사물인터넷 센서와 인공지능을 이용한 이상 징후 차단 보안관리 시스템

강윤모, 강윤호, 신재성, 유승형, 유상오*
가톨릭대학교 정보통신전자공학부
*우리카드
ymk961028@catholic.ac.kr, go5man@catholic.ac.kr, skullant16@catholic.ac.kr,
seunghy1468@catholic.ac.kr, sangoh.yoo@gmail.com

Security Management System to Block Abnormal Symptoms Using IoT Sensors and Artificial Intelligence

Yun-Mo Kang, Yun-Ho Kang, Jae-Seong Shin,
Seung-Hyeong Yoo, Sang-Oh Yoo*
Dept. of Information Communication and Electronic Engineering,
Catholic University of Korea
*Corp. Wooricard

요 약

본 논문은 사물인터넷과 인공지능을 융합하여 영상 데이터양을 감소시켜 실시간 모니터링의 어려움을 해소하고, 불법 침입 및 이상징후 차단, 화재 징후를 효율적으로 포착하고 관리하여 범죄 차단 및 이상징후 차단을 목적으로 설계한 시스템을 소개하고 있다.

1. 서론

최근 사물인터넷과 인공지능을 결합한 첨단산업이 주목을 받고 있으며 그 중 스마트홈 IoT서비스의 사용자 수는 크게 증가하였다. 이와 같은 사용자수 증가에따라 해킹 공격 역시 증가하였는데. 종류로 네트워크(펌웨어)해킹, 통신시스템(공유기)장악, 감시 카메라 공격 등 다양하다.[1].

본 논문에서는 효율적으로 IoT 서비스를 구축함과 더불어 통합관리 서비스를 통한 보안 시스템을 소개한다. IoT의 경우 크게 불법침입 관리, 이상징후 포착을 구현하였고 통합 보안 시스템의 경우 GCP(Google Cloud Platform)을 통하여 방화벽 규칙 설정과 IAP(Identity-Aware Proxy)를 통해 보안 수준을 높였다.[2],[3]. 추가로 기존 IoT서비스에 Edge Detection을 추가해 효율적 시스템 설계를 하였다

2. 본론

본 논문은 사물인터넷과 인공지능을 이용한 보안시스템 설계에 목적이 있다. 설계에 쓰인 기술을 나열하면 효율적으로 데이터를 저장하기 위해 에지 검출(edge detection)기술을 이용하고, 물체를 식별하기 위한 객체 검출(object detection)기술로 딥 러닝(deep learning) 기반의 YOLO(you only look once)라는 실시간 객체 검출 알고리즘(real-time object detection algorithm)을 이용했다. 또한 실시간으로 관리자에게 정보를 전달하기 위해 애플리케이션을 설계했다.

2-1. CCTV

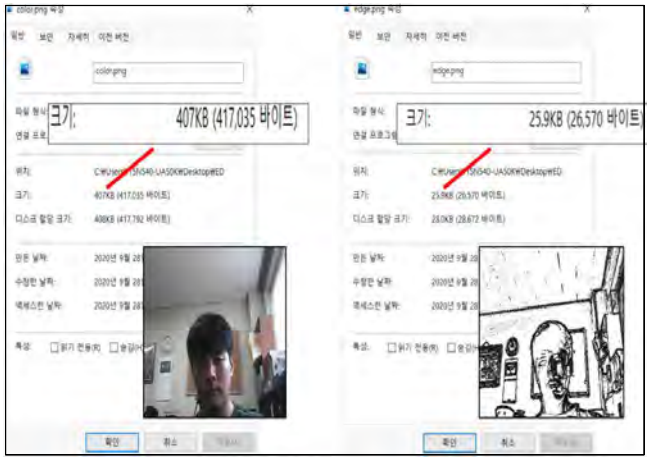
방범, 감시, 화재예방 등의 보안을 목적으로 가장 대표적인 시스템은 CCTV(closed-circuit television)이다. CCTV는 범죄 발생 시, 즉시 범죄차단을 하는 시스템이 아니라 사후처리에 치중되어있는 시스템이다. 즉, 범죄 예방 가능성을 증가시키는 효과가 있지만 범죄에 즉각적인 대처에는 부적합하고, 범죄가 발생한 후에 범인의 신상을 조사하는데 사용된다. 그러나 영상의 경우 오랫동안 저장되어야 하므로 높은 용량의 데이터 저장 공간을 필요로 한다. 이러한 문제점을 해결하기 위해 인공지능을 이용하여 사물을 인식하고 에지 검출기술을 적용하여 영상 데이터의 크기를 줄여 효율적으로 데이터를 관리한다.

