

# Screen Guarder

정보보안융합S/W

이슬기 윤성준 진영훈 이재희

2019.01.10

지도 교수 : 윤종문 이병천



# 목차

1. 주제선정 이유
2. 개발환경
3. 동작원리
4. 시연
5. Q&A

# 주제 선정 이유

# 주제선정 이유

현실태 :

PC 모니터 정보에 대한 물리적 보호대책이 부족.



따라서, 카메라로 모니터 정보가 유출될 때를 실시간으로 탐지하는 시스템 구현을 목표로 하였다.

# 주제선정 이유

## T-WaterMark

카메라 촬영으로 인한  
기밀 정보 유출 방지

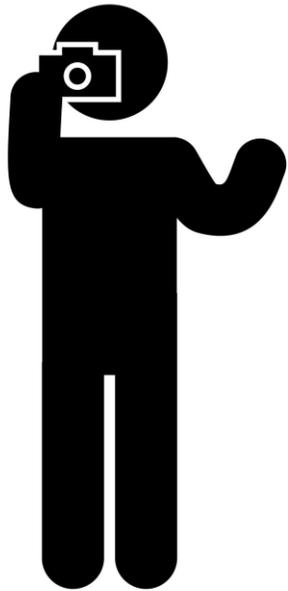


현재 '(주)테르텐' 에서는  
T-WaterMark 라는  
모니터 정보보안 솔루션이  
상업적으로 제시됨.

**하지만,**  
이미 유출된 후 ..!  
실시간 대응 방법은 ??

# 시행착오

## Challenge 1 : 주파수를 통한 탐지

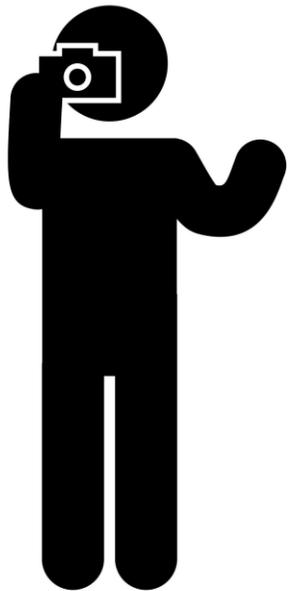


주파수 탐지기를 통해  
카메라 촬영을 인지할  
수 있지 않을까 ?



# 시행착오

## Challenge 1 : 주파수를 통한 탐지



AT007-PRO



AT007-Pro



# 시행착오

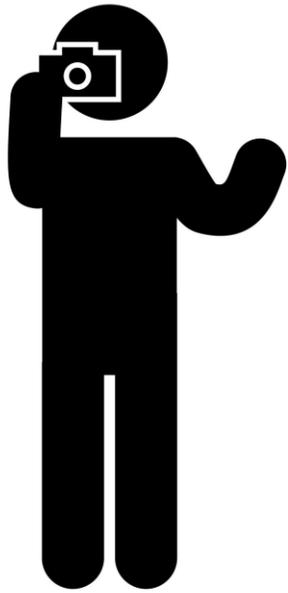
## Challenge 1 : 주파수를 통한 탐지 - 한계



1) 수많은 주파수가  
존재하기 때문에  
특정 주파수만을  
탐지하기엔 어렵다.

# 시행착오

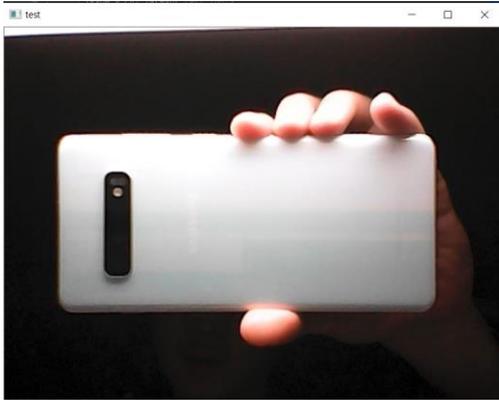
## Challenge 2 : Open CV를 통한 탐지



웹캠 프레임에서  
스마트폰과 비슷한  
물체를 탐지 할 수 있지  
않을까 ?



