Secured Data Transmission using Video Steganography

[1]Anusha D B , [2]Ashwini B S, [3]Lakshmi N S, [4]Sindhura B L, [5]Nalina H.D
Dept. of ECE, GSSSIETW, Mysuru,
Karnataka, India

Abstract— **The development of high speed computer networks and Internet has increased the easiness of Information Communication. Information security has become the area of concern. Emergence of internet has made it possible to transfer the data from one place to another place rapidly and accurately. This data when goes through the internet may become a victim of the hackers who can steal, modify and misuse the information. Steganography is one such solution to this problem. The data security approach when combined with encryption and steganographic techniques for secret communication by hiding it inside the multimedia files has gained importance.**

Video and images are very common choice for hiding data. It is very important for effective and successful embedding process to select appropriate pixels in the video frames, which are used to store the secret data. Original message is converted into cipher text by using secret key and then hidden into the LSB of original image using the AES encryption algorithm. We use video based Steganography because of large size and memory requirements. This paper will focus on hiding information in specific frames of the video and in specific position of the frame by LSB substitution.

Keywords— Security ;Steganography ;LSB;AES Encryption technique ; Cryptography.

I. INTRODUCTION

Video is an electronic medium for recording , copying , playback , broadcasting and display of moving visual media. Video security has gained importance over time in numerous applications where in information in the form of video is to be secured from an unauthorized user. Video consisting of several frames is nothing but images.

The use of internet has increased tremendously over the years and the concept of data security is gaining momentum. The word steganography combines the Greek words steganos meaning “covered” and graphein meaning “writing”. The art and science of hiding information by embedding messages within other is known as Steganography. It is an encryption technique that can be used along with cryptography as an extra-secure method in which to protect data. It can be applied to images, a video file or an audio file. Steganography is used to supplement encryption. An encrypted file may still hide information, by using Steganography even if the encrypted file is deciphered , the hidden message is not seen.

Cryptography involves creating written or generated codes that allow information to be kept secret.Cryptography converts data into a format that is unreadable for an unauthorized user, allowing it to be transmitted without unauthorized entities decoding it back into a readable format, thus compromising the data. Cryptography is the study of hiding information, while Steganography deals with composing hidden messages so that only the sender and the receiver know that the message even exists. In Steganography, only the sender and the receiver know the existence of the message, whereas in cryptography the existence of the encrypted message is visible to the world. Due to this, Steganography removes the unwanted attention coming to the hidden message.

Cryptographic methods try to protect the content of a message , while Steganography uses methods that would hide both the message as well as the content. By combining Steganography and Cryptography, one can achieve better security. Hiding information in a carrier file uses least significant bit (LSB) insertion technique. In Least significant bit (LSB) insertion technique, for hiding information, we change the LSB of video file with the information bits [3]. LSB insertion is the simplest technique for implementing Video Steganography. The LSB method substitutes the LSBs of the hidden message with the LSBs of cover video frames. Substituting data in the LSBs of any cover media is not detectable by human eyes (Human Visual System) i.e. very less change in the color [4]. Here the bits of image from video are directly embedded into the least significant bit plane of cover frame in deterministic sequence.

AES (acronym of Advanced Encryption Standard) is a symmetric encryption algorithm. The algorithm was developed by two Belgian cryptographers Joan Daemen and Vincent Rijmen.AES was designed to be efficient in both hardware and software, and supports a block length of 128 bits and key lengths of 128, 192, and 256 bits [2]. AES is more secure than its predecessors DES and 3DES as the algorithm is stronger and uses longer key lengths. It also enables faster encryption than DES and 3DES, making it ideal for software applications, firmware and hardware that require either low latency or high throughput. We use 128 bit key for an AES algorithm which specifies the number of repetitions should be 10 cycles transformation rounds that convert the input called plain text into final output called cipher text. Each round consists of several processing steps that depends on the encryption key [5].

II. OBJECTIVES

Now days hacking activities are growing day by day and hackers can easily hack important information and security is not sufficient to stop hacking. It would be of greater problem in reputed organizations. Hence, we need better solutions which have good security level with lower cost. The confidential or important information, which sent with normal format, there might be a chance of misuse cases. To avoid this, data has to be encrypted while sending. Hiding secret data into carrier in order to convey secret message confidentially plays a major role. The main objective of our project is

- To design and create the web page for sending and receiving the video file.
- To develop code for data encryption using AES algorithm.
- To ensure secured transmission using video Steganography.

