논문 17-42-02-06 The Journal of Korean Institute of Communications and Information Sciences '17-02 Vol.42 No.02
https://doi.org/10.7840/kics.2017.42.2.331

가역적 데이터 은닉에서 암호화된 이미지의 공간 상관관계를 측정하기 위한 새로운 섭동 함수 연구

파테마 투즈 조허라 카남◆, 김 성 환°

New Fluctuation Functions to Measure Spatial Correlation of Encrypted Images in Reversible Data Hiding

Fatema-Tuz-Zohra Khanam◆, Sunghwan Kim°

요 약

본 논문에서는 암호화된 이미지에서 Zhang의 가역적 데이터 은닉 기법을 개선하는 알고리즘을 제안한다. 기존의 기법에서는 주변 픽셀의 평균값이 섭동함수로 사용되었고 모의실험 시 오류 성능이 저하됨을 확인되었다. 제안하는 시스템에서는 비트 오류율을 줄이고자 섭동을 측정 할 때 주변 함수와의 차이의 합을 더하여 계산한다. 또한 경계 픽셀을 고려한 변동함수의 새로운 계산법을 제안한다. Zhang과 Hong의 시스템과 비교 시 제안 기법의 성능이 우수함을 모의실험을 통해 확인할 수 있다. 이 결과로부터 제안 시스템을 사용할 경우 오류 없이 정보를 더 전송할 수 있음을 확인할 수 있다.

Key Words : Data-hiding, encrypted image, fluctuation function

ABSTRACT

In this work, we propose an improved form of Zhang's reversible data hiding technique in encrypted image. In the original work, average value of neighboring pixels is used for fluctuation calculation which fails to give good performance. In proposed scheme, to reduce the bit error rate a new function is calculated by summing difference from four neighboring pixels for measuring fluctuation. Moreover, modified calculation of fluctuation function is also proposed where border pixels are considered. The simulation results show that the performance of proposed method outperforms Zhang's and Hong's work. From the results, more information can be sent by using proposed system.

Ⅰ. Introduction

Reversible data hiding in images is a methodology that embeds secret message or information bits into some distortion-unacceptable cover media, such as medical, military or law forensic images, with a reversible manner that the original covers can be losslessly recovered after the embedded information is extracted. Several reversible data hiding techniques have been introduced[1-8]. Tian[1] proposed a reversible data hiding method based on the difference expansion technique where data hiding is done in the difference of bits. Ni et al.[2] utilized the minimum

※ 본 연구는 한국연구재단의 신진연구지원사업(NRF-2014R1A1A1004521)과 기본연구지원사업(NRF-2016R1D1A1B03934653)의 지원으로 수행되었습니다.
◆ First Author : School of Electrical Engineering, University of Ulsan, polash_cuet@yahoo.com, 학생회원
° Corresponding Author : School of Electrical Engineering, University of Ulsan, sungkim@ulsan.ac.kr, 종신회원
논문번호 : KICS2016-08-208, Received August 23, 2016; Revised December 9, 2016; Accepted December 9, 2016

and maximum point of the image histogram and embedded the data by shifting the histogram. Celik et al.[3] proposed a lossless compression technique for carrying data. Moreover, to improve the performance, different schemes have been proposed into the typical reversible data hiding approaches[4-8]. A fully homomorphic encryption method without key switching was proposed to reduce the complexity[9].

Now a days, data hiding in encrypted domain has attracted considerable research interest. With regard to providing confidentiality for images, encryption is an effective and popular means for a content owner to convert the original and meaningful content to incomprehensible one. Encryption and data hiding are two effective and popular means of privacy protection and secret communication. While the encryption technique converts the plaintext content into unreadable cipher text, the data hiding technique embeds secret message or information bits into cover media like pictures, images, audios or videos by introducing a small modification. In many fields, like legal, medical and military encrypting the image before data hiding and recovering the exact original image after data extraction are two desirable properties. In this case, the host image is encrypted by the content owner before passing it to the data hider for data embedding. The receiver side can extract the hidden information and recover the original host image without any loss or distortion. The host image is encrypted before data embedding is actually performed[10-12].

A novel reversible data hiding by using Reed-Solomon code was proposed for efficient transmission in encrypted image[13]. The improved fluctuation function from Zhang's reversible data hiding scheme in encrypted image was proposed[14]. New fluctuation function was proposed to reduce errors made from extracting embedded data[15].

