암호화와 DnCNN을 활용한 문서 복원능력 향상에 관한 연구

장현희[1], 하성재[2*], 조기환[3]
[1]한국폴리텍대학 신기술교육원장, [2]한국폴리텍대학 AI융합과 교수, [3]전북대학교 컴퓨터공학부 교수

An Enhancement Method of Document Restoration Capability using Encryption and DnCNN

Hyun-Hee Jang[1], Sung-Jae Ha[2*], Gi-Hwan Cho[3]
[1]Drector, Korea Polytechnic College, New Technology Education Institute
[2]Professor, Korea Polytechnic College, Artificial Intelligence Department
[3]Professor, Jeonbuk National University, Division of Computer Science and Engineering

요 약 본 논문은 문서의 보안과 손실 및 오염에 대하여 복원능력을 향상시키는 방안을 제안한다. 이를 위해서 암호화로 DnCNN(DeNoise Convolution Neural Network)을 제시한다. 암호화 방법을 구현하기 위하여 2D이미지정보를 광학에 사용되는 공간주파수 전달함수(Spatial Frequency Transfer Function)의 수학적 모델을 적용한다. 공간 주파수 전달함수를 사용하여 광학적 간섭 패턴을 암호화로 사용하고 공간 주파수 전달함수의 수학적 변수를 복호화하는 암호로 사용하는 방법을 제안하였다. 또한, 딥러닝을 적용한 DnCNN 방법을 적용하여 노이즈 제거하여 복원 성능을 개선한다. 실험결과, 65%의 정보 손실이 있는 경우에도 Pre-Training DnCNN Deep Learning을 적용한 결과 공간 주파수 전달함수만을 활용한 복원 결과 와 비교하여 PSNR(Peak Signal-to-noise ratio)을 11% 이상 우수한 성능을 확인할 수 있다. 또한, CC(Correlation Coefficient)의 특성도 16% 이상 우수한 결과를 보이고 있다.

주제어 : 암호화, 노이즈 제거 컨벌루션 네트워크, PSNR, CC, SFTF

Abstract This paper presents an enhancement method of document restoration capability which is robust for security, loss, and contamination, It is based on two methods, that is, encryption and DnCNN(DeNoise Convolution Neural Network). In order to implement this encryption method, a mathematical model is applied as a spatial frequency transfer function used in optics of 2D image information. Then a method is proposed with optical interference patterns as encryption using spatial frequency transfer functions and using mathematical variables of spatial frequency transfer functions as ciphers. In addition, by applying the DnCNN method which is bsed on deep learning technique, the restoration capability is enhanced by removing noise. With an experimental evaluation, with 65% information loss, by applying Pre-Training DnCNN Deep Learning, the peak signal-to-noise ratio (PSNR) shows 11% or more superior in compared to that of the spatial frequency transfer function only. In addition, it is confirmed that the characteristic of CC(Correlation Coefficient) is enhanced by 16% or more.

Key Words : Encryption, DnCNN, PSNR, Correlation Coefficient, Spatial Frequency Transfer Function

*교신저자 : 하성재(sungjae@kopo.ac.kr)
접수일 2022년 2월 8일 수정일 2022년 3월 15일 심사완료일 2022년 3월 21일

1. 서론

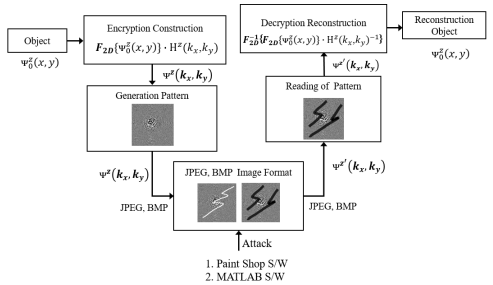
현재 정보 및 컨텐츠 사회에서 보안은 중요한 이슈 중 하나이다. 최근 컴퓨터 지식과 기술의 발전에 의해 문서 및 코드를 위조하거나 복제할 수 있는 가능성이 증가하여 주민등록증, 여권과 같은 ID카드뿐만 아니라 공공기관의 증명서나 제품의 정품인증 코드 등의 위변조 사례가 증가하고 있다. 불법으로 사용되거나 오염된 내용으로 정보가 변질되는 등의 일을 방지하기 위해서 많은 연구들이 진행되고 있다. 특히, 광학적 이론과 방법을 활용하여 암호화 및 복호화는 여러 가지 많은 시스템 변수를 가지고 있어 암호화에 광범위하게 연구 되어져 왔다[1-7].

