Journal of KIIT. Vol. 19, No. 2, pp. 89-95, Feb. 28, 2021. pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2021.19.2.89

이미지의 텍스처 분석을 통한 적대적 섭동 후처리 방법

김정훈*, 김영모**[1], 최두현**[2]

Inconspicuous Adversarial Perturbation Post-processing Method with Image Texture Analysis

Jung-Hun Kim*, Young-Mo Kim**[1], and Doo-Hyun Choi**[2]

요 약

최근 들어 심층 신경망은 높은 성능을 보여주고 있지만, 간단한 적대적 공격에도 취약한 공격을 보여주고 있다. 적대적 공격은 영상에 작은 섭동을 첨가하여 신경망이 전혀 다른 결과로 인식하게 한다. 이러한 공격으로 생성한 섭동은 사람이 구분할 수 없을 정도로 본래 이미지에 적절히 섞는 것이 목적이다. 그러나 이러한 공격은 강도가 강해질수록 사람 눈에는 잘 띄게 된다. 본 논문에서는 인지학적 측면에서 섭동이 눈에 덜 띄게 만드는 필터를 만들어 적대적 공격을 통해 생성해낸 섭동에 적용시키는 공격기법을 제안한다. 이미지의 텍스처 분석을 통해 생성한 필터를 기존 공격방법으로 생성된 섭동에 적용하여 이미지의 텍스처가 복잡한 곳에 높은 강도를, 텍스처의 복잡도가 낮은 영역에 상대적으로 낮은 강도의 섭동을 적용시켜 공격이 보다 사람의 눈에 띄지 않도록 하였다. 이를 6가지 적대적 공격 기법에서 실험하였고, 비슷한 세기의 공격에서 기존 공격 기법들보다 섭동 특유의 노이즈가 눈에 덜 띄는 모습을 보였다.

Abstract

In recent years, deep neural networks have shown high performance, but they have also shown vulnerabilities. Adversarial attacks add small perturbations to the image, causing the neural network to recognize them as different results. The perturbations generated by these attacks are indistinguishable from the human. However, these attacks become more visible to the human as they become more intense. In this paper, we propose a filter that makes perturbations less noticeable in terms of cognition. Filters generated through texture analysis of images are applied to perturbations generated by conventional attack methods. The application of perturbations with relatively high strength in areas with complex textures and weak intensity in low places reduces the recognition of perturbations. Experiments on 6 adversarial attack methods showed less perturbation noise compared to conventional attack methods.

Keywords

artificial intelligence, deep learning, adversarial attack, adversarial examples, human vision perception

* 경북대학교 전자공학과 석.박사통합과정
- ORCID: https://orcid.org/0000-0002-5418-6790
** 경북대학교 전자공학부 교수(**[1]교신저자)
- ORCID[1]: https://orcid.org/0000-0003-1600-2732
- ORCID[2]: https://orcid.org/0000-0002-4950-8863

· Received: Jan. 27, 2021, Revised: Feb. 19, 2021, Accepted: Feb. 22, 2021

· Corresponding Author: Young-Mo Kim
School of Electronics Engineering.. Kyoungbook University, 80 Daehakro, Bukgu, Daegu 41566
Tel.: +82-53-950-5541, Email: ymkim@ee.knu.ac.kr

Ⅰ. 서 론

컴퓨터 비전 분야에서 컨볼루션 신경망(CNN)[1]-[3]은 이미지 특징 추출에 널리 사용되며 대부분의 컴퓨터 비전 분야에서 높은 성능으로 인정받고 있다. 그러나 일반적으로 딥 러닝 알고리즘은 두 가지 단점이 지적 되고 있다. 첫 번째는 딥 러닝 알고리즘에 내재된 불확실성[4] 이고, 두 번째는 훈련된 딥 러닝 모델의 추론결과를 설명할 수 없다는 블랙박스적 특징이다[5].

그 중 불확실성 문제로 인해 최신 신경망 모델을 포함한 여러 머신 러닝 모델이 적대적 공격에 매우 취약한 것으로 나타났다. Szegedy 등은 딥 러닝 모델은 다양한 컴퓨터 비전 분야에서 높은 성능을 보여주지만 이미지 분류 문제에서 흥미로운 약점을 제시한다[6].

