CT 데이터 위조 생성 및 검출 모델의 성능 비교에 관한 연구

최민지, 허용도*
건양대학교, *건양대학교
miiiingzz112@gmail.com, *ydher@konyang.ac.kr

A Study on the Performance Comparison of CT Data Forgery Creation and Detection Model

Choi Min-Ji, Her Yong-Do*
Konyang Univ., *Konyang Univ.

요 약

전 세계적으로 딥 러닝 연구가 활발하게 진행되는 와중에 의료 분야에서 딥 러닝을 활용해 이를 악용하는 사례가 발생하고 있다. 본 논문은 위조 CT 이미지를 생성하고 생성된 데이터와 실제 데이터를 검출해내는 모델을 구축한다. 생성 모델로 DCGAN과 Cycle-GAN을 사용해 합성 데이터 품질을 평가한다. 검출 모델로 ResNet과 CNN을 사용해 수치를 정량적으로 나타내어 두 모델의 성능을 비교하여 검출 모델의 성능이 뛰어남을 증명하였다. 이를 통해 위조 문제를 방지할 수 있다.

Ⅰ. 서론

전 세계적으로 딥 러닝 연구가 활발하게 진행되고 있다. 인공지능은 사물 인식, 번역기, 자율 주행, 스마트폰 인식, 의료 산업 등 광범위하게 연구가 진행 중이다. 특히, 의료 분야에서 환자의 임상 정보나 전염병 등 다채롭게 빅데이터를 분석 및 활용하고 있다. 또한, 제약회사는 인공지능을 통해 질환과 유전자, 대사, 신규 후보물질 생성 등을 하도록 준비하고 있다[1]. X선 촬영, CT(Computed Tomography) 촬영, 자기공명영상(MRI; Magnetic Resonance Imaging) 사진을 분석해 증상을 초기에 짚어내 질병의 조기 발견 확률을 높일 수 있다[2]. 또한, 병원이 보유한 X선 촬영 영상에 딥 러닝 기술을 접목할 수 있다는 것이다. 딥 러닝의 발전으로 이로운 점이 많지만 해로운 점도 잇따른다. 이스라엘의 벤구리온대학과 소로카 대학병원은 한 가지 실험을 진행했는데 해킹을 통해 CT 검사 결과를 조작할 수 있는지에 대한 여부였다[3]. GAN(Generative Adversarial Network)이라는 머신러닝 기술을 통해 CT 스캔 이미지 조작에 성공했다. 환자의 CT 이미지 원본에 GAN 기술을 활용해 인위적으로 폐 결절을 주입한 것이다. 이처럼 CT 이미지의 조작 가능성은 여러가지 문제를 발생시킨다. 예를 들어, 의도적으로 의료인의 오진을 꾀해 범죄 등에 활용할 수 있다. 그리고 장애나 희귀 난치 질환을 의도적으로 진단받아 군 면제에 이용하거나 복지시스템을 악용할 수 있다는 것이다. 따라서 본 논문은 딥 러닝을 통해 CT 이미지 위조 및 검출 모델을 제시해 각 성능을 비교한다.

Ⅱ. 본론

(1)활용데이터

연구에 활용한 데이터는 간 병변 CT 데이터로 CANCER IMAGING ARCHIVE 데이터를 사용하였다. Open Dataset으로 CT 데이터 파일 형식은 DICOM(Digital Imaging and Communications in Medicine)으로 구성되어 있다. 이 데이터는 이미지 크기를 (128, 128) 사이즈로 모두 변환하였으며 정상 간 CT 데이터는 6,084개, 간 병변 CT 데이터는 6,271개를 사용하였다. 데이터의 비율을 8:2로 나누어 모델 학습과 이미지 위조 생성에 사용하였다.

(2)데이터전처리

본 연구에서는 첫 번째로 데이터를 Grayscale을 이용해 회색조로 만들었다. 두 번째로 대비 제한 히스토그램 평준화 중 CLAHE(Contrast Limited Adaptive Histogram Equalization) 전처리 방식을 사용하였다. 이는 변환된 이미지의 특성 변화와 노이즈를 최소화할 수 있다. 그림 1의 (A)는 원본 이미지이고 (B)는 CLAHE 전처리를 적용한 것이다.

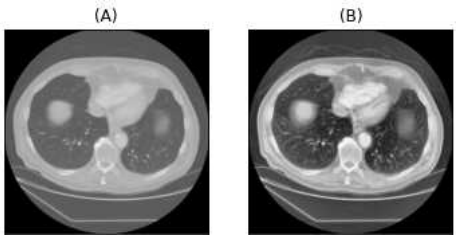

그림 1. CLAHE 전처리 이미지 비교

(3)모델구성및결과

본 연구의 생성 모델에서 사용한 방법은 DCGAN과 Cycle-GAN이다. 검출 모델에서 사용한 방법은 ResNet과 CNN이다. 동일한 전처리 방식으로 진행된 데이터셋을 이용하였으며 각각의 모델에 데이터를 학습시켰다. DCGAN은 Generator와 Discriminator 구조에 CNN을 적용시킨 것으로 Generator는 noise를 입력받아 가짜 이미지를 생성하고 Discriminator는 입력받은 이미지를 진짜와 가짜 이미지로 식별하는 이진 분류를 수행한다[4]. Cycle-GAN의 구조는 그림 2와 같다. Cycle-GAN은 각각 두 개의 Generator와 Discriminator가 존재하며 정상과 병변 간을 비교하여 차이를 책정해 학습을 진행한다. 그림 3은 원본 이미지와 위조 생성된 이미지이다. 두 이미지를 비교하면 차이를 느낄 수 있다.

