

CCTV에서 딥페이크를 방  
지하는 방법

How to prevent Deep Fakes in  
CCTV systems

1771026 김나연

1771273 최혜림



# 목차

- 프로젝트 개요
- 주제 선정 배경
- 유사 프로젝트와의 차별성
- 프로젝트 구조
- 주요 기능 및 기술, 기능 시연
- 향후 계획
- 팀원별 담당 업무
- 프로젝트 수행 후기

# 프로젝트 개요

# 프로젝트 개요

- 프로젝트 주제

- CCTV 를 통해 촬영되는 사람들의 얼굴이 딥페이크 등으로 악용되는 것을 막기 위한 프로젝트

- 프로젝트 개요

- 얼굴이 촬영 된 사진, 영상을 가지고 딥페이크에 악용되는 것을 방지하기 위해 촬영되는 영상에서 얼굴 부분을 인식하여 모자이크 처리를 하고 영상을 저장한다.
- 복호화가 필요할 경우를 대비하여(예를 들어, 범죄자 신상파악) 모자이크가 되기 전에 이미지를 1초 한 번씩 캡처하고 aes 암호화를 수행하여 binary 파일로 저장한다.
- 암호화 된 파일을 추후에 필요한 경우 aes 복호화하여 이미지를 확인한다.

- 주요 기능

- OpenCV 를 통한 녹화 시, 즉시 얼굴을 모자이크 처리한다.
- 1분에 한번씩 캡처한 사진을 Base64URL로 변환하고 aes 암호화를 한다.
- 암호화한 사진을 복호화하여 캡처본을 볼 수 있다.

## 주제 선정 배경

# 주제 선정 배경

- 현재 대한민국에는 2014년 기준으로 3,676,875개의 CCTV가 설치되었으며, 최근 들어 CCTV 대수는 이보다 훨씬 더 많이 늘었다.
- 보안 목적으로 설치된 CCTV나 IP Camera는 초상권 침해의 우려가 있고, 이는 딥페이크로 인한 피해로 이어질 수 있음을 시사한다.
- 텔레그램의 딥페이크 봇로 인한 피해자 수는 2020년 4월 약 5만 3천 명, 2020년 7월 10만 4852명으로 피해가 심각한 상황이다.  
(텔레그램 딥페이크 봇: 텔레그램에 인물 이미지를 올리면 자동으로 여성의 나체에 그 인물의 얼굴을 합성해주는 이미지 자동 생성 알고리즘.) 기사

# 내가 비키니 입고 마약? 가짜영상 범인은 친구 엄마였다

[중앙일보] 입력 2021.03.15 05:00 수정 2021.03.15 09:44



가

가

## 딥페이크... 진짜보다 더 진짜 같은 가짜가 나타났다

심층 학습하는 인공지능 이용해  
2013년 사망한 만화 '심슨'의  
성우 목소리 똑같이 재현

박건형 기자

입력 2021.03.11 03:00 | 수정 2021.03.11 03:00

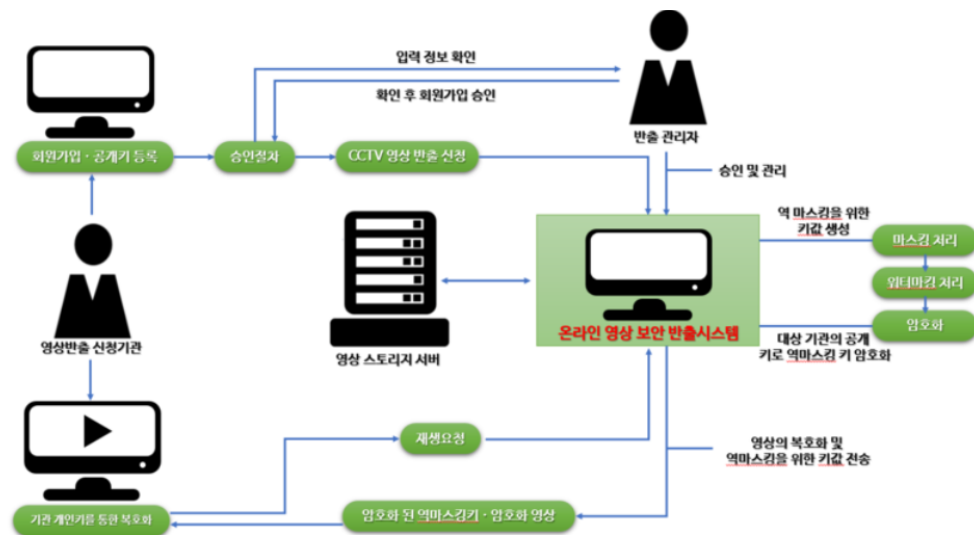


# 유사 프로젝트와의 차별성



# 유사 프로젝트 1

## MWSTORY



## 멀티 센서 CCTV

움직임 포착 기술 + 얼굴 영역 검출 기술 => 얼굴 암호화 및 복호화 기술

Face Detecting 기능을 활용해 얼굴 정보를 파악한 후 얼굴을 실시간으로 암호화  
영상을 받는 사람은 복호화 기술을 통해 안전하게 CCTV 영상자료를 받을 수 있다

## 차별성

- 6조는 이미지의 Base64URL을 암호화 한다. 그러므로 픽셀 정보를 암호화하는 부분과 차이가 있다.

