ISSN 2395-1621

Modern Technique to secure Information by using Audio Video Steganography

[#1]Rahul Auti, [#2]Kondiram Sonawane, [#3]Dnyaneshwar Murumkar, [#4]Gopal Pawar, [#5]Prof. R.B.Rothod

[1]rahulauti7@gmail.com
[2]konds9975@gmail.com
[4]gopaljp93@gmail.com

[#1234]Department Of Computer Engineering
[#5]Prof. Department Of Computer Engineering

PDEA's College of Engineering, Manjari (Bk)
Hadapsar, PUNE 412307.

ABSTRACT

Steganography is the technique of hiding any secret information like password, data and image behind any cover file. This project proposes a method which is an audio-video steganography system which is the combination of audio steganography and video steganography using DES algorithm as the secure encryption method. The aim is to hide secret information behind image and audio of video file. Since video is the application of many audio and video frames. We can select a particular frame for image hiding and audio for hiding our secret data.4LSB substitution can be used for image steganography and LSB substitution algorithm with location selection for audio steganography. DES algorithm can be used for encryption and decryption of data and images. Suitable parameter of security and authentication such as PSNR value, histograms are obtained at both the receiver side and transmitter sides which are found to be identical at both ends. Reversible data hiding methods for both video and audio are also being mentioned. Hence the security of the data and image can be enhanced. This method can be used in fields such as medical and defense which requires real time processing.

ARTICLE INFO

Article History

Received :5th April 2016

Received in revised form :

7th April 2016

Accepted : 9th April 2016

Published online :

11th April 2016

Keywords: Steganography, Messaging, Secure communication, Audio/video files.

I. INTRODUCTION

The Popularity of digital media increase day its raise security related issues are created and it is very most important issue. 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. 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 and audio 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. LITERATURE SURVEY

Evaluation of Various LSB based Methods of Image Steganography on GIF File Format

Review: This paper describes LSB base method hiding data, Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet. There have been many steganographic techniques available for hiding message in image having its own strength and weaknesses. Steganography can be carried out on any digital media. The chosen media for this system are GIF images. It is chosen due to wide use in web pages. In this paper we look at all the available image based steganography along with the cryptography technique to achieve security. This paper will focus on hiding the message in the least significant bits of the colors of the pixels of a GIF image. We discuss results obtained from evaluating available steganographic techniques and compare the different methods according to the vulnerability. In this paper we also discuss some application of steganography in network security.

Stegnography An Art of Hiding Data.

Review: In today's world the art of sending & displaying the hidden information especially in public places, has received more attention and faced many challenges. Therefore, different methods have been proposed so far for hiding information in different cover media. In this paper a method for hiding of information on the billboard display is presented. It is well known that encryption provides secure channels for communicating entities. However, due to lack of covertness on these channels, an eavesdropper can identify encrypted streams through statistical tests and capture them for further cryptanalysis. In this paper we propose a new form of steganography, on-line hiding of information on the output screens of the instrument. This method can be used for announcing a secret message in public place. It can be extended to other means such as electronic advertising board around sports stadium, railway station or airport. This method of steganography is very similar to image steganography and video steganography. Private marking system using symmetric key steganography technique and LSB technique is used here for hiding the secret information.

Image Watermarking Method Using Integer-to-integer Wavelet Transforms.

Review: Digital watermarking is an efficient method for copyright protection for text, image, audio, and video data. This paper presents a new image watermarking method based on integer-to-integer wavelet transforms. The watermark is embedded in the significant wavelet coefficients by a simple exclusive OR operation. The method avoids complicated computations and high computer memory requirements that are the main drawbacks of common frequency domain based watermarking algorithms. Simulation results show that the embedded watermark is perceptually invisible and robust to various operations, such as low quality joint picture expert group (JPEG) compression, random and Gaussian noises, and smoothing (mean filtering).

StegTorrent: a Steganographic Method for the P2P File Sharing Service

Review: The paper proposes StegTorrent a new network steganographic method for the popular P2P file transfer service—BitTorrent. It is based on modifying the order of data packets in the peer-peer data exchange protocol. Unlike other existing steganographic methods that modify the packets' order it does not require any synchronization. Experimental results acquired from prototype implementation proved that it provides high steganographic bandwidth of up to 270 b/s while introducing little transmission distortion and providing difficult detectability.

III. PROPOSED SYSTEM

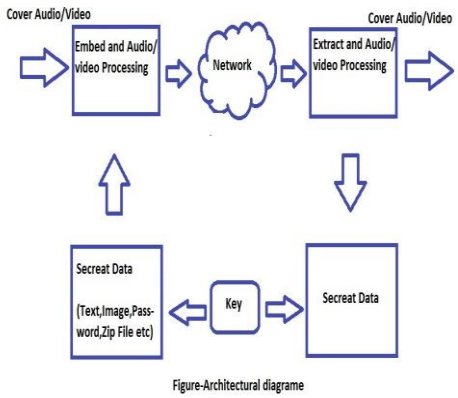

Fig 1. System Architecture

The aim of this project is to develop a set of effective stego techniques for concealing information within video and audio, this is the ideal medium for hiding information. The project involved. Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message; this different from cryptography, the art of secret writing, which is intended to make a message unreadable by a third party but does not hide the existence of the secret communication. The purpose of steganography is covert communication to hide the existence of a message from a third party. Generally, a steganographic message will appear to be something else: a picture, an article, a shopping list, or some other message. This apparent message is the cover text. For instance, a message may be hidden by using invisible link between the visible lines of innocuous documents.

IV. CONCLUSION

Steganography especially combined with cryptography, is a powerful tool which enables people to communicate without possible eavesdroppers even knowing there is a form of communication in the first place. These meth-ods used in the science of steganography have advanced a lot over the past centuries, especially with the rise of computer era. Although the techniques are still not used very often, the possibilities are endless. Many different techniques exist and continue to be developed, while the ways of detecting hidden messages also advance quickly.

REFERENCES

1)Domain Specific Search Of Nearest Hospital And Healthcare Management System, Rashmi A.Nimbalkar, MTech II year, Department of Information Technology, Yeshwantrao Chavan College of Engineering, March 2014

2)Bahga and V. Madisetti, Healthcare Data Integration and Informatics in the Cloud, 2015.

3)Electronic Medical Records/Health Information Technology: Background Information and Resources, Society for vascular surgery ed., SVS Clinical Practice Council, 2013.

4)(2014, March) 2011 Waiting Room Solutions Web Based EHR and Practice Management System 4.0. Waiting Room Solutions.[Online].Available: www.waitingroomsolutions. com

5)J. L. Fern´andez-Alem´an, C. L. Seva-Llor, A. Toval, S. Ouhbi, and L. Fern´andez-Luque, "Free Web-based Personal Health Records: An Analysis of Functionality," Journal of medical systems, vol. 37, no. 6, pp. 1–16, 2013

6)J. C. Crosson, P. A. Ohman-Strickland, D. J. Cohen, E. C. Clark, and B. F. Crabtree, "Typical electronic health record use in primary care practices and the quality of diabetes care," The Annals of Family Medicine, vol. 10, no. 3, pp. 221–227, 2012.

7)Raed M. Salih Leaszek T. Lilien, Protecting Users Privacy in Healthcare Cloud Computing with APB_TTP, 2015

