Impact Factor (SJIF): 5.301

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 5, Issue 6, June-2018

SECURE DATA HIDING IN AUDIO VIDEO STEGANALYSIS BY ANTIFORENSICS TECHNIQUE

Tejas Raut [1], Sameer Shegokar [2], Poonam Chaskar [3], Jyoti Bodake [4], Prof. Supriya Pawar [4]

[1] tejasraut322@gmail.com, [2] samshegokar2393@gmail.com, [3] poonamchaskar233@gmail.com ,
[4] jyotibodke158@gmail.com , [5]padalesupriya@gmail.com

[1]*Computer Engineering, Dr. D Y Patil COE, Ambi*
[2]*Computer Engineering, Dr. D Y Patil COE, Ambi*
[3]*Computer Engineering, Dr. D Y Patil COE, Ambi*
[4]*Computer Engineering, Dr. D Y Patil COE, Ambi*
[5]*Computer Engineering, Dr. D Y Patil COE, Ambi*

Abstract — *Steganography is the technique for concealing any mystery data like secret key, content, and picture, sound behind unique spread record. In this paper we proposed the sound feature crypto-steganography which is the blend of picture Steganography and sound steganography utilizing PC crime scene investigation method as an instrument for confirmation. Our point is to shroud mystery data behind picture and sound of feature document. As feature is the use of numerous still edges of pictures and sound, we can choose any casing of feature and sound for concealing our mystery information. Suitable calculation, for example, 4LSB is utilized for picture steganography and stage coding calculation for sound steganography. Suitable parameter of security and verification like PSNR, histogram is acquired at collector and transmitter side which are precisely indistinguishable, and subsequently information security can be expanded. This paper center the thought of network criminology method and its utilization of feature steganography in both investigative and security way.*

Keywords: *Audio Stegnography, Video Stegnography Data hiding, Stegnography, Histogram, Computer Forencies, Authentication*

I. INTRODUCTION

Stenography is the method of hiding any secret information like password, text and image, audio behind original cover file. Original message is converted into cipher text by using secret key and then hidden into the LSB of original image. The proposed system provides audio-video cryptostegnography which is the combination of image steganography and audio steganography using Forensics Technique as a tool to authentication. The main aim is to hide secret information behind image and audio of video file. As video is the application of many still frames of images and audio, we can select any frame of video and audio for hiding our secret data. Suitable algorithm such as LSB is used for image steganography suitable parameter of security and authentication like PSNR, histogram are obtained at receiver and transmitter side which are exactly identical , hence data security can be increased. This paper focus the idea of computer forensics technique and its use of video steganography in both investigative and security manner.

II. LITERATURE SURVEY

1. Data Hiding in Video
Author: Arup kumarBhaumik, Minkyachoi

Description:
We propose a video data embedding scheme in which the embedded signature data is reconstructed without knowing the original host video. The proposed method enables a high rate of data embedding and is robust to motion compensated coding, such as MPEG-2. Embedding is based on texture masking and utilizes a multidimensional lattice structure for encoding signature information. Signature data is embedded in individual video frames using the block DCT. The embedded frames are then MPEG-2 coded. At the receiver both the host and signature images are recovered from the embedded bit stream. We present examples of embedding image and video in video

2. Information Hiding in BMP Image Implementation, analysis Evaluation
Author: Alkhraisathabes.

Description:
Steganography comes from the Greek words Stefano's, roughly translating to covered writing. Stenographic techniques allow one party to communicate information to an- other without a third party even knowing that the communication is occurring. The ways to deliver these secret messages vary greatly. This paper explores several methods in detail, and attempts to test them out in code, and in practice, through several examples. The goal of steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second secret message present.

III.PROPOSED SYSTEM

- Information security using data hiding audio video stegnography with the help of computer forensic techniques provide better hiding capacity and security.
- Computer forensic technique at receiver side to cross check the security parameters and providing authentication at receiver side hence our data is triple secured.
- We are hiding encrypted data using stegnography and Cryptography behind selected frame of video using 4LSB insertion method and audio using phase coding algorithm transmitter side.

