International Journal of Innovative Research and Advanced Studies (IJIRAS)
Volume 4 Issue 1, January 2017

ISSN: 2394-4404

Video Steganography By Using Discrete Wavelet Packet Transform: A Survey

Parinita Sahu

M. Tech. Scholar, Department of ETC,
GDRCET, Bhilai

Swapnil Sinha

Assistant Professor, Department of ETC,
GDRCET, Bhilai

Abstract: ***The survey on video Steganography has been investigated over many years. As the world has moved to the digital era, the whole content of the living being has been uploaded to the server over internet. As the number of people using the internet is increasing, the misuse of the private content has increased. Hence there is a requirement of securing the data which is uploaded to the internet irrespective of the necessity. Now a day's with the increase in the use of internet, the security and confidentiality of sensitive data and secret data has became a prime concern. Steganography is one of the most popular techniques for security purpose. Steganography is a technique in which we hide the secret data into other medium. In this paper we have surveyed different technique of Steganography for the security and confidentiality of secret data.***

This paper provides an overview of analysis of different existing methods of video Steganography. Finally, some suggestions have also provide based on the theoretical study.

Keywords: Video Processing, Video Frame, Cover Media, Discrete Wavelet Transform.

I. INTRODUCTION

Data security is most important requirement for the protection of secret data from the hackers in secure communication. Now as the world becomes more digitized it has become very important to secure our secret data from eavesdroppers. Now a day a lot of applications are internet based and in some cases it is desired to made secure communication. For the data security there are two techniques: one is cryptography and second is Steganography. In cryptography technique the secret data is changed its character such that it can't be understood by unauthorized user. While in Steganography technique the secret data is hiding inside cover medium. Message, image, audio, video etc can be used as cover medium. The word Steganography comes from Greek word Steganos which means "covered writing" or "concealed writing". Cryptography and Steganography are different technique. In cryptography scrambling of messages is applied where as in steganography message is unobservable and undetectable.

Steganography is the art of insensible communication. The aim of Steganography is to hide a secret message by embedding a message in such a way that a third person cannot see the presence of hidden message, on other hand cryptography is the technique to change the original message into cipher text by encrypting original secret message. Steganography provides on more security by hiding cipher text into another cover message [2]. Both technique can be used together for better security.

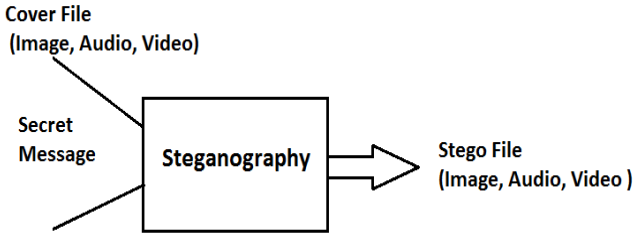


Figure 1: Basic Steganography System

After applying Steganography on secret data the output of Steganography system is known as stego file. Here we are

dealing with video so the output is known as stego video. The quality of stego video can be measured by performance parameters such as peak signal to noise ratio (PSNR), mean square error (MSE) [1].The technique in Steganography can be divide into two category one is spatial domain methods and second is transform domain methods. In spatial domain method, the processing is applied on the image pixel values. For example, Least Significant Bit (LSB) replacement and matching technique of video Steganography is spatial domain method. In transform domain method, the transformation is applied on image, firstly cover image transforms into frequency domain. The method comes under this category are Discrete cosine transform (DCT), Discrete Fourier Transform(DFT), Discrete Wavelet Transform(DWT) [6]. Time domain method is computationally complex than spatial domain method. Recent video Steganography technique use swapping algorithm and UTF-32 coding scheme for secure the secret data. This method involves hiding the secret data first in an image then it will attach to a cover media which is video file [5].The evolution of Steganography technique is characterized by three different aspects. They are capacity, security, and robustness. Capability means how much system have capable of hiding the information into cover media, security means it should be secure the content of secret data from unauthorized user attacks, and robustness tends to it should be robust to any changes [3], [5].

