بسم الله الرحمن الرحيم

Sudan University of Science and Technology

College of Graduate Studies

Master of Computer Science Program

Design and Implementation of a System for Data Encryption and Hiding Using Video Tomography

تصميم وتطبيق نظام لتشفير واخفاء البيانات باستخدام الاخفاء في الفيديو

A Thesis Submitted In Partial Fulfillment of the Requirements for the Degree of Master of Information Technology

By:

Saria Elsir Mohamed Ahmed Khalid

Supervised:

Dr. Faisal Mohamed Abdallah Ali

January 2023

Dedications

Who taught me how to take the science of wealth …

To whom I try to achieve a dream as long as he sees … To who gave me the fruits of his life …

To who taught me patience …

My Father …

To the big Heart … To the rivers of tender tenderness …

And tried to grow up… To who will the heaven rise under their feet …

To who was her prayer the secret of our progress

My Mother's soul …

To those who were almost ready to be apostles … To those who enlightened our way with their knowledge …

My distinguished teachers…

To those who dream together … To those who share the sweetness of life and happiness …

To whom we wish all beautiful …

My Brothers…

To those who joined us the path … To whom we met with them without time were the sweetest memories…

My Friends…

ACKNOWLEDGMENT

Firstly, all thanks belong to ALLAH, the almighty for giving me the will power to make this work; truly without his grace nothing is achievable.

I would like to express my sincere gratitude to my advisor ***Dr. Faisal Mohammed Abdallah*** *for the continuous support I am extremely thankful for his valuable guidance, advice, motivation, encouragement, moral support, sincere effort.*

Abstract

The internet provides a method of communication to distribute information to the masses with the growth of data communication over computer network, the security of information has become a major issue.

Cryptography and Steganography are the two popular methods for secure data. Cryptography is the science of change the format of text from readable to unreadable text. Steganography is technique and art of hiding a secret message in carrier file.

Steganography is the technique and art of hiding a secret message in a carrier file.

A method proposed in this paper to improve the security system is to combine encryption and concealment.

In this research the proposed to improve security system by combination between cryptography and steganography.

Firstly, the International Data Encryption algorithm (IDEA) is used to encrypt the secret message.

Secondly, the encrypted message has been embedded and distributed in even-frame in the video file using LSB steganographic and then applying DCT steganographic also to this stego-video.

Thus, two levels of security have been provided using the proposed hybrid technique.

In addition, the proposed technique provides high embedding capacity and confidentiality.

المستخلص

يوفر الإنترنت وسيلة اتصال لتوزيع المعلومات و مع نمو عملية اتصالات البيانات عبر شبكة الكمبيوتر ، أصبح أمن المعلومات مشكلة رئيسية.

التشفير و الاخفاء هما طريقتان شائعتان لتأمين البيانات. حيث ان علم التشفير هو علم تغيير تنسيق النص من نص مقروء إلى نص غير قابل للقراءة. اما إخفاء المعلومات هو تقنية وفن لإخفاء رسالة سرية في ملف الناقل.

حيث ان إحدى الطرق المقترحة في هذا البحث لتحسين نظام الأمان هي الجمع بين التشفير والإخفاء.

أولاً ، يتم استخدام خوارزمية تشفير البيانات الدولية (IDEA) لتشفير الرسالة المراد تشفيرها،

ثانيًا ، يتم تضمين الرسالة المشفرة وتوزيعها علي إطارات-صور الزوجية في ملف الفيديو باستخدام واحدة من تقنيات الاخفاء وهي LSB ومن ثم أيضًا تطبيق تقنية اخري من تقنيات الاخفاء وهي DCT على مقطع الفيديو هذا.

وهكذا، تم توفير مستويين من الأمان باستخدام التقنية المختلطة المقترحة. بالإضافة إلى ذلك ، توفر التقنية المقترحة قدرة تضمين عالية وسرية.

List of Contents

3. Chapter Three System Design

4. Chapter Four Implementation

5. Chapter Five Conclusion And Recommendation

List of Tables

List of Figures

List of Abbreviation

IDEA: International Data Encryption Algorithm

LSB: Least Significant Bit

RGB: red, green, blue

HVS: human visual system

HAS: human auditory system

TCP: Transmission Control Protocol

IP: Internet Protocol

IDS: Intrusion Detection System

DCT: Discrete Cosine Transformation

IDCT: inverse Discrete Cosine Transformation

AES: Advanced Encryption Standard

RC4: Rivest Cipher 4

RSA: Rivest–Shamir–Adleman

DES: Data encryption standard

DNA: Deoxyribonucleic acid

OTP: One Time Password

PSNR: Peak Signal-to-Noise Ratio

CHAPTER ONE
INTRODUCTION

CHAPTER I

INTRODUCTION

1.1 Background

In the current time, The Internet provides essential communication between millions of people. Internet is sometime used to share data from side to other side. It increased dramatically and noticeably in the past years. It provides ability for many people to send and receive any type of data, be it audio or video through the internet just by click of a button but did they ever think how securely their data begin transmitted or sent to other person safely without any leakage of information. Computer security : is the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/ data, and telecommunications)[1].

Computer security is fascinating and complex challenges. Some of the reasons Include:

1. Security is not as simple as it might first appear to the novice. The requirements seem to be straightforward, But the mechanisms used to meet those requirements can be quite complex, and understanding.
2. In developing a particular security mechanism or algorithm, one must always consider potential attacks on those security features.
3. Because of point2, the procedures used to provide particular services are often counterintuitive .Typically, a security mechanism is complex, and it is not obvious from the statement of a particular requirement.
4. Security mechanisms typically involve more than particular algorithm or protocol.
5. Security is still too often an afterthought to be incorporated into a system after the design is complete rather than being an integral part of the design process.

1.2 Research Motivation

The major purpose of this research is to design a secure data transmission system which merges between cryptography and steganography to achieve the goals of promoting security, availability and confidentiality for secret message.

In this research, two level of security is provided which means the first layer of security is cryptography after realization cryptography then concealing encrypted data inside the video-frames using steganography technique and this is the second layer.

1.3 Problem Statement

One of the major problems when sending data over the Internet is the security threat it poses i.e. the personal or confidential data can be modify or leakage in many ways. One of the solutions is secure data transferring is using cryptographic algorithms. Although Cryptography scrambles the information, it discloses its existence. Steganography hides the existence of the secret information. Using features of both cryptography and steganography is needed.

1.4 Objective

The main objective is promoting a system that applies multilevel of data security to concealing encrypted data into video-image by applying two methods of steganography. In addition, there is a some sub-objectives:

- increasing the secrecy of the secret information by using two level of security in one the system.
- Develop and implementation a System that provides a high degree of data confidentiality.
- prevent unauthorized access to the data.

1.5 Scope of Research

The scope of this research will be cryptography and steganography technique in multilevel especially steganography on video-frames avoiding key exchange. The security of data (text) will be achieved by two levels of security ; level one is encryption that change

text to unreadable text using IDEA cipher . whereas level two uses the steganography technique to hide the encrypted data into video-frames using hybrid method which it LSB and DCT.

1.6 Research Important

Transmitting data in a safe and secure in difficult fashion. With combination between cryptography and Steganography. Provide additional level of security

1.7 Research Methodology

This research aims to design and promote a secure transferring system. The proposed solution in this research is to create a secure transferring between sender and receiver by applying Cryptography technique to the secret data, which results is scrambled data and then apply steganography technique to hide the data in the video frames. Figure 1.1 shows the methodology

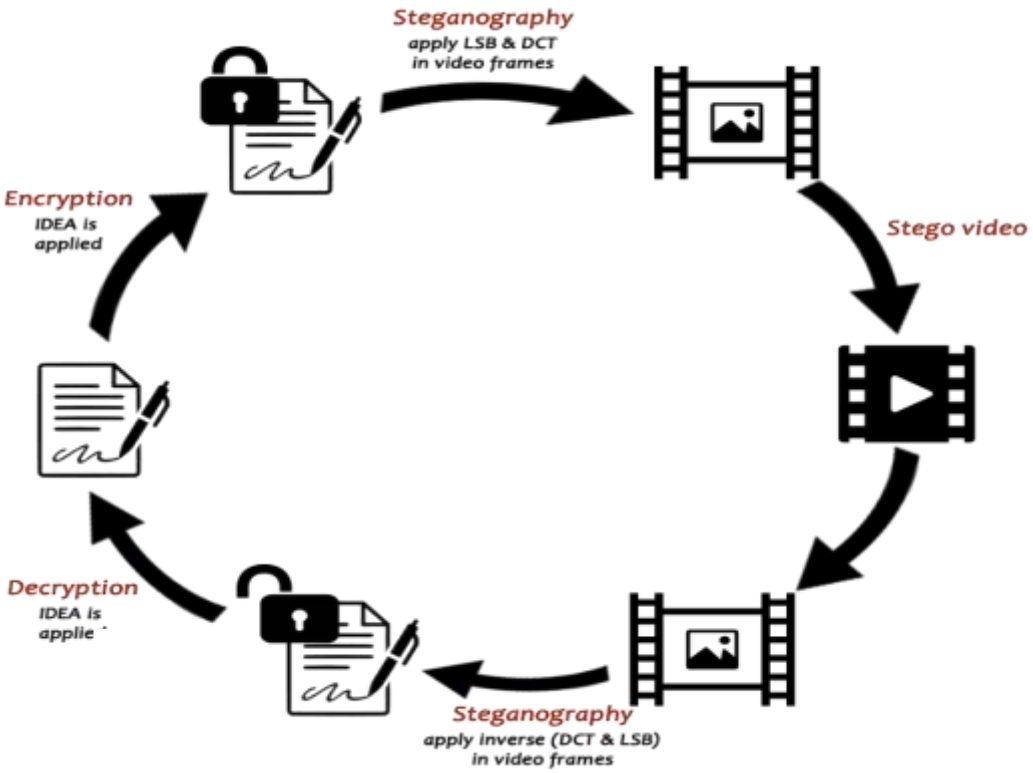


Figure (1.1) methodology

1.8 Thesis Layout

This thesis consists of five chapters, Chapter one is the introduction that submit the problem and the solution. Chapter two discuss the literature review and related work of cryptography and steganography. Chapter three appearance the system design. Chapter four show the implementation and results of the proposed scheme. Finally Chapter five present the Conclusions and Recommendation.

CHAPTER TWO
LITERATURE REVIEW AND RELATED WORKS

CHAPTER II

LITERATURE REVIEW AND RELATED WORKS

2.1 Introduction

In the present scenario, any type of communication over the internet and other network applications need to be secure due to their increasing utility. For this task, lots of algorithms for security have been implemented and used so far. With these developments, attackers have also come up with the new ideas to penetrate the communication mediums. Till now cryptography has been the mainstay for defending the secure data transmission. Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents where we change the natural form of data by using different security algorithms, to increase security of the communication process.

Steganography has also taken space for security purpose, in Steganography information is kept hidden from the attacker for communicating the information safely with the use of images, audios, videos… etc.

Steganography is applied in various fields for the purpose of security and confidentiality it can be divided into (text, image, audio, video and network or protocol). [1].

2.2 Cryptography

Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it. this term is derived from the Greek word kryptos, which means hidden. It is closely associated to encryption, which is the act of scrambling ordinary text into what's known as ciphertext and then back again upon arrival.

In computer science, cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms, to transform messages in ways that are hard to decipher. These deterministic algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on the internet, and confidential communications such as credit card transactions and email. there are two types of cryptographic algorithm to accomplish

these goals: symmetric cryptography and asymmetric cryptography. The initial unencrypted data is referred as normal text.

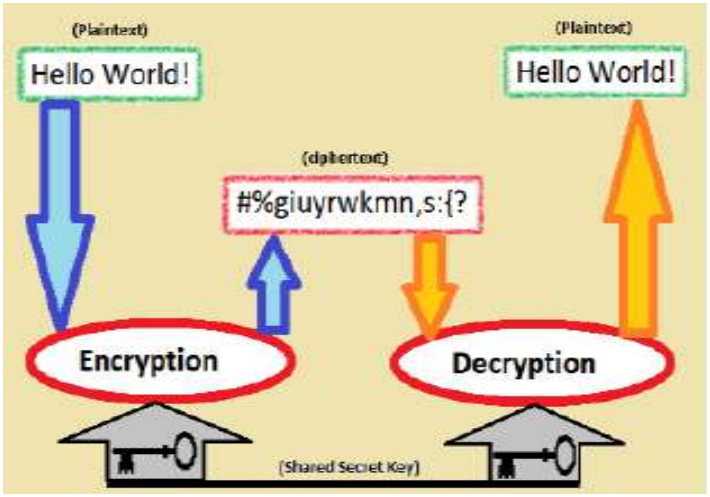


Figure (2.1) process of cryptography [2]

Science of cryptography and secret writing it goal of hiding the meaning of a message. systems are generically classified along three independent dimensions: [1]

1. The type of operations used for transforming plaintext to ciphertext. All encryption algorithms are based on two general principles: substitution and transpositions .In substitution which each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element, but in transposition which elements in the plaintext are rearranged.
2. The number of keys used. If both sender and receiver use the same key, the system is referred to as symmetric, single-key, secret-key, or conventional encryption. If the sender and receiver each use a different key, the system is referred to as asymmetric, two-key, or public-key encryption.
3. The way in which the plaintext is processed. A block cipher processes the input one block of elements at a time, producing an output block for each input block. A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along.

2.2.1 Cryptography Techniques

Cryptography is closely related to the discipline of cryptology and cryptanalysis. It includes techniques such as microdots, merging words with images, and other ways to hide

information in storage or transit. However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as cleartext) into ciphertext (a process called encryption), then back again (known as decryption). Individuals who practice this field are known as cryptographer. Modern cryptography concerns itself with the following four objectives:

1. Confidentiality: the information cannot be understood by anyone for whom it was unintended
2. Integrity: the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected
3. Non-repudiation: the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information
4. Authentication: the sender and receiver can confirm each other's identity and the origin/destination of the information

There are Basic terminology needs to know, there is:

Plaintext: This is the original message or data that is fed into the algorithm as input.

Enciphering or encryption: the process of converting plaintext into ciphertext. This process is illustrated in the figure (2.2).

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

Secret key: The secret key is also input to the algorithm .The exact substitutions and transformations performed by the algorithm depend on the key and input.

Ciphertext: This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts.

Deciphering or decryption: recovering plaintext from ciphertext. This process is illustrated in the figure(2.3).

Decryption algorithm: This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the same secret key and produces the original plaintext.

Figure (2.2) Encryption process in cryptography [3]

Figure (2.3) Decryption process in cryptography [3]

2.2.2 Cryptography Types

In general there are three types of cryptography:

1. **Symmetric Cryptography**

It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange key in a secure manner.

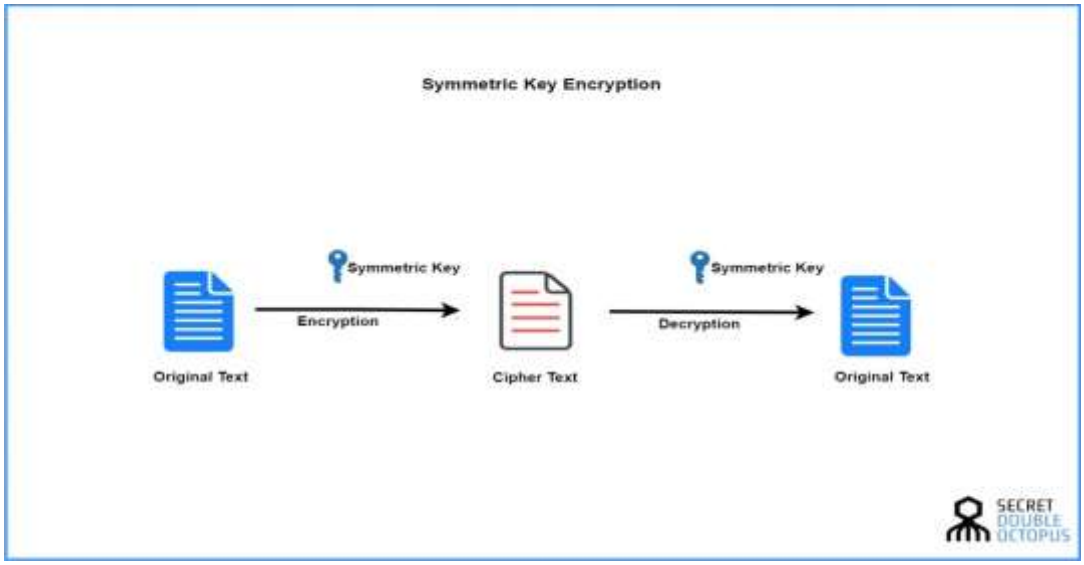
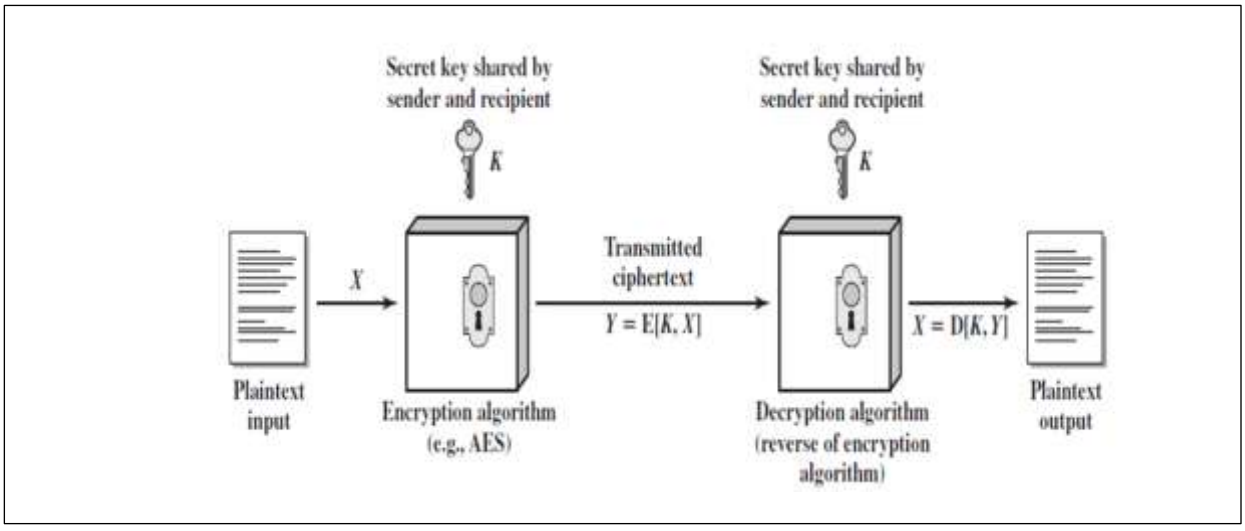


Figure (2.4) symmetric encryption scheme [4].

2. Asymmetric Cryptography (Public key)

Different keys used for encryption and decryption the public key of every party may be known by everyone, whereas the private key must be kept secret. Party 1 may encrypt a message for Party 2 using Party 2's public key, which creates a cipher text which only Party 2 can decrypt. Party 1 can also sign any message using their private key so that Party 2 (or anyone else listening in) can verify that the message is indeed from that Party 1. The blowing figure (2.5) show A symmetric encryption scheme.



Figure(2.5) A symmetric encryption scheme [1].

3. Hash Functions

A cryptographic hash function is a particular class of hash function that is suitable for use in cryptography. It maps data of arbitrary size to a bit string of fixed size. It is designed to be a one-way function, i.e., irreversible. By making the output string large enough, brute-force attacks (trying every possible input) becomes intractable. hash functions. Fig 2.6 shows the general idea how a cryptographic hash function works [26].

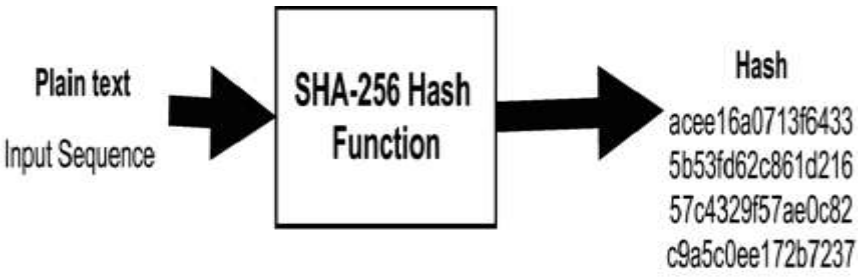


Figure (2.6) Basic Function of the SHA-256 [5]

According to Cryptodox, "a cryptographic hash function should behave as much as possible like a random function while still being deterministic and efficiently computable" [5]. A cryptographic hash function is considered insecure if either of the following is computationally feasible:

1. Finding a previously unseen message that matches a given hash value.
2. Finding collisions, in which two different messages have the same hash value.

2.2.3 Cryptanalysis

Cryptology has two parts namely, Cryptography which focuses on creating secret codes and Cryptanalysis which is the study of the cryptographic algorithm and the breaking of those secret codes. The person practicing Cryptanalysis is called a Cryptanalyst. It helps us to better understand the cryptosystems and also helps us improve the system by finding any weak point and thus work on the algorithm to create a more secure secret code. For example, a Cryptanalyst might try to decipher a ciphertext to derive the plaintext. It can help us to deduce the plaintext or the encryption key.

To determine the weak points of a cryptographic system, it is important to attack the system. This attacks are called Cryptanalytic attacks. The cryptanalyst depends on the available

information like nature of the algorithm and also knowledge of the general characteristics of the plaintext.

Table 2.1 summarizes the various types of cryptanalytic attacks based on the amount of information known to the cryptanalyst.

Table (2.1) Types of Attacks on Encrypted Messages [1]

Type of Attack	**Known to Cryptanalyst**
Ciphertext only	• Encryption algorithm. • Ciphertext to be decoded.
Known plaintext	• Encryption algorithm. • Ciphertext to be decoded. • One or more plaintext–ciphertext pairs formed with the secret key.
Chosen plaintext	• Encryption algorithm. • Ciphertext to be decoded. • Plaintext message chosen by cryptanalyst, generated with the secret key.
Chosen ciphertext	• Encryption algorithm. • Ciphertext to be decoded. • Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key.
Chosen text	• Encryption algorithm. • Ciphertext to be decoded. • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key • Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key.