III. LITERATURE REVIEW

Every software development requires the survey process. The survey process is needed to get the requirement for the software. The survey also consists of studying the present system and also studying about the tools needed for the development of the software. A proper understanding of the tool is very much essential. Following is the extract of the information of the literature review.

In paper [1] , an introductory look at information hiding techniques and historical details is discussed several methods for hiding data in audio, video is described with appropriate to environment of each medium as well as strength and weakness of each medium. Information about secret key, transmission protocol,computer file system ,hiding techniques are discussed.

In paper [2] the different types of Steganography methods its pros and cons are discussed in detail. It gives information about efficient method for sending safely to this destination, The use of Steganography application is to hide different types of data within cover file. This is done according to the embedding algorithm and a secret key that performs the actions of embedding process .

In paper [4], it explains the prime need of hiding data from eavesdroppers is accomplished by the use of steganography. It explains about the wide researches that have been carried out on video steganography due to high capacity of information been stored in video file. This paper presented using LSB insertion which is very efficient method to embed data into a cover medium. It has explained the LSB insertion method for video steganography and its application.

In paper [5], the focus on the data security approach with combined encryption and steganographic techniques for secret communication by hiding it inside a multimedia files is done. The file such as images, audio, video contains collection of bits that can be further translated into same. The files composed of insignificant bits or unused areas which can be used for overwriting of other data. This paper explains the proposed algorithm using video steganography for enhancing data security.

In paper [6], the explanation on combination of cryptography and steganography is used for data hiding in video clips. A random frame selection, pixel swapping and encryption of message has been done to enhance security of secret information which goes under the cover of video clips. Video steganography method has been developed to transfer secret data.

In this paper, the modern secure image steganography presents a challenging task of transferring embedded information to destination without being detected. Here, a simple approach for embedding message into image or the video from pixel of carrier image is replaced with message information so that it cannot be observed by human visual system.

IV. METHODOLOGY

A Video can be viewed as a sequence of still images. Data embedding in video seems very similar to images. However, there are many differences between data hiding in images and videos, where the first important difference is the size of the host media, since videos contain more sample number of pixels, a video has a higher capacity than a still image and more data can be embedded in the video.

In the process of hiding the secret data in the video which acts as a cover carrier, that secret data will be encrypted using AES Algorithm. The AES algorithm is most secure and robust cryptographic algorithm against attacks. AES has a symmetric block cipher and hence uses same key for encryption and decryption. After the encryption the data is divided into number of chunks, these chunks will be given to the LSB technique, by this technique the chunks will be placed in the marked frame.

The overall process is divided into two parts i.e. sender and receiver. When sender wants to send the secret data, he will register to the access and extract the video file along with the secret data. The secret data will be encrypted using AES Algorithm while sending a video i.e. stego video. The encryption key will be generated at the time of sending. The authorized receiver can only access the video file with the help of encrypted key.

