Data-Hiding Method using Digital Watermark in the Public Multimedia Network

Jung-Hee Seo*, and Hung-Bog Park**

Abstract: In spite of the rapid development of the public network, the variety of network-based developments currently raises numerous risks factors regarding copyright violation, the prohibition and distribution of digital media utilization, safe communication, and network security. Among these problems, multimedia data tend to increase in the distributed network environment. Hence, most image information has been transmitted in the form of digitalization. Therefore, the need for multimedia contents protection must be addressed. This paper is focused on possible solutions for multimedia contents security in the public network in order to prevent data modification by non-owners and to ensure safe communication in the distributed network environment. Accordingly, the Orthogonal Forward Wavelet Transform-based Scalable Digital Watermarking technique is proposed in this paper.

Keywords: Digital Watermark, Scalable, Wavelet, Public Multimedia Network

1. Introduction

In recent years, application of audio·visual has appeared owing to the public multimedia network. Such growth has been apparent in video applications in the network including the video phone, video conference, video e-mail, video streaming, digital TV, HDTV (high-definition TV), VoD (Video on Demand), distance learning, and distance cooperation research and monitoring. Accordingly, the application by audio·visual offers the transmission of a vast volume of data and real time communication [9] as its advantages. However, data storage is carried out in the distributed environment. The seriousness of the problems relating to the reliability and safety of data transmission and storage in the distributed processing and data management has been recognized.

However, the seriousness of the problems regarding the protection of developed multimedia contents in the distributed environment has not been fully recognized. The connection based on the network has been tried for different properties such as resolution, storage capacity, and processing ability, and for the various demands of users deriving from the increased numb of devices available. Furthermore, it is desirable to create contents that can be sent in as small a form as possible so that the server can deliver the information to users within an accessible time. Thus the contents should be scalable in order to suit the devices themselves as well as the users' demands to provide multimedia contents on the network [2, 3, 4].

The advantages of multimedia protection protocol-based Data-Hiding are indicated, rather than the protection of the typical meaning based on the encryption, scrambling and firewall system.

This paper is intended to generate a watermark which can adapt to the frequency domain of each level using the Orthogonal Forward Wavelet Transform (FWT) through a process of trial and error [7], and which can visually recognize the robustness of the watermark containing the copyright information to be included in the original image in order to obtain better results. The emphasis is on a robust watermark which cannot be visually recognized in the original image, and we suggest a scalable watermark algorithm by selecting certain frequency coefficients.

2. Data Protection for Multimedia Contents

As an example of multimedia data protection, the protection method in the electronic commerce system uses the existing encryption technology for the safety of the transaction process, ensuring data secrecy and data authentication and approval. Recently, online services and electronic commerce systems have been able to decipher the sign and perform the processing for contents protection after escaping the user control domain, so that a customer can use precise information of a useful type. Safe transmission, and the control technology of multimedia contents, uses a method that hides data on the basis of encryption techniques and expresses the contents by acquiring a security key through payment by the user. The general concept of use and control technology, such as workstations, personal computers, and DVD players, is to develop alteration and resistant factors in the user's device, perform safe processing, and then control the protected

Manuscript received October 4, 2005; accepted May 26, 2006
Corresponding Author: Jung-Hee Seo
* Dept. of Computer Engineering, Tongmyong University, Busan Korea (jhseo@tu.ac.kr)
** Div. of Electronic, Computer and Telecommunication Engineering, Pukyong National University, Busan Korea (git@pknu.ac.kr)