2.2.4 Advanced Encryption Standard Algorithm (AES)

In past DES was existed, it was based on an algorithm developed by IBM, and it was considered unbreakable. But no long, it was broken by brute-force attacks in 1990s in several manners.

Resulting of this, DES can not to take advantage of the rapid development in microprocessors that happened in the last two decades of the 20th century.

After breaking the previous cipher algorithms easily on modern computing systems. that was required a new encryption algorithm.

The National Institute of Standards and Technology (NIST) wanted to help in the creation of a new standard; the idea was to develop a new encryption algorithm that would be used for protecting sensitive, non-classified, U.S. government information. The proposal ciphers had to achieve a lot of requirements.After all this examination NIST finally chose an algorithm known as Rijndael algorithm of Belgian cryptographers Joan Daemen and Vincent Rijmen in October 2000. [9]

The AES algorithm standardized version of Rijndael and also referred to Rijndael algorithm is a symmetrical block cipher algorithm this means that it uses the same key for both encryption and decryption , AES algorithm uses 128,192, or 256 bit keys to transform a block of 128 bits message into a 128 bits of ciphertext which is the main reason why it is strong ,secure and stronger than the DES that uses 56 bit key

A substitution-permutation, or SP network, with several rounds is used by the AES algorithm to generate ciphertext. The key length used will determine the number of rounds. the advantages and disadvantages of AES:

a. advantages:

1. it is the most security protocol, since it is applied in both hardware and software.
2. It used key sizes of greater length for encryption ,such as 128.192 and 256 bits, this makes it very difficult to hack.
3. Used for a wide range application.
4. It is one of the world's most commonly used commercial and open source solutions.

b. disadvantages:

1. It use algebraic structure that are too simple and easy.
2. All blocks are encrypted in the same way at all time.
3. Difficult to implemented in software.

2.2.5 International Data Encryption Algorithm (IDEA)

The International Data Encryption Algorithm (IDEA) is a symmetric-key, block cipher. It was published in 1991 by Lai, Massey, and Murphy. In the Second Edition (1996) of Applied Cryptography Bruce Schneier describes IDEA as "... the best and most secure block algorithm available to the public at this time" [6]

IDEA algorithm, it was considered among the best publicly known algorithms and it the block cipher algorithm. IDEA is generally considered to be very secure. The block cipher IDEA operates with 64-bit plaintext and cipher text blocks and is controlled by a 128-bit key and it is divided in 52 sub keys. The fundamental innovation in the design of this algorithm is the use of operations from three different algebraic groups of Exclusive OR, multiplication modulo, and addition modulo. The substitution boxes and the associated table lookups used in the block ciphers available to-date have been completely avoided. the encryption process is identical to the decryption process.[7]

2.3 Steganography

Steganography is a technique of hiding information in digital media in such a way that no one apart from the intended recipient knows the existence of the information. Show in figure (2.8).[8]

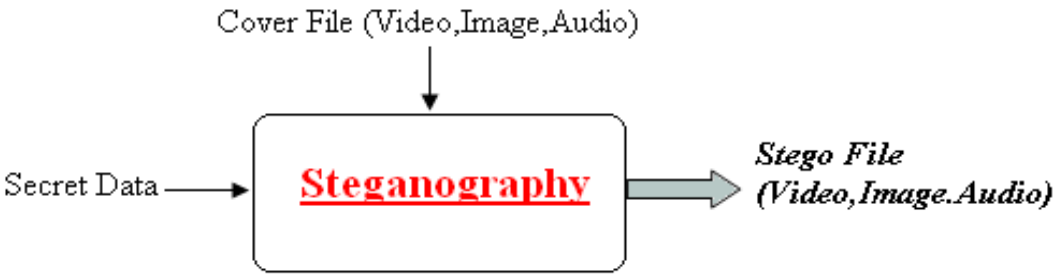


Figure (2.7) Basic Steganography System [8]

Steganography or Stego as it is often referred to in the IT community, literally means, "covered writing" which is derived from the Greek language. Steganography is defined by Markus Kahn as follows, "Steganography is the art and science of communicating in a way which hides the existence of the communication. In contrast to Cryptography, where the enemy is allowed to detect, intercept and modify messages without being able to violate

certain security premises guaranteed by a cryptosystem, the goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second message present". [11]

In a digital world, Steganography and Cryptography are both intended to protect information from unwanted parties. Both Steganography and Cryptography are excellent but neither technology alone is perfect and both can be broken. for this reason the most experts would suggest using both to add multiple layers of security. Steganographic technologies are a very important part of the future of Internet security and privacy on open systems such as the Internet.

In steganography, the secret message is concealed using a cover medium (i.e., carrier) before it is transmitted on a public communication channel. It therefore, impedes the unauthorized access to the message and protects its confidentiality. Before the application of steganography for increasing the security and reduction in the amount of data to be embedded, the secret message can be encrypted or compressed. (note: the carrier object can be text, video, or audio too) only the parties know existing of the secret message. steganography and data embedding technology or stego format is generally classified into two main types namely:

frequency domain and method in spatial domain [10]

The evaluation of steganography technique is done with three parameters such as capacity, robustness and security. [10]

The system should be capable of hiding the information into cover media, it should be robust to the changes and it should be secured enough from eavesdroppers or attackers that tends to identify or alter the contents of the secret data.

Modern steganography uses the opportunity of hiding information into digital multimedia files and also at the network packet level. The aims of steganography creating a communication channel between two parties, without an intermediary noticing the existence of the particular channel.

2.3.1 History of Steganography

Steganography has been with us in many forms since the time of the Greek empire. Even the word steganography comes from the Greek steganos, hidden or covered, plus graphein, to write. Herodotus, the Greek historian recorded the story of a slave used as the medium to transmit the hidden message. The slave’s head was shaved and the message

tattooed on the bare skull after which the hair was allowed to re-grow. The slave was sent to the message recipient who shaved the slave's head to reveal the message. Hopefully the message was not time-dependent! Lord Robert Baden-Powell, as scout for the British during the Boer War marked the positions of Boer artillery bases by embedding maps into drawings of butterflies. Appearing innocent to a casual observer, certain markings on the wings were actually the positions of the enemy military installations. Later, Axis and Allied spies used invisible inks containing fruit juice or urine to transmit messages that would reveal themselves when heated or when in the presence of ultraviolet light.

In the mid-90s a number of the older techniques of hiding messages inside other messages and even images became more popular with the advent of modern software and powerful computers.[11]

Regardless of the technique used, the key similarity in all cases was that messages were hidden in plain view. steganography used in various forms for 2500 years ago in various fields, in military, diplomatic, personal and intellectual property applications. Briefly, steganography is the term applied to any number of processes that will hide a message within an object, where the hidden message will not be apparent to an observer.

2.3.2 Steganography as communication System

The studying of communications security includes not just encryption, but also traffic security, a steganographic message (the plain text) is often first encrypted by some traditional means, producing a cipher text. Then, a cover text modified in some way to contain the cipher text, resulting in stagiest. For example, the letter size, spacing, typeface or other characteristics of a cover text can be manipulated to carry the hidden message; only the recipient (who must know the used technique) can recover the message and then decrypt it. Let us look at what a theoretically perfect secret communication (Steganography) would consist of, to illustrate this concept; we will use three fictitious characters named (Alice), (Bob) and (Windy). As shown in figure 2.9, (Alice) Wishing to Send a secret message **m** to (Bob). In order to do so, he "embeds" **m** into a cover-object **c**, to obtain the stego-object **s**. The stego-object **s** then sent through the public channel. (Windy) who examines all messages in the channel, he should not be able to distinguish in any sense between cover-objects (objects does not containing any secret message) and stego-objects (objects that contains a secret message). In this context, steganalysis refers to the body of techniques that aid (windy) in distinguishing between cover-objects and stego-objects. It should be noted that (Windy)

has to make this distinction without any knowledge of the secret key which (Alice) and (Bob) may be sharing and sometimes even without any knowledge of the specific algorithm that they might be using for embedding the secret message.

As cryptanalysis is the counterpart of cryptography, steganalysis is the counterpart of steganography. A steganalyst known as tries to determine the existence of a covert communication channel between two parties and either break or alter their communication. As we mention (windy) in pervious scenario.

.

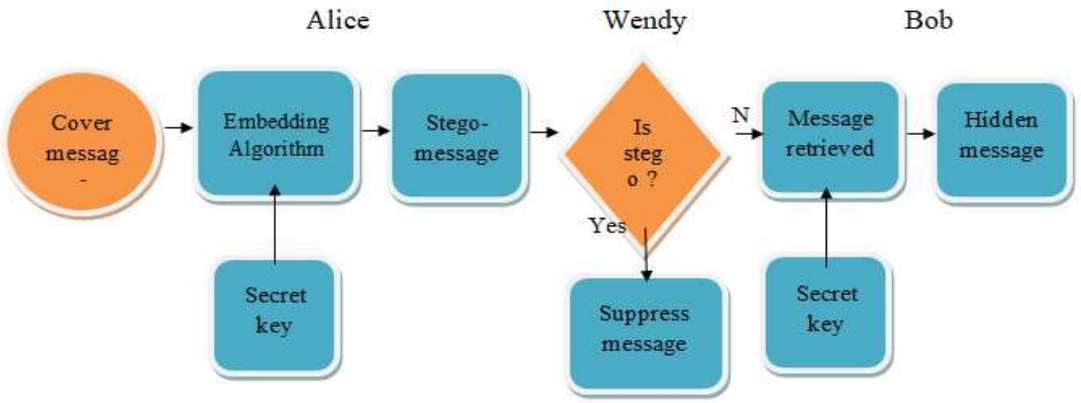


Figure (2.8) Frame Work for key Steganography

2.3.3 Steganographic protocols

In practice, there are basically three types of steganographic protocols used, Pure steganography, Secret key steganography and Public key steganography [12].

1. **Pure Steganography**

Pure steganography defined as a steganographic system that does not require exchange of a cipher such as a stego-key. This method is the least secure because the sender and receiver can rely only upon the presumption that no other parties are aware of this secret message. Using open systems such as the Internet, we know this is not the case at all.

2. **Secret Key Steganography:**

Secret key steganography defined as a steganographic system that requires the exchange of a secret key (stego-key) prior to communication. It takes a cover message and embeds the secret message inside it, and the process reversed to read the secret message using the secret key. Unlike Pure Steganography where a perceived invisible communication channel is

present, Secret key steganography exchanges a stego-key, which makes it more susceptible to interception. The benefit of this method is even if it was intercepted; only parties who know the secret key can extract the secret message.

3. **Public Key Steganography:**

   Public key steganography provides a more robust way of implementing a steganographic system because it can utilize a much more robust and researched technology in public key cryptography. It also has multiple levels of security in that unwanted parties must first suspect the use of steganography and then they would have to find a way to crack the algorithm used by the public key system before they could intercept the secret message.

2.3.4 Requirements for Steganography Algorithms

A steganography algorithm should be consistent over following properties and parameters [13]:

1. **Transparency:** The most fundamental requirement for any Steganography method shall be such that it is transparent to the end user. The Steganography content should be consumable at the intended user device without giving annoyance to the user. Steganography only shows up at the Steganography-detector device.
2. **Security:** Steganography information shall only be accessible to the authorized parties. Only authorized parties shall be able to alter the Steganography content. Encryption can be used to prevent unauthorized access of the Steganography data.
3. **Ease of embedding and retrieval:** Ideally, Steganography on digital media should be possible to perform "on the fly". The computation need for the selected algorithm should be minimum.
4. **Robustness:** Steganography must be robust enough to withstand all kinds for signal processing operations, "attacks" or unauthorized access. Any attempt, whether intentional or not, that has a potential to alter the data content is considered as an attack. Robustness against attack is a key requirement for Steganography and the success of this technology for copyright protection depends on this.
5. **Effect on bandwidth:** Steganography should be done in such a way that it does not increase the bandwidth required for transmission. If Steganography becomes a burden for the available bandwidth, the method will be rejected.

6. **Interoperability:** Digitally Steganography content shall still be interoperable so that it can be seamlessly accessed through heterogeneous networks and can be played on various plays out devices that may be Steganography aware or unaware.

2.3.5 Steganography Techniques

The effective steganography should have property of remaining intact irrespective of the tampering, the secret message should be invisible and it should go undetected. The capacity of the technique to hide the data should be well achieved. Many steganographic methods have been proposed in the past years. [14]

A. Spatial Domain Technique

Spatial domain steganographic techniques, also known as substitution technique, are a group of relatively simple techniques that create a covert channel in the parts of the cover-object in which changes are likely to be a bit scant when compared to the human visual system (HVS) and human auditory system(HAS). In this technique, the Least significant bit of every pixel of frames is used to hide the secret information bit. This method of steganography is simple and require less computational power.

B. Transform domain

In transform domain methods, the first step is to transform the cover image into different domain. The transformed coefficients are then processed to hide the secret information. Then these changed coefficients are transformed back into spatial domain to get stego media. The advantage of transform domain methods is the high ability to face signal processing operations. However, this type of methods is computationally complex.

2.3.6 Type of Steganography

Steganography can be classified into text, image, audio, video and protocol steganography depending on the cover media used to embed secret data. figure (2.10) takes look of these type, and will discuss this type on details.

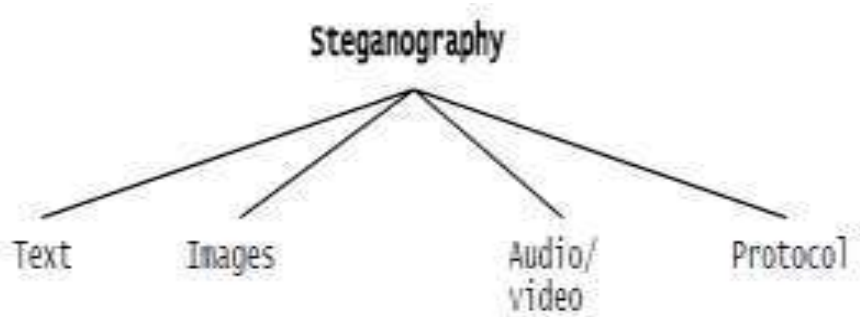


Figure (2.9)Type of Steganography [14]

1. **Plaintext Steganography**

Text steganography can involve anything from changing the formatting of an existing text , to generating random character that being readable texts . The techniques in text steganography are number of tabs, white spaces, capital letters, just like Morse code is used to achieve information hiding.[15]

Storing text file require less memory and its faster as well as easier communication makes it preferable to other types of steganographic methods. Text steganography can be broadly classified.

2. Image steganography

The most widely used technique today is hiding of secret messages into a digital image .In recent years, this steganography technique became more popular than others, possibly because of the flood of digital cameras and high-speed internet distribution . In this type, we can hide image into image or text into image. A picture can be represented by a collection of color pixels. Each of these characteristics can be digitally expressed in terms of 1s and0s.

RGB Images: An RGB image has three channels: red, green, and blue. RGB channels roughly follow the color receptors in human eye, and used in computer displays and image scanners. If the RGB image is 24-bit (the industry standard as of 2005), each channel has 8 bits, for red, green, and blue in other words, the image is composed of three images (one for each channel), where each image can store discrete pixels with conventional brightness intensities between 0 and 255. If the RGB image is 48-bit (very high color-depth), each channel is made of 16-bit images.

This steganography technique exploits the weakness of the human visual system (HVS). HVS cannot detect the variation in luminance of color vectors at higher frequency side of the visual spectrum.

3. Audio steganography

A steganography technique that uses audio as a cover, called audio steganography.one of the properties being excessively used for concealing the secret information in audio files is that they have large space. In audio steganography, the cover is an audio and the secret information can be a text file, an image or an audio. audio steganography techniques are explored taking cover audio in WAV and MP3 format. WAV files produce integer samples and MP3 files give floating point numbers as samples. the audio files are available in various

file formats.WAV file is the simplest format. Unlike MP3 and other compressed formats. It is the most challenging task in steganography, because the human auditory system (HAS) has a large dynamic range can be listen over. Thus, the human ears can detect even a minute change in audio quality. In fact, the availability and the popularity of audio files make them eligible to carry hidden information. In addition, most steganalysis efforts are directed towards digital images leaving audio steganalysis relatively unexplored.

4. IP datagram steganography

This is another approach of steganography, which employs hiding data in the network datagram level in a TCP/IP based network like Internet. Network covert Channel is the synonym of network steganography. Overall goal of this approach to make the stego datagram is undetectable by Network watchers like sniffer, Intrusion Detection System (IDS) etc. In this approach information to be hide is placed in the IP header of a TCP/IP datagram. Some of the fields of IP header and TCP header in an IPv4 network are chosen for data hiding.

5. video steganography

This technique hides information in the video signal. Video files are a combination of images and audio files.is used to overcome the problem of capacity because it is a collection of images and audio. Any image or audio signal can be used for hiding data. As the information in video signal flows continuously, small distortion in the original file might not be observed by humans. The main advantage of using video signal is the huge size which can hide large amount of data without noticeable distortions. The use of video files as a carrier medium for steganography is more eligible when compared to other techniques.

2.4 Comparisons of Different common Steganographic Techniques

The scientific paper "Information Security through an Improved Image Steganography Algorithm " shows difference between types of Steganography

Table (2.2) Comparisons of Different common Steganographic Techniques [16]

Technique	**Security**	**Capacity**	**Transparency**	**Integrity**	**Temper resistance**	**Robustness**
Text steganography	High	Low	Low	Low	High	Low
Image steganography	High	High	Low	High	High	High
Audio steganography	Low	Low	Low	Low	High	Low
Video steganography	High	High	High	Low	High	Low

2.5 Least Significant Bit

Least significant bit is used for embedding secret information in a cover video least significant bit (LSB) insertion is a simple approach for embedding information in a cover video. Video is converted into a number of frames, and then convert each frame into an image. The least significant bit (i.e. the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message.

In each of the Red, Green and Blue color components can be used, since they are each represented by a byte. In other words, one can store 3 bit in each pixel. [17]

In 24-bit image, a bit of each of the red, green and blue color components can be used, since they are each represented by a byte. For example, a grid for 3 pixels of a 24-bit image can be as follows:

(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)

If the number 200, the binary representation is 11001000, is embedded into the least significant bits of this part of the cover image, then the resulting grid is:

(00101101 00011101 11011100)
(10100110 11000101 00001100)
(11010010 10101100 01100011)

So if the number was embedded into the first 8 bytes of the grid, only the three underlined bits needed to be changed according to the embedded message. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size.

The secret data is placed in the least significant bit of the frame it is not easy for the human eye to detect the message.

2.6 Discrete Cosine Transformation (DCT)

Main aim of this method is to increase the payload capacity while keeping the robustness and simplicity intact and is widely used. It transforms a time domain signal into its frequency components. Many frequency coefficients are obtained from DCT, such as single direct current DC coefficients, low frequency coefficients, mid frequency coefficients, and high frequency coefficients. The JPEG compression technique utilizes this property to separate and remove insignificant high frequency components in images and embedding the secret message in it. it avoids the most visual important parts of the image without over exposing themselves through compression and noise attacks. In this method, DCT coefficients of I-frames are computed and then secret information is embedded by performing modulation between quantized DCT coefficients and secret information. This proposed technique showed robustness against steganalysis methods by exploits the blocks with high complexity for hiding and precludes the one with the low complexity to reduce the statistical modifications thus, provides high security. Hence, the primary focus for this work was on security [18].

2.7 compression between LSB and DCT techniques

The scientific paper "A Survey on different techniques of steganography "discusses the differences between LSB and DCT technology.

Table (2.3) compression between LSB and DCT techniques [10]

Techniques	Domain	Invisibility	Capacity	Detectability	Robustness	Complexity	Comments
LSB	Spatial	High	High	High	Low	Low	Independent of image format and Texture
DCT	Transform	High	Medium	Low	Medium	Medium	Simplest in the transform domain

2.8 compression between Cryptography and Steganography

The table below shows the differences between the steganography and cryptography using some criteria. The comparison is based on, definition, objective, carrier, input file, key, visibility, security services offered, type of attack, attacks, result and applications.

Table (2.4) compression between Cryptography and Steganography [25]

Criteria/Method	**Cryptography**	**Steganography**
Definition	Secret writing	Cover writing
Objective	Maintaining contents of a message secret ,Data protection	Maintaining existence of a message secret ,Secret communication
Carrier	Usually text based	Any digital media
Input file	Necessary	Optional
Visibility	Always	Never
Security services	Confidentiality,	Authentication,

offered	Identification, Data Integrity and authentication Nonrepudiation	Confidentiality, Identification
Type of Attack	Cryptanalysis	Steganalysis: Analysis of a file with an aim of finding whether it is stego file or not
Attacks	Broken when attacker can understand the secret message. known as Cryptanalysis	Broken when attacker reveals that steganography has been used. known as Steganalysis.
Result	Ciphertext	Stego file
Applications	Used for securing information against potential eavesdroppers	Used for securing information against potential eavesdroppers

2.9 Security analysis

The attacks on security systems aim to find weakness in information hiding techniques. This is also referred to as breaking. One of the most common example of breaking the security code is brute force approach. To break the security lock of 3-digits, it simply needs 1000 combinations. There are two terms for finding the weakness and trying to break-through the code: cryptanalysis and steganalysis.

2.9.1 Steganalysis

Steganalysis is the discovery of the existence of hidden information, hidden using steganography. This is analogous to cryptanalysis and cryptography. The goal of steganalysis is to identify suspected packages, to determine whether they have a message encoded into them, and to try and gain access to that message. It differs from cryptanalysis in the sense that the existence of message is obvious in cryptanalysis, that is one knows that the signal contains encrypted data. Whereas in case of steganalysis, the steganalyst starts with a pile of

suspect data and then try to determine whether it contains encrypted message and then retrieving the message.

