International Journal of Research
Available at https://edupediapublications.org/journals

p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 07
June 2017

Video Steganography Using Lazy Wavelet Transform

Shailesh Yadav[1], Prof. Abhishek Jain[2], Prof. Aman Sharma[3]
[1]M. Tech. Scholar, [2,3] Assistant Professor,
Dept. of Electronics and Communication, Samrat Ashok Technological Institute, Vidisha (M.P.)-464001

ABSTARCT

Steganography is the expertise skill of secret communication, concealing the very existence of communication. It resolute the issue of network security and favor secure communication through public and private channels. The hidden message can be in any format like text, audio, image or video. Nowadays, video files are drawing more and more attention. They are transmitted frequently on internet websites such as Instagram, YouTube etc dignifying a factual significance on video steganography. Video file usually consist of some identical frames, which are selected to hide the data. When video steganography is used, the anticipation to discover the secret information by an attacker is very less as compared to the other methods to hide data in a sequential manner. In this paper a modified technique has been used to embed the data. It involves the application of transformation to hide the encrypted data in cover file comprising of group of frames in sequential manner instead of using a single frame or image unlike existing video steganography methods [1]. The performance metrics such as Peak Signal to Noise Ratio (PSNR), RGB Intensity, Mean Square Error (MSE) and Data Recovery Ratio (DRR) have also been considered for experimental verification of the study. Simulation results are performed on MATLAB R2011b.

Keywords: LWT, Lazy Wavelet Transform, Steganography, Object Processing Method, Data Recovery Ratio.

INTRODUCTION

Today, digital media and internet are getting highly popular and the revolution in digital information has created new challenges for sending messages in a safe and secure way. So, demand of secure transmission of data has also increased. Data security basically intents at preserving the confidentiality and integrity of data and protection of data from unauthorized users or hackers. For this, various techniques are proposed and employed into practice. But whatever method we choose, the most essential is its degree of security. Various approaches have been developed for approaching the issue of information security such as digital watermarking, cryptography and steganography [2].

STEGANOGRAPHY

Steganography is the artistry of invisible communication. It is the process of secretly or mystically embedding information inside a data source without altering its perceptual quality. The word “Steganography” comes from the greek word steganos meaning “covered” and graphic denotes “writing”, i.e. covered writing. The most common use of steganography is to hide a file inside another. Although, in data hiding; the factual information is not adapted in its original format and is transformed into an alternative multimedia files like images, audio or video. Its purpose is to hide the existence of communication by embedding messages in such a way that a third person couldn’t sense the hidden message. Steganography is having variety of applications which includes Distributed Steganography, Online challenge, alleged use by intelligence services and in modern printers.

TYPES OF STEGANOGRAPHY

There are multiple ways [3] to hide the messages using steganography like in images, word file, audio and video. All are briefly described below

Steganography in Image: Digital images are the most generally used cover objects for steganography. The availability of various file formats for different applications differs according to the algorithm used for these formats.

Steganography in Audio: Embedding secret messages into an audio file is the most assertive technique in steganography. This is why, the human auditory system (HAS) has such a dynamic range that it can listen over multiple frequencies at a time.

Steganography in Document: Steganography in documents targets on amending some of its characteristics. They can either be distinctive of text or even doc formatting.

Steganography in Video: In this method, to hide the secret messages, a video file would be enclosed with accompanying data. In this procedure, an intermediate signal would be generated which is a function of hidden message data and data of content signal. There are different approaches for video Steganography like Least Significant Bit Insertion and Real time video Steganography.

- Least Significant Bit Insertion:

It is the most popular and lucid approach for all types of steganography. In this method the digital video file is estimated as separate frames and alters the exposed image of each video frame. LSB of 1 byte is used to store the encrypted data in the image.

- Real time video steganography:

It hides the secret information in the frames of video and considers each one of the frame irrespectively. The image is then dissected into the blocks. If pixel colors are almost similar then change the color characteristics of these pixels of the blocks to some expanse. It would become easier to identify the missing parts of secret information by labeling each frame with a sequence number. Now the displayed image should be certified first and compatible program is used to extract the encrypted information.