ResNet은 VGG-19의 구조를 기반으로 Convolution Layer와 Residual

block을 추가한 것이다. 많은 Layer를 가질수록 ResNet의 성능이 높아지는 것을 확인했다. 하지만 PC의 한계로 인해 ResNet의 성능이 잘 나오지 않았다. CNN은 Concatenate Layer를 추가하여 사용하였다[5]. Concat block을 3번 추가하고 Flatten과 Fully Connected를 거쳐 Real과 Forgery를 분류하였다.

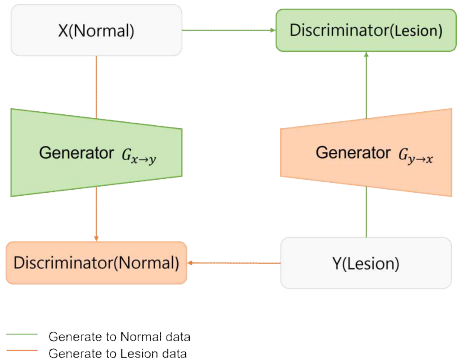

그림 2. Cycle-GAN 구조

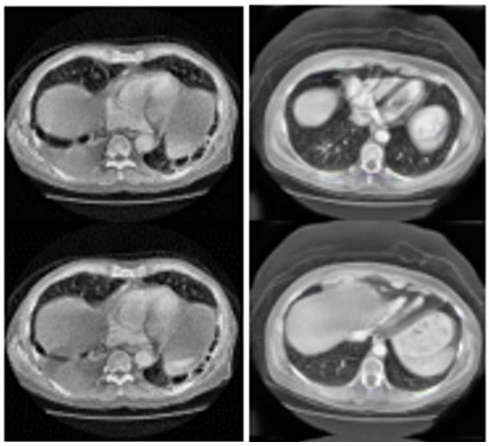

그림 3. 원본 이미지와 위조 이미지

위조 CT 이미지를 평가하기 위해 RMSE와 SSIM, FID를 사용하였으며 DCGAN과 Cycle-GAN의 평가 지표를 표 1과 같이 나타내었다. 성능은 DCGAN보다 Cycle-GAN이 더 우수함을 보였다.

표 1. 위조 CT 이미지 평가 지표

	RMSE		SSIM		FID	
	Normal	Lesion	Normal	Lesion	Normal	Lesion
DC GAN	63.35	61.47	0.21	0.23	98.12	107.28
Cycle-GAN	52.73	50.01	0.25	0.26	90.02	102.64

검출 모델을 평가하기 위해 Precision과 Recall, F1-Score를 사용하였으며 ResNet보다 CNN이 더 높은 성능을 보였다. 이 평가 지표를 통해 모델 성능을 정량적으로 수치를 확인할 수 있었으며 본 연구의 검출 모델 성능이 뛰어나다는 것을 볼 수 있다.

표 2. 검출 모델 성능 평가 지표

	Precision		Recall		F1-Score	
	Train	Test	Train	Test	Train	Test
ResNet	0.97	0.96	0.96	0.97	0.98	0.97
CNN	0.99	1.00	1.00	0.99	1.00	1.00

Ⅲ. 결론

본 논문에서는 딥 러닝 기술을 활용하여 위조 CT 이미지를 생성해 위조 이미지를 통해 발생할 수 있는 문제를 방지하기 위하여 검출 모델을 구성하였다. DCGAN과 Cycle-GAN을 사용하여 CT 이미지 데이터를 생성하고 ResNet과 CNN을 사용하여 위조 이미지 검출 모델을 사용하여 각각 비교하였다. 그 결과 Cycle-GAN과 CNN을 사용하였을 때 테스트 값은 Precision 0.99, Recall 0.99, F1-Score 1.00이며 학습 값은 Precision 0.99, Recall 1.00, F1-Score 1.00으로 가장 높은 성능을 보였다. 위조 CT 이미지 품질 평가 지표에서는 원본과 위조 간의 차이가 컸으나 이는 CT 데이터 특성상의 문제로 볼 수 있다. CT 데이터는 연속적인 슬라이드 형태로 구성되어 슬라이드 각각은 독립적이지 못하다. 연속성을 일정 개수 내에서 보이며 슬라이드 개수도 불분명하다. 또한, 검출 모델의 분류 성능 평가 지표는 성능이 높았으며 검출 모델의 성능이 뛰어난 것을 확인할 수 있다. 검출 모델을 통해 위조 CT 데이터를 판별하여 악용하는 사례를 방지하고 해결할 수 있을 것이다.

ACKNOWLEDGMENT

본 성과는 교육부와 한국연구재단의 재원으로 지원을 받아 수행된 3단계 산학연협력 선도대학 육성사업(LINC 3.0)의 연구 결과입니다(NTIS 과제번호. 1345356198).

참 고 문 헌

[1] Guk G. W, “Application cases by AI technology and industry”, Information and Communication Planning and Evaluation Institute, Vol. 15, No. 27, 2019.

[2] Kidwell, Chelsea S., et al. "Comparison of MRI and CT for detection of acute intracerebral hemorrhage.", 1823-1830, 2004.

[3] Moon G. Y, “If you hack into a medical scanner, you can make cancer that didn't exist”, 2019. (https://www.boannews.com/media/view.asp?idx=78493)

[4] Fang, Wei, et al. "A method for improving CNN-based image recognition using DCGAN." Computers, Materials and Continua, 167-178, 2018.

[5] H-J. Song, and K-W. Song. A study on the reproduction of fundus image using U-Net model, KOREA knowledge information technology society, Vol. 17, No. 3, pp. 435-443, 2022.