논문에서 딥 러닝 모델의 높은 분류 정확도에도 불구하고 인간의 눈으로 거의 인식할 수 없는 약간의 섭동을 추가하면 이미지의 분류 결과가 바뀌었다는 것을 보여주었다. 이러한 적대적 공격을 통해 생성된 이미지, 즉 적대적 사례는 딥 러닝 모델 개발에서 중요한 문제로 간주된다. 이러한 문제를 해결하기 위해 최근 많은 연구가 이루어지고 있다[7]-[9].

그러한 적대적 공격에 의해 생성 된 섭동의 주요 목적 중 하나는 인간에게 보이지 않는 것이다. 대부분의 연구에서 섭동의 가시성의 정도는 L^p norm 형태로 측정하고 있다. 그러나 이러한 제약조건은 실제 섭동이 인간 지각하는 변화와 차이가 있다. 일반적인 디지털 거리는 인간 인식의 뉘앙스를 반영하지 않고 있다. 그림 1에서는 이러한 적대적 사례의 데이터 셋에서 같은 제약조건의 공격이더라도 섭동이 눈에 띄는 정도는 서로 다른 것을 확인 할 수 있다[10].

본 논문에서는, 공격에 사용된 섭동 특유의 텍스처를 효과적으로 숨기기 위해 시각 인지적 측면으로 접근하였다[11][12]. 적대적 섭동들은 대개 색조가 강한, 복잡한 형태의 노이즈 텍스처로 이루어져 있다. 게슈탈트 이론에서는 인간의 주의가 다른 요소들과는 다르게 보이는 요소들에 대비에 집중되는 것을 설명한다[13][14].

그림 1. 동일한 제약조건으로 공격한 적대적 사례
Fig. 1. Adversarial examples attacked with the same constraints

따라서 이러한 논문들에 기반하여 이미지 분석을 통해 적대적 사례들에서 섭동이 인지되기 쉬운 부분들에 대하여 섭동을 차등 적용시키는 방법을 제안한다.

본 논문의 구성은 다음과 같다. 1장에서는 연구의 배경 및 목적에 대해 서술하였다. 2장에서는 이론적 배경 및 알고리즘에 대해 설명하고 3장에서는 제시하는 알고리즘에 대해 설명한다. 4장에서는 실험에 사용한 데이터 및 조건들을 정리하고 실험 내용 및 결과를 분석한다. 5장에서는 본 논문에서 제안한 시스템 구성에 대한 결론을 내리고 향후 연구 방향을 제시한다.

Ⅱ. 이론적 배경

2.1 적대적 공격 알고리즘

적대적 공격은 특정 노이즈 또는 섭동을 생성하여 신경망 분류기의 정확도를 줄이거나, 오 분류를 유도하는 방법이다. Goodfellow등이 2014년 처음 FGSM[15]을 제안한 이래로 다양한 방법론이 나왔다. 그 중 대표적인 방법은 CW[16], PGD[17], 등이 있다. FGSM(Fast Gradient Signed Method)은 기존 신경망의 학습 방법인 경사 하강법을 역전시키는 방법이라고 할 수 있으며, 경사의 반대 부호방향으로 손실함수를 증가시킨다. 적대적 예제 x^{adv}에 대한 식은 다음과 같다.

$$x^{adv} = x + \epsilon \cdot \ sign(\nabla_x J(\theta, x, y)) \quad (1)$$

(1)의 ϵ가 증가하면 생성된 섭동의 강도가 강해

지는 것으로 해석할 수 있으며 θ는 모델의 가중치, x는 Input image, y는 x에 대한 Label을 나타낸다. $J(\theta,x,y)$는 Optimization loss이다. FGSM은 신경망 분류기를 효과적으로 방해하는 대표적인 one-step 공격 알고리즘이다.

