International Journal of Security and Its Applications
Vol.8, No.2 (2014), pp.211-220
http://dx.doi.org/10.14257/ijsia.2014.8.2.22

Block Shuffling Approach for Contents Protection

Gwanggil Jeon

Department of Embedded Systems Engineering, Incheon National University
119 Academy-ro, Yeonsu-gu, Incheon 406-772, Korea
gjeon@incheon.ac.kr

Abstract

A scrambling approach is a method which is employed on almost all commercially manufactured system including image and video systems. In this paper, we proposed a new scrambling approach which uses random process. We first separate blocks into certain size, and relocated them randomly. This is block shuffling which is proposed for the purpose of randomizing the block location. The relocated blocks have three channels, R, G, and B, and each color channel's luminance values are complemented. Experimental results show that the proposed method well-protect contents.

Keywords: *Image scrambling, video scrambling, contents protection*

1. Introduction

A valuable content scrambling approach is a raising issue as protecting contents copyright is important. Image and video scrambling is well employed, and its general way is to hide unwanted information and disclose uninterpretable image and video. There have been many methods regarding image and video scrambling [1-11].

Traditional works took into account the application of conventional cryptographic approaches to encode the code-stream output from their compression [12-14]. However, there is complexity issue. When they are examined to other types of information, image or video data may be characterized by a very high bitrate, which makes the product expensive [15]. Thus, traditional scrambling methods are known to be complex, and simple method is needed.

In this paper, we proposed a new scrambling approach which uses random process. First of all, we separate image or video with certain sized blocks, and relocated all blocks randomly. This process is block shuffling which is presented for the purpose of randomizing the block location. As our test color images have three channels, R, G, and B, each color channel's luminance values are complemented.

The rest of this report is composed as follows. In Section 2, we describe the proposed method and its flowchart. Section 3 shows simulation results. Conclusion remarks are drawn in Section 4.

2. Proposed Method

Figure 1 shows the block diagram of the proposed scrambling approach. The proposed approach consists of following stages.

