Detection of real time video attacks in camera systems

Joris Janssen

Prof. Z.J.M.H. Geradts

CCTV systems around the world

Security Vulnerabilities

- Zero-day vulnerabilities
- Delayed updates
- Man-in-middle attacks


Microsoft Warns of Critical Windows Zero-Day Flaws

Hackers Actively Exploit 0-Day in CCTV Camera Hardware

Author:
Tom Spring
March 23, 2020

Home > Features

Vulnerabilities in smart IP cameras expose users to privacy, security risks

By Liviu Arsene April 11, 2019

Bitdefender has found new vulnerabilities in IoT cameras that are meant to be protecting people's homes.

Setup

- Motion detection
- Attack model
- Movement based attack detection
- Electrical Net Frequency (ENF) based attack detection

Background

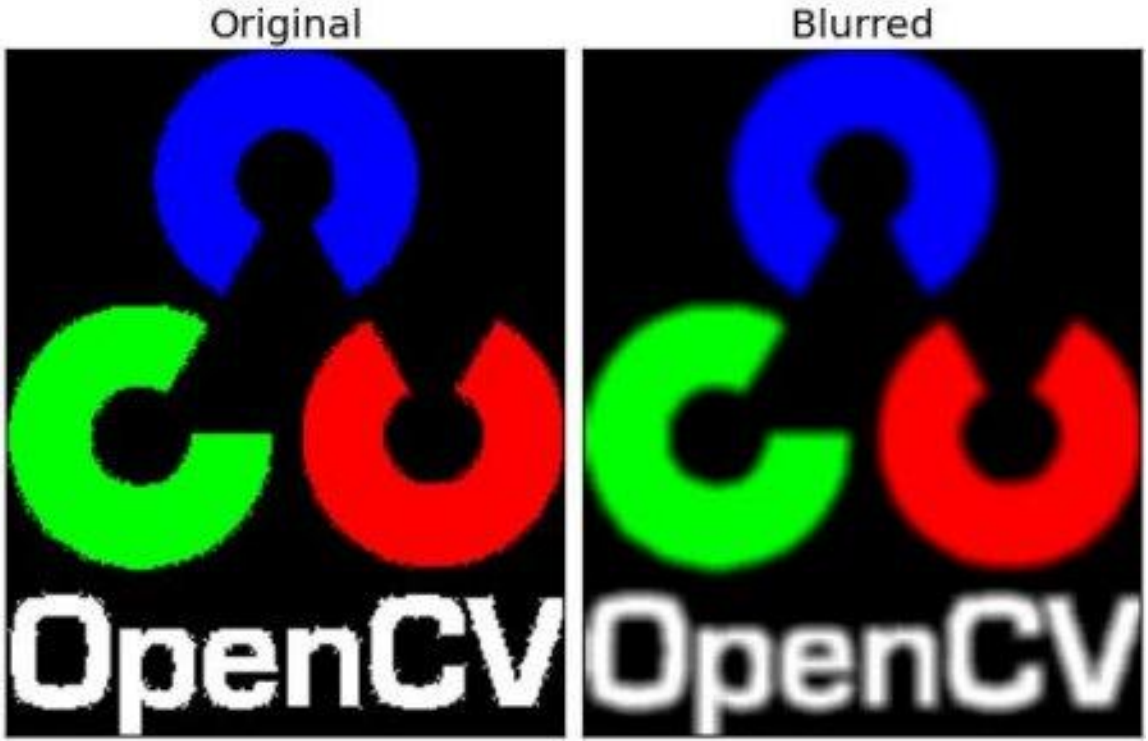
Movement in frame

Smoothen Image

```
kernel = np.ones((5,5),np.float32)/25
detect_frame = cv2.filter2D(frame,-1,kernel)
```

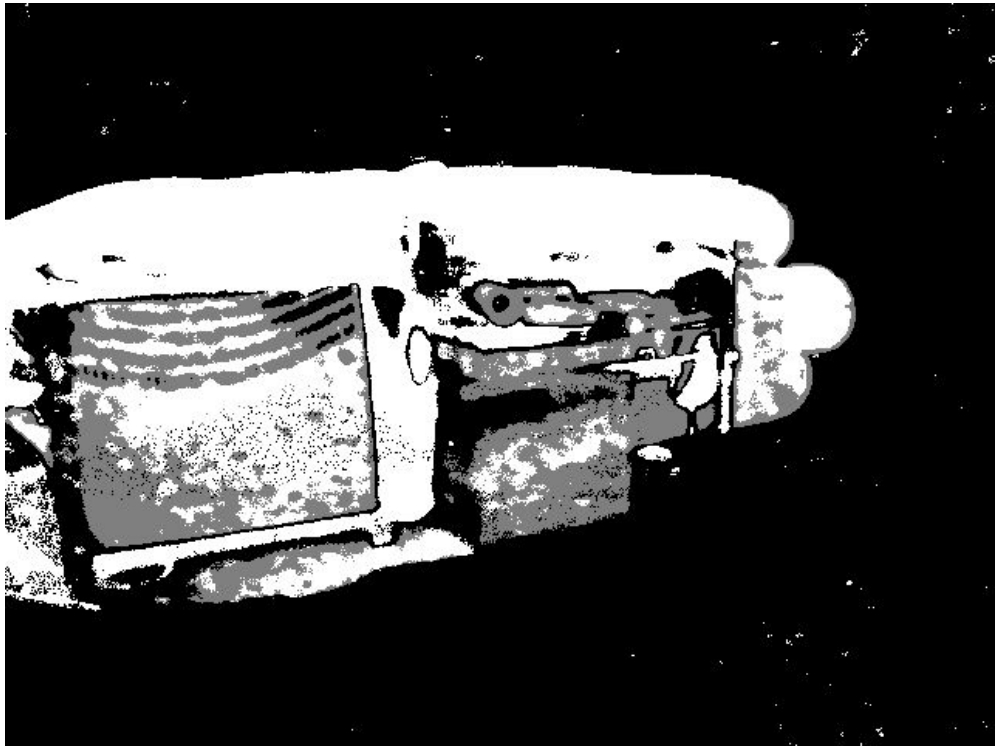
Smoothen Image

```
kernel = np.ones((5,5),np.float32)/25
detect_frame = cv2.filter2D(frame,-1,kerne
```



