

Video Steganography Method based on Haar DWT and Spread Spectrum Technique

D.Elakkiya¹, Dr.K.Mahesh²

¹Research Scholar, ²Professor

Department of Computer Science and Engineering, Alagappa University,
Karaikudi-600 003, Tamilnadu, India.

Abstract— In the development of the network field, the necessity for hiding the information is more important for protecting the information from the third party in an open network. In order to overcome this video steganography technique is used. It is the profession of hiding the information which helps to conceal the sensitive data than other medium. In steganography different cover objects are used for video, it can be separate into images and audio and accommodate massive amount of secret information. In this proposed work, introduce the new method for hiding the secret data into a video file using video steganography technique. In this technique, Haar DWT and spread spectrum to get a stego video. And obtain extraction procedure is similar to embedding procedure vice versa. So that this proposed method is convenient and extracting data easily from stego video.

Keywords— Video Steganography, Haar DWT, Spread spectrum.

I. INTRODUCTION

The Steganography is of Greek word which is hiding secret information within cover media such as image, text, audio or video so that imposters can't detect what data is hidden in it. In the cryptography, render message unintelligible but in Steganography cover the existence of the message. Video steganography means video file is use as a cover medium for hiding secret information. Among all the steganography, video steganography beaten some restrictions because it has capability to embed massive amount of secret data inside the carrier and also it is difficult to detect by third person. This steganography use H.264, Mp4, MPEG, AVI, etc., file formats. In practice, Video steganography technique can be classified into two types which are temporal and spatial domain. In temporal domain, transforming cover data by using DCT, DWT etc., and on this transformed coefficients, secret information can be embedded. In spatial domain, data bits are embedded in LSBs positions. If SNR and PSNR value is large means small difference between original image and stego image [1]. The data is hidden in sub bands which address the robustness and good visual quality. It is mapping an integer to integer data. With usage of Integer wavelet transform for floating point values of the wavelet filters can be avoided. Use of Lifting schemes, Integer wavelet transform is perform in which transforms from integer pixel values of an image into the integer wavelet coefficients[2]. One of the Wavelet transform a families known as "Haar" has been implemented work. It converts an image from spatial domain to the

frequency domain by applying horizontal and vertical operations, respectively. The Haar DWT is used in the proposed Steganography technique to convert the cover image into four sub-bands are approximation, vertical, horizontal, diagonal coefficients, which represent low-low, high-low, low-high and high-high frequencies respectively. Approximation coefficients will not be used to conceal secret information since human eyes are very sensitive to small changes low-low frequency. However, the rest of the coefficients contain high frequencies, thus secret data will be corrected and concealed within these bands by the use of both least significant bit and pseudo random number techniques. Once the embedding process is completed, the inverse Haar DWT is applied in order to form the stego-image.

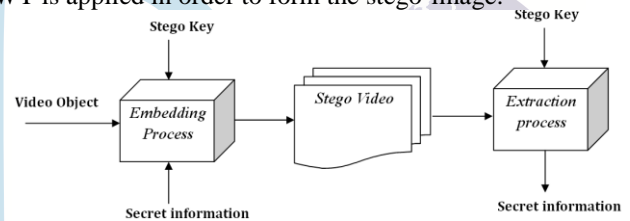
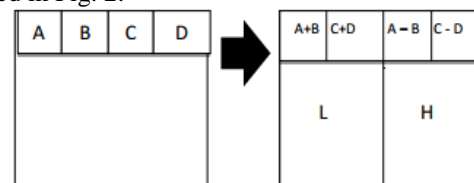


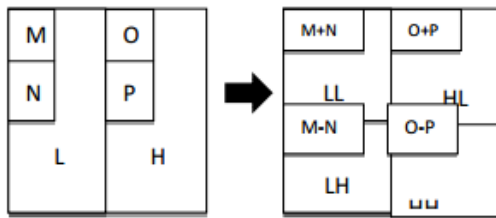
Fig.1 Basic structure of video steganography

Horizontal Operation: In this operation, an image will be divided in to two bands that are low and high frequencies. Pixels are scanned from left to right in the horizontal direction. Addition and subtraction operations are performed on the neighbouring pixels .The results of the addition are on the left represents the low frequency band. However, the subtractions which represent the high frequency is held on the right side, as illustrated in Fig. 2.



