ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

Implementation on Hiding Data and Image in Audio- Video Using Anti Forensics Technique

Vaishali Sarangpure [1], Prof. Roshani Talmale [2] , Prof. G.Rajesh babu [3]

Final Year M. Tech, Dept. of CSE, T.G.P.C.E.T, RTMNU, Nagpur, India[1]

Assistant Professor, Dept. of CSE, Tulsiramji , T.G.P.C.E.T, RTMNU, Nagpur, India[2]

Assistant Professor, Dept of CSE, T.G.P.C.E..T, RTMNU, Nagpur, India[3]

ABSTRACT: Security is most important issue in digital communication. Data security means protective digital privacy measures that are applied to prevent unauthorized access to computers, huge databases and online data it is also protects data from corruption. Security is most important issue in digital communication. Cryptography and steganography are two popular methods available to provide security. Steganography focuses on hiding information in such a way that the message is undetectable for outsiders and only appears to the sender and intended recipient. It is useful tool that allows covert transmission of information over and over communications channel. Steganography is a technique which is used to hide the message and prevent the detection of hidden message. Various modern techniques of steganography are: a) Video Steganography b)Audio Steganography
Audio Video stegnography is a modern stegnography of hiding information in a way that the unwanted people may not access the information. The propose method is to hide secret information and image behind the audio and video file respectively.

KEYWORDS: Stegnography,Audio Stegnography, Video Stegnogrpahy

I. INTRODUCTION

Popularity of digital media increase day to day its raise security related issues. Steganography is a Greek work Steganous meaning “covered” and graphy meaning “writing”. Now a days, digital media and network are getting more use and more popular. So that requirement of secure transmission of data also increased. Data Hiding is the technique of writing hidden messages in such a way that no one apart from the sender and intended recipient even realizes there is a hidden message. Steganography is a technique which is used to hide the message and prevent the detection of hidden message. Audio- video steganography is a modern way of hiding information in a way that the unwanted people may not access the information. In audio steganography consists of Carrier that is audio files and this file modified in such a way that they contain hidden information means data hide in the sound file and in video stegnography data is hide in video frame and these modifications must be done in such a way that data is recovery correctly without destroying the original signal.

II. RELATED WORK

There is different technique available for video steganography. [1] Advance video steganography algorithm describes data embedding and extraction for high resolution AVI videos. In this method instead of changing the LSB of the cover file, the LSB and LSB+3 bits are changed in alternate bytes of the cover file. There encrypt secret message using a simple bit exchange method before the actual embedding process starts**. [**2] Video Steganography for Hiding Image with Wavelet Coefficients**.** This method based on discrete wavelet transform and used random coefficient selection approach as well as the methods using the discrete wavelet transform.[3]

In this work author has aimed to hide secret information behind image and audio of video file. By embedding text behind audio file and an authentication image is embedded behind frames of video file. As video is the application of many still frames of audio and picture (i.e. image), any frame can be selected from video and signals from the audio for

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

hiding secret data. Authors have used 4LSB method for image steganography whereas Phase Coding algorithm for audio steganography. [3] An approach to hide data in video using steganography apply double hash function technique to choose a pixel from row and column. But after Appling the hash function on pixel may not found in the frame to resolve this problem using collision function. [4] Steganography In Mpeg Video Files Using Macro blocks Data Hiding Technique: Audio Steganography using LSB Technique in this technique use a flexible micorblocks ordering feature of H.264/AVC [7] have proposed a method which is an audio-video crypto- steganographic system, it is the combination of audio steganography and video steganography using advanced chaotic algorithm as the secure encryption method. Their aim is to hide secret information behind image and audio of video file. Since video is an application of many audio and video frames. A particular frame can be selected for image hiding and audio for hiding a secret data. They have used 4LSB substitution for image steganography and LSB substitution algorithm with location selection for audio steganography.

The use of the video based steganography can be more eligible than other multimedia files because of its size and memory requirements. Video are set of frames and the number of still pictures per unit of time of video ranges from six to eight frames per second. There are different type of video files like MPEG, AVI, MOV etc.

There are different technique and algorithm for video steganography like LSB substitution, Bit exchange method etc. The best technique is that hide Secret message without affecting the quality of video, structure and content of the video file. In video steganography after hiding a secrete data in video create "stego" video file which send to the receiver side. Proposed system introduce a novel and more secure method of video steganography.

