International Research Journal of Engineering and Management Studies (IRJEMS)
Volume: 03 Issue: 04 | April -2019 ISSN: 1847-9790 || p-ISSN: 2395-0126

Novel Approach to Secure Video Steganography

Surabhi Adak, Ashwini Sarode, Santosh Yadav, Ashish pawar, Mrs.Jyoti Kundale, Mr.Sachin Bhopi

Ramrao Adik Institute of Technology Nerul ,India surabhiadak8@gmail.com
Ramrao Adik Institute of Technology Nerul ,India ashwini9sarode@gmail.com
Ramrao Adik Institute of Technology Nerul ,India santoshyadav3210@gmail.com

Ramrao Adik Institute of Technology Nerul ,India pawar.ashish.ap7@gmail.com
Ramrao Adik Institute of Technology Nerul ,India jyoti.jadhav@rait.ac.in
Ramrao Adik Institute of Technology Nerul ,India sachin.bhopi@rait.ac.in

---

Abstract - *The rapid development of data communication in modern era demands secure exchange of information. Steganography is the technique of data hiding. Thus, a video steganography means hiding of data inside a video file. Existing systems work on the LSB technique and has a defined format in which data is stored and can be easily guessed by the intruder. The proposed method is based on Pixel Value Extraction of RGB model which uses Bit insertion technique to insert the text within the Video file. Usually, the hackers focus on LSB bits for secret data extraction but the proposed technique utilizes the MSB bits that make it more secure from unauthorized access. This system focuses on the data security approach when combined with encryption and steganographic techniques for secret communication by hiding it inside the video.*

Key Words: Steganography, Encryption, LSB technique, RGB model, Pixel value Extraction

1.INTRODUCTION

As demand for the secret transmission of data over the network has been increased there are many data hiding techniques which have been used widely for transmission of data. They are classified as Watermarking, Cryptography and Steganography. Cryptography means to make data unreadable to third person, Digital watermarking is the method of embedding dossier into digital multimedia content whereas the goal of steganography is to hide the existence of data [2]. Steganography means covered writing. Steganography is an art of embedding secret data that is to be hidden in a medium like image and video file in a way that no one can see or even realize that there is a secret message in that particular file [6].

Fig.1 describes the basic Steganography process which includes message to be sent along with the medium and encoding is applied on them and to get original message back at the receiver side decoding is followed.

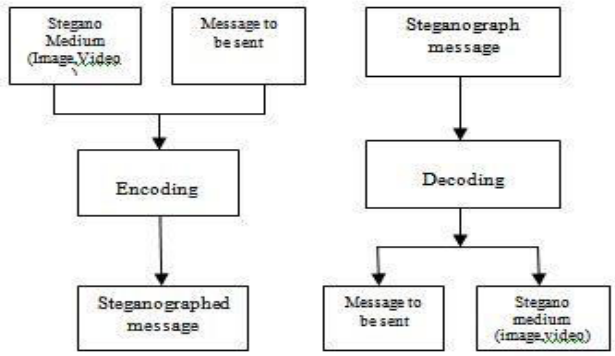

Figure 1. Steganograhy process

Many algorithms have been developed for steganography. These are mainly classified into Spatial domain and Frequency domain algorithms. LSB(Least Significant Bit) technique is the most common technique in spatial domain which can hide more amount of data. In LSB few last bits are replaced by some dossier which does not make any visible changes to the image or video. In frequency domain instead of hiding message in pixels, message is hidden in frequency coefficients of image.

By combining Steganography and Cryptography we can make it difficult for the third person to identify the secret message.Even if third person suspects that there is message hidden in video he will not be able to read that message as cryptography algorithm is used to convert the plain text into cipher text. Double work has to be performed to get the original message back at the receiver side, First is to extract message from video and sceond is to apply decryption to get original message[4].

A lot of research work has been carried out on video steganography which includes LSB technique to hide

secret message. This paper proposes video steganography which includes hiding of secret message in video and transmission of video over the network. The secret message is first converted into cipher text by using cryptographic algorithm known as AES(Advanced Encryption Standard) which is highly secure. Then cipher text is converted in binary format for each part of the frame a pixel is selected and two bits of selected pixel is replaced by two bits of the character to be hidden in the frame and this process continues diagonally from MSB(Most Significant Bit) to LSB(Least Significant Bit).

