A Secure Data Transmission By Integrating Cryptography And Video Steganography

Shafna P K
Computer Science Department
KMEA Engineering College
Ernakulam, India
shabanapk9999@gmail.com

Abstract— **Advances in digital content transmission have increased in past few years. Security and privacy issues of the transmitted data have become an important concern in multimedia technology. In this paper proposes a video steganography method for transmitting data securely. Steganography means covered writing it includes process of concealing information within other file and also conceals the fact that a secret message is being sent .Video Steganography is to hide the existence of the message from unauthorized party using Video as cover file and hiding data in video. In this work a very simple and real time algorithm is used for the encryption of the images which are the basic building blocks of any video file. In the proposed research paper the video is distributed into the photo frames using a matlab code and all the frames are sequentially stored. Each such frame contains a combination of red, blue and green layers. If we consider a pixel as an 8 bit value than each pixel has the value in the range of 0 to 255. In this work, for each frame four pixels situated at the top left and right and the bottom left and right corner are modified so as to insert text in each image. Text data is encrypted using AES algorithm. After the completion of the pixel value changing all the images is placed in a sequential manner and then all the frames are cascaded for generation of the original video file with encryption. This new video is almost similar to the original video file with no changes visible to the naked eye.**

Keywords*: **Video steganography, AES encryption, PSNR, MSE***

I. INTRODUCTION

Now a day's the use of internet increases. As the use of internet increases providing security to the information is also important thing. Providing security means protecting information systems from unauthorized access, use, disruption, modification and recording or destruction. There are two methods to provide security. They are cryptography and steganography. Cryptography is the way of hiding information and it is used when communicating over untrusted medium. Steganography is a kind of science and art of hiding a secret message inside the other digital files.

Depending on the type of the cover object there are many suitable steganography techniques which are followed in order to obtain security. It can be shown in Figure 1.1.

1.1. Image Steganography: Taking the cover object as image in steganography is known as image steganography. Pixel intensities are used to hide the information in an image.

1.2. Network Steganography: When taking cover object as network protocol, such as TCP, ICMP, IP, UDP etc.., where protocol is used as carrier known as network protocol steganography.

1.3. Video Steganography: Video Steganography is a technique to hide any kind of files or information into digital video format. Video (combination of pictures) is used as carrier for hidden information. Generally discrete cosine transform (DCT) alter values (e.g., 8.667 to 9) which is used to hide the information in each of the images in the video, which human eye cannot noticeable. Video steganography uses such as MPEG, H.264, AVI, Mp4 or other video formats.

1.4. Audio Steganography: When taking audio as a carrier for information hiding it is called audio steganography. Audio steganography uses digital audio formats such as WAVE, AVI MPEG, MIDI or etc for steganography.

1.5. Text Steganography: General technique in text steganography, such as white spaces, capital letters, number of tabs just like Morse code and etc.., is used to achieve hiding of information.

In this work video steganography is adopted. For normal human being the ability to perceive the motions of other animated frames or video has been extensively studied and it is shown that for the movements created in the running video only the small amount of the pixels are modified and rest all the pixels remain static if we compare the pixels of any consecutive frames in a video. So by the changes made in the smaller number of pixels in a sequence of images all the movements are described perfectly in a video file. This is very simple and easy method for visualizing any process under study. Research shows that among the consecutive images having million numbers of pixels only few hundred pixels are modified for showcasing the movements happening in the particular video

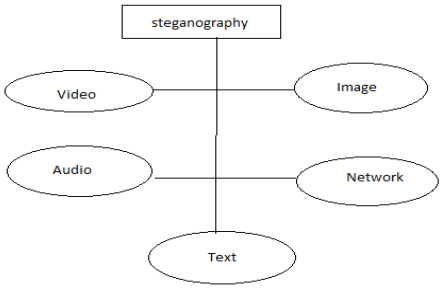

Figure 1.1: Digital Medium to Achieve Steganography

The video steganography uses some frames of Video files to embed the secret message. This steganography hides information in such a way that it appears like that no information is hidden. Whenever any person views that video in which data is hidden but they have no idea that any information will not be decoded by unwanted person. Steganography provide security by obscurity. Video Steganography technique will not only hide data but also hide the presence of data. The data is hidden even from receiver but receiver can decode data as they know the password that is used to embed data. The video file can hide large quantity of information because it carries large number of frames and its storage capacity is also more. Video files are larger than audio and image files, and hide more information.