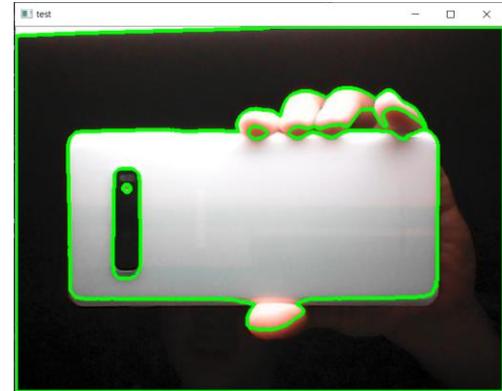
## Challenge 2 : Open CV를 통한 탐지



임의의 Frame

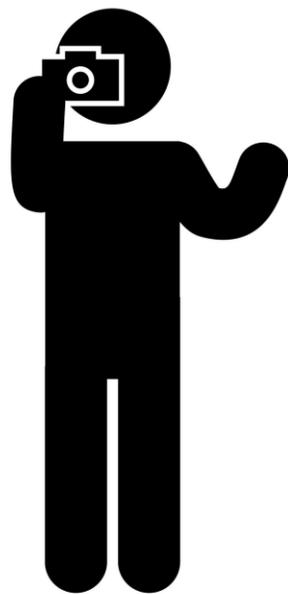


1) Frame 처리에 대한 **경우의 수**를 줄이기 위한 Grayscale 화.



2) 물체의 변 개수와 둘레의 길이정보를 이용해 **오차범위를 최소화**.

## Challenge 2 : Open CV를 통한 탐지 - 한계



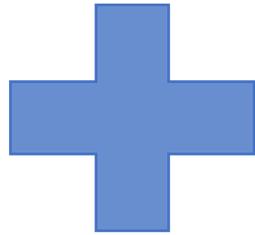
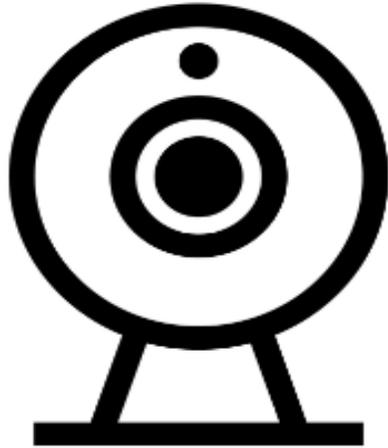
1) 스마트폰이 웹캠  
중앙에 인식 되어야  
하는 한계

2) 손으로 스마트폰을  
가리면 미탐지

# 주제선정 이유

개선 방안 :

웹캠과 머신러닝을 이용해 프레임을 판단하여 실시간 물리적 보안을 수행.



# 개발 환경

# 개발 환경

개발 언어



**Python v3.7**

OpenCV란?

물체 인식등의 실시간 처리를 목적으로 한 라이브러리이다.

라이브러리



**OpenCV**



TensorFlow란?

인공지능, 머신러닝을 위한 오픈소스 라이브러리이다.

에디터



**PyCharm**

# 동작 방식

## 두가지 버전으로 개발

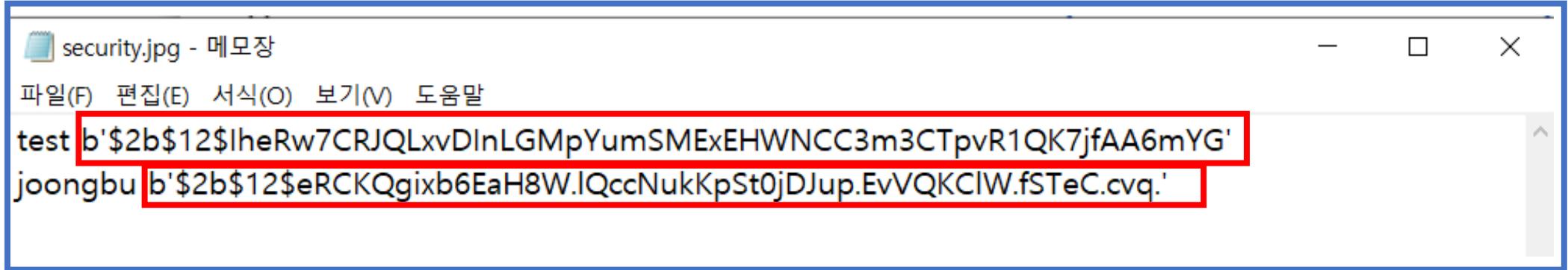
- 1) 설정 관리를 위한 UI 방식
- 2) 탐지기능만 수행하는 방식

# 동작 방식 - 설정 관리를 위한 UI

The image illustrates the user interface for the Screen Guarder application during the registration process. It consists of three overlapping screenshots:

- Left Screenshot:** Shows the main application window. The '소개' (Introduction) and '매뉴얼' (Manual) buttons are highlighted with red checkmarks. The '켜기' (Turn On) button is also visible. The application icon in the top right corner is crossed out with a red 'X'.
- Middle Screenshot:** Shows the 'Manual' screen. The application icon in the top right corner is crossed out with a red 'X'. A red checkmark is placed over the '패스워드 관리' (Password Management) button at the bottom.
- Right Screenshot:** Shows a '완료' (Complete) dialog box with a yellow warning icon and the message '등록이 완료되었습니다.' (Registration is complete.). An 'OK' button is visible at the bottom of the dialog box.