CW(Carlini and Wagner) 공격 알고리즘은 Carlini와 Wagner가 제안한 공격 방법으로 FGSM만큼 자주 사용되는 공격방법이다. L_0, L_2, L_∞세가지 측면에서 공격하는 방법을 제안하여 섭동의 크기를 작게 만들어 공격하였다. 목적함수 CW는 적대적 공격에 대한 방어 수단으로 제안된 Defensive distillation의 한계를 지적하고 있으며, 높은 공격성능을 보여준다.

Madry등은 MinMax 함수를 활용하여 적대적 공격을 가하고, 적대적 훈련을 통해 공격에 대해 강건한 모델을 생성하는 방법인 PGD(Projected Gradient Descent) 공격을 제안하였다. $\|\delta\|_\infty \leq \epsilon$를 만족하는 노이즈 집합에서 반복적으로 FGSM 알고리즘을 이용하여 δ를 갱신하는 알고리즘이다.

III. 텍스처 분석을 통한 후처리 방법

3.1 Superpixel segmentation

슈퍼 픽셀 Segmentation은 컴퓨터 비전 전처리에서 다양하게 사용되어왔다. 이러한 영상 분할 기법은 이미지에서 물체에 해당하는 영역을 추출하는 과정으로 이미지 분석을 위한 필수적인 단계라고 할 수 있다. 슈퍼 픽셀을 이용하여 이미지에서 비슷한 특성을 가진 화소들을 묶을 수 있는데, 이렇게 묶여진 영역들을 기본단위로 하여 영상처리를 한다. 여기서 작게 나눠진 영역을 슈퍼픽셀이라고 한다. 슈퍼 픽셀은 밀집성(Compactness), 경계일치도(Boundary precision/recall), 과소분할(Undersegmentation)의 최소화, 균일성(Uniformity)등의 특징이 요구된다[18].

슈퍼픽셀을 구하는 방법에 따라 그래프 기반 방법과 기울기 기반 방법이 있다. 본 논문에서는 기울기 방법 중 가장 최근에 제안된 방법인 SLIC (Simple Linear Iterative Clustering)[19]를 사용하였다. (L, a*, b*, x, y)의 5차원 특징공간에서 슈퍼픽셀을 구하는 방법으로 O(N)의 복잡도를 가지는 속도가 빠른 알고리즘이다.

3.2 텍스처 분석

Gianluigi Ciocca등은[20] 인지학적 측면에서 이미지의 텍스처의 복잡성 인식에 대해 연구하였다. 이를 위해 13가지 복잡성 척도를 설문 조사를 통해 테스트하였고 그 중 높은 피어슨 상관계수를 보여주는 것은 Energy, Edge density[21], Compression ratio[22], Feature congestion이었다. 여기서 Energy 측도는 Grey Level Co-occurrence Matrix (GLCM)의 제곱 합이고 Edge density는 에지 검출기를 그레이스케일 이미지에 적용시켜 얻은 것이다.

Compression ratio는 JPEG로 압축된 이미지와 압축되지 않은 이미지의 비율이며 Feature congestion은 색상, 질감, Orientation congestion 세 가지 척도를 적절하게 결합하여 단일 측정값을 얻은 것이다. 본 논문에서는 그 중 가장 높은 상관계수를 가졌던 Edge density 방법을 사용하여 SLIC를 통해 도출된 이미지의 Segmentaion 영역에서의 텍스처 복잡도를 계산하였다. 그림 2는 원본 이미지에 대한 SLIC Segmentation후 해당 영역에 대한 Edge density를 시각적으로 나타낸 결과이다.

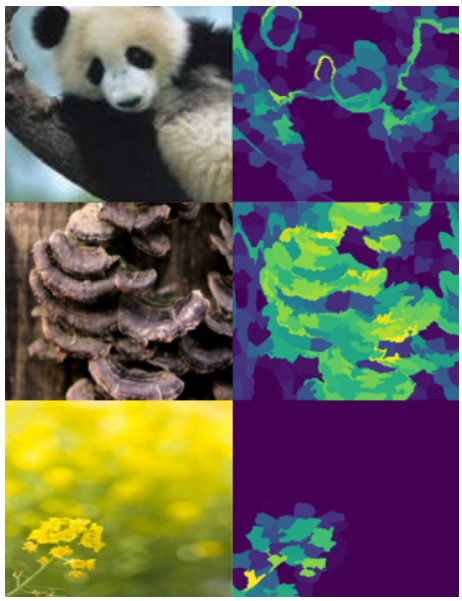

그림 2. SLIC segmentation 영역의 edge density
Fig. 2. Edge density of each segmentation area

