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. 3, Issue 7, July 2014

DOI: 10.15662/ijareeie.2014.0307014

Concealed Message Transfer Using Lifting Scheme Based On Video Steganography

P. Sherubha[1], P. Abinaya[2]

Assistant Professor, Department of CSE, Dhanalakshmi Srinivasan Institute of Research and Technology, Perambalur, Tamil Nadu, India[1].

Assistant Professor, Department of ECE, Dhanalakshmi Srinivasan College of Engineering, Perambalur-621212, Tamil Nadu, India[2].

ABSTRACT: Nowadays security threats become increased, confidential information, such as medical records, chemical formulas and banking data are at risk. This paper provides a technique for communicating the data secretly using cryptography and steganography. Cryptography is the encrypting process in which the plain text converted into another form (i.e. cipher). Steganography is a technique of hiding the data in any media such as, image, audio and video. In this paper steganography performed on video files and hide the message in an encrypted format. The common method used for concealing the data is LSB. Instead of that we will use an encoding technique which will first transform the video using Lazy Lifting Wavelet transform and then apply LSB in the sub bands of the video. Bit Exchanging method is used for encryption. The encrypted data hidden on video using LSB. Steganography method provides robustness, capacity, undetectability and invisibility.

KEYWORDS: Steganography, Lazy wavelet transform, bit exchanging, stego key, data hiding

I.INTRODUCTION

Cryptography and steganography are the two main methods for hiding the information and security. Steganography is a Greek work which means the covered writing. Steganography is an art of hiding data in any media (image, audio, video, text) which cannot be detectable. Cryptography is the technique which scrambles the data itself so that it cannot be understood without unscrambling it. In such a way that the third parties cannot detect or even notice the presence of the communication. On comparing video with image and audio it has high storage capacity. AVI (Audio Video Interleave) video file has high resolution so that data can be hidden. There are many cryptography algorithms are created which convert the data into unreadable ciphers. There are two basic methods: symmetric key cryptography and public key cryptography. Symmetric key cryptographic uses a common key for both encryption and decryption of the data which should be known to sender as well as the receiver. This algorithm is less complex and execute faster as compared to other algorithms.

We shall perform steganography on video files and hide the message in an encrypted format. The most commonly used technique is Least Significant Bit steganography. But instead of traditional LSB encoding, Lazy Lifting Wavelet Transform is performed, which will first transform the video. And then apply LSB in the sub bands of the video to hide data. The secret data is encrypted by using an Simple Bit Exchanging method before the hiding process starts.

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. 3, Issue 7, July 2014

DOI: 10.15662/ijareeie.2014.0307014

II.BASIC CONCEPT

At transmitting side the data is encrypted using symmetric key algorithm and then hide the data into a video file, which will act as a cover file. At receiving side we first extract the hidden data from the received file and then decryption method is performed using shared key that we already used for encryption. Encryption and hiding the data done by cryptography and steganography technique.

III.PROPOSED TECHNIQUE

There are four techniques used for covert communication, Lazy Lifting Wavelet Transform, Bit Exchanging method and Least Significant Bit.

Lazy Lifting Wavelet transform

A video file is composed of multiple frames. Each frame is treated as a different image and an image steganography method is applied. This method uses some frames of the video to hide the secret data. By applying a Lazy Lifting Wavelet transform on each frame to get four sub bands. The data can be hidden on these four sub bands. We usually use wavelets to transform the given image in the spatial domain into the frequency domain. The data are stored as integers, but many wavelet transform return real values. It makes loss of data while transferring. To avoid this problem we use Lazy Lifting scheme which calculates Wavelet transforms in an efficient way.

Wavelet Transform

Wavelet is a small wave used to approximate the given signal effectively. Wavelet transforms are faster, provide better compression as images are sparse after wavelet transform, and wavelets are more adaptive compare to other transforms. Hence wavelets are useful in various applications such as image compression, noise removal, seismic data processing and speech processing. Wavelets are the mathematical function defined over a finite interval and having an average value of zero that transform data into different frequency component, representing each component with a resolution matched to its scale. All wavelet function are derived from a single mother wavelet.

