Research Journal of Engineering Sciences ISSN 2278 – 9472
Vol. **6(7),** 1-7, July **(2017)** *Res. J. Engineering Sci.*

Enhanced security for video steganography using discrete wavelet packet transform

Parinita Sahu[1] and Swapnil Sinha[2]
[1]Department of ETC, GDRCET, Kohka Bhilai, India
[2]Dept. of Electronics and Telecommunication Engg., GDRCET, Kohka Bhilai, India
parinita1205@gmail.com

Available online at: www.isca.in, www.isca.me
Received 8th April 2017, revised 2nd July 2017, accepted 15th July 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 ununderstood. 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.

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 and 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 define as art of science of writing hidden message. Steganography is the one of the best data security technique in which private information is conceal into another information. In this technique the secret data is hiding inside multimedia file, here multimedia file act as a cover of secret data that's why it is called cover file. The secret file can be hide into any one of these multimedia file that is another data, image, audio and video.

Steganography is the art of insensible communication. In steganography technique hiding of secret message is done by embedding process in such a way that the presence of original secret information is not noticeable by other person and eavesdropper. While in cryptography technique encryption process is performed on secret message to change the original secret data into ciphertext. For high security both steganography and cryptography can be used together.

In this paper video steganography is used. 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 defined 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].

Related Work: Various methods on steganography have been investigated over many years, 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 introduced 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 based on the expanded markov and joint distribution on the transform domain – detecting MSU stego video[8].

Methodology

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.

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.

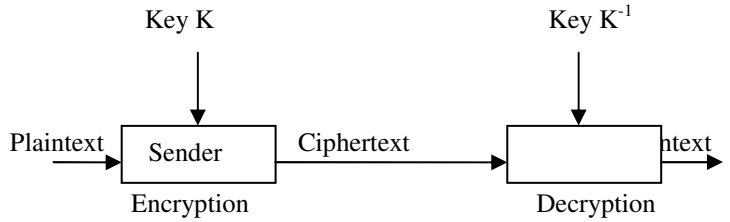

Figure-1: Basic Cryptography System.

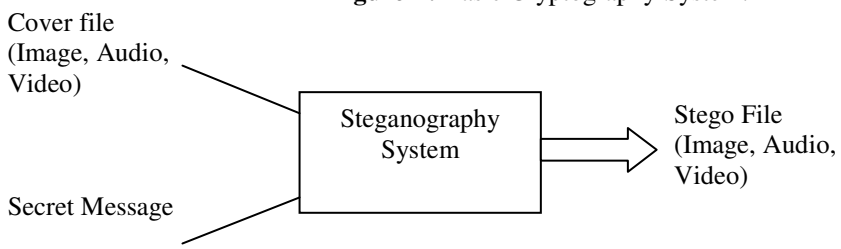

Figure-2: Basic Steganography System.

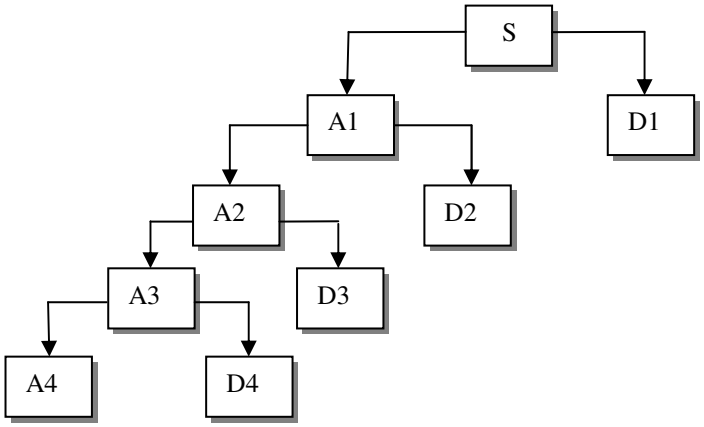

Figure-3: DWT Decomposition Tree.

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.

Encoding: 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 individual frame in a separate folder.

Step 2: One specific frame of cover video is selected and two level 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.

Decoding: 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.

Results and discussion

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 fig 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-1.