(1) Given color image/video

(2) Keys

(3) Image separation with NxN block size

ISSN: 1738-9976 IJSIA

(4) Block shuffling by random process

(5) Color channel complementation by random process

(6) Contents display to subscribers or scrambled displayed to viewers

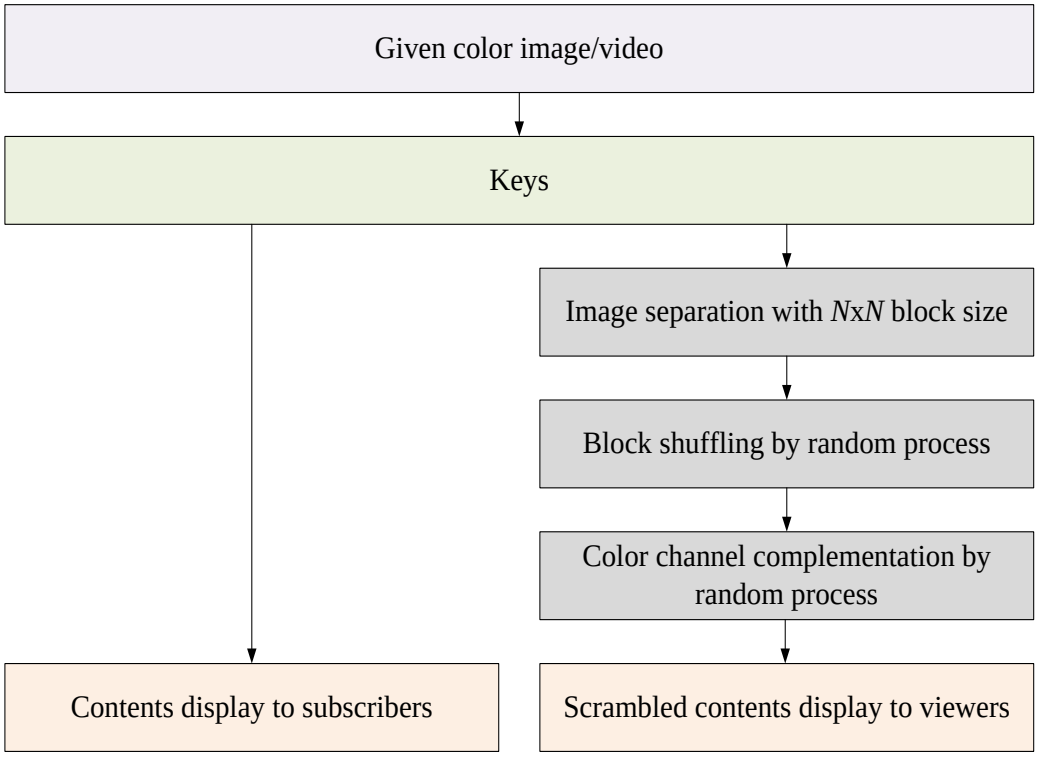


Figure 1. Block Diagram of the Proposed Method

Here are our scenarios. When an image/video stream is provided, first the system yields a key to discern whether the viewer is subscriber. Once the viewer is known as subscriber, unchanged contents are provided to display on the device. However, if the viewer is determined is not a subscriber, then scrambling process is applied.

The system firstly separates image/video with certain sized blocks (*N*x*N*). The size *N* can be any number with 2^n, where *n* is integer number. Then the system shuffles the blocks with the rule of random process. System designer can adopt any kinds of random process, and we used Matlab function magic for our system. The function magic(n) is an *n*-by-*N* matrix generated from the integers, one through n^2 with equal column, row, and diagonal sums. Function magic(n) generates logical magic squares for all $n > 0$ except $n = 2$. For example, answer of magic(4) is,

$$\text{answer}=\begin{bmatrix} 16 & 2 & 3 & 13 \\ 5 & 11 & 10 & 8 \\ 9 & 7 & 6 & 12 \\ 4 & 14 & 15 & 1 \end{bmatrix} \quad (1)$$

As fuction magic(*n*) always returns the same results, we also provide following shuffling rule: (1) We general a sequence of random numbers, (2) then, we scan the blocks in the image by the ascending (or descending) order.

Finally each color channel of the shuffled blocks is changed with the rule of random process as shown in Eq. (2).

$$\begin{aligned} &\text{if } \{rand() \text{ is smaller than } \kappa_R\}, \\ &\quad \text{R channel intensity is } imcomplement(\text{R}) \\ &\text{otherwise}, \\ &\quad \text{R channel is unchanged} \end{aligned} \tag{2}$$

