Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 02, February-2018

Data Security using Audio-Video Steganography

Ms. Srushti Save, Ms. Pracheta Raut, Ms. Prajakta Jadhav, Ms.Tejaswini Yadav
Undergraduate Student,
Department of Electronics & Telecommunication,
St. John College of Engineering and Management
Palghar, Mumbai,India

***Abstract*: Steganography is a method of hiding any secret information like text, image, audio behind original cover file .In this paper we proposed the combination of image steganography and audio steganography with face recognition technology as a tool for authentication. The aim is to hide the secret information behind audio and the recipient's face image of video, as it is an application of many still frames of images and audio. In this method we have selected any frame of video to hide recipient's face image and audio to hide the secret data. Suitable algorithm such as improved LSB and RSA Algorithm is been used to hide secret text and image. PCA Algorithm is used for face recognition. The parameter for security and authentication are obtained at receiver and transmitter side which are exactly identical, hence the data security can be increased.**

Keywords- Steganography, Python,Principle Component Analysis, Least Significant Bit, RSA Algorithm etc.

I. INTRODUCTION

The term 'steganography' encapsulates the practice of secretly embedding data into digital mediums including video, image and audio files. Although steganography is often associated with wicked activities, conceptually it asserts several characteristics that render it useful in contemporary security applications.

Information security plays a vital role in internet communication with today's era of technology. It is one of the most challenging issues now days. It is extremely important to people committing e-transactions like online shopping, money transfer etc. Steganography is the method that is used for secure communication. The principle of steganography is to mask the very presence of communication; it hides the existence of message. This technique is widely used to prevent not deliberated receiver's attacks of unauthorized access. Not just a mechanism for criminals to communicate secret information about a digital channel, steganography is also used as a logical method of ensuring integrity of digital media artifacts and for identification of same.

This application of steganography allows for identification images storing additional information to verify both the identity of the subject as well as the authenticity of the image.

Audio steganography is one of the popular data hiding techniques that embeds secret Data in audio signals. It is based on the masking effect of Human auditory system (HAS). This means that a week sound is undetectable in the presence of the large one. Data hiding in audio signals has numerous applications such as; protection of copyrighted audio signals and safely covering communication data.

Steganography literally means covered writing. Its goal is to hide the fact that communication is taking place. This is often achieved by using a (rather large) cover file and embedding the (rather short) secret message into this file. The result is the stego file that contains the secret message. Now, it is gaining new popularity with the current industry demands for digital watermarking and fingerprinting of audio and video Steganography has seen exponential usage since the 1990s. Governments, military, businesses, and private citizens all over the world now use steganography for security and privacy purpose. In our project an audio steganography technique is propose to hide message signal in audio in the transform domain. The message signal in any format is encrypted and carried by audio without revealing the existence to anybody. The quality of stego file is measured by PSNR. The quality of extracted secret message signal is measured by SNR. The format is regenerate into an alternate equivalent multimedia system files like images, video or audio, which is being covered up inside another object. For audio-video steganography improved LSB and RSA algorithm is used to hide text and recipient image. Face recognition technique using PCA algorithm is used for providing authentication.

II. PROBLEM STATEMENT

As the usage of internet in the world is increased very highly, hence all are needed more security. The internet developers are always tries to make internet free from jamming. For that there are many techniques and algorithms are proposed. They are also worked on how the hackers are acting smartly to hack information and also invents new techniques to stop hacker's intentions. Any techniques which tries to improve the embedding payload or robustness should preserve imperceptibility. Different embedding payload may have different effects on audio quality. In this project, LSB method used for audio-video steganographyas to get efficient results and with less distortion.

III. BACKGROUND AND LITERATURE REVIEW

Steganography has been perform in two domain: Temporal domain &Transform domain. The steganography can be done in various techniques such as LSB coding, Parity coding, Echo hiding, Phase coding, Spread Spectrum, Wavelet domain. The proposed method is applied to various audio files such as speech and music envelope signals. These audio files were used as covers and secret messages and it all giving remarkable results on steganography concept [1].

