International Journal of Multimedia and Ubiquitous Engineering
Vol.9, No.6 (2014), pp.385-396
http://dx.doi.org/10.14257/ijmue.2014.9.6.37

Video Steganography for Hiding Image with Wavelet Coefficients

Chantana Chantrapornchai[1], Kornkanok Churin[2], Jitdamrong Preechasuk[2] and Suchitra Adulkasem[2]*

[1]*Department of Computer Engineering, Faculty of Engineering, Kasetsart University, Bangkok, Thailand*
[2]*Department of Computing, Faculty of Science, Silpakorn University, Nakorn Pathom, Thailand*

[1]*fengcnc@ku.ac.th, *suchitraa@hotmail.com*

Abstract

We study the video steganography method in which the image is hidden in a video file. The method is based on the discrete wavelet transform. The video frames are transformed and then the proper positions of the coefficients are selected to hide the secret image pixels. The heuristic considers the coefficients that have the similar values to that of secret images. The similar values mean the same or the values that are closed to the cover media pixels. We compare this approach to the random coefficient selection approach as well as the methods using the discrete wavelet transform. Different payloads are also considered to study the effect of secrete image size to the cover video. The results shows that the lifting multiple wavelet transform with similar coefficients yields the best results for all the test case.

Keywords: *Video Steganography; Wavelet Transform; Intensity*

1. Introduction

Steganography is a science that considers the method to hide information in the cover media. The direct purpose is the communication with the secret information. The methods can be classified based on the cover media and secret message type. The cover media can be audio, video, image or even text message. Similarly, the secret message can be images, audio, video and text messages. The challenge here is to cover the secret information properly without degrading the cover media, without noticing, and with security.

In this work, we are interested in the cover media that is the video file and the secret information is an image. Even though it is likely that the video can be used to cover the secret image properly, the difficulty arises on selecting frames and positions to hide image pixels. The framework begins as follows: We first transform the video and image using a kind of wavelet transform. We attempt to hide the image pixel in the coefficients of the frames. The two wavelet transforms are studied: discrete wavelet and lifting multiple wavelet. The coefficients of each frame are compared to the coefficients of the secret image. The similar coefficients are used to hide to image pixels. Obviously, the coefficient values are not exactly the same and the available positions may not be enough which is the main issue of efficiency.

2. Backgrounds

Steganography is very popular in the decade. The research work usually considers two domains, either spatial domain or frequency domain. In this work, we focus on the frequency domain. For such a domain, the two common transformations are used: wavelet and DCT.

ISSN: 1975-0080 IJMUE

For these works, some considers the text and some considers the image as a message while some uses the video and some uses the audio as the cover media. Wu and Sun [15] proposed the method for image sharing and checking for the validity of it. The method for reconstruction is developed for the case of a stego image. Kavitha and Murugan [10] attempted to hide maximum information while preserving against the detection by an unauthorized person. A steganographic system will be secured and effective when the statistics of the cover message and the stego data are identical. The system proposed to increase the strength of the key by using UTF-32 encoding in the swapping algorithm and lossless stegano technique in the AVI file. Liu, Liu and Ni [5] proposed a new low complexity chaotic steganography method to MPEG-2 videos. Prabakaran and Bhavani [12] presented the modified secure and high capacity based steganography scheme of hiding a large-size secret image into a small-size cover image. They applied Arnold transformation to scramble the secret image. Discrete wavelet transform (DWT) is applied to perform in both images using the alpha blending operation.

Alkhraisat and Habes [2] presented a new method for hiding the secret image inside the cover image. Elham, Jamshid and Nima [9] applied the wavelet transform and the genetic algorithm to embed data in the discrete wavelet transform coefficients in 4x4 blocks on the cover image. Safy, Zayed and Dessouki, [13] proposed the adaptive steganographic technique which considered the bits of the payload to be embedded in the integer wavelet coefficients of the cover image. Sarreshtedari and Ghaemmaghami [14] presents the image steganography method using the wavelet transform coefficients of the original image to embed the secret data by maintaining integrity of the wavelet coefficients. Battacharya, Dey and Chaudhuri [4] presented a steganography technique for hiding multiple images in a color image based on DWT and DCT. Dinesh and Ramesh [7]'s method is based on DWT transforms which allows to perfect embedding of the hidden message and reconstruction provide an efficient capacity for data hiding without sacrificing the original image quality.