1. Stego-only attack –in this type of attack, only the stego media (i.ethe medium containing hidden data) is available for analysis.
2. Known carrier attack –in this type of attack, the steganalyst has access to both the target object which is used for hiding information and the stego object that contains the hidden information. The stego media or stego object is compared with the cover object and the differences are detected. For example: the original image and the image containing the hidden information are available and compared to deduce the message.
3. Known message attack –in this, the original message prior to embedding in the carrier is known. This attack is the analysis of known patterns that correspond to hidden information. This type of analysis can help against attacks in the future. Even with the message available, this type of attack may be very difficult and considered same as stego-only attack.
4. Chosen stego attack –in this attack, the algorithm used for hiding information and the stego object, that is the final hidden file is known and available for analysis.
5. Known stego attack –in this type of attack, the steganography algorithm, the original file and the stego object is known, that is, all the components are available for analysis

2.9.2 Cryptanalysis

Cryptanalysis is the study of analyzing information systems in order to study the hidden aspects of the systems. In other words, it is the art of deciphering encrypted communication without knowing the proper keys. It is used to breach cryptographic security systems and to gain access to the encrypted messages. Breaching the security in this way involves knowing how the system works and finding a secret key. Cryptanalysis is the attempt to circumvent the security of various types of cryptographic algorithms and protocols. Types of cryptanalysis attacks:

1. Cipher text only attack –in this, the attacker has access only to a set of ciphertexts. The aim is to deduce plaintexts maybe by making assumptions and guesses.
2. Known plain-text attack -In this, the cryptanalyst has knowledge of a portion of the plaintext from cipher text. The attempt is to deduce key to decrypt the rest of the ciphertext.

3. Chosen-plaintext attack –this is also known as chosen-cipher text attack or differential cryptanalysis. In this, the cryptanalyst has the ability to choose plaintexts arbitrarily to be encrypted and obtain the corresponding ciphertexts. The cryptanalyst aims to deduce the key by comparing the entire ciphertext with the original plaintext.
4. Cipher-text only analysis –In this, the cryptanalyst has no knowledge of the plaintext and must work only from ciphertext. It requires guesswork to know what the message can be. Any type of prior knowledge about ciphertext, the sender or the topic in general can be helpful.

2.10 Related Works

2.10.1 Zeyad ed.al .[19] the proposed a method for data hiding in video by utilizing the least significant bit (LSB) method and improving it by utilizing the knight-tour algorithm for concealing the data inside the AVI video file and using a key function encryption method for encrypting the secret message. First, the secret message is encrypted by utilizing a mathematical equation. The key used in the equation is a set of random numbers. These numbers differ in each implementation to warrant the safety of the hidden message and to increase the security of the secret message. Then, the cover video was converted from a set of frames into separated images to take the advantage of the large size of video file. Afterward, the knight tour algorithm is utilized for random selecting of the pixels inside the frame utilized for embedding the secret message inside it to overcome the shortcoming of the conventional LSB method that utilized the serial selection of pixel and to increase the robustness and security of the proposed method. Afterward, the encrypted secret message is embedded inside the selected pixels by utilizing the LSB method in bits (7 and 8). The observational results have drawn that the proposed method has a superior performance compared to the previous steganography

This method preserves the security where the secret message cannot be drawn out without knowing the decoding rules. [19]

2.10.2 Prof.Dipt Mukadam ed.al [20] Emergence of internet has made it possible to transfer the data from one place to another place rapidly and accurately. This data

when goes through the internet may become a victim of the hackers who can steal, modify and misuse the information. Therefore it is necessary to transfer the data with almost security. The steganography is the art of hiding message inside another medium such as Video, Image, Audio. In this paper, combination of cryptography and steganography is used for data hiding in video clips. This project focuses on the data security approach when combined with encryption and steganographic techniques for secret communication by hiding it inside the multimedia files provides a high level of security. The files composed of insignificant bits or unused areas which can be used for overwriting of other data.

In this paper we presented several types of hiding the secret data inside the cover medium such as image, audio, video. The proposed system for data hiding uses AES for encryption and LSB for Steganography which results in more secure technique for data hiding.We can conclude that the proposed system is more effective for secret communication over the network channel.

2.10.3 Syed juwairah ed.al [21] The progression of entrenching the information into the digital carrier signal is known as steganography. The information that is send remains secure from any unauthorized access if the concept of steganography is applied to the transferred data. Various Stenographic techniques related to the video steganography have been proposed earlier but the security of the system was not achieved as required. So in this paper a new method of video steganography is introduced in which the encryption algorithms have been used. Before embedding the data into the carrier signal, the data is firstly encrypted with the help of the encryption algorithm .In this approach the DES (Data Encryption Standard) algorithm is used for the data encryption and LSB i.e. Least Significant Bit mechanism is used to embed the data behind the cover video frames. The proposed work achieves the high level security to the embedded data. From the results obtained it is concluded that proposed algorithm is better and efficient than the traditional algorithm of the video steganography as the security is increased. It is bring to the front that the results obtained after implementing the proposed work posses more efficiency as compare to the traditional work.

2.10.4 Mumthas sa ed.al [22] Now a days digital communication is a large pool of information and so its security and privacy are very sensitive and vital characteristics of the system. As far as success of any event is concerned, the keystone is effective and safe communication. We are presenting here a novel approach wherein RSA, random DNA encryption, Huffman encoding and DCT steganography method. to give a system with guaranteed three levels of security. As compared to existing methods, the new approach is found to improve the quality of steganographic system and deciphering the codes will be much more cumbersome. Furthermore, security of the proposed algorithm has been improved because of adding randomness to usual DNA encryption. All these advantages make any valuable communication more secure and that itself is the ultimate aim of transmission of vulnerable information.

2.10.5 Naveen Chandra Gowda ed.al [23] the target of this venture is to obtain secured encryption and authentication using steganography. So as to accomplish this, numerous organizations & universities in the world have given solutions to secured communication, in the interim many algorithms have been created, including like AES, RSA, LSB etc. But though these algorithms have been developed they were endured to breakdown by hackers which make them obsolete. In this paper we try to combine many already existing algorithms like AES, LSB into one proposed system. Firstly, the utilization of steganography along with traditional encryption is implemented in the proposed system. Second, we try to achieve authentication of user using OTP (The One Time Password) via E-mail , the OTP will be generated and shared to the clients, which will be used for authentication at entry level. Thirdly, the encrypted data is divided and sent across many servers so it's impossible to get complete encrypted data in one path. By applying the proposed model, the probability of data compromise becomes very minimal and very hard to hack. In the end every security system becomes obsolete and cannot be failsafe so its required to keep upgrading our security through new policies, new schemes. Our system aims to combine all the existing algorithms together and provide more secure system.

2.10.6 Sri Ram Polisetty ed.al [3] Steganography is the art of hiding data within data where it is an encryption technique that can be used along with cryptography as an extra-secure technique to secure data. The security of information can be prospered by using encryption and steganography. In cryptography, at first the original form of data is encrypted into another form and then it is transferred. The proposed system improves the security system by combining these two techniques. In this system, the encrypted data is sssembedded in a BMP/JPEG image file and intends for data confidentiality, data authentication and data integrity. Data is encrypted with RC4 encryption algorithm and then embedded the encrypted data in the BMP/JPEG image file using LSB steganographic method where the primary goal of this system could be attained. By comparing the existing and proposed systems the second objective is achieved. More over the proposed system is more secured than the existing one by making use of embedded RC4 and LSB techniques. [3]

2.11 Summary of related work

Table (2.5) summary of related work

	Paper name	date	Publisher/author	Techniques
1	Video Steganography using Knight Tour Algorthim and LSB Method for Encrypted Data	2020	J. Intell. Syst / Zeyad Safaa Younus and Ghada Thanoon Younus	utilizing the least significant bit (LSB) method and improving it by utilizing the knight-tour algorithm for concealing the encrypted data inside the AVI video file. And mathematical equation for encryption
2	secure data Transfer using video Steganography	2018	International Journal of pure and Applied Mathematic/ [1]Prof. Dipti Mukadam, [2]Sunita Mahale and others	combination of cryptography and steganography that used AES for encryption and LSB for steganography
3	Secure Data	2018	International	method of video

	Transmission Based On Combined Effect Of Cryptography And Steganography Using Visible Light Spectrum		Journal of Pure and Applied Mathematics/ [1]Syed Juwairah Indrabi, [2]Neha Saini, [3]M. Mohan	steganography is introduced in which the encryption algorithms have been used DES. Before embedding the data and for embedding used LSB
4	Transform Domain Video Steganography Using RSA, Random DNA Encryption and Huffman Encoding	2017	7th International Conference on Advances in Computing & Communications/[1] Mumthas Sa, [2]Lijiya Ab	presenting here a novel approach where in RSA, random DNA encryption, Huffman encoding and DCT steganography method
5	Steg Crypt (Encryption using steganography)	2019	International Journal of Engineering and Advanced Technology/ [1]Naveen Chandra Gowda, [2] P. Sai Venkata Srivastava and other	combine many already existing algorithms like AES, LSB into one proposed system. And achieve authentication of user using OTP (The One Time Password) via E-mail
6	A NOVEL APPROACH TO THE INFORMATION SECURITY USING RC4 AND LSB TECHNIQUES		Journal of Emerging Technologies and Innovative Research (JETIR) /[1]Sri Ram Polisetty, [2]Niharika Tangella and others	combining two techniques encryption and steganography, RC4 for encryption and LSB for steganography

2.12 Differentiate from previous research

The research proposal agrees with previous researches in the use of two levels of data security, there is encryption and steganography, but the proposal of this work differs from the previous works by using two hidden functions of steganography.

also there is additional feature it is distributing the encrypted text on the video frame and selecting even-frames.

CHAPTER THERE
SYSTEM DESIGN

CHAPTER III

SYSTEM DESIGN

3.1 Introduction

This chapter describe techniques that have two levels of security, the first level includes encryption and another level is steganography that development a method of video steganography which was worked in both spatial and transform domain all that are combined with each other to provide a secure transmission system.

this chapter will also discuss the technical information about security algorithms, including the methods that are used in encryption and steganography, the structure of the system and data flow diagram

3.2 System Technique

The technique that will be used in the system it IDEA for encryption and LSB and DCT for hiding data in cover video.

3.2.1 IDEA algorithm

IDEA is best known as the block cipher algorithm used within the popular encryption program PGP. In generally it considered to be very secure. It provides high level security not based on keeping the algorithm a secret, but rather upon of the secret key. IDEA fully easily understood and available to everybody also it suitable for use in a wide range of applications. IDEA can be economically implemented in electronic components and can be used efficiently.it patent protected to prevent fraud and piracy and completely avoided using of any substitution boxes(s-box) and the associated table lookups used in the block ciphers.

3.2.2 LSB technique

Least Significant Bit it a common steganography techniques. This technique is very efficient because of its simplicity and its ability to be undetectable to the naked eye. LSB coding technique has the advantage of low computational complexity. By this technique, least significant bits of the individual pixels of carrier files are changed with the message bits.

3.2.3 DCT technique

Discrete Cosine Transform DCT is one of the most popular frequency transformations in image and video processing due to its simplicity and high energy compaction. It also very efficient and Reduce the storage

3.3 Implementation details

The project was design, executed and tested under the following environment: ASP.NET platform and Windows 10 with 64-bit operating system. The system branch of the following modules: encryption, embedding text in frames, extracting frames and decryption.

3.3.1 Encryption

This module provides the text encryption functionality using IDEA cipher. The key generate at the user device this resolves the key distribution issue cause no keys will exchange. The key is “master” it 128 bits. After the key generated, a user write the text or upload document to be encrypted using the key. The result will be encrypted text or document.

3.3.2 Embedding text in frame

This module provides to hide data in side media. User has ability uploading video. Uploaded video was read and separate audio from video and then extract frames , from these frames only even frames was taken depend on mathematical equation. In this frames, the encrypted text will be hidden using LSB technique that applying in 24-bit image and read the high and width of each frames each pixel is represented in three byte.

Data concealed in three bits into each pixel, each pixel is linked with a color. basic color (red ,green and blue) was effected it replace least significant bit of those colors with secret massage.

After applying LSB in selected frames DCT also will apply in same selected frames. The frames or images were broken into 8x8 block it worked from left to right and top to bottom, the DCT applied to each block. Then the extracted frames and audio are recovered into a video and play video. all this process happen in sender side and then send the video file.

3.3.3 Extracting frames

In receiver side, the recipient receives the sent message. firstly the recipient plays the video, and then extracts the images or frames from the video.it takes even-frames that carry the secret data and applied in those extracted frames IDCT and next step apply inverse LSB in same extracted frames and obtained the encrypted text.

3.3.4 Decryption

After obtained the secret data the receiver use the same key used in sender side to get the original massage.

3.4 Data flow diagram

3.4.1 Embedding Algorithm

Embedding algorithm work with the following steps:

1. Select the file of secret message.
2. Insert ciphering key and apply the ciphering algorithm to get ciphered message.
3. Select cover video.
4. Read video information.
5. To reconstruct the video correctly, video and audio signals must be separated from each other in container, the embedding process will be in video frames and the audio will be added back later, if it was silent, so there is no audio signal to separate, the process will continue directly.
6. Get frames from the container.
7. Embedding data in frames.

Reconstruct the video from frames and audio signal with message embedded inside it. As show in figure (3.1)

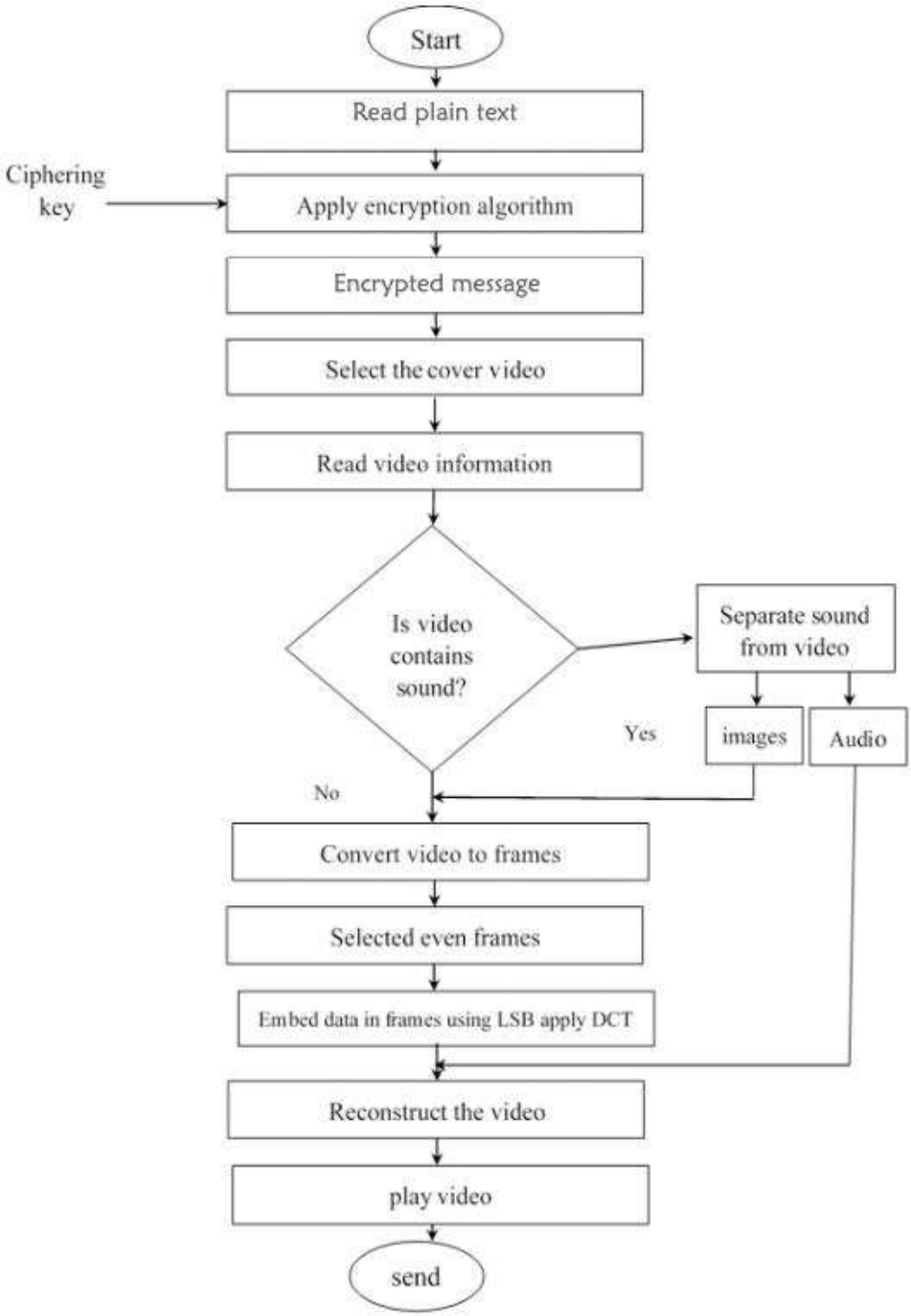


Figure (3.1) Embedding Algorithm

3.4.2 Extracting Process

The extracting algorithm is consisted of the following steps as shown in figure (3.2) below:

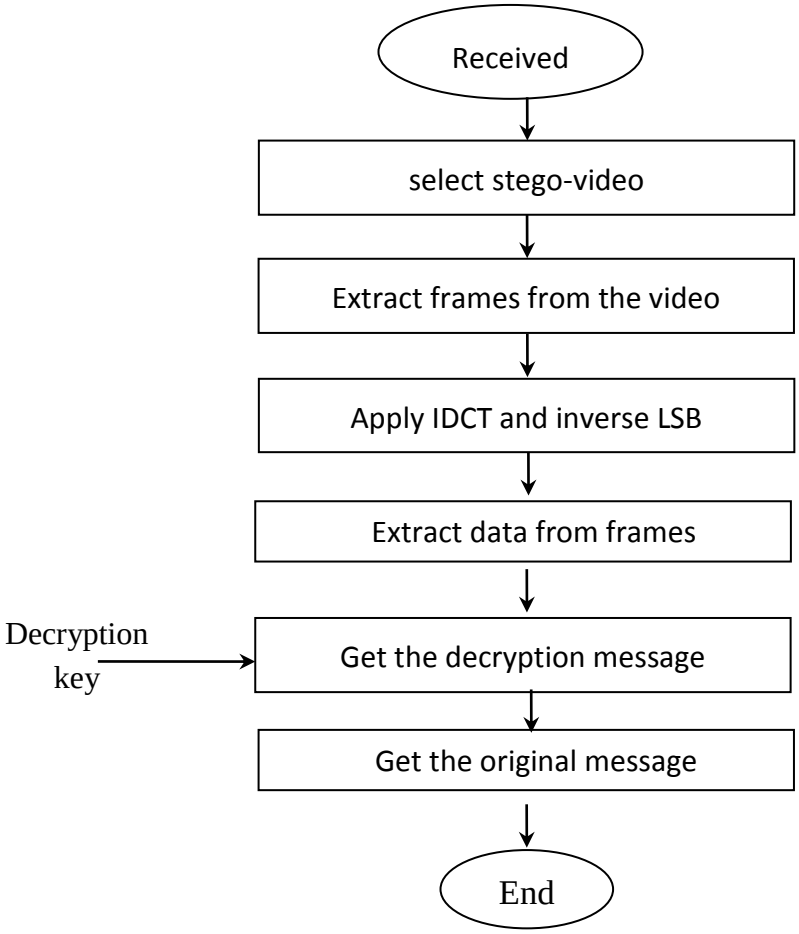


Figure (3.2) Extraction Algorithm

Extracting algorithm work with the following steps:

1. The user selects stego-video that contains the secret message.
2. The program extracts all video frames, and applies IDCT and inverse LSB.
3. Extracting data from the frames.
4. Get deciphering key from the user and use it decipher the message and save it a text file.

CHAPTER FOUR
IMPLEMENTATION

CHAPTER IV

IMPLEMENTATION

4.1 Introduction

In this chapter the implementation of the proposed system is introduced the screen shots show all process that happen during the system. System implementation hide text data in video-frames file, a software program has been developed using ASP.NET, this program consist of two parts:

1. Embedding program: this part converts plaintext to ciphertext and embedded in the video-frames file,
2. Extracting program: this part extracts data from the video-frames and obtained the secret message to retrieves the original massage.

4.2 system Implementation

This section contain figures of all system process.

Figure (4.1) and (4.2) clarifies login process that allowed only authentication user to enter the system using User name and Password then press on Login Button to entry the system.

