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

A Nifty Collaborative (LSB-TXOR) for Secret Video Steganography

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 Diploma in Science / Computer Science

By

Shahad Rafeeq Musa

Supervised By

Prof. Majid Jabbar Jawad (Ph.D.)

2021 A.D. 1442 A.H.

قال تعالى:

بِسۡمِ ٱللَّهِ ٱلرَّحۡمَٰنِ ٱلرَّحِيمِ

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

صدق الله العلي العظيم

سورة المجادلة: الآية11

Supervisors Certification

I certify that this research entitled “**A Nifty Collaborative (LSB-TXOR) for Secret Video Steganography** ” was done by (**Shahad Rafeeq Musa**) under my supervision.

Signature:

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

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 research entitled “**A Nifty Collaborative (LSB-TXOR) for Secret Video Steganography”** for debate by the examination committee.

Signature:

Name: Dr. Farah M. Hassan (PhD)

Date: / / 2021

Address: University of Babylon/College of Science for Women

Certification of the examing committee

We are the member of the examing committee, certify that we have read this project entitled “***A Nifty Collaborative (LSB-TXOR) for Secret Video Steganography***” and after examining the higher diploma student (**Shahad Rafeeq Musa**) in its content in 28/12/2021, and that in our opinion it is accepted as a project for the degree of higher diploma in science\computer science with a degree (excellent).

Committee Chairman:	**Committee Member:**
Signature:	**Signature:**
Name: ***Faez Ali Rashid***	**Name:** ***Samaher Hussein Al-Janabi***
Scientific order: Prof., PhD	**Scientific order: Prof., PhD**
Date: / 1 /2022	**Date: / 1 /2022**

Committee Member (Supervisor):

Signature:

Name: ***Majid Jabbar Jawad***

Scientific order: Prof., PhD

Date: / 1 /2022

Date of Examination: 28\12\2021

Deanship authentication of college of science for women.

Approved for the college committee of grade studies.

Signature:

Name: ***Faez Ali Rashid***

Scientific order: Prof., PhD

Address: Dean of College Science for Women

Date: / 1 /2022

Dedications

To my family especially my great parents…

To my husband and daughter…

To my teachers and friends,

I dedicate this work.

Shahad

Acknowledgments

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

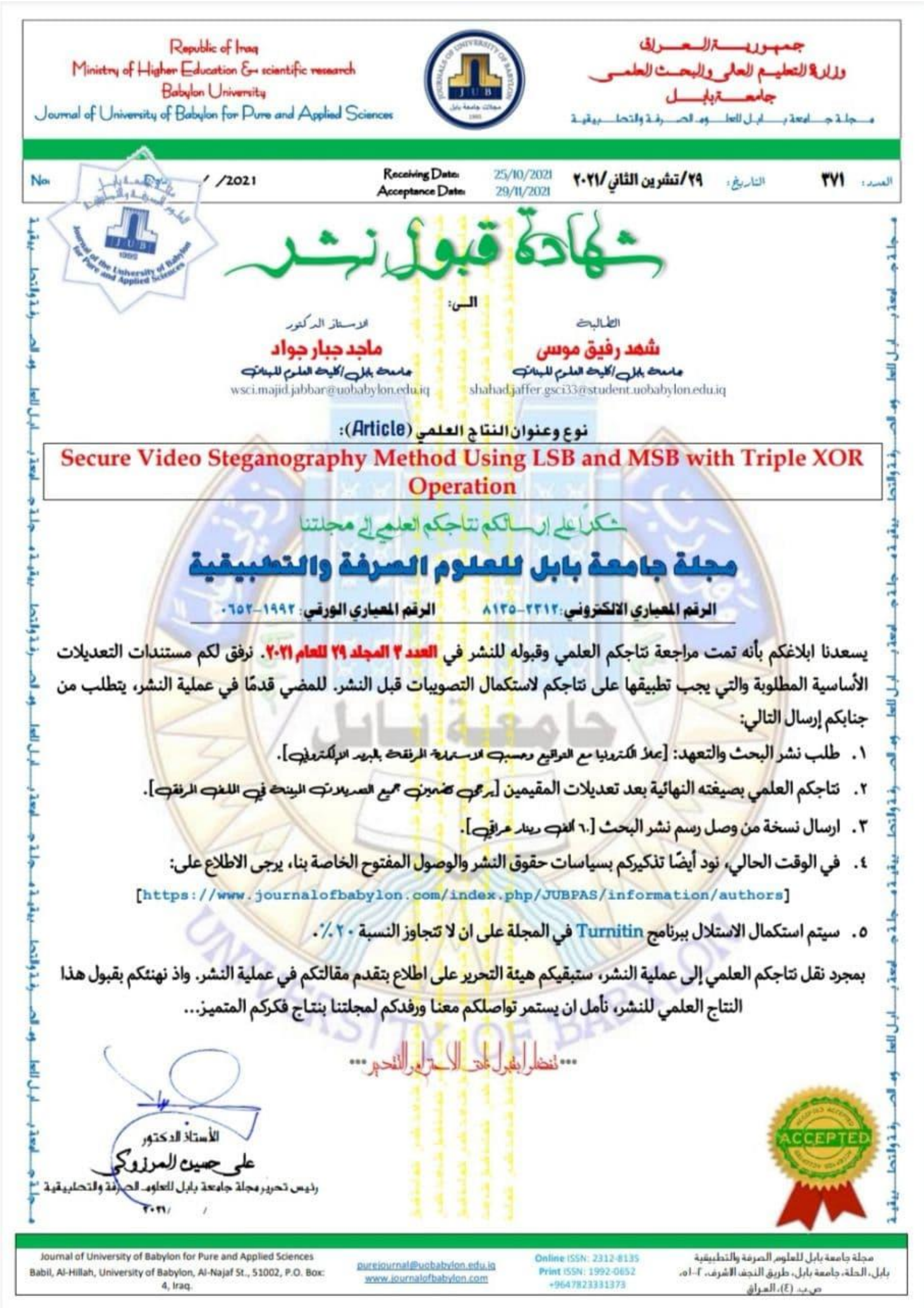
I would like first to express my sincere appreciation to my supervisor **Prof. Majid Jabbar Jawad (Ph.D.)** for his advice, guidance, continues encouragement, and his generous dedication of precious time through the work of this project.

