Audio Video Steganography for Authentication and Data Security

[1]Yugeshwari Kakde, [2]Priyanka Gonnade,[3]Prashant Dahiwale
Rajiv Gandhi College of Engineering & Research
RTMNU Nagpur University
Nagpur, India

***Abstract*— Steganography is the art and science of writing messages which is to be hide behind original cover file which may be audio, video or image. In this paper we are working on audio-video steganography which is the combination of Audio steganography and Image steganography, in this we are using computer forensics technique for authentication purpose. In this paper our aim is to hide secret information behind audio and image of video file. As we know that video is the combination of many still frames of images and audio. We can select any frame of video and audio for hiding our secret data. This paper proposed an algorithm for hiding image in selected video sequence is an image-hiding technique based on Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) and random LSB (Least Significant Bit) audio steganography method for hiding secret text information inside audio of the audio-video file, it reduce embedding distortion of the host audio. This paper focuses the idea of computer forensics technique which is use as a tool for authentication and data security purpose and its use in video steganography in security manner.**

Index Terms- **Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD), LSB (Least Significant Bit), Computer Forensic.**

I. INTRODUCTION

Information security is very important part of IT industries in day today's life and it's a rapidly growing area in IT sector. Data hiding is one of the emerging techniques that provide for security by hiding secret information into the multimedia contents by altering some components in the host or cover file. Data hiding, Steganography, and Watermarking are three closely related fields that have a great deal of overlap and share many technical approaches as private, confidential and Secret data in modern society and because malicious hackers and intruders are using more and more sophisticated methods and technologies, developing powerful data protection become an urgent need and due to the ease with which multimedia content can be manipulated, measures to verify the authenticity of multimedia content are in pressing need. The objective of steganography is to hide secret information within a cover-media in such a way that others cannot discern the presence of the hidden secret information. In this paper our aim is to hide the fact that communication is taking place. This is often achieved by using a rather large cover file and embedding the rather short secret message into this cover file. The result is an innocuous looking file which is the stego file that contains the secret message. Figure 1 shows the general steganography operation.

Hiding information into a media requires following elements- The carrier (C) media file that will hold the hidden data. The secret message (*M*) may be plain text, cipher text or any type of data. The stego function (*Fe)* for data hiding and its inverse (Fe^{-1}) for extracting data. A stego-key (*K*) that specifies the location in carrier file where secret message is to be hidden. The stego function operates over cover media and the message (to be hidden) along with a stego-key to produce a stego file (*S*). The schematic of steganography operation is shown below.

In our paper as video is the application of many still frames of images and audio. We can select any single frame of video and audio for hiding our secret data. This paper provides an algorithm for hiding authentication image in selected video sequence by using Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD**)**.

And a random LSB (Least Significant Bit) audio steganography method it reduces quantization error of the host audio file Recently cyber-crimes are also increase and to avoid such computer forensic method is use to reach to the root and put the criminal behind the bars.