# 유사 프로젝트 2



## 딥핑소스의 익명화

### 특징

- 기존의 대량 비디오 데이터를 전송하여 학습 및 분석하던 방식에서 AI 카메라에서 바로 블러링/마스킹 한다.
- 사진 전체를 익명화 하는 기술

### 차별성

- 6조는 녹화 영상에서 얼굴 부분만 모자이크를 하고, 이미지를 캡처하여 이미지를 base64URL 변환, 암호화하여 db에 저장을 하는데서 차이가 있다.

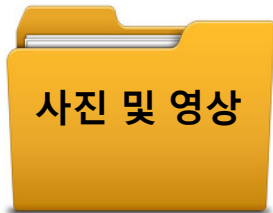
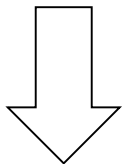
# 프로젝트 구조

# 프로젝트 구조

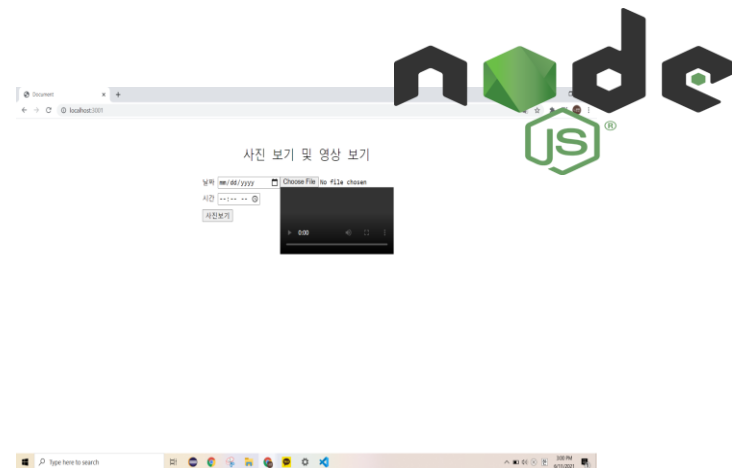
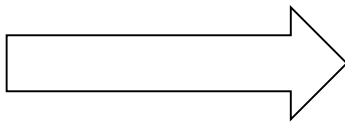


1. openCV 얼굴 인식 후 캡처한 사진 및 녹화 영상 저장
2. 저장된 사진 및 영상 웹에서 불러옴

AES 암호화



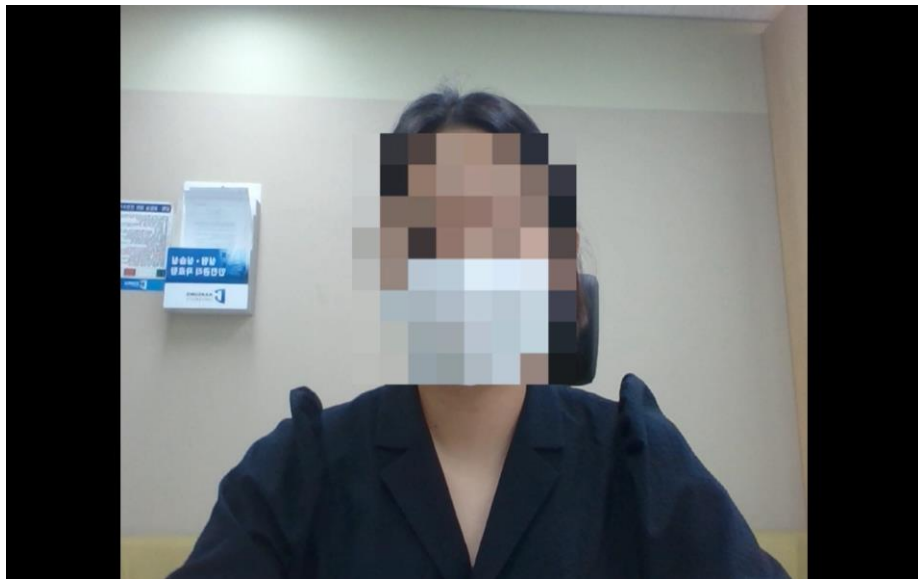
AES 복호화



**주요 기능 및 기술, 시연**

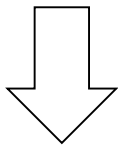
# 주요기능 1 - 녹화 중 모자이크

- 평상시에 cctv 역할의 녹화가 진행될 때, 얼굴에 모자이크 처리가 된다.

