Analysis Method of Digital Forgeries on the Filtered Tampered Images

Jin-Tae Kim, Chang-Hee Joo, *Member, KIMICS*

***Abstract*— Digital forensics is the emerging research field for determining digital forgeries. Key issues of the tampered images are to solve the problems for detecting the interpolation factor and the tampered regions. This paper describes a method to detect the interpolation factors and the forged maps using the differential method and fast Fourier transform (FFT) along the horizontal, vertical, and diagonal direction, respectively from digital filtered tampered images. The detection map can be used to find out interpolated regions from the tempered image. Experimental results demonstrate the proposed algorithm proves effective on several filtering images by Adobe Photoshop™ and show a ratio of detecting the interpolated regions and factors form digital filtered composite images.**

***Index Terms*— Digital forgery, Differential method, Interpolation factor, Detection map, Fast Fourier transform.**

I. INTRODUCTION

Digital image forensics is one of the emerging research fields for determining digital forgeries. Most of digital image forgeries are created by Adobe Photoshop™. The filters among functions of Adobe Photoshop use also a lot of images for reproduction. The filtered forged images consist of the interpolated regions. An important task of the tampered image is to detect an interpolation factor and regions. Therefore, key issues for forgery detectors are to solve the problems of interpolation technologies between tampered pixels for determining the interpolation factor and the tampered regions [1]-[5]. The detectors should allow us to estimate the accurate interpolation factor and the robust interpolated region from the forged image. This paper deals with detecting traces of the interpolation for forged images produced by the filters of Adobe Photoshop.

A few researches have been published in the field of digital forgery. A.C. Gallagher [4] addressed that linear and cubic interpolated signals were detected for periodicity by computing the variance function of their second order derivative. The periodicity can be simply found by estimating the fast Fourier transform (FFT) of an averaged signal obtained from the second derivative of the investigated signal. However, the major weakness of this method can be applied only to the entire zoomed-in area except for digital composite image.

A. C. Gallagher and T. Chen extended the proposed algorithm by [11] to examine images locally [6]. The extended local version estimated the variance of each pixel by using Maximum Likelihood Estimation (MLE). Because this method depends on using many pixel samples to estimate variance statistics, the detection accuracy is affected along a central square window size. Therefore, the disadvantages of this extended local version are that reported lower detection accuracy in a small 64x64 region of the tampered image and cannot detect the resampling factors in downsampled image.

A.C. Popescu and H. Farid proposed that each interpolated image was precisely determined for the same linear combination factor of its adjacent two neighboring pixels for the entire re-sampled one-dimension (1-D) and 2-D signal. The first proposed approach is to detect re-sampled factors and the probability map for forged area using the EM (expectation-maximization) algorithm and the statistical method for gray-scaled images [1], [2] and the second one is to detect traces of digital tampering in lossless and loss compressed image for eight different color filter array (CFA) interpolation algorithms from CFA interpolated images [3]. Unfortunately, these approaches can detect only counter-attacks such as the first interpolation consisting of the tampered image.

B. Mahdian and S. Saic [5] described that specific periodic properties presented in the covariance structure of interpolated signals and their derivatives. This method is used for the larger window size (128x128) in determining the interpolated portions. However, the approach cannot clearly detect the smaller interpolated portions.

Another work concerned with the interpolation detection is proposed by S. Prasad and K. R. Ramakrishnan [11]. The authors only presented that the second derivative of an interpolated signal produced detectable periodic properties. The periodicity is detected from the frequency domain by analyzing a binary signal obtained from zero-crossings of the second derivative of the interpolated signal. Unfortunately, this approach is similar to A. C. Gallagher [4] and cannot clearly detect the resampling factor for the resampled region of the digital composite image.

In this paper, we present a new method to detect the interpolation factors and the forgery areas using the

Manuscript received November 29, 2010; revised December 20, 2010; accepted January 1, 2011.

Jin-Tae Kim is with the Department of Computer and Information Engineering, Hanseo University, ChungNam 356-756, Korea. (Email: jtkim@hanseo.ac.kr)

Chang-Hee Joo is with the Department of Computer Control, Bucheon University, 424 Shimgok Dong, Bucheon City, Korea. (Email: eyeineye@bc.ac.kr)

differential method and FFT along the horizontal, vertical, and diagonal direction, respectively, from digital filtered composite images. Our approach for the interpolation factor is extended from the method proposed by A.C Gallagher [4]. According to scanning along the horizontal, vertical, and diagonal direction, interpolated images respectively, we can detect easily the interpolation factor and tampered region for the optimal window size (64x64) from forged image.

