

# INFORMATION SECURITY THROUGH VIDEO STEGNOGRAPHY

Pranjali Kuche<sup>1</sup>, Kimaya Taru<sup>2</sup>, Supriya Supekar<sup>2</sup>, Suvarna Erande<sup>2</sup>, Vrushali Mahalim<sup>2</sup>

<sup>1</sup> Professor, Information Technology, MMCOE, Karvenagar, Pune, Maharashtra, India

<sup>2</sup> Student, Information Technology, MMCOE, Karvenagar, Pune, Maharashtra, India

## ABSTRACT

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. 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. This paper focus the idea of computer forensics technique and its use of video steganography in both investigative and security manner.

**Keyword:** - Advanced Encryption Standards(AES), Stego-video, Steganography, Stego-analysis, Least Significant Bit (LSB), Embed, Authentication Frame, Forbidden Zone Data Hiding(FZDH), Peak Signal to Noise Ratio (PSNR) Encryption, Block Selection

## 1. INTRODUCTION

To produce a robust system that provides security and privacy for critical information files through encryption and embedding of data into a frame of video file and to prevent unauthorized persons from becoming aware of the existence of a message we work on hiding image and text behind video file and extracting data from a video file at receiver side we use steganography. When transmitting data over the network, it is likely to be intercepted by a third party for traffic analysis or active attacks. This is where encryption comes in to the scenario. But many advanced technologies provide encryption detection and decoding of such messages. Other option for secure transmission of data is data hiding, which alone is not sufficient to safely deliver critical information. Therefore, to overcome such limitation, we intend to device a unique solution that combines encryption as well as hiding of message in a frame of a video file. Using a video file adds to the robustness of the system as the interceptor is unlikely to know the frame division, frame number and the decryption key all at once.

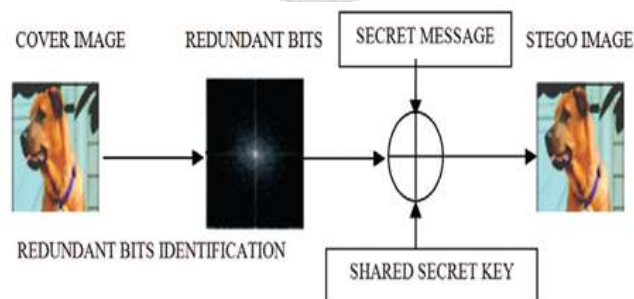


Figure 1. Generating a Stego-Image[2]

## 2. RELATED WORK

The paper discusses the optical crypto techniques with adaptive steganography for video sequence cryptography having more hiding capacity and security. The paper provides implementation of two level encryption of user data by combining two areas of network security, cryptography and steganography [6]. Author also discusses the combination of LSB technique with XORing method, which gives additional level of security [6]. A simple steganography method is to take the individual pixels in an image. Each of these pixels is made up of a string of bits. The paper suggested, the 4LSB of 8 bit true color image to hold 4 bit of our secret message by simply overwriting the data that was already there [7]. As quantization level are increased the PSNR value also increase [8]. To compare the performance of a given method, a metric should be adopted and applied twice: to compare cover images before (initial cover) and after encoding (stegno image) and to compare initial object with the reconstructed object after decoding. The paper provides a new video data hiding method that makes use of erasure correction capability of repeat accumulate codes and superiority of forbidden zone data hiding [9]. The paper provided the robust method of imperceptible audio, video, text are image hiding, this techniques are efficient for sending secure data from sender to receiver [10].

## 3. METHODOLOGY

- Select video file.
- Select any audio-video file, behind which user wishes to hide data.
- Separate audio and video from that file.
- Separate audio and video from selected video file using available software FFM- PEG. Separate all frames of video file. Get frame number from user behind which an authentication image is to be hidden.
- Select the text for data hiding.
- Select the data which you want to securely transfer to receiver side. AES algorithm is applied before embedding data in an image. Data encrypted before sending to server using AES algorithm.