본 논문은 훼손된 원본 정보 데이터를 복원력을 최대화하는 연구로써 공간 주파수전달함수(Spatial Frequency Transfer Function)의 수학적 모델을 제안한다. 또한, 수학적 모델을 기존의 Digital signal Processing에 적용되는 다양한 잡음 제거 필터 성능과 DL(Deep learning) CNN 성능을 비교하여 복원 성능을 개선하는 방안을 제시한다. 또한, 본 논문에서 우리는 문서의 활자를 암호 복호화가 가능하고 손실에 대한 복원의 우수한 보안마커에 적용함을 연구의 범위로 한다. 특히, 컴퓨터로 생성된 간섭 패턴을 암호화 보안마커로 사용하고자 할 경우 종이에 프린트되어 잡음 및 손실에 대한 복원 특성이 주요 연구의 내용으로 한다.

2. 관련 연구

2.1 본 논문의 암호화 검증과정

그림 1 은 본 논문에서 수행된 암호화 생성과 복원 검증을 보인 것이다. Object는 암호화를 위한 원본 데이터이다.

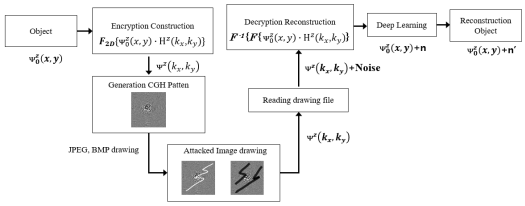


[Fig. 1] Processing for encryption and decryption

암호화 패턴은 다양한 손실, 잡음 및 오염을 강제로 추가하여 복원 알고리즘으로 다시 복원한다. 그리고, 성능을 개선하고자 디지털 신호처리 잡음제거 필터링 알고리즘과 딥러닝의 CNN 기법을 적용하여 성능을 개선 하였다. 최종으로 복원된 데이터는 원본 데이터와 정량적 성능을 비교하여 최종으로 성능개선 방안을 제시한다.

2.2 암호화 및 복원화 방법

그림 2는 그림 1의 수행방법에 따라서 수학적 모델을 제시한 것이다. 본 논문에서 적용된 공간주파수전달함수(Spatial Frequency Transfer Function)의 수학적 모델 사용하여 암호화 패턴을 JPEG와 BMP 파일 형식의 그림으로 출력한 후 다양한 잡음 및 손실을 인위적으로 추가한 후 복원하여 원본과 복원된 결과를 비교하는 과정이다. 식 2-1은 본 고에서 사용된 패턴 생성 식이다.



[Fig. 2] Modeling and Processing for encryption and decryption

식 2-1은 암호화를 위한 수학적 모델이다.

$$\Psi^z(x,y) = \Psi_0^z(x,y) * h^z(x,y) \qquad (2\text{-}1)$$
$$= F_{2D}^{-1}[F_{2D}\{\Psi_0^z(x,y)H^z(k_x,k_y)\}]$$

