International Journal of Advance Research in Science and Engineering
Volume No.06, Special Issue No.(01), Nov 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

A Review on Various Techniques for Video Steganography

Karamjit Kaur[1], Vijay Laxmi[2]

[1]M.Phil Scholar], [2][Professor in Computer Application
Guru Kashi University, Talwandi Sabo, (India)

ABSTRACT

Nowadays, Due to technological advancement in communication, a large amount of data can be transform from one location to another on the internet. However, the privacy and security from unauthorized access remains an issue. To protect confidential information during transmission, it is necessary to conceal the information. Steganography is an art or science in which secret data is embedded in any media like text, image, audio and video. In video Steganography, we embed the secret data into a video file. Different video Steganography techniques to hide data include Least Significant bit (LSB), Hash based Least Significant bit (HLSB), Most Significant bit (MSB), Pixel Value Differencing (PVD) etc. Each Steganography techniques have different performance parameter like embedding capacity, video quality and robustness. This paper presents a study on different existing video Steganography techniques along with their performance evaluation parameter.

Keywords: DCT, DWT, LSB, MSE, LSB.

I. INTRODUCTION

In 90's, the emergence of internet in all over the world has generated a drastic change in the people's life style. With the advancement of internet and information revolution, shopping, rail reservation and even money transfer has become online i.e. people need not go anywhere, they are able to make these entire job done even in sitting in their respective home. Apart from these, the emergence of social sites has made all the people to be in touch with each other 24/7 hours. People are now able to exchange the information with each other very rapidly. Interchanging the information online has started creating problems of stealing this information by some unauthorized, unsocial group of people famously known as hackers. So this is need to design or develop some kind of application which can be able make secure transfer of utmost important or valuable information without being recognized by the unauthorized person.

The solution of these problems lies in two most widely used techniques i.e. Cryptography and Steganography.

Steganography is an art or technique which is designed to fight with such type of problems. Steganography is basically developed for hiding the valuable or confidential data in a cover file in such a way that no one other than an authorized person knows the presence of such hidden information in cover file. Audio, Video Text or even image can be used as a cover file [7].

Cryptography is basically an art of jumbling the secret information (otherwise known as Encryption) in such a way that nobody can understand it. So it can also be used to counter the above mentioned problems.

Though both the techniques are designed for the same purpose to keep the information secret from unauthorized person, both techniques are different the way they present the secret information to the real world. Cryptography encrypts the secret information in to the jumbled word which is very difficult to decipher. But for the hackers, jumbled word indicates that some kind of secret or confidential information is hidden behind these jumbled words. So they know that there is some kind of secret information but they are not able to decrypt it. On the other hand in steganography, the secret or confidential information is hidden in a innocent cover file in such a way that nobody can even imagine that such kind of information is hidden inside the cover file which may be any image, audio or video.

Another technique that is based on both steganography and cryptography is Watermarking. Watermarking is the process of protecting the copyright of original data by identifying the unauthorized person [6].

Embedding payload and embedding efficiency are the two crucial parameters of any steganography system [8]. Amount of data which can be hidden in the cover file is known as the embedding payload. The capacity of steganography system to hide as much data as it can with inducing as least distortion as it can on the cover file is known as the embedding efficiency [1].

High embedding efficiency is the prime requirement of any steganography system. High embedding efficiency means least distortion in the cover file and hence it is very difficult to imagine an existence of any secret information in the cover file. This makes it difficult to extract out the information from the cover file [1].

Embedding efficiency and embedding payload are generally having inverse proportional relationship. Increasing the embedding efficiency will decrease the embedding payload and vice versa.

II. VIDEO STEGNOGRAPHY SYSTEM

Steganography is combination of two Greek words “steganos” which means to cover, conceal or protect and “graphein” means to write [4]. Steganography is the art of hiding the information in some other host object. It has been used since ancient time by the people. In ancient time, secret information is hidden in the back of wax, scalp of the slaves, in rabbits etc [5].

With passage of time, the application of steganography and its area has become widened. Different types of steganography techniques are Linguistic, Image, Audio, Video and Network Steganography commonly used. Among these video steganography is more reliable as video is collection of pictures and audio signals. A video file contains large number of redundant bits and message can be easily embedded in repeating portion of video.

Video Steganography is a method to hide different types of files into a video file. It is difficult to detect the secret file by Human Visual System (HVS), as frames are display on screen at very fast rate. Different existing technique of image and audio steganography are also applied on video Steganography. The steganogaphy model consists of carrier video or cover object which is the carrier for secret message; secret image is secret file that is embedded and stego key for encoding and decoding. It can be described as:

(Cover object + hidden data + stego key=stego medium)

III. LITERATURE SURVEY

Ramadhan J.Mstafa et al. *(2017)* proposed a robust and secure video steganography based on motion based method in DWT-DCT domain. In this paper the steganography model has three stages, first is motion based multiple object tracking in which movement of each object is detected using Gaussian Mixture Model, second is data embedding stage in which Discrete Cosine Transformation (DCT) and Discrete Wavelet Transformation (DWT) method is used and third is data extraction stage. Hamming code and BCH code are also used to decrypt data. The PSNR value of proposed algorithm is 49.01 dB and Hiding Ratio (HR) is 3.40% [1].

