IJSTA

International Journal of Scientific and Technical Advancements

ISSN: 2454-1532

Review on Various Techniques of Video Steganography

Heena Gupta[1], Richa Gupta[2], Bhawna Sharma[3], Sheetal Gandotra[4]

[1,3,4] Computer Department,GCET, J&K, India
[2] Computer Faculty,VPPHSS Jammu,J&K, India
[#] heenagupta1.2011@gmail.com

Abstract- The dynamic growth in communication technology and use of Internet has greatly facilitated data transfer. However, such open channels have greater vulnerability to security threats causing unauthorized access of information. Although, encryption is used for providing security to communication channels yet once decoded valuable information is unprotected. Steganography is the art of communicating in a way that hides the existence of the communication. Valuable information is firstly hidden in a host data, such as text, digital image, audio or vedio, and then secretly transmitted to the receiver. This paper gives a review of video steganography and the various techniques that can be used for hiding valuable information in video cover media.

INTRODUCTION

Steganography is derived from the Greek words Steganós meaning Covered and Graptos meaning Writing. The need to send safe and secure message has been the discussion point since immemorial time. The wealth of an organization is information. Hence the organization dealing with confidential data have made security-issues top priority .Whatever method we choose for the security purpose, the major concern is the degree of security it provides. Steganography is the science of hidden or covered writing. The aim of steganography is to hide a message from a third party while communicating that is to provide a covert communication.

Steganography versus Cryptography

Cryptology is often confused with Steganography because the two are similar in the way that they both provide protection to information which is important. The two differ by the fact that Steganography deals with hiding information in a way that it appears that no information is hidden at all. If a person views the object in which the information is hidden , he or she will not have any idea that any hidden information is present in the object, hence the person will not try to decrypt it. Steganography in modern sense usually refers to information or a file that has been hidden inside an Audio file, digital Picture or Video file. Steganography usually works by exploiting human perception; as human senses are not trained enough to look for objects that have hidden information inside them.

Generally, the actual information is not maintained in its original format in steganography, instead it is converted into an alternative equivalent multimedia file like audio, image or video file which in turn is hidden within another object. This message (usually known as cover text) is sent through the communicating channel to the recipient, where the actual message is separated from it.

Terms used In Steganography

Carrier File A file which contain the hidden information inside.

Steganalysis The process of detecting information which is hidden inside a file.

Stego-Medium The medium in which the hidden. information is present.

Redundant Bits Pieces of information which can be altered or overwritten inside a file without damaging it.

Payload The information which is to be concealed.

Video Steganography

Today, the most widely used technique is to use the digital files or data for hiding the secret messages. This technique of steganography exploits the weakness of the human visual system (HVS). At higher frequency side of the visual spectrum HVS cannot detect the variation in luminance of color vectors. A collection of color pixels can be used for representing a picture. For representing the individual pixels their optical characteristics like 'brightness', 'chroma', ‘luminance’ etc can be used. Each of these characteristics can be digitally expressed in terms of 0s and 1s.

For example: a 24-bit bitmap image in RGB (red ,green, blue) format will use 8 bits each pixel , for representing each of the three color values. If we consider just the green there will be 28 different green values. The human eye cannot decide the difference between 11111111 and 11111110 in the value for green color intensity .Hence , if human visual system (HVS) is the terminal recipient of the data then the Least Significant

Heena Gupta, Richa Gupta, Bhawna Sharma, and Sheetal Gandotra, “Review on various techniques of video steganography,” *International Journal of Scientific and Technical Advancements*, Volume 4, Issue 1, pp. 161-164, 2018.

Bit (LSB) can be used for something else other than color information.

We can directly apply this technique on digital image in bitmap format as well as for the compressed image format like JPEG.

When video is used as a media for hiding the information, the program or person hiding the information will use the DCT (Discrete Cosine Transform) method. DCT works by making slight changes in each of the images in the video, only so much that human eye does not notice. To be more precise DCT works by altering values of certain parts of the images, that is it usually rounds them up.

Video Steganography is almost similar to Image Steganography, apart from the fact that the frames of the video files are used for hiding the secret information. The secret information becomes almost unnoticeable when only a small amount of information is hidden inside the video file.

Various Techiques Of Video Stegnography

LSB Substitution Using Different Polynomial Equations

LSB substitution Video Steganography technique is used to hide any kind of files into a carrying Video file by exploiting the LSB bit of each video frame making the change unnoticeable by human eye . Because of its size and memory requirements the video files are used as a carrier file and hence they are more eligible than other multimedia files. An important approach for embedding information in a carrier file is Least significant bit (LSB) insertion. In this technique LSB bit of the media file are operated to hide the information bit. In LSB using different polynomial equations, a data hiding scheme is developed which hides the information in specific frames of the video file and in specific location of the video frame by using polynomial equation for LSB substitution.

