Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 4, April 2017, pg.356 – 362

Steganalysis by using Anti-Forensic Technique for Secure Data Hiding in Audio and Video

Mrs. Anjali Bhosale[1], Kumar Katake[2], Sayali Kamthe[3], Gaurav Kawade[4], Nikhil Khedekar[5]
Professor Computer Engineering, KJCOEMR, Pune, India
Student Computer Engineering, KJCOEMR, Pune, India
Student Computer Engineering, KJCOEMR, Pune, India
Student Computer Engineering, KJCOEMR, Pune, India
Student Computer Engineering, KJCOEMR, Pune, India
[1] anjali.bhosale6@gmail.com; [2] kumarkatake26@gmail.com; [3] sayalikamthe2495@gmail.com,
[4] gauravkawade5757@gmail.com, [5] nikhilkhedekar75@gmail.com

***Abstract*— Steganography is the technique to patch any secret data like key, content, and image, sound behind picture. In this method, the sound feature crypto steganography which is the combination of picture steganography and sound steganography utilizing cybercrime investigation method as a tool for communication. Our aim is to cover secret data behind picture and sound of feature document. An image steganography and audio steganography using for computer forensics technique as tool for authentication. Suitable calculation, for algorithm, 4LSB is utilized for picture steganography and stage coding calculation for sound steganography. The parameter of security and verification like PSNR, payload is acquired at collector and transmitter side which are precisely indistinguishable, and subsequently information security can be expanded. This method provides good security as well as we can use it in investigative security way.**

***Keywords*— 4LSB, Data Hiding, Steganography, Computer Forensics, Histogram, PSNR, Authentication**

I. INTRODUCTION

A steganography is really required for secured written work. This can be frequently accomplished by utilizing a unfold document and implanting the short message into this record. The final result could be a harmless trying record that contains the mystery message. Currently, it's increasing new presence with the momentum business requests for advanced watermarking and process of sound and have Steganography has seen exponential use following the Nineties. Stego algorithm downloads are accessible on the web as software package. All over throughout the planet currently utilize steganography for security and protection reason like as governments, military, organizations, and personal subjects The music and film industrial enterprises incessantly devise new material management techniques, as an example, reserving early conveyance of show screenings through steganography. As these days crime is in addition increasing exponentially and to take care of a

strategic distance from such computer sociology routines are used to achieve to the foundation and place the criminal behind the bars. A computer scientific and various alternative legal fields, like an example, computerized measurable, interchange data reposition sociology then on are growing quickly thanks to advances in computer frameworks and data reposition gadgets and additionally totally different computer specialized routines. During this manner there are totally different in private closely-held businesses are making and conducive money for improvement of various computer legal devices to research the knowledge on the online. "The goal of IADS is to integrate of these information Security and Authentication techniques for secured communication of 2 parties and maintain secrecy". Our aim is to secure communication over geographically distributed space and avoid cybercrime. A Video is assortment of still frame pictures and additionally consists audio, we select it as a carrier media for information transmission appropriate algorithmic rule like 4LSB is employed for image steganography and section secret writing algorithmic rule for audio steganography. As addition we tend to introduced FZDH (Forbidden zone data hiding algorithm)to avoid alteration of knowledge throughout method of knowledge activity and additionally cropping attack. With this planned system and use of FZDH will transfer video file with any format (such as .mp4, .3gpp, avi) as a video file. The security parameters and authentication like bar chart, PSNR will be obtained at receiver and transmitter facet that are specifically identical, so steganography is to cover secret information within the medium while not dynamical the general quality of canopy medium. In steganography actual data isn't maintained in its original format however regenerate in manner that may be hidden within transmission file e.g. image, video, audio. An ear recognition system is similar to face recognition system and which has five components: image acquisition, preprocessing, feature extraction, model training and template matching.

