기계학습 기반 CCTV 영상 분석을 통한 이상행동 실시간 탐지 예방 시스템 개발

고신우, 김태옥, 박현아, 임다연, 김명주*
*서울여자대학교 정보보호학과
e-mail : dwgoo123@naver.com

Towards Anomaly Detection System in Human Behaviors Using Machine Learning-based CCTV real-time monitoring

Shin-Woo Ko, Tae-Ok Kim, Hyun-Ah Park, Da-Yeon Lim, Myuhng-Joo Kim*
*Department of Information Security, Seoul Women's University

요 약

최근 학교폭력 및 성폭력 등의 범죄가 증가함에 따라 CCTV 의존도가 높아지고 있으나, 경제력 및 인력의 한계가 있다. 이에 지능 보안 시스템의 필요성이 커지고 있으며, 본 논문은 폭행상황 검출 방법에 관한 내용을 다룬다. 보다 구체적으로는 입력되는 프레임 영상 내의 움직이는 객체 중 사람객체를 검출하고, 고위험 수준 판단 시 알림을 주면서 영상 데이터를 송신 시 암호화하는 단계를 거친다. 연구 결과를 통하여 위급한 상황에 기계학습 기반 CCTV 를 더 적극적으로 이용할 수 있으며, 안전한 도시를 만드는 데 기여할 것이다.

1. 서론

본 연구는 네트워크 보안을 활용한 지능형 CCTV 및 그 방법이 개시된다.

범죄예방, 학교 치안 등을 목적으로 CCTV 가 도입되고 있으나 CCTV 가 사후 발견과 증거 목적 이외에는 예방 차원에서 유의한 효과가 없다는 것을 발견하였다. 이는 과학적 분석을 통해 현실을 반영하여 운영되어야 함을 의미한다[1]. 예방을 위해서 실시간 판독과 상황 연계를 추가한 본 시스템을 개발한다.

입력된 영상 내 객체를 탐색하여 위험 수준을 분류하도록 학습된 모델을 활용한 폭행 상황 인식 방법을 제공한다.

영상 데이터 송신 시 암호화하는 단계; 고위험 수준 판단 시 알림을 주는 단계; 영상 데이터 접근 시 무결성 보증 단계를 포함한다.

2. 연구의 필요성 및 문제점

CCTV 는 다양한 업계에서 활용되고 있으며, 그 효과를 인정받아 설치 수가 증가하고 있다. 그러나 운영 인력이 경비원이나 관리 사무소 직원인 경우에는 전문지식의 부족이나 업무 과다로 인해 정작 범죄를 사전에 예방하는 역할을 수행하지 못하고 있다[2]. 국내에서 진행된 방범용 CCTV 의 범죄예방효과에 대한 선행연구를 분석하면 방범용 CCTV 가 범죄 예방 효과가 있다고 할 수 없다[3].

최근 CCTV 사각지대나 골목길에 타인을 '묻지 마 폭행' 해 상해를 입히거나 살해하는 경우가 발생하여 충격을 주고 있다. CCTV 가 설치되어 있지만, 관제에서 제때 파악을 하지 못해 출동 시간이 늦어져 사건이 발생하는 경우, 혹은 위급한 상황 등이 찍히고 있으나 CCTV 를 지속해서 지켜보고 있는 것이 아닌 이상 문제 상황을 지나쳐버리는 경우도 많다. 또한 사건, 사고가 일어날 때 CCTV 의 사각지대에서 일어나는 경우에는 물적 증거를 수집하기 어렵다[4].

도움 요청이나 직접 호출 혹은 비상벨을 이용한 호출 등 방법이 있지만, 현실적으로 피해자가 이러한 행위를 할 여건이 안 되는 경우가 많다. 지능형 CCTV 는 피해자가 특정 행위를 하지 않더라도 움직임과 비명을 감지해 위험 상황을 판단하므로 방범과 신속한 호출, 즉각적인 조치에 유리하다.

또한, 현재 출시된 지능형 CCTV 의 가격은 약 2000 만원 이상으로 이미 기존에 사용 중인 기기를 교체하기에는 교체해야 하는 기기의 수가 많을 뿐만 아니라 교체 비용이 부담스럽다. 기계학습 기반 CCTV 는 기기 교체의 부담 없이 기존의 CCTV 를 이용하면서 영상을 실시간으로 호스트 상에서 분석하여 빠른 속도와 낮은 비용으로 정확하게 판단할 수 있다는 장점이 있다.

IoT 분야의 성장에 따라 보안 우려가 커지면서 CCTV 영상 보안의 중요성도 커지고 있다. 이에 따라 CCTV 에 AI 를 탑재하려는 연구 등이 활발히 이루어지고 있다. 본 논문에서는 CCTV 영상 속의 특정인의 행동 인식에서 이상 행동에 대하여 감시하고 사람의 움직임을 탐지하여 위험 수준을 판단하는 AI CCTV 구현하고자 한다[5].

