International Journal of Mineral Processing and Extractive Metallurgy
2017; 2(1): 7-12
http://www.sciencepublishinggroup.com/j/ijmpem
doi: 10.11648/j.ijmpem.20170201.12

Discrete Wavelet Packet Transform Based Video Steganography

Parinita Sahu, Swapnil Sinha

Department of ETC, Rungta Group Colleges, Bhilai, India

Email address:
parinita1205@gmail.com (P. Sahu), swapniletc1@gmail.com (S. Sinha)

To cite this article:
Parinita Sahu, Swapnil Sinha. Discrete Wavelet Packet Transform Based Video Steganography. *International Journal of Mineral Processing and Extractive Metallurgy*. Vol. 2, No. 1, 2017, pp. 7-12. doi: 10.11648/j.ijmpem.20170201.12

Received: May 23, 2017; **Accepted**: June 12, 2017; **Published**: July 21, 2017

Abstract: Now the world became more digitalized and the digital communication over the internet increases day by day. At present days the digital data is widely transfer over the internet and the whole information of living being has been uploaded on the server. With the increase of internet use, the misuse of private data also increases. There exist are many hackers and they may easily hack our private data too. So now a days security of private data has become major part of concern. For the prospective of security, cryptography and steganography of secret data can be used. In cryptography the original secret message is converted into ciphertext that is understood. While in steganography technique the secret data is hiding in cover media. Cover media may be multimedia file such as data, images, audios and videos. In this paper we are introducing video steganography technique using discrete wavelet packet transform (DWPT). Additional security can be achieved by using combined cryptography and steganography for better security of secret information. Result shows that the video steganography using discrete wavelet transform provide better performance parameter as compare to other technique of steganography.

Keywords: Video Steganography, Cryptography, Video Frame, Cover Media, Discrete Wavelet Packet Transform

1. Introduction

For the protection of our private information the data security is most necessity. Now a day use of internet increases so there are chance of secret data can be hacked by cyberpunk. Currently, it is extremely simple to create an unrestricted number of copies of digital information & their distribution or allocation does not require complex action. In addition, to this sociable software editing tool allows simply altering the content of multimedia data. Thus, it is essential to build up technique which able to defend sensitive information from unauthorized exercise. There are numerous techniques associated with the data security are developed some of them most popular techniques are cryptography and steganography.

Cryptography is branch of science that define art of secret writing. Cryptography is a technique in which secret data is change by its character in such a way that third any intruder can't identify the message. Modern cryptography is generally founded on mathematical theory, cryptography algorithms are design around computer hardness assumptions and making such algorithms that is difficult to break by any adversary.

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.

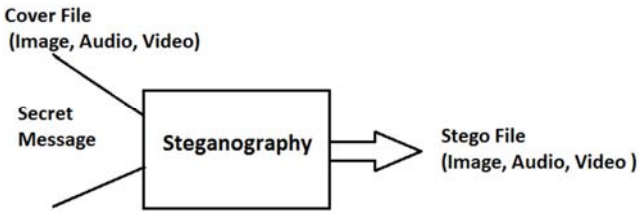

Figure 1. *Basic Steganography System.*

In this paper video steganography is used. After applying Steganography on secret data the output of Steganography system is known as stego file. After embedding secret message inside video the resultant video is called stego

video. The quality of stego video can be measured by different performance parameters such as peak signal to noise ratio (PSNR), mean square error (MSE). For video steganography there are two approaches which are generally used, one is spatial domain approach and second is frequency domain approach. One of the simple and common technique of steganography is least significant bit (LSB) method is belongs to spatial domain approach but this method is not much sufficient. While discrete cosine transform (DCT) and Discrete wavelet transform (DWT) methods are based on frequency domain approach [6]. The characteristics of steganography can be define by three different aspects that are capacity, security, and robustness. Capacity means that 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 system should be roust to any change in the content of secret message [3], [5].

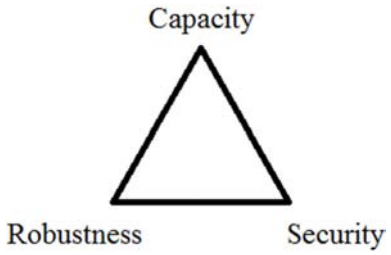

Figure 2. *Video steganography system feature.*

2. Related Work

Various method on steganography has been investigated over many year, a secure technique of video steganography was proposed. In this paper the proposed method is create an index to secret data and then that index is placed in a video frame [5]. LSB substitution technique was introduce in an improved method of data hiding based on back propagation neural network. In this method XOR operation is performed by using neural network and secret data is embedded into video by using LSB substitution method [11]. A high payload capacity video steganography method was proposed is based on lazy lifting wavelet transform method. In this method it uses modified encoding technique of traditional LSB encoding technique. In this method firstly lazy lifting wavelet transform is applied on the video frames then data is hide in the coefficient of video frame by using LSB substitution method [9]. Recently data hiding technique is based on discrete cosine transform and discrete wavelet transform. This method is introduced in video steganography baced on the expanded markov and joint distribution on the transform domain – detecting MSU stego video [8].