# 동작 방식 - 설정 관리를 위한 UI



**Bcrypt** 라는 라이브러리를 통해 패스워드를 **랜덤한 Salt값**과 함께 **암호화**하여 저장한다.

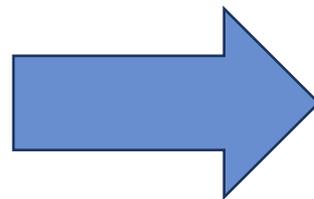
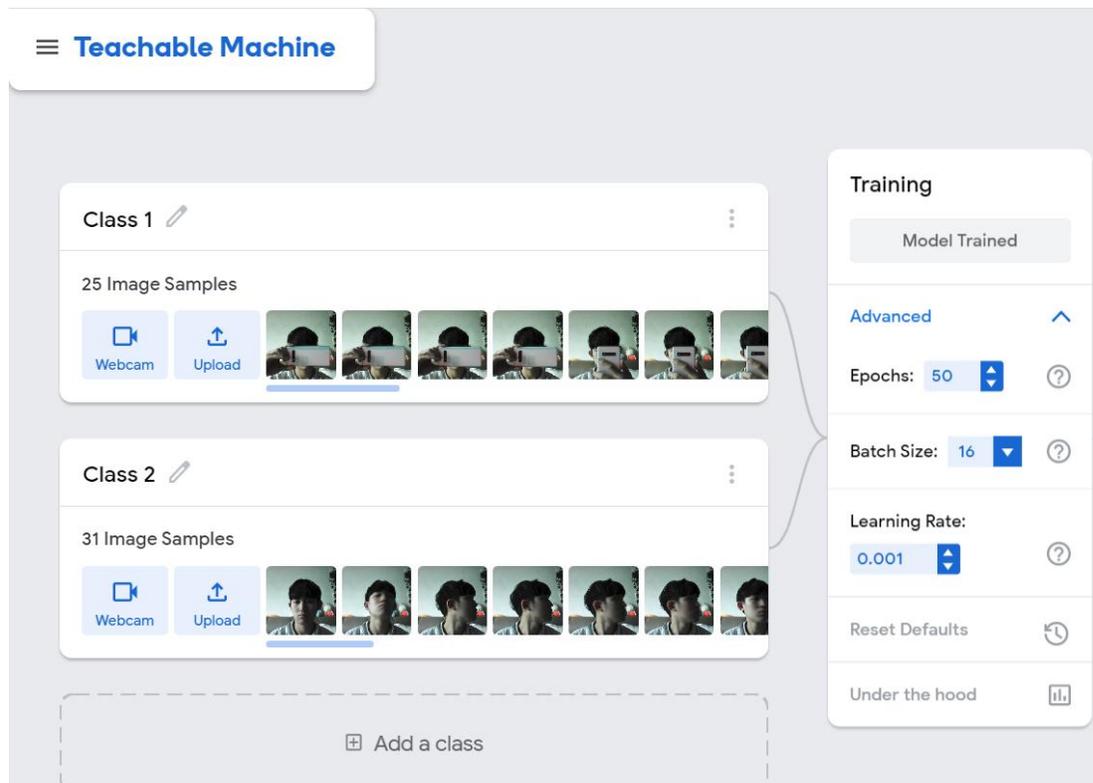


```
def manage_pw(self):  
    f = open("security.jpg", "a")  
    f.write(str(self.inputID.text()))  
    f.write(" ")  
    bc_pw = bcrypt.hashpw(self.inputPW.text().encode(), bcrypt.gensalt())  
    f.write(str(bc_pw))  
    f.write("\n")  
    QtWidgets.QMessageBox.warning(self, '완료', '등록이 완료 되었습니다.')  
    self.accept()
```

[ 암호화를 수행하는 클래스내의 함수 ]