The original test image is first encrypted by using an encryption key in Zhang's algorithm[11]. Then, the encrypted image is divided into non-overlapping blocks sized by $s \times s$. After that, by adopting bit flip mechanism one bit of information is embedded in one block. For data extraction and image restoration, Zhang[11] proposed the fluctuation function, f_z

$$f_z = \sum_{u=2}^{s-1}\sum_{v=2}^{s-1}\left|p(u,v) - \frac{p(u-1,v)}{4} - \frac{p(u,v-1)+p(u+1,v)+p(u,v+1)}{4}\right|, \quad (1)$$

where $p(u,v)$ denotes the pixel value at position (u,v) in a block. Nevertheless, in Zhang's system average value of neighboring pixels is exploited for fluctuation measurement which gives worse performance. Moreover, the border pixels of blocks are not included in the fluctuation calculation which can also be the reason for worse performance.

Zhang's algorithm[11] was further improved by Hong et al.[16] by using side match technique. Hong et al.[16] proposed the fluctuation function, f_H by exploiting the summation of the absolute difference of pixels and their neighboring pixels expressed as:

$$f_H = \sum_{u=1}^{s_2}\sum_{v=1}^{s_1-1}|p(u,v)-p(u,v+1)| + \sum_{u=1}^{s_2-1}\sum_{v=1}^{s1}|p(u,v)-p(u+1,v)| \quad (2)$$

However, in Hong's system only two neighboring pixels are used which could reduce the correctness of the data extraction.

This work proposes an improved reversible data hiding scheme for encrypted image, which consists of image encryption, data hiding, image decryption, data extraction, and image recovery. The original test image is completely encrypted by using an encryption key before sending it to the data hider. Then, the information bits are concealed by modifying a small portion of encrypted data. Finally, at receiver side, the hidden bits are successfully extracted and the original test image is exactly recovered without any distortion by means of spatial correlation in natural image. For fluctuation calculation, we propose two functions. We consider four neighboring pixels for fluctuation calculation in both functions. In the first one, the actual value of neighboring pixel is used instead of average value to

reduce the bit error rate. But it does not include the border pixels. In the second function, all the pixels including border and corner pixels of blocks are included for fluctuation calculation. Furthermore, we consider four neighboring pixels instead of two.

The rest of this paper is organized as follows. The proposed method is described in Section II. Then, the experimental results are discussed in section III. Finally, conclusion is given in section IV.

Ⅱ. Proposed Data Hiding System

The block diagram of the proposed system is shown in Figure 1. The proposed system is composed of sender and receiver. The transmitter is composed of two phases, image encryption and data hiding. Similarly, the receiver is composed of two phase, image decryption and data extraction & image recovery.

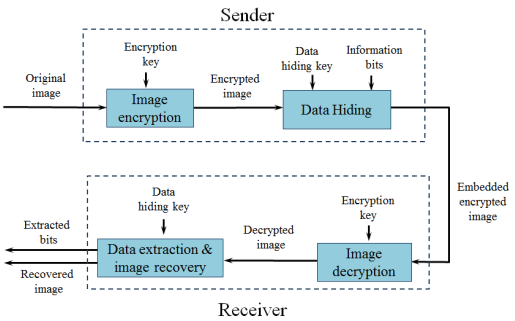


Fig. 1. Block diagram of the proposed data hiding system

2.1 Image Encryption

The original image is encrypted by an encryption key using a standard stream cipher. It is assumed that, O is an uncompressed image sized by $X \times Y$ in which every pixel is represented by 8 bits. Let $O_{i,j}$ be pixel with gray value at position (i,j) where $O_{i,j}$ belongs to [0, 255] and $1 \le i \le X$, $1 \le j \le Y$. $O_{i,j}$ denotes 8 bits of each pixel where $0 \le k \le 7$. The relation between bit in a pixel and pixel with gray value is denoted by

$$O_{i,j,k} = \left\lfloor \frac{O_{i,j}}{2^k} \right\rfloor \bmod 2 \tag{3}$$

and

$$O_{i,j} = \sum_{k=0}^{7} O_{i,j,k}\, 2^k \tag{4}$$

To encrypt the original image a random sequence, $K_{i,j,k}$ is generated according to the encryption key. Then a bitwise exclusive or (XOR) of O and K is performed using the following equation as

