Hierarchical Watermarking Structure for Combined LSB and Wavelet Methods

Jaejoon Kim
School of Computer and Communication, Daegu University,
201 Daegudaero Jillyang, Gyeongsan, Gyeongbuk, 712-714 Korea
jjkimisu@daegu.ac.kr

Abstract—In this study, we present a scheme that combines LSB (Least Significant Bit) DWT (Discrete Wavelet Transform) watermarking techniques. Data compression has rapidly evolved due to variable mobile terminals and the vast amount of images and video. It is necessary to prevent access to and maintain the confidentiality of data. LSB and wavelet watermarking methods have arisen to address this need. However, unlike the LSB insertion method, the proposed scheme is effective against several attacks. The scheme first inserts a watermark using LSB in a test image, and 3-level DWT decomposition is implemented for robustness and security. We measured the Mean Squared Error (MSE) and Peak Signal to Noise Ratio (PSNR) to validate the scheme and acquired reasonable results. This study highlights the hierarchical structure of the LSB and wavelet-based watermarking technique.

Keyword-Digital watermarking, LSB, DWT, usage control

I. INTRODUCTION

The rise in the number of cars has led to more traffic accidents and the frustrating problem of illegal parking. To counter this problem, we previously presented a novel application that can reduce the number of police interventions by allowing residents to enforce parking themselves. The application works by sending two video images of the illegally parked car along with information regarding the time and duration that the car was parked. During this process, we foresaw the possibility of tampering with the images. Therefore, to counter this, we implemented a watermark technique. We previously used LSB (Least Significant Bit) insertion as a watermarking technique to determine if an image had been tampered with [1, 2]. In this paper we implement a combination of LSB [3] and DWT (Discrete Wavelet Transform) [4-7] as watermarking techniques as a better solution to prevent tampering.

Invariant features for video processing in feature selection have been pointed out [8, 9]. One study showed the possibility of using geometric distortions found unequally in an entire image for image analysis [10]. The present study involves image encryption and decryption in a wireless environment [11] that could involve smartphones. Thus, damage to the information transmitted using smartphones needs to be prevented [12, 13].

Section 2 discusses the original method of LSB watermarking. Afterwards, the new wavelet watermarking technique is explained. Section 3 identifies the technique validated by several experiments that test the level of toughness against various attacks. Sections 4 and 5 conclude the paper by discussing future works and possible solutions for better protection of information.

II. RELATED WORKS

This section briefly explains the LSB and wavelet watermarking techniques and shows how the two techniques differ from each other.

A. LSB Watermarking Technique

The LSB (Least Significant Bit) technique hides a decryption key in the lowest bit in a video image. It first divides the video into RGB (Red Green Blue) channels and then performs bit slicing on the watermarked image [5]. This sequence is hidden in the lowest bit in the blue channel, and then the modified channel is switched with the original one, as shown in Figure 1.

B. Wavelet Watermarking Technique

The wavelet watermarking technique disassembles the original video and converts it to a wavelet space. To insert a watermarked image in the wavelet space, the method processes the image first and then inserts the original image that has been wavelet-disassembled. The method can then recover the entire wavelet areas that have been manipulated, as shown in Figure 2. There are many processes that prepare the watermarked image, which shall be discussed in section 3.