II. THE PROPOSED ALGORITHM

As shown in Fig. 1, the proposed algorithm consists of 5 phases in order to detect interpolation factors and the tampered regions from the digital composite images.

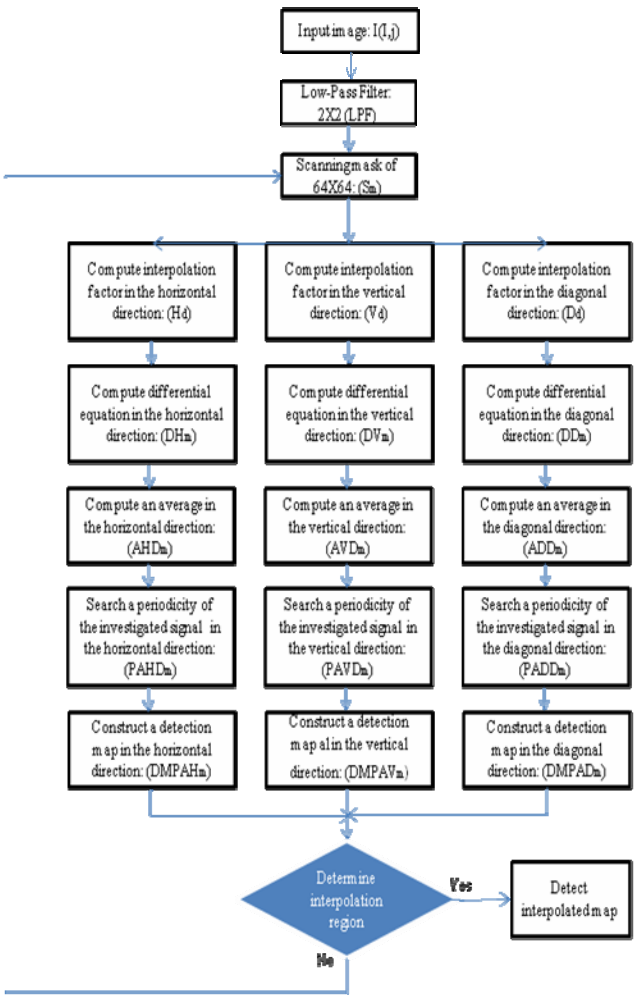


Fig. 1. Overall of the proposed algorithm

The first phase is the preprocessing step. First of all, this phase is to convert digital input image to a grayscale for detecting the interpolated images. The grayscale image *I(i,j)* is convolved with a low-pass filter *H* in order to accurately detect the interpolated forgery region between the original image and the interpolated one, and remove the noise from the image.

$$LPF = I(I,j) * H \tag{1}$$

The low-pass filter applies a 2x2 size mask. After processing the filter, the interpolated image can be eliminated by a steep intensity transition of the object from the composite image.

The second one involves the process of the scanning mask of 64x64 sizes. To find all interpolated regions, the image *LPF* can be tiled by overlapping blocks, S_m of 64x64 sizes. The blocks can be horizontally scanned along intervals of 8 pixels rightwards from the upper left corner to the bottom right one for the image. Each block can be analyzed by the proposed algorithm for the region of the image.

The third one is to estimate interpolation factors by using differential equation for the horizontal, vertical, and diagonal direction, respectively into each block of 64x64 sizes. We can detect the presence of the periodic properties for re-sampling in this phase. The third phase again consists of 3 steps:

Step 1 is to compute the differential equation in all directions of the preprocessed image along the horizontal, vertical, and diagonal direction, respectively. This approach is performed by the derivative operator calculating differences between neighbor pixels of row, column, and diagonal direction, respectively. The used horizontal derivative kernel H_d is 1x3 size of [-1, 0, 1], and the used vertical derivative kernel V_d is 3x1 size of [-1; 0; 1]. The diagonal derivative kernel D_d is used for 3x3 sizes of [1,0,-1; 0,0,0; -1,0,1;]. The second derivative signals of all directions are computed for $0 \le i < r$ and $0 \le j < c$ with the following differential equation:

$$\begin{aligned} DH_m &= LPF * H_d \\ DV_m &= LPF * V_d \\ DD_m &= LPF * D_d \end{aligned} \tag{2}$$

where r is the number of rows for the image, and c is the number of columns for the image. DH_m, DV_m, and DD_m denote the second derivative row, column, and diagonal direction, respectively.

