ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 9, September 2018

Performance Analysis of Video Steganography Techniques

Shree Raksha

Student, Department of Computer Science and Engineering, The National Institute of Engineering, Mysore, India

ABSTRACT: The rapid growth in technology and internet has facilitated transfer of data through public domain channels. There is lot of security threat as these public domains are highly vulnerable. However, the data transmission can be protected by using various methods like cryptography, steganography, hashing and authentication. At the apex of these methods is Video steganography, a technique to hide confidential data in visual medium, which gives reliability and privacy of data. The intricacy of the structure of the video file makes it hard for hacker to recognize by naked eye that promises security against steganalysis. The paper illustrates the progress in the field of video steganography, its uses and aims to give the performance comparison of the techniques based on secret media. Performance analysis of these techniques gives an overview of the suitable method for different media.

KEYWORDS: K-means clustering, LSB, DCT, TPVD, Random Byte Hiding

I. INTRODUCTION

Steganography is a modus operandi to implant secret information into various multimedia files such as audios, images, and videos. These files are used as cover media in which secret information (any multimedia file) is hidden. Steganography is categorized as Image Steganography, Audio Steganography and Video Steganography based on the cover media used.

Video Steganography is used for hiding data in a video file. Video steganography methods can be categorised as spatial (time) domain method and transformation domain method. Spatial domain techniques hide information by using pixel grey levels and their colours for encoding message bits. This method has high capacity, and more data can be transmitted in public domain.Transformation domain techniques are equipped with strong function to encode the message bits in the transform domain coefficients of the image. Military, industrial applications, copyright, intellectual property rights etc. are the most commonly used applications.

The Video Steganography technique is an attempt to use the bits of the secret medium to replace the redundant bits of the cover medium. The secret data is implanted in a cover video by using embedding algorithm. The cover medium to be selected is decided by the type of data, the size of the secret message and other carrier file formats. The obtained video is the stego video which is transmitted by the sender to the receiver through communication channel. The receiver uses extraction algorithm to extract the secret data as shown in Fig 1.

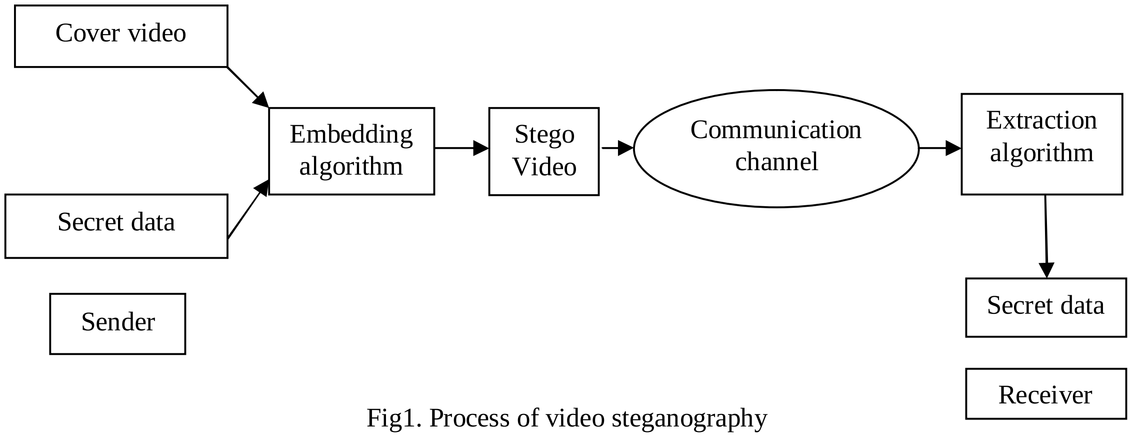

Fig1. Process of video steganography

DOI: 10.15680/IJIRCCE.2018. 0609044

Following are the characteristics of an effective Steganography technique:

(1) *Confidentiality*: the hidden information cannot be extracted without proper authentication.
(2) *Imperceptibility*: the data hidden is completely undetectable by observer and computer analysis.
(3) *Capacit*y: the highest length of the hidden message that can be embedded in a video.
(4) *Precision*: the accuracy and reliability of the hidden data extracted from the medium.

The next section of the paper is dedicated to give an overview of related works of video steganography techniques followed by description of techniques, comparison tables and result.