An algorithm for hiding image in selected video sequence is an image-hiding technique based on Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) and random LSB (Least Significant Bit). This method is used that reduces the embedding distortion of the host audio file. The method focuses the idea of computer forensics technique

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 02, February-2018

which is use as a tool for authentication and data security purpose and its use in video steganography in security manner [2]. The Genetic Algorithm operators are used to get the next generation chromosomes. Next select the best chromosome according to the best fitness value. Fitness value is a value of LSB position for which we get a chromosome with the minimum deviation comparing to the original host audio sample. Here higher LSB layer is given higher preference in case of layer selection. The original audio sample and inserting message bit in different LSB layer positions we get some new samples. Sometimes it can happen that for more than one LSB layer and get the same difference between original audio sample and new audio samples. In this case, we will choose the higher LSB layer .The decryption part gets complicated as thelong text message cannot be hidden using these method [6]. This method approach face recognition technique using PCA algorithm. In PCA based face recognition the algorithm for real-time human face tracking is realized. The algorithm takes the advantage not only of geometric relations between a human face, but also of a good feature extraction. In this system PCA is used for feature extraction and Genetic Algorithm is used for recognition [9].

IV. PROPOSED SYSTEM

A. *BLOCK DIAGRAM*

a. Encryption:

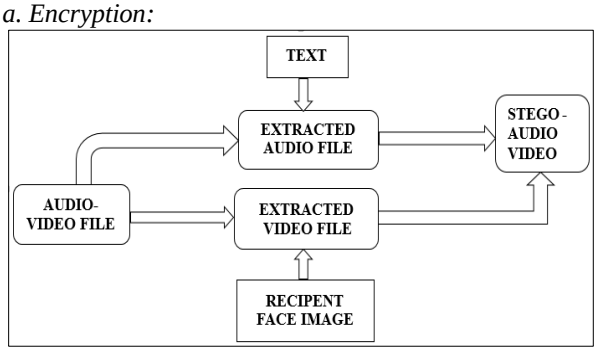

Fig.1. Encryption Process of proposed system

In Fig.1, the block diagram of hiding text content behind audio is shown. Any accessible .mp4 audio-video file is selected. Next step is to extract audio from selected .mp4 file, and separate the audio and video part. Behind extracted audio hide the secret text and behind extracted video hide the recipient face image. Finally the stego audio-video file is generated at the sender side.

b. Decryption:

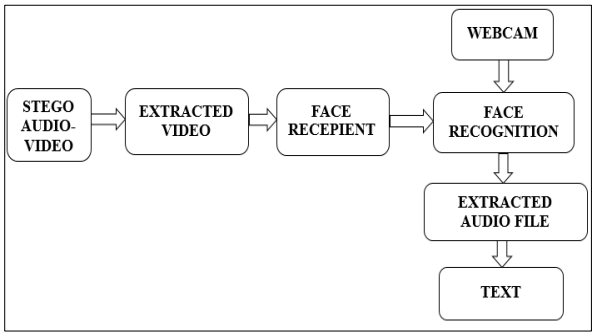

Fig. 2. Decryption Process of proposed system

In Fig.2, at receiver side the stego audio-video file is appeared, then select the extracted video part and recover the authorized recipient's face image from the selected frame. Compare recovered authorized face image with the input image from webcam. If both the images are authenticated, then only user can recover the text behind audio else process will wait until authorized recipient appears in front of webcam. When authentication procedure is done it will be able to extract secret text from stego-audio file.

