Data Hiding using Lazy Wavelet Transform Strategy

Ekansh Agarwal
Department of CSE
IMSEC, Ghaziabad
UP India

Shaili Gupta
Department of CSE
IMSEC, Ghaziabad
UP India

Mayank Arya Chandra
Department of CSE
IMSEC, Ghaziabad
UP India

ABSTRACT

Steganography is an art of hiding the secret information inside digitally covered information. The hidden message can be text, image, speech or even video and accordingly the cover can be chosen from either an image or a video. The message is concealed in lowest bits of cover. We shall perform steganography on videos and hide message in encrypted form, by this security is increased by two times. The mostly used technique is LSB (Least Significant Bit)[1] steganography. But instead of simple LSB technique, we will use Lazy Lifting Wavelet transform [2] and then apply LSB in the sub-bands of the video that has been obtained. The proposed approach will utilize the video as well as audio component to hide message, in video component we will hide the encrypted message and in audio we hide the length, up to which the message is hide in video, using LSB technique. Experimental results show that the proposed technique has a high payload capacity and low computational requirement.

General Terms

AES Algorithm, Information hiding, Information retrieval.

Keywords

Sub bands, RGB component, Lazy Wavelet, LSB.

1. INTRODUCTION

Steganography is the art of hiding secret information in the form of cover which can be any multimedia file like image, audio, video, by which third party cannot recognizes that message which is existed [10]. The goal of cryptography [3] is to protect the content of messages. Steganography is little bit contrast to cryptography. In steganography, existence of the message will be hidden but in cryptography, meaning of the message will be hidden. Steganography is often confused with cryptography because they both are similar in the way that both are used to protect important and secret information. The difference between the steganography and the cryptography is that steganography involves hiding information so it appears that no information is hidden at all. If the object is viewed by person to know whether there is something hidden in it or not, then he or she will get no idea that there is any information which is written, so the person will not try to decrypt the information.

In today's era the challenge is to send and display the hidden information especially in public places. The reason that intruders attain information from a system is in a form that they can read and understand it. Intruders may modify it to misrepresent an individual or organization, reveal the information to others, or use it to launch an attack. The problem can be solve by using steganography[11].

Multimedia files, such as images, audio and video are widely use today. Data can be hidden in images, which are good medium, to hide data. The more detailed the image, the lesser constraints there are on how much data it can hold without it becoming conspicuous. For hiding data in audio files, there are many tools available for it. The large size of audio files made it less popular than image files as a medium for steganography. But both these mediums have a lot less storage capacity as compared to videos, since videos can be taken as a collection of frames (images) and audio [4]. There are many cryptography algorithms have been created which turn the data into unreadable ciphers (an encrypted text). There are two basic methods: symmetric key cryptography [5] and public key cryptography [6]. We will discuss symmetric key cryptography in this paper, Advanced Encryption Standard (AES) [7][19], which are applied on plain text message to produce a cipher text.

Now In this paper we propose a new efficient scheme for video steganography using Lazy wavelet mechanism along with Encryption. This paper consists following sections: In section 2nd Related Work. Section 3rd Proposed Technique, 4th section describes the Information Hiding and Information retrieval algorithms, 5th section describes the experimental results, and 6th section describes the conclusion and 7th section references.

2. RELATED WORK

Steganography in video is done by applying transformation techniques. It can be achieve either in spatial domain or in frequency domain. In spatial domain computation is done on pixel value directly while in frequency domain, firstly it is converted into frequency domain and then computation is done. There are many LSB techniques by which data can be encoded in image or video or any multimedia file. Depending upon the size of cover and technique use the amount of data can be hidden. Before hiding the data, it can be secured by applying some cryptography technique which will convert the readable message into cipher text(which is not readable). Random Byte hiding [8] and Wavelet [9] technique also has been used in steganography.