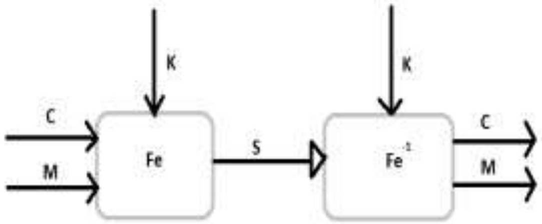


Fig 1.Steganography Operations

II. LITERATURE SURVEY

In [1] Data hiding in audio signal, video signal text and JPEG Images: In this paper the author introduced a robust method of imperceptible text, audio, video and image hiding. They provide an efficient method for hiding the data from hackers and it will sent to the receiver in a safe manner. Thus we know that data hiding techniques in audio, this can be used for number of purposes other than covert communication._In [3] Image hiding in video Sequence based on MSE: This paper proposes a method for hiding image in selected video sequence based on MSE. The proposed algorithm is an image-hiding scheme based on discrete wavelet transforms (DWT) and singular value decomposition (SVD). In this, the author is not directly embedding the secret image on the wavelet coefficients but on the singular values elements of the cover images DWT sub bands the cover image and they also find the SVD of the each block cover image or of the cover image, and then the singular values get modified to embed the watermark. First the video sequence and frame conversion is to be done. Calculate MSE for each frame and the watermark is to be embedded on a frame which has low MSE. The model proposed by the author is more secured against attacks and satisfied both imperceptibility and robustness. In [6] Steganography and cryptography in computer forensics: In this paper Computer forensic technique is use to find the parameter like height and width, frame number of data, PSNR, histogram of secrete message data before and after hiding to audio-video. If all these parameters are varified and found to be correct then only it will send to receiver otherwise it stop the secrete message data in computer forensic block. In [8] Anti-Forensics with steganography data embedding in digital images: In this paper digital images are used to communicate visual information. Author gives various forensic techniques which have been developed to verify the authenticity of digital images. They proposed a set of digital image forensic techniques capable of detecting global and local contrast enhancement, identifying the use of histogram equalization, and detection the global addition of noise to a previously JPEG compressed image.

III. PROPOSED SYSTEM

A. Proposed approach:

In this paper our aim is to hide secret information behind image and audio of video file. In image steganography technique we hide secret authentication image in color cover image which is nothing but the selected single frame in the video file using discrete wavelet transforms (DWT) and singular value decomposition (SVD) methods, and for audio steganographya random LSB (Least Significant Bit) method is used that reduces the embedding distortion of the host audio file. Computer forensic techniques at receiver side to cross check the security parameter and providing authentication image at receiver side hence our data is triple secured.

B. Proposed architecture:

In the following figure2, figure.3 and figure.4 the block diagram of hiding text information, authentication of received file and recovery of image using computer forensic techniques is shown. In Fig. 2 we have to select any available .avi audio-video file, behind which user wants to hide data. Separate audio and video from selected audio-video file, and save the audio in the video file in .wav format, then select the Separated audio wave file from for hiding secret text message behind the audio- wave file by using the random LSB method. In this the sender embeds the bits of secret text in a cover audio file using location selection inside the coefficient, which produces a Stego-audio-file

Procedure for hiding secret text message:

- Select a carrier wave file, where payload of audio file is directly proportional to size of carrier file.
- Select a secret message which may be available in the text file format.
- From the carrier 16 bit audio sample first (MSB) 2 bits to be read and converted into decimal value.
- That generated values which is nothing but the insertion position of the secret bit at the LSB of the same audio sample.

- Insert a secret bit into a selected position as explained by the previous step.
- Repeat the steps until all the secret text bit values are replaced.
- The secret message will embed inside the carrier file and save the resultant wave file.

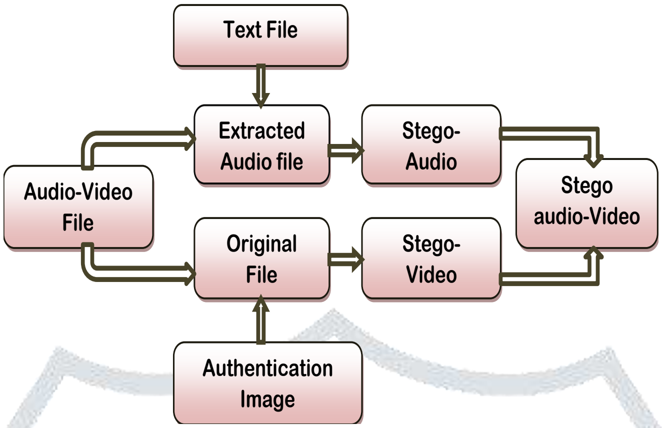


Fig.2: Block diagram of Hiding Text Information

Now, Select original video .avi file. Accept one of the frame no. from user, behind which an authentication image is to be hidden by using discrete wavelet transforms (DWT) and singular value decomposition (SVD).