2.1. Discrete Wavelet Transform [8]

We apply the wavelet transform which, particularly, is Haar-DWT, the simplest DWT. A 2-dimensional Haar-DWT contains two operations, one is the horizontal operation and the other is the vertical one. Both splits the image into a lower resolu-tion approximation image or band (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH). The Haar wavelet transform is easy to implement. The algorithm is fast. It consumes the small memory space. It has the reversed operation that has no the edge effect. However, the limitation is on the discontinuity. The result of the wavelet transform is a set of wavelet coefficients. The equation of a 2-D Haar-DWT is in Eq. (1).

$$\psi(x) = \sum_{k} (-1)^k c_{M-k} \phi(2x-k) \tag{1}$$

where $\varphi =$ the host function that is calculated from , $\phi_{jk} = \phi(2^j x - k)$, and C_{M-k} the translation factor.

2.2. Lifting Based Multi-Level Wavelet Transform [1, 3]

The lifting scheme is an algorithm which is used for the hardware and the software implementation of DWT. Its steps of predictions and updating are displayed in Figure 1.

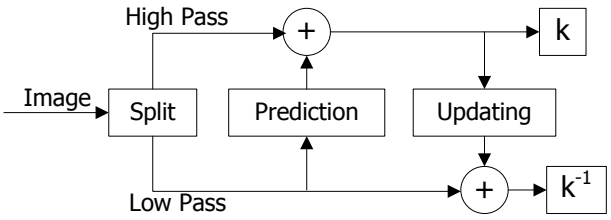


Figure 1. Lifting Scheme Forward transform [6]

Figure 1 presents the lifting scheme of the wavelet filter which computes the one-dimension signal. It consists of the following steps.

-Split step: The signal is split into the even and odd points. The maximum correlation between the adjacent pixels can be used for the next step.

-Predict step: The even samples are multiplied by the predicted factor. The results are added to the odd samples to generate the new coefficients.

-Update step: the new coefficients computed by the predict step are multiplied by the update factors. The results are added with the even samples to get the coarse coefficients.

The advantage of lifting scheme is the forward and inverse transform was obtained from the same architecture. The inverse goes from right to the left, by inversing the coefficients of normalized and changes the sign positive to negative. The *k* is the constant of normalization and the steps of the predictions and the updating at decomposition in polyphase matrix. The polyphase representation of discrete filter h(n) is defined as Eq. (2):

$$h(z) = h_e(z^2) + z^{-1}h_0(z^2) \qquad (2)$$

where $h_e(z)$ and $h_o(z)$ are respectively obtained from the even and odd zeta transform respectively. If we represent $g_e(z)$ and $h_o(z)$ the low pass and high pass coefficients of the synthesis filter respectively, the polyphase matrix written as Eq. (3):

$$p(z) = \begin{bmatrix} h_e(z) & g_e(z) \\ h_0(z) & g_0(z) \end{bmatrix} \qquad (3)$$

The filters $h_e(z)$, $h_0(z)$, $g_e(z)$ and $g_0(z)$ are Laurent polynomials, as the set of all polynomials exhibits a commutative ring structure, within which polynomial division with remainder is possible, the long division between two Laurent polynomials is not a unique operation. Figure 2 is the difference between the two wavelet transforms.

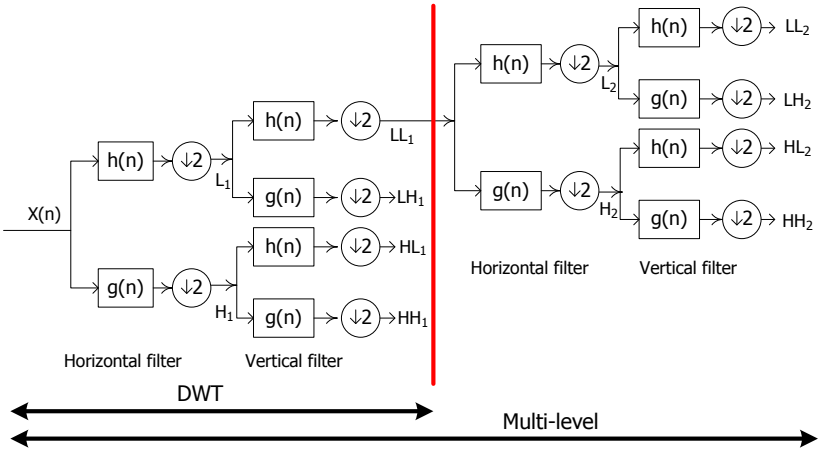


Figure 2. Difference between Discrete Wavelet Transform and Lifting based Multi-level Wavelet Transform [6]

