Steganography in Video

A report

Submitted by

Aryan Bisht

Roll No. 19010119

Under the supervision

Dr. Kaushal Bhardwaj

in partial fulfillment of the requirements for 7th semester End Term Examination

Department of Computer Science and Engineering

Indian Institute of Information Technology Manipur

Imphal, India - 795002

November 2022

Declaration

The work embodied in the present report entitled "Steganography in video" has been carried out in the name of the Computer Science Department. The work reported herein is original and does not form part of any other report or dissertation on the basis of which a degree or award was conferred on n earlier occasion or to any other student.
I understand the Institute's policy on plagiarism and declare that the report and publications are my own work, except where specifically acknowledged and have not been copied from other sources or been previously submitted for award or assessment.

Signature of the student
Name: Aryan Bisht
Enrollment no: 19010119
Department of Computer Science Engineering
IIIT Senapati, Manipur

Department of Computer Science and Engineering
Indian Institute of Information Technology Manipur

Certificate

This is to certify that the project report entitled **Steganography in video** submitted to Department of Computer Science Engineering, Indian Institute of Information Technology Senapati, Manipur in partial fulfillment for the award of the degree of Bachelor of Technology in Computer Science Engineering is a record of bonafide work carried out by the Aryan Bisht bearing roll number 19010119

Dr. Kaushal Bhardwaj
Supervisor
Assistant Professor, Department of Computer Science and Engineering
Indian Institute of Information Technology Senapati, Manipur

Signature of Examiner

Abstract

Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Intern For hiding secret information in images, there exists a large variety of steganography techniques some are more complex than others and all of them have respective strong and weak points. Different appli- cations have different requirements of the steganography technique used. For example, some applications may require absolute invisibility of the secret information, while others require a larger secret message to be hidden, This project hides the message with in the image . For a more secure approach, the project it allows user to choose the bits for replacement instead of LSB replacement from the image. sender select the cover image with the secret text or text file and hide it in to the image with the bit replacement choice, it help to generate the secure stego image .the stego image is sent to the destination with the help of private or public communication network . on the other side i.e. receiver. receiver download the stego image and using the software retrieve the secret text hidden in the stego image.

Keywords - Stegnography, Image processing, LSB, pixels

Acknowledgement

I am pleased to present this Project report entitled STEGNAOGRAHY. It is indeed a great pleasure and a moment of immense satisfaction for me to express my sense of profound gratitude and indebtedness towards my guide Dr. Kaushal Bhardwaj whose enthusiasm are the source of inspiration for me. I am extremely thankful for the guidance and untiring attention, which he bestowed on me right from the beginning. His valuable and timely suggestions at crucial stages and above all his constant encouragement have made it possible for us to achieve this work, Would also like to give my sincere thanks to Dr. Kaushal Bhardwaj for necessary help and providing me the required facilities for completion of this project report. We would like to thank the entire Teaching staff who are directly or indirectly involved in the various data collection and software assistance to bring forward this semester report. I express my deep sense of gratitude towards my parents for their sustained cooperation and wishes, which have been a prime source of inspiration to take this project work to its end without any hurdles. Last but not the least, I would like to thank all my B.Tech. colleagues for their co-operation and useful suggestion and all those who have directly or indirectly helped me in completion of this project work.

- Aryan Bisht

Contents

List of Figures

List of abbreviations

	A
ASCII	American Standard Code for Information Interchange
	B
Stegno	Stegnography
	C
JPEG	Joint Photographic Experts Group
	D
PNG	Portable Network Graphics
	E
GIF	Graphics Interchange Format
	F
TIFF	Tagged Image File Format

Chapter 1

Introduction

Outline: This chapter presents the following:

1. Introduction
2. Gantt Chart.
3. Problem Statement
4. Scope of Project
5. AES (Advance Encryption Standard)
6. Summary

”Steganography” is of Greek root and signifies ”secured or shrouded composing”. The fundamental point in steganography is to conceal the very presence of the message in the spread medium [1]. Usually mistook for cryptography, not in name but rather in appearance and utilization. The most straightforward approach to separate the two is to recollect steganography disguises the substance of the message as well as the simple presence of a message.

1.1 Introduction

The word steganography originates from the Greek word "Steganos", which mean secured or secret and graphy implies composing or drawing. In this way, steganography implies,truly, secured composing. Steganography is the craftsmanship and art of concealing data with the end goal that its quality can't be detectet and a correspondence is going on. Steganography is the specialty of concealing data indistinctly in a spread medium. The first steganographic applications utilized "invalid figures" or clear content. An invalid figure passes on that the message has not been encoded at all, regardless of whether it is utilizing fundamental character moving, substitution or propelled advanced encryption calculation. In this way, the message is regularly on display however for a reason can either not be identified as being available or can't be seen once recognized. As is regular with cryptography, steganography has its underlying foundations in military and government applications and has progressed in inventiveness and multifaceted nature. The secret data by and large is installed into certain media document like picture or sound and in this manner it is transmitted in order to keep an adversary from speculating that a few secret data is being transmitted. In this way, the fundamental target of Steganography isn't to let the rival surmise that any sort of data separated from the media document itself is transmitted. The craft of data stowing away was first represented in the work Histories by Herodotus around 440 B.C, where he portrays a strategy to convey secret messages by engraving the secret message on the shaved leader of a slave. Upon hair development, the unimportant nearness of the message was obscure to an adversary. The historical underpinnings of the term steganography is Greek and gets from steganos – covered up and graphein – composing. In the following area, hypothetical bits of knowledge into the field of steganography are given with a data theoretic methodology, stressing on the measurements that a steganography calculation is portrayed by. In the third area, a few steganography methods are depicted as references for the imagined tests to be performed.

1.2 Gantt Chart

Gantt charts are useful for planning and scheduling projects. They help you assess how long a project should take, determine the resources needed, and plan the order in which you'll complete tasks.
Below is the Gantt chart, which shows the management plan for this project.

As it can be seen from the Figure 1.2, the whole project has been slotted into various phases, which are Research, planning, implementation,coding etc. All the tasks within

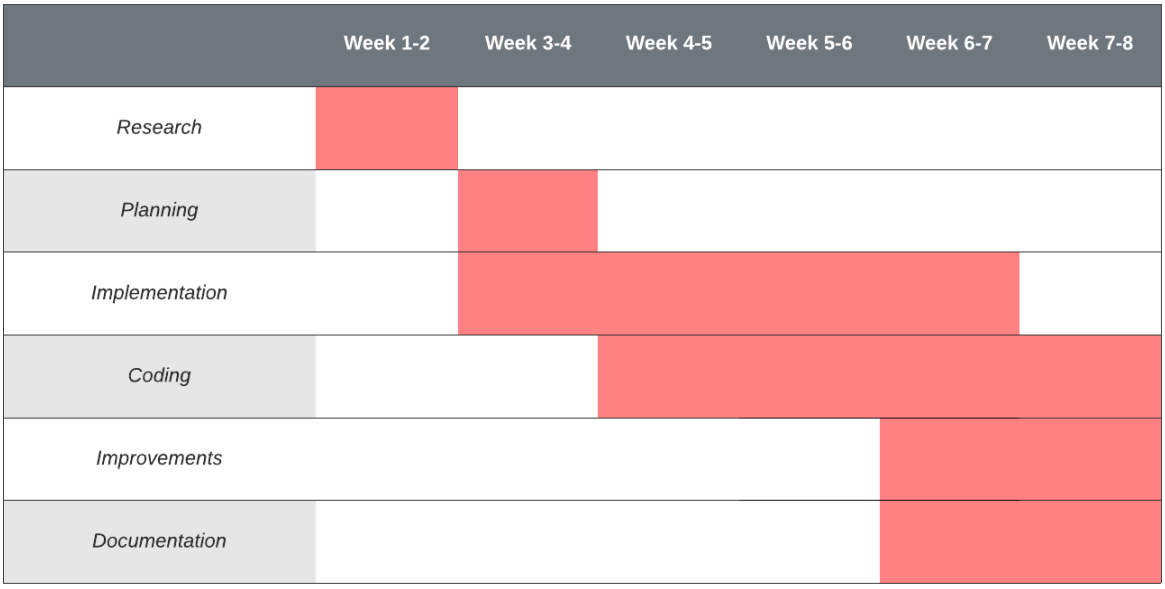

Figure 1.1: Gantt Chart

these phases have been assigned some timeline in which those tasks are supposed to be completed.

1.3 Problem Statement

1.3.1 Statement

Computer security involves safeguarding computing resources, ensuring data integrity, limiting access to authorized users, and maintaining data confidentiality. Confidentiality which means that the non-authenticated party does not examine the data whereas integrity guarantee that the data which is received by the receiver has not been change or modified after the send by the sender.Furthermore, with the development of large open network, security threats have increased significantly. For example, there are modification of information, masquerade, disclosure, denial of service (DOS) and other threats. This kind of threats causes security for information transmission during communication more vulnerable. Besides that, steganography techniques have been applied to secure

data during transmission. However, using only steganography method is no longer secured. Hence, cryptography technique must be combined together with steganography method to provide better security. However, for the cover media, video file is being used which generally a collection of images and sounds, so most of the presented techniques on images and audio can be applied to video files too. The great advantages of video are the large amount of data that can be hidden inside and the fact that it is a moving stream of images and sounds. Therefore, any small but otherwise noticeable distortions might go by unobserved by humans because of the continuous flow of information. In this research will be hidden data in images after cutting up video to frames.

1.3.2 Overview

The usage of Internet in the world is increasing very highly. Present day transactions are considered to be "untrusted" in terms of security, i.e. they are relatively easy to be hacked. We also have to consider the transfer of large amount of data through the network which will give errors at the time of transferring and only the single level of security is present in the existing systems. Now days, hacking activities are growing day-by-day and they easily hack important information and security mechanisms is not sufficient to stop it. Though security status increased at a higher level but the major drawback of new status of security is costly. For that we need better solutions with good security level and lower cost. There are many techniques to overcome this problem like Image steganography, cryptography, and audio steganography. But many limitations have aroused in Image, audio and text steganography related to security, encryption, decryption and the space provided by these techniques. To overcome all these problems, the technique which gained a special importance is "Video steganography". It has gained a considerable amount of attention due to its possible applications in multimedia fund information security

1.3.3 Objectives

In my project I primarily targeting the info security issues while sending the info over the network using stenographic techniques.
The main objectives of the project are:
• Requirement of this steganography system is that the hider message carried by Stego-media shouldn't be sensible to citizenry.