Vanket P.Patil et al. (2017) represents Most Significant Bit technique to enhance PSNR, payload capacity and security of image .In MSB, the most significant bits of original image are used to hide information. The encoding algorithm calculates difference between 5th and 6th bit and compare it to secret data bit. If difference is not equal to data bit it transverse 5th bit. In this paper the PSNR value for color image is 52.68 and payload capacity is 786432 bits of transmitting [2].

K.Rosemary Euphrasi et al. *(2016*) represent the comprehensive approach based on spatial domain and IWT domain. In spatial domain Random LSB substitution method is used in which secret data is randomly distributed into red, green and blue channels. In transform domain, Haar Wavelet transforms technique in which divide the frequency domain into four sub bands. In this paper, the algorithm is implement using avi video file with PSNR, MSE and BER as performance parameter [3].

Amritpal Singh et al. *(2015)* provide an improved LSB based image steganography technique for RGB images to improve the image quality. In this paper bit plane slicing scheme is used to convert he image into red green and blue plane. To embed the 8 bit message with the original image, 2 bits of red plane, 2bits of green and 4 bits of blue plane is used. The value of PSNR obtained in proposed technique is 47.5897 and MSE is 0.1654 [4]. ***K.Steffy Jenifer et al.*** (2014) proposed LSB approach which selects the least significant bits to hide the information. In this paper, masking filtering technique is elaborated that takes 24 bits and gray scale image. Each color image is first converted into gray scale image then the transformation techniques DFT and Wavelet Transform are applied to hide the message in different areas in the image.LSB approach is simple, user-friendly and easy to implement [5].

IV. EXISING TECHNIQUES

Video steganography techniques convert the video into frame of still images and then each frame is used individually to embed the secret information. After embedding, the frames are merged together to produce a stego video that can be transmitted from one location to other. The classification of video steganography techniques represent as:-

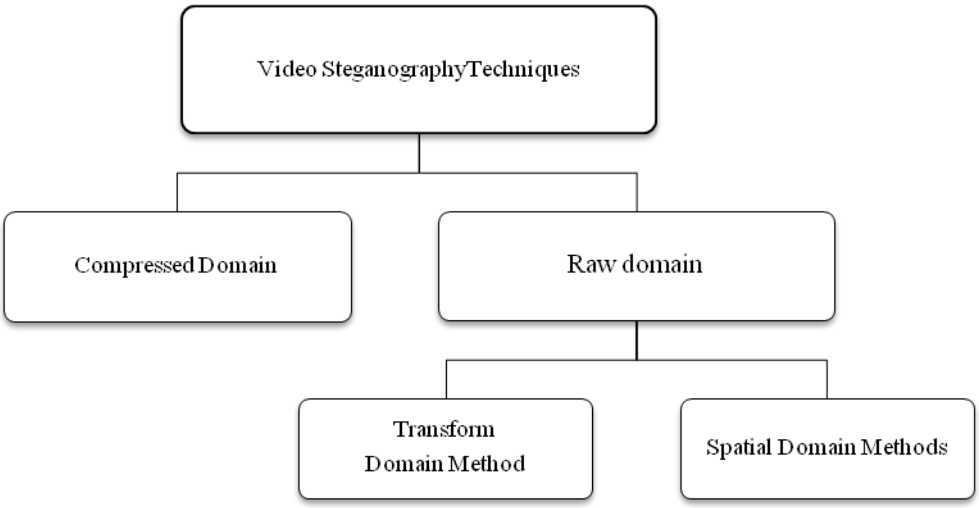

Figure1 Classification of Video Steganography Techniques

4.1 Video Steganography methods in Compressed domain

1) *Intra frame prediction*: Intra frame is independent frame that is not related to any other frame. Intra frame prediction techniques are used for video compression in which micro blocks are encoded with the help of different intra prediction modes.

2) *Inter frame prediction:* Inter frame prediction technique allow mapping of each block to embed the secret message.

3) *Motion vector:* In motion vector, Intra coded, Predicted and Bi directional frames are used to conceal the data. Each micro block contains the motion vector.