3. Methodology

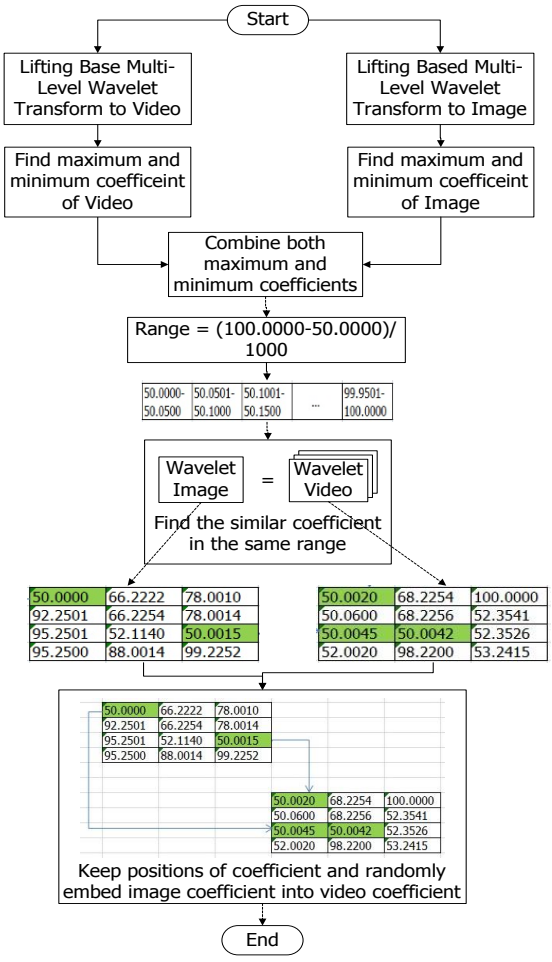


Figure 3. A Block Diagram of Finding the Similar Wavelet Coefficients

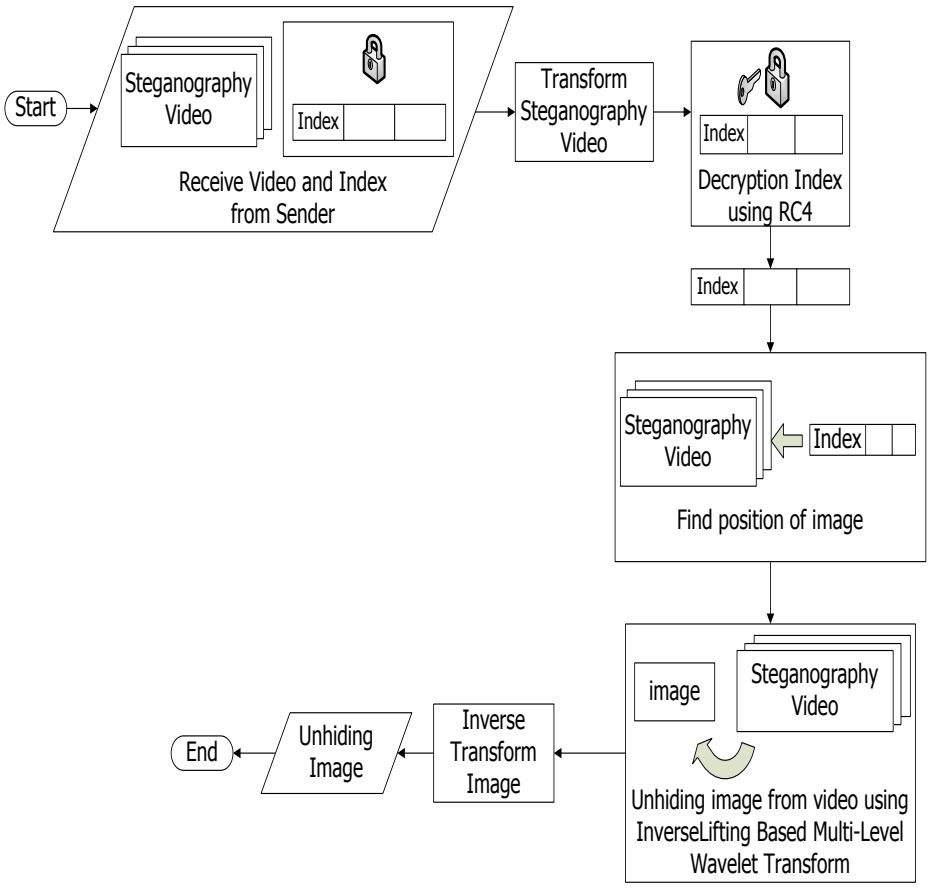


Figure 4. A Block Diagram of the Proposed Doffing Model

The proposed method for the hiding phase is as shown in Figure 3. The proposed doffing model is as shown in Figure 4. Figure 3, in Step 1) brings the secret image and the video file to transform using the lifting based multi-level wavelet transform. We find and keep the positions with the similar coefficient of each color between the secret image and the frame of the video. Since we are interested in hiding in the frames containing pixels with the similar coefficient as those of the secret image, this step finds these positions. From simplicity, we round the coefficients to integer values. The similar coefficients can be found by exact comparison. However, when it is possible that the values are closed to more than one value, the smallest difference is chosen. When there are two values with the save absolute values, we prefer the darker positions (the smaller value). Among these, we have to check whether the coefficient positions are already used. Step 2) embeds the pixels of the secret image with the similar coefficient into those frames. In particular, we find the positions with the similar coefficient values for each wavelet plane. If the cover video frames has more number of coefficients that are similar to that of the image, the algorithm works fine. Finally, we may not find any coefficient positions, e.g. the picture is dark background or white backgrounds. Hence, we randomly pick the positions.

After embedding, the indices are kept in a file separately from the stego video. Particularly, we keep the frame numbers, the row and column positions etc. They are also encrypted. For example, (1, 5, 5) means we keep the position at frame1, row5 and column5. Next, we perform the inverse transform back for all the stego video frames.

Upon the decryption side, Figure 4 presents the steps. First, we doff the pixels of the each frame of video file using the lifting discrete wavelet transforms. Then, we decrypt the index files. The indices are used to locate frames and pixel positions to hide value. We extract the coefficient values from and save them to as the image coefficients. Then we perform the inverse lifting wavelet transforms to obtain the hidden image.

4. Results

We carry out the experiments to demonstrate the efficiency of the proposed scheme. The proposed method has been simulated using the MATLAB 2013 program on the Windows 7 platform. A test set of image of size are 100 × 100, 256 × 256 and 512 × 512 and they all are used for the experimental test as an original secret. A set of the video file of any size are used for the tests. They are obtained from (http://www.reefvid.org/). A set of video of any size are used for the experimental test as the cover image that the video is about 307 seconds long. The total fame is 7,750 frames and the frame rate is 25 Fps.

