Impact Factor (SJIF): 3.632

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 3, Issue 6, June-2016

Implementation of Audio Video Steganography Using Anti Forensic Technique for Authentication and Data Security

Kapil Adhar Wagh[1], Asst. Prof. Mayur Rathi[2]

[1]*Department of Computer Science Engineering, RIT, Sanwer Road, Indore*
[2]*Department of Computer Science / Information Technology, RIT, Sanwer Road, Indore*

Abstract *— Steganography is the technique of hiding any secret information like password, text and picture, audio behind original cover file. Original message is converted into cipher text by using mystery key and then hidden into the LSB of original image. The proposed system provides audio-video crypto steganography which is the combination of image steganography and audio steganography using Forensics Technique as a tool to authentication. The main aim is to hide secret data behind image and audio of video file. As video is the utilization of many still frames of images and audio, we can select any frame of video and audio for hiding our secret information. Suitable algorithm such as AES is used for image steganography suitable parameter of security and authentication; hence data security can be increased. And for data embedding we use 4LSB algorithm. This paper focuses the thought using so as to send vast information FZDH.*

Keywords: *FZDH, 4LSB, Hiding, steganography, cryptography.*

I. INTRODUCTION

Steganography is the method of hiding of the data or any other secret information like password, text, image into the cover file [1]. Steganography makes the data more secure as its aim is to keep the attacker unknown about the secret information. Data is needed to be encrypted using the encryption algorithm before it is hidden into the file.

The aim is to hide secret information into the audio as well as video of the audio video file. We can select the particular frame of the video behind which we have to hide the important data. By applying the suitable algorithm data will be hidden into the selected frame of the video. After hiding the data into the audio and video separately both the audio and video files needed to be merged to make a complete audio video file. The large amount of the secret data can be hidden by making the use of video Steganography. The receiver needs to be known about the procedures through which it can gain the required important and secret data.

Video is the application of many still frames of images and audio, we can select any frame of video and audio for hiding our secret data. Suitable algorithm technique such as LSB is used for image steganography. The suitable parameter of security and authentication like PSNR, histogram analysis are obtained at receiver end and transmitter side which are exactly identical, hence the data security can be increased [2] [5]. This paper focus the idea of computer forensics technique and its use of video steganography in both investigative and security purpose [1] [7].

II. LITERATURE REVIEW

1) LSB Insertion Technique

Least Significant Bit (LSB) insertion is a common and simple approach to embed the information in a cover video. Video is converted into the number of frames, and then converted the each frame into the image. Later on, the Least Significant Bit (in other words the 8 bit) of some or all of the bytes inside the image is changed to a bit of each of the Red, Green and Blue color components can be used, since they are each represented by a byte. In other words one can store 3 bit in each pixel. An 800 x 600 pixel image can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data. We implemented our project such that it can accept the video of any size.

Advantages:

- There is less chance for degradation of the original image.
- More information can be stored in an image

Disadvantages:

- Less robust, the hidden data can be lost with image manipulation.
- Hidden data can be easily destroyed by simple attacks.

2) 4LSB Insertion Technique

Each frame or image is made up of number of individual pixels. Each of these pixels of an image is made up of a string of bits the 4 least significant bit of 8-bit true color image is used to hold 4-bit of our secret message image by simply overwriting the data that was already there. By experimentation, it has been proved that the impact of changing the 4least significant bits is almost imperceptible. In hiding process, the last 4 bits of image or frame pixel is replaced with 4 bits of our secret data. For this secret data which is also sequence of bytes are broken down into set of 4 bits. To hide each character of secret message we need two pixels. So the number of characters that we can hide in (m x m) image is given by the following equation.

Total size of one frame ÷ 8 ---- (1)

Suppose size of a single frame is 160KB, then for 1LSB, maximum data that can be hidden is 1×20KB = 20KB. For 2LSB it is 2×20KB = 40KB. For 3LSB it is 3x20=60KB. For 4LSB it is 4×20KB =80KB. If steganographic process go beyond 4LSB,

Advantages:

- Retrieved exact secret image
- Quality of a video file is strictly preserved even after secret data embedding.

Disadvantages:

- Large payload.
- Limited amount data can be embedded behind cover image.

3) Hash based LSB Technique

The Hash Based Least Significant Bit for Video Steganography Technique has been proposed in which it perform encoding and decoding for hiding message and extracting message respectively [4]. First of all message file will be embedded within the cover file by using the steganographic tool as here use of MATLAB software. This steganographic file is again applied to steganographic tool to extract embedded data. A cover video consists of collection of frames and the secret data is embedded in these frames as payload.

