Scientific Journal of Impact Factor (SJIF): 4.14

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 3, Issue 6, June -2016

# Data Security Using Audio Video Steganography

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

[1,2]*Department of Computer Engineering, Sanwer Road, R I T, Indore,*

**Abstract** — *Steganography is the technique of hiding any secret information like password, text and picture, audio behind the 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 cryptostegnography 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 the 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

Pure Steganography is defined as a steganographic system that does not require the exchange of a cipher such as a stego key. There is two input, carrier object and message object. The steganographic algorithm is used to embed message object onto carrier object. The main criteria for this embedding is no third party observer can see, listen or suspect about the message. It should be lie in secret. Different type of object can be used as carrier and message object. It can be Image, Text, audio and video. But we can't send large data through this method.

Stenography is the method of hiding any secret information like password, text and image, audio behind original cover file. Original message is converted into cipher text by using secret key and then hidden into the LSB of original image [1]. 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 information behind image and audio of video file. As 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 such as LSB is used for image steganography suitable parameter of security and authentication like PSNR, histogram are obtained at receiver and transmitter side which are exactly identical , hence 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 manner [1] [7].

## II. LITERATURE REVIEW

**1) Techsnology**: *LSB*

**Description:** Least Significant Bit (LSB) insertion is a common, simple approach to embedding information in a cover video. Video is converted into a number of frames, and then convert each frame in to an image. After that, the Least Significant Bit (in other words the 8 bit) of some or all of the bytes inside an 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 and 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) Technology:** 4LSB

**Description:** Each frame or image is made up of number of individual pixels .Each of these pixels in an image is made up of a string of bits the 4least 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 video file is strictly preserved even after secret data embedding.

**Disadvantages:**

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

**3) Technology:** Hash Based LSB

**Description:** 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 the 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 fordegradation of image
- More information can be stored

**Disadvantages:**

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

**4) Technology:** FZDH

**Description:** 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. 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. Steganography 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. ALGORITHMS

- ***Data Hiding using 4LSB Algorithm:***

The idea of the LSB algorithm is to insert the bits of the hidden message into the least significant bits of pixels. LSB (Least Significant Bit) substitution is the process of adjusting the least significant bit pixels of the carrier image. It is a simple approach for embedding message into the image. The Least Significant Bit insertion varies according to number of bits in an image. Video is a sequence of images displayed at faster rates taking the advantage of human vision system. An extremely simple steganographic method is to hide the information at pixel level.

1) Each frame or image is made up of no. of individual pixels .Each of these pixels in an image is made up of a string of bits the 4least 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.
2) In hiding process, the last 4 bits of image or frame pixel is replaced with 4 bits of our secret data.
3) 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.
   No. of characters that we can hide in image = Total size of one frame ÷ 8 ---------- (1)
4) 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, i.e. for 5LSB it is 5×20KB=100 KB, means that size of the data can be hide is more than 50%, hence it is look like visible watermarking.
5) For implementing steganography proposed method is using 4LSB algorithm. Any data change in least significant bit does not change the value of data significantly.

- **THE AES ALGORITHM**

The AES-256 algorithm is composed of three main parts: Cipher, Inverse Cipher and Key Expansion. Cipher converts data to an unintelligible form called cipher text while Inverse Cipher converts data back into its original form called plaintext. Key Expansion generates a Key Schedule that is used in Cipher and Inverse Cipher procedure. Cipher and Inverse Cipher are composed of specific number of rounds for both of its Cipher and Inverse Cipher, the AES algorithm uses a round function that is composed of four different byte-oriented transformations:

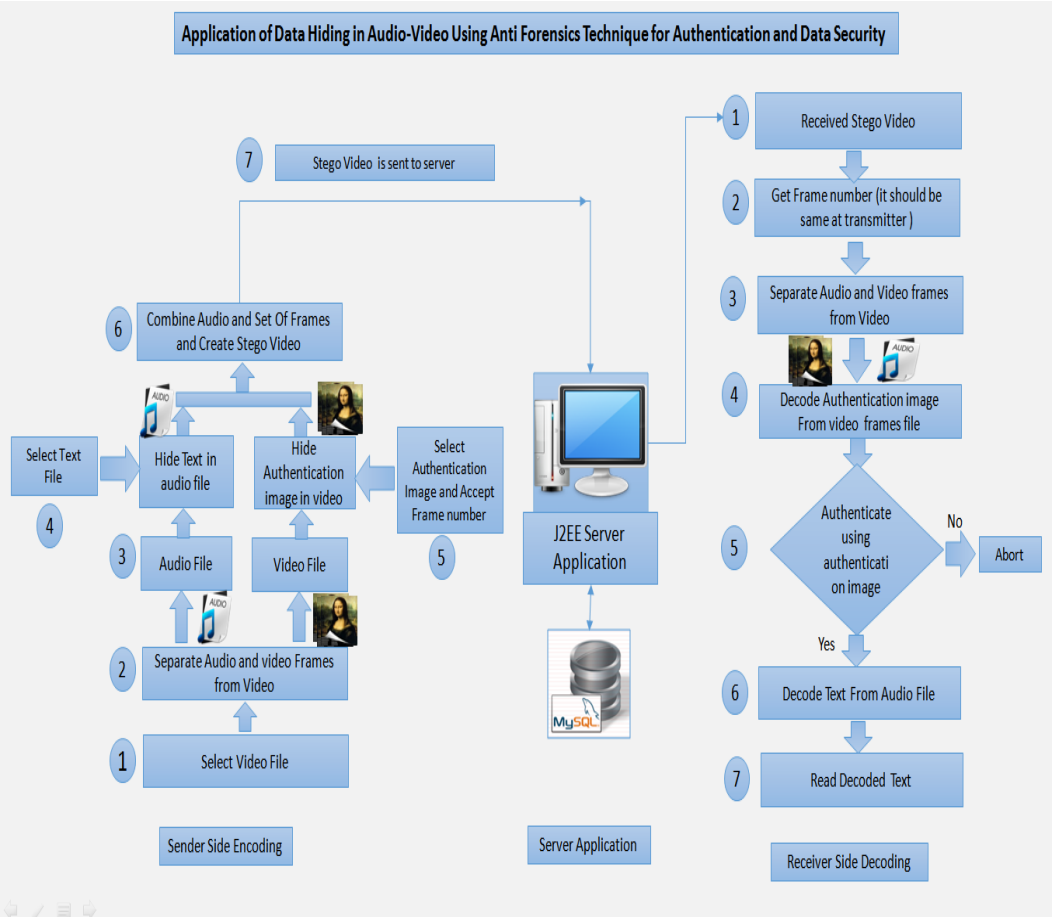
1) Byte substitution using a substitution table (S-box)
2) Shifting rows of the State array by different offsets
3) Mixing the data within each column of the State array
4) Adding a Round Key to the State

The Cipher transformations can be inverted and then implemented in reverse order to produce a straightforward Inverse Cipher for the AES algorithm. The individual transformations used in the Inverse Cipher.
1) Inverse Shift Rows
2) Inverse Sub Bytes
3) Inverse Mix Columns
4) Add Round Key

The AES inverse cipher core consists of a key expansion module, a key reversal buffer, an initial permutation module, a round permutation module and a final permutation module. The key reversal buffer first store keys for all rounds and the presents them in reverse order to the rounds. The round permutation module will loop maternally to perform 14 iterations (for 256 bit keys).

## V. SYSTEM ARCHITECTURE




## VI. 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: Is used for audio steganography.
LSB = Least Significant Bit: use of (LSB) algorithm for embedding the data into the bit map image (.bmp).
O = Output
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.

## VII. CONCLUSION

In this paper, proposed Information security utilizing data hiding audio video stegnography 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.

## VIII. REFERENCES

[1] Shoji Sakurai, Shinobu Ushirozawa, "Input Method against Trojan Horse and Replay Attack", Information Theory and Information Security (ICmS), pp.3S4-3S9, Jan 2010.
[2] Ken Birman, "In Computers We Trust" Distributed Systems Online, Dec2005.
[3] Microsoft Security Intelligence Report http://www.microsoft.comlsecurity/sir/keyfindings/default .aspx
[4] J. Hursti, "Single Sign-On", in Proceeding of Helsinke University of Technology, Seminar on Network Security, 1997.
[5] Aloul.F, Zahidi.S, EI-Hajj.W, "Two factor authentication using mobile phones" Computer Systems and Applications(AICCSA 2009), pp. 641644,May 2010
[6] A.Vapen, D.Byers and N. Shahmehri, "2-c1ickAuth – optical challenge response authentication," in Proc. Conference on Availability, Reliability and Security (ARES), 2010.
[7] “Symposium on 3D Data Processing, Visualization and Transmission (3DPVT'04)”, pp. 258- 261, September 2004.