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

All Thanks and Gratitude to all my family for their support and encouragement.

I would like to thank my friends for helping me.

Shahad (2021)



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

No: / /2021 Receiving Date: 25/10/2021 Acceptance Date: 29/11/2021 التاريخ: ٢٩/تشرين الثاني/٢٠٢١ العدد: ٣٧١

Journal of the University of Babylon for Pure and Applied Sciences JUB 1992

شهادة قبول نشر

الى:

الاستاذ الدكتور	الطالبة
ماجد جبار جواد	**شهد رفيق موسى**
جامعة بابل/كلية العلوم للبنات	جامعة بابل/كلية العلوم للبنات
wsci.majid.jabbar@uobabylon.edu.iq	shahad.jaffer.gsci33@student.uobabylon.edu.iq

نوع وعنوان النتاج العلمي (Article):

Secure Video Steganography Method Using LSB and MSB with Triple XOR Operation

شكراً على ارسالكم نتاجكم العلمي الى 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: [يملأ الكترونيا مع التواقيع وحسب الاستمارة المرفقة بالبريد الالكتروني].

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

Abstract

The amount of data and information that transfers through the internet and the ability of unauthorized person to access these information that gave motivation to protect it through information hiding.

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 based on the Least Significant Bit (LSB) is used for embedding the secret message.

In order to satisfying the security requirement, the philosophy of cryptography is used in the suggested method. In this method the XOR operator is used with embedding operation. XOR is used with three keys in order to increase the security layer. In addition, according to the experimental results, the suggested method satisfied the imperceptibility requirement which is very important requirement in the image steganography field.

The experiment results show that the value of all PSNR values (after embedding the secret message in more than cover image) are between 30 and 50dB which mean that the suggested method reduced the distortion that may be occur in the cover after embedding the secret message. The proposed method is efficient then other method from speed of performance and the result of PNSR more than 30 which means all stego frames has less distortion as compare with other methods and increase the layer of security by using TXOR rather than one operation

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 that the internet is important and impact on everyday life. It provides the speed and ease of communication and information processing, however, this revolution in the internet world came with many challenges . One of the most important challenges is 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 are developed 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 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 Problem Statement

The data transfer through internet through unsecure channel and the ability of unauthorized person to get access to these data that gave motivation to hide it.

1.3 Objective of the Project

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

1.4 The existing works

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

1.5 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].

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 [9].

2.4 Information Security

In the age of knowledge, 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. [10].

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) [11].

3.Integrity: It is a certification for information that got by the collector has not been a change or modified after sending by the sender [12].

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. [11].

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 [13].

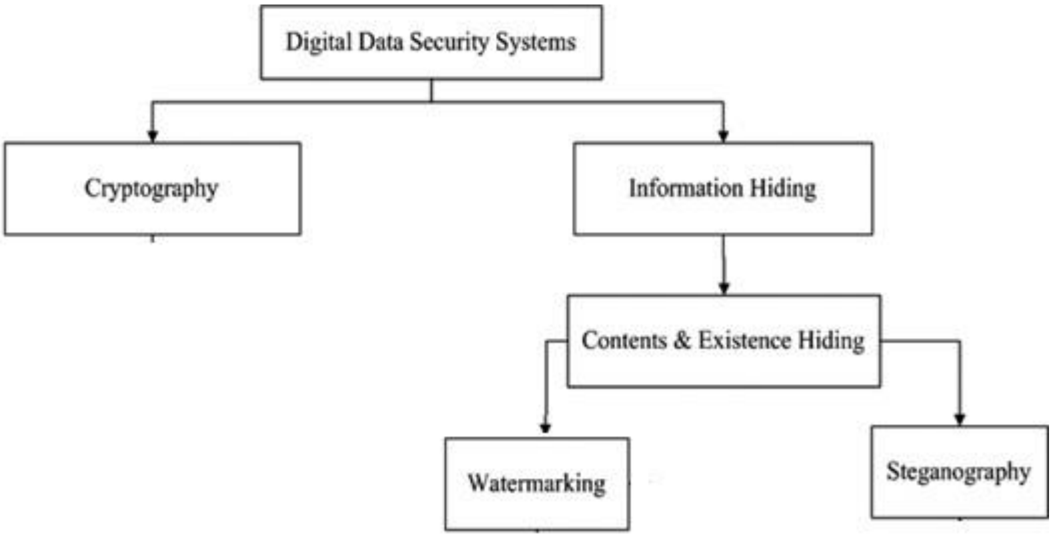


Figure (2.1): Categorization of information security systems

2.4.3 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 [13]. 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. [14].

2.4.3.1 Basic Components of Steganography

Figure (2.2) illustrates the basic components of steganography. The components of steganography can be listed as follows:

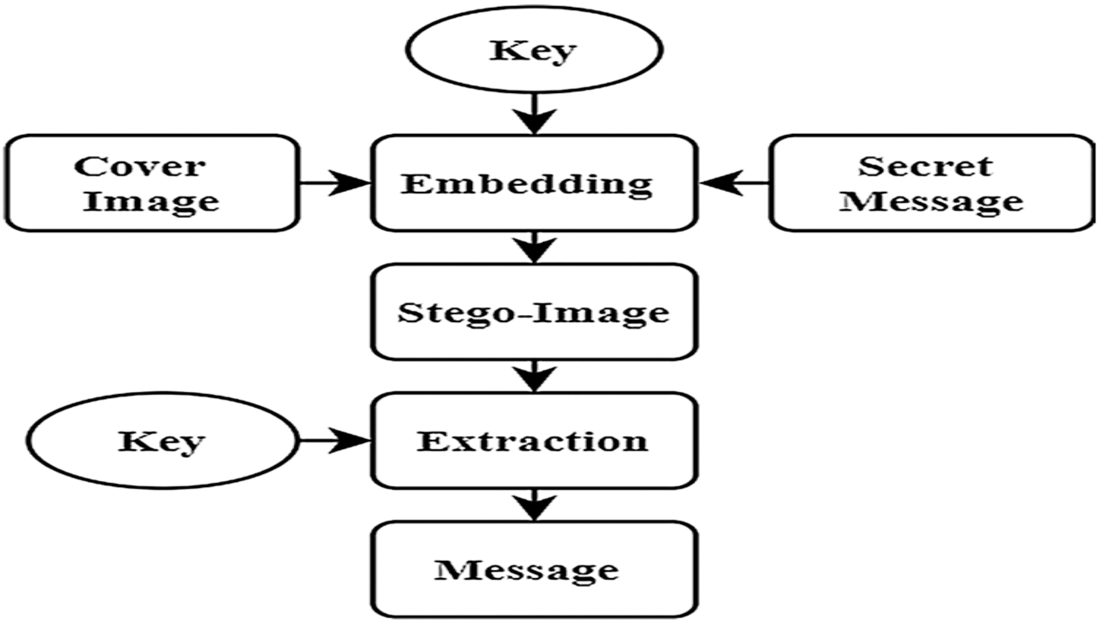


Figure (2.2): **Basic components of steganography**

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 [13].

2.4.3.2 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 [15].

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.

2.4.3.3 Applications of Steganography

Herein some applications of steganography [16]:

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.

2.4.3.4 Video Steganographic Techniques [17]

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 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), [18].

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

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

Where*h*, *g* is the image's size. A_f is the image’s cover; S_f is image.

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.

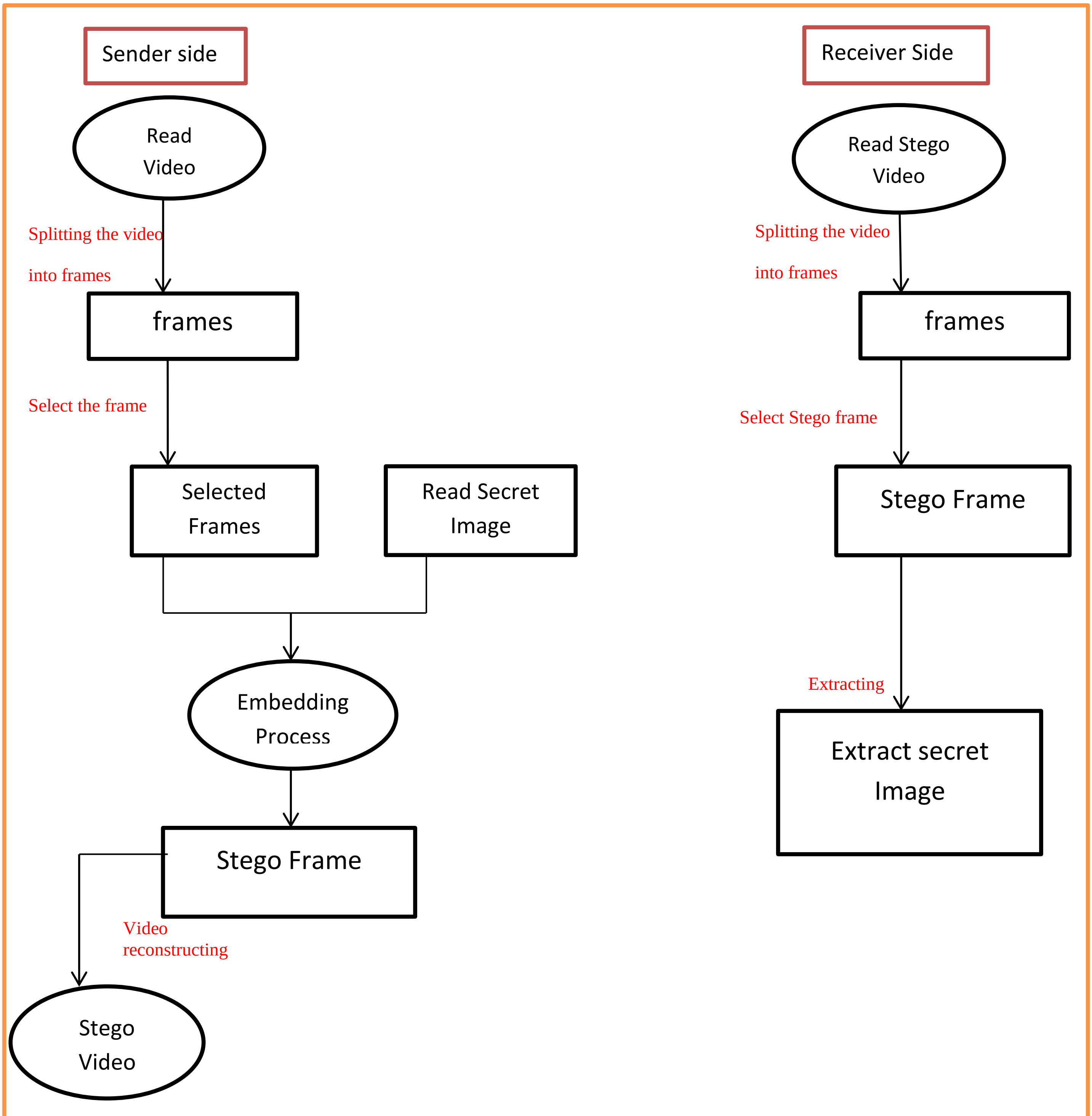
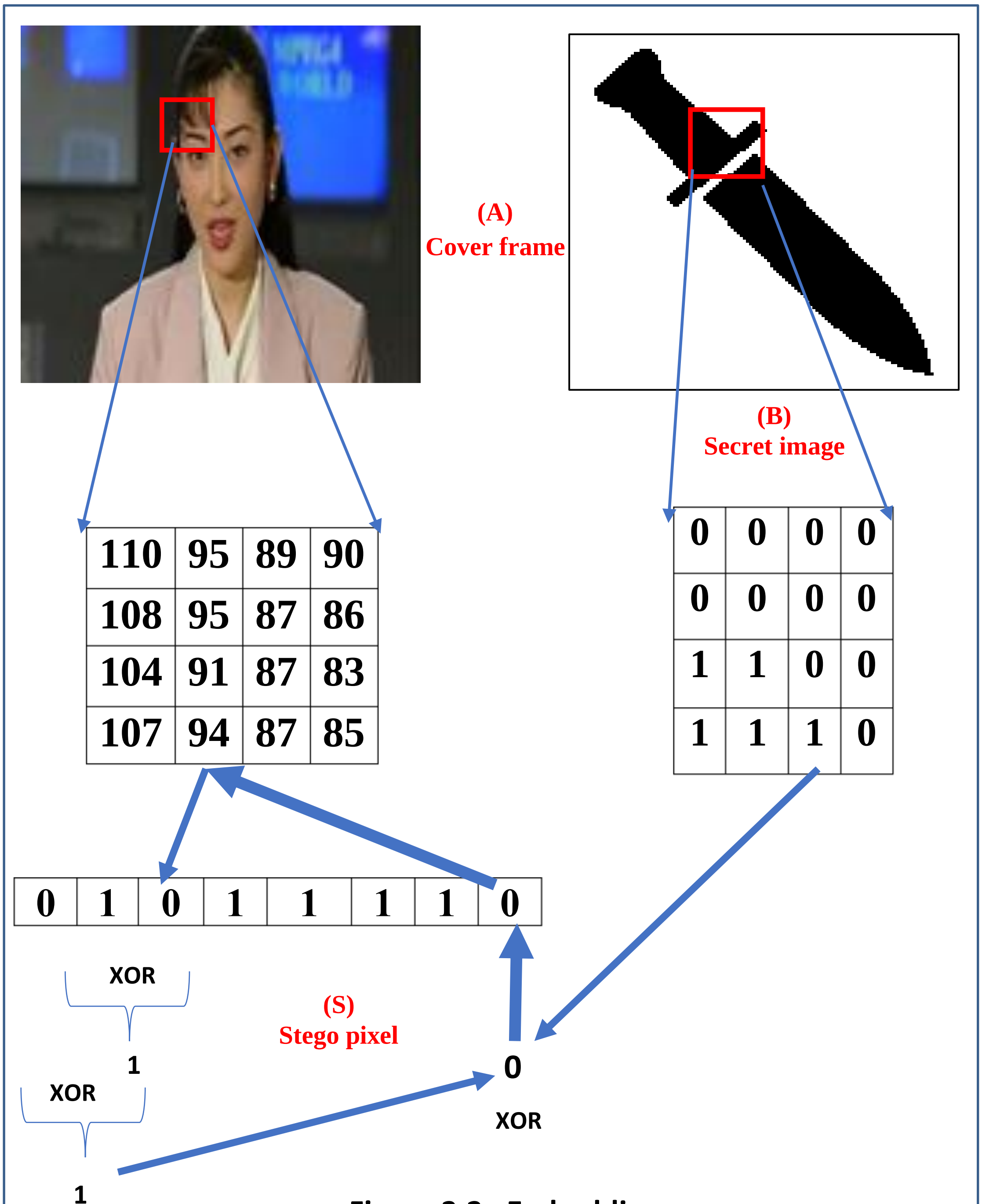


