International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 3 | ISSN : 2456-3307

Data Hiding In Audio & Video Files Using Steganography

R. Sivaranjani, A.Suhasini
[1]M.E Scholar. Computer Science Department, Annamalai University, Chidambaram, Tamilnadu, India
[2]Associate Professor, Computer Science Department, Annamalai University, Chidambaram, Tamilnadu, India

ABSTRACT

To provide an efficient technique to hide data in image, audio or video files in which embedding the secret text without damaging the files. Applying the encryption techniques using the password and then uploading onto cloud storage. In Reversible data hiding, the receiver can retrieve the file from cloud storage and decrypt the file using the decryption techniques and extracting the secret text. Finally the user can access the files without any loss in quality or distortion in file. Intruders always try to access the secret data from the internet. It is easy to access data when the data is hiding in files. To overcome this problem, we introduce certain level of robustness against frame drop, repeat and intruder attacks.

Keywords: Embedding, Encryption, Cloud storage, Decryption, Extraction.

I. INTRODUCTION

The digital information revolution has brought about profound changes in our society and our lives. The many advantages of digital information have also generated new challenges and new opportunities for innovation. The issues are regarding multimedia data hiding and its application to multimedia security and communication, addressing both theoretical and practical aspects, and tackling both design and attack problems. In the fundamental part, we identify a few key elements of data hiding through a layered structure. The rapid growth in the demand and consumption of the digital multimedia content in the past decade has led to some valid concerns over issues such as content security, authenticity, and digital rights management. Multimedia data hiding, defined as imperceptible embedding of information into a multimedia host, provides potential solutions, but with many technological challenges.

Data hiding is modeled as a communication problem where the embedded data is the signal to be transmitted. Various embedding mechanisms target different robustness-capacity tradeoffs. We study this tradeoff for two major categories of embedding mechanisms. In addition, we have found that the unevenly distributed embedding capacity brings difficulty in data hiding. We propose a comprehensive solution to this problem, addressing the considerations for choosing constant or variable embedding rate and enhancing the performance for each case.

In the design part, we present new data hiding algorithms images, and videos, covering such applications as annotation, tamper detection, copy/access control, fingerprinting, and ownership protection. The designs provide concrete examples regarding the choice of embedding mechanisms, the selection of modulation/multiplexing techniques for hiding multiple bits, and the handling of uneven embedding capacity. Data hiding can also be used in video communication to convey side information for additional functionalities or better performance.

APPLICATIONS

- ✓ Secure Confidential Files and documents.
- ✓ Transmit Highly Private Documents between International Governments.
- ✓ Confidential communication and secret data storing.
- ✓ Protection of data alteration.
- ✓ Access control system for digital content distribution.

II. LITERATURE SURVEY

Priyanka Mathur, Shambhu Adhikari [1] Presented a presents a state of the art of the data hiding techniques in grayscale image using LSB and its modified versions. Further a comparative analysis of the same is presented. It is techniques by which secret information can be hidden in any image or audio or video file which is being transferred over the communication channel. Least Significant Bit Steganography techniques are the commonly used data hiding techniques using images as cover image.

The comparison of simple LBB and pseudorandom LSB are presented. In simple LSB, secret information is embedded in the least significant bits representing pixels or samples of the cover file. In pseudo random LSB the pixel where secret data is to be inserted is picked up randomly. Also we have proposed adding the bit arbitrarily in 1st or 2nd LSB to increase the security. Using pseudorandom LSB without changing the quality of image security is enhanced.

B.Chitradevi, N.Thinaharan and M.Vasanthi[2], presented a brief idea about the image steganography that make use of Least Significant Bit (LSB) algorithm for hiding the data into an image. The reversible perturbation of values used in steganography enables the embedding of data into a cover medium. Choosing to modify values that have a small affect on the cover medium limits the ability to detect the embedding. Embedding strategies may be easily derived and implemented to complicate detection and inhibit the retrieval of the message by a third party, while still allowing easy retrieval by the intended recipient. LSB Embeddings may be detected simply through visual inspection of an image and its bit-planes, or more reliably through methods which use statistical metrics to identify the likelihood an image contains hidden data. While an embedding may be detected, it may not be easily decoded, nor may a stego object be discovered due to the sheer number of images available.

