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

Studying the effecting of embedding the Most Significant Bit (MSB) of secret image in the Least Significant Bit (LSB) of video

A Research

Submitted to the Council of the College of Science for Women, University of Babylon in Partial Fulfillment of the Requirements for the Degree of Bachelors in Science / Computer Science

By

Zahraa Thabit Abbas

supervised By

Prof. Majid Jabbar Jawad (Ph.D.)

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

قال تعالى:

بسم الله الرحمن الرحيم

(يَرْفَعِ اللَّهُ الَّذِينَ آمَنُوا مِنْكُمْ
وَالَّذِينَ أُوتُوا الْعِلْمَ دَرَجَاتٍ
وَاللَّهُ بِمَا تَعْمَلُونَ خَبِيرٌ)

صدق الله العلي العظيم

سورة المجادلة: الآية 11

Supervisors Certification

I certify that this research entitled "**Studying the effecting of embedding the Most Significant Bit (MSB) of secret image in the Least Significant Bit (LSB) of video**" was done by (**Zahraa Thabit**) under my supervision.

Signature:

Name: Prof. Majid Jabbar Jawad (Ph.D.)

Date: / / 2023

Address: University of Babylon- College of Science for Women

The Head of the Department Certification

In view of the available recommendations, I forward the research entitled “**Studying the effecting of embedding the Most Significant Bit (MSB) of secret image in the Least Significant Bit (LSB) of video**” for debate by the examination committee.

Signature:

Name: Dr. Saif M. Khalaf (Ph.D)

Date: / / 2023

Address: University of Babylon/College of Science for Women

الاهـــداء

الحمد لله الذي بنعمته تتم الصالحات بعد مسيرة دامت سنين وحملت في طياتها الكثير من الصعوبات والتعب نقطف جزء من ثمرها و الحمد لله على البلوغ ثم الحمد لله على لذة الإنجاز والتخرج اللهم ليس بجهدي واجتهادي إنما بتوفيقك وكرمك وفضلك علي أقدم نجاحي إلى من كان لهم الفضل في تقدمي و تميزي اساتذتي الأعزاء جميعا ..

والى من أرضعتني الحب والحنان الى رمز المحبة وبلسم الشفاء و النور الذي انار دربي والسراج الذي لا ينطفيء نوره ابدا والتي بذلت جهد السنين من اجل ان اعتلي سلالم النجاح والدتي العزيزة

وإلى القلوب الطاهرة والعزيزة ورياحين حياتي إخوتي الأحبة

وإلى فخري في هذه الحياة إلى من زرع في طموحا صار يدفعني نحو الإمام نحو مستقبل ناجح..

الى من سيضل حبا يحكيه دعائي دائما ...ابي العزيز...

لقد نلتُ ما تمنيته لي فقد اقطفت زرعك الذي انبتة لي اشعر واعلم علم اليقين بأنك امامي وخلفي وواضع يدك بضهري تدفعني الى الامام نحو التقدم والرقي لولاك لما كان لي شئناً ولا وجود فأهدي تخرجي لك.

زهراء

شكر وعرفان

يسرني أن أوجه شكري لكل من نصحني أو أرشدني أو وجهني أو ساهم معي في إعداد هذا البحث بإيصالي للمراجع والمصادر المطلوبة في أي مرحلة من مراحله، وأشكر على وجه الخصوص أستاذي الفاضل البروفسور**(أ.د. ماجد جبار جواد)** على مساندتي وإرشادي بالنصح والتصحيح وعلى اختيار العنوان والموضوع، كما أن شكري موجه لإدارة كلية العلوم قسم الحاسوب على رعايتهم ودعمهم للمجهودات المبذولة من قبل أساتذتنا الكرام في الجامعة لتوفير أفضل بيئة لتدريس علوم الحاسوب في أفضل الأحوال التي تلائم طلبة العلم.

زهراء (2023)

Abstract

Steganography is the science and art of hiding a secret message in a cover media, without any imperceptible changing in the it.

Steganography can be applied in several media such as image, audio, video. This project suggested video steganography method for preserving the confidentiality which is the important requirement in the security field.

Two domains namely spatial and frequency domains can be used in the video steganography for embedding the secret message. In this method, a spatial domain is used for embedding the secret message. The effecting of embedding the Most Significant Bit (MSB) of secret image in the Least Significant Bit (LSB) of frame within video is studied in this project. In this project n bit(s) of MSB of secret image is embedded in n bit(s) LSB of cover frame of video. The experimental results show that the value of PSNR is affected by the number of embedded bit(s). As the number of embedded bit(s) increased, the value of PSNR is decreased and vice versa. The project is implemented with Matlab programming language.

List of Contents

List of Figures

List of Tables

List of Abbreviations

Term	Meaning
LSB	**Least Significant Bit**
MSB	**Most Significant Bit**
HVS	**Human Visual System**
RGB	**Red Green Blue**
OPA	**Optimal Pixel Adjustment**
DCT	**Discrete Cosine Transform**
DWT	**Discrete Wavelet Transform**
PSNR	**Peak signal-to-noise ratio**
MSE	**Mean Square Error**

Chapter one

General Introduction

Chapter One: General Introduction

1.1 Introduction

It is wildly known the internet importance and its impact on everyday life in all the fields of life. Since it provides the speed and ease of communication and information processing, however, this revolution in the internet world came with many challenges is One of the most important challenges in internet security. Since it has a large impact on the privacy, integrity, and accessibility of the internet, therefore, many theoretical and practical approaches to secure communication between the internet application is developed since the invention of the internet. And it is still updated field because of the many challenges arise each time a new solution is given. One of the very important parts of internet security is data encryption. Data encryption is a subfield of information security. Which is concerned about reconstructing the data in a way that only the intended party could access it. The motivation is that the data is hidden from unauthorized parties. Thus, the field of information hiding occurred.

Information hiding general field consists of two subdisciplines, steganography and watermarking. For the first glance, they may seem similar to each other. But steganography is an approach to hide data in other data. For example, they were hiding data (e.g. message, image, audio) in another data form, like hiding a secret message in image. So, if an unauthorized person accesses the image, he/she will not be able to access the secret message. While watermarking has the goal of protecting the intellectual property of the media (e.g. books, images, audio) [1].

1.2 The Existing Working

A big wide variety of schemes were counseled for hiding image in video primarily based totally at the Steganography techniques. Herein some works related to the above procedure.

In 2020, M.Hemalatha, G.Manisha, P.Mounika, SK.Saleemaand ,Mrs. K.L Prasanna [2] This article aims to improve the security of secret data that communicate through video files by hiding the data using the technology cryptography .The input video file is converted into frames , and then the video is encrypted using AES encryption. And choose one of the frames to hide the secret data for secure data communication. Suggested technology After the data is encrypted, the data concealer uses an adaptive embedding algorithm to hide the secret encrypted data in the selected frame. Encryption improve many security aspects , it makes secret information difficult to identify and has no meaning. In the extraction, the secret data is extracted using the relevant key used to select the pixel coefficient, and the encryption key is used to decrypt it to obtain the original data. Finally, using images and data to analyze the performance of the program in terms of encryption and hidden data.

