A

Seminar-II Report

on

SECURED AND IMPROVED TECHNIQUE FOR DATA HIDING IN VIDEO

Submitted in Partial Fulfillment of
the Requirements for the Final Year
of

Bachelor of Engineering

in

Computer Engineering

to

North Maharashtra University, Jalgaon

Submitted by

Ms.Madhuri Rajendra Patil

Under the Guidance of

Mr.Dipak D.Bage

DEPARTMENT OF COMPUTER ENGINEERING
SSBT's COLLEGE OF ENGINEERING AND TECHNOLOGY,
BAMBHORI, JALGAON - 425 001 (MS)
2016 - 2017

SSBT's COLLEGE OF ENGINEERING AND TECHNOLOGY, BAMBHORI, JALGAON - 425 001 (MS)

DEPARTMENT OF COMPUTER ENGINEERING

CERTIFICATE

This is to certify that the seminar-ii entitled *Secured and Improved Technique for Data Hiding in Video*, submitted by

Ms.Madhuri Rajendra Patil

in partial fulfillment of the Final Year of *Bachelor of Engineering* in *Computer Engineering* has been satisfactorily carried out under my guidance as per the requirement of North Maharashtra University, Jalgaon.

Date: October 5, 2016
Place: Jalgaon

Mr.Dipak D.Bage
Guide

Prof. Dr. Girish K. Patnaik
Head

Prof. Dr. K. S. Wani
Principal

Acknowledgement

No work can be accomplished unless it has evolved as a result of co-operating, assistance and understanding of some knowledgeable group of people.I take the opportunity to thank our Principal Prof.Dr.K.S.Wani and Head of Department Prof. Dr.Girish K. Patnaik for providing all the necessary facilities, which were indispensable in the completion of seminar. I would like to thank my guide Mr.Dipak D. Bage for providing to be a great help by giving us guidance through their vast experience and intellectual skills. I would also thankful to all the staff members of the Computer Engineering Department.I would also like to thank the college for providing the required magazines, books and access to the internet for collecting information related to the project.Finally,I would like to thank my parents.

Ms.Madhuri Rajendra Patil

Contents

List of Figures

Abstract

Data hiding techniques have taken important role with the rapid growth of intensive transfer of multimedia content and secret communications. The method of Steganography is used to share the data secretly and securely. It is the science of embedding secret information into the cover media with the modification to the cover image, which cannot be easily identified by human eyes. Steganography algorithms can be applied in audio, video and image file. Hiding secret information in video file is known as video steganography. Video Steganography means hiding a secret message that can be either a secret text message or an image within a larger one in such a way that just by looking at it, an unwanted person cannot detect the presence of any hidden message. For hiding secret information in the video, there are many Steganography techniques which are further explained is along with some of the research works done in some fields under video steganography by some authors. Here describes the progress in the field of video Steganography and intends to give the comparison between its different uses and techniques.

Chapter 1

Introduction

Steganography is the practice of concealing a file,message, and important information of any format as text, image, audio or video within another file, message, of any format. Steganography is the art of hiding the information in some other host object. In ancient time this technique is used as, secret information is hidden in the back of wax, scalp of the slaves, in rabbits etc. The word steganography used from the past combines the Greek words steganos, meaning "covered, concealed, or protected", and graphein meaning "writing".[1]

In chapter,section 1.1 describes the introduction related to Video Steganography.Section 1.2 describes the summary of chapter.