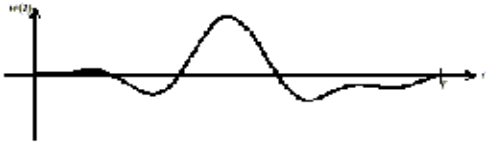

Fig.1 Wavelet Transform

In wavelet domain the signal or image f(x) can be define as the combination of ϕ and W. The function f(x) is given as

$$\mathbf{f(x)} = \sum_{l\in Z} \boldsymbol{c(l)}\boldsymbol{\varphi}_{\mathbf{l}}\mathbf{(x)} + \sum_{j=0}^{j-1}\sum_{k\in Z}^{n} \boldsymbol{d(j,k)}\boldsymbol{W}_{\mathbf{j,k}}\mathbf{(x)}$$

CRYPTOGRAPHY TECHNIQUE

Bit Exchanging Method

To encrypting any file, simple bit exchanging method is introduced. The secret message encrypted using shifting of bits and XOR operations. Following steps are used for encrypting the data.

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. 3, Issue 7, July 2014

DOI: 10.15662/ijareeie.2014.0307014

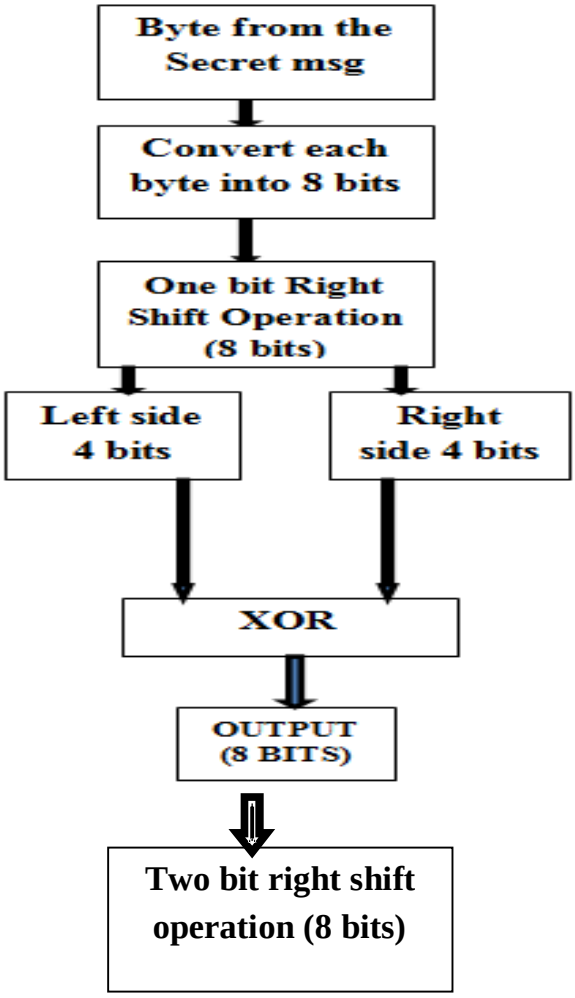

Fig.2 Bit Exchanging Method

Step 1: In the secret message file, read one by one byte and convert each byte into eight bits. Then one bit right shift operation applied on the entire file so that each bit will be modified according to it.

Step 2: Divide the eight bits into two blocks, four bits for left side and four bits for right side. The XOR operations performed on four bits on the left side with four bits on the right side. Output of this will be XOR with left four bits and same thing repeated for all bytes in the file.

***Step* 3:** Repeat step 1 by performing two bits right shift for all bytes in the secret message file. And then step 2 is repeated.

Maximum five bits are shifted to right side. For decryption process we follow the reverse process of above.

Steganography Algorithm

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. 3, Issue 7, July 2014

DOI: 10.15662/ijareeie.2014.0307014

There are many coding methods are used to hide the data. In that very popular methodology is the LSB (Least Significant Bit) algorithm is proposed to embed secret information within video file. It is used to replaces the Least Significant Bit in some bytes of the cover file to hide a data. LSB method allows large amount of secret information to be encoded in a video file.