In 2017 , Paramesh.G1, Pavithra.K.V2 , Ranjitha.N3, Swetha.S4 and T.Anushalalitha5 [3] This article discusses a video steganography technique that can provide acceptable security and high computational speed by embedding secret information in video uses LSB technology to embed data in video frames. Prior to this, symmetric XOR operations were used to encrypt confidential information, this way provides two levels of security : Data Hiding and Extraction procedure, With the amount of data that can be embedded in it, this method is more efficient than other methods and shows a PSNR of more than 30 dB.

In 2017,Gat Pooja Rajkumar and Dr V. S. Malemath.[4] This article makes use of the idea of video steganography, wherein information is hidden at the back of video frames. This article gives tiers of safety for the facts : Steganography and cryptography. The data is encrypted using an encryption algorithm, and then the encrypted data is embedded in the video frame. The LSB encoding technique used to embed data. And it is used very commonly , because it can embed a large amounts of data in simply and efficient way.

In 2016, Bharti Chandel , Dr.Shaily Jain [5] , Steganography is a technology for concealed protection and concealment of multimedia information. It can also be said to be the study of invisible communication. Steganography is a mixture of compression, encryption, watermarking and cryptography. Generally Steganography uses images, text, video, and audio to hide confidential information. In this research , video steganography is analyzed . Video steganography involves including secret information in a video to protect it from intruders. In this article, the basic concepts, performance indicators and security of video steganography is analyzed. Various methods are being explored to protect confidential information by using video as cover .

In 2011, Ashawq T. Hashim, Dr.Yossra H. Ali [6] This article contains an AVI hidden information system development. Based on steganography technology to prevent attacker from accessing the secret information. This work use the combination of steganography and cryptography techniques to improve security so that the information can’t be accessed by attackers. In this work, the AVI file is divided into two parts, video and audio. The video is a combination of frames ; each frame is saved as a BMP file image, and several frames that are needed or needed are selected as the cover. The Type-3 Feistel network is the encryption algorithm that used, it is used domestically and used to make exportable use useful, and the variable length key will make it more difficult for attackers to perform cryptanalysis. Two concealment methods are used in this work, the first method is the least significant bit (LSB), and the second method is the Haar wavelet transform (HWT). The proposed hidden information system was tested using standard subjective measurement methods, such as mean square error (MSE) and peak signal-to-noise ratio (PSNR). All measurement results gained as test results show good results for PSNR (over 50 dB) and increase with the number of frames used for coverage

1.3 Problem Statement

The wide and fast development and innovations in the different fields of the technology sector had a high impact on information communications. Maintaining protection throughout knowledge transfers is important in this new age and should be maintained

1.4 Objective of the Project

This project proposes a method for embedding and extracting the secret image in a video based on the steganography and philosophy of cryptography technique for preserving confidentiality.

1.5 Project Layouts

This project is organized as follows:

Chapter Two:

The overall objective of this chapter is to present fundamentals details, and characteristics of all approaches which have been used steganography method, where the chapter starts with a short introduction to image and video steganography, then it explains the methods have been used.

Chapter Three:

This chapter presents the designed steps of the entire project's stages and the description of all algorithms that have been used to implement the project.

Chapter Four:

This chapter displays the implementation results, and a discussion on obtained results.

Chapter Five:

This chapter lists the conclusions after applying the suggested project. Besides, this chapter lists some future works for enhancing the suggested project.

Chapter Two

Theoretical Background

Chapter Two: Theoretical Background

2.1 Introduction

This chapter explains some a theoretical background related to the suggested project such as steganography, cryptography , digital image and digital video.

2.2 Image Definition [7]

A electronic image is made up of a limited components' number, each of which has a clear position and meaning. Those components are named components of the camera, elements of the camera and pixels. The word more widely used to describe the atmosphere of a photographic image is Pixel, which is the photos captured from satellite and regular and portable camera. A pixel can be the shortest image unit in a digital photo that can be managed and handled by co-ordinates, and thus the strength of each pixel was dependent. They're described in a matrix of quite 2-D.

There are several forms of digital images:

1. **Binary Image**: A binary image with 2 meanings, white and black, or '1' and '0', is the simplest form of image. Because every pixel still has one binary digit, the image of binary is related to as a 1 bit / pixel image.

2. **Grayscale Image**: A greyscale image is a one-color images or monochrome images. It consists only brightness details and no colour detail. Intensity levels are then represented by Greyscale data matrix magnitudes. The basic 8-bit / pixel picture helps the picture to represent different brightness (grey) rates (0-255).

3. Indexed Image: An categorized picture contains of a colour map matrix and an array. In a color diagram, the pixel magnitudes in the list are direct indicators. The color map matrix seems to be an m-by-3 array containing floating-point magnitudes within the [0,1] range. The red, green , and blue attributes of a specific color are listed on every section. An indexed image requires pixel magnitudes to be translated directly to color map magnitudes.

4. RGB Image: A color map doesn't utilize the RGB image, and representing an image by 3 intensities of the color variable, including blue, green, and red. The image of RGB utilizing the standard 8-bit monochrome and contains 24 bits/pixel, whereas 8 bits are (red, green and blue) for each color.

2.3 Video Definition

A video is a visible multimedia that mixes a series of Frames to shape a transferring Frame which can be accomplished via way of means of audio information. The explosive boom of video content material over the last decade has caused a completely pressing want to efficaciously control this content material. it captures the video, saves , transmitted and compress diverse virtual with different sorts and quantities [8]. Video processing is a unique case of sign processing in which the video documents or video streams are the enter and output signal Video processing are utilized in televisions, VCRs, DVDs, video codecs, video gamers and different devices. Typically handiest the format and video processing range among TVs from one-of-a-kind manufacturers , for example[9].

2.3.1 AVI File

In general, AVI documents include a couple of streams of various styles of records. Most AVI sequences will use each audio and video streams a well-known package deal to permit its simultaneous playback. A easy variant for an AVI collection makes use of video records and does now no longer require an audio stream. Specialized AVI sequences would possibly consist of a manipulate song or MIDI song as a further records stream. The manipulate song ought to manipulate outside gadgets including an MCI videodisc player. The MIDI song ought to play heritage track for the collection [10].

2.4 Information Security

In the age of knowledge, we are living. We need to keep track of all our lives' facets. In many other words , data is an object that seems to have a meaning like every other commodity, because database knowledge has to be secured from attacks.

2.4.1 Information Security Objectives

The primary goal of information protection is to suggest the approach and objectively examine the characteristics that can aid to transfer data or knowledge without changes across a network. Accessibility, validity, secrecy and honesty are the essential features of content.

1.Obtainability: Ensuring access to and use of information in a timely and effective manner. A loss of functionality is a disturbance of transparency to the usage of software or an information structure. [11].

2.Authentication: On all persons and knowledge itself, this feature occurs. By going into a dialogue, two parties can identify each other. Information supplied through a channel must be verified in terms of origin, originated date, content of the data, duration of sending, etc. Data root verification indirectly offers data confidentiality (for the source has modified when a message is reconfigured) [12].

3.Integrity: It is a certification for information that got by the collector has not been a change or Modified after the send by the sender [13].

