딥러닝을 활용한 이상 행동 검출 방법

정현구*, 강현수**

Anomaly Detection Method Using Deep Learning

Jeong Hyeon Gu* and Kang Hyun Soo**

요 약

본 논문은 현대 감시 시스템의 중요성을 고려하여 이상 행동 탐지에 중점을 둔 심층 학습 기반 방법을 제시하였다. 다양한 카테고리('abuse', 'arrest' 등)의 공개 비디오 데이터를 활용하였다. 데이터 확장기법을 적용하여 원본 데이터로부터 다양한 변형된 이미지를 생성하고, 이를 통해 모델의 강인성을 향상시켰다. 또한 정확도 점수 등의 성능 평가 지표를 사용하여 모델의 성능을 평가하였다. 실험 결과, 본 논문의 접근 방식이 감시 시스템에서의 이상 행동 탐지에 효과적인 것을 보여준다.

Abstract

This study presents a deep-learning-based methodology focused on anomaly detection, considering the significance of modern surveillance systems. We utilized publicly available video data spanning various categories as 'abuse' and 'arrest'. By employing data augmentation techniques, we generated various transformed images from the original data, thereby enhancing the robustness of our model. The model's performance was evaluated using metrics like accuracy scores. Experimental results demonstrate the effectiveness of our approach in detecting anomalous behavior in surveillance systems.

Key words

Deep learning, Anomaly detection, Surveillance systems, Data augmentation, Video data, Performance metrics

Ⅰ. 서 론

현대 사회에서 감시 시스템은 사람들의 안전과 재산 보호를 하는 데 중요한 역할을 하게 되었다. 공공장소의 범죄 예방부터 상업 시설의 보안 강화까지, 감시 카메라의 활용은 계속해서 확대되고 있다. 이러한 배경 속에서, 감시 시스템의 효율성을 높이기 위해 이상 행동이나 예상치 못한 사건의 자동 탐지 기술에 대한 필요성이 증가하고 있다.

전통적인 감시 시스템은 대부분의 이상 행동 탐지가 사람에 의해 이루어졌다. 그러나 이러한 방식은 인력과 시간이 많이 소모되며, 지속적인 모니터링 중 주의력 저하로 인해 이상 행동을 놓칠 가능성이 있다. 이에 따라, 자동화된 이상 행동 탐지 기술 연구가 활발히 진행되고 있으며, 특히 심층 학습과 같은 기계 학습 방법론이 주목받고 있다.

* 충북대학교(Chungbuk National Univ.) 정보통신공학부 학부생, wjdgusrn951@naver.com
** 충북대학교 정보통신공학부 교수 hskang@cbnu.ac.kr

※ 이 논문은 과학기술정보통신부 및 정보통신기획평가원의 SW중심대학사업(2019-0-01183)의 지원을 받아 작성되었음

이 연구에서는 다양한 카테고리의 공개 비디오 데이터를 활용하여 감시 시스템에서의 이상 행동을 탐지하기 위한 심층 학습 기반의 방법론을 제안한다. 데이터 확장기법을 통해 학습 데이터의 다양성을 높이고, 제안된 모델의 유효성을 AUC (area under the curve) 지표로 검증한다.

II. 감시 비디오에서의 이상 탐지를 위한 ConvNeXt 적용

본 연구에서는 주요 데이터셋으로 활용한 UCF Crime Dataset 은 감시 비디오에서 발생하는 다양한 범죄 및 정상 활동을 포함하고 있다. 이를 바탕으로 이상 행동 탐지에 적합한 데이터를 구축하였다. 각 비디오로부터 10번째 프레임을 추출하고 이를 클래스별로 집계하여 64x64 크기의. png 이미지로 구성하였다. Abuse, Arrest, Arson, Assault, Burglary, Explosion, Fighting, RoadAccidents, Robbery, Shooting, Shoplifting, Stealing, Vandalism의 13종 범죄 현장과, 1종의 Normal Videos 비범죄 현장으로 구성되어 있다. 훈련 데이터셋에는 1,266,345장으로, 테스트 데이터셋에는 111,308장이 사용되었다. 본 연구의 목표는 이 데이터셋을 활용하여 심층 학습 기반의 이상 행동 탐지 모델을 개발하고, 데이터 확장 기법을 통해 모델의 다양성과 견고성을 높이는 것이다.

