International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6S3, September 2019

Video Steganography using IWT, DWT, LBP Methods and its Comparative Research

Dhandapani Samiappan, PR.Buvaneswari

Abstract:- ***Steganography is a method used for inserting the secret information into an another medium such as text, images, audio signals or video signals, without revealing its existence in the medium. In video steganography, a video file will be used as a cover medium and secret message embedded inside the cover medium. Video are picture perfect for embedding the secret message because of its large embedding capacity. We propose three secure steganography algorithms that embed a bit stream of the secret message into the approximation coefficients of the integer wavelet transform(IWT), DWT and using LBP method to form stego video. The geometric alteration between the cover video and the stego video is measured by using the Mean Square Error (MSE) and the PSNR. The new results show that, the proposed algorithms can hide the secret message with a great payload capacity with a high level of security and a greater invisibility.***

Keywords: Video steganography, image processing, IWT, DWT, PSNR, MSE

I. INTRODUCTION

Nowadays the data is transmitted in digital form through the networks. But at the same time the development of technology introduced threads for the data transmitted through the networks. So information security is important to overcome the above problem. Information hiding[1] is one of the method for information security. Cryptography is another method for information security .Steganography is one of the methods for implementing the information hiding by using the approach of secret information .Watermarking is another method for information hiding which is mainly used for copyright applications. In steganography secret data [6] is embedded into cover object. The cover object is used to hide the data. The word 'Stegano' is a Greek word which means that the writing is covered. Typically the cover object is a image. The stego image [8] is the one which the data is secretly embedded into cover image. The stego image is transmitted over the network. After receiving the stego image the embedded image can be take out using extraction algorithm [5]. The cover can be an image, video or audio[11].When the cover chosen as video, it is called as video steganography. For the purpose of embedding the secret message spatial domain methods and transform domain methods are used. Least significant bit (LSB) method is a popularly used spatial domain method. Discrete wavelet transform (DWT) is the famous method used in transform domain techniques [7]. So based on the domain video steganography methods are classified. Also the video steganography methods are classified based on compression techniques. Sometimes video steganography is classified into format oriented and video codec methods.H.264/Advanced Video Coding (AVC) is the recent video compression standard with high efficiency in compression and well adaptation for network transmission [12]. Due to simple structure and small size flash video (FLV) format video files are used to be very popular in the internet

Local binary pattern (LBP) is another method used for video steganography. In cover video can be divided into frames and any frame can be randomly selected as stego frame. Stego frame is further divided into windows. Either 0 or 1 is written into pixel position and can be converted into decimal number. Histogram is also used in this process. In the Extraction of secret message the stego frame is taken from the received object and processed further [20].

II. LITERATURE SURVEY

Video steganography is the best techniques for embedding the message in a secret way [2]. The secret message is hidden into the cover video and the secret message becomes safe [4]. It is very difficult for the hacker to know about the presence of secret message. Also the algorithms are developed to increase the hiding capacity.

Wavelet filters are used in DWT domain. The secret image is embedded in this domain by changing its frequency coefficients [14] and [15]. Integer wavelet transform (IWT) and DWT transform are used to embed the secret message over the cover video. Wavelet transform is having advantage over other frequency domain steganography techniques [16].

Video steganography methods are developed from image steganography. Image steganography techniques are suitable for video processing also. Since the video frames are changing continuously, the probability of discovering the secret message is less. The general attacks for videos are compresson, rotation, frame rate variation, frame exchange, insertion and deletion of frames etc. The video provides very high capacity for embedding the secret message in comparison with other types of medium.

Manuscript published on 30 September 2019.
***** Correspondence Author (s)
Dhandapani Samiappan, Professor, ECE department, Saveetha Engineering College, Chennai, Tamilnadu, India(Email: dhandapani.me@gmail.com)
PR.Buvaneswari, Assistant Professor, ECE department, Saveetha Engineering College, Chennai, Tamilnadu, India.(Email: bhuvaneswaripr@saveetha.ac.in)

The data can be embedded either in compression video format or uncompressed video format. Compressed video format includes H.264, MPEG, AVI and etc. For the purpose of embedding the message into cover video, approximation coefficients or other suitable coefficients are selected, so that it is not discovered by human visual system. Video steganography is classified based on color histograms or similar and dissimilar histograms and further divided into frame based and block based.

