International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 6 | Issue 3 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT2063181

Audio and Video Steganography for Secure Data Hiding

Swathi*, Supriya A V, Soundarya Shridhar Patgar
Information Science and Engineering, Srinivas Institute of Technology, Mangaluru, Karnataka, India

ABSTRACT

Today, the protection is getting the imperative interest due to the elevated use of internet. As the use of internet is increased, the charge at which the records are interchanged per day is additionally increased. The data that is interchanged every day might also turn out to be the target of fraudsters. To take action to do something in particular to resolve this hassle one of the powerful technology is the Steganography. The Steganography is a process of concealing secret information behind an harmless cover file, such that the existence of information is no longer usually admitted. This paper uses the idea of Audio and Video Steganography, where the data is hidden behind the audios and frames of videos.

Keywords: Steganography, Cryptography, AES Algorithm

I. INTRODUCTION

While sending data, there is commonly a problem with its security. Sensitive information can be hacked by a third party. In this modern era internet presents magnificent comfort in transmitting massive volume of data. However the safety and security of long distance communication remain an issue in order to solve the probem has led to the development of audio and video steganography. The main hassle is that the commonly due to fear of encryption services getting unlawful and copyrights proprietor who desires to tune confidential and intellectual property copyright towards unauthorized access and digital materials.

Steganography is the powerful technology of hiding the secret message in a cover file in such a way that no one, other than the sender and intended recipient, guess the existence of the message. Steganography relies on hiding convert message in unsuspected multimedia data and is normally utilized in secret communication between acknowledged parties.

That is, Steganography is about hiding a secret message into another media file. The secret message and the media file can be in any form. It can be in the form of image, video or audio. The main objective of steganography is to hide the secret message from a third party. Anyone can modify and misuse the valuable information through hacking at the time transferring information.

Audio steganography is a approach used to transmit hidden information by usage of altering an audio signal in an imperceptible manner. It is the approach of hiding some secret textual content or audio information in a host message.

Video comprises of stream of frames (images) and audio. Any frame of the video can be chose for hiding the secret data. The big advantage with video-based steganography technique is that a long secret message can be hidden behind it.

II. LITERATURE SURVEY

1. A Literature Review on Various Recent Steganography Techniques:

In this paper [2], they reviewed exclusive Steganography techniques which no longer only hides the message behind the image but also gives security. The survey was once performed on quite variety of steganography methods which are very useful and advisable for imparting higher information security along with some cryptography methods and some other methods such as LSB, LSBM, LSBMR, SSHDT, RSTEG, OPA, Genetic-X mean algorithm, VSS, SDSS, FDSS, BPCS, GLM algorithm, SDS, Transform domain techniques, Distortion techniques etc. In this paper offers literature evaluation on typical strategies and procedures used in the security & transmitted data over the data networks.

2. A Robust Audio and Video Steganographic Scheme:

In the previous few years, various strategies for information hidden in audio sequences have been presented. All of the developed techniques take gain of the perceptual residences of the human auditory system (HAS).Genetic Algorithm primarily based approach[8] encrypt textual content using RSA encryption algorithm. Then by making use of proposed Least Significant Bit algorithm, embed message bits to the audio bit steam in greater Least Significant Bit layer positions at randomly to urge a sequence of chromosomes. Then Genetic Algorithm operators are used to get the subsequent generation chromosomes. It affords increased stage of protection alternatively increases computational complexity. In this paper[1], pre-processing is utilized on secret message. In pre-processing secret message is transformed into variant dimension of bits using Huffman coding. Then these bits are transformed into hexadecimal digits. Hexadecimal digits are encrypted usage of quicker and powerful AES (Advanced Encryption Standard) algorithm. Generated cipher textual content is transformed into binary and concatenates this binary bits form a binary string of message that is embedded in an audio file the use of modified dual randomness LSB method.

3. A Technique for Data Hiding using Audio and Video Steganography:

In this paper [3], they provided an approach where user is not able to see an audio information hiding. This machine is supposed to provide an efficient approach for embedding and hiding the statistics from attackers and send safely to its destination. This will now not alter the dimension of the file even after encoding of information in an audio file. Thus, they infer that audio data hiding strategies can be utilized for a quantity of duties different from conversation data and its storage, these methods described above can be further altered as it is in the world of Information Technology.