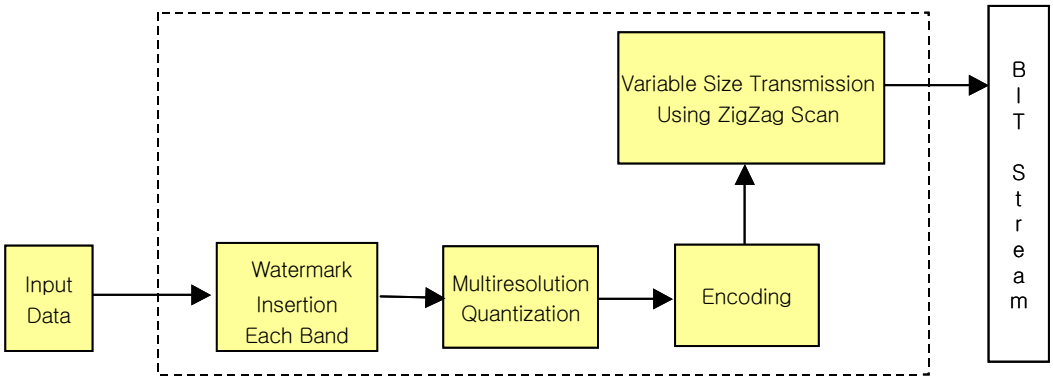

Fig. 1. Scalable Digital Watermarking in the Compression Domain

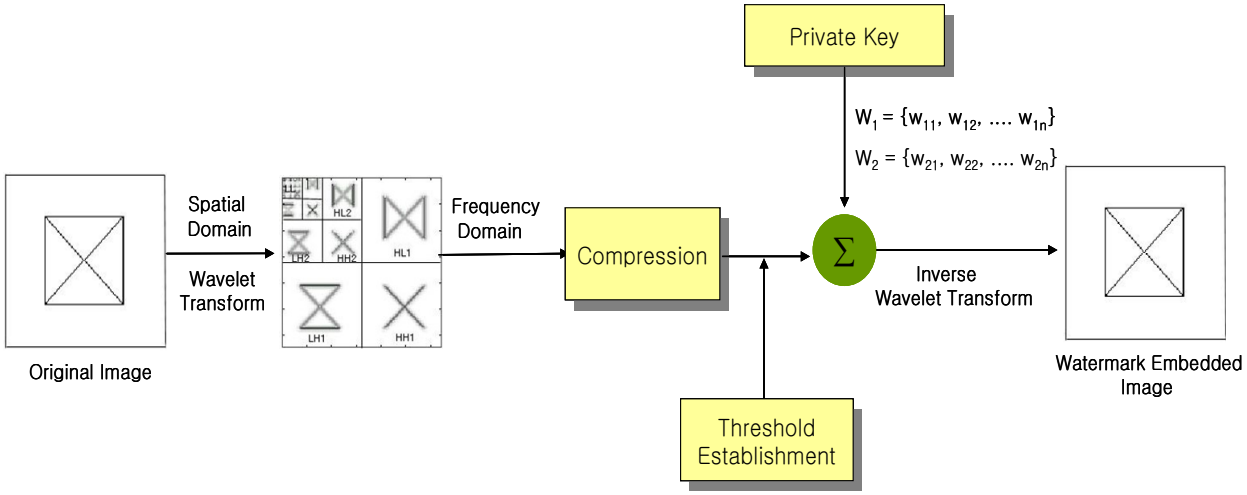

Fig. 2. Watermark Built-in Algorithm

contents. However, today's Internet users transmit or store images without providing credit accessibility for the owners of the multimedia contents. Therefore, digital watermarking technology can solve the problems of ownership protection by having one's own personal information built-in to the multimedia data [5, 6, 7].

2.1. The Required Conditions of Digital Watermark

Because the use of digitalized images and videos has greatly expanded owing to the rapid development of information telecommunication technology, electronic documents on the Web have become greatly popularized and generalized.

Because the objective of the digital watermark is to provide copyright information (which is an incidental information without the visual transformation of image), the copyrighting of an individual's digitalized information could be insisted upon. In general, the essential requisites of digital watermarking are as follows:

The first requisite is robustness. The watermark in intentional and accidental image processing and transformation must not be deleted. That is, it should be possible to extract the watermark containing copyright information from the transformation of filtering, noise addition, and lossy compression, which are the general features of image processing.