3.3 텍스처 분석을 통한 후처리 방법

제안하는 알고리즘의 순서는 다음과 같다. 우선 원본 이미지에다 슈퍼 픽셀 Segmentation을 통해 나온 영역에 대한 텍스처를 분석하여 이미지의 텍스처 맵을 만든다. 이 때 최대 Segmentation 갯수는 200개로 설정하였다.

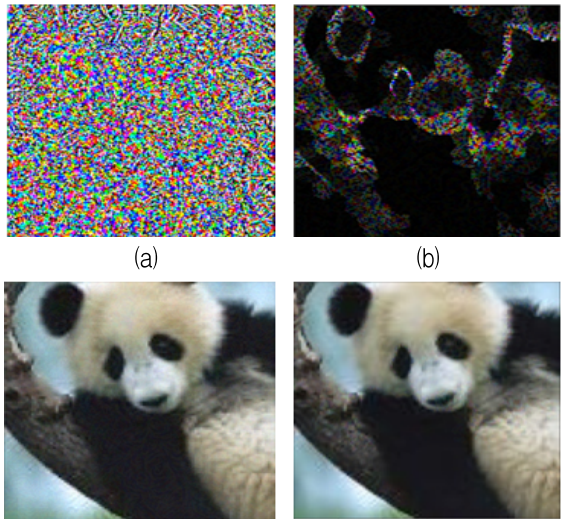

그림 3. FGSM 공격과 텍스처 필터를 사용한 결과 비교
Fig. 3. Comparison of perturbation (b) using FGSM attack result (c) and using texture filter perturbation (b) result (d)

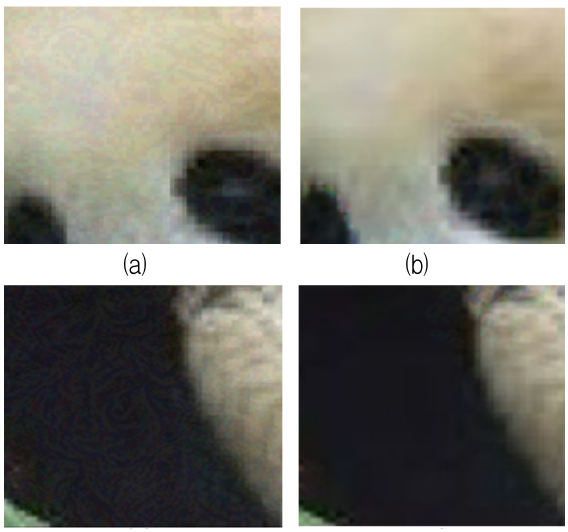

그림 4. 그림 3(c)을 확대한 영역 (a), (b)와 그림 3(d)을 확대한 영역 (c), (d)의 텍스처 비교
Fig. 4. Texture comparison of the cropped area (a) and (b) in Fig. 3(c) and the cropped area (c) and (d) in Fig. 3(d)

이후, 공격 과정에서 생성한 섭동을 원본 이미지에 적용할 때 텍스처 맵을 사용하여 차등 적용시킨다. 제안하는 적대적 예제에 대한 식은 다음과 같다.

$$x^{adv} = x + \epsilon \cdot \ k \cdot \ F \cdot \ sign(\nabla_x J(\theta, x, y)) \qquad (2)$$

여기서 F는 계산한 텍스처 맵을 의미하며, k는 기존 공격과 동일한 LSE(least squares error)을 가지게 하기 위한 값이다. 이는 공격을 통해 달라지는 공격 강도를 기존 공격과 동일한 수준으로 맞추어 주는 역할을 한다. 기존 실험에 사용되는 공격들은 L_∞ norm 형태의 제약조건으로 섭동의 공격의 강도를 결정하는데, 본 논문에서 제안하는 공격은 한 이미지에서 여러 강도의 세기를 가지는 특징을 가지고 있기 때문에, 같은 제약조건으로 비교하면 공격의 강도가 약해지는 결과가 나타난다. 이를 위해 본 실험에서는 L_2 norm 측면으로 비교하였다. 따라서 기존 공격강도와 비슷한 공격을 위해 해당 알고리즘을 사용한 공격의 강도는 기존 공격과 동일한 Least Squares Error(LSE)를 가지도록 한다.