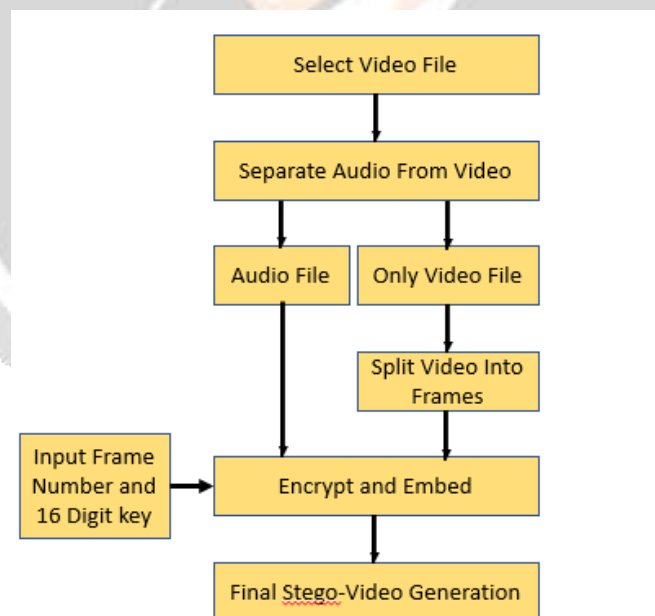


Figure 3.1. Generating a Stego Video

- Generate stego video.
- Data which is encrypted is hidden in authentication image using LSB steganography method. Read authentication image. This 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. This forms a stego frame overwriting this stego frame with original video file create stego video file.

• Combine stego audio and stego video file using 'cute audio video merger' soft-ware. This forms the stego audio video file at transmitter site which has hidden text and image in it. •Receive audio-video file and decode authentication image from video.

•After transmission of the stego audio video file obtained at receiver side. Read the stego audio video file. 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). Authentication image data is available at LSB of frame is recovered. Select the authentication image at receiver side compare recovered authenticated image with the selected image. If both the images matched, then only user can recover the text behind audio else process is terminated.

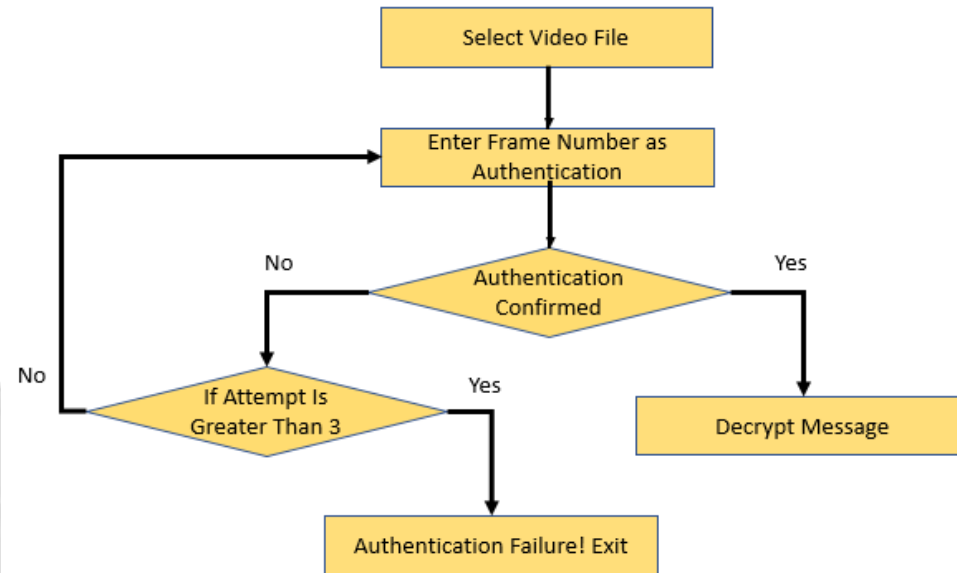


Figure 3.2. Authentication during recovery of hidden data

## 4. TECHNOLOGIES USED

Forbidden Zone Data Hiding (FZDH) is used along with Advanced Encryption Standard (AES) and 4-Least Significant Bit (4LSB) algorithms. A brief insight of their working is explained below.

### 4.1 FZDH

A block based data hiding framework that uses FZDH is proposed here. Selective embedding is utilized in the proposed method to determine host signal samples suitable for data hiding[3]. By means of simple rules applied to the frame markers, we introduce certain level of robustness against frame drop, repeat and insert attacks. The main high resolution video file is nothing but a sequence of high resolution image called frames. Initially we will like to stream the video and collect all the frames in bitmap format. And also, collects the following information:

1. Starting frame: It indicates the frame from which the algorithm starts message embedding.
2. Starting macro block: It indicates the macro block within the chosen frame from which the algorithm starts message embedding.
3. Number of macro blocks: It indicates how many macro blocks within a frame are going to be used for data hiding. These macro blocks may be consecutive frame as per a predefined pattern. Apparently, the more the macro blocks we use, the higher the embedding capacity we get. Moreover, if the size of the message is fixed, this number will be fixed, too. Otherwise it can be dynamically changed.