In this paper, video steganography is done using a modified version of wavelet transform. This transform is termed as lazy wavelet transform. This method provides a number of benefits above other existing methods of steganography [4]. In general, the image file has a confined expanse compared to a video file as it is a collection of numerous images known as frames of video. When an image file is used as a cover medium it is easy for the attacker to recover the message. But if we use a video for cover medium then more than one frame or image can be used simultaneously to hide data and this makes it more difficult for attacker to recover message data, because as sequence of the stego frame(s) within the video is remote for the attacker.

Wavelet Transform

The continuous-time wavelet transform [5, 6] has most of its utilizations in data analysis, out turning an affine invariant time-frequency representation. The most famous version is the discrete wavelet transform (DWT). It has admirable signal compaction properties for real-world signals while being computationally very efficient. Therefore, it has been applied in almost all technical fields including image compression, denoising, numerical integration and pattern recognition.

$$[W_{\varphi} f](a,b) = \frac{1}{\sqrt{|a|}} \int_{-\infty}^{\infty} \overline{\varphi[(x-b)/a]}\, f(x)dx$$

Here, $[W_{\varphi} f](a, b)$ is the Wavelet Coefficient, where, 'a' is 2^{-j} and 'b' is $k2^{-j}$.

LAZY WAVELET TRANSFORM

A video be composed of many sequential frames[7]. Transformation technique is applied to these sequential frames. Wavelet transformation is usually performed to convert the spatial domain into frequency domain producing real values by most of the wavelet techniques, resulting in data loss when hid and retrieved. To overcome this lazy wavelet transform is used, by applying Integer Wavelet Transform which in turn produces integer values. Thus four sub bands are generated applying Integer Wavelet Transform.

Lazy wavelet transform divides the signal $s_j[n]$ in two new signals: the odd samples signal designated as $s_j^o[n]$ and the even samples signal designated by $s_j^e[n]$. It involves the following steps:

- Prediction step is aimed to compute a prediction for the odd samples, constructed on the basis of even samples (or vice versa). This prediction gets eliminated from the odd samples by generating an error signal$e_{j+1}[n]$.
- Update step recalibrates the low frequency branch with some energy extracted during sub sampling. Thus, in the case of classical Lifting, it is used to prepare the signal for the upcoming prediction step. It utilizes the predicted odd samples $e_{j+1}[n]$ to generate the even ones $s_j^e[n]$ (or vice versa) and this update gets eliminated from the even samples producing the signal denoted by $s_{j+1}[n]$.

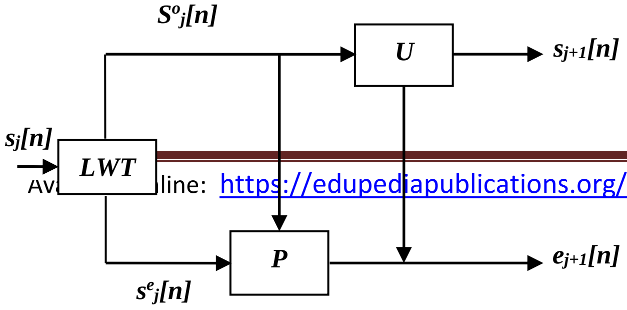


Figure 1: Working of LWT

PERFORMANCE PARAMETERS

MSE (Mean Square Error)

The Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) are the two error metrics used to correlate or consider image compression quality. The MSE corresponds to the cumulative squared error between the compressed and the original image, whereas PSNR represents a measure of the peak error. The lower the value of MSE, lower the error.

$$MSE = \frac{\sum_{MN}[I_1(M,N) - I_2(M,N)]^2}{M * N}$$

Where, I_1 and I_2 represents the pixels of the image, also M and N are the number of rows and columns in the input frame, respectively.

RGB Intensity

The RGB color model is a complementary color model in which red, green and blue light are added conjointly in numerous ways to develop an extensive array of colors. The RGB model gets its name from the initials of the three additive primary colors, red, green and blue.