There are many algorithms that achieve the video security in the form of Cryptography [12].In the field of neural network, chaotic theory is very popular for encryption and decryption.[14][13][15][16][17], main advantage of chaotic network is that it is low cost, which is suitable to large amount of data. **H**ongmei Tang et al., [20] proposed a image encryption and Steganography scheme. The combination of a gray value substitution operation and position permutation encrypts the secret message. R O El Safy et al., [21] proposed an adaptive steganographic technique based on integer wavelet transform for hiding data in digital images by combining the use of adaptive hiding capacity function that hides secret data in the integer wavelet coefficients of the cover image with the Optimum pixel adjustment algorithm.

Since communications via chat room become more and more popular in people's lives; Wang and Chang proposed new text steganography method in 2009 [22]. The proposed method embeds secret information into emotional icons (emoticons) in chat rooms over the Internet. Por et al. (2012) proposed a data hiding method based on space character manipulation called UniSpaCh [23]. UniSpaCh is proposed to embed information in Microsoft Word document using Unicode space characters.

3. PROPOSED TECHNIQUE

3.1 Cryptographic Model

In this model we will use the AES(128 bits key) symmetric key algorithm, which will convert the readable text into cipher (unreadable) text, which provide a high security. And this data is stored in frames of Video after that video can be send. At the receiving side, the cipher text is retrieved and converted to plain text by decrypting the cipher using the shared key, which is already known to receiver.

3.2 Hiding Procedure

A video is consisted of multiple frames. We will use some frames of video in sequential order, and each frame (image) is treated as unique image and is use to store encrypted message. A steganography technique is use to store message, we use the 2D - Lazy Wavelet Transform [2] on each frame to get four sub-bands. The data is then hidden in subbands of frames using LSB technique. The length of data which is stored in frames is hide in audio using simple LSB technique.

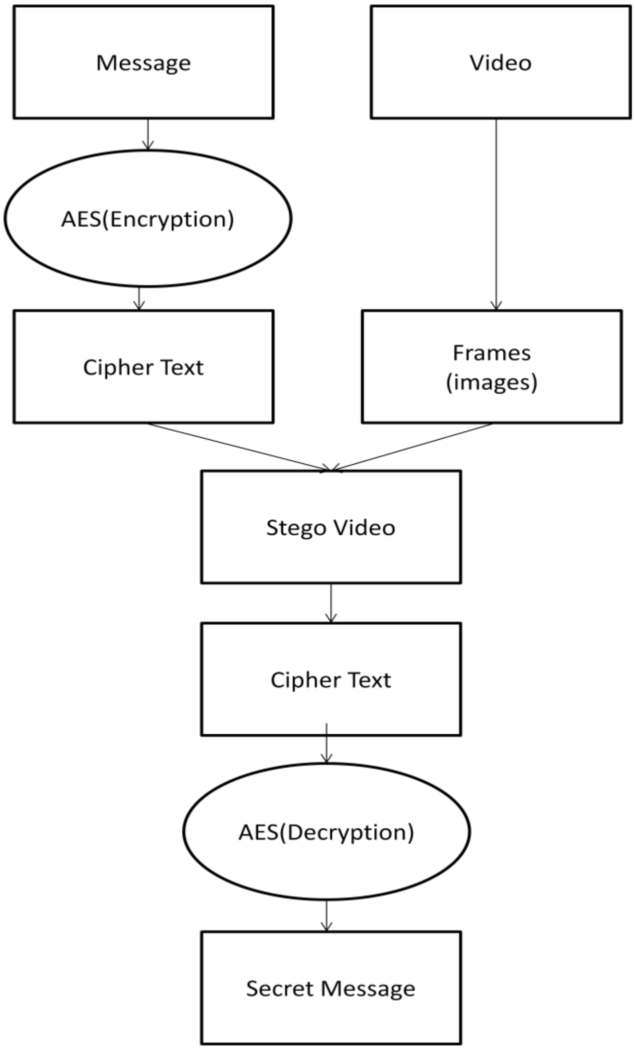

Fig.1 Flowchart representing the proposed technique

3.3 Converting Given Encrypted Cipher Data into a Stream of Bits

The encrypted data is read character by character and is converting to stream of bits (as each character in ASCII is represented in 8 bits). And now the stream of bits can be encoded in the frames.