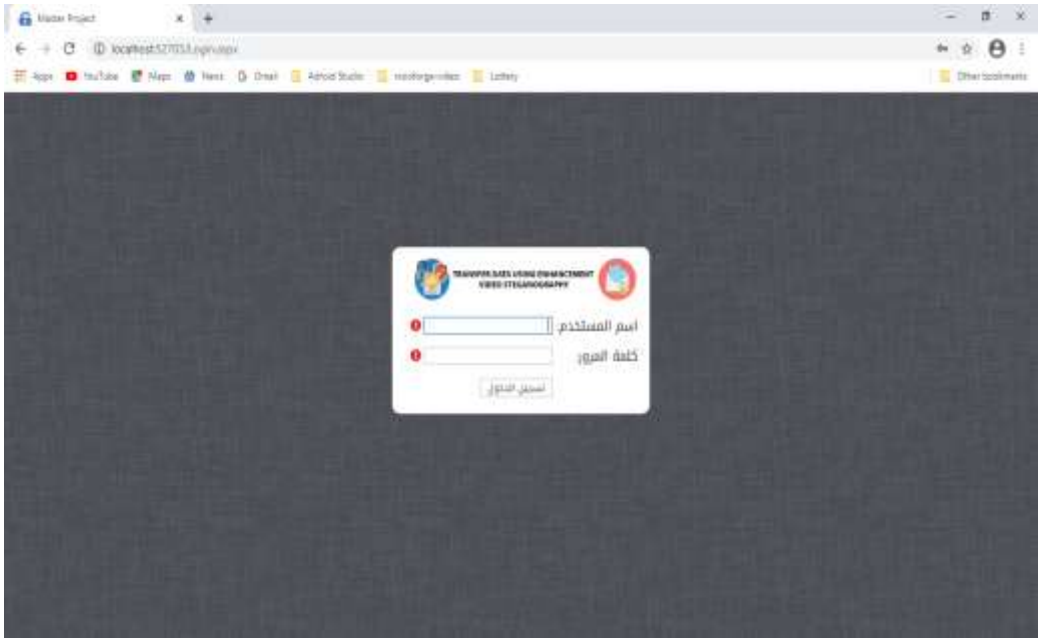


Figure (4.1) system login validation

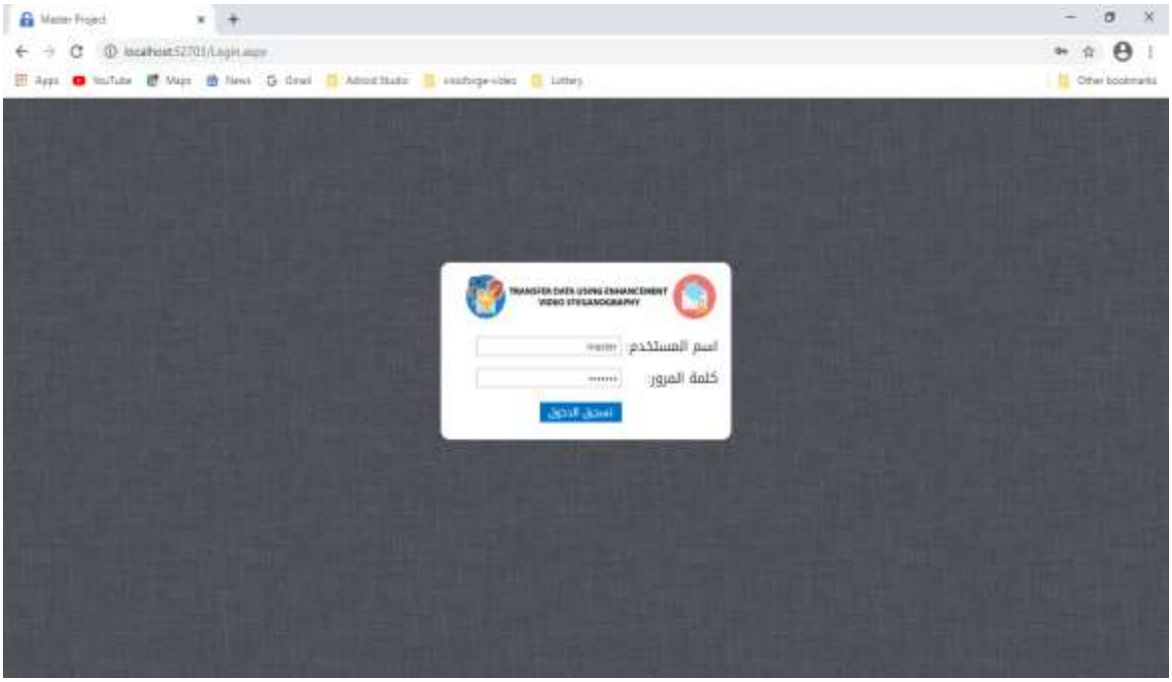


Figure (4.2) system login

4.2.1 Sender side procedures

Figure (4.3) show the sender side that have two tabs one for encryption process and another tab for steganography. In tab's encryption it allows the sender to write text message in the specified field, for more feature, it also able to select text file to be uploaded as show in figure (4.4).after uploading file the system notify that process complete successful as show in figure (4.5).

The system read the entire message and then convert the plain-text message to encrypted-text using IDEA cipher that display in figure (4.6).

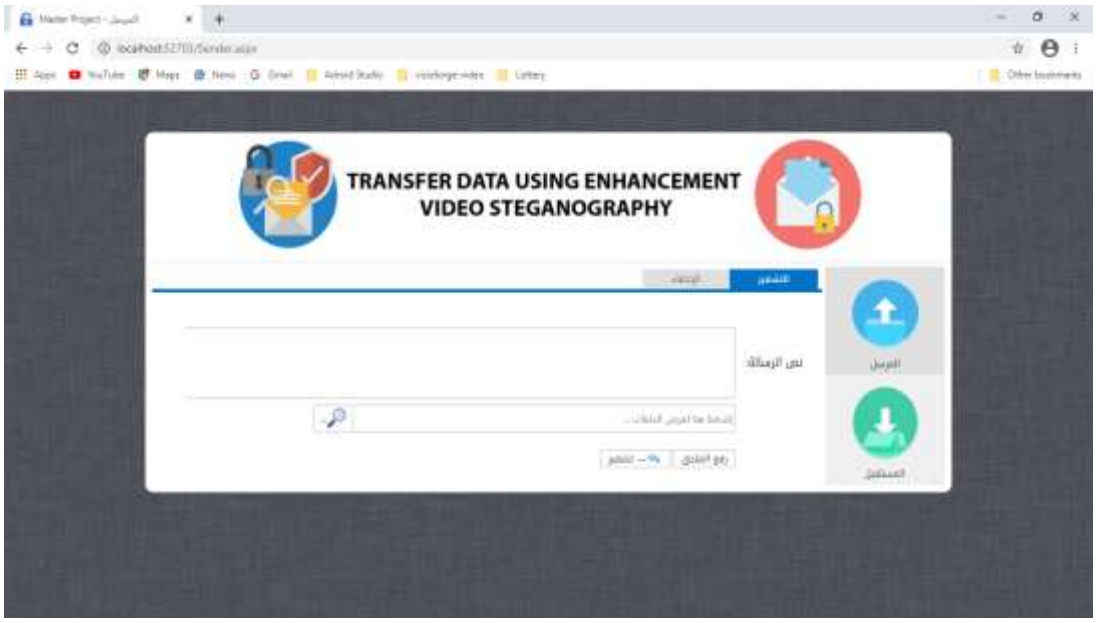


Figure (4.3) screen of the sender side.

Figure (4.4) selection of uploading file

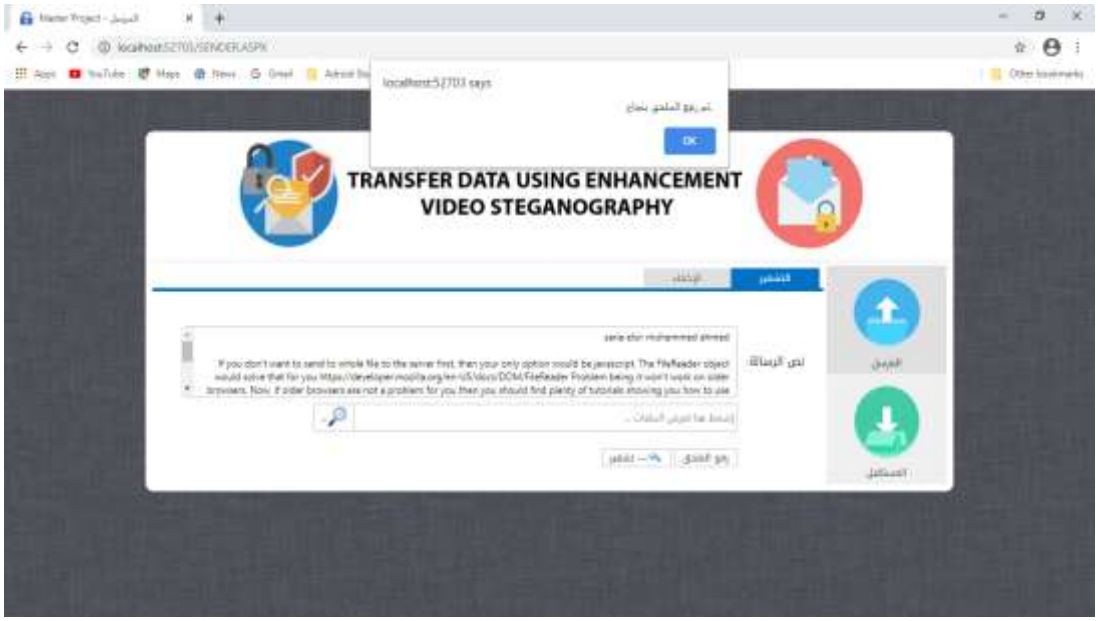


Figure (4.5) complete process of uploaded file

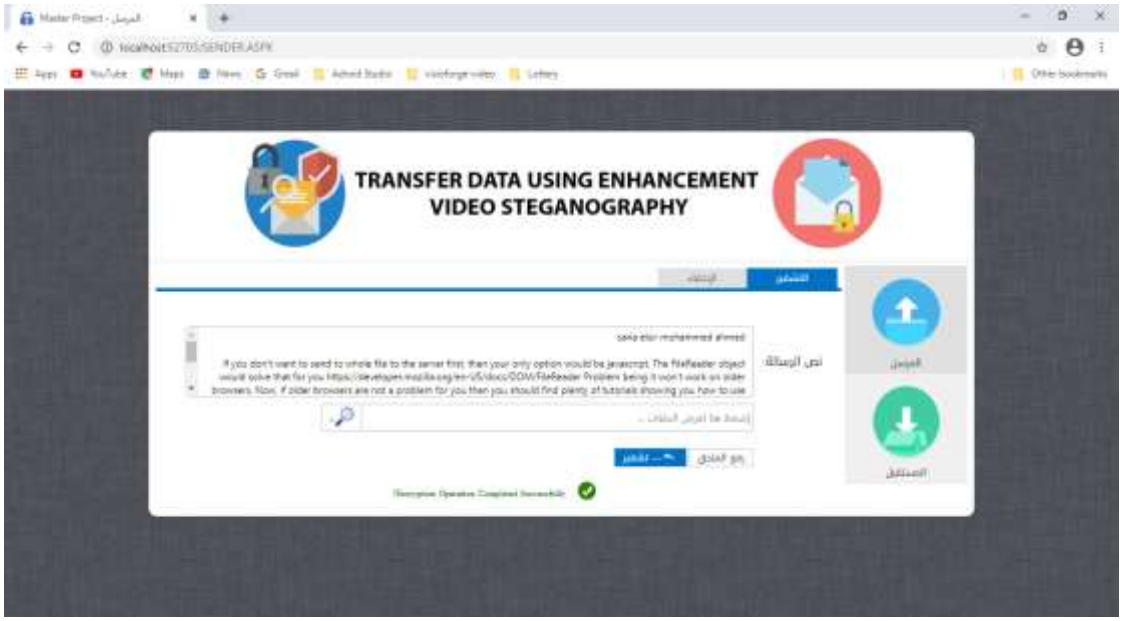


Figure (4.6) process of encryption in front

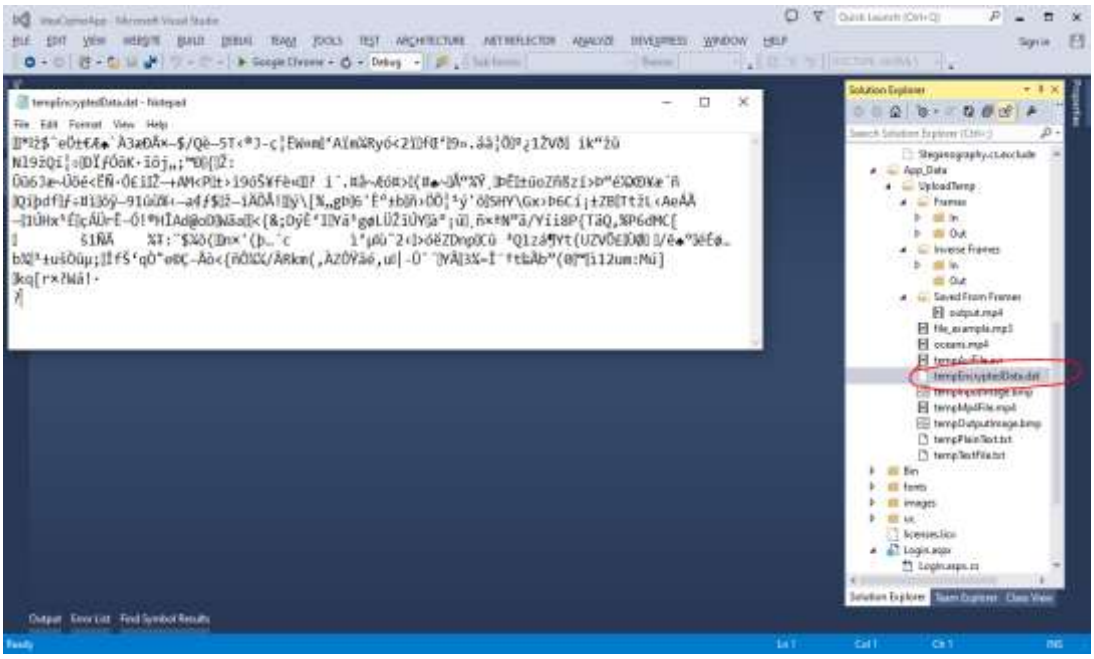


Figure (4.7) process of encryption in background

Tab two in sender screen is steganography that is second level of security.as show in figure (4.8).

Firstly, the sender select the video file to upload, the system gives user notify when upload process complete successfully, the sender can change selected file by press in new button .

Secondly, the uploaded video file will extract to image-frames. After extracting image-frames from a video, hence LSB and DCT techniques will apply to specific selected frames to hide secret massage in image-frames.

Third, after applying LSB and DCT techniques the result is stego-frames.

After that the stego-frames construct in the video file and sent to the receiver. all these processes show in below figures.