Figure 3.1 : General block Diagram of the proposed project

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

3.2.1 The Embedding process

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



110	95	89	90
108	95	87	86
104	91	87	83
107	94	87	85

0	0	0	0
0	0	0	0
1	1	0	0
1	1	1	0

0	1	0	1	1	1	1	0

Figure 3.2 : Embedding process

In this process, the secret binary image is embedded in the cover frame Also, this process requires an image in a binary for to be as a secret message. The two images must have the same size (n*n). The resulted image will be as stego image. The embedding process is illustrated in the figure (3.2) shows. The steps of the embedding process can be listed as follows:

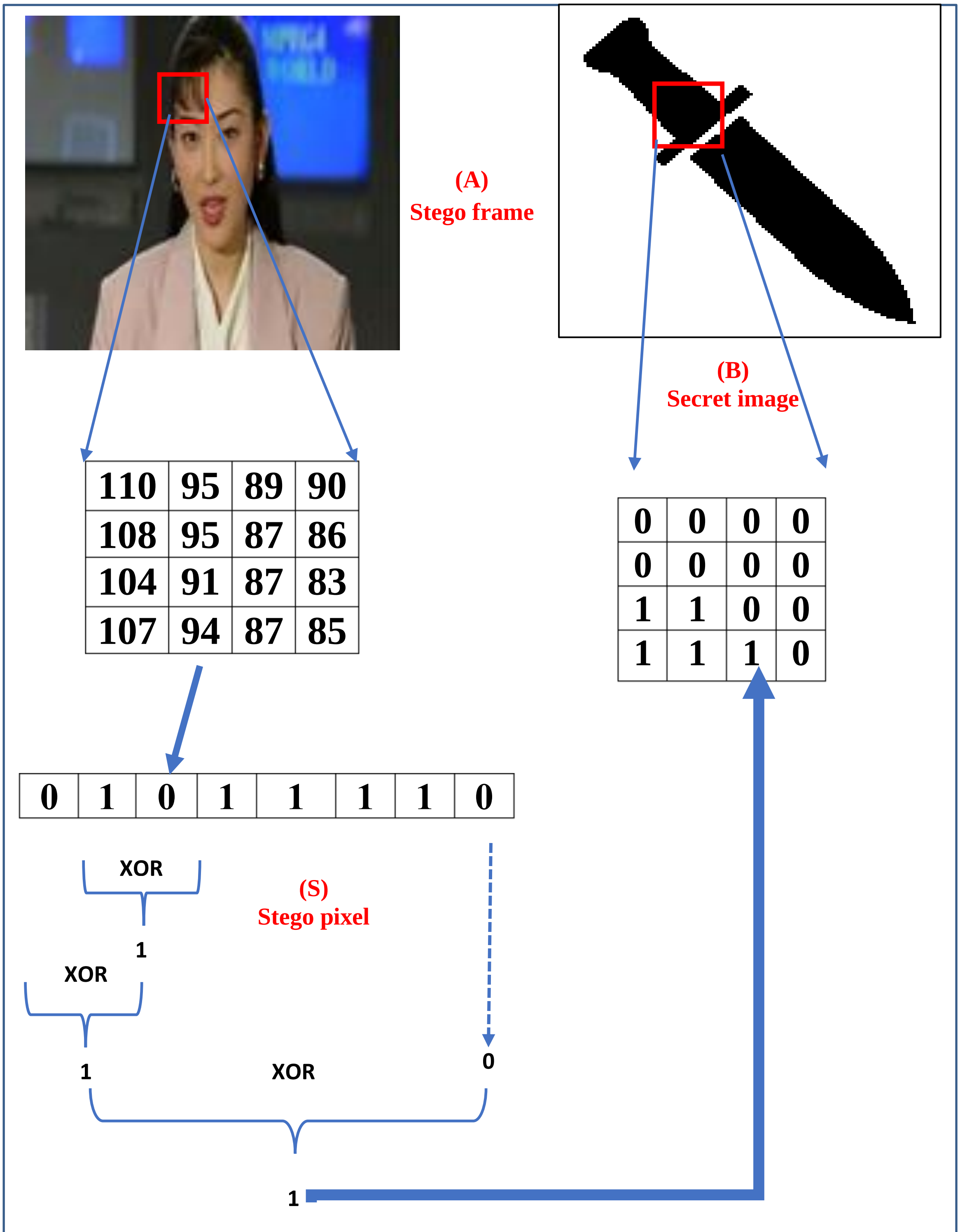
```
Input : cover video
        Secret image

Output : Stego video

Step 1: read the video cover (V).
Step 2: split V into frame and select a specific cover frame (A).
Step 3: read the secret binary image (B)
Step 4: convert the pixels of A into binary.
       For i =1to n
          For j =1to n
          Step 5: doing XOR operations between 7th and 6th bit of A(i,j).
          Step 6: doing XOR operation between bit 8th of A(i,j) and the result of step5.
           Step 7: doing XOR between secret message bit of B(i,j) and result of step6.
            Step 8: substitute the result of step 7 with 1st bit (LSB) of pixel A(i,j) to get
                     stego pixel S(i,j).
         next j
       next i
Step 9: get the stego frame S.
Step 10 : combine S with other frames of V to create stego video SV
```

