International Journal of Linguistics and Computational Applications (IJLCA) ISSN 2394-6385 (Print)
Volume 4, Issue 4, October – December 2017 ISSN 2394-6393 (Online)

Video Steganography and Security Cryptography

C. Ezhilarasi[#1], R.Anitha[#2]

[1]*Student, Master of Computer Application, S.A Engineering College, Chennai-77*
ezhil04chandran@gmail.com
[2]*Asst. Prof., Master of Computer Application, S.A Engineering College, Chennai-77*

Abstract— Today's world is growing rapidly over internet technologies. Steganography play an important role in the field of information security [1]. Video and images are very common choice for hiding data. In Visual cryptography we upload an image and embed encrypted data into color component using LSB audio steganography .The advantage of video cryptography is that, large amount of data can be hidden inside and the fact that it is a moving stream of images [2]. The data security approach when combined with encryption and steganography techniques for secret communication by hiding it inside the multimedia file. The data is hidden in horizontal and vertical components of the moving objects. The file such as images, audios and videos contains collection of bits that can further be translated into images, audios and videos. The file composed of insignificant bit and unused areas which can be used for overwriting of other data. This paper explains the algorithm using video steganography for enhancing data security. Key frame extraction technique is new in video steganography and is used.

Keywords— *Video Steganography; Protocol; Advanced Encryption Standard; Visual Cryptography*

1. Introduction

Cryptography system uses symmetric key in which the sender and the receiver has single key. In public key system two keys are used, a public key known to everyone and a private key known to recipient. Nowadays the internet is used mostly in all places. Video and images are very common choice for hiding data. Through video background, the information has been transformed securely. Visual Cryptography allows visual information to be encrypted in such a way that decryption becomes the work of the receiver.

All messages can converted into cipher text by using cryptographic methods. A secure video communication system is used in which multiple encryptions are done at the transmitter side and the corresponding decryption should be done using the key at the receivers end. Multiple encryption gives great security and the data hiding brings additional security.

The system as a whole can be used for secure transmission of digital videos to hide the data in the moving file. To improve the security of data, Advanced Encryption Standard *(*AES) algorithm is used [3] [4].

2. Existing System

The Least Significant Bit (LSB) algorithm in the existing system, which is not efficient, because it hides the message in consecutive bytes received from video files. Video steganography used poses more restrictions on choosing of video files. Texting is the first mode for sending information. Then with the help of Rivest–Shamir–Adleman (RSA) algorithm, information passed through audio in the secure way. Images and color components are also used to hide data and to transmit them to the receivers end.

2.1 Disadvantages

- No provision of encryption key,
- Lack of good user interface,
- Consumes more time to encode and decode the data.

In video steganography, the Data Encryption Standard (DES) algorithm is far slow and is already broken and also produces inefficient software code. These are the disadvantages in the existing system which we should overcome.

3. Proposed System

Enhanced video Steganography is a method of hiding messages in video files of any formats. Many secure transmissions are used nowadays. The texting audio and color images are used for secure transmission of data. Even in video stegnography, different methods are followed for hiding data and to save information. In encryption, block video is first divided into frames by using a video cutter. These frames also contain the audio information.

3.1 Advantages

- User can understand easily.
- Consumes less time to encode and decode
- The AES algorithm is most secure and robust.

4. Methodology

The steganography is the art of hiding data inside another data. Another approach for hiding data is to use network steganography by sending data with the help of network protocol [5] [6]. This focuses on the data security approach

when combined with encryption and hiding data inside the multimedia file. So we propose an algorithm using video steganography for enhancing data security. The uses of video files as a carrier medium for steganography are more eligible as compared to other techniques. The basic model of steganography consists of messages, embedding algorithm and stego key [7][8]. The video steganography is the composition of two phases which are extraction of video files and embedding of secret message. The AES algorithm is used to encrypt secret message. Using AES algorithm we can send the information through video. The AES algorithm is used for secure and robust cryptographic algorithm against attacks. AES has symmetric block cipher and hence uses same key for encryption and decryption.

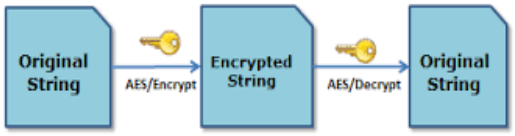

Fig. 1: AES string

The extraction of video files is results in frames. Videos generally composed of still images and audio. So the audio and image frames from the video file are extracted.

