International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

Application of Data Hiding in Audio-Video using Advance Algorithm

Ketki Deshpande†* and Nagesh.D Kamble†

†Department of Computer Science & Engineering, Shreeyash College of Engineering & Technology, Aurangabad, India

Accepted 26 Dec 2015, Available online 28 Dec 2015, **Vol.5, No.6 (Dec 2015)**

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*

1. Introduction

Digital communication has become an important part of infrastructure now a days, a lot of applications are Internet based and in some cases it is required that, the communication should be made secret. To achieve this secrecy there are available:

a) Cryptography and
b) Steganography

Cryptography is a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data for to keep the message secret (Ali M Ahmad, Ghazali Bin Sulong,Mohd.Shafry,B.Mohd.Rahim,Saparudin,2012). Unfortunately in some cases it is not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message to be secret (Vijay Kumar Sharma, Vishal Shrivastava,2012).The technique used to implement this process is called Steganography. Steganography is nothing but the invisible communication. The word steganography is derived from the Greek word 'Stegos' meaning 'Cover' and 'Grafia' meaning 'writing' defining it as "covered writing"(Johnathan Cummins, Patrick Diskin, Samuel Lau, Robert Parlett,).

In the steganography the information is hidden completely in images. Steganography is differs from cryptography targets on keeping the contents of a message secret while the steganography focuses on keeping the existence of a message to be secret. Cryptography and steganography are both ways to protect information from unauthority parties but neither technology alone is perfect and can be compromised. Once the existence of secret message is revealed or even suspected, the use of steganography is partly defeated. The strength of steganography can be amplified by combining it with cryptography.

In this paper, we propose a new block based selective embedding type data hiding framework that encapsulates Forbidden Zone Data Hiding (FZDH) and Repeat Accumlate (RA) codes in accordance with an additional temporal synchronization mechanism. FZDH is a practical data hiding method which is shown to be superior to the conventional Quantization Index Modulation (QIM)(B.Chen,G.W.Wornell,2001).RA codes are already used in image and video data hiding due to their robustness against erasures. This robustness allows handling desynchronization between embedded and decoder that occurs as a result of the differences in the selected coefficients. In order to incorporate frame synchronization markers, we partition the blocks into two groups. One group is used for frame marker embedding and the other is used for message bits. By means of simple rules applied to the frame markers, we introduce certain level of robustness against frame drop, repeat and insert attacks. We utilize systematic RA codes to encode message bits and frame marker bits. Each bit is associated with a block residing in a group of frames. Random interleaving is performed spatio-temporally; hence, dependency to local characteristics is reduced. Host signal coefficients used for data hiding are selected. Next, only some predetermined low frequency DCT coefficients are permitted to hide data.

*Corresponding author: **Ketki Deshpande**

Then the average energy of each coefficient is compared against another threshold. The unselected blocks are labelled as erasures and they are used to embed and decode single message bit by employing multi-dimensional form of FZDH that uses cubic lattice as its base quantizer.

2. Existing Scheme

Least significant bit (LSB) is the simplest form of Steganography. LSB is based on inserting data in the least significant bit of pixels, which lead to a slight change on the cover image that is not noticeable to human eye. Since this method can be easily cracked, it is more vulnerable to attacks.

LSB method has intense effects on the statistical information of image like histogram. Attackers could be aware of a hidden communication by just checking the Histogram of an image .A good solution to eliminate this defect was LSB matching was a great step forward in steganography methods and many others get ideas from it.