4. Confidentiality: seems to be a facility that is utilized by everyone of those allowed to utilize it to retain the content of knowledge. A concept associated with anonymity and confidentiality is confidentiality. There have been various privacy methods, varying from physical security to mathematical formulas that render details unintelligible. [12].

2.4.2 Categorization of information security systems

Information security systems can be classified into two main categories cryptography, information hiding. Also, information hiding classified into watermark and steganography. Figure (2.1) shows the categorization of information security systems [14].

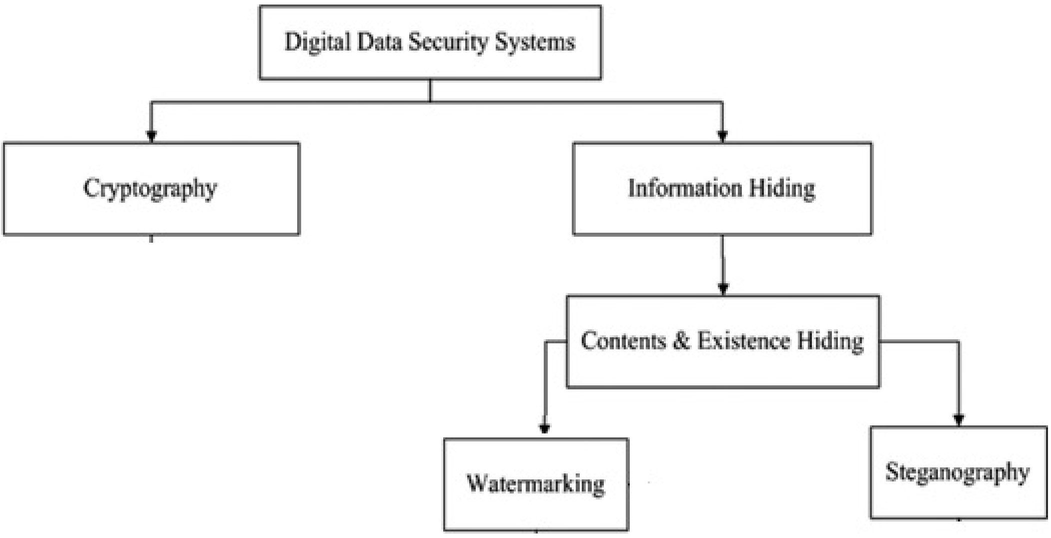


Figure (2.1): Categorization of information security systems

2.4.2.A Cryptography

In order to achieve secrecy of the details, the essential principle of a cryptographic scheme is to encrypt information or data in a manner that an unauthorized user will be unable to extract its significance. 2 of cryptography's more important applications will be to utilize it to transfer data via an unreliable medium, including the telephone, or to guarantee that unauthorized persons may not realize what they are staring at in a situation during that they have obtained the details [15]. Figure (2.2) shows the cryptography concept.

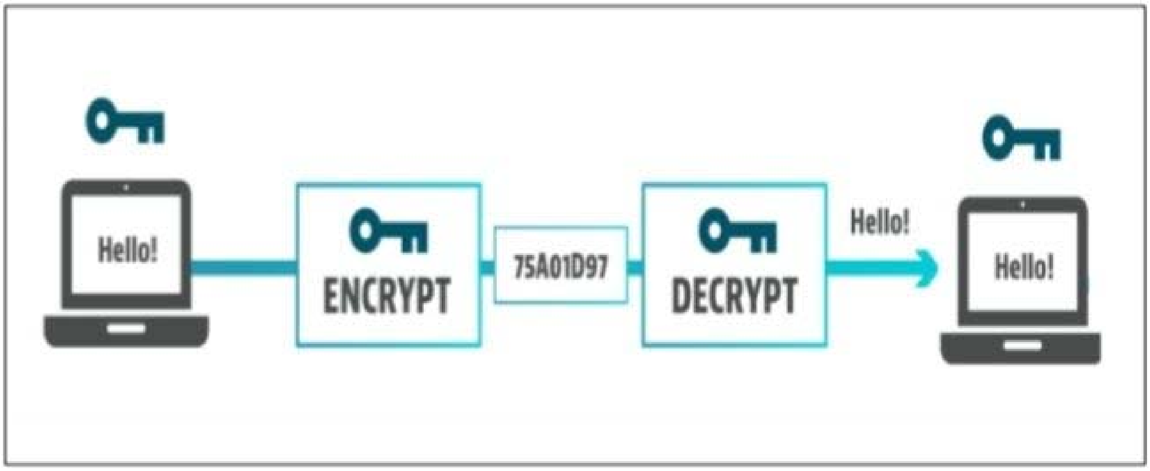


Figure (2.2): Cryptography concept

2.4.2.A.1 Basics Terminology of Cryptography

a- **Text's Plain:** This is the initial decipherable text or knowledge that as data is inserted into the algorithms.

b- **Text's Cypher:** This is the scrambled message generated as a production. The plaintext and the secret key are based on it. Two different keys can generate two different cypher texts for a given message. The cypher text is a randomly data stream and is unintelligible, as it stands c- **Cyphers:** A cypher/algorithm is a transformation that utilizes the original message as input and encodes the message as an output.

d- **Encryption:** The encryption algorithm performs various substitutions and transformations on the plaintext.

e- **Decryption**: Basically this is the encryption algorithm that's work in reverse. This algorithm produces the original plaintext by tacking the cypher text and the secret key.

f- **Key**: The key is an input to the Encryption algorithm. By using a specific secret key at the time, the Encryption algorithm can produce various output. The accurate substitutions and transformations through the algorithm is relay on the key [11].

2.4.2.A.2 Mechanisms of Cryptography

While cryptography in the past referred only to the encryption and decryption of messages using secret keys, today it is described as involving three separate mechanisms.

a-Private/Secret Symmetric Key Cryptography

In this cryptography method, the secret key is known by both the data sender and the receiver. They know the passwords used to encrypt and decrypt the information in advance [16]. Alice and Bob percentage a secret key to encrypt the plaintext. This key can't be detected by any 3rd party. The process is shown in figure (2.3).

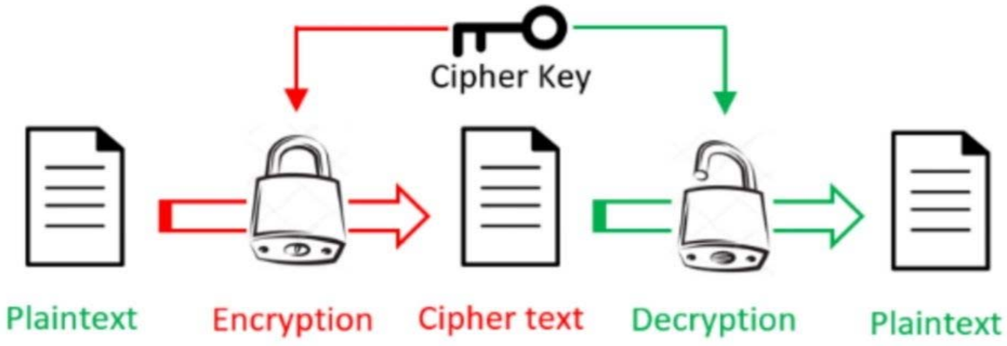


Figure (2.3): Symmetric private-key encryption system

b-Asymmetric/Public Key Cryptography

In this method, two different keys are usually used, as shown in fig.2 to encrypt the information. One of the secret keys is known to the public while the other is kept secret. The public key can be shared out and is the one used in encryption while the secret key is only known and used by the few that have been given to decrypt the information [16]. The process is shown in figure (2.4).