Jasril, Ismail Marzuki, Faisal Rahmat[3], based on the steganography indicates two of the principal requirements such the messages and the carrier file. Besides, it should have three aspects: capacity, imperceptibility, and robustness. This paper will show how to enhance the capacity of two types of carrier files for embedding message. By using Least Significant Bit method and modifying the four last bits of carrier files, bitmap and wav files could show the increasing of message size to be inserted to the carrier than only modifying the last 1 bit of carrier files. Particularly bitmap file which still had good quality visual showed PSNR value in 31.5460 dB, but wav file was only 3.8929 dB.

Neeraj Kumari and Babita Yadav[4], explained the goal of Audio steganographic technique is to embed data in audio cover file that must be robust and resistant to malicious attacks. This paper presents various audio steganographic methods like LSB, echo hiding, spread spectrum etc. Merits and demerits of each method are described.

The message in which secret message is hidden is called the host message or cover message. Digital images, audio files, video files, text files, executable files and even voice can be used as cover. Embedding secret data in digital audio cover is more challenging than using digital images as a cover since human auditory system(HAS) is more sensitive than human visual system (HVS).

Hazem Kathem Qattous[5], ensures that data will be transmitted under a cover of an innocent media file. This paper introduces an idea of combining both cryptography and steganography to increase the level of security that is required to transfer data. To achieve this, two encryption algorithms, Pohlig-Hellman and One-Time-Pad, are used to encrypt data before hiding it. To hide encrypted data, Least Significant Bit (LSB) technique is used whereby audio wave file (.wav) is used as a cover file to hide data into it.

This paper described the development of a software that uses above algorithms and technique to encrypt and hide data into audio wave files. The developed software allows the user to hide data into two different forms, file format and text format. In file format, the software allows the user to hide a file of any type into an audio wave file while, to hide the text format, it allows the user to write a text message before asking the software to encrypt and hide it. To be able to hide a larger data size, a compression algorithm, LZ77, is used to compress the text before encrypting and hiding it.

Combining of cryptography and steganography is suggested by many authors. They say that cryptography and steganography could be combined by encrypting the message then hiding it into a cover file. Although the idea has been discussed and suggested previously, research still active in this field as different encryption algorithms used with different steganography methods leads to different results regarding security, memory requirements, time, and memory and covert file space required for applying the techniques.

III. PROPOSED SYSTEM

In this work, information security utilizing information concealing image, audio and video Steganography with the assistance of PC measurable strategies gives better concealing limit we have taken a shot at concealing picture and content behind video and audio document and separated from an AVI record utilizing 4 minimum noteworthy piece insertion technique for video steganography and stage coding audio steganography.

Steganography is the strategy for concealing any mystery data like watchword, content and picture, audio behind unique spread record. Unique message is changed over into figure content by utilizing mystery key and after that covered up into the LSB of unique picture. The primary point is to shroud mystery data behind picture and audio of video record. As video is the use of numerous still casings of pictures and audio, we can choose any casing of video and audio for concealing our mystery information.

Suitable algorithm, for example, DES, 3DES or RSA encryption algorithm is utilized for cover file steganography suitable parameter of security and confirmation, thus information security can be expanded. Also, for information implanting we utilize 4LSB algorithm. This paper is using to send expansive information for data hiding in forbidden zone.