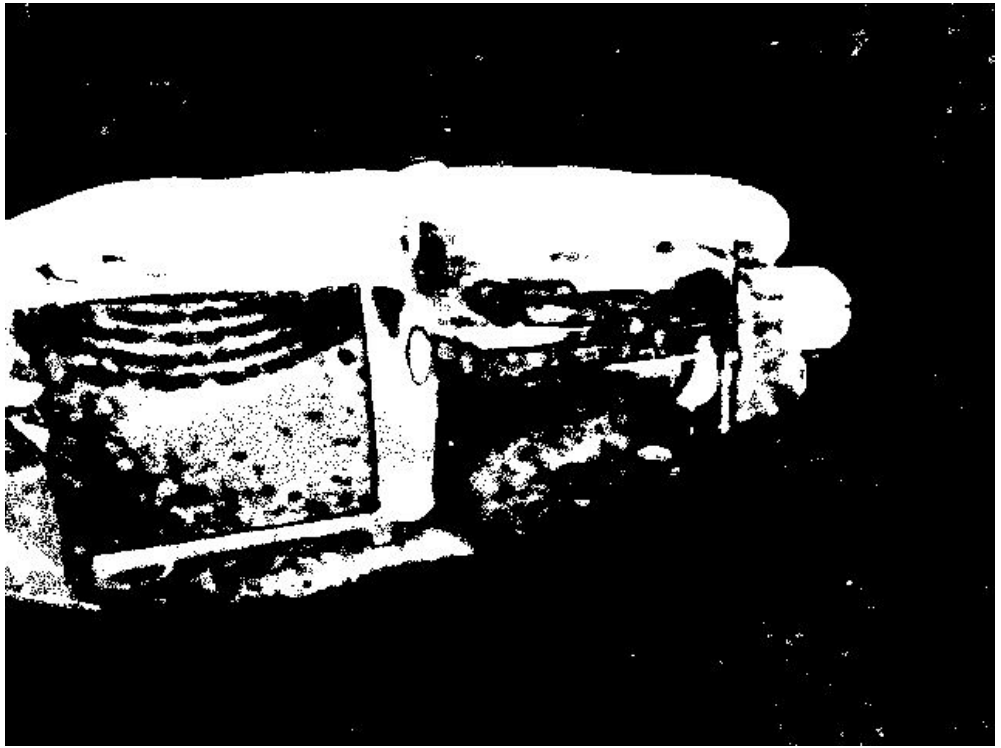
Remove Background

```
backSub = cv2.createBackgroundSubtractorKNN()
fgMask = backSub.apply(frame)
```