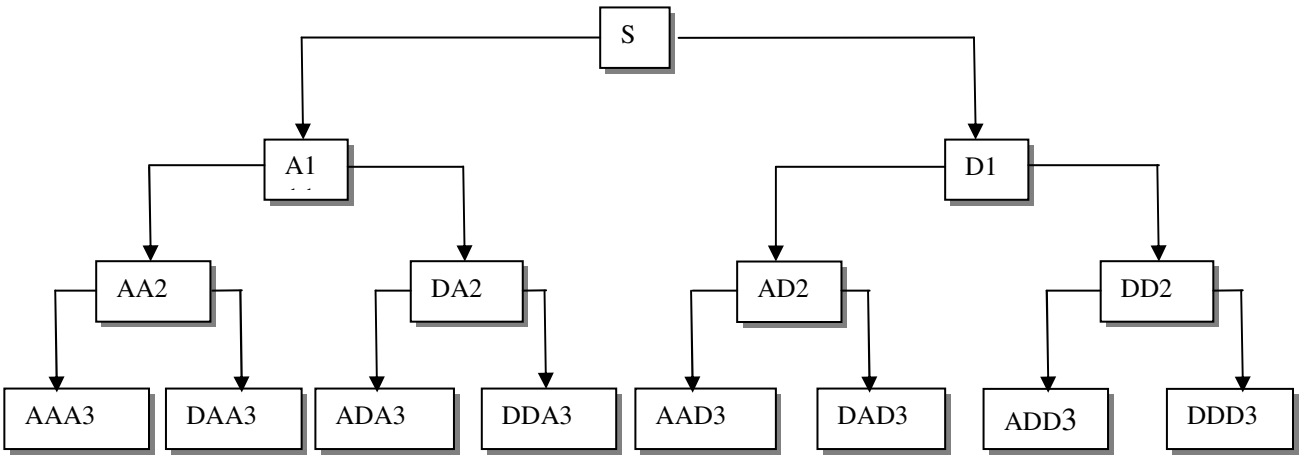

Figure-4: DWPT Decomposition Tree.

