Imperial Journal of Interdisciplinary Research (IJIR)
Vol-2, Issue-5, 2016
ISSN: 2454-1362, http://www.onlinejournal.in

A Survey: Secure Data Transmission Using Video Steganography

Firdaus Anjum*[1], Shikha Yadav[2], Rumaiza Aafreen[3] & Tasneem Hasan[4]
[1,2,3,4]Department of Computer Science and Engineering, ITM college of Engineering

Abstract-- *Security has become the area of concern as a result of widespread use of communication medium over the internet. The steganography is the art of hiding message inside another medium such as Video, Image, Audio. The data security approach when combined with encryption and steganographic techniques for secret communication by hiding it inside the multimedia files provides a high level of security. The files composed of insignificant bits or unused areas which can be used for overwriting of other data. Various available techniques are studied and analyse in this paper. This paper presents a detailed survey of discussed steganography method which will be helpful for future research work.*

Keywords-- *Steganography, Cryptography, Digital Watermarking, LSB, Encryption, AES.*

1. Introduction

With the introduction of computer, the need for automated tools for protecting files and other information stored on the computer became evident. This is especially the case for the shared system, such as a time-sharing system, and the need is even more acute for the systems that can be accessed over the public telephone network, data network or the Internet. There are various techniques for providing security that is cryptography, Steganography and Digital Watermarking are most common techniques. The Steganography, Cryptography and Digital Watermarking techniques can be used to obtain security and privacy of data. The steganography is the art of hiding data inside another data such as cover medium by applying different steganographic techniques. While cryptography results in making the data human unreadable form called as cipher thus cryptography is scrambling of messages. Whereas the steganography results in exploitation of human awareness so it remains unobserved and undetected or intact. It is possible to use all file medium, digital data, or files as a cover medium in steganography. Generally steganography technique is applied where the cryptography is ineffective [1].

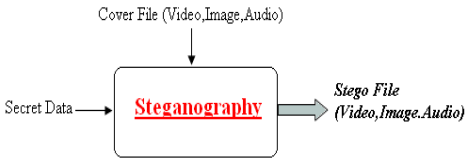

Fig1. Basic Steganography System

The steganography system consists of the cover file (image, , video etc) and the secret message that is hidden inside the cover file by applying steganography the secret message is hidden and stego file is generated which is same as cover image and go undetected or unaltered.

2. Related Work

Researchers have implemented various approaches for information and data security to achieve secret communication. Steganography is a method of hiding the secret messages into the carrier medium such as image, , video etc. steganography technique is generally classified into three main types namely, technique exploiting image format, method embedding in frequency domain and method in spatial domain[2].Stego is a greek word which means hidden. The ancient people used various techniques to send the secret messages during the war time. The evaluation of steganography technique is done with three parameters such as capacity, robustness and security[3].The system should be capable of hiding the information into cover media, it should be robust to the changes and it should be secured enough from eavesdroppers or attackers that tends to identify or alter the contents of the secret data[4].

3. Steganography Techniques

The effective steganography should have property of remaining intact irrespective of the tampering, the secret message should be invisible and it should go undetected. The capacity of the technique to hide the data should be well achieved.

A. Image Steganography

According to computer system an image can be said as array of numbers which represents light intensities at pixels, which results in data. Image is composed of 8 bits per pixel i.e.256 colors.

The colors are generated from three primary colors as red, green and blue (RGB)[28][11-13]. various approaches has been designed for image steganography some of common approaches are LSB(Least Significant Bit) substitution which is the easy and most common approach of hiding data inside images. Masking is another technique of embedding messages in significant areas.

B. Video Steganography

The separation of video into and images or frames results in the efficient method for data hiding. The use of video files as a carrier medium for steganography is more eligible as compared to other techniques. As a result of this technique is discussed and proposed in this paper.

C. Network Steganography

The another approach for hiding data is to use network steganography by sending data with the help of network protocol. Network or transport layer such as IP/TCP or ICMP and UDP protocols are used for sending messages

4. Analysis

An image is selected for the data hiding. The Stream ciphers are an important class of symmetric encryption. It encrypts binary digits of a plain-image one at a time using an encryption transformation which varies with time. A stream cipher is an encrypted key where plain-image bits are combined with a key stream. Image encryption is an important and effective technique to protect image from unauthorized access. Bit stream-based approach is designed for encryption without the need for recompression, which is useful when there is no possibility to intercept the encoding process. In Data hiding the fast intra prediction mode algorithm is used which virtually increase the memory capacity of an allowing data. Image recovers to the original images.

A novel approach for encryption key generation is proposed which is further is used to encrypt the created image encryption and for fast transmission of that encrypted image lossless compression technique is used if the receiver has only data hiding key, receiver cannot extract the original content. If the receiver has both encryption and data hiding key, receiver can recover original images. The working of each of the module is explained in detailed below

Reading the average value of RGB

Reading the images from hard disk and calculating there pixel information and writing on the picture box. The pixel scanning stores the information of pixel in the buffers memory In the form of the color information by using a RGB function which shows the capacity of the pixel so that the compressed data can be stored accordingly The compressed data with key is calculated in from bit size which will be stored in pixel. While storing these data in the image pixel we have get the matching size so that the image should not get damage.