3.2.2 The Extraction process

This process requires the stego video to get the stego image for the extraction the secret image from it. Figure (3.3) illustrates the extraction process. Extraction process is listed as follows:



110	95	89	90
108	95	87	86
104	91	87	83
107	94	87	85

0	0	0	0
0	0	0	0
1	1	0	0
1	1	1	0

0	1	0	1	1	1	1	0

Figure 3.3 :Extracting process

Input : Stego video

Output : Original Secret image

```
Step 1: read  the stego video (VS)
Step 2: select  the stego frame (S).
Step 3: convert the pixel of S into binary.
    For i =1 to n
      For j =1 to n
        Step 4: doing XOR operations between 7th and 6th bit of S(i,j).
        Step 5: doing XOR operation between bit 8th of S (i , j) and the fourth step result
        Step 6: doing XOR between 1th  bit of S (i , j)  and the fifth step result.
        Step 7: Saving the result of step 1 in the E(i.j)
      Next j
    Next i
Step 7: get the extracted secret image E.
```

Chapter Four

Experimental Results and Discussions

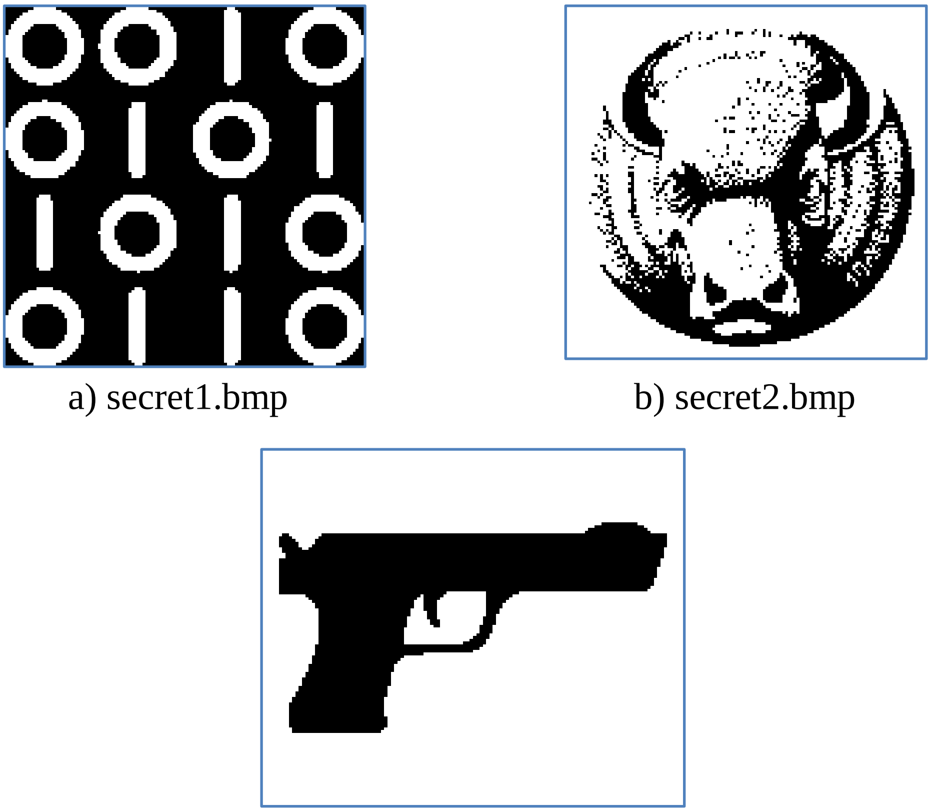
Chapter Four: Experimental Results and Discussions

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 binary image of size (128*128) bits 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 AVI cover video respectively.



a) secret1.bmp

b) secret2.bmp

c) secret3.bmp

Figure (4.1): Secret images

a) boy

b) news

c) two men

d) traffic

Figure (4.2): AVI videos

4.3 Experiential Results

In this section different results will be reviewed for different test videos. The Tables bellows shows the results after applying the suggested project.