식 2-1에서는 z 축 방향으로 진행되는 회절파이다. $\Psi^z(x,y)$는 원본 데이터를 나타내며, 2D이미지정보(문서, 그림 등) 형식이다. $\Psi_0^z(x,y)$를 이미지 신호처리를 하기 위해서 2D 정보를 픽셀 $\Psi_0^z(M,N)$로 변환하여 나타낼 수 있다. 여기서 M과 N은 2D 이미지 정보를 구성하는 전체 픽셀 행렬(M행 N열)을 나타낸다. $h^z(x,y)$ 는 공간주파수 전달함수(Spatial Frequency Transfer function)이다. k_x, k_y는 각각 (x:가로),(y:세로)축 방향의 전파상수(Wave Number)를 나타낸다. $H^z(k_x,k_y)$, 는 $h^z(x,y)$를 2D Fourier Transform 한 것을 나타내

며 2D 정보를 픽셀 행렬($\Psi_0^z(M,N)$)로 변환한 것과 동일한 픽셀 크기를 갖는 $h^z(M,N)$ 의 행렬이다. 본 고에서는 복원력이 우수하도록 식 2-2를 사용한다[8-11].

$$H^z(k_x,k_y)=F_{2D}\{h^z(x,y)\}=e^{-j2\pi z\sqrt{\frac{1}{\lambda^2}-(\frac{p\,k_x}{k_0})^2-(\frac{q\,k_y}{k_0})^2}} \quad (2\text{-}2)$$

여기에서, p, q는

$\frac{-M}{2}\le p\le \frac{+M}{2}-1$, $\frac{-N}{2}\le q\le \frac{+N}{2}-1$ 이다. 각각 M, N은 2D 정보를 이미지로 변환하여 생성된 동일한 크기의 행렬을 나타내며 각각 y축을 나타내는 인덱스이다. λ(m)는 알고리즘에 사용되는 주파수의 파장이다.

식 2-2에서의 $k_x=\frac{2\pi}{M\triangle x}$, $k_x=\frac{2\pi}{M\triangle y}$ 그리고, $k_0=\frac{2\pi}{\lambda}$ 이다. 여기서, $\triangle x=\triangle y=i\cdot\ \lambda$의 값을 갖도록 설정하고 i를 정수($i=1,2,3..$)로 선택하면 수식 2-3이 된다.

$$\begin{aligned}H^z(k_x,k_y)&=H^z(p,q)\\&=e^{-j2\pi z\sqrt{\frac{1}{\lambda^2}-(\frac{p}{M\cdot\ i\cdot\ \lambda})^2-(\frac{q}{N\cdot\ i\cdot\ \lambda})^2}}\\&=e^{-jk_0z\sqrt{1-(\frac{p}{M\cdot\ i})^2-(\frac{q}{N\cdot\ i})^2}}\end{aligned} \quad (2\text{-}3)$$

식2-3에서 보인 것처럼 $\Psi^z(x,y)$신호의 방향 거리 +z, 사용주파수의 파장 λ(m) 또는 $k_0=\frac{2\pi}{\lambda}$ 가 $H^z(k_x,k_y)$ 변수가 된다. 또한, p, q는 x, y축 방향으로의 픽셀 변위 거리 인텍스를 나타낸다.

수식 2-1과 2-3은 암호 패턴의 각각 픽셀 거리 p및 q의 값들에 대하여 각각 $\frac{-M}{2}\le p\le \frac{+M}{2}-1$ 과 $\frac{-N}{2}\le q\le \frac{+N}{2}-1$ 범위의 해당 값을 갖으며 모두 $H^z(k_x,k_y)$ 값의 정보를 갖고 있음을 보여준다. 각각의 1개 픽셀은 나머지의 픽셀의 값도 갖을 수 있도록 알고리즘을 연산하고 2D 정보와 동일한 크기의 이미지 형식으로 출력하면 출력된 이미지($\Psi_0^z(x,y)$)의 일부 픽셀이 손실되어도 다른 픽셀의 값에서 손실된 정보를 추출할 수 있게 된다.

