IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 12, December 2015

A Survey on Mechanism of Data Hiding in Audio-Video using Anti Forensics Technique for Data Authentication

Pallavi Phartade [1], Vandana Nawale[2]

ME Student, Dept of Computer Engineering, DPCOE, Pune, India.[1]

Assistant Professor, Dept of Computer Engineering, DPCOE, Pune, India.[2]

Abstract: Steganography is the mechanism of hiding any secret information like password, textand image, audio behind original cover file. Original message is translate into cipher text by using secret key and then hidden into the LSB of original image. The updated system provides audio-video cryptostegnography which is the combination of image steganography and audio steganography using Forensics Technique as a tool to authentication of data. 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 vital issue in digital communication. Cryptography and steganography are two popular techniques 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 vital tool that allows covert transmission of information over and over communications channel. Steganography is a most popular technique which is used to hide the message and prevent the detection of hidden message in a systematic manner. Various modern techniques of steganography are:

a) Video Steganography
b)Audio Steganography

Audio Video stegnography is a latest stegnography of hiding information in such a way that the unwanted people may not permissible the information in any manner. The updated new method is to hide secret information and image behind the audio and video file respectively.

Keywords: Audio Stegnography, Video Stegnography, Data hiding, Stegnography, Histogram, Computer Forencies, Authentication.

I. INTRODUCTION

Due to the 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 invideo frame and these modifications must be done in such a way that data is recovery correctly without destroying the original signal. Stegnography is the method of hiding any secret information like password, text and image, audio behind original cover file. Original message is converted into cipher text by using secret key and then hidden into the LSB of original image. The proposed system provides audio-video crypto stegnography which is the combination of image steganography andaudio steganography using Forensics Technique as a tool to authentication. The main aim is to hide secret information behind image and audio of video file. As video is the application of many still frames of images and audio, we can select any frame of video and audio for hiding our secret data. Suitable algorithm such as LSB is used for image steganography suitable parameter of security and authentication like PSNR, histogram are obtained at receiver and transmitter side which are exactly identical, hence data security can be increased. His paper focus the idea of computer forensics technique and its se of video steganography in both investigative and security.

II. RELATED WORK

Information security using data hiding audio video stegnography with the help of computer forensic techniques provides better hiding capacity we have worked on hiding image and text behind video and audio file and extracted from an AVI file using 4 least significant bit. Insertion method for video steganography and phase coding audio stegnography.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

DOI 10.17148/IJARCCE.2015.41211

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 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 is 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 introduces 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. MECHANISM OF AUDIO AND VIDEO STEGANOGRAPHY

A. AUDIO STEGANOGRAPHY

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.

B. VIDEO STEGANOGRAPHY

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.

V. PROPOSED LSB MECHANISM

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

DOI 10.17148/IJARCCE.2015.41211

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.

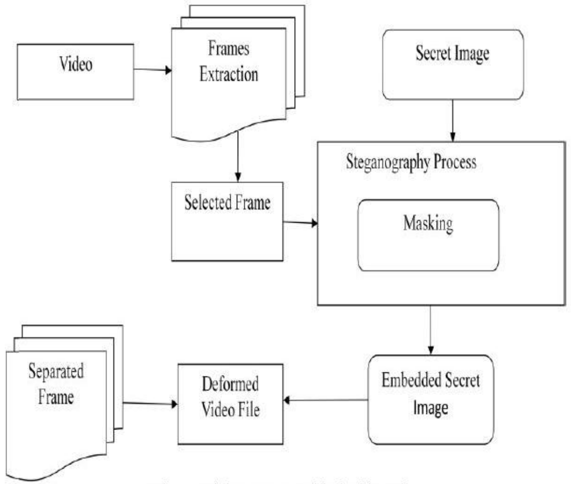

Fig 1 :-Hiding Image Behind Video File

VI. ALGORITHM USED

ALGORITHM FOR HIDING DATA IN AUDIO

1. AES encryption algorithm:

AES is based on a design principle known as a substitution-permutation network, and is fast in both software and hardware. Unlike its predecessor DES, AES does not use a Feistel Network. AES operates on a 4×4 column-major ordermatrix of bytes, termed the state, although some versions of Rijndael have a larger block size andhave additional columns in the state. Most AES calculations are done in a special finite field. We use 128 bit key for an AES cipher which specifies the number of repetitions should be 10 cycles' transformation rounds that convert the input, called the plaintext, into the final output, called the cipher text. Each round consists of several processing steps, each containing four similar but different stages, including one that depends on the encryption key itself. A set of reverse rounds are applied to transform cipher text back into the original plaintext using the same encryption key.

ALGORITHM FOR HIDING DATA IN VIDEO

1. Least Significant Bit (LSB) based steganography

The simplest and most common type of steganography is LSB (least significant bit). The one's bit of a byte is used to encode the hidden information. Suppose we want to encode the letter A (ASCII 65 or binary 01000001) in the following 8 bytes of a carrier file.

VII. CONCLUSION

Information security using data hiding Audio video steganography with the help of computer forensic tech provide better hiding capacity and security. 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 media after hiding the secrete data as well as decrease the distortion rate of cover file.

REFERENCES

[1] D. Gourley, B. Totty, M. Sayer,S. Reddy, and A. Aggarwal, HTTP The Definitive Guide, 1st ed., O'Reilly Media, US, 2002.

[2] D. Kristol, "HTTP State Management Mechanism,", in Internet Society,2000. Available: http://www.ietf.org/rfc/rfc2965.txt.

[3] "Cross Site Scripting Techniques and mitigation,", GovCertUK, revision 1.0,October 2009. Available: www.govcertuk.gov.uk.

[4] J. Garcia-Alfaro and G. Navarro-Arribas, "Prevention of Cross-Site Scripting Attacks on Current Web Applications,". Available: http://hacks-galore.org/guille/pubs/is-otm-07.pdf

[5] S. Saha, "Consideration Points: Detecting Cross-Site Scripting," (IJCSIS) International Journal of Computer Science and Information Security,Vol. 4, No. 1 & 2, 2009.

[6] A. Klein, "DOM Based Cross Site Scripting or XSS of the Third Kind,",July2005.Available:http://www.webappsec.org/project s/articles/ 071105.shtml.

[7] A. Wiegenstein, M. Schumacher, X. Jia, and F. Weidemann "Whitepaper: The Cross Site Scripting Threat,", 2007. Available: http://www.virtualforge.de.

[8] "White paper: How to Gain Visibility and Control of Encrypted SSL Web Sessions,". Available: http://www.bluecoat.com

[9] "Technology Overview: Cisco IronPort Web Usage Controls,". Available: http://www.ironport.com.

[10] "Solution Brief: McAfee Web Gateway,". Available: http://www.mcafee.com

DOI 10.17148/IJARCCE.2015.41211