ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

A Review on Data Security Using Video Steganography

Jayashri Joshi[1], Mithilesh Choudhary[2], Vikash Tiwari[3], Suraj Bhagasara[4]

Assistant Professor, Dept. of E&TC, PCCOE, Pune, Maharashtra, India [1]

UG Student, Dept. of E&TC, PCCOE, Pune, Maharashtra, India [2,3,4]

ABSTRACT: Information security has become the area of concern as a result of wide spread use of communication medium over the internet. This project focuses on the data security approach when combined with encryption and steganographic techniques for secret communication by hiding it inside the multimedia files. The high results are achieved by providing the security to data before transmitting it over the internet. The files such as images, audio, video contains collection of bits that can be further translated into images, audio and video. The files composed of insignificant bits or unused areas which can be used for overwriting of other data. This project explains an AES algorithm using video steganography for enhancing data security.

KEYWORDS: Steganography, Cryptography, Digital Watermarking, LSB, Encryption, Decryption, AES.

I.INTRODUCTION

In the current trends of the world, the technologies have advanced so much that most of the individuals prefer using the internet as the primary medium to transfer data from one end to another across the world. There are many possible ways to transmit data using the internet: via e-mails, chats, etc. The data transition is made very simple, fast and accurate using the internet. However, one of the main problems with sending data over the internet is the security threat it poses i.e. the personal or confidential data can be stolen or hacked in many ways. Therefore it becomes very important to take data security into consideration, as it is one of the most essential factors that need attention during the process of data transferring.

The objectives of the project are to provide a secure means of data communication using steganography techniques. The project will allow the user to transmit sensitive data within cover media and provide a less suspicious means of data communication as opposed to cryptography. The project is designed to transmit data through wired/wireless means or through the internet depending on the user convenience.

The Steganography, Cryptography and Digital Watermarking techniques can be used to obtain security and privacy of data. The steganography is the art of hiding data inside another data such as cover medium by applying different steganographic techniques. While cryptography results in making the data human unreadable form called as cipher thus cryptography is scrambling of messages. Whereas the steganography results in exploitation of human awareness so it remains unobserved and undetected or intact. It is possible to use all file medium, digital data, or files as a cover medium in steganography.

II.STEGANOGRAPHY TECHNIQUES

A. Image Steganography

An image can be said an array of numbers which represents light intensities at pixels which results in data.

Image is composed of 8 bits per pixel i.e.256 colors.Common approach designed for image steganography are LSB(Least Significant Bit) substitution which is the easy and most common approach of hiding data inside images.Masking is another technique of embedding messages in significant areas.The DCT based on image transformation involve the mathematical function for hiding data inside the images.[4]

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

B. Audio Steganography

Audio steganography works by 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.

C. Video Steganography

The separation of video into audio and images or frames results in the efficient method for data hiding.The use of video files as a carrier medium for steganography is more eligible as compared to other techniques. As a result of this this technique is discussed and proposed in this paper.[6]

III.BLOCK DIAGRAM

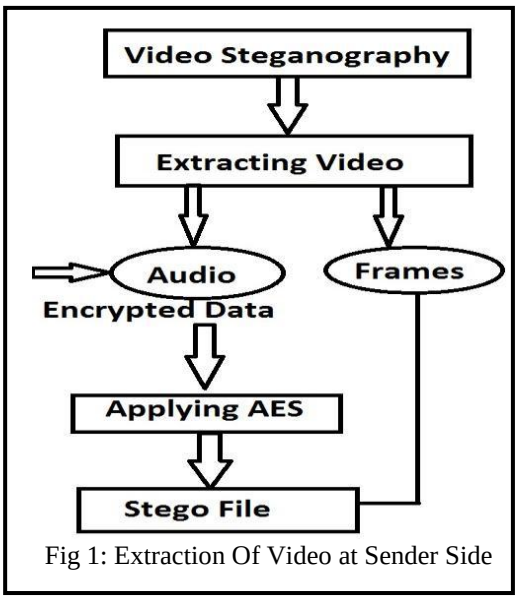

Fig 1: Extraction Of Video at Sender Side

1)Video input and data input:

Here we select the data and video behind which data is to be hidden. Data can be any type audio, video or text. But we will be dealing with text only.