3.4 Applying Lazy Wavelet Transform on the Frames of the Video

A video is comprised of many frames. On each frame we apply a image transformation technique. Wavelet transformation is use to convert the spatial domain into frequency domain but most of the wavelet techniques produce real values, which will result in data loss when is hide and retrieved. So to overcome this we use lazy wavelet scheme, by applying Integer Wavelet Transform which produces integer values. After applying Integer Wavelet Transform we get four subbands.

3.5 Hiding bits in the Four Sub-bands

For each subbands we find out RGB components, and now we start encoding data in RGB components in sequential order of each subbands of each frame using LSB technique

3.6 Hiding the Total Length and the Number of Bits in the Last Frame in the Audio using LSB

Since we are storing the data sequentially in the frames, we will store maximum payload in all the frames, which will be fixed by the frame size. But in the last frame in which the message bits will be hidden, a fewer number of bits might be hidden. When we will decode our original message at the receiver end, we will need this number to extract the exact message. Also, the total number of frames in which the data is stored will need to be sent along with the message. So we will store these numbers sequentially in the audio using the LSB method.

4. Algorithm for Information Hiding

Definition

Frame: I
Encrypted message: m

Step 1: Extract all frames from video
Step 2: Select 1st Frame I from Video
Step 3: Apply Lazy wavelet scheme to produce 4 subbands (cA cH cV cD).
Step 4: Extract RGB component from choosen sub band
Step 5: Select 1st pixel P from RGB Component
Step 6: Get 24 bit corresponding pixel value
Step 7: Perform $m_n \oplus P_n(k)$ where k=1,2,3 and n=1……n-1
Step 8: Repeat step 3, 4, 5 for all frames
Step 9: Construct the video from all encoded frames.
Step 10: Transmit Video, secret Key through secure channel

5. Algorithm for Information retrieval

Step 1: Extract all frames from video
Step 2: Select 1st Frame I from Video
Step 3: Apply Lazy wavelet scheme to produce 4 sub bands (cA cH cV cD).
Step 4: Extract RGB component from chosen subband
Step 5: Select 1st pixel P from RGB Component
Step 6: Get 24 bit corresponding pixel value

Step 7: Perform $msg=p_n(k)$ where k=1,2,3 and n=1….n-1
Step 8: Repeat step 3,4,5 for all frames and save message.
Step 9: Apply AES decryption to convert cipher message to plain text (we get the secret message)

6. Experimental Result

This section deals with the result analysis of proposed technique. The above algorithms have been successfully implemented and the results are shown in the table below.

