GAZİANTEP ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

COMPARATIVE STUDY OF LSB BASED VIDEO STEGANOGRAPHY TECHNIQUES

M.Sc. Thesis

In

Electrical and Electronic Engineering

BY

IVIN ADNAN AL-SALIHI

OCTOBER 2017

OCTOBER 2017 M.Sc. Thesis In Electrical and Electronic Engineering IVIN ADNAN ALSALIHI

COMPARATIVE STUDY OF LSB BASED VIDEO STEGANOGRAPHY TECHNIQUES

M.Sc. Thesis

In

Electrical and Electronic Engineering

University of Gaziantep

Supervisor

Assoc. Prof. Dr. Sema KOÇ KAYHAN

by

Ivin Adnan AL-SALIHI

OCTOBER 2017

REPUBLIC OF TURKEY

GAZIANTEP UNIVERSITY

GRADUATE SCHOOL OF NATURAL & APPLIED SCIENCES

ELECTRICAL AND ELECTRONICS ENGINEERING

Name of Thesis: A comparative Study of LSB Based Video Steganography Techniques

Name of Student: IVIN AL-SALIHI

Exam date: 06.10.2017

Approval of The Graduate School of Natural Applies Sciences

Prof. Dr. A. Necmeddin YAZICI

Director

I certify that this thesis satisfies all requirements as a thesis for the degree of Master of Science

Prof. Dr. Ergün ERÇELEBİ

Head of Department

This is to certify that we have read this thesis and in our consensus opinion; it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

Assoc. Prof. Dr. Sema KOÇ KAYHAN

Supervisor

Examining Committee Members:

Signature

Assoc. Prof. Dr. Sema KOÇ KAYHAN .....

Assist. Prof. Dr. Serkan ÖZBAY .....

Assoc. Prof. Kemal DELIHACIOĞLU .....

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Ivin Adnan AL-SALIHI

ABSTRACT

COMPARATIVE STUDY OF LSB BASED VIDEO STEGANOGRAPHY TECHNIQUES

AL-SALIHI, Ivin Adnan
M.Sc. Thesis in Electrical and Electronic Engineering
Supervisor: Assoc. Prof. Dr. Sema KOÇ KAYHAN
October 2017
66 Pages

Video Steganography is one of the crucial strategies for concealing user information in secure way. Nowadays, the use of video files and their transmission on internet has increased tremendously. There exist many methods for information hiding in video. Video Steganography is a method to hide different file types into a video file. The steganography algorithm consists of mainly two parts: message embedding process in the video sequence and the second part is the extraction of message from the stego video. It is essential to develop an effective embedding procedure to select suitable pixels in the video outlines to store the hide information. In this thesis, a brief analysis of two different methodologies for information embedding and for extracting embedded information in a video files having an outstanding quality is presented. In these methods, information encryption processes are based on least significant bit (LSB) procedure. The first improved LSB image steganography approach utilizes Bit-Inverse in 24 Bit color image, and the second LSB image steganography procedure utilizes RGB color components and image patterns are compacted using weighted principal elements. The efficiency and comparison of these two methods are realized using Peak-to-Signal Noise Ratio (PSNR), Mean Square Error (MSE) metrics and also histogram examination demonstrates the frequency distribution on the color videos. Our proposed steganography procedure tries to enhance payload capacity of image steganography and give greater security to the stego video through utilizing the RGB pixel element.

Key Words: Data hiding, Video steganography, LSB Insertion.

ÖZET

LSB TABANLI VİDEO STEGANOGRAFİ TEKNİKLERİYLE KARŞILAŞTIRMALI BİR ÇALIŞMA

AL_SALIHI, Ivin Adnan
M.Sc. Thesis in Electrical and Electronic Engineering
Supervisor: Assoc. Prof. Dr. Sema KOÇ KAYHAN
October 2017
66 Pages

Video Steganografi, kullanıcı bilgilerini gizlemek için önemli stratejilerden biridir. Günümüzde, video dosyalarının kullanımı ve internet üzerinden iletimi çok büyük ölçüde bir artış göstermiştir. Video bilgi gizleme için pek çok yöntem bulunmaktadır. Video Steganografi, farklı dosya türlerini, video içerisine gizlemek için kullanılan bir yöntemdir. Steganografi algoritması başlıca iki bölümden oluşmaktadır: video dosyalarına mesaj gömme süreci ve ikinci kısım, stego videodan mesaj çıkarılmasıdır. Gizlenecek bilgiyi saklamak için video dosyalarında uygun pikselleri seçmek için etkili bir gömme işlemi geliştirmek önem taşır. Bu tezde, yüksek kaliteli bir video dosyasına bilgi gömme ve gömülü bilginin çıkarılması için iki farklı metodolojinin kısa bir analizi sunulmuştur. Bu yöntemlerde bilgi şifreleme süreci En Düşük Anlamlı Bit (LSB) işlemine dayalıdır. Birinci method; gelişmiş LSB görüntü steganografi yaklaşımı, 24 Bit renkli görüntüde Bit-Tersi kullanmaktadır ve ikinci LSB görüntü steganografi yaklaşımı RGB renk bileşenlerini kullanmaktadırve görüntü unsurları ağırlıklı ana unsurlar kullanılarak sıkıştırılmaktadır. Bu iki yöntemin etkinliği ve karşılaştırılması, Tepe-Sinyal Gürültü Oranı (PSNR), Ortalama Kare Hata (MSE) ölçümleri ve ayrıca renk videolarındaki frekans dağılımını gösteren histogram incelemesi kullanılarak gerçekleştirilmektedir. Önerilen steganografi prosedürü, görüntü steganografisinin yük taşıma kapasitesini artırmayı ve RGB piksel unsurunu kullanarak stego videosunu daha güvenli hale getirmeyi amaçlamaktadır.

Anahtar Kelimeler: Veri gizleme, Video steganografisi, Düşük Anlamlı Bit (LSB) yerleştirme.

To my Family

ACKNOWLEDGEMENTS

First of all, I thank Allah for having given me the strength to carry on this project and for blessing me with many great people who have been my greatest support in both my personal and professional life.

A sincere gratitude and appreciation goes to my supervisor, Assoc. Prof. Dr. SEMA KOÇ KAYHAN for her knowledge, advice and support throughout my studies.

A big thank you to all members of electric electronic engineering group past and present, whom I was fortunate enough to work with.

A special thanks must go to my friends in Turkey and Baghdad for their everlasting friendship.

Above all I thank my family (father, mother, brothers and sisters) who are the most important part of my life, who have always being there for me in all difficult circumstances, for their love, moral support, encouragement and continuous prayers, for their faith in my ability during my experience in Turkey .

This thesis dedicated to those most dear to me- my beloved family.

Many thanks to you all...

Ivin, October 2017

TABLE OF CONTENTS

Page

LIST OF FIGURES

Page

LIST OF TABLES

Page

LIST OF SYMBOLS/ABBREVIATIONS

HTML	Hyper Text Markup Language
WAV	Waveform Audio Format
AU	Audio file format
MP3	MPEG-1 Audio Layer3
LSB	Least Significant Bit
OSI	Open System Interconnection
TCP/IP	Transmission Control Protocol/Internet Protocol
DCT	Discrete Cosine Transform
JPEG	Joint Photographic Experts Group
PIXEL	Picture Element
FPS	Frame Per Second
XOR	Exclusive OR
RGB	Red, Green and Blue
CMYK	Cyan ,Magenta, Yellow and Black
DWT	Discrete Wavelet Transform
BPP	Bit Per Pixel
AVI	Audio Video Interleaved format
PSNR	Peak Signal to Noise Ratio
MSE	Mean Square Error
EC	Embedding Capacity

CHAPTER 1
INTRODUCTION

1.1 General Introduction

Information transmission security has turned into a crucial field of research, because of the fast rise in cybercrime, data theft, industrial espionage and assaults on private people's information. Even business documents that are not sent over the web can be at a risk, by insider's assault. One essential defense against such assaults is a procedure to conceal the presence of private documents from un-authorized people Steganography is to conceal secret data in carriers (media) such as text files, images, audio files, videos and information transmission channels [1, 2].

Steganography literally implies covered writing which derived from two Greek words *"steganos"*, signifying "covered," and *"graphein"*, signifying "to write. Steganography is concealing data through a secret channel with the goal that it will not be detected; so that only the proposed receiver or the sender understands that there is a concealed message [3]. The aim of Steganography is sending a message through network to a proposed recipient and anticipating any other person to know whether the message is being delivered [1]. Steganography is the science and art of encoding confidential message into an existing communication channel or into a payload (information unit) such that the sender and proposed recipient are aware of its reality [4]. The fundamental goal of Steganography is to communicate securely and to prevent drawing doubt to transmission of a concealed information [5].

Steganography is the procedure that takes some data and conceals them within other data. Computer documents such as audio, images and videos comprise unutilized or unimportant areas of information. Steganography takes the data that we need to conceal, and displacing them with these areas. At that point the communication parties can exchange data without knowing of the third party what truly lies within them [1].

A large number of strategies for steganography have been utilized all through history, the first utilized of steganography back to 440 BC [6]. There are numerous Methods utilized such as; the physical techniques by utilizing the body and the material items, digital procedures, network techniques, and digital text strategy. Throughout history, there are a significant number of the stories about the utilization of steganography in a few strategies and procedures; the most prominent was the utilization of physical specialized. There is a story about king of Sparta "Demaratus". (from 515 until 491 BC) when he needed to inform Sparta that "Xerxes" is planning to attack Greece. To avoid being arrest, he scratched the wax off of the slabs then composed a message on the basic wood. Subsequently, he protected the slabs with a new layer of wax. This has helped him to keep the tablets look like new, and they can easily pass the inspection by sentries. Alternatively, the massage was recalled on a messenger head, which was shaved for this purpose. Subsequent hair growing will cover the message. The messenger's hair was shaved once again at the final destination for the message [4]. The use of current steganography started in 1985 [7] in the presence of devices being connected to conventional steganography issues. Below are some examples of these methods:

1. Concealing data inside the lowest bits of sound or images files.
2. Concealing data inside random data or encrypted data.
3. Including information in ignored sections of a file such as concealing information in altered executable files.
4. Hiding pictures in a video file.
5. Adjusting the echo of a sound file (Echo Steganography).
6. Making content the same color as the background in discussion posts, word processor documents and e-mails. .

Network steganography is an universal term of all data concealing methods that may be utilized for data exchange in tele-communication networks. "Krzysztof Szczypiorski" was presented this term in 2003 [8]. Network steganography utilize the communication methods control components and their fundamental intrinsic functionality, unlike the typical steganography techniques which apply digital media such as images, audio and video files as a cover for concealing information [9]. Typical network steganography strategies include change of the characteristic of the network procedure. Such alteration can be connected to the PDU (Protocol Data

Unit). [10, 11] said that "Unicode steganography utilizes twin characters of the typical ASCII set to look usual, while truly carrying additional bits of data. If the content is shown correctly, there should be no visual contrast from normal content. Some frameworks, however, may show the fonts differently, and the additional data would be effectively spotted".

At the present time because of the enormous amounts of sensitive and crucial information that is stored on computers and transmitted by the Internet, there is an critical need to guarantee security and safety of this data. Steganography and cryptography are strategies to guarantee security and safety of data.

Encryption is a science concerned with changing data into a form that is immeasurable to the reader; this data may be stored in the storage media or transported by means of communication systems [12]. The distinction between Steganography and cryptography is that Steganography conceals the existence of a message, whereas cryptography is making a message indiscernible even when the message is found by unauthorized parties [13]. Figure 1.1 demonstrates the encryption and decryption in cryptography.

Figure 1.1: Cryptography Processes

From [14].

In cryptography distinctive operations may be utilized according to the purpose of cryptography, for example, key generation, message authentication, secrecy or privacy, cryptography, and no repudiation; No repudiation is an approach to guarantee that a message has been delivered and received by the parties of communication, which imply that the sender of a message cannot later deny send the message and that the receiver cannot deny obtain the message [14].

Video Steganography is a method to conceal different sort of documents into a carrying video file. Depending on their size and their memory requirements, video Steganography can be significantly qualified than usual multimedia files. It is crucial for proper and operative embedding process to choose effective pixels in the file outlines, which are utilized to store the secret information. The least significant bit (LSB) insertion is a crucial approach for embedding data in a carrier file. Least significant bit (LSB) insertion strategy works on LSB bit of the media file to conceal the data bit. In this thesis, an information concealing scheme will be created to hide the data in particular frames of the video and in particular area of the frame by LSB alteration utilizing two different methodologies [15, 16].

1.2 Objective of the thesis

The main aim of this thesis is to improve data concealing of content documents in digital video file. In addition give an effective, high capacity and a protected strategy for video steganography, utilizing two different methodologies based on LSB approach.

1.3 Overview of the Chapters

This thesis is organized into six chapters:

Chapter One: The current chapter is the introduction to the general aspect of steganography and, objectives of the thesis**,** and the organization of the project.

Chapter Two: This chapter presents the terms and basic concept of steganography.

Chapter Three: This Chapter consists of the literature survey and the related works.

Chapter four: This chapter demonstrates the methodology of the proposed approaches.

Chapter five: This chapter shows the experimental work and discussion of results.

Chapter six: This chapter including the conclusions and the Suggestion for future work

CHAPTER 2

Terms & Basic Concepts of Steganography

2.1 Introduction

The appearance and the generally usage of the internet is thought to be one of the primary events of the most recent years, information become noticeably accessible on-line, all users who have a personal computer can without much of a stretch connect to the internet and search for the data they want to discover. The outcome is that everybody can read the most recent news on-line and furthermore consult computerized libraries; read about firms, colleges, cultural occasions, exhibitions, etc. but also the companies can offer their items through the Internet, using electronic trade [17].

In the last couple of years, there was a rapidly developing interest in ways to conceal data in other data. The fact that a boundless number of excellent copies can be illegally delivered driven people to study methods for embedding hidden copyright data and serial numbers in audio and video information; therefore individuals inspired to study and discover techniques for communicating secretly [18]. Information concealing science considers a wide research field, which includes numerous applications, for example, copyright security for digital media, steganography, watermarking and fingerprinting [19].

1. Watermarking applications normally applied for copyright security. In this application the message contains data, for instance, owner ID and a digital time symbol.
2. Fingerprint, in this technique, the owner hides a sequential digital which specifically recognizes the user of the information set. This information adds to copyright data enabling the follow up of any unapproved utilization of the data set back to the user.
3. Steganography hides the secret message inside another informational collection, which means conceal the presence of the message.