The PSNR of the approach is computed against the given data set. The equation for computing *MSE* is in Eq. (4).

$$MSE = \left[\frac{1}{N * N} \right] \sum_{i=1}^{N} \sum_{J=1}^{N} \left(x_{ij} - \overline{x}_{ij} \right)^2 \tag{4}$$

where x_{ij} is the intensity value of the pixel in the secret image, $\overline{x}_{ij}$ is the intensity value of the pixel in the frame and N is the size of the image.

The Peak Signal to Noise Ratio (PSNR) measure is the quality of the stego image frame by comparing with the original image. The equation is in Eq. (5).

$$PSNR = 10 \log_{10} 255^2 / MSE(db) \tag{5}$$

For the video, the average PSNR values of all the video frames are calculated. Table 1 shows the PSNR values of embedded video using lifting based multi-level wavelet transform with the similar coefficients (LMWT-Sim), using multi-level wavelet transform with the random coefficients (LMWT-Random), discrete wavelet transform with the similar coefficients (DWT-Sim) and discrete wavelet transform with random coefficients (DWT-Random). The PSNR of LMWT-Sim is better for all the methods due to the lifting scheme have been developed as a flexible tool suitable for constructing the second generation wavelet.

The average PSNR values of the video frames are calculated to compare the stego video with the original video. However, for the average PSNR values, we calculate from all frames and then divide with the total number of all frames as the following equation.

$$\frac{\sum_{i=1}^{n} PSNR_i}{n} \tag{6}$$

where $PSNR_i$ = PSNR of frame *i* and
N = the total number of frames.

Table 1. Comparison of the Methods with Different Images and Different Video Files

Video name	Secret image	LMWT-Sim	LMWT-Random	DWT-Sim	DWT-Random
		PSNR	PSNR	PSNR	PSNR
clip235 (data rate: 2677 kbps, frame rate:25 frames/second)	Lena image (100*100)	54.594	40.374	49.558	35.966
	Lena image (256*256)	53.221	40.229	48.795	34.107
	Lena image (512*512)	53.101	39.495	46.669	31.580
clip396 (data rate: 3103 kbps, frame rate: 25 frames/second)	Lena image (100*100)	56.483	43.783	48.566	36.798
	Lena image (256*256)	54.205	42.173	47.395	34.704
	Lena image (512*512)	54.089	41.059	46.290	32.176
clip535 (data rate: 2453 kbps, frame rate: 25 frames/second)	Lena image (100*100)	58.238	45.382	51.395	35.363
	Lena image (256*256)	56.494	43.208	50.990	34.227
	Lena image (512*512)	55.960	41.897	49.281	32.683

Table 1 compares the PSNR for all test-size pictures with varying approaches. The smaller the value is, the worse the picture is. The good approach should be scaled to the method corresponding. The size of the pictures has an effect to the quality of the secret image. The smaller the image is, the better the PSNR value.