Procedure for hiding authentication Image:

- Use one-level Haar -DWT to decompose the cover image A into four sub-bands (i.e. LL, LH, HL and HH).
- Apply SVD to LL sub-bands, i.e., $A = USV^T$
- Apply SVD i.e., $S + \alpha W = U_W S_W V_W^T$, where W is hidden image and α denotes the scale factor the scale factor is used to control the strength of the hidden to be inserted.
- Obtain the Hidden image AW by performing the inverse DWT using one set of modified DWT coefficients and three sets of no modified DWT coefficients.
- From this we get Stego-video file and random LSB (Least Significant Bit) audio steganography method that gives us a Stego-audio file.

.

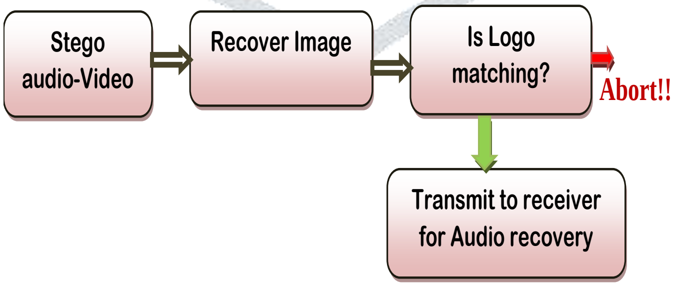


Fig. 3: Block diagram of Authentication of incoming .avi file

Then, Combine Stego-audio and Stego-video file, and we get Stego audio-video file. Transmit Stego audio- video file at the receiver side.

As shown in the following figure for authentication purpose match the logo with the hidden image to identify whether the received video is correct or not. In figure 3, after transmission the Stego audio-video file obtained at receiver side. Recover the authentication image from the selected frame, Compare recovered authenticated image with the selected image. If both the images matched, then only user can recover the text behind audio else process is terminated.

When authentication image are get matched we will send that stego audio-video file to the desired receiver for extracting secret text from stego-audio file.

In figure 4, at receiver side again separate audio and video from selected audio-video file. Select original video .avi file. Recover image by using discrete wavelet transforms (DWT) and singular value decomposition (SVD) method Andy using new 4th bit replacement LSB (Least Significant Bit) audio steganography recover the message.

Apply the following procedure for extracting authentication image from the stego-video file and secret text from the stego- audio file.

Procedure for extracting authentication image:

- Use one-level Haar DWT to decompose the hidden (possibly distorted) image A*W into four sub-bands: LL, LH, HL and HH.
- Apply SVD to the LL sub-band, i.e.,
- $A_W = US_W V^T$
- Compute $D^* = U_W S *V^T$,
- Extract the hidden image from LL sub-band.
- $W^*= (D^* – S)/\alpha$.
- End

Procedure for Extracting hidden text message:

- Select Stego-audio wave file
- First we have to select the random bits from the Stego-audio sample which was generated by the proposed way.
- If the secret message is present into the audio file then recognize the random bit positions and Decrypt the values using proposed algorithm
- Repeat the previous step until we will get the whole secret message.
- Save the resultant text file
- In this way, Secrete text is successfully get recovered from stego audio-video file by applying above procedure.

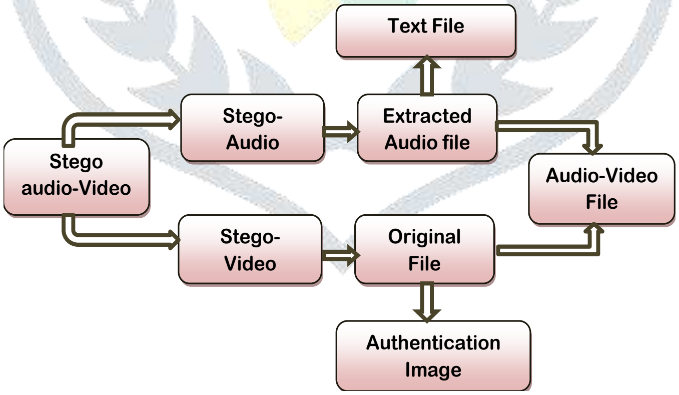


Fig .4: Block diagram of recovering of text information with authentication video.