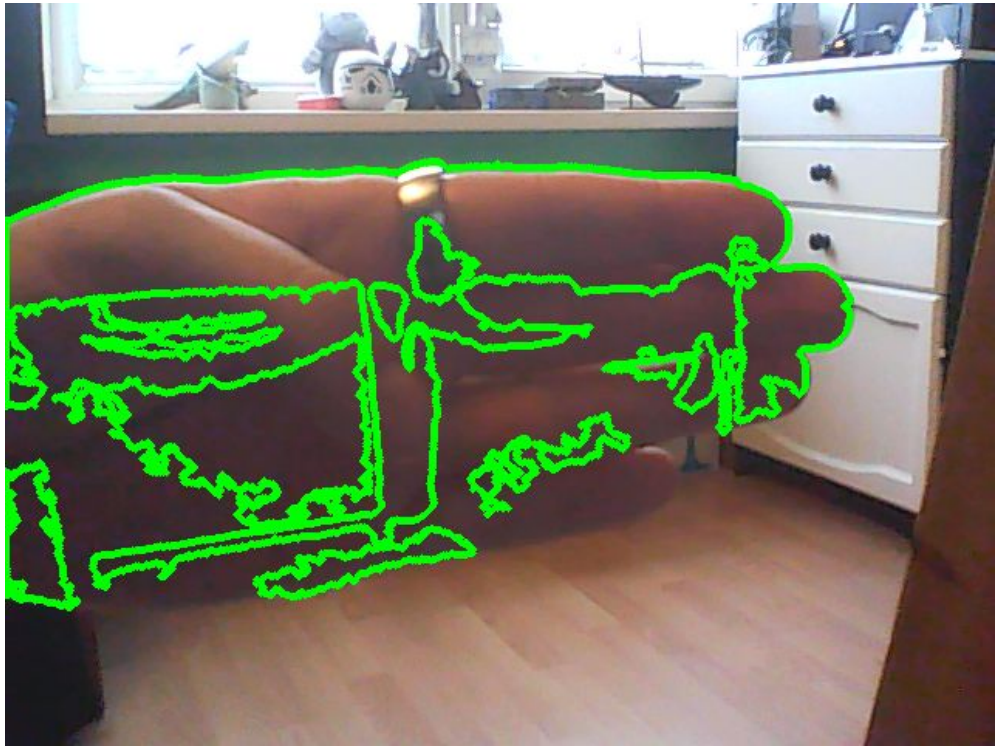
Filter movement

thresh = cv2.threshold(fgMask, 127, 255, 0)



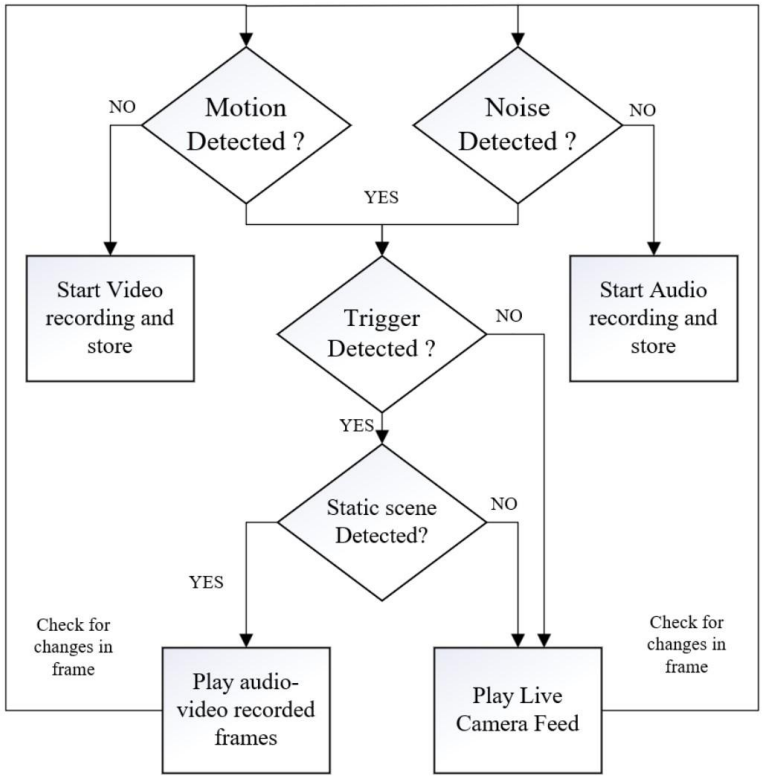
Find Area's of movement

contours, _ = cv2.findContours(thresh)