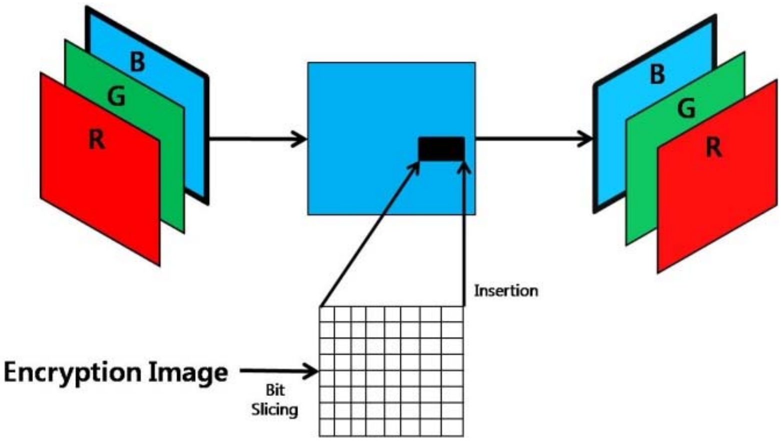

Fig. 1. LSB Watermarking scheme on blue channel

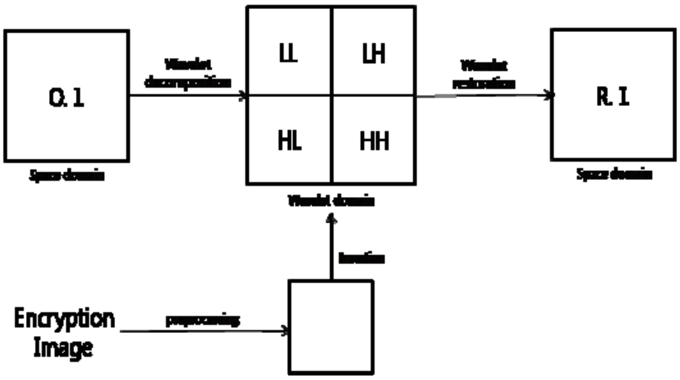

Fig. 2. Wavelet watermarking block diagram (O.I and R.I mean original and resulting images.)

III. PROPOSED WORK

This section discusses the proposed watermarking technique. The technique was subjected to several attacks and evaluated for the recoverability of the original data. The entire experiment was performed through MATLAB using the Daegu University logo as the watermarked image.

A. Watermarking Insertion

As shown in Figure 3, the proposed method inserts 8 random characters into the watermark video by LSB watermarking. 3-level wavelet decomposition was performed on the original and watermarked video. We defined the decomposed areas as LL3, LH3, HL3, HH3, LH2, HL2, HH2, LH1, HL1, and HH1, and the wavelet decomposed areas from the watermark video were defined as LL3', LH3', HL3', HH3', LH2', HL2', HH2', LH1', HL1', and HH1'. The LL3 and LL3' areas merge together. Here, the coefficient of LL3' is important. When inserting the watermark, it should not be seen by the naked eye, and the original image must also be recoverable.

If the coefficient was less than 1/1000, the watermark was visible, but not when the coefficient was larger. The coefficient was set as 1/1000 to insert the watermark. Equation (1) shows this process. We defined the merged wavelet area as LL3". If we subject LL3" and the remainder of the original video to the reverse wavelet transform, we can recover the image.