B. *FLOW CHART*

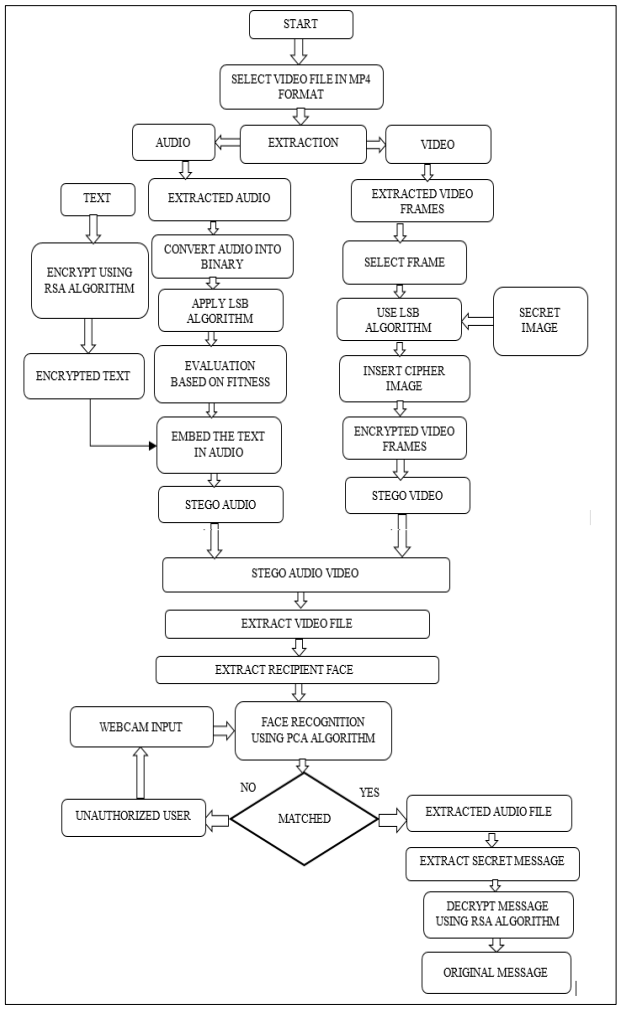

Fig.3. Flowchart of proposed system

In Fig.3, the message is embedded in audio by following methodology as proposed system is using the video file (.mp4) for carrying out the whole procedure, first the video file is separated in two different sections that is extracted audio and video file. Both the sections perform a vital role for executing the idea of the project, the extracted audio file is use for hiding the secret text before hiding, the text is encrypted using RSA algorithm this algorithm uses two keys for encryption and decryption here public key is use for encryption. These technique is use to make the data more secure, after these hiding part is carried out by LSB algorithm. The LSB algorithm is simpler and widely use algorithm as it provides the best position in audio to hide the text so that there is less distortion in stego-audio file, thus the difference between original audio and stego-audio is less. Now the extracted video

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 02, February-2018

file is use for hiding the face image of authorize person to whom the secret data is intended to send these method leads to the formation of stego-video. After this both stego files are combined to form the stego audio-video file. Now the Decryption is perform to get the hidden secret message from stego audio-video file in decryption part the video file is extracted from stego audio-video file to recover the authentication image from selected frame, then the face input is taken from webcam for authentication purpose and the input image is matched with the hidden image, the face recognition is done using PCA algorithm, the PCA algorithm verifies the input image on basis of the eigen values of face image store in video frame if it gets matched the audio part is extracted to get the secret data from it .After extracting the hidden text the text is decrypted using private key of RSA algorithm for getting the original secret message.

V. EXPERIMENTAL RESULTS

1. Encryption:

a) *Audio extraction*:

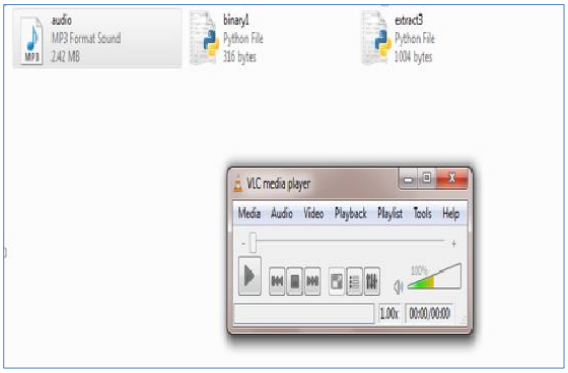

Fig.4. Audio extraction process

The video file .mp4 format of size 0.99Mb is selected. Then audio and video are extracted from mp4 video file. The extracted audio file size is 1.96Mb. This extracted audio file is in the mp3 format. Now behind this extracted audio file the secret message is embedded by proposed algorithm.