*본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 SW 중심대학지원사업의 연구 결과로 수행되었음(2016-0-00022)

또한 불법 침입자가 그 영상에 접근할 수 없도록 차단하는 네트워크 보안 기술을 이용하여 전달하는 것을 목표로 한다[6].

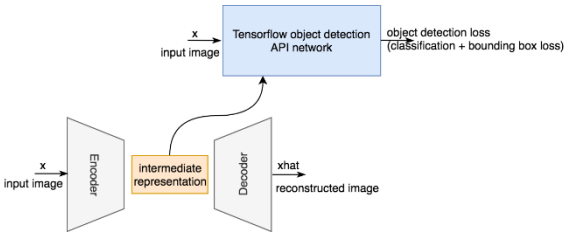
3. 시스템 구성도

3.1 딥러닝

기계 학습된 객체 행위 식별자 학습모델을 이용하여 입력된 영상에 대해 영상 내 객체를 탐색한다.

3.1.1 사람의 움직임 가속도

검출된 신체 각각의 조인트 및 뼈대 이미지 정보로부터 조인트와 뼈대 이미지의 이동 경로를 분석하여 추출한다. 탐색 된 객체 또는 객체의 행위를 인식하고 확률적 기반 또는 논리적 기반의 방법으로 이상 상황을 판별하는 획득한 영상에 대한 상황 판단 데이터를 이용한 현장 판단 방법이다.



[그림 1] Tensorflow object detection API models

3.1.2 폭력성 수준

위험 수준은 1 단계부터 5 단계로 분류되며, 분류 기준은 몸의 가속도이다. 영상 속 사람의 움직임을 탐지하여 위험 수준을 판단한다.

1 단계는 특별한 접촉이 없는 경우이다. 2 단계는 인사 등의 가벼운 접촉이 있는 경우이다. 3 단계는 살짝 밀치는 정도 등의 장난 섞인 접촉이다. 4 단계는 주먹질, 발차기 등의 폭력이 섞인 접촉이다. 5 단계는 도구를 사용한 폭행, 집단 폭행, 과도한 폭행 등이 해당한다.

4 단계 이상의 고위험 수준으로 판단되는 경우 업계에 알림이 가도록 한다.

3.2 네트워크 암호화

영상 데이터를 송신하는 중에도 불법적인 도청과 서버에 대한 불법적인 접근 가능성이 존재한다. CCTV 영상 데이터 송수신은 유/무선 네트워크 환경을 기반으로 하기 때문에, 기본적으로 프로토콜 및 네트워크 보안, 정보 보호 및 사생활 보호와 시스템 장애 방지를 위한 보안 기술을 요구할 것이다[7]. 보안 프로토콜은 올바른 암호화 및 복호화, 인증 및 인가 기능을 정상적으로 수행할 수 있는 프로토콜이어야 한다[8]. 또한 영상 데이터의 무결성 인증을 위하여 FIPS(Federal Information Processing Standard) 등의 표준에 따라 안전한 키 값을 통한 난수 생성 기능이 필요하다[9]. 네트워크 보안 프로토콜에 대한 API 뿐만 아니라 시스템 보안에 사용하는 기법에 대한 API 도 포함하는 OpenSSL 을 사용할 계획이다. 따라서 프로토콜 및 네트워크 보안을 위해 SSL/TLS 암호화, POST 방식 기반 영상 전송과 방화벽에 의한 WL, BL 를 판단하여 인가된 Inbound/Outbound 만을 허용하도록 한다.

3.3 CCTV 위/변조 방지

CCTV 영상 데이터를 수신하여 분석하는 호스트 자체의 취약성 또한 존재한다. 호스트에 대한 Malware 감염 가능성, DDoS 공격, 시스템 장애, 영상 데이터에 대한 위/변조 가능성이 있다. 호스트에 대한 불법적인 접근 혹은 불법적인 도청을 방지하기 위하여 호스트 자체에 대한 보안 기술이 필요하며, 수신한 영상이 일관된 상태를 유지하도록 공개키 암호 기술, 해시 함수 등을 적용한 무결성 보증 기술이 요구될 것이다.

3.4 프라이버시 보호 기술

CCTV 는 기본적으로 안전을 목적으로 개인의 행위를 감시하는 기능을 가지고 있기 때문에, 영상 속 객체에 대한 프라이버시 보호를 위한 보안기술이 필요하다. 법률을 준수하여 CCTV 영상 데이터를 수집하기 위해 법률 위반에 대한 모니터링 기술, 호스트 상에서 개인의 이상 행위 분석 시 장치 및 서비스 시스템에 대한 접근통제 기술인 인증 기술이 별도로 요구된다[10].