2.2 The Steganography

Steganography can be defined as a kind of concealed transmission process that basically signifies “covered writing” (as indicated by the Greek, the word stegano or “covered” and graphs or “to write”). The objective of this tool, is to conceal a data message inside unapparent cover medium, in order to keep these messages unrecognized. [20]. Although, some of these coded messages have been caught, it was not possible to decode them. While this secures the data hidden in the cipher, the arrest of the message can be

Similarly as harming because it informs the enemy that somebody is collaborating with an opponent. Steganography adopts the inverse strategy and try to cover all evidence that could refer to the communication process [21]. Basically, the data-hiding procedure in a Steganographic framework starts with recognizing a cover medium’s excess bits (those that would be changed without ruining that medium’s quality or the origin information values). The embedding procedure makes a stego medium through changing these excessive bits with data from the hidden message. Contemporary steganography will likely keep its simple existence untraceable. However, the steganographic frameworks, due to their diffusion nature, it leaves behind measurable follows in their cover media through adjusting its statistical sets. Along these lines, eavesdroppers can distinguish the distortions in the subsequent stego medium’s statistical properties. The way toward discovering these alterations is called Statistical Steganalysis calculations [22].

2.3 Steganography Categories According Carrier Types

There are many sorts of cover in which data are implanted. Some of which are public, another are not. Continuously, steganography users find new types of cover, in this way, types of cover cannot be counted. In every day we expect another kind of cover. Figure (2-1) demonstrates the main classifications of file formats that could be utilized in steganography.

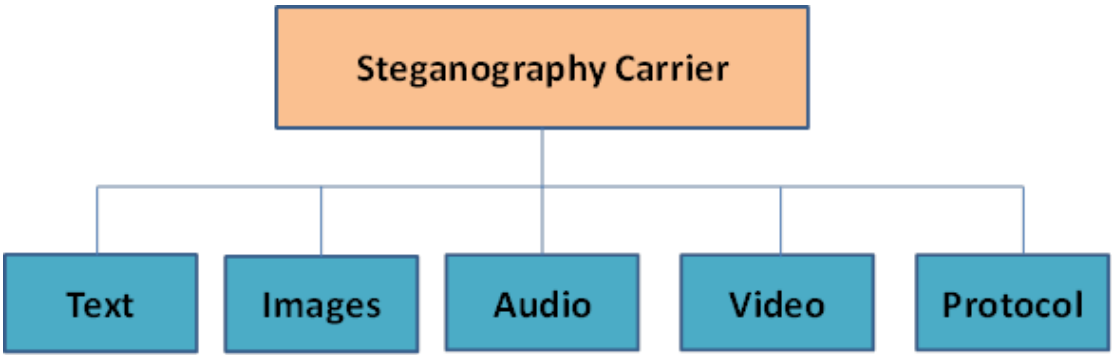

Figure 2.1: Steganography Categories According Carrier Types

From [22].

2.3.1 The Hiding in Text

Since everybody able to read, converted content in impartial information is doubtfully compelling. Yet, considering the start of each word of the earlier sentence, you will able to see that it is conceivable and it is not extremely difficult. Concealing data in simple content can be achieved in several ways [22]. Some methods include the alteration of the outline of a script, guidelines like utilizing each character or the modifying of the quantity of clear space after rows or within words [23].

Invisible inks turn to be a prominent medium. Computers convey greater capacity to information hiding. The layout of a document may likewise uncover information. Documents may be checked recognized by modulations in the places of lines and words. Including spaces and "invisible" characters to content gives a method to pass concealed information. An Interesting approach to see this is to include spaces and additional line breaks in an HTML file. Web browsers overlook these "additional" spaces and lines, however, uncovering the source of the web page shows the additional characters. For an extra text-based concealing strategies and an algorithm for mimicking the statistical distribution of content to pass data [22].

The last technique was effectively utilized as a part of training, after content has been written and derivative on sheet for several times, the confidential message can be recovered. Other likely method for putting away a confidential data inside a content is utilizing a freely accessible protection source, such as a newspaper or a book, and utilizing a code which comprises for instance of a mix of a character, line and page

number. In this way, no data put away into the cover template will prompt to the concealed text. Discovering these codes are exclusively depends on the background of these secret keys [24].

2.3.2 The Hiding in Image

Image is considered as an excellent media used to hold data by utilizing steganography strategies huge data contained in images give a decent range to conceal data in it. Image view may remove the detector attention from the hidden data, which give another reason to conceal data in image.

2.3.3 The Hiding in Audio

In the presence of computer-based audio steganography system, confidential messages can be hidden in digital sound. The confidential message can be combined by cautiously adjusting the binary arrangement of a sound file. Current audial steganography programming embeds messages in AU, WAV in addition to MP3 sound files [24]. Hiding confidential messages in digital sound is generally more problematic process than hiding information into other media, for instance, digital images. Keeping in mind the end goal to conceal confidential messages effectively, divers' strategies for hiding data in digital audio have been presented. This kind of methods run from rather straightforward algorithms that embed data in the type of signal noise to all capable techniques that can exploit sophisticated signal processing techniques to conceal data. The strategies that can be utilized for audio steganography are explained below [24].

1- LSB coding
2- Phase coding
3- Parity coding
4- Echo hiding
5- Spread spectrum

2.3.4 The Hiding in video

Video files are for the most part assembly of images and sounds, therefore, most of the accessible methods on images and sound can be functional for video files too. The great benefits of videos are the extensive quantity of information which could be concealed inside and the way that it is a stirring stream of images and sounds. Accordingly, any small, however generally visible alterations might go by overlooked by people due to the constant flow of data [25]. This method of steganography is the predetermined approach of this thesis; therefor it is going to be clarified in some details.

2.3.5 The Hiding in Protocol

The term protocol steganography implies to the procedure of embedding data inside messages and system control tools utilized in network communications [25]. In the pieces of the OSI network template there exist hidden channels where steganography can be utilized. A case of where data can be embedded is in the heading of a Transmission Control Protocol /Internet Protocol (TCP/IP) packet in a few areas which are either discretionary or are never been utilized [26].

2.4 Steganography Process

Steganography process has the following components (Figure 2.2):

1. **Secret message**: The information to be hidden which can be in the format of text, audio, video, or image.
2. **Cover – Media**: It assigns to the item used as a transporter to hide the secret message inside it.
3. **Embedding Algorithm**: Known as hiding message procedure.
4. **Extracting Algorithm**: Known as unhide/uncover the message procedure.
5. **Stego-media:** is usually refers to the generated object that can carry a hidden text.

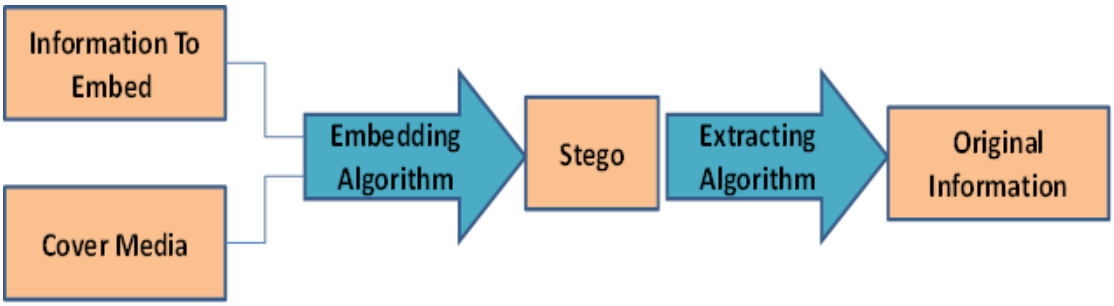

Figure 2.2: The Steganography Process

From [22].

2.5 Uses of Steganography

Steganography is used by the two sides of society, great individuals and terrible individuals. It is known that criminals of utilization a few of sorts steganography to smuggle files and instructions to their partners, hoping to keep away from the law. Dueling with this unlawful utilization of steganography is the examination center of Steganalysis. The good individuals Steganalysis to protect secrets and confidential files for instance it is utilized by government departments, banks, commercial entities in addition people who want to ensure their information.

2.6 Steganography algorithms

1. Spatial domain

In this algorithm the videos format can be described as a rectangular grid of pixels. The human visual system (eye), does not see an video as a grid [26].

2. Transform domain

This algorithm concentrates on representing videos that are anything but difficult to compress. Such methods are normally loss and subsequently form an approximation of the initial video with some loss of detail [26].

2.7 Security services offered by Steganography

Steganography guarantees the security of sensitive data by hiding information in other data, in this way confidentiality is offered. Identification and confirmation must

be offered if a steganographic key is utilized, since knowledge of the key can recognize a person to be who he says he is. Nonetheless, the way in which the data is hidden and the methods utilized could likewise serve as proof of identity. The strategy used to embed the data thus turns into the shared secret, and when accurately inserted and extracted provides a means of distinguishing proof and authentication by Steganography.

2.8 Steganography problems

Steganography is misused by keeping secrets that could be unsafe to innocent individuals. The greatest concern in the field of steganography is the rapid progression of research in Steganalysis, the counter-innovation of Steganography [27]. Because of the increase importance of copyright assurance; the watermarking procedure has numerous researchers consideration. The computer specialists and security analysts have perceived that the Illegal utilization of steganography may turn to a risk to the safety of the worldwide. Steganography could enable terrorists to impart in secret without law authorization knowing about this communication. Due to this threat, specialists have been succeeding to discover imperfections in existing steganography frameworks. These flaws are misused for the detection of concealed data, and also include the extraction and destruction of the concealed information [28].

2.9 Types of Steganography

As indicated by the embedding procedure, steganography can be classified into three main types. The main objective of them is to implant a secrete message in a computerized protection by utilizing a private procedure for each of them. They attempt to make stego-project and innocent cover perceptually comparable [29] they are:

2.9.1 The Pure Steganography

Pure steganography algorithms conceal data in a computerized cover without utilizing any sorts of key [29]. This strategy of Steganography is the minimum protected means through which impart cautiously in light of the fact that the source

and receiver can depend just upon the assumption that no different gatherings know about this secret message, [30]. In this technique stego-object contains the cover and the concealed message only [31]. The embedding procedure can be defined as a mapping:

$$E: C \times M \rightarrow C \ldots\ldots 2.1$$

Where;

C is the set of possible covers,

M is the set of possible messages.

The extraction process includes the mapping.

$$D: C \rightarrow M \ldots\ldots 2.2$$

And extracting the secret message out of a cover [32].

2.9.2 The Secret Key Steganography

This procedure utilizes a type of concealing key, which is known the secret key [29]. The stego-object contains the cover, concealed message and the secret key. Individual members who know the undisclosed key can turn around the method and realize the secret information. In contrast to Pure Steganography where an apparent unseen transmission channel is available, Secret Key Steganography swaps a stego-key, which makes it more vulnerable to interruption. The advantage to Secret Key Steganography is regardless of the possibility that it can be blocked; only individual who knows the secret key can solve the hidden information [30, 31].

The mapping procedure could be written as follows:

$$E_k : C \times M \times K \rightarrow C \ldots.. 2.3$$

And

$$D_k : C \times K \rightarrow M \ldots.. 2.4$$

With the property that

$$D_k (E_k (c, m, k) = m \ldots\ldots 2.5$$

For all c ϵ C and k ϵ K, is known as a secret key steganography system [32]

2.9.3 The Public key Steganography

This strategy utilizes two types of key to implant the secret message into the cover. The initial key is known as the private key, and the second key is called open key. The stego-object encompasses the cover, concealed message, private key, and the public key [29]. The correspondent will utilize the communal key amid the programming procedure and only the specific key, which has a direct numerical association with the public key, can analyze the secret message. Public Key Steganography gives a more powerful method of implementing a steganography framework since it can utilize plenty of robust and explored technology in Public Key Cryptography [30, 31].

2.10 Steganographic techniques for embedding data in digital Covers

Currently there exist a few methods of concealing secret data in a digital cover medium. All these procedure have different degree of achievement [33]. As indicated by [34], the following are the three essential information embedding techniques as utilized in digital steganography.

2.10.1 Substitution

The substitution procedure replaces the desired Least Significant Bits of the original image file with the bits of the secret data in a way that does not reveal any alteration to the original file. Substitution procedure is utilized as a part of the conventional Least Significant Bit algorithm.

2.10.2 Injection

This procedure adds bits to unused areas of digital files to conceal the secret message. This way, file bits related to an end-user are not changed sendoff the cover document perfectly functioning. The end-user sometimes cannot recognize that the file encompasses extra concealed data.

2.10.3 Generation

In contrast to substitution and injection, this strategy does not involve a standing cover file. This procedure produces a cover document for the sole purpose of concealing the message.

2.11 Famous Types of Steganography Methods

There are several sorts of image steganography, [29]. The common strategies are:

2.11.1 Least Significant Bit (LSB) insertion

Least significant bits (LSB) insertion is a straightforward procedure to hidden data in an image file. The easiest steganographic systems hide the bits of the message specifically into least important bit plane of the cover-video in a deterministic arrangement. Regulating the least significant bit cannot bring about human-perceptible distinction due to the sufficiency of the modification is minor [35]. For instance, if we analyze video steganography, then the letter A can be concealed in three pixels (accepting no compression). The unique raster information for 3 pixels (9 bytes) might be;

(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)

The binary value for A is 10000001. Inserting the binary value for A in the three pixels would generate

(00100111 1110100**0** 11001000)
(0010011**0** 11001000 1110100**0**)
(11001000 0010011**0** 11101001)

The underlined bits are the main three actually changed in the 8 bytes utilized. Typically, LSB involves that only half the bits in a video been altered. We can

conceal information at all and second minimum substantial bits and still the naked eye would not have the capacity to observe it [24].

2.11.2 Masking and filtering

Masking and filtering procedures, normally limited to 24 bits and gray scale videos, cover data by denoting a video, in a way like paper watermarks. These methods perform investigation of the video; consequently hide the data in significant areas so that the concealed message is more necessary to the cover video than simply concealing it in the noise level [35].

2.11.3 Transform techniques

Transform tools hide the message by modifying coefficients in a change area, for example, the Discrete Cosine Transform (DCT) utilized in JPEG compression, Discrete Fourier Transform, or Wavelet Transform. These techniques conceal messages in important areas of the cover-frame, making them more powerful to attack. Transformations can be connected over the whole frame, to obstruct all though the frame or other alternates [35].