The second requisite is security. It should be impossible to delete the watermark by illegal methods in order to prevent the non-owner's illegal manipulation, even though the watermark's insertion procedures are disclosed.

The third requisite is invisibility. It must not be distinguished visually between the original image and the watermark embedded image. The fourth requisite is the absence of ambiguity. There must be a precise method to authenticate the ownership of the image with a built-in watermark; additionally, there must be a method to insert e ownership even when illegal users insert their own watermark into the watermark embedded image.

2.2. Digital Watermark

Digital watermarks can be largely divided into fragile watermarking and robust watermarking.

Fragile watermarking is mainly used for protecting data that cannot be copied, but some problems remain to be solved such as methods for data build-in and authentication, and the types of data to be inserted for data authentication. The protection of a fragile watermark can be guaranteed by maintaining security either by the insertion method or

inserted data.

Robust watermarking emphasizes the robustness of the watermark information built into the digital image. Thus, the extraction of ownership information should be possible even from intentional or unintentional image transformation and lossy compression [5, 6]. As such, robust watermarking is mainly used for the ownership protection of multimedia contents.

This paper suggests a method for multimedia contents to prevent illegal manipulation and to authenticate the ownership of the transformed information. It also emphasizes a robust watermark algorithm that is not visually recognizable on the basis of wavelet transform-based watermarking, and suggests a built-in watermark for developed multimedia contents and scalable digital watermarking in the compression domain. Furthermore, the paper evaluates performance improvement with regard to the robustness of digital watermarking, the bit error rate, and non-visual aspects.

3. Digital Watermarking Algorithm

The provider of multimedia contents requires an efficient mechanism to prove the ownership information of images, but does not want to wait until the whole image has been downloaded to prove one's ownership information. Thus, users can confirm blurred or rough images during their transmission by applying progressive image coding [3].

The concept of scalable watermarking (Wang and Kuo[8]) comprises the expansion of progressive coding and the watermark system. Progressive watermarking should transmit images with a built-in watermark progressively and extract the watermark from the decoded images. Scalable digital watermarking combines with scalable video coding; Therefore, scalable digital watermarking protects contents regardless of the transmission of a specific domain, and can extract a watermark from any domain of scalable contents, while an increase in the scalable domain can also reduce errors in watermark extraction [4].

Therefore, by progressively transmitting the image from a low frequency band to a high frequency band, the receiver can extract the watermark from the part of the image with a built-in watermark, and the bit error rate will decreased as the transmitted data of the images with a built-in watermark increases.

The transform of multimedia data from the spatial domain to the frequency domain used the wavelet transform, which performed the octave-based QMF (Quadrature Mirror Filter). Here, a multi-resolution analysis performs Lowpass Filter and Highpass Filter through QMF.

3.1 Watermark built-in algorithm

The watermarking technique for multimedia contents suggested in this paper generates a private key, the information that can authenticate the ownership, and this generates the watermark cycle. Then, the original image is transformed to the wavelet frequency domain, and the watermark cycle is inserted into a coefficients value that is larger than the threshold value over the entire frequency spectrum, from a low frequency band to a high frequency band.

Thus, the n-bit ASCII-type digital signature $S_{1i} = \{s_{11}, s_{12}, ..., s_{1n}\}$ generates a watermark for the image as in Formula (1). The built-in watermark can define the watermark channel to the original image as a linear combination $p_i(x)$, and n primary orthogonal functions ($p_i(x)$) select the location of the coefficients to be inserted into the frequency domain and define watermark W_1, W_2.

The procedure of digital watermarking transform the original image I into the frequency of freq(I, W_1, W_2), insert watermark on the watermarking channel and then generates C'. The image I' with the watermark embedded, executes a counter transformation from a frequency domain to a spatial domain according to $freq^{-1}(C')$.