1.1 Introduction

In todays scenario of high speed internet, people are worried about the information being hacked by attackers. However, the safety and security of long distance communication remains an issue. So in order to overcome this problem many algorithms of steganography have been proposed. The word steganography is derived from the ancient Geek words steganos meaning covered, concealed, or protected and graphein meaning writing. There are other two technologies which are closely related to steganography . One of them is watermarking. In a digital watermarking technique, a signal is permanently embedded into digital data like audio, image, video and text. It can be detected or extracted afterwards to confirm the authenticity of the data. Second is the fingerprinting, in which unique marks are embedded in the copies of carrier object that are supplied to different customers. Basically, these two properties are used for intellectual property protection .[2]

The premise from which to measure a secure video steganography system is to assume that the opponent knows the system being employed, yet still cannot find any evidence of the hidden message. Video steganography algorithm tries to replace the redundant bits of the cover medium by the bits of the secret medium. Now the availability of those redundant bits to be inserted in the cover media depends on the quality of video or sound. Military, industrial applications, copyright, intellectual property rights etc. are some of the most commonly used applications of video steganography.

The advantages of using video stream as the cover file are to get extra security against the attacker because the video file is much more complex that the image file. One more advantage of embedding the secret data to the video is that the secret data is not recognized by the human eye as the change of a pixel color is negligible. In video steganography,It also very secretly hide data in audio files as it contains unused bits.It can store secret data up to about four least significant bits in the audio file. So it is more beneficial to use video steganography rather than other steganography methods when we need to store more amounts of secret data.[3]

1.2 Summary

In this chapter, an overview of the problem statement along with its solution for the work contained in this dissertation is provided. In the next chapter, related work of Video Steganography is presented.

Chapter 2

Literature Survey

In conventional cryptography, even if the information contents are protected by encryption, the existence of encrypted communications is known. In view of this, digital steganography provides an alternative approach in which it conceals even the evidence of encrypted messaging. Generally, steganography is defined as the art and science of communicating in a covered fashion. It utilizes the typical digital media such as text, image, audio, video, and multimedia as a carrier (called a host signal) for hiding private information in such a way that the third parties (unauthorized person) cannot detect or even notice the presence of the communication. In this way, steganography allows for authentication, copyright protection, and embedding of messages in the image or in transmission of the image.[1]

In chapter,Section 2.1 describes background of Steganography.Section 2.2 describes the defination of steganography and section 2.3 is describes the types of video steganography and summary of chapter.

2.1 What is Steganography ?

Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video. The word steganography combines the Greek words steganos , meaning "covered, concealed, or protected", and graphein meaning "writing".The first recorded use of the term was in 1499 by Johannes Trithemius in Steganographia, a treatise on cryptography and steganography, disguised as a book on magic. Generally, the hidden messages appear to be (or be part of) something else: images, articles, shopping lists, or some other cover text. For example, the hidden message may be in invisible ink between the visible lines of a private letter. Some implementations of steganography that lack a shared secret are forms of security through obscurity, whereas key-dependent steganographic schemes adhere to Kerckhoffs's principle.

Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. For example, a sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it.[5]

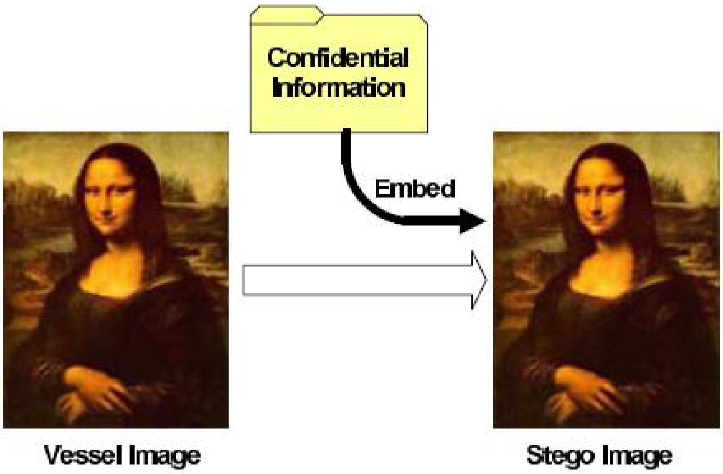


Figure 2.1: Text Steganography

2.2 Types of Steganography

The Steganography method is different from the traditional cryptography method in following ways. Cryptography is the practice and study of secure communication. Steganography is the art and science of covert communication. Cryptography protect the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message.