# 동작 방식 - 탐지 기능만 수행

## 1. 머신러닝을 통한 학습 데이터 셋 생성.



**keras\_model.h5**

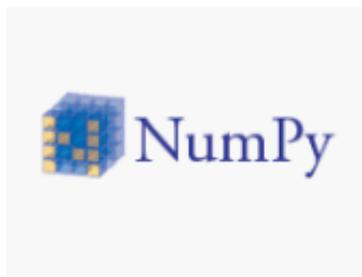
출처 : <https://teachablemachine.withgoogle.com/>

# 동작 방식 - 탐지 기능만 수행

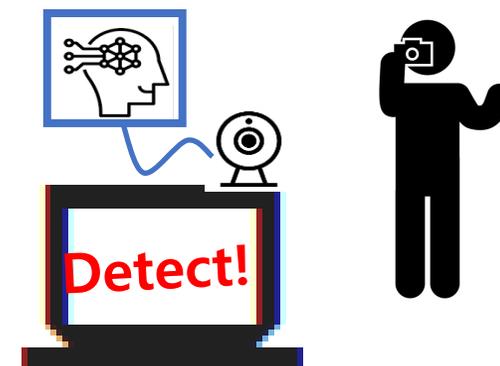
## 2. 데이터 셋을 통한 웹캠 프레임 예측 정도를 통해 탐지



TensorFlow 중에서 신경망 학습을 이용하는 학습 라이브러리이다.

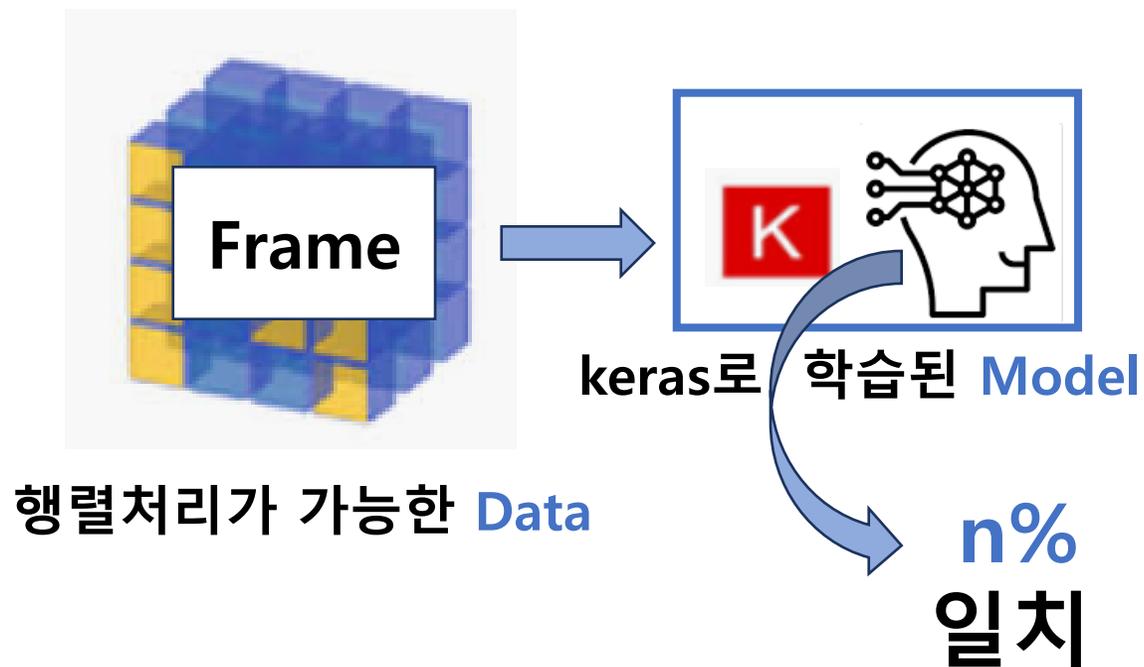


NumPy는 행렬이나 다차원 배열을 쉽게 처리 할 수 있도록 지원하는 파이썬의 라이브러리이다.



# 동작 방식 - 탐지 기능만 수행

## 2. 데이터 셋을 통한 웹캠 프레임 예측 정도를 통해 탐지



```
def lensDetect(self):
    while True:
        _, frame = self.cam.read()
        cv2.imwrite("a.jpg", frame)
        image = Image.open("a.jpg")
        # Make sure to resize all images to 224, 224 otherwise they won't fit in the array
        image = image.resize((224, 224))
        image_array = np.asarray(image)
        # Normalize the image
        normalized_image_array = image_array.astype(np.float32) / 127.0 - 1
        self.data[0] = normalized_image_array
        # run the inference
        prediction = self.model.predict(self.data)
        pred = str(prediction[0])
        if int(pred[3:6]) >= 800:
            cv2.imwrite("proof " + str(self.index) + ".jpg", frame)
            self.index += 1
            self.camDetect()
```

예측정도가 80% 이상일 경우 탐지로 인식

[ 예측을 수행하는 클래스내의 함수 ]

# 동작 방식 : 탐지가 될 경우

1) 화면에 경고창을 띄워서  
모니터의 내용을 보호.



