edge In Detection Techniques", University, India Dr.MGR University, India Dr.Velammal Engineering College University College Of Engineering, Panruti,2015.

[34] Ahmed Shihab, "Comparative Study Among Sobel, Prewitt And Canny Edge Detection Operators Used In Image Processing", University of Baghdad College of Nursing, October 2018.

[35] A. K. Saxena "Edge Detection Operators on Digital Image" , Srcem, Banmore(M.P.), India,2013.

[36] Yuanxi Fu. "Automatic License Plate Recognition UsingNeural Network and Signal Processing ", Msc. Thesis, Master of Science in Electrical Engineering, University Of California Riverside, March 2019.

References

[37] Muthukrishnan R. "Edge Detection Techniques For Image Segmentation", International Journal of Computer Science & Information Technology (IJCSIT) Vol 3, No 6, Dec 2011.

[38] S. Bellamkonda and N. P. Gopalan, "Facial Expression Recognition Using Kirsch Edge Detection, LBP and Gabor Wavelets," 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2018, pp. 1457-1461, doi: 10.1109/ICCONS.2018.8662971.

الخلاصة

في وقتنا الحاضراصبح أمن المعلومات محط اهتمام لكثير من الباحثين ومحط اهتمامهم ، حيث يسعون دائماً من اجل إيجاد أفضل الطرق وأكثرها أمانًا لنقل المعلومات الخاصة والمهمة عبر قنوات آمنه للحفاظ عليها من القرصنة والهجمات الشائعة على الإنترنت و في هذا البحث حاولنا تمثيل إحدى طرق حماية البيانات. يركز هذا البحث على حماية البيانات النصية المرسلة من الملاحظة أو التغيير من قبل المهاجمين بتضمينها داخل الفيديو. تتضمن الطريقة المقترحة إخفاء بيانات نصية عربية وإنجليزية ، وكلاهما بنفس الكفاءة. حيث يتم اولا، تتم قراءة الفيديو والبيانات المراد إرسالها ، ثم يتم إخفاءالبيانات النصية في فيديو الغلاف عن خلال استخدام طرق كشف الحافة للبتات الثلاث الاعلى أهمية من عنصر الصورة باستخدا مرشحات الكشف عن الحواف التي يمثلها (Sobel, Robert, Krich, prewitt) ، حيث ان الحافة تعتمد على حد العتبة الذيسوف يتم اختياره من قبل المستخدم ،بعد ذلك يتم اختبار العنصر في الصورة الأصلية فيما اذا كان يمثل نقطة حافة ام لا، فسوف يتم إخفاء أربعة بتات من النص في العنصرواذا كان العنصر لا يمثل نقطة حافة فيتم اخفاء بتين فقط. في هذه الطريقة تكون أكثر أمنية من عملية الاخفاء بكل عناصر الصورة بشكل متسلسل. وصل هذا المشروع إلى أعلى مقياس للPSNR (69.308) من خلال جميع مرشحات الكشف عن الحواف عندما يتم التضمين للنص الإنجليزي وكانت نسبة PSNR التي تم الحصول عليها (68.4558) عند تضمين النص العربي.

Republic of Iraq
Ministry of Higher Education & scientific research
Babylon University
Journal of University of Babylon for Pure and Applied Sciences

جمهورية العراق
وزارة التعليم العالي والبحث العلمي
جامعة بابل
مجلة جامعة بابل للعلوم الصرفة والتطبيقية

العدد: ٣٤١ التاريخ: ٧/تشرين الثاني/٢٠٢١ Receiving Date: 1/10/2021 Acceptance Date: 7/11/2021 No: Date: / /2021

شهادة قبول نشر

الى:

السيدة
ايمان خالد عبيس
جامعة بابل/كلية العلوم للبنات/الحاسبات
iman.hamed.gsci25@student.uobabylon.edu.iq

الأستاذ الدكتور
سهاد احمد علي
جامعة بابل/كلية العلوم للبنات/الحاسبات
suhad_ali2003@yahoo.com

نوع وعنوان النتاج العلمي (Article):

Video steganography algorithm based on edge detection

شكراً على إرسالكم نتاجكم العلمي إلى مجلتنا

مجلة جامعة بابل للعلوم الصرفة والتطبيقية

الرقم المعياري الالكتروني: ٢٣١٢-٨١٣٥ الرقم المعياري الورقي: ١٩٩٢-٠٦٥٢

يسعدنا ابلاغكم بأنه تمت مراجعة نتاجكم العلمي وقبوله للنشر في **العدد ٣ المجلد ٢٩ للعام ٢٠٢١**. نرفق لكم مستندات التعديلات الأساسية المطلوبة والتي يجب تطبيقها على نتاجكم لاستكمال التصويبات قبل النشر. للمضي قدمًا في عملية النشر، يتطلب من جنابكم إرسال التالي:

١. طلب نشر البحث والتعهد: [بملأ الكترونيا مع التواقيع وحسب الاستمارة المرفقة بالبريد الإلكتروني].
٢. نتاجكم العلمي بصيغته النهائية بعد تعديلات المقيمين [يرجى تضمين جميع التعديلات المبينة في الملف المرفق].
٣. ارسال نسخة من وصل رسم نشر البحث [٦٠ الف دينار عراقي].
٤. في الوقت الحالي، نود أيضًا تذكيركم بسياسات حقوق النشر والوصول المفتوح الخاصة بنا، يرجى الاطلاع على:
[https://www.journalofbabylon.com/index.php/JUBPAS/information/authors]
٥. سيتم استكمال الاستلال ببرنامج Turnitin في المجلة على ان لا تتجاوز النسبة ٢٠٪.

بمجرد نقل نتاجكم العلمي إلى عملية النشر، ستبقيكم هيئة التحرير على اطلاع بتقدم مقالتكم في عملية النشر. واذ نهنئكم بقبول هذا النتاج العلمي للنشر، نأمل ان يستمر تواصلكم معنا ورفدكم لمجلتنا بنتاج فكركم المتميز...

تفضلوا بقبول فائق الاحترام والتقدير

الأستاذ الدكتور
علي حسين المرزوكي
رئيس تحرير مجلة جامعة بابل للعلوم الصرفة والتطبيقية
٢٠٢١/ /

ACCEPTED

وزارة التعليم العالي والبحث العلمي

جامعة بابل

كلية العلوم للبنات

قسم علوم الحاسوب

خوارزمية اخفاء في الفيديو بالاعتماد على كشف الحواف

مشروع مقدم الى

مجلس كلية العلوم للبنات في جامعة بابل

وهي جزء من متطلبات الحصول على درجة الدبلوم العالي في

العلوم/ علوم الحاسبات

من قبـل

إيمان خالد عبيس الجبوري

باشـــــــراف

أ. د. سهــاد احمد علي

2021 م

1443 هـ