Visual purposes only

Frame duplication attack

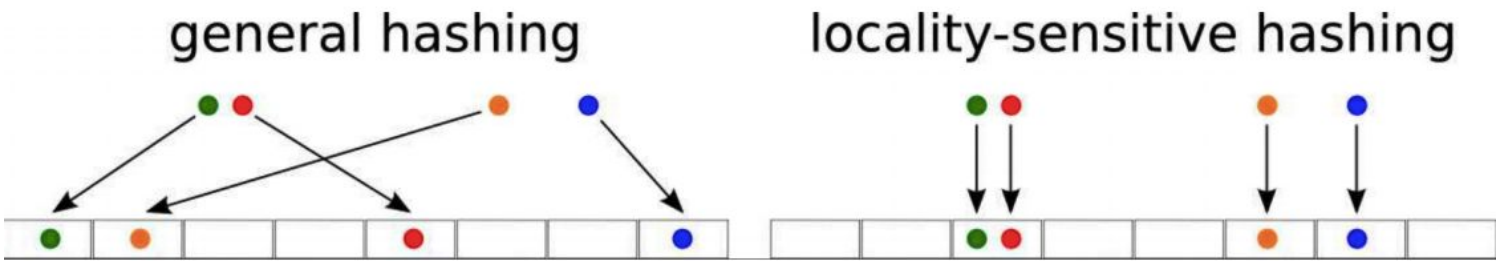


Frame duplication attack

Send →

Real →

Detection of duplicated frames

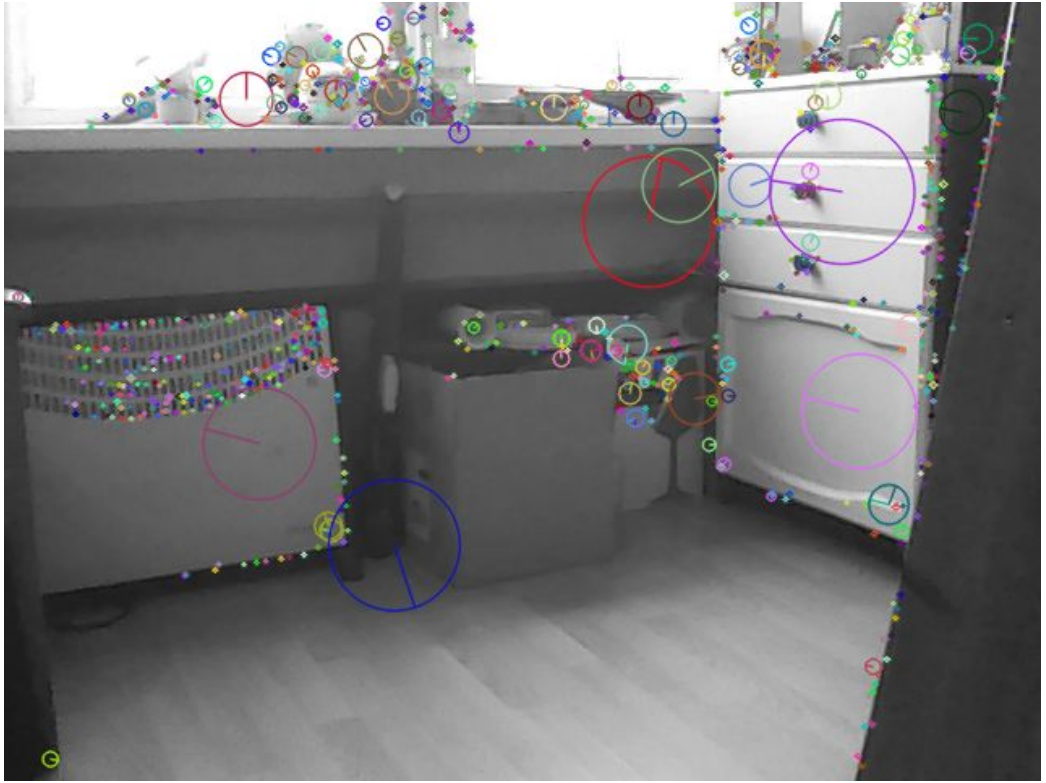


Movement based protection

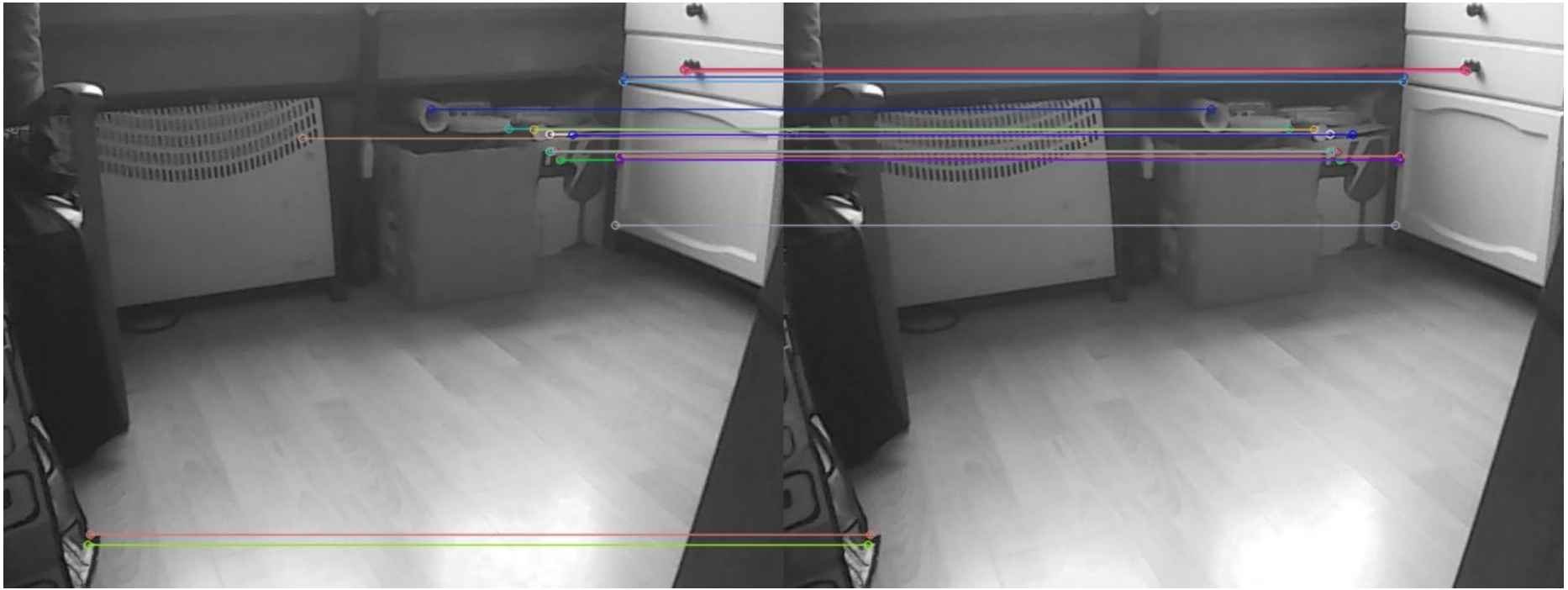
Needs a motorized Camera

Feature Matching

Movement based protection