$$O'_{i,j,k} = O_{i,j,k} \oplus K_{i,j,k} \tag{5}$$

2.2 Data Hiding

As the image is encrypted, the data hider will not know anything about the original image but still he can insert data in the encrypted image, O' according to following process. Firstly, the encrypted image is divided into a number of non-overlapping blocks sized by $s \times s$. Each block will contain one bit of information. Then, according to the data hiding key, the pixels of each block is divided into two sets A_0 and A_1 pseudo randomly. The probability that a pixel belongs to one of two sets is uniformly distributed.

If bit to be inserted is '0' then three least significant bits (LSB) of each pixel in set, A_0 are flipped i.e.

$$O''_{i,j,k} = \overline{O}'_{i,j,k} \text{ for } (i,j) \in A_0 \text{ and } 0 \le k \le 2, \tag{6}$$

while pixels in set A_1 remain unchanged. On the other hand, if bit to be inserted is '1', then three LSBs of each pixel in set, A_1 are flipped i.e.

$$O''_{i,j,k} = \overline{O}'_{i,j,k} \text{ for } (i,j) \in A_1 \text{ and } 0 \le k \le 2. \tag{7}$$

The five most significant bits (MSB) of each pixel in both sets remain same only the three LSBs are changed. Then the encrypted image containing information bits, O'' is sent to the receiver.

2.3 Image Decryption

After receiving the embedded encrypted image, O'' a receiver first decrypts the image. By using

the encryption key, the image is decrypted by applying bitwise XOR of received data, O'' and random sequence K.

$$D_{i,j,k} = O''_{i,j,k} \oplus K_{i,j,k}. \tag{8}$$

From the decrypted image bit $D_{i,j,k}$, the decrypted pixel $D_{i,j}$ can be obtained as

$$D_{i,j} = \sum_{k=0}^{7} D_{i,j,k}\, 2^k \tag{9}$$

The first five MSB of the decrypted pixel $D_{i,j}$ in decrypted image are identical to the pixel in the original image.

2.4 Data Extraction & Image Recovery

The decrypted image is partitioned into non-overlapping blocks sized by $s \times s$. According to the data hiding key, the pixels of each block are divided into two sets, A_0 and A_1 pseudo randomly, which are same with data hiding phase. For each decrypted block, two new blocks, L_0 and L_1 are obtained. In L_0, all the three LSBs of each pixel in A_0 are flipped and in L_1, all the three LSBs of pixels in A_1 are flipped. Between L_0 and L_1, one is the original block and another one is the flipped block because of three LSBs flip. To determine which one is the original block, fluctuations of L_0 and L_1 are calculated according to the following equation,

$$\begin{aligned} f_{p1} = \sum_{u=2}^{s-1}\sum_{v=2}^{s-1} \{ & |q(u,v) - q(u-1,v)| \\ & + |q(u,v) - q(u+1,v)| + |q(u,v) - q(u,v-1)| \\ & + |q(u,v) - q(u,v+1)| \} \end{aligned} \tag{10}$$

where $q(u,v)$ denotes the pixel value at position (u,v) in a block. However in (10) the border pixels of blocks are included for fluctuation calculation which could reduce the correctness of data extraction. So we propose another fluctuation function to solve this problem.

For the pixels in four borders except the corner pixels which have three neighboring pixels the following function is defined,

$$\begin{aligned} f_b = & \sum_{v=2}^{s-1} \{ |q(1,v) - q(1,v-1)| + |q(1,v) - q(1,v+1)| \\ & + |q(1,v) - q(2,v)| + |q(s,v) - q(s,v-1)| \\ & + |q(s,v) - q(s,v+1)| + |q(s,v) - q(s-1,v)| \} \\ & + \sum_{u=2}^{s-1} \{ |q(u,1) - q(u-1,1)| + |q(u,1) - q(u+1,1)| \\ & + |q(u,1) - q(u,2)| + |q(u,s) - q(u-1,s)| \\ & + |q(u,s) - q(u+1,s)| + |q(u,s) - q(u,s-1)| \} \end{aligned} \tag{11}$$

For the fluctuation calculation of the pixels in four corner of blocks which have only two neighboring pixels the following function is given,

$$\begin{aligned} f_c = & |q(1,1) - q(1,2)| + |q(1,1) - q(2,1)| \\ & + |q(1,s) - q(1,s-1)| + |q(1,s) - q(2,s)| \\ & + |q(s,1) - q(s,2)| + |q(s,1) - q(s-1,1)| \\ & + |q(s,s) - q(s,s-1)| + |q(s,s) - q(s-1,s)| \end{aligned} \tag{12}$$

For the pixels in the middle of blocks which have four neighboring pixels the fluctuation function, f_{p1} in (10) is used.