CHAPTER 3

Literature Survey

3.1 Introduction

Recently, video steganography has turned out to be exceptionally well-known research area for concealing vast amount information behind video without being seen by the human eye and exchange it over the system with high security and without any deterioration in the quality of the video. Steganography is a data concealing method, which is utilized since the ancient times to assure the confidential data from the hacker‘s attacks utilizing different sort of computerized media like text, image, audio, protocol based and so on, and video steganography is one of the essential parts of steganography concept [36]. The key motive of video steganography is to conceal the secret data within the cover video. So it is a nontangible masking of confidential data. Steganography concept is unique in relation to the cryptography and computerized watermarking. As cryptography is a procedure of encrypting or alter the concealed message in an unreadable configure. It just scrambles the secret message bits and steganography is a procedure of concealing the presence of secret message by hiding it inside the video from intruders. It indeed ensures the confidential information. Digital watermarking is also information concealing method but, it saves the media file from being pirated and gives copyright insurance for authentication by implanting logos, captions and so on [37].

3.2 Digital video basics

Depending on the video standards, a set of frames that encompasses digital video can be played constantly at steady frame rates.. Number of pixels, frames per second (fps) as well as frame size are the parameters for computerized video quality.. As the fps value ranges from 24 to 30, it considered one of universal video formats. However, the other two standards represent the differences between videos.. Each video image named a frame that encompasses several pixels containing a set of

Colors (three or four) such as Red, Green and Blue (RGB), or CMYK Cyan, Magenta, Yellow and Black (CMYK). The remaining mediator colors are made from a collection of these basic colors [27, 38]. Generally, human eyes are sensible to green color, therefore, the number of bits of each color mixture can differ. Figure2 describes 16-bit color from which red and blue are comprising 5 bits while the green color having 6 bits. In the 24-bit RGB standard, each color contains 8 bits length and has 256 options in color intensity. Whereas, the 32-bit CMYK standard is needed, and this parameter is mainly utilized contemporary computer displays [39].

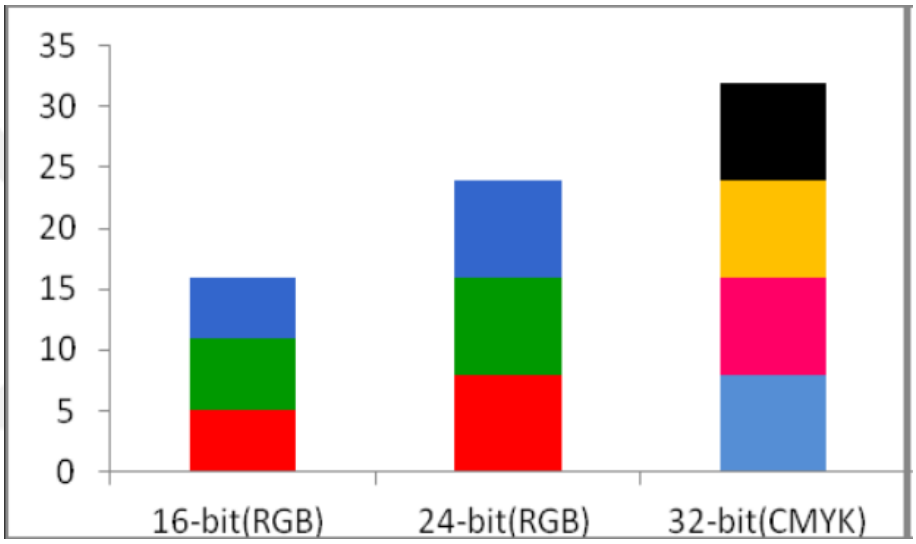

Figure 3.1: Overview of bit distribution of digital image of 16-bit (RGB), 24-bit (RGB), 32-bit (CMYK)

From [27].

3.3 Video steganography properties

A good quality video steganography should have three properties [40], which are clarified as follows:

1 .Capacity

It implies the total amount of information or number of bits that can be concealed inside carrier video. It characterizes the maximum size of the secret message or its length.

2. Perceptual Transparency (Perceptibility)

The information should be concealed in such a way that it should not be noticeable to the human visual framework. So it should be transparent. If we increment the limit of information then its transparency will be influenced. Perceptual transparency is of two sorts: Quality and fidelity.

3. Security

Attackers can extract the important data by applying different attacks. So security of video steganography should be high utilizing different encryption and security algorithms.

3.4 Video Steganography Benefits

Video steganography is the field of computerized steganography that is less investigated than image steganography, yet it gives a set of advantages [41]:

1. The changes are less detectable for the human visual framework as frames are noticeable only for a short length of time;
2. Frames individually can be less clear and focused, small colour changes are not as visible contrasted with photography.

3.5 Video steganography methods

Video steganography techniques can arrange in different ways [41]:

1. By compression:
   - ❖ Methods for compressed video files;
   - ❖ Methods for uncompressed (raw) video files.

2. By embedding domain:
   - ❖ Spatial domain;
   - ❖ Transform domain (discrete wavelet transform – DWT, discrete cosine transform – DCT, etc.).

3. By embedding method:
   - ❖ Embedding into still images;

- ❖ Embedding based on the video codec;
- ❖ Embedding based on the video format.

As most of the videos on the World Wide Web are compressed video files and a raw video file alone can raise doubt [42].

3.6 Techniques of video steganography

Video steganography can be utilized in different strategies. The most suitable one is to conceal the confidential information in which the quality of the cover video is not affected, so that it might not be recognized within human vision. The concealed video is distinguished as the "stego" video which is reached to the recipient side via the sender [43]. Different type of video steganography procedures is utilized for the time being, to protect essential data. Some investigated techniques are briefly clarified in the following sections, and their comparisons are explained in table 3.1.

3.6.1 LSB method

This procedure is popular standout amongst the most prominent methods for the security of information due to its ease and as often as possible utilized approach. For embedding the information, it is the least complex and effective approach. In this procedure, the pixel values (bytes) of cover videos are eliminated, and then its least significant bits are substituted by the secret bits that we will be embedded. The virtual look of the actual host video will not be distorted if we only change its LSB bits [44].

3.6.2 Non-uniform rectangular partition

This procedure is utilized steganography for unpacked domain; by concealing an uncompressed confidential video document in the host video file we can conceal the information. But we need to guarantee that both the confidential and the cover file must be of the equivalent dimensions. The secret video will be hided in the leftmost 4 LSB bits of all frames of the source video [44].

3.6.3 Compressed video steganography

This procedure is for the packed videos only, where information can be hidden in block of frame with extreme part modification and in P and B block with extreme enormousness of signal directions [45].

3.6.4 Anti-forensics technique

These methods are the exercises which are involved to damage, hide and operate the information to attack the computer legal sciences. It offers security for shielding from unofficial people. Steganography resembles anti-forensic where we attempt to hide information under host file. Steganography and anti-forensics at the same time makes the system more secured from unauthorized access [44].

3.6.5 Masking and filtering

This approach is taken a shot at 24 bits/pixel images and is appropriated for both gray and colored scale images. It looks alike as watermarking overlapping an image and doesn't altering the perfection of the image. Comparing to other methods, in data covering the confidential message is very processed so that it would appear as multimedia document. Information masking cannot easily be disclosed by predefined steganalysis [44].

Table (3.1): Comparison of Video Steganography Techniques.

Video Steganography Techniques	Descriptions	Advantage	Limitations
LSB method	The cover video's pixel values are extracted (in bytes), then its LSB are replaced by the secret message bits that we will embed.	Easy to embed the data & implement & high message payload.	Easy to embed the data & implement & high message payload.
Non uniform rectangular partition	Hiding an uncompressed confidential video file in the source video stream with most similar size.	Conceal a source video without any alteration in source video.	Confidential and cover files must be in the same size..
Compressed video steganography	Data hiding operations are executed entirely in the compressed domain.	Extraction of data without requiring original video.	Useful only for compressed videos.
Anti-forensics Technique	Hide data under some host file.	Prevent data from unauthorized access.	Mainly used to attack the computer forensics.
Masking &filtering	Hide a signal by different signal	Can't easily detected, useable for both gray and colored scale images, more robust	It can be detected by simple statistical analysis and tools & apply only to gray scale images.

3.7 Image processing

Image processing is a procedure to improve original images captured by cameras (sensors) attached to satellites, aircrafts and space probes. in addition to pictures collected from daily life for different applications. Different methods have been investigated in image processing in the last five decades. The majority of the methods are produced for improving images acquired from military reconnaissance flights, remote-controlled spacecraft and space probes. Image processing frameworks become noticeable due to easy acquiring of effective devices, for example, personnel computers, graphics software's and large size memory devices.

Image processing is utilized as a part of different applications, for example:

(Remote sensing, medical imaging and film industry). The regular steps in image processing are image scanning, storing, enhancing and interpretation. There are two procedures accessible in Image Processing:

Analog image processing assigns to the modification of image through electrical means. The most widely recognized example is the television image[46]. Digital image processing in this case, digital computers are utilized to handle the image. The

image will be transformed to digital form utilizing a scanner – digitizer and then prepare it. It is characterized as the subjecting numerical representations of objects to a set of operations to achieve a desired result. It begins with one image and creates a changed form of the same. It is hence a procedure that takes an image into another. The process of a two-dimensional picture acquires by a digital computer is known as digital image processing. In a more extensive context, it means computerized processing of any two-dimensional information. A computerized image is an array of real numbers represented by a limited number of bits, the main characteristic of digital image processing techniques is its repeatability, flexibility and the preservation of unique information precision [47].

3.8 Digital Image

A digital frame is a two – dimensional matrix of the intensity values, every component in this matrix is assigned as pixel. Pixel values (intensities) specify image colors in the pixel. Images can be categorized based on the color of the image, or on the bits needed to represent a pixel (depth). In addition, there are other different orders of images as indicated by other features, which can be found in [29].

3.8.1 Types of Digital Image

There are four main sorts of images as per the scope of the image colors, some of the them has an inner categorization, these types are:

3.8.1.1 Gray – Scale Image

Gray scale image is also known as gray level image. It is an array of single class (uint8) or double class (uint16) whose pixel values determine intensity values [48]. The pixel values of paired image can be extended to (0-256) range, in which there are 256 color accessible, White, Black, and 254 levels of gray color. This image may provide a good quality view when color details are not required, or less capacity region are accessible, see figure (2-4). If the color levels are of another color (Red, Green, or Blue), then the image is known as a Monochrome image [29]. Paired image can be obtained from gray scale image, by specifying a threshold and setting any value greater than threshold to (255) and the other to (0).

Figure (3.2): The Gray scale image

3.8.1.2 Binary Image

In this sorts of images, there are only two colors white and black, every pixel value is either (1) for white, or (0) for black. Paired image demonstrates the boundaries of the objects in the image, with on inner detail see figure (2-5). Paired images can be utilized in screen controlling of industrial production lines, edge identification in image enhancement applications, and numerous different applications [29].

Figure (3.3): The Binary image

3.8.1.3 The Color Image

It can be recognized as an RGB image, each pixel in a true color image is determined by three values; one for each component (red, blue, and green) of the pixel scalar [48]. There are three basic colors Red (R), Green (G) and Blue (B), i.e. any color can be created by mixing them Instead of storing massive number of colors, computers store three values for every pixel R, G, and B respectively and produce colors by showing these values on the screen at the same time, see figure (2-6). This system is called RGB framework [29].

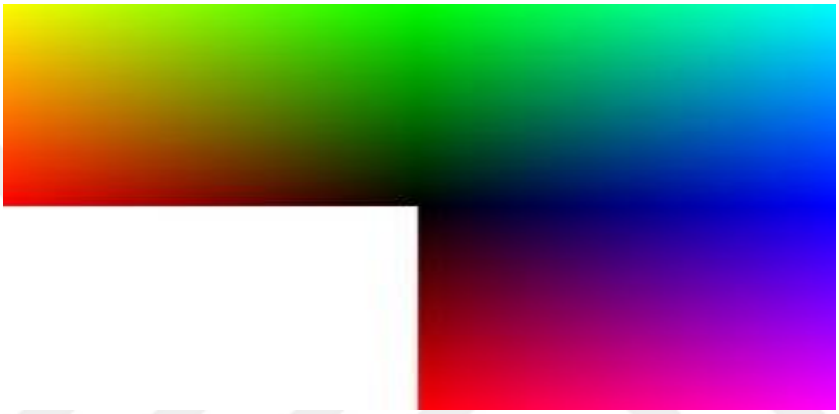

Figure 3.4: The color image

3.8.1.4 Multi-spectral Image

This type of image commonly contains data outside the normal human perceptual range. This may encompass infrared, ultraviolet, acoustic, or radar images are not images in the typical sense since data represented is not specifically visible by the human visual system. It can be shown as a visual mode by mapping the diverse spectral bands to RGB system [29].

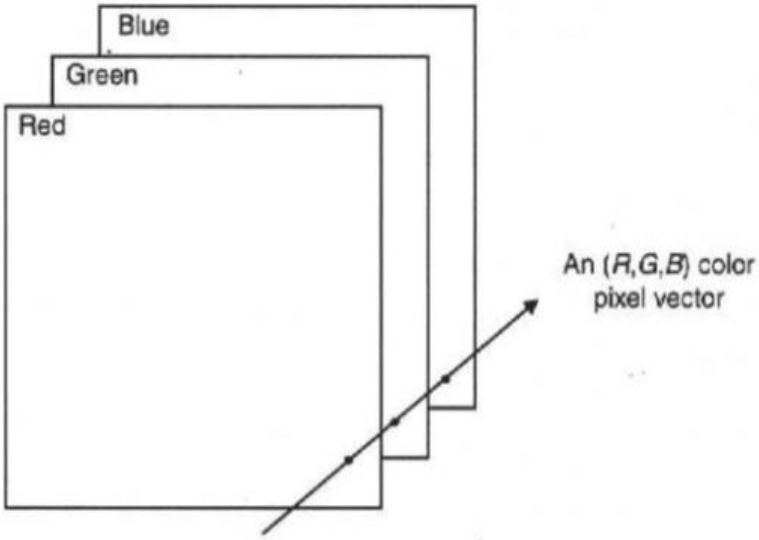

Figure (3.5): The RGB System of Color Image

3.8.2 Types of Image Depths

There are various types of Image as indicated by the depth bit per pixel (BPP), [29], and for each BPP there are (2 Bpp) colors range in the frame. The most utilized structures in windows applications are:

1. Binary frame (1BPP)

2. Gray scale frame (8BPP)

3. 16 Colors frame (4BPP)

4. 256 Colors frame (8BPP)

5. True colors (24BPP)

3.9 Related Work

The first introduction of video steganography framework in light of non-uniform rectangular partition was by ShengDun Hu, KinTak U in 2011. This method is utilized in unpacked videos. Video steganography is used to conceal a confidential video in a cover video and both should be in similar size. In order to conceal the

video stream, a mechanism should be connected to each frame of the both videos. Each frame of confidential video is divided into non-uniform rectangular part which is encoded. T furthest four least significant bits of each frame of the host video stream is the place where the confidential video stream is concealed in. By utilizing this method, changes cannot be observed; therefore, no one will consider the sort of information that has been concealed in the frames. It is worth mentioning that all the PSNR values of the frames that have been used were larger than 28db [49].