2-2. 에지검출

사람의 출입을 불허하는 시간에 사람이 보안구역 내에 침입한다면 침입자라고 볼 수 있을 것이다. 이는 다시 말하면 침입자가 발생하는 특정 시간 외에는 고화질로 녹화를 할 필요가 없음을 의미한다. 따라서 영상처리를 통해 사물을 서로 구분할 수 있을 정도로만 영상이 촬영되어도 문제가 없으므로, 이러한 영상에 에지 검출 영상처리 기술을 적용함으로써 침입자가 발생하는 시간 외에는 물체끼리 비교할 수 있을 정도로의 화질로 영상을 저장한다. 에지 검출 과정은 우선 영상을 [그림 1]과 같이 회색조(gray scale)로 처리함으로써 흑백 이미지로 바뀌기 때문에, 영상에 쓰이는 화소 하나에 소모되는 데이터 용량을 1/3로 줄일 수 있으며, 추후 에지 검출 기술을 적용함에 있어서 간단해진다. 회색조 이후, [그림 2]와 같이 에지 검출을 이용하면 [그림 3]을 통해 알 수 있듯이 기존 이미지의 데이터 양 대비 90%를 감소시킬 수 있다.

[그림 1] 에지 검출 이전의 정지 영상

[그림 2] 에지 검출 이후의 정지 영상

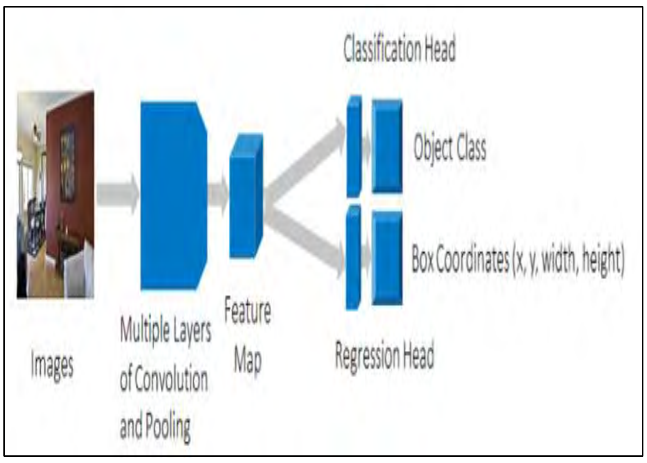


[그림 3] 기존 영상과 에지 검출 영상 크기 비교

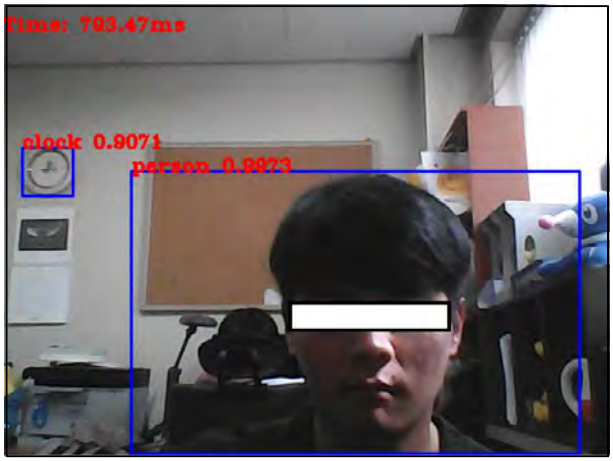
2-3. 실시간 보안 문제

그러나 에지 검출을 통한 영상만을 이용한다면 침입자를 구분하기 어려운 문제점이 존재하므로, 이를 방지하기 위해 침입자가 발생했을 시에는 고화질의 영상을 그대로 저장한다. 이를 위한 것이 인공지능 기반의 YOLO 알고리즘과 인체감지 센서를 이용한다.

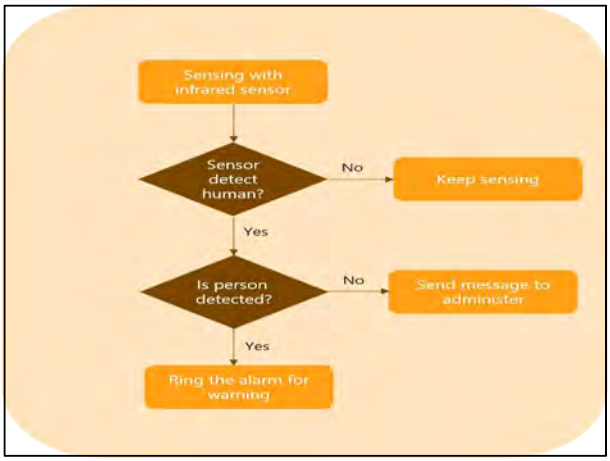
우선, 적외선 인체감지 센서를 이용하여 보안구역 내 침입자의 유무를 체크한다. 적외선 센서에 침입자가 감지되면 [그림 4]과 같이 YOLO 알고리즘을 적용한 CCTV로 촬영하여 침입자가 사람인지 아닌지를 판단하여 사람이라면 경보를 울리면서 침입자가 있음을 즉각적으로 알린다. 만약, 침입자가 사람이 아니라고 판단 될 경우에는 [그림 6]의 알고리즘에 따라 관리자에게 보안구역 내 침입이 발생했음을 알리는 메시지를 보냄으로써 조치를 취한다.