2 LITERATURE SURVEY

By adding one more layer to security it provides a accurate procedure to hide dossier. It is not easy to detect data as it is randomly stored in frames based on Divide and conquer strategy using midpoint logic. This paper [1], also presents usage of many encryption algorithms like XOR, AES, DES, and Hashing for security purpose.

In this paper [2], Symmetric (Blowfish, AES and DES) and Asymmetric (RSA) algorithms are evaluated by examining different types of files such as binary files and image files. Results generated from this analysis showcased AES as a better encryption algorithm due to its complexity to unreveal the working in the background. AES has both the throughput and decryption time ahead of other algorithms.

This paper [3] states that Steganography is performed by changing LSB of the original file bit stream into a message file. Conversion of message is done into the bye code and before embedding it into a carrier file it is encrypted. With C# wrapper files the functions of avifill32.dll are used. Even though a successful evaluation of work is done, still the issue of uncompressed carrier file remains.

In proposed scheme [4], a secret video is to be hidden in other cover video stream. Frames of video is broken into components and the conversion is done into 8 bit binary value, and encryption is done using XOR with secret key and the frames which are encrypted will be hidden in the LSB of each frames using sequential encoding of cover video. To have more security each bit of secret frames are stored in cover frames using this pattern: BGRRGBBGR.

In this paper [5], LSB approach is used to hide the data into the video file. That means the bits invisible to the eye are used. Signal to noise ratio is determined for the clear understanding of how data is secured is LSB. AES i.e. Advanced Encryption Technique is used for encryption purpose.

Work presented in this paper [6], provides a feasible solution for Video Steganography. The method proposed here considers video as set of frames or images and any changes in the output image by hidden data is not visually recognizable. And this is possible as it uses indexing method to hide the data. It also makes use of simple mathematical calculations which bring down the computational time very less making it a very simple and effective method for video Steganography.

3 PROPOSED METHODOLOGY

The method we propose here encrypts the confidential message into cipher text which is unreadable to third person using AES encryption algorithm then that secret message which is already encrypted is then stored in the frames of video file using steganography and then the video is transmitted to the receiver end, and same process is followed by receiver to read the message. A video file is usually composed of image frames. This method uses some frames to hide secret message. Usually in previous methods the message was hidden in least significant bits [1] but proposed method is based on Pixel Value Extraction of RGB model which uses Bit insertion technique to insert the text within the Video file. Here the secret data is inserted into video frames after applying some checks onto it, related to its imperceptibility and capacity.

A number of Steganography methods have been proposed and implemented in literature, most of which is based on Spatial Domain. A lot of algorithm has been used for inserting confidential bits in an image file. Here the image file is replaced with the same number of bits of the secret message. In a robust Video Steganography technique with AES (Advance Encryption Standard) encryption is used. It is implemented as 1-bit, 2-bit and 3-bit insertion and also improved the security level of hidden Information.

This procedure is quite different than traditional LSB methods. In this technique user has to select the video where he has to apply video steganography. Once the video is uploaded the video is divided into frames and each frame is then divided in smaller parts (images). The message which is to be hidden is encrypted and converted to binary format. For each part of the frame a pixel is selected and two bits of selected pixel is replaced by two bits of the character to be hidden in the frame. For second pixel two bits from 3 and 4 position is selected and replaced by third and fourth bit of character. This continues in diagonal form. This repeats till all the characters of the message is hidden in the frames of the video. This is later on merged into video.