The application of LSB matching revisited algorithm has been investigated on Video Steganography by R. Shanthakumari and Dr.S. Malliga in 2014, where the video stream of AVI was the format. . In their paper they have divided the cover video into frames. Nowadays, the size of the message does not make any difference in video steganography technique, because the message can be embedded in multiple frames. To form the stego video, all embedded multiple frames of the cover video must be grouped together. This video will then be divided again into frames and the information will be removed from the receiver side. The proposed technique in this paper was found to have two issues which were low inserting rate and lack of security. LSBMR algorithm has a low replacement rate and thus the Mean Square Error (MSE) is low, because of which LSBMR is more secured than the LSB algorithm for information concealing. The PSNR value decreases on increase of the inserting unit [50].

An improvement on LSB based Video Steganographic System for Secure and Efficient Data Transmission has been investigated by. In this work, the researchers have spitted the host video into frames, and to embed the file, they compacted it utilizing the ZIP compressor. The main purpose of compressing information before loading them over the network is to minimize additional burden of the network. Also, the color can be computed in RGB 24 bit format for each color pixel. The removed bytes of the confidential message are used to generate chunks of bits which then are embedded in the video frames. Before sending the video files, text files are merged with them. Although the suggested method is basically designed for MPEG file format, it can also be used for other type of video file format such as 3GP and AVI. In their calculation, they found that the Mean Squared Error(MSE) and Peak Signal to noise ratio(PSNR) was sufficiently low, that it cannot be seen easily in the Steganalysis procedure. Then they have additionally contrasted their procedure with

LSB technique and they discovered that the proposed method presents better MSE and PSNR values than the LSB technique [51].

A LSB based hybrid method has been used to demonstrate a video steganography by Hemant Gupta, Dr. Setu Chaturvedi in 2013, and this approach is utilized in AVI videos. This video is transformed into 20 equivalent gray scale images. Information concealing is complete in the host video by utilizing Single, two and three bit LSB substitution and after that Advanced Encryption Standard Algorithm is connected. The information concealing methods are used to process the source video and the encrypted AVI video is then sent to be decrypted by the recipient. They also discovered the PSNR and correlation factor between Original and embedded image for one, two and three bit LSB substitution and AES approach. They also noticed that with the increase of LSB substitution bit, PSNR value decreases and security increases. In addition to that, they discovered no correlation between encrypted image and original image for various frames [52].

A framework based on least significant bit procedure was applied by Eltahir, L. M. Kiah, and B. B. Zaidan to introduce a high rate video streaming steganography [22]. When this method applied on instant images, it can save up to 33.3% of the image for information concealing, and enhancement of LSB accordingly. The idea of the proposed technique is by utilizing 3-3-2 method, which utilizes the LSB of RGB (red, blue, green) colors in 24 bits image. In this procedure, the least 3 bits of red, 3 bits of green and only 2 bits from blue color are taken. This is because human vision framework is more sensitive to blue than green and red, to think of 1 byte which is utilized for information concealing. This method (3-3-2) is very efficient to generate high resolution image. The size of the obtained information was significant (33.3%), as the human vision system particularly was not able to distinction between the two frames and their histograms [53].

A video steganography with encryption and LSB substitution approach was presented by Pooja Yadav, Nischol Mishra and Sanjeev Sarma in 2013. They had two video streams; host and the secret video. Those videos had the same number of frames and equivalent frames per second (12 frames and 15 fps). A header of 8 bits was attached in the beginning of each frame, to show the frame size of the concealed video.. After this, a symmetric encryption was utilized to encrypt the attached header and the secret frames. By applying sequential encoding, secret videos are encoded to the host videos, subsequently, secret videos are created. In order to recover the

original data, they utilized XOR transformation through which secret keys were used to encrypt and decrypt the secret message. Message encoding in the LSB, was successful via utilizing a pattern of BGRRGBGR (Blue (B), green (G) and red (R)). 2 AVI video files were used and similar PSNR values (35 dB) were observed for both stego video and host video. To evaluate the result, they calculated the PSNR value, frame by frame, ultimate, least and average PSNR value of total frames. No distortion was observed between the stego and the host video when a frame by frame comparison was applied. This has indicated the similarity between the host and the embedded video. The host video was observed to be less altered and furthermore the recovered video stream had additionally a reliable quality [54].

CHAPTER 4

Proposed Methodology

4.1 Introduction

All the communicating bodies need the privacy, integrity and authenticity of secret data. Different methodologies are utilized to adapt to these security issues like computerized certificate, digital signature and cryptography however these techniques alone cannot be compromised. Steganography is the best solution to these problems as it conceals the presence of secret information. This proposed method presents video steganography for information embedding and extracting embedded data in video files by utilizing LSB insertion approach. The technique implements two methodologies for hiding data [15, 16]. The following section outlines these two methods in details.

4.2 Video Steganography Approach

The designed and implemented framework works in two segments; Embedding and extraction procedure, Figure (4.1):

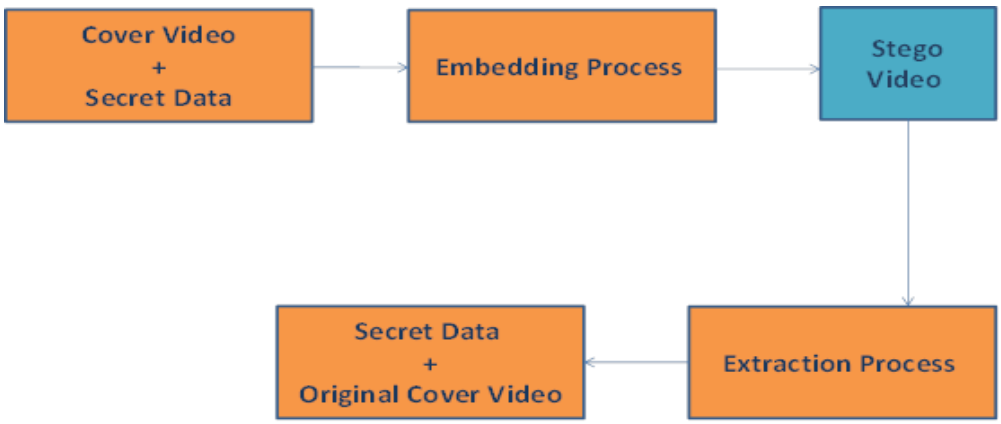

Figure 4.1: Process of Video Steganography.

From [26].

In embedding procedure, we essentially conceal the secret information inside video utilizing the proposed inserting algorithms and this process is performed at the sender side. while; extraction process is completed at the receiver side and only approved users can extract secret message utilizing Stego key, which is recognized by sender and receiver only to increase the security of concealing information from intruders. It is the reverse procedure of embedding segment. These two functions included several sub functions to finish the job, which can be illustrated as figures below:

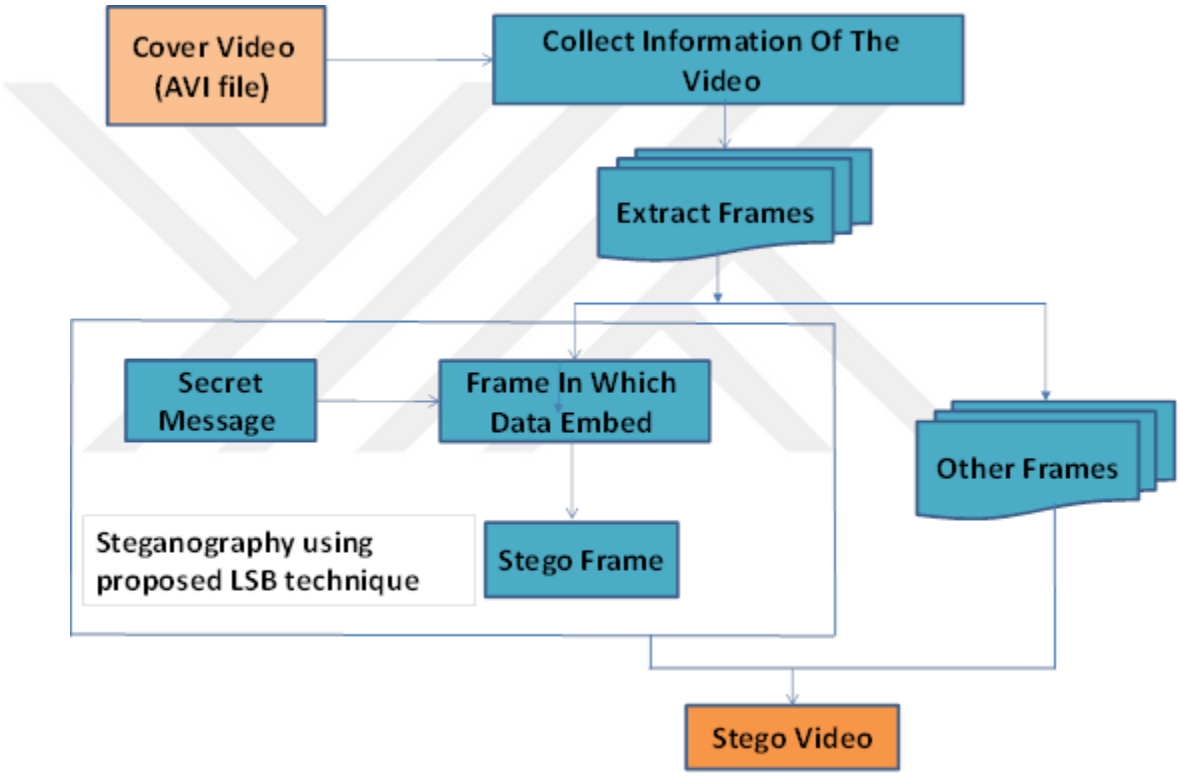

Figure 4.2: Block Diagram of Embedding Process for Video Steganography

From [26].

A Video stream (AVI) comprises of collection of frames and the secret information is embedded in these outlines as payload. The cover video is then separated into outlines. Presently the proposed algorithm is performed to hide the data in the carrier outlines. The size of the massage does not matter in video steganography as the massage can be embedded in multiple outlines. After hiding information in multiple

frames of the carrier video, frames are then organized together to design a stego video, which is presently an embedded video.

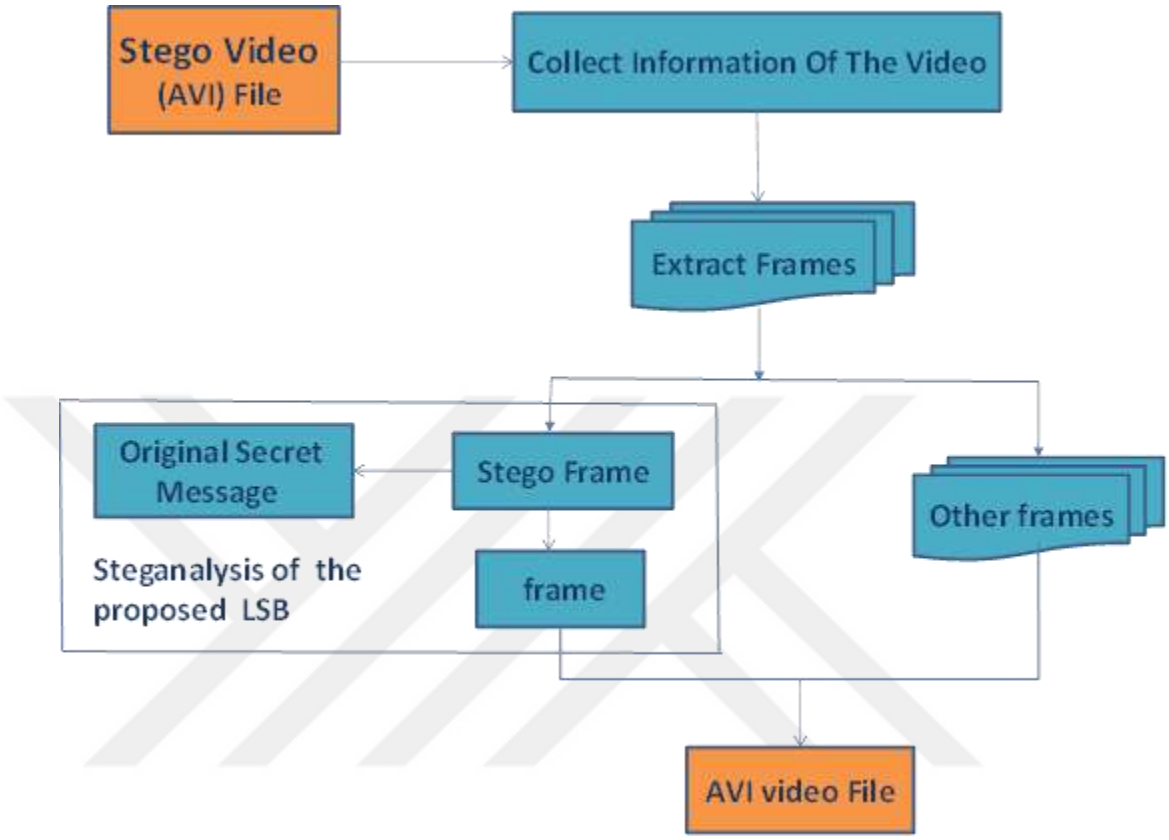

Figure 4.3: Block Diagram of Extracting process for video steganography.
From [26].

In the receiver side, the reverse steps are utilized to translate the secret information, the stego video and cover video file is read and collected frames information then extract those frames on which information is concealed. Then extracting algorithm is performed utilizing secret key on chosen frame to obtain the initial message from frame.