- **Text Steganography** Steganography can be classified into image, text, audio and video steganography depending on the cover media used to embed secret data. Text steganography can involve anything from changing the formatting of an existing text, to changing words within a text, to generating random character sequences or using context-free grammars to generate readable texts. Text steganography is believed to be the trickiest due to deficiency of redundant information which is present in image, audio or a video file. The structure of text documents is identical with what that observe, while in other types of documents such as in picture, the structure of document is different from what that observe. Therefore, in such documents, It can hide information by introducing changes in the structure of the document without making a notable change in the concerned output . Unperceivable changes can be made to an image or an audio file, but, in text files, even an additional letter or punctuation can be marked by a casual reader . Storing text file require less memory and its faster as well as easier communication makes it preferable to other types of steganographic methods . Text steganography can be broadly classified into three types: Format based Random and Statistical generation, Linguistic methods.

Figure 2.2: Image Steganography

- **Image Steganography**

  In image steganography, a secret data (image or text) can be embedded in the cover image.Image are used as the message carriers.Image are most popular cover objects used for steganography.In this approach, the least significant bits of the cover image are replaced with secret image without modifying the complete cover image. LSB is the most common and simplest method for data hiding . Another method of steganography was proposed to hide a secret data into a gray cover image. In this, a cover image is partitioned into blocks of two consecutive pixels. This technique of hiding the secret data gives better result as compare to LSB techniques. The main drawback of LSB technique is the ease of extraction. So to overcome this drawback researcher found better way for embedding the secret message so that it dont attract the eavesdroppers.

- **Audio Steganography**

  Audio steganography worksby slightly changing the binary sequence and concealing with the secret message.Several methods are proposed such as Least Significant Bit(LSB) replacing last digit of carrier file.Parity coding involves breaking down of signal and then hiding the message in parity bits of each sample.Phase coding involves encoding of secret data to phase shifts.Spread spectrum distributes secret data into frequency spectrum,in which direct sequence and frequency hopping is used.The Echo method generates echo for insertion of secret data into signal.

Figure 2.3: Audio Steganography

- **Video Steganography**

  Video Steganography is the art of hiding information in ways that avert the revealing of hiding messages in videos. Actually message like text, image, audio, video and etc. It is focused on spatial and transform domain. Spatial domain algorithm directly embedded information in the cover image with no visual changes with good quality. The result of algorithms has the advantage in Steganography capacity. Transform domain algorithm is embedding the secret information in the transform space. This kind of algorithms has the advantage of good stability, but the disadvantage of small capacity.[4]

Figure 2.4: Video Steganography

2.3 Summary

In this chapter, an background of Steganography is provided. In the next chapter, methodology used to implement Video Steganography is presented.

Chapter 3

Methodology

The best technique is to hide the secret data along with the quality of the cover video, is that it cannot be detected by naked eyes. The embedded video is known as the stego video which is sent to the receiver side by the sender. Variety of video steganography techniques are used now days, out of which to secure important information have use the combination of some methods as Advanced Video Steganography. In advanced video steganography technique, It make use of combination of video Compression, video Encryption and finally embedding that video. This advanced video steganography technique is proposed in further section. There also consist of Literature Survey of some methods used by some authors and advantages of this advanced video steganography methods.[2]

In chapter,Section 3.1 describes Video Steganography Architecture and Section 3.2 describes various technique of video steganography.Section 3.3 discuss summary of chapter.