6.1. Video data

1) Vipmen.avi

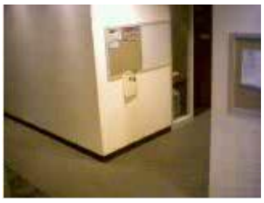

Fig.1(a) Before Hiding

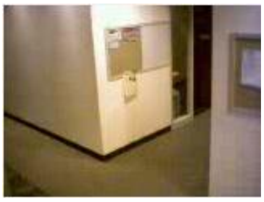

Fig.1(b) After Hiding

2) Haky_car.avi

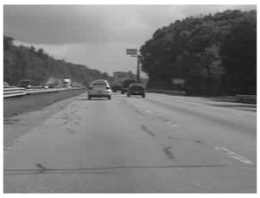

Fig.2(a) Before Hiding

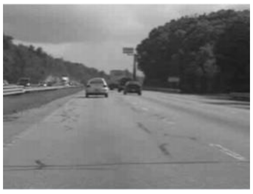

Fig.2(b) After Hiding

3) Vipmosaicking.avi

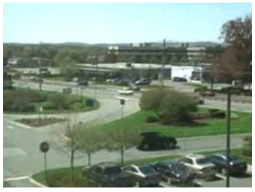

Fig.3(a) Before Hiding

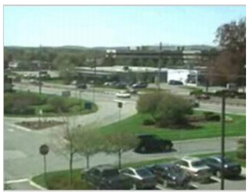

Fig.3(b) After Hiding

4) Viptraffic.avi

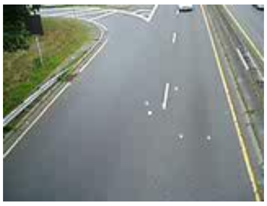

Fig.4(a) Before Hiding

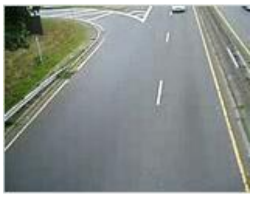

Fig.4(b) After Hiding

6.2 Result Analysis

Table-1 Result Analysis

Video	**MSE**	**RMSE**	**PSNR**
Vipmen.avi	0.7436	0.8623	49.4172
Haky_car.avi	0.7609	0.8723	49.3173
Vipomosaicking.avi	0.7601	0.8718	49.3221
Viptraffic.avi	0.7417	0.8612	49.4285

6.3 HISTOGRAM FOR FRAME

1. Vipmen Video

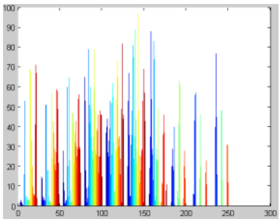

Fig.1(a) Before Hiding

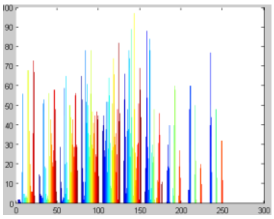

Fig.1(b) After Hiding

2. Haky_car Video

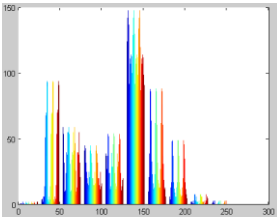

Fig.2(a) Before Hiding

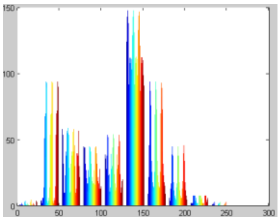

Fig.2(b) After Hiding

3. Vipmosaicking Video

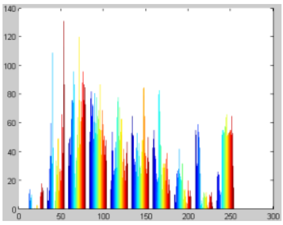

Fig.3(a) Before Hiding

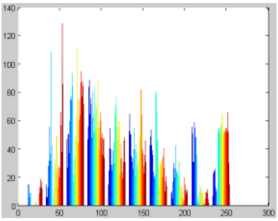

Fig.3(b) After Hiding

4. Viptraffic Video

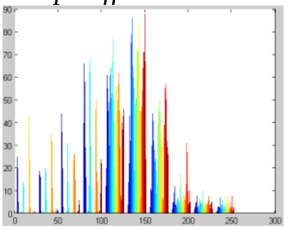

Fig.4(a) Before Hiding

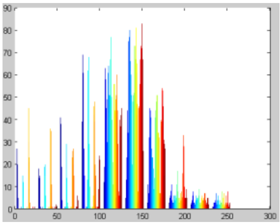

Fig.4(b) After Hiding

7. CONCLUSION

Steganography is the art of hiding information in digital media in order to conceal the existence of the information. The paper provides a good method of steganography in video by using AES algorithm, Lazy Wavelet Scheme and LSB technique. The data is hidden in video and the length is hidden in audio component using LSB technique, and the changes which are done in both the components is not recognizable. The proposed technique provides two layer securities by cryptography and Steganography. The technique provides a good capacity to store a high load message.

Experiments were conducted to demonstrate that video-Frame stenography provides a good trade-off between encryption, steganography robustness, flexibility, and real-time processing. The Lazy Wavelet Scheme is applied on each frame to derive sub bands. The proposed algorithm is robust since the payload is embedded into the transform cover image indirectly. The algorithm can be tested in future with some more transform techniques to improve the performance.

The proposed technique can be use in copyright control of materials, medical records, TV broadcasting, financial companies data safe circulation, smart Id cards and banking.