3. Working Principal

In this DWPT based video steganography technique two process are used that are encoding and decoding. In this section the proposed work is discussed in detail.

3.1. Discrete Wavelet Transform (DWT)

The discrete wavelet transform represents the signal in its sub-band coefficients. The discrete wavelet transform decompose the signal into its wavelet coefficients. In DWT the decomposition of signal using discrete wavelet transform decomposed in two parts, approximated component and detailed component. Then approximated component again decomposed into two parts but further decomposition of detailed component is not possible.

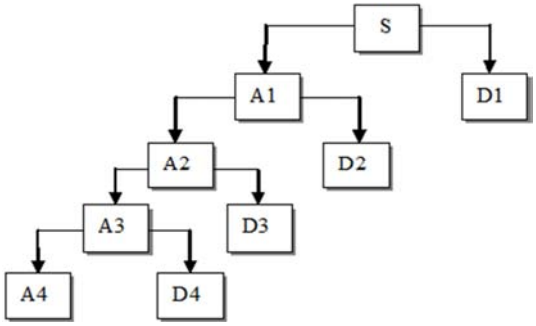

Figure 3. *DWT Decomposition Tree.*

3.2. Discrete Wavelet Packet Transform (DWPT)

Discrete wavelet packet transforms similar to the DWT, with difference between them is that the DWPT uses more filters than DWT to decompose the discrete time signal. In the decomposition of signal using wavelet packet transform first of all signal is decomposed into two part approximated component and detailed component then there are further decomposition of both component is possible. There is more data loss occur in discrete wavelet transform as compare to wavelet packet transform because of in DWT the further decomposition of detailed component is not possible where as in WPT further decomposition of detailed component is possible.