II. RELATED WORK

In line with K U Singh, LSB (least significant bit) insertion technique on video steganography[1] can be used to hide text information. The LSB of a video file is changed with information bits. The cover video is split into frames, whose least significant bits are identified. The least significant bits of the individual pixels of cover files are changed with message bits to obtain the stego video. Each pixel has RGB components which contains 3 bits of secret message. 24 bit image like bitmap is used to hide 3 bits of message in each pixel. By obtaining the positions of the embedded bits, the secret information can be extracted.

Sherley A P and Amritha P P proposed a new compressed video steganography scheme for hiding text information where data hiding operations are executed entirely in the compressed domain. The data are embedded in the macro blocks of I frame with maximum scene change and in the block of P and B frames with maximum magnitude of motion of vectors. In tri-way pixel value differencing scheme(TPVD) the edges in an image are categorized into horizontal, vertical and two other kinds of diagonal directions[2]. Two-way pixel pairs on one directional edge work efficiently for information hiding by considering four directions from four two-pixel pair which can be implemented by dividing the image into 2*2 blocks. Change in pixel values of the fourth pixel pair affects first and second pair; the fourth place pair is useless and must be discarded. Therefore three pairs are used to embed the data.

PrajnaVasudev and Kumar Saurabh proposed a videosteganography method using 32*32 vector quantization for DCT for hiding text information[3]. The cover video is sliced into number of images. All the sliced images are passed to the 32*32 pixel management procedure followed by the LSB quantization method through which the vacant spaces of the images are found. The text message to be embedded is converted to the ASCII encoded bits to make it compatible to the vector table of the current segment of the video. Those bits that have low intensity are filled first and the rest are embedded into high intensity bits.

U Kin Tak et.al, proposed an algorithm of non-uniform rectangular partition of image according to the pixel grey values[4]. The three main factors in the process are initialpartition, bivariatepolynomial and control error. When all these factors are determined, the adaptive partition algorithm can be applied to do the non-uniform rectangular partition of image. This algorithm uses the optimalquadraticapproximation with a specified bivariate polynomial to approximate the grey values within the sub-images. If the determined bivariate polynomial can recover the original sub-image, the partition process will be terminated, otherwise the current sub-image will be divided into four smaller congruent rectangles and approximation process is repeated again until the approximation requirement is reached. Based on the partitioned codes obtained, the original image is reconstructed approximately.

According to K. Steffy Jenifer et.al, the LSB approach along with masking filtering is used to hide the secret image in video steganography[5].The bits of the image are directly embedded into least significant bit plane of the cover-frame in deterministic sequence. The embedding capacity can be increased by using two or more least significant bits.
Masking and filtering are used on 24 bits/pixel images and are applicable for both colored and gray scale images. It hides information by marking an image.This technique embeds the information in significant areas so that the hidden message is integral to cover image than just hiding it in the noise level. In order to provide security the original image is converted into the gray scale image which contains the black and white pixels.In data masking the secret message is so processed that it appears similar to a multimedia file.

DOI: 10.15680/IJIRCCE.2018. 0609044

Prabira Kumar Sethy et.al, proposed a video steganography of image using K-means clustering and direct mapping[6].In this method the message bits are clustered and grouped together using K-means clustering algorithm. Cover video and secret image are selected,their information is collected and K-means clustering algorithm is applied for image quantization.Clustered message is embedded inside the cover medium by using direct mapping resulting instego video.

Rachna Patel and Mukesh Patel proposed a method for hiding information inside another video file using random byte hiding and LSB technique[7].In random byte hiding technique,the information is hidden at different places of each line of the video frame. The selected cover video is split into frames, the secret message or image is split into byte stream and using random byte allocator the message byte is inserted inside the cover video frame at random location to obtain the stego video. All frames that contain data are extracted from the stego video anddecryptor is used to extract hidden data byte from these frames which are then merged to obtain the required secret data.
In LSB technique, first the cover video file is read and then segmented into frames. Simultaneously the secret message is split into bit stream of R × C group size and then rearranged. Small messages are encrypted into a byte of data bit on LSB and checked if all small messages are completed or not.Ifhidden messages are included in these messages then rule list is created and stego video is generated. To obtain back the secret video, the stego video is segmented into frames, small messages are decrypted from the frame for each column, row and LSB is extracted. Then all the data are mergedto generate the secret video message.