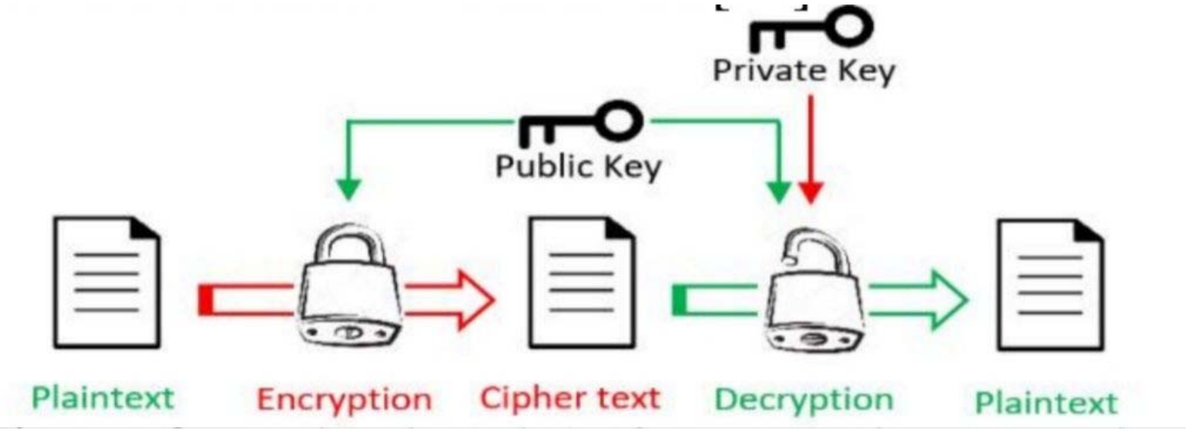


Figure (2.4): Public-key encryption system

c- Hashing

Throughout hashing, a constant-message length digest is created from a changeable-message length. The digest is usually far shorter comparison with the message. When both letter and the digest have to be submitted to Bob to be effective. Hash function is utilized to include control principles that have been previously addressed about the availability of data integrity. [17].

2.4.2.B Watermarking

Water-marking isn’t a original phenomenon. Watermarks on paper have been used for almost a thousand years to denote a specific publisher distinctly and to prevent currency counterfeiting. A watermark is a design imposed on a sheet of paper throughout processing and utilized for copyright recognition. A template, a slogan, or any other illustration may be the template. Proving legitimacy has an extremely significant function in the modern world, when most data and knowledge are collected and exchanged in electronic format. As a consequence, embedded watermark is a mechanism by which subjective knowledge is embedded into a picture in such a manner that an outsider is unaware of it. [18].

2.4.2.C Steganography

Steganography is a technique to protect the hidden message from unidentified users. Steganography includes hiding important information (secret message) inside another medium, i.e. cover data. The Greek terms "steganos" (hidden or covered) and "graphy" (having written or trying to draw) derive in steganography. It explains the traditional art of hiding messages in a hidden way so that the presence of messages is revealed only to the receiver [14]. In steganography, knowledge should never be visible to a spectator ignorant of its existence, and only if the hidden key is identified can modern steganography be observable. Human vision capacity is not good sufficient to see the subtle improvements in the medium's cover. [19].

2.4.2.C.1 Basic Components of Steganography

Figure (2.5) illustrates the basic components of steganography. The components of steganography can be listed as follows:

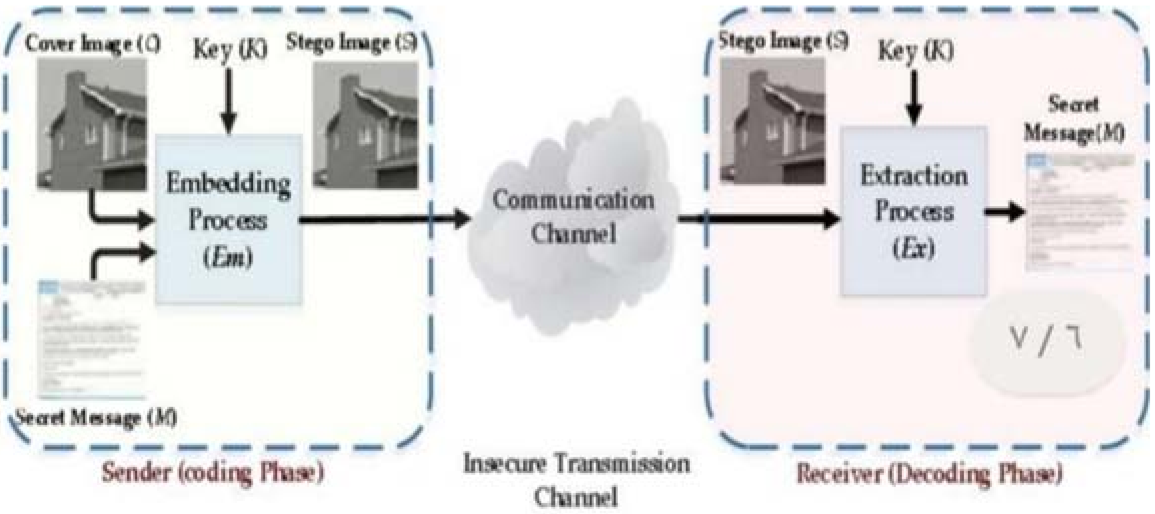


Figure (2.5): **Basic components of steganography**

a- **Cover object (C):** The cover object represents the transporter middle utilized to hidden the secret message (m).

b- **Stego object (S):** The stego object refers to the modified cover object after concealing the secret message.

c- **Message (M):** This refers to the data that needs to be hidden within the cover object without raising suspicion.

d- **Key (K):** The stego key is an optional component used to control the embedding process.

e- **The processing of Embedding (Em):** The producing process a stego object by hidden secret data in the cover object.

f- **The processing of Extraction (Ex):** The retrieving process secret data from the stego object [14].

2.4.2.C.2 Properties of a Steganography Scheme

The principal targets for any steganography calculation are limit, imperceptibility, and vigour even though it is troublesome for a steganography calculation to have every one of the attributes, which may mean that there is by and massive change off among these qualities [20].

a- **Imperceptibility (perceptual transparency):** Imperceptibility or perceptual transparency refers to the quality of the stego carrier. Even though the content of the stego carrier will have some difference to the original one, if this difference is not noticeable by the human visual system (HVS), then We may assume that the imperceptibility condition is satisfied by this steganography algorithm. The main requirement of any steganography technique is imperceptibility.

b- **Capacity (payload):** On the plaintext, the algorithm of encryption executes different replacements and transforms.

c- **Security:** Security is an essential demand for steganography as the steganography method should resist attacks. A steganography scheme is considered secure if the accuracy value of the categorization tool is random guessing.

d- **Robustness (resistance):** Robustness refers to the capability of the stego medium to resist the various type of manipulations. In other words, the embedded secret data is hard for attackers to` remove or modify illegally. Cropping, compression, filtering and noise adding are instances of some attacks that might be utilized to detect or change the secret data.