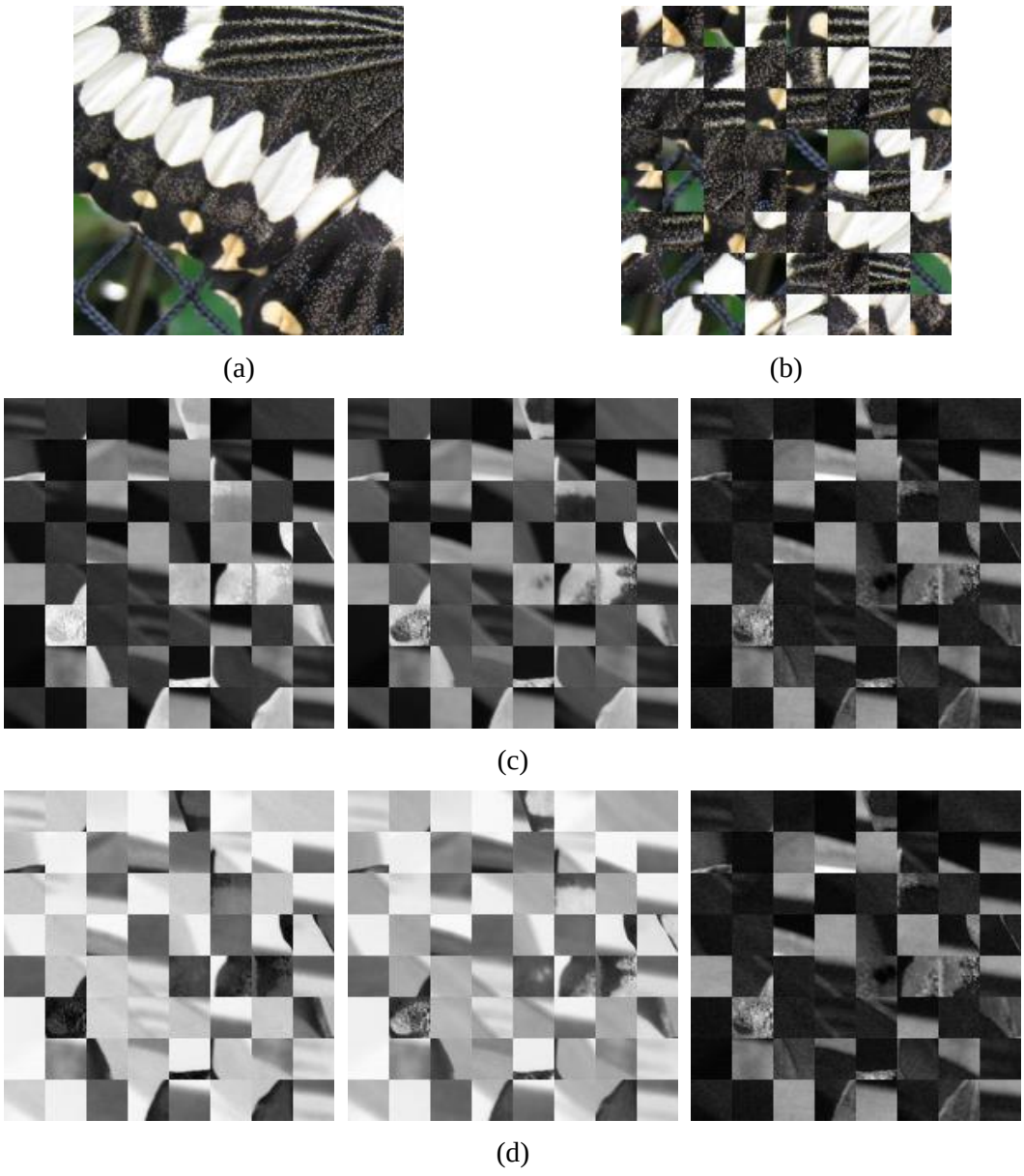
This rule can be applied to other color channels, green and blue.

$$\begin{aligned} &\text{if } \{rand() \text{ is smaller than } \kappa_G\}, \\ &\quad \text{G channel intensity is } imcomplement(\text{G}) \\ &\text{otherwise}, \\ &\quad \text{G channel is unchanged} \end{aligned} \tag{3}$$

$$\begin{aligned} &\text{if } \{rand() \text{ is smaller than } \kappa_B\}, \\ &\quad \text{B channel intensity is } imcomplement(\text{B}) \\ &\text{otherwise}, \\ &\quad \text{B channel is unchanged} \end{aligned} \tag{4}$$

where *rand*() generates uniformly distributed pseudorandom numbers and parameters κ_R, κ_G, and κ_B are pre-determined threshold values. The maximal and minimal possible outcomes are 1 and 0, and the sequence of numbers generated by *rand*() is decided by the internal state of the uniform pseudorandom number generator that underlies *rand*().

Figure 2 shows an examples of original McM images and its scrambling processed images. Figure 2(a) shows the original McM #1 image which is assumed to the original contents. Figure 2(b) shows its shuffled image. When viewers are determined as non-subscriber, scrambling process is followed. Figures 2(c) and 2(d) are results of shuffling step and function *imcomplement*() step.