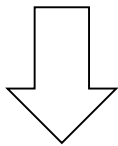


## 주요기능2 - AES 암호화, 복호화

- 이미지를 base64로 바꿔서 aes 암호화를 진행한다.



- 암호화된 url을 binary 파일로 저장하고 mac 값을 db에 저장해둔다.



- 웹을 통해 날짜와 시간을 선택하면 db를 통해 mac 값을 조회하여 해당하는 binary 파일을 aes 복호화한다.



15.22.bin

id	mac	datetime
483	c3de86dc3afb36478d4f4a15d66d94f0	2021-05-29 14:42:00
484	ad0f76b80673d7a16a00bc08f21042bd	2021-05-29 14:46:00

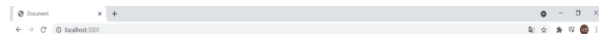
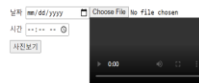
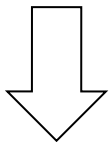


사진 보기 및 영상 보기

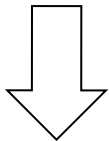


# 주요기능 3 - 웹으로 확인

- 날짜, 시간을 입력



- 복호화된 이미지 확인



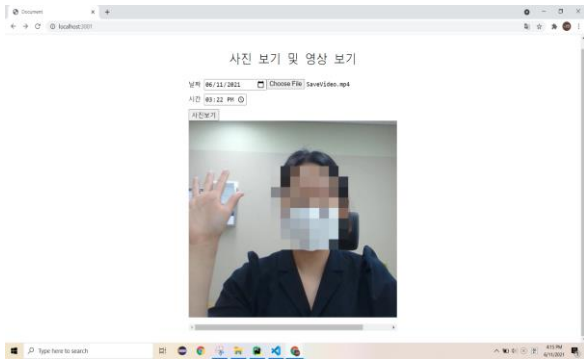
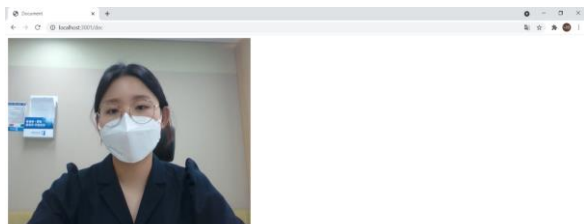

- 해당 날짜에 촬영 된 영상 확인

사진 보기 및 영상 보기

날짜 06/11/2021 Choose File No file chosen

시간 03:22 PM

사진보기





# 시연영상

시연영상 : [https://youtu.be/oxQAL\\_kJLmM](https://youtu.be/oxQAL_kJLmM)

# 향후 개발 계획

# 향후 개발 계획

- 얼굴 인식 고도화
  - 현재는 얼굴 정면만 인식을 하여 모자이크 처리가 된다. 추후에 얼굴 옆면도 인식하게 하여 모자이크 처리가 되도록 구현
- 웹 발전
  - 권한이 있는 사람만 웹에 접속하여 복호화 된 이미지를 볼 수 있도록 구현
  - 암호화 키 값을 사용자가 직접 입력하여 복호화를 할 수 있도록 구현

## 팀원별 담당 업무

# 팀원별 담당 업무

## 팀원별 담당업무

김나연	웹 구현, aes 복호화, mysql
	기여도 : 50
최혜림	opencv, aes 암호화, mysql
	기여도 : 50

## 사용 기술

- openCV 및 Python
- node.js
- MySQL

## GitHub 주소

[https://github.com/nayeonkiim/security\\_faceMasking](https://github.com/nayeonkiim/security_faceMasking)

# 프로젝트 수행 후기

# 프로젝트 수행 후기

- 1771026 김나연
  - 멀게만 느껴지던 보안 문제가 직접 실생활 문제에 연관지어 프로젝트를 수행해 보니 매우 중요하고 우리 생활과도 밀접하게 연관되어 있다는 걸 느끼게 되었습니다.
- 1771273 최혜림
  - 기능, 기술이 발전되면 보안을 해야할 것들이 많다는 걸 느끼게 되었고, 암호화 작업 보다는 복호화 작업이 복잡하고, 힘들다는 것을 깨닫게 되었다.

**감사합니다.**