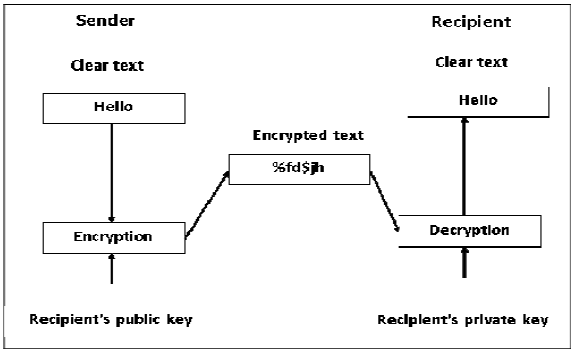

Fig. 2: Message passing using encryption and receiving decryption file

5. Implementation

The main problem with sending data over the internet is security threat. The personal or confidential data can be stolen or hacked. It is very important to take data security into consideration, as it is one of the most hiked factors that need concentration during the process of data transferring. Here we propose a system "Data security using video steganography" which prevents the user from any kind of hacking data. We use texts, images, audios and videos for hiding the secret data inside the cover medium. AES is the algorithm proposed for encryption which results in more secure technique for data hiding.

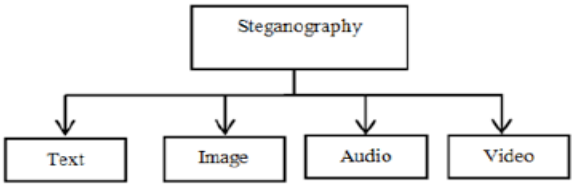

Fig. 3: Video is playing with the help of text, image and audio

6. Result

The Video steganography is used to transfer the information from one end to the other end by using AES algorithm. There are several techniques and metrics that can be measured objectively and automatically and also evaluated by a computer program. In this paper, information has been passing through video by using AES Algorithm through image, audio and video. The messages are embedded into cover image using encryption and decryption.

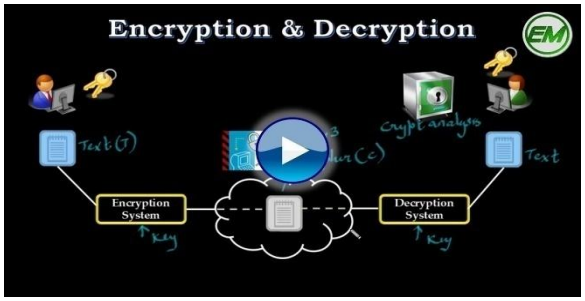

Fig. 4: Text message passing through two keys

7. Conclusion

AES algorithm is used to pass secret information through a video from sender to receiver. AES algorithm is used against secure and also robust cryptographic attack. Steganography can be classified based on many criteria and one among them is based on the type of cover media. Video is the collection of images combined with audio. All videos under this category can be used for video stegnography. This can be used in security system as future research work.

References

[1] Manoj Kumar Ramaiya ,Naveen Hemrajani, AnilKishor Saxena, "Security Improvisation in image Steganography using DES",3rd IEEE Trans. International Conference IACC -2013, Page(s): 1094 – 1099.

[2] Manoj Kumar Ramaiya, Naveen Hemrajan Anil Kishor Saxena, Monika Sharma "Image Stenography: Self Extraction Mechnanism", UACEE International Journal of Advances in Computer Science and its Applications-IJCSIA Vol -3, Issue -2 , Page(s): 145-148, 2013.

[3] C. Shi and Bhargava, "A Fast MPEG Video Encryption Algorithm", Proceedings of 6th ACM International Multimedia Conference ,Bristol, UK, pp. 81-88, September 1998.
[4] C. Shi and Bhargava, "A Fast MPEG Video Encryption Algorithm", Proceedings of ACM International Multimedia Conference, Bristol, UK, pp. 81-88, September 1998.
[5] Neil F. Johnson, Sushil Jajodia, "Exploring Steganography: Seeing the Unseen", IEEE, Feb1998, pp. 26-34.
[6] F. Piper, "Basic Principles of Cryptography", IEEE Colloquium on Public uses of Cryptography, April 1996, pp. 2-3.
[7] Dr. R. Sridevi, Vijaya Lakshmi Paruchuri, K.S. Sadasiva Rao, "Image Steganography combined with Cryptography", International Journal of Computers & Technology, Vol.9, July 2013, pp. 976-984.
[8] Lokesh Kumar, "Novel Security Scheme for Image Steganography using Cryptography Technique", Inter. Jour. of Advanced Research in Computer Sci. & Software Engineering, Vol.2,April 2012,pp. 143-146.