The video steganography involve two steps. The first step deals with embedding secret message in the video files. The second step is the extraction of secret message from video files. This video steganography have more hiding capacity (the amount of information that can be embedded) which is always an important factor when developing a steganography algorithm. The second main advantage of hiding data into video file is the added security against the attack of the third party or unintended receiver due to relative complexity of the structure of video as compared to image & audio. In video steganography technique pixel mapping method is used to hide data in video cover file. Any video is basically a combination of different frames and all the frames constituting a video has a fixed frame rate. Generally the frame rate is 25 so we can say that 25 frames are captured within one second time. For the efficient and successful implementation of this particular algorithm there is a requirement that the video needs to be segmented.

For a particular case if we suppose that the video is of 5 minutes duration than this video majorly contains 7500 frames in it. These frames are the building block for the video as well as for video encryption process. In this work also the video steganography technique is used. Also the steganography technique is faster and efficient in terms of time required for marking the particular set of images. Steganography is going to gain its importance due to the exponential growth and secret communication of potential computer users over the internet. It can also define as the study of invisible communication that usually deals with the ways existence of the hiding of the communicated message. In order to achieve high security encrypted information content is embedded into the video. In this work AES encryption is used to encrypt text data.

II. RELATED WORKS

There are various steganography methods have been proposed in literature. Video file hides a large amount of secret data hence it is more useful.

B.SUNEETHA et. al has proposed in his work Steganography and Cryptography based system for hiding data in video by encrypting it with ASCII code. Thus it provides an additional layer of security. Steganography is intended to provide secrecy of text data whereas Cryptography provides privacy [2].

In Secured data transmission Steganography technique works on compression technique which is evaluated such that the data is been embedded in the vertical and horizontal component. There are three types of images (or frames) used in video compression which is used to evaluate frames, they are : I-frames, B-frames and P-frames defined on amount of data compression. They have different characteristics: I (Intra-coded) frames don't require other video frames to decode but are least compressible. P- (Predicted) frames use data from previous frames to decompress and are more compressible than I-frames. To get the higher amount of data compression B- (Bi-predictive) frames use both previous and forward frames for data reference. In which first read the input video file and fragmented into frames, then required information is read from the cover file. Using LSB method text data is embedded into the video frames. The given Secured Data Transmission Technique provides high capacity and imperceptible, for human vision of the hidden secret information. By embedding the data in the moving pictures the quality of the video is increased. The compressed video is used for the data transmission as it can hold large amount of text data.

Kousik Dasgupta, J.K. Mandal and Paramartha Dutta has proposed a secured hash based LSB technique for video steganography which uses cover video files in spatial domain to hide the presence of sensitive data regardless of

its format. Performance analysis of the hash based LSB technique after comparison with LSB technique is better[3].

The Hash based Least Significant Bit (HLSB) technique for Video Steganography has been used, here the secret data is hided in the LSB of the cover frames. In HLSB method eight bits of text data to be transmitted is divided in 3, 3, 2 format and inserted into the RGB pixel values of the video frames. To select the position of insertion in LSB bits a hash function is used.

A. Swathi , Dr. S.A.K Jilani Video File(Cover, Carrier) Data/Message(Text, Audio,Image,Video) Steganography algorithm Stego File(Video with secret data) has proposed in his paper the LSB substitution using polynomial equation is developed to hide the information in specific frames of the video and in specific location of the frame by LSB substitution using polynomial equation. Here the text data will be embedded based on the key and the key is in the form of polynomial equations with different coefficients. By this method the capacity of embedding bits into the cover image can be increased [4].

Mritha Ramalingam has proposed a more secured LSB method way in which video file is used as a host media to hide secret message without affecting the file structure and content of the video file. Because degradation in the video quality leads to visible change in the video which may lead to the failure of the objectives of Steganography[5]

Ashawq T. Hashim et al has proposed a Hybrid Encryption and Steganography technique where there are two methods of hiding used, the first method is the Least Significant Bit (LSB) and the second is the Haar Wavelet Transform (HWT). This work is based on a combination of steganography and cryptography techniques to increase the level of security and to make the system more complex to be defeated by attackers.