BLOCK DIAGRAM:

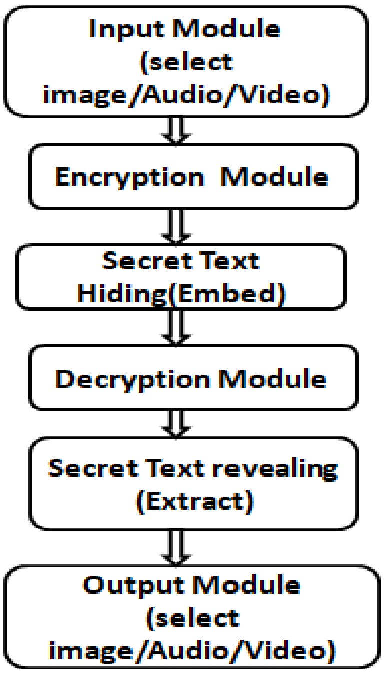

Input Module (select image/Audio/Video)
Encryption Module
Secret Text Hiding(Embed)
Decryption Module
Secret Text revealing (Extract)
Output Module (select image/Audio/Video)

Figure 1. Block Diagram

IV. IMPLEMENTATION

A. Input Module:

The Input Module is designed in such a way that the proposed system must be capable of handling any type of data formats, such as if the user wishes to hide any image format then it must be compatible with all usual image formats such as jpg, gif, bmp, it must be also compatible with video formats such as .avi, .flv, .wmf etc.. And also it must be compatible with various document formats, so that the user can be able to user any formats to hide the secret data.

B. Encryption Module

In Encryption module, it consists of Key file part, where key file can be specified with the password as a special security in it. Then the user can type the data or else can upload the data also though the browse button, when it is clicked the open file dialog box is opened and the user can select the secret message. Then the user can select the image, audio or video file through another open file dialog box which is opened when the cover file button is clicked. The user can select the cover file and then the Hide button is clicked so that the secret data or message is hidden in cover file using the Data Hiding Technique. And the user can select any encryption technique as DES, Triple DES or RSA Algorithm.

- **DES:**

  This module consists of same as Encryption and Decryption part using DES algorithm. DES takes 64-bit input and transforms it into a 64-bit output. The Data Encryption Standard (DES) is a block cipher that uses shared secret encryption.

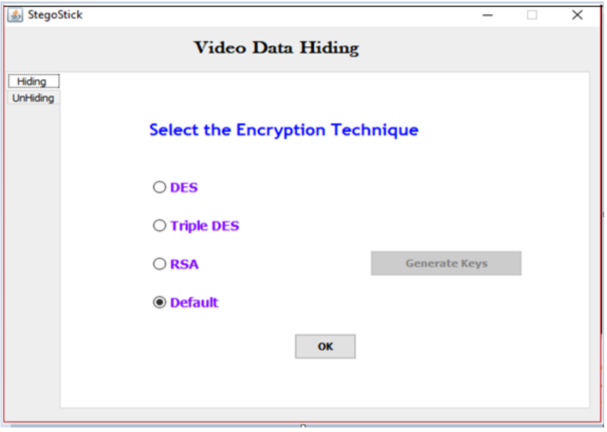
- **Triple DES:**

  This module consists of same as Encryption and Decryption part using Triple DES algorithm. Triple DES is the common name for the Triple Data Encryption Algorithm (TDEA or Triple DEA) block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. It uses three 56-bit DES keys which creates a key with the total length of 168 bits.

- **RSA:**

  This module consists of same as Encryption and Decryption part using RSA algorithm. RSA is the first algorithm known to be suitable for signing as well as encryption, and was one of the first great advances in public key cryptography. It is an asymmetric cryptographic algorithm.

  It is a block cipher in which the plaintext and cipher text are integers between 0 and n-1 for some n. A typical size for n is 1024 bits, or 309 decimal digits.