To calculate the total fluctuation of the block the following function is defined by combining (10), (11) and (12)

$$f_{p2} = f_{p1} + f_b + f_c \tag{13}$$

Fluctuation function of the original block is generally lower than that of the flipped one due to the spatial correlation in natural image. Hence, by comparing f_0 and f_1 data extraction and image recovery can be performed. If $f_0 < f_1$, then L_0 will be the original block and '0' will be the extracted hidden bit. Otherwise, L_1 will be the original block and '1' will be the extracted hidden bit. Eventually, extracted hidden bits are concatenated to get the information and recovered blocks are collected to make the original image.

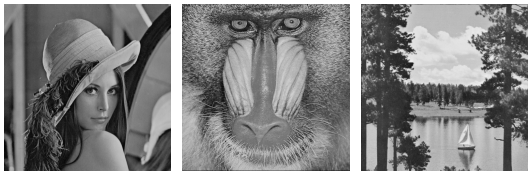
Ⅲ. Experimental Results

In our simulation, three gray level images are

considered, which are Lena, Baboon and Sailboat sized by 512×512, as test images as shown in Fig. 2.

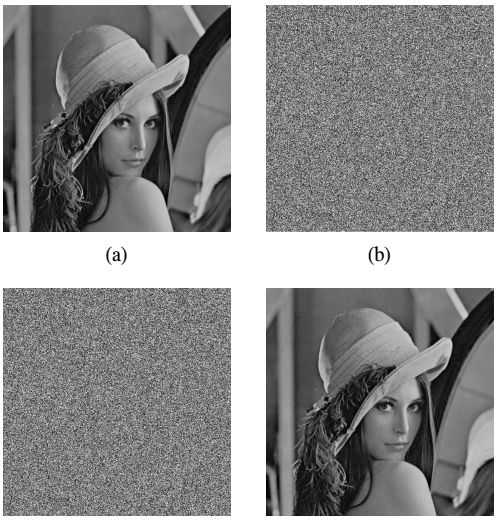
As shown in Fig. 3(a) test image, Lena was encrypted to generate the encrypted version of it as presented in Fig. 3(b). Then, we embedded 1024 bits into the encrypted image by using each block of size 16×16 as given in Fig. 3(c). After that, the image was decrypted as represented in Fig. 3(d). Finally, the hidden information bits were successfully extracted and the original image was perfectly restored from the decrypted image.

Fig. 4, Fig. 5, and Fig. 6 represent the error rate comparison between proposed system and Zhang's and Hong's system for test image Lena, Baboon and Sailboat respectively. For comparison we consider Hong's result without side match technique. These figures depict that proposed function, f_{p1} in (10) presents lower bit error rates than that of Zhang[11] and proposed function, f_{p2} in (13) presents lower bit error rates than that of Zhang[11] and Hong[16] for all three images. For Lena image, as shown in Figure 4, when block size is 8×8, the error rates of proposed functions, f_{p1} in (10) and f_{p2} in (13) are 0.85% and 0.36% respectively whereas the error rate of Zhang[11] is 1.21% which is around 1.5 times higher than that of function, f_{p1} in (10) and more than 3 times higher than function, f_{p2} in (13). The error rate of Hong[16] is 0.49% without side match which is lower than function, f_{p1} in (10) but higher



(a) (b) (c)

Fig. 2. Three original images for simulation (a) Lena, (b) Baboon, (c) Sailboat



(a) (b)

(c) (d)

Fig. 3. Procedure of image encryption, data embedding, image description of Lena image.
(a) original Lena, (b) encrypted Lena, (c) encrypted Lena containing information bits, (d) decrypted Lena containing information bits.

