Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 6, June 2016, pg.401 – 406

Application of Data Hiding in Audio-Video Using Advance Algorithm

[1]Ketki Deshpande, [2]Nagesh Kamble
[1]Department of Computer Science & Engineering
[2]Department of Computer Science & Engineering
[1]Shreeyash College of Engineering & Technology, Aurangabad
[2]Shreeyash College of Engineering & Technology, Aurangabad
[1] ketki.deshpande17@gmail.com, [2] nageshce@gmail.com

Abstract: Steganography means a method for hiding secret information for example password, text or image inside a cover file. The existing system provides audio-video crypto-steganography which is the combination of image steganography and audio steganography using forensics technique as a tool to authentication. Our aim is to hide secret data in the audio and image of a video file. Video has so many still frames of image and audio, we can select any frame for hiding our data.

Video data hiding is a very important research topic. We propose a new video data hiding method that makes use of correction capability of repeat accumulate codes and superiority of forbidden zone data hiding (FZDH). FZDH is used for no alteration is allowed while data hiding process.

Keywords: Steganography, LSB, data hiding, FZDH, PSNR

I. INTRODUCTION

"The goal is to integrate all these Data Security and Authentication techniques for secured communication of two parties and maintain secrecy". Our Moto is to secure communication over geographically distributed area and avoid cyber crime. Video is collection of still frame images and also consists audio, we choose it as a carrier media for data transmission. Suitable algorithm such as 4LSB is used for image steganography and Phase coding algorithm for audio steganography. As addition we introduced FZDH (Forbidden zone data hiding) to avoid alteration of data during process of data hiding and also cropping attack. With this proposed system and use of FZDH can upload video file with any format (such as .4mp, .3gp, .avi) as a cover file. Security parameters and authentication like histogram, PSNR can be obtained at receiver and transmitter side which are exactly identical, thus increasing data security.

II. EXISTING SCHEME

In existing system investigated adaptive mechanisms for high-volume transform-domain data hiding in MPEG-2 video which can be tuned to sustain varying levels of compression attacks. The data is hidden in the uncompressed domain by scalar quantization index modulation (QIM) [7] on a selected set of low-frequency discrete cosine transform (DCT) coefficients. It propose an adaptive hiding scheme where the embedding rate is varied according to the type of frame and the reference quantization parameter (decided according to MPEG-2 rate control scheme) for that frame. For a 1.5 Mbps video and a frame- rate of 25 frames/sec, It is to embed almost 7500 bits/sec. Also, the adaptive scheme hides 20% more data and incurs significantly less frame errors (frames for which the embedded data is not fully recovered) than the non-adaptive scheme.

III. PROPOSED SCHEME

In this paper, 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 technique 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 cryptostegnography 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 center the thought using so as to send expansive information FZDH[6].

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

- Quality of video file is strictly preserved even after secret data embedding.
- Ability to encrypt and decrypt the data with the images
- With this system, an image, after hiding the data, will not degrade in quality
- More information can be stored in an image.