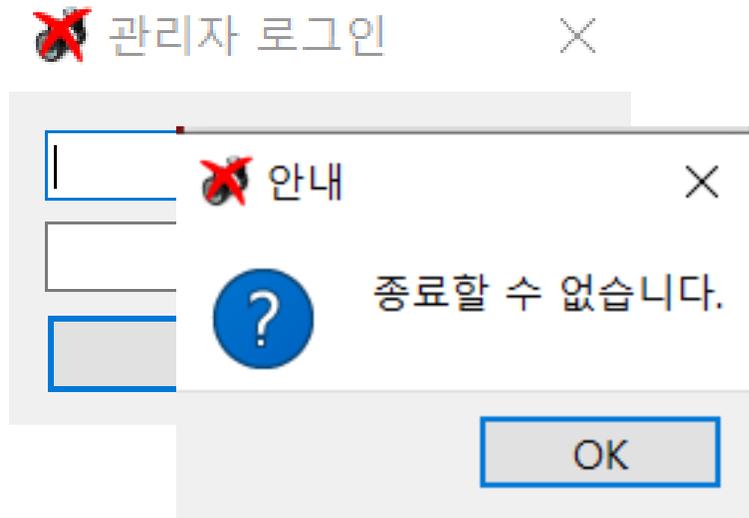
2) 탐지된 Frame을  
.jpg 파일로 저장.

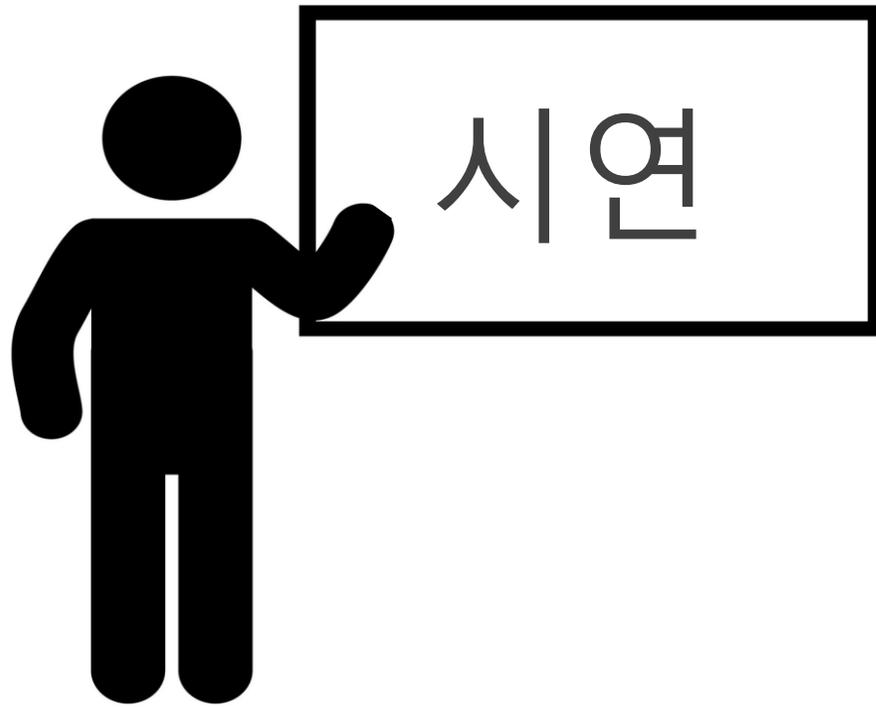


## 동작 방식 : 탐지가 될 경우

3) 잠금을 해제하기 위해선 ID/Password 입력 필요.  
또한, X 버튼의 기능을 막아둬م.

4) 내장된 .mp3 파일을 이용해 경고 소리를 알림.





**Q & A**



**HP : 010-2303-8619**

**E-mail : [seolki100480@gmail.com](mailto:seolki100480@gmail.com)**

**Git : [github.com/JBU-seol/cam\\_detect](https://github.com/JBU-seol/cam_detect)**

감사합니다