III. SYSTEM ARCHITECTURE

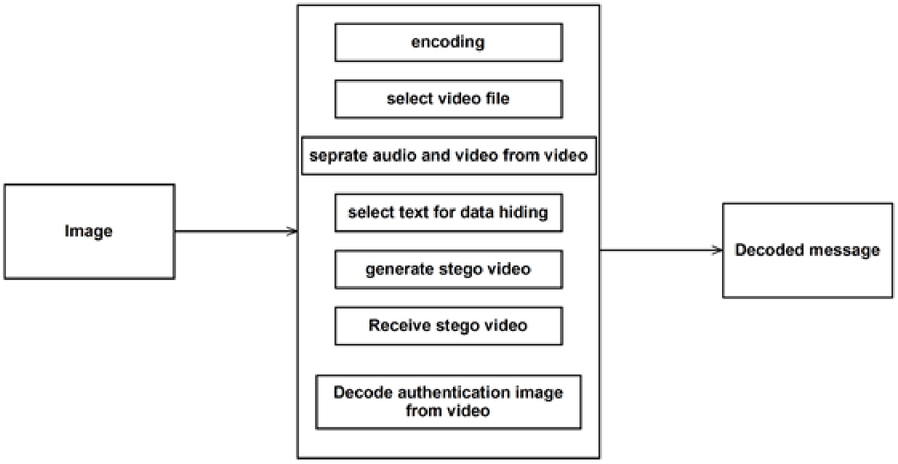


Image
encoding
select video file
seprate audio and video from video
select text for data hiding
generate stego video
Receive stego video
Decode authentication image from video
Decoded message

Selecting Audio Video File:
1. Select any available .avi audio-video file, behind which user want to hide data.
2. Separate audio and video from selected audio-video file using available software
3. Save audio file as .wav file, this is the original separated audio file.

Video Steganography:(At transmitter side)
1. Select original video .avi file. Read the file using VideoReader Function.
2. Collect all frames structure in one variable using mov function.
3. Read that structure. Play video using 'movie' function.
4. Accept one of the frame no. from user, behind which an authentication image is to be hidden.
5. Read that frame and store it in variable 'a'.
6. Select one of authentication image read that image and store it in variable 'b'.
7. To extract msb of frame, bitand frame with 240 using function 'bitand'.

8. To extract msb of authentication image, bitand image with 240 using function ‘bitand’.
9. Reverse the place of msb of authentication image to lsb by dividing each element by 16.
10. Reshape the image bits into one row.
11. This reshaped row vector of authentication image data is embedded on the frame matrix, by adding each row vector bits to last 4 bits of frame bits.
12. This forms a stego frame, overwriting this stego-frame with original video file create stego-video file.
13. Using WideoWriter’ function create new stego video file, in which authentication image is hidden.
14. Close the file.

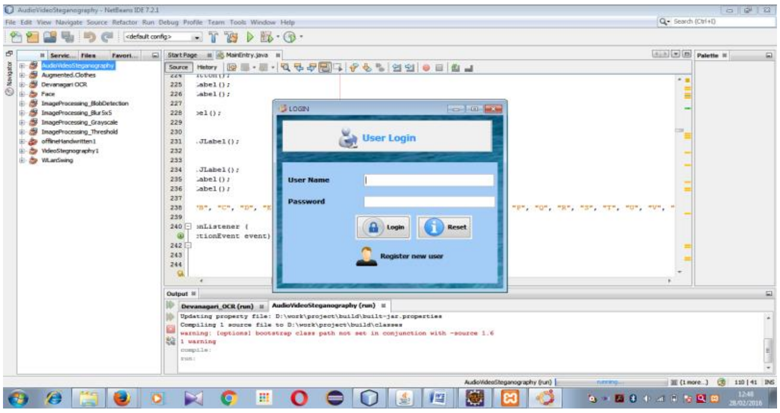
Creating Stego Audio File:
1. Combine stego audio and stego video file using Cute audio video marger.
2. This forms the stego audio-video file at transmitter side which has hidden text and image in it.