(a) (b)

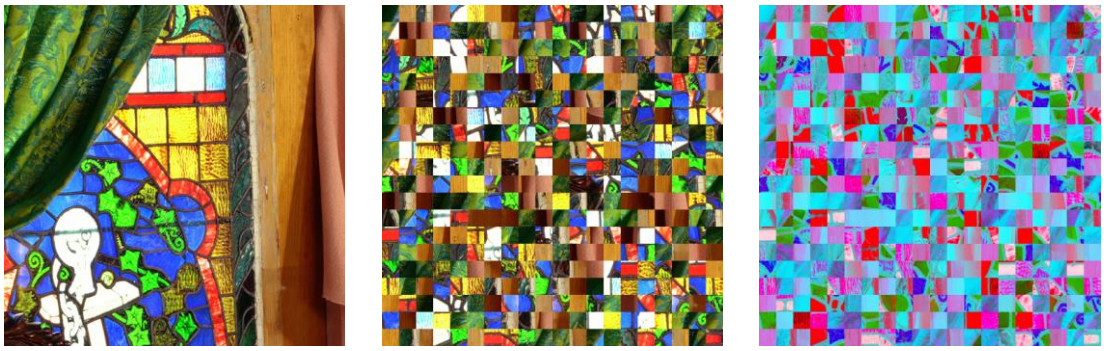
(c)

(d)

Figure 2. (a) Original McM #1 Image; (b) and its Shuffled Image; (c) Results of Shuffling Step; (d) Results of *imcomplement*() step. Note that Left, Mid, and Right Images are Red, Green, and Blue Channels, Respectively

3. Simulation Results

In this section, we provide simulation results which were obtained with the proposed method on McM test imageset. Four images were used for comparison: #1, #9, #14, and #17. Results images on those test images are shown in Figs. 3-6. Parameters κ_R, κ_G, and κ_B were set to 0.45, 0.45, and 0.45, respectively, and all values were obtained empirically.

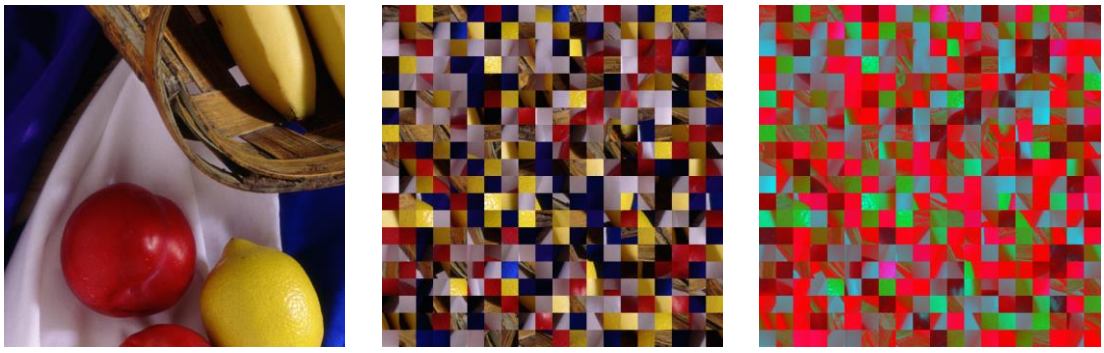


(a) (b) **(c)**

Figure 3. (a) Original McM Image #1, (b) Randomly Shuffled Image, (c) and *imcomplement*() Applied Image

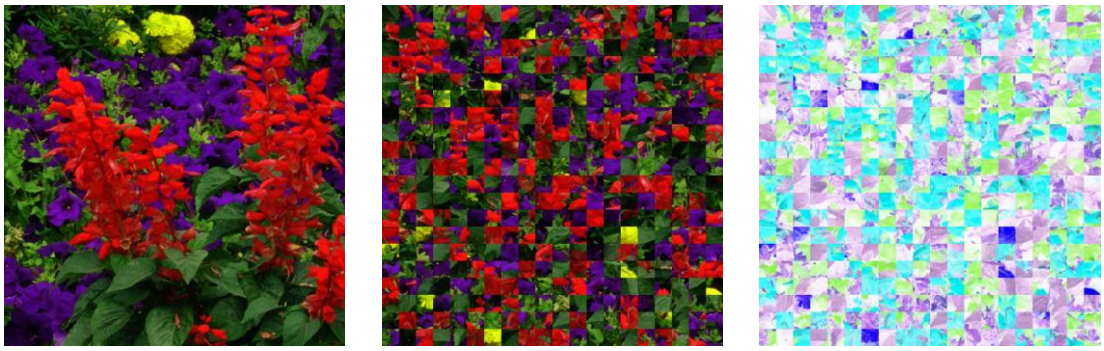
(a) (b) (c)