R. Shanthakumari and Dr.S. Malliga in their proposed work has stated a LSB Matching Revisited algorithm (LSBMR) selects the embedding regions according to the size of secret message and the difference between two consecutive pixels in the cover image. LSBMR scheme addresses two problems Lack of Security and Low Embedding rate[7].

LSB Matching Revisited(LSBMR) algorithm for Video Steganography selects the embedding regions according to the size of secret message and the difference between two consecutive pixels in the cover image. [7]

III. PROPOSED SYSTEM

Earlier various kinds of steganography techniques are introduced for the video. In this work proposes a new video steganography method for transmitting data securely. In this technique steganographic tool is developed in MATLAB software which perform Encoding and Decoding. Figure 3.1 narrate the flowchart showing the sequence of steps to be executed for generating the encrypted video file for secured text data transmission. The algorithm is briefly described in terms of flowchart for the better understanding of the whole process. The complete algorithm is coded in a Matlab code showing the detailed process involved in the video encryption and the text insertion in the video file for secured transmission.

As shown in the algorithm in figure 3.1 the complete video is segmented into number of frames using a small matlab code module and after the processing of the video by the Matlab code module the video gets divided into different frames of same size. Then the text string which is to be inserted among the images is partitioned into the group of two bits each. As we need to modify only four pixels per image so we divide the text data into the group of two bits. Each character in the text data can be represented by a specific ASCI value so each of the character occupies 1 byte or 8 bits in an image.

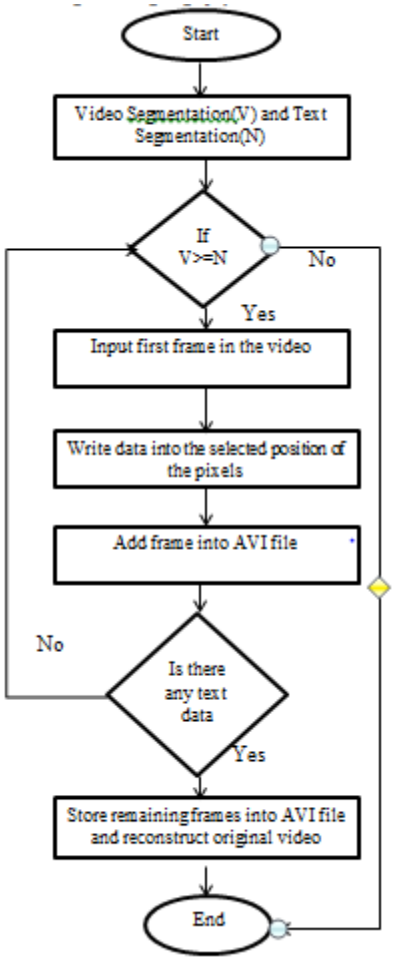

Figure 3.1 : Algorithm for secure text transmission using video steganography

In this particular algorithm each of the image has to be modified by two pixel value and that also only the last two bits so each of the character in the text data to be inserted is represented by its ASCI value in line. After this each of the characters represented into the group of 8bits is subdivided into the groups of 2 bits only. So now we have four groups for each of the character in the text data to be inserted into the images. In this algorithm to represent one particular character we require four pixels to store one particular character, So we store one character in one frame using its four corner pixels.

As per the grassman law importance of three basic colors which are red, blue and green are different. As per grassman law the importance of the green layer is the most because it contains 59% weightage to generate any color in a particular pixel Due to this in this algorithm only the value of blue layer is changed for processing the image so as to retain the original shade in the frame. The green and red layer in each of the images is unchanged. Only the blue layer pixels are modified in each of the image frames.

Now we have frames as well as very well distributed text data available so the next step to be followed is to encode or map the text data into the pixels of individual frames till the end of the text data. In the proposed work, to store one character into one frame so there is a requirement of n number of frames for storing n number of characters in the text data. For a particular image frame by modifying only two pixels at top and bottom of the image file does not make any significant changes in the visual effects of the frame so they are not visible to the human eye.