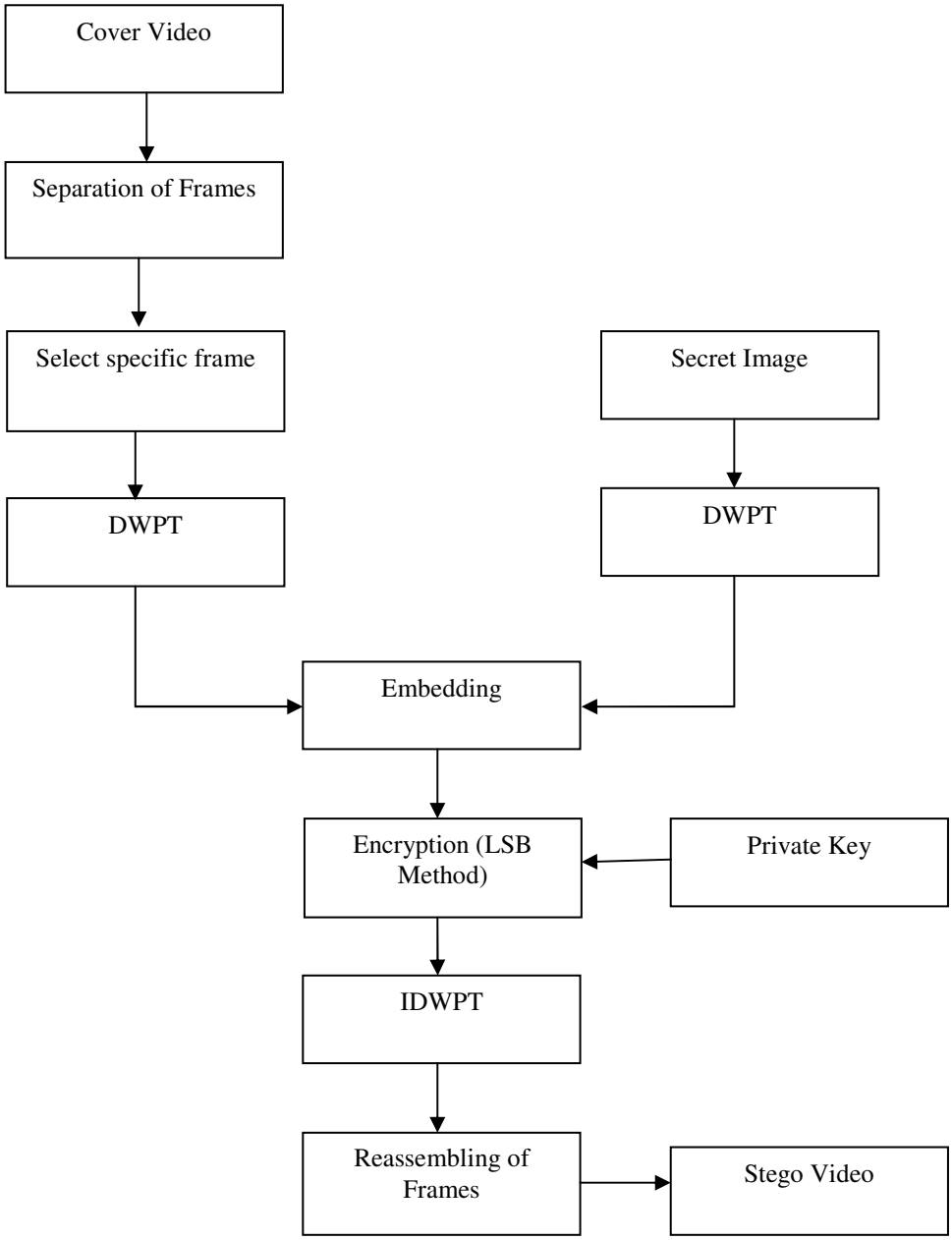

Figure-5: Flow Chart of Encoding Process.

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

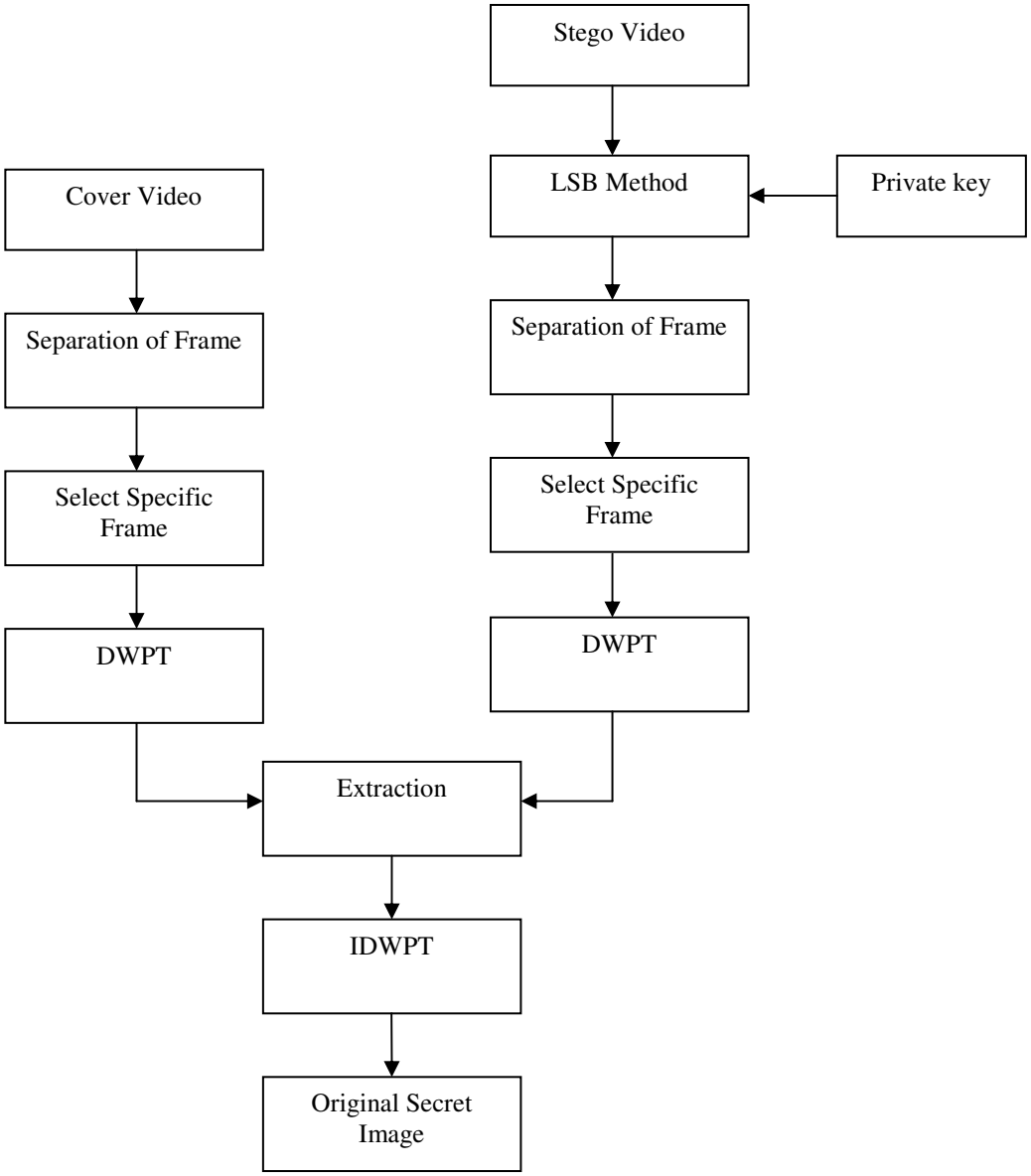

Figure-6: Flow Chart of Decoding Process.