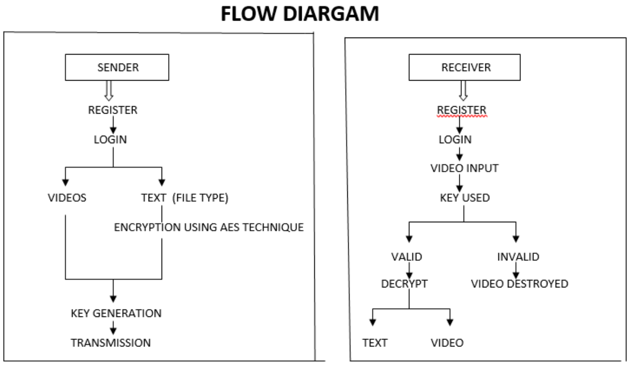
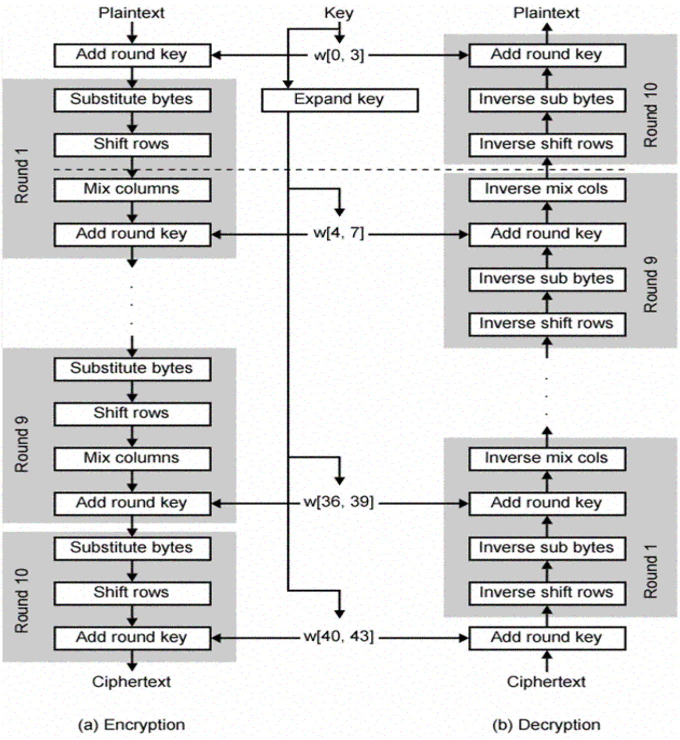


Fig1. Flow diagram of video steganography.

If the encryption key is invalid vide will be destroyed automatically

A. *AES Algorithm*

AES is based on a design principle known as a substitution-permutation network, and is fast in both software and hardware. AES operates on a 4×4 column-major order matrix of bytes, termed the state. We use 128 bit key for an AES cipher which specifies the number of repetitions should be 10 cycles' transformation rounds that convert the input, called the plaintext, into the final output, called the cipher text.



B. *LSB Technique*

Least Significant Bit (LSB) insertion is a common, simple approach to embedding information in a cover video. Video is converted into a number of frames, and then convert each frame in to an image. Here, the bits of the image are directly embedded into least significant bit plane of the cover-frame in a deterministic sequence.

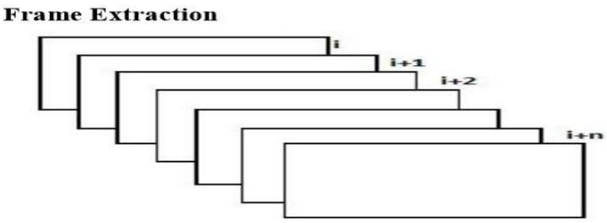


Fig 3. LSB Technique frame extraction

C. *System design*

Activity Diagrams:

Activity diagrams represent the business and operational work flow of a system. An Activity diagram is a dynamic diagram that shows the activity and the event that causes the object to be in the particular state.

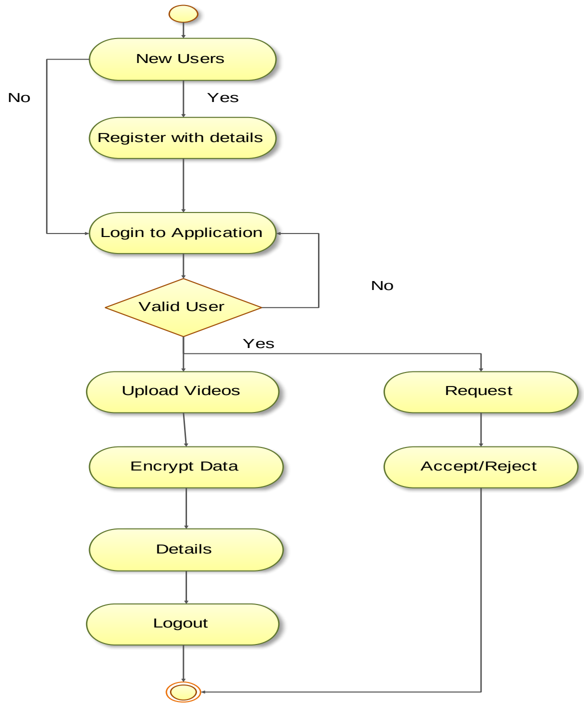


Fig. 4: Flow Chart

V. APPLICATIONS

- In the business world Steganography can be used to hide a secret chemical formula or plans for a new invention
- Steganography can also be used for corporate espionage by sending out trade secrets without anyone at the company being any the wiser
- The simplest and oldest are used in map making, where cartographers sometimes add a tiny fictional street to their maps, allowing them to prosecute copycats. A similar trick is to add fictional names to mailing lists as a check againstunauthorizedresellers.
- Most of the newer applications use steganography like a watermark, to protect a copyright on information. Photo collections, sold on CD, often have hidden messages in the photos which allow detection of unauthorized use.

