ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 5, Issue 5, May 2016

AUDIO-VIDEO STEGANOGRAPHY USING FACE RECOGNITION TECHNIQUE FOR AUTHENTICATION

Sumanth C, Dr. M B Meenavathi

Abstract - Steganography is a method of hiding any secret information like password, text, image and audio behind original cover file. In this paper we proposed the combination of image steganography and audio steganography with face recognition technology as a tool for authentication. Our aim is to hide the secret information behind audio and recipient's face image behind the video. As video is a application of many still frames of images and audio, we select any frame of video to hide recipient's face image and audio for hiding our secret data. Suitable algorithm such as improved LSB is used for image steganography and audio steganography, PCA algorithm is used for face recognition. Suitable parameter of security and authentication like PSNR, histogram are obtained at receiver and transmitter side which are exactly identical, hence the data security can be increased.

Keywords- improved LSB; Data Hiding; Steganography; face recognition; Histogram; PSNR; PCA; Authentication.

I. Introduction

Steganography literally means covered writing. Its goal 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 file. The result is an the stego file that contains the secret message. Now, it is gaining new popularity with the current industry demands for digital watermarking and fingerprinting of audio and video Steganography has seen exponential usage since the 1990s.Governments, military, businesses, and private citizens all over the world now use steganography for security and privacy purpose. The music and movie industries continually devise new material control methods such as watermarking early distribution of movie screenings via steganography. In "traitor tracing" each copy of a given movie contains a digital watermark with a unique serial number and the movie distributor knows to whom each serial number has been delivered. When a copy becomes compromised, the movie company only needs to extract the serial number from the copy in question and start tracing it to the point of origin. In "broadcast monitoring" broadcast detectors are used to extract the watermark of a given file or medium and report to the broadcasting events to notify the owner or distributor of broadcast status (medium was played, time and date). Thus for every nation it has become primary need to secure its border lines as well as the communication methods, which field are currently been most favored area of interest and importance. As the communication is majorly through internet it has become prime necessity for every nation to adopt some counter measures to foul use of internet.

II. RELATED WORKS

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 also find the SVD of the cover image or each block 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 [4] Applying public key watermark techniques in forensic imaging to preserve the authenticity of the evidence: In this paper public key Public key cryptography, infrastructure and watermarking techniques are used to design a novel encryption and decryption method using LSB algorithm by maintaining integrity using forensic imaging method .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 verified 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 point is to hide secret data behind picture and audio of video document. In picture steganography procedure we hide recipient's face picture in color cover image which is only the single frame in the video document utilizing Improved LSB method, and for audio steganography improved LSB method is used to hide text. Face recognition technique using PCA algorithm is used for providing authentication at receiver side hence our data is secured.

B. Proposed architecture:

In the following figure.1, figure.2 and figure.3 the block diagram of hiding text content in audio, recovery of text content from audio and face recognition methods is shown. In Fig. 1 we need to choose any accessible .avi sound video document, behind which sender needs to hide information. Separate audio and video from chose audio video document, and select the audio in the video record in .wav format, then select the Separated sound wave document for hiding secret instant message behind the audio wave document by utilizing the improved LSB method. In this the sender inserts the bits of secret data in cover audio file using location selection inside the coefficient, which produces a Stego audio file.

Technique 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 last (LSB) 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.
- Save the resultant wave file.

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 improved LSB method.

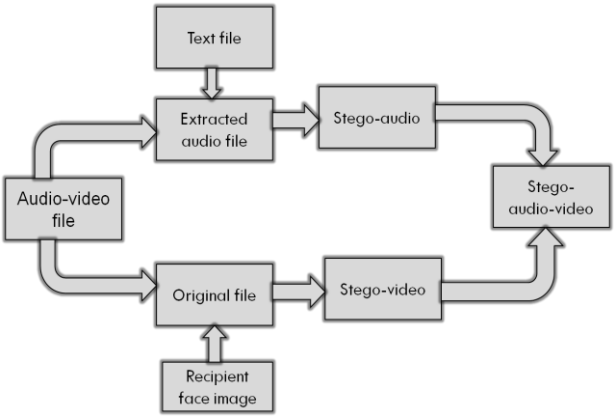

Fig.1: Block diagram of hiding Recipient face image and text information.