Steps to hide Secret Data using LSB are:

- Covert the video file into bit stream.
- Convert each character in the secret information into bit stream.
- Replace the LSB bits of video file with the LSB bit of character in the secret information.

This method provides greater security and it is very efficient method for hiding the secret data from hackers and send to the receiver in a safe and undetectable manner.

Stego Key

To make the data more secured we have introduced the password while hiding an encrypted secret message in the video frame. The program will read the file size from the cover file and start work on the cover file when the password is correct. To extract the original secret message we perform the reverse process of the encryption method. The program first matches the password. If it is correct then it will read the size of the secret message file from the embedded cover file. Then it will read 8bytes and extracts 8 bits from four alternate bytes and convert them to a character and write onto an external file. If the bytes extracted from the cover file we run the decryption program to get the original secret message file.

IV.ADVANTAGES

- ***Secure Communication***
  The attacker cannot detect or even notice a presence of communication of secret data. Highly confidential data like military secrets, chemical formulas, and bank account details can be easily steganographed in video and can be transmitted secretly.

- ***Capacity***
  While hiding the data in image and video, it has the capacity of carrying data upto 50% only. But there is a limitation to hide the data in an image and audio. To overcome this problem video steganography has been found to hide large amount of data.

- ***Imperceptibility***
  Because of quickly displaying of the frames, so it's become harder to be suspected by human vision system.

- ***Large Availability***
  Today world the videos are present everywhere and many websites also used for sharing videos. So it is very easy to share a video without arousing suspicion. Even social media sites also allow easy sharing of videos. Because of this sharing of video files has been made very easy to hide the data.

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. 3, Issue 7, July 2014

DOI: 10.15662/ijareeie.2014.0307014

Fig 3: Secret Information Hidden in one frame

V.RESULT

VI.CONCLUSION

Our intension is to provide a protection on data during transmission. The secret data which we want to transmit is first encrypted and then the whole encrypted data is hidden in the audio of the video file using LSB. The Implementation is simple and also provides security. It doesn't affect the higher and lower ends of the frequency distribution of the signal. It can be easily extended, resulting in better robustness, better data security and higher embedding capacity.

REFERENCES

[1] DiptiKapoorSarmah and NehaBajpai, "A new horizon in data security by Cryptography & Steganography," *International Journal ofComputer Science and Information Technologies*, vol. 1, no. 4, pp. 212-220, 2010.
[2] PritishBhautmage, Prof. AmuthaJeyakumar "Advanced Video Steganography Algorithm" *International Journal of Engineering Research*, January 2013.
[3] D. Artz, "Digital Steganography: Hiding Data within Data," *IEEE Internet Computing Journal*, June 2001.
[4] J. Daemen and V. Rijmen, "AES Proposal: Rijndael," *National Institute of Standards and Technology (NIST)*, Technical Report2000.
[5] Jayaram .P and Ranganatha .H.R " Information hiding using Audio Steganography – a survey" *The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, August 2011*.
[6] K. Gopalan, "Audio steganography using bit modification," *In Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing, (ICASSP '03)*, pp. 421-424, 2003.
[7] G. Doerr and J.L. Dugelay, "Security pitfalls of frame-by frame approaches to video," *IEEE Trans. Sig. Proc.*, vol. Supplement on Secure Media, no. 52, pp. 2955-2964, 2004.
[8] J. Daemen and V. Rijmen, "AES Proposal: Rijndael," *National Institute of Standards and Technology (NIST)*, Technical Report2000.
[9] R. Balaji, G. Naveen, *"Secure Data Transmission Using Video Steganography"*
[10] AgniswarDutta, Abhirup Kumar Sen, Sankar Das, ShalabhAgarwal, AsokeNath, New Data Hiding Algorithm in MATLAB using Encrypted secret message,*IEEE ICCSNT-201*,pp.262-267.