II. RELATED WORK

Arup kumar Bhaumi[2] He proposed a video knowledge embedding theme within which the embedded signature knowledge is reconstructed while not knowing the first host video. The projected technique allows a high rate of information embedding and is strong to motion salaried committal to writing, like MPEG-2.An Embedding relies on texture masking and utilizes a multi-dimensional lattice structure for secret writing signature info. Signature knowledge is embedded in individual video frames victimization the block DCT. The embedded frames are then MPEG-3 coded. At the receiver each the host and signature pictures are recovered from the embedded bit stream.

Disadvantages: Adversary knows about your message but can't read it.

The AES Algorithm :

- A byte substitution using a substitution table (S-box)
- Shifting rows of the State array by different offsets
- Mixing the data within each column of the State array
- Adding a Round Key to the State

S.Gao, R. M. Zeng H. Jai [4] Steganography means hiding a sensitive message. Information hiding technique is a new type of secret communication technology. Information hiding system uses multimedia object files like audio, images and text. Digital audio, images, text are increasingly furnished with distinguishing but imperceptible marks, which may contain a hidden copyright notice or serial number or even help to prevent unauthorized copying directly. Today the growth in the information technology, especially in computer networks such as internet, mobile communication and digital multimedia tools such as digital camera, handset video etc.

Sghier Guizani, Nidal Nasser [6]He focus on detecting the existing of data hidden in audio files with spread spectrum (SS) data hiding. SS data hiding is considered as a process of adding noise. The technology of classier and feature vector extraction are used to achieve the detection. First, we divide an audio signal into several frames. The wavelet coefficients before and after wavelet de-noise in each frame are calculated. Then, we pick some stat, of their difference as the feature vectors of the audio signal. Finally, according to the feature vectors of the audio signal, classier will decide whether the audio signal have been processed by SS or not. In our experiment, support vector machines (SVM) play role of classier, 600 audio _les are used to be our experiment samples. After the feature vectors of all the samples are calculated, those feature vectors of samples are divided into two parts. One is testing part and the other is training part. The result of experiment shows that if the strength of data hiding is higher than 0.005, the rate of correct detection of training part is higher than 86.5

Wen Chao Yang, Che Yen Wen[7]A method of passive steganalysis is proposed. We focus on detecting the existing of data hidden in audio files with spread spectrum (SS) data hiding. SS data hiding is considered as a process of adding noise. The technology of classifier and feature vector extraction are used to achieve the detection. First, we divide an audio signal into several frames. The wavelet coefficients before and after wavelet de-noise in each frame are calculated. Then, we pick some stat, of their difference as the feature vectors of the audio signal. Finally, according to the feature vectors of the audio signal, classifier will decide whether the audio signal have been processed by SS or not. In our experiment, support vector machines (SVM) play role of classifier, 600 audio files are used to be our experiment samples.

Disadvantages: when data hiding was done at the same time noise was added so data was not clear.
Problems and possible solutions:
Having stated that LSB insertion is good for steganography, we can try to improve one of its major drawbacks: the ease of extraction. We don't want that a malicious attacker be able to read everything we are sending. This is usually accomplished with two complementary techniques:
Encryption of the message, so that who extracts it must also decrypt it before it makes sense Randomizing the placement of the bits using a cryptographical random function (scattering), so that it's almost impossible to rebuild the message without knowing the seed for the random function.