The procedure for the built-in watermark is shown in Formula (2) and Formula (3).

$$W_1(x,y) = \sum_{i=1}^{n} p_i(S_i) \tag{1}$$

$$C'(x,y) = freq(I, W_1, W_2) \tag{2}$$

$$I'(x,y) = freq^{-1}(C') \tag{3}$$

Thus, the built-in watermark algorithm suggested in this paper is shown in Figure 2.

The procedure for watermark embedding according to this paper is as shown in Table 1.

Wavelet-based compression is performed in the frequency domain, and when the reverse wavelet transform is performed from the frequency domain to the spatial domain after performing frequency quantization and encoding on the coefficients in the frequency domain, an image with a built-in watermark is generated.

3.2. Watermark Extraction and Authentication Algorithm

As shown in figure 3, as the method for watermark extraction and authentication, the original image (I) and transformed image (I") are converted to Wavelet Transform and are then transformed into the hierarchy structure which is a pyramid structure. Then, the difference between the frequency domain of the original image and that of the transformed image is calculated.

At this time, the watermark pattern (W') in the transformed image can be extracted. The extracted watermark pattern (W') is divided by a 32×32 Block. In the same manner, the original watermark pattern (W) is divided by a 32×32 Block, and then the correlation for each block is calculated.

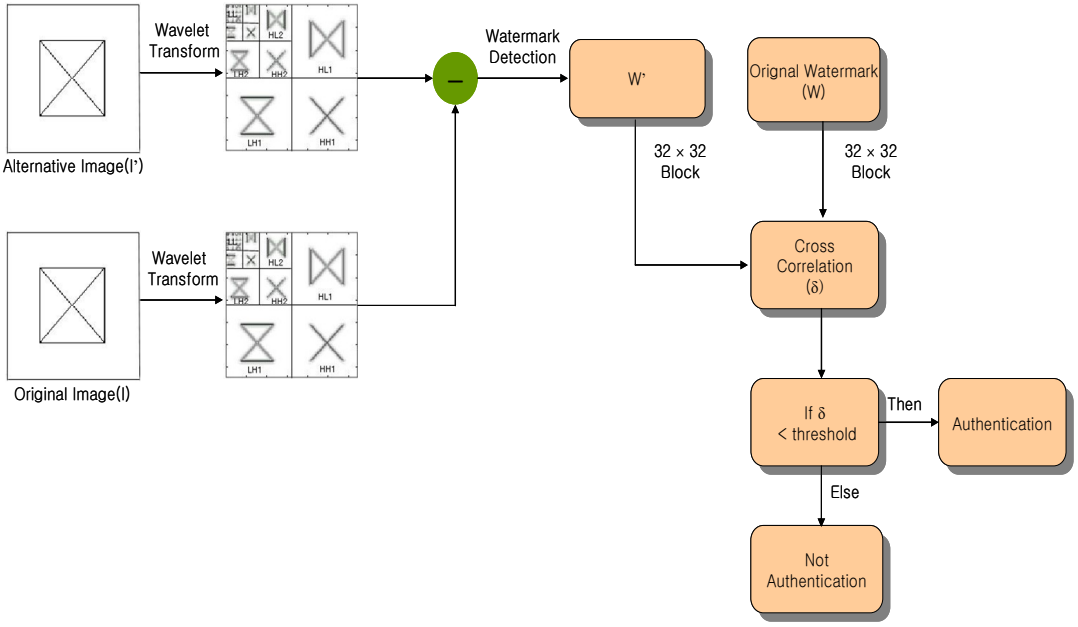

Fig. 3. Watermark Extraction and Authentication Algorithm

Table 1. Procedure for a Built-in Watermark

1. Initialize variables
   - I: Original Images.
   - I': Watermark built-in images.
   - W_{1i}, W_{2i}: Watermark cycles, W_{1i}, W_{2i} , i=1, ..., n.
   - S_i: Digital signature, i=1, ..., n.
   - C: Coefficient values of I in the frequency domain.
   - C': Coefficients embedded watermark in the frequency domain.
   - FWT: Forward Wavelet Transform.
   - IWT: Invert Wavelet Transform.
2. Create Watermark pattern of $W_1(x, y)$ and $W_2(x, y)$ by $\sum_{i=1}^{n} p_i(S_i)$.
3. Compress image using sparse coding after performing FWT on I.
   C(x, y) = FWT(I(x, y))
   C'(x, y) = Compression(C(x, y)).
4. Perform watermark embedding in wavelet coefficients.
5. Perform each-level invert FWT and transformed the spatial domain