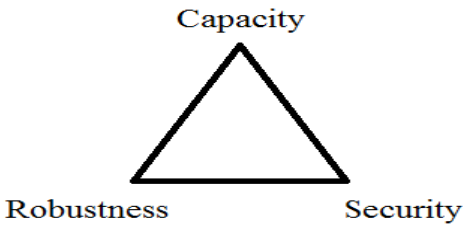


Figure 2: Video steganography system feature

II. RELATED WORK

Securing the video content is not easy in the present scenario hence some amount of processing is required to detect any fraud over it. To understand the video processing using various methods this paper provides a survey on processing and securing the video content as discussed below.

Lio et al. proposed video Steganography based on the Expanded Markov and joint distribution on the transform domains – detecting MSU stego video. In this paper scheme of detection of hiding data in stego video is explained. Discovering the presence of hidden information is known as steganalysis. The detecting scheme of hiding data in video is based on the transform domain, including discrete cosine transform DCT and discrete wavelet transform. The steganalysis performance in multiple JPEG images is successfully improved by expanding approach to the inter-bands of the DCT domain, combined the Expanded Markov feature and polynomial fitting of the histogram of the DCT coefficient. In this paper data is hide in MSU stego video so the feature matrices are extracted from original and stego video then optimal or suboptimal feature set is determined from the feature matrices then construct the classification model [8].

Balaji et al. proposed secure data transmission using video Steganography. In this paper the proposed method is based on creates an index for the secret data then that index is placed in a frame of the video. In this method the secret data is not hidden in the sequential frames of video. Rather than it uses random frames of video to hide the secret data. Instead of searching secret data in entire video it creates an index for secret data just like the index of book, so that without analyzing the full video we can find the position of frame that contain secret data with the help of index. This method decreases the probability of finding the hidden data by eavesdropper compare to the other method of hiding secret data in sequential frame of video as well as it reduces computational time and provide better security. In this method secret data is hiding in some random frames of video and remaining frames of video contain random value this provides additional security [5].

Patel et al. proposed lazy wavelet transform based Steganography in video. Least significant bit (LSB) technique mostly use for Steganography but in this paper instead of traditional LSB encoding technique they use a modified encoding technique in which at first transform is applied on video by using lazy lifting wavelet transform and then secret data is hidden in the sub-bands of the video by using LSB method. The lazy wavelet transform is applied on visual frames and the secret data is store in the component of the visual frame. Here the secret data is hidden in sequential frames. The method proposed in this paper consist following phases: encrypting the given secret data file, converting given encrypted cipher data into a stream of bits, applying lany wavelet transform on the frames of the video, hiding the total length and number of bits in the last frame in the audio using LSB. This method provides high payload capacity and has low computational requirement [9].

Khare et al. suggested video Steganography by LSB technique using neural network. The performance of video Steganography can be improved by using neural networks methods such as artificial neural network (ANN) and back propagation neural network (BPNN). This paper present an improved method of secret data hiding is based on the back propagation neural network method. Neural method is used to perform XOR operation. In this method secret data is hiding in frames of video by using secret key and bit number with the help of XOR which is trained by neural network. The encrypted message is embedded in the least significant bit of the selected frame of video. The neural network algorithm prepare pattern that has input layer, output layer, one or more hidden layer which provide confidentiality. The neural network algorithm is shared between sender and receiver through a protected channel. Neural network enhances the security [11].

Thakur et al. proposed secure video Steganography based on discrete wavelet transform and Arnold transform. In this paper video Steganography technique in which secret data is hiding in cover video is explained. For data hiding discrete wavelet transform (DWT) is used in this paper. Firstly, cover video is decomposed into its frames (images) and select frame for hide secret information. Now DWT is performed on

selected frame then it decomposes the image into four different coefficients: approximate coefficient, horizontal coefficient, vertical coefficient, diagonal coefficient. The secret data is firstly encrypted by using Arnold transform algorithm and private key then this encrypted data is embedded with approximate coefficient of selected frame for hide secret data such that no one observes the secret data. Then inverse discrete wavelet transform is applied on stego image after then reassembling frame with the rest of the frame to form a stego video. The Arnold Transform has been presented in the paper with encoding and decoding process as discussed in section 3.

III. WORKING PRINCIPAL

A. ENCODING PROCESS

In encoding process secret image is embedded into cover video. Frames of cover video is separated, out of these frames a specific frame is selected.