(a) Horizontal Operation

Vertical Operation: Low and high frequencies obtained from the horizontal operation are sub-divided further into low-high, low-low, high-low, and high-high frequencies. All pixels will be scanned over for the addition and subtraction operations, but in the vertical direction. The addition of the neighbouring pixels will be held in the top, while the subtraction result will be located in the bottom, as illustrated in fig.2



(b) Vertical Operation

Fig.2. Horizontal and Vertical Operation

Spread spectrum techniques are most important one in which CDMA mobile communication. In this technique, the secret data is transmits through radio waves. It address cover image as noise and adding pseudo noise to conceal the image [3]. If any part is removing from some bands, still information is present in other bands. It is unenviable to removing information without completely destroying the carrier [4].

II. RELATED WORK

Varying methods are proved that secret data is hidden without change the quality of visuals, structure of video file.

Mritha Ramalingam et al [5] have proposed Haar Integer Wavelet Transforms based steganography for transfer data with highest level of security. In embedding process, cover video is partitioned into RGB frames and apply Haar DWT on this frames to get wavelet coefficients. Then, read the secret message and convert into bits. Embed this binary formed message into LSBs of IWT coefficients of RGB frames. To extract the data from these coefficients, inverse process of embedding data procedure is used. In this work, AVI Video file is used for hide and extract the data. This algorithm has less complexity.

Avinash K. Gulve et al [6] use Integer Wavelet Transform with PVD technique to improve security of secret data which is cover by image. 2D Haar integer wavelet transform is employed to transform the image into four subbands. Then PVD technique is used to embed the secret data into wavelet coefficients of four subbands. This proposed method enhancing the security by calculating the difference between the two IWT coefficients in the pair and modify these difference values. This modified value is used to hide the secret data. This method gives PSNR values are near 39.5 which demonstrates that the stego images are good in quality and resist to RS attack.

Seyyed Amin Seyyedi et al [7] use integer Haar wavelet transform to achieve high both in data capacity and security of secret data. In this method, the cover image is split into 8×8 blocks and these blocks are transformed in to two subsets by using two levels integer Haar wavelet transform. Then, secret data is embedded into suitable subset. To improve higher secure, one level integer Haar wavelet transform is applied to secret data before embedding.

Tanmay Bhattacharya et al [8] use DWT and spread spectrum method for embedding secret image into a cover image. In this proposed algorithm, the cover image is split into 4 sub bands by using DWT. On each band, the secret image is embedded with the help of pseudo random sequence and

session key. This algorithm can be applicable to color image and also audio steganography.

Lisa M. Marvel et al [9] have introduced new method for data is hidden in the digital image by inherent noise. A binary signal is embedded within samples of a low-power white Gaussian noise sequence consisting of real numbers. To obtain the stego image, this signal is combined with the cover image. The Power of the embedded signal is less than cover image that so it is difficult to detect by an observer.

III. PROPOSED METHOD

The aim of the proposed video steganography method achieve the security and robust by using Haar DWT and Spread Spectrum. The cover video object is break in to 3 different frames(R, G, B) and divide the frames in to 8×8 blocks. These blocks are transformed using one level Haar Integer wavelet transform to get wavelet coefficients. Then Direct Sequence Spread Spectrum (DS-SS) is used in this proposed work. Generate a PN sequence and information is modulated with pseudo noise sequence and this resultant signal is inserted on RGB frame. Thereafter, inverse Haar DWT is employed to obtain stego video. Now this stego video object is send to recipients. In receiver side, to extract the secret data, use reverse process of embedding process. The block diagram of the proposed architecture is given below:

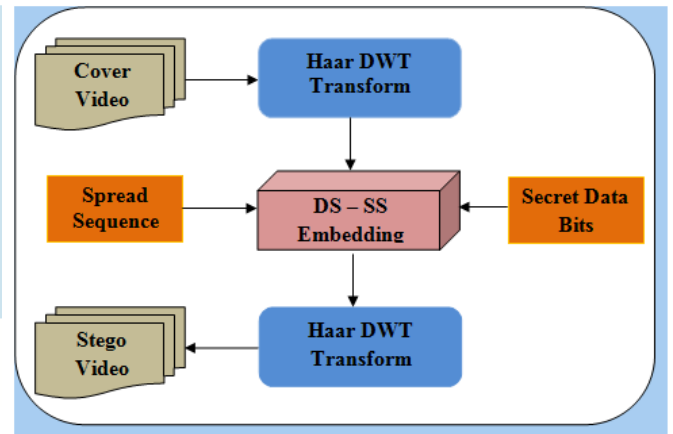


Fig.2 Block diagram of proposed data embedding process

A. Algorithm for Embedding Procedure

- Step 1:** Input: cover video and secret data.
- Step 2:** Cover video is partitioned into three frames (R, G, and B)
- Step 3:** Divide these frames into 8×8 blocks
- Step 4:** Each frame are transformed by using one level Haar DWT.
- Step 5:** Convert each character in the secret data into bits.
- Step 6:** Prepare pseudo noise sequence.
- Step 7:** Information is modulated with PN sequence.
- Step 8:** Insert the resulting signal with each transformed frame.
- Step 9:** Video cover object is transform back using inverse Haar DWT
- Step 10:** Output: Stego video

B. Algorithm for Extraction Procedure

- Step 1:** Input: stego video
- Step 2:** Stego video is partitioned into three frames (R, G, and B)
- Step 3:** Divide these frames into 8x8 blocks
- Step 4:** Each frame are transformed by using one level Haar DWT.
- Step 5:** Use spread spectrum technique on RGB frame.
- Step 6:** Extracting Hidden data bits.
- Step 7:** Convert binary data in to text.
- Step 8:** Apply inverse Haar DWT to get video object
- Step 9:** Output: Cover video and Text.

IV. RESULT AND DISCUSSIONS

A. Experimental Results







In this section, experiments are done to prove the efficiency, data payload, quality, and security of the proposed method. The proposed work is lossless and reversible as embedding data frame results in a stable distortion of the original frame or concealed data but within suitable range. This method of

video or frame are not loss this real shape or streaming after embedding secure data in video file. Experimental results are in a single frame on several sample videos as shown in table 1.

B. Performance analysis

The performance of the proposed system is analyzed based on the variation in the size of the test videos that are used to hide secret data. We embedded different secret data on different cover-video sequences and observed the performance that means there is no variation in the size of the AVI videos after embedding. (Refer Table 1). For example, the secret data, Data1.txt in binary form is hidden in the cover-video, vipfly with a size of 355 KB. Embedded Text is “Video steganography means video file is use as a cover medium for hiding secret information. Among all the steganography, video steganography beaten some restrictions because it has capability to embed massive amount of secret data inside the carrier and also it is difficult to detect by third person”. It is clearly noticed that the distortions occurred in the cover-video by applying the proposed algorithm is highly imperceptible to human eyes.

TABLE I
SIMULATED RESULTS OF THE PROPOSED METHOD IN VARIOUS SAMPLE VIDEOS

Cover Video	Sample Secret data	Stego Video
	The Steganography is of Greek word which is hiding secret information within cover media such as image, text, audio or video so that imposters can't detect what data is hidden in it. In the cryptography, render message unintelligible but in Steganography cover the existence of the message.	
	MATLAB is the high-level language and interactive environment used by millions of engineers and scientists worldwide. It lets you explore and visualize ideas and collaborate across disciplines including signal and image processing, communications, control systems, and computational finance.	
	Video is an electronic medium for the recording, copying, playback, broadcasting, and display of moving visual media. Video systems vary greatly in the resolution of the display, how they are refreshed, and the rate of refreshed, and 3D video systems exist.	

