APPLICATION OF DATA HIDING IN AUDIO-VIDEO USING ANTIN FORENSICS TECHNIQUE FOR AUTHENTICATION AND DATA SECURITY.

Mr.Wagh Rahul S.
Department of computer Department, SCSCOE, Rahuri Factory
Mr. Bagul Kunal S.
Department of computer Department, SCSCOE, Rahuri Factory
Mr. Shinde Dinesh R.
Department of computer Department,SCSCOE,Rahuri Factory.
Mr. Vathare Mahesh S.
Department of computer Department, SCSCOE,Rahuri Factory

ABSTRACT

Steganography is the art of covered or hidden text message. The purpose of steganography is covert communication-to hide the existence of a secret message from a third party. This paper is intnded as a high-level technical introduction to steganography for those unfamiliar with the field. It is directed at forensic computer examiners who need a practical understanding of steganography without study into the mathematical, although references are provided to many of the ongoing research for the person who needs or wants additional detail covered by audio-video file. Although in this paper gives a historical context for steganography, the significance is on digital applications use anti Forensics technique, focusing on hiding information in online audio and video files. Examples for tools of software that employ steganography to hide data inside of audio-video file as well as software to detect such hidden files will also be presented. Suitable algorithm such as LSB is used for image steganography suitable parameter of security and authentication is like PSNR, histogram are obtained at transmitter\sende and receiver side which are exactly identical, hence data security can be increased. This paper focus on the idea of computer anti forensics technique and its use of video steganography in both investigative and security manner.

KEYWORDS: 4LSB; Data Hiding; Steganography; Histogram; PSNR; Computer anti Forensics; Authentication

INTRODUCTION

Steganography is the art of covered or hidden information. The purpose of steganography is covert communication to hide a secret message from a third party. This differs from cryptography, the art of secret message, which is intended to make a message unreadable by a third party but does not hide the existence of the secret communication. Although steganography is distinct and separate from cryptography, there are many analogies between the both, and some authors categorize steganography as a form of cryptography since hidden communication is a form of secret writing. Nevertheless, this paper will treated steganography as a separate field[5].

Steganography hides the covert data but not the fact that two transactions are communicate with each other. The steganography process generally involves placing a hidden information in some transport medium like audio-video file, called the carrier[4]. The secret message is embedded in the carrier to form the steganography medium. The use of a steganography key may be employed for encryption of the hidden message and/or for randomization in the steganography scheme. In summary[4].

steganography_medium = (hidden_data + carrier + steganography_secrate key.)

The proposed system is provides audio-video cryptostegnography which is the combination of audio-video steganography using anti Forensics Technique as a tool to authentication. Stenography is the method of hiding any secret message like password, text and image, audio behind original cover file[2]. Original message is converted into cipher text by using secret key and then hide into the LSB of original file. The proposed system is provides audio-video cryptostegnography which is the combination of image steganography and audio steganography using anti Forensics Technique as a software tool to authentication. The main aim is to hide secret data behind image and audio of video file[1]. As video is the tool of many still frames of audio and video, we can select any frame of video for hiding our secret information. Suitable algorithm such as LSB is used for frame of video steganography suitable parameter of security and authentication like PSNR, histograms are obtained at transmitter\sender and receiver side which are exactly identical , hence data security can be increased. This paper focus the idea of computer anti forensics technique and its use of video steganography in both investigative and security manner[2].

LITERATURE SURVEY:

COMPARISON OF EXISTING SYSTEM

In existing system for any site we use password and username in textual format .When we use this format to any site there is changes getting hacking of the data when sending data from client to server for validating. If we use text format then it readable to anyone. Next time encryption algorithm used for to prevent the hacking of the data. Now a days there are deferent encryption algorithms are used. This technique is not scent to now a days. So now we develop new technique for securing data when we transferring data for client to server we use the video steganography. Which is more powerful technique for transferring? data for client to server.

PRESENT SYSTEM IN USE

The most basic form of user authentication, particularly on the Web, is the password authentication protocol. This method of authentication forces you to remember username/password combinations to access accounts or special sections of a website. While elective and in some ways fundamentally a part of online security, password authentication protocols fail when you don't address them seriously. This means constructing complex passwords and maintaining secrecy. This also means that entities implementing password authentication must safeguard passwords in some way. Next use to Storage and Encryption When you use pass- word authentication, you must store passwords and usernames in a database to authenticate users. If you don't have strong server security, someone can break into the database and read the passwords. One way to address this is to use password "hashing," which involves running the password through a hash algorithm that produces a unique value based on the password and stores the hash value instead of the password itself. If the database is breached, the attacker can read only the hashes and have no idea what the passwords are. However, hashing
in this sense exists only due to the inherent weakness of plain text password authentication. The glory of Internet and its merits are being highly masked by the drawback associated with it. Of them the prime issue is Internet vulnerability, leading to data modi_cation and data thefts. Many Web applications store the data in the data base and retrieve and update information as needed. To overcome this type of disadvantages developed an video stegnography.