The MPEG video steganography uses different methods to conceal the secret message. The remaining section of the paper is structured as given below. Part III explains the proposed methods. Part IV explains the experiments, Results and its comparison analysis and Part V explains the conclusion.

III. PROPOSED METHODS

A. Video Steganography using Integer Wavelet Transform

The cover video is taken as an AVI file. The cover video is converted into images and cover image is chosen randomly using a key. The cover is splitted as sub bands represented as AC, HC, VC, DC using the haar transform shown in Figure.1.

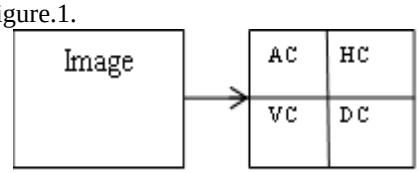

Fig. 1. Wavelets of 2D IWT

Each sub band is a copy of the original cover frame of cover video but they are having different frequency coefficients The first subband is approximation band (AC) which denotes the cover frame filtered with a low pass filter. The other three bands, HC, VC, DC are called 'detailed coefficients' which denotes the cover frame filtered with a high pass filters. These three bands contain directional characteristics. The secret message is then embedded in the frequency coefficients of AC sub band. After embedding the secret message into the cover frame then inverse IWT transformation is applied to get the stego frame is transformed back to its original form.

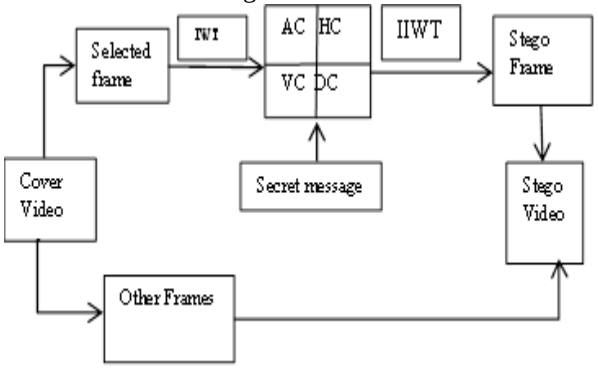

Fig. 2. Embedding process in IWT domain

Embedding Process in IWT method

1. The data to be secured is converted to binary form.
2. The cover video is divided into number of frames.
3. Select a frame randomly from the video using key.
4. IWT Transform is used to divide the cover frame into sub bands.
5. 5.The data to be secured is embedded to the approximation sub band
6. After the secret message is hidden using AC frequency components, then converted back to frame by applying IIWT (Inverse Integer wavelet transform).
7. Finally, stego frame combined to the original file and embedded video is generated.

The embedded file is transmitted using any transmission method. The secured data can be recovered from the embedded file with the help of the procedure mentioned below.

Extraction process in IWT domain

For retrieving the secured data from the embedded file using IWT domain is explained in the Figure. 3.

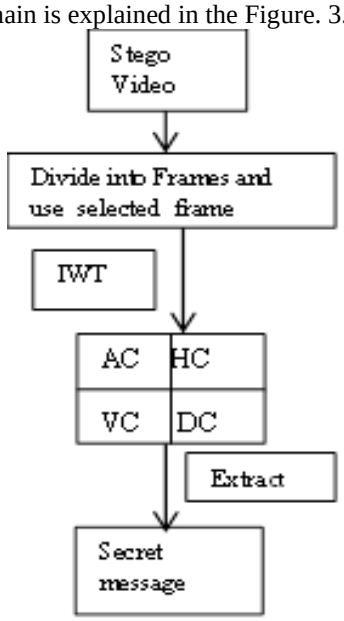

Fig. 3. Extraction process in IWT Domain

1. The Embedded video file is chosen.
2. The embedded video file is splitted as number of frames.
3. The embedded frame from the embedded video is chosen using the same key.
4. Divide the stego image into sub bands using integer wavelet transform.
5. Extract the sequence of binary bits from the AC component of the stego frame.
6. Convert the sequence of binary bits for getting the secured data

B. VIDEO STEGANOGRAPHY using Discrete Wavelet Transform

Discrete Wavelet Transform (DWT) is used to transform the frame from a spatial domain to a frequency domain where the wavelet coefficients are modified according to the secret message. DWT transform is to transform the frame into four sub band frequency coefficients.