• To propose a combination of steganography and cryptography techniques to provide authentication and confidentiality of that secret data
• To design the proposed techniques to protect the secrecy of data.
• To implement and test if quality of the cover media is loss after the encrypted message is hidden into it.

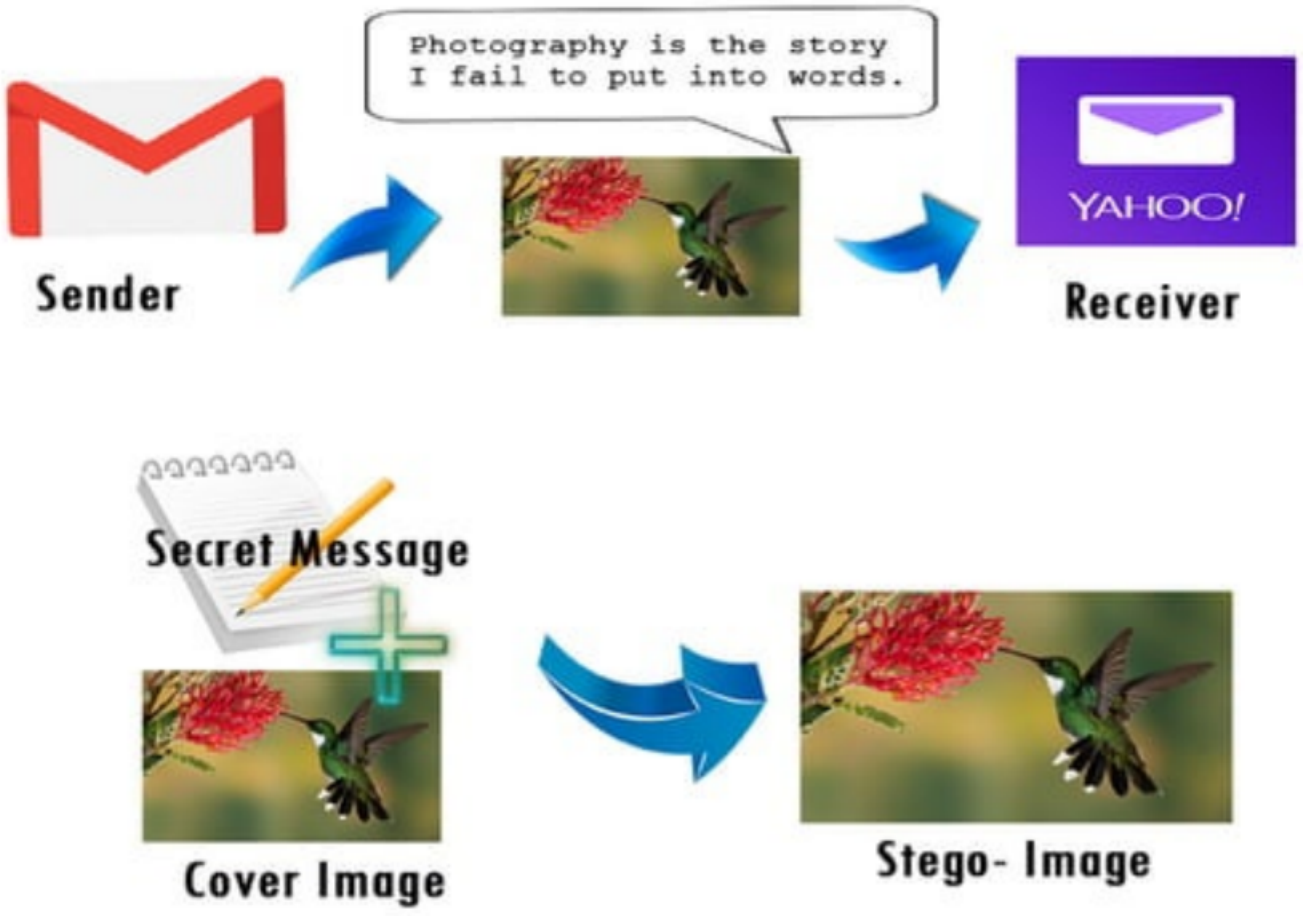

Figure 1.2: Communication using stegnography

1.4 Scope of Project

In my project scope, security acts as an important role which have double layer of data hiding. Message will be encrypted first using AES algorithm and then embedded into video using LSB techniques. Then, for the user scope, it involved between the sender side

and the receiver side. As for the sender side, video will be inserted using file format like mp4, mov etc. Encryption key will be selected for the use both of sender and receiver, if sender chooses the password, otherwise no key will be used. At the receiver side, video steganography will extract the encrypted message from its video. Then, the same key used for encryption will be used to decrypt message.

Chapter 2

Literature Survey & Research

Outline: This chapter presents the following:

1. A brief introduction.
2. What is an Image.
3. Stegnography and Cryptography
4. Algorithms
5. AES (Advance Encryption Standard)
6. Summary

A pixel is the smallest unit of a digital image or graphic that can be displayed and represented on a digital display device. A pixel is the basic logical unit in digital graphics. Pixels are combined to form a complete image, video, text, or any visible thing on a computer display. An RGB image, is stored as an m-by-n-by-3 data array that defines red, green, and blue color components for each individual pixel. Digital images can be made by putting together lots of tiny squares, known as pixels -short for picture element.When an image is digitised to be stored on a computer, it's turned into a set of pixel.

2.1 Introduction

This chapter provides an overview of previous research on the work of video steganography. Many techniques have been proposed to perform steganography. There are many types of cover media and technique used to make better security while sending or transferring data or message to the authorized user. While transferring the data, there might be intruders or eavesdropper that might be steals our data. Thus, steganography plays an important role in securing while transmitting the data. To make a better security, cryptography and steganography should be combined

2.2 What is an image

Digital images can be made by putting together lots of tiny squares, known as pixels - short for picture element. When an image is digitised to be stored on a computer, it's turned into a set of pixels.Imagine an avatar you have made with a square grid placed over it.Every one of the squares is a pixel. To store the image, the computer records a number to represent the colour of each square. It works a bit like a digital colour by numbers! The more squares in the grid, the better the images will look, as more pixels are used to represent the image. If you look closely at a computer screen, you will see that it is made up of millions of tiny squares. Each one of those squares is a pixel.To display an image, the computer tells the screen to show a particular colour for each of the pixels. Images made up of pixels can be saved as a file using a number of formats.

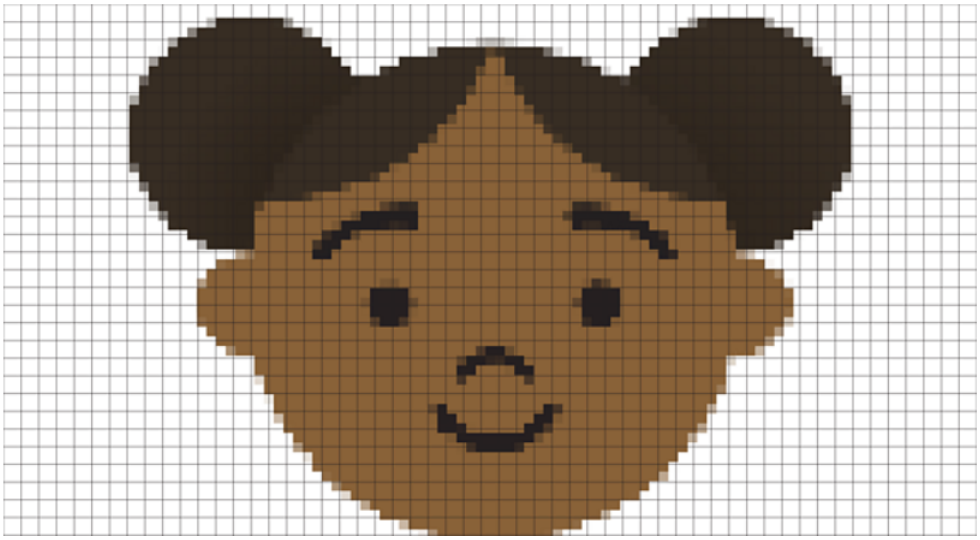

Figure 2.1: Image pixel

Different file types all use pixels in some way to store the image. These include:

1. JPEG
2. TIFF.
3. PNG
4. GIF
5. BMP

2.3 Stegnography and Cryptography

The word stegnography is of Greek origin and means "covered or hidden writing". Stegnography is the art and science of communication in way which hides the existence of the communication. By contrast, cryptography obscures the meaning of a message, but it doesn't conceal the fact that there is a message.
Research in science and technology has played a vital role in improvising human life at great extent. With the development of instrumentation and computation facilities, research on frontier areas has gone manifold. The discussion on the frontier areas of research in inter- disciplinary subject has always yielded novel ideas and collaborative research. In view of this, the First International Conference on Smart Technologies in Computer and Communication (SmartTech-2017) is meticulously planned to muster innovative ideas from researchers, scientists, academicians, Industry professionals and students. The aim of the conference is to provide a common platform to share and discuss the novel ideas, technologies and research findings to promote interdisciplinary research and to ignite young brains.

Cryptography — the science of writing in secret codes — addresses all of the elements necessary for secure communication over an insecure channel, namely privacy, confidentiality, key exchange, authentication, and non-repudiation. But cryptography does not always provide safe communication. Consider an environment where the very use of encrypted messages causes suspicion. Consider the following text file; what else is it likely to be if not encrypted?

The message above is a sentence in English that is encrypted using Pretty Good Privacy (PGP), probably the most commonly used e-mail encryption software today. The advantage of steganography over cryptography alone is that messages do not attract attention to themselves, to messengers, or to recipients. Whereas the goal of cryptography

Figure 2.2: Image caption

is to make data unreadable by a third party, the goal of steganography is to hide the data from a third party. Often, steganography and cryptography are used together to ensure security of the covert message.