ShengDun Hu, KinTak U presented a video steganography system based on non-uniform rectangular partition. This technique is used for uncompressed videos. In this method a secret video is hidden in a cover video. In each frame of both the videos, a mechanism is applied for hiding the video stream[8]. The frame length of the cover video should be greater than or equal to the frame length of the secret video. Each frame of secret video is partitioned into non-uniform rectangular part which is encoded. The secret video stream is hidden in the leftmost four least significant bits of each frame of the host video stream.

III. VIDEO STEGANOGRAPHY TECHNIQUES

A.K-means Clustering

K-means clustering is a method of vector quantization. It aims to partition ‘n’ observations into ‘k’ clusters. Each of ‘n’ observation belongs to the cluster with the nearest mean, serving as a prototype of the cluster. steganographic system hides information by identifying a cover medium’s redundant bits. The embedding process is made by creating stego medium to replace these redundant bits with data from the hidden message.

B. Discrete Cosine Transform (DCT)

Discrete Cosine Transform (DCT) is a mechanism used in the JPEG compression algorithm. DCT transform successive 88-pixel blocks of the image from spatial domain to 64 DCT coefficients each in frequency domain. The least significant bits of the quantized DCT coefficients are used as redundant bits into which the hidden message is embedded. The advantage of DCT over other transforms is the ability to minimize the block-like appearance resulting when the boundaries between the 8x8 sub-images become visible (known as blocking artifact).

C. Least Significant Bit (LSB)

Least Significant bit (LSB) is said to be the superior method for data protection because of its simplicity and commonly used approach. The first frame is selected as index frame. The index frame consists of information regarding where the information is stored, in which form information is getting stored, what is file type of the information, etc. If the first frame is received properly and if the receiver recognized the information then it is very easy to get hidden information from steganography video file.

D. Random Byte Hiding

In this technique, the information is hidden in each line of the video frame at different place. For example, if the line begins with the pixel value of ‘zz’, the information is stored over the ‘zz’+x location, where x is only known to the authorized receiver. So, when unknown person view the video, he sees it as normal video, while the person knowing the steganography can detect the hidden message. The same kind of technique can be implemented by using ‘y-zz’ where y must be taken above the 256 (a bit higher than logical high level) so that ‘y-zz’ does not go negative. The similar technique can be implemented over the column line also.

E.Pixel-Value Differencing (PVD)

The pixel-value differencing method uses the difference value between two consecutive pixels in a block to determine how many secret bits should be embedded. There are two types of the quantization range table. The first is based on selecting the range widths of [8, 8, 16, 32, 64, 128], to provide large capacity. The second is based on selecting the range widths of [2, 2, 4, 4, 4, 8, 8, 16, 16, 32, 32, 64, 64], to provide high imperceptibility. Here data are embedded in the macro blocks of I frame with maximum scene change and in block of P and B frames with maximum magnitude of motion vectors. To enlarge the capacity of the hidden secret information and to provide an imperceptible stego-image for human vision, a novel steganography approach called tri-way pixel-value differencing (TPVD) is used for embedding. In this scheme all the processes are defined and executed in the compressed domain.

F. Non-Uniform Rectangular Partition

This method is for uncompressed videos. In non-uniform rectangular partition, data hiding is done by hiding an uncompressed secret video file in the host video stream. But we have to make sure that both the secret as well as the cover file should be of almost the same size. Each of the frames of both the secret as well as cover videos is applied with image steganography with some technique. The secret video file will be hidden in the leftmost four least significant bits of the frames of the host video.

G. Masking and Filtering

Masking and filtering technique, usually restricted to 24 bits or grayscale images, take a different approach in hiding a message. This method is effectively similar to paper watermarking, creating markings in an image. This can be achieved for example by modifying the luminance of parts of the image.

IV. Comparison of Techniques Based on Secret Media

The secret information can be in the form of text, image or video. Based on the secret media used, the video steganography techniques can be compared as shown in the below tables.

