Scientific Journal of Impact Factor(SJIF): 4.14

e-ISSN(O): 2348-4470
p-ISSN(P): 2348-6406

International Journal of Advance Engineering and Research Development

Special Issue for ICPCDECT 2016,Volume 3 Issue 1

Data Hiding Behind Audio and Video

Rupali Kate[1], Amruta Badgujar[2], Aditya Nemade[3]

[1-3]*Computer, AISSMS IOIT*

Abstract — *Data encryption is an essential topic now a days due tremendous amount of hacking. The previous systems hid the data or relevant information behind audio and video files. We provide the similar way but differ in working and providing output. The previous versions had a distorted audio and video files which made the hackers easily hack the files. We are using the combination of various algorithms mainly RSA, DES, Triple DES for providing encryption security. Also the files we are targeting are all types of audio as well as video files for the cover whereas the hidden files can be of the format pdf, text, audio, video or message. The encryption will take place per frame. This forensics in computer will help keep secret information.*

Keywords- *Security, encryption, decryption, private key, public key.*

I. INTRODUCTION

Discrete cosine transform (DCT) is mostly used for hiding information behind any video in the program. Working of DCT is due to constant change of image in the video and hence human is unable to notice the change. To be more accurate DCT make different values of some portion of the image, it is rounding off the values. Taking an example that if the value is 4.679, it will round off to 5. Steganography in Audio/Video as well as in images is the same but the only difference is each frame in audio/video includes the information. Document include white spaces and tabs, but this will not make any difference or may create doubt that something is hidden behind the document or steganography is being used.

Motivation: Motivation of choosing this project was to hide any kind of data behind video as well as audio without any distortion of cover file.

Objective: Our system will hide any kind of data like pdf, document and text file behind audio and video.

II. RELATED WORK

Yugeshwari Kakde, Priyanka Gonnade, Prashant Dahiwale[1] To hide secret information behind image and audio of video file.

Mrudul Dixit, Nikita Bhide, Sanika Khankhoje, Rajashwini Ukarande [2] To hide any kind of files into a cover Video file.

Cbiswajita Datta, Souptik Tat, Samir Kumar Bandyopadhyay [3] Minimize the data lost.

S.G.Shelke, S.K.Jagtap [4] Pair of pixels from the carrier image, Large data storing, capacity with minimum distortion.

Sheetal A. Kulkarni , Shubhangi B. Patil [5] Audio signal encryption for robust hiding, Multiple times secret message encrypting procedure.

M. Radhika Mani, V. Lalithya, P.Swetha Rekha [6] Hide a secret message in every n^{th} letter of every word of a text message.

Prashant Johri, Arun Kumar, Amba [7] Embed the secret message in audio file in such a way the there will be as much as possible less distortion in the stego- audio file as compared to original audio file.

Ammar Odeh, Khaled Elleithy, Miad Faezipour, Eman Abdelfattah [8] Merging more than one algorithm to improve the hidden ratio range of the carrier file.

K.Thangadur, G.Sudha Devi [9] Using GIF and PNG file format for cover image for hiding data.

Qia Wang, Wenjun Zeng, Jun Tian [10] Compressive sensing based secure signal processing framework that enables simultaneous secure watermark detection and privacy preserving storage.

III. ARCHITECTURE OF THE SYSTEM

Our system is going to hide data like text, document, pdf and behind any audio and video. Firstly we are going to do encryption from the sending side and at the receiving end we are going to do decryption. For encryption and decryption we are going to need private key.