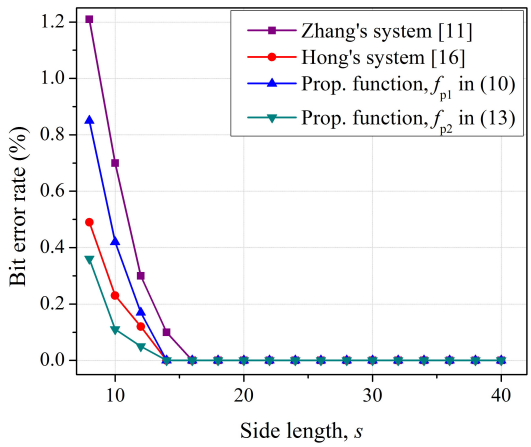


Fig. 4. The error rate comparison between proposed system and referenced systems for test image Lena.

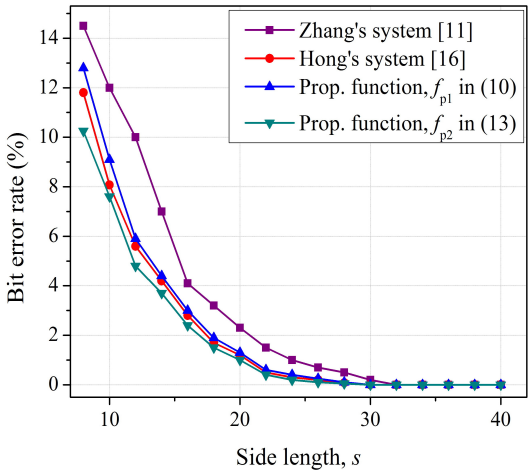


Fig. 5. The error rate comparison between proposed system and referenced systems for test image Baboon.

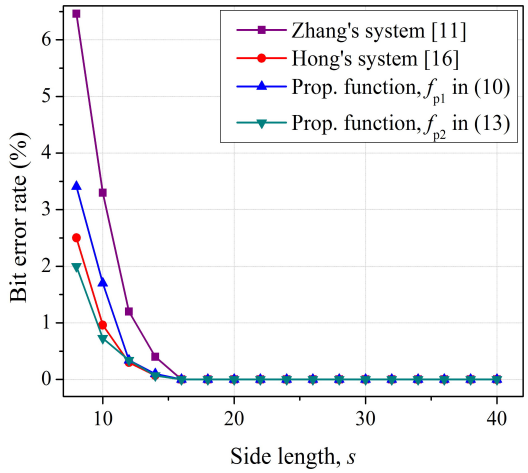


Fig. 6. The error rate comparison between proposed system and referenced systems for test image Sailboat.

than proposed function, f_{p2} in (13). According to Figure 4, by using proposed scheme we can embed at least 1296 (s=14) bits without any error but in case of Zhang[11] only 1024 (s=16) bits can be embedded error freely. So, not only in terms of error rate but also in terms of payload proposed method is better than Zhang[11]. For the complex image, such as Baboon, as shown in Figure 5, the proposed work outperforms the Zhang's work[11] and Hong's work[16] as well. Moreover, for the sailboat image, as shown in Figure 6, at s=8 the error rates of f_{p1} in (10) and f_{p2} in (13) are 3.3% and 2.02% respectively whereas the error rate of Zhang[11] is 6.5 which are approximately 2 and more than 3 times less than that of Zhang's system respectively. The error rate of Hong[16] is 2.5 % which is lower than f_{p1} but higher than f_{p2}. Because, for the fluctuation calculation of each block, the actual value of neighboring pixels is exploited instead of average value in (10). Moreover, all the pixels including border and corner pixels of blocks are included in (13). Furthermore, we consider four neighboring pixels instead of two in (13).

Ⅳ. Conclusion

This paper proposes an improved data extraction and image recovery technique based on Zhang's work. A better scheme for calculating fluctuation of blocks is used to reduce the bit error rate of extracted data. To measure fluctuation, we have used the real value of adjacent pixels instead of mean value of them in the first function. Furthermore, in the second function, all the pixels including the border and corner pixels of blocks are included for fluctuation calculation. The simulation results demonstrate that the proposed system effectively develops Zhang's and Hong's work. Moreover, by using proposed system more payloads can be embedded without any error.