$$\mathrm{LL3}'' = \mathrm{LL3} + \frac{1}{1000}\mathrm{LL3}' \quad (1)$$

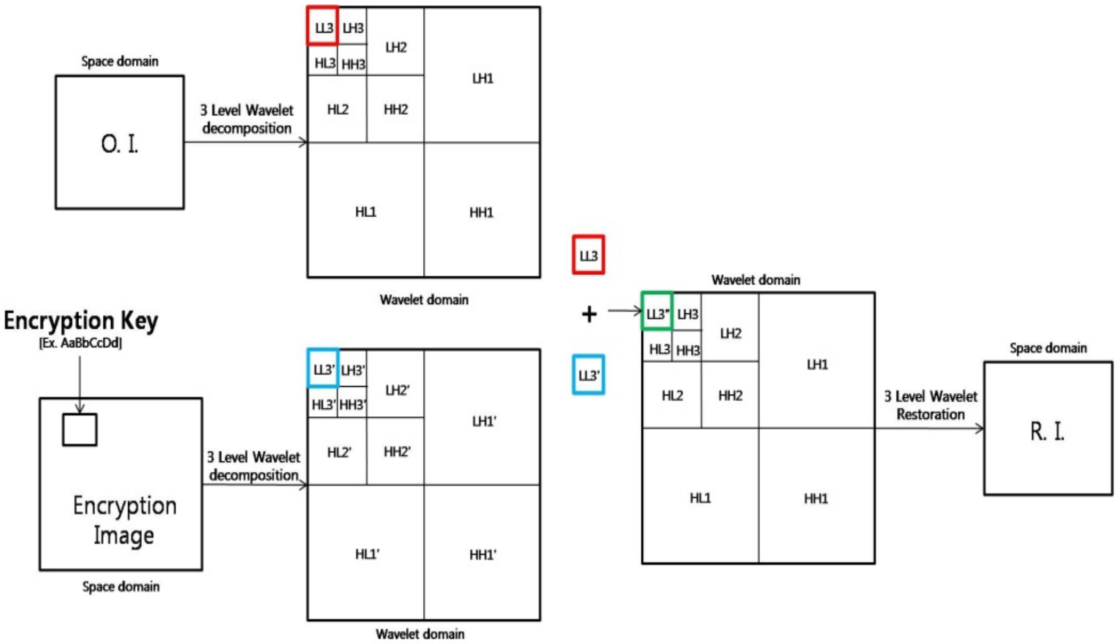

Fig. 3. Proposed wavelet watermarking embedded scheme (O.I and R.I mean original and resulting images.)

B. Watermark extraction

The recovery of the image can be achieved simply by reversing the process of inserting the watermark, as shown in Figure 4. We performed 3-level wavelet restoration on a video with a watermark. The 3-level decomposed LL part corresponds to the LL3' area, and we can erase the LL3 area of the current video from the original video. The watermarked video can be obtained by taking the inverse transformation in the previous equation while inverting the original coefficient. We then extract the key through the LSB recovery process and compare it with the original.

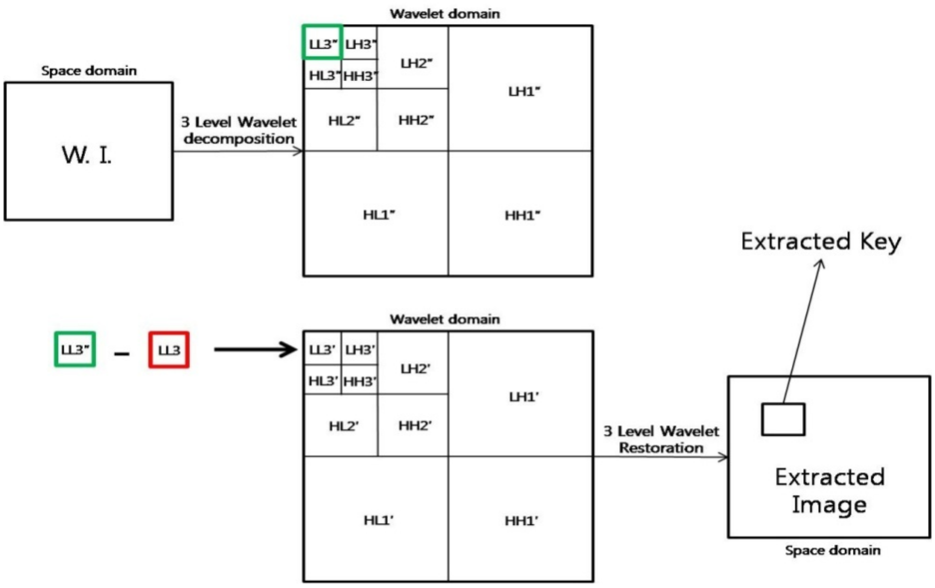

Fig. 4. Proposed DWT watermarking extraction scheme (W.I. means watermark inserted image.)

IV. Experimental results

A. Comparison of images after watermark insertion

Fig. 5-(a) shows the original image, and Fig 5-(b) shows the result of inserting a watermark. We also inserted an 8-character string, ‘ytHBEOIc’, into the image. There are no distinguishable differences in the two images. The Mean Squared Error (MSE) and Peak Signal to Noise Ratio (PSNR) [4] results are shown in Table I.

(a) (b)

Fig. 5. (a) Original Image and (b) watermarked image

TABLE I
Experimental result of MSE and PSNR with watermark embedding

	MSE	PSNR
Value	$7.1845e^{-9}$	81.7629

B. Comparison of images after watermark extraction

Fig. 6-(a) shows another watermarked image, and Fig. 6-(b) shows a watermarked image with a string embedded by the LSB method. Again, there is nothing that can distinguish the two different images. Lastly, Fig 6-(c) shows the image after the watermark was extracted. We extracted the 'ytHBEOIc' string inserted earlier. Table II shows the MSE and PSNR comparison between Fig. 6-(b) and Fig. 6-(c).

