Data Hiding in Audio-Video using Antiforensics Technique for Authentication

Mr.Sunil S. Khatal[1] Mr. K.S. Kahate[2]
[1]M.E Student [2]M.E Co-Ordinator
[1,2]Department of Computer Engineering
[1,2]SPCOE, Dumberwadi, Otur

Abstract— Stegnography is method of hiding any information like password, text and image, audio behind original file. Original message is converted into cipher text by using secret key and then hidden into the Least Significant Bit(LSB) of original image. This system provides audio-video cryptostegnography. Cryptostegnography is the combination of image steganography and audio steganography. It using Forensics Technique as a tool of authentication. The main goal is to hide secret information behind image and audio of video file and video is the application of many frames of images and audio, we can select any frame of video and audio for hiding our secret data. LSB algorithm is used for image steganography suitable parameter of security and authentication like PSNR, histogram are also obtained at receiver and transmitter side which are exactly identical, hence data security can be increased. This system focus the idea of computer forensics technique audio and video steganography is used in both investigative and security manner.

Key words: 4LSB, Datahiding, Stegnography, Histogram, Computer Forencies, Authentication

I. INTRODUCTION

Stegnography is method of hiding any information like password, text and image, audio behind original file . Original message is converted into cipher text by using secret key and then hidden into the Least Significant Bit(LSB) of original image. Theis system provides audio-video cryptostegnography.

Cryptostegnography is the combination of image steganography and audio steganography.It using Forensics Technique as a tool of authentication. The main goal is to hide secret information behind image and audio of video file and video is the application of many frames of images and audio, we can select any frame of video and audio for hiding our secret data. LSB algorithm is used for image steganography suitable parameter of security and authentication like PSNR, histogram are also obtained at receiver and transmitter side which are exactly identical, hence data security can be increased. This system focus the idea of computer forensics technique and video steganography is used in both investigative and security manner.

II. RELATED WORK

Data hiding using audio video stegnography with the help of computer forensic techniques. It 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.

We are hiding encrypted data using stegnography and cryptography behind selected frame of video using 4LSB insertion method.

III. SELECT AUDIO VIDEO FILE

1) Select Video File
2) Select AVI video file, behind which user to hide data.
3) 3. Separate audio and video file from selected video file using available software.
4) Save audio file as .wav file which is the original separated audio file.

IV. VIDEO STEGANOGRAPHY

(at Transmitter Side)

1) Select original video file (.AVI).
2) Separate all frames of video file.
3) Get frame number to from user behind which an authentication image is to be hidden.
4) Read authentication image.
5) To extract msb(most significant bit) of frame bit AND frame with 240(11110000).
6) To extract msb of authentication image bit AND frame with 240(11110000).
7) Reverse the place of msb of authentication image to lbs. by dividing each element by 16.
8) Reshape the image bits into one row.
9) This reshaped row vector of authentication
10) image data is embedded on the frame matrix by adding each row vector bits two last 4 bits of frame bits.
11) This forms a steno frame overwriting this steno frame with original video file create steno video file.
12) Create new steno video file in which authentication images is hidden.

V. CREATE STEGO AUDIO FILE

1) Combine stego audio and stego video file using ‘cute audio video merger’ software.
2) This forms the stego audio vedio file at transmitter site which has hidden text and image in it.

VI. AUTHENTICATION (AT RECEIVER SIDE)

1) After transmission of the stego audio video file obtained at receiver side.
2) Read the stego audio video file.
3) Select the frame number(the frame number should be same at transmitter at receiver side then only the authentication process start else it gets terminated)
4) To recover the authentication image from the selected frame bit AND the frame data with 15.
5) Authentication image data is available at LSB of frame is recovered.

6) Select the authentication image at receiver side compare recovered authenticated image with the selected image.
7) If both the images matched, then only user can recover the text behind audio else process is terminated.

VII. AUDIO RECOVERY

1) Read audio file.
2) Open this stego audio file in read mode.
3) Read wave file's first 40 bytes of header.
4) Then read all its data after 40th byte and close file.
5) Recover the size of identity key from LSB of .wav file. Recover identity key from further LSB bits of .WAV file.
6) 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.
7) As identity key is matched recover the size of message from further LSB bits of .wav file. Recover the message.
8) Secrete text is recovered.

VIII. ALGORITHM FOR HIDING DATA IN AUDIO

A. AES Encryption Algorithm:

– AES is based on a design principle known as a substitution-permutation network.It is fast in both software and hardware.
– AES operates on a 4×4 column-major order matrix of bytes, termed the state, although some versions of Rijndael have a larger block size and have 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.

IX. ALGORITHM FOR HIDING DATA IN VIDEO

– 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.