4.2 Video Steganography methods in Raw domain

1) *Spatial domain Methods*: In spatial domain technique, secret data is directly embedded into pixel of video files. The carrier video is called cover image which contain secret data as a part its pixel. Different spatial domain algorithm include:

i. Least Significant bit (LSB): In least significant bit method, the secret message that we want to send is embedded with least significant bit of video file. It protects data because there is low alteration rate of least significant pixel bits. In this method, modifications are made to the least significant bits of the carrier file’s individual pixels to encoding hidden data.

ii. Hash based LSB (HLSB): In HLSB technique, hash function is used to select the position of bits where the secret message is to be embedded. It use RGB color image which use 3 bits of red color pixels,3 bits of green color pixels and 2 of blue color pixel are used with any hash function. As the hash function is known to the intended the user, it calculates the k values to get the position of insertion. Taking the same embedded RGB value.

iii. LSB substitution using different polynomial Equations (LSB poly): In this technique, it selects the specific frame and embeds the secret data at specific location in each frame using polynomial equation. In this each character of secret message is first converted to binary form of 8-bits.It first read the original video signal and text, and then embeds the text into the video signal for converting the text data into the binary format. Binary conversion is done by taking the ASCII value of the character and converting those ASCII values into binary format

iv. LSB Matching Revisited Algorithm (LSBMR): In this technique, the secret data is embedded in specific region of video frame. The capacity of selected region is estimated to hide the secret message.

v. Most Significant bit (MSB): MSB technique allows to hide the secret message into most significant bits.MSB is an efficient technique to protect data from unauthorized access. In MSB secret data is embedded in the most significant bit of video file. It select 5th and 6th bit of and calculate difference between them to hide information.

2) Transform domain methods: In transform domain secret message is located in frequency coefficients of video file. It conceals the secret message into different area of cover video which enhances the robustness against attack. Different transform domain method are:

i.Discrete Fourier Transformation (DFT): DFT transformation convert spatial domain to frequency domain. Discrete Fourier transformation is combination of two parts, one part is real and another is imaginary parts.DFT transform one type of complex numbers to another type of complex numbers.

DFT has two variations, first is (inverse DFT (IDFT) which performs inverse transform of frequency domain to spatial domain and second is Fast Fourier method (FFT).

ii.Discrete Cosine Transformation (DCT): DCT represents a sequence of data points in terms of a sum of cosine function at different frequency.DCT is a Fourier related transformation similar to DFT but using only real numbers. It is mostly used in video compression.DCT transforms the image pixel into visual quality sub bands that may be low, middle and high [5].

iii.Discrete Wavelet Transformation (DWT): DWT transformation decomposes the video frame into horizontal, vertical and diagonal sub bands with the help of high and low frequency filters. In DWT each frame is divided into LL, HL, LH and HH sub bands. It first scans the pixel in horizontal direction and performs addition and subtraction to neighbor pixels. After that it scan pixel from in vertical direction to find low and high frequency portion [5].

V. CONCLUSION AND FURTURE SCOPE

Steganography is an efficient technique to protect information from unauthorized access over the internet. Video is more secure carrier to transmit the data because it contain many redundant bits .Video steganography techniques can be classified based on different parameter. Each technique has its own algorithm to hide the secret message into video file so that only the sender and intended recipient know about presence of secret message. This paper represents review work in different techniques that have been proposed in last few years. In future, more secure video steganography technique is required to secure the data so that it can be used in real world situations and emerge new technologies.

REFERENCES

[1] Ramadhan J. Mstafa, Khaled M. Elleithy,Eman Abdelfattah, “A Robust and Secure Video Steganography Method in DWT-DCT Domains Based on Multiple Object Tracking and ECC”, *IEEE(2017).*

[2] Venkat P. Patil, Umakant Bhaskar Gohatre, R.B. Sonawane,“An Enhancing PSNR, Payload Capacity and Security of Image using Bits Difference Base on Most Significant Bit Techniques”, *International Journal of Advanced Electronics & Communication Systems,21 March, 2017.*

[3] K.Rosemary Euphrasi, M. Mary Shanthi Rani, “A Comparative Study On Video Steganography in Spatial and IWT Domain”, *IEEE International Conference on Advances in Computer Applications (ICACA),Oct2016.*

[4] Amritpal Singh, Harpal Singh “An Improved LSB based Image Steganography Technique for RGB Images”, *IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT),March 2015.*

[5] K. Steffy Jenifer , G. Yogaraj , K. Rajalakshmi “LSB Approach for Video Steganography to Embed Images”, *International Journal of Computer Science and Information Technologies, (IJCSIT), Vol. 5 (1) , 2014, 319-322.*

[6] Paramjit kaur,Vijay laxmi, “An Upgraded approach for robust Video Watermarking Technique Using Stephens Algorithm”,*International Journal of Computer Science and Mobile Computing” Vol.3,Issue.11,Nov 2014,pg. 612-622.*

[7] Paramjit kaur,Vijay laxmi, “Review on different video watermarking techniques”,*International Journal of Computer Science and Mobile Computing” Vol.3,Issue. 9,Sept. 2014,pg. 190-195*

[8] Ramadhan J. Mstafa,Khaled M.Elleithey and eman Abdelfattah “Video Steganography Techniques: Taxonomy, Challenges, and future directions”,*IEEE Long Island Systems, Applications and Technology Conference (LISAT), May 2017.*