Retrieval Number: F12870986S319/2019©BEIESP
DOI:10.35940/ijeat.F1287.0986S319
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

They are low-low frequency (LL), horizontal band High - Low Frequency(HL), Vertical Band Low - High Frequency (LH) and Diagonal band High Frequency Tape. (HH). The LL sub band covers most of the important information of the spatial domain cover frame, and the other bands contain high frequency data, such as edge information.

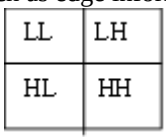

Fig. 4. Sub bands of 2D-DWT

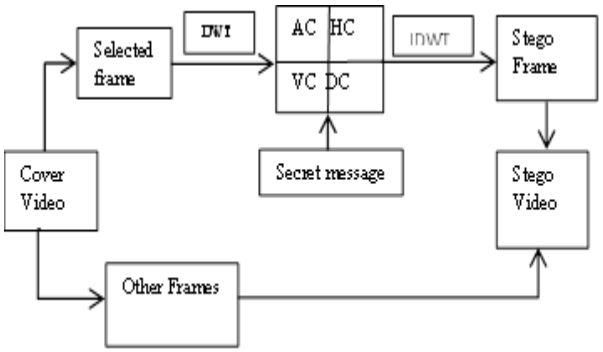

Fig.5 Embedding process using DWT domain

Embedding process in DWT domain

1. The data to be secured is converted to binary form.
2. The cover video is divided into number of frames.
3. Select a frame randomly from the video using key.
4. DWT Transform is used to divide the cover frame into sub bands.
5. The data to be secured is embedded to the approximation sub band
6. After the secret message is hidden using AC frequency components, then converted back to frame is called as stego frame by applying IDWT (Inverse Discrete wavelet transform).
7. Finally, stego frame combined to the original file and embedded video is generated.

Extracting process in DWT domain

In Extraction phase, extract the embedded secret message from stego video using DWT transform by the following steps.

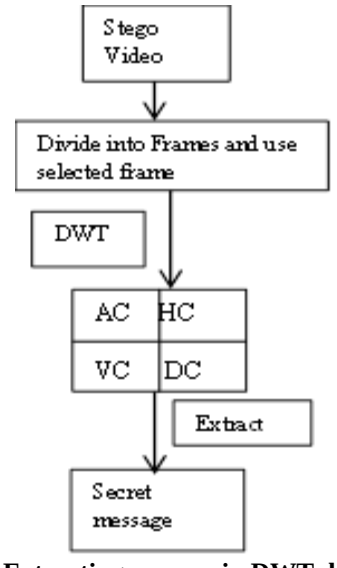

Fig.6.Extracting process in DWT domain

1. The Embedded video file is chosen.
2. The embedded video file is splitted as number of frames.
3. The embedded frame from the embedded video is chosen using the same key.
4. Divide the stego image into sub bands using discrete wavelet transform.
5. Extract the sequence of bits from the AC component of the stego frame.
6. Convert the sequence of binary bits for getting the secured data

Video Steganography using Local Binary Pattern method

To increase the performance of video Steganography, Local Binary method is used in section. In LBP method, divide the Cover Video into frames and select the frame randomly for embedding the secret information. Further divide the selected frame into group of sub images. After grouping the images select few images for embedding the secret message. Now apply Local binary pattern (LBP) method on the selected group of images for embed the secret message.

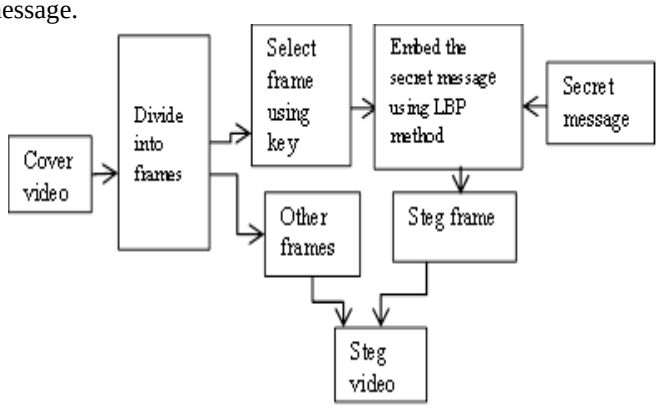

Fig .7. Embedding processin LBP method

Embedding Process

For Embedding the secret message using LBP method follow the given steps

1. The data to be secured is converted to binary form.
2. The cover video is divided into number of frames.
3. Select a frame randomly from the video using key.
4. Divide the frame into a number of sub images.
5. Embed the secret the message into sub images using LBP method.
6. Combine all the sub images to form a stego frame
7. Finally combine the stego frame and other frames to form a stego video.