실세계의 감시 환경은 다양한 조건과 상황이 공존하므로, 모델의 견고성을 향상시키기 위해 다양한 이미지 변환 기법을 활용하여 데이터 확장을 수행하였다. 본 연구의 핵심은 딥러닝 기반의 아키텍처 ConvNeXt를 활용하여 감시 비디오에서의 이상 행동을 탐지하는 것이다.

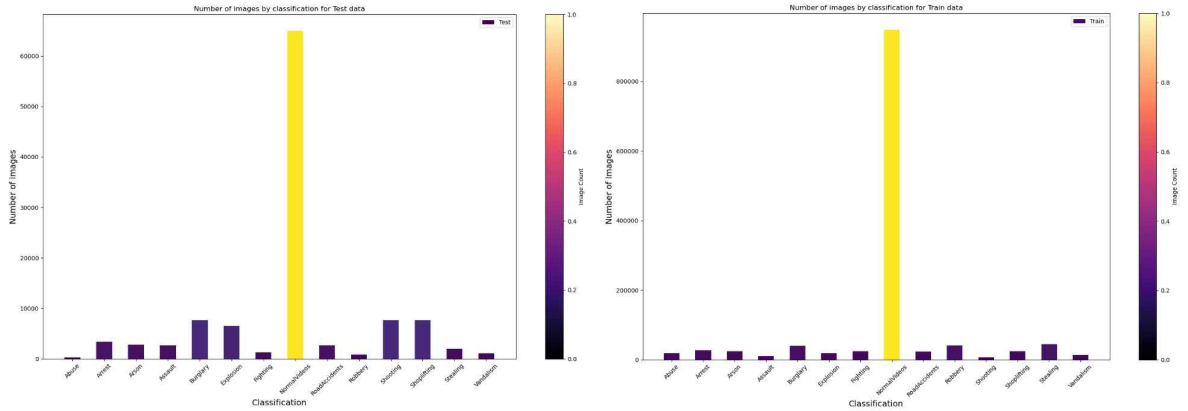

그림 1. 훈련 데이터와 테스트 데이터
Fig. 1. Train data and Test data

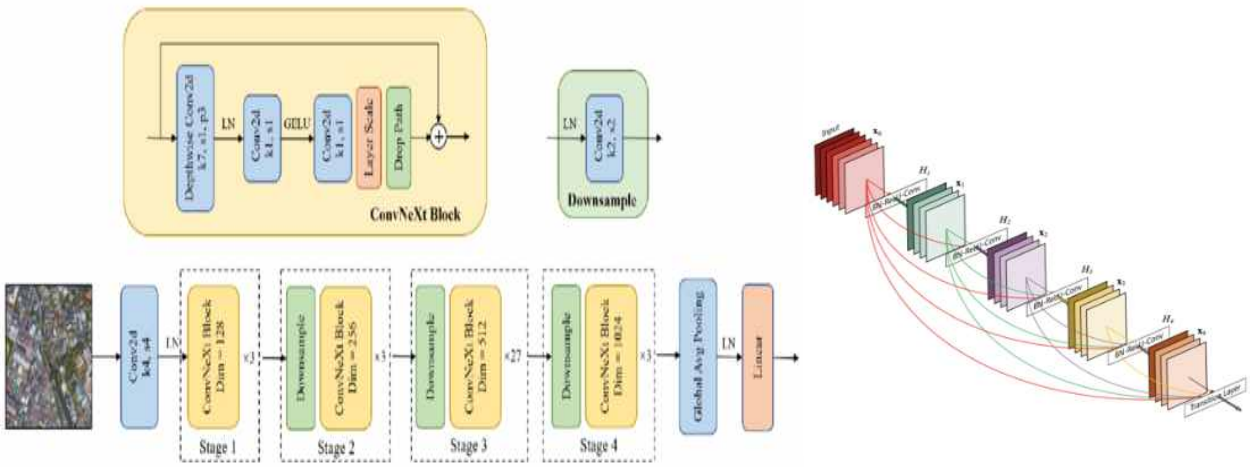

그림 2. ConvNeXt Block 구조와 DenseNet구조
Fig. 2. ConvNeXt Block Structure and DenseNet Structure