Advantages:

- There is less chance for degradation of image
- More information can be stored

Disadvantages:

- Less Robust as the hidden data can be lost with image manipulation

4) FZDH Technique

The least significant bit (LSB) algorithm is used in this stego machine to conceal the data in a video file. The main advantage of the LSB coding method is a very high watermark channel bit rate and a low computational complexity. The robustness of the watermark embedded using the LSB coding method, increases with increase of the LSB depth is used for data hiding. In this method, modifications are made to the least significant bits of the carrier file's individual pixels, thereby encoding hidden data. Here each pixel has room for 3 bits of secret information, one in each RGB values. Using a 24-bit image, it is possible to hide three bits of data in each pixel's color value using a 1024x768 pixel image; also it is possible to hide up to 2,359,296 bits. The human eye cannot easily distinguish 21-bit color from 24-bit color

Advantages:

- Ability to encrypt and decrypt the data with the images
- With this system, an image, after hiding the data, will not degrade in quality

Disadvantages:

- Long coding time.

III. SURVEY OF PROPOSED SYSTEM

In this paper, proposed Information security utilizing information concealing audio video steganography with the assistance of PC measurable strategies gives better concealing limit we have taken a shot at concealing picture and content behind video and audio document and separated from an AVI record utilizing 4 minimum noteworthy piece insertion techniques for video steganography and stage coding audio steganography. Stegnography is the strategy for

concealing any mystery data like watchword, content and picture, audio behind unique spread record. Unique message is changed over into figure content by utilizing mystery key and after that covered up into the LSB of unique picture. The proposed framework gives audio-video crypto steganography which is the mix of picture steganography and audio steganography utilizing Forensics Technique as an instrument to validation. The primary point is to shroud mystery data behind picture and audio of video record. As video is the use of numerous still casings of pictures and audio, we can choose any casing of video and audio for concealing our mystery information. Suitable algorithm, for example, AES is utilized for picture steganography suitable parameter of security and confirmation, thus information security can be expanded. Also, for information implanting we utilize 4LSB algorithm. This paper centers the thought using so as to send expansive information FZDH.

IV. MATHEMATICAL MODEL

Let S is the Whole System Consist of
S= {I, P, O}
I = Input.
I = {AF, VF}
AF = Audio File, VF = Video File.
P = Process
P = {4LSB, phase coding algorithm, LSB}
4LSB = Used for image steganography.
Phase Coding: It is used for audio steganography.
LSB = Least Significant Bit: Used for embedding the data into the bit map image (.bmp).
Step1: Selecting audio-video file.
Step2: Video Steganography.
Step3: Creating stego audio file.
Step4: Authentication (at receiver side).
Step5: Audio recovery.
Step6: Computer forensics and authentication.