To assess the efficiency of the proposed method different parameters are utilized MSE, PSNR and Histogram analysis for every video after concealing a secret message in the videos to investigate the effect of quality.

The embedding algorithms are classified into two essential domains i.e. spatial domain and transform domain. Spatial domain manages a video file as it by exchanging the secret bits with video frame‘s pixels directly. It is also called as time

domain. The most fundamental spatial technique is least significant bits (LSB). Our proposed approach is depend on the (LSB) method, two algorithms for hiding information in cover video are implemented in this thesis, sorted as follows:

4.3 Least Significant Bit (LSB)

Least Significant Bit is the oldest and simplest technique that have been used for steganography. Secret information is hidden into least significant bits of a byte representing an intensity value of a pixel [55]. The criterion of using only LSB or last two, three or four LSBs are based on the amount of data to be hidden and the importance of the secret data and also the type of cover video and frequency of the pixels used in a video. Therefore, best LSB steganography algorithm can be designed on the basis of the above parameters of a cover video and secret information that have to be hidden. The stego-video is the result after the secret message is embedding. The binary code below represents the process of message embedding in cover video.

Cover video Pixels:

00110011 11101001 01101010 10101001
11011000 10001101 10001100 01101101

Secret Message:

1 0 0 0 1 1 1 0

Result (Stego-video):

00110011 1110100**0** 01101010 1010100**0**
1101100**1** 10001101 1000110**1** 0110110**0**

For RGB, a technique from [56] alternates the least significant bits of each pixel of Red, Green or Blue with the secret message bits. The result of the LSBs alternation causes minor changes in the RGB colors and therefore, it is difficult to be noticed by the human eye.

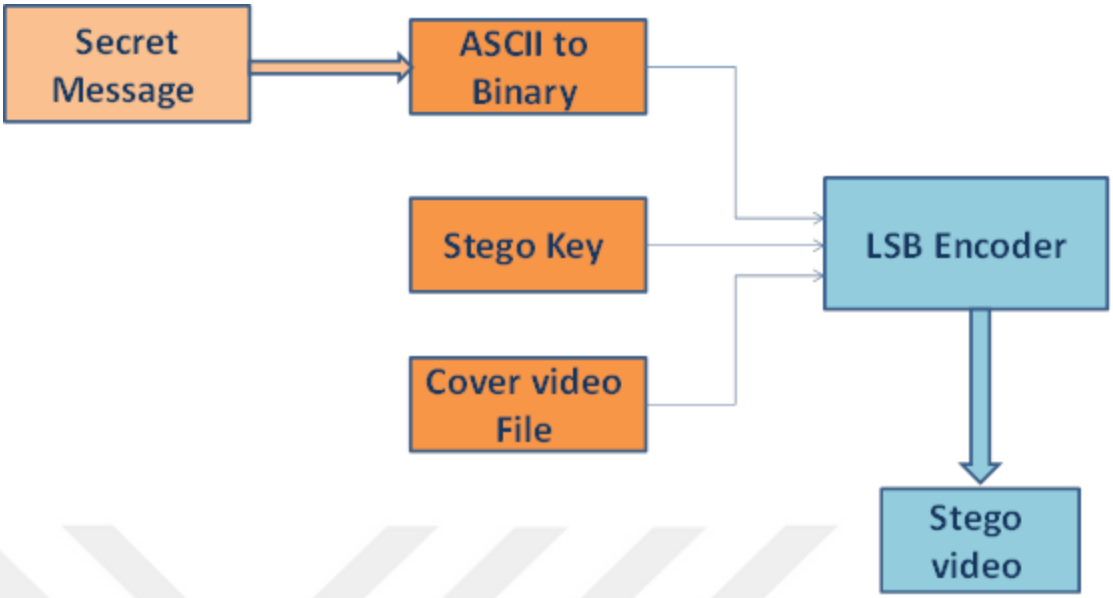

Figure 4.4: LSB insertion mechanism

From [26].

4.4 Improved LSB technique for video steganography (First Approach)

An improved method of LSB technique has been developed. According to this method, all three colors are required for embedding the secret code. As only manipulating of the least significant bit of the pixel is not enough for information hiding.

Therefore, the data is hidden in all three color component i.e. red, green and blue of the host frame by EX-oring of the data bit and pixel bit. The confidential message is transformed into binary sequence and each bit is Xored with R-component pixel value of host frame. The resultant XOR value is utilized to manipulate the R-, G- and B-component frames for binary sequence insertion to generate the stego video. A reversed process can be applied to extract the inserted code from the stego video. Three parameters (i.e. MSE, PSNR and histogram analysis) for host and stego videos are used to assess the functionality of the algorithm. Using the three color component

can improve the embedding area for the host video three folds. These method allows three folds space in host video to hide as many textual information.

4.5 The Proposed video Steganography Algorithm

The proposed algorithm for hiding secret message in an input video (AVI format) is implemented as follows:

Embedding Algorithm

Input: Cover Color Video, Secret Massage.

Output: Stego Video.

- Load cover video file.
- Read cover video data.
- Calculate the Embedding Capacity of the cover video.
- Extract cover video file to separate frames.
- Select frame to embed secret message randomly.
- Decomposition of input frame into red, green and blue color component images.
- Conversion of secret message into binary form.
- Sequencing each character (binary form) of message in single column matrix (array).
- Get the length of the binary array (character) or no. of bits to be embedded in Host frame.
- Generate the random locations in host random equal in no. of bits to be embedded.
- Generate the two LSBs of first location pixel from red component frame and XOR with first bit of frame to be embedded.
- If the XOR result is '00' or '11', then exchange the red component pixel with bits to be embedded. If XOR (RLSB, MB) = 00. OR If XOR (RLSB, MB) = 11. Then, RLSB = MB

  Where, MB = Message Bit.
- If the XOR result is '01', then exchange the green component pixel with bits to be embedded. If XOR (RLSB, MB) = 01. Then, GLSB = MB. Where, MB = Message Bit.

- If the XOR result is ‘10’, then exchange the blue component pixel with bits to be embedded. If XOR (RLSB, MB) = 10. Then, BLSB = MB. Where, MB = Message Bit.
- Concatenate the R-, G- and B-component frames to get stego frame.
- Generate the stegno video file by compose the stegno frame with rest frames .
- Evaluate the performance indices mean square error, peak signal to noise ratio, Histogram analysis.

End Of Embed Algorithm.

Extraction Algorithm

Input: Stego Video.

Output: Secret Massage.

- Load stegno video file.
- Read stegno video data and information.
- Extract stegno video to separate frames.
- Get stegno frame.
- Decomposition of stegno frame into red, green and blue color component frame.
- The key file is used to get the stego coordinates.
- The stego coordinates and XOR value are used to get the R-, G- and B-constituents color information. XOR to get LSB bits values.
- get back the Least Significant Bit (LSB) in order to convert the binary sequence into ASCII code.
- This is the message that was embedded using Least Significant Bit.

End of Extract Algorithm.

4.6: The proposed Bit Inversion Technique (Second Approach)

Least significant bit (LSB) inversion method is a process that inverses the bit of each pixel within the cover-video based on the values of the secret video. This standard LSB method can be completed when all secret messages' bits are embedded or hidden in the cover-video. The proposed inversion technique based on the comparison between the cover-video (i.e., 2nd last and 3rd last bit) and the bits from the stego video, which can be obtained from applying the standard LSB method.

The step-by-step process of the proposed method is as follows:

1. Calculate the pattern occurrences of these two bits on the cover-video, which are either 00, 10, 10, or 11. Classify the cover video according to these four patterns.
2. Apply the standard LSB method to obtain the stego-video.
3. from the stego-video, once again, calculate the pattern occurrences in the 2nd last and 3rd last bit of the stego-video. From these patterns, we use them as a guide for the inversion steps.
4. Compare between each pattern from cover video with the same pattern in the stego-video.

Step five: Inverse the LSB bits if the number of pixels that have been changed is greater than the number of pixel that has not change.

5. Store the status of the patterns that inverse its pixel in specific location.

In order to recover the secret message from the stego-video, we need to save these patterns for which the corresponding LSB bit is inverted. Since we have checked all possible combinations of the 2nd and the 3rd bit of all pixels, we may need to store maximum of 4 patterns information in the stego video. Secret message that are exhibited in the stego-video can be recovered by storing these patterns for which the corresponding LSB bit is inverted. Therefore, in de-steganography, the information that guides us to the pixels patterns that has been inversed is to firstly read from the stego-video to be able to identify the inversed and non-inversed patterns. After that, the stego-video is classified according to the four patterns and then re-inversing the bits to extract the massage bits.

4.7 The proposed Bit Inversion Technique Algorithm

Embedding Algorithm

Input: Cover Color Video, Secret Massage.

Output: Stego Video.

- Load cover video file.
- Read cover video data and info.
- Calculate the Embedding Capacity of the cover video.
- Extract the cover video to separate frames.
- By using encryption key Select frame to embed secret message inside it .
- Decomposition of stegno frame into red, green and blue color component frame.
- Decomposition of stegno frame pixels into red, green and blue component.
- Convert secret message to ASSCII code characters.
  For i = 1 to n Get char from msg

For each 2 bits Get pixel from frame For each colour from green and blue Get colour value Cover value = value Identify the pattern of 2nd and 3rd bits of the Cover value which are either (00, 01, 10, or 11) If msg bit = 1 Insert a 1 in the lest significant bit of the pixel value Else Insert a 0 in the lest significant bit of the pixel value Replace the value in the frame stego value = value Identify the pattern of 2nd and 3rd bits of the stego value (00, 01, 10, or 11)

End for
End for
End for
For i = 1 to n

- Compare between cover value and stego value to count how many pixel are changed and how many are not If number of changed pixels in any pattern of frame was more than pixels that not changed in alternative pattern in the stego Get pixel from frame For each colour from green and blue Get colour value

  If the last significant bit of the value = 1 Insert 0 in the last significant bit of pixel value Else Insert 1 in the last significant bit of the pixel value Replace

the value in the frame Store the status of pattern that inversed his pixels as a map in specific location End for End for.

- Compose the stegno frame with rest frames and create stegno video file.
- Evaluate the performance indices mean square error, peak signal to noise ratio and Histogram analysis.

End Of Embed Algorithm

Extraction Algorithm

Input: Stego Video.

Output: Secret Massage.

- Load stegno video file.
- Read stegno video data and info.
- Extract stegno video to separate frames.
- By using number of frame get stegno frame.
- Decomposition of stegno frame into red, green and blue color component frame.
- The key file or encryption key is used to get the stego coordinates.
- The stego coordinates and XOR value are used to get the R-, G- and B-constituents color information. XOR to get LSB bits values.
- Get back the Least Significant Bit (LSB) in order to convert the binary sequence into ASCII code.
- This is the message that was embedded using Least Significant Bit.

End of Extract Algorithm

CHAPTER 5

Simulation Studies and Results

5.1 General Introduction

Any steganography system is characterized generally by two properties, imperceptibility and capacity. Imperceptibility means the embedded information must be imperceptible to the eyewitness (perceptual invisibility) and computer examination (statistical invisibility). The efficiency of the proposed method is assessed utilizing three different videos (Cat.avi, Road.avi and Train.avi) and one secret information (message). The perceptual imperceptibility of the embedded information is shown by comparing the initial video to its stego counterpart so that their visual differences, assuming any, can be resolved. Moreover, as a goal measure, the Mean Squared Error (MSE) and Peak Signal to Noise Ratio (PSNR) between the stego frame and its relating cover frame are examined. Histograms demonstrate the frequency distribution on the color videos. Contrasting histograms of two same looking videos can give a thought if there is any alteration on videos. The quantities are given as below.

5.1.1 Mean Squared Error (MSE)

MSE is the ratio of sum of the square of the differences in the pixel values between the comparing pixels of the two videos over total pixel number. MSE can be calculated if two videos dimensions are equal. If two videos are identical MSE value is 0. Formula (5-1) illustrates how to calculate MSE value [57].

$$MSE = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(\alpha_{i,j} - \beta_{i,j})^2 \cdots\cdots\cdots (5-1)$$

M: numbers of rows of cover video

N: number of column of Cover video

α_{ij}: Pixel value from cover video

β_{ij}: Pixel value from Stego video

Higher value of MSE indicates dissimilarity between Cover video and Stego video.

5.1.2 Peak Signal-to-Noise Ratio (PSNR):

PSNR is the standard estimation utilizes to examine the quality of the stego videos. PSNR describes ratio lies between the maximum possible power of a signal and the power of corrupting noise that influences the fidelity of its demonstration [58]. In this situation, the signal is the cover video, and the noise is the error that is presented by the bits of the secret information. Higher value of PSNR implies higher quality of the stego video. To demonstrate that, consider a cover video C of size M × M and the stego-video S of size N × N. Then, each cover-video C and stego-video S will have pixel values of (x, y) from 0 to M-1, and 0 to N-1 respectively [59].

$$PSNR = 10 \log_{10} \frac{MAX^2}{MSE} \cdots\cdots\cdots (5-2)$$

Where MAX is maximum possible pixel value of video a (i,j). MSE is the mean square error.

A large PSNR value brings up that the difference between cover video and stego video is significantly considered unobserved to the individual eye.

5.1.3 Histogram Analysis

In steganography, mainly, histogram analysis is utilized to compare video pixels between the cover video and the stego video. Histograms show the number of pixels that have colors in each fixed list of color ranges and span the video's color space. It encompasses a group of every single possible colors in a video.

$$n_i = \sum_{i=1}^{k} m_i \cdots\cdots\cdots (5-3)$$

k is the maximum pixel value in an video, m is the pixel value, and n is total repetition of n in video [60].

5.2 Embedding Capacity Calculation of the cover Video

Embedding capacity is considered as an important characteristic term for video steganography. Embedding capacity is calculated by using the following formula;

$$EC = \sum_{i=1}^{n}\sum_{j=1}^{m} n(i,j) \cdots\cdots\cdots (5-4)$$

$if \bar{x}(i,j) > Threshold$

$\bar{x}(i,j)$ is a quantized wavelet coefficient matrix,

m is a number of rows and n is number of columns,

Then (i,j) is the adaptive embedding depth for each quantized wavelet coefficient$\bar{x}(i,j)$.