Generation of random key

The process will be generating random key to provide security. Using this key reverse process will be done by receiver side. The secret key is used for providing security to image. so that intruder can't access the original image.

Regeneration of image

In this module original image is recovered which is same as transmitted image. Data is recovered from image. After that quality of recovered image is checked based on the some image parameter.

TABLE I. Comparative Analysis

Parameters	Methods	Description
Image pixel density	Reversible data hiding	Image recover to the receiver
Histogram value	Recursive histogram modification	Input the stego - sequence
Message bit	Error correction codes Used to encodes the plain message bit	Correct extraction of the secret data

Signal	Rate distortion model	Improve the image quality
Pixel	Intra prediction mode	Divide the pixel capacity

From the above comparative analysis intra prediction mode (IPM) approach is well suited for providing more security to image, so that image quality is improved.

6. Proposed Solution

From the idea of the proposed system we are clear with two outcomes. The outcomes will be secure transmission among receivers. These two outcomes are discussed below.

1. Improving image quality:
It should not be damage target image and Improve the Image quality.

2. Security enhanced in encrypted images:
Initially for more privacy protection content owner encrypt the original images using encryption key. by using both key receiver can extract hidden data and recover the original image without any error.
According to the video sequence characteristics, the B-frame and P-frame are dependent on the I-frame. And the raw video data can also be considered as a sequence of several still images.

5. Conclusion

In secure transformation of data in encrypted image is to provide high security for data transformation. Extract the hidden data and recover the original content without any error by exploiting spatial correlation in natural image if the amount of data is not too large. When using a colour image instead of gray, each bit of the red, green and blue colour components can be used, so a total of 3 bits can be stored in each pixel. It gives a relatively large amount of space to hide data. The image based data hiding technique is tried to improve the capacity of hidden data since, there is a limitation on how much information can be hidden into an image. To overcome the capacity problem, the data hiding has been achieved and to provide high security separate key should be used for encryption and decryption.

7. References

[1] Ya-Lin Lee, " A New Secure Image Transmission Technique Via Secret Fragment Visible Mosaics Images By Nearly Reversible Color Transformation. ," IEEE Transaction On Circuit and System For Video Technology, Vol . 24 no. 4 April 2014.

[2] Zhenxing Qian,"Reversible Data Hiding In Encrypted JPEG Bit Stream," IEEE Transaction On Multimedia Vol.16 no. August 2014

[3] W. Zhang, "Reversible Data Hiding In Encrypted Images By Reserving Room Before Encryption," IEEE Transaction on Information Forensic and Security,Vol,8 no. 3 March 2013.

[4] Xiaochen Hu, Recursive Histogram Modification Establishing Equivalency Between Reversible Data Hiding And Lossless Data Compression," IEEE Transaction On Image Processing Vol, 22 no 7, July 2013.

[5] P. Kadam," Separable Reversible Encrypted Data Hiding In Encrypted Using AEs Algorithm And Lossy Technique", International Conference On Pattern Recognition February 2013.

[6] C. Anuradha, "Secure And Authentication Reversible Data Hiding In Encrypted Image", International Journals of Advanced Research in Computers Science Vol no.3, 4 April 2013.

[7].Marvel, L. ,M., Boncelet Jr.,C.G.& Retter,C.,"Spread Spectrum Steganography",IEEE Transactions on Image Processing,1999.

[8]. Wang,H & Wang,S,"Cyber Warfare:Steganography vs. Steganalysis",Communications of the ACM,47:10,October 2004.

[9].Stefan Katznbeisser, Fabien.A., P.Petitcolas editors,Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Boston.London,2000.

[10].Jamil,T.,"Steganography:The art of Hiding Information is Plain Sight",IEEE Potentials,18:01,1999.

[11].B.Pfitzmann,"Information Hiding Terminology,"proc.First Int'l Workshop Information Hiding,Lecturer Notes in Computer Science No.1,174,Spring –Verlag,Berlin,1996,pp.347-356.

[12].Yeuan-Kuen Leea and Ling-Hwei Cheng,"High capacity steganographic model",IEEE Proc.Visual Image Signal Process.,Vol.147,No.3,June 2000.

[13].Ross J.Anderson,Fabien A.P.Petitcols,on The limits of steganography,IEEE Journal of Selected Areas in Communication,16(4);474-481,May 1998.

[14].M.Ashourian,R.C. Jain,and Y.H.Ho,Dithered Quantization for Image Data Hiding In DCT domain,Proc.of IST2003,2003,171-175.

[15].C.C.lin,P.F.Shiu,High Capacity Data Hiding scheme for DCT- based images.Journal of Information Hiding and Multimedia Signal Processing,1(3),2010,314-323.

[16].A.Nag,S.Biswas,D.Sarkar,P.Sarkar,A Novel Technique for Image Steganography based on Block-DCT and Huffman Encoding,International Journal of Computer Science and Information Technology.

[17].C.C.Chang,C.C.Lin,C.S.Tseng,and W.L.Tai Reversible hiding in DCT-based Compressed Images,Information Sciences Journal,177(13),2007,2768-2786.