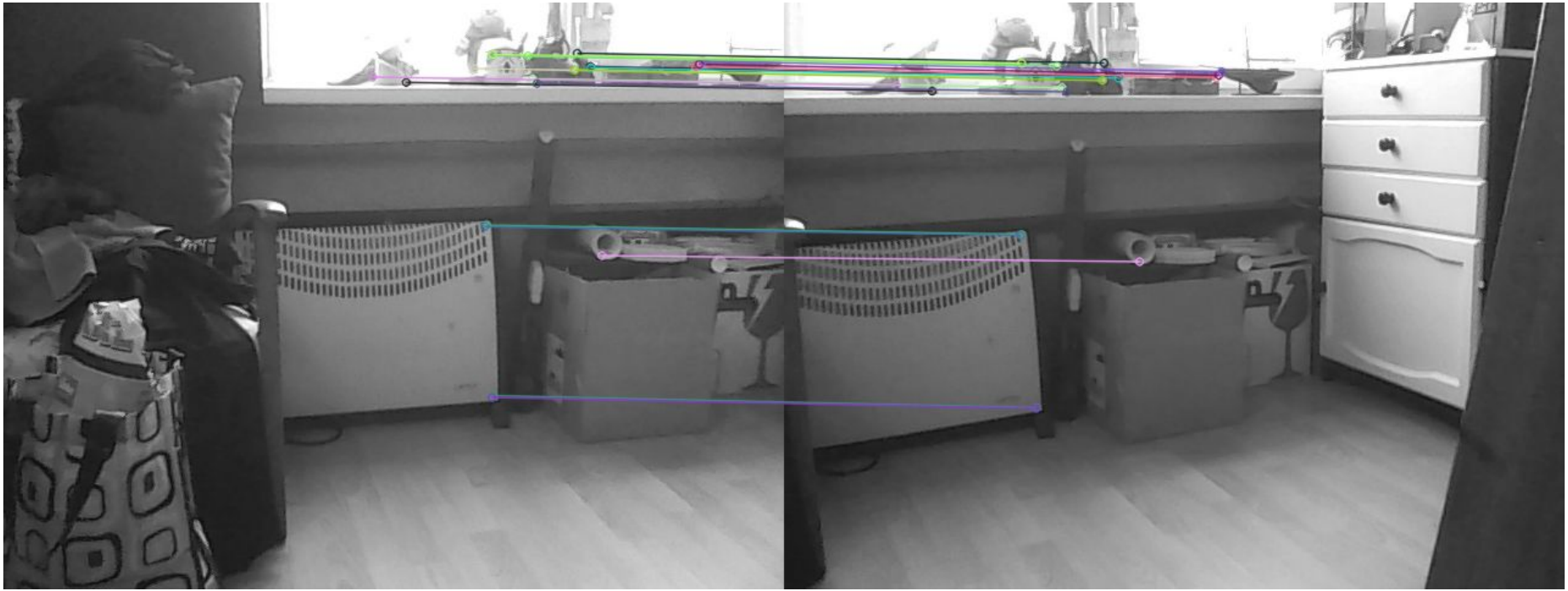
Movement based protection



Current Frame

Previous Frame

Movement based protection



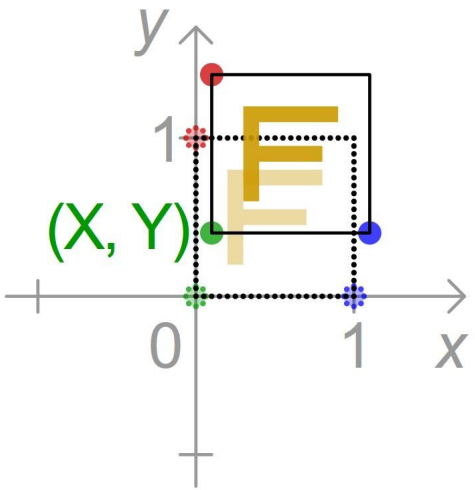
Current Frame

Previous Frame

Movement based protection

Translate

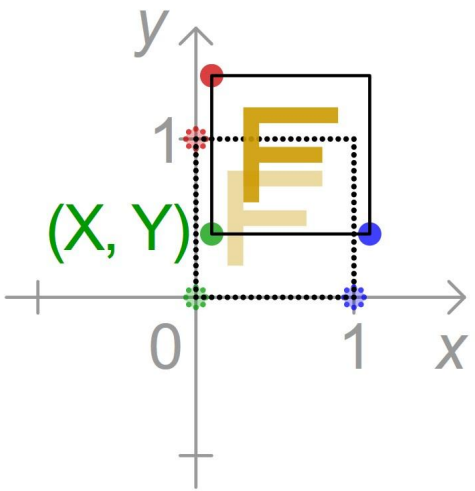
$$\begin{bmatrix} 1 & 0 & X \\ 0 & 1 & Y \\ 0 & 0 & 1 \end{bmatrix}$$