3.1 Architecture

3.1.1 Algorithm

Block diagram of the proposed video steganography technique is shown in the figure 2. The overall process is divided into a two parts. First part deal with the message embedding process in the video sequence i.e. making stego video while the second part deal with the extraction of message from the stego video. **Algorithm steps which are used in this algorithm to hide the message in the video sequence are as follows-**

1. Input the video.

2. Resize the video.

3. Convert the video in to a frames and store all the frames in to a folder.

4. With the help of Key1 select the random frames for data hiding.

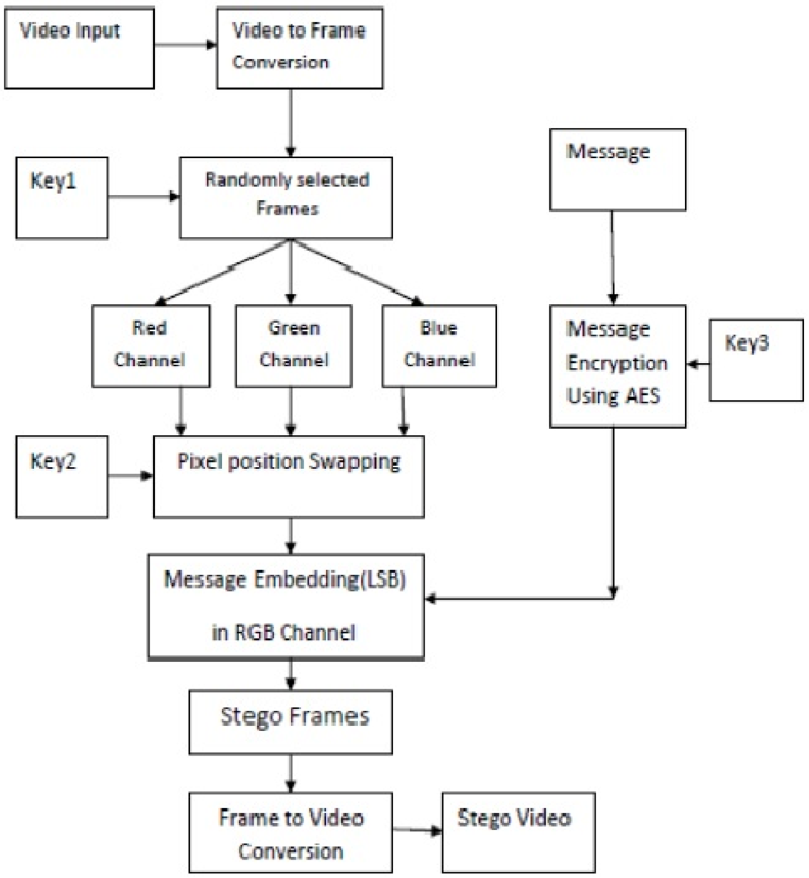


Figure 3.1: Block Diagram of Proposed Video Stegnography Algorithm

5. Separate the Red , Green and Blue channel from the selected frames.

6. Separate the Red , Green and Blue channel from the selected frames.

7. Select the Blue channel of each frames for data hiding.

8. With the help of Key 2 swap the position of pixel of the blue channel of the selected frames.

9. Enter the message which is to be hidden.

10. Encrypt the message by applying AES algorithm with the help of Key 3.

11. Embed each message bit to the pixel obtain in the step 7 using LSB method to get the stego frames