IV. SYSTEM ARCHITECTURE

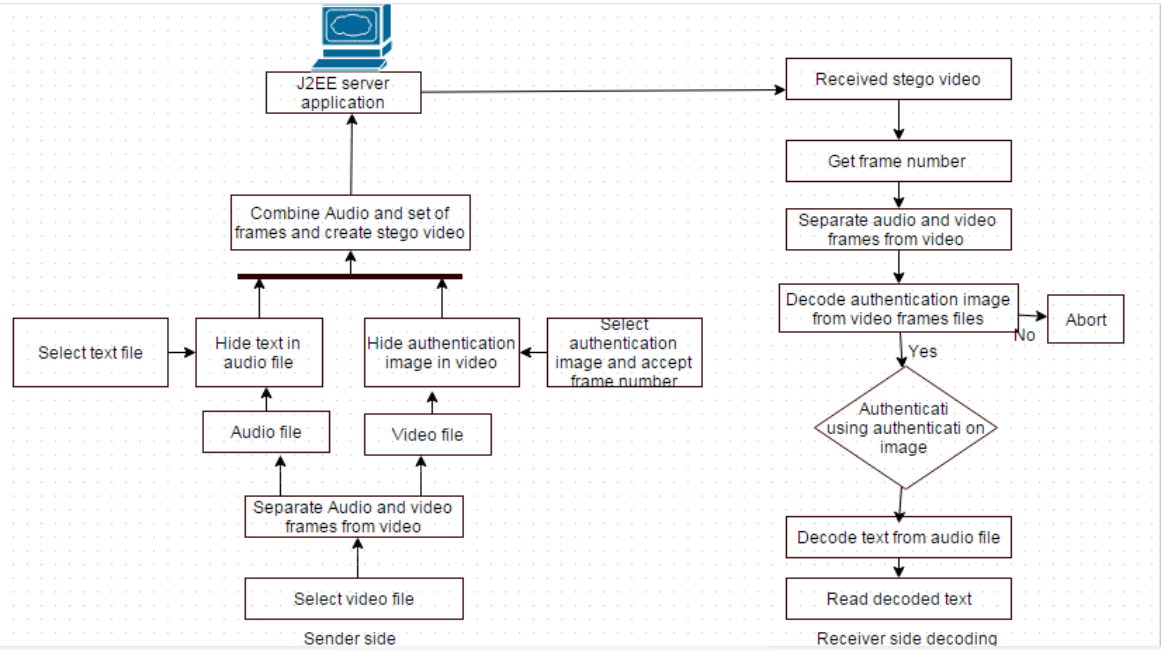

Fig 1.1 System Architecture

V. IMPLEMENTATION AND EXPERIMENTAL RESULTS

A. Implementation

1) *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 its Cipher and Inverse Cipher, the AES algorithm uses a round function that is composed of four different byte-oriented transformations:

- Byte substitution using a substitution table (S-box)
- Shifting rows of the State array by different offsets
- Mixing the data within each column of the State array
- 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.

- Inverse Shift Rows
- Inverse Sub Bytes
- Inverse Mix Columns
- 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).

2) *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.

- 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.
- 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 (mx 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, 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.
- For implementing steganography proposed method is using 4LSB algorithm. Any data change in least significant bit does not change the value of data significantly.

3) *Forbidden Zone Data Hiding :* Each round consists of several processing steps, each containing four similar but different stages, including one that depends on the encryption key itself. A set of reverse rounds are applied to transform cipher text back into the original plaintext using the same encryption key.

- Data hiding in video sequences is performed in two major ways: bit stream-level and data-level.
- It proposes a new block-based selective embedding type data hiding framework that encapsulates Forbidden Zone Data Hiding (FZDH)
- 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 collect the following information:

- Starting frame: It indicates the frame from which the algorithm starts message embedding.

- Starting macro block: It indicates the macro block within the chosen frame from which the algorithm starts message embedding.
- 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 according to 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.
- Frame period: It indicates the number of the inter frames, which must pass, before the algorithm repeats the embedding. However, if the frame period is too small and the algorithm repeats the message very often, that might have an impact onto the coding efficiency of the encoder [8].

Apparently, if the video sequence is large enough, the frame period can be accordingly large. The encoder reads these parameters from a file. The same file is read by the software that extracts the message, so as both of the two codes to be synchronized.

After streaming the video file into frames we will like to use the conventional LSB replacement method. LSB replacement technique has been extended to multiple bit planes as well. Recently[9] has claimed that LSB replacement involving more than one least significant bit planes is less detectable than single bit plane LSB replacement. Hence the use of multiple bit planes for embedding has been encouraged. But the direct use of 3 or more bit planes leads to addition of considerable amount of noise in the cover image. Still as my work is in high resolution video so we are getting a RGB combination of each pixel hence if we consider one LSB we will have a choice of 3 bits for each pixel. That will overcome the clam of [10]. And will give a higher security of the Data Hiding method.

B. Experimental Results

The most important factor on steganography system is Peak Signal Ratio to Noise Ratio (PSNR). PSNR represents quality of image i.e. the higher the PSNR lower is the difference between cover image and stego image. The measurement of the quality between the cover image f and stego image g sizes N×N is defined by PSNR as

$$\text{PSNR} = 10 \times \log(255^2 / \text{MSE})$$

where

$$\text{MSE} = 1/mn \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [f(x,y) - g(x,y)]^2$$

Here, MSE represents Mean Squared Error and f(x,y) and g(x,y) represent the pixel value at the position (x,y) in the cover image and the stego image respectively. The goal of the stego system is to achieve high PSNR value inorder to make steganography successful.