2)Encryption And Extraction:

Here data will be converted into binary which will be plain text and converted into cipher text to hide data. Here steganography is used to encrypt so as to hide the data. The secret key is used for this purpose.

The video steganography composed of two main phases namely extraction of video files and embedding of secret message,as the secret message is already encrypted using AES and it can be easily embedded into carrier video.The extraction of video results in frames as video generally composed of still images and audio,the audio and image frames from the file video is extracted.From this extracted audio the stego file is generated as a secret data is hided in the audio not in the image frames.Audio contains unused bits or free bits of information in which secret data can be very easily hided. For making this file more robust against attack or identification stego file is again encrypted using the Advanced Encryption Standard. The stego file generated is then transmitted over the communication channel which remains intact as a result of this complex data hiding method.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

3)Transmission channel:
We are using wireless medium for transmission.

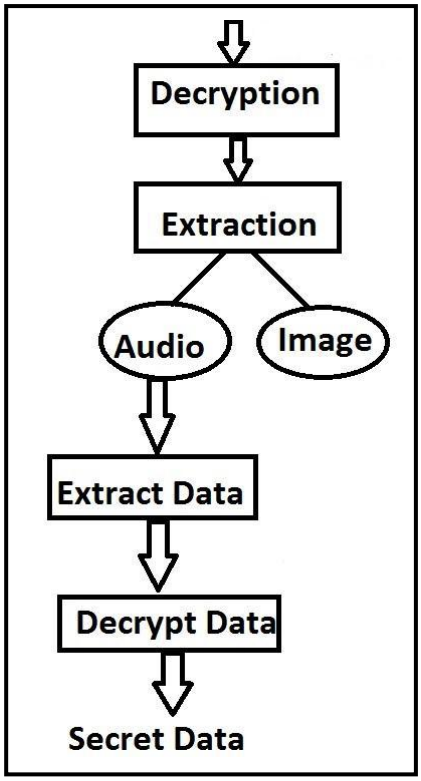

Fig 2: Extraction Of Stego File at Receiver Side (Decryption)

4)Decryption:
This block is used to separate the video and the data as we receive them. The same key used at the transmitter side is used for this purpose also i.e. symmetrical key is important here.The stego file can be extracted at receivers side by performing decryption of stego file and then by extracting the carrier video which is nothing but a collection of audio and image frames.The resultant data is the encrypted secret data which is again decrypted to obtain original data.Thus the proposed system provides the most secure approach using two layer of encryption the first is performed on the secret data itself and another on the audio file.

IV.THE PROPOSED METHOD

The proposed method for the data hiding is based on video steganography where we have used the AES algorithm to make the steganography more secure and robust.The video steganography is achieved by embedding the video files with the secret data that is to be transmitted with the intention of keeping the secret data unaltered or remains intact at receivers end.

AES (Advanced Encryption Standard):
The AES algorithm is most secure and robust cryptographic algorithm against attacks.Unlike the DES which is far slow and is already broken and also produce inefficient software code. Triple DES on the other hand is comparatively slower than DES as it has three more rounds
AES has symmetric block cipher and hence uses same key for encryption and decryption.The block size of AES varies from 128, 192, and 256 bits, the substitution and permutation are performed in AES.The number of rounds depends upon the key length i.e. 10 rounds for 128 bit key,12 for 192 bit key and 14 for 256 bit key. The next stage is to

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

perform actual steganography where this secret data is given to hide inside the video carrier the stego video is generated as a result of video steganography.