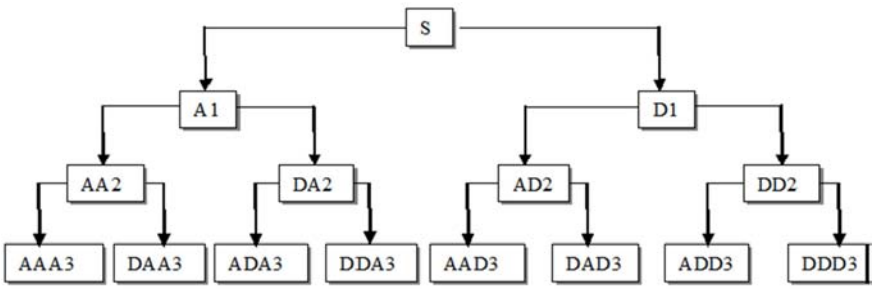

Figure 4. *DWPT Decomposition Tree.*

3.3. Encoding

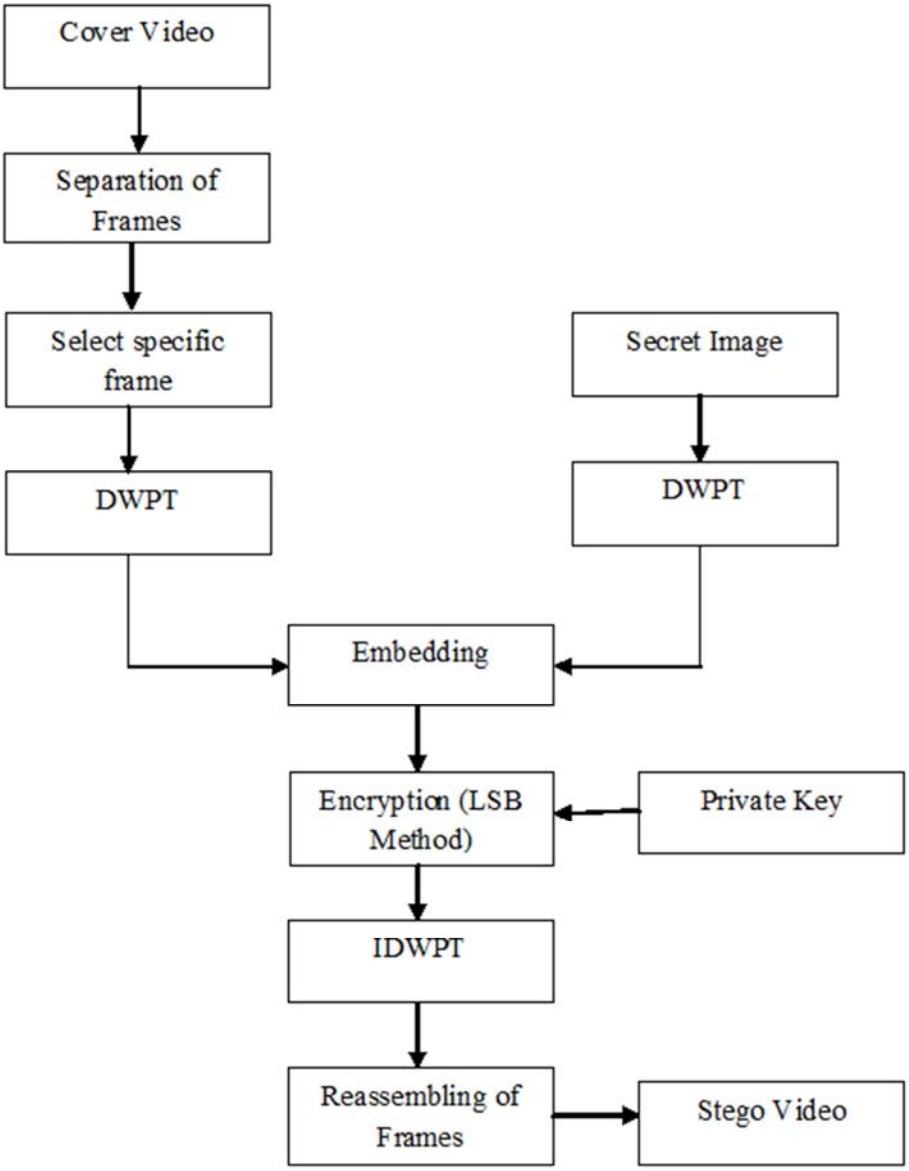

Figure 5. *Flow Chart of Encoding Process.*

Step 1: One video is taken as a cover video in which we want to hide our secret image, and separates the frames of cover video and save indivisual frame in a separate folder.

Step 2: One specific frame of cover video is selected and twolevel DWPT is performed on the selected frame. Then frame is decomposed into its coefficients.

Step 3: Secret image is taken and two level DWPT is performed on it. Secret image is decomposed into its coefficients.

Step 4: Now embeds the coefficients of specific frame of cover video with the coefficients of secret image and then apply LSB encryption by using private key.

Step 5: Finally IWDPT is performed to get stego image in which our secret image is hidden and then the stego image is integrated with the rest of frames of the cover video to get a stego video.