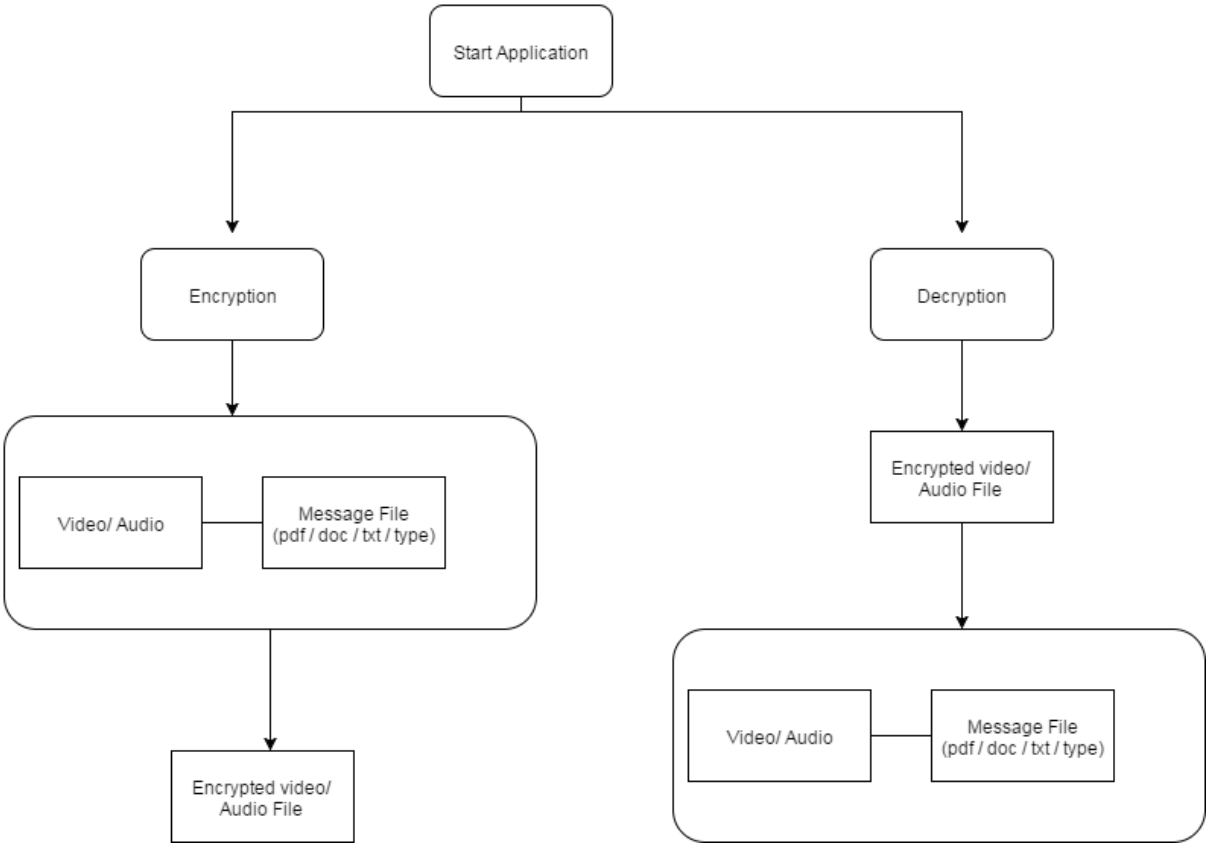

Fig.1 State Flow Diagram

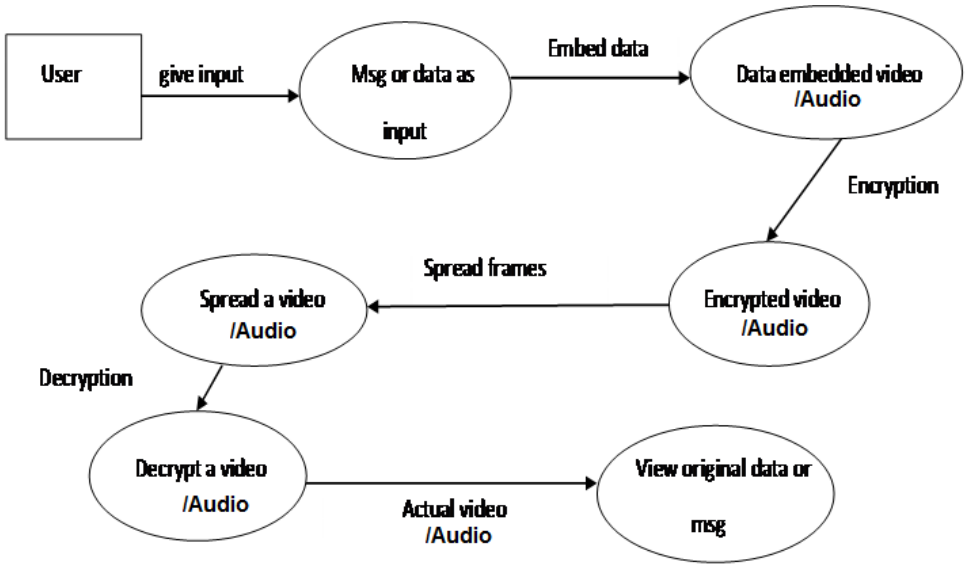

Fig.2 Architecture Diagram

IV. PROPOSED SYSTEM

Encryption safe guards computers which are connected through internet from hackers and online intruders. This process is mostly used in banks to safe guard the private information of the clients and they can transact easily through internet without any fraud. Encryption also helps in securing music, audio, video, etc. from internet thief's and hence it becomes compulsion to pay for any music, videos, audios, etc. which needs to be paid. This system will help in hiding the information behind audio/video having no idea about it to the third person. This system will help in department of defense and security.

V. PURPOSE

Due to this document we will be able to analyze the requirements of the existing system and also for the operating characteristics of the system. The main aim of the system is to hide the message in such a way that there should be no doubt that something is hidden i.e. hiding must be clean. The main aim of cryptography is that data should not be read by third person and that of steganography is that hiding data from third person using computer software, etc. with high privacy and check on privacy which is watermarking.