2.4.2.C.3 Applications of Steganography

Herein some applications of steganography [21]:

1. Steganography is beneficial to transference the secret message from places of source to the destination one.
2. Also Steganography has been utilized for transferring and storing the secret sites information.
3. Steganography could be utilized for protected voting online.
4. Steganography could be utilized for banking privacy.
5. Steganography could be utilized for purposes of military.

2.4.2.C.4 Video Steganographic Techniques [22]

Various video steganographic techniques used today to protect significant information

a) LSB (Least Significant Bit) :

The LSB method is determined best method for the security of data due to : the simplicity , higher embed strength , widely used method. This is simple and effective way to embed data. In the LSB, extract the pixel value of the cover video in bytes, and then replace its LSB with bits of secret message that we will embed. Now we only replace the LSB bit of the cover video, it is not deformed and look as the same as : original video.

b) Non-uniform rectangular partition

This procedure is considered the best way for uncompressed video. In this method , hidden data is accomplished by hiding a uncompressed video file in the cover video. However, we must ensure that the size of the confidential file and the cover file should be approximately the same. Each frame of confidential video and cover video is frames, and image steganography is provided through a certain technology. The secret video hides in the four LSB on leftmost side of the cover video frame.

c) Compressed video steganography

This procedure runs on the compress domains. Information will be embed in blocks of (I) frames with maximum changes, as well as P and B blocks with maximum motion vector size. AVC coding technology provides the greatest compression efficiency.

d) Anti-forensics technique

Anti-forensics technology is a measurement of destruction , hidden and/or manipulation the data in order to attack the forensics computer. Ant-forensic gave protection by denying the unauthorized access ,and it used for criminal side as well. Steganography is a type of anti-forensics, by hiding information in the cover file. Steganography as well as anti-forensics would make the system much secure

e) Masking and filtering

This procedure is applied in 24 (bit/pixel) images, They are suitable for gray-scale ,colored images as well . It is seems as a watermarking in images but with advantage that the image's quality will not be effected. Compared with other steganography technologies, the way that data shielding handles secret messages seems as multimedia file. The Data can't be reveal by Steganalysis.

2.5 Performance Analysis

The disparity between the image of stego and the image's cover could not be distinguished in plain view by humans. So, we need an instrument to calculate the accuracy of the picture of the stego. MSE formulas are utilized to calculate the accuracy of the stego picture in a PSNR. The analysis is achieved by matching a stego picture with the cover image. To determine the formula utilized for MSE (1.1) and to determine the formula utilized for PSNR (2.2), [23].

$$MSE = \sum_{h=1}^{H-1}\sum_{g=1}^{G-1}\|A_f(h,g) - S_f(h,g)\| \qquad (2.1)$$

$$PSNR = 10log_{10}\left(\frac{256-1}{MSE}\right) \qquad (2.2)$$

Chapter Three

The Suggested Project

Chapter Three: The Suggested Project

3.1 Introduction

This chapter illustrates the suggested project. The suggested project is explained using some figures and steps.

3.2 The Suggested Project

Figure (3.1) illustrates the overall block diagram of the suggested project. The suggested project includes two schemes:

- Embedding process
- Extraction process.

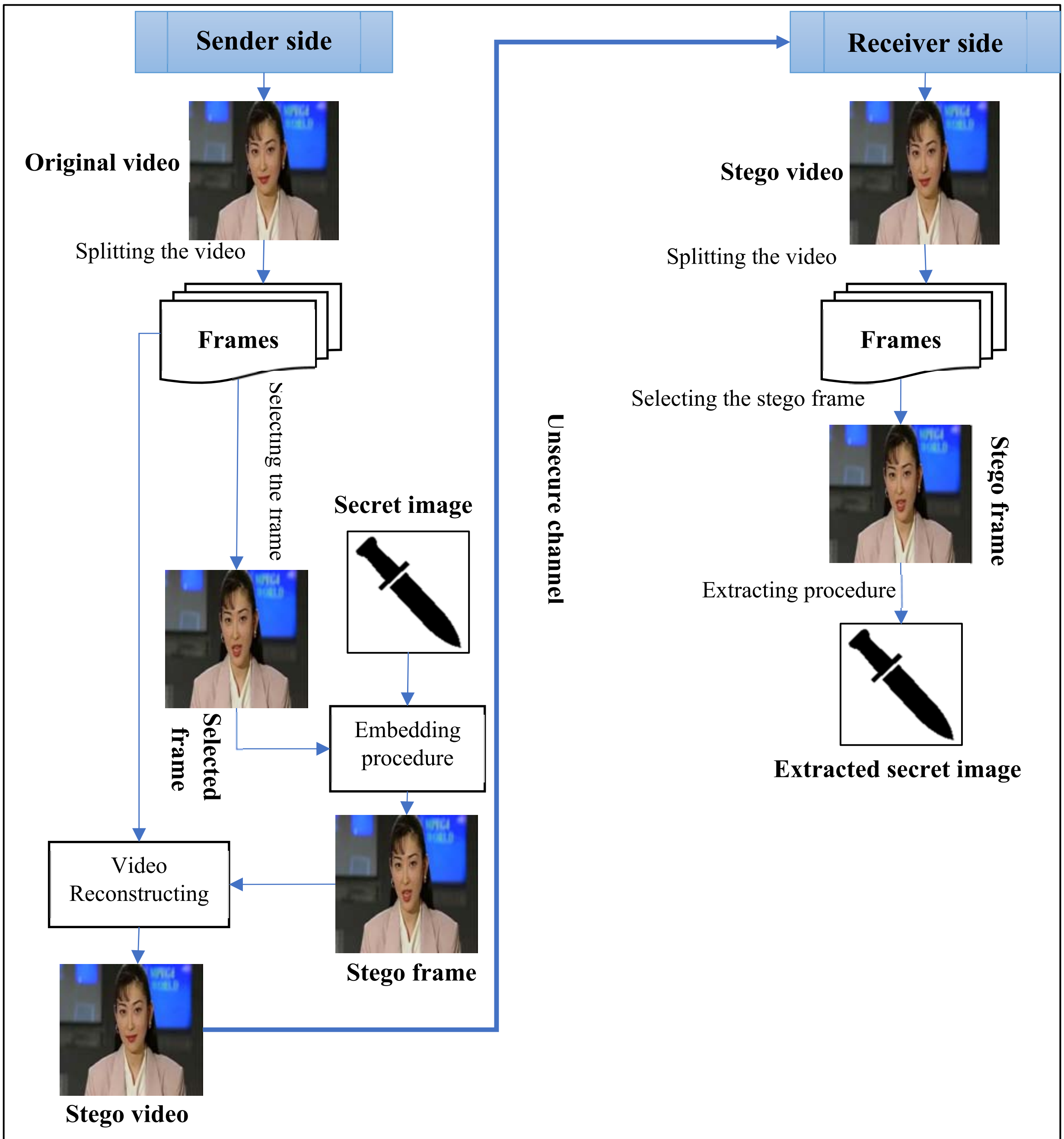


Figure 3.1: General block diagram of the suggested project

The details of the embedding and extraction secret message procedures can be listed as follows:

3.2.1 The Embedding process

Figure (3.2) illustrates the embedding process. In this process, the video is chosen firstly. Then a desired frame is selected in order to be cover for embedding the secret image.

