International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 8, ISSN No. 2455-2143, Pages 294-298
Published Online June - July 2016 in IJEAST (http://www.ijeast.com)

WAVELET BASED COLOR VIDEO STEGANOGRAPHY USING SEQUENCE AND RANDOM TECHNIQUE

Ajit Danti
Department of MCA
JNN College of Engg.,
Shimoga 577204, India

G R Manjula
Department of CSE
JNN College of Engg.,
Shimoga 577204, India

Pallavi B M
Department of CSE
JNN College of Engg.,
Shimoga 577204, India

***Abstract*— Wavelet Based Color Video steganography is the algorithm developed to hide a secret color video sequence within another cover color video sequence. An approach to apply a wavelet transforms in order to decompose the cover video sequence and then replace the less significant wavelet band with "secret" video frames. On the receiver side, process is reversed and the hidden color video recovered from stego color video. And it is done for both sequence and random embedding techniques, finally experimental results of both embedding techniques is discussed, results shows that the wavelet based color video steganography is better robust and complexity.**

Keywords— **cover video, stego video**, **Haar Wavelet, DWT, PSNR**

I. INTRODUCTION

Steganography is introduced by a Greek word and it implies the secured composing. Steganography is a craft of concealing information in a secured media (picture, sound, and video, content). The secured media is picked in such a way, to the point that it has power to hide the information and robustness that gives good quality of stego image. As in the up and coming years the need of information concealing, copyright insurance, and confidentiality expands, steganography assumes a vital part in this field on account of its someone of a kind components. The fundamental reason for Steganography is that, which signifies 'writing in hiding' is to hide information in a cover media with the goal that others won't have the capacity to notice it. While cryptography is about ensuring the substance of messages, steganography is about hiding their extremely presence [1].

Steganography is one of the strategy in which the information is covered up in the cover object with the utilization of secret key. The extractor should to have secret key to remove the information.

Privileged secrets can be covered up inside a wide range of cover data. The accompanying formula gives an extremely non specific depiction of the bits of the steganography procedure:

cover_media+ hidden_data + stego_key = stego_medium

In this context, the cover medium is the document in which the hidden_data will be encrypted utilizing the stego_key. The resultant file is the stego_medium. Figure 1.1 demonstrates the block diagram of steganography system.

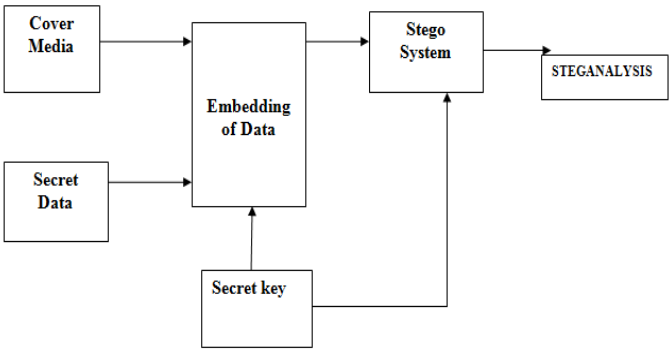


Fig.1. steganography system

Video steganography is a technique where carrier file will be video in which the secret information can be hidden. In the proposed system cover and secret file both are video file is used. When video is used as the cover file, there will be additional security [2] as structure of video file is quite complex compared to other types of media. Another important aspect in steganography is storage capacity of cover file and secret file. Larger the storage capacity of cover file, greater the amount of data that can be hidden it. Video files have more storage capacity than audio and image as data can be hidden in one or more frames of the cover video.

A modification to the traditional LSB technique by replacing LSB bits by LSB+3 bits has been proposed [3]. Utilization of integer wavelet transforms in video steganography has also been presented [4] and the possibility of extending the scheme to color images proposed. Use of discrete cosine transform (DCT) in combination with LSB has been reported [5], although in this scheme only text data

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 8, ISSN No. 2455-2143, Pages 294-298
Published Online June - July 2016 in IJEAST (http://www.ijeast.com)

have been hidden as well as retrieved from the cover video file.
The developments to hide more complex data inside a video can be achieved by the implementation of two-dimensional discrete wavelets transforms (DWT2). The more detailed discussion of the DWT2working and implementation in this work is illustrated in the following sections.
The rest of the paper is organized as follows. Proposed embedding and extraction algorithms are explained in section II. Experimental results are presented in section III. Concluding remarks are given in section IV.

II. PROPOSED ALGORITHM

A. Discrete Wavelets Transforms

Another possible area for video steganography embedding is that of the wavelet stream. The DWT [3] gives a image into a lower plan estimation image(LL) and also horizontal(HL), vertical (LH) and diagonal(HH) purpose of interest parts. The strategy can then be reiterated to enroll diverse scale wavelet de-structure, as in the 2 scale wavelet transform exhibited in Figure 2.