The main aspiration of the RGB color model is for the sensing, illustration and exposure of images in electronic systems, such as computers, televisions and many more. Although it has also been used in conventional photography. Since the electronic age, the RGB color model already had a rigid and firm theory behind it, on the basis of human perception of colors.

$$\boldsymbol{Color\ Intensity\ (I) = \frac{1}{3} * (R + G + B)}$$

Here R, G, B denoted the value of Red, Green, Blue components of an image or in this instance for sequential frames of video.

PSNR (Peak Signal to Noise Ratio)

For calculating PSNR, the block first determines the mean-squared error using the following equation

$$\mathrm{PSNR} = 10\log_{10}(I^2/MSE)$$

In this equation, I denote the RGB component intensity value for input data taken from sequential frames of video file. Likewise to any single frame or image, the values in this instance will also range from 1 to 255, if the sequential frame is of 8-bit data type.

PROPOSED TECHNIQUE

Hiding Procedure

A video is usually comprised of multiple frames. In this paper, some sequential frames of video are used, and each frame is used to store encrypted message in it. A steganography technique is usually used to store messages, and here the Lazy Wavelet Transform on sequential frame is applied to get four sub-bands. The data is then hidden in these sub bands.

Applying Lazy Wavelet Transform on the Video

Wavelet transformation produces real values by most of the wavelet based techniques, resulting in data loss when hide and retrieved. For overcoming this shortcoming, lazy wavelet scheme is used. LWT produces integer values applying Integer Wavelet Transform. Thus we get four sub bands after applying Integer Wavelet Transform.

Hiding bits in the Sub-bands

In the proposed work, RGB Intensity for each sub bands is calculated and encoding of data is performed in sequential order of each sub bands of frames. The data stored in the frames is sequential, maximum payload in all the frames will be fixed by the frame size. But a fewer number of bits might be hidden in the last frame in which the message is hidden. In other words we can say that the capacity of carrier data to handle message data depends on quality i.e. resolution of carrier data. In the proposed work, the number of sequential frames and the size of particular frame should be kept in consideration before deciding the size of data to be encrypted. At the receiver end, hidden data is extracted from the original message using the information like position, sequence and resolution of transmitted data provided during transmission.

Algorithm for embedding the message in video:

Step-1: Import video file and select no. of sequential frames to be used for performing Steganography.

Step-2: Perform Histogram modification on selected frames.

Step-3: Apply lazy wavelet transform.

Step-4: Generate key for embedding message.

Step-5: Select message to be embedded and this message can be an alphanumeric data. The minimum and maximum length of data that can be selected depends on the number of sequential frames taken from video.

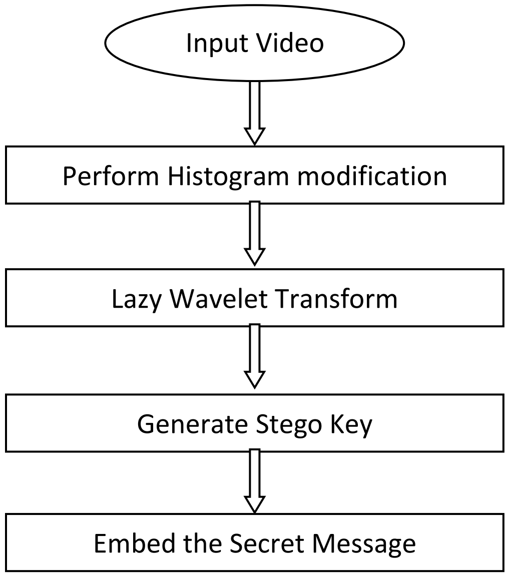


Figure 2: Algorithm for embedding message in video file

Algorithm for separating carrier and message at receiver end

Step-1: Identify the position and sequence frames containing message within the received video.
Step-2: Apply OPA to minimize the error.

Step-3: Perform Inverse Lazy Wavelet Transform.

Step-4: To extract the identified frames & perform LWT.

Step-5: You will get a text file containing the recovered data.