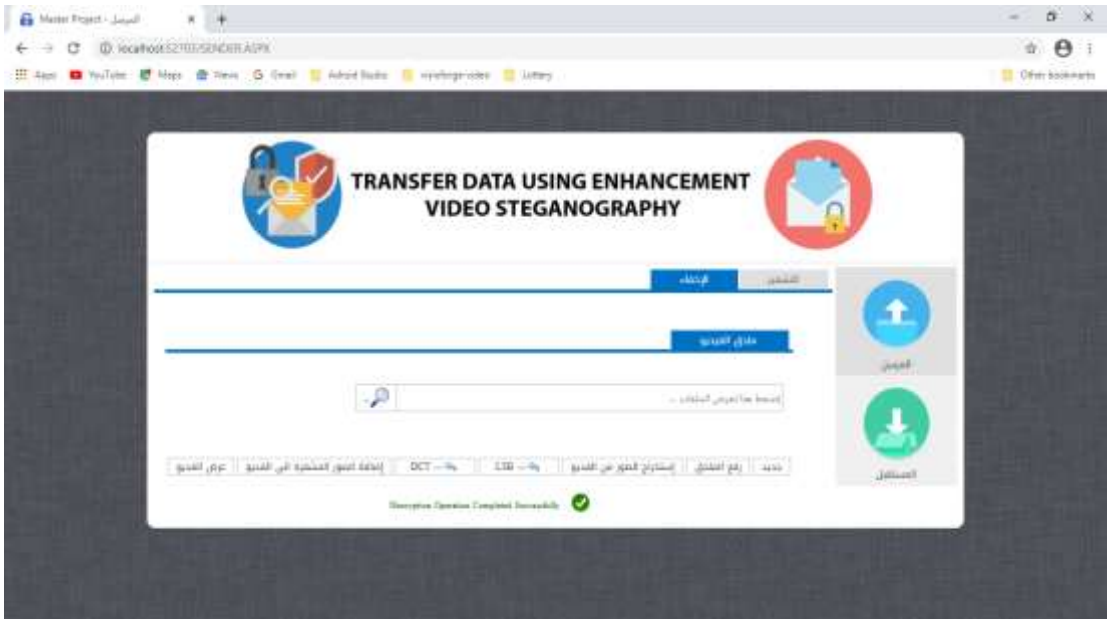


Figure (4.8) steganography screen

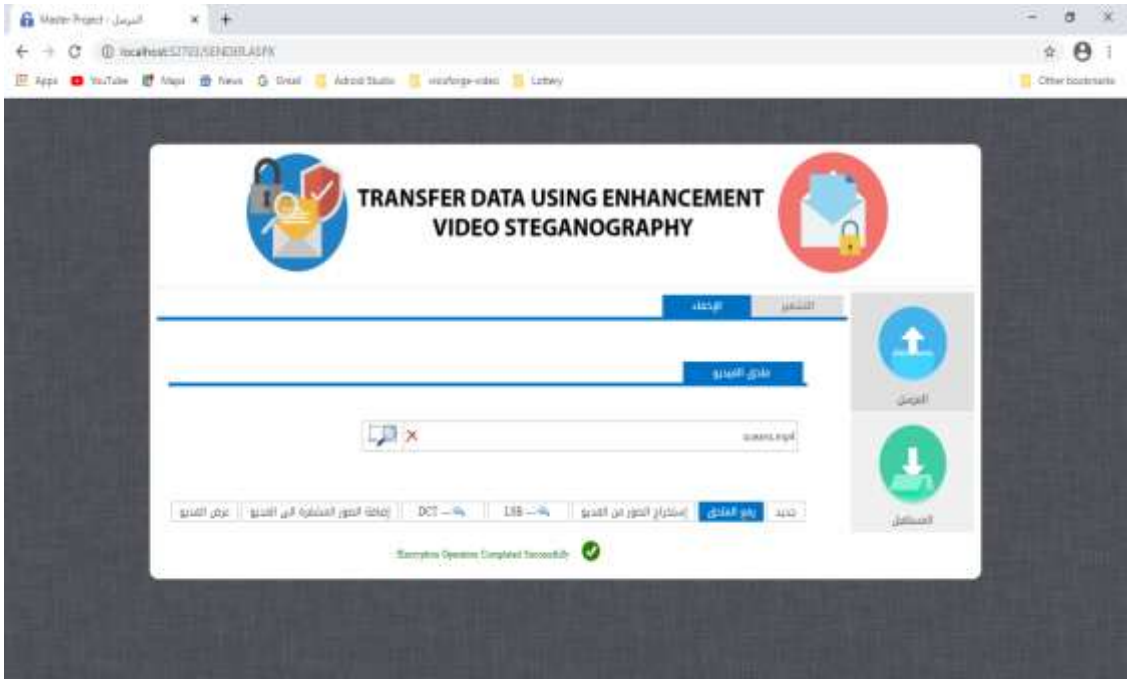


Figure (4.9) upload video file

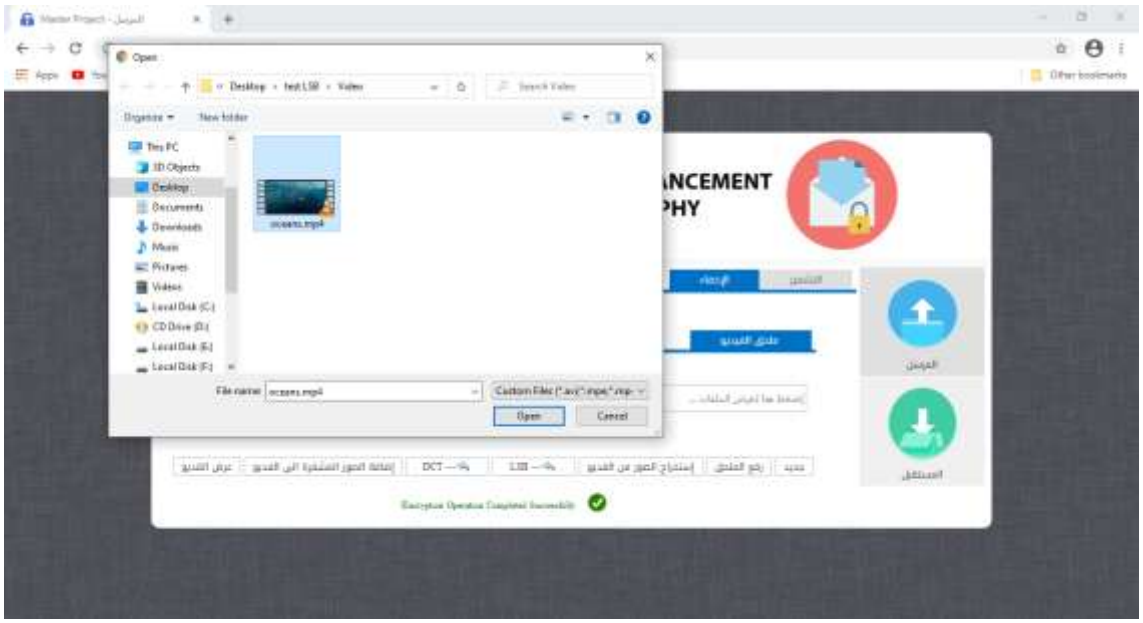


Figure (4.10) selecting video file

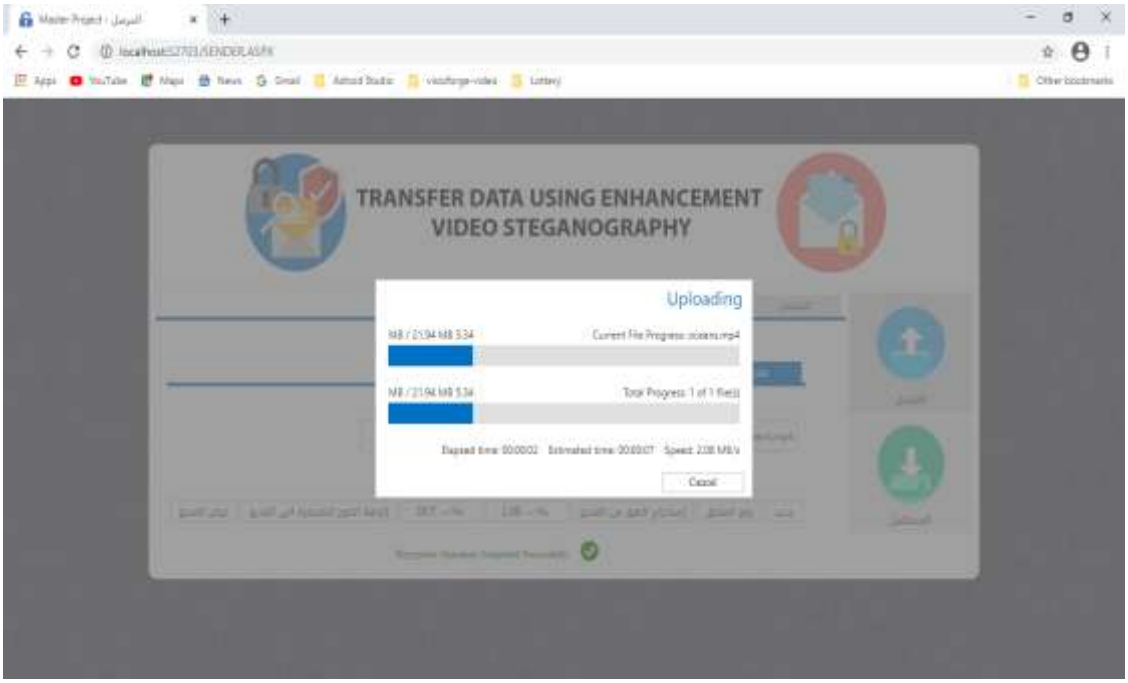


Figure (4.11) uploading for selection video file

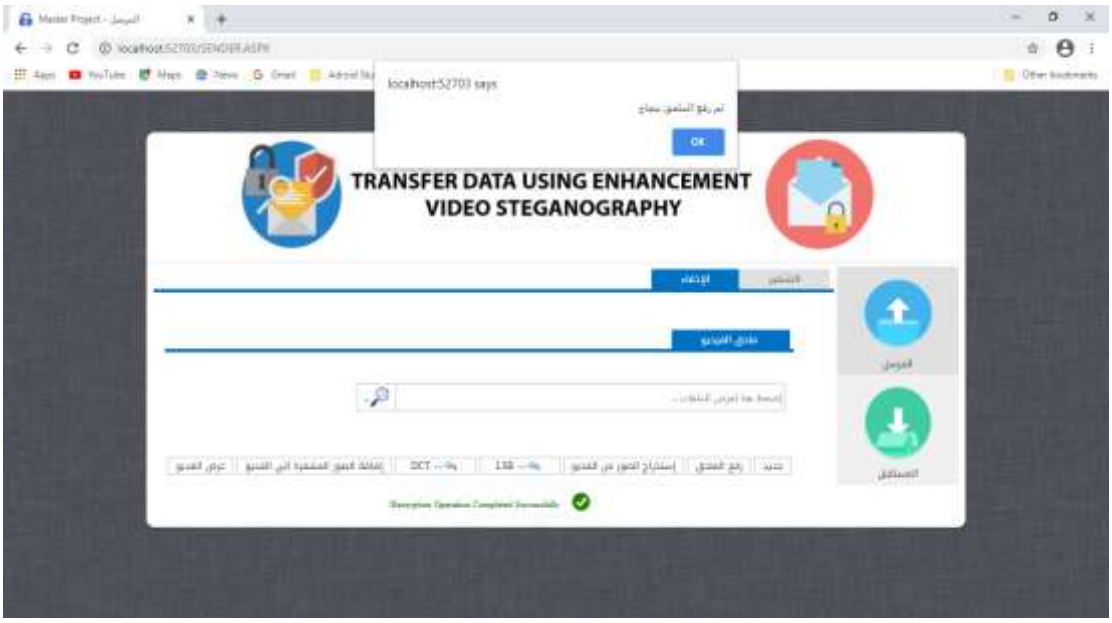


Figure (4.12) selected video file has been uploaded

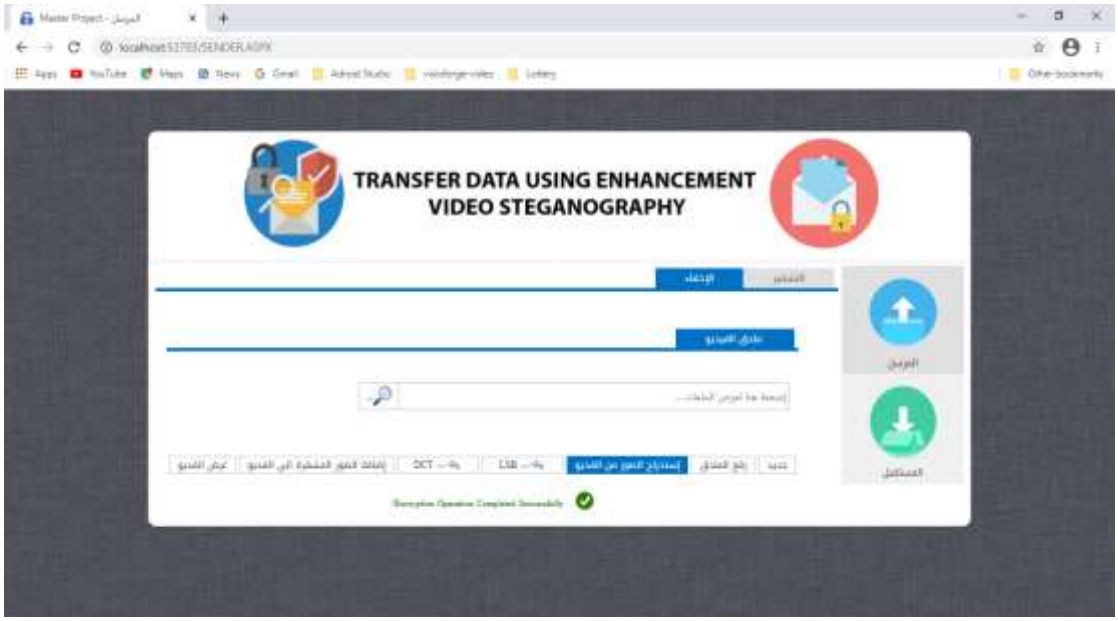


Figure (4.13) extract image button from video

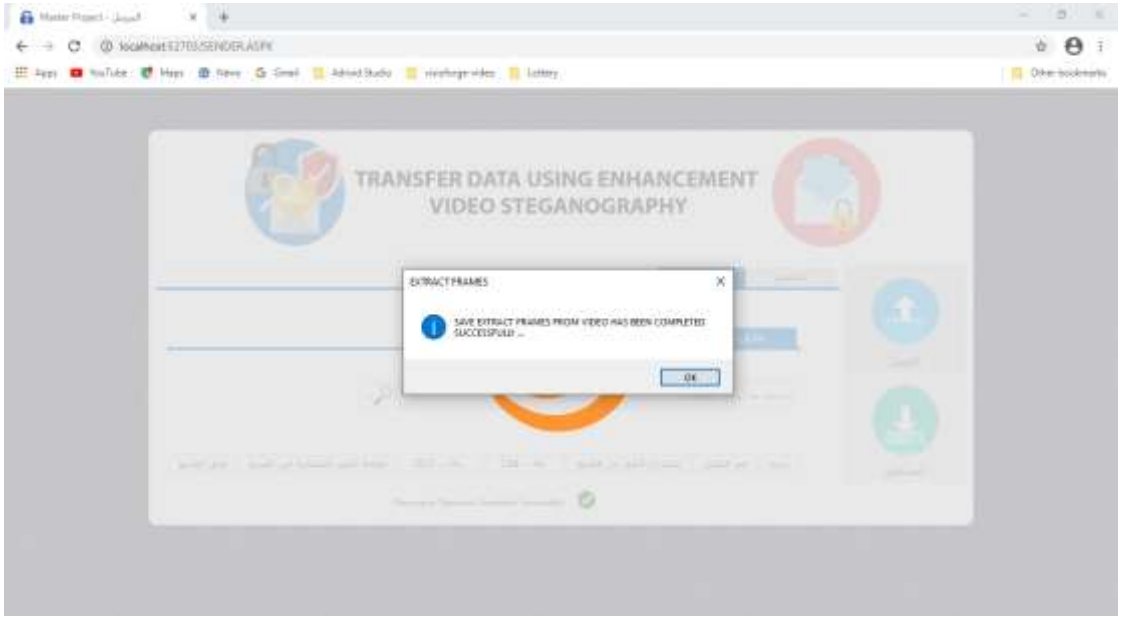


Figure (4.14) extracting process

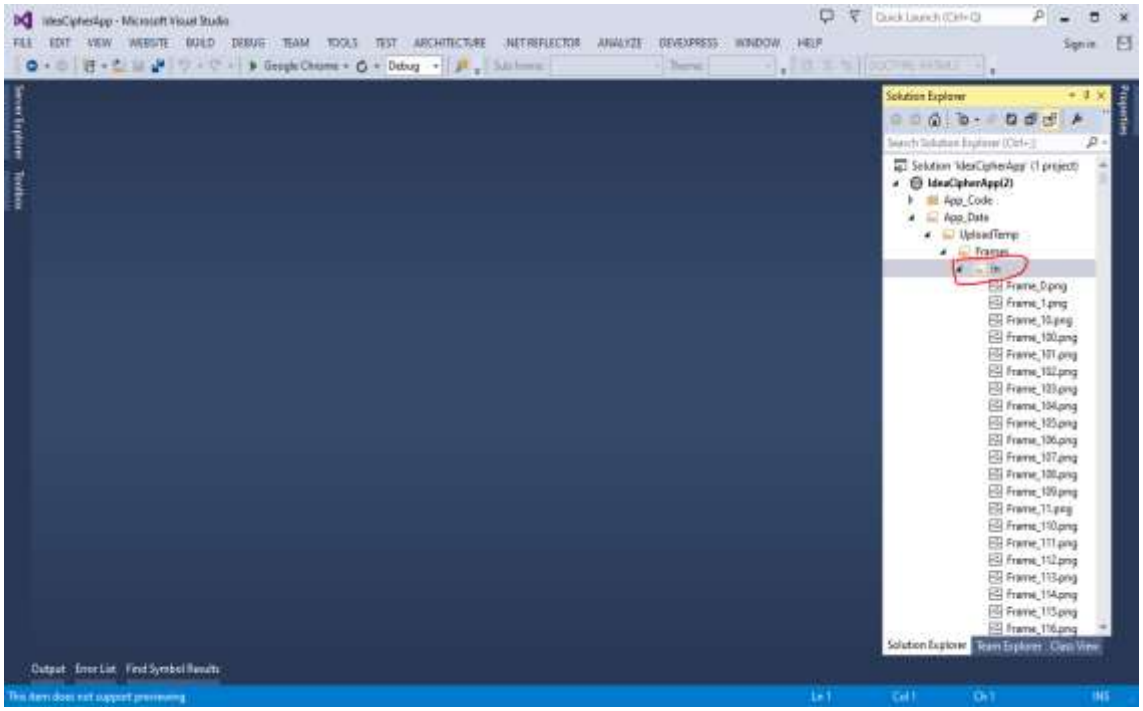


Figure (4.15) extracting frame in background

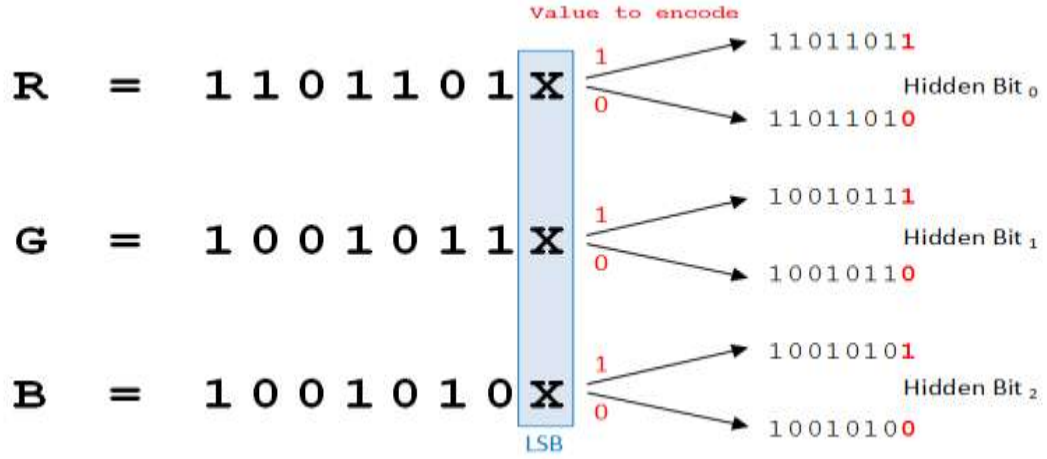


Figure (4.16) Example of LSB techniques

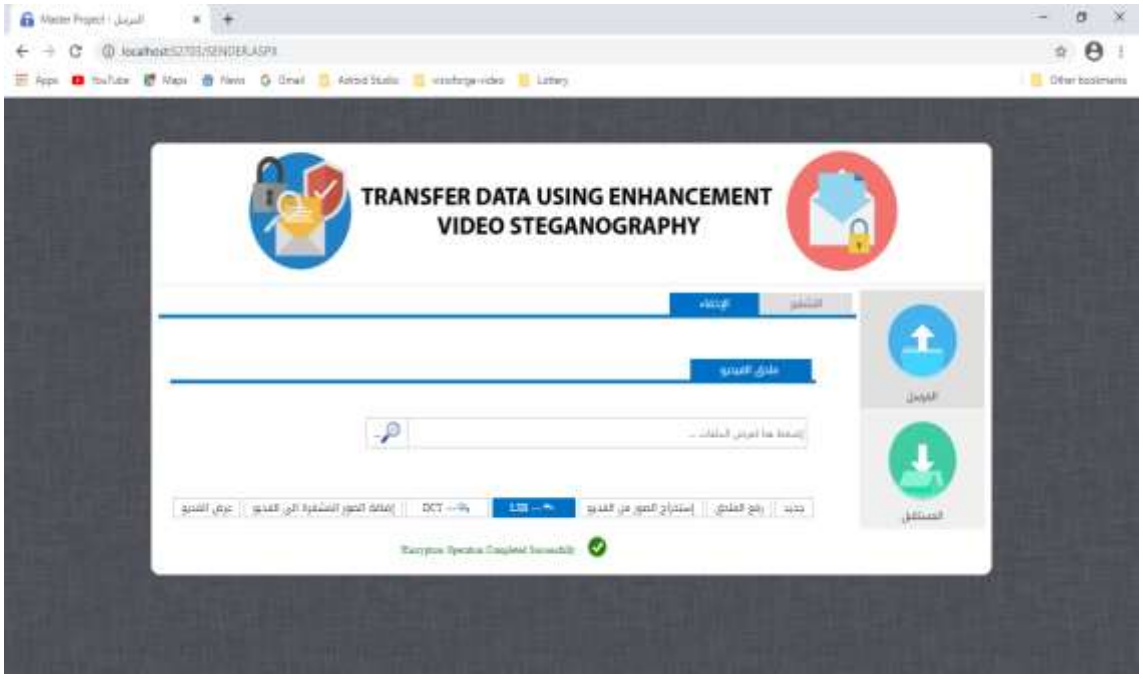


Figure (4.17) LSB process

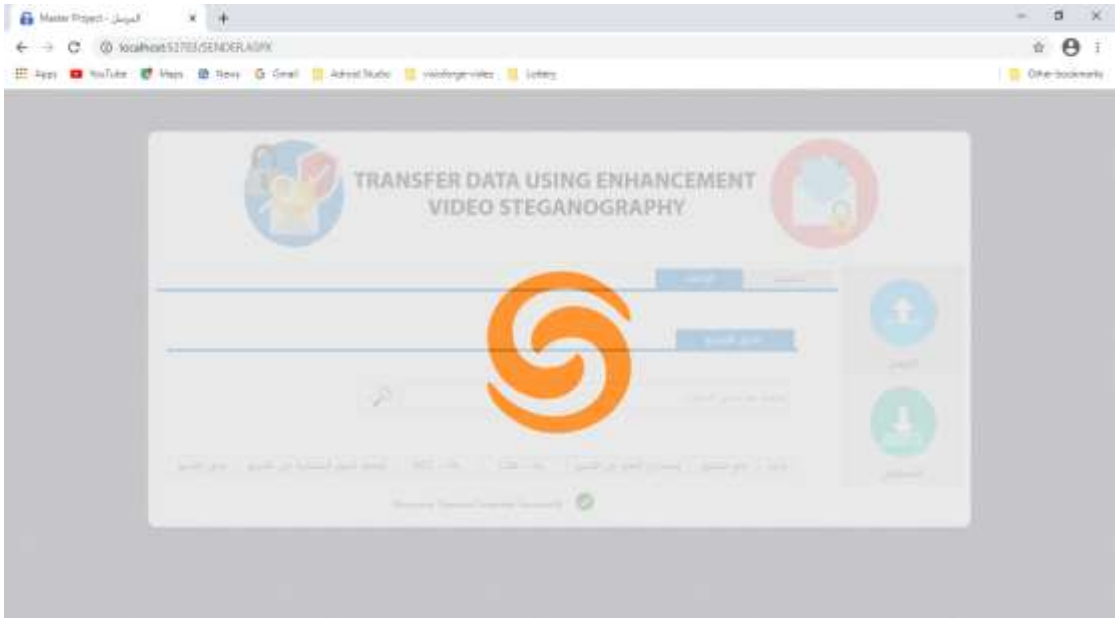


Figure (4.18) processing of LSB

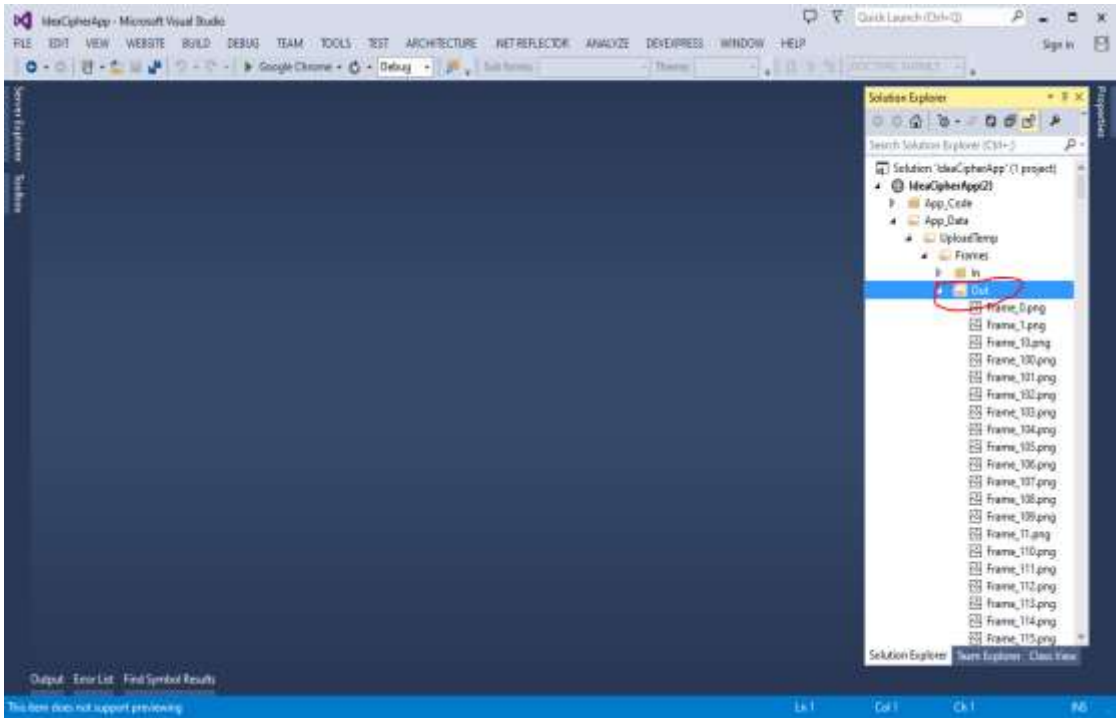


Figure (4.19) LSB applied in background

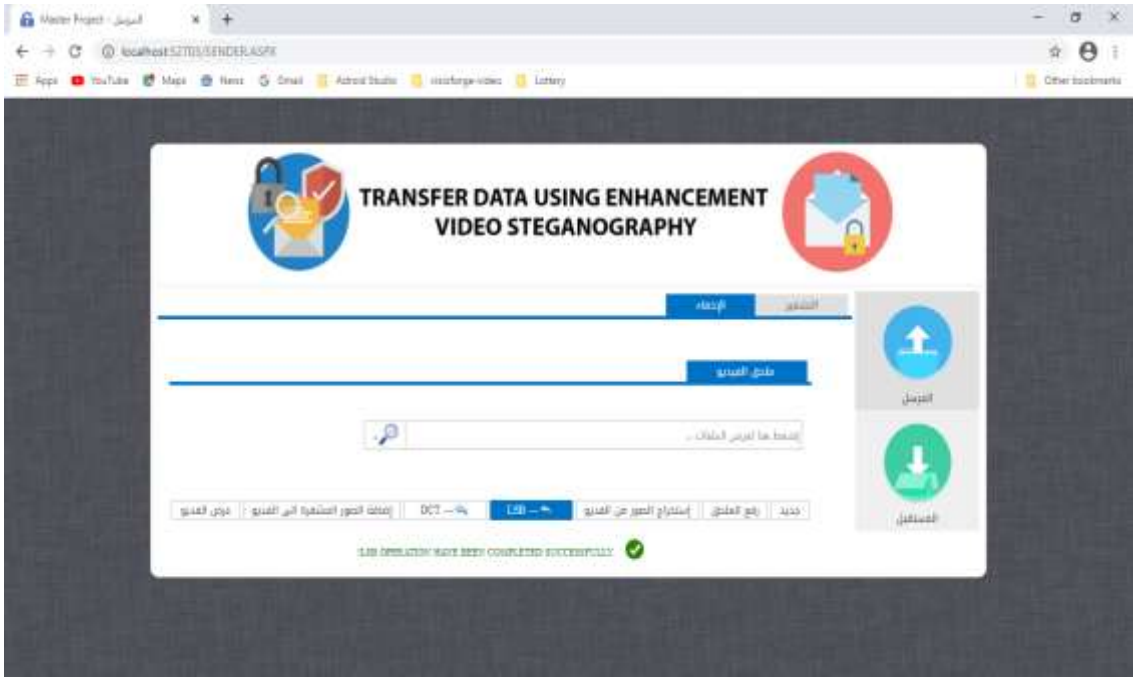


Figure (4.20) completion of the LSB process

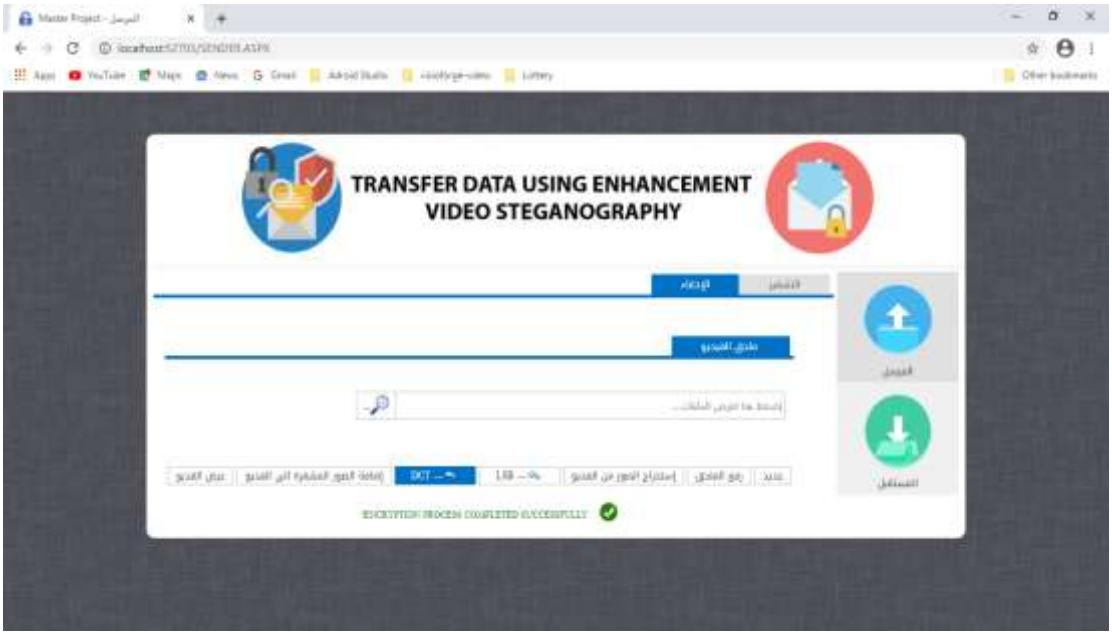


Figure (4.21) DCT process

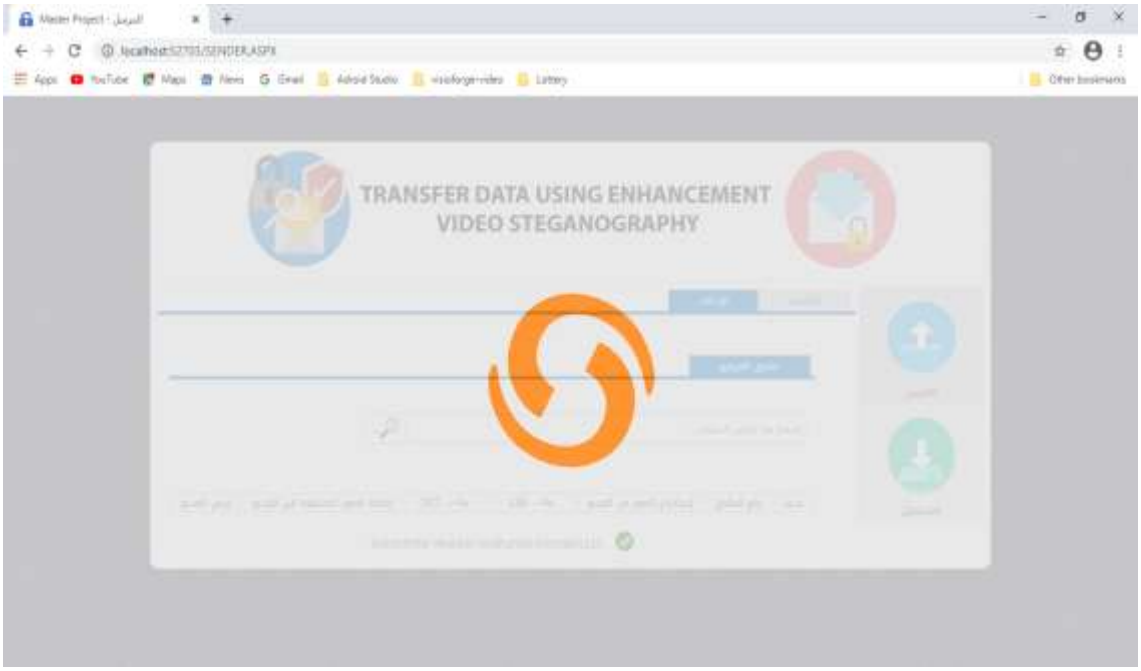


Figure (4.22) processing of DCT