Figure 4. (a) Original McM Image #9, (b) Randomly Shuffled Image, (c) and *imcomplement*() Applied Image



(a) (b) (c)

Figure 5. (a) Original McM Image #14, (b) Randomly Shuffled Image, (c) and *imcomplement*() Applied Image



(a) (b) (c)

Figure 6. (a) Original McM Image #17, (b) Randomly Shuffled Image, (c) and *imcomplement*() Applied Image

From Figures 3-6, we found that with block shuffling, better contents projection was made since results images are less interpretable.

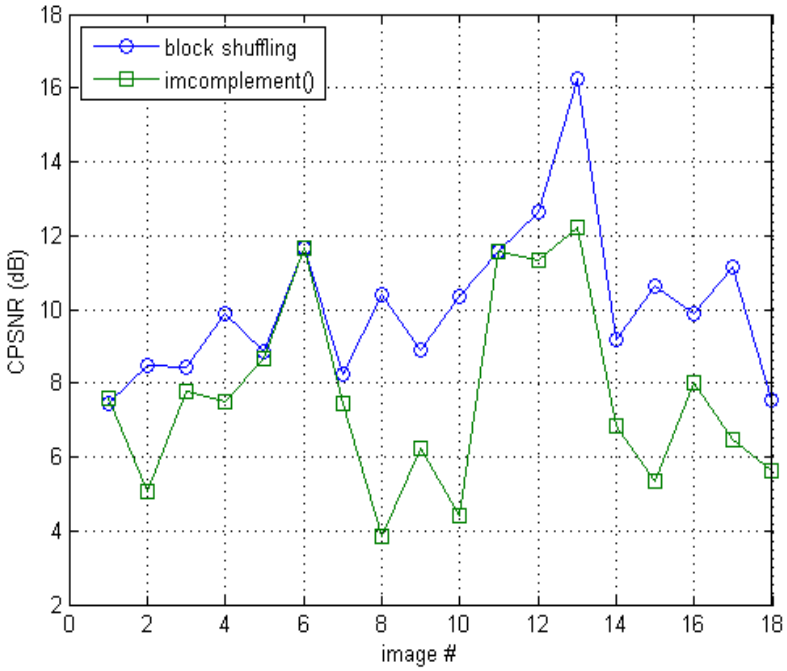