본 연구는 식 2-1에서 $\Psi_0^z(x,y)$의 2D 정보에 $M(m,n)$을 $\Psi_0^z(x,y)$와 동일한 크기인 행렬($e^{-j2\pi M(m,n)}$)을 곱하고 2진수로 $\Psi^z(x,y)$ 의 최종값을 출력한다. 이러한 행렬이 암호키로 사용 되어지므로 암호화 수준은 상당히 높다고 하겠다. 식 2-4는 식 2-1을 수정한 것이다.

$$\Psi^z(x,y)=F_{2D}^{-1}[F_{2D}\{\Psi_0^z(x,y)\,e^{-j2\pi M(m,n)}\}\,H^z(k_x,k_y)] \quad (2\text{-}4)$$

본 논문에서는 식 2-4를 사용하여 복원성 검증을 실시하였다. $\Psi^z(x,y)$는 $e^{j2\pi M(m,n)}$로 각각의 픽셀에 곱한 후에 2진수로 $\Psi^z(x,y)$를 출력한다. 이러한 2진수의 패턴 형태는 출력된 패턴에 손상을 가하여 $\Psi^{z'}(k_x,k_y)$을 생성한다. 식 2-5은 식 2-4로 암호화를 진행하고 다양한 형태의 손실 및 잡음을 추가하여 손실된 암호화 ($\Psi^{z'}(k_x,k_y)$)를 복원하기 위한 것이다 [7-9].

$$\Psi^{z_0}(x,y)=F^{-1}[\Psi^{z'}(k_x,k_y)H^z(k_x,k_y)^{-1}]e^{j2\pi M(m,n)} \quad (2\text{-}5)$$

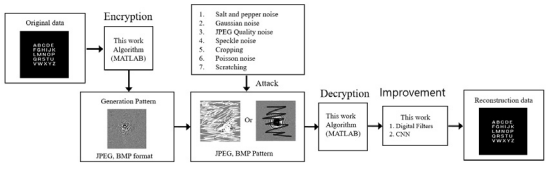
식 2-5에서 $\Psi^{z_0}(x,y)$를 복원하기 위해서 $H^z(k_x,k_y)$ 정보가 있어야 복원이 가능함을 보여준다.

그러므로 암호화된 정보를 복원 시에는 암호키에 해당하는 $H^z(k_x,k_y)$,$e^{j2\pi M(m,n)}$정보를 알고 있어야 한다. 본 논문에서의 $H^z(k_x,k_y)$ 는 랜덤형태의 1024 × 1024의 행렬이며 소숫점을 고려 할 경우 암호화 수준은 상당히 높다고 판단된다. 본 연구의 암호화에는 이러한 랜덤 행렬이 외도 암호화 파장의 정수배를 고려하면 더욱 불법 사용의 가능성은 낮다고 할 수 있다.

본 연구에서는 이러한 암호화와 더불어 손실률을 최소화한 복원성을 중요한 요소로 여겨 중첩성을 갖는 공간주파수전달함수의 암호화를 제안한다. 또한, $\Psi^{z_0}(x,y)$의 공간주파수 전달함수는 회절파를 의미하므로 모든 픽셀로부터 전파되는 신호원이며 이러한 파동의 중첩되는 특성이 손실된 정보로 원형정보를 복원할 수 있는 물리적인 의미를 나타낸다.

3. 성능검증 시험

본 논문의 복원 성능 검증 절차는 그림 3과 같다. 분석을 위해서 식 2-4를 활용하여 2D 이미지의 암호화 패턴을 생성한다.