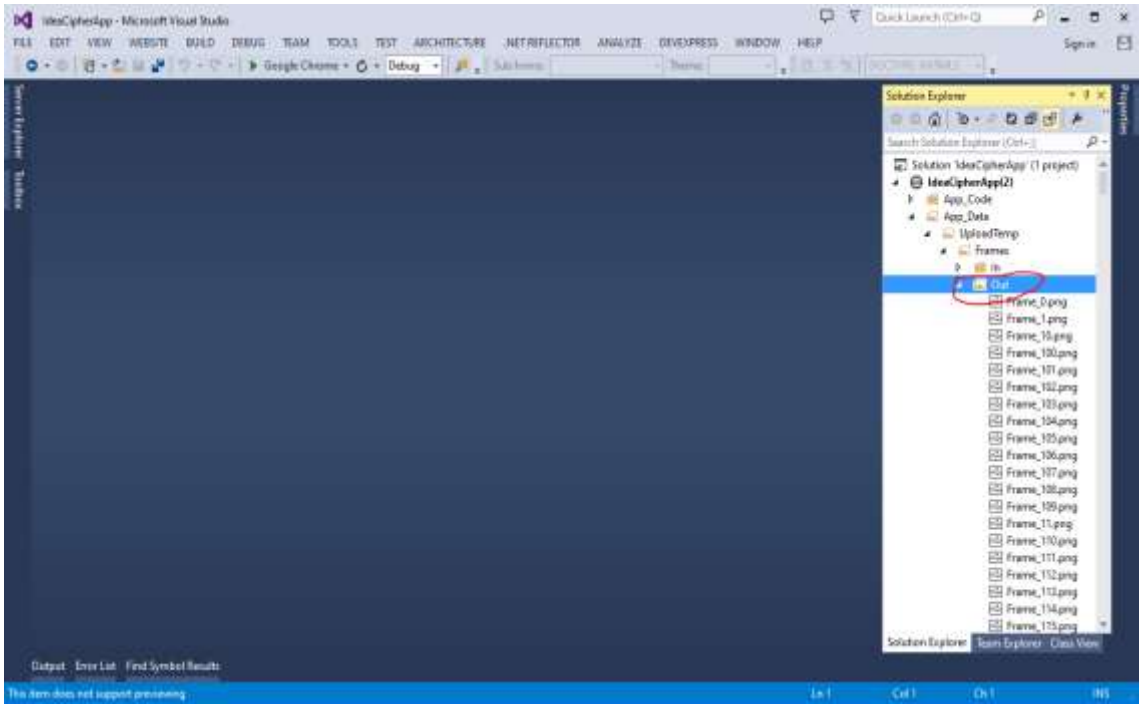


Figure (4.23) DCT applied in background

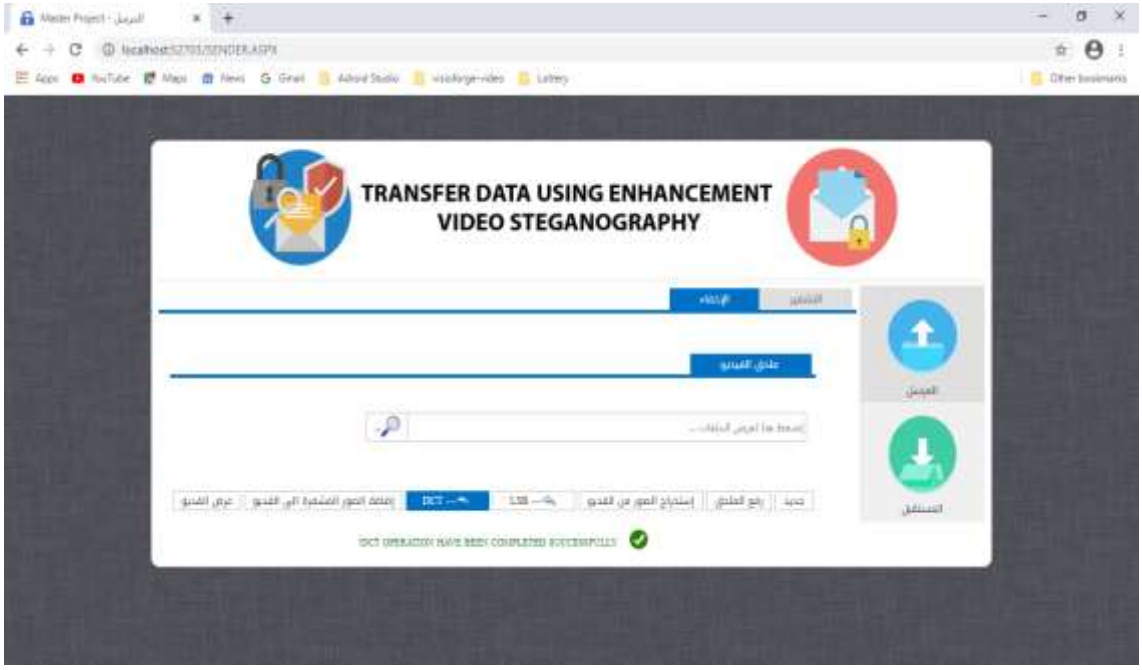


Figure (4.24) completion of the DCT process

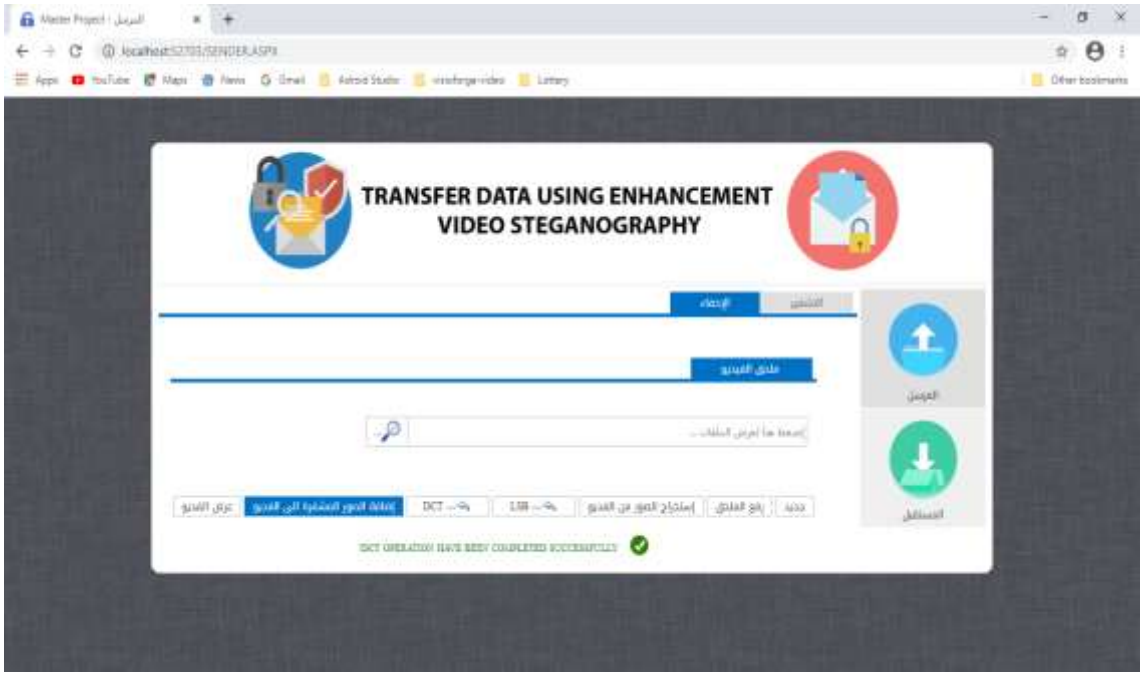


Figure (4.25) processing of adding images

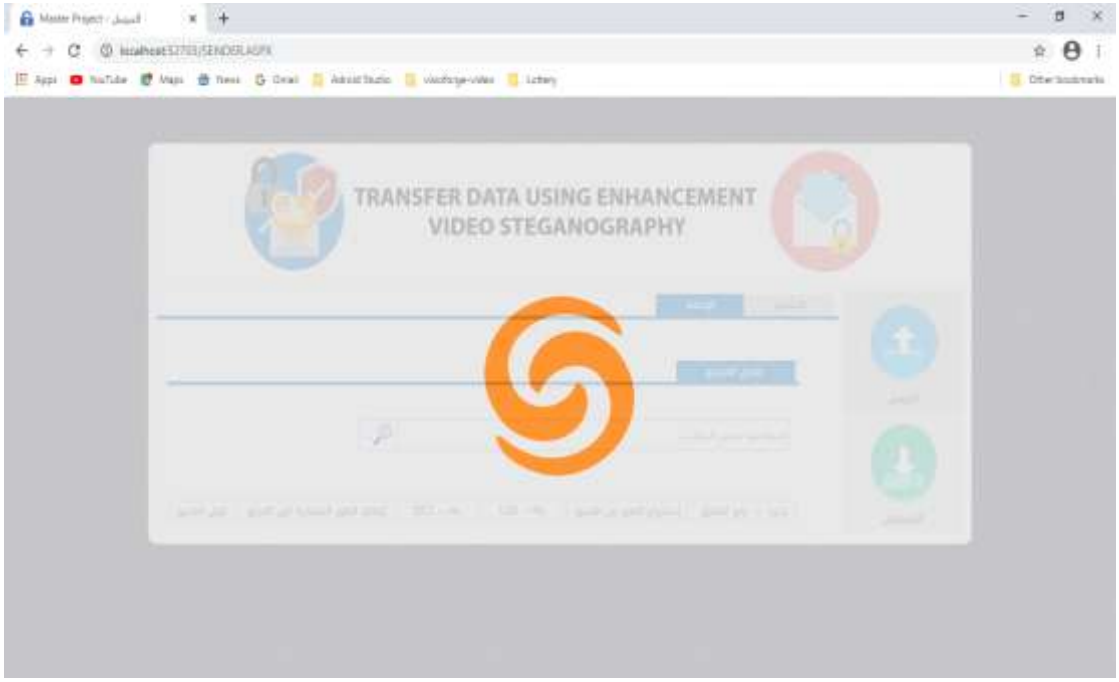


Figure (4.26) processing adding LSB-DCT images

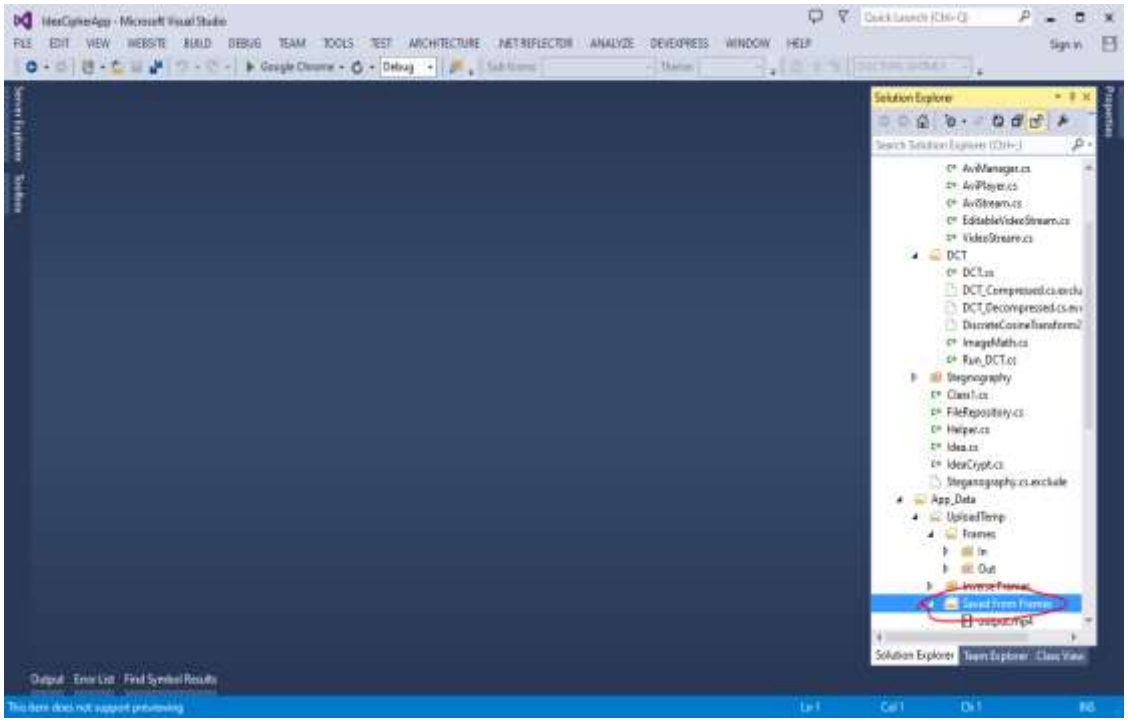


Figure (4.27) processing of adding LSB-DCT images in background

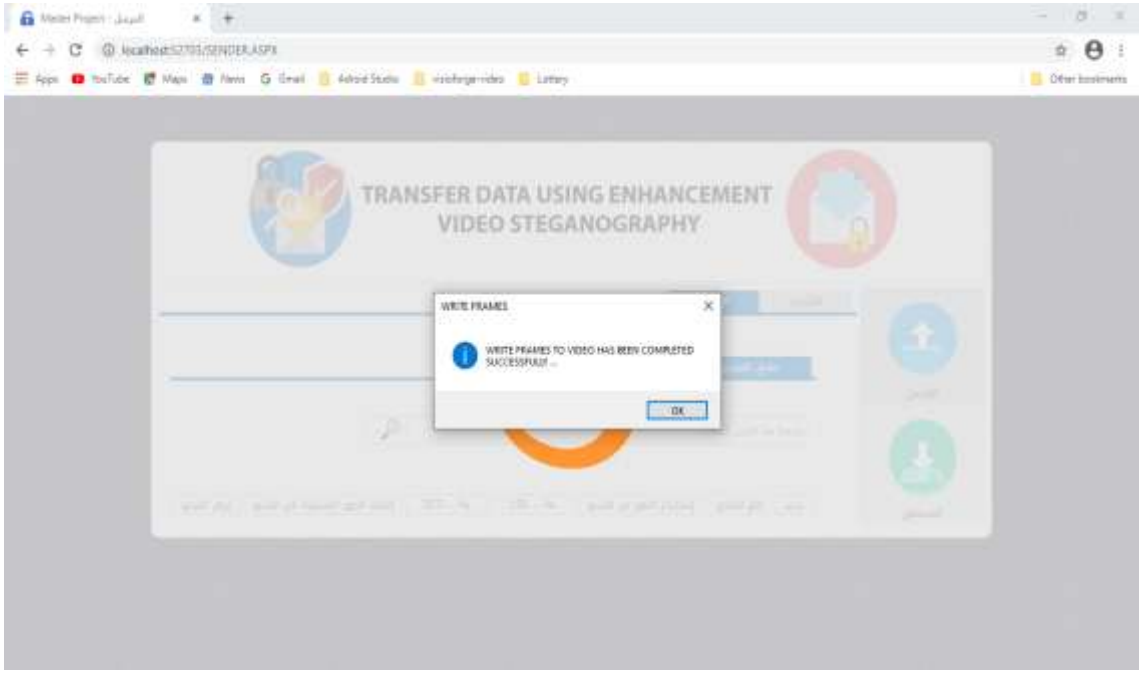


Figure (4.28) completion of adding LSB-DCT images in video

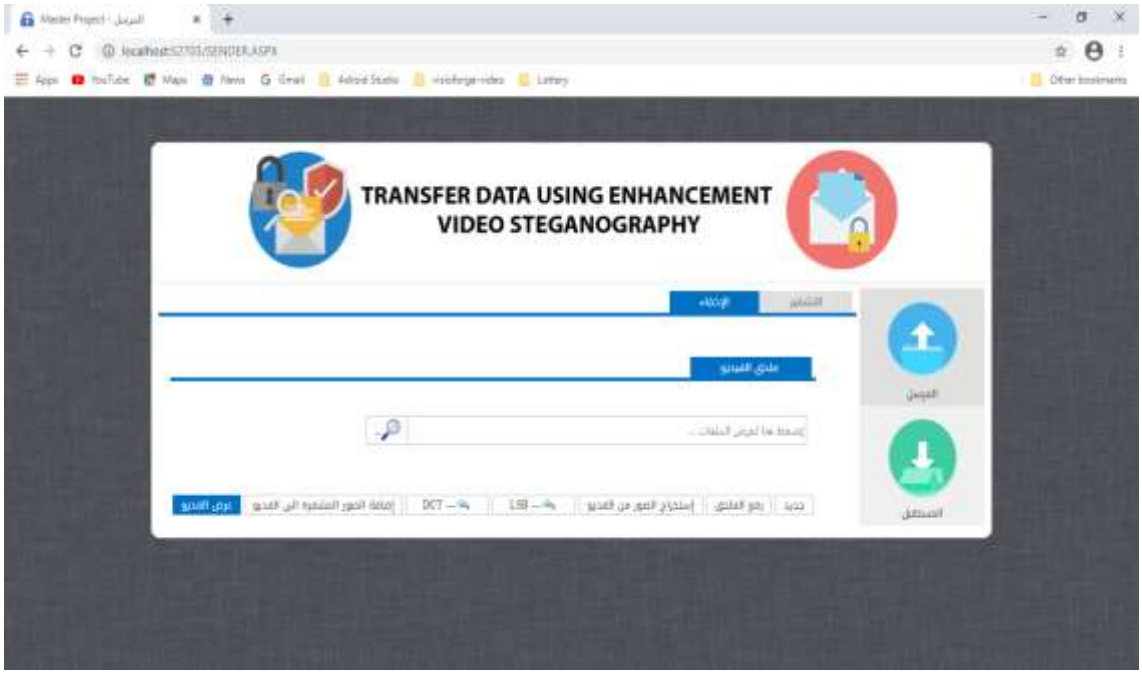


Figure (4.29) processing of display video

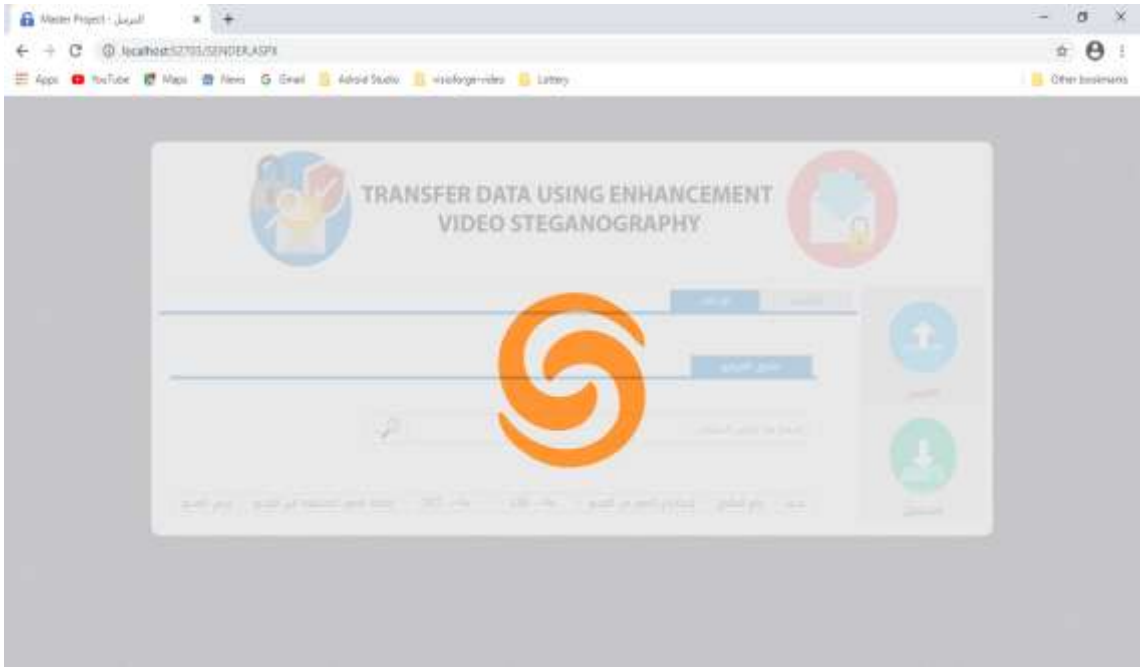


Figure (4.30) waiting display video

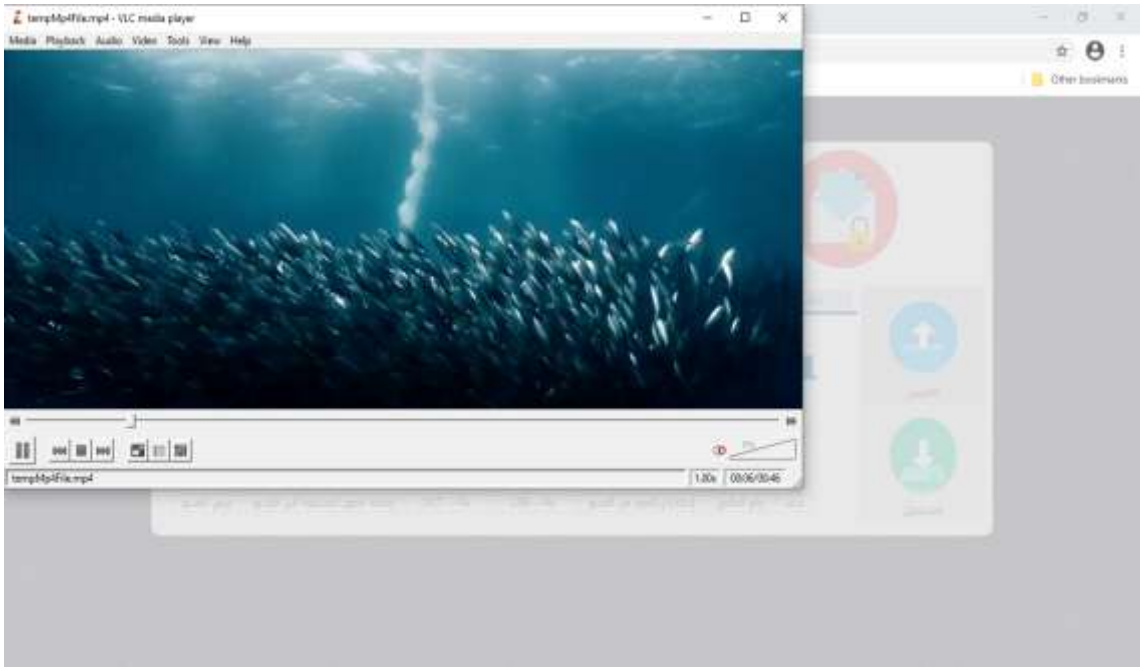


Figure (4.31) displaying video

4.2.2 Receiver side procedures

Receiver has one tab contain many buttons (display video, extract frames, IDCT, Invers LSB and decryption)

Hence the process will be opposed, receiver can play the video and then extracted images from video (that images carry the secret message) after that apply inverse of DCT and inverse of LSB to get encrypted message and finally decrypt the message to obtain the original message. all these processes show in blew figures.