b) Audio in binary format:

Fig.5. Audio in binary format

First the text message is encrypted using RSA algorithm. Then that encrypted message is converted into binary format for these extracted audio file is use and converted that file into binary format.

c) Stego-audio is created:

Stegoaudio is created by hiding encrypted message behind audio using LSB algorithm.

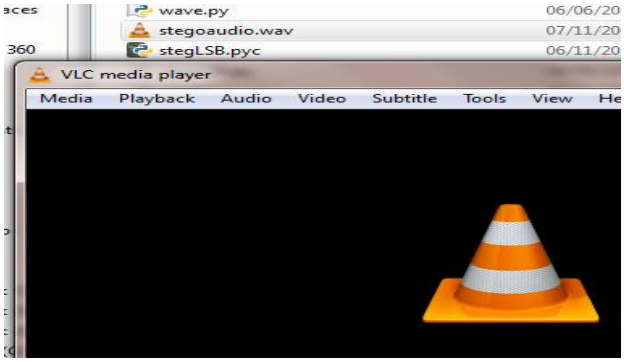

Fig.6.Stegoaudio

d) Created frames:

Fig.7. created frames

For video part, extracted video file in the .avi format and size is 696KB, then video is converted into frames. Each frame size is 23KB. From frames created a single frame is selected to hide the recipient image behind the selected frame.

e) Audio Responses:

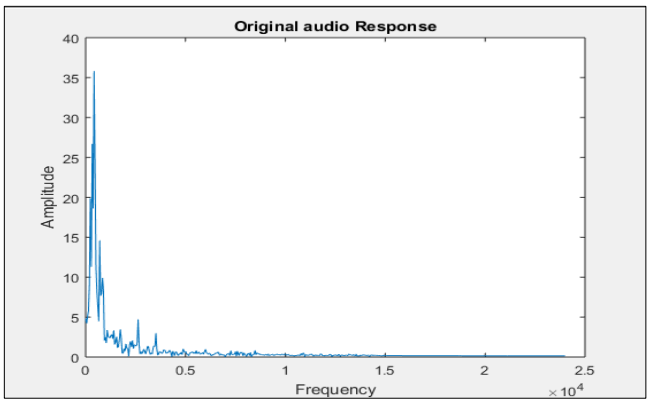

Fig. 8(a). Original audio response

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 02, February-2018

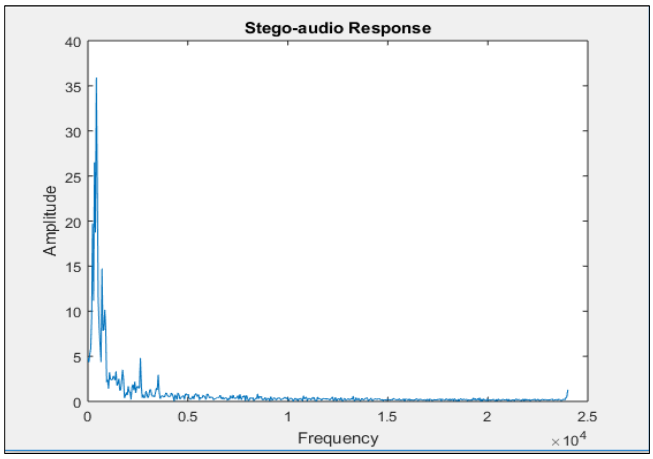

Fig. 8(b). Stego audio response

It can be observed from both the Fig. 8(a) and 8(b)that there is no change in waveforms. Both the waveforms are identical; it means there is no change in characteristics of audio signal after embedded with data.

f) Stego video:

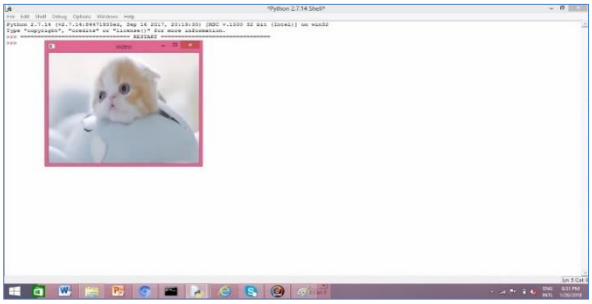

Fig. 9. Stego video

In Fig. 9, the stego video is created by combining the all separated frames along with stego frame.

g) Comparison of various Videos:

VIDEOS	FRAMES	SIZE OF FRAME
Video1(0.99MB)	576	16.9KB
Video 2(8.7MB)	1 4 1 0	118KB
Video 3(14.1MB)	326	175KB

Table 1. Comparison of various frames

From above comparison table, it is observed that the video which have more contrast difference creates more frames where as the video having less contrast difference creates less frames.

VI. CONCLUSION

Hiding information may introduce enough visible noise to raise suspicion. Therefore the carrier or cover audio must be carefully selected. This proposed system is to provide a good, efficient method for securing the data from hacker and sent to the destination in a safe manner. Embedding picture and text behind video and audio file and then combine into stego file at sender side and thereafter face authentication technique is carried out at receiver side to cross check the security parameter by authorizing the recipient hence ,the data is significantly secured.The secret text information is archive in audio successfully moreover interpret the audio file and focused to extract secret text.

VII. FUTURE WORK

The work presented in this project is, hopefully included within the defined scope therefore, future decryption research is expected to explore beyond the scope of this project.The effectiveness and efficiency of the proposed system can be enhanced in the way of capacity, security and robustness. However, whether the proposed method can be detected by other high-statistics steganalytic algorithms should be further studied. The future work mainly focuses on audio-video steganography with confusing algorithm and reversible data hiding mechanism. As these project has succeeded in encryption part of it thus the decryption part can be performed through reversible data hiding method the exact image and data can be retrieved along with the cover video and audio. The audio and video quality can also be preserved.

REFERENCES

[1] MazharTayel, Ahmed Gamal, HamedShawky, “A Proposed Implementation Method of an Audio Steganography Technique”, ICACT2016, Issue Feb 3, 2016.

[2] YugeshwariKakde, Priyanka Gonnade, Prashant Dahiwale , ”Audio-Video Steganography”, ICIIECS’15, Issue 2015 IEEE.

[3] Juanita Blue, Joan Condell, Tom Lunney,” Identity Document Authentication using Steganographic Techniques”,**Signal and System Conference (ISSC) -21 June 2017.**

[4] Ankit Gambhir, SibaramKhara,” Integrating RSA Cryptography & Audio Steganography”,International Conference on Computing, Communication and Automation(ICCCA), Conference on 29-April-2016.

[5] Ratul Chowdhury, Debnath Bhattacharyya, Samir Kumar Bandyopadhyay and Tai-hoon Kim,” A View on LSB Based Audio Steganography”, International Journal of Security and Its Applications, Vol. 10, No. 2 (2016).

[6] V. Santhi and LogeswariGovindaraju,” Stego-audio Using Genetic Algorithm Approach”, Research Journal of Applied Sciences, Engineering and Technology, June 2014.

[7] Prashant Johri, Arun Kumar, Amba,” Review Paper On Text And Audio Steganography Using GA” International Conference on Computing, Communication and Automation, 2015 IEEE.

[8] Krishna Bhowal, “Audio Steganography using GA” 2010 International Conference on Computational Intelligence and Communication Networks.

[9] Firoz Mahmud, Md. EnamulHaque, Syed TauhidZuhori, Biprodip,” Human Face Recognition using PCA based on Genetic algorithm”, Electrical Engineering and Information & Communication Technology (ICEEICT), 2014 IEEE.