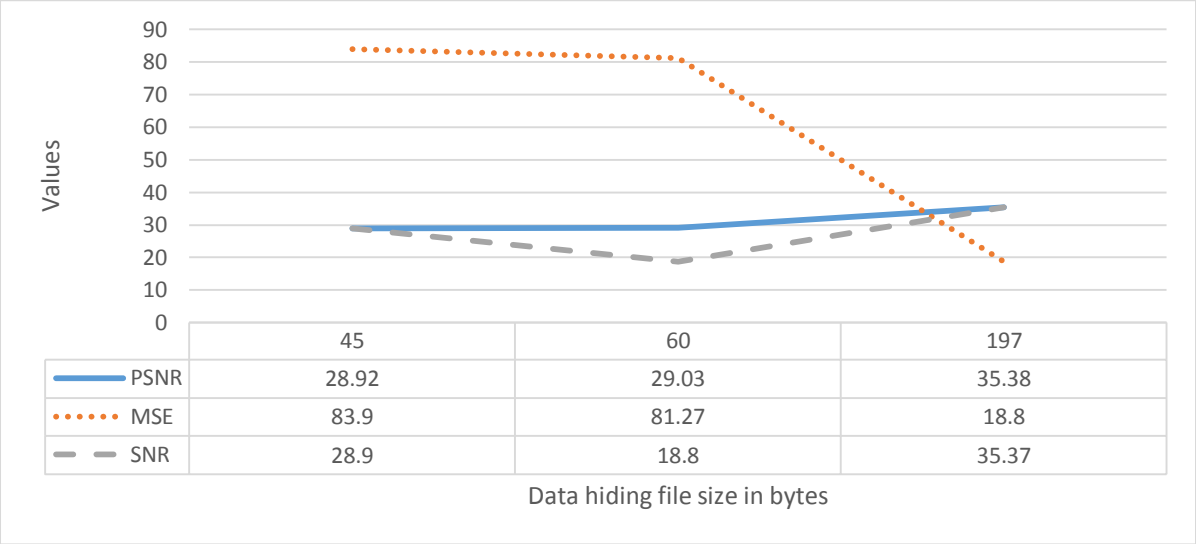

Table 1: Shows the different data security parameters

VI. CONCLUSION

A new video data hiding framework that makes use of erasure correction capability of RA codes and superiority of FZDH. The method is also robust to frame manipulation attacks via frame synchronization markers. First, we compared FZDH and QIM as the data hiding method of the proposed framework. We observed that FZDH is superior to QIM, especially for low embedding distortion levels. Typical system parameters are reported for error-free decoding. The results indicate that the framework can be successfully utilized in video data hiding applications.

REFERENCES

1. Ali M Ahmad, Ghazali Bin Sulong, Mohd.Shafry, B.Mohd.Rahim, Saparudin (April 2012), A 2-tier Data Hiding Technique Using Exploiting Modification Direction Method And Huffman Coding, *ACEEE Int. J. on Information Technology*, Vol. 02, No. 02
2. Vijay Kumar Sharma, Vishal Shrivastava (February 2012), A Steganography Algorithm For Hiding Image In Image By Improved LSB Substation By Minimise Detection, *Journal of Theoretical and Applied Information Technology*, Vol. 36 No. 01
3. Johnathan Cummins, Patrick Diskin, Samuel Lau, Robert Parlett, Steganography: The Art of Hiding, *School Of Computer Science, The University Of Birmingham.*
4. B.Chen, G.W.Wornell,(May 2001), Quantization Index Modulation: A Class Of Probably Good Method For Digital Water Marking And Information Embedding, *IEEE Transactions on information theory*, Vol. 47, pp 1423-1443
5. Nagesh D. Kamble, J.Dharani, (2014), Implementation of Security Systems Using 3- Level Authentication, *IJEDR*, Vol.2 Issue 2.
6. E. Esen and A. A. Alatan, "Forbidden zone data hiding," in IEEE International Conference on Image Processing, 2006, pp. 1393—1396.
7. A. Sarkar, U. Madhow, S. Chandrasekaran, and B. S. Manjunath, "Adaptive MPEG-2 Video Data Hiding Scheme," in Proceedings of SPIE Security, Steganography, and Watermarking of Multimedia Contents IX, 2007.
8. Jonathan Cummins, Patrik Diskin, Somuel Lau, Robert Parlett, "Steganography: The Art of Hiding", School of computer Science,The University of Birmingham.
9. Spyridon K. Kapotas, Eleni E. Varsaki and Athanassios N. Skodras, "Data Hiding in H.264 Encoded Video Sequences", IEEE 9th Workshop on Multimedia Signal Processing, October 1-3, 2007, Crete, pp. 373-376 .
10. A. Ker,"Steganalysis of Embedding in Two Least-Significant Bits", IEEE Trans. on Information Forensics and Security, vol. 2, no. 1, March 2007, pp. 46-54.