Next step to be followed as per the flowchart is to select the first frame from the sequence of the frames and identify the blue layer of the first pixel and overwrite the last two bits with the first two bits of the character in the text data. Similarly also over write the last two bits of the blue layer pixel by the corresponding next two bits of the character. Same process is to be done for the pixels present in the bottom section of the frame. In this way we can impose one character into one frame and the same process is to be followed for all the characters present in the text data with consecutive different frames.

In this work mainly there are two modules. First module involves encryption of text message using AES algorithm. Second module involves embedding text data into selected position of video frames.

3.1. CRYPTOGRAPHY

Cryptography is an art of protecting the information by transforming it into an unreadable and untraceable format known as cipher text. Only the person who have the secret key can decipher or we can say decrypt the message into the original form. Cryptography provides a number of security goals to ensure the privacy of data, non-alteration of data and so on

In this work, AES encryption algorithm used for encrypting text data. AES is an algorithm for performing encryption and decryption. AES is a symmetric block cipher. Symmetric block cypher means it uses the same key for encryption and decryption. The algorithm Rijndael allows for a variety of key and block sizes. The key and block can be chosen independently from 128, 160, 192, 224, 256 bits and no need of the same. AES standard states that the

algorithm can only accept a block size of 128 bits and a choice of three keys - 128, 192, 256 bits. It is not a feistel structure. The entire data block is processed in parallel during each round using substitutions and permutations. Each round is a uniform and parallel composition of 4 steps,

- SubBytes: Byte-by-byte substitution using a non-linear S-box
- ShiftRows: Is a permutation, circular left-shift on the last three rows in the state
- MixColumns: Substitution that uses Galois Fields, i.e each column of State is replaced by another column obtained by multiplying that column with a matrix in a particular field.
- AddRound key : Performs a bit-by-bit XOR with an expanded key

AES was designed to achieve the following characteristics:

- Resistance against all known attacks.
- To attain speed and code compactness on heterogeneous platforms.
- To gain design Simplicity.

The decryption of AES algorithm is not same with the encryption algorithm, but uses the same key. There is also a way of implementing the decryption with an algorithm that is equivalent to the encryption algorithm (each operation replaced with its inverse), however, in this case, the key schedule must be changed.

3.2. STEGANOGRAPHY

Stenography is the art of hiding information by embedding message within each other. It works by replacing the very useless bits by the information content to be transmitted. It works by hiding information inside a cover. The cover may be an image file or a video file as per the user requirement. Even though the cover looks very simple and unchanged but it has information contained in it.

First of all the video file is converted into a series of frames of equal size. The information content which is to be transmitted by mapping onto the video file is distributed into small portion depending on the size of the frames in the video file. From each frame a smaller region is modified depending upon the private key. Due to this the selected groups looks very random to the third party who does not have the private key with them. The selected pixels are then converted into the frequency domain with the help of the discrete cosine transform. Usually a predefined portion of the pixels like we say the last two or three bits are then replaced by the spilled message portion and then the pixel portion is again converted back into the spatial domain. The conversion from the frequency domain to the spatial domain is done with the help of inverse DCT. Then that group of pixels is placed back into the particular frame. This process is followed until the end of the whole information content. The frames are then arranged into a sequential manner and the video is constructed from it. Now this video contains the information which gets transmitted along with the transmission of the video file.

The Steganography encoder has to keep some control message into the video file by which the receiver can understand the data format, way of hiding the information content, type of encryption done etc. This is known as the rule list for a particular steganography process. This rule list is generated and mostly it is placed in the first frame of the video file. This rule list acts as a reference for a particular desired receiver. Without rule list the receiver may not be able to understand and retrieve the original information content hidden within the received video file. So the rule list plays a vital role at the receiver side.

The main blocks in a Steganography Decryptor is as shown in figure 3.5. From the figure 3.5 it is very clear that if the private key is not known than it is impossible to extract the original information content in the received video file. There are certain methods like some steg-analysis tools by which the information can be detected without the use of the private key also.