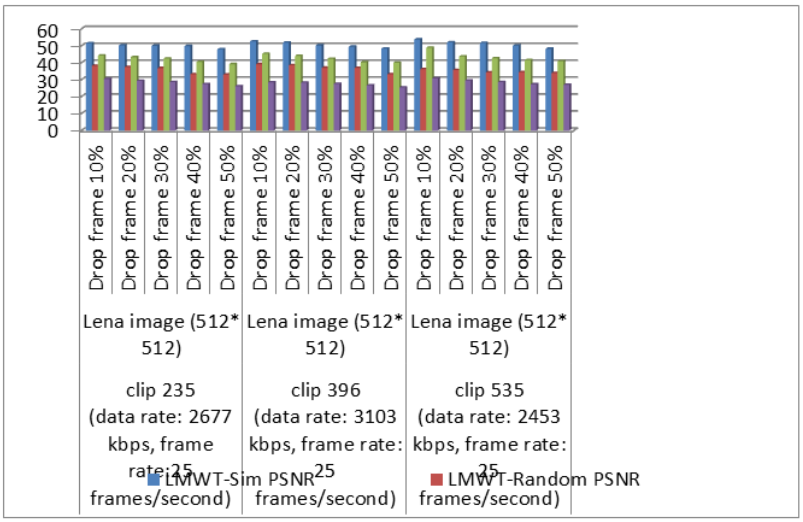


Figure 5. Comparison of Different Drop Frame Rates with Different Video Files with Lena Image

Figure 5 compares the PSNR when the frame drop percentage is varied by 10%, 20% 30% 40% and 50% of all frames of the video file. Dropping frame is done by random and is

done for all the stego video. The dropped frames are skipped and the overall PSNR of the secret images are calculated. The more frame drops the less PSNR values.

Figure 6 compares the PSNR values of the various methods for the varying payload size. For example, when the payload is 10%, we consider the case where the size of the secret image size is 10% of the total size of all the frames. Obviously, the larger payload is, the worse PSNR is. Still, LMWT-Sim performs better for all the cases. Also, the lower payload size, the better the performance. That is is because the values to hide are less compared to the coefficient values of the frames.

