© 2018 IJSRST | Volume 4 | Issue 7 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

Audio-Video Stegnography for Better Security of Data

Jaishree Meshram, Prof. Pragati Patil
CSE Engineering, AGPCE, Nagpur, Maharashtra, India

ABSTRACT

Security is most important issue in digital communication. Data security means protective digital privacy measures that are applied to prevent unauthorized access to computers, huge databases and online data it is also protects data from corruption. Security is most important issue in digital communication. Cryptography and steganography are two popular methods available to provide security. Steganography focuses on hiding information in such a way that the message is undetectable for outsiders and only appears to the sender and intended recipient. It is useful tool that allows covert transmission of information over and over communications channel. Steganography is a technique which is used to hide the message and prevent the detection of hidden message. Various modern techniques of steganography are: a) Video Steganography b)Audio Steganography. Audio Video steganography is a modern steganography of hiding information in a way that the unwanted people may not access the information. The propose method is to hide secret information and image behind the audio and video file respectively.

Keywords : Audio-Video Steg, LBS, MSB

I. INTRODUCTION

Steganography focuses on hiding information in such a way that the message is undetectable for outsiders and only appears to the sender and intended recipient. It is useful tool that allows covert transmission of information over and over communications channel. Steganography is a technique which is used to hide the message and prevent the detection of hidden message. Various modern techniques of steganography are

a) Video Steganography c) Audio Steganography

Audio Video stegnography is a modern way of hiding information in a way that the unwanted people may not access the information. The propose method is to hide secret information and image behind the audio and video file respectively.

Audio Steganography

Audio steganography software can embed messages in WAV, AU,and even MP3 sound files. In audio steganography sound file is modified in a a way they contain a hidden information. This modification done in such a way that secrete data must be secure and without destroying the original signal.

The basic model of Audio steganography consists of Carrier (Audio file), Message and Password. Carrier is also known as a cover-file, which conceals the secret information. Encoding secret messages in audio is the most challenging technique because the human auditory system (HAS) has such a dynamic range that it can listen over. Audio files are usually compressed for storage or faster transmission. Audio files can be sent in short stand-alone segments. There are various types and technique of data hiding in audio like Least Significant Bit Encoding and Phase coding. Embedding secret messages in audio file is more difficult than embedding messages in digital image. In order to hide secret messages, various methods for

embedding information in digital audio like Least significant bit, parity bit coding, phase coding, spread spectrum etc..

II. LITERATURE SURVEY

Arup Kumar Bhaumik, Minkyu Choi et.al, [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.

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.

Praveen. P, Arun. R, [7] have proposed a method which is an audio-video crypto- steganographic system, it is the combination of audio steganography and video steganography using advanced chaotic algorithm as the secure encryption method. Their aim is to hide secret information behind image and audio of video file. Since video is an application of many audio and video frames. A particular frame can be selected for image hiding and audio for hiding a secret data. They have used 4LSB substitution for image steganography and LSB substitution algorithm with location selection for audio steganography. Advanced chaotic algorithm can be used for encryption and decryption of data and images. Suitable parameter of security and authentication such as PSNR value, histograms are obtained at both the receiver side and transmitter sides that may be identical at both ends. Hence they have tried to enhance the security of the data and image. This method can be used in fields such as medical and defence which requires real time processing.

Lovey Rana, Saikat Banerjee, [8] implemented an audio steganographic system that provides improved security. To achieve this, dual layer randomization approach is used. First layer of randomization is achieved by randomly selecting the byte number or samples. An additional layer of security is provided by randomly selecting the bit position at which embedding is done in the selected samples. Using this proposed algorithm the transparency and robustness of the steganography technique is increased.