Steganography is a method of hiding secret message behind cover media or cover message which include audio, text, image and video. Secret message will be embed in those cover media to not letting unauthorized people know the message that being transfer between the trusted two parties. Basic requirements of steganography system are imperceptibility, capacity and robustness. Imperceptibility is the property in which a person should be unable to distinguish the original and the steganography image. Imperceptibility refers to the visibility of modification inside the cover media. High Imperceptibility means increasing the invisibility of slight modifications in cover object. Modern day steganography approaches are highly intelligent to detect slight modifications. High Imperceptibility has motivated researches to design steganography resistant video steganography methods. Besides that, capacity refers to the amount of secret information that can be embedded without degradation of the quality of the image. Steganography aims at hidden communication and therefore usually requires sufficient embedding capacity. Steganography capacity is the maximum number of bits that can be embedded in a given cover file without affecting the quality of the cover medium and also minimizing the perception of the hidden data in the steganography medium. The capacity of the secret message that is to be embedded must be less than the size of the cover medium. Furthermore, robustness refers to the degree of difficulty required to destroy embedded information without destroying the cover image. The robustness requirement is required when traded with data hiding capacity. In steganography, robustness is not a top priority, thus steganography systems are either not robust against modifications or have limited robustness against technical modifications. Then, steganography consist of three types which are pure steganography, secret key steganography and public key steganography. Furthermore, pure steganography where there is no steganography

key. It is based on the assumption that no other party is aware of the communication whereas secret key steganography uses a type of hiding key, which is called the secret key. The steganography object contains the cover, hidden message and the secret key. Only the parties who know the secret key can reverse the process and read the secret message .Unlike Pure Steganography where a perceived invisible communication channel is present, Secret Key Steganography exchanges a steganography key, which makes it more susceptible to interception. The benefit to secret key Steganography is even if it is intercepted only parties who know the secret key can extract the secret message. Public key steganography where a public key and a private key is used for secure communication.

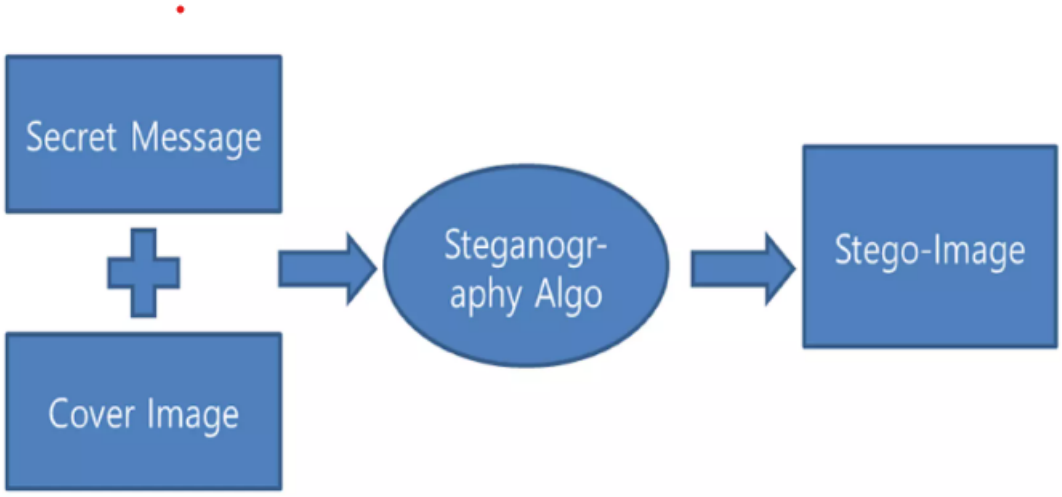

Figure 2.3: Stegno-Image

2.3.1 Image Stegnography

Hiding the data by taking the cover object as image is referred as image steganography. In image steganography pixel intensities are used to hide the data. In digital steganography, images are widely used cover source because there are number of bits presents in digital representation of an image. An image is represented as an N*M (in case of grayscale images) or N*M*3 (in case of color images) matrix in memory, with each entry representing the intensity value of a pixel. In image steganography, a message is embedded into an image by altering the values of some pixels, which are chosen by an

encryption algorithm. The recipient of the image must be aware of the same algorithm in order to know which pixels he or she must select to extract the message.

2.3.2 Video Stegnography

It is a technique of hiding any kind of files or data into digital video format. In this case video (combination of pictures) is used as carrier for hiding the data. Generally discrete cosine transform (DCT) alter the values (e.g., 8.667 to 9) which is used to hide the data in each of the images in the video, which is unnoticeable by the human eye. H.264, Mp4, MPEG, AVI are the formats used by video steganography. In all of these methods, the basic principle of steganography is that a secret message is to be embedded in another cover object which may not be of any significance in such a way that the encrypted data would finally display only the cover data. So it cannot be detected easily to be containing hidden information unless proper decryption is used.

2.3.3 Audio Stegnography

In audio steganography, secret message is embedded into digitized audio signal which result slight altering of binary sequence of the corresponding audio file. There are several methods are available for audio steganography. We are going to have a brief introduction on some of them. It involves hiding data in audio files. This method hides the data in WAV, AU and MP3 sound files. There are different methods of audio steganography. These methods are
i) Low Bit Encoding
ii) Phase Coding
iii) Spread Spectrum.

2.4 Algorithms

2.4.1 LSB Algorithm

Least significant bit (LSB) coding is the simplest way to embed information in a digital Image or Audio file. By substituting the least significant bit of each sampling point in

Figure 2.4: LSB Operation

Audio and each pixel in Image with a binary message, LSB coding allows for a large amount of data to be encoded.By substituting the least significant bit of each examining point with a twofold message, LSB coding takes into consideration a lot of information to be encoded. The 372 after chart outlines how the message 'Hello' is encoded in a 16-bit CD quality example utilizing the LSB technique: In LSB coding, the perfect information transmission rate is 1 kbps per 1 kHz. In certain usage of LSB coding, in any case, the two least significant bits of an example are supplanted with two message bits. This expands the measure of information that can be encoded yet additionally builds the measure of coming about clamor in the sound document also. In this way, one ought to consider the flag content before settling on the LSB activity to utilize. For instance, a sound document that was recorded in a clamoring tram station would cover low-bit encoding commotion. Then again, a similar clamor would be capable of being heard in a sound. LSB stands for Least Significant bit. The idea behind LSB embedding is that if we modify the last bit value of a pixel, there won't be much visible change in the

color. For example, 0 is black. Changing the value to 1 won't make much of a difference since it is still black, just a lighter shade. Least significant bits (LSB) insertion is a simple approach to embedding information in image file. The simplest steganography techniques embed the bits of the message directly into least significant bit plane of the cover-image in a deterministic sequence. Modulating the least significant bit does not result in human-perceptible difference because the amplitude of the change is small, [13]. For example, if we consider image steganography then the letter A can be hidden in three pixels (assuming no compression). The original raster data for 3 pixels (9 bytes) may 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 result in
(00100111 11101000 11001000)
(00100110 11001000 11101000)
(11001000 00100111 11101001)
The underlined bits are the only three actually changed in the 8 bytes used. On average, LSB requires that only half the bits in an image be changed. You can hide data in the least and second least significant bits and still the human eye would not be able to discern it.

2.4.2 e-LSB Algorithm

It is same as LSB but here we only change the bits for blue colour because human eyes are not able to see change in blue colour as compared to other colours.

(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)
(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)
(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 result in
(00100111 11101000 11001001)
(00100111 11001000 11101000)
(11001000 00100111 11101000)
(00100111 11101000 11001000)
(00100111 11001000 11101000)
(11001000 00100111 11101000)
(00100111 11101000 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101000)

Enhanced Least Significant Bit algorithm. In case of a 24-bit image, LSB algorithm all the three components are used for embedding the hidden message. But in ELSB algorithm only one component among three components (Red, Green, and Blue) can be used to store 3 bits of the secret message. Since only one component is changed we can minimize the distortion.level in the image. Security can be further increased by performing XOR encoding and XOR decoding operations. Main Advantage of Enhanced Least Significant Bit minimizes the distortion level of the image file and security can also be increase

2.5 AES (Advance Encryption Standard)

Advanced Encryption Standard (AES) is one of cryptography algorithm which is published by National Institute of Standard and Technology (NIST) at 2001. This algorithm is a part of symmetric encryption which operated in a 4x4 array byte that called a state. [15] A state could be encrypted using three kinds of AES cryptographic key. AES consist of three key types, those are 128, 192, and 256-bit.The state could be encrypted and decrypted with applying four-transformation in a certain number of rounds (10, 12, and 14 rounds). The number of rounds depending on the chosen key, where 10 rounds assign for 128-bit key, 12 assign for 192-bit key, and 14 rounds assign for 256-bit key. Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S National Institute of Standards and Technology (NIST) in 2001. AES is widely used today as it is a much stronger than DES and triple DES despite being

harder to implement.
Points to remember

1. AES is a block cipher
2. The key size can be 128/192/256 bits.
3. Encrypts data in blocks of 128 bits each.

That means it takes 128 bits as input and outputs 128 bits of encrypted cipher text as output. AES relies on substitution-permutation network principle which means it is performed using a series of linked operations which involves replacing and shuffling of the input data. Working of the cipher : AES performs operations on bytes of data rather than in bits. Since the block size is 128 bits, the cipher processes 128 bits (or 16 bytes) of the input data at a time. The number of rounds depends on the key length as follows:

1. 128 bit key – 10 rounds
2. 192 bit key – 12 rounds.
3. 256 bit key – 14 rounds.

Creation of Round keys :
A Key Schedule algorithm is used to calculate all the round keys from the key. So the initial key is used to create many different round keys which will be used in the corresponding round of the encryption. Encryption : AES considers each block as a 16 byte (4 byte x 4 byte = 128) grid in a column major arrangement. Each round comprises of 4 steps :

1. SubBytes
2. ShiftRows
3. MixColumns
4. Add Round Key

The last round doesn't have the MixColumns round. The SubBytes does the substitution and ShiftRows and MixColumns performs the permutation in the algorithm.
SubBytes:

This step implements the substitution. In this step each byte is substituted by another byte. Its performed using a lookup table also called the S-box. This substitution is done