[그림 4] 이미지 내 단일 객체 탐지 네트워크



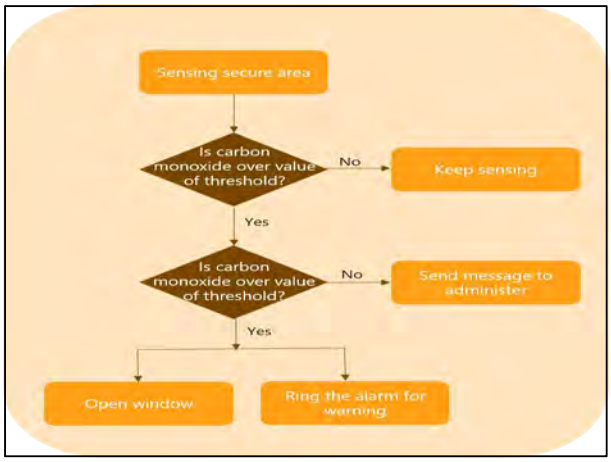
[그림 5] YOLO 알고리즘을 이용한 사물 식별



[그림 6] 센서 탐지 알고리즘

2-4. 화재감지

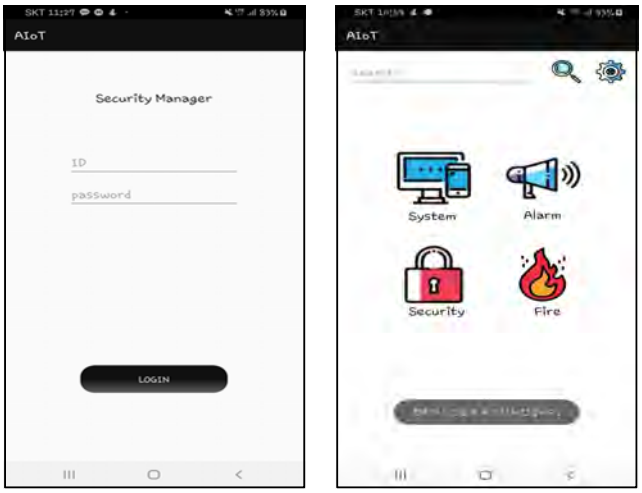
화재감지를 위한 시스템은 온습도 감지 센서와 일산화탄소 센서를 이용한다. [그림 7]와 같이 일산화탄소 센서에서 일산화탄소가 일정수준 이상이 감지된다면, 화재발생 확인을 위해 보안구역 내 해당 위치에 설치된 온습도 센서의 값이 일정수준 이상을 넘었는지 확인을 한다. 만약 온습도 센서 값이 일정수준의 임계 값을 넘었다면 화재인 것으로 판단하여 즉시 화재 경보를 울린다. 그러나 임계 값을 넘지 않을 경우에는 관리자에게 연기가 감지되었다는 경고 메시지를 보낸다. 즉 두 가지 센서를 통합하여 화재감지를 더욱 정확하게 하였다.



[그림 7] 화재감지 알고리즘

2-5. 애플리케이션

관리자가 어떠한 상황에서도 효율적인 업무를 볼 수 있도록 애플리케이션을 설계했다. 보안 관리를 위한 애플리케이션은 첫 로그인 후 메인 인터페이스가 나오며, [그림 8]과 같이 시스템, 알람, 보안, 화재로 구성되어 있다. 시스템 탭은 CCTV가 촬영하는 실시간 영상을 볼 수 있으며, 알람 탭은 불법침입 및 화재와 같은 보안 관련 이슈가 발생할 경우 알람을 위한 탭이다. 보안 탭의 경우에는 에지 검출 영상처리를 통해 저장된 영상과 사건이 발생하여 고화질로 촬영된 영상들을 볼 수 있다. 화재 탭은 시간별로 체크된 온습도와 일산화탄소 농도들이 나열되며 날짜별로 분류된다. 애플리케이션은 데이터들을 서버를 통해 데이터베이스에서 가져와 관리자에게 보여준다. 앱의 경우 GCP의 IAM(Identity and Access Management)을 통해 보안 유지가 된다.