In this process, the secret image is embedded in the selected frame. The selected frame and secret image must have the same size (n*n). The steps of the embedding process illustrated in algorithm (3.1):

Input:

- Video (V).
- Secret image (SI).
- Number of embedded bit(s) (NB).

Output:

- Stego frame (STF)
- Stego video (SV)

```
Step 1: Start.
Step 2: Read V.
Step 3: Read S.
Step 4: Split V into frames and select frame (SF) as cover.
Step 6: For i =1 to n
    Step 7: For j =1 to n
        Step 7: Initialize MN bit(s) of LSB SF's(n,n,) pixel with zero(s)
        Step 8: Shift right the SI's(n,n) pixel by (8- NB).
        Step 9:  Do embedding by adding SF(n,n) and SI(n,n) and getting stego
                 frame (STF(n,n)).
    Step 10: End for
Step 11: End for
Step 12: Combine STF with other frames of V to create stego video SV
Step 13: End
```

In order to understand the method, suppose that we have the following data:

- Pixel with value 129 represented as cover.
- Pixel with value 211 represented as secret message.
- The number of embedded bits is two.

Figure (3.2) illustrates the embedding operation of two last bits from most significant bit of secret in the two first bits of least significant bit of cover.

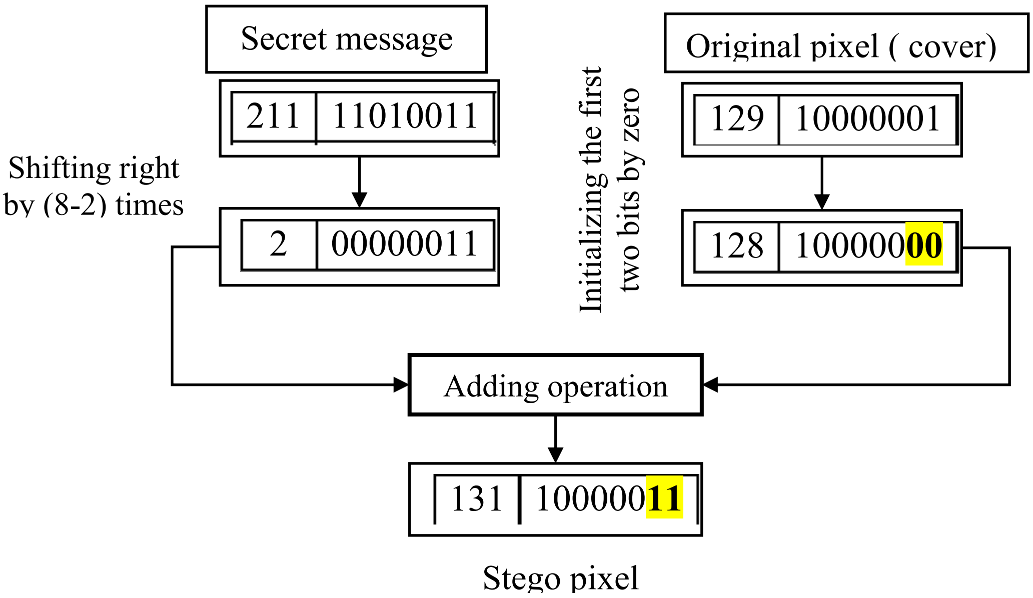


Figure (3.2): Embedding operation

3.2.2 The Extraction process

Figure (3.3) illustrates the extraction process. Extraction process is listed as follows:

Input:

- Stego video (SV).
- Stego frame (STF).

Output:

```
Step 1: Start.
Step 2: Read SV.
Step 4: Split SV into frames and select stego frame (STF).
Step 5: For i =1 to n
    Step 6: For j =1 to n
        Step 8: Shift left the STF's(n,n) pixel by (8- NB) for extracting secret image (ESI(n,n)).
Step 7: Get the ESI.
Step 8: Stop.
```

Chapter Four

Experimental Results

Chapter Four: Experimental Results

4.1 Introduction

In this chapter, the results are discussed implementing the suggested method. some figures and table are displayed for showing the performance of the suggested method.

4.2 Test Material

The suggested project uses two types of materials. The first one is grey image of size (128*128) pixels which represent the secret image. The second one is AVI video of size (128*128) pixels which the cover video. Figures (4.1) and (4.2) represent the secret image and videos covers respectively.

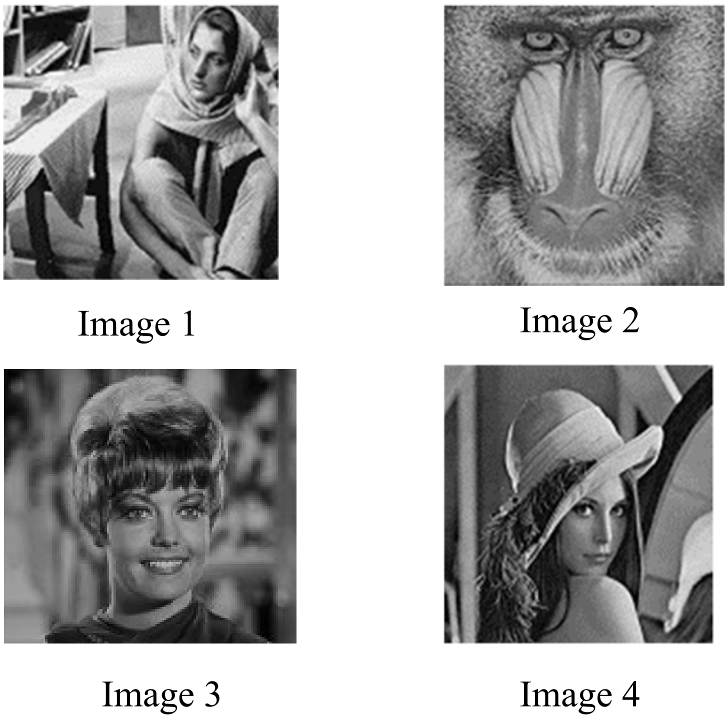


Image 1

Image 2

Image 3

Image 4

Figure (4.1): Secret images

boy

news

Two men

traffic

Figure (4.2): Videos covers

4.3 Experiential Results

This section illustrates the results after implementing the suggested project. Tables (4.1) and (4.2) illustrates some results after implementing the suggested project.