Step 2 is to compute an average for all directions from the second derivative signals. The absolute values of the second derivative row, column, and diagonal directions, respectively are averaged together in order to obtain the mean of the second derivative trace:

$$\begin{aligned} AHD_m &= \sum |DH_m| \\ AVD_m &= \sum |DV_m| \\ ADD_m &= \sum |DD_m| \end{aligned} \tag{3}$$

where AHD_m, AVD_m, and ADD_m represent the mean second derivative row, column, and diagonal direction, respectively.

Step 3 is to search for a periodicity of the investigated

signal from the previous one. To emphasize and easily detect the periodicity, the magnitudes of FFT are computed from the mean of the second derivative signal. If the image has been interpolated, the investigated signal exhibits a periodicity related with the interpolation rate. The periodicity can be known from the frequency domain of the analyzed image. The FFT of the mean of the second derivative signal gives as follows:

$$\begin{aligned} PAHD_m &= FFT[AHD_m] \\ PAVD_m &= FFT[AVD_m] \\ PADD_m &= FFT[ADD_m] \end{aligned} \quad (4)$$

where $PAHD_m$, $PAVD_m$, and $PADD_m$ illustrate the FFT of the mean of the second derivative row, column, and diagonal direction, respectively. The magnitudes of FFT are represented as a spectrum for the image and ignored for the phase of FFT. The observed periodic properties for the FFT spectrum are divided into three types:

Type 1) detecting aliasing: If the distortion artifacts in the shape of a valley exhibit near 0.5 normalized frequency, it means that the image has been down-sampling.

Type 2) detecting peaks: If distinct peaks for normalized frequency appear, it means that the image has been up-sampling. The peak f_p is the candidate peak having the greatest magnitude. The interpolation factor is estimated from the peak f_p. The relationship between the peak and interpolation factor is given as follows:

$$P = 1 / f_p \quad (5)$$

where P denotes the interpolation factor and f_p represents the peak magnitude of the FFT normalized frequency.

Type 3) detecting indistinct peaks: If the peak detection yields nothing, it means that no interpolation has been performed on the image.

The fourth one is to construct a detection map of the forgery for detecting interpolated regions. Detecting maps of the forgery consist of the interpolation factors measured along the horizontal, vertical, and diagonal directions, for the blocks of size 64x64. In this paper, the magnitudes of interpolation factors for the detection map of the forgery are classified by the colors red, blue, and green. It is possible to distinguish the colors used between adjacent blocks for detection map of the forgery. By using the color comparison of detection map of the forgery, we can accurately detect the interpolated regions. If the distinguished region makes a semantic sense to the observer, the image determines accurately the tampered region. We can then verify the first forgery in this phase.

The fifth one is finally to determine candidates for interpolated regions from digital composite images. For detection map which is estimated from the proposed algorithm, we can surely divide the digital composite image into the areas M_1 and M_2. Here, M_1 is the interpolated region and M_2 is the non-interpolated region. The magnitudes of interpolation factors are estimated for each area and then we determine whether the areas are up-sampling or down-sampling. Therefore, we can affirm the second forgery detection for region segmentation in this phase.

III. EXPERIMENTAL RESULTS

Various types of the filtered forged images have been used for the experimental mages. The experimental resolution is 512x512 images. These are classified into arbitrary 100 TIFF images using interpolations by the filters of Adobe Photoshop™. We create test images according to the scaling factors. All of the experiments were performed using Matlab™. The interpolation factors are estimated for the horizontal, vertical, and diagonal directions, respectively. A detection map of the forgery consists of the measured interpolation factors for the 64x64 block size. Results of the detection map are used as a tool for detecting forgery of the proposed algorithm. In order to detect tampered regions in a digital composite image, we apply scanning intervals at 8 pixels. As shown in Fig. 2, Fig. 2(a) shows a *Rhinoceros* image which is a scaled-up 2 times for an interpolated tampered image. Fig. 2(b), (c), and (d) illustrate a detection map of forgery image for the horizontal, vertical, and diagonal direction, respectively. Therefore, we can know that the proposed approach shows the detection of the interpolation factor and region for the tampered image.