12. Continue this process till all the message bit is embedded.

13. Convert all the stego frames in to a video to get a stego video.

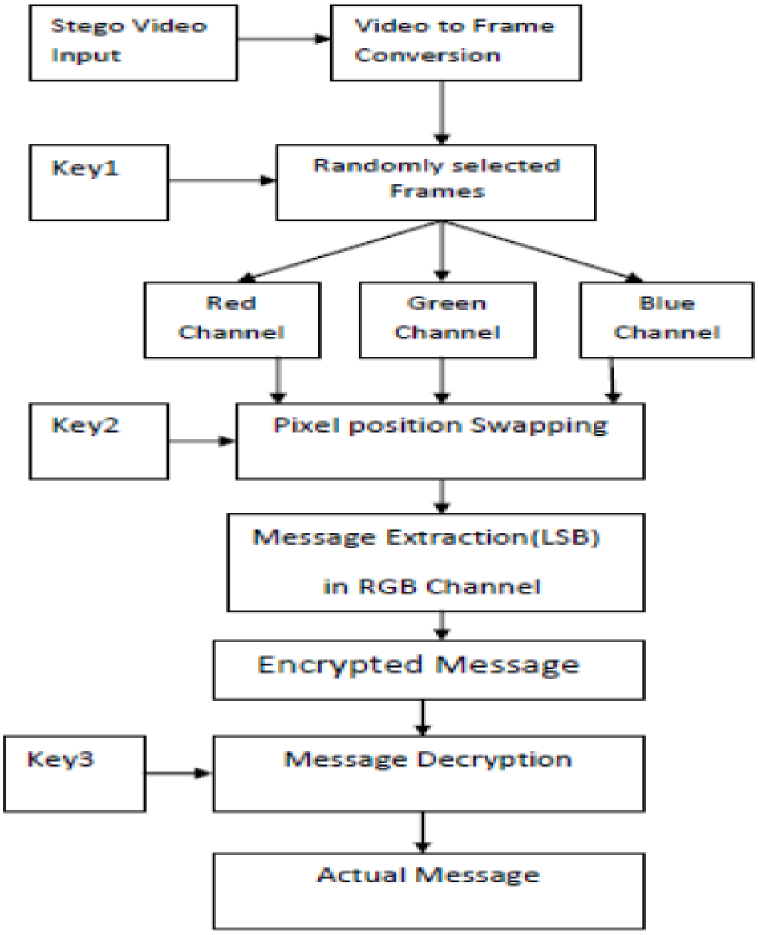


Figure 3.2: Block Diagram of Message Extraction Process

Algorithm steps for encrypting the message are as follows-

1. Input the stego video.

2. Convert the video in to a frames and store all the frames in to a folder.

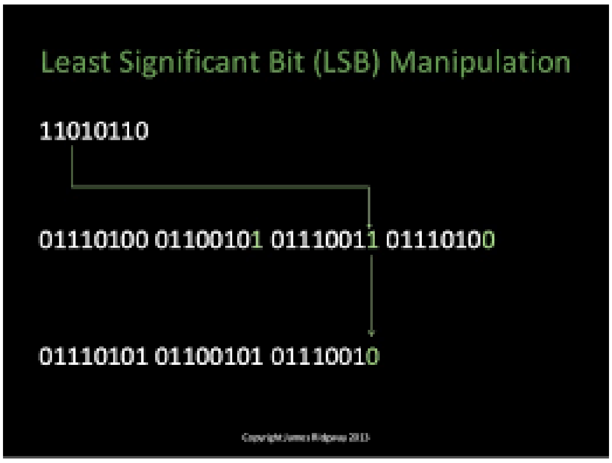
3. With the help of Key1 select the random frames for data hiding.

4. Separate the Red , Green and Blue channel from the selected frames.

5. Select the Blue channel of each frames for data hiding.

6. With the help of Key 2 swap the position of pixel of the blue channel of the selected frames get the message in encrypted form.

7. Apply the AES decryption method to get the original message from the encrypted form.[3]



Least Significant Bit (LSB) Manipulation

11010110

01110100 01100101 01110011 01110100

01110101 01100101 01110010

Copyright James Ridgeway 2013

Figure 3.3: Method of Least Significant Bit

3.2 Various Techniques

3.2.1 Video Steganography Techniques

- Least Significant Bit.
- The Discrete cosine Transform.
- Non-uniform rectangular partition.