III. PROPOSED ALGORITHM

In propose work we introduce novel method for audio video steganography. In this method we can hide secret image behind video and text behind audio. For video stegnography LSB algorithm is used and for audio stegnography parity algorithm is used. In proposed work sender used any audio video file and divide it separately as audio file and video file. After that image hide behind the video using passkey and video converted into "stego video" same as secret text hide behind the audio and audio become the "stego audio". These stego audio and stego video file combine and send to the receiver side.

At receiver side this stgo audio-video file again separated and using passkey. The secret image and data from stego video and stego audio recover respectively. Video is a set of images. It is an electronic medium. In audio steganography sound file is modified in a way they contain hidden information. In video per unit of time of video ranges from six to eight frames per second. Video stenography algorithm based on fact on each pixel represented by 3 bytes where each byte representing 3 primary colors that is red, green, blue (RGB).Size of image file is directly related to number of pixels and granularity of color definition. For hide a secrete image behind the video we need AVI audio video interleave) video. There are different format of video file like MPEG,MPG these all file first convert into AVI format first.

IV. AUDIO STEGNOGRAPHY

Audio steganography is a technique of hiding secret information in an innocent cover audio file. Audio steganography software can embed messages in WAV, AU, and even MP3 sound files. In this steganography sound file is modified in a way they contain hidden information. This modification done in such a way that secrete data must be secure and without destroying the original signal. Encoding secret messages in audio is the most challenging technique because the human auditory system (HAS) has such a dynamic range that it can listen over. Embedding secret messages in audio file is more difficult than embedding messages in digital image.

In the proposed system the algorithm used for audio stegnography is a parity coding Parity coding is one of the robust audio steganographic techniques. In parity coding Instead of breaking a signal into individual samples, breaks a signal into separate samples and embeds each bit of the secret message from a parity bit. If the parity bit of a selected region does not match the secret bit to be encoded, the process inverts the LSB of one of the samples in the region. Thus, the sender has more of a choice in encoding the secret bit. If the parity bit of a selected region does not

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

match the secret bit to be encoded, the process flips the LSB of one of the samples in the region. The sender has more of a choice in encoding the secret bit, and the signal can be changed in a more unobtrusive fashion

V. VIDEO STEGNOGRAPHY

Video is an electronic medium for the recording, copying and broadcasting of moving visual images. . The best technique is that to hide secret message without affecting the quality of video, structure and content of video. After hiding a secret data in video create "stego " video file which is send to the receiver.

VI. LSB (LSB LEAST SIGNIFICANT BIT HIDING)

Least significant bit (LSB) is the best method for data protection. In this method uses bits of each pixel of the image, it is necessary to use a lossless compression format, otherwise the hidden data will get lost in the transformations of a lossy compression algorithm. The algorithm we are used for hiding a secrete image 4 LSB. In this process of adjusting the least significant bit pixels of the carrier image. In this method some information from the pixel of the carrier video is replaced with the secrete image so that it can't be observed by the human visual system therefore it exploits some limitations of the human visual system. To our human eye, changes in the value of the LSB are imperceptible.

VII. CONCLUSION AND FUTURE WORK

The simulation results showed that the proposed algorithm performs better with the total transmission energy metric than the maximum number of hops metric. The proposed algorithm provides energy efficient path for data transmission and maximizes the lifetime of entire network. As the performance of the proposed algorithm is analyzed between two metrics in future with some modifications in design considerations the performance of the proposed algorithm can be compared with other energy efficient algorithm. We have used very small network of 5 nodes, as number of nodes increases the complexity will increase. We can increase the number of nodes and analyze the performance.