FLAWS IN CURRENT SYSTEM

In the _rst and second step, program we accept cover audio and convert it into samples.Then we apply spread spectrum stenographic algorithm and hide the encrypted data in audio frame. In third and fourth step we hide authentication logo in _xed frame and recombine frames to from stego-audio. At receiver end above steps are repeated in reverse manner.

BUSINESS CONTEXT

Nowadays, users can access the Internet and get the information globally spread on the websites. Upon receiving a request for information, the server requests the user ID and password to prove whether the user intends to be authenticated is a legitimate user or not. However, there are several malicious activities that could possibly make the authentication scheme vulnerable. One of those is a web phishing, in which an attacker attempts to acquire sensitive information such as usernames, passwords, and personal information such as credit card number or registration number. So provide an audio-video cryptography is used for data hiding stegnography for transferring data from source to destination.

Table: Literature survey

Paper Name	Author	Method	Algorithm	Addvantage	Disadvantage
Image Encryption And Decryption (2003)	Prof.shen chen,ron-gjian chen	Scan Method	Encryption Decryption Algorithm	Loss less Encryption Of Image,Security can be incre-ased using more encryption loop	It can not used Any multimedia system.
Data hiding binary image for Authentication and annotation(2006)	Prof.min wu,Prof. bede liu	Digital Watermarking & Data Hiding Technique	Data Hiding of Binary Image	It Can Stored data in digital form	Low Security.Digital Data can be easly access.
Data Hiding in	Prof. P.	watermarkig,	data hid-	It iS used To	It cant be used

Image and Video Part IFundamental Issues and Solutions(2008)	Diaconis,Profs. B. Dickinson, E. Cinlar, and S. Kulkarni	modulation and multiplexing, shuffe.	ing algorithms.divied	framework system.It used Lay-ered structure of data hiding.	audio _les.It Can Not Mension Size of hidden data.
Application Of data Hiding in Audio Video using Anti-Forensics tech For Authentica -tion and Dasecrity 2014	Prof.Sunil kmoon, Prof. Rajeshree D Raut	Steganography, Authentication of Frames	LSB Algo,AES Algo,RLSB Algo	High Security provided.Secure Data transfer for _nancial purpose.	Future work Not Mentioned

PROPOSED SYSTEM:

In existing system for ay site we use password and username in textual format .When we use this format to any site there is changes getting hacking of the data when sending data from client to server for validating. If we use text format then it readable to anyone. Next time encryption algorithm used for to prevent the hacking of the data. Now a days there are different encryption algorithms are used. This technique is not sufficient to now a day. So now we develop new technique for securing data when we transferring data for client to server we use the video steganography. Which is more powerful technique for transferring data for client to server?

SYSTEM ARCHITECTURE:

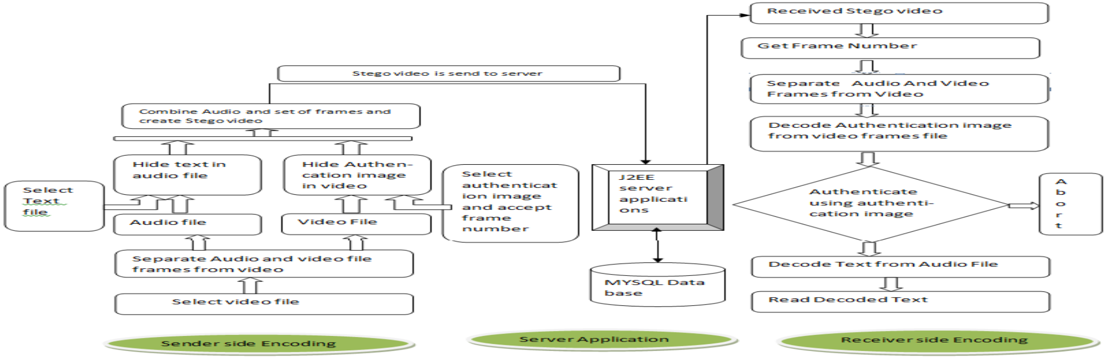
Stego video is send to server
Combine Audio and set of frames and create Stego video
Hide text in audio file
Hide Authen-cation image in video
Select Text file
Select authenticat ion image and accept frame number
Audio file
Video File
Separate Audio and video file frames from video
Select video file
J2EE server applicati ons
MYSQL Data base
Received Stego video
Get Frame Number
Separate Audio And Video Frames from Video
Decode Authentication image from video frames file
Authenticate using authenti-cation image
Abort
Decode Text from Audio File
Read Decoded Text
Sender side Encoding
Server Application
Receiver side Encoding

Fig 1.System Architecture

The main aim is to hide secret information behind image and audio of video le. 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 information. 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. This paper focus the idea of computer forensics technique and its use of video steganography in both investigative and security manner.

ALGORITHMS:

1)Least Signi_cant Bit (LSB) based steganography:

The simplest and most common type of steganography is LSB (least signi_cant 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.