[그림 8] 로그인 화면(좌) 및 메인 화면(우)

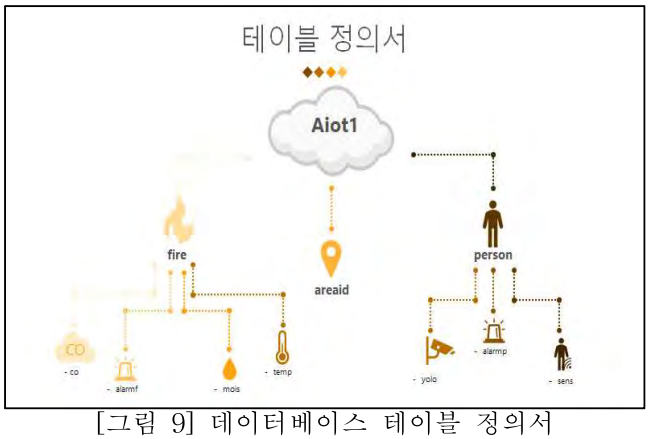
2-6. 서버 및 보안

서버는 구글에서 제공하는 클라우드 플랫폼(google cloud platform)을 이용하여 구현하였다. 운영체제는 우분투(ubuntu) 20.04를 이용한다. 웹 서버 구현을 위해 아파치2(apache2)와 PHP, MySQL을 연동시켜 사용한다. 또한, 서버는 센서 데이터 서버와 영상 이미지 서버로 나누어, 온습도 및 일산화탄소의 농도, 인체감지 적외선 센서의 값 등은 센서 데이터 서버의 DB에 저장될 것이며, 영상처리 과정을 거친 영상은 영상 이미지 서버의 저장 공간에 저장된다. 보안 관련하여 특정 IP의 접근만 허용하는 방화벽 규칙을 설정하였으며. IAP 설정을 통해 IoT서비스에 등록된 사용자만 실시간 영상 감시가 가능하다.

2-5. 데이터베이스 및 보안

데이터베이스 역시 GCP를 이용한다. [그림 9]와 같이 데이터베이스의 구성은 보안 구역관리를 위한 areaid, 침입자 관리를 위한 person과 화재 감지를 위한 fire로 나누어져 있으며, person 안에는 YOLO에서 사람이 탐지되었을 경우를 위한 yolo 테이블과 인체감지 센서에서 사람을 탐지했을 때의 값을 저장하기 위한 sens 테이블, 알람을 울리기 위한 alarmp 테이블로 이루어져 있으며, fire DB 온도를 위한 temp 테이블, 습도를 위한 mois 테이블, 일산화탄소를 위한 co 테이블, 알람을 울리기 위한 alarmf 테이블로 이루어져 있다. 데이터 베이스의 보안의 경우 Putty프로그램을 통해 생성된 SHA-2을 GCP 프로그램에 저장하였고, 서버 접근과 마찬가지로 접근 시 허용된 방화벽과 등록된 개인정보만 열람 가능하다.

[그림 9] 데이터베이스 구성



[그림 9] 데이터베이스 테이블 정의서

3. 결론

4차 산업혁명에 있어 사물인터넷과 인공지능을 결합한 보안 관리 시스템 개발 및 시뮬레이션을 통해 새로운 기술을 설계하고 구현함으로써 앞으로의 보안시스템에 새로운 첨단기술의 요구를 설명하고자하는 목적에 의의가 있다. 향후 사물인터넷과 인공지능을 결합한 시스템을 구현하는 데 있어 기존 영상 데이터 용량에 대한 문제점, 불법침입 및 이상징후 관련 효율적 대안을 제시한다

[본 논문은 과학기술정보통신부 정보통신창의인재양성사업의 지원을 통해 수행한 ICT멘토링 프로젝트의 결과물입니다.]

참고문헌

[1] 한국어 APA 단행본 / 내주-참고문헌
김성민, 정혜선, 이용우. (n.d.). 정보보안산업 기반 스마트시티 사이버 보안 (pp. 129-136). n.p.: 한국정보기술학회.
[2] 한국어 APA 단행본 / 내주-참고문헌
공배완. (n.d.). 중소기업 산업기술 보안관리 실태와 보안대책 (pp. 1-26). n.p.: 한국민간경비학회보.
[3] 한국어 APA 단행본 / 내주-참고문헌
신민지, 이창무, 조성필. (n.d.). 중소형 의료기관의 개인정보 보안실태 및 개선방안 (pp. 123-132). n.p.: 한국융합보안학회.
* [그림 4] 참조
- SAS KOREA, <딥러닝을 활용한 객체 탐지 알고리즘 이해하기>, 2018년 12월 21일, url-https://blogs.sas.com/content/saskorea/2018/12/21/