Pixel-Value Differencing (PVD)

Pixel value differencing technique involves the process of embedding a secret message, in a cover image which is partitioned into blocks that are non-overlapping and the two pixels are consecutive. The values of the two pixels in each block are used to calculate the difference value which is used further. A number of range are used for classifying all possible difference values. The range intervals are selected based on the characteristics of human visions that is, sensitivity to gray value variations from smoothness to contrast. A new value is used to replace the difference value that is used to embed the value of a sub-stream of the secret message. The width of the range that the difference value belongs to decides the number of bits which can be embedded in a pixel pair. The method is designed in such a way that the modification is never out of the range interval. This method produce more imperceptible result than those yielded by simple least-significant-bit replacement methods. The embedded secret message can be extracted from the resulting stego-image without referencing the original cover image. Moreover, a pseudorandom mechanism may be used to achieve secrecy protection.

Tri-way Pixel-Value Differencing (TPVD)

Tri-way Pixel Value Differencing techniques apply the algorithm in which the compressed domain is used for performing the data hiding operations in other words the message is hidden in compressed domain. In this technique the macro blocks of I frame are used for embedding the data in with maximum scene change occurs and data is also embedded in block of P and B frames in which maximum magnitude of motion vectors occurs . In this scheme all the processes are defined and executed in the compressed domain. To enlarge the hidden secret information capacity and to provide an imperceptible stego-image for human vision, this novel steganographic approach called tri-way pixel-value differencing (TPVD) is used for embedding.

Hash Based Least Significant Bit Technique (HLSB)

Hash Based Least Significant Bit technique is a spatial domain technique where the secret information is embedded in the LSB of the cover frames. Eight bits of the secret information is divided into 3,3,2 and embedded into the RGB pixel values of the cover frames respectively. A hash function is used to select the position of insertion in LSB bits.

Video Steganography based on Non-uniform Rectangular Partition

Video Steganography technique that can hide an uncompressed secret video stream in a host video stream with almost the same size. Each frame of the secret video will be Non-uniform rectangular partitioned and the partitioned codes obtained can be an encrypted version of the original frame. These codes will be hidden in the Least 4 Significant Bits of each frames of the host video. This algorithm can hide a same-size video in the host video without obvious distortion in the host video.

CONCLUSION

The steganography methods for hiding messages reduces the chance of intrusion by intruders by making the messages invisible to them. The paper discuss a small review about of the art of video steganography and the various techniques available . It presents various types of video stegnography approaches. Comparing the performance of techniques is difficult unless identical data sets and performance measures are used. Security technologies make use of these techniques. The discussion includes the current trends in the video stegnography.

REFERENCES:

[1] Ko-Chin Chang., Chien-Ping Chang., Ping S. Huang., and Te-Ming Tu,: A Novel Image Steganographic Method Using Tri-way Pixel-Value Differencing, Journal of Multimedia , VOL. 3, NO. 2,JUNE 2008

[2] Sherly A P and Amritha P P: A Compressed Video Steganography using TPVD International Journal of Database Management Systems (IJDMS) Vol.2, No.3, August 2010

[3] Kousik Dasgupta, J.K. Mandal and Paramartha Dutta : Hash Based Least Significant Bit Technique International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, No 2, April 2012

[4] ShengDun Hu, KinTak U : A Novel Video Steganography based on Non-uniform Rectangular Partition IEEE International Conference on Computational Science and Engineering CSE/I-SPA

[5] A. Swathi , Dr. S.A.K Jilani : Video Steganography by LSB Substitution Using Different Polynomial Equations International Journal Of Computational Engineering Research Vol. 2 Issue. 5

[6] Hussein A. Aly : Data Hiding in Motion Vectors of Compressed Video Based on Their Associated Prediction Error IEEE Transactions on Information Forensics And Security, Vol. 6, No. 1, March 2011

[7] Tamer Shanableh : Data Hiding in MPEG Video Files Using Multivariate Regression and Flexible Macroblock Ordering IEEE Transactions on Information Forensics And Security, Vol. 7, No. 2, April 2012

[8] Souvik Bhattacharyya, Indradip Banerjee and Gautam Sanyal : A Survey of Steganography and Steganalysis Technique in Image, Text, Audio and Video as Cover Carrier Journal of Global Research in Computer Science Volume 2, No. 4, April 2011.