V. SYSTEM ARCHITECTURE

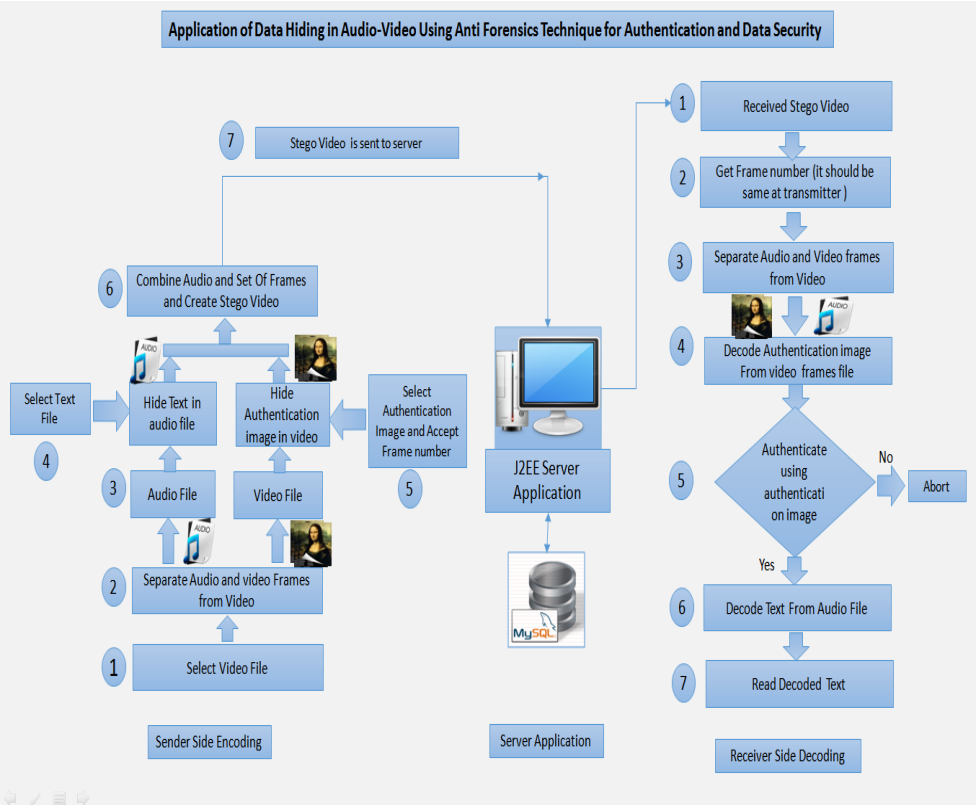

Figure 1. Audio video steganography system architecture

VI. IMPLEMENTATION

1. Selecting Video File

a. Select AVI video file, behind which user wants to hide data.
b. Separate audio and video from selected video file using available software.
c. Save audio file as .wav file which is the original separated audio file.

2. Data Encryption Using AES Algorithm

a. AES algorithm is applied before embedding data in an image.
b. Data encrypted before sending to server using AES algorithm.

3. Encrypted Data hiding in video Using LSB steganography

a. Select original video file (.AVI).
b. Separate all frames of video file.
c. Get frame number to from user behind which an authentication image is to be hidden.
d. Read authentication image.
e. To extract msb (most significant bit) of frame bit AND frame with 240(11110000).
f. To extract msb of authentication image bit AND frame with 240(11110000).
g. Reverse the place of msb of authentication image to lsb by dividing each element by 16.
h. Reshape the image bits into one row.
i. This reshaped row vector of authentication image data is embedded on the frame matrix by adding each row vector bits two last 4 bits of frame bits.
j. This forms a steno frame overwriting this steno frame with original video file create steno video file.
k. Create new steno video file in which authentication images is hidden.

4. Creating stego audio file

a. Combine stego audio and stego video file using 'cute audio video merger' software.
b. This forms the stego audio video file at transmitter site which has hidden text and image in it.

5. Authentication (at receiver side)

a. After transmission of the stego audio video file obtained at receiver side.
b. Read the stego audio video file.
c. Select the frame number (the frame number should be same at transmitter at receiver side then only the authentication process start else it gets terminated)
d. To recover the authentication image from the selected frame bit AND the frame data with 15.
e. Authentication image data is available at LSB of frame is recovered.
f. Select the authentication image at receiver side compares recovered authenticated image with the selected image.
g. If both the images matched, then only user can recover the text behind audio else process is terminated.

6. Audio Recovery

a. Read audio file.
b. Open this stego audio file in read mode.
c. Read wave file's first 40 bytes of header.
d. Then read all its data after 40th byte and close file.
e. Recover the size of identity key from LSB of .wav file. Recover identity key from further LSB bits of .wav file.
f. Accept identity key from user and compare entered identity key with recovered identity key. If both the keys matched then only user can recover the hidden text else processes will be aborted.
g. As identity key is matched, recover the size of message from further LSB bits of .wav file. Recover the message.
h. Secrete text is recovered [11].

VII. RESULT ANALYSIS

Analysis 1 Title: Performance analysis of video size & accuracy system.

Table 1. Video size and accuracy in different systems

Methodology	Video size	Accuracy
Enhanced Proposed System	7	9
Proposed System	5	8.3
Existing	2.3	5

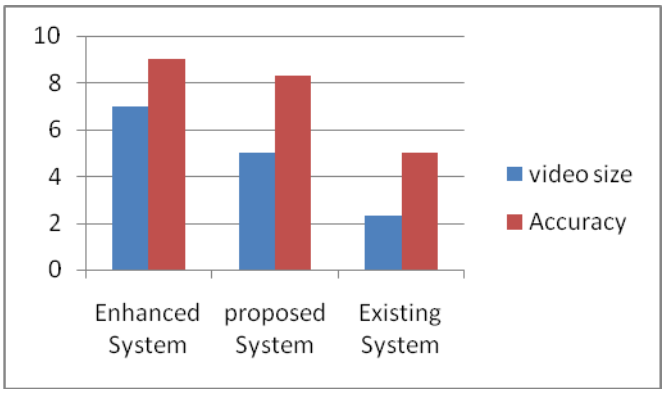

Figure 2. Variance of different systems in the form of bar graph

Analysis 2 Title: Comparison of Algorithms with Enhanced Proposed and Proposed System.