▮ *Least Significant Bit:*

The above Fig:3.3 shows LSB is the lowest bit in a series of numbers in binary. E.g. in the binary number: 10110001, the least significant bit is far right. The LSB based Steganography is one of the steganographic methods, used to embed the secret data in to the least significant bits of the pixel values in a cover image. e.g. 240 can be hidden in the first eight bytes of three pixels in a 24 bit image.Simple bit exchange method is introduced for encrypting any file. The following are the steps for encryption method.Read one by one byte from the secret message file and convert each byte to 8-bits Then apply 1 bit right shift operation on the entire file so that each byte will be modified accordingly.We read 8 bits at a time and divide into two blocks 4 bits each and then perform the XOR operations with 4-bits on the left side with 4 bits on the right side and substitute the new bits in right 4-bit positions. The same thing repeated for all bytes in the file.

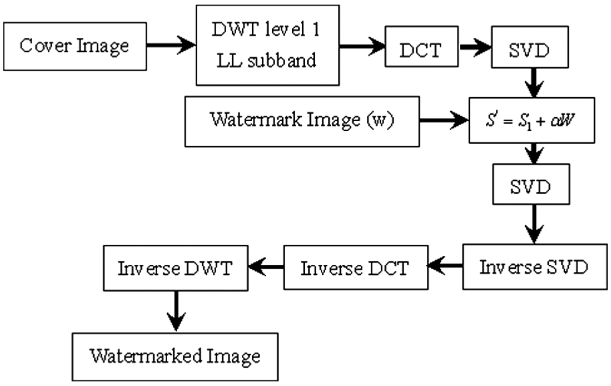


Figure 3.4: Method of Discrete Cosine Transform

- *The Discrete Cosine Transform:*

The above Fig:3.4 shows DCT coefficients are used for JPEG compression. It separates the image into parts of differing importance. It transforms a signal or image from the spatial domain to the frequency Here, the input image is of size N X M. c(i, j) is the intensity of the pixel in row i and column j; C(u,v) is the DCT coefficient in row u and column v of the DCT matrix. Signal energy lies at low frequency in image; it appears in the upper left corner of the DCT. Compression can be achieved since the lower right values represent higher frequencies, and generally small enough to be neglected with little visible distortion. DCT is used in steganography as: Image is broken into 88 blocks of pixels. Working from left to right, top to bottom, the DCT is applied to each block. Each block is compressed through quantization table to scale the DCT coefficients and message is embedded in DCT coefficients.

- *Non-uniform Rectangular Partition:*

The above Fig:3.5 shows Proposed the algorithm of the non-uniform rectangular partition of image according to the pixel gray values. When the initial partition, the bivariate polynomial and the error control value are all determined, this adaptive partition algorithm can be applied to do the non-uniform rectangular partition of image. The main principle of this algorithm is that it uses the Optimal Quadratic Approximation with a specified bivariate polynomial (with undetermined coefficients) to approximate the gray values within the sub-images, if the determined bivariate polynomial can recover the original sub-image under the required control error, then the partition process will be stopped, otherwise the current sub-image will be divided into four smaller congruent rectangles and repeat the approximation process again until the approximation requirement reaches or the number of the undetermined coefficients of the bivariate polynomial is less than or equal to the pixel number within the sub-rectangle. Finally, according to the partitioned codes obtained, the original image can be reconstructed approximately.[3]

3.3 Summary

In this chapter, an overview of the methodology used to implement technologies is presented. In the next chapter,discussion related with Video Steganography is presented.

Chapter 4

Discussion

The proposed scheme is a data embedding method that uses high resolution digital video as a cover signal. The proposed scheme provides the ability to hide a significant quality of information making it different from typical data embedding mechanisms because we consider application that require significantly larger payloads like video-in-video and image-in-video. The purpose of embedding such information depends on the application and the needs of the owner/user of the digital media.[2]

In chapter,Section 4.1 describes application of Video Steganography.Section 4.2 describes the advantage and disadvantage of video steganography.Section 4.4 describes the summary.

4.1 Application

- The main object of steganography is hiding data, and there are a lot of applications that use this technique for hiding data such as digital watermarking, secret communication, terrorists, copyright protection, and feature tagging, this sub-section introduces a brief description of each mentioned application.