   I'(x, y) = IWT(C'(x, y))

4. Results and Analysis

This experimental image used MATLAB in an environment with Windows 2000 server, and used 256×256 Lena, Pepper, Baboon images. Wavelet transform was performed using Daubechies Wavelet to change the images into progressive structures and the ownership information was inserted.

Figure 4 shows the process of executing wavelet compression on the watermark-embedded image shown in the upper-right corner of the figure. The wavelet transform according to each frequency domain was executed on the watermark-embedded image shown in the lower-left corner of figure 4. The lower-right image shows the results of executing sparse coding for wavelet compression transformation.

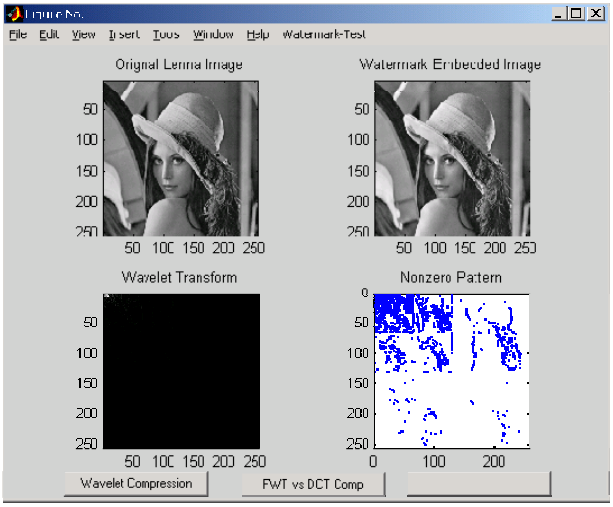

Fig. 4. Perform Wavelet Compression on the Watermark Embedded Image of the Lena Image

Figure 5 indicates a 95% Wavelet-compressed image in the watermark-embedded image after Figure 4.

The image on the lower part shows the watermark-embedded image and the results of the visual extraction of embedded watermarks within the 95% wavelet compressed multimedia.

Figure 6 indicates the rate of error in the image where compression is conducted in the watermark-embedded image in order to analyze the quality performance of Wavelet and DCT in the results of Figure 5. As shown in the figure, Wavelet is superior to DCT in terms of image quality.

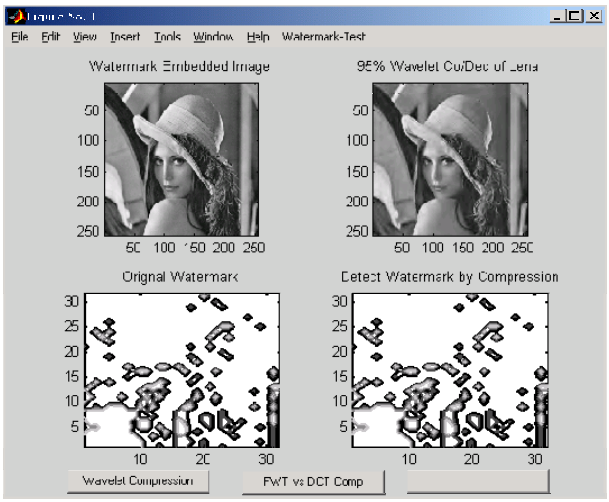

Fig. 5. Watermark Extraction after Performing Wavelet Compression on the Watermark Embedded Image

Figure 7 showed the correlation between each block for extracting the watermark from intentionally transformed test images. The comparison between the watermark cycle installed in the original image and that extracted from the transformed image showed that the correlation of the embedded watermark was 1, demonstrating the consistency between the extracted watermark and the built-in watermark. While the gamma correlation of the Pepper and Baboon images were 0.33 and 0.44, respectively, and the correlation of random noise in the Lena image was as low as 0.53, the correlation in other image transforms was relatively higher, which satisfy the permissible error ratio of 0.05 and thus can be authenticated for ownership.