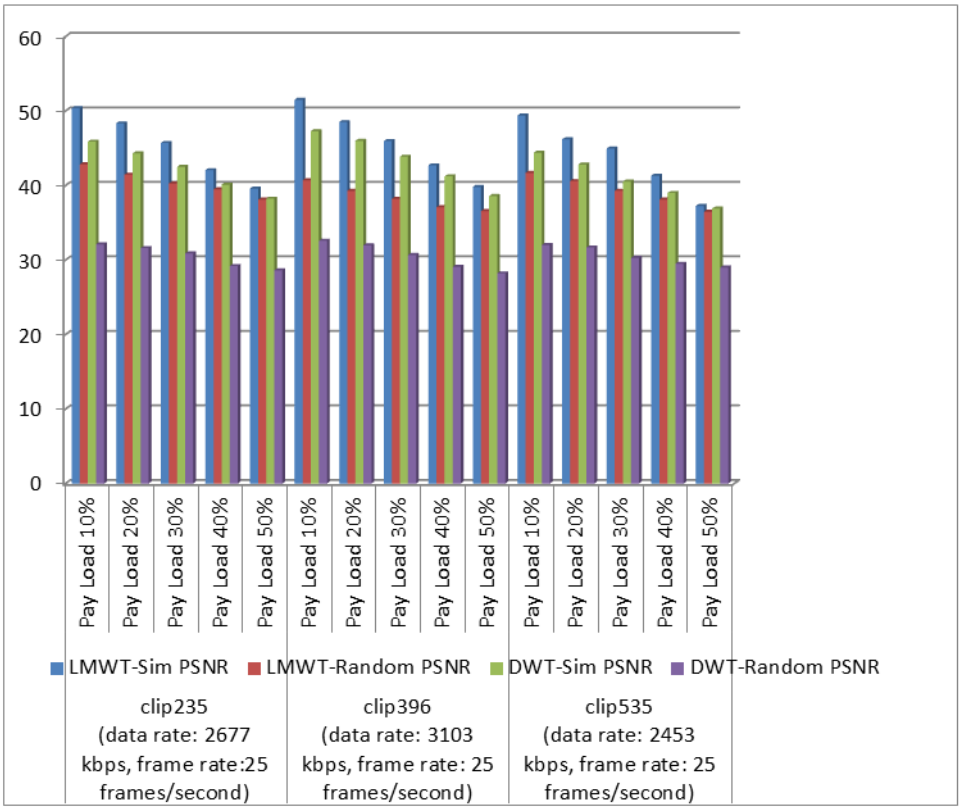
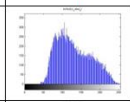
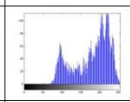
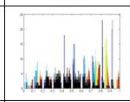
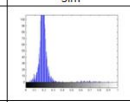
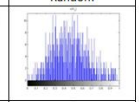
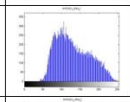
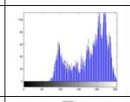
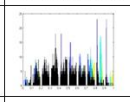
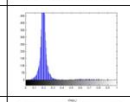
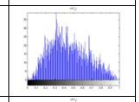
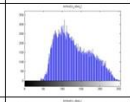
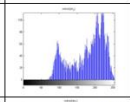
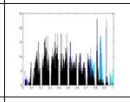
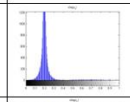
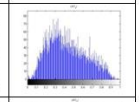
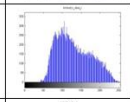
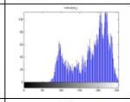
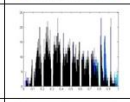
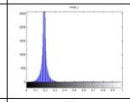
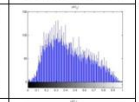
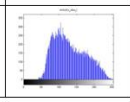
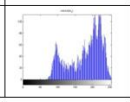
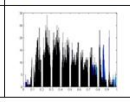
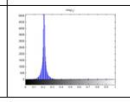
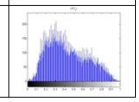


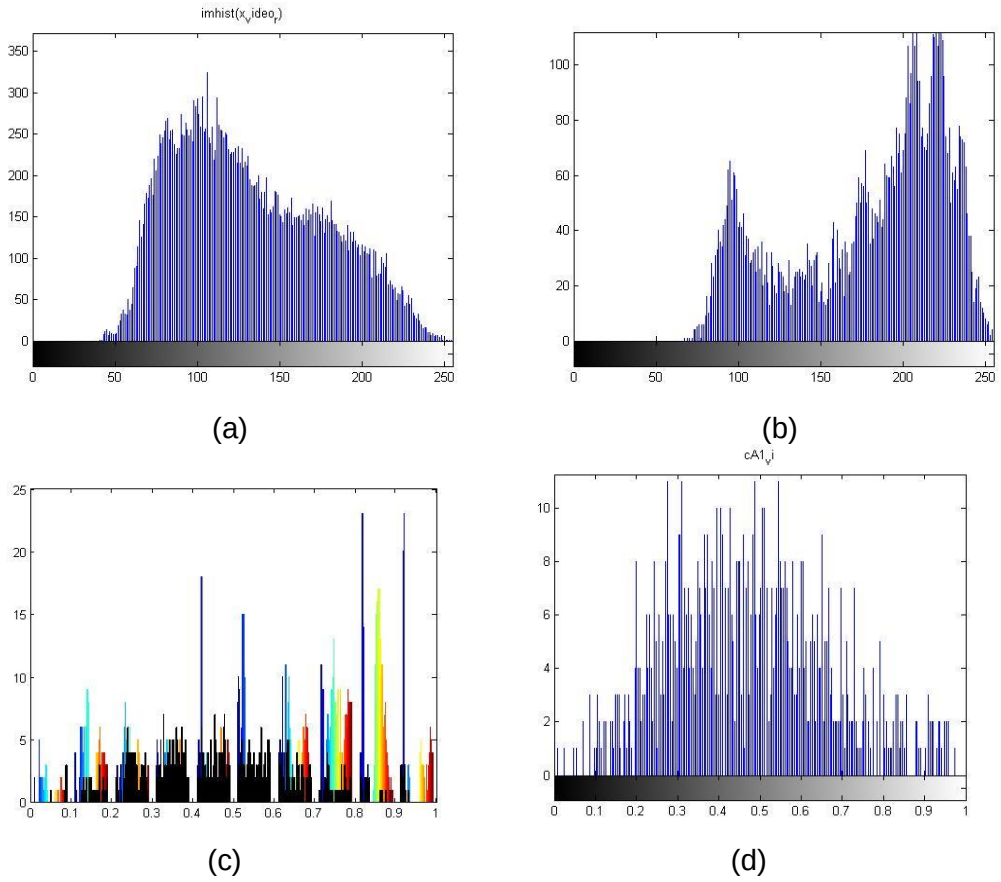
Figure 6. Comparison of the Different Payload Size with Different Video Files