Figure 7. CPNSR Results on 18 McM Imageset

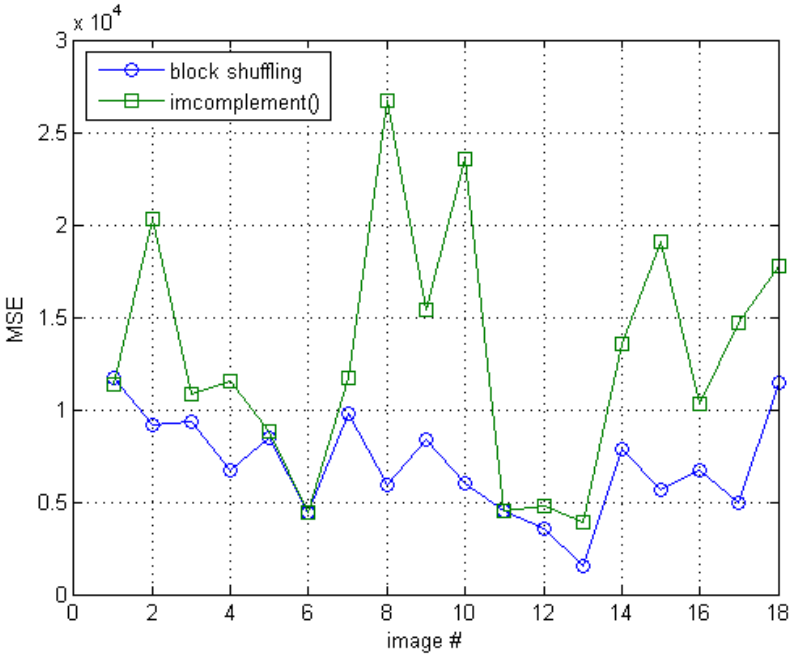


Figure 8. MSE Results on 18 McM Imageset

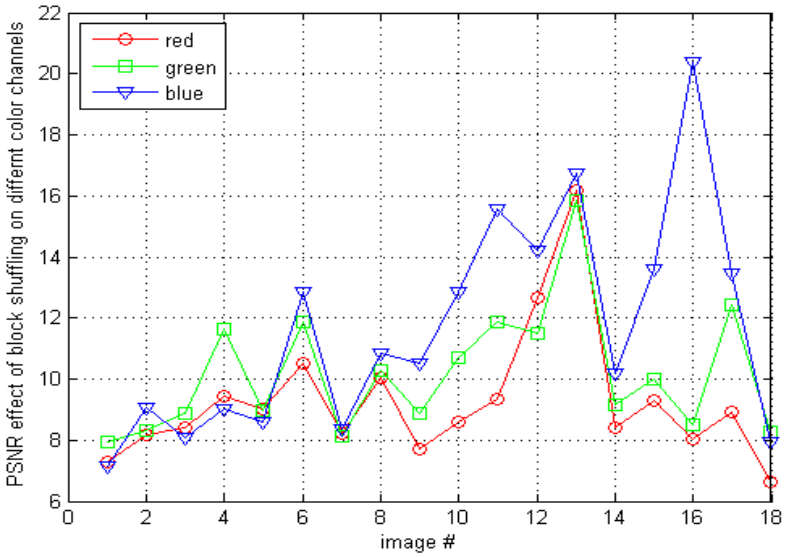


Figure 9. PSNR Effect of Block Shuffling on Three Color Channels

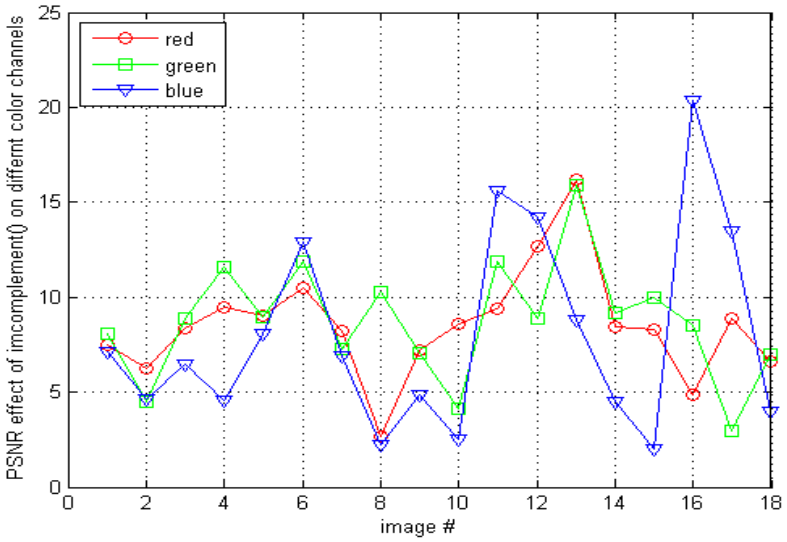


Figure 10. PSNR Effect of *imcomplement*() Function on Three Color Channels

Figures 7 and 8 show the CPSNR and MSE results on McM imageset. Figure 9 shows PSNR effect of block shuffling on three color channels. Figure 10 shows MSE effect of block shuffling on three color channels.