### 4.2 AES

The AES algorithm is most secure and robust cryptographic algorithm against attacks. Unlike the Data Encryption Standard (DES) which is slower and is already broken and produces inefficient software code. Triple DES on the other hand is comparatively slower than DES as it has three more rounds AES has symmetric block

cipher and hence uses same key for encryption and decryption. AES selection criteria are based on three main criteria: safety, cost, and characteristics factor of implementation[4]. The block size of AES varies from 128, 192, and 256 bits, the substitution and permutation are performed in AES. The number of rounds depends upon the key length i.e. 10 rounds for 128bit key, 12 for 192bit key and 14 for 256bit key. The next stage is to perform actual steganography where this secret data is to be hidden in the carrier video.

### 4.3 4-LSB

One of the most common techniques used in steganography today is called least significant bit (LSB) insertion [5]. The idea of the LSB algorithm is to insert the bits of the hidden message into the least significant bits of pixels. An extremely simple steganography method is to hide the information at pixel level. Each frame or image is made up of number of individual pixels. By experimentation, it has been proved that the impact of changing the 4 least 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) image is given by the following equation:

$$\text{Total size of one frame} \div 8 \text{ ————— (1)}$$

Suppose size of a single frame is 160KB, then for 1LSB, maximum data that can be hidden is  $1 \times 20 \text{KB} = 20 \text{KB}$ . For 2LSB it is  $2 \times 20 \text{KB} = 40 \text{KB}$ . For 3LSB it is  $3 \times 20 = 60 \text{KB}$ . For 4LSB it is  $4 \times 20 \text{KB} = 80 \text{KB}$ .

## 5. EXPERIMENTAL RESULTS

The proposed system accepted a video file as input and split it into frames and audio. The next step is to provide the key and the frame number in which the data is to be hidden. Once that is done, the data can be encrypted and embedded into the frame and the final stego-video is generated by combining the altered frames and audio. On the receiver side, authentication in the form of frame number is required for the receiver to be able to decrypt the file and view the data.