Authentication:
1.After transmission the stego audio-video file obtained at receiver side.
2. Read the stego audio video file, store the data in one variable al.
3. Select the frame no. The frame no. should be same at transmitter and receiver side, then only the authentication process start else it gets terminated.
4. To recover the authentication image from the selected frame bland the frame data with 15 using ’bitand’ function.
5. Authentication image data is available at Lsb of frame is recovered. It is in row vector.
6. Reshape the row vector data into matrix using ’reshape’ function.
7. Select the authentication image at receiver side. Compare recovered authenticated image with the selected image.
8. If both the images matched, then only user can recover the text behind audio else process is terminated.

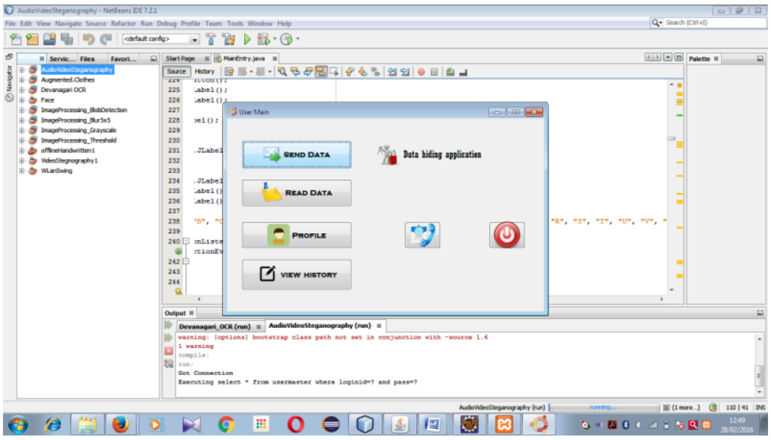
Audio Recovery:
1. Audio file is read using function ’wavread’, sample data is store in ’y’.
2. Open this stego audio file in re ad mode using function ’fopen’.
3. Read wave file’s first 40 bytes of header using ’tread’ function and store it in a variable ’header’.
4. Then read all its data after 40th byte using same function and store it in ’dtal’variable.
5. Close file using if closes function.
6. Recover the size of identity key from Isb of .wav file. Recover identity key from
further lsb bits of .wav file.
7. Accept identity key from user and compare entered identity key with recover identity key. If both the keys matched then only user can recover the hidden text else
processes will be aborted.
8. As identity key is matched recover the size of message from further Lsb bits of
.wav file. Recover the message.
9. Secrete text is recovered.

OUTPUT: Secrete text is recovered.

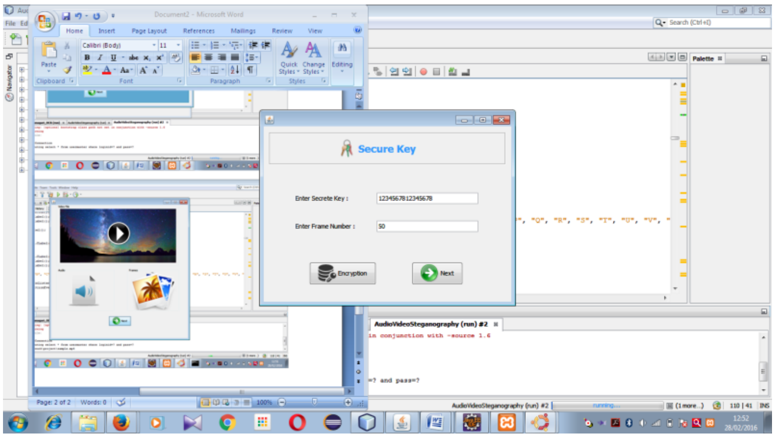
V. SNAPSHOTS



```
Updating property file: D:\work\project\build\built-jar.properties
Compiling 1 source file to D:\work\project\build\classes
warning: [options] bootstrap class path not set in conjunction with -source 1.6
1 warning
compile:
run:
```