StegoStick

Video Data Hiding

Select the Encryption Technique

○ DES

○ Triple DES

○ RSA

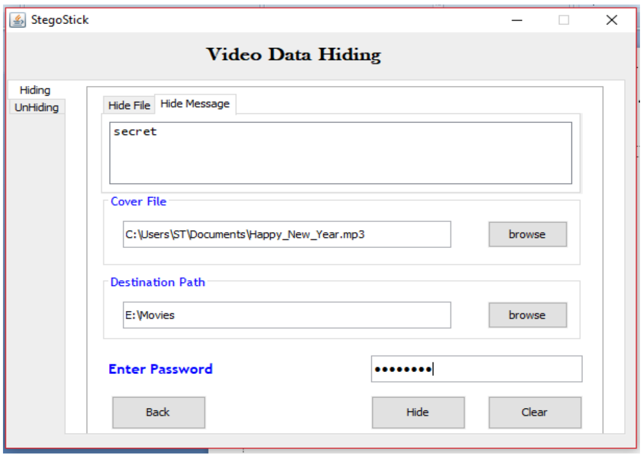
● Default

Figure 2. The user can select any encryption technique

C. Embedding Module:

In this the cover file will be embedded with secret text which is given by the user. In the embedding module, steganography is applied to hide the secret text. The intruders cannot attempt to break the embedded file and will not find changes in the cover file. Here, the user can particularly hide message or hide file and using the password it will be embedded. Then the user can upload into cloud storage and the file will be protected.

For implementing steganography proposed method is using 4LSB algorithm. Any data change in least significant bit does not change the value of data significantly. The basic selective encryption is based on the MPEG I-frame, P-frame, and B-frame structure. It encrypts the I-frame only because, conceptually P and B- frame are useless without knowing the corresponding I-frame.



StegoStick

Video Data Hiding

Hide Message: secret

Cover File: C:\Users\ST\Documents\Happy_New_Year.mp3

Destination Path: E:\Movies

Enter Password: ••••••••

Figure 3. Embedding process

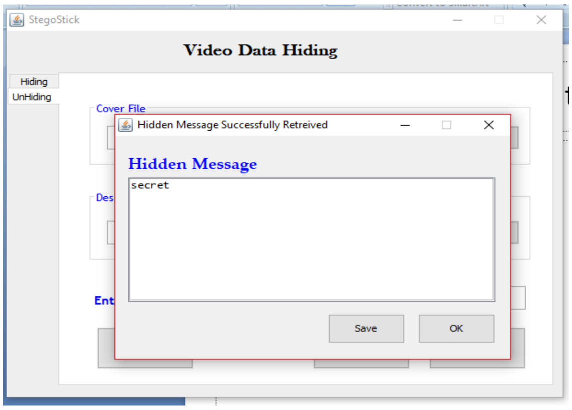
D. Decryption Module:

This module is the opposite as such as Encryption module where the Key file should be also specified same as that of encryption part. At receiver side, the user can retrieve the cloud storage without any damage or distortion in the file. If any loss or changes in the file we can easily find out in the file.

User should select the encrypted cover file and then should select the extract button so that the hidden message is displayed in the text area specified in the application or else it is extracted to the place where the user specifies it.

E. De-Embedding Module:

This module, the user can extract the hidden message/hidden file by using the steganography Algorithm from the cover file successfully by using the password. By means of simple rules applied to the frame markers, we introduce certain level of robustness against frame drop, repeat and insert attacks.



Hidden Message Successfully Retreived

Hidden Message

secret

Figure 4. De-embedding process

V. PERFORMANCE EVALUATION

Main purpose here is to calculate the Encryption and Decryption speed of each algorithm for different packet sizes. This implementation is tried to optimize the maximum performance for the algorithm. The throughput for encryption as well as decryption is calculated one by one. Encryption time is used to calculate the throughput of an encryption scheme.

A. Encryption Computation Time
B. Decryption Computation Time

The encryption algorithm is calculated by dividing the total plaintext in MB by total encryption time in Second for each algorithm. If the throughput value is increased, the power consumption of this encryption technique is decreased .Similar procedure has been followed to calculate the throughput of decryption scheme.

A. Comparative Execution Times(in Ms) of Encryption Algorithms with Different packet size:

Table 1

Input size in (Kbytes)	DES	3DES	RSA
50	31	56	56
108	35	48	40
246	46	109	110
320	80	165	162
695	145	227	212
781	86	171	165
900	241	301	260
5500	248	307	258
7311	1692	178	1365
22300	1716	179	1366
Average Time	432	496	399.4
Throughput (MegaBytes/Sec)	8.64	7.52	9.35

B. Comparative Execution Times(in Ms) of Decryption Algorithms with Different packet size:

Table 2

Input size in (Kbytes)	DES	3DES	RSA
50	51	54	64
108	47	50	57
246	71	75	75
320	73	85	147
695	121	149	144
781	121	153	152
900	152	171	172
5500	166	178	170
7311	954	110	880
22300	119	170	883
Average Time	295	371	274
Throughput (MegaBytes/Sec)	12.6	10.0	13.6

VI. CONCLUSION

In this proposed work, the user can select any multimedia files to store/retrieve in cloud server and it provides efficient ways to transfer data securely. The goal of the technique is difficult for the unauthorized person to determine the presence of secret text and the security is increased more. So the proposed technique fulfills the requirement of steganography technique.