VI. SCOPE

This Document plays a vital role in the Software Development Life Cycle (SDLC) .This document gives a brief idea about the requirement of the system. This will be used by developers during basic testing phase. A formal approval be will be required if any changes are made to the requirements in future. Due to massive global availability of computer and internet, security is required at both final user and enterprise level. For so long, the computational security needs have been focused on various different features like identification, verification, confidentiality and secrecy.

Due to embedding of data, the pixels of cover data should not burst or degrade, also the data which is embedded should be as imperceptible as possible. The data embedded should remain safe from external modifications and attacks from hackers. Hence, before steganography, the data should be well encrypted

VII. MATHMATICAL MODEL

1. S is System such that S= {I, O, Su, F, SF}
2. I is the Input such that I= {video/audio, data}
3. O is the Output such that O= {Encrypted Video/audio}
4. Su is the Success such that Su= {Encrypted & Decrypted Successfully}
5. F is Failure such that F= {Invalid Input}
6. SF is set of Functions such that SF= {SF1,SF2,SF3,SF4}
7. SF1=Input Video
8. SF2=Input Data
9. SF3=Perform Encryption
10. SF4=Perform Decryption

11. Lets video/Audio = X1
    Split the stego video/audio into frames
12. Frames = images

    Frames = f1, f2 , f3, f4……fn

13. Lets data = D
    Split the Data into frames
14. Frames = d1, d2 , d3, d4……dn

15. Take one frame/image to operation

16. Split the image f1 into Red ,Green , Blue planes (R,G and B respectively)

17. For each pixel in R do following:

    6.1 let b[0]= LSB/RSA/DES /triple DES of the current pixel in R
    6.2 let b[1]= Next LSB/RSA/DES /triple DES of the current pixel in R
    6.3 if b=00 then
    Go to next pixel
    Else if b= 01 then
    Call recovery to recover secret data of data d1 from current pixel G
    De-scramble data of user with key k [1]
    Else if b= 10 then
    Call recovery to recover secret data of data d2 from current pixel B
    De-scramble data of user with key k [2]
    Call recovery to recover secret data of data d1 and data2 from current pixel of both
    G and B
    De-scramble data of user with data d1 and d2 with key k [1] and k[2] respectively Store the resulting data into video as a secret data.

VIII.ADVANTAGES AND DISADVANTAGES

- User cannot find the original data.
- It is not easily cracked.
- To increase the security.
- To increase the size of stored data.
- We can hide more than one bit.
- We can hide pdf/doc/txt files data as well as typing text.
- Video/audio not affected.
- If the quality of video is low then there are the chances of video getting distorted.
- Have the limitation of data that is to be hidden behind the actual data.

IX. SUMMARY AND CONCLUSION

In this project we gave an overview of steganography. It can hid the data behind the audio and video file using encryption-decryption method.We have also presented an image steganographic system using DES and triple DES, as well as RSA algorithm. Some advantages and disadvantages of implementing RSA on data hiding as a carrier. All these are definitely based on perceptual, transparency, hiding capacity, robustness and secure data transfer. This will lead us to define the best approach of steganography to hide information.

X. REFERENCES

[1] Nutzinger,M.C.Fabian, and M.Marschalek. ”Secure Hybrid Spread Spectrum System for Steganography in Auditive Media”. In Intelligent Information Hiding and Multimedia Signal Processing(IIH-MSP), 2010 Sixth International Conference.

[2] Changyong Xu et al “Steganography in Compressed Video Stream” First IEEE International Conference on Innovative Computing,
Information and Control 2006.

[3] ShengDun Hu et al "A Novel Video Steganography based on Nonuniform Rectangular Partition" The 14th IEEE International Conference on Computational Science and Engineering 2011.

[4] W. Jyun-Jie, C. Houshou, L. Chi-Yuan, and Y. Ting-Ya, "An embedding strategy for large payload using convolutional embedding codes," in *ITS Telecommunications (ITST), 2012 12th International Conference on*, 2012, pp. 365-369.

[5] C.S. Lu: Multimedia security: steganography and digital watermarking techniques for protection of intellectual property. Artech House, Inc (2003).

[6] Niels Provos, Peter Honeyman, Hide and Seek: Introduction to Steganography 2003.
[7] ShengDun Hu, KinTak U, ―A Novel Video Steganography based on Non-uniform Rectangular Partition,‖ The 14th IEEE conference on computational science and engineering 2011.

[8] N Sathisha1, Madhusudan G N, Bharathesh S, K Suresh Babu, K B Raja, Venugopal K R, ―Chaos based Spatial Domain Steganography using MSB,‖ 2010 5th International Conference on Industrial and Information Systems, ICIIS 2010, Jul 29 - Aug 01, 2010.

[9] Guo X., Song P., "Simulink Based LTE System Simulator", M. Sc.Thesis, Goteborg, Sweden, 2010

[10] Lubacz J., Mazurczyk W., Szczypiorski K., "Network Steganography", Telecommunication Review and Telecommunication News, in Polish, no 4/2010, pp. 134–135