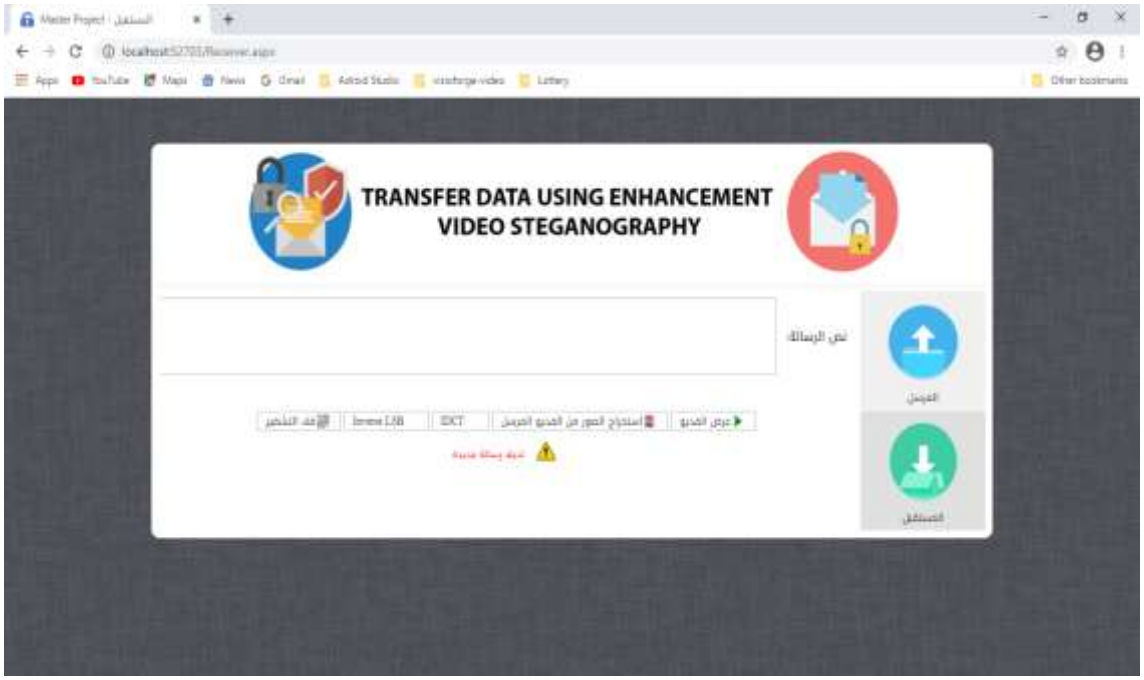


Figure (4.32) screen of the receiver side

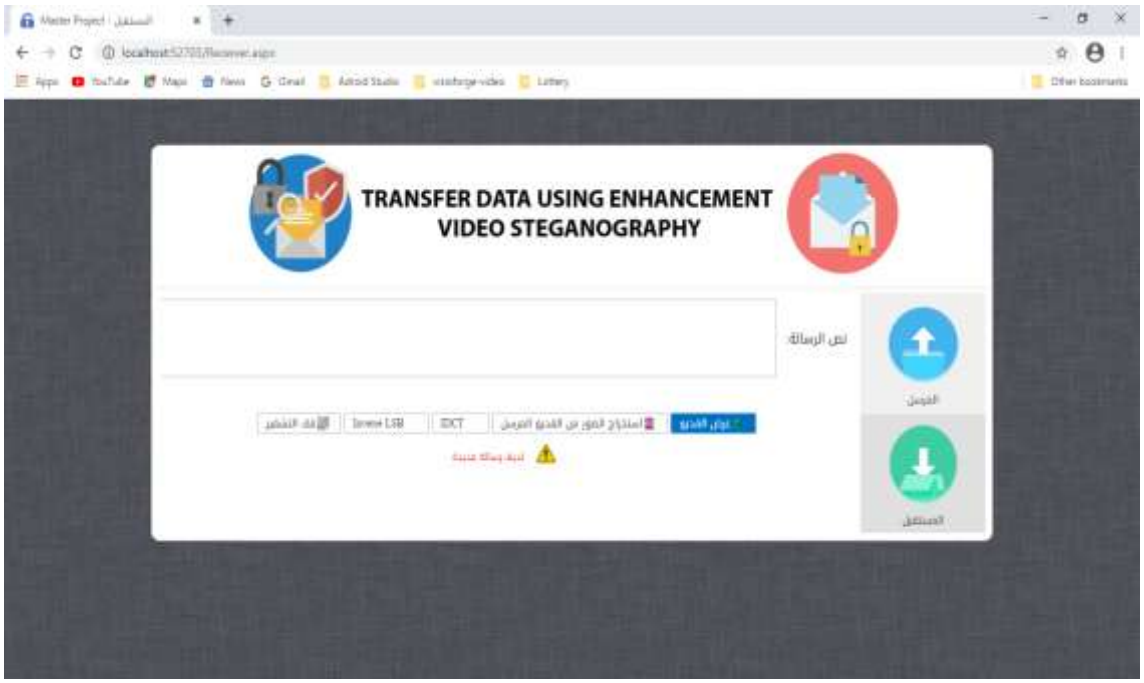


Figure (4.33) button displaying embedded video

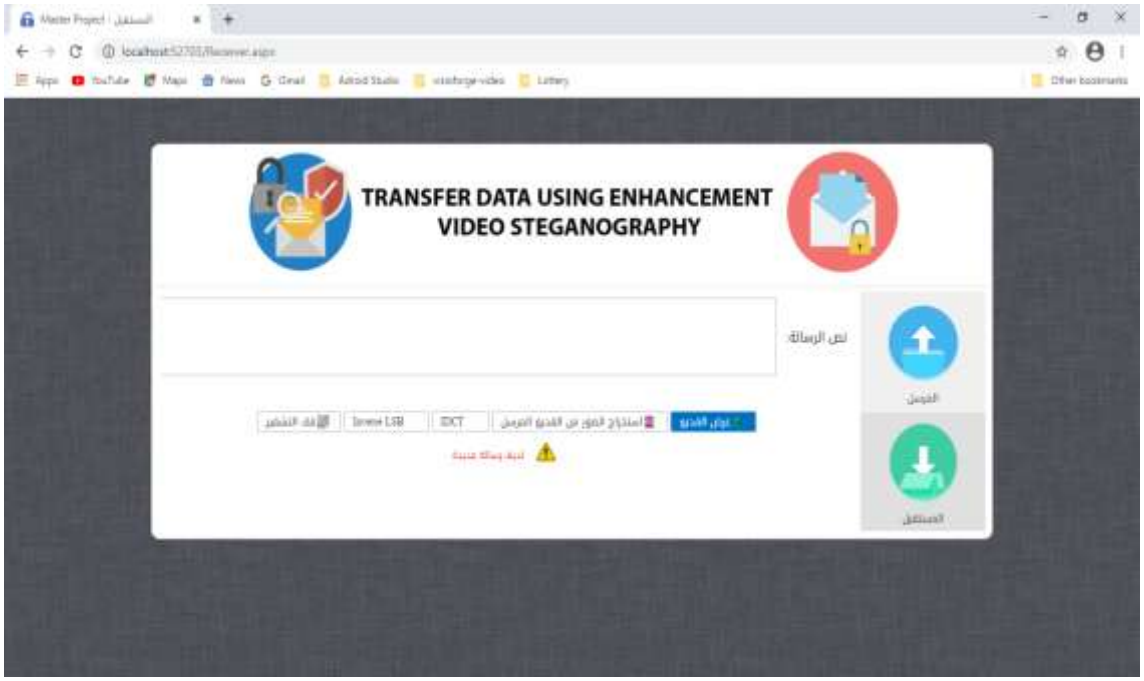


Figure (4.34) embedded video are displaying

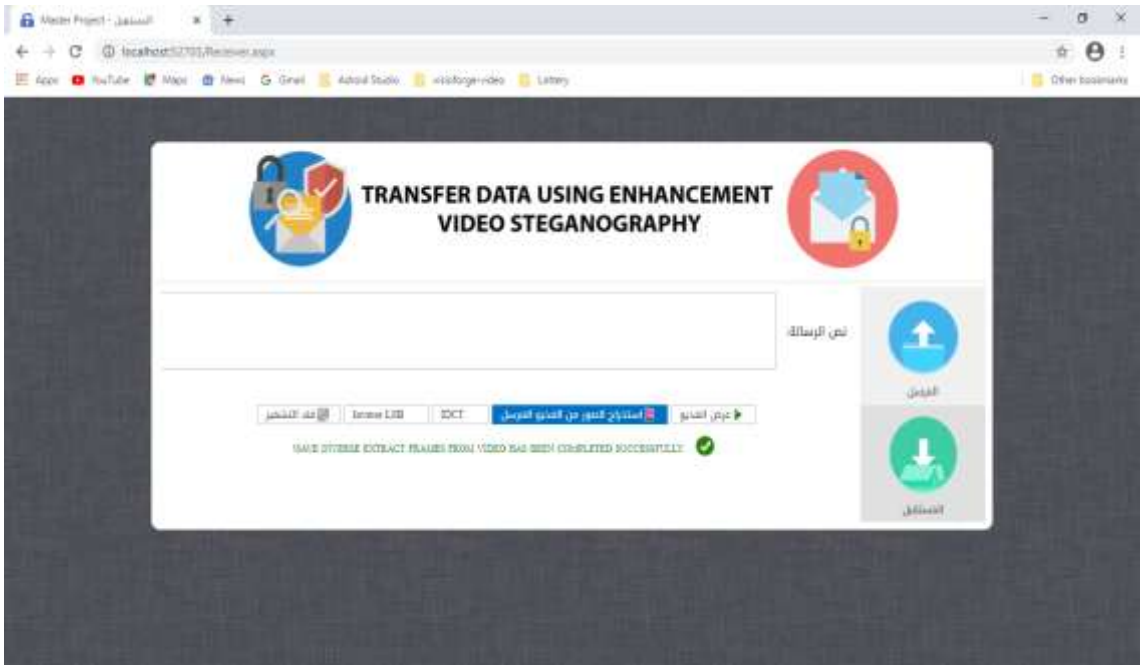


Figure (4.35) extract image button from received video

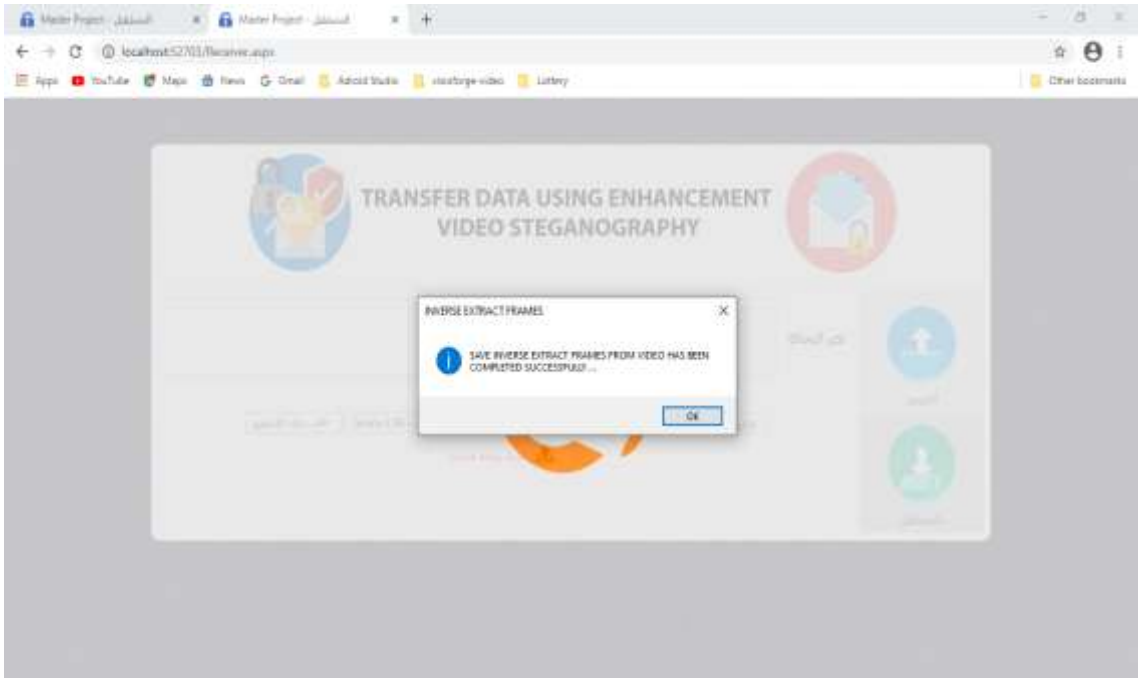


Figure (4.36) extracting process completed

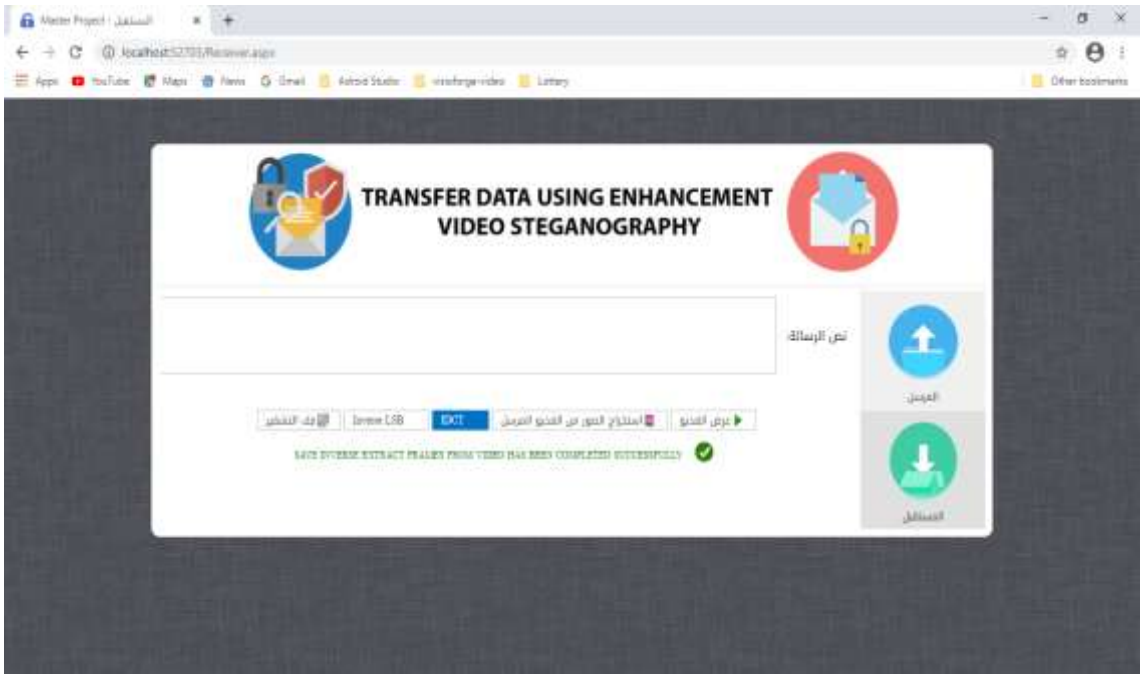


Figure (4.37) applying inverse DCT

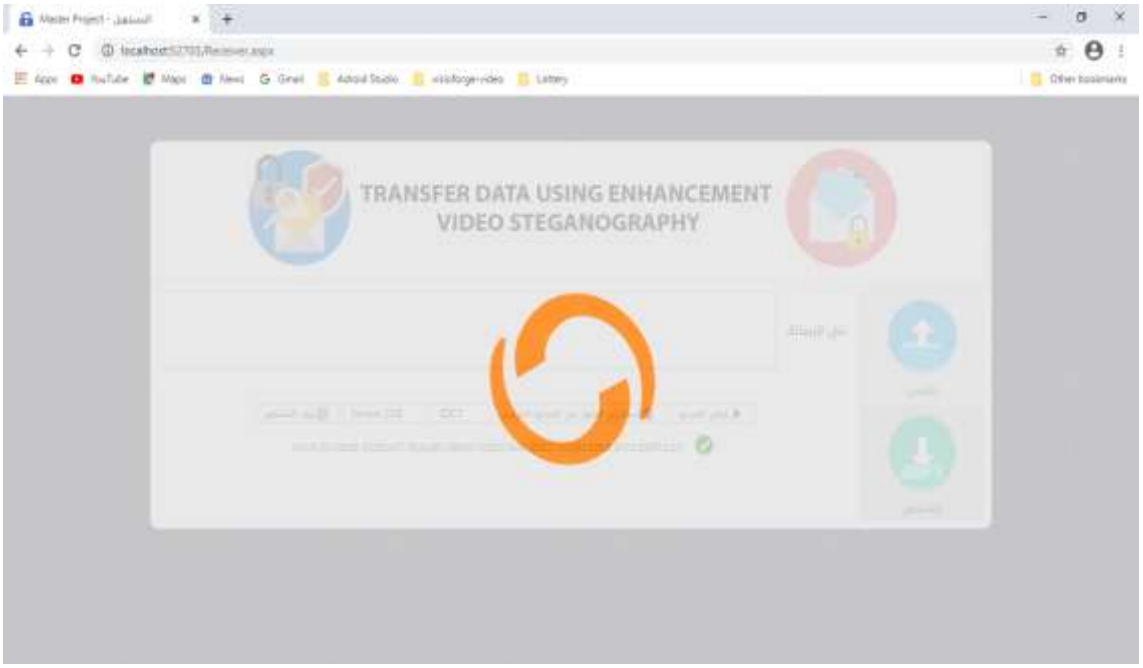


Figure (4.38) processing of inverse DCT

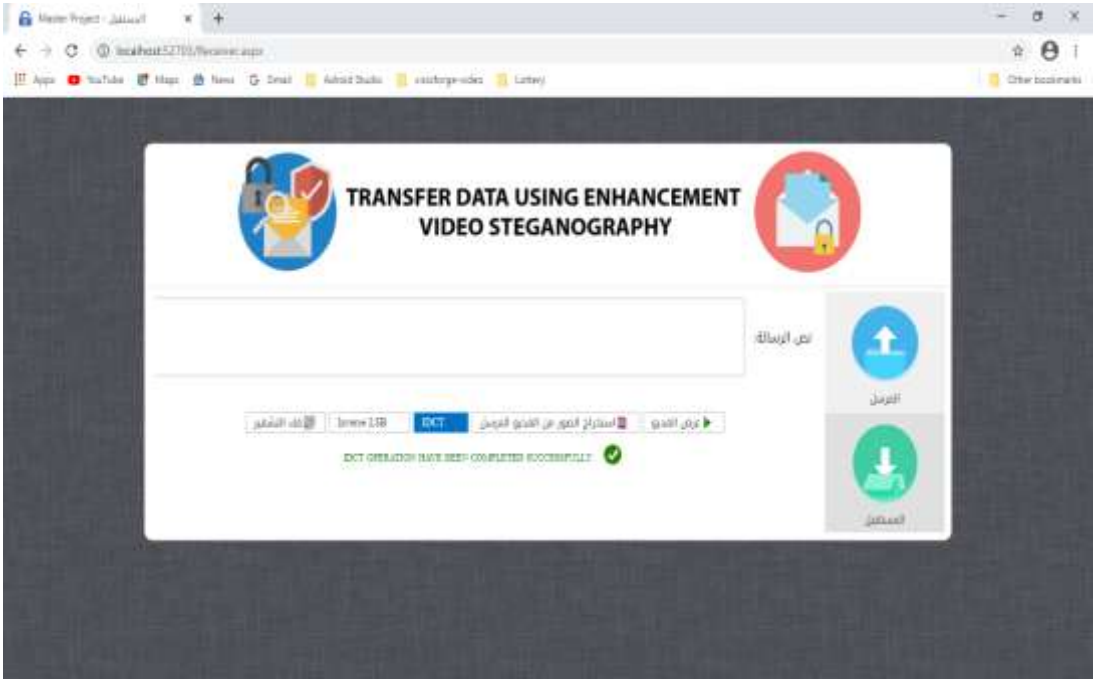


Figure (4.39) inverse DCT process completed

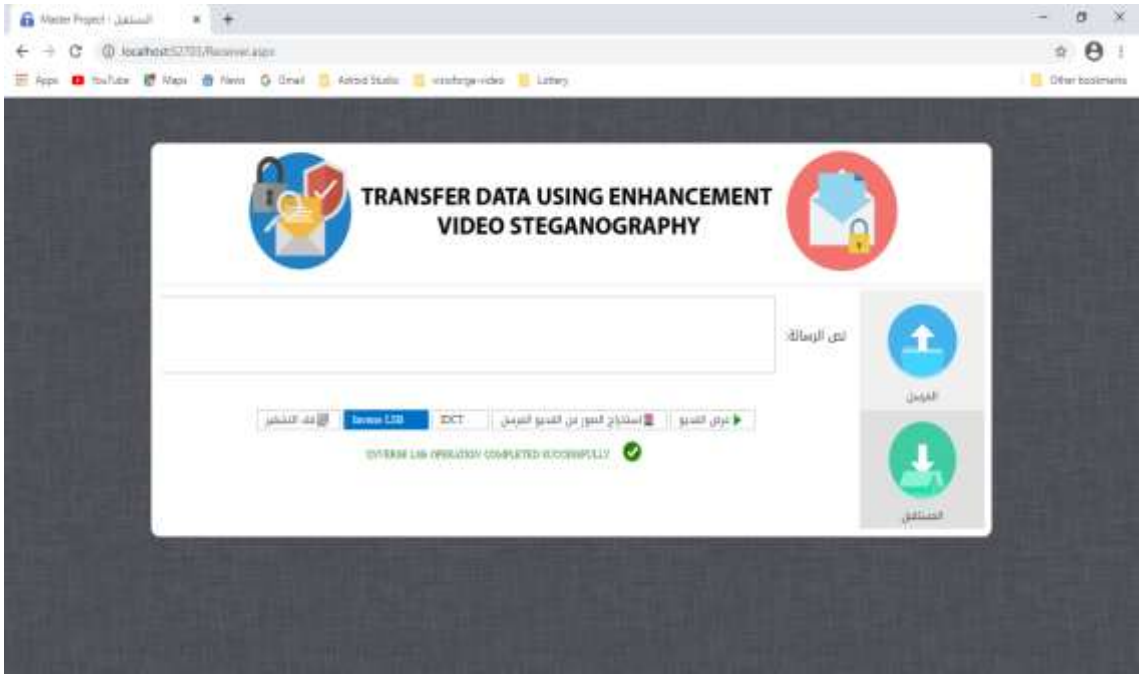


Figure (4.40) applying inverse LSB

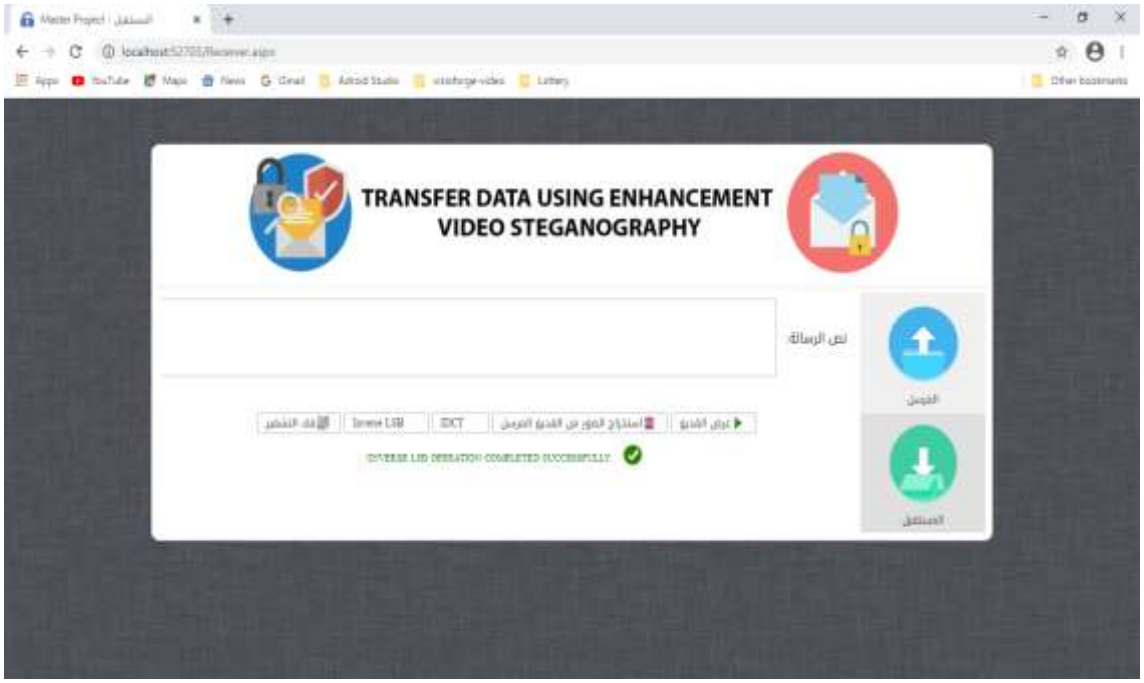


Figure (4.41) inverse LSB process completed

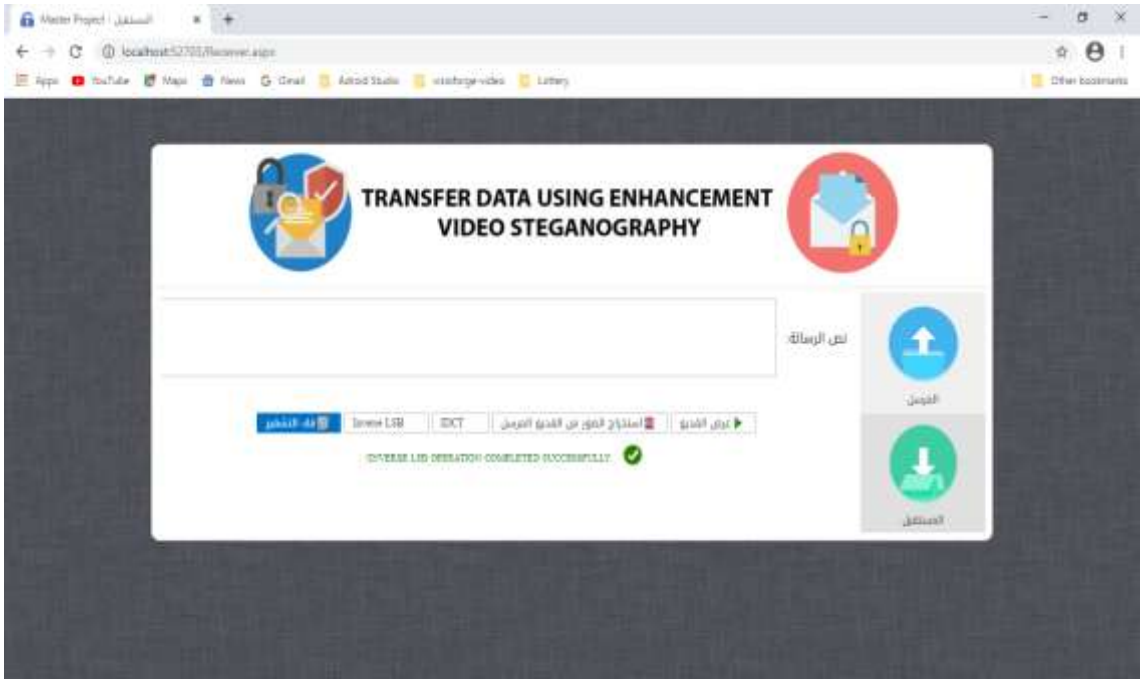


Figure (4.42) button decryption process

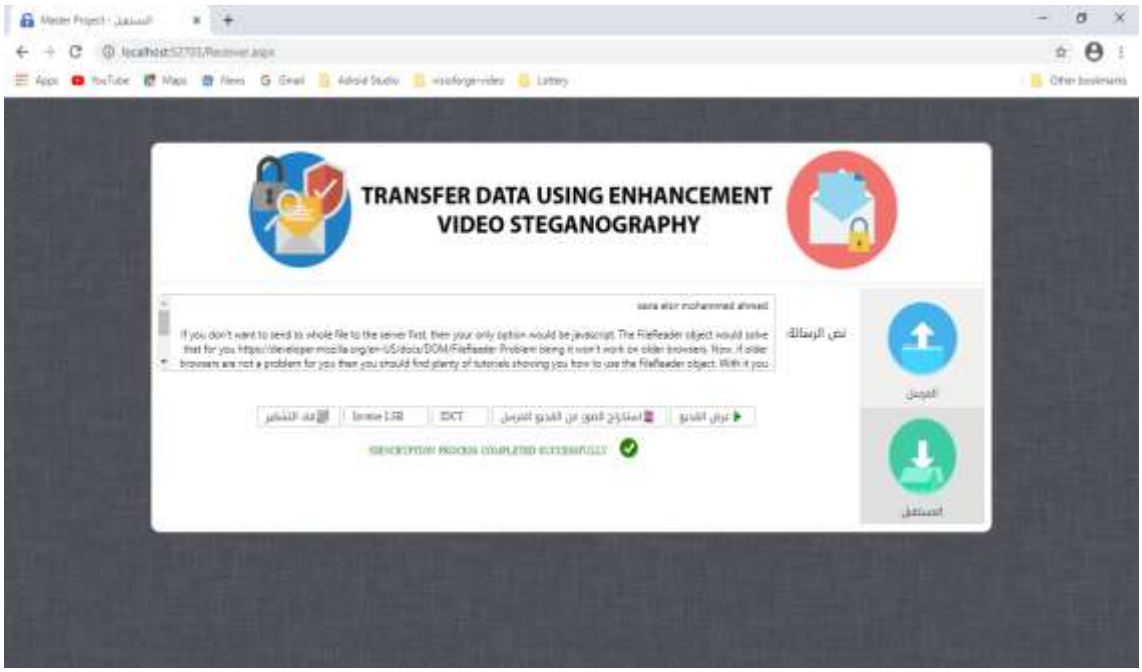


Figure (4.43) decryption process completed

4.3 Results

The method proposed has proved successful to achieve security, availability and confidentiality by concealing encryption text in video-images.

The methods that use sequential hiding at a constant pace are more likely to be discovered and suspicious of snipers or hackers. Using even-images that allowed for breaks between selected images used two techniques of steganography to concealing the data. The distance between image pixels reduces the possibility of detecting hidden text. The encrypted text distribution in even images. The distribution of data lead to be hard detectable.

The method Provide enable control of the text size to be hidden, the maximum text size is 2 GB and video can be any size, when using large video size that affect in system efficiency and system slow down.

It is preferable to use images with more details (ie high-text images) in the hiding process to increase efficiency by hiding data on the three colors (red, green, blue),thus that each part of the character of text hidden in a different pixel of the image to reduces the possibility of detection.

In this proposed method, video files are the better cover object than image and audio. Because of their high capacity.

The table below explains the process of calculating the PSNR values using different text length in same image. The PSNR values are variable when I use the original image with different text messages.

Peak Signal-to-Noise Ratio (PSNR) value			
Original Image Frame name	Encrypted Message Size	LSB Image Frame	DCT Image Frame
Frame_1.png	1 KB	78.93772197940774 dB	28.89865082435414 dB
Frame_1.png	2 KB	66.98345081736286 dB	28.899553643702806 dB
Frame_1.png	161 KB	51.160246607927114 dB	28.930146142155184 dB

Table(4.1) The PSNR values

CHAPTER FIVE
CONCLUSION AND RECOMMENDATION

CHAPTER V

CONCLUSION AND RECOMMENDATION

5.1 Conclusion

The user of internet has increased and growth thus they need protection for their data. Cryptography and Steganography they are type of protection techniques used to protect the data.

The proposed of transferring data using video Steganography system to provide two level of security data, the first level is cryptography and the second level is Steganography. The resulting of proposed system is concealing the encrypted text successfully into the video frames.

Concealment the encrypted text that encrypted with IDEA algorithm in video-frames specifically in even frames using LSB technique in these selected frames depend on mathematical equation and then applied DCT technique at the same frames that selected before.

The proposed system is allowed taking different size of videos and different size of text maximum 2 GB. The stego video is sent to the receiver safely and securely to the destination.

The video are better than image and audio they have high degree of capacity to stored data in their frames. Finally proposed method achieve terms of security, availability and confidentiality.

5.2 Recommendation

1. Conceal data in random frames.
2. Change encryption key in every process and make it random.
3. Running the program on a different platform like android and IOS that provide new facility.

REFERENCES

References

[1] William Stallings , "Network security essentials" , 2004.