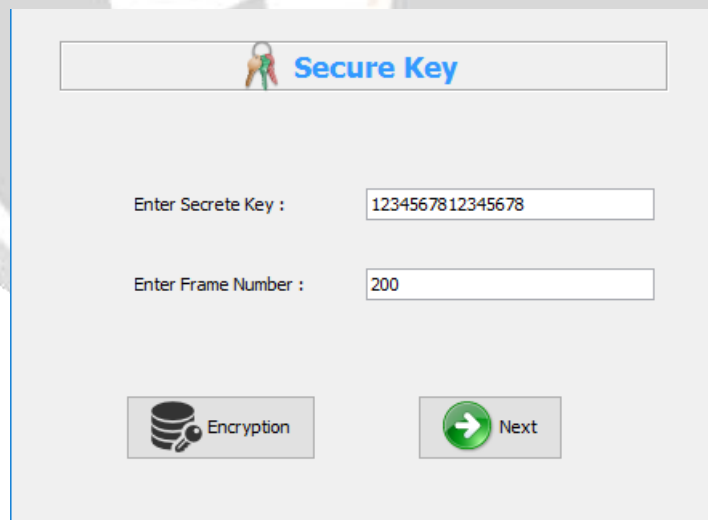


Figure 6.1. Entering 16digit key and frame number



Figure 6.2. Input data to be hidden

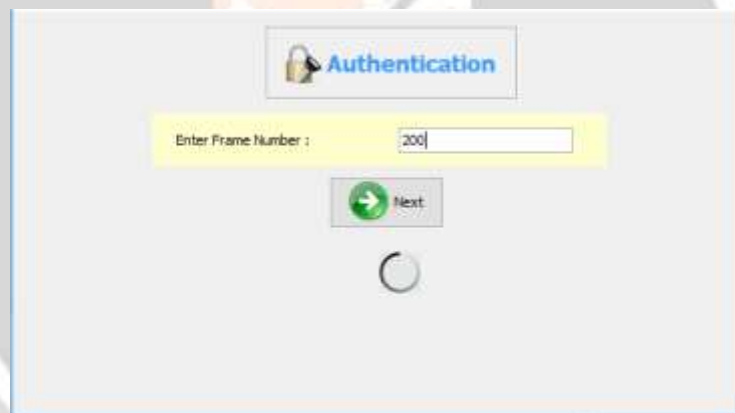


Figure 6.3. Receiver authentication

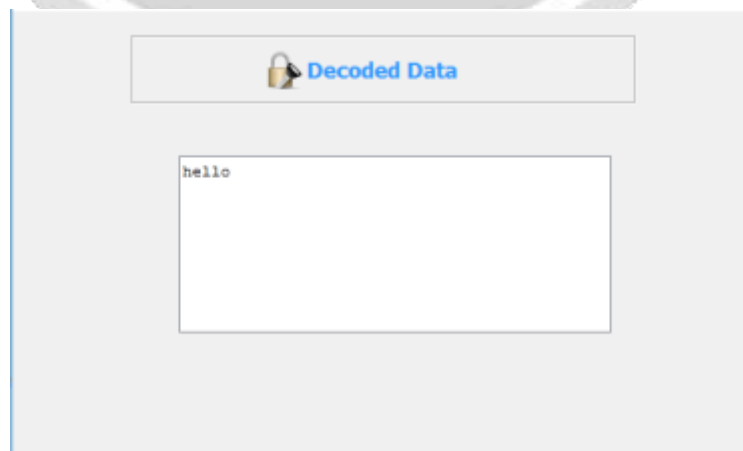


Figure 6.4. Decoded Message

## 6. CONCLUSIONS

After studying number of techniques for hiding information in digital media, we focus our concern in image because of its wide use. Securing the secret data by embedding it in audio-video file with AES as encryption algorithm is providing high security. We are hiding an encrypted secret file or message behind a video frame using 4LSB method. Comparative study suggests, 4-LSB substitutions as a good method for embedding an acceptable amount of data, that's because this algorithm permits a better size ratio of embedded message to carrier's size. 4-LSB data embedding, can be easily implemented and does not visually degrade the image to the point of being noticeable. Furthermore, the encoded message can be easily recovered. Using 4-LSB method we can exchange secret messages over public channel in a safe way. This proposed method can also withstand different attacks and thus is a very strong and secure method of data hiding can be obtained.

## 7. ACKNOWLEDGEMENT

We take this opportunity to thank our project guide Prof. Pranjali Kuche and Head of the Department Prof. Rupali Chopade for their valuable guidance and for providing all the necessary facilities, which were indispensable in the completion of this project report. We are also thankful to all the staff members of the Department of Information Technology of Marathwada Mitra Mandal's College of Engineering, Pune for their valuable time, support, comments, suggestions and persuasion. We would also like to thank the institute for providing the required facilities, Internet access and important books.

## 8. REFERENCES

- [1]. Qingzhong Liu, Andrew H. Sung, and Mengyu Qiao, "Secure Data Hiding in Audio-Video Steganalysis by Anti-Forensics Technique", IEEE Transactions, Vol. 4, July 2016
- [2]. Babloo Saha, Shuchi Sharma, "Steganographic Techniques of Data Hiding using Digital Images", Defence Science Journal, Vol. 62, Jan 2012
- [3]. Ersin Esen ad Aydin Alatan, Member, IEEE, "Robust Video Data Hiding Using Forbidden Zone Data Hiding and Selective Embedding", IEEE Transactions, Vol. 21, August 2011
- [4]. Nurhayati, Syukri Sayyid Ahmad, "Steganography for Inserting Message on Digital Image Using Least Significant Bit and AES Cryptographic Algorithm", Syarif Hidayatullah State Islamic University (UIN) Jakarta, Indonesia
- [5]. Anil Kumar, Rohini Sharma, "A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique", IJARCSSE, Vol. 3, July 2013
- [6]. V.Sathya, k Delforouzi "LSB based steganography method based on lifting wavelet transform" 2007 IEEE International symposium on signal processing and information technology, pp600-603.
- [7]. Alkhraisathabes. "Information Hiding in BMP Image Implementation, analysis Evaluation" Information transmission in computer network, fall2006, Volume 52, issue, pp.1-10
- [8]. SghierGuizani, Nidal Nasser, "An Audio/Video Crypto Adaptive Optical Steganography Technique" IEEE 2012 2012, pp, 1057-1062.
- [9]. Ersin Esen and A. Aydin Alatan, Member, IEEE, "Robust Video Data Hiding Using Forbidden Zone Data Hiding and Selective Embedding" IEEE transactions on circuits and systems for video technology, vol. 21, no. 8, august 2011.
- [10]. Balsubramaniam, N, Murali, "Data hiding in audio signal, video signal text and JPEG Image", IEEE ICAESM 2012, March 30-3-2012, pp741-746