Wavelet transform is one of the set up strategies to finish time-frequency transformation of a signal or image. As a rule it is thought to be better than Fourier transform because of the way that wavelets can catch frequency and in addition location in-time data about the broke down waveform or image [6]. Truth be told transform domain strategies have been appeared to hold better to decryption endeavors and attacks[7], [8]. A portion of the regularly utilized discrete wavelet changes incorporate Haar, Daubechies and Symlets wavelets.

One of the most established and easiest wavelet transform is the Haar wavelet. This transform cross multiplies a function or a given waveform with the Haar wavelet with different shifts and stretches. Primary idea of Daubechies wavelets is like that of Haar wavelets however the two techniques vary in the way scaling and wavelets are characterized. Here, a scaling capacity called "father" wavelet produces multi resolution orthogonal perceptions [9]. Symlets are a part of the wavelet family and an altered version of Daubechies with upgraded symmetry [10], [11].

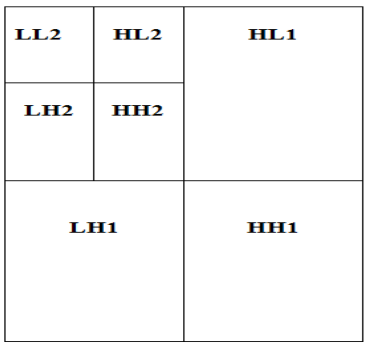


Fig 2.2 Scale 2-Dimensional Discrete Wavelet Transform

B. Wavelet Based Steganography

Wavelet transform is normally refined through two phases - quantization and encoding. Strategies for embedding information or data which should be hidden up are typically connected after the wavelet transform. The coefficients got after the application of discrete wavelet transform are adjusted by stego information - information which requires hiding up with the expect to be recreated once the information has been gotten toward the end of the hiding procedure. The hidden information is recovered by turning around the hiding procedure and applying the inverse discrete wavelet transform application on the stego image [12][13]. This procedure is illustrated in Figure 3.

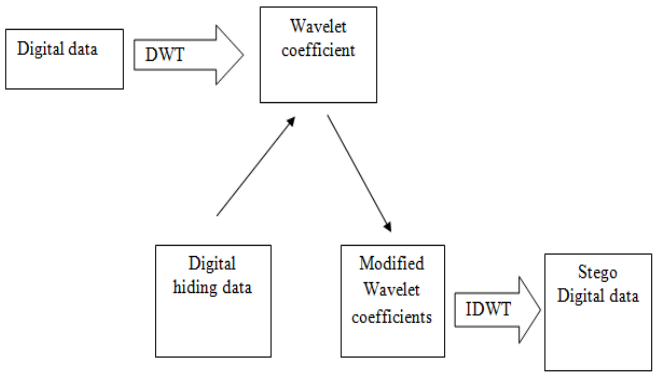


Fig 3: Embedding process using DWT and IDWT.

Color video and secret video is broken down into red, green, blue channels. Only the red channels are extracted from the cover color video and wavelet transformed into four wavelet bands. The total numbers of cover color video frames are divided into 3 equal blocks. All the frames of the color video are wavelet transformed and wavelet bands are obtained. Red, green and blue channels of the secret video are embedded by using random embedding or sequential embedding of the HH bands. At the receiver side inverse discrete wavelet transform is performed and stego red channels are reconstructed with the modified bands. Stego red channels are concatenated with untouched green and blue channels to obtain stego video frames. Finally frames are arranged sequentially to obtain stego video and is identical to the cover color video.
Encryption process consists of seven steps.

1. The cover color video is broken down in red, green and blue channels.
2. The secret color video is also broken down in red, green and blue channels.
3. The red channels are extracted from the cover color video and wavelet transformed into four wavelet bands.

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 8, ISSN No. 2455-2143, Pages 294-298
Published Online June - July 2016 in IJEAST (http://www.ijeast.com)

4. The total numbers of cover color video frames are divided into 3 equal blocks (i.e. if the total number of cover color video frames are 300, then 00 HH bands are replaced with 100 blue channels of secret color video frames.
5. In this step, the stego red channels are reconstructed with modified bands. This reconstruction process results in stego red channels of cover color video.
6. The stego red channels are concatenated with untouched green and blue channels to obtained stego video frames.
7. The frames are stitched sequentially to obtain a color video which is known as the stego video and is identical to the cover color video.

C. Embedding algorithm

Embedding data or information which needs to be hidden are usually applied after the wavelet transformation. The coefficients obtained after the application of discrete wavelet transforms are modified according to the stego data - data which requires hiding with the aim to be reconstructed once the data has been received at the end of the hiding process.