References

[1] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Trans. Cir. Syst. Video Technol.*, vol. 13, no. 8, pp. 890-896, 2003.

[2] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Trans. Cir. Syst. Video Technol.*, vol. 16, no. 8, pp. 354-362, 2006.

[3] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless generalized-LSB data embedding," *IEEE Trans. Image Process.*, vol. 14, no. 2, pp. 253-266, 2005.

[4] D. M. Thodi and J. J. Rodriguez, "Expansion embedding techniques for reversible watermarking," *IEEE Trans. Image Process.*, vol. 16, no. 3, pp. 721-730, 2007.

[5] C. C. Chang, C. C. Lin, and Y. H. Chen, "Reversible data-embedding scheme using differences between original and predicted pixel values," *Inform. Secur.*, vol. 2, no. 2, pp. 35-46, 2008.

[6] L. Luo, Z. Chen, M. Chen, X. Zeng, and H Xiong, "Reversible image watermarking using interpolation technique," *IEEE Trans. Inf. Foren. Secur.*, vol. 5, no. 1, Mar. 2010.

[7] W. Hong and T. S. Chen, "Reversible data embedding for high quality images using interpolation and reference pixel distribution mechanism," *J. Vis. Commun. Image Represent.*, vol. 22, no. 2, pp. 131-140, 2011.

[8] S. Kang, H.-J. Hwang, and H.-J. Kim, “Reversible watermark using an accurate predictor and sorter based on payload balancing,” *ETRI J.*, vol. 34, no. 3, pp. 410-420, Jun. 2012.

[9] J.-H. Kim, S.-K. Yoo, and S.-H. Lee, “Fully homomorphic encryption scheme without key switching,” *J. KICS*, vol. 38C, no. 5, pp. 428-433, Jun. 2013.

[10] K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, “Reversible data Hiding in encrypted images reserving room before encryption,” *IEEE Trans. Inf. Foren. Secur.*, vol. 8, no. 3, Mar. 2013.

[11] X. Zhang, “Reversible data hiding in encrypted images,” *IEEE Signal Process. Lett.*, vol. 18, no. 4, pp. 255-258, 2011.

[12] X. Zhang, “Separable reversible data hiding in encrypted image,” *IEEE Trans. Inf. Foren. Secur.*, vol. 7, no. 2, Apr. 2012.

[13] T. Kim, M.-H. Jang, and S. Kim, “Transmission methods using RS codes to improve spacial relationship of images in reversible data hiding system,” *J. KICS*, vol. 40, no. 8, pp. 1477-1484, Aug. 2015.

[14] F.-T.-Z. Khanam, D. M. Nguyen, and S. Kim, “Improved reversible data hiding in encrypted image using new fluctuation function,” in *Proc. KICS Int. Conf. Commun*, Jeju island, Jun. 2016.

[15] Y.-H. Kim, D.-W. Lim, and Y.-S. Kim, “Design of fluctuation function to improve BER performance of data hiding in encrypted image,” *J. KICS*, vol. 41, no. 3, pp. 307-316, Mar. 2016.

[16] W. Hong, T. S. Chen, and H.-Y. Wu, “An improved reversible data hiding in encrypted images using side match,” *IEEE Sign. Process. Lett.*, vol. 19, no. 4, pp. 199-202, Apr. 2012.

파테마 투즈 조허라 카남 (Fatema-Tuz-Zohra Khanam)

2012년 12월 : Chittagong University of Engineering and Technology 전기전자공학부 졸업

2015년 3월~현재 : 울산대학교 전기공학부 석사과정

<관심분야> 데이터 은닉, 암호학, 정보이론

김 성 환 (Sunghwan Kim)

1999년 2월 : 서울대학교 전기공학부 졸업

2001년 2월 : 서울대학교 전기컴퓨터공학부 공학석사

2005년 8월 : 서울대학교 전기컴퓨터공학부 공학박사

2005년 10월~2007년 4월 : Georgia Institute of Technology 박사후 과정

2007년 5월~2011년 2월 : 삼성전자 DMC 연구소 책임연구원

2011년 3월~현재 : 울산대학교 전기공학부 부교수

<관심분야> 디지털 통신, 오류정정부호, LDPC 부호, 양자 정보, 가시광 통신, 데이터 은닉