Table 2. Efficiency of different algorithms in different systems

Methodology	4LSB	AES	FZDH
Enhanced Proposed System	80%	90%	90.6%
Proposed System	70%	76%	65%
Existing System	60.5%	52.5%	35%

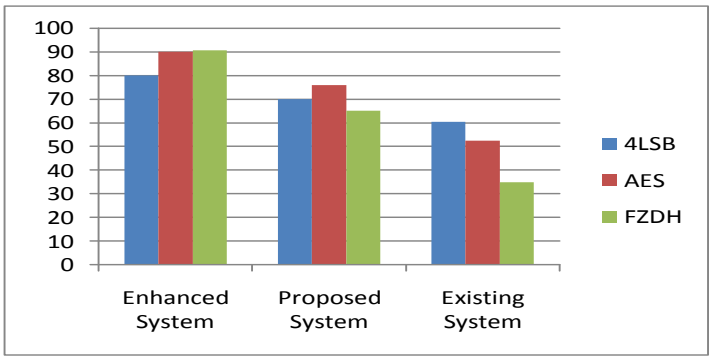

Figure 3. Efficiency of different algorithms in different systems in the form of bar graph

VIII. CONCLUSION AND FUTURE WORK

In this paper, proposed Information security utilizing data hiding audio video steganography with the assistance of PC measurable strategies gives better concealing limit we have chipped away at concealing picture and content behind video and sound record and removed from an AVI document utilizing 4 minimum noteworthy piece insertion techniques for video steganography and stage coding audio steganography. We are hiding encrypted data using steganography and cryptography behind selected frame of video using 4LSB insertion method.

REFERENCES

[1] Praveen. P, Arun. R, "Audio Video Crypto Steganography using LSB substitution and advance chaotic algorithm", International Journal of Engineering Inventions 2014.

[2] Pathak P, A. K. Nag, "A new Audio steganography scheme based on Location with Enhanced Security", ACES First International Conference 2014.
[3] Bassem Bakhache, Joseph M. Ghazal, and Safwan EI Assad, "Improvement of the Security of Zigbee by a New Chaotic Algorithm", IEEE System Journal 2013.
[4] V. Sathyal, K. Balasubramaniyam, N. Murali, M. Rajakumaran, Vigneswari, "data hiding in Audio signal, video signal, text and jpeg images", IEEE-International Conference on Advances in Engineering, Science and Management(ICAESM-2012).
[5] Sghaier Guizani, Nidal Nasser, "An Audio/Video Crypto Adaptive Optical Steganography Technique" IEEE 2012, pp, 1057-1062.
[6] P. P. Balguruji, S. K. Jagtap, "Intelligent processing, An approach of Audio Steganography", IEEE 2012 ICCICT, Oct 19-20, Mumbai, India, pp, 1-6.
[7] Fatiha Djebbar, Beghdad Ayad, Habib Hamamand Karim abed-Meraim, "A view on latest audio steganography technique", International Conference on innovations in Information Technology 2011.
[8] K. A. Navas, Vidya. V, Sonia. V. Dass, "High security data embedding in video", Recent Advances in Intelligent Computational Systems (RAICS), 2011 IEEE.
[9] George Abboud, Jeffery Marean, "Steganography and Visual Cryptography in Computer Forensics" 2010 IEEE, Fifth International workshop on systematic application to digital Forensic Engineering, pp. 25-30.
[10] S. Gao, R. M. Hu. W. Zeng H. Jai, "A Detection algorithm of audio spread spectrum data hiding", 2008 IEEE-International Conference, ppl-4.
[11] S.K. Moon, Rajashree Raut, "Application of Data Hiding in Audio Video Using Anti Forensic Technique for Authentication and Data Security", 2014 IEEE International Advance Computing Conference (IACC).
[12] M. Pooyan, A. Delforouzi, "LSB based steganography method based on lifting wavelet transform" 2007 IEEE International symposium on signal processing and information technology, pp, 600-603.