III.PROPOSED SYSTEM

BLOCK DIAGRAM FOR STEGO AUDIO-VIDEO

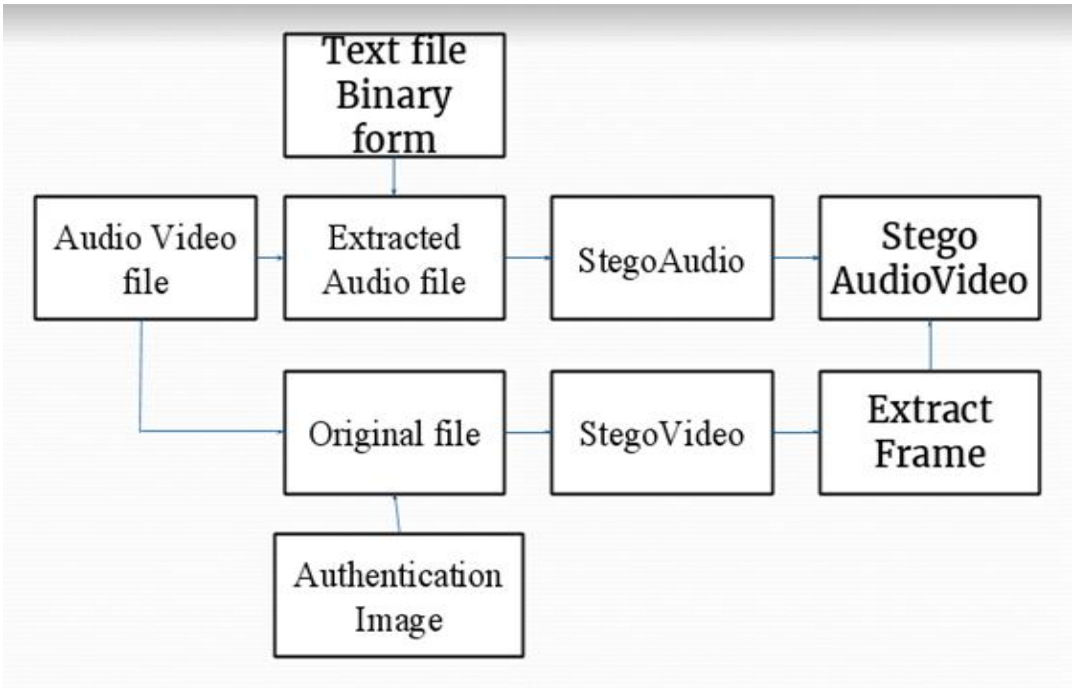

FIG.1 SYSTEM ARCHITECTURE FOR PROPOSED SYSTEM

In this paper we proposed audio video steganography with the assistance of different techniques offer higher concealing capability and security. The laptop rhetorical technique at receiver aspect are used to cross check the safety parameters and providing authentication at receiver aspect thence our knowledge is triple secured. A tendency to concealing encrypted knowledge victimization steganography and Cryptography behind hand-picked frame of video victimization 4LSB insertion technique and audio victimization part committal to writing rule transmitter aspect.

1. Choosing Audio – Video File
a. choose any accessible .Avi audio-video file, behind that user wish to cover knowledge.
b. Separate audio and video from hand-picked audio-video file victimization accessible software package 'Easy Audio-Video Separator'.
c. Save audio file as .wav file, this is often the first separated audio file.

2. Video Steganography:(At transmitter side)
In steganography of video file at transmitter aspect is perform during this module. 1st video file is chosen and hold on and every one of its frames are hold on. Then associate degree coding image is hide behind frame of video designated by users then all alternative perform are execute on it file.

3. Receiver aspect
Get the stego feature and split it into range of casings. 1. Take verification key from shopper and cross check it thereupon within the stego feature at indicated edge. Within the event that Authentication falls flat visit step seven typically proceed with; a pair of. Enter the pass-key once asked and pass-key chooses stego define aboard close casings. 3. Utilizing legal sciences check locality of any shrouded info. Within the event that legal check comes up short got step seven typically proceed. 4. Separate info from stego define by the use of opposite 4LSB calculation and store it in a very document.

4. Advantages
a. A first information cannot
b. It's not simply cracked.
c. To extend the safety.
d. To extend the scale of hold on knowledge.
e. We will hide over one bit.

ALGORITHM

A] Selecting Audio – Video File:

1. Select any .avi audio-video file, behind which user want to embed the data.

2. Separate audio and video from selected audio-video file using any software 'Audio-Video Separator'.

B] Video Steganography:(At transmitter side)

1. Select original video .avi file.

2. Collect all frame's structure in one

3. Accept any one frame no. from user, behind which an authentication image is to be hidden.

5. Accept that frame and store it.

6. Select one of authentication picture read that image and store it.
7. To extract MSB of frame, bitand frame with 240 using function 'bitand'.
8. This forms a stego frame, overwriting this stego-frame with original video file create stego-video file.
9. Generate new stego video file, in which authentication image is hidden.
10. Close the open file.