그림 3은 그림 1의 첫 번째 이미지에 대한 FGSM 공격으로 인한 (a)섭동과 (c)결과 이미지, 그리고 생성한 텍스처 맵을 이용하여 생성한 섭동이미지(b)를 사용하여 공격한 결과 이미지 (d)를 보여준다. 그림 4는 그림 3(c)와 3(d)의 상 하단 부분을 확대한 결과이다. 기존 공격인 (a), (c)에 비해 (b), (d)는 섭동 특유의 섭동이 안 보이는 것을 확인 할 수 있다.

Ⅳ. 실험 및 평가

4.1 실험 환경

실험에 사용된 코드는 딥러닝 프레임워크인 Pytorch를 사용해서 작성되었다. 또한, 실험에 사용된 컴퓨터는 Intel Zeon@4.20GHz CPU, 128GB 메모리 그리고 NVIDIA RTX Titan GPU 3대로 구성하였다. 데이터 셋으로는 ImageNet[23] 데이터셋을 사용하였다. 전체 데이터셋을 사용하기엔 컴퓨터 자원의 한계가 있어 1,000 클래스에 대해 각 3장의 랜덤 이

미지로 구성된 평가 데이터 셋을 사용하였다. 모든 사진은 299×299 사이즈로 리사이징 하였다.

4.2 공격 모델

베이스 라인 분류기 모델은 추가학습 없이 Pretrained된 Resnet50[24]이 사용되었다. 해당 분류기의 ImageNet 데이터 셋에 대한 기본 분류 정확도는 92.56%로 높은 정확도를 보여준다.

공격 모델은 FGSM[15]와 FGSM기반 알고리즘인 FFGSM[25], RFGSM[26]과 PGD[17]와 PGD기반 알고리즘인 APGD[27], TPGD[28]을 사용하여 검증였다. 6가지 공격 모델 모두 L_∞ Distance measure을 사용하는 white-box 공격모델이다.

표 1은 각 모델에서 사용한 파라미터를 제시한다. one-step공격이 아닌 경우 7 step으로 모두 설정하였고 적대적 공격에 대한 공격반경 값인 ϵ 값과 반복 공격의 경우 step 사이즈 α 값은 공격에 대한 강건성이 0%이상이 나오도록 설정 하였다.

표 1. 적대적 공격 모델과 파라미터
Table 1. Parameters of adversarial attack models

Attack models	ϵ	α	step
FGSM	3/255	.	.
FFGSM	3/255	12/255	.
RFGSM	4/255	4/255	7
PGD	4/255	2/255	7
APGD	4/255	2/255	7
TPGD	4/255	2/255	7

4.3 실험 결과

표 2는 공격에 대한 결과를 제시한다. 여기서 Accuracy는 해당 공격모델을 통해 생성된 적대적 이미지들의 데이터 셋에 대한 사전 학습된 Resnet50의 정확도이며, 적대적 모델이 강력할수록 오 분류를 유발하기 때문에 Accuracy는 낮아진다. 실험에서 사용한 6가지 공격 모델의 공격성능은 각각 차이가 있으나 비슷한 성능을 가지도록 성능을 조정하였다. 기존 6가지 적대적 모델들에 본 논문에서 제안하는 알고리즘을 적용한 후에도 비슷한 Accuracy를 유지하는 것을 볼 수 있다. 제안하는 알고리즘은 섭동 특유의 시각적 노이즈 패턴을 최소화 하면서도 기존 공격 모델과 마찬가지로 기존 강력한 분류기에 대해 매우 높은 공격성능을 유지하고 있다. 하지만 제안하는 알고리즘은 CPU을 사용하는 특성상 기존 방식에 비해 처리 속도는 늦은 모습을 보여주고 있다. 이는 앞으로 많은 데이터를 대상으로 공격할 경우 GPU상에서 처리하는 등의 기법을 활용하여 속도를 개선해야 될 점이다.