- Digital watermarking considers as one of the most important applications of steganographyand may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. It basically embeds a digital watermark into an image.

- In secret communication application, there are two parties can communicate secretly without anyone knowing about the communication. The application depends only on an encoding the message and on the other side hides the existence of the message in some cover media.

- The terroriststeganography application can be used in large scale, they hide their secret messages in innocent or needing for donating and they cover the main targets to spread terrorism across the region or a part of the world.

- The copyright protection application related to watermarking, for example,a secret message is embedded in the images which serve as the watermark and thus identify it as an intellectual property which belongs to a particular owner.
- Feature tagging application such as captions, annotations, and thename of the individuals in a photo or location in a map can be embedded in an image.
- Copying the stego-image also copies all of the embedded features and only parties who possess the decoding stego-key will be able to extract and view the features[1]

4.2 Advanteges and Disadvantages

4.2.1 Advanteges:

- Since random data are also placed in unused frames in the video, the attacker is left clueless to know the real secret data hidden in the video. Hence highly confidential data like military secrets and bank account details can be easily steganographed in ordinary video and can be transmitted over internet even in unsecured connection.
- Text based steganography has limited capacity and Image steganography tried to improve the capacity where 50 percent of original image size can be used to hide the secret message. But there is limitation on how much information can be hidden into an image. Video Steganography has been found to overcome this problem.
- Lowest chances of perceptibility because of quickly displaying of the frames, so its become harder to be suspected by human vision system.
- Since the transmission of any data is always subject to corruption due to errors, then the video transmission must deal with these errors without retransmission of corrupted data. This is another application for steganography rather than security purpose.
- Since use of indexing concept, the process of retrieving the secret data from the steganographed video becomes very simple and requires very less time.
- This stage maintains the visual quality of the video. The output of this stage is stego video. The two stages enhance the security of the secret text message by using steganography twice.

4.2.2 Disadvantages

- **Lossless Process:**Encrypted video file is too big to be a cipher even for a small message.

- **No sound is there in stego video:**The hiding process does not take into account the audio component of the video.
- **Possibility of same character occurrence:** It is expected that generated random numbers in key will be distinct. No two numbers in a key will be same at a particular run.[4]

4.3 Summary

In this chapter,discussion on related with Video Steganography. In the next chapter,conclude the Video Steganography.

Chapter 5

Conclusion

In general, steganography is used to transfer secret information in communication system. A video steganograpgy method has been developed to transfer the secret data. Text, image, audio and video can be taken as the secret data which can be hidden in the video clips. In this scheme, though, least significant bit method is used for data hiding. LSB method of data hiding is not secure method for data hiding therefore in this method random frames selection algorithm and pixel swapping algorithm is incorporated to enhance the security of this method. Moreover the data itself is encrypted before embedding operation to make this system more secure. Both the modification in the existing method enhanced the security.Hiding a message with steganography methods reduces the chance of a message not visible for intruders. A small review about of the art of video steganography. Various types of video stegnography techniques. Comparing the performance of video stegnographic technique is difficult unless identical data sets and performance measures are used. The video stegnographic techniques are obtained good for certain applications like security technologies in videos.

Bibliography

[1] International Journal of Advanced Research in Computer Engineering and Technology Volume 4 Issue 10, October 2015.

[2] International Journal of Computer and Organization Trends Volume 5 February 2014.

[3] Uma Sahu et al, International Journal of Computer Science and Communication Networks,Vol 5(5),348-357.

[4] Pritish Bhautmage, Prof. Amutha Jeyakumar / International Journal of Engineering Research and Applications ISSN: 2248-9622 www.ijera.com Vol. 3, Issue 1, January -February 2013, pp.1641-1644.

[5] International Journal of Computer Applications (0975 8887) Volume 95 No.20, June 2014