4. Data Security using Audio-Video Steganography:

In this paper[4], an audio steganography approach is advice to hide message signal in audio in the transform domain. The message signal in any format is encrypted and carried with the aid of audio besides revealing the existence to anybody. The quality of stego file is measured by PSNR. The quality of extracted secret message signal is measured by way of SNR. The format is regenerate into an alternate equivalent multimedia machine documents like images, video or audio, which is being protected up inside every other object. For audio-video steganography accelerated LSB and RSA algorithm is used to conceal textual content and recipient image. Face recognition technique using PCA algorithm is used for imparting authentication.

III. IMPLEMENTATION

Steganography implements an encryption approach in which communication takes vicinity with the aid of hiding information. A hidden message is the combination of a secret message with the carrier message. This technique can be used to hide the message in an audio file, video file or in a file system. concealing information into a medium and extracting information from the medium requires following elements:

a) The cover medium that holds the secret message.
b) The secret message, it can be a plain text or any kind of data.
c) The steganography techniques which can be used to conceal the information.
d) A key that can be used for hiding and extracting the message.

Concealing Data:

Step 1: Loop the message.
Step 2: For each bit in the message.
Step 3: Read a byte from the key.
Step 4: Skip a couple of samples.
Step 5:Copy one sample from clean stream to the carrier stream (using for loop).
Step 6: Read one sample from the wave stream.
Step 7: Get the next bit from current message byte.
Step 8: Place it in the last bit of sample.
Step 9: Write the result to the destination stream.
Step 10: Copy the rest of the frame for the rest of the byte.

Extracting Data:

Step 1: For each bit in message read a byte from the key.
Step 2: Skip a couple of samples.
Step 3:Read one sample from the wave stream.
Step 4: Get the last bit of sample.
Step 5: Write it into the message byte.
Step 6:Add the reconstructed byte to the message.
Step 7:First four byte contains the length of message.

IV. RESULTS

The result of this paper is analysed with different audios and videos as input. This result provides the double security to any given input. First level security is provided through encrypting the secret information and second level security is provided through Steganography. The Steganography is used to hide secret information behind the innocent cover media. There are different algorithms for implementing the encryption of secret data. The one used in this paper is AES encryption algorithm. The reason behind using the AES algorithm is, it is the simplest and fastest algorithm for encryption of data.

The motivation behind the concept implemented in this paper is security. Security to the important data transmitted is major concern now days. As data transmission rate is increased, security must be provided to these data transmitted. By using the concept implemented in this paper, we can provide a better security to the every important document. Sender can securely transfer the data to the receiver.

Figure 1 shows the page where the text is hidden in an audio. First, the system accepts the input from the user that is the cover file to hide the data behind. Here cover file must be audio file. Next, the system gets the secret data from the user to hide behind cover file.

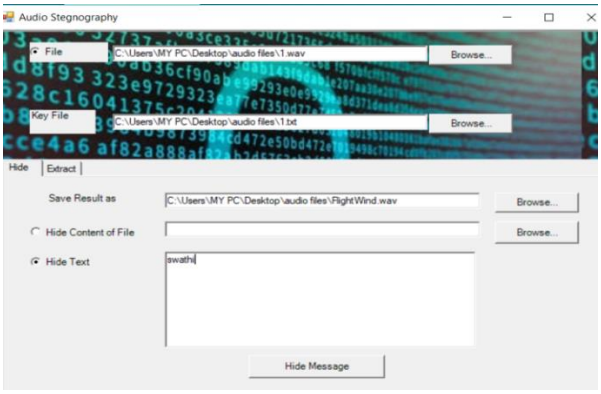

Figure 1. Hiding the text inside the audio

This project implemented with secret data as text. The system accepts secret key as an input from the user to provide security to the data.

Figure 2. Extracting the text from the audio

This is the page where the hidden text is extracted in an audio. The sender must share the secret key with receiver. The secret key is used to provide security to the data. The same key must be known to the receiver to decrypt the data.