Computer forensic

In various computer systems and data storage devices as well as computer communication methods like Computer forensic and many other forensic fields such as digital forensic and alternate data storage forensic etc. have been developing rapidly. Authentication part helps in differentiating fake video sending from transmitter to receiver using computer forensic check. Thus there are various private companies are developing and investing money for development of various computer forensic tools to analyze the data on the internet.

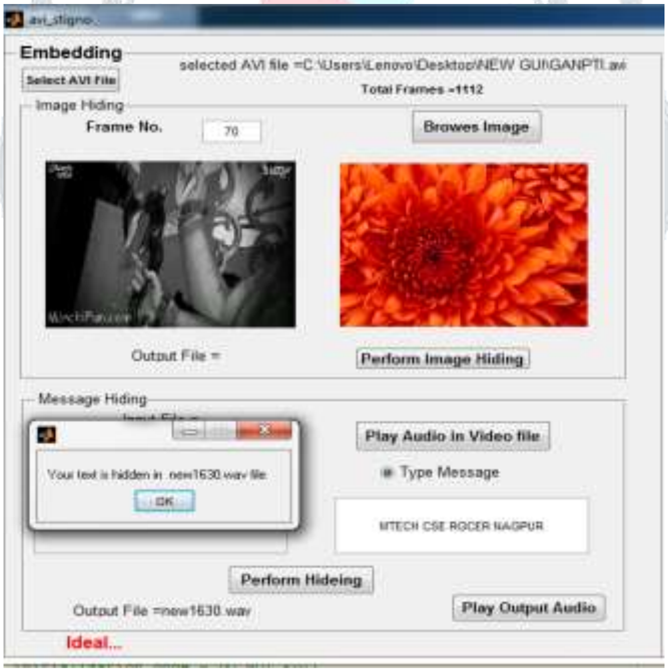
IV. RESULTS

A. Data hiding in audio:

- Read the audio file from the audio-video file by using MATLAB audioread() function and by using audiowrite() functions we can extract audio from Audio-Video file .
- Read the file using ‘wavread’ function. This function returns the sampled audio data, number of bits per second, and sampling frequency.
- Apply the random LSB algorithm for hiding the text message by selecting each secret bit is embedded into the selected position of a cover coefficient. The position for insertion of a secret bit is based on the upper two MSB (Most Significant Bit**)** of the host audio file from which the 0th (Least Significant Bit) to 3rd LSB is selected of the audio wave file up to length of the text file to hide the secret. .
- A new audio file get open in “write” mode with random name by using ‘’new’randname.wav’ function.
  From this we get the Stego-Audio wave file.

B. Data hiding in video:

- Here we are selecting one single frame in the Video file as a cover image
- Apply DWT on that frame, from this we get 4 bands(LL, HL, LH, HH)
  Then apply SVD on LL sub-band.
- Now we have an authentication logo which we want to hide inside the selected frame in the video.
- Apply SVD on that authentication image .i.e.,$S +\alpha W = U_W S_W V_W^T$, where W is hidden image and α denotes the scale factor the scale factor is used to control the strength of the hidden to be inserted. $A = US_W V^T$
- Obtain the Hidden image AW by performing the inverse DWT using one set of modified. DWT coefficients and three sets of no modified DWT coefficients.
- From this we get stego image which is nothing but the single encrypted frame in video file. Following figure. 6. Shows the original selected frame in the video and the authentication image which we have to hide in the original frame in video which is selected by the sender. After hiding the authentication image we get the encrypted and the encrypted video frame.



avi_stigno

Embedding

selected AVI file =C:\Users\Lenovo\Desktop\NEW GUI\GANPTI.avi

Total Frames =1112

Image Hiding

Frame No. 70

Output File =

Message Hiding

Your text is hidden in new1630.wav file

● Type Message

MTECH CSE RGCER NAGPUR

Output File =new1630.wav

Ideal...

Fig.5. Data is hidden Audio Video file.