표 2. 실험결과
Table 2. Experiment result

Attack models	Original		Original + texture filtering	
	Accuracy (%)	Elapsed time per image (sec)	Accuracy (%)	Elapsed time per image (sec)
FGSM	20.42	0.01	18.78	2.97
FFGSM	16.72	0.01	16.28	3.29
RFGSM	8.48	0.01	5.72	3.81
PGD	16.84	0.04	17.70	3.29
APGD	12.75	0.36	11.87	3.45
TPGD	12.59	0.06	13.78	3.15

V. 결론 및 향후 과제

본 논문에서는, 이미지의 텍스처를 분석하여 기존 적대적 공격의 특유의 노이즈 패턴이 눈에 띄지 않게 하는 필터를 제안하였다. 이를 위해 SLIC 알고리즘을 통해 이미지의 영역을 나눠 텍스처 패턴을 분석하였으며, 기존 공격과 동일한 L_2 Distance measure를 가지도록 하였다. 제안한 방법은 기존 L_∞ norm 공격 모델들에 적용하여 노이즈 식별에 대한 더 나은 성능을 보였다.

본 논문에서는 기존에 시도되지 않았던 적대적 공격의 본질에 대해 접근하여, 인지학적 측면에서 공격이 더 잘 보이지 않도록 하는 방법을 제안했다는 점에서 연구의 의의를 찾을 수 있다. 그러나 공격 단계에서 이미지 분석을 한 것이 아닌 필터를 사용하여 후처리를 통한 방법이라는 점과 CPU에서 처리함으로써 발생하는 병목현상으로 인한 비교적 느린 처리속도, 설문조사 등을 통한 방법이 아닌 시각에 눈에 띄는 정도를 정량적으로 계산할 수 있는

방법이 아직 없다는 점 등에서 본 연구의 한계를 찾을 수 있다. 따라서 이들 한계점을 극복하기 위한 연구를 본 논문의 향후 과제로 한다.

References

[1] Y. LeCun, Y. Bengio, and G. E. Hinton, "Deep learning", Nature 521. pp. 436-444, 2015.

[2] A. Krizhevsky, I. Sutskever, and G. E. Hinton. "Imagenet classification with deep convolutional neural networks", Communications of the ACM, Vol. 60, No. 6, May 2017. https://doi.org/10.1145/3065386

[3] K. He, X. Zhang, and J. Sun, "Deep residual learning for image recognition", Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Las Vegas, Nevada, pp. 770-778, Jun. 2016.

[4] Y. Gal, "Uncertainty in deep learning", PhD thesis, 2016.

[5] A. Holzinger, "From Machine Learning to Explainable AI", 2018 World Symposium on Digital Intelligence for Systems and Machines (DISA), Kosice, Slovakia, pp. 55-66, Aug. 2018.

[6] C. Szegedy, W. Zaremba, and I. Sutskever, "Intriguing properties of neural networks", arXiv:1312.6199, Dec. 2013.

[7] K. Eykholt, I. Evtimov, and E. Fernandes, "Robust physical-world attacks on deep learning visual classification", Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Salt Lake City, Utah, pp. 1625-1634, Jun. 2018.

[8] N, Papernot, P. McDaniel, and X. Wu, "Distillation as a defense to adversarial perturbations against deep neural networks", In 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, pp. 582-597, May 2016.

[9] F Haque, D S Kang, “Deep Adversarial Residual Convolutional Neural Network for Image Generation and Classification”, Korean Institute of Information Technology, Vol. 10, No. 1, Jul. 2020.

[11] J. Shen, "On the foundations of vision modeling. I. Weber’s law and Weberized TV restoration", Physica D: Nonlinear Phenomena, Vol. 175, No. 3-4, pp. 241–251, Feb. 2003.