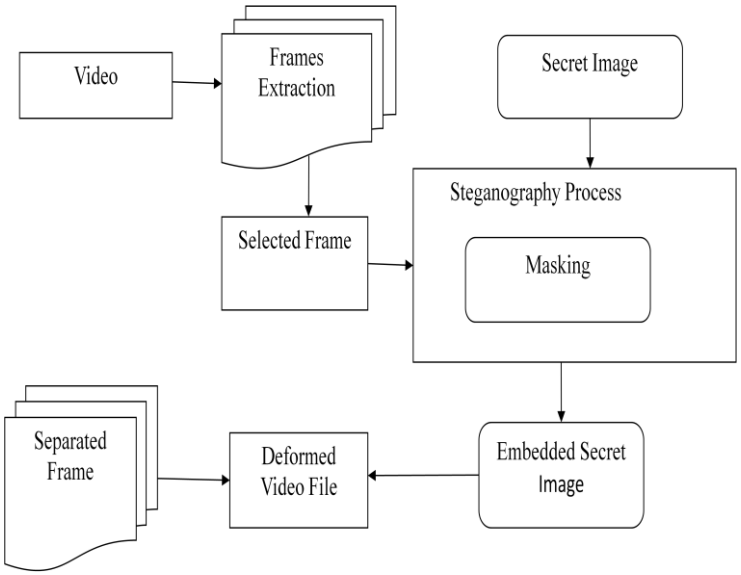

Fig 1 :-Hiding Image Behind Video File

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

VII. RESULT OF THE SYSTEM

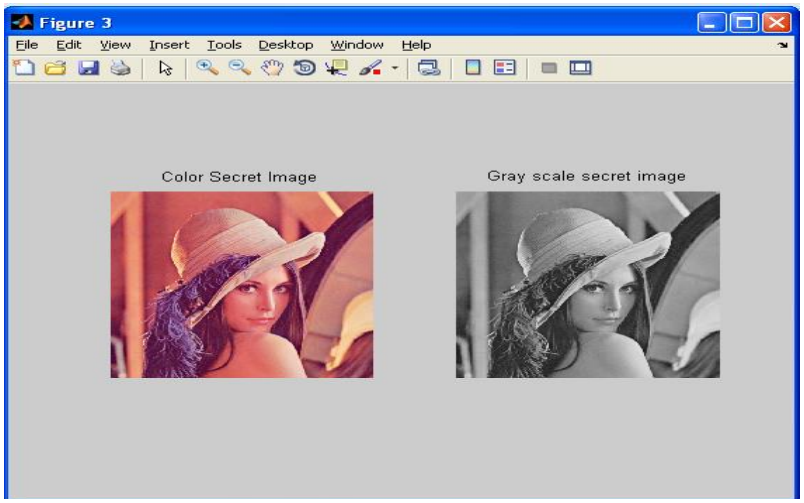

Fig 2:color image into grey scale image

This output form display the secrete image which want to be hide. The color image first converted into the grey scale image.

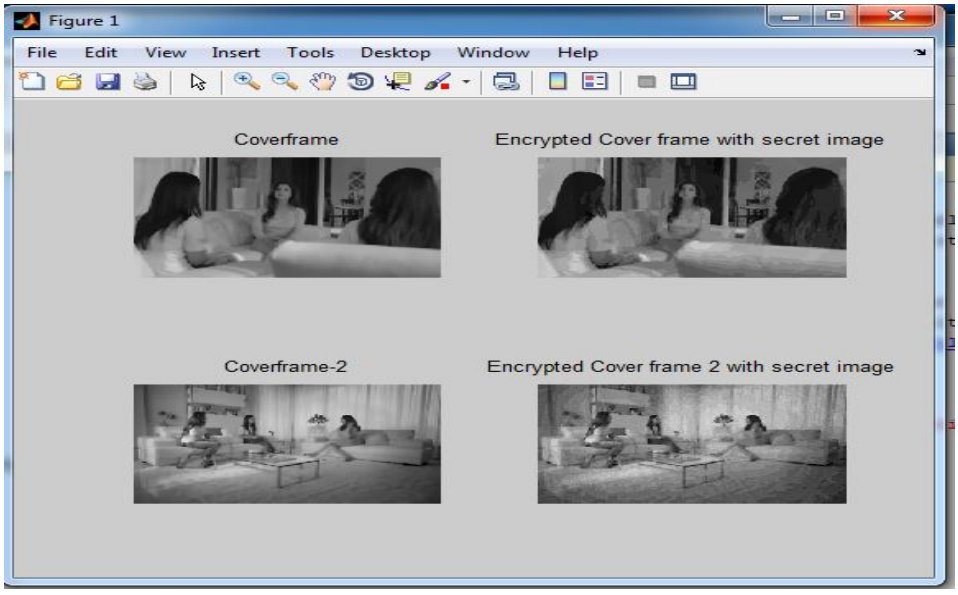

Fig 3: Encrypted cover frame with secret image

In this form the secret image hide behind the cover frames of the video. To hide the image system select the 2 frames. First frame select manually by the user and second frame select by the system consequently.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

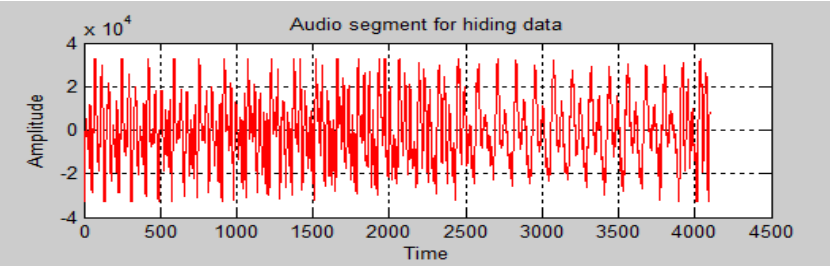

Fig 5: Audio segment

Secret data will be hide behind the audio. The above fig show the actual amplitude of the sound before the hide the secret data