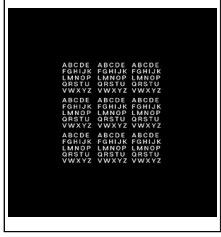
[Fig. 3] Processing for encryption and decryption

생성된 암호화 패턴 $\Psi^{z}(x,y)$은 JPEG와 BMP 파일로 출력된다. 출력 파일은 다시 Paint shop 소프트웨어 나 MATLAB으로 읽어서 잡음이나 손실을 그림에 직접 추가하여 암호화 패턴에 문제를 발생시킨 후 다시 JPEG나 BMP 파일패턴 $\Psi^{z'}(x,y)$로 저장한다. 잡음과 손실이 발생된 파일을 복원하기 위해서 식 2-5를 활용한다. 그리고, 잡음 및 손실의 특징에 따라서 복원된 2D 이미지의 정보 특성을 개선하기 위해서 다양한 잡음제거 필터와 최근 연구되고 있는 De-noise CNN 기법을 비교하여 복원 성능을 검증한다. 잡음제거 컨볼류션 신경망(DnCNN)은 이미지의 시각적 분석을 수행하는 심층 신경망의 한 종류이다. 이미지 노이즈 제거는 이미지 처리의 고전적인 연구 분야이지만 여전히 활발한 주제이다. 잡음제거 컨볼루션 신경망의 등장은 다양한 장점으로 인해 본 논문에 적용한다. 첫째로 성능개선하기 위한 시간소모가 적절하다. 두 번째로 잡음제거를 위한 학습이 매우 잘되어져 있다. 본 논문에서는 Matlab에서 지원하는 net = denoisingNetwork('DnCNN')을 활용한다[13].

검증과정에서 신호처리필터링과 딥러닝의 결과를 비교하기 위해서 PSNR(Peak Signal Noise Ratio), CC (Correlation Coefficient)의 특성을 비교한다[12-15]. PSNR은 식 3-1과 같다.

Table 1은 본 논문의 암호화의 성능을 확인하기 위한 원시 정보데이터 및 잡음의 종류를 보인 것이다. Table 1 원시데이터는 12 폰트 크기의 225개의 글자를 데이터로 하였다. 잡음의 종류는 4가지의 잡음으로 시험하여 비교한다.

〈Table 1〉 Test conditions

Raw Information Data	Noise type	How to improve performance
	1. Speckle 2. Salt&Pepper 3. Cropping 4. Scratching	Adative Gauss Guided Min. Median Max. NON CNN

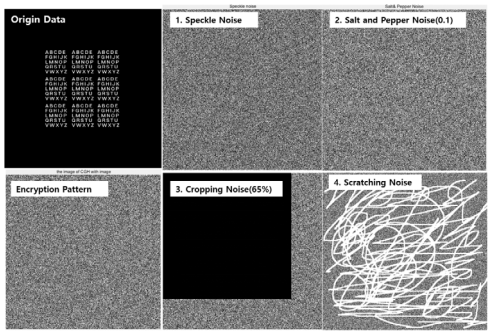
$$PSNR(dB) = 10.\log_{10}(\frac{255^2}{MSE}) \quad (3\text{-}1)$$

여기에서, MSE(Mean Square Error), $MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}[I_{\mathrm{or}iginal}(i,j) - I_{*acked}(i,j)]^2$ 이다. 또한, CC는 식 3-2와 같다.

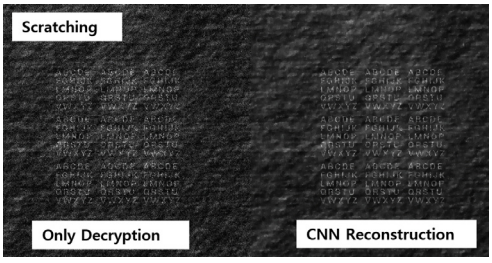
$$CC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(I_{\mathrm{or}iginal}(i,j) - I_{\mathrm{or}iginal/average}(i,j)(I_{recovered}(i,j) - I_{recovered/average}(i,j)}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}(I^2_{\mathrm{or}ginal}(i,j) - I_{\mathrm{or}iginal/average}(i,j)}\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}((I^{2_{recovered}}(i,j) - I_{recovered/average}(i,j)}} \quad (3\text{-}2)$$

