Novel Approach towards Higher Security Using Crypto-Stego Technology

Minal Rawde[1], Mousami Kumbhare[2], Sanika Chaudhari[3], Shital Bhongade[4], Vaishali Bhagat[5]

[1]Dept. of Computer Science and Engineering, S.R.M.C.E.W. Nagpur, Maharashtra, India

[2]Dept. of Computer Science and Engineering, S.R.M.C.E.W. Nagpur, Maharashtra, India

[3]Dept. of Computer Science and Engineering, S.R.M.C.E.W. Nagpur, Maharashtra, India

[4]Dept. of Computer Science and Engineering, S.R.M.C.E.W. Nagpur, Maharashtra, India

[5]Asst. Professor, Dept. of Information and Technology, S.R.M.C.E.W., Nagpur, Maharashtra, India[5]

Abstract

Steganography is the method of hiding any text, password, image or file behind an original cover file. In this paper, we propose the audio-video crypto-stego technique which is combination of image steganography and audio steganography, using cryptography as a tool for authentication. Our aim is to hide secret image in encrypted form behind the audio of a video file and its key and authentication behind the frames of video file. As we know video is an application of many still frames of images and audio, we can select any frame of video and signals of audio to hide our secret data. Thus, we are providing a multi-layered security to our secret data. Here, we are using LSB substitution technique for image steganography and location selection for audio steganography. Advanced Encryption standard (AES) is used for encryption and decryption of image.

Keywords: Cryptography, Steganography, LSB, AES

1. INTRODUCTION

Securing information is the most common issue in information technology and communication sector. Therefore, it necessary to provide security to information in such a way that its existence remains secret or no one can decode it. We can secure our information by using any of the two ways: cryptography and/or steganography.

A technique called cryptography, i.e. secret-writing is used to modify the data which is being transmitted. Cryptography is the science of conversion of a “plain” i.e. readable data (text, media) into a “cipher” i.e. unreadable data and thus protecting the communicating data. This consist of two phases, firstly the sender convert the data into cipher data using some algorithm (known as Encryption) and then receiver use the same algorithm to decipher the media (known as decryption). Cryptography’s main part is that the information is somehow misrepresented; the sender uses an encryption key also known only by the intended receiver who decrypts the message. The difficulty with cryptography is that a user obstructs the message so as to prevent them from continuing to destination, although he cannot decrypt it, he might know that there is encrypted, secret information.

Steganography is the method of hiding any text, password, image or file behind an original cover file. In steganography the secret data is hidden in a way that unauthorized persons are not aware of the existence of the embedded data without altering the quality of the cover file. Audio steganography is one of the popular data hiding techniques that embeds secret data in audio signals. Video Steganography is a technique to hide any kind of files into a frame of Video file. The use of the video based Steganography can be more eligible than other multimedia files, because of its size and memory requirements. In this paper, we propose a data hiding technique in which we are hiding secret encrypted image behind audio signals and its encryption key behind the frames of video file thus, transmitting an audio-video stego file.

Our aim is to hide secret data in encrypted form behind the audio of a video file and its key, a username and password used for authentication which is to be hidden behind the frames of video file. As we know video is an application of many still frames of images and audio, we can select any frame of the video to hide our secret data. Thus, we are providing a multi-layered security to our secret data.

2. LITERATURE REVIEW

Arup Kumar Bhaumik, Minkyu Choi, Rosslin J. Robles, and Maricel O. Balitanas, [1] there are three main requirements of any data hiding system i.e. security, capacity and robustness. All these factors are inversely proportional to each other and therefore, it is very difficult to achieve them together. Here, the authors have focused on increasing the two factors, security and capacity of data hiding method. This data hiding scheme uses a high resolution digital video as a cover signal that means a video is embedded behind a video and they have also used an image for authentication. Thus, they have used large payloads like video in video and an image in video as a cover media. The objective of hiding such data depends on the application and the requirements of the user of that digital media.

Prof. D. P. Gaikwad, Trupti Jagdale, Swati Dhanokar, Abhijeet Moghe, Akash Pathak,[2] have stated the fact that steganography can be successfully implemented and used into a next generation of computing technology with image and video processing abilities. They have concentrated on the Video Frame in order to create a stego Video file. They have used LSB method that satisfies the requirement of steganography protocols. In their work, they have included implementation of steganographic algorithm for embedding data inside video files, as well as technique to extract the original data. The proposed work first compresses the secret message depending on its size and then encrypted it, where they have given a password for authentication which will be provided at the time of embedding secret message.

Sunil K. Moon, Rajshree D. Raut, [3] in this work author has aimed to hide secret information behind image and audio of video file. By embedding text behind audio file and an authentication image is embedded behind frames of video file. As video is the application of many still frames of audio and picture (i.e. image), any frame can be selected from video and signals from the audio for hiding secret data. Authors have used 4LSB method for image steganography whereas Phase Coding algorithm for audio steganography. They have tried to increase the security of data by using suitable parameter of security and authentications such as PSNR and histogram that can be obtain at transmitter and receiver side.