VII. REFERENCES

[1] Priyanka mathur, Shambhu adhikari, ”Data Hiding In Digital Images Using Stagnography Paradigm” ,ISSN: 2393-2835,Issue-2, Feb.-2017, pages: 98-102.

[2] B.Chitradevi, N.Thinaharan and M.Vasanthi, “Data Hiding Using Least Significant Bit Steganography in Digital Images”, ISSN: 2349 – 4891, 2017, pages: 144-150.

[3] Jasril, Ismail Marzuki, Faisal Rahmat, “Capacity Enhancement Of Messages Concealment In Image And Audio Steganography”, vol-6, pages: 1970-1985.

[4] Neeraj Kumari and Babita Yadav, “Audio Steganography”, ISSN: 2349-6002, IJIRT-144526 ,pages: 115-119.

[5] Hazem Kathem Qattous,"Hiding Encrypted Data into Audio File", vol-17, No-6, June 2017,pages: 162- 170.

[6] Sonali Ranaa and Rosepreet Kaur Bhogal, "A Highly Secure Video Steganography using LSB Insertion Technique", ISSN : 0974-5572 , pages: 76-80.

[7] S.Kamesh K.Durga Devi, S.N.V.P.Raviteja, "Dwt Based Data Hiding Using Video Steganography", ISSN: 2277-9655, pages: 361-367.

[8] Harshitha H.P, Navya R Kumar, Sindhu N, Uthpala S, Darshan K R, "Multimedia Data Hiding in Video Using Selective Bit Technique", ISSN (O): 2348-4098 , ISSN (P): 2395-4752.

[9] Ms.Prachi P. Sadawarte, Prof. P. A. Tijare, "Video data hiding using Video Steganography ", DOI: 10.17148, JARCCE, 2017, 6271, pages: 305-308.

[10] Gat Pooja Rajkumar , Dr V. S. Malemath, "Video Steganography: Secure Data Hiding Technique", DOI: 10.5815/ijcnis.2017.09.05, pages: 38-45.

[11] Divya Prasannan 1, Renjith Thomas, "Hybrid Technique for Hiding Data Inside Video Using Combined Cryptography and Steganography", DOI:10.15680/IJIRSET. 2017.0605061, pages: 7775- 7779.

[12] D. Jagadish, K. Sindhu Priya, V. Saranya, B. Akshaya, T. Mahalakshmi, "Secure Data Transfer in Double Image Using Reversible Data Hiding Technique", Issue 6: March 2017, ISSN: 0974-2115, pages: 162-166.

[13] Maria Michael.E, Mr.Harikrishnan.N, " Audio Copyright Protection against Various Attacks" , Issue – May 2017, ISSN: 2348 – 8549, pages: 14-19.

[14] Shreya Jain, Santhosh Kumar Banoth, "Improvised Image Steganography & Cryptography using LSB Information Hiding Algorithm", Vol. 5, Issue 04, 2017 | ISSN (online): 2321-0613, pages: 1239- 1243.

[15] Sachin Kumar, 2Sumit Dalal, 3Ravi Kant Kaushik," Optimization of Steganography on Audio Wave and Embedding Minimum and Maximum Message into Various Layers", ISSN : 2230-7109, IJECT Vol. 8, Issue 2, April - June 2017, pages: 99- 101.

[16] Deepa Verma, Mr. Pushpendra Singh, "SRWD Technique for Security Enhancement of Audio Steganography", Volume 5 Issue VI, June 2017, IC Value: 45.98 ISSN: 23, Pages: 1789-1792.