From this we get the stego video frame, which contain the encrypted video frame.
Following figure 7. Shows the extraction module after successful extraction of the hidden authentication image it will show the dialog that “authentication was successful” and then only we can extract the text from the audio wave file.
Now from this we have the separate encrypted video file and the encrypted audio file separately that we can say the Stego-Audio file and Stego-Video file.

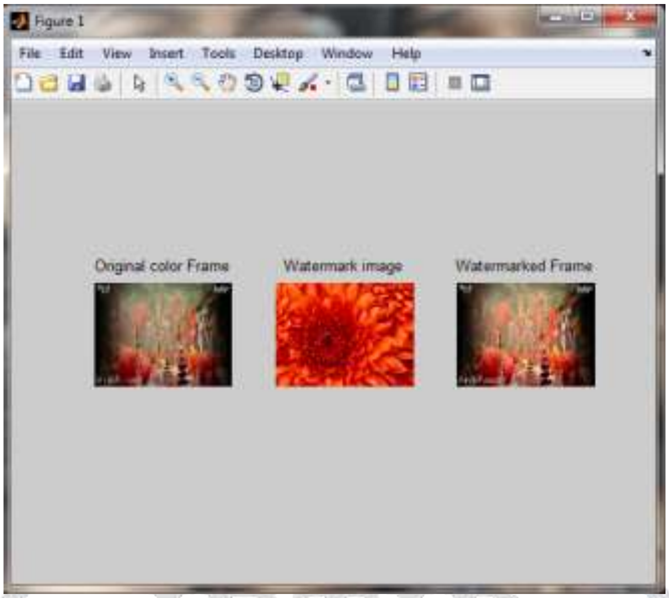
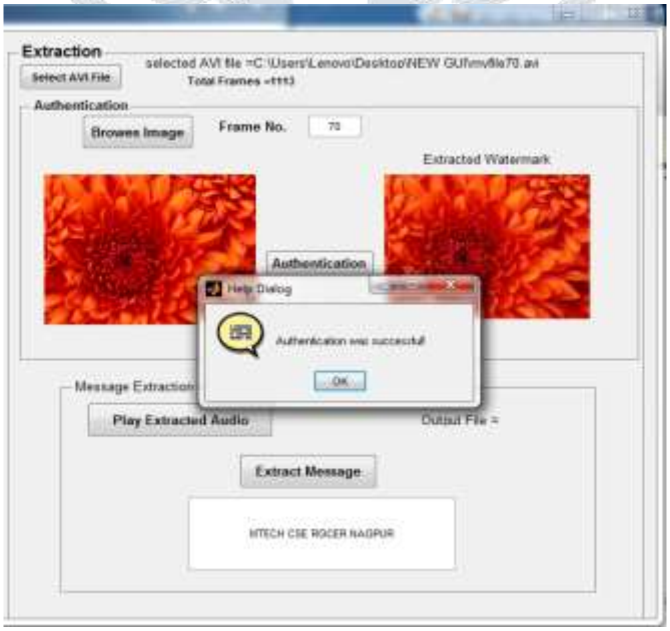


Fig. 6. Authentication Image is hidden in video

Following figure .7. Shows that we have to select the encrypted video file after this user have to give the correct frame number when we click on authentication button, if the images are same then it will show the dialog box “Authentication was Successful” and we can successfully extract the text from the audio wave file, otherwise if the images are not it will show the help dialog “Authentication Failure” and process get abort over there, In the following figure we successfully extract the text from the audio-video file.

- Now we have to merge that Stego-Audio and Stego-Video File by using MATLAB functions. From this we will get Stego Audio-Video file.
- Transmit that Stego Audio-Video File to the Receiver.
- At the receiver Side by using Computer Forensics technique match the logo with the authentication image by selecting the frame number.
- If the logo get match we will transmit it for audio recovery otherwise the process gets Abort.
- Receiver receives Stego Audio-Video file, Receiver Separate Audio from Stego Audio-Video file.
- We will read the random LSB of the Stego Audio wave then we will convert that bit stream into text message. And we will get our secret text as it is. And from Stego Video file we will get the authentication image



selected AVI file =C:\Users\Lenovo\Desktop\NEW GUI\mv6le70.avi
Total Frames =1113

Frame No. 70

Authentication was successful

Output File =

MTECH CSE RGCER NAGPUR

Fig 7. Image Authentication and data extraction.