C] Creating Stego Audio File:
1. Merged stego audio and stego video
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. Accept the stego combination of audio video file, store the data in one variable 'a".
3. Select the frame number. The frame number should be same at sender and receiver side, then only the authentication process start else it gets failed.
4. To recover the authentication image from the selected frame bland the frame data.
5. The authentication image data is available at Least Significant Bit(LSB) of frame is recovered. LSB is in row vector.
7. Select the authentication image at receiver side. Compare recovered authenticated image with the selected image.
8. If both the images are same, then only user can recover the text behind audio else process is existed.

D] Audio Recovery:

1. Read the audio file and sample data is store in 'x'.

2. Open this stego audio file an read .

4. Then fetch all its data after 40th byte using same function and store it.

5. Close audio file.

6. Recover the size of identity key from LSB of audio file as well as recover key from LSB bits of .wav file.

7. Receive 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 terminated

8. If identity key is matched recover the size of message from further LSB bits of audio file and recover the accepted message.

9. finally it is recovered secrete text .

ACTIVITY DIAGRAM FOR SYSTEM

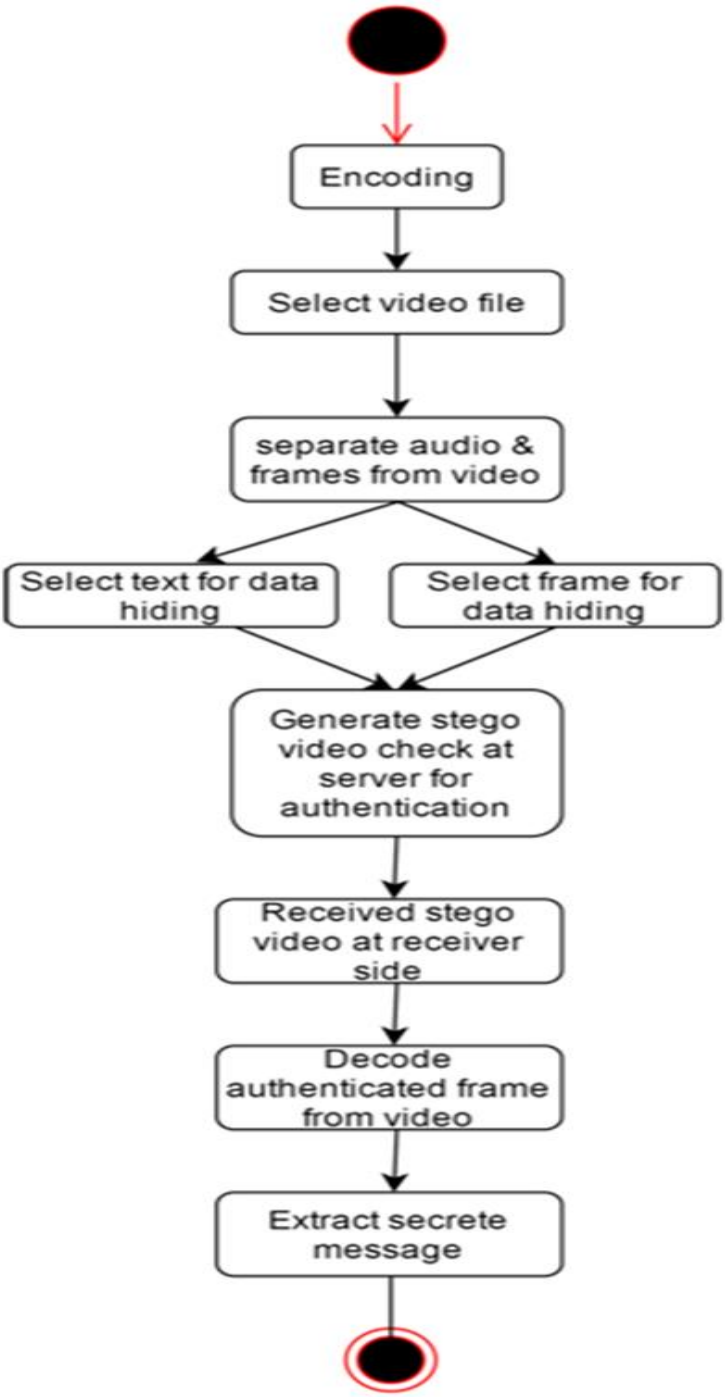

Fig.2 Activity Diagram

RESULTS AND DISCUSSION

The following fig 2. shows the browse the video file (.avi,mp4,3gp etc)from system. After browsing the video its generates different audio and video frames. Then it ask for secure key which is 16 bit and also frame number for more security. Then encrypt this secure key.

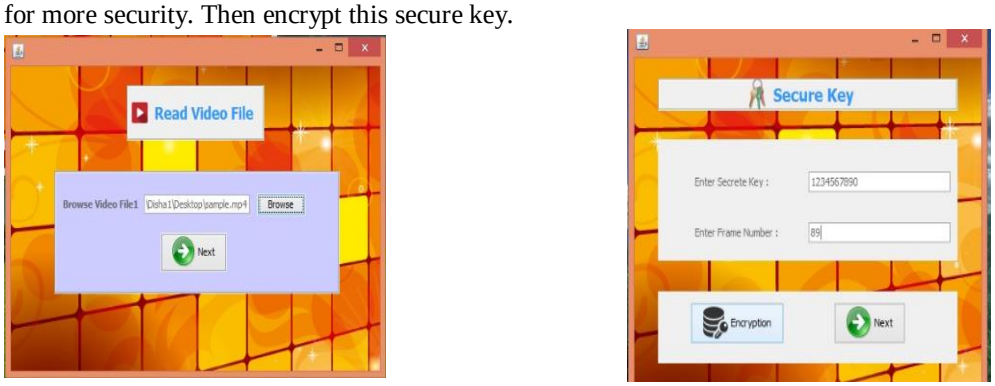

Fig 3:Selecting audio video file.

In below fig.4 after encrypting the secure key the video is play.Then you have to type the message or browse the file from text file and encrypt it into video. After adding message also the quality of video is maintained.

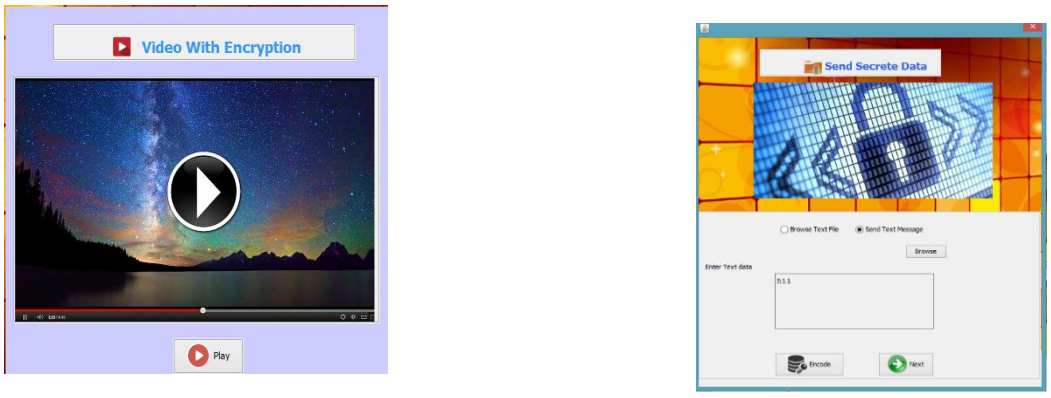

Fig 4: Encrypting the message into the audio video file

In below fig.5when message is encrypted into the video then read data is selected and after selecting it authentication window is open in that it ask for the frame number which sender have encrypted into it for security. that frame number can send through(mail,call,sms,etc).ehn correct frame number is entered receiver can see the message behind the video.