After completing the process of embedding the secret message, then stego video is ready to transmit to the receiver side.

Extraction process

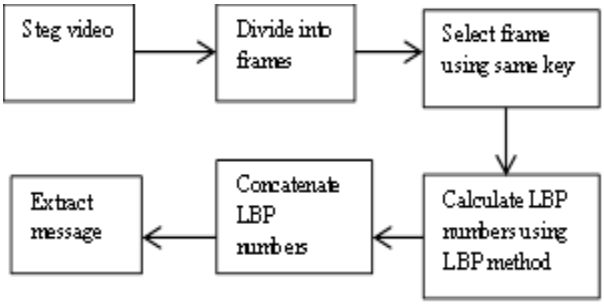

Fig.8. Extraction process in LBP method.

After receiving the stego video from the transmission side, the secured data is retrieved from the embedded file using the procedure given below.

1. The Embedded video file is chosen.
2. The embedded video file is splitted as number of frames.
3. The embedded frame from the embedded video is chosen using the same key.
4. Divide the stego frame into a group of sub images
5. Apply LBP method to sub images and calculate the LBP numbers.
6. Concatenate the LBP numbers and finally extract the secret message from LBP numbers,

IV EXPERIMENTAL RESULTS AND ANALYSIS

To analyze the performance of video steganography Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) are used. The metrics show that difference between the stego frame and cover frame.

Mean Square error determined by comparing the original video and embedded video by using equation (1).

$$\text{MSE} = \frac{1}{mn}\sum_{0}^{m-1}\sum_{0}^{n-1}||f(i,j) - g(i,j)||^2 - - - - \qquad (1)$$

PSNR is measured in decibels (dB).PSNR is calculated using the formula given the equation (2)

The PSNR (in dB) is defined as:

$$\text{PSNR} = 20\log_{10}\frac{\text{MAX}_I}{\sqrt{\text{MSE}}} - - - - - - - - - (2)$$

Where

MAX_I is the total possible pixels of the frame.

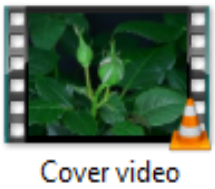

Image processing is very interesting domain. Image processing is used in computer vision. Video is

Fig.9.Cover video **Fig.10.Secretmessage**

Fig .11. Frame 1

Fig .12. Frame 2

Fig.13.Frame 3

Fig.14.Frame 4

Fig.15. Frame 5

In Video steganography using IWT method, we are taking five different frames from the cover video for hiding the secured data. The PSNR and MSE values of above frame shown in Table.1.

Table.1.PSNR and MSE parameter measurements for various frames used in IWT method

Input frames for IWT method	PSNR	MSE
Frame 1	54.04	0.2583
Frame 2	54.04	0.2583
Frame 3	54.04	0.2583
Frame 4	54.04	0.2583
Frame 5	54.04	0.2583

In Video steganography using DWT method, we are taking five different frames from the cover video for hiding the secured data. The PSNR and MSE values of above frame shown in Table.2.

Table.2. PSNR and MSE parameter measurements for various frames used in DWT method

Input frames for DWT method	PSNR	MSE
Frame 1	39.65	0.0145
Frame 2	37.54	0.1142
Frame 3	39.35	0.1451
Frame 4	39.65	0.0145
Frame 5	39.35	0.1451

In Video steganography using LBP method, we are taking five different frames from the cover video for hiding the secured data. The PSNR and MSE values of above frame shown in Table.3.

Table.3. PSNR and MSE parameter measurements for various frames used in LBP method

Input frames for LBP method	PSNR	MSE
Frame 1	29.96	66.10
Frame 2	29.81	68.34
Frame 3	29.69	70.23
Frame 4	30.01	65.29
Frame 5	29.92	66.65

V. CONCLUSION

This paper proposes secure video steganography algorithms for embedding a secret message by using the IWT transform, DWT transform and LBP method. The proposed algorithms can be applied on both gray scale and color images.

Furthermore, the proposed algorithms extract the hidden secret message effectively without using the original cover video. The experimental results prove that the proposed algorithms can embed a larger secret message with better results of PSNR and MSE. Also the proposed algorithms can hide the secret message with a large payload capacity with a high level of security and a higher invisibility.