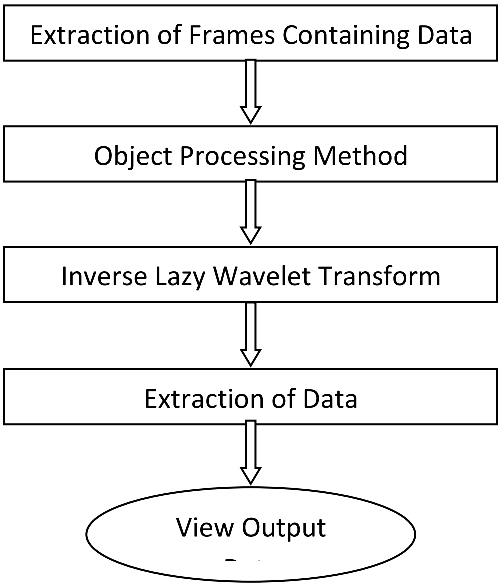

Extraction of Frames Containing Data
Object Processing Method
Inverse Lazy Wavelet Transform
Extraction of Data
View Output

Figure 3: Algorithm for message retrieval at receiver end

Validation Process

The recovered message is compared to the original message and some parameters are calculated, i.e. PSNR, MSE, RGB component Intensity and Data Recovery Ration (DRR).

RESULT

The simulations were performed on different video files, with varying number of sequential frames, while the message length is also varied.

Result for Video-1: Vipmosaicking.avi

The figure 4 shows the original, embedded and recovered frames of video**.** After embedding data in 10-sequential frames of video high PSNR=69.3752, RGB intensity=77.9576, DRR=100% is obtained.

Original Frame

After Embeding

Recovered Frame

Figure 4: Original, Embedded and Recovered Frames of Video Vipmosaicking.avi.

No. of Frames	MSE	PSNR	RGB Intensity	DRR %
10	0.007509	69.3752	77.9576	100
20	1.3356	46.8741	39	100
30	12.0008	37.3387	27	100
40	26.9997	33.8172	18	100
50	33.3327	32.9021	15	100
60	40.3323	32.0743	12	100
70	40.3323	32.0743	12	100

Table-1: Showing the values of MSE, PSNR & RGB intensity and Data Recovery Ratio varies according to the number of sequential frames of used at the time of message embedding.

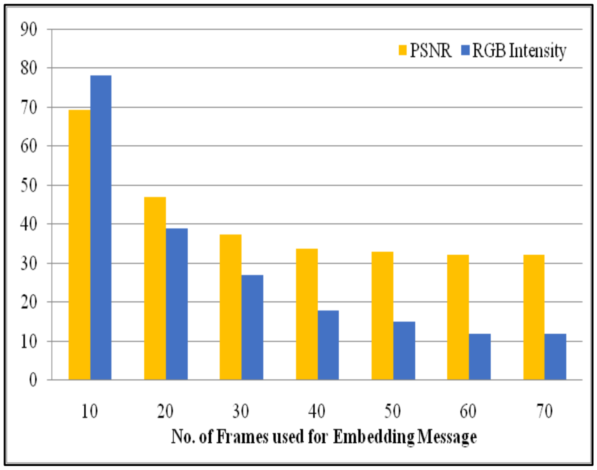


Figure 5: illustrating comparison between the values of PSNR, RGB intensity and sequential frames of video: Vipmosaicking.avi.

Result for Video-2: Viptraffic.avi

The figure 6 shows the original, embedded and recovered frames of video. After embedding data in 10-sequential frames of video high PSNR=48.5959, RGB intensity=77.4298, DRR=100% is obtained.

Original Frame

After Embedding

Recovered Frame

Figure 6: Original, Embedded and Recovered Frames of Video Viptraffic.avi

No. of Frames	MSE	PSNR	RGB Intensity	DRR %
10	0.89844	48.5959	77.4298	100
20	1.9833	45.157	38.8622	100
30	12.3707	37.2069	26.9419	100
40	27.2575	33.7759	17.9268	100
50	33.4341	32.8889	14.973	100
60	40.3543	32.0719	11.9855	100
70	40.468	32.0597	11.9591	100
80	48.0763	31.3115	8.9776	100
90	48.0297	31.3157	8.9909	100
100	48.0724	31.3118	8.9777	100
110	56.3432	30.6224	5.9954	100
120	56.3364	30.6229	5.9968	100

Table-2 shows the values of MSE, PSNR & RGB intensity and Data Recovery Ratio varies according to the number of sequential frames of used at the time of message embedding.