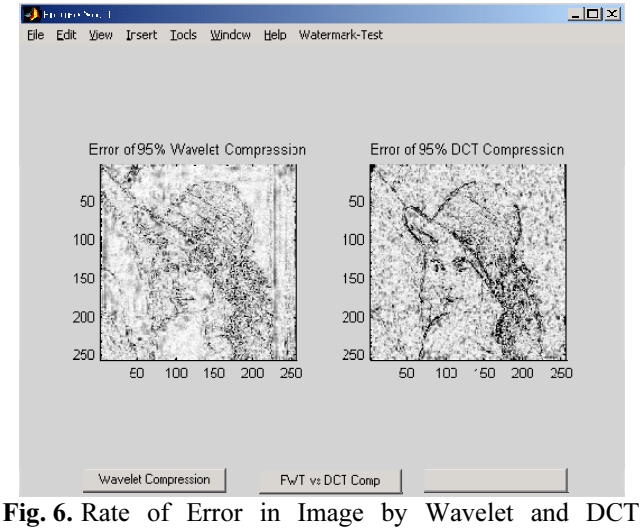

Fig. 6. Rate of Error in Image by Wavelet and DCT Transform

Then, PSNR (Peak Signal to Noise Ratio) was used on the original image and the transformed image with a built-in watermark to evaluate the picture quality of the image. Figure 8 showed that all of the 3 test images had a lower picture quality of 13dB~21dB in image transforms such as brightness and gamma correlation for the 95% compression rate of tested images, but better picture quality of 26dB~33dB in image transforms such as median, blur, sharpen, and despeckle.

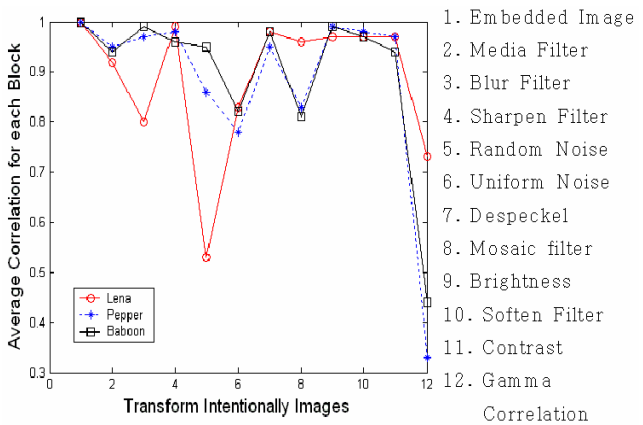

Fig. 7. Correlation for each Block for Extracted Watermark

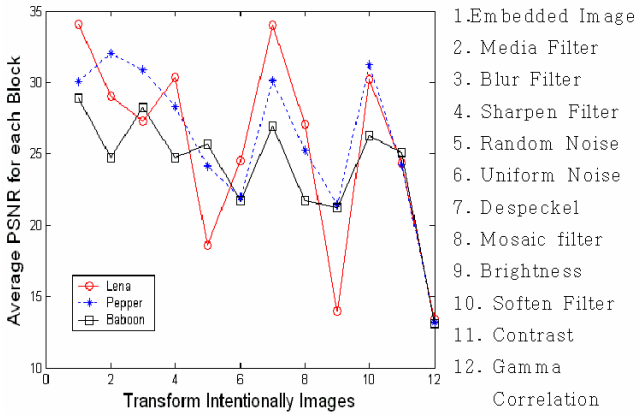

Fig. 8. Quality of the Image using PSNR

5. Conclusion

This paper is intended to generate a watermark which can adapt well to the frequency domain of each level using the Orthogonal Forward Wavelet Transform (FWT) through trial and error, and which can visually recognize the robustness of the watermark containing the copyright information to be included in the original image in order to obtain better results. The emphasis is on a robust watermark which cannot be visually recognized in the original image, and we propose a scalable watermark algorithm by selecting certain frequency coefficients.