Steps in embedding:

(1) Select the cover image/video.
(2) Select the secret image/video.
(3) Separate source image into 4 bands using DWT i.e (LL, HL, LH, HH)
(4) Select the band to embed the secret image/video.
(5) Insert the secret image/video in the source image/video as shown in Figure 4

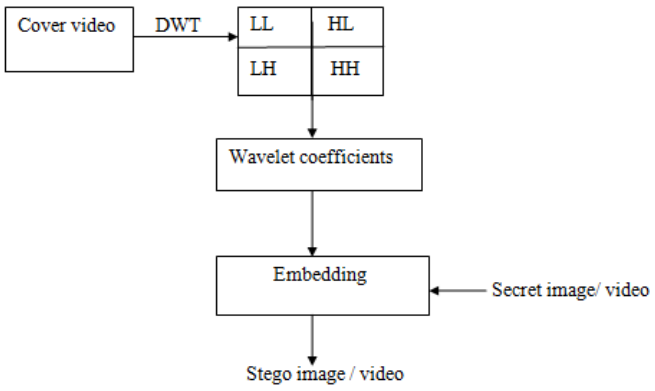


Fig.4: Embedding Process

D. Extraction algorithm

The hidden data is extracted by reversing the hiding process and applying the inverse discrete wavelet transform (IDWT) application on the stego image/video.

Steps in extraction:

(1) Embedded media is subjected to IDWT.
(2) Stego channels are reconstructed with modified bands.
(3) Cover media and secret media is separated in the extraction process.
(4) The frames are arranged sequentially to obtain the stego media and it is identical to the cover media. It is illustrated in Figure 5.

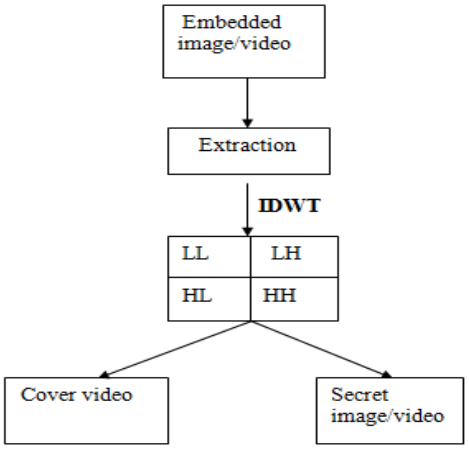


Fig.5. Extraction algorithm Block Diagram

III. Experiment and Result

The test set for this evaluation experiment video randomly selected from the internet. Matlab 14.0 software platform is use to perform the experiment. The PC for experiment is equipped with an Intel P4 2.4GHz Personal laptop and 2GB memory.

In evaluation of a steganography technique, it is always expected that the perceptual quality of the resulting stego file should be good. Greater the PSNR value better the quality of the stego video which makes the embedded data imperceptible.
The perceptual imperceptibility of the stego data can be obtained by comparing the cover video to its embedded counterpart so that their visual differences can be determined. Additionally, as an objective measure, the MSE,PSNR between the stego frame and its corresponding cover frame are studied. To measure perceptual quality of stego video, two metrics are commonly used.

$$MSE(m) = \frac{1}{N}\sum_{i,j}\left(Y_{out}(i,j,m) - Y_{in}(i,j,m)\right)^2$$

$$PSNR(m) = 10\log_{10}\left(\frac{(2^{B-1})^2}{MSE(m)}\right)$$

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 8, ISSN No. 2455-2143, Pages 294-298
Published Online June - July 2016 in IJEAST (http://www.ijeast.com)

The proposed method is tested using five secret videos for a cover video (Rhinos.avi). The cover video chosen is in AVI (Audio Visual Interleaved) format. The size of the cover video is 240×320 and this video has 114 frames which are nothing but still images. The experimental results are shown in Table 4.1.

Table 1: Comparison of the Sequence embedding and Random Embedding Techniques for cover video rhinos.avi

Secret videos (Test videos)	**Sequence Embedding**		**Random Embedding**	
	PSNR	**MSE**	**PSNR**	**MSE**
dfs.avi	48.9437	0.8358	48.0516	1.02
Swirlique.avi	40.0161	6.5294	39.4704	7.40
Pkc.avi	35.3230	19.2387	34.5652	22.9
Cookie.avi	37.1205	12.7184	36.7070	13.9
Pkcmpeg.mpg	35.3949	18.9231	34.5230	23.1

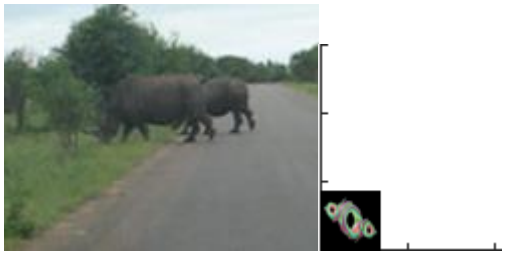
The proposed method is tested using five secret videos for a cover video (Rhinos.avi). The cover video chosen is in AVI (Audio Visual Interleaved) format. The size of the cover video is 240×320 and this video has 114 frames which are nothing but still images. The experimental results are shown in Table 4.1.