5.3 Software's used for Algorithm Implementation

The practical platform was programmed in MATLAB Version 8.6 R 2015b, MATLAB is a fourth-generation programming language and numerical analysis environment (Figure 5.1). The main functions of MATLAB are: matrix calculations, developing and running algorithms, creating user interfaces (UI) as well as information visualization. Programming developers were able to interface with programs created in various languages due to use of multi-paradigm numerical calculating environment. This makes it possible to harness the unique advantages of each language for different purposes. MATLAB is can be utilized by engineers and researches in many fields, for example, communications, image and signal processing, smart grid design, control systems for industry, robotics as well as computational finance [61].

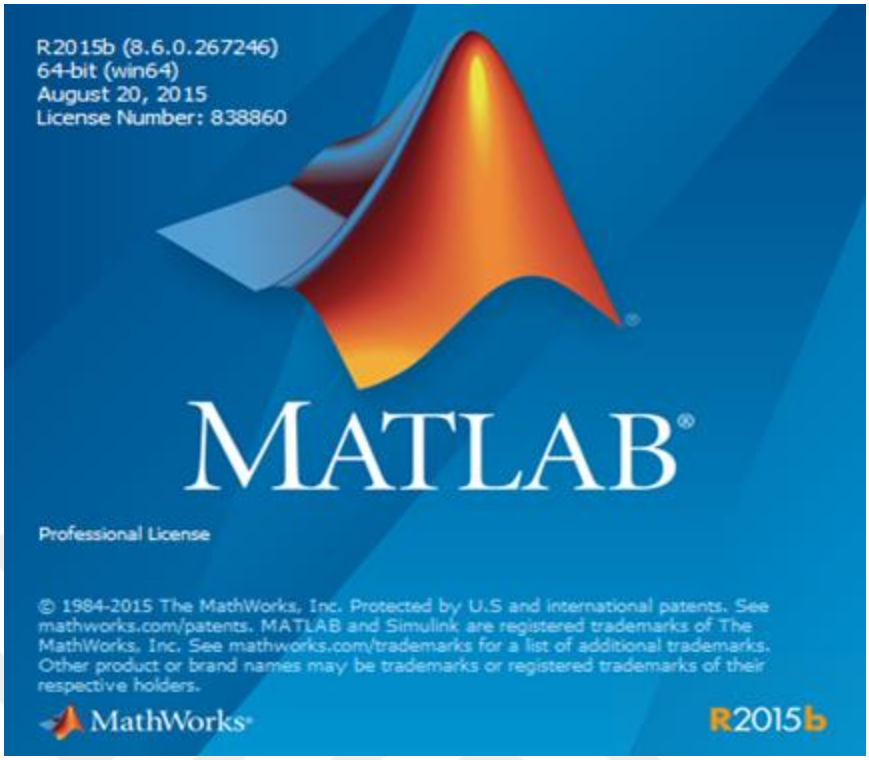

Figure 5.1: MATLAB version

5.4 Input (AVI) Video File Data

The proposed specified methodologies is based on the examination to conceal message into video (AVI) file format which gives a robust and secure approach of information transmission. The proposed inserted video steganography has many strengths like ease of use, straightforward and successful process of implanting secret message with greater security. Three different video files that carry out as a cover for encrypted secret information are utilized; properties of the test videos are characterized in table 5.1.

Table (5.1): Properties of the Tested Videos.

S. No.	Cover Video File Information					
	Name of video file	Size	Resolution (W*H)	Frame/Sec.	No. of Frames	Embedding capacity
1	Cat.avi	29.2 MB	240*176	24	241	126720
2	Road.avi	19.3 MB	360*180	30	297	194400
3	Train.avi	10.0 MB	360*240	30	626	259200

5.5 Original/Secret Message

The following text message assimilate one paragraph includes 352 characters or (2880) bits. This text has been selected to test the proposed methods, *"Video steganography has become very popular research area for concealing large amount data behind video without being noticed by the human eye and transfer it over the network with high security and without any degradation in the quality of the video, also can be more eligible than other multimedia files, because of its size and memory requirements."*

5.6 Simulation Studies

Implementation of the proposed Algorithms consist of two phases, Embedding and Extraction process, figure(5.2); which are explained as follows:

Figure 5.2: Video Steganography user interface system (GUI).

5.6.1 Embedding phase

In embedding processes the inputs are color (AVI) video file, and a secret message (text file). The output is Stego with hidden data, this process consist of the following steps:

Step1: Load the color AVI video file as a cover, figure (5.3).

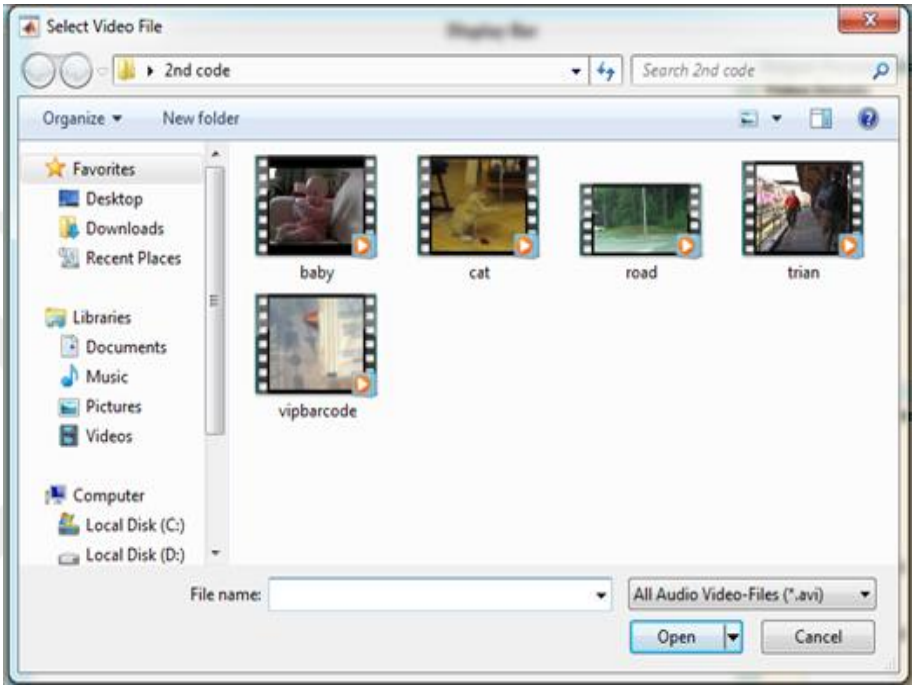

Figure 5.3: Load cover video.

Step2: Load Text Massage, as secret massage, figure (5.4).

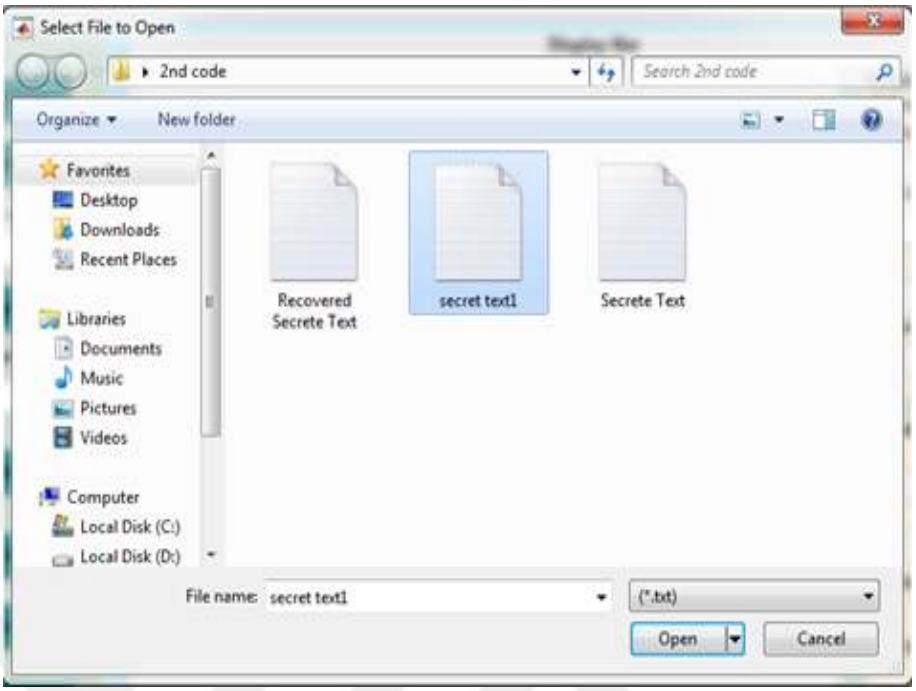

Figure 5.4: Load text file

Step3: Save stego video after embedding the text massage, figure (5.5).

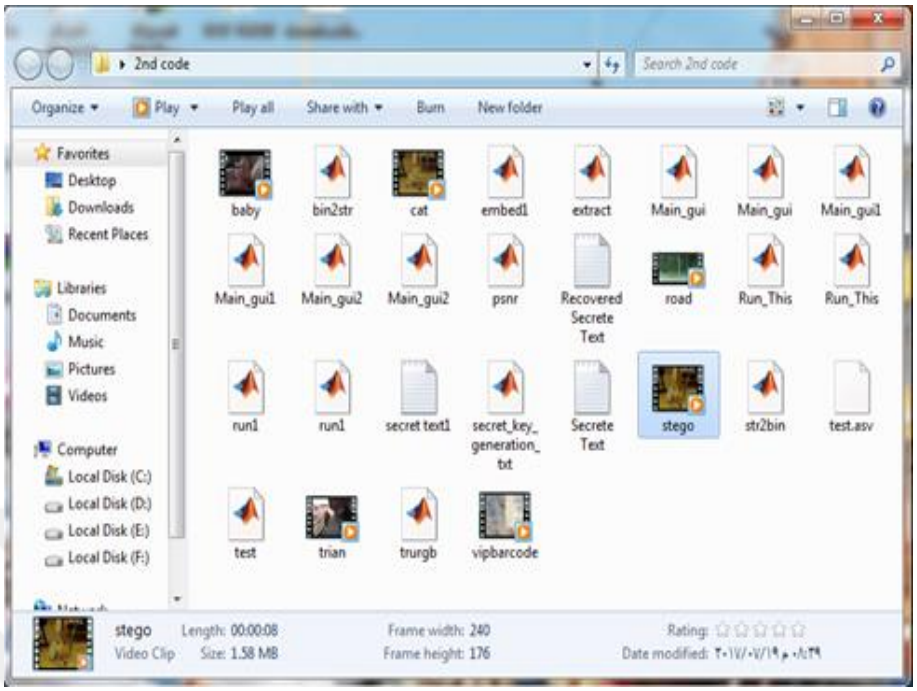

Figure 5.5: Saving stego video.

5.6.2 Extraction phase

In extracting processes the inputs is stego video. The output is text file contain the secret message, which described as follow:

Step1: Load stego video

Figure (5.6) shows the window of loading the stego video that contains the secret message.

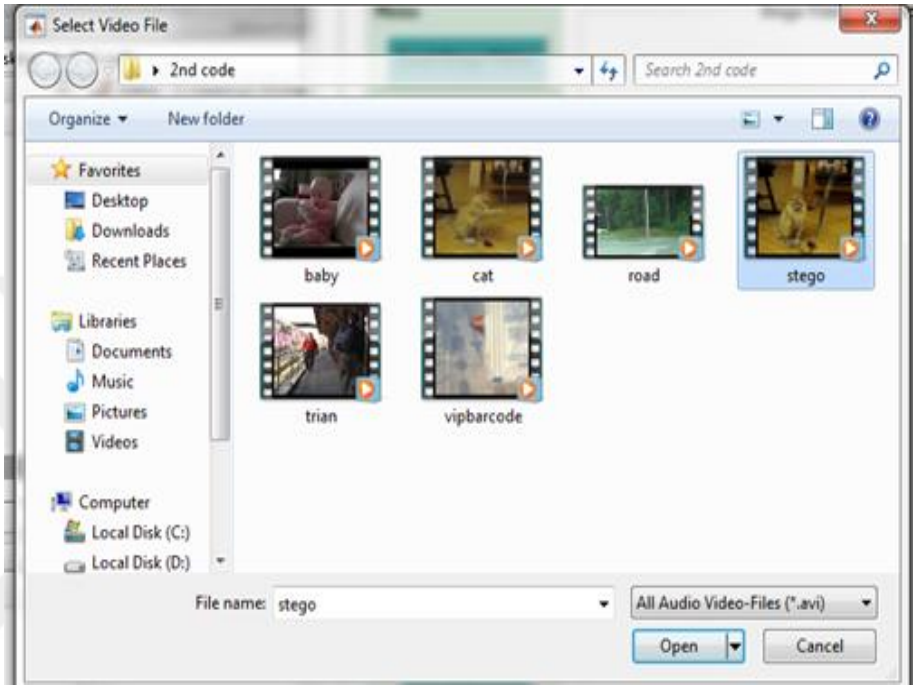

Figure 5.6: Chossing stego video.

Step2: Save extracted message

Figure (5.7) shows the window of text file after extracting the information, were the text file will be saved in the directory named output.

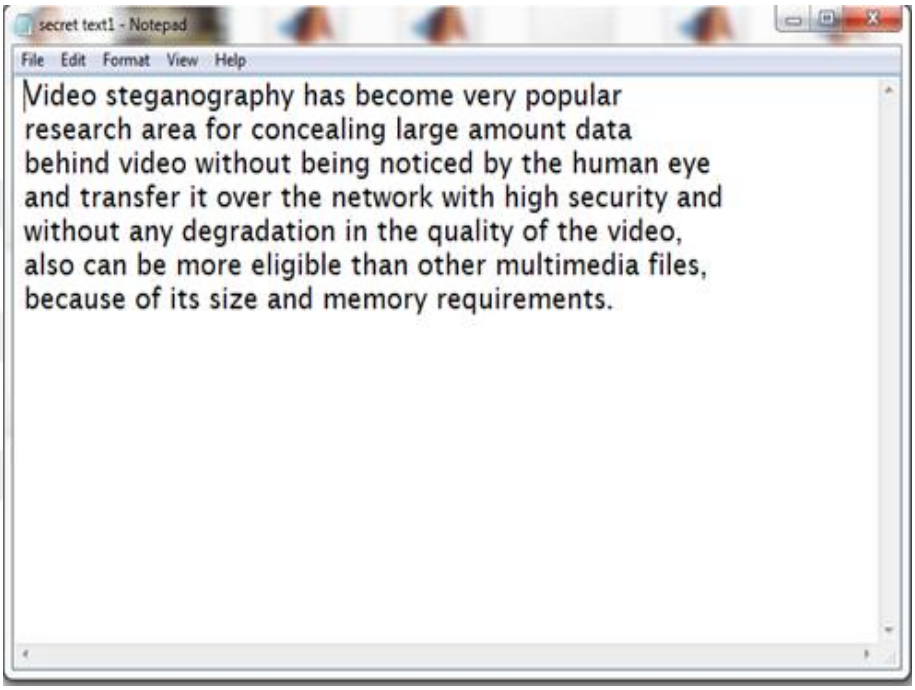

Figure 5.7: Extracted information

5.7 Results and Discussion

The original videos are selected frames from above mentioned video files, used for hiding secret data and after hiding the data resultant videos is known as stego videos, (Figures 5-8, 5-9 and 5-10) shows cover videos and their stego videos of Video steganography proposed approach. (Figures 5.11, 5.12 and 5.13) Shows cover videos and their stego videos of Bit inversion technique approach.