Movement based protection

Translate

$$\begin{bmatrix} 1 & 0 & X \\ 0 & 1 & Y \\ 0 & 0 & 1 \end{bmatrix}$$




```
Transformation Matrix:
 [[   1.    0. -213.]
 [   0.    1.   -2.]
 [   0.    0.    1.]]
Distance:  213.0
Angle:  -90.0
Movement Direction: Left
```

Attack on Movement based protection

Stitching of images

Complete Recording of area

Attack on Movement based protection

Attack on Movement based protection

Useful in practise?

- Expensive Algorithm
- Only real time detection
- Needs motorized camera

Electrical Net Frequency (ENF) based detection

Normally 50 Hz +- 10mHz (60 Hz in US +-20mHz)

Difficult to predict

ENF is similar across different buildings

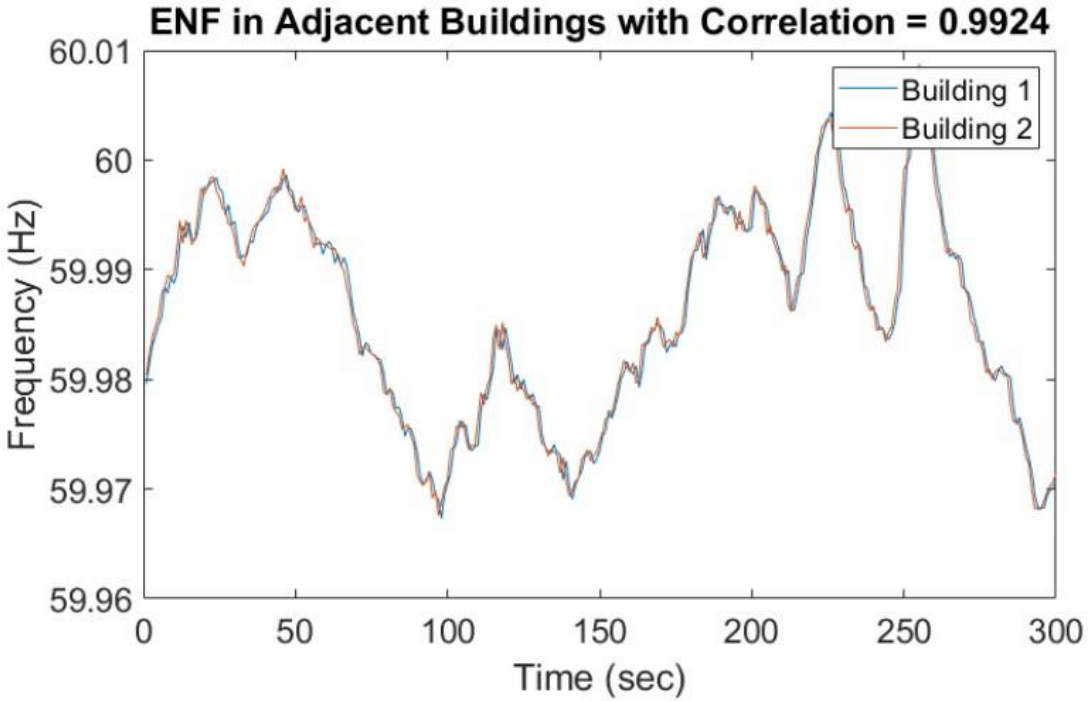


Figure 4. ENF captured in adjacent Buildings.