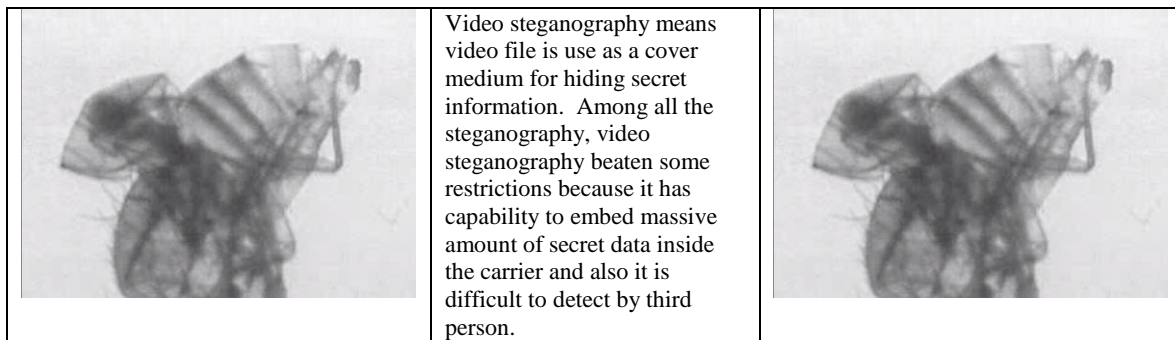


TABLE II
PERFORMANCE OF THE PROPOSED METHOD IN VARIOUS SAMPLE VIDEOS

Video Name	Cover Video			Secret Data		
	Resolution	Frame /Sec	Size(kb)	Name	File Format	Size
vipfly	320×240	15	355	Data1	*.txt	987bytes
viplane	360×168	25	299	Demo2	*.doc	1kb
vipsnowydays	320×240	8	296	Demo1	*.txt	812bytes
viptraffic	160×120	15	204	Data2	*.doc	50bytes

V. CONCLUSION

The proposed steganography method provides high capacity and imperceptible stego-image for human vision of the hidden secret information. The performance of the proposed method is studied and experimental results shows that this scheme can be applied on videos with no noticeable degradation in its quality. This method extracts the data as identically, without any loss in quality and size of the original video.

In future this work can be enhanced to generate key for automatically using user data and also supports other video formats like mp4, mkv etc. Embedding capacity of this method is much better than other exiting methods in transform domain

REFERENCES

- [1] B.Suneetha, Ch.Hima Bindu And S.Sarath Chandra, "Secured Data Transmission Based Video Steganography", International Journal of Mechanical and Production Engineering (IJMPE), Vol-2, Iss-1, 2013.
- [2] Nur Azman Abu, Prajanto Wahyu Adi and Othman Mohd, "Robust Digital Image Steganography within Coefficient Difference on Integer Haar Wavelet Transform", International Journal of Video & Image Processing and Network Security IJVIPNS-IJENS, Vol:14 No:02, 2014.
- [3] Barnali Gupta Banik and Samir K. Bandyopadhyay, "Review on Steganography in Digital Media", International Journal of Science and Research (IJSR), Volume 4 Issue 2, February 2015
- [4] Jasleen Kour and Deepankar Verma, "Steganography Techniques –A Review Paper", International Journal of Emerging Research in Management & Technology, Vol:3, Issue:5, 2014.
- [5] Mritha Ramalingam and Nor Ashidi Mat Isa, "Video Steganography based on Integer Haar Wavelet Transforms for Secured Data Transfer", Indian Journal of Science and Technology, Vol 7(7), 897–904, July 2014.
- [6] Avinash K. Gulve and Madhuri S. Joshi, "An Image Steganography Method Hiding Secret Data into Coefficients of Integer Wavelet Transform Using Pixel Value Differencing Approach", Mathematical Problems in Engineering, Vol.2015, pp.1-14, 2015.
- [7] Seyyed Amin Seyyedi and Nick Ivanov, "High Payload and Secure Steganography method Based on Block Partitioning and Integer Wavelet Transform", International Journal of Security and Its Applications Vol.8, No.4 , pp.183-194, 2014.
- [8] Tanmay Bhattacharya, Nilanjan Dey and S. R. Bhadra Chaudhuri, "A Novel Session Based Dual Steganographic Technique Using DWT and Spread Spectrum", Vol.1, Issue1, pp-157-161.
- [9] Lisa M. Marvel, Charles G. Boncelet and Charles T. Retter, "Spread Spectrum Image Steganography", IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 8, NO.8, pp: 1075-1083, 1999.