The results after applying the suggested project

Table (4.1): (boy video-Red band of frame)

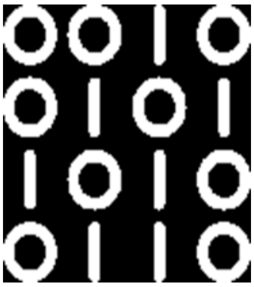
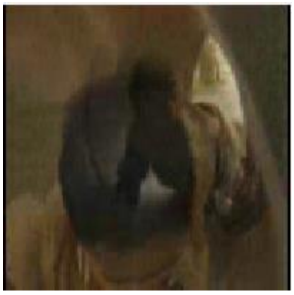
Secret Image	**Frame no.**	**Cover frame**	**Stego frame**	**MSE**	**PNSR**
	**1**			0.16429	31.9094
	26			0.16646	31.8522
	53			0.16469	31.8986

Table (4.2): (boy video-Green band of frame)

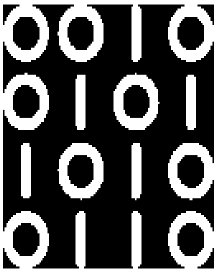
Secret Image	Frame no.	Cover frame	Stego frame	MSE	PSNR
	**1**			0.1672	31.8332
	26			0.16935	31.7775
	53			0.16062	32.0073

Table (4.3): (boy video-Blue band of frame)

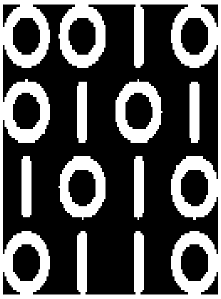
Secret Image	Frame no.	Cover frame	Stego frame	MSE	PSNR
	1			0.16418	31.9121
	26			0.16941	31.7759
	53			0.16414	31.9132

Table (4.4): (Traffic video-Red band of frame)

Secret Image	Frame no.	Cover frame	Stego frame	MSE	PSNR
	1			0.16233	31.9613
	60			0.16701	31.8379
	120			0.16467	31.8992

Table (4.5): (Traffic video-Green band of frame)

Secret Image	Frame no.	Cover frame	Stego frame	MSE	PSNR
	1			0.16813	31.8089
	60			0.16713	31.8347
	120			0.16597	31.865

Table (4.6): (Traffic video-Blue band of frame)

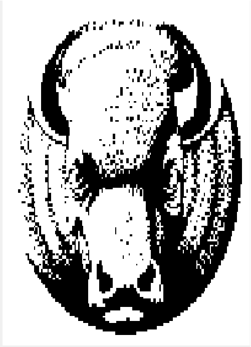
Secret Image	Frame no.	Cover frame	Stego frame	MSE	PSNR
	1			0.17025	31.7546
	60			0.16667	31.8469
	120			0.16823	31.8063

Table (4.7): (Two men video-Red band of frame)

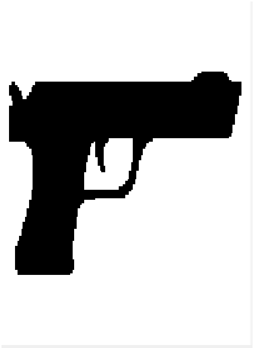
Secret Image	Frame no.	Cover frame	Stego frame	MSE	PNSR
	**1**			0.16921	31.7811
	141			0.16416	31.9126
	250			0.16652	31.8506

Table (4.7): (Two men video-Green band of frame)

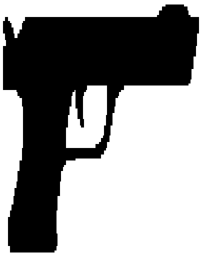
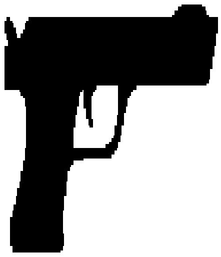
Secret Image	Frame no.	Cover frame	Stego frame	MSE	PSNR
	1			0.16667	31.8469
	141			0.16978	31.7666
	250			0.16811	31.8094

Table (4.8): (Two men video-Blue band of frame)

Secret Image	Frame no.	Cover frame	Stego frame	MSE	PNSR
	1			0.16862	31.7963
	141			0.17358	31.6703
	250			0.17183	31.7143

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.