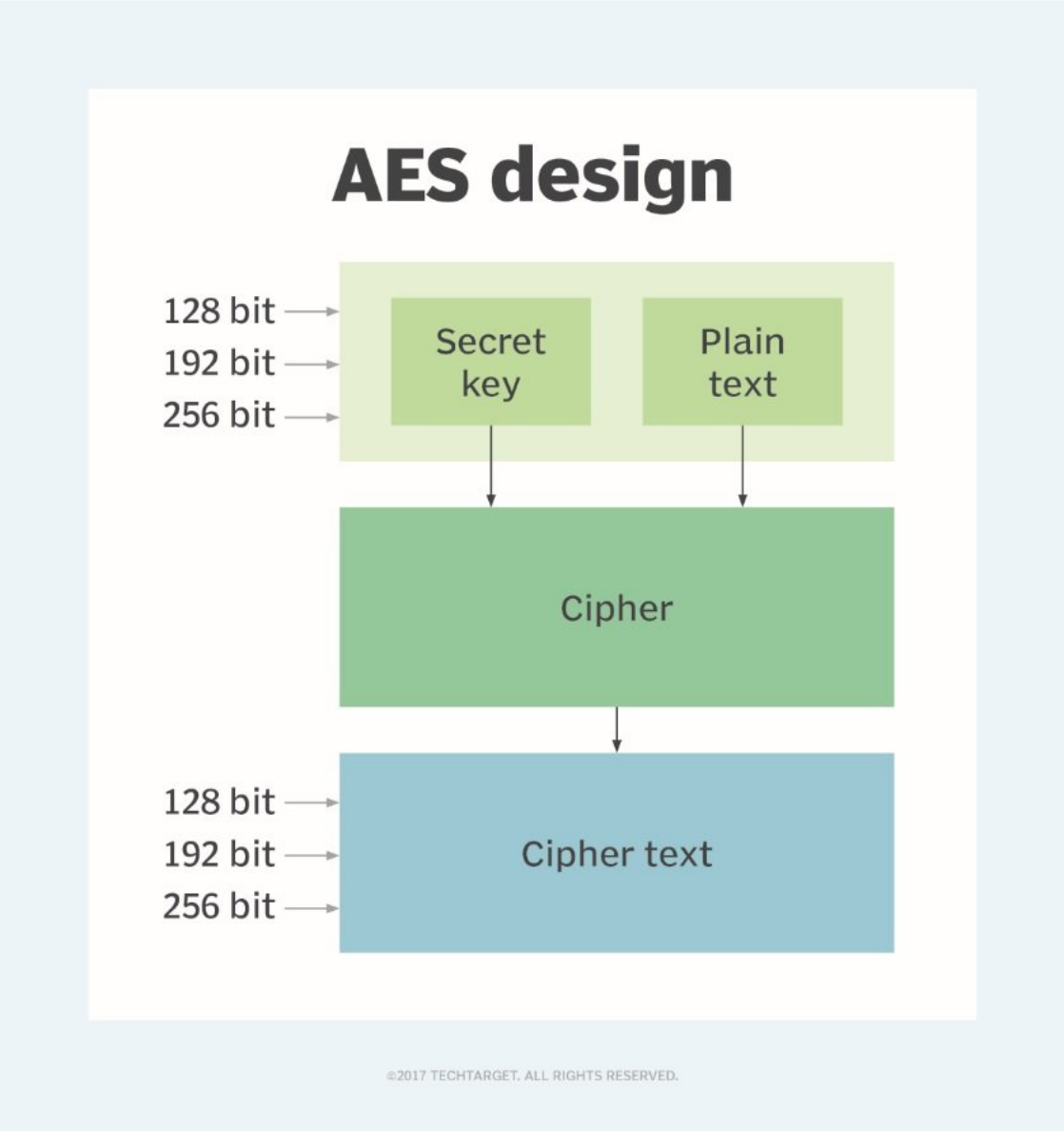

Figure 2.5: AES Example

in a way that a byte is never substituted by itself and also not substituted by another byte which is a compliment of the current byte. The result of this step is a 16 byte (4 x 4) matrix like before.

The next two steps implement the permutation.

ShiftRows :

This step is just as it sounds. Each row is shifted a particular number of times.

The first row is not shifted

The second row is shifted once to the left.

The third row is shifted twice to the left.

The fourth row is shifted thrice to the left.
(A left circular shift is performed.)
’ **MixColumns:**

This step is basically a matrix multiplication. Each column is multiplied with a specific matrix and thus the position of each byte in the column is changed as a result.
This step is skipped in the last round.

Add Round Keys:

Now the resultant output of the previous stage is XOR-ed with the corresponding round key. Here, the 16 bytes is not considered as a grid but just as 128 bits of data.
After all these rounds 128 bits of encrypted data is given back as output. This process is repeated until all the data to be encrypted undergoes this process.

Decryption :

The stages in the rounds can be easily undone as these stages have an opposite to it which when performed reverts the changes.Each 128 blocks goes through the 10,12 or 14 rounds depending on the key size.
The stages of each round in decryption is as follows :

1. Add round key
2. Inverse MixColumns
3. ShiftRows
4. Inverse SubByte

The decryption process is the encryption process done in reverse so i will explain the steps with notable differences.

Inverse MixColumns :

This step is similar to the MixColumns step in encryption, but differs in the matrix used to carry out the operation.

Inverse SubBytes :

Inverse S-box is used as a lookup table and using which the bytes are substituted during decryption.

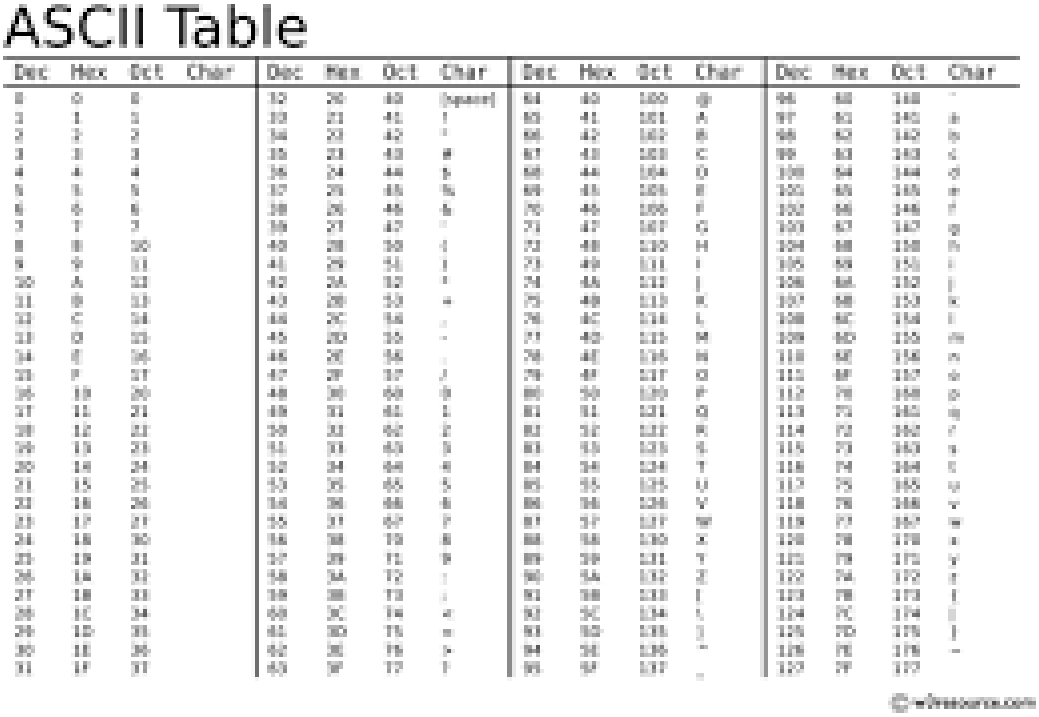

Figure 2.6: ASCII Table

2.6 ASCII Values

ASCII stands for the "American Standard Code for Information Interchange".It was designed in the early 60's, as a standard character set for computers and electronic devices. ASCII is a 7-bit character set containing 128 characters.

It contains the numbers from 0-9, the upper and lower case English letters from A to Z, and some special characters.

The character sets used in modern computers, in HTML, and on the Internet, are all based on ASCII. The following tables list the 128 ASCII characters and their equivalent number. ASCII (which stands for American Standard Code for Information Interchange) is a character encoding standard for text files in computers and other devices. ASCII is a subset of Unicode and is made up of 128 symbols in the character set. These symbols consist of letters (both uppercase and lowercase), numbers, punctuation marks, special characters and control characters. Each symbol in the character set can be represented by a Decimal value ranging from 0 to 127, as well as equivalent Hexadecimal and Octal values. The following is a listing of ASCII values displaying the Decimal, Hexadecimal, Octal and Character values for each ASCII character.

2.7 ANALYSIS OF EXISTING PAPER

The main aim of this research of "Image Steganography Using Secured Force Algorithm for Hiding Audio Signal into Colour Image" is to hide audio signal into colour image using Advance Encryption Standard (AES) algorithm and circular LSB algorithm. This embedded output is secured using secured force algorithm which provides another layer of security. At decryption side Advance Decryption Standard (ADS) algorithm provides decrypted output. This image steganography provides hiding of data more effective and efficient manner with help of circular LSB and secured force algorithm. This paper present a more efficient way for hiding secret data into an image and also provides a more secure way of secret communication. It is also the way of hiding an audio signal into colour image and transmitting through more secured way. This will prevent attackers from hacking the hidden data into the cover medium because only using password the decryption process can be carried out on steganography image.[8] In this journal of "Video Steganography: A Survey", we have analyzed only video steganography. In video steganography secret information is enveloped inside a video to make it safe from intruders. In this paper we have critically analyzed fundamental concepts, performance metrics and security aspects of video steganography. Different methods used for protecting secret information by using a video as cover media are explored. Comparisons between different video steganography techniques are also provided. The research of video steganography techniques can be explored in effective selection of cover media, to identify methods for embedding secret message with high imperceptibility, high embedding capacity, high embedding efficiency with optimum data hiding locations, low computational cost of data retrieval and data embedding rate, high security, different video files extension, different types of secret message like video inside video, image inside video, audio inside video and so on steganography is also discussed in brief.

From research paper named, "A Secure Image Steganography Using Hash LSB Technique and RSA Algorithm within Digital Signature Framework" by Sonupriya P S uses Hash-LSB technique to hide secret data in the LSB of the carrier image file. Prior to embedding process, secret message is converted into cipher text using RSA encryption algorithm. Integrity and authentication of data transmission is ensured using digital signature. Here cryptography is incorporated with steganography to provide more security. Digital signature means signing the digest. It is used for data integrity, image authentication, non-repudiation and data confidentiality. At the sender side, a message digest is generated from the original message using hash function. Then the message digest is encrypted using the private key of the sender. Encrypted message digest is transmitted with the original message to the receiver. At the receiver side a message digest is created

from the received message. At the same time encrypted message digest received along with the original message is decrypted using the sender's public key to get the message digest of the original message created by the sender. Then a content based verification is performed between the message digest created by the sender and the message digest created by the receiver. If they are same, the message is authentic and correct. If there is any discrepancy, it is discarded.