Cover Video **Stego Video**

Figure 5-8: Cat.avi, Cover and Stego video based on video steganography proposed approach.

Cover Video **Stego Video**

Figure 5-9: Road.avi, Cover and Stego video based on video steganography proposed approach.

Cover Video **Stego Video**

Figure 5-10:Train.avi, Cover and Stego video based on video steganography proposed approach.

Cover Video **Stego Video**

Figure 5-11:Cat.avi, Cover and Stego Video Based on Bit Inversion Technique Approach.

Cover Video **Stego Video**

Figure 5-12:Road.avi, Cover and Stego Video Based on Bit Inversion Technique Approach.

Cover Video **Stego Video**

Figure 5-13:Train.avi, Cover and Stego Video Based on Bit Inversion Technique Approach.

For result analysis MSE (Mean Square Error) and PSNR (Peak Signal to Noise Ratio) are measured for original video and stego video. Table 5.2 and 5.3 shows the MSE and PSNR values of mentioned test videos for each approach:

Table 5.2: MSE and PSNR Values of the First Approach.

Proposed Video Steganography Approach		
Cover Video Name	MSE	PSNR
Cat.avi	0.0339962	60.4864
Road.avi	0.0227006	64.5704
Train.avi	0.0171065	65.7992

Table 5.3: MSE and PSNR Values of the Second Approach

Bit Inversion Technique Approach		
Cover Video Name	MSE	PSNR
Cat.avi	0.0336411	60.3064
Road.avi	0.0205556	65.0015
Train.avi	0.0166088	65.9274

A large PSNR value points out that the variation between cover video and stego video is significantly considered unnoticed to the human being eye.

5.8 Histograms for Frame

Histogram represents the tonal distribution of digital video. These figures show the histogram of frame before steganography and after steganography with used techniques. (Figures 5.14, 5.15 and 5.16) shows histogram analysis of video steganography proposed approach and (Figures 5.17, 5.18 and 5.19) shows Bit Inversion Technique approach.

Cover Video **Stego Video**

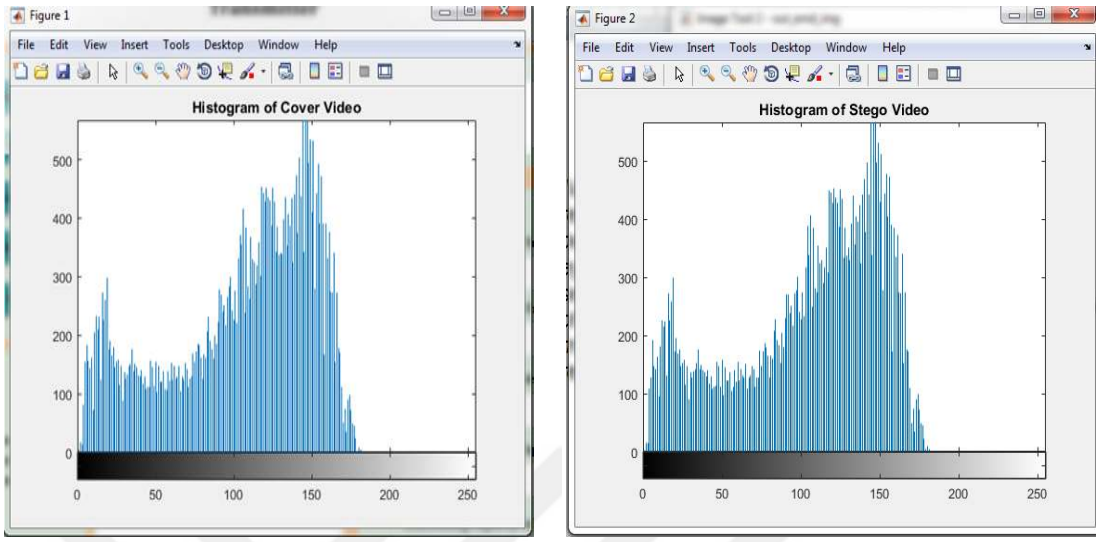

Figure 5.14: Cat.avi, Histogram analysis of Video Steganography Proposed Approach

Cover Video **Stego Video**

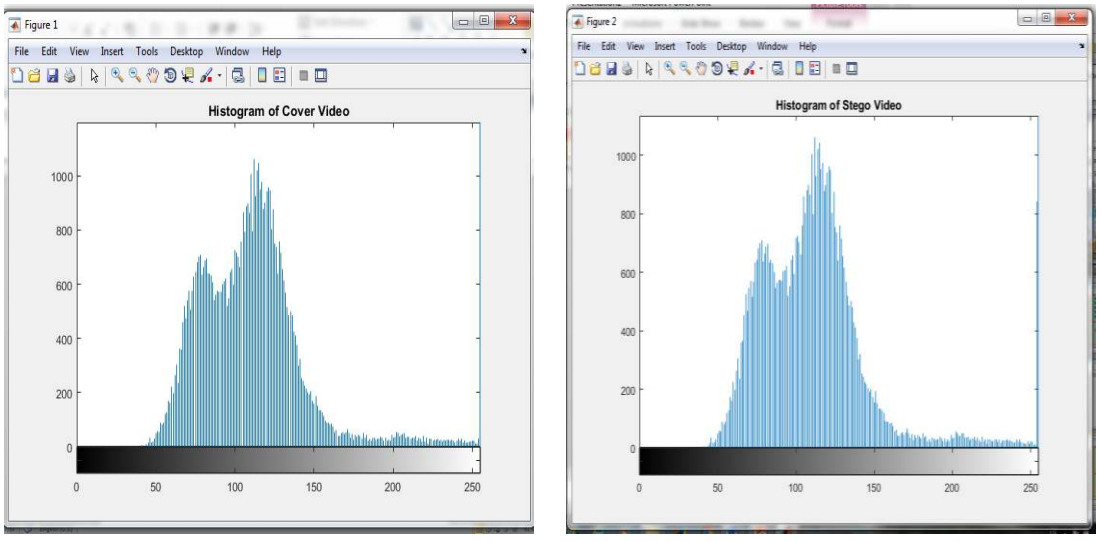

Figure 5.15: Road.avi, Histogram analysis of Video Steganography Proposed Approach.

Cover Video **Stego Video**

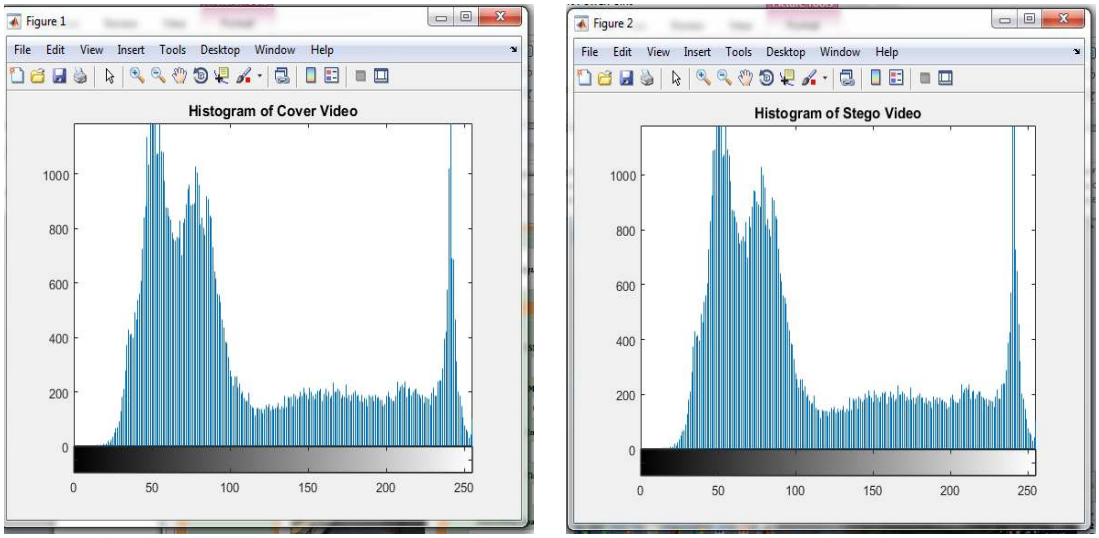

Figure 5.16: Train.avi, Histogram analysis of Video Steganography Proposed Approach.

Cover Video **Stego Video**

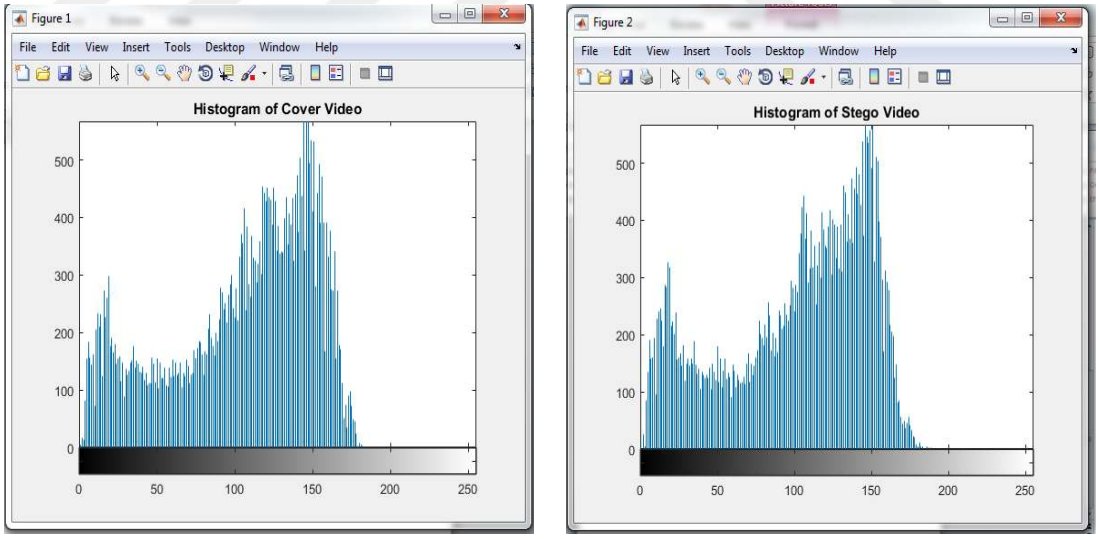

Figure 5.17:Cat.avi, Histogram Analysis of Bit Inversion Technique approach.

Cover Video **Stego Video**

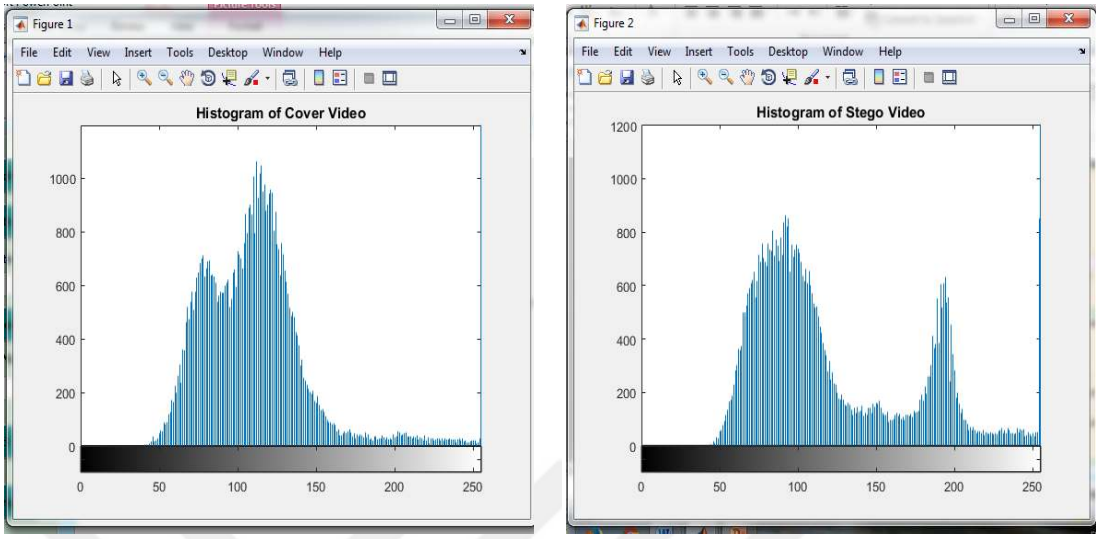

Figure 5.18:Road.avi, Histogram Analysis of Bit Inversion Technique approach

Cover Video **Stego Video**

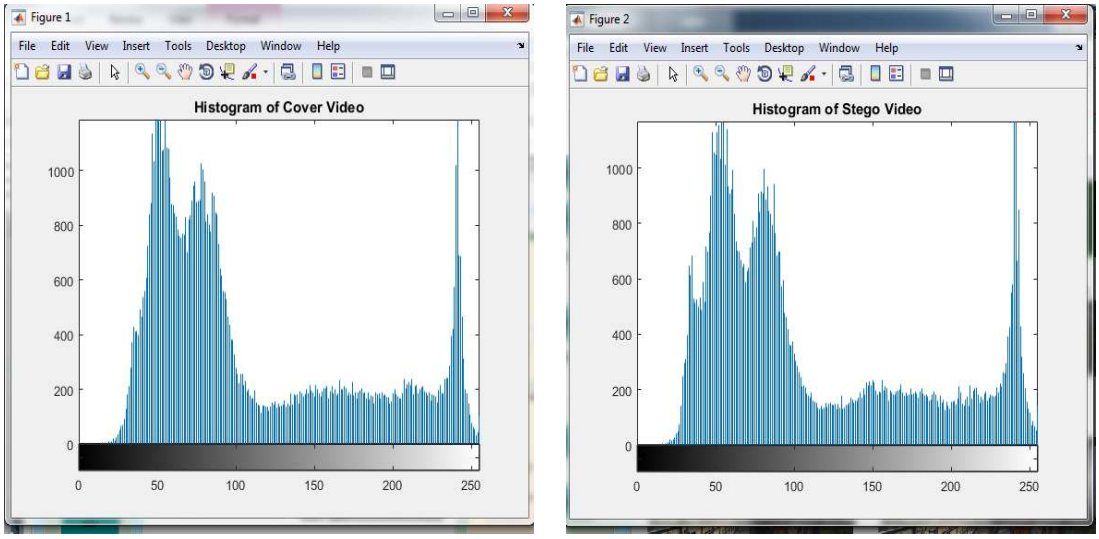

Figure 5.19:Train.avi, Histogram Analysis of Bit Inversion Technique approach.