4. Conclusions

In this paper, we proposed a new scrambling method. We separated blocks into determined size, then we apply block shuffling approach to relocate the blocks. The relocated blocks have three channels, R, G, and B, and each color channel's luminance values could be complemented depending on the results of *rand*(). Simulation results expresses that the presented method protects contents adequately.

Acknowledgements

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Science, ICT and Future Planning(2013R1A1A1010797).

References

[1] G. L. Hobbs, "Video Scrambling", U.S Patent, 5815572, **(1998)** September 29.
[2] W. Zeng and S. Lei, "Efficient frequency domain selective scrambling of digital video", IEEE Transactions on Multimedia, vol. 5, **(2003)** March, pp. 118-129.
[3] C. Wang, H.-B. Yu and M. Zheng, "A DCT-based MPEG-2 transparent scrambling algorithm", IEEE Transactions on Customer Electronics, vol. 49, **(2003)** November, pp. 1208-1213.
[4] F. Defaux and T. Ebrahimi, "Scrambling for privacy protection in video surveillance systems", IEEE Trans. Circuits Syst. Video Technol., vol. 18, no. 8, **(2008)**, pp. 1168-1174.
[5] L. Tong, F. Dai, Y. Zhang and J. Li, "Prediction restricted H.264/AVC video scrambling for privacy protection", Electron. Lett., vol. 46, no. 1, **(2010)** January 7, pp. 47-49.
[6] M. S. Kankanhalli and T. Guan, "Compressed-domain scrambler/descrambler for digital video", IEEE Trans. Consumer Electronics, vol. 48, no. 2, **(2002)** May, pp. 356-365.
[7] G. Ye, "Image scrambling encryption algorithm of pixel bit based on chaos map", Pattern Recognition letters, vol. 31, **(2009)** November, pp. 347-354.

[8] A. Martin del Ray, "A Novel Cryptosystem for Binary Images", Studies in Informatics and Control, vol. 13, **(2004)**, pp. 5-14.
[9] M. S. Baptista, "Cryptography with chaos", Phys. Lett. A 240, **(1999)**, pp. 50-54.
[10] S. N. Elaydi, "Discrete Chaos", Chapman & Hall/CRC, **(1999)**, pp. 117.
[11] Data Encryption Standard. FIPS PUB, vol. 46, **(1977)** January.
[12] I. Agi and L. Gong, "An empirical study of secure MPEG video transmissions", Proc. of The Internet Society Symposium on Network And Distributed System Security, **(1996)** February.
[13] T. Maples and G. Spanos, "Performance study of a selective encryption scheme for the security of networked, realtime video", Proc. 4th Int. Conf. Computer Communications and Networks, Las Vegas, NV, **(1995)** September.
[14] Y. Sadourny and V. Conan, "A proposal for supporting selective encryption in JPSEC", IEEE Trans. on Consumer Electronics, vol. 49, no. 4, **(2003)** November, pp. 846-849.
[15] B. Macq and J. Quisquater, "Cryptology for digital TV broadcasting", Proc. of IEEE, vol. 83, no. 6, **(1995)**, pp. 944-957.

Author

Gwanggil Jeon received the BS, MS, and PhD (summa cum laude) degrees in Department of Electronics and Computer Engineering from Hanyang University, Seoul, Korea, in 2003, 2005, and 2008, respectively.

From 2008 to 2009, he was with the Department of Electronics and Computer Engineering, Hanyang University, from 2009 to 2011, he was with the School of Information Technology and Engineering (SITE), University of Ottawa, as a postdoctoral fellow, and from 2011 to 2012, he was with the Graduate School of Science & Technology, Niigata University, as an assistant professor. He is currently an assistant professor with the Department of Embedded Systems Engineering, Incheon National University, Incheon, Korea. His research interests fall under the umbrella of image processing, particularly image compression, motion estimation, demosaicking, and image enhancement as well as computational intelligence such as fuzzy and rough sets theories.

He was the recipient of the IEEE Chester Sall Award in 2007 and the 2008 ETRI Journal Paper Award.