Audio steganography methods advantages and disadvantages have been mainly discussed in journal of "Information Hiding Using Audio Steganography" by Jayaram P, Ranganatha H R, Anupama H S. The main disadvantages associated with the use of existing methods like echo hiding, spread spectrum and parity coding are, human ear is very sensitive to noise and it can often detect even the slightest bit of noise introduced into a sound file and another problem is robustness. Phase coding has main disadvantage of low data transmission rate because of the fact that the secret message is encoded only in the first signal segment. Hence this method is used only when a small amount of data needs to be transferred. Among different information hiding techniques proposed to embed secret information within audio file, Least Significant Bit (LSB) coding method is the simplest way to embed secret information in a digital audio file by replacing the least significant bit of audio file with a binary message. Hence LSB method allows large amount of secret information to be encoded in an audio file. This method provide better security and also ensure that the size of the file is not changed even after encoding and it is suitable for any type of audio file format.

From "Video Steganography through LSB Based Hybrid Approach" by Hemant Gupta, Dr. Setu Chaturvedi had stated that they proposed an advance approach for dynamic data protection using LSB and hybrid approach. The proposed methods for replacing one or two or three LSB of each pixel in video frame and apply Advance encryption standard (AES). It becomes very difficult for intruder to guess that an image is hidden in the video as individual frames are very difficult to analyze in a video. In this paper, they are calculating PSNR and correlation between Original and embedded image for 1 bit LSB 2 bit LSB 3 bit LSB Substitution and AES method. In this observation PSNR is decreased when number of LSB substation bit increased. So that hackers cannot easily hack important information and security is sufficient to stop hacking. Result analyze the correlation coefficient has the value r=1 if there is not difference in the original image. The number of LSB Substitute is increase then correlation factor is decreased. In this paper observation autocorrelation between original image and encrypted image for different frame (Images) are not related as AES algorithm is generated Key lengths of 128, 192, and 256 bits are supported. So that hackers cannot easily hack important information and security is sufficient to stop hacking.

In this "MP4 Video Steganography Using Least Significant Bit (LSB) Substitution And Advanced Encryption Standard (AES)" research, they will applied in Android platform, and the inputs used MP4 video format (.mp4extension) as the host (cover media) and JPEG image (.jpg extension) as the secret data which embedded into the host. The image embedded into the video using LSB substitution algorithm, which is encrypted first using AES encryption. The image was embedded into the first sample of the video. Sample is obtained by mapping all the MP4 video's atoms. MP4 video has atoms which its arrangement is almost constant, although generated from different devices. It makes a possibility for the mapping process to get a sample from the video. The results of experiment and analyses showed that steganography video did not suffer damage as seen by the human eye, and video could be played by the video player on the smartphones or desktop computers. The same results were also obtained when extracting images from steganography video, where the image was not damaged and identical with the original image. Steganography video quality is measured with Qualify software. Steganography video has excellent quality with a value of 80. This research could be developed by embedding data in more than one sample, with the number of images inserted more than one image. This research would be applied to various operating systems in many devices, thus will be more useful.

From research "Data Hiding Technique Using Video Steganography and Watermarking", they present video steganography with digital watermarking techniques as an efficient and robust tool for protection. This paper is a combination of Steganography and watermarking; which provides a strong backbone for its security. Here considers video as set of frames or images and any changes in the output image by hidden data is not visually recognizable. This proposed system not only hides large volume of data within a video; but also limits the perceivable distortion that might occur while processing it.

In this "Improved chaos-based video steganography using DNA alphabets" research, they propose a DNA properties-based mechanism to send data hidden inside a video file. DNA properties involved as DNA polymeric chain reaction and DNA cutting properties with a linear congruently generator and a Burger chaotic map. Initially, the video file is converted into image frames. Random frames are then selected and data is hidden in these at random locations by using the Least Significant Bit substitution method. They will analyse the proposed architecture in terms of peak signal-to-noise ratio as well as mean squared error measured between the original and steganography files averaged over all video frames. We have also checked histogram differences and pixel correlation of original and steganography videos. All obtained experimental results indicate a high standard and a good visual quality for the steganography video, which is not likely to be suspicious.

From "Biometric Steganography Technique Using DWT and Encryption" journal, steganog-

raphy method used in this paper is based on biometrics and the biometric feature used to implement steganography is skin tone region of images. Here secret data is embedded within skin region of image that will provide an excellent secure location for data hiding. Before embedding, secret data is needed to be encrypted using stream cipher encryption scheme RC4. Skin colour tone detection is performed by using HSV colour space. DWT is the frequency domain in which this biometric steganography is implemented. Secret data is embedded in one of the high frequency subbed by tracing the number of skin pixels in that band. Different embedding steps are embedded on the cropped region of the image will act as a key at the decoder side. Embedding data only within the skin regions provide an excellent secure location for data hiding. Encrypt secret image using RC4 stream cipher algorithm before embedding enhances the security level. The quality of recovered message is not degraded even if the steganography image is attacked after transmission. The proposed approach provides invisibility and fine image quality of the steganography image, higher security and satisfactory PSNR.

From journal of "Sequential Multiple LSB methods and real-time data hiding: variations for Visual Cryptography ciphers", a general model approach of real time data hiding and watermarking for image, video and audio communications is proposed. The aim is the development of security robustness variations and data-rate (capacity) extensions of Steganography fast schemes for RT (real time) or NRT (near real time) image, video and audio media communication and data hiding, with no significant distortion of the medium. Additionally, this paper includes the proposal of specific case models such as Steganography of the total of Visual Cryptography schemes of black and white images. SMLSB is a different approach on real-time and non-real-time data hiding, which gives an advantage of robustness, while it provides various modes of the method depending on the requirements. The method can be used for the specific occasion of Visual Cryptography Ciphers Steganography. Despite the models' disadvantages, they can provide security robustness and higher capacity under the correct use. In some cases, the generalized method has minor computational costs and has no difference comparing LSB methods for real-time use while in others the computational cost should be considered, measured and compared.

"An Optimized Colour Image Steganography Using LFSR and DFT Techniques" journal stated that a colour image steganography method to conceal a secret data into the cover image in the frequency domain is suggested. In this method, Lempel– Ziv–Welch (LZW) compression is used to obtain a low bit rate whereas Linear Feedback Shift Register (LFSR) technique is used to enhance the security of the scheme. In the embedding process, an Adaptive Phase Modulation (APM) mechanism and Discrete Fourier Transform (DFT) are used for secret data embedding. The proposed method are high speed and

security, because of using hardware element LFSR and Data Encryption Standard (DES) cryptography.

2.8 Summary

In general, this chapter have discussed about the existing techniques, algorithms, encryption techniques and approach that has been used by other researcher to perform video steganography. We have also learned all the basic knowledge we require to make this project work.

Chapter 3

Methodology & System Design

Outline: This chapter presents the following:

1. Introduction
2. System Architecture
3. Technologies Used
4. Methodology

System Design is the process of designing the architecture, components, and interfaces for a system so that it meets the end-user requirements.System Design is the process of designing the architecture, components, and interfaces for a system so that it meets the end-user requirements. It's a wide field of study in Engineering and includes various concepts and principles that will help you in designing scalable systems.Systems design interfaces, and data for an electronic control system to satisfy specified requirements. System design could be seen as the application of system theory to product development. There is some overlap with the disciplines of system analysis, system architecture and system engineering.

3.1 Introduction

Managing a project, whether we're talking about prototype development or planning a corporate event, can be daunting, to say the least. The reality is that there is no secret formula that will make your project unwrap flawlessly; very often you'll stumble upon a series of challenges and obstacles before you reach success. And the ability to overcome those unexpected challenges and deal with them on the go is what makes us standalone in the crowd. In this chapter, we will talk about the model design for the project and discuss about the technical terms that will be engaged throughout the whole project. In this project, the proper methodology is chosen and will be followed until the end of the project. Proper project methodology plays the main role to make sure the project can be done well. Research on this topic is done to understand in depth on the technique and algorithm used during implementation. By using the methodology, it can ensure an exact process and increases the probability of achieving the desired final objective.

3.2 Technologies Used

3.2.1 Python

Figure 3.1: Pyhton

Python is a very popular general-purpose interpreted, interactive, object-oriented, and high-level programming language. Python is dynamically-typed and garbage-collected programming language. It was created by Guido van Rossum during 1985- 1990. Like Perl, Python source code is also available under the GNU General Public License. Python is a general-purpose, versatile, and powerful programming language. It's a great first language because Python code is concise and easy to read. Whatever you want to do, python can do it. From web development to machine learning to data science, Python is

the language for you.

3.2.2 VS Code

Visual Studio Code, also commonly referred to as VS Code,is a source-code editor made by Microsoft with the Electron Framework, for Windows, Linux and macOS. Features include support for debugging, syntax highlighting, intelligent code completion, snippets, code refactoring, and embedded Git. Users can change the theme, keyboard shortcuts, preferences, and install extensions that add additional functionality. Visual Studio Code is a source-code editor that can be used with a variety of programming languages, including Java, JavaScript, Go, Node.js, Python, C++, C, Rust and Fortran.[16][17][18][19] It is based on the Electron framework,[20] which is used to develop Node.js web applications that run on the Blink layout engine. Visual Studio Code employs the same editor component (codenamed "Monaco") used in Azure DevOps (formerly called Visual Studio Online and Visual Studio Team Services)
Visual Studio Code is a lightweight but powerful source code editor which runs on your desktop and is available for Windows, macOS and Linux. It comes with built-in support for JavaScript, TypeScript and Node.js and has a rich ecosystem of extensions for other languages and runtimes (such as C++, C, Java, Python, PHP, Go, .NET).