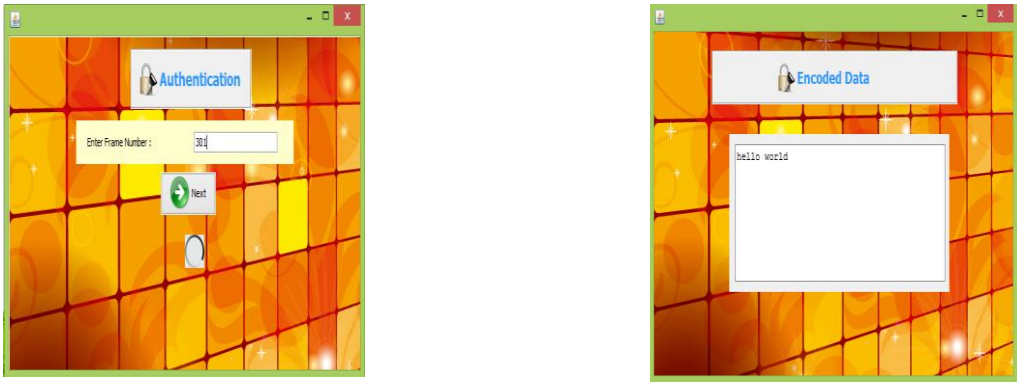

Fig 5: Entering the frame no for decrypting the message from audio video file

CONCLUSIONS

In this paper, we have used 4LSB algorithm to encrypt the secret data. And also we done steganalysis by FZDH to provides the security. The parameters are key, security, quality of video etc. By considering above parameters FZDH is better than existing system. A steganalysis by using anti forensic technique for secure data hiding in audio and video is our proposed system which follows these steps Framing, Blocking, Coefficient selection, Combination process etc.

ACKNOWLEDGEMENT

Thanks to our guide Prof. Anjali Bhosale, and KJCOEMR College for providing resources and helping us in all possible ways. We also thank readers of this journal for showing interest in this topic and contributing towards enhancement of this topic as well.

REFERENCES

[1] M. Krause and H. U. Simon, "Determining the optimal contrast for secret sharing schemes in visual cryptography," Combinatorics, Probab. Comput., vol. 12, no. 3, pp. 285–299, 2003.
[2] K.-H. Lee and P.-L. Chiu, "An extended visual cryptography algorithm for general access structures," IEEE Trans. Inf. Forensics Security, vol. 7, no. 1, pp. 219–229, Feb. 2012. [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
[3] S. Gao, R. M. Zeng H. Jai,A "A Detection algorithm of audio spared spectrum data hiding" 2008 IEEE international conference, pp1-4.
[4] SghierGuizani, Nidal Nasser, "An Audio/Video Crypto Adaptive Optical Steganography Technique" IEEE 2012 2012, pp, 1057-1062.
[5] Fatiha Djebbar,Ayady"A view on latest audio steganography techniques"IEEE International Conference on I nnovations in Information Technology2011.
[6] George Abboud, Jeffery Marean, "Steganography and cryptography in computer Forensics." 201 0 I EEE, Fifth international workshop on systematic application to digital Forensic application. pp. 25-30.
[7] 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.
[8] S. Cimato, R. De Prisco, and A. De Santis, "Optimal colored thresholdvisual cryptography schemes," Des., Codes Cryptogr., vol. 35, no. 3,pp. 311–335, Jun. 2005.
[9] S. Cimato and C.-N. Yang, Visual Cryptography and Secret ImageSharing. Boca Raton, FL, USA: CRC Press, 2012.
[10] P. D'Arco and R. De Prisco, "Secure two-party computation: A visualway," in Information Theoretic Security (Lecture Notes in ComputerScience). New York, NY, USA: Springer-Verlag, 2014, pp. 18–38.
[11] D. Wang, D. Lin, and X. Li, "Towards shift tolerant visual secretsharing schemes," IEEE Trans. Inf. Forensics Security, vol. 6, no. 2,pp. 323–337, Jun. 2011.