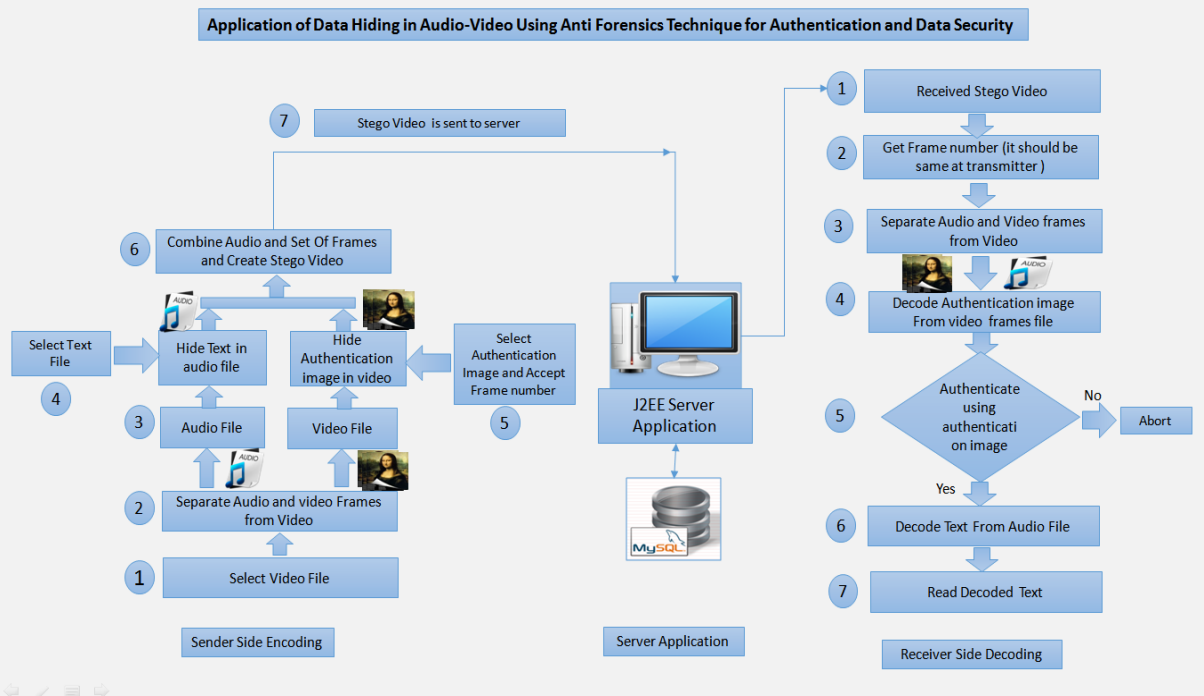

Fig: Block Diagram of Existing System

Below are the major steps involved in the existing system

1) Selecting Video File
2) Data Encryption Using AES Algorithm
3) Encrypted Data Hiding in video Using LSB steganography
4) Creating stego audio file
5) Authentication(at receiver side)
6) Audio Recovery

3. Proposed Scheme

Data hiding in video sequences is performed in two major ways: bit stream level and data level. In this paper, we propose 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.

- User cannot find the original data.
- It is not easily cracked.
- To increase the security.
- To increase the size of stored data.
- We can hide more than one bit.

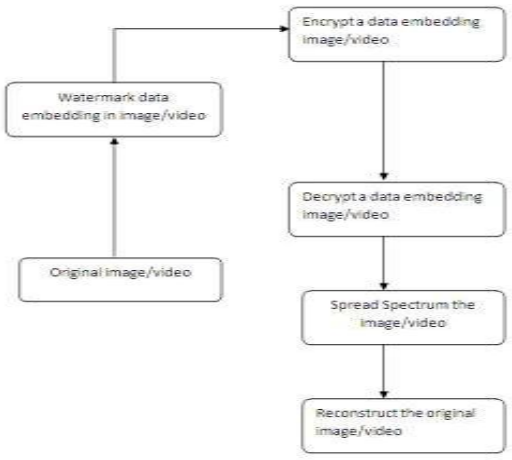

Fig: Block Diagram

References

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

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

Johnathan Cummins, Patrick Diskin, Samuel Lau, Robert Parlett, Steganography: The Art of Hiding, *School of Computer Science, The University of Birmingham.*

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

Nagesh D. Kamble, J.Dharani, (2014), Implementation of Security Systems Using 3- Level Authentication, *IJEDR,* Vol.2 Issue 2