Figure 3.2: Visual Studio Code

3.2.3 Hardware Requirements

1. INTEL 15 2.50 GHZ 4 GB RAM

2. Minimum Hardware Requirement:
   Pentium 3 166 MHZ or Higher 128 mb RAM

3.3 System Architecture

3.3.1 Architecture

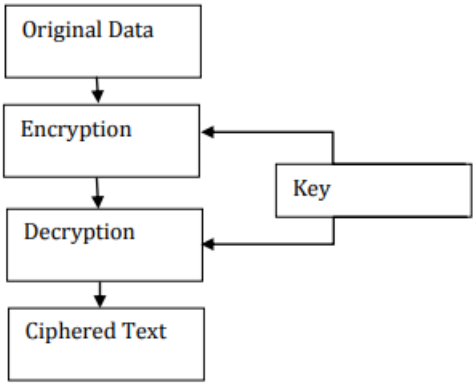

Fig2. Block Diagram

Figure 3.3: System Architecture

3.3.2 Block Diagram

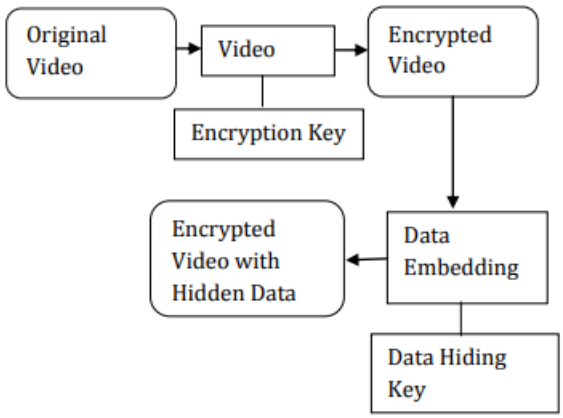

Figure 3.4: Block Diagram

3.3.3 Flow Diagram

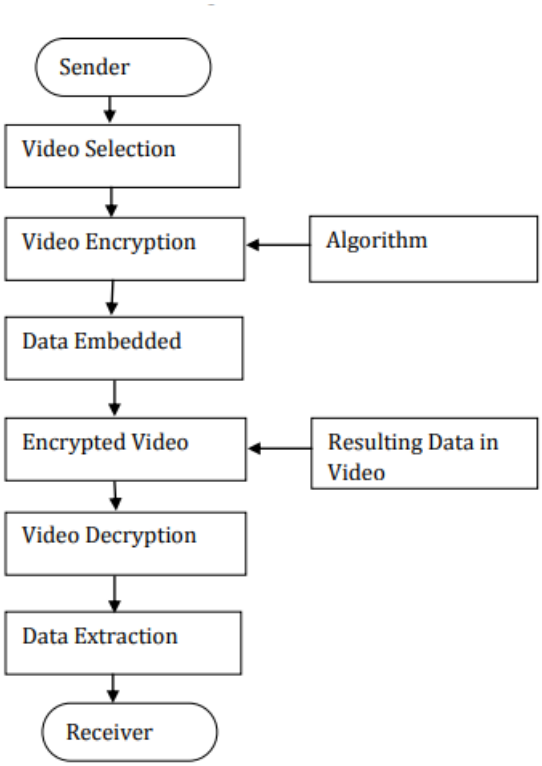

Figure 3.5: Flow Chart

3.3.4 Use-Case Diagram

A Use case diagram at its simplest is a representation of user's interaction with the system. First user writes secret text then he select the cover image and data gets hidden inside image, then user sends stegno image to receiver through image. At the receiver side, user selects the stego image and applies decryption on stego image. After that he can get text hidden in the text.

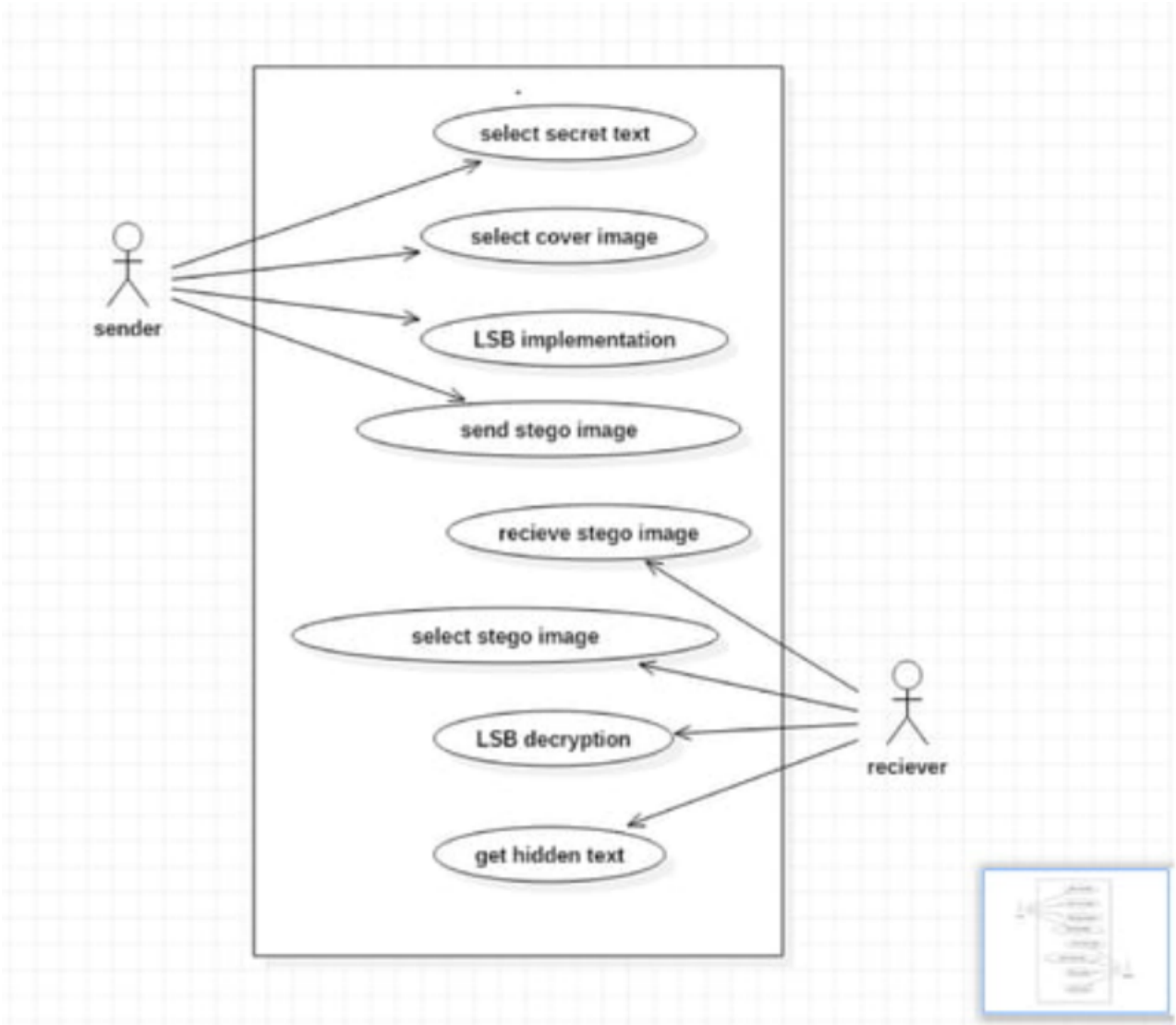

Figure 3.6: UseCase Diagram

3.4 Methodology

3.4.1 EMBEDDING PROCESS(IMAGE)

Step 1: Extract all the pixels from the given image and store them in some array named (imagearray).

Step 2: Extract all the characters from the given text file(message file) and store it in the array called (messagearray).

Step 3: Retrieve the characters from the Stego key and store them in a array called Keyarray. A stego- key is used to control the hiding process so as to restrict detection

and/or recovery of the embedded data.
Step 4: Take first pixel and characters from Key- array and place it in first component of pixel. If there are more characters in Key array, then place rest in the first component of next pixels.
Step 5: Place some terminating symbol to indicate end of the key. 0 has been used as a terminating symbol in this algorithm.
Step 6: Place characters of message Array in each component of next pixels by replacing it.
Step 7: Repeat step 6 till all the characters has been embedded.
Step 8:: Again place some terminating symbol to indicate end of data.
Step 9: Obtained image will hide all the characters that input.
The simplest steganography techniques embed the bits of the message directly into least significant bit plane of the cover image in a deterministic sequence. Modulating the least significant bit does not result in human-perceptible difference because the amplitude of the change is small. To hide a secret message inside an image, a proper cover image is needed. Because this method uses bits of each pixel in the image, it is necessary to use a lossless compression format, otherwise the hidden information will get lost in the transformations of a lossy compression algorithm. When using a 24-bit color image, a bit of each of the red, green and blue color components can be used, so a total of 3 bits can be stored in each pixel. In this case, only three bits needed to be changed to insert the character successfully. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximal cover size, The result changes that are made to the least significant bits are too small to be recognized by the human visual system (HVS), so the message is effectively hidden. As you see, the least significant bit of third color is remained without any changes. It can be used for checking the correctness of 8 bits which are embedded in these 3 pixels. In other words, it could be used as parity bit.

3.4.2 EMBEDDING PROCESS(VIDEO)

Step 1: Take the video from the user. And ask for the message and the password.Password will be used as AES key.
Step 2: A password is used for encoding secret text.
Step 3: Message is changed into ASCII format. Later message will be divided into small parts and store in an list.
Step 4: Extract the frames of the video.Hide the message in frames using encode method

which uses LSB algorithm

Step 5: Now we get encrpyted images which will be used as frame for the videos

Step 6: Now make video from the frames.

3.4.3 Extracting process

Step 1: Load the stego video.

Step 2: Use a password if given at encryption time.

Step 3: The regressive call decode image for each frame of the video

Step 4: Then, apply the LSB procedure on the stego picture.

Step 5: Get the riddle message and one of a kind video.

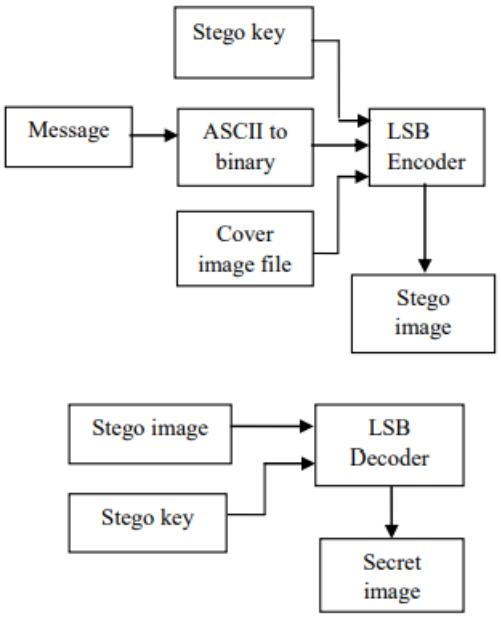

Figure 3.7: StegnoGraphy Process

Chapter 4

Implementation and Coding

Outline: This chapter presents the following:

1. Implementation
2. Coding
3. Result

Implementation is the execution or practice of a plan, a method or any design, idea, model, specification, standard or policy for doing something. As such, implementation is the action that must follow any preliminary thinking for something to actually happen. In an information technology (IT) context, the definition of implementation encompasses the processes that happen after the customer buys the product to get it operating properly.