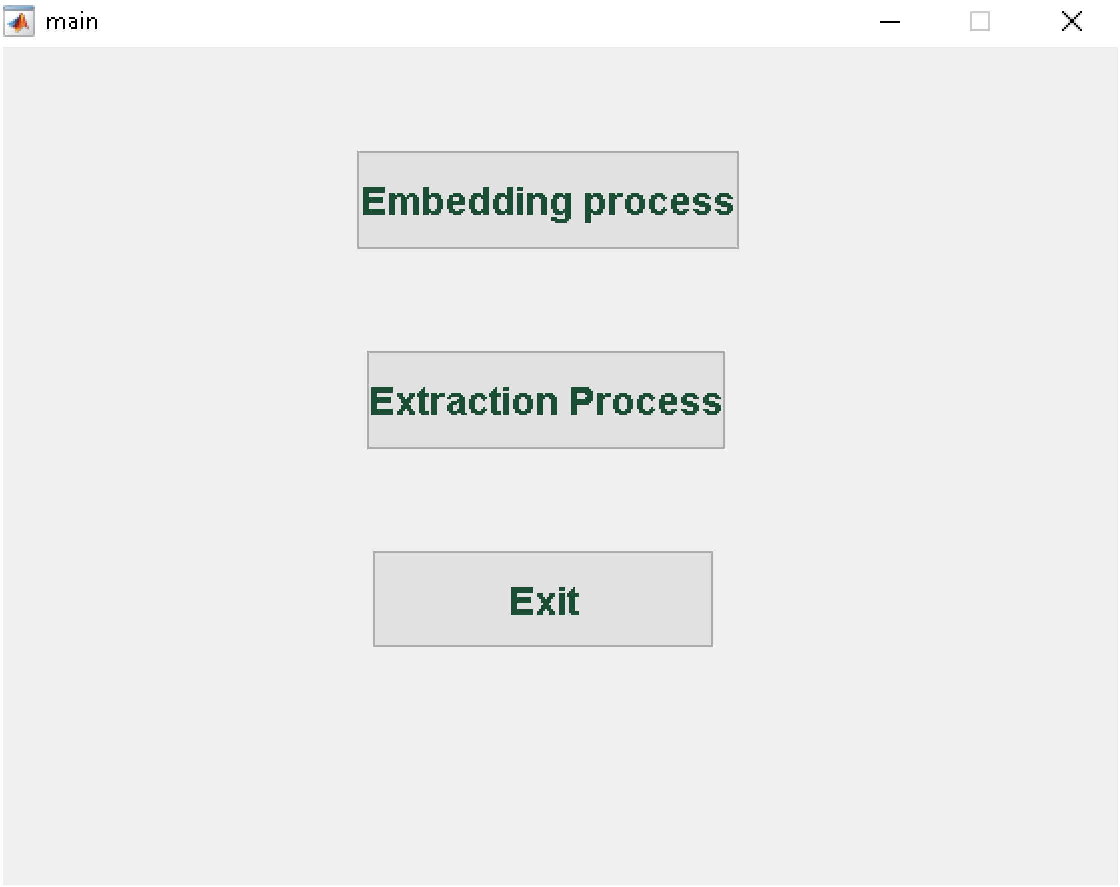
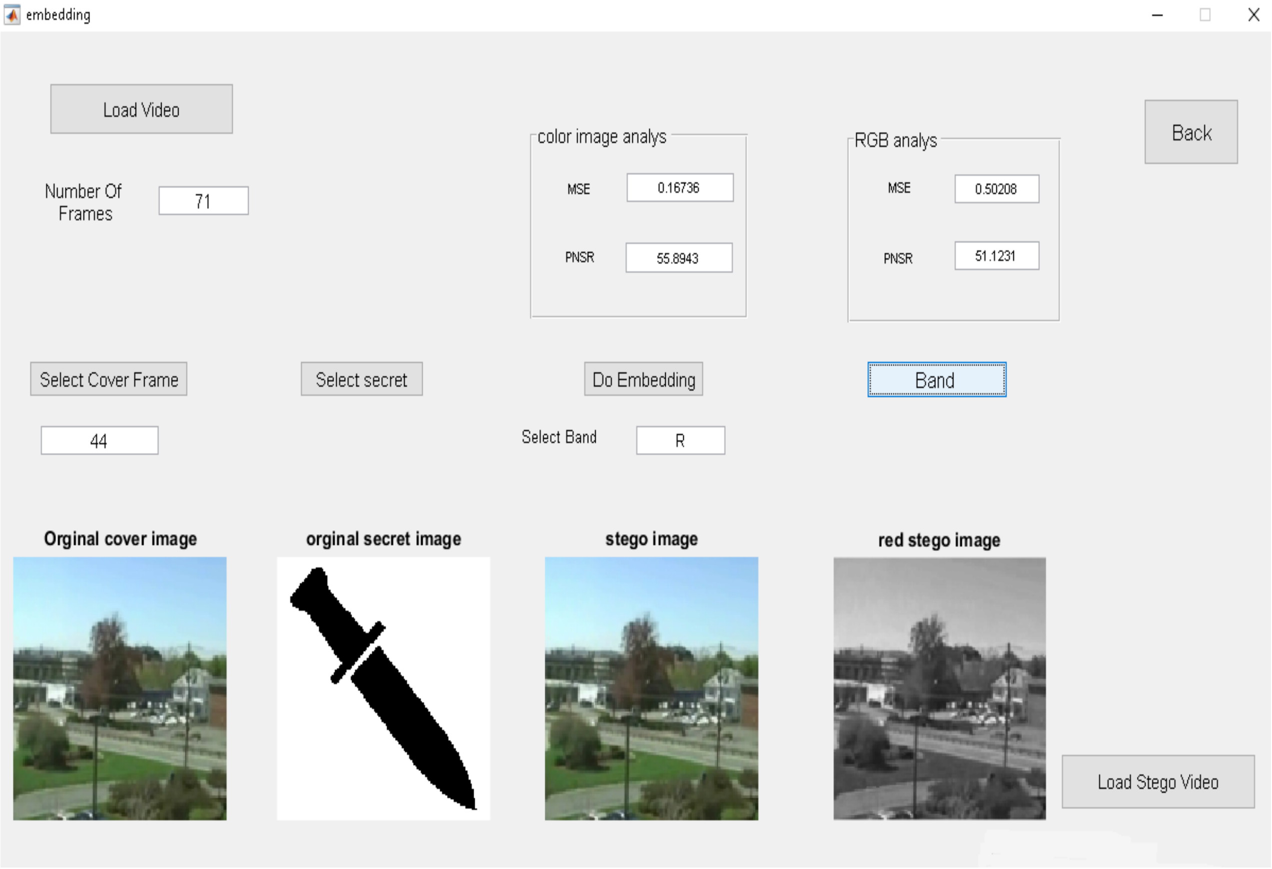