Table (4.1): The results after apply the project)
(secret 1 image and boy video)

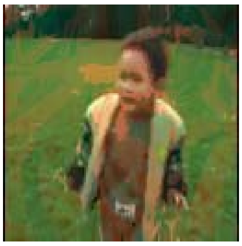
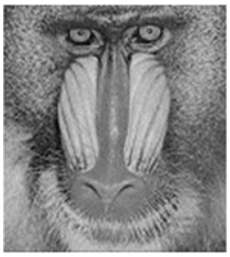
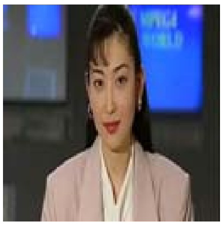
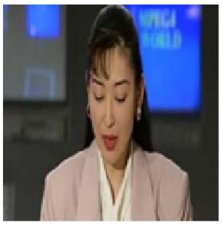
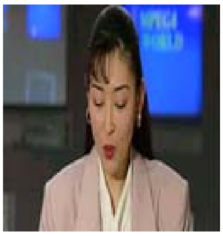
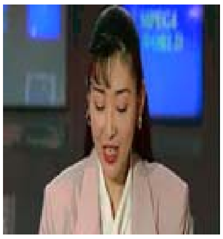
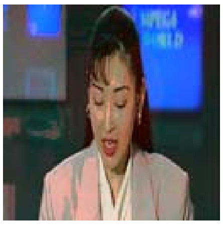
Secret Image	Frame no.	Bit number	Cover frame	Stego frame	PSNR
	1	1			51.1105
	17	3			38.0945
	53	6			20.0149

Table (4.2): The results after apply the project)
(secret 2 image and news video)

Secret Image	Frame no.	Bit number	Cover frame	Stego frame	PSNR
	1	1			51.0343
	50	2			45.8336
	100	4			33.6861
	150	5			27.6619
	250	6			22.5922

4.4 Interfaces of the Suggested Project

This section explains the interfaces of the suggested project after running it.

4.4.1 Starting the Project

Figure (4.3) shows the starting interface after running the project.

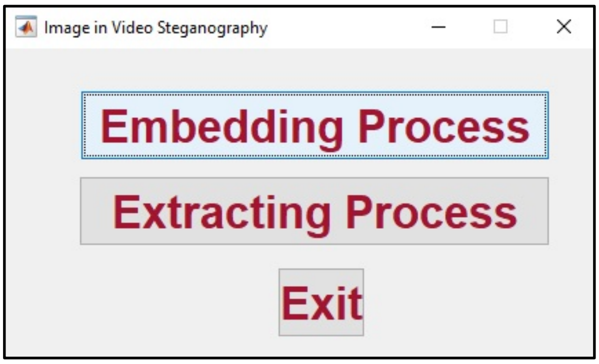
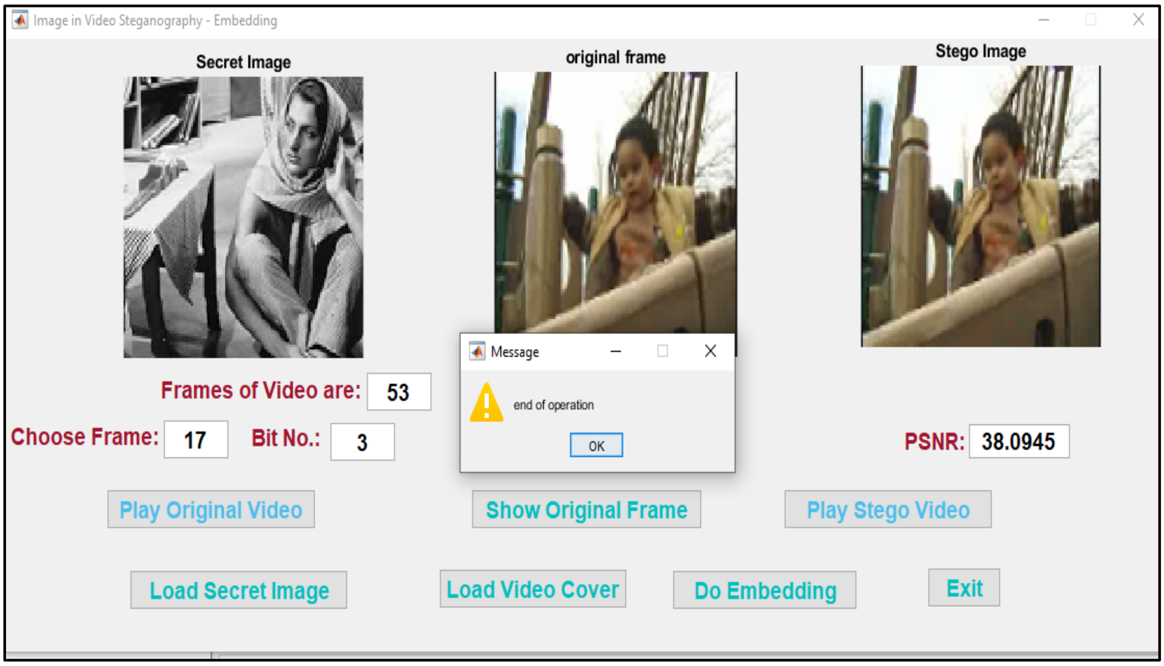


Figure (4.3): The starting of the project

4.4.2 Embedding Procedure.

Figure (4.4) shows the embedding procedure.



Frames of Video are: 53

Choose Frame: 17 Bit No.: 3

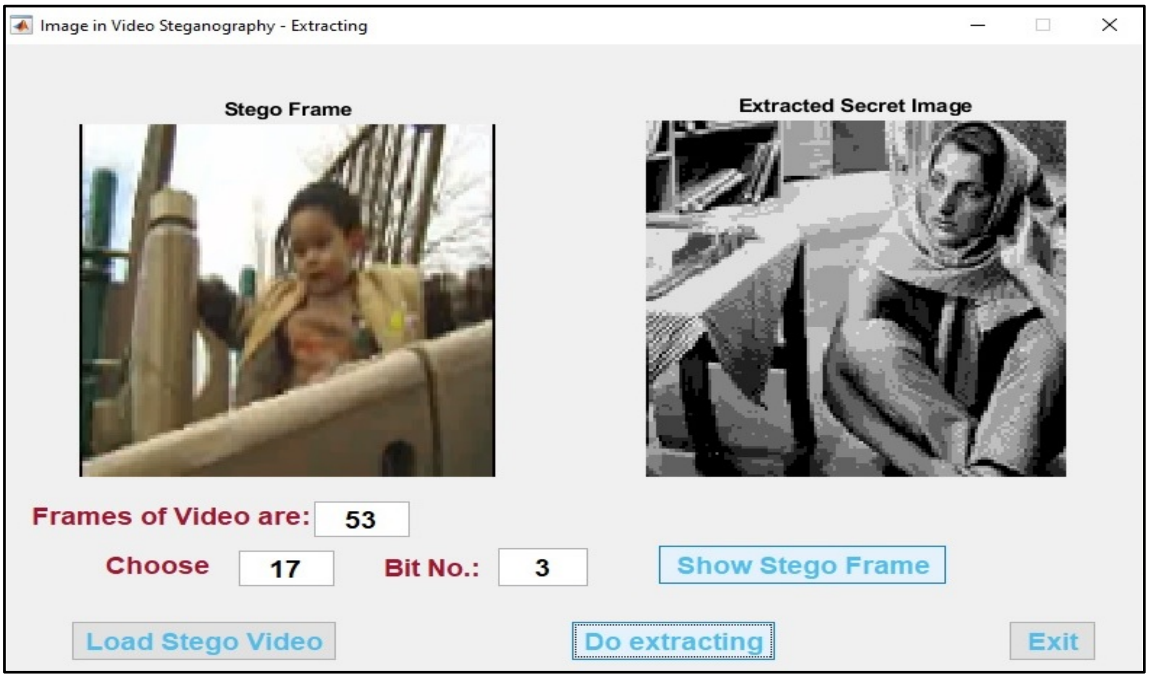
end of operation

PSNR: 38.0945

Figure (4.4): The embedding procedure

4.4.3 Extraction Procedure.

Figure (4.5) shows the embedding procedure.