4.1 Implementation

4.1.1 Encoding

Traverse through each pixel of the image and do the following:

1. Convert the pixel value to binary
2. Get the next bit of the message to be embedded
3. If the message bit and the LSB of the pixel are same, set temp = 0
4. If the message bit and the LSB of the pixel are different, set temp = 1
5. This setting of temp can be done by taking XOR of message bit and the LSB of the pixel
6. Update the pixel of output image to input image pixel value + temp
7. Keep updating the output image till all the bits in the message are embedded
8. Finally, write the input as well as the output image to local system.

4.1.2 Decoding

Traverse through each pixel of the image and do the following:

1. Load the stego-image that is sent from the sender.
2. Extract each of LSB bit from the stego image until to find out the end bit.
3. Reconstruct the collecting LSB bits from the stego-image.

4.1.3 Encrypt and decrypt

In this we change our password to AES value to encrypt or decrypt the data

1. Get the password from the user.
2. Using SHA-256 to make a new AES key which will help to encrypt and decrypt message into image.

4.2 Coding

4.2.1 Functions

4.2.1.1 def splitString(Message, count)

This functions is used to split message into small-small parts so that it can be stored in different different frame of the video. Here, Message contain the actual message and count means how many parts should be there. It return a list of strings which will be stored in stegno-images.

4.2.1.2 def FrameCapture(path, op, password, message="")

This functions is used to used to create frames from the video in which all tasks are done encryption and decryption.

4.2.1.3 def makeVideoFromFrame()

This function will create video from the frames which we get after encryption of the data.These frames are the stegno-images.

4.2.1.4 def encrypt(key, source, encode=True)

This function will take key, source, encode values which are password , message and boolean value if we want to encrypt or not respectively. This function will create AES key from the password.This AES will be used to encrypt the message into the images.

4.2.1.5 def decrypt(key, source, decode=True)

This function will take key, source, encode values which are password , message and boolean value if we want to encrypt or not respectively. This function will create AES key from the password. This AES will be used to decrypt the message into the images.

4.2.1.6 def encodeImage(image, message, filename)

This functions is used to encode the message into the image which we take both in argument and will store new stegno-image with specified filename also given in argument.

4.2.1.7 def decodeImage(image)

This functions is used to decode the message from the image which we take from argument and will return.

4.2.1.8 def getPixelCount(img)

This functions will return the number of pixel in an image.This function take input image.

4.2.2 Variables

4.2.2.1 headerText

This variable will store a predefined text which will be added to each stegno-image so that when we are extracting data from images the data is correct by checking if the header is present at decoded text, if yes then correct data is present otherwise there is not valid data.

4.2.2.2 tempFolder

This variable will store the name of the folder where all the frames and extracted audio will be stored.

4.2.3 Libraries

4.2.3.1 OS

We use this library to make new folders, delete frames which we generated, or to access images or videos.Python OS module provides the facility to establish the interaction between the user and the operating system. It offers many useful OS functions that are used to perform OS-based tasks and get related information about operating system. The OS comes under Python's standard utility modules. This module offers a portable way of using operating system dependent functionality.

4.2.3.2 cv2

We use this library to access, modify and edit videos.From this library we access frames of the video. CV2 is the huge open-source library for the computer vision, machine learning, and image processing and now it plays a major role in real-time operation which is very important in today's systems. By using it, one can process images and videos to identify objects, faces, or even handwriting of a human.

4.2.3.3 shelx

We use this library to write commands.The shlex class makes it easy to write lexical analyzers for simple syntaxes resembling that of the Unix shell. This will often be useful for writing minilanguages, (for example, in run control files for Python applications) or for parsing quoted strings.

4.2.3.4 AES and SHA256

We use this library to form key and get symmetric keys.The Advanced Encryption Standard (AES) is a symmetric block cipher chosen by the U.S. government to protect classified information. AES is implemented in software and hardware throughout the world to encrypt sensitive data. It is essential for government computer security, cybersecurity and electronic data protection.This module implements a common interface to many different secure hash and message digest algorithms. Included are the FIPS secure hash algorithms SHA1, SHA224, SHA256, SHA384, and SHA512 (defined in FIPS 180-2) as

well as RSA's MD5 algorithm (defined in internet RFC 1321). The terms "secure hash" and "message digest" are interchangeable. Older algorithms were called message digests. The modern term is secure hash.

4.2.3.5 ffmpeg

FFmpeg is a collection of libraries and tools to process multimedia content such as audio, video, subtitles and related metadata.
ffmpeg is a command line toolbox to manipulate, convert and stream multimedia content.
To install FFmpeg on Ubuntu/Debian, we can run the following command:

```
$ sudo apt install ffmpeg
```

```
> def encrypt(key, source, encode=True):···

> def decrypt(key, source, decode=True):···

> def convertToRGB(img):···

> def getPixelCount(img):···

> def encodeImage(image, message, filename):···

> def decodeImage(image):···

> def main(op, password, img_path, message=""):···

> if __name__ == "__main__":···
```

Figure 4.1: code for image

```
  temp_folder = "frame_folder"


> def split_string(s_str, count=10):···


> def createTmp():···


> def countFrames(path):···


  # Function to extract frames
> def FrameCapture(path, op, password, message=""):···


> def makeVideoFromFrame():···

> def main():···


> if __name__ == "__main__":···

  # ------------------------
```

Figure 4.2: code for video

4.3 Result

The following project was a successful attempt at employing stenography through the use of automation for the encryption and detection of the codes and messages through a picture and in later stages,on a video.This technique has been around since Greek times and has been used since long for concealing important and secret information in images and videos. This is extremely advantageous in ciphering data into seemingly normal images and videos. The code has successfully demonstrated the encoding as well as decoding of messages into images which is tested and proven in the sample test cases implemented above. We have implemented this using LSB and e-LSB.
Objective of any data hiding algorithm is to hide the data in such way that it should become difficult to retrieve the hidden data for unintended user. Code Word substitution is used to hide data in host video. Using this scheme file size of the host video is preserved alongside the confidentiality. This algorithm can achieve a better performance compared

with the other algorithms. So, the proposed framework features a potential to supply excellent RDH algorithms.

