

인공지능 기반 COVID-19 진단 시스템 보안에 관한 연구

손인수

동국대학교 전자전기공학부

isohn@dongguk.edu

A Study on the Security of AI based COVID-19 Diagnosis Systems

Insoo Sohn

Dongguk University

1. 서론

의료 영상은 의학에 혁신적인 영향을 미치며 인체 장기, 세포 및 병리학 적 표본을 영상화하여 질병을 진단한다. 인공지능에서 가장 효율적인 인공지능망 기술 중 하나인 심층 신경망(DNN)을 응용하여 최근 의료 영상 분야에서 의료진단 개선에 효과를 보고 있다. COVID-19 진단 분야에서도 인공지능 기반 지능형 진단 기법에 대한 연구가 활발하게 연구가 되고 있으며 또한 AI 기반 COVID-19 시스템에 대한 사이버 공격 및 방어에 대한 연구도 최근에 많은 관심을 받고 있다.

2. 본론

2.1 인공지능 기반 COVID-19 시스템 데이터

인공지능 기반 예측 및 분석 시스템에서 제일 중요한 요소 중 하나는 훈련 데이터이다. COVID-19 진단을 위한 인공지능 기반 시스템도 훈련 데이터가 중요한 역할을 하며 주요 데이터는 영상 기반의 흉부 엑스레이(CXR) 및 컴퓨터 단층촬영(CT-Scan) 이미지 데이터로 구성된다.

AI 기반 COVID-19 진단 시스템의 성능 평가 분석을 위해 사용되는 다양한 Dataset[1] 중에 제일 큰 규모의 샘플 수를 가지고 있는 Open Dataset은 Wang et al.[2]이 제안한 COVIDx 데이터 세트이며 현재까지 가장 큰 오픈 액세스 벤치마크 데이터 세트이다. 본 데이터 세트는 가장 많은 COVID-19 양성 환자의 사례를 기반으로 하며 13,8710 명의 환자의 13,975 개의 CXR 이미지로 구성되어 있다.

2.2 인공지능 기반 COVID-19 시스템 보안

인공지능 시스템에 가장 많이 적용하는 공격 방법은 적대적 훈련 세트를 증가시키는 Adversarial Attack 기법이며 인공지능 기반 COVID-19 시스템 공격을 위해 Qi et al.[3]은 SMIA(Stabilized Medical Image Attack) 공격 방법을 제안하였다.

인공지능 기반 COVID-19 시스템 공격에 대비한 방어기법에 대한 연구는 소수이며 최초로 Hirano et al.[4]은 인공지능 기반 COVID-19 시스템의 보안문제에 대한 분석을 하였다. 또한 CNN(Convolutional Neural Network) 기반 COVIDNet 모델을 COVID-19 공격 탐지를 위해 제안 하였으며 CXR 이미지를 사용하였다.

3. 결론

4 차 산업혁명의 중요한 인공지능 기술 기반의 의료영상 시스템 발전에서 환자의 개인정보 보호는 중요한 문제이며, 지능형 COVID-19 진단 시스템에 대한 사이버 공격에 대한 분석과 대응 기술 개발은 매우 중요하다. 본 논문에서는 최근에 연구되고 있는 AI 기반 COVID-19 시스템에 대한 사이버 공격 기술과 방어 기술을 검토하였다.

ACKNOWLEDGMENT

본 논문은 2018 년도 교육부의 재원으로 한국연구재단(2018R1D1A1B07041981)의 지원을 받아 수행된 기초연구사업입니다.

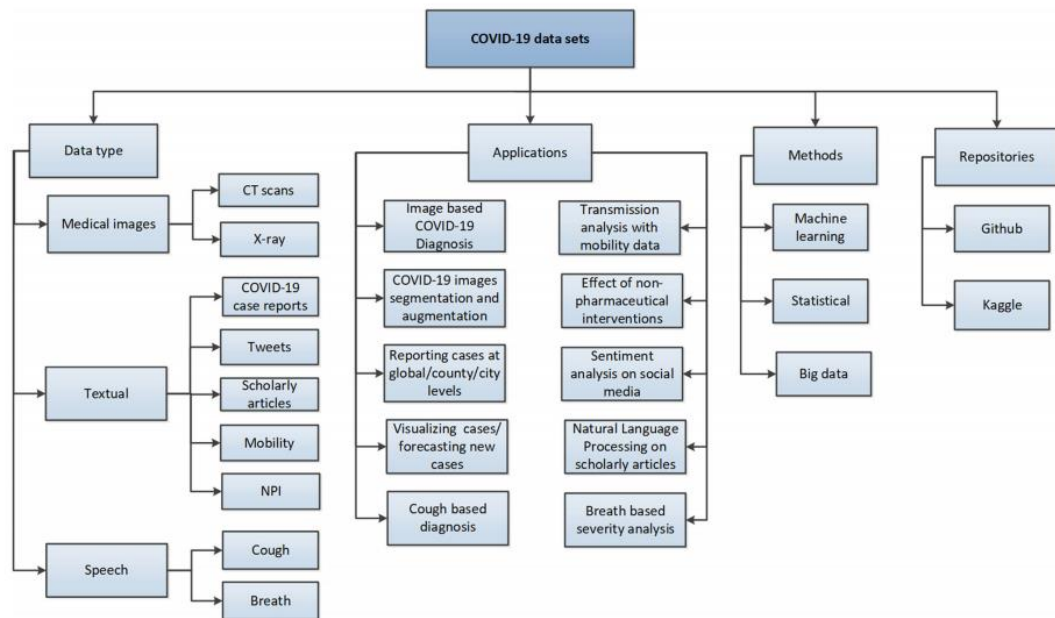


그림 1. COVID-19 Open Dataset [1]

참고 문헌

- [1] J. Shuja, E. Alanazi, W. Alasmay, A. Alashaikh, "COVID-19 open source data sets: a comprehensive survey", Applied Intelligence, pp. 1296–1325, Sept. 2020.
- [2] L. Wang, A. Wong, "COVID-Net: A tailored deep convolutional neural network design for detection of COVID-19 cases from chest radiography images", arXiv preprint arXiv:2003.09871, 2020.
- [3] G. Qi, L. Gong, Y. Song, K. Ma, Y. Zheng, "Stabilized medical image attacks", arXiv preprint arXiv:2013.05232v1, 2021.
- [4] H. Hirano, K. Koga, K. Takemoto, "Vulnerability of deep neural networks for detecting COVID-19 cases from chest X-ray images to universal adversarial attacks", Plos One vol. 15, no. 12, 2020.