3.4. Decoding

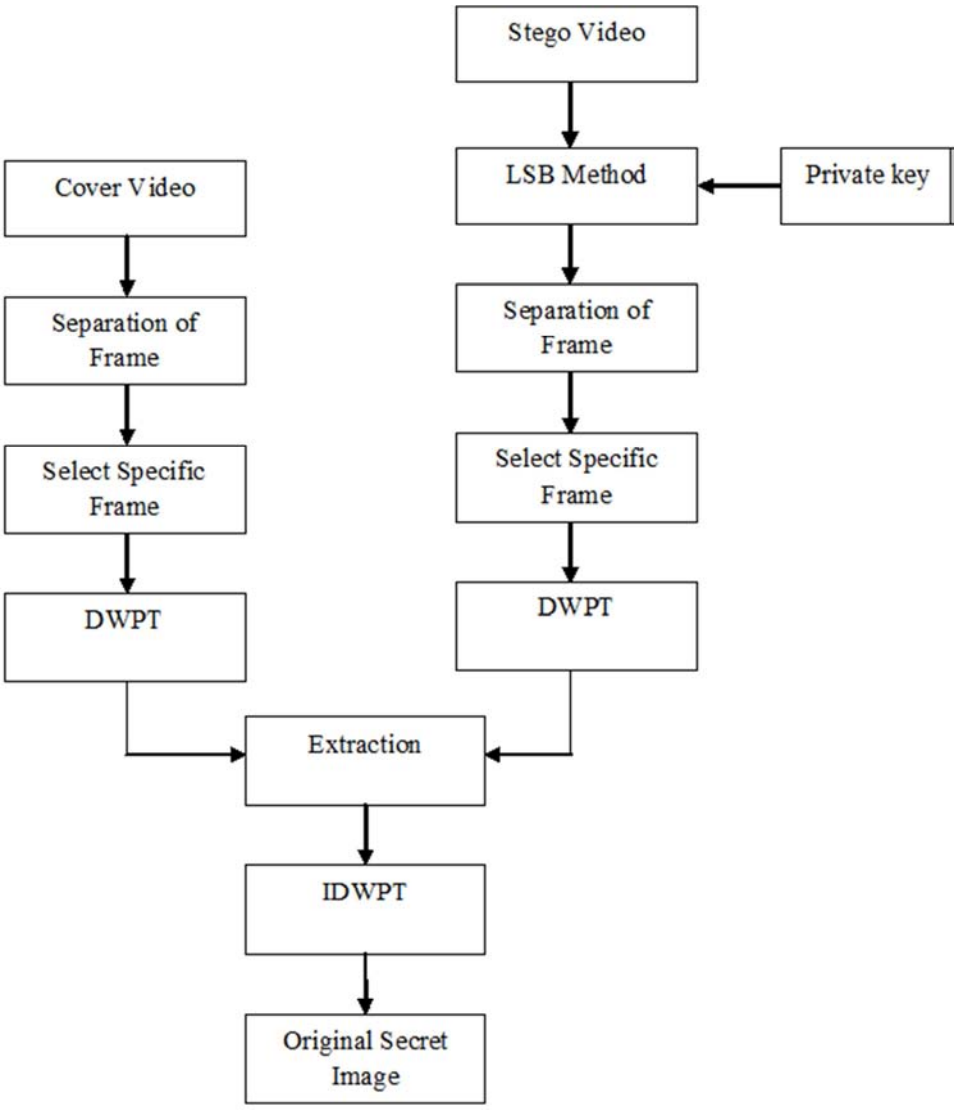

Figure 6. *Flow Chart of Decoding Process.*

Step 1: Stego video is taken and performed LSB method on it to decrypt stego video by using private key. After decryption process separates the frames of stego video and save individual frame as.jpeg image.

Step 2: Now select a specific frame in which secret image is hide and two level DWPT performed on it to decompose frame into its coefficient.

Step 3: Cover video is taken and separate video into its frames then select a specific frame. Now decompose the coefficients of this frame by applying two level DWPT.

Step 4: Extracts the coefficients of original secret image from the coefficients of stego image.

Step 5: Finally IDWPT is performed on the coefficients of original secret image to reconstruct the original secret image and at last we get original secret image.

4. Result

Application of the proposed method provides the better results in terms of security of the image. In this method, the input video is taken and then the secret image is taken. After decomposition using DWPT the frames of the video and the secret image are fused in such a manner that the presence of secret image can't be identified by the unknown parson. Moreover if any how the intruder identifies the presence of secret image it can't be extracted without the secret key and the decoding algorithm. This provides enormous security to the secret information to be transmitted over the channel. The stego image after embedding and recovered secret image is shown in the figure below. Two level DWPT is used for embedding and extracting the secret image using Haar wavelet. Results are obtained by using MATLAB R2016a. Using this method the sender can be very much satisfied and restful regarding the video as the identification and extraction of the secret information is not possible without the original video which is kept secured to the owner (sender) of the video. The performance of the proposed method in terms of PSNR and MSE is presented in the table below.

Figure 7. *Frames of Original Video.*

Figure 8. *Hiding Secret Image.*

Figure 9. *Frames of stego Video.*

Table 1. *Performance Measurement.*

Videos	PARAMETERS		
	MSE	PSNR (in dB)	NC
Real Video (Cat video)	0.7782	49.5198	0.052
Real Video (Flower)	9.3628e-04	44.8692	0.049
Video of Akiyo	9.8337e-05	40.93	0.0316
Video of Foreman	2.1811e-04	37.3744	0.0401

5. Conclusion

In the era of fast information interchange using internet, steganography has beome necessity tool for secure communication and secret exchange of secret information. In this paper a discrete wavelet packet based video steganography is proposed. The use of private key along with LSB make it more secure than other methods. In DWT there are loss of information in terms of detailed coefficients to overcome thos problem we are using DWPT. Additionaly this method provides more capacity and high security to transfer image in communication over the network channel. Experimental result shows that this method provides stego video with perceptual invisibility and certain robustness. We can conclude that proposed system is more effective as compare to other method for secure communication.

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.