V. CONCLUSION

Data hiding in audio video file with the help of computer forensic technique provide better hiding and security to the secret information. We are working on hiding image and text behind video and audio file and extracted from an .avi file at sender side and computer forensic techniques at receiver side to cross check the security parameter by providing authentication at receiver side hence our data is triple secured. We are hiding text into audio file successfully and also decode the audio file and extract the secrete text message. This method is very safe, secure and strong method of hiding secret information and achieving secrecy for the purpose of convenient communication between two parties. This is currently done in .avi file can be extended to any other video file format. We are using frequency domain techniques which improve security that can be used for detecting data presence in suspected multimedia file. It helps in detecting terrorist activities on web. We have obtained satisfactory result with audio and video steganography. Techniques like correlation, Entropy, PSNR, MSE can be used for detecting data presence in suspected multimedia file. It helps in detecting terrorist activities on web.

REFERENCES

[1] V. Sathya, K Balasubramaniyam, N Murali “Data hiding in audio signal, video signal text and JPEG Images" IEEICAESM 2012.Mrach 30-3 I 2012, pp74l -746.

[2] K. Bhowal, D. Bhattacharyya, A Pal, T-H Kim A GA basedaudio steganography with enhanced security, Telecommunication Systems April 2013, Volume 52, Issue 4, pp 2197-2204.

[3] A. Hamsathavani. “Image hiding in the video sequence based on MSE” International Journal of Electronics and Computer Science Engineering IJECSE, Volume1, Number 2013

[4] Che Yen Wen, Wen Chao Yang “ Applying a public key watermarking techniques in forensic imaging to preserve the authenticity of the evidence” ISI 2008 Workshop, LNCE 5075.Springer Verlag Berlin lleidelberg.Pp278-287.

[5] Nidal Nasser, Sghaier Guizani “An Audio/Video Crypto Adaptive Optical Steganography Technique "IEEE 20l2, pp. 1057-I062.

[6] George Abboud, Jeffery Marean, “Steganography and cryptography in computer forensics." 2010IEEE Fifth international workshop on systematic application to digital forensic application. pp. 25-30.

[7] Matthew CStamm, K.J Ray Liu. “Forensic detection of image manipulation using statistical intrinsic finger prints "IEEE transaction on information forensic and security, Vol .No.3 September 2010.pp492-506.

[8] Hung min Sun, Chi Yao Weng, Chin Feug Lee.“Anti-Forensics with steganography data embedding in digital images” IEEE journal on selected areas in Communication vol. 29.no.7 pp. 1392- 1403. August 2011.

[9] Lee, Y., Chen, L. “High capacity image steganography model”, IEEE Proceedings on Vision, Image and Signal Processing 2000, 147, 3, 288-294.

[10] P., Pitas, I., Nikolaidis N.: “Robust audio watermarking in the time domain”, IEEE Tran. on Multimedia, Volume 3, Issue 2, Page(s):232 –241. June 2001.

[11] Matthew C Stamm, K.J Ray Liu, “Forensic detection of image manipulation using statistical intrinsic fingerprints,’’ IEEE transaction on information forensic and security, Vol No.3September 2010,pp 492-506.

[12] Hung min Sun, Chi Yao Weng, Chin Feng Lee, “Anti Forensics with steganography data embedding in digital images,’’ IEEE journal on selected areas in communication, Vol, 29.No, 7August2011, pp.1392-1403.

[13] George Abboud, Jeffery Marean, “Steganography and visual cryptography in computer Forensics,” 2010 IEEE, Fifth international workshop on systematic approaches to digital Forensic application pp. 25-30.

[14] S. Katzenbeisser, F.A.P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Norwood, MA, 2000.