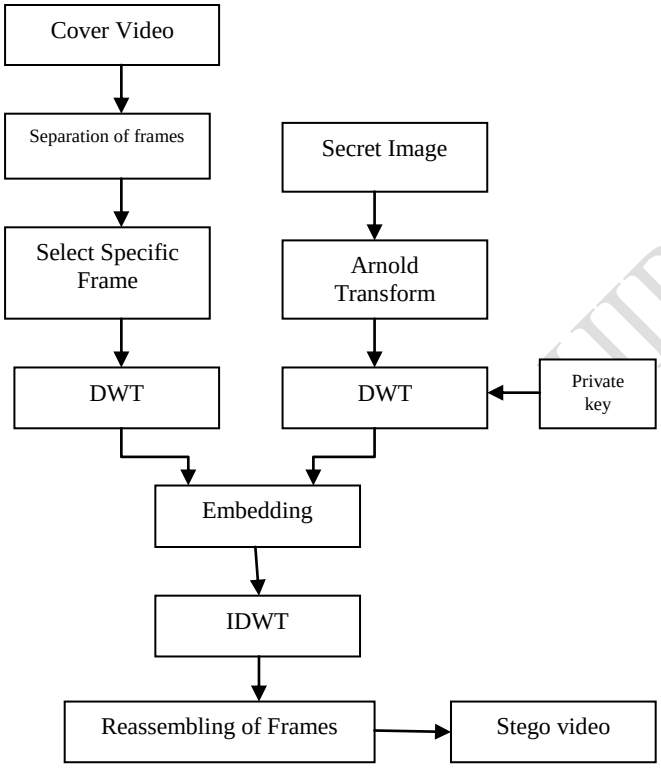


Figure 3: Block Diagram of Encoding Process

Now DWT applied on this specific frame. On other hand secret image is encrypted using private key and then DWT applied on it. Then secret encrypted image is embedded with the sub-band of specific frame or image. Apply IDWT on embedding image and reassembling the specific frame and remaining frames of cover video to get stego video.

B. DECODING PROCESS

In decoding process, the original secret image is extracted from stego video. In this process first of all cover video and stego video decomposed into its frames, and then select specific stego image from frames of stego video and select specific frame from cover video and discrete wavelet transform is applied on both specific image and stego image. Now embedding the resultant images is performed. Then IDWT is performed on this embedded image to reform encrypted image the by using private key decrypt this image and finally we get the original secret image.