V. RESULT AND DISCUSSION

Using the AES algorithm, the project work was embedding of text into video as a case of steganography. The two primary criteria for successful steganography are that the stego signal resulting from embedding is perceptually indistinguishable from the host video signal, and the embedded message is recovered correctly at the receiver.
The proposed project is executed in Matlab using GUI as shown below.

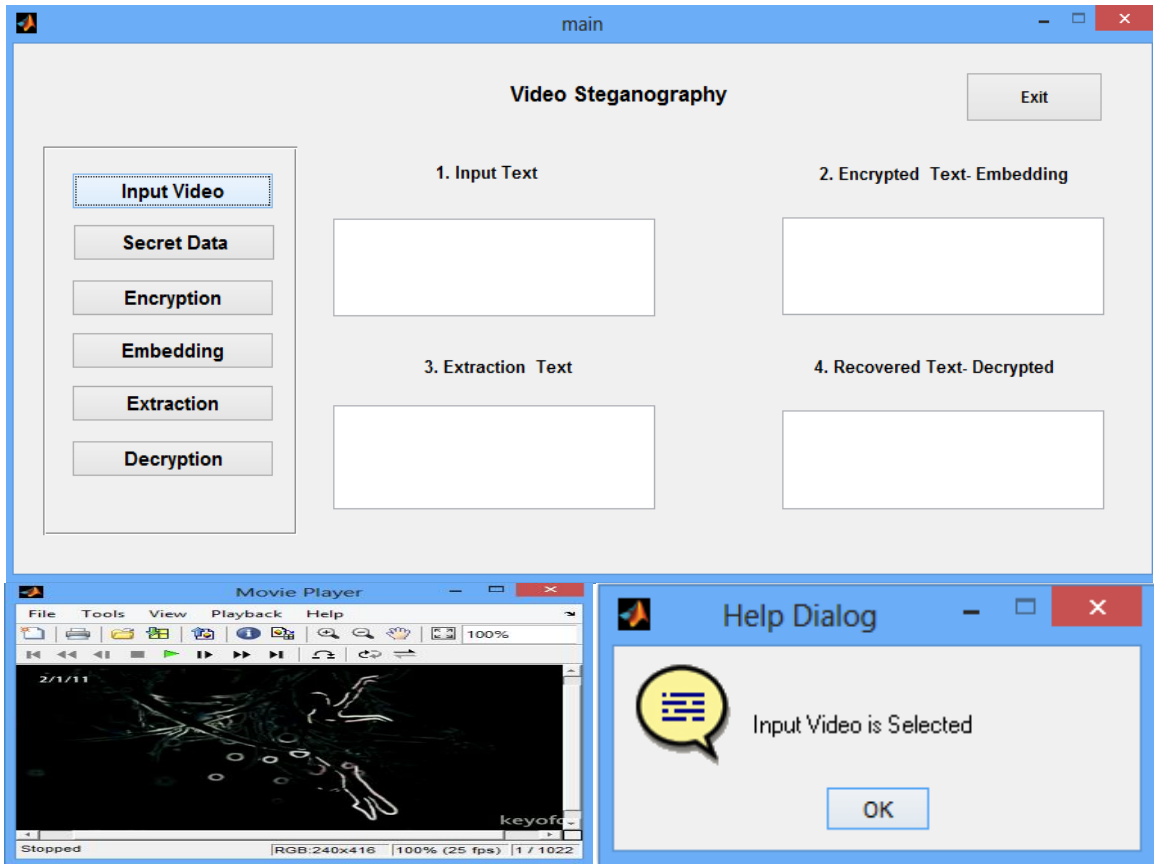

Fig. 3 Input video is selected and the media player

In Fig 3, Input video is selected and media player. Here the carrier vedio is selected on which secret text data is hided and transmitted over the channel.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