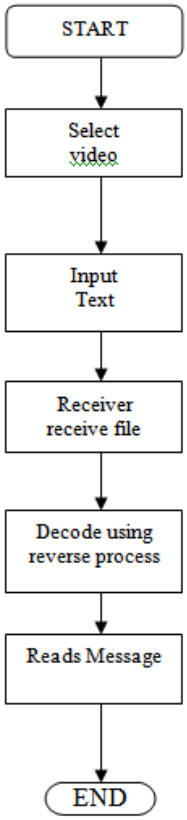

Figure 2. Flowchart

Fig.2 describes the basic flow diagram of steganography system which states that firstly user have to select the video file and then put the encrypted secret message which is to be hidden in video frames, once this is done the video file with secret message is transmitted to receiver using Steganography. Receiver decodes this message from video file using De-steganography i.e. reverse process is followed by receiver and then the message is decrypted into its original form.

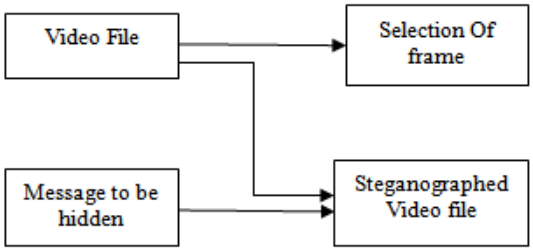

Figure 3. Block diagram

Fig.3 describes the basic block diagram which shows that the frames need to be selected from video file and then the secret message is hidden in those frames using Steganography and edited video file is sent to the receiver.

4. COMPARARTIVE STUDY

Table -1: DATA HIDING TECHNIQUES

	Description	Encryption used	Is Reliable/Effective?	Embedding technique
1	Indexing done within frames	No	Less Effective	LSB
2	Image hiding using hybrid approach	AES	Reliable as image cannot be guessed with this technique	LSB
3	Divide and conquer	AES	Very Effective	Midpoint logic
4	Encryption Analysis	AES	Most Effective	-
5	Hide a video in visual	AES & cryptography methods	Less reliable	LSB
6	Sequential coding to hide video in cover video	Encryption using XOR	Effective	LSB

Analysis-

Above discussed methods in Table1.shows the current evolution in the area of steganography. Here we have seen different techniques which uses AES and other cryptography methods for encryption and LSB and midpoint logic techniques for embedding data using steganography. The table also shows which technique is more reliable and effective.

3. CONCLUSIONS

In this system we have presented several ways of hiding the secret data inside the cover medium such as video. The proposed system for data hiding uses AES for encryption,

which results in more secure technique for data hiding. After studying different techniques of video steganography, we analyze that proposed technique is more secure as this method uses MSB as well as LSB bits diagonally to store the data. Usually hackers focus on LSB bits for secret data extraction. But this technique utilizes the MSB bits that is more secure from unauthorized access

REFERENCES

[1]PRANITA SANGIT and SWAPNIL SHINDE 'STEGANOGRAPHY IN VIDEOS USING UNIQUE FRAME SELECTION TECHNIQUE' International Journal of Advanced Computational Engineering and Networking, ISSN: 2320-2106.[2016] Volume-3, Issue-9, Sept.-2015

[2] Madhumita Panda 'Performance Analysis of Encryption Algorithms for Security' International conference on Signal Processing, Communication, Power and Embedded System (SCOPES)- [2016]

[3] A. MUNASINGHE, ANUJA DHARMARATNE,, KASUN DE ZOYSA 'Video Steganography ', University of Colombo School of Computing Colombo, Sri Lanka, INTERNATIONAL CONFERENCE ON ADVANCES IN ICT FOR EMERGING REGIONS (ICTER): 056 – 059 [2013].

[4] Pooja Yadav , Nishchol Mishra , Sanjeev Sharma ,A Secure Video Steganography with Encryption Based on LSB Technique IEEE International Conference on Computational Intelligence and Computing Research [2013] p.1-5, .

[5] Hemant Gupta , Dr. Setu Chaturvedi \cite{hemant gupta}, Technocrats Institute of Technology Bhopal(M.P.) .'Video Steganography through LSB Based Hybrid Approach' International Journal of Engineering Research and Development Volume 6, Issue 12 (May 2013), PP. 32-42 [2013].

[6] R. Balaji and G. Naveen \cite{balaji} 'Secure Data Transmission Using Video Steganography' 2011 IEEE INTERNATIONAL CONFERENCE ON ELECTRO/INFORMATION TECHNOLOGY, 2011. p.1-5.