Burate D. J., M. R. Dixit, [4] used a new technique for hiding text in speech in noise free environment. They have worked in the digital domain to hide the text information within speech signal using audio steganography technique. Data hiding rate can be increased due to this method. They have maintained the originality of the speech carrier signals by embedding the secret text rather than performing replacement operation on it. They have combined steganography with cryptography to increase security of the system, but instead of using any of the cryptography technique, they have used coding techniques in this method. Due to this approach the robustness of the cover signal is maintained and a higher hiding capacity for different audio and speech signal sampled at different frequencies is achieved as well as read at different bit rates. So this method provides higher hiding capacity as compared to other techniques.

Padmashree G, Venugopala P S, [5] the important properties for audio steganography are transparency, capacity and robustness. These properties make steganography more secure because it has less quantization errors. An encoding mechanism is used for embedding the message into the audio file. The secret message is embedded in the 4th bit of LSB this reduces the embedding distortion of the host audio. Similarly, embedding at the 4th and 5th bit LSB of the original audio file with same data and different data also reduces distortion of the host audio. The quality of the audio file after encoding remains unaffected. A public key cryptographic algorithm, RSA was also used to ensure greater security.

K. A. Navas, Vidya V, Soniya V Dass, [6] have developed an algorithm for data embedding in AVI videos. In this method the secret data is embedded within the cover video in two phases. The first phase uses a new embedding method for self-generation of a key which depends on the data to be embedded and the cover media. In the second phase, the encrypted image is embedded in a video. This method uses high resolution digital video as a cover signal for embedding data. Thus, this method gives the ability to hide a significant quality of information which makes it different from the other data embedding methods because the authors have considered an application that requires significantly larger payloads like video-in-video and image-in-video.

3. PROPOSED WORK

We are combining cryptography and steganography for hiding color image in audio-video file. The audio file is embedded with an encrypted image and its key is embedded in the frame of its video part. The video frame also embeds a username and password for authentication purpose. Here, LSB substitution technique is used for steganography and AES algorithm is used for cryptography.

Sender's side: A colorful image of any resolution is selected and converted into a gray scale image. This gray scale image is encrypted using 16 bit key (According to the AES algorithm). Then, an audio-video file is selected and audio part and frames are extracted from this selected file. The audio signals are embedded with the encrypted grey scale image and the 16 bit key is embedded in one of the frames of the video file. Also the frame embeds a username and password. All this is done with the help of LSB substitution technique. This stego audio and stego video files are combined and transmitted over the network towards the recipient.

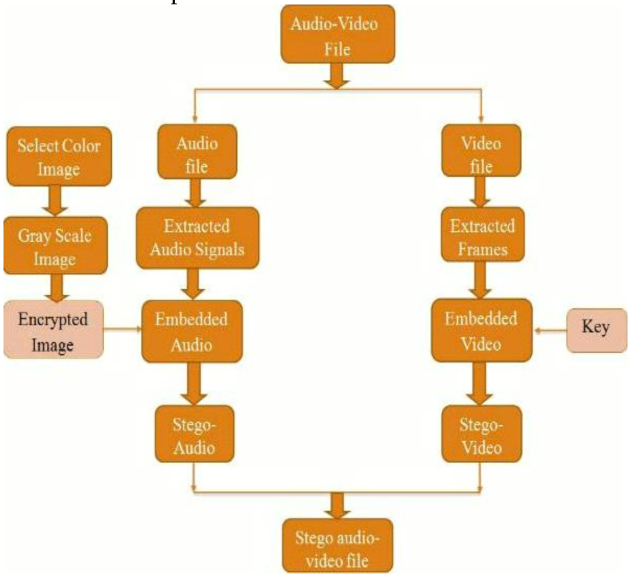

Fig1: Sender side

Receiver's side: The receiver extracts the audio and video part from the received stego audio-video file. The username and password is used for authentication purpose in stego-video part. This makes the recipient available with the 16bit key (which is being used by the sender for encryption purpose). The key is used for decrypting image which is being extracted from the stego audio file and thus the original secret image is obtained by recipient.

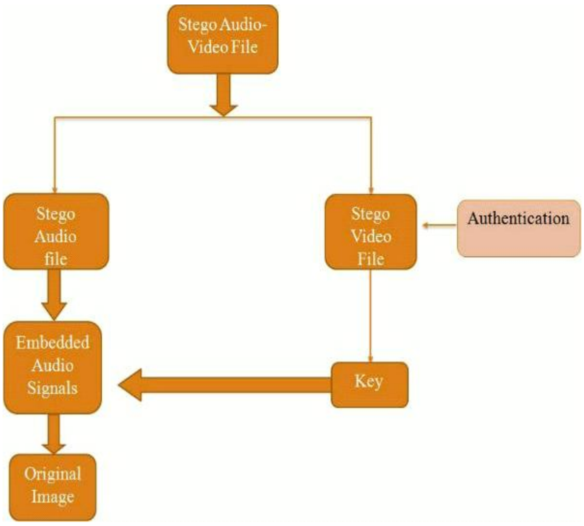

Fig2: Receiver side

4. METHODOLOGY

4.1 AES Encryption Process

The encryption process uses a set of specially derived keys which is called as round key.