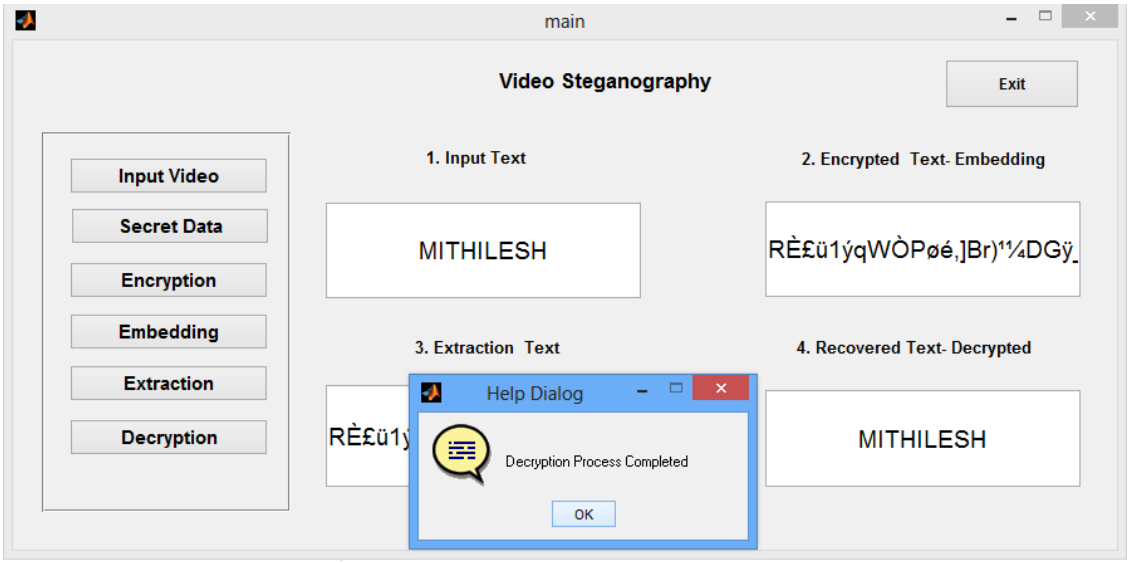

Fig. 4 Decryption Process Completed

In Fig 4, Decryption Process Completed. The recovered data at the receiveing end is the same original secret data as shown in fig.

VI.CONCLUSION

Today one of the main problems with sending data over the internet is the security threat it poses i.e. the personal or confidential data can be stolen or hacked in many ways. Therefore it becomes very important to take data security into consideration, as it is one of the most essential factors that need attention during the process of data transferring.
By taking this problem into consideration, we have designed a system "Data security using video steganography" which prevents the user from any kind of hacking data.In this paper we presented several ways of hiding the secret data inside the cover medium such as image,audio,video.The proposed system for data hiding uses AES for encryption which results in more secure technique for data hiding.We can conclude that the proposed system is more effective for secret communication over the network channel.

REFERENCES

[1] A.Swathi, Dr.S.S.K Jilani, "Video Steganography by LSB Substition Using Different Polynomial Equations," International Journal Of Computational Engineering Research, Vol.2, Issue.5, Sept.2012.
[2] Vipula Madhukar Wajgade, Dr.Suresh Kumar ,International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com ,ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 4, April 2013.
[3] Dawen Xu, Rangding Wang , Yun Q. Shi, "Data Hiding in Encrpted H.264/AVC Video Streams by Codeword Substition," IEEE Transaction ON Information Forensics And Security,Vol. 9, no. 4, April 2014.
[4] www.sciencedirect.org
[5] www.ijcaonline.org/journal/number15/pxc387502.pdf
[6] http://www.jjtc.com/pub/r2026.pdf_
[7] V.Lokeswara Reddy, Implementation of LSB Steganography and its Evaluation for Various File Formats
[8] Mrs.Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav, Steganography Using Least Signicant Bit Algorithm
[9] Anil.K.Jain , Fundamental of Digital image processing (Book: Eastern economy edition)
[10] Milan Sonka,Vadav Hlavac,Roger Boyle ,Image processing & analysis & machine vision (Book: Second edition).
.