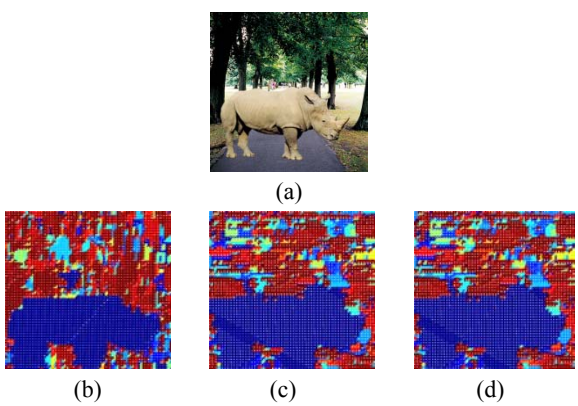


Fig. 2. (a) An interpolated tampered image for scaled-up 2 times, (b) A detection map of forgery image for the horizontal direction, (c) A detection map of forgery image for the vertical direction, (d) A detection map of forgery image for the diagonal direction.

Fig. 3, Fig. 4, Fig. 5, Fig. 6, and Fig. 7 represents experimental results for blur filters such as lens blur filter, blur filter, motion blur filter, radial blur filter, and smart blur filter. The blur filters have the property of low pass filter. The filters are difficult to detect the interpolation coefficients for the forgery images. However, we can know that the diagonal among the directions to scan the

64x64 block size shows the best results of the interpolation region for the tampered image.

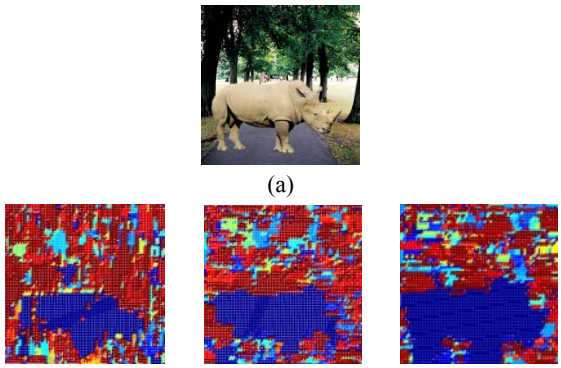


Fig. 3. (a) A forgery image for applying by lens blur filter, (b) A detection map of horizontal direction, (c) A detection map of vertical direction, (d) A detection map of diagonal direction.

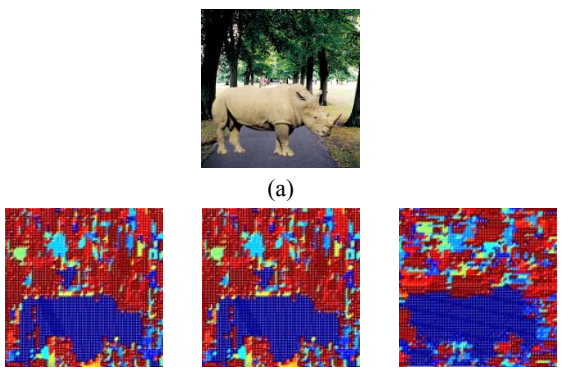


Fig. 4. (a) A forgery image for applying by blur filter, (b) A detection map of horizontal direction, (c) A detection map of vertical direction, (d) A detection map of diagonal direction.

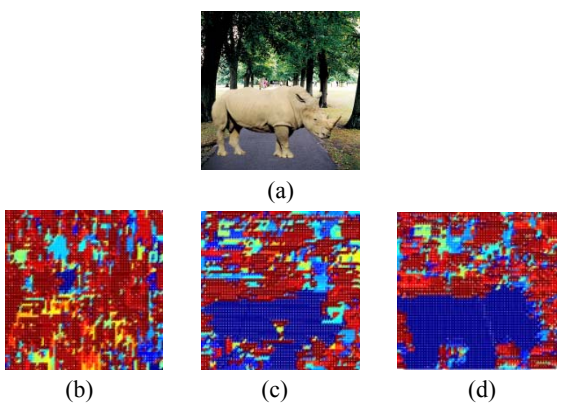


Fig. 5. (a) A forgery image for applying by motion blur filter, (b) A detection map of horizontal direction, (c) A detection map of vertical direction, (d) A detection map of diagonal direction.