4. 시스템 구현을 위한 계획

호스트에 CCTV 영상 데이터를 안전하게 전송하기 위한 네트워크 보안 기술, 호스트 및 CCTV 단말기 상에서의 정보 보호와 사생활 보호 기술 등을 연구할 예정이다. 이외에도 하드웨어 공격에 대응하기 위하여 시큐어 부트, 펌웨어/코드 암호화, 실행 코드, 영역제어 등 다양한 하드웨어 보안 기법을 적절히 적용할 필요가 있다[5].

영상 데이터에 대한 암호화 알고리즘 구현과 더불어, 이상행동을 감지하기 위한 딥러닝 알고리즘 구현을 위한 데이터셋을 수집할 예정이다. 수집한 데이터셋을 기반으로 Tensorflow 를 통해 호스트를 학습시켜 정확한 상황인지를 가능하게 할 것이다.

5. 구현 완성에 따른 기대효과

이 연구 결과물을 통하여 다음과 같은 효과를 기대할 수 있다.

첫째, 지능형 CCTV 가 아닌 기존의 일반 CCTV 를 이용하면서 서버 단에서 실시간으로 이를 학습, 분석함으로써 불필요한 CCTV 교체 비용을 줄일 수 있다.

둘째, 관리자에게 바로 알림 서비스를 제공하기 때문에 관제사에 의해 감지되던 기존 감시 체계보다 더욱 정확하고 빠르게 위험 상황을 인지할 수 있다. 이전의 감시체계로는 수백 대의 CCTV 카메라 영상에 대하여 한정된 인원으로 관제하는 데 한계가 있기

*본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 SW 중심대학지원사업의 연구 결과로 수행되었음(2016-0-00022)

때문에 미래의 CCTV 영상보안 시스템의 운영에 필수적인 요소가 될 것이다[11].

셋째, 중요한 증거자료인 CCTV 영상을 서버로 이동할 때 경량 암호화를 실시함으로써 불법적인 도청, 인가되지 않은 접근을 차단할 수 있다.

넷째, 녹화된 영상을 재생하여 사건 사고의 사후 분석에도 적극적으로 활용할 수 있다.

다섯째, 폭행에 의한 위험 상황을 판단하는 CCTV 는 실생활뿐만 아니라 사내, 교내 등 사람이 생활하는 모든 곳에 적용할 수 있기 때문에 향후 널리 쓰일 것으로 예상된다.

여섯째, 최근에는 CCTV 영상보안시스템 응용을 통해 새로이 창출될 수 있는 비즈니스가 많아지고 있다. 공공기관 또는 지방자치단체를 중심으로 한 방범 또는 방재를 목적으로 활용하는 것뿐만 아니라, 지능형 영상분석 기술을 적용하여 민간 영역에서 성별, 나이 분포에 따른 분석을 하는 등 정교한 마케팅 분석을 시도할 수도 있다.

이상의 효과를 고려할 때 본 연구에서 개발 예정인 기계학습 기반 CCTV 를 위급한 상황에 더 적극적으로 이용할 수 있을 것이다. 더 나아가 CCTV 를 포함한 IoT 의 기계학습 활용과 발전된 경량 암호화를 확대할 수 있을 것이다.

참고문헌

[1] 허선영, 문태헌. "범죄예방을 위한 CCTV 위치 적절성 및 효과성 분석." 한국지역지리학회지, 21.4 (2015.11): 739-750.

[2] 한재경. (2018). 범죄예방용 CCTV 의 설치 및 운영에 관한 소고. 공공사회연구, 8(4), 109-137.

[3] 송봉규, 박경민. (2010). 방범용 CCTV 정책의 평가와 한계. 한국행정학회 학술발표논문집, , 135-156.

[4] 서태웅, 이성렬, 배병철, 윤이중, 김창수. (2012). CCTV 보안관제 취약성 및 성능 분석. 멀티미디어학회논문지, 15(1), 93-100.

[5] 박화진. (2013). 객체 추적을 통한 이상 행동 감시 시스템 연구. 한국디지털콘텐츠학회 논문지, 14(4), 589-596.

[6] 김봉현, 조동욱. (2014). 네트워크 보안 기술 동향과 전망. 한국통신학회지(정보와통신), 31(4), 99-106.

[7] 김시정, 조도은. (2015). IOT(Internet of Things) 보안 기술 동향. 한국콘텐츠학회지, 13(1), 31-35.

[8] 한국인터넷진흥원, “빅데이터 환경에서 개인정보보호를 위한 기술”, 2013

[9] NIST, “FIPS Announcements”, 2016

[10] 한국인터넷진흥원, “IoT 공통 보안 가이드”, 2016

[11] 강희조. (2016). 사회안전을 위한 지능형 영상감시분석시스템. 한국디지털콘텐츠학회 논문지, 17(4), 273-278.

*본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 SW 중심대학지원사업의 연구 결과로 수행되었음(2016-0-00022)