III. PROPOSED METHODOLOGY

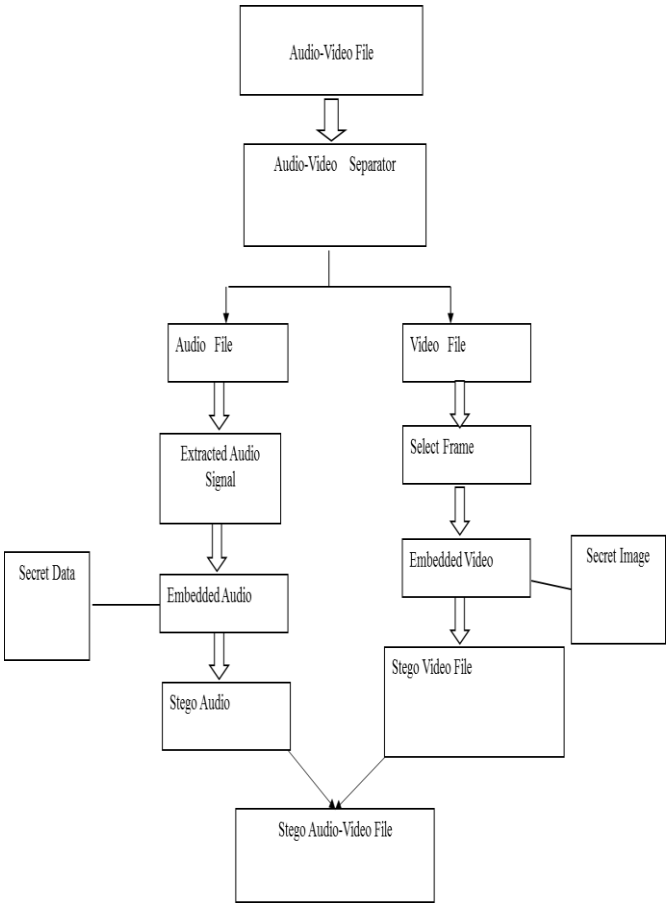
In propose work we introduce novel method for audio video steganography. In this method we can hide secret image behind video and text behind audio. For video stegnography LSB algorithm is used and for audio stegnography parity algorithm is used. In proposed work sender used any audio video file and divide it separately as audio file and video file. After that image hide behind the video using passkey and video converted into “stego video” same as secret text hide behind the audio and audio become the “stego audio”. These stego audio and stego video file combine and send to the receiver side. At receiver side this stgo audio-video file again separated and using passkey. The secret image and data from stego video and stego audio recover respectively. Video is a set of images. It is an electronic medium. In audio steganography sound file is modified in a way they contain hidden information. In video per unit of time of video ranges from six to eight frames per second. Video stenography algorithm based on fact on each pixel represented by 3 bytes where each byte representing 3 primary colors that is red, green, blue (RGB).Size of image file is directly related to number of pixels and granularity of color definition. For hide a secrete image behind the video we need AVI audio video interleave) video. There are different format of video file like MPEG,MPG these all file first convert into AVI format first.

Working of Sender side

We are combining cryptography and steganography for hiding data behind audio and image behind video in audio-video file. For hiding image behind video we used LSB replacement technique and for hiding data behind the audio used Parity coding algorithm. Data is encrypted for more security purpose.

Sender selects any one audio-video file. This audio-video file separate using in build software. Now sender will select a secret image which will be transmitted to the receiver. In next step select the video file. Video is nothing but a collection of multiple frames. The number of still pictures per unit of time of video ranges from six to eight frames per second. The algorithm of video stegnography is based on the fact that each pixel represented by 3 bytes where each byte representing the intensity of 3 primary colors that is RGB Red, Green and Blue) Size of image file is directly related to number of

pixels and granularity of color definition. Sender selects the more than one frame and using LSB algorithm embedded the secret image into the frame. The part of LSB of secret image embedded in one frame and MSB in another frame. The selection of frames is depend on the user or sender. He can be selecting each time new frames.



The receiver will now perform extraction of key and image from the output video received by the transmitter. The receiver gives the output video as input to the system. The system separates the stego audio-video file (i.e. the received video) into stego audio signals and stego frames using matlab function "vision.VideoFileReader ()".. Then the embedded image is being extracted from the audio signals and the key is being extracted from the video frame. This extracted key is then matched with the 16 byte key. If the keys are matched then the key is provided to the extracted encrypted image, for its decryption and thus, the secret image is finally received by the receiver. And if the keys do not match the system get to know that the user is an unauthenticated user and thus, it displays a "Keys do not match" message and stops the system. Thus if any unauthorized user tries to extract the secret image from the stego audio-video file, the system will decline the process and will not show the embedded image to the user in any condition. Thus, a secret image is securely transmitted from one user to another by informing the username and password to receiver end privately. Pixels and granularity of color definition. Sender selects the more than one frame and using LSB algorithm embedded the secret image into the frame. The part of LSB of secret image embedded in one frame and MSB in another frame. The selection of frames is depending on the user or sender. He can be selecting each time new frames.

IV. CONCLUSION

Securing the secret data by embedding it in audio-video file with an appropriate stenographic 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 (Least Significant Bit) replacement technique. Satisfactory results are obtained in both audio and video steganography. The use of LSB substitution technique for steganography and encryption has made it possible to maintain the integrity of the secret image. Here, a robust method of imperceptible data hiding is introduced. The system provides a good and efficient method for hiding the data from hackers and sent to the destination in a safe manner. This method do not compromise with the quality of the data sent, exact image is recovered at the receiver side.

V. 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. 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
6. K.A. Navas, Vidya V., Sonia V. Dass, "High security data embedding in video", Recent Advances in Intelligent Computational Systems (RAICS), 2011 IEEE
7. Praveen. P, Arun. R, "Audio-video Crypto Steganography using LSB substitution and advanced chaotic algorithm", International Journal of Engineering Inventions e-ISSN: 2278-7461, p-ISSN: 2319-6491 Volume 4, Issue 2 (August 2014) PP: 01-07
8. Lovey Rana, Saikat Banerjee, "Dual Layer Randomization in Audio Steganography Using Random Byte Position Encoding" , International Journal of Engineering and Innovative Technology, Volume 2, Issue 8, February 2013
9. Muhammad Asad, Junaid Gilani, Adnan Khalid, "Three Layered Model for Audio Steganography", 2012 International Conference on Emerging Technologies (ICET)
10. Kamalpreet Kaur, DeepankarVerma, "Multi-Level Steganographic Algorithm for Audio Steganography using LSB, Parity Coding and Phase Coding Technique", IJARCSSE, Volume 4, Issue 1, January 2014