[2] Charu Rohilla, Rahul Kumar Yadav , Sugandha Singh,"Encryption and Decryption for Secure Communication" , International Journal of Engineering Technology, Management and Applied Sciences, 2018.

[3] Sri Ram Polisetty, Niharika Tangella, Lavanya B ,Geetha Sri DS, Ishwarya L , "a novel approach to the information security using rc4 and lsb techniques",Journal of Emerging Technologies and Innovative Research (JETIR), April 2019.

[4] mihir bellare, kenneth G.paterson, phillip,"security of symmetric encryption against mass surveillance".2014

[5] M. I. L. Francesco Fusco1, Filippo Eros Pani2 and Andrea Pinna2 and V. M. 1NET SERVICE SPA, 4/d Bologna Italy, "Crypto-Voting, a blockchain based e-voting system," 2019.

[6] Sandipan Basu ,"international data encryption algorithm (idea) – a typical illustration", Journal of Global Research in Computer Science, 7, July 2011.

[7] Osama Almasri, Hajar Mat Jani ," Introducing an Encryption Algorithm based on IDEA", International Journal of Science and Research (IJSR),2015

[8] Firdaus Anjum, Shikha Yadav, Rumaiza Aafreen ,Tasneem Hasan," A Survey: Secure Data Transmission Using Video Steganography", Imperial Journal of Interdisciplinary Research (IJIR) 2016.

[9] Ahmad-Loay Sousi, Dalia Yehya, Mohamad Joudi "AES encryption study and evaluation", November 2020.

[10] Harpreet Kaur, a and Jyoti Rani, " A Survey on different techniques of steganography", MATEC Web of Conferences **57**, 02003 (2016).

[11] jammi ashok, y.raju, s.munishankaraiah, k.srinivas," steganography: an overview"**,** Jammi Ashok et. al. / International Journal of Engineering Science and Technology,2016.

[12] Sellars, D., "An Introduction to Steganography",7th Ed Sutton ,2007.

[13] SANS Institute 2002, by Bret Dunbar, "A detailed look at Steganographic Techniques",2002.

[14] Shivani Khosla, Paramjeet Kaur, "Secure Data Hiding Technique Using Video Steganography and Watermarking", International Journal of Computer Science &Information Technology,March 2014

[15] Harpreet Kaur, Jyoti Rani,"A Survey on different techniques of steganography",MATEC Web of Conferences 57, 2016.

[16] Elsie Wangui Ngatia and Dr. Alice Njuguna, "Information Security through an Improved Image Steganography Algorithm" , Stratford Peer Reviewed Journals and Book Publishing Journal of Information and Technology, 2018

[17] Eric Gyamfi, Isaac kofi nti, justice aning, "Using LSB Steganography Technique and 256 bits Key Length AES Algorithm for High Secured Information Hiding", International Journal of Advanced Research in Computer Science and Software Engineering ,2017.

[18] Wafaa Mustafa Abduallaha, Abdul Monem S. Rahmab," A Review on Steganography Techniques", American Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS),2017

[19] Zeyad Safaa Younus and Ghada Thanoon Younus ,"Video Steganography Using Knight TourAlgorithm and LSB Method for Encrypted Data", . 2020.

[20] Prof. Dipti Mukadam, Sunita Mahale, Aayushi Dalvi, Prajakta Magar, Swapnil Gawade, "secure data Transfer using video Steganography", International Journal for Research in Engineering Application & Management (IJREAM) , Feb 2018.

[21] Syed Juwairah Indrabi, Neha Saini, M. Mohan, " Secure Data Transmission Based On Combined Effect Of Cryptography And Steganography Using Visible Light Spectrum" , International Journal of Pure and Applied Mathematics , Volume 118 No. 20 2018.

[22] Mumthas Sa, Lijiya Ab,"Transform Domain Video Steganography Using RSA, Random DNA Encryption and Huffman Encoding",7th International Conference on Advances in Computing & Communications, ICACC-2017, 22-24 August 2017.

[23] Naveen Chandra Gowda, P. Sai Venkata Srivastav, Guru Prashanth.R, Raunak.A, Madhu Priya R **,** "Steg Crypt (Encryption using steganography)" , International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, May 2019.

[24] Anmol D Kulkarni, Esti Bansal, Hole Rajashree B, Jadhav Rasika R, Lakshmi Madhuri,"Improved Data Security Using Video Steganography", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) , October 2015.

[25] Ahmed AL-Shaaby, Talal AlKharobi,"Cryptography and Steganography: New Approach", Transactions on Networks and Communications, December 2017.

[26] J. Lopes, J. L. Pereira, and J. Varajão, "Blockchain based E-voting system: a proposal," 2019.