IV. RESULT ANALYSIS & DISCUSSIONS

The algorithms are implemented using MATLAB version R2015a. Matlab provides easier application development and a well defined user interface

Steganography technique is characterized mainly by imperceptibility and capacity. Imperceptibility means the embedded data must be perceptually invisible to the observer. In order to evaluate the performance of the stego video, there are some quality measures such as PSNR and MSE

The **MSE (mean square error)** is defined as average squared difference between a reference image and a distorted image. It is calculated by the formula given below

$$MSE = 1/XY[\sum_{i=1}^{X}\sum_{j=1}^{Y}(c(i,j) - e(i,j))\text{^}2$$

X and Y are height and width respectively of the image. The c (i, j) is the pixel value of the cover image and e (i, j) is the pixel value of the embed image

The PSNR (peak signal to noise ratio) is used to determine the degradation in the embedded image with respect to the host image. It is calculated by the formula as

PSNR = 10 log10 (L*L/MSE)

L is the peak signal value of the cover image which is equal to 255 for 8 bit images.

Steganography technique is characterized mainly by imperceptibility and capacity. Imperceptibility means the embedded data must be perceptually invisible to the observer. The performance of the proposed technique is evaluated using two different video streams (shakyc_car.avi,wildlife)and one secret text(text_to_hide.txt).The perceptual imperceptibility of the embedded data is indicated by comparing the original video with its stego_video.When we hide secret text in video there will be no loss in quality of video and even none can guess the presence of data within a video.

In this section, we evaluate the performance of scheme through numerical simulations. It can be simulated using NS2 [7], network simulator. The scenarios had a deployment area of 200 x 200 meters. Wireless networks employ 802.11 access technology. The simulation period can be 30 seconds and simulation model has a queue length of 50. The source transmits their data to the sink node and then suddenly a large number of nodes involves in data transfer. By using the proposed scheme we can render a drastic change in energy, throughput and efficiency with communication overhead.

Video file	No:of characters to hide	PSNR	MSE
Wildlife.mp4	48	98.5661	.0000012
Shaky_car.avi	48	88.1843	.0001245
Road.mp4	50	77.0348	.0124
Stream.mp4	50	79.0453	.000084

From above table we observed that by using Secure text transmission using video steganography technique for video steganography using MATLAB software as steganographic tool we get more PSNR and as video has large hiding capacity so more hiding capacity gives more PSNR and small MSE. It gives different values of PSNR which deals with quality of video. For different resolution this quantity shows variation.

V. CONCLUSION

In this paper a robust and secure video steganography method is proposed. The proposed method is efficient and good for hiding data in video. One of the important features of the proposed work is it helps to transmit data securely by embedding it in a video file and without disclosing to the unintended receiver and without any alternation in secret message. The information underlying the video is not visible to the naked eye. An efficient AES encryption algorithm is used for the encryption of the text data. Only the person having the key and the rule list can identify and decode the original information from video into its original form. With the combination of the cryptography and steganography information security can be increased.

REFERENCES

[1] Prabhishek Singh, R S Chadha "A Survey of Digital Watermarking Techniques, Applications and Attacks" , IJEIT Volume 2, Issue 9, March 2013

[2] B.SUNEETHA, CH.HIMA BINDU & S.SARATH CHANDRA ―SECURED DATA TRANSMISSION BASED VIDEO STEGANOGRAPHY‖International Journal of Mechanical and Production Engineering (IJMPE) ISSN No.: 2315-4489, Vol-2, Iss-1, 2013

[3] Kousik Dasgupta, J.K. Mandal and Paramartha Dutta,‖ Hash based Least Significant Bit Technique‖, International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, No 2, April 2012

[4] A. Swathi 1, Dr. S.A.K Jilani,, ―Video Steganography by LSB Substitution Using Different Polynomial national Journal Of Computational Engineering Research (ijceronline.com) Vol. 2 Issue. 5

[5] Mritha Ramalingam: Stego Machine – Video Steganography using Modified LSB Algorithm World Academy of Science, Engineering and Technology Vol:50 2011-02-26

[6] Ashawq T. Hashim*, Dr.Yossra H. Ali** & Susan S. Ghazoul*‖ Developed Method of Information Hiding in Video AVI File Based on Hybrid Encryption and Steganography‖ Engg.and tech journal, vol 29,No.2,2011.

[7] R Shanthakumaril and Dr S Malliga, - Video Steganography Using LSB Matching Revisited Algorithm,IOSR Journal of Computer Engineering e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 6, Ver. IV(Nov – Dec. 2014), PP 01- 06