Table I.Text as secret medium

Techniques	Domain	Payload Capacity	Imperceptibility	Advantages	Disadvantages
LSB	Spatial	Low	High	simple, low computation, high bit rate	Lossy technique
TPVD	Spatial	High	High	No degradation in visual capacity	Leads to distortion, Lossy technique
DCT	Transform	Low	Medium	High Robustness Decreased colour and visual distortion	Lossy technique

DOI: 10.15680/IJIRCCE.2018. 0609044

Table II.Image as secret medium

Techniques	Domain	Payload Capacity	Imperceptibility	Advantages	Disadvantages
Non Uniform Rectangular Partition	Spatial	High	Medium	Simple computation, High encoding and reconstruction speed, no visual Distortion	Long coding time
LSB	Spatial	High	High	Simple and effective	Image fidelity degrades, robustness is low
Masking & Filtering	Spatial	Low	High	High Robustness	Lossy compression technique, restricted to 24bits per pixel
K-means clustering	Spatial	High	High	High PSNR value, Lossless technique, High robustness	Difficult to predict the number of clusters
Random Byte Hiding	Spatial	Medium	Medium	Randomness of hidden information provides security, less encryption and decryption time	Lossy technique, low hiding data ratio

Table III. Video as secret medium

Techniques	Domain	Payload Capacity	Imperceptibility	Advantages	Disadvantages
LSB	Spatial	High	High	Size of secret and cover video is same	Not robust against compression, Hides in independent frames
Non Uniform Rectangular Partition	Spatial	High	Medium	No visual distortion in host video, All PSNR value > 28db	Inaccurate retrieval of secret bits leads to poor PSNR of the extracted frames

DOI: 10.15680/IJIRCCE.2018. 0609044

V. RESULTS

The comparative study of various video steganography techniques gives quick look of suitable methods that can be used based on different secret media used. For transmitting text type data in secret mode, the TPVD technique is the most suitable when compared to LSB and DCT techniques as shown in Table I due to high capacity and imperceptibility of TPVD technique. When the secret medium is an image then K-means clustering is the most appropriate method. It is lossless technique to safeguard secret medium from attacks using steganalysis and statistical as described in Table II. When secret medium is video both LSB and non-uniform rectangular partition techniques have high capacity. But, LSB is more suitable as it has high imperceptibility and better PSNR value when compared to rectangular partition techniques as shown in Table III.Taking all the requirements and constraints into consideration sender and receiver must chose the appropriate technique for transmission of information.

VI. CONCLUSION AND FUTURE WORK

This paper gives a synopsis of different video steganography techniques applied to the three most commonly used domains such as Image, Text and Video. When information is hidden in video, it is difficult for unauthorized users to detect even by using steganalysis. Comparing the performance of video steganography techniques is difficult unless identical data sets and performance measures are used. Internet banking, mobile communication security, cloud security and so on are new application areas than can make best use of steganography to maintain secrecy of information transmitted.

REFERENCES

1. K. U. Singh, ‘Video Steganography : Text Hiding In Video By LSB Substitution’, *Int. J. Eng. Res. Appl.*, vol. 4, no. 5, pp. 105–108, 2014.
2. K. Group, ‘A Compressed Video Steganography using TPVD A Compressed Video Steganography using TPVD’, vol. 2, no. February, pp. 67–80, 2016.
3. Prajna Vasudev,Kumar Saurabh ," Video steganography using 32*32 vector quantization of DCT", International Journal of Software & Hardware Research in Engineering Vol. 1 Issue. 3,Nov.2013.
4. Z. Tang and D. Qi, ‘A non-uniform rectangular partition coding of digital image and its application’, pp. 995–999, 2009.
5. K. S. Jenifer, G. Yogaraj, and K. Rajalakshmi, ‘LSB Approach for Video Steganography to Embed Images’, vol. 5, no. 1, pp. 319–322, 2014.
6. P. K. Sethy, K. Pradhan, and S. K. Behera, ‘A security enhanced approach for video Steganography using K-Means clustering and direct mapping’, *Int. Conf. Autom. Control Dyn. Optim. Tech. ICACDOT 2016*, pp. 618–622, 2017.
7. R. Patel and M. Patel, ‘Steganography over video file by hiding video in another video file, random byte hiding and LSB technique’, *2014 IEEE Int. Conf. Comput. Intell. Comput. Res. IEEE ICCIC 2014*, 2015.
8. S. D. Hu and K. T. U, ‘A novel video steganography based on non-uniform rectangular partition’, *Proc. - 14th IEEE Int. Conf. Comput. Sci. Eng. CSE 2011 11th Int. Symp. Pervasive Syst. Algorithms, Networks, I-SPA 2011 10th IEEE Int. Conf. IUCC 2011*, pp. 57–61, 2011.

DOI: 10.15680/IJIRCCE.2018. 0609044