VI IMPLEMENTATION

This chapter gives information about the implementation of the proposed system.

A. *SOFTWARE REQUIREMENTS*

MATLAB R 2012:

MATLAB (Matrix Laboratory) is multi-paradigm numerical Computing environment. MATLAB allows creation of user interface, interfacing with programs written in other languages, including C, C++, C#, Java, Fortran and python.

MS VISUAL STUDIO:

Visual Studio includes a code editor supporting Intel liSense (the code completion component) as well as co de refactoring. The integrated debugger works both as a source-level debugger and machine- level debugger.

D. RESULTS

Following are the snapshots of software implementation of proposed system which includes the steps involved in programming.

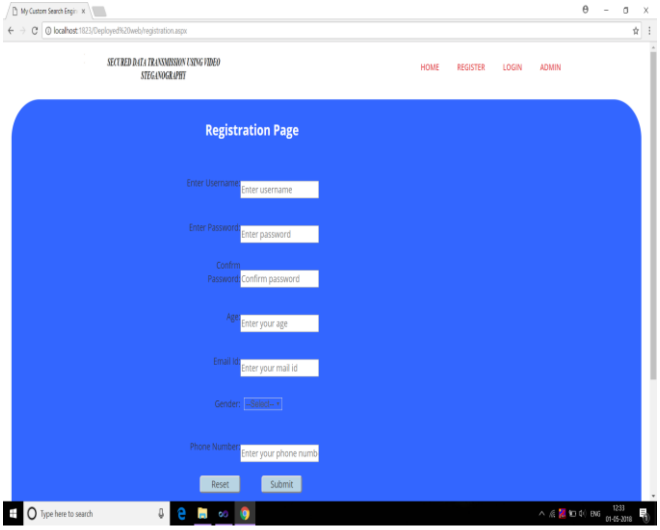


Fig1: The registration Webpage.

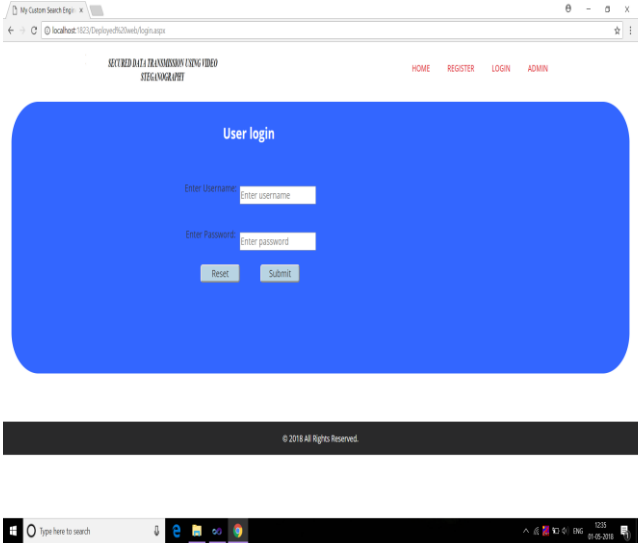
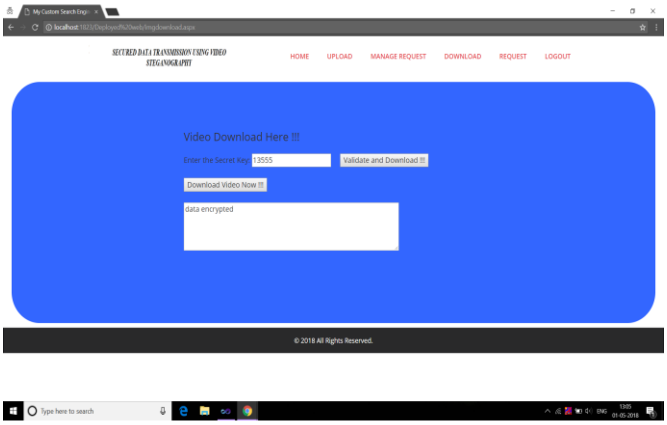


