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

Volume 3, Issue 11, November -2016

Review on audio-video Steganalysis

Kumar Katake[1], Sayali Kamthe[2], Nikhil Khedekar[3], Gaurav Kawade[4]

Department of Computer Engineering, K.J. College of Engineering and Management Research, pune

Abstract — *Steganography is the technique for embedding any secret data like key, content, and picture, sound behind image. In this method, the sound feature crypto steganography which is the combination of picture steganography and sound steganography utilizing PC crime scene investigation method as an instrument for confirmation. Our aim is to cover secret data behind picture and sound of feature document. In this method ,the audio video crypto steganography which is combination of image steganography and audio steganography using computer forensics technique as tool for authentication. Suitable calculation, for algorithm,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 method provides good security as well as we can use it investigative security way.*

Keywords- *4LSB, Data Hiding, Steganography, Computer Forensics, Histogram; PSNR, Authentication.*

I. INTRODUCTION

Steganography actually suggests that secured written work. Its can in all probability shroud the manner that correspondence is going on. this can be frequently accomplished by utilizing a (fairly extensive) unfold document and implanting the (somewhat short) mystery message into this record. the end result could be a harmless trying record (the stegofile) that contains the mystery message. Presently, 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 presently accessible on the web as software package. Governments, military, organizations, and personal subjects all over throughout the planet currently utilize steganography for security and protection reason. 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. computer scientific and various alternative legal fields, as 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 Moto is to secure communication over geographically distributed space and avoid cyber crime. Video is assortment of still frame pictures and additionally consists audio, we elect 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 information activity 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 .4mp, .3gp, .avi) as a canopy file. Security parameters and authentication like bar chart, PSNR will be obtained at receiver and transmitter facet that are specifically identical, so increasing information security.

II. INTRODUCTION TO INFORMATION SECURITY

In this digital world the information security and electronic communication is dynamical and Advancing day by day. the foremost excited factor is to understand that advancement in these fields had diode to the advance in secure information transmission. Broad band net connections virtually associate degree perfect transmission of information helps individuals to distribute massive transmission files and makes identical data copies of them. causation sensitive messages over net are transmitted in associate degree unsecured type however everybody possesses one thing to stay on the QT. The aim of steganography is to cover secret information within the quilt 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.

III. OVERVIEW OF SECURE DATA HIDDING

Traditional method for description of ear features and ear identification have been developed for more than 10years. During crime investigation, in the absence of (valid) fingerprints and footprints ear marks are used for identification. Just like fingerprints ,use of ear shapes recommends its use for human identification. 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. During image gaining, an image of the ear is captured, mostly with a camera. For preprocessing, standard techniques like histogram equalization and normalization are used. Ear recognition and identification has been done in many ways.

1) DATA HIDING IN VIDEO

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

The AES algorithm :

- 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

2) INFORMATION HIDING IN BMP IMAGE IMPLEMENTATION, ANALYSIS EVALUATION

Steganography comes from the Greek words steganos, roughly translating to “covered writing”. Steganography techniques enable one party to speak data to a different while not a 3rd party even knowing that the communication is going on. The ways in which to deliver these “secret messages” vary greatly. This paper explores many strategies well, and tries to check them get into code, and in follow, through many examples. “The goal of steganography is to cover messages within different harmless messages during a approach that doesn't enable any enemy to even sight that there's a second secret message gift.
Data Rate :
The most basic of LSBs insertion for 24bit pictures inserts 3 bits/pixel. Since every pixel is 24 bits, we can hide 3 hidden_bits/pixel / 24 data_bits/pixel = 1/8 hidden_bits/data_bits So for this case we hide 1 bit of the embedded message for every 8 bits of the cover image.If we pushed the insertion to include the second LSBs, the formula would change to: 6 hidden_bits/pixel / 24 data_bits/pixel = 2/8 hidden_bits/data_bits And we would hide 2 bits of the embedded message for every 8 bits of the cover image. Adding a thirdbit insertion, we would get: 9 hidden_bits/pixel / 24 data_bits/pixel = 3/8 hidden_bits/data_bits

3 DATA HIDING IN AUDIO SIGNAL, VIDEO SIGNAL TEXT AND JPEG IMAGE

Steganography suggests that concealing a message. info concealing technique may be a new reasonably secret communication technology. info concealing system uses transmission objects like audio, pictures and text. Digital audio, images, text are more and more furnished distinctive however invisible marks, which can contain a hidden copyright notice or serial variety or perhaps facilitate to stop unauthorized repeating directly. these days the expansion within the info technology, particularly in pc networks like net, mobile communication and digital transmission applications like photographic camera, phone video etc.
Disadvanges: The combination of multimedia data hiding was not possible.
LSB Technique:
The LSB is the lowest significant bit in the byte value of the image pixel.The LSB based image steganography embeds the secret in the least significant bits of pixel values of the cover image (CVR).The concept of LSB Embedding is simple. It exploits the fact that the level of precision in many image formats is far greater than that perceivable by average human vision. Therefore, an altered image with slight variations in its colours will be indistinguishable from the original by a human being, just by looking at it. In conventional LSB technique, which requires eight bytes of pixels to store 1byte of secret data but in proposed LSB technique, just four bytes of pixels are sufficient to hold one message byte. Rest of the bits in the pixels remains the same.