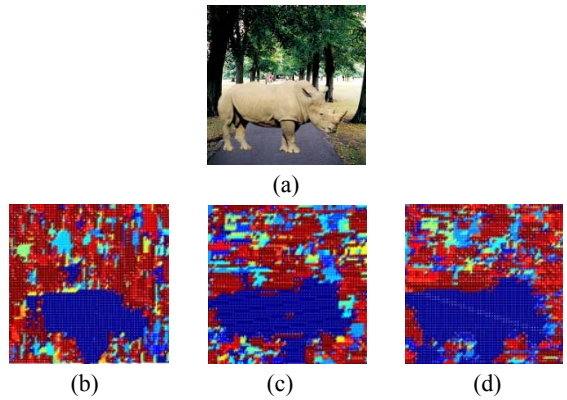


Fig. 6. (a) A forgery image for applying by radial blur filter, (b) A detection map of horizontal direction, (c) A detection map of vertical direction, (d) A detection map of diagonal direction.

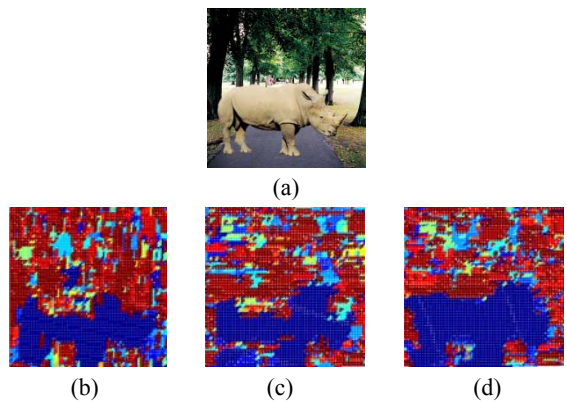


Fig. 7. (a) A forgery image for applying by smart blur filter, (b) A detection map of horizontal direction, (c) A detection map of vertical direction, (d) A detection map of diagonal direction.

Fig. 8, Fig. 9, and Fig. 10 show experimental results for noise filters such as add noise filter, despeckle filter, and dust & scratches filter.

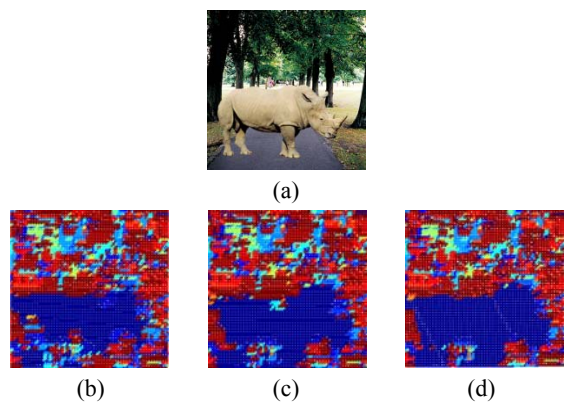
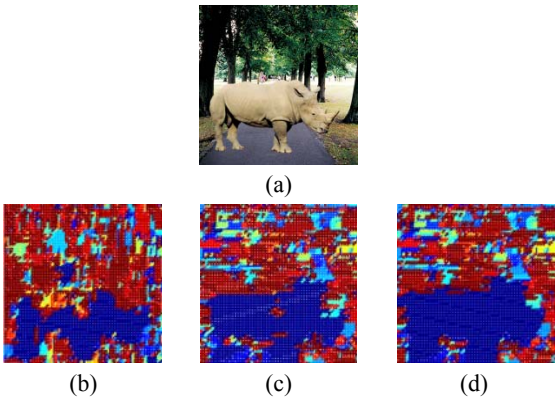
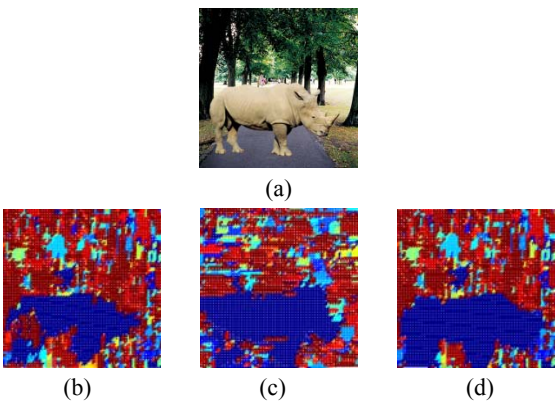


Fig. 8. (a) A forgery image for applying by add noise filter, (b) A detection map of horizontal direction, (c) A detection map of vertical direction, (d) A detection map of diagonal direction.