Technique for hiding authentication Face Image:

- Select the cover image.
- Multiply the red plane by 254 to make last bit0. Obtain first MSB i.e. eighth piece of secret image and after that inserted it in last LSB of red plane.
- Last LSB of red plane.
- Now take green plane of spread picture and change over its last 2 LSB's to 0. Acquire beside MSB i.e, seventh and sixth piece of secret image and installed it into green plane.
- Lastly take blue plane of spread picture and change over its last 3 LSBs to 0 multiply every pixel by 248.
- Get next 3 MSB i.e. fifth, fourth and third bit of secret image and implanted it into blue plane.

at that point, Combine Stego-audio and Stego-video document, and we get Stego sound video record. Transmit Stego audio video document at the receiver side. As appeared in the accompanying figure for validation reason coordinates the recipient's face with the concealed face picture. In figure 2, at receiver side again isolate audio and video from received audio video file. Select original video .avi file. Recover image by using improved LSB method .In figure 3, after transmission the Stego audio-video file obtained at receiver side. Recover the authentication recipient's face image from the selected frame, Compare recovered authenticated face image with the input image from webcam. If both the images matched, then only user can recover the text behind audio else process will wait until proper recipient appears in front of webcam. When authentication image are get matched we will be able to extract secret text from stego-audio file. Apply the following procedure for extracting authentication image from the stego-video file to match recipient's face image and secret text from the stego- audio file.

Technique for Extracting hidden text message:

- Select Stego-audio wave file
- First we have to select the LSB bits from the Stego-audio sample which was generated by the proposed way.

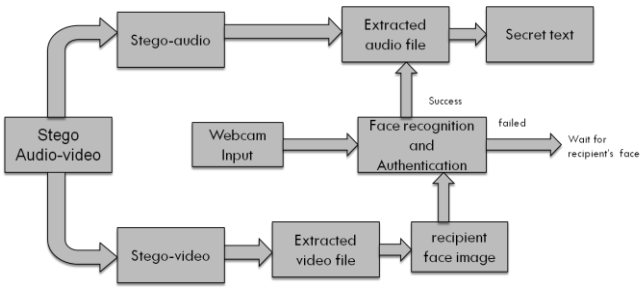

Fig.2: Block diagram of recovering of text information from stego-audio after Authentication.

- If the secret message is present into the audio file then recognize the 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.

IV. FACE RECOGNITION AND AUTHENTICATION

Our face-recognition framework comprises of three modules and every module is made out of a grouping of
steps

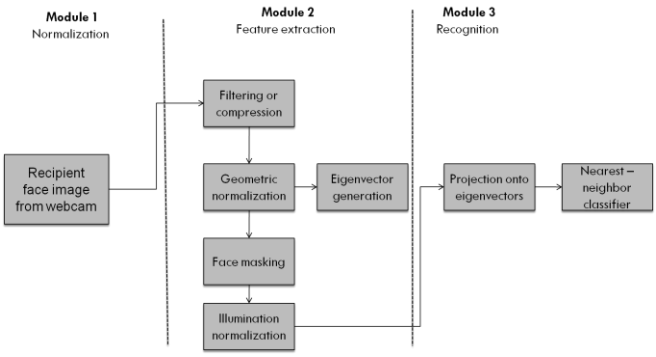

Fig.3: Face recognition system using PCA algorithm.

The first module normalizes the input image. The objective of the normalization module is to change the facial image into a standard format that evacuates or constricts varieties that can influence recognition performance. This module comprises of four stages. The initial step low-pass filters or compresses the original image. Images are filtered to remove high-frequency noise. A picture is compacted to spare storage room and lessen transmission time. The second step puts the face in a standard geometric position by turning, scaling, and interpreting the focal point of eyes to standard areas. The objective of this stride is to evacuate varieties in size, orientation, and location of the face in a image extracted from webcam. The third step masks background pixels, hair, and garments. This forestalls picture varieties that are not straightforwardly identified with the face from meddling with the distinguishing proof procedure. The fourth step lessens brightening variety among pictures, which is a basic component in calculation execution. The second module performs the PCA decomposition on the training set, which delivers the eigenvectors and eigenvalues. The second step distinguishes faces with a nearest neighbor classifier. On the other hand, all the more accurately, the classifier positions the gallery images by similarity to the probe. The critical design decision in this step is the similarity measure in the classifier.

V. RESULTS

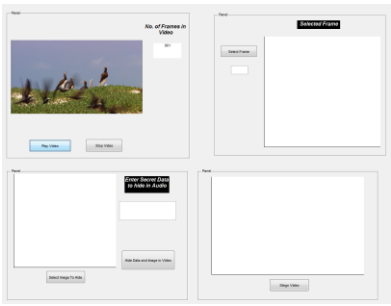

Fig.4: playing .avi file.