You take the following steps to encrypt a 128-bit block:

- Derive the set of round keys from the cipher key.
- Initialize the state array with the block data i.e. plaintext
- Add the initial round key to the starting state array.
- Perform nine rounds of state manipulation.
- Perform the tenth and final round of state manipulation.
- Copy the final state array out as the encrypted data i.e. cipher text.

When cipher message is processing based on bit the loops will for 9, 11, and 13 if there are 128, 192, 256 bit respectively and final round is different (10th, 12th, 14th). The final round has certain process:

- Sub bytes
- Shift rows
- Mix columns
- Add round key

4.2 LSB Technique

“One of the earliest techniques studied in the information hiding of digital audio (as well as other media types) is LSB coding. In this technique LSB of binary sequence of each sample of digitized audio file is replaced with binary equivalent of secret message.”

Least significant bit (LSB) coding is the easiest way to embed information in a digital audio signal. By substituting the least significant bit of each sampling point with a binary message, LSB coding allows a large amount of data to be encoded. Among many different data hiding techniques proposed to embed secret data within an audio file, the LSB data hiding technique is one of the simplest methods. This mainly allows for insertion of data into digital signals in a noise free environment, which entirely embeds the secret message-bits in a subset of the LSB planes of the audio stream. The following steps are:

a. Receives the audio file in the form of bytes and converted in to bit pattern.

b. Each character in the message is converted in bit pattern.

c. Replaces the LSB bit from audio with LSB bit from character in the message.

This proposed system provides a good and efficient method for hiding the data from hackers and sending it to the destination in a safe manner. This does not affect the size of the file even after encoding and is also suitable for any type of audio file format.

5. CONCLUSION

Securing the secret data by embedding it in audio-video file with an appropriate steganographic technique provides high security. We are hiding an encrypted secret image behind audio signals of the audio-video file and the encryption key behind a video frame using LSB substitution technique. Satisfactory results are obtained in both audio and video steganography. The use of LSB substitution technique for steganography and AES for encryption has made it possible to maintain the integrity of the secret image.

This proposed method can also withstand different attacks and thus a very strong and robust method of data hiding can be obtained.

REFERENCES

[1] A. K. Bhaumik, Minkyu Choi, Rosslin R. Robles, Maricel O. Balitanas “Data Hiding In Video” from International Journal of Database Theory and Application Vol.2-2 June 2009.

[2] Prof. D. P. Gaikwad, Trupti Jagdale, Swati Dhanokar, Abhijeet Moghe, Akash Pathak “Hiding the Text and Image Message of Variable Size Using Encryption and Compression Algorithms in Video steganography”, International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 1, Issue 2, pp.102-108

[3] Sunil k. Moon, Rajshree D. Raut, “Application of data hiding in Audio-Video using anti forensics techniques for authentication and data security”, Advanced Computing Conference (IACC) 2014IEEE International.

[4] Burate D. J., M. R. Dixit “Performance Improving LSB Audio Steganography Technique” Volume 1, Issue 4, September 2013 International Journal of Advance Research in Computer Science and Management Studies.

[5] K.A. Navas, Vidya V., Sonia V. Dass, "High security data embedding in video", Recent Advances in Intelligent Computational Systems (RAICS), 2011 IEEE

[6] Padmashree G., Venugopala P. S., "Audio Steganography and Cryptography: Using LSB algorithm at 4th and 5th LSB layers", ISSN: 2277-3754 ISO 9001:2008 Certified International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 4, October 2012

[7] William Stalling, "Cryptography and Network Security: Principles and Practices", 5th ed., Pearson Education, Prentice Hall, 2011

BIOGRAPHIES

1. Miss Minal B. Rawde is pursuing B. E. in CSE from RTMNU, Maharashtra, India. She has participated in three National level paper presentations. Her area of interest is Computer System and Security (CSS) and Networking.

2. Miss Mousami V. Kumbhare is pursuing B. E. in CSE from RTMNU, Maharashtra, India. She has participated in two National level paper presentations. Her area of interest is Computer System and Security (CSS) and Networking.

3. Miss Sanika M. Chaudhari is pursuing B. E. in CSE from RTMNU, Maharashtra, India. She has participated in three National level paper presentations. Her area of interest is Computer System and Security (CSS) and Networking.

4. Miss Shital K. Bhongade is pursuing B. E. in CSE from RTMNU, Maharashtra, India. She has participated in National level paper presentation. Her area of interest is Computer System and Security (CSS) and Hardware Networking.

5. Miss Vaishali Bhagat has received B. E. degree in Information Technology from RTMNU, Maharashtra, India in 2008 & pursuing M. Tech in CSE, from RTMNU since 2010. She is working as an Asst. Professor in the department of Information Technology, SRMCEW, Nagpur, Maharashtra, India. Her area of interest is CSS and Visual Cryptography. She has published seven papers & is member of IAENG, ISTE, Academic.edu, reviewer of premier publication