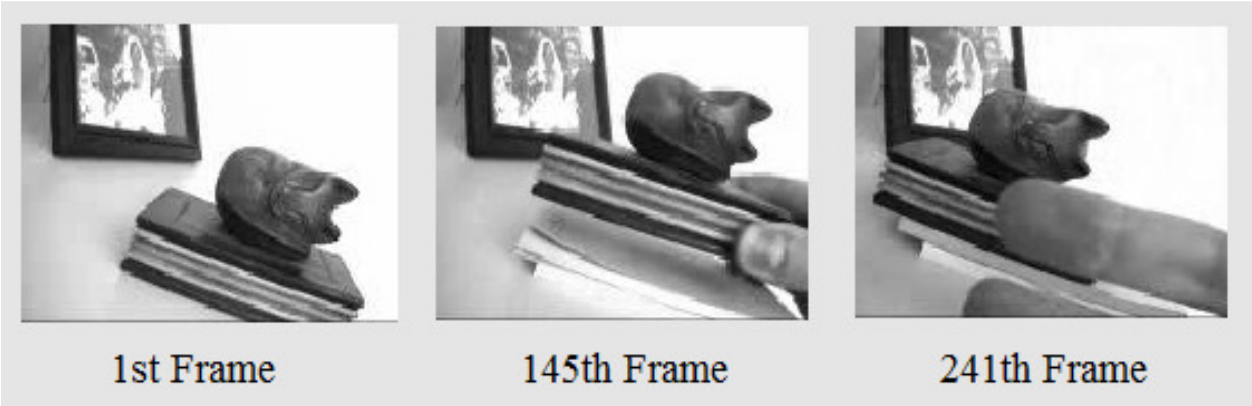

Figure-7: Frames of Cover Video.

Figure-8: Hiding Secret Image.

Figure-9: Frames of Stego Video.

Conclusion

In the era of fast information interchange using internet, steganography has become 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 method makes it more secure than other methods. In DWT there are loss of information in terms of detailed coefficients to overcome those problem we are using DWPT. Additionally 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. Thakur Abhinav, Thakur Harbindar and Sharda Shikha (2015). Secure Video Steganography Based on Discrete Wavelet Transform. *International journal of computer application*., 123(11), 25-29.
2. Sweta V., Prajit V. and Kshema V. (2015). Data Hiding Using Video Steganography- A Survey. *International Journal of Science, Engineering and Computer Technology*, 5(6), 206-213.
3. Wajgande Vipul Madhukar and Kumar Suresh (2013). Enhancing Data Security Using Video Staganography. *International journal of emerging technology and advance engineering*, 3(4), 549-552.
4. Prabhakaran G. and Bhavani R. (2012). A Modified Secure Digital Image Steganography Based on Discrete Wavelet Transform. International conference on computing, electronics and electrical technologies, 1096-1100.
5. Balaji R. and Naveen G. (2011). Secure Data Transmission Using Video Steganography. IEEE international conference on electro/information technology, 1-5.
6. Mandal Pratap Chandra (2014). A Study of Steganography Technique Using Discrete Wavelet Transform. *Journal of global research in computer science*, 5(5), 7-14.
7. Chae J.J. and Manjunath B.S. (1999). Data hiding in Video. IEEE Proceedings 1999 International Conference on Image Processing , 1, 311-315.
8. Liu Qingzhong, Andrew H. and Qiao Mengyu (2008). Video Steganography Based on the Expanded Markov and Joint Distribution on the Transform Domains. IEEE 2008 seventh international conference on machine learning and applications, 671-674.
9. Patel Khushman, Rora Kul Kauwid, Sing Kamini and Verma Shekhar (2013). Lazy Wavelet Transform Based Steganograohy in Video. IEEE 2013 international conference on communication system and network technologies, 497-500.

10. Negi Pooran singh and Labate Demetrio (2012). 3D Discrete Shearlet Transform and Video Processing. *IEEE transactions on Image processing*, 21(6), 2944-2954.

11. Khare Richa, Mishra Rachana and Arya Indrabhan (2014). Video Steganography By LSB Technique using Neural Network. IEEE 2014 sixth international conference on computational intelligence and communication networks, 898-902.

12. Kour Prabhjot (2015). Image Processing using Discrete Wavelet Transform. *International journal of electronics and communication*, 3(1).