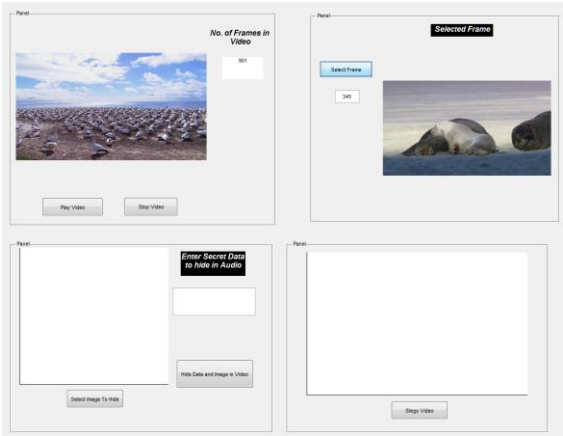

Fig.5: selecting single frame by its number.

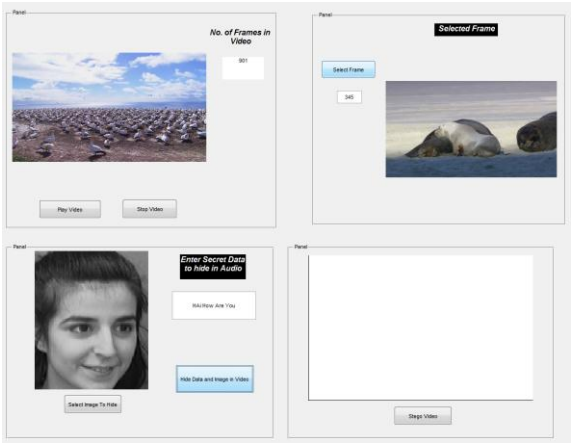

Fig.6: Recipient's face image to be hidden in frame.

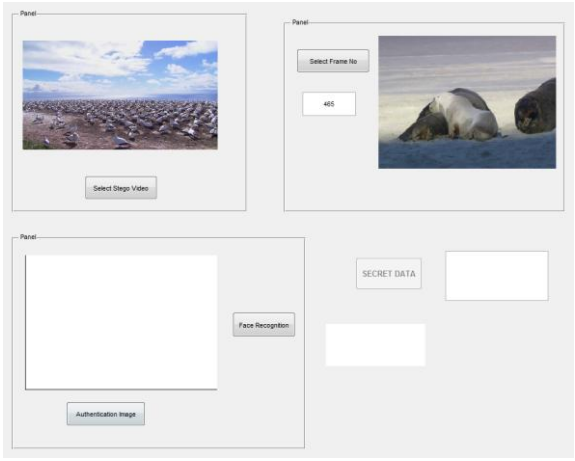

Fig.9: Receiver selects the frame number provided by sender

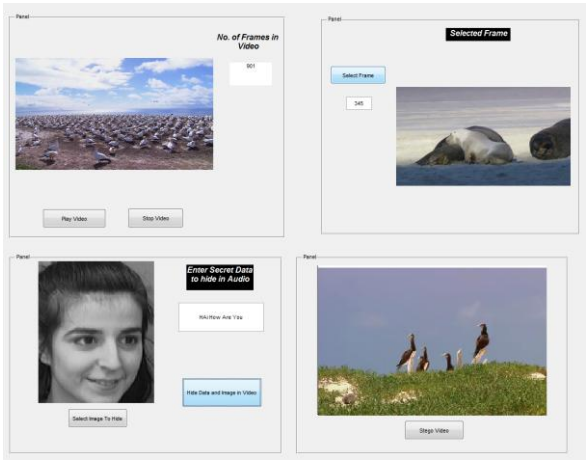

Fig.7: playing stego .avi file.