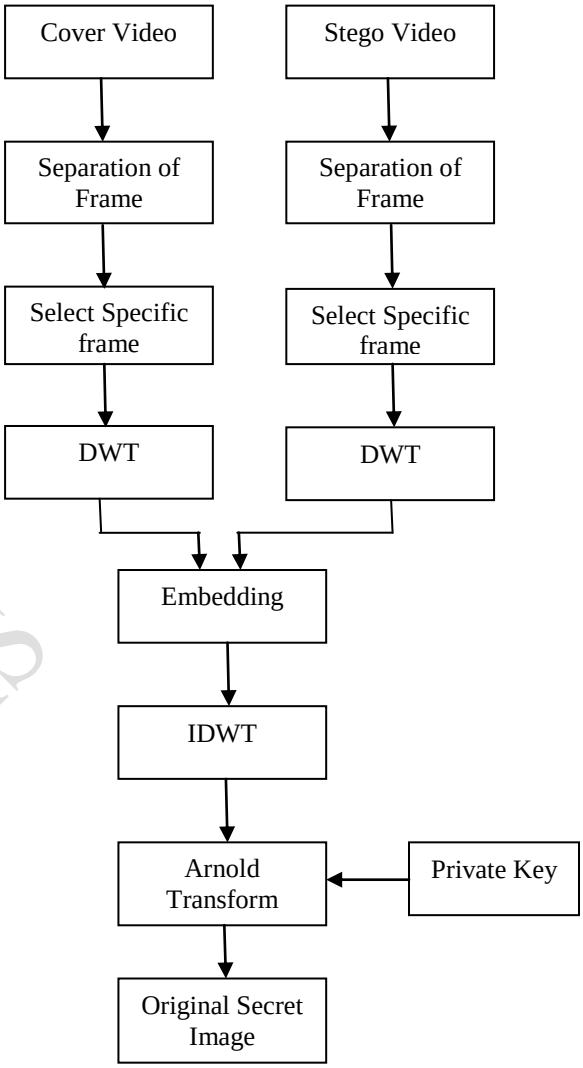


Figure 4: Block Diagram of Decoding Process

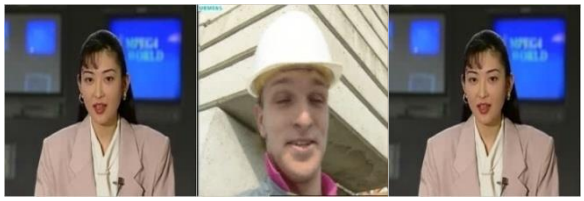
IV. RESULT

The result obtained by the researchers shows that there is no considerable change in the image characteristic of the frames and hence provides a better way to process the video signal for the purpose of security and to preserve the information content in the video. Some results obtained after applying the methods are shown in figure below.

(a) 1st Frame (b) 20th Frame (c) 40th Frame

Figure 5: Frames of Original Video

ISSN: 2394-4404



(a) Original 20th frame (b) Secret image (c) Stego image

Figure 6: Hiding Secret Image

(a) 1st Frame (b) 20th Frame (c) 40th Frame

Figure 7: Frames of stego Video

V. CONCLUSION

Today's world is of high speed internet; people are worried about the information being hacked by unauthorized person or attackers. So to solve this problem many techniques of Steganography have been proposed. By analyzing different method of Steganography we conclude that the hiding of secret data is not enough the main focus in Steganography technique is to increase the capacity to hide the secret information, it should robust to change in information and provide high security as possible as. Several many researches provide high security by combining cryptography and Steganography techniques which gives better performance compared to using only Steganography system.

ACKNOWLEDGEMENT

The review on Video signal processing is in important part for my research work and to clearly understand the processing on it, the paper used here provided immense information. Therefore I acknowledge all the researchers whose paper has been utilized for the survey.

REFERENCES

[1] Abhinav Thakur, Harbindar Thakur, Shikha Sarad, "Secure Video Steganography Based on Discrete Wavelet Transform," in International journal of computer application., vol.123, no. 11, pp. 0975–8887, Aug 2015.

[2] Sweta V, Prajit V, Kshema V, "Data Hiding Using Video Steganography- A Survey", IJCSET, vol. 5, issue 6, pp. 206-213, June 2015.

[3] Vipul Madhukar Wajgande and dr. Suresh Kumar, "Enhancing Data Security Using Video Staganography," in International journal of emerging technology and advance engineering, vol. 3, issue 4, April 2013, pp. 2250–2459.

[4] Prabhakaran. G and Bhavani. R, "A Modified Secure Digital Image Steganography Based on Discrete Wavelet Transform," International conference on computing, electronics and electrical technologies, year 2012.

[5] R. Balaji and G. Naveen, "Secure Data Transmission Using Video Steganography," IEEE international conference on electro/information technology, year 2011.

[6] Pratap Chandra mandal, "A Study of Steganography Technique Using Discrete Wavelet Transform," in Journal of global research in computer science, vol. 5, no. 5, may 2014

[7] J. J. chae and B. S. Manjunath , "Data hiding in Video ," IEEE Proceedings 1999 International Conference on Image Processing , vol, 1, year 1999.

[8] Qingzhong Liu, Andrew H. Sung, and Mengyu Qiao, "Video Steganography Based on the Expanded Markov and Joint Distribution on the Transform Domains," IEEE 2008 seventh international conference on machine learning and applications, year 2008.

[9] Khushman Ptel, Kul Kauwid Rora, Kamini Sing, Shekhar Verma, "Lazy Wavelet Transform Based Steganograohy in Video," IEEE 2013 international conference on communication system and network technologies, year 2013.

[10] Pooran singh negi and Demetrio Labate, "3D Discrete Shearlet Transform and Video Processing," IEEE transactions on Image processing, vol.21, year 2012.

[11] Richa Khare, Rachana Mishra, Indrabhan Arya "Video Steganography By LSB Technique using Neural Network," IEEE 2014 sixth international conference on computational intelligence and communication networks, year 2014.

[12] Prabhjot Kour, "Image Processing using Discrete Wavelet Transform", International journal of electronics and communication, vol. 3, issue 1, jan 2015.