The above table contains the PSNR and MSE values for different Secret videos, throughout the project the cover video is same and the cover video size is 3MB. Different size of secret video are taken for testing, we can observe from the above table that the PSNR and MSE values will change from one secret video to the other it will mainly depend on the size, quality and type of the secret video.

(a) (b)

(c) (d)

Fig. 6. (a) Original video (b) dfs.avi secret video (c) stego video(d) extracted video for sequence embedding.



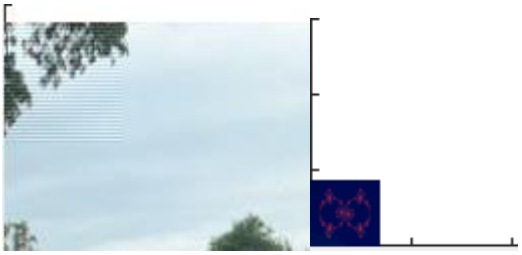
(a) (b)

(c) (d)

Fig. 7. (a) Original video (b) cookie secret video (c) stego video (d) extracted video for random embedding

(a) (b)

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 8, ISSN No. 2455-2143, Pages 294-298
Published Online June - July 2016 in IJEAST (http://www.ijeast.com)



(c) (d)

Fig. 8. (a) Original video (b) Swirlique secret video (c) stego video(d) extracted vide

IV. CONCLUSION

In Video steganography security and robustness is more important.LSB, LSB+3, integer wavelet transform, discrete cosine transform (DCT) in combination with LSB techniques are used in video steganography by using these technique security can be achieved but it is not so robust for video steganography.

Implementation of wavelet based video steganography has been done in two ways Sequence embedding and random embedding. Sequence embedding is tested which shows good results in PSNR,MSE and shows less distortion compared to random embedding technique as shown in table 4.1.random embedding technique shows more distortion compared to sequence embedding, but less susceptible to attackers. The proposed technique shows promising results on quality and accuracy. For example, concealing dfs.avi video inside rhinos.avi video gives PSNR value of 48.9437 db and MSE value of 0.8358 using sequence embedding technique which is better compared to random embedding technique which gives PSNR value of 48.0516 db and MSE value of 1.02.

V. REFERENCE

[1] [1] I.J Cox, Digital Watermarking and Steganography, 2nd ed. Amsterdam, Netherlands: Morgan Kaufmann Publishers, 2008.

[2] [2] K. S. Petitcolas and A. P. Fabien, Information Hiding Techniques for Steganography and Digital Watermarking, Boston: Artech House, 2000.

[3] P. Bhautmage, A .Jeykumar, and A. Dahatonde, "Advanced Video Steganography Algorithm," International Journal of Engineering Research and Applications(IJERA), vol. 3, no. 1, pp. 1641-1644, February 2013.

[4] K. L. Narayanan, G. Prabakaran, and R Bhavani, "A high capacity video steganography based on interger wavelet transform," Journal of Computer Appilications, vol. 5, no. EICA2012-4, February 2012.

[5] P. V. Bodhak and B. L Gunjal, "Improved protection in video steganography using DCT and LSB," International Journal of Engineering and Innovative Technology (IJEIT), vol. 1, no. 4, April 2012.

[6] N. Moldovyan and A. Moldovyan, Innovative Cryptography, Boston: Charles River Media, 2007.

[7] [12] S. Thepade and S. Chavan, "Appraise of multifarious image steganography techniques," International Journal of Engineering Research and Applications, vol. 3, no. 2, pp.1067-1174.

[8] [13]H.B.Kekre, A.B.Patankar and Koshti ,"Performance comparison of simple orthogonal transforms and wavelet transforms for image steganography," International Journal of Computer Applications, vol. 44,no.6,April2012

[9] [14] H. Jahankhani, Handbook of Electronic Security and Digital Forensics, Singapore: World Scientific, 2010.

[10] [15] B. J. Blake, Secret Language, Oxford, UK: Oxford University Press,2010.

[11] [16] F. Keinert, Wavelets and multiwavelets, London, UK: Chapman &Hall/CRC,2004.

[12] M. Holschneider, Wavelets: An Analysis Tool, Oxford, UK: Clarendon Press,1995.

[13] [18] M. D. Valle, R. M. Guerrero, and J. M. G. Salgado, Wavelets Electronic Resource: Classification, Theory and Applications, Hauppauge, N.Y: Nova Science Publishers, 2012.