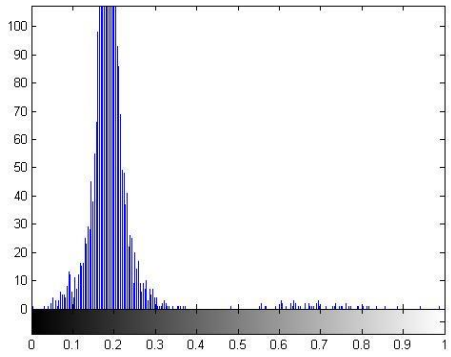
Table 2 presents the difference of the coefficient values between various methods considering different payload videos. Columns 'Video clip' and Lena present histogram of the coefficients. Column 'Combine' is the merge of coefficients of the previous two columns. Columns 'Stego video LMWT-Sim', and 'Stego video LMWT-Random' show the coefficient values of the resulting stego video using LMWT with similar values and LMWT with random coefficients accordingly. It is found that LMWT-Random's histograms are very different from the combination of both more.

Table 2. Wavelet Cofficient Histogram of Clip 235 of Original Video and Stego Video

% of payload	Video clip 235	Lena image	Combine	Stego video LMWT-Sim	Stego video LMWT-Random
Lena Payload 10%					
Lena Payload 20%					
Lena Payload 30%					
Lena Payload 40%					
Lena Payload 50%					

For example, the first row is presented in detailed as Figure 7. Figures 7(a)-(b) are the histogram of the coefficients of the video frame and the hidden image. Figure 7(c) is the sum of the two histograms. Figures 7(d)-(e) are the coefficients of the stego frames using LMWT-Sim and LMWT-Random.



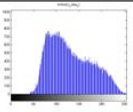
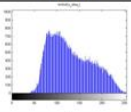
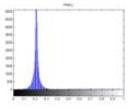
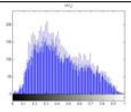
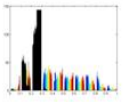
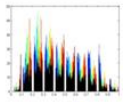
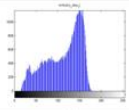
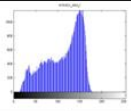
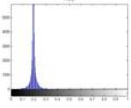
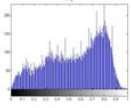
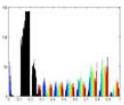
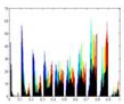


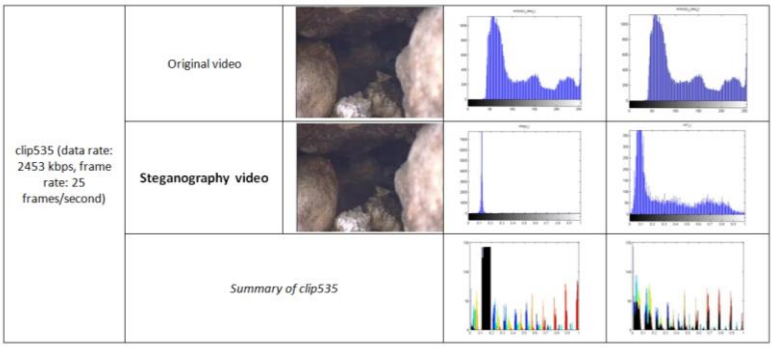
(e)

Figure 7. The details of Figure 6 (first row): (a) coefficients of the selected frame (b) coefficients of the hidden image (c) combined coefficients (d) coefficients of the stego frame using LMWT-Sim (e) coefficients of the stego frame using LMWT-Random

Table 3 presents the histograms of each method along with the video files. The row "Original video" shows the sample frame of the original and the row “Steganography video“ is the resulting frame. In the column“ Histogram“, we show the histogram of the stego frame in the same row. The row“Summary“ is the summary of the differenece between the stego of the histogram of the original and the histogram of the stego frame and the original frame. The purpose is to show the difference histogram of two methods on the selected frame. This is to check how much different they are. Also, this is to compare the original frame and the resutling stego frame.