In figures above, the distinction in the histogram results of the cover-video and stego-video frames obviously demonstrate that the algorithms effectively hides the information into the video having valuable results to the HVS.

The benefit of the proposed algorithms is that it gives high security as the information is hidden in RGB color component. This framework gives good quality resulting videos. Hence the proposed video steganography techniques is demonstrated to be clear to transfer highly confidential information like medical reports, banking details, military information and other crucial information.

CHAPTER 6

Conclusion and Suggestions for Future Work

6.1 Conclusion

A video steganography algorithm for secured data transmission using two different techniques have been proposed with imperceptible distortions in the resulting AVI videos. We embedded secret data bits in RGB color components of the cover video. Also, the proposed method extracts the data without any loss in size of the original video files. The overall process is performed with less computational complexity.

Both techniques have been implemented using least significant bit (LSB) insertion technique, for hiding a particular text message in the host video, hide it securely with minimum mean square error and as a result gives maximum PSNR. This will assist the transmittance of the data securely by embedding it in a video file and without disclosing to the unintended receiver and any alternation in secret message.

In addition, using video files as a cover object increasing the payload capacity with minimal distortions in the host video. The tested results indicate that the considered hiding techniques have an acceptable performance, and the produced stego-videos are not extremely different from the original video to the human eye.

Therefore, these techniques have good quality of invisibility and detect ability for the host video. Worth to mention that the goal of the techniques are not just to increase the capacity of the message but making it difficult to any unauthorized party to determine the presence of a secret message.

6.2 Suggestions for Future Work

1. Further improvement on the video steganography technique is required in order to hide multiple data as well as different types of confidential messages using various types of video file format without affecting the quality of the video files.
2. Also, the data to be hidden and the secret key is encrypted before embedding, which can enhance further security.
3. Likewise, the processing of binary transformations can be adaptive in many ways in order to increase the security of data transfer.
4. Using another technique of steganography in order to decrease the amount of resulting hidden data.
5. In addition to, employ added items of quality parameter to indicate the efficacy of the approaches.

REFERENCES

[1] Johnson, N. F., Duric, Z., & Sushil G. J. "Information Hiding: Steganography and Watermarking - Attacks and Counter- measures", *Advances in Information Security*, (2001).

[2] Curran, K., & Bailey, K. (2003), "An Evaluation of Image Based Steganography Methods", *International Journal of Digital Evidence*, **2(2)**, pp1-5.

[3] Cachin, C. "An information-theoretic model for Steganography", *Information and Computation*, **192(1),** pp41-56, (2004).

[4] Petitcolas, F. A., Anderson, R. J., & Kuhn, M. G. "Information hiding: A survey", *Proceedings of IEEE*, **87(7),** pp1062–1078, (1990).

[5] Johnson, N. F. & Jajodia, S. "Steganalysis of Images Created Using Current Steganography Software", *Proceeding for the Second Information Hiding Workshop, Portland Oregon, USA*, pp273-289, (1998).

[6] Uma Devi. G. "Steganography-Survey on File Systems", MS by Research – CSEIIIT Hyderabad, retrieved online from: http://researchweb.iiit.ac.in/~umadevi/steg.pdf, (2006).

[7] Gaggar, A., Manek, K., & Jain, N. "Steganography", *International Journal of Students Research in Technology & Management*, **1(2),** pp253-259, (2013).

[8] Krzysztof, S."Steganography in TCP/IP Networks", State of the Art and a Proposal of a New System – HICCUPS, Warsaw University of Technology, Poland Institute of Telecommunications, Warsaw, Poland. Retrieved online from: http://vanilla47.com/PDFs/Cryptography/Steganography/Steganography%20in%20TCP-IP%20Networks.pdf, (2003).

[9] Craig, H. R. "Covert Channels in the TCP/IP Suite", *First Monday Journal*, 2(5),(1997).

[10] Murdoch, J. S., & Lewis, S. "Embedding Covert Channels into TCP/IP", *In Information Hiding: 7th International Workshop*, 3727 of LNCS, pp247–261,(2005).

[11] Akbas, A. E. "A New Text Steganography Method By Using Non-Printing Unicode Characters", *Eng. & Tech. Journal*, **28 (1),** pp72-83. Available at: http://www.uotechnology.edu.iq/tec_magaz/volume282010/No.1.2010/researches/Text%20%287%29.pdf, (2010).

[12] Kumar, M. "Cryptographic Study of Some Digital Signature Schemes", A thesis for degree of philosophy PHD in Mathematics, (2003).

[13] Conrad, E. "Explanation of the Three Types of Cryptosystems. London University, ISSN pp 0521-8521, (2007).

[14] Barker E., & Barker W. "Recommendation for Key Management Part 2: Best Practices for Key Management Organization", *NIST Special Publication*,(2008).

[15] Pooja Jain and Navdeep Kanwal, "Image Steganography in RGB Color Components using Improved LSB Technique Image Pattern Compression using Weighted Principal Components Algorithm", Indian Journal of Science and Technology, 9(45), (2016).

[16] Mohammed Abdul Majeed and Rossilawati Sulaiman, "An improved LSB image steganography technique using bit-inverse in 24 bit colour image", Journal of Theoretical and Applied Information Technology, **80(2),** pp342-348, (2015).

[17] R. Popa, "An Analysis of Steganographic Techniques", The "Politehnica" University of Timisoara Faculty of Automatics and Computers, Department of Computer Science and Software Engineering, MSc thesis, (1998).

[18] Isbell, R. A. "Steganography: Hidden Menace or Hidden Saviour", Steganography White Paper, (2002).

[19] T. Morkel, J.H.P. Eloff and M.S. Olivier,"An Overview of Image Steganography", in Proceedings of the Fifth Annual Information Security

South Africa Conference, Sandton, South Africa, (Published electronically), (ISSA),(2005).

[20] Lu S., "Multimedia Security Steganography and Digital Watermarking Techniques for Protection of Intellectual Property", Idea Group Publishing, 7(4), (2005).

[21] N. Provos and P. Honeyman, (2003), "Hide and Seek: An Introduction to Steganography", *Computer Journal of IEEE Security and Privacy Magazine*, **2(3),** pp32-40, (2003).

[22] J. Robert Krenn "Steganography and steganalysis", **6(5),** pp6, (2004).

[23] N. F. Johnson and S. Jajodia, "Steganalysis: The Investigation of Hidden Information", Center for Secure Information Systems, George Mason University, this article will appear in the Proceedings of the IEEE Information Technology Conference, Syracuse, New York, USA, (1998).

[24] S. K. Bandyopadhyay, D. Bhattacharyya, D. Ganguly, S. Mukherjee and P. Das, "A Tutorial Review on Steganography", University of Calcutta, UFL & JIITU, IC3, pp107-108, (2008).

[25] T. Morkel, J.H.P. Eloff and M.S. Olivier, "An Overview of Image Steganography", in Proceedings of the Fifth Annual Information Security South Africa Conference, Sandton, South Africa, (Published electronically), (ISSA), (2005).

[26] Fridrich, "Steganography in digital media: Principles, algorithms and applications", Cambridge University Press, (2010).

[27] Wang H., Wang S.,"Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM-Voting Systems, **47(10),** pp76-82.

[28] Kovacich, G. & Jones, A., "What infosec professional should know about information warfare tactics by terrorists", *Computer & Security*, **21(1),** 35-41, (2002).

[29] Al- Ethawi G. A. Salman, "Text hiding in image border" , Dean of the Military College of Engineering, MSc thesis, (2002).

[30] J. Ashok, Y. Raju, S. Munishankaralah and K. Srinnivas, “Steganography: An Overview”, *International Journal of Engineering Science and Technology*, **2(10),** pp5985-5992, (2010).

[31] S. Katzenbeisser, F. A.P. Petitcolas,“Information hiding techniques for steganography and digital watermarking”, pp20 – 23, (1999).

[32] AL Kubaisi R. T. Mohammad," image in image steganography using DCT", University of Baghdad, College of Science, Department of Computer , MsC. thesis, 2004.

[33] Neil, F. J. and Jajodia, S., “Exploring Steganography: Seeing the Unseen”, *IEEE Computer*, **31(2),** pp26-34, (1998).

[34] Clair, B., “Steganography: How to Send a Secret Message”, Saint Louis University, (2001).

[35] M. M. Amin, P.S. Ibrahim, P.M. Salleh and M.R. Katmin, “Information hiding using Steganography”, University Teknologi Malaysia, MSc thesis, (2003).

[36] Ramandeep Kaur, Pooja, and Varsha, “The NonTangible Masking of Confidential Information using Video Steganography‖”, *International Journal of Computer Applications (IJCA)*, **119(17),** (2015).

[37] Vijay Kumar Sharma, Vishal Shrivastava, “A steganography algorithm for hiding the image in image improved LSB substitution by minimizing Detection‖”, *Journal of Theoretical and Applied Information Technology*, **36(1)**, (2012).

[38] Chincholkar A.A. and Urkude D.A., “Design and Implementation of Image Steganography", *Journal of Signal and Image Processing*, ISSN: 0976-8882 & E-ISSN: 0976-8890, **3(3),** pp111-113, (2012).

[39] Nagham Hamid, Abid Yahya, R. Badlishah Ahmad and Osamah M. Al – Qershi ,“Image Steganography Techniques: an Overview”, *International Journal of Computer Science and Security (IJCSS)*, **6(3).** (2012).

[40] Ramandeep K. and sharanjeet K., " XOR-EDGE based video steganography and testing against chi-square steganalysis", Image, graphics and signal processing, **9,31-39,** (2016).

[41] M. M. Sadek, A. S. Khalifa and M. G. M. Mostafa, "Video steganography: a comprehensive review", *Multimedia Tools and Applications*, pp1–32. Available at http://dx.doi.org/10.1007/s11042-014-1952-z, (2014).

[42] A. P. Sherly, P. P. Amritha, "A Compressed Video Steganography using TPVD", *Int. J. of Database Management Systems (IJDMS)*, **2(3),** pp67–80. Available at http://dx.doi.org/10.5121/ijdms.2010.2307, (2010).

[43] Arup Kumar Bhaumik, Minkya choi, "Data hiding in video", *IEEE International journal of database application*, **2(2),** pp9-15, (2009).

[44] https://edupediapublications.org/journals/index.php/ijr/article

/view/678/309

[45] C.P.Sumathi1, T.Santanam2 and G.Umamaheswari, "A Study of Various Steganographic Techniques Used for Information Hiding", *International Journal of Computer Science &*

Engineering Survey (IJCSES), **4(6),** (2013).

[46] K. M. Rao, "Over View of Image Processing", Deputy Director, National Remote Sensing Agency(NRSA), Hyderabad, India, **7(6),** pp500-037, (1999).

[47] K. Kmm, "Design and Fabrication of Color Scanner", *Indian Journal of Technology*, **15(3),** pp1, (1997).

[48] T. Kumar and K. Verma, "A Theory Based on Conversion of RGB image to Gray Image", Computer Science and Engineering Department, *International Journal of Computer Applications*, **7(2),** pp0975-8887, (2010).

[49] ShengDun Hu, KinTak U, "A Novel Video Steganography based on Non-uniform Rectangular Partition", *IEEE International Conference on Computational Science and Engineering*, pp57-61, (2011).

[50] R. Shanthakumari and Dr.S. Malliga,"Video Steganography using LSB matching revisited algorithm", *IOSR Journal of Computer Engineering*, **16(6),** pp01-06, (2014)

[51] Vivek Kapoor and Akbar Mirza, "An Enhanced LSB based Video Steganographic System for Secure and Efficient Data Transmission", *International Journal of Computer Applications*, **121(10),** pp0975–8887, (2015).

[52] Hemant Gupta and Dr. Setu Chaturvedi, "video steganography through LSB based hybrid approach", *International Journal of Engineering Research and Development*, **6(12),** pp32-42, (2013).

[53] M. E. Eltahir, L. M. Kiah, and B. B. Zaidan, "High Rate Video Streaming Steganography", Information Management and Engineering, ICIME '09. International Conference on 2009, pp550-553, (2009).

[54] Pooja Yadav, Nischol Mishra and Sanjeev Sarma, "video steganography technique with encryption and LSB substitution", School Of Information Technology, Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal, India, (2013).

[55] Sanjiv Manchanda, Mayank Dave and S. B. Singh, "Customized and Secure Image Steganography Through Random Numbers Logic", *In Signal Processing: An International Journal*, **1(1).**

[56] Chan, C.-K. and L.-M. Cheng, "Hiding data in images by simple LSB substitution. Pattern recognition", **37(3),** pp469-474, (2014).

[57] Wang, Z., Bovik, A., "Mean Squared Error: Love it or Leave it? A New Look at Signal Fidelity Measures", *IEEE Signal Processing Magazine*, **26,** pp98-117, (2009).

[58] Rawat, D. and V. Bhandari, "A Steganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Color Image", *International Journal of Computer Applications*, **64(20),** pp0975–8887, (2013).

[59] Wang, c. m., et al., "A high quality steganographic method with pixel-value differencing and modulus function", *Journal of systems and software*, **81(1),** pp150-158, (2008).

[60] Available at: http://www.dpreview.com/learn/?/Glossary/Digital_Imaging/Histogram_01.htm

[61] Available at: https://www.mathworks.com/solutions/image-video-processing.html