REFERENCES

1. Nichal, Arjun, "A Review Paper on Video Steganography", International Advanced Research Journal in Science, Engineering and Technology, Vol. 3, pp. 204-207, 2016.
2. T.Venkat Narayana Rao, M.Likhitha, A.Anukritha Reddy, K.Sravani," A Novel Approach of Encrypted Video Steganography", International Journal of Computer Trends and Technology, Vol .50,No.1, pp.14-19, August 2017.
3. Shashidhara H N. and Usha B A., "Video Steganography using Zero Order Hold Method for Secured Data Transmission"Vol .176, No. 5, pp. 44-48, October 2017.
4. Abhishek Saxena, Suraj Sharma, "A review of different methodologies for video steganography", National Journal of Multidisciplinary Research and Development, Volume 3; Issue 1; Page No. 965-967, ; January 2018.
5. Parinita Sahu, Swapnil Sinha, " National Journal of Multidisciplinary Research and Development", 2017; Vol. 2, No. 1, pp. 7-12.
6. Shivali Bansal, Manpreet Kaur, Amit Doegar, Vandna Kumari," Improved Data Security and Secrecy Using Randomized Video Steganography", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 5, No. 2, February 2017.
7. S.Kamesh, K.Durga Devi, S.N.V.P.Raviteja, "DWT based data hiding using video steganography", International Journal of Engineering Sciences & Research Technology, pp. 361-367, Vol. 6, No.4, April 2017.
8. Nishi Khan, Kanchan S. Gorde," Video Steganography by Using Statistical Key Frame Extraction Method and LSB Technique",International Journal of Innovative Research in Science,Engineering and Technology, Vol. 4, No. 10, October 2015.
9. Heena Goyal,Preeti Bansal," An Analytical Study on Video Steganography Techniques", International Journal of Advanced Research in Computer Science, Volume 6, No. 5, May - June 2015.
10. Aishwarya Pandey, Prof. Jharna Chopra," Comparison of Various Steganography Techniques using LSB: A Review", International Journal of Scientific Research Engineering & Technology , Vol. 6, No. 5, May 2017.
11. A. Soria-Lorente and S. Berres," A Secure Steganographic Algorithm Based on Frequency Domain for the Transmission of Hidden Information" Vol. 2017, pp. 1-14.
12. Sachin Jangid, Somesh Sharma, "A Review of Different Methodologies for Video Steganography", International Journal of Innovative Science and Research Technology, Vol. 2, No. 2, February 2017.
13. Mandeep Singh, Garima Mahajan, "Secure Secret Information Transmission with Audio-Video Steganography Using Encryption and Data Authentication", International Journal of Science and Research, Vol. 5, No. 9, pp. 668-673, September 2016.
14. Bharti Chandel, Dr.Shaily Jain,"Video Steganography: A Survey", IOSR Journal of Computer Engineering , Vol. 18, No. 1, pp. 11-17, Jan – Feb. 2016.
15. Iti Naidu, Deepak Xaxa," Survey on Video Steganography Algorithms", International Journal of Recent Technology and Engineering , Vol. 6, No. 2, pp .19-23, May 2017.
16. Pooja Dixit, Munesh Chandra Trivedi," Video Steganography using Concept of DNA Sequence and Index Compression Technique", International Journal of Engineering and Advanced Technology , Vol.8, No.5, June 2019.
17. Dipti Mukadam, Sunita Mahale,"Secure data transfer using video steganography", International Journal for Research in Engineering Application & Management, Vol. 3, No. 11, pp.7-9, Feb 2018.
18. J.Mary Jenifer, Dr.S.Raja Ratna," Video Steganography based on Scene Change Detection", International Journal for Research Trends and Innovation , Vol. 2, No. 4, pp. 102-108, 2017.
19. Shivani Gupta, Gargi Kalia, Preeti Sondhi," Video Steganography Using Discrete Wavelet Transform and Artificial Intelligence", International Journal of Trend in Scientific Research and Development, Vol. 3, No. 4, pp. 1210-1215, May 2019.
20. Roopa Raju, Felix.M.Philip, "Video Steganography in Haar Wavelet Domain Based on Multiple Object Tracking and Error Correction Codes", International Research Journal of Engineering and Technology, Vol. 5, No. 4, pp. 3985-3990, April 2018.