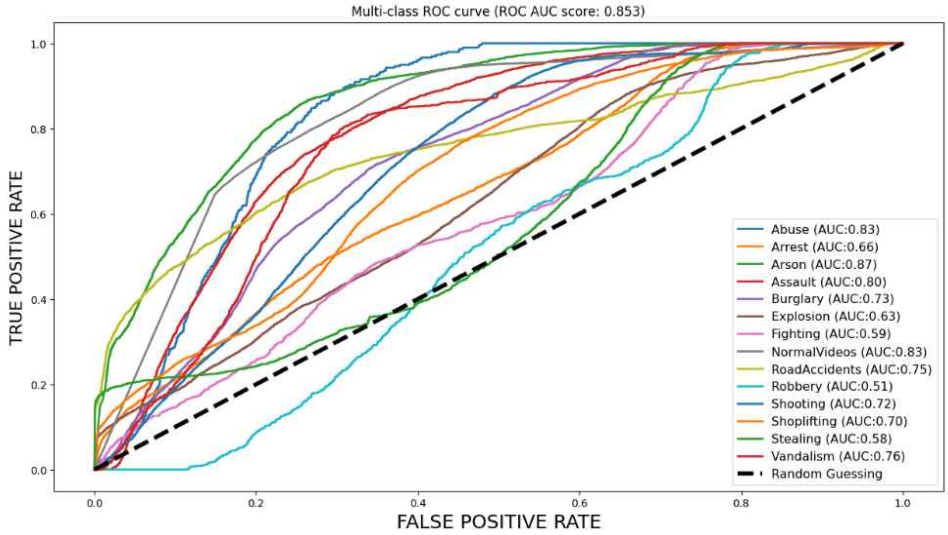

그림 3. 각 클래스에 대한 AUC
Fig. 3. AUC for each Class

ConvNeXt는 DenseNet121의 각 계층에서 발생하는 'Dense Connectivity'와 달리, ConvNeXt Block은 특정 연산들의 조합을 사용하여 정보의 흐름과 특징의 추출을 최적화한다. ConvNeXt는 다양한 크기의 특징을 추출할 수 있으며, 반면 DenseNet은 모든 계층간의 연결을 제공한다. 이렇게 모델이 복잡한 경우 과적합에 대해 유의해야 하는데 ConvNext는 과적합을 방지하고 네트워크의 견고성을 높이기 위해 DropPath를 도입한다. 그렇기에 DenseNet121 보단 ConvNext를 활용하는 것이 조금 더 효율적이다.

최종적으로, Test Dataset 에 대한 해당 분류 모델의 성능을 평가한 결과, 최종 ROC AUC의 값은 0.853로 1에 가까운 높은 성능을 보여주었다. 각 클래스 모두 Random Guessing의 수치 0.5보다 높게 나왔고, 대부분의 정확도가 1에 가까운 것으로, 매우 성공적으로 결과가 나타났다.

III. 결 론

본 논문에서는 감시 시스템에 적용할 수 있는 이상 행동을 탐지하기 위한 딥러닝 방법론을 제시하였다. UCF Crime Dataset 을 활용하여 실세계의 감시 비디오에서 나타나는 다양한 이상 행동을 정밀하게 포착하고 분석하였다. 학습 및 검증 데이터셋에서의 정확도와 AUC의 값이 매우 높게 나타났다.

결과적으로 본 연구는 현대 감시 시스템의 중요성을 고려하였을 때, 접근 방식이 실제 환경에서의 이상 행동 탐지에 유용하게 적용될 수 있음을 보여주었다. 데이터가 조금 더 충분한 상황에서 실험한다면, 보다 더 우수한 모델을 개발할 수 있을 것으로 보인다. ICT에 발전과 함께 감시 시스템의 중요성은 더욱 증가하고 있으며, 이러한 디지털 시대에 본 연구의 접근 방식이 효과적인 감시 및 이상 행동 탐지에 큰 도움이 될 것이다. 향후 IOT 기기와 연계하여 감시 시스템이 복잡한 환경에서도 안정적으로 운영될 수 있게 만든다면, 본 연구의 기술적 접근법이 더욱 더 의미가 커질 것이다.

참 고 문 헌

[1] Pablo Ruiz 'Understanding and visualizing DenseNets' Towards Data Science Oct 11, 2018

[2] Shivam Baldha 'Introduction to DenseNets(Dense CNN)' April 7th 2022

[3] Shenglong chen, Yoshiki Ogawa, Yoshihide Sekimoto, 'Large-scale individual building extraction from open-source satellite imagery via super-resolution-based instance segmentation approach' November 6th 2022