01011101 11010000 00011100 10101100
11100111 10000111 01101011 11100011

Becomes

01011100 11010001 00011100 10101100
11100110 10000110 01101010 11100011

2)AES ALGORITHM FOR ENCRYPTION:

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 44 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 di_erent 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.

Random Least Signi_cant Bit(RLSB)

Image steganography, is one kind of steganographic system where the secret message is hidden in a digital image with some kind of hiding strategy. The conventional image steganographic algorithm is the Least Signi_cant Bit (LSB) algorithm, the advantage of LSB is its simplicity to embed the bits of the message directly into the LSB plane of the cover image and many applications use this method. The storage of information bits in the least signi_cant bits of the image does not a_ect the image in a greater scale and hence the change is not perceived by the Human Visual System (HVS). LSB embedding when applied to the pixels of an image sequentially make it easy for any intruder to uncover the information, hence the bits can be embedded in a random fashion to present a more secured way of information hiding.

FLOW OF EXISTING SYSTEM :

AT THE SENDER SIDE:

Choose Audio-Video file:

Following are the steps for selecting a specific audio-video file and the separation of audio and video part are explained.

1.Select any available format audio-video file in which user wants to hide data.
2.Apart the video and audio from the Video file using specific software.
3.Then save the give audio files and video files isolation separately.

Hiding Frame in Video (Sender)

Following are the steps for insert a secret image in one of the selected video frame are give below

1. Choose the video file and read the videofile.
2. Now play the video.
3.We See No Any change in the Give Video File.
4 Choose the random frame in which the user want to hide Image in it.
5. Choose the encrypted image in which the user want to hide
6. We use data encryption Using AES Algorithm
7.Then extract the most significant bit MSB of the frame by bitand frame with 240 using "bitand" function.
8.Now extract the givemsb of the encrypted image byBitand image with 240 using "bitand" function.
9. Reverse the give place of msb to lsb by dividing by 16.
10. The given reshaped row vector of Real image data is to be embedded on the given frame
matrix in which addition of each row vector bit's by two last 4 bits of the given frame bit.
11.FinallyStego Video is created.
12.Then check Either Stego video is played or Not.
13. Close the given file.

Now Hiding data in Audio

Following are the steps for Hiding data in Audiofile are to be explained.

1. First step is Encrypted message is take.
2. Then it convert to ASCII format
3. Supply the hiding key.
4. Translate eachan every audio sample into 8 bits sequences.
5. From each sample read first two MSBbits and convert it to decimal.
6. Addthe given secret bits into a specific position refer using the last method.
7. Same Process will be conducted until the secret bits are changed.

Creating stego Audio-Video file

Combine stego audio and stegovideo file by using specific software. then we get Stego audio-video file is the combination of Data and original file at the transmitter side.

AT THE RECIVER SIDE

Recovering data from Audio(Reciver)

1.Read the stego audio file from the given stego audio-video at receiver.

2. 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)

3.To recover the authentication image from the selected frame bit AND the frame data with 15.

4.Authentication image data is available at LSB of frame is recovered.

5.Select the authentication image at receiver side compare recovered authenticated image with the selected image.

6.If both the images matched , then only user can recover the text behind audio else process is terminated.

7.Audio Recovery

8.Read audio File.

9.Open this stego audio file in read mode.

10.Read wave file's first 40 bytes of header.

11.Then read all its data after 40th byte and close file.

12.Recover the size of identity key from LSB of .wav file. Recover identity key from further LSB bits of .WAV file.message to the end user

message to the end user

CONCLUSION:

Data hiding in audio-video file with the help of computer forensic technique provide better hiding and security for the secret information. We are working on hiding image and text behind video and audio file and extracted from an any video file at sender side and computer forensic techniques at receiver side.

REFERENCES

[1] Sunil K.Moon And Rajashree D.Raut"Application Of Data Hiding In Audio Video Using Anti Forensic Technique For Authen- Tication And Data Security"Ijeec:International Journal Of Electrical Electronics And Communication 2014ieee.

[2]Yugeshwarikakde And Priyankagonnade, Audio Video Steganography For Authentication Anddata Security"Ieee International Journal On Recent And Inno- Vation Trends In Computing And Communication Vol: 1 Issue: 4, April 2013.

[3]Ms. M. Sujana[M.Tech] And Mr. K.L.L. Lokesh,[M.Tech] Application Of Data Hiding In Audio-Image Using Anti Forensics Technique For Authentication And Data Security In Linux Platform"Ijeec : International Journal Of Electrical Elec- Tronics And Communication

[4]Athiramohananand And Dr. Sasidharbabusuvanam," Audio - Video Steganography Using Forensictechniquefor Data Security"International Journal Of Engineering And Computer Technology(Ijcet)Issn 09766367volume 5, Issue 12, December (2014), Pp. 154-157

[5] P. Srilatha And J. Vijaya Lakshmi, Anti Forensic Techniques Used For Data Security By Using Audio Video Files"International Journal Of- Scientic Engineering And Technologyissn 2319-8885vol.04,Issue.35,August-2015,Pages:6949-6952