8. References

[1] H S Manjunatha Reddy. Wavelet based Non LSB Steganography. Department of ECE, Global Academy of Technology, Bangalore-98, India

[2] Khushman Patel, Kul Kauwid Rora, Kamini Singh, Shekhar Verma. Lazy Wavelet Transform Based Steganography in Video. Dept of CSE, IIIT Allahabad, Allahabad (U.P.)

[3] Cryptography. From Wikipedia http://en.wikipedia.org/ wiki / Cryptography

[4] G. Doerr and J.L. Dugelay, "Security pitfalls of frame-byframe approaches to video," IEEE Trans. Sig. Proc., vol. Supplement on Secure Media, no. 52, pp. 2955-2964, 2004.

[5] Symmetric key cryptography. From Wikipedia http://en.wikipedia.org/wiki/Symmetric_key_cryptography

[6] Public key cryptography. From Wikipedia http://en.wikipedia.org /wiki/Public-key_cryptography

[7] AES from http://en.wikipedia.org/wiki/ Advanced_ Encryption_ Standard

[8] Ashish T. Bhole, Rachna Patel. Steganography over Video File using Random Byte Hiding and LSB Technique Department of Computer Engineering, SSBT's COE & T, Bambhori, Jalgaon, India

[9] T. Natramizhnangai and R. SenthilRajan A Novel Steganography Method based on Integer Wavelet Transform and Genetic Algorithm.

[10] Ming Chen, "Analysis of Current Steganography Tools: Classifications & Features," in International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2006, pp. 384 – 387, 2006

[11] D. Artz, "Digital Steganography: Hiding Data within Data," IEEE Internet Computing Journal, June 2001.

[12] Mayank Arya Chandra Ravindra Purwar, Navin Rajpal "A Novel Approach of Digital Video Encryption" International Journal of Computer Applications (0975 – 8887) Volume 49– No.4, July 2012

[13] Alligood, K. T., Sauer, T., Yorke, J. A. : Chaos: an introduction to dynamical systems. Springer, Heidelberg (1997).

[14] Devaney, R. L. :An introduction to chaotic dynamical systems, 2nd edn.West- view Press, San Francisco (2003).

[15] Yang, T., Wu, C. W., Chua, L.O. : Cryptography based on chaotic systems. IEEE Transactionson Circuits and Systems-I : Fundamental Theory and Applications 44, 469…472 (1997).

[16] Solak, E. : Cryptanalysis of observer based discrete-time chaotic encryption schemes. International Journal of Bifurcation and Chaos 15 (2), 653…658 (2005).

[17] He, J., Qian, H., Zhou, Y., Li, Z.: Cryptanalysis and improvement of a block cipher based on multiple chaotic systems. Mathematical Problems in Engineering 2010,1…14 (2010).

[18] Mohd. Arif Siddique, Mayank Arya Chandra, Kunwar Babar Ali. "Improved Graphical Password Authentication using Dynamic Grid and Image Zoom" IJAER Volume 6, Number 18 (2011)

[19] Zeghid, M., Machhout, M., Khriji, L., Baganne, A., et al.: A modified AES based algorithm for image encryption. International Journal of Computer Science and Engineering 1 (1), 70…75(2007).

[20] Hongmei Tang, Gaochan Jin, Cuixia Wu and Peijiao Song, A New Image Encryption and Steganography Scheme, IEEE International Conference on Computer and Communications Security,2009, 60-63.

[21] R O El Safy, H H Zayed and A El Dessouki, An Adaptive Steganographic Technique Based on Integer Wavelet Transform, IEEE International Conference on Networking and Media Convergence, 2009, 111-117.

[22] Wang Z, Chang C, Lin C, Li M (2009) A reversible information hiding scheme using left-right and updown Chinese character representation. J Syst Softw 82:1362–1369

[24] Por, L.Y., Wong, K., Chee, K.O., 2012. UniSpaCh: a text based data hiding method using unicode space characters. Journal of Systems and Software, http:// dx.doi.org/10.1016/ j.jss.2011.12.023.