X. ARCHITECTURE

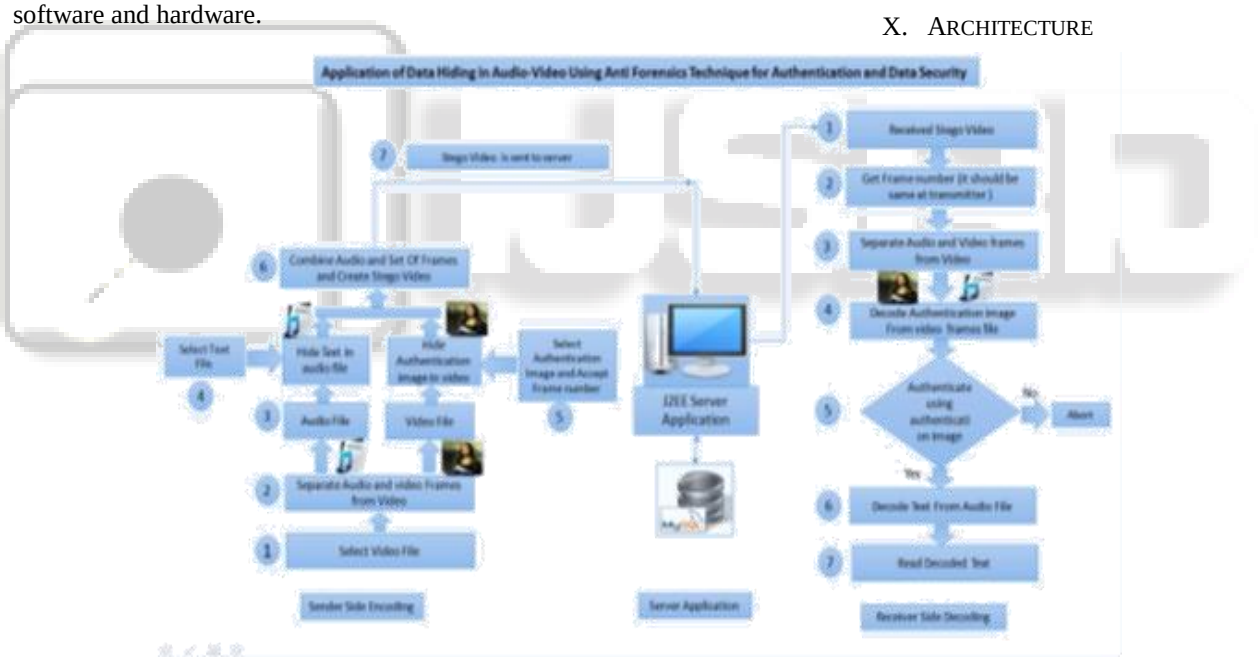

Fig. 1:

XI. FUNCTIONAL REQUIREMENTS

A. Functional Requirements:

1) Functional Requirements:

– User should knowledge about the computer
– Also User should be able to do perform task.
– Client should be able recognized these request from server very efficiently.
– Response speed should be good enough.

B. Cost and Schedule:

Use Function point calculation method to calculate the size of the project. The function point method was originally developed by Bij Albrecht. A function point is a rough estimate of a unit of delivered functionality of a software project. Function points (FP) measure size in terms of the amount of functionality in a system. Function points are computed by first calculating an unadjusted function point count (UFC).

Counts are made for the following categories

1) Number of user inputs
2) Each user input that provides distinct application oriented data to the software is counted. Number of user outputs
3) Each user output that provides application oriented information to the user is counted. In this context "output" refers to reports, screens, error messages, etc.

Individual data items within a report are not counted separately. Number of user inquiries

4) An inquiry is defined as an on-line input that results in the generation of some immediate software response in the form of an on-line output. Each distinct inquiry is counted. Number of files
5) Each logical master file is counted. Number of external interfaces
6) All machine-readable interfaces that are used to transmit information to another system are counted.
7) Once this data has been collected, a complexity rating is associated with each count according to Table

XII. DESIGN CONSTRAINTS

A. Design Constraints:

- Error Recognition: Error should be easily recognized and get solved out.
- Screen resolution: Screen should be visible enough.
- Exception: All kind of exception should be handle properly.

B. General Constraints:

- Processing speed -. Processing speed depends on the network connection

C. User Documentation:

- Currently we will be using, Android for developing program.
- Developing tool to be used Eclipse

D. Assumptions And Dependencies:

Assumptions:

- User must have basic knowledge of computer
- Must be familiar basic with Networking and communication.
- Admin only the user who is allow to access network.

Dependencies:

- Speed of the recognition may be depending upon the network traffic.
- Screen resolution depend totally depends upon hardware
- Admin cell phone should be WI-FI enable.
- Cell phone should be compatible with Android.

XIII. FEATURE HIGHLIGHT

JDK 7

- Project Coin support
- Editor enhancements: Code completion, hint

File System Database

- Simplified connection wizard
- No installation is required
- Editing and deployment of stored procedures

XIV. CONCLUSION

Data hiding using Audio video steganography with the help of computer forensic tech provide better hiding capacity and security.

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