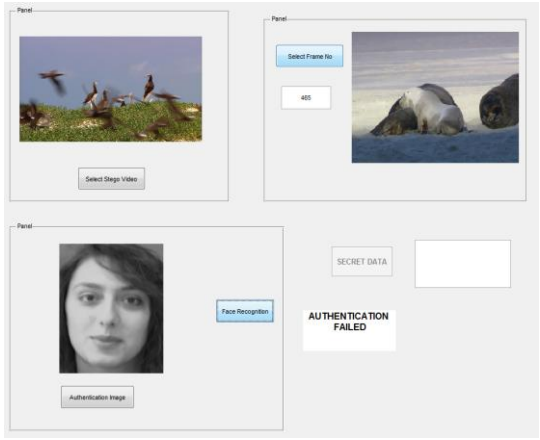

Fig.10: Authentication failed using face recognition technique

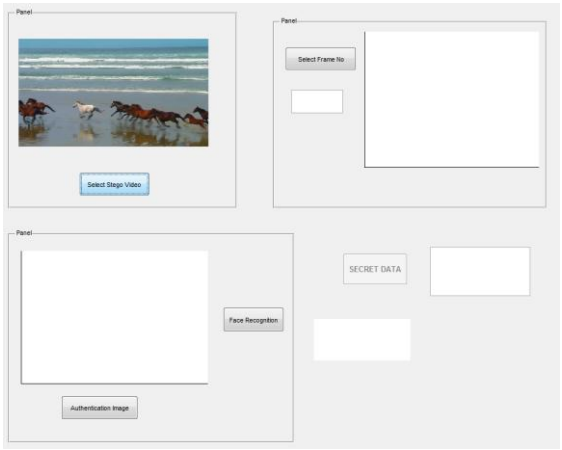

Fig.8: playing stego.avi file in at receiver.

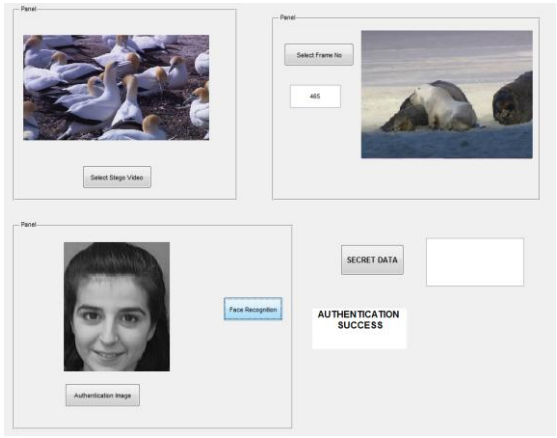

Fig.11: Authentication success using face recognition technique.

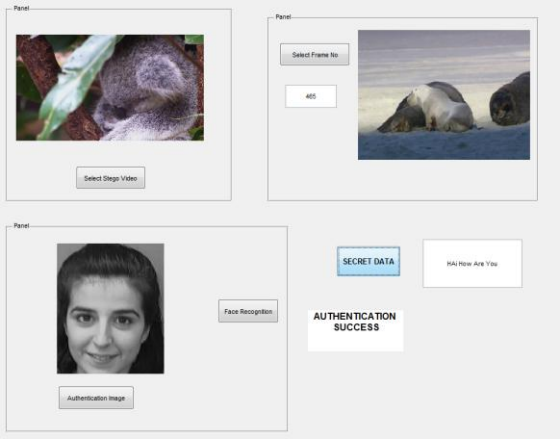

Fig.12: Authentication success so secret text in Audio is extracted.

VI. CONCLUSION

Data hiding in audio video file with the help of face authentication framework provides better hiding and security to the secret information. We are managing disguising picture and substance behind video and audio file and removed from an .avi file at sender side and face authentication technique at receiver side to cross check the security parameter by giving authentication at recipient side hereafter our data is significantly secured. We have hidden text information into audio archive successfully moreover interpret the audio file and focused to extract secret text. This system is especially shielded, secure and strong technique for hiding secret information and achieving secrecy with the final objective of worthwhile communication between two parties. This is now done in .avi file can be extended to whatever other video archive bunch. We have obtained appealing result with sound and video steganography authenticated by face recognition technique.

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 based audio 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. Pp 278-287.

[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.3 September 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.

Sumanth C received the B.E. degree in Electronics and Communication Engineering from visvesvaraya technological university, Karnataka, India in 2014. Presently he is pursuing his final year M.Tech with

specialization in signal processing Engineering in Bangalore Institute of Technology (BIT), Bangalore, Karnataka, India from Visvesvaraya Technological University, Karnataka, India. The proposed research work in this paper is part of his M.Tech thesis.

Dr. M B Meenavathi received the B.E. degree in Electronics and Communication Engineering from Mysore University, Karnataka, India, in 1989. She completed M.E. with specialization in Digital techniques and Instrumentation from university of Indore, Madhya Pradesh, India in 1994. She received Ph.D. form Department of Electronics and Communication Engineering, Dr. M G R University, Chennai in 2010.she is presently working as Professor and Head, Department of Electronics and Instrumentation Engineering, Bangalore Institute of Technology, Bangalore India. Her research interest include Image filter designs, Image restoration and segmentation.