Then, it is possible to efficiently provide multimedia contents on the public network by progressively selecting contents to be transmitted which suit the contents to the performance of devices and user demands. Also, it proposes scalable digital watermarking and controls the calculation properly by selecting the scale to be decoded, and emphasizes a robust watermark algorithm that is not visually recognizable, using Orthogonal Forward Wavelet Transform (FWT). Therefore, as the results of this paper, a watermark insertion method that can extract built-in

watermark from the intentional image transform and the watermark key was generated. This should guarantee watermark information extraction in the partial domain of the image and minimize the problems concerning intellectual property rights or the ownership of multimedia contents on the Internet.

References

[1] B. Girod, F. Hartung and U. Horn, " Multiresolution Coding of Image and Video Signals," Proceedings European Signal Processing Conference (EUSIPCO 98), sept. 1998.

[2] U. Horn and B. Girod, "Scalable video transmission for the internet," Computer Network and ISDN Systems, Nov. 1997.

[3] T. P-C. Chen and T. Chen, "Progressive Image Watermarking," Proc. of IEEE Intel. Conf. on Multimedia and Expo. July 2000.

[4] A. Piper, R. Safavi-Naini, and A. Mertins, "Coefficient Selection methods for Scalable Spread Spectrum Watermarking," IWDW 2003, pp. 235-246, 2004.

[5] M. D, Swanson, Bin zhu, A.H.Tewfik, "Transparent robust image watermarking," Proceeding of the IEEE International Conference on Image Processing, vol.3, pp.211-214, 1996.

[6] D. Kundur, D. Hatzinakos, "A robust digital image watermarking method using wavelet-based fusion," IEEE, pp. 544-547, 1997.

[7] X. Xia, C. G. Boncelet, G. R. Arce, "A multiresolution watermark for digital image," Proceedings of the IEEE International Conference Image Processing, vol.3, pp. 548-551, 1997.

[8] M.K. Uz, M. Vetterli, and D.J. LeGall, " Interpolative multiresolution coding of advanceed television with compatible subchannels," IEEE Trans. on Circuits and Systems for Video Technology, Mar. 1991.

[9] S. Voloshynovskiy, F. Deguillaume, O. Koval and Thierry Pun, "Information-theoretic data-hiding problems," International Journal of Image and Graphics, 5, 1, pp. 1-31, 2005.

[10] A. Piper, R. Safavi-Naini, and A. Mertins, "Coefficient Selection methods for Scalable Spread Spectrum Watermarking," IWDW 2003, pp. 235-246, 2004.

Jung-Hee Seo

She received a B.S. degree in Computer Science from Silla University in 1994, M.S. degree in Computer Science and Statistics from Kyungsung University in 1997, and Ph.D. degree in Electronic Commerce System from Pukyong National University in 2006. She has been a full-time instructor with the Department of Computer Engineering, Tongmyong University, since 2000. Her research interests include Remote Education, Multimedia, Image Processing, Information Protection.

Hung-Bog Park

He received B.S and M.S. degree in Computer Engineering from Kyungpook National University in 1982 and 1984. Ph.D. degree in Computer Science from Inha University in 1995. Since 1996, he has been a professor with the Division of Electronic, Computer and Telecommunication Engineering, Pukyong National University. His research interests include Multimedia Application, Remote Education, Industry Automation, Programming Language and Compiler.