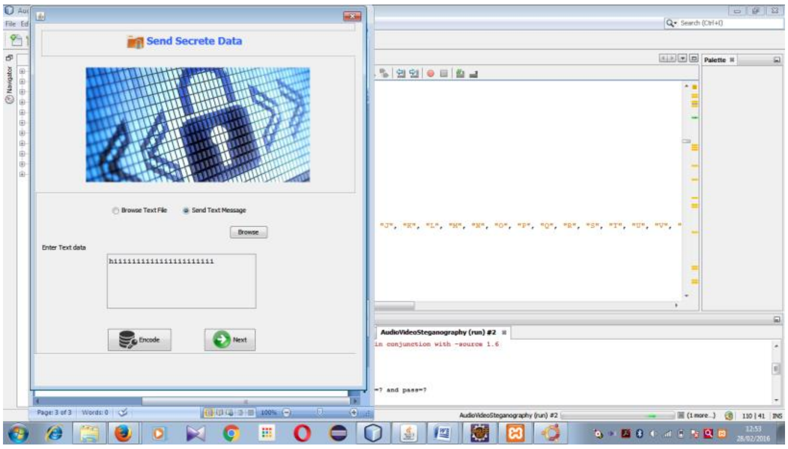


```
warning: [options] bootstrap class path not set in conjunction with -source 1.6
1 warning
compile:
run:
Got Connection
Executing select * from usermaster where loginid=? and pass=?
```



Enter Secrete Key : 1234567812345678

Enter Frame Number : 50



○ Browse Text File ● Send Text Message

Enter Text data: hiiiiiiiiiiiiiiiiiiiiii

V. CONCLUSION

In this paper we have introduced a robust method of imperceptible audio data hiding. This system is to provide a good, efficient method for hiding the data from hackers and sent to the destination in a safe manner. This proposed system will not change the size of the file even after encoding and also suitable for any type of audio file format. Thus we conclude that audio data hiding techniques can be used for a number of purposes other than covert communication or deniable data storage, information tracing and finger printing, tamper detection. As the sky is not limit so is not for the development. Man is now pushing away its own boundaries to make every thought possible. So similarly these operations described above can be further modified as it is in the world of information technology. After designing any operation every developer has a thought in his mind that he could develop it by adding more features to it.

REFERENCES

[1] Arup kumarBhaumik, Minkyachoi, Data Hiding in Video IEEE International journal of data base a application, vol 2no.2 june 2009. Pp.9-15

[2] Alkhraisathabes. Information Hiding in BMP Image Implementation, analysis Evaluation Information transmission in computer net- work, fall2006, Volume 52, issue, pp.1-10

[3] V.Sathya, k Balsubramaniyam, N, Murali, Data hiding in audio signal, video signal text and JPEG Image, IEEE ICAESM 2012, March 30-3-2012, pp741-746

[4] S. Gao, R. M. Zeng H. Jai,A A Detection algorithm of audio spared spectrum data hiding 2008 IEEE international conference, pp1-4.

[5] Wen Chao Yang, Che Yen Wen, Applying public key watermarking technique in forensic imaging to preserve the authenticity of the evidence ISI 2008 Workshop, LNCE 5075, Springer verlag Berlin Heidelberg, pp278-287.

[6] M,Pooyan, A, Delforouzi LSB based steganography method based on lifting wavelet transform 2007 IEEE International symposium on signal processing and information technology, pp600-603.

[7] SghierGuizani, Nidal Nasser, An Audio/Video Crypto Adaptive Optical Steganography Technique IEEE 2012 2012, pp, 1057-1062.

[8] Fatiha Djebbar,Ayady"A view on latest audio steganography techniques"IEEE International Conference on I nnovations in Information Technology2011.

[9] George Abboud, Jefiery Marean, "Steganography and cryptography in computer Forensics." 201 0 I EEE, Fifth international workshop on systematic application to digital Forensic application. pp. 25-30.

[10] Hamid A. Jalab, A.A.Zaidan "Frame selectionapproach for data hiding within MPEG Video us ing bit pla ne complexity segmentation" IEEE journal of computing, vo I,Issue 1,dec 2009.pp 108-112.