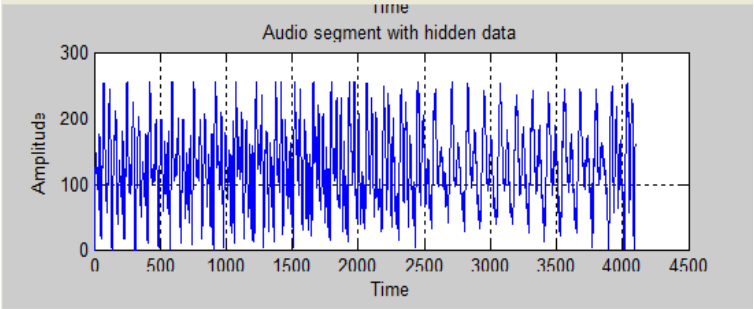

Fig 6: Audio segment after hiding a data.

Audio is collection of segments. Secret data hide behind the audio segment . The above fig. Display the amplitude of the audio segment after hiding the secret data behind the image.

VIII. CONCLUSION

The proposed method based on image hiding behind the video and data behind the audio improve the embedding capability of audio -video and increase the quality of cover midea after hiding the secrete data as well as decrease the distortion rate of cover file.

REFERENCES

1. Vaishali Sarangpure, R. B. Talmale, " Survey paper Audio-Video Steganography Using Anti Forensics Technique", International Journal of Research (IJR), Vol-1, Issue-9, October 2014.
2. Vaishali Sarangpure, R. B. Talmale," Image Security Mechanisum in Video Using LSB Method ", International Conference on Emerging Trends in Computer Engineering 2015.
3. A. K. Bhaumik, Minkyu Choi, Rosslin R. Robles, Maricel O. Balitanas "Data Hiding In Video" from International Journal of Database Theory and Application Vol.2-2 June 2009.
4. Prof. D. P. Gaikwad, Trupti Jagdale, Swati Dhanokar, Abhijeet Moghe, Akash Pathak "Hiding the Text and Image Message of Variable Size Using Encryption and Compression Algorithms in Video steganography", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 1, Issue 2, pp.102-108
5. Sunil k. Moon, Rajshree D. Raut, "Application of data hiding in Audio-Video using anti forensics techniques for authentication and data security", Advanced Computing Conference (IACC) 2014IEEE International.
6. Muhammad Asad, Junaid Gilani, Adnan Khalid, "Three Layered Model for Audio Steganography", 2012 International Conference on Emerging Technologies (ICET)
7. Kamalpreet Kaur, DeepankarVerma, "Multi-Level Steganographic Algorithm for Audio Steganography using LSB, Parity Coding and Phase Coding Technique", IJARCSSE, Volume 4, Issue 1, January 2014
8. S.S. Divya, M. Ram Mohan Reddy, "Hiding Text In Audio Using Multiple LSB Steganography And Provide Security Using Cryptography", International Journal of Scientific &Technology Research, Vol. 1, pp. 68-70, July 2012.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

BIOGRAPHY

Vaishali Sarangpure is a Student of final year M.TECH in the computer Science & Engineering Department, College of Tulsiramji Gaikwad Patil College of Engineering & Technology Nagpur, Rashtrasanth Tukdoji Maharaj University Nagpur. She Recived Bachelor of Computer Technology degree in 2010 from RTMNU, Nagur, India. Her research interests are Cryptography and Stegnography

Prof Roshni Talmale is a H.O.D of M.TECH in the Computer Science & Engineering Department, College of Tulsiramji Gaikwad Patil College of Engineering & Technology Nagpur, Rashtrasanth Tukdoji Maharaj University Nagpur. She Recived Bachelor of Computer Technology degree in 2010 from RTMNU, Nagpur, India. Her research interests are Cryptography and Stegnography.

Prof. G.Rajesh babu is a Assistance Professor of M.TECH in the C omputer Science & Engineering Department, College of Tulsiramji Gaikwad Patil College of Engineering & Technology Nagpur, Rashtrasanth Tukdoji Maharaj University Nagpur His research interests are Stegnography and wireless network