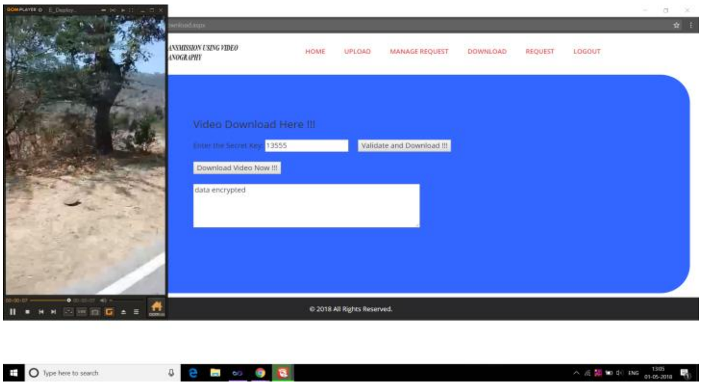
Fig 2: Webpage created for Login Procedure.


localhost:1823/Deployed%20web/imgdownload.aspx
SECURED DATA TRANSMISSION USING VIDEO STEGANOGRAPHY
HOME
UPLOAD
MANAGE REQUEST
DOWNLOAD
REQUEST
LOGOUT
Video Download Here !!!
Validate and Download !!!
Download Video Now !!!
© 2018 All Rights Reserved.
Type here to search

Enter the Secret Key: 13555

data encrypted

Fig 3: Webpage for uploading the video cover file.



Enter the Secret Key: 13555

data encrypted

Fig 4: Webpage showing the retrieved secret data by a valid receiver along with the video cover.

VII. CONCLUSION

Secured transmission of data from sender to receiver in real time is demonstrated. AES algorithm is developed to encrypt the data. LSB technique is used to hide the encrypted data into video frames. The proposed system results in more secured technique for data hiding. We can conclude that system is more effective for secret communication over the network channel.

REFERENCES

[1] Sabu M Thampi, " Information hiding techniques", computer Science Engineering (LBSCE),published on 2014.

[2] ChhayaVarade, Danish Shaikh, and Girish Gund, "Technique for data hiding using audio and video steganography", information technology at GHRIET, Pune vol 6, Issue 2, Feb 2016.

[3] Hemanth Guptha and Dr.SetuChaturdevi, "Video data hiding through LSB substitution Technique", Technocrats Institute of technology Bhopal. Vol 2, Issue 10, April 2013.

[4] Sonali Rana and RosepreetkaurBhogal, "A highly secure video steganography using LSB insertion technique", vol.10 , no 22, 2017

[5] Vipula Mahdhuka, Dr .Suresh Kumar "Enhancing data security using video steganography", SGT technology Gurguoan, vol.3, Issue 4, April 2013.

[6] Preet Inder Kaur, " Matlab Based Image Hiding using steganography technique"., GurerGranth Sahib World University vol.6 Issue 4, March 2016.

[7] Ronak Doshi, Prathik Jain, Lalit Guptha, " Steganography and its applications in security", electronics and telecommunication(IJMER) vol.2, Issue.6, Nov Dec 2012.

[8] Ms.Umasahu, Mr.SaurabhMitra, "A secure data hiding technique using video steganography", TCE(IJCSCN) ,Vol.5, Issue 3, 2016.

[9] Savkar tushar, Dhanak prasad, Jadhav gaurav, Salunke sachin," Application of data hiding in audio-video for authentication and data ", Nov 2014.

[10] Abhishek Mangudkar, Prachi Kshirsagar, Vidya Kawatikwar, Umesh Jadhav," Data Hiding Technique using Steganography and Dynamic Video Generation " vol-6,issue-3, june 2012.

[11] Kamreed Udaam Singh, "Data Hiding Technique using Steganography and Dynamic Video Generation " vol-6,issue-2, May 2014.

[12] K. Steffy Jenifer , G. Yogaraj , K. Rajalakshmi, "LSB Approach for Video Steganography to Embed Images ", vol-5, 2015.