4 A DETECTION ALGORITHM OF AUDIO SPARED SPECTRUM DATA HIDING

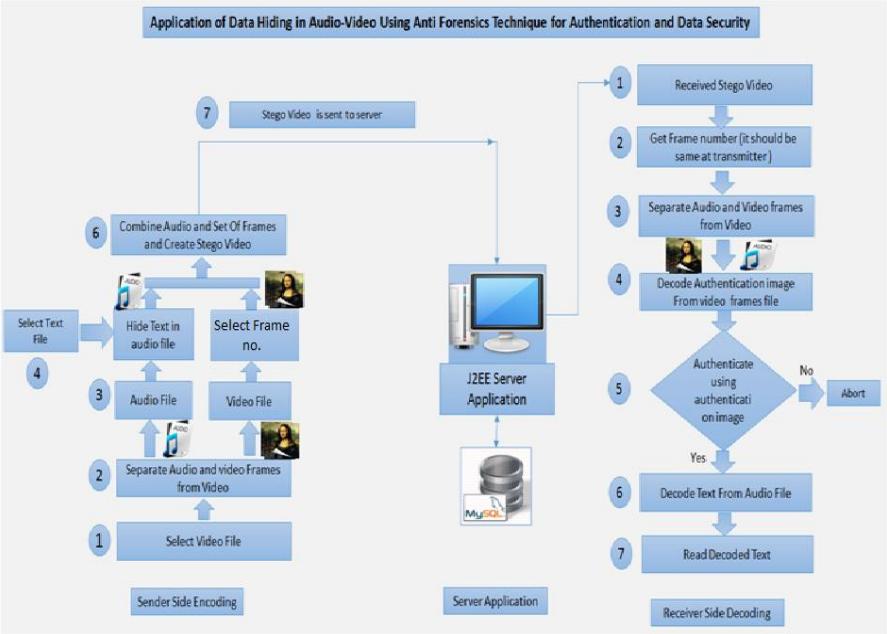
A method of passive steganalysis is proposed. We focus on detecting the existing of data hidden in audio files with spread spectrum (SS) data hiding. SS data hiding is considered as a process of adding noise. The technology of classifier and feature vector extraction are used to achieve the detection. 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.

IV. DATA HIDING OF AUDIO AND VIDEO BY ANTI FORENSIC TECHNIQUE

Information security victimization knowledge concealing audio video steganography with the assistance of laptop rhetorical techniques offer higher concealing capability and security. laptop rhetorical technique at receiver aspect to cross check the safety parameters and providing authentication at receiver aspect thence our knowledge is triple secured. we have 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.

3.1 choosing Audio – Video File

1. choose any accessible .avi audio-video file, behind that user wish to cover knowledge.
2. Separate audio and video from hand-picked audio-video file victimization accessible software package 'Easy Audio-Video Separator'.
3.Save audio file as .wav file, this is often the first separated audio file.



3.2 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 ar execute on it file.

3.3 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.

3.4 . Advantages

a. User cannot notice the initial knowledge.
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.

V. ALGORITHM

A. 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 'Easy Audio-Video Separator'.
3. Save audio file as .wav file, this is the original separated audio file.

B. Video Steganography:(At transmitter side)

1.Select original video .avi file. Read the file using 'VideoReader' Function.
2. Collect all frame's 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.

C. 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.

D. 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 ifcloses 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.

V. CONCLUSION

Data security utilizing data concealing sound feature steganography with the help of computer scientific methods offer higher concealing limit and security. In this paper we have compared data hiding methods. Anti forensic system is to provide a good, efficient method for hiding the data from hackers and sent to the destination in a safe manner. This system will not change the size of the file even after encoding and also suitable for any type of audio file format.

VI. ACKNOWLEDGMENT

We might want to thank the analysts and also distributers for making their assets accessible. We additionally appreciative to commentator for their significant recommendations furthermore thank the school powers for giving the obliged base and backing.

VII. REFRENCES

[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 network, 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.

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

[09] 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.

[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.