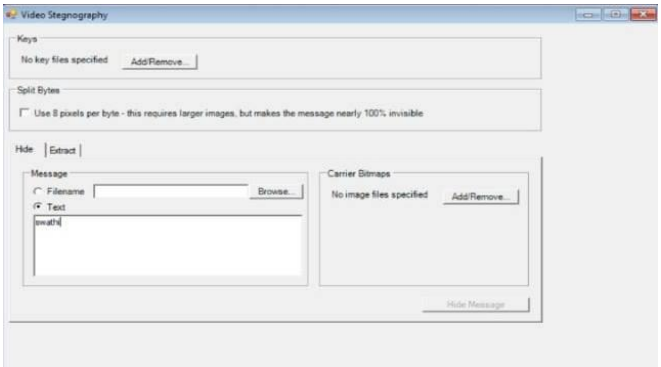

Figure 3. Hiding the text inside the video

This is the page where the text is hidden in the video. First the system accept the input from the user that is the cover file to hide the data behind. Cover file can be text, audio or video. Here the project is implemented with accepting video as cover file. Next the system gets the secret data from the user to hide behind the frames. The system also accept the document as the secret data. The secret data can also be image, but processing image or hiding behind image is critical process so this project is implemented with secret data as text. Then the system accepts secret key as a input from the user to provide security to the data.

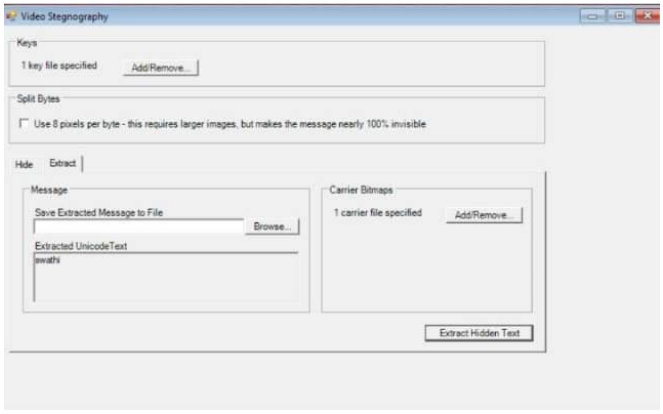

Figure 4. Extracting the text from the video

This shows the page where the hidden text is extracted from the video. The sender must share the secret key with receiver. The secret key is used to provide security to the data. The same key must be known to the receiver to decrypt the data. This process provides the output as stego video, which contains the encrypted data hidden behinds frames. We can retrieve the encrypted data from the video. The output produced is the original data.

V. V. CONCLUSION

The ultimate goal of any steganography technique is to insert secret messages into a chosen media, such as images, audio and video files without easily noticed by any unintended third party. The proposed audio and video steganography system affords two levels of security, first with cryptography and second with steganography. The proposed machine consequences in hiding encrypted information into audio or video files. The system is examined by taking awesome dimension of audio, video file and specific measurement of secret data. It suggested that no noticeable noise delivered in encrypted video. The existence of secret information is not possible to detect. Hence the information transferred safely and securely to the destination.

VI. FUTURE SCOPE

There are constant advancements within the computer field, suggesting advancements within the field of steganography also. It's likely that there'll soon be more efficient and more advanced techniques for Steganalysis. A favourable advancement is that the improved sensitivity to small messages. Knowing how difficult it's to detect the presence of a reasonably large document within an audio or video, imagine how difficult it is to detect even one or two sentences embedded in an audio or video. It is like finding a microscopic needle within the ultimate haystack. What is terrifying is that such a little file of just one or two sentences may also be all that is needed to commence a surprice attack. Within the future, it is hoped that the technique of Steganalysis will advance such that it will become much easier to detect even small messages within an audio or video. During this work it explores only a little part of the science of steganography.

VI. REFERENCES

[1] Hinal Somani, Kaushal M. Madhu, "Robust and High Capacity Audio Steganography using Modified Dual Randomness LSB method" ,IJARIIE, 2016.

[2] Anupriya Arya and Sarita Soni, "A Literature Review on Various Recent Steganography Techniques", IJFRCSCE, January 2018.

[3] Chhaya Varade, DanishShaikh,Girish Gund,Vishal Kumar,Shahrukh Qureshi, "A Technique for Data Hiding using Audio and Video Steganography", IJARCSSE, February 2016.

[4] Ms.Srushti Save, Ms.Pracheta Raut, Ms.Prajakta Jadhav, Ms.Tejaswini Yadhav, "Data Security using Audio-Video Steganography",IJERT2018, February 2018.

Cite this article as :

Swathi, Supriya A V, Soundarya Shridhar Patgar, "Audio and Video Steganography for Secure Data Hiding", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6 Issue 3, pp. 703-707, May-June 2020. Available at doi : https://doi.org/10.32628/CSEIT2063181
Journal URL : http://ijsrcseit.com/CSEIT2063181