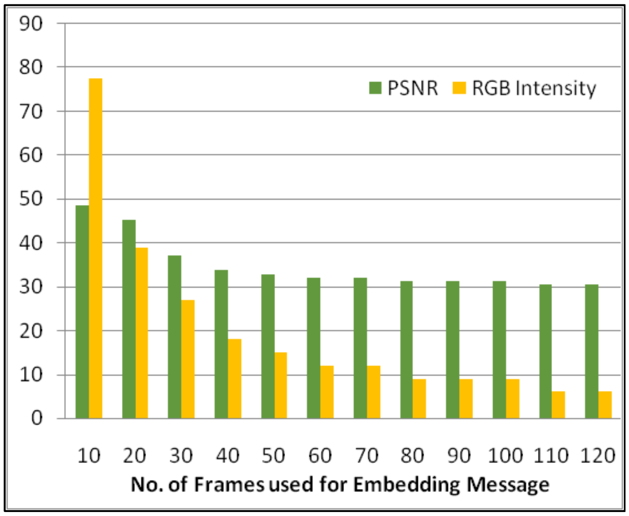
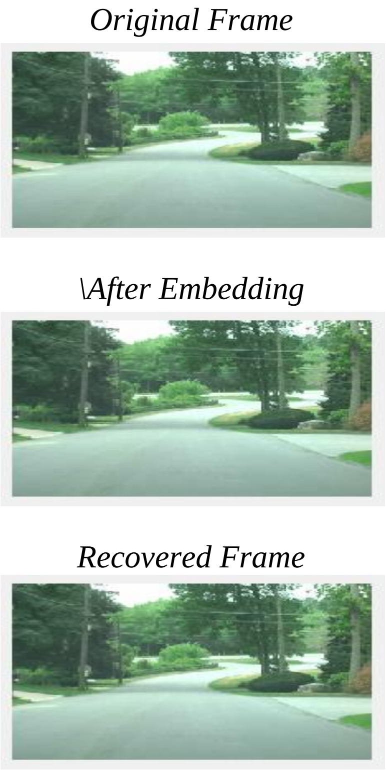


Figure 7: illustrating comparison between the values of PSNR, RGB intensity and sequential frames of video: Vipmosaicking.avi.

Result for Video-3: Vipunmarkedroad.avi

The figure 8 shows the original, embedded and recovered frames of video. After embedding data in 10-sequential frames of video high PSNR=56.8007, RGB intensity=77.9937, DRR=100% is obtained.


Original Frame

\After Embedding

Recovered Frame

Figure 8: Original, Embedded and Recovered Frames of Video Vipunmarkedroad.avi

No. of Frames	MSE	PSNR	RGB Intensity	DRR %
10	0.13583	56.8007	77.9937	100
20	1.4433	46.5373	39	100
30	12.0581	37.318	27	100
40	27.0193	33.8141	18	100
50	33.3397	32.9012	15	100
60	40.3323	32.0743	12	100
70	40.3323	32.0743	12	100
80	47.9986	31.3185	9	100

Table-3 shows the values of MSE, PSNR & RGB intensity and Data Recovery Ratio varies according to the number of sequential frames of used at the time of message embedding.

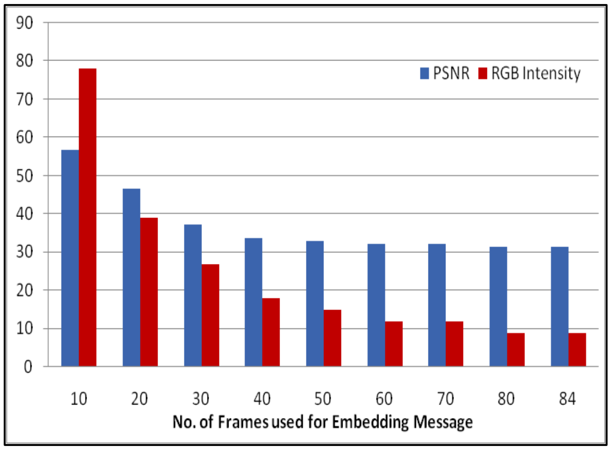


Figure 9: illustrating comparison between the values of PSNR, RGB intensity and sequential frames of video: Vipunmarkedroad.avi.