3.1 복원 성능검증 시험 결과

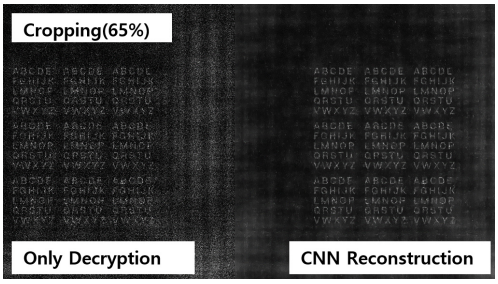
그림 4는 논문에서 제시한 시험순서로 Matlab을 활용하여 원본데이터(Origin Data)를 Encryption 화 하고 Encryption 된 이미지에 Speckel 잡음, Salt and Pepper 잡음(0.1), Cropping 잡음(65%) 그리고 Scratching을 가한 것을 보인 것이다. 그림 5는 Scratching과 Cropping 잡음을 인가하고 공간주파수 방정을 활용한 복원과 DnCNN을 적용한 성능 개선을 보인 것이다. 그림 6은 DnCNN과 기존의 디지털 신호처리에 사용되는 잡음 제거 필터링을 적용하여 비교한 결과를 보인 것인다. 다양한 디지털 필터링 과 비교 한 결과는 모든 잡음에서 CC, PSNR 특성이 각각 11%, 16% 성능 개선을 보였다.



[Fig. 4] The result of encryption and decryption with attacks

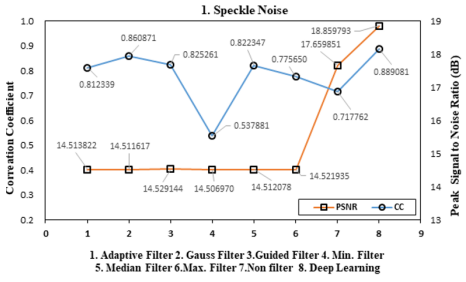


(a) The decryption with Scratching noise

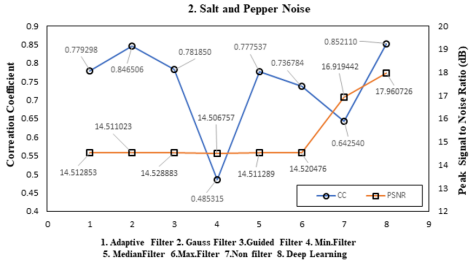


(b) The decryption with Cropping noise

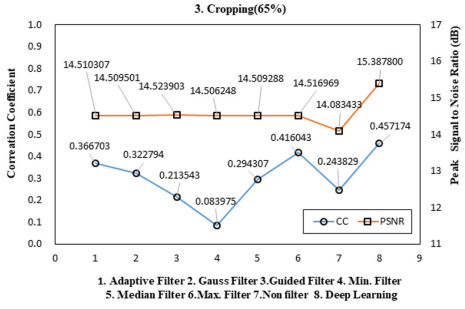
[Fig. 5] The result of compare digital filtering with DnCNN for reconstruction



(a) Speckle Noise



(b) Salt and Papper Noise



(c) Cropping

[Fig. 6] The result of compare digital filtering with DnCNN for reconstruction

4. 결론

본 논문에서는 복원성이 우수한 암호화를 위하여 수학적 모델인 공간주파수함수와 복원 성능을 개선하기 위하여 DnCNN을 제안하였다. 이러한, 수학적 모델을 활용하여 암호화 및 복원 성능을 확보하였으며, 복원된 정보의 성능을 개선하기 위하여 기존의 잡음제거 디지털 신호처리 필터링 기술과 노이지 제거 CNN 기술을 비교하여 분석하였다.

본 연구에서 제안한 수학적 모델과 DnCNN은 12 폰트 크기의 256개의 글씨를 65% 까지 손실(Cropping) 했을 경우에도 판독 가능한 성능을 보였다. 향후 과제로는 딥러닝을 적용하여 진보된 성능개선과 학습을 위한 데이터확보 방법들의 연구가 있다.