Image source: nagothu2019detecting

Setup

Audio

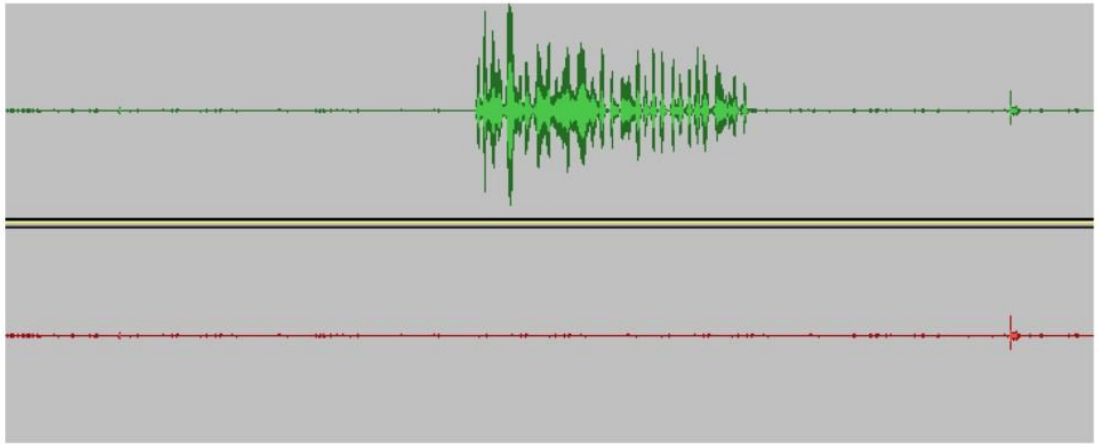


Image source: nagothu2019detecting

Harmonics at 60, 180, 300 Hz

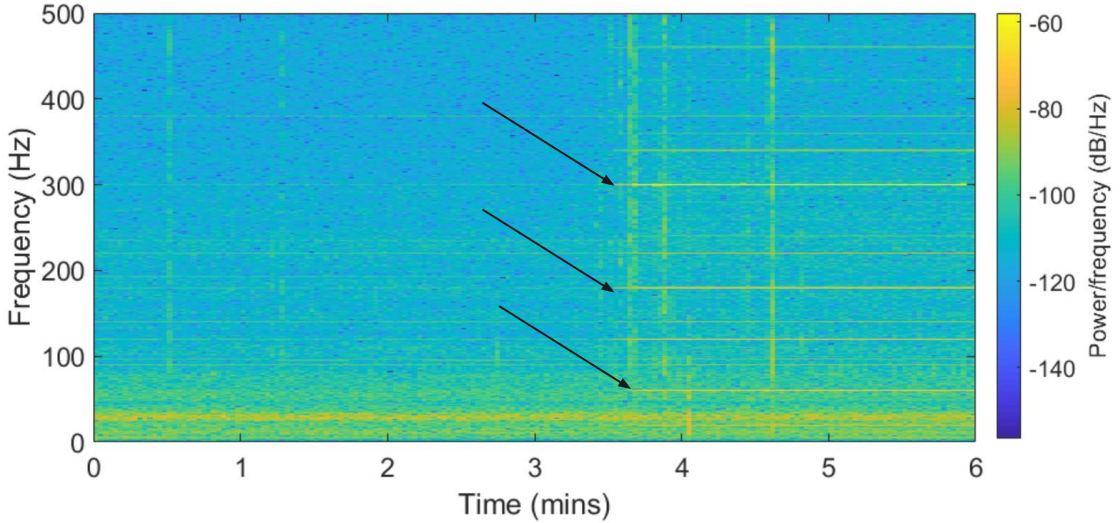
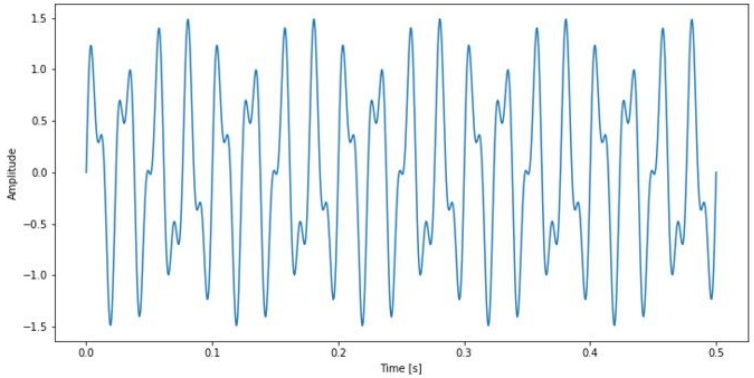


Figure 2. Spectrogram of audio recording with noise source after 3.5 min.