(a) (b) (c)

Fig.6. Image comparison after watermark extraction: (a) watermarked image, (b) string embedded watermarked image, and (c) watermark extracted image

TABLE II
Experimental result of MSE and PSNR after watermark extraction

	MSE	PSNR
Value	10.3442	37.9838

V. CONCLUSION

The combined LSB and DWT-based watermarking technique has been shown and validated. The designed system protects images and video frames from damage. However, the approach needs further evaluation and improvements. The method should be tested for usage control and variable attacks in future works. This paper has shown the possibility of protecting valuable information and could be applied to ID integrated environments [14] and human face processing [15].

ACKNOWLEDGMENT

This work is supported by Daegu University Research Program in 2014.

REFERENCES

[1] Kim, G.N., Choi, H.M., Kim, D.Y., Kim, J., Watermarking Imaged-based Vehicle Parking Enforcement Program for Preventing Evidence Manipulation. Journal of Applied Sciences, Vol. 13, pp. 5260-5264, 2013.
[2] Verma, O.P., Nizam, M., Ahmad, M., Modified Multi-Chaotic Systems that are Based on Pixel Shuffle for Image Encryption, Journal of Information Processing System, Vo. 9, No. 2, pp. 271-286, 2013.
[3] Chan, C.K., Cheng. L.M. Hiding data in image by simple LSB substitution. Pattern Recognition, Vol. 37, pp. 469–474, 2003.
[4] Rioul, O., Vetterli, M., Wavelets and signal processing. IEEE Signal Processing Magazine, Vol. 8, pp. 14-38, 1991.
[5] Gonzalez, R.C., Woods, R.E., Digital Image Processing, 3rd ed.; Prentice Hall, New Jersey, USA, 2007.
[6] Nikolaidis. N., Pitas. I., Robust Image Watermarking in the Spatial Domain. Signal Processing, Vol. 66, pp. 385-403, 1998.
[7] Kundur. D., Hatzinakos. D., A Robust Digital Image Watermarking Method using Wavelet-Based Fusion, Proceedings of ICIP'97, Santa Barbara, CA, USA, October 26-29, 1997, Vol I, pp. 544-547.
[8] Ho, Y.S., Challenging Technical Issues of 3D Video Processing, Journal of Convergence, Vol. 4, No.1, pp. 1-6, 2013.
[9] Chang, S.M., Chang, H.H., Yen, S.H., Shih, T.K., Panoramic human structure maintenance based on invariant features of video frames, Human-centric Computing and Information Sciences, pp. 3-14, 2013.
[10] Liew, L.H., Lee, B.Y., Wang, Y.C., Cheah, W.S., Aerial Images Rectification Using Non-parametric Approach, Journal of Convergence, Vol. 4, No.2, pp. 15-21, 2013.
[11] Bagade, A.M., Talbar, S.N., A High Quality Steganographic Method Using Morphing, Journal of Information Processing Systems, Vol. 10, No. 2, 256-270, 2014.
[12] Cho, M., Lee, I.H., Optical Image Encryption and Decryption Considering Wireless Communication Channels, Journal of Information Processing Systems, Vol. 10, No. 2, pp. 215-222, 2014.
[13] Feese, S., Burscher, M., Jonas, K., Tröster, G., Sensing spatial and temporal coordination in teams using the smartphone, Human-centric Computing and Information Sciences, pp. 4:15, 2014.
[14] Seo, H.J., Choy, Y.C., ID Credit Scoring System Based on Application Scoring System: Conceptual online ID credit for ID integrated environment, Journal of Convergence, Vol. 5, No.1, pp. 38-43, 2014.
[15] Bhattacharjee D., Adaptive polar transform and fusion for human face image processing and evaluation, Human-centric Computing and Information Sciences, 4:4, 2014.

AUTHOR PROFILE

Jaejoon Kim received his B.S. degrees in Mathematics and Electronics Engineering from Hanyang University, Korea in 1988 and 1991. He received his M.S. and Ph.D degrees in the Department of Electrical Engineering, Iowa State University, USA in 1995 and 2000. From 2001 to 2002, he worked for the Electronics and Telecommunications Research Institute (ETRI) in Korea. Currently, he serves as a professor at Daegu University. His research interests include multimedia codec, image processing and nondestructive evaluation.