Frames of Video are: 53

Choose 17

Bit No.: 3

Figure (4.5): The extraction procedure

Chapter Five

Conclusions and Suggestions for Future Works

Chapter Five: Conclusions & Suggestions for Future Works

5.1 Introduction

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

5.2 The Conclusions

The effecting of embedding the Most Significant Bit (MSB) of secret image in the Least Significant Bit (LSB) of frame within video is studied in this project. In this project n bit(s) of MSB of secret image is embedded in n bit(s) LSB of cover frame of video. The experimental results show that the value of PSNR is affected by the number of embedded bit(s). As the number of embedded bit(s) increased, the value of PSNR is decreased and vice versa.

5.3 The Suggestions for Future Works

After applying the suggested project, it is good idea to do the following:

1. Discuss the capability of applying suggested process with sensitive images.
2. Attempt to apply the suggested procedure in the digital watermarking applications.
3. Studying the effect of using the suggested technique in different types of videos such compressed video.

References

References

1. M. Hussain, A. W. Abdul Wahab, and Y. I. Bin Idris, A. T. S. Ho, and K. Jung, “Image steganography in spatial domain: A survey”, Signal Processing: Image Communication, volume (65), p. (46-66), 2018.
2. .M.Hemalatha, G.Manisha, P.Mounika, SK.Saleema and Mrs. K.L Prasanna,” Matlab Code for Video Steganography, 2020
3. Paramesh.G,*, Pavithra.K.V , Ranjitha.N, Swetha.S and T.Anushalalitha,” Video Steganography using MATLAB”,2017.
4. .Gat Pooja Rajkumar and KLE Dr M S Sheshgiri,” Video Steganography: Secure Data Hiding Technique”, 2017.
5. .Bharti Chandel, Dr.Shaily Jain,” Video Steganography: A Survey”, 2016
6. .Ashawq T. Hashim, Dr.Yossra H. Ali && Susan S. Ghazoul, ” Developed Method of Information Hiding in Video AVI File Based on Hybrid Encryption and Steganography”, 5/1/2011
7. http://www.microscopist.co.uk/wpontent/uploads/2017/04/digital-basics.pdf]
8. Manasa K. and Sumohana S. Channappayya, „„,An Optical Flow-Based Full Reference Video Quality Assessment Algorithm,“““ IEEE transactions on image processing, vol. 25, no. 6, june 2016.
9. Wikipedia http://en.wikipedia.org/wiki/Video_processing
10. M. Owens, “A Discussion of Covert Channels and Steganography”,2002.

11. W. Stallings, " Cryptography and Network Security Principles and Practice”, Sixth Edition, book, 2006.

12. M. Ashouri, “ Design of a New Stream Cipher: PALS”, University of Potsdam, Germany , 2018.

13. S. Tayal, N. Gupta, P. Gupta, D. Goyal, and M. Goyal, "A Review paper on Network Security and Cryptography", *Advances in Computational Sciences and Technology*, vol. 10, no. 5, pp. 763-770, 2017.

14. H.S. 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.

15. M. Qadir and N.Varol, “A Review Paper on Cryptography”, 7th International Symposium on digital forensics and security (ISDFS), 2019.

16. S. Kaur, R. K. Bansal and S.Bansal, “Steganography using Spatial Domain Techniques”, International Journal of Recent Technology and Engineering, Volume(8), Issue(4), 2019.

17. H. Dutta, R. K. Das, S. Nandi and S. R. M. Prasanna, “An overview of digital audio steganography”, IETE Tech Rev. https://doi.org/10. 1080/02564602.2019.1699454, 2019.

18. F.Y. Shih, “Digital Watermarking and Steganography: Fundamentals and Techniques”, CRC Press, Boca Raton (2017).

19. R. J. Mstafa, K. M. Elleithy, and E. Abdelfattah, “Video steganography techniques: Taxonomy, challenges, and future

directions", In 2017 IEEE Long Island Systems, Applications and Technology Conference (LISAT) (pp. 1-6). IEEE, 2017.

20. H. Dutta, R. K. Das, S. Nandi, and S. M. Prasanna, "An overview of digital audio steganography", 2019.

21. A. S. Ansari, M. S. Mohammadi, and M. T. Parvez, " A Comparative Study of Recent Steganography Techniques for Multiple Image Formats", International Journal of Computer Network and Information Security, 2019.

22. https://edupediapublications.org/journals/index.php/ijr/article/view/678/309

23. Y. P. Astuti, D. R. I. M. Setiadi, E. H. Rachmawanto and C. A. Sari, "Simple and secure image steganography using LSB and triple XOR operation on MSB", In International Conference on Information and Communications Technology (ICOIACT), Yogyakarta, 2018.

الخلاصة

الستيغانوغرافي هو علم وفن إخفاء رسالة سرية في وسائط الغلاف ، دون أي تغيير غير محسوس فيها.

يمكن تطبيق Steganography في العديد من الوسائط مثل الصورة والصوت والفيديو. اقترح هذا المشروع طريقة إخفاء المعلومات بالفيديو للحفاظ على السرية التي تعد مطلبًا مهمًا في مجال الأمن.

يمكن استخدام مجالين هما المجالات المكانية والترددية في إخفاء المعلومات بالفيديو لتضمين الرسالة السرية.

في هذه الطريقة ، يتم استخدام المجال المكاني لتضمين الرسالة السرية.

تمت دراسة تأثير تضمين الجزء الأكثر أهمية (MSB) من الصورة السرية في الجزء الأقل أهمية (LSB) للإطار داخل الفيديو.

في هذا المشروع ، يتم تضمين n في MSB للصورة السرية في n بت LSB للاطار الموجود داخل الفيديو.

بينت النتائج التجريبية أن قيمة PSNR تتأثر بعدد البت المضمنة.

كلما ازداد عدد البتات المضمنة تنخفض قيمة PSN، والعكس صحيح.

تم تنفيذ يتم تنفيذ المشروع بلغة برمجة الماتلاب

وزارة التعليم العالي والبحث العلمي
جامعة بابل - كلية العلوم للبنات
قسم علوم الحاسوب

دراسة تأثير اخفاء البت الاكثر اهمية للصورة السرية في بيانات البت الاقل اهمية للفيديو

بحث مقدم إلى

كلية العلوم للبنات، جامعة بابل

جزءا من متطلبات نيل درجة البكالوريوس في علوم الحاسوب

مقدمة من قبل
زهراء ثابت عباس

بإشراف
ا.د. ماجد جبار جواد

1444هـ	2023م