Image source: nagothu2019detecting

Fast Fourier Transform



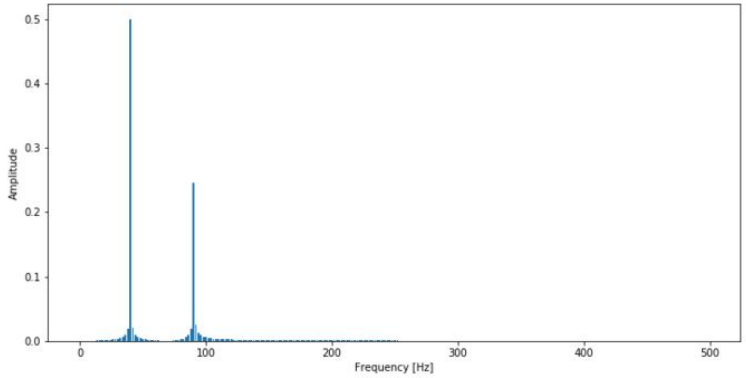


Image source: nagothu2019detecting

Fast Fourier Transform

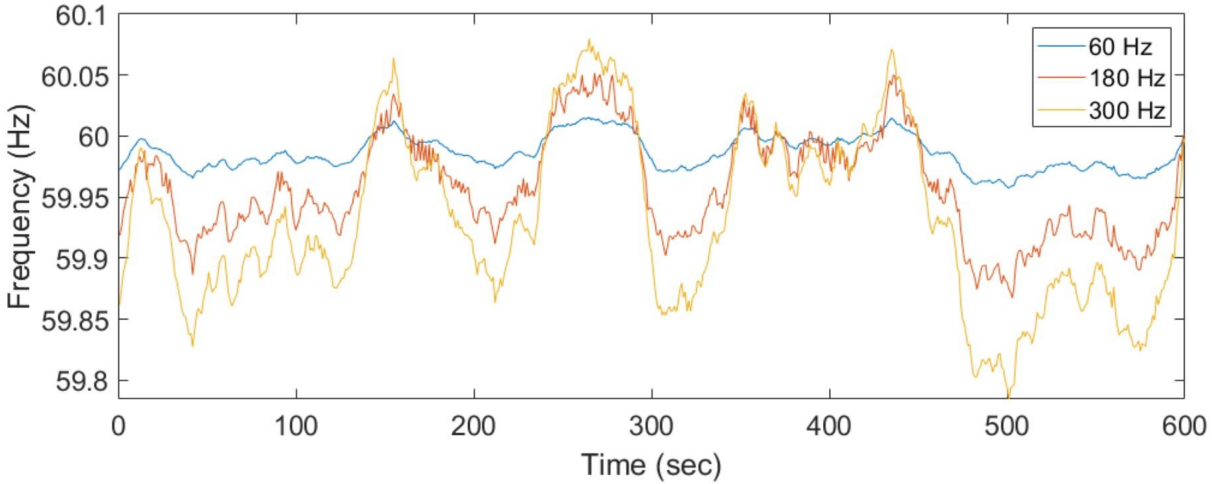


Figure 8. Different harmonics of power recording shifted to 60 Hz for comparison.

Image source: nagothu2019detecting

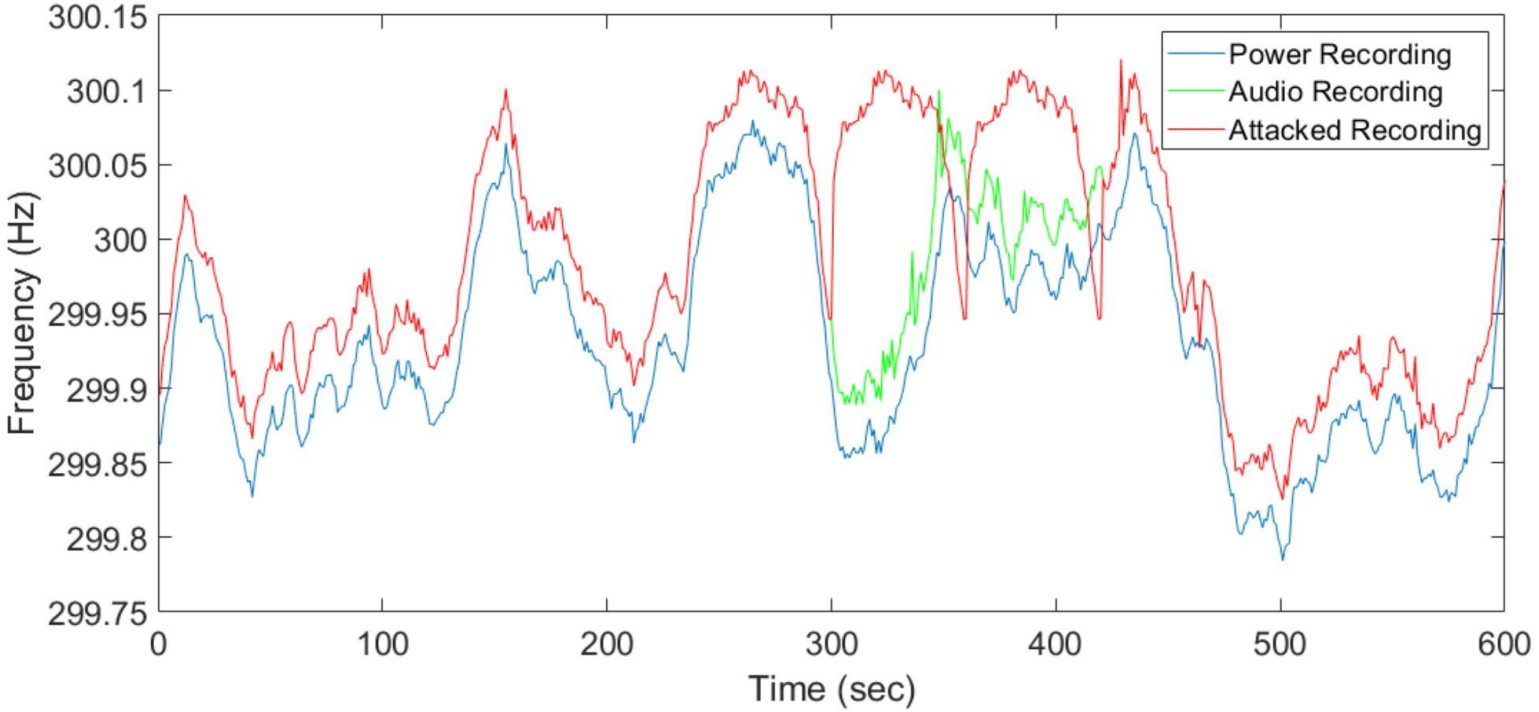


Image source: nagothu2019detecting