[12] J. Shen, "On the foundations of vision modeling. II. Mining of mirror symmetry of 2-D shapes", Journal of Visual Communication and Image Representation, Vol. 16, No. 3, pp. 250-270, Jun. 2005.

[13] M. Wertheimer, "Laws of organization in perceptual forms", in A Sourcebook of Gestalt Psychology, pp. 71–88, 1938. https://doi.org/10.1037/11496-005.

[14] I. Kovacs, "Gestalten of today: early processing of visual con- tours and surfaces", Behavioural Brain Research, Vol. 82, No. 1, pp. 1–11, Dec. 1996.

[15] I. J. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and harnessing adversarial examples", arXiv:1412.6572, Dec. 2014.

[16] N. Carlini and D. Wagner, "Toward sevaluating the robustness of neural networks", IEEE symposium on security and privacy, San Jose, CA, USA, pp. 39-57, May 2017.

[17] A. Madry, A. Makelov, and L. Schmidt, "Towards deep learning models resistant to adversarial attacks", arXiv:1706.06083, Jun. 2017.

[18] J. H. Lee, "A Setting of Initial Cluster Centers and Color Image Segmentation Using Superpixels and Fuzzy C-means(FCM) Algorithm", Journal of Korea Multimedia Society, Vol. 15, No. 6, pp. 761-769, Jun. 2012.

[19] R. Achanta, A. Shaji, and K. Smith, "SLIC Superpixels", EPFL Technical Report, pp. 1-15, 2010.

[20] G. Ciocca, S. Corchs, and F. Gasparini, "Complexity Perception of Texture Images", ICIAP 2015 Workshops, Genoa, Italy, pp.

119-126, Sep. 2015.

[21] M. L. Mack, and Oliva A., "Computational estimation of visual complexity", The 12th annual Object, Perception, Attention, and Memory Conference, Minneapolis, Nov. 2004.

[22] D. Comaniciu and P. Meer, "Mean shift: A robust approach toward feature space analysis and the edge detection algorithm", IEEE Transactions on Pattern Analysis nd Machine Intelligence, Vol. 24, No. 5, pp. 603-619, May. 2002.

[23] J. Deng, W. Dong, and R. Socher, "ImageNet: A large-scale hierarchical image database", Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Miami, FL, USA, pp. 248-255, Jun. 2009.

[24] K. He, X. Zhang, and S. Ren, "Deep Residual Learning for Image Recognition", Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Las Vegas, Nevada, pp. 770-778, Jun. 2016.

[25] E. Wong, L. Rice, and J. Zico Kolter, "Fast is better than free: Revisiting adversarial training", arXiv:2001.03994, Jan. 2020.

[26] F. Tramèr, A. Kurakin, and N. Papernot, "Ensemble Adversarial Training : Attacks and Defences", arXiv:1705.07204v5, May 2017.

[27] S. Roland. Zimmermann, "Adv-BNN: Improved Adversarial Defense through Robust Bayesian Neural Network", arXiv:1907.00895, Jul. 2019.

[28] C. Szegedy, V. Vanhoucke, and S. Ioffe, "Rethinking the Inception Architecture for Computer Vision", Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Las Vegas, Nevada, pp. 2818-2826, Jun. 2016.

저자소개

김 정 훈 (Jung-Hun Kim)

2018년 2월 : 경북대학교 컴퓨터학부 학사
2018년 2월 ~ 현재 : 경북대학교 전자공학과 석·박통합과정
관심분야 : 신호처리, 인공지능 보안, AutoML

김 영 모 (Young-Mo Kim)

1976년 2월 : 경북대학교 전자공학과 학사
1983년 2월 : KAIST 전자공학과 석사
1989년 8월 : KAIST 전자공학과 박사
1992년 3월 ~ 현재 : 경북대학교 전자공학부 교수
관심분야 : 영상처리, 인공지능

최 두 현 (Doo-Hyun Choi)

1991년 2월 : 경북대학교 전자공학과 졸업
1993년 2월 : Postech 전기전자공학과 석사
1996년 8월 : Postech 전기전자공학과 박사
2003년 3월 ~ 현재 : 경북대학교 전자공학부 교수
관심분야 : 지능신호처리, 소프트컴퓨팅