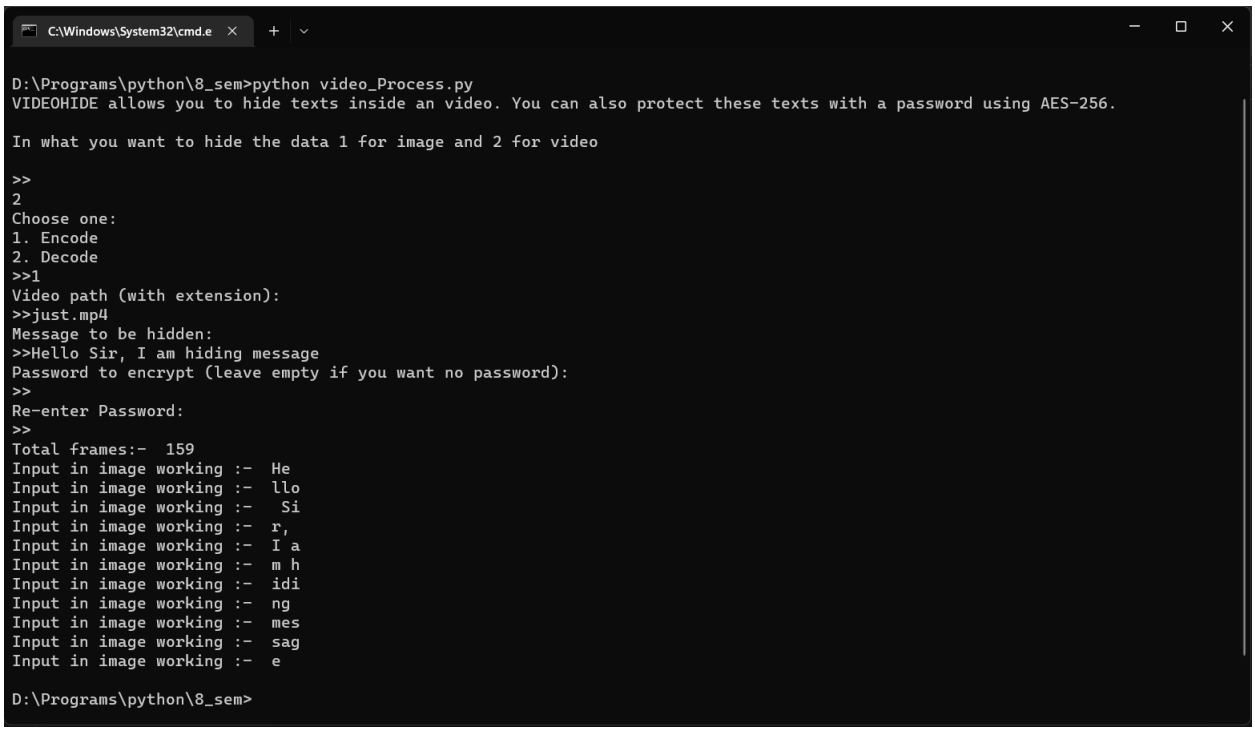

Figure 4.3: Data hiding

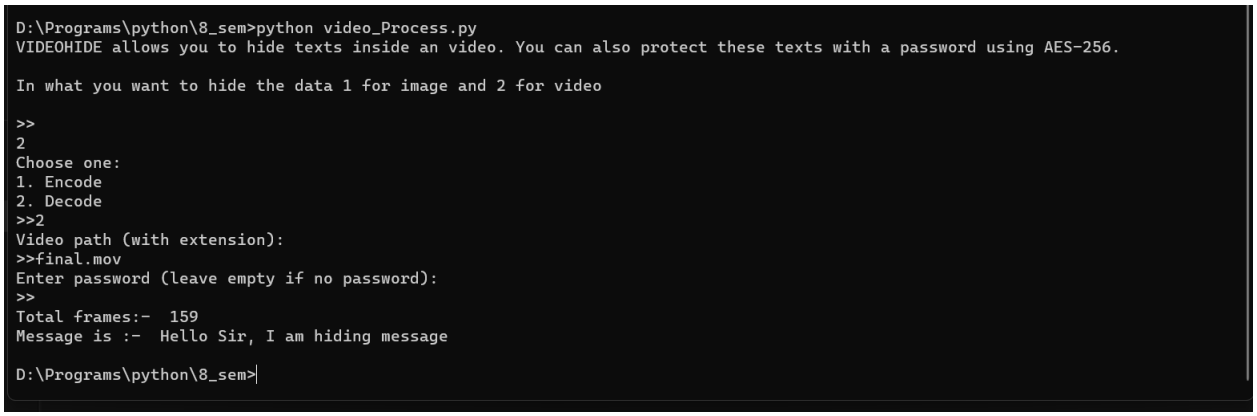

Figure 4.4: Data decoding

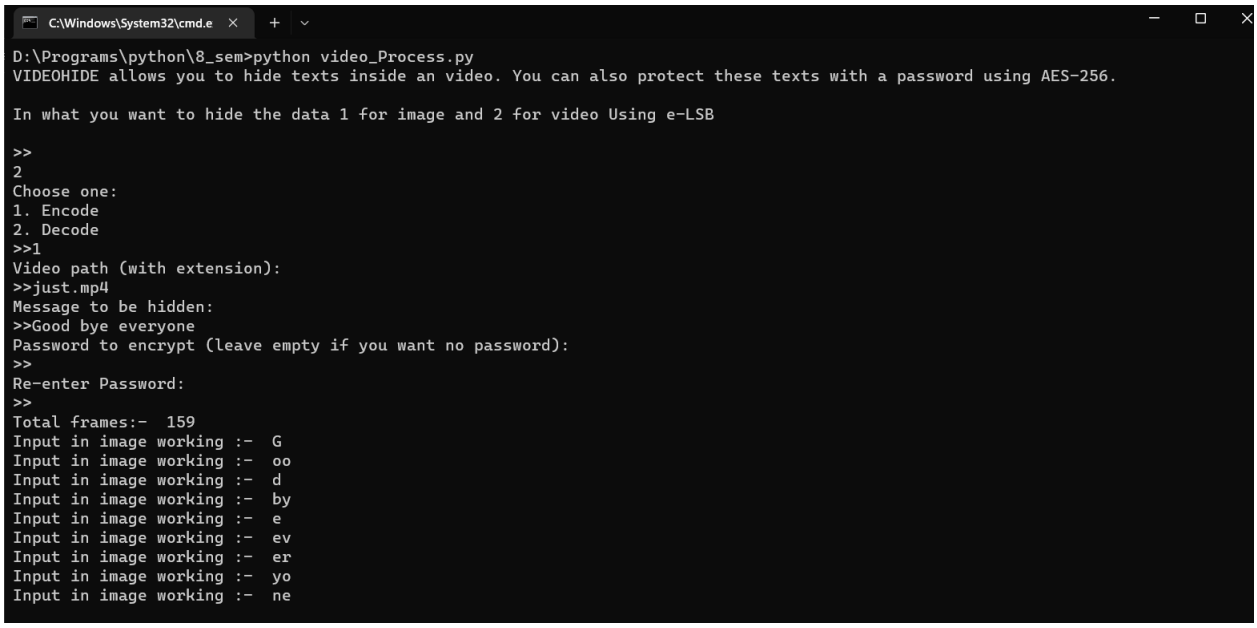

Figure 4.5: Data hiding using e-lsb

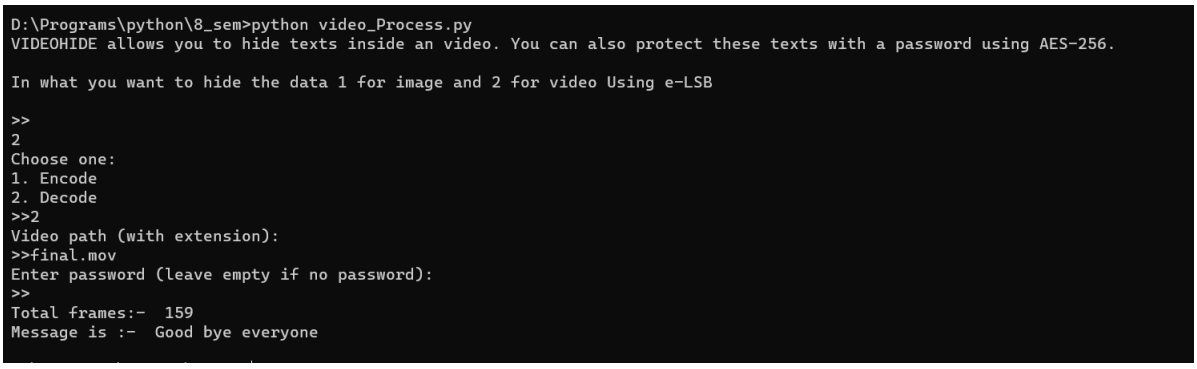

Figure 4.6: Data decoding using e-lsb

Chapter 5

Conclusion

Outline: This chapter presents the following:

1. Conclusion
2. Future direction

Future directions continue to be improvements in software and algorithms. There are always bigger or grander challenging problems to solve and any advantage is welcomed. Increasing the level of parallelism is desired for dealing with large scale computational and memory requirements. Algorithms that are able to parallelize dynamic programming problems over time such as time-clustering and that reduce the state space computation by targeting the neighborhood of the optimal trajectory. Also desired is the use of accurate upwinding schemes for more stability and the use of methods like multigrid which make convergence less sensitive to mesh size by using small and large mesh grids to filter out errors.

5.1 Conclusion

A successful project is the one which keeps on getting updated and upgraded with the new features, latest technologies and upgraded versions of itself. Before starting the project, it seemed to be way difficult, but as the research continued, the picture started getting clear. The development seemed to be quite easy.
Steganography is a really interesting subject and outside of the mainstream cryptography and system administration that most of us deal with day after day. "You never know if a message is hidden", this is the dilemma that empowers steganography. As more emphasis is placed on the areas of copyright protection, privacy protection, and surveillance, we believe that steganography will continue to grow in importance as a protection mechanism.
This projected system is to supply an honest, economical technique for activity the info from programmers and sent to the goal in an exceedingly protected means. This projected framework will not modification the span of the document even within the wake of encryption and what is more applicable for a sound record position. secret writingand secret writing strategies are used to form the safety framework robust. The projected framework captivated with the examination discoveries engineered up associate application which might possibly shroud data into video photos (AVI) that provides a robust and secure technique for datatransmission. This Stego framework executes steganography in video image associated uncover method while notrestarting the applying or starting an alternate application. Likewise this framework may be a Platform-free application with high convenientce and high Consistency.

5.2 Future direction

Steganography, though is still a fairly new idea. There are constant advancements in the computer field, suggesting advancements in the field of steganography as well. It is likely that there will soon be more efficient and more advanced techniques for Steganalysis. A hopeful advancement is the improved sensitivity to small messages. Knowing how difficult it is to detect the presence of a fairly large text file within an image, imagine how difficult it is to detect even one or two sentences embedded in an image! It is like finding a microscopic needle in the ultimate haystack. What is scary is that such a small file of only one or two sentences may be all that is needed to commence a terrorist attack.

In the future, it is hoped that the technique of Steganalysis will advance such that it will become much easier to detect even small messages within an image. In this work it explores only a small part of the science of steganography. As a new displine, there is a great deal more research and development to do. The following section describe areas for research which were offshoots of, or tangential to,our main objectives.

1. Detecting Steganography in Image Files: Can steganography be detected in images files? This is difficult question. It may be possible to detect a simple Steganographic technique by simple analyzing the low order bits of the image bytes. If the Steganographic algorithm is more complex, however, and spreads the embedded data over the image is random way or encrypts the data before embedding, it may be nearly impossible to detect.

2.Steganography on the World Wide Web: The world wide web(www) makes extensive use of inline images.There are literally millions of images on various web pages worldwide. It may be possible to develop. an application to serve as a web browser to retrieve data embedded in web page images. This stego-web could operate on top of the existing WWW and be a means is seminating informat of covertly.

3.Steganography in printed media: If the data is embedded in an image, the image printed, then scanned and stored in a file can the embedded data be recovered? This would require a special form of a steganography to which could allow for in accuracies in the printing and scanning equipment.

The scope of the project is to limit unauthorized access and supply better security during message transmission. To meet the wants, I exploit the straightforward and basic approach of steganography.

• During this project, the proposed approach finds the acceptable algorithm for embedding the info in a picture using steganography which provides the higher security pattern for sending messages through a network.

• For practically implementing the function of the discussed algorithms, Matlab framework is employed.

Bibliography

[1] "Steganography: How to Send a Secret Message By Bryan Clair" http://www.strangehorizons.com/2001/20011008/steganography.s html

[2] "A detailed look at SteganographicTechniques and their use in an Open-SystemsEnvironment" http://www.scribd.com/word/full/20529?access_key=34h2xr3z7wokx

[3] Steganography from Wikipedia http://en.wikipedia.org/wiki/Steganograph

[4] Image Steganography and Steganalysis http://www.ims.nus.edu.sg/Programs/imgsci/files/memon/sing_stego.pdf

[5] J. J. Chae, B. S. Manjunath, "Data Hiding in Video",Proceedings of the 6th IEEE International Conference on Image Processing, 1999, pp.311-315

[6] M. Wu, H. Yu, and B. Liu, "Data hiding in image and video: II. Designs and applications," IEEE Trans. Image Process, vol. 12, no. 6, pp. 696–705, Jun. 2003.

[7] B. Chen and G. W. Wornell, "Quantization index modulation: a class of provably good methods for digital watermarking and information embedding," IEEE Transactions on Information Theory, vol. 47, May 2001, pp. 1423-1443, May 2001.

[8] K. Steffy Jenifer , G. Yogaraj , K. Rajalakshmi, "LSB Approach for Video Steganography to Embed Images", IJCSIT, Vol. 5 (1) , 2014, 319-322, ISSN:0975-9646

[9] Kousik Dasguptaa, Jyotsna Kumar Mondal and Paramartha Dutta, "Optimized Video Steganography using Genetic Algorithm (GA)", International Conference on Computational Intelligence: Modeling, Techniques and Applications (CIMTA), Procedia Technology 10 (2013) 131 – 137.

[10] Miss. Komal R. Hole, Prof. Vijay S. Gulhane, Prof. Nitin D. Shellokar, "Application of Genetic Algorithm for Image Enhancement and Segmentation", IJARCET, ISSN: 2278 – 1323, Volume 2, Issue 4, April 2013

[11] Amrita Khamrui, J K Mandal, "A Genetic Algorithm based Steganography using Discrete Cosine Transformation", International Conference on Computational Intelligence: Modeling Techniques and Applications (CIMTA) 2013.

[12] Dr.Ban A . Mitras and Dr. Nada F. Hassan," Using Hybird Genetic Algorithm In Audio Steganography", Iraqi Journal of Statistical Sciences (25), pp [150-164], 2013.
[11]Juhi Saurabh, Asha Ambhaikar, Audio Steganography