CONCLUSION

This paper provides a good method of steganography in video by using Lazy Wavelet Scheme. In the proposed work, data is hidden in video sequence instead of few frames. Experiments were conducted to evince that video-frame stenography provides a good intervene between encryption, steganography robustness, flexibility and real-time processing.

The proposed algorithm is tested on both RGB and gray scale videos of different lengths with different types of alphanumeric messages to hide. On the basis of different performance parameters like MSE, PSNR, RGB Intensity, DRR, simulation is carried out on three different RGB videos. Simulation results concluded that irrespective of the size of message, better PSNR and MSE values are obtained in video steganography with perfect data recovery ratio.

It has been observed that optimum MSE, PSNR and Data Recovery Ratio is attained, when lower number of possible frames is used for hiding the data. Results also show that lesser the RGB component, lower is the PSNR of the stegnographed video.

Simulation results also show that the length of message to be embedded and length of the video is directly correlated. For videos of 0.3-.10 seconds, 256 KB of data is embedded and recovered successfully. Thus, LWT provides optimum results for hiding the data providing more security and robustness to the system.

REFERENCES

[1] Mennatallah M. Sadek & Amal S. Khalifa & Mostafa G. M. Mostafa, “*Video steganography: a comprehensive review*”, 2014, Multimed Tools Appl DOI 10.1007/s11042-014-1952-z.

[2] Nikita Lemos, Kavita Sonawane, & Bidisha Roy, “*Secure data transmission using video*”, Eighth International Conference on Contemporary Computing (IC3), 2015

[3] Jasleen Kaur, & Deepankar Verma, “*Steganography Techniques –A Review Paper*”, IJERMT, ISSN: 2278-9359 (Volume-3, Issue-5), May 2014.

[4] Abhinav Thakur, Harbinder Singh, & Shikha Sharda, *Secure Video Steganography based on Discrete Wavelet Transform and Arnold Transform*, International Journal of

Computer Applications (0975 – 8887) Volume 123 – No.11, August 2015

[5] P. P. Vaidyanathan, “*Multirate systems and filter banks*”, Prentice Hall, Englewood Cliffs, 1993.

[6] P. P. Vaidyanathan, Igor Djokovic, “*An Introduction to Wavelet Transforms*”, Caltech, Pasadena, CA 91125, August, 1994.

[7] Agrawal E., Gupta S, & Chandra M A, “*Data Hiding Using LWT Strategy*”, International Journal of Computer Applications, (0975 – 8887), (ICACEA-2014) at IMSEC, GZB

[8] A.K. AL Frajat, H.A. Jalab, Z.M.Kasirun, A.A.Zaidan & B.B.Zaidan “*Data hiding in video file: An overview*”, 2010, Journal of Applied Sciences 10 (15): 1644-1649, ISSN 1812-5654.

[9] C.P.Sumathi, T.Santanam & G.Umamaheswari, “*A Study of Various Steganographic Techniques Used for Information Hiding*”, 2013, IJCSES Vol.4, No.6, December 2013.

[10] K.Parvathi Divya & K.Mahesh, “*Various Techniques in Video Steganography -A Review*”, International Journal of Computer & Organization Trends – Volume 5, ISSN: 2249-2593, 2014.

[11] K.Rosemary Euphrasi & M. Mary Shanthi Rani, “*A Comparative Study On Video Steganography in Spatial and IWT Domain”*, 2016, 2016 IEEE International Conference on Advances in Computer Applications (ICACA).

[12] Park J.S. “*MATLAB GUI Tutorial for beginners*” University of Incheon.

[13] Sudhanshi Sharma & Umesh Kumar, “*Review of Transform Domain Techniques for Image Steganography*”, 2013, International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064.

[14] Sukhjinder Singh, Neeraj Gill, & Gagandeep Kaur, “*Identical Frames Based Video Steganography*”, 2014, International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering, Vol. 2, Issue 7, July 2014.

[15] Tinku Acharya, Ping-Sing Tsai, JPEG2000 Standard for Image Compression: Concepts, Algorithms and VLSI Architectures, 2004.