Table 3. Wavelet Cofficient Histogram of Original Video and Stego Video

Video file	Type of video	Sample frame of video file	Histogram of LMWT-Sim	Histogram of LMWT-Random
clip235 (data rate: 2677 kbps, frame rate:25 frames/second)	Original video			
	Steganography video			
	Summary of clip235			
clip396 (data rate: 3103 kbps, frame rate: 25 frames/second)	Original video			
	Steganography video			
	Summary of clip396			



5. Conclusion

We present the steganography method for hiding the image in the video. The approach uses the lifting multi-level wavelet and hides the image coefficients in the video coefficients. The coefficients with similar values are used to hide to reduce the errors in the resulting stego video. We compare the efficiency of the technique using PSN, considering various test cases such as different payloads, and frame dropping. The hiding in coefficients of lifting multi-level wavelet gives better results compared to the random coefficient selection of discrete DWT about 40%.

References

[1] T. Acharya and C. Chakrabarti, "A Survey Lifting-based Discrete Wavelet Transform Architectures. In: Journal of VLSI Signal Processing, vol. 42, no. 13, (**2006**) February, pp. 321-339.
[2] M. Alkhraisat and M. Habes, "4 least Significant Bits Information Hiding Implementation and Analysis", In: ICGST Int. Conf. on Graphics, Vision and Image Processing (GVIP-05), (**2005**), Cairo, Egypt.
[3] S. Barua, J. E. Charletta, K. A. Kotteri and A. E. Bell, "An efficient architecture for lifting-based two-dimensional discrete wavelet transforms", In: Intergration, the VLSI Journal, vol. 38, (**2004**) July 21, pp. 341-352.
[4] Battacharya, T. N. Dey and S. R. B. Chauduri, "A session based multiple image hiding technique using DWT and DCT", In: J. Comput. Applic., vol. 38, (**2012**), pp. 18-21.
[5] L. Bin, L. Fenlin and N. Daping, "Adaptive compressed video steganography in the VLC-domain Daping", In: Wireless, Mobile and Multimedia Networks, IET, (**2006**), pp. 1-4.
[6] D. Dhaha, Z. Medien, S. Taoufik, A. Mohamed, B. Belgacem, M. Mohsen and T. Rached, "Multi-level Discrete Wavelet Transform Architecture Design", In: Proceedings of the World Congress on Engineering 2009 vol. IWCE 2009, July 1 – 3, pp. 191-195, London, U.K (**2009**).
[7] Y. Dinesh and A. P. Ramesh, "Efficient capacity image steganography by using wavelets", In: J. Eng. Res. Applic., vol. 2, (**2012**), pp. 251-259.
[8] D. Donoho, "Nonlinear Wavelet Methods for Recovery of Signals, Densities, and Spectra from Indirect and Noisy Data", In: Different Perspectives on Wavelets, Proceeding of Symposia in Applied Mathematics, vol. 47, I. Daubechies ed. Amer. Math. Soc., Providence, R.I., (**1993**), pp. 173-205.
[9] G. Elham, S. Jamshid and F. Nima, "High Capacity Image Steganography using Wavelet Transform and Genetic Algorithm", In: Multi Conference of Engineers and Computer Scientists, vol. 1, (**2011**).
[10] R. Kavitha and Murugan, "Lossless Steganography on AVI File Using Swapping Algorithm", In: Conference on Computational Intelligence and Multimedia Applications, IEEE (**2007**), vol. 4, pp. 83-88.
[11] M. Michel, M. Yves, O. Georges and P. Jean, "Wavelet Toolbox for Use with MATLAB", In: Wavelet Toolbox User's Guilde 1996 - 1997 by The MathWorks, Inc.
[12] G. Prabakaran and R. Bhavani, "A modified secure digital image steganography based on Discrete Wavelet Transform", In: Computing, Electronics and Electrical Technologies (ICCEET), IEEE (**2012**), pp. 1096-1100.
[13] R. O. El Safy, H. H. Zayed and A. El Dessouki, "An Adaptive Steganographic Technique Based on Integer Wavelet Transform", In: Networking and Media Convergence, (**2009**) March, pp. 111-117.

[14] S. Sarreshtedari, and S. Ghaemmaghami, "High Capacity Image Steganography in Wavelet Domain", In: Consumer Communications and Networking, (**2010**), pp. 1-6.
[15] X. Wu and W. Sun, "Secret image sharing scheme with authentication and remedy abilities based on cellular automata and discrete wavelet transform", In: Journal of Systems and Software, Science Direct, vol. 86, issue 4, (**2013**) April, pp. 1068-1088.