figure (4.3): The starting of the project

4.4.2 Embedding Procedure.



Number Of Frames 71

color image analys
MSE 0.16736
PNSR 55.8943

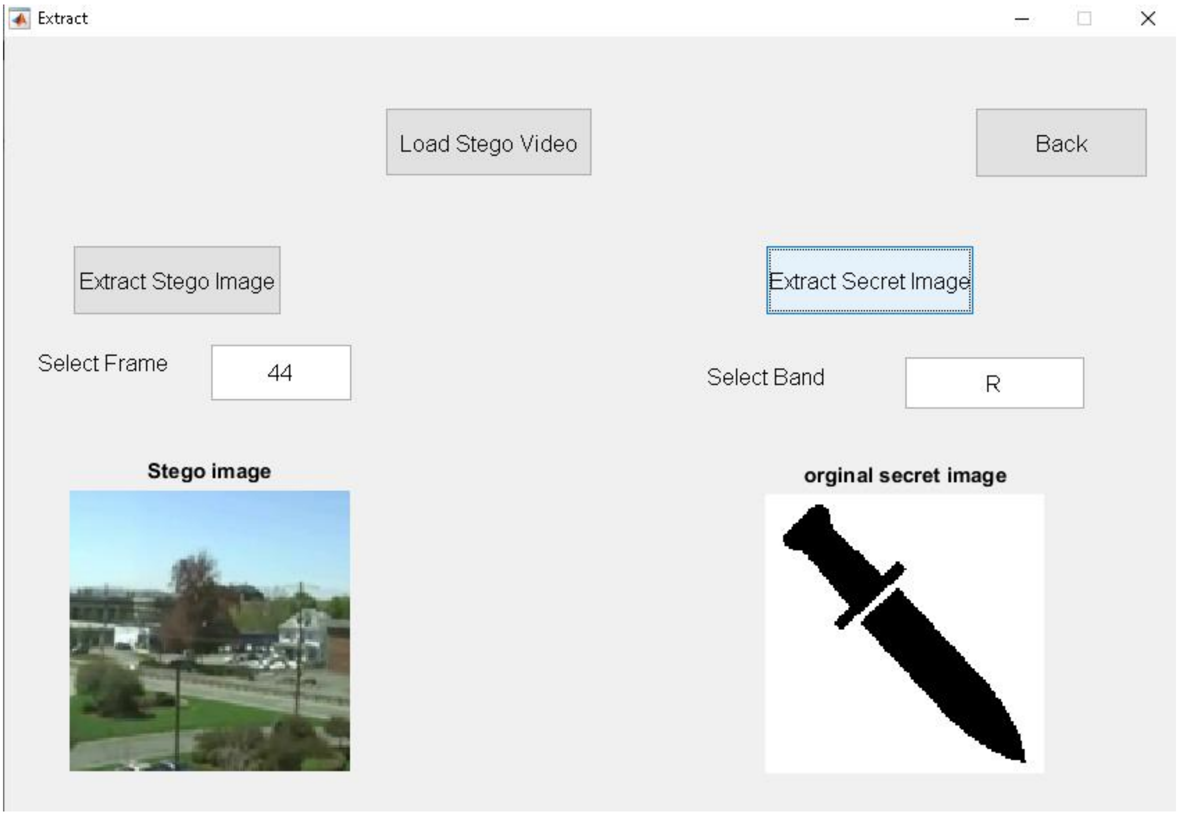
RGB analys
MSE 0.50208
PNSR 51.1231

44

Select Band R

figure (4.4): Embedding process

4.4.3 Extracting Procedure



Select Frame 44

Select Band R

figure (4.5): Extracting process

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

After applying the suggested method, the following concussions are recorded:

After applying the suggested method, the following concussions are recorded:

1- A steganography method has been suggested for satisfying the confidentiality demand which is the most important need security requirements.

2- The secret message is embedded in the spatial domain of frame that was selected from a specific video. Also, XOR operation is used for applying the encryption. By combining the cryptography and steganography techniques the security layer is increased.

3- Two keys(number of frames and band) are used for embedding the secret message which means that the suggested method satisfied the security requirement.

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 like medical or military images.
2. study the effect of using the suggested technique in different types of video such compressed video.
3. Increasing the layer of security by encrypting the secret image before doing the embedding procedure.
4. Doing the XOR operation on the other bits rather than (6^{the},7^{the}, and 8^{the}) in order to enhancing the PSNR value.
5. Studying the ability of choosing the desired frame randomly by using key rather than choosing it directly in order to increase the layer security

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,87, 1548-7741, 2020
3. Paramesh.G,*, Pavithra.K.V , Ranjitha.N, Swetha.S and T.Anushalalitha,” Video Steganography using MATLAB”,10.4108/eai.20-12-2017
4. .Gat Pooja Rajkumar and KLE Dr M S Sheshgiri,” Video Steganography: Secure Data Hiding Technique”, 38,10.5815,5.9.2017.
5. .Bharti Chandel, Dr.Shaily Jain,” Video Steganography: A Survey”,11, 2278-8727 , Jan – Feb. 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” ,359, 360, 5/1/2011
7. Jonathan Sachs,” Digital Image Basics”, 1996
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. M. Owens, “A Discussion of Covert Channels and Steganography”,2002.

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

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

12. 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.

13. 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.

14. 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.

15. H. Dutta, R. K. Das, S. Nandi, and S. M. Prasanna, “An overview of digital audio steganography”, 2019.

16. 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.

17. Syeda Musfia Nasreen , Gaurav Jalewal, Saurabh Sutradhar ,”A Study on video Steganography techniuqes", 30, 2250 – 3005, October – 2015

18. 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

ان كمية البيان والمعلومات التي يتم تناقلها يوميا عبر الانترنت وامكانيه الوصول اليها من الاشخاص غير المخولين ولضمان حماية هذه البيانات ضهر دافع لإخفاء البيانات

المشروع المقدم يقترح تطبيق Steganography في الفيديو للحفاظ على الخصوصية والتي تعتبر من المتطلبات المهمة في حقل الامنية هنالك بيئتان في الصورة ممكن اخفاء الرسالة السرية فيها ، البيئة المكانية والبيئة الترددية .

في هذا المشروع المقدم، تم الاخفاء في البيئة المكانية بالاعتماد على طريقة least Significant Bit(LSB) لغرض تحقيق الامنية، فقد تم اقتراح استخدام Encryption. في هذه الطريقة تم استخدام عملية XOR في اخفاء الرسالة السرية.

اضافة الى ذلك، فقد اثبتت نتائج التجارب ان الطريقة المقترحة حققت كذلك متطلب عدم المحسوسية الذي هو ايضا متطلب مهم من متطلبات الامنية، حيث ان قيمة PSNR كانت بين ال30 – 50 dp

هذه الطريقة كفؤة اكثر من باقي الطرق المستخدمة في بحوث اخرى نسبه لسرعه الاداء ولكون قيمه ال PNSR اكثر من 30 db فكان الاخفاء باقل تشوه حاصل واستخدام TXOR operation والذي ادى لزيادة في مستوى الامان

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

تعاون انيق بين (LSB-TXOR) لإخفاء المعلومات السرية في الفيديو

بحث مقدم إلى

كلية العلوم للبنات، جامعة بابل

جزءا من متطلبات نيل درجة الدبلوم العالي في علوم الحاسوب

مقدمة من قبل

شهد رفيق موسى

بإشراف

ا.د. ماجد جبار جواد

1442هـ 2021م