Advanced Science and Technology Letters
Vol.35(Security 2013), pp.46-49
http://dx.doi.org/10.14257/astl.2013.35.11

Image Steganograpy via Video Using Lifting Wavelet Transform

K. Churin J. Preechasuk S. Adulkasem*

Department of Computing, Faculty of Science, Silpakorn University
Nakhon Pathom,Thailand

C. Chantrapornchai

Department of Computer Engineering, Faculty of Engineering, Kasetsart University
Bangkok,Thailand, and
Department of Computing, Faculty of Science, Silpakorn University
Nakhon Pathom,Thailand
Email: suchitraa@hotmail.com*

Abstract. We study the steganography method which hides an image in the video. We transform the video and image the lifting multiple discrete wavelet transform [1]. The coefficients of both are compared and the proper position of the coefficients are selected to hide the secret image pixel. The heuristic considers the coefficients that have the similar values to that of secret images are used to hide. The experiments compare this approach to the random selection approach as well as the methods using discrete wavelet transform. Different payloads are also considered to study the effect of secrete image size to the cover video. The experiments show that the selecting the similar coefficients give better results than the random approach for such a wavelet transform.

Keywords: Video Steganography; Lifting Wavelet; Multi-Level Wavelet Transform; Intensity.

1 Introduction

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 is 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.

ISSN: 2287-1233 ASTL

Steganography has becoming popular in the past ten years. The work can be classified into spatial domain and frequency domain. Since we are considering the frequency domain, in the following we describe previous work in this domain and the work uses the cover media/secret message similar to us. Common two transformations are used: wavelet and DCT. Some of them works on images and some works on video or audio cover media.

Prabakaran and Bhavani [4] presented the modified secure and high capacity based steganography scheme of hiding a large-size secret image into a small-size cover image. Elham, Jamshid and Nima [3] 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, [5] 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 [6] 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 [2] presented a steganography technique for hiding multiple images in a color image based on DWT and DCT.

3 Methodology

The proposed method has the following steps: Step 1) brings the secret image and the video file to transform using the lifting based multi-level wavelet transform [1]. 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 number, 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, 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 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 $MSE = \frac{1}{N \times N}\sum\sum (x_{ij} - x'_{ij})^2$ where x_{ij} is the intensity value of the pixel in the secret image, 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 $PSNR = 10\log_{10} 255^2 / MSE\ (db)$. 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 has 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.

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

where $PSNR_i$ = PSNR of frame i, 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

From Table 1,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.

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%					

5 Conclusion

We present the steganography method for hiding the image in the video. The approach uses the lifting multi-level wavelet and hide 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 PSNR. 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. Acharya T. and Chakrabarti C.: A Survey Lifting-based Discrete Wavelet Transform Architectures. In: Journal of VLSI Signal Processing 42, 13 February, pp.321-339. (2006).
2. Battacharya, T. N. Dey and S.R.B. Chauduri.: A session based multiple image hiding technique using DWT and DCT. In: J. Comput. Applic., 38: 18-21. (2012)
3. Elham, G., Jamshid, S., Nima, F.: High Capacity Image Steganography using Wavelet Transform and Genetic Algorithm. In: Multi Conference of Engineers and Computer Scientists, vol. 1. (2011)
4. Prabakaran, G., Bhavani, R.: A modified secure digital image steganography based on Discrete Wavelet Transform. In: Computing, Electronics and Electrical Technologies (ICCEET), pp. 1096-1100. IEEE (2012)
5. 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, pp.111-117, March. (2009)
6. Sarreshtedari, S. and Ghaemmaghami S.: High Capacity Image Steganography in Wavelet Domain. In: Consumer Communications and Networking, pp.1-6. (2010)