(a) (b) (c) (d)

Fig. 9. (a) A forgery image for applying by despeckle filter, (b) A detection map of horizontal direction, (c) A detection map of vertical direction, (d) A detection map of diagonal direction.



(a) (b) (c) (d)

Fig. 10. (a) A forgery image for applying by dust & scratches filter, (b) A detection map of horizontal direction, (c) A detection map of vertical direction, (d) A detection map of diagonal direction.

These results demonstrate the proposed algorithm is robust for noise filters from the tampered image. Therefore, we can know that the diagonal among the directions to scan the 64x64 block size shows the best results of the interpolation region for the tampered image.

IV. CONCLUSIONS

We presented the new method to detect the interpolation factors and the forgery areas using the differential method and FFT along the horizontal, vertical, and diagonal direction, respectively, from digital filtered composite images. We also have demonstrated the performances of the proposed algorithm on a standard test set of 1000 images. The proposed approaches performed well in detecting the interpolation factors and the tampered regions using the blur and the noise filter, respectively. Experimental results show that the proposed method can detect the interpolation factors for each interpolation technology. The detection map of our algorithm could accurately detect tampered regions from a digital composite image for the diagonal direction. We can know that the detection map of forgery represents the properties for each interpolation technique. Future works have been studied for Internet images on the on-line.

REFERENCES

[1] A. Popescu and H. Farid, "Exposing digital forgeries by detecting traces of re-sampling," *IEEE Trans. Signal Processing*, vol. 53, no. 2, pp.758-767, 2005.

[2] A. Popescu and H. Farid, "Statistical tools for digital forensic," *Proc. 6th International Workshop on Information Hiding*, pp. 128-147, 2004.

[3] A. Popescu and H. Farid, "Exposing digital forgeries in color filter array interpolated images," *IEEE Trans. Signal Processing*, vol. 53, no. 10, pp. 3948-3959, 2005.

[4] A. C. Gallagher, "Detection of linear and cubic interpolation in JPEG compressed images," *Proc. 2nd Canadian Conference on Computer and Robot Vision*, pp. 65-72, 2005.

[5] B. Mahdian and S. Saic, "Blind authentication using periodic properties of interpolation," *IEEE Trans. Information Forensics and Security*, vol. 3, pp. 529-538, 2008.

[6] B. Mahdian and S. Saic, "Blind methods for detecting image fakery," *Proc. IEEE International Conference on Security Technology*, pp. 280-286, 2008.

[7] J. B. Lee, S. B. Youn, Y. I. Yoon, K. S. Doo, and D. H. Har, "A study on detecting digital forgeries using an interpolation," *J. The Society of Korean Photography*, vol. 16, pp. 20-29, 2007.

[8] G. S. Song, Y. I. Yun, and W. H. Lee, "Analysis on digital image composite using interpolation," *J. Korea Multimedia Society*, vol. 13, no. 3, pp. 457-466, 2010.

[9] Y.-I. Yun, G.-S. Song, and J.-T. Kim, "Detecting digital forgeries from the filtered tampered images," *Proc. International Conference on Information and Multimedia Technology*, vol. 1, pp. 21-24, 2010.

[10] A. C. Gallagher and T. Chen, "Image authentication by detecting traces of demosaicing," *Proc. IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, pp. 1-8, 2008.

[11] S. Prasad and K. R. Ramakrishnan, "On resampling detection and its application to image tampering," *Proc. IEEE International Conference on Multimedia and Exposition*, Toronto, Canada, pp. 1325-1328, 2006.

Jin-Tae Kim received his B.S., M.S., and Ph.D. degree in Electronics Engineering from Chung Ang University, Seoul, Korea, in 1987, 1989, and 1993, respectively. He worked at Institute of Industrial and Technology at Chung Ang University from 1993 to 1995. Since 1995 he has been a faculty member of Department of Computer and Information Engineering, Hanseo University. From January 2008 to January 2009, he was a visiting professor at the University of North Carolina at Charlotte, USA. His research interests include image compression, augment reality, face recognition, and digital watermarking.

Chang-Hee Joo received his B.S., M.S., and Ph.D. degree in Electronics Engineering from Chung Ang University, Seoul, Korea, in 1982, 1984, and 1993, respectively. He worked for Samsung Electronics from 1984 to 1986. Since 1990 he has been a faculty member of Department of Computer Control, Bucheon University. His research interests include image processing, thermal imaging, microcontroller application.