REFERENCES

[1] Yoshinao Aoki, "Watermarking technique using computer-generated holo-grams," Electron Commun. Jpn., 84(1), pp.21-31, 2001.

[2] G. Unnikrishnan, J. Joseph, K. Singh, "Opticalencryption

by double-random phase encodinging thefractional Fourier domain," Opt. Lett.,25(12), pp.887-889, 2000.

[3] N. Takanori, B. Javidi, "Optical encryption using ajoint transform correlator architecture," Opt. Eng., 39(8), pp.2031-2035, 2000.

[4] L. Chen, D. Zhao, "Optical color image encryptionby wavelength multiplexing and lensless Fresnel transform holograms," Opt. Express, 14(19), pp.8552-8560, 2006.

[5] P. Clemente, V. Durán, E. Tajahuerce, J. Lancis,"Optical encryption based on computational ghost imaging," Opt. Lett.,35(14), pp.2391-2393, 2000.

[6] S. J. Ha et al., "A study on the Metal detection using RNN algorithms for MI sensors". Journal of Industrial Technology Research, Vol.26, No.2, pp.103-111, 2021.

[7] M. S. Kang, "A Study on the Characteristics of Digital-Affordance Exhibition Space for AI Utilization". ournal of Industrial Technology Research, Vol.26, No.4, pp.15-28, 2021.

[8] T.-C. Poon, and P. P. Banerjee, "Contemporary Optical Image Processing with MATLAB," Elsevier Oxford, UK, 2001.

[9] J. W. Goodman, "Introduction to Fourier Optics," Roberts and Company Publishers, 2005.

[10] G. Unnikrishnan, J. Joseph, K. Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain," Opt. Lett., 25(12) pp.887-889, 2000.

[11] P. W. M. Tsang, T. C. Poon, C. Zhou, and K. W. K. Cheung, "Binary mask programmable hologram," Optics Express, ch. 20, pp.26480-26485, 2012.

[12] Matlab image processing toolbox. 2021.

[13] C. Zhu, "A novel image encryption scheme based on improved hyperchaotic sequences," Optics Communication, 285, pp.29-37, 2012.

[14] S. Behnia, A. Akhshani, H. Mahmodi, A. Akhavan, Chaos, 'Solitons & Fractals," 35, pp.408, 2008.

[15] C. Li, S. Li, G. Chen, W.A. Halang, "Image and Vision Computing," 27, pp.1035, 2009.

장 현 희(Hyun-Hee Jang) [정회원]

- 2006년 8월 : 전북대학교 일반대학원 컴퓨터정보학과 (공학박사수료)
- 1991년 6월 ~ 현재 : 한국폴리텍대학 교수
- 2022년 1월 ~ 현재 : 한국폴리텍대학 신기술교육원 원장

〈관심분야〉
사물인터넷, 인공지능, 클라우드

하 성 재(Sung-Jae Ha) [정회원]

- 2006년 2월 : 삼성탈레스 전문연구원
- 20010년 2월 : Old Dominion University VMASC 초빙교수
- 2014년 8월 ~ 현재 : 한국폴리텍대학 교수

〈관심분야〉
인공지능, Edge 컴퓨팅, 레이다 시스템

조 기 환(Gi-Hwan Cho) [정회원]

- 1985년 : 전남대학교 계산통계학과 학사
- 1987년 : 서울대학교 계산통계학과 석사
- 1987년 ~ 1997년 : ETRI 컴퓨터 연구단 선임연구원
- 1996년 : Univ. of Newcastle 전산학과 박사
- 1997년 ~ 1999년 : 목포대학교 컴퓨터과학과 전임강사
- 1999년 ~ 현재 : 전북대학교 컴퓨터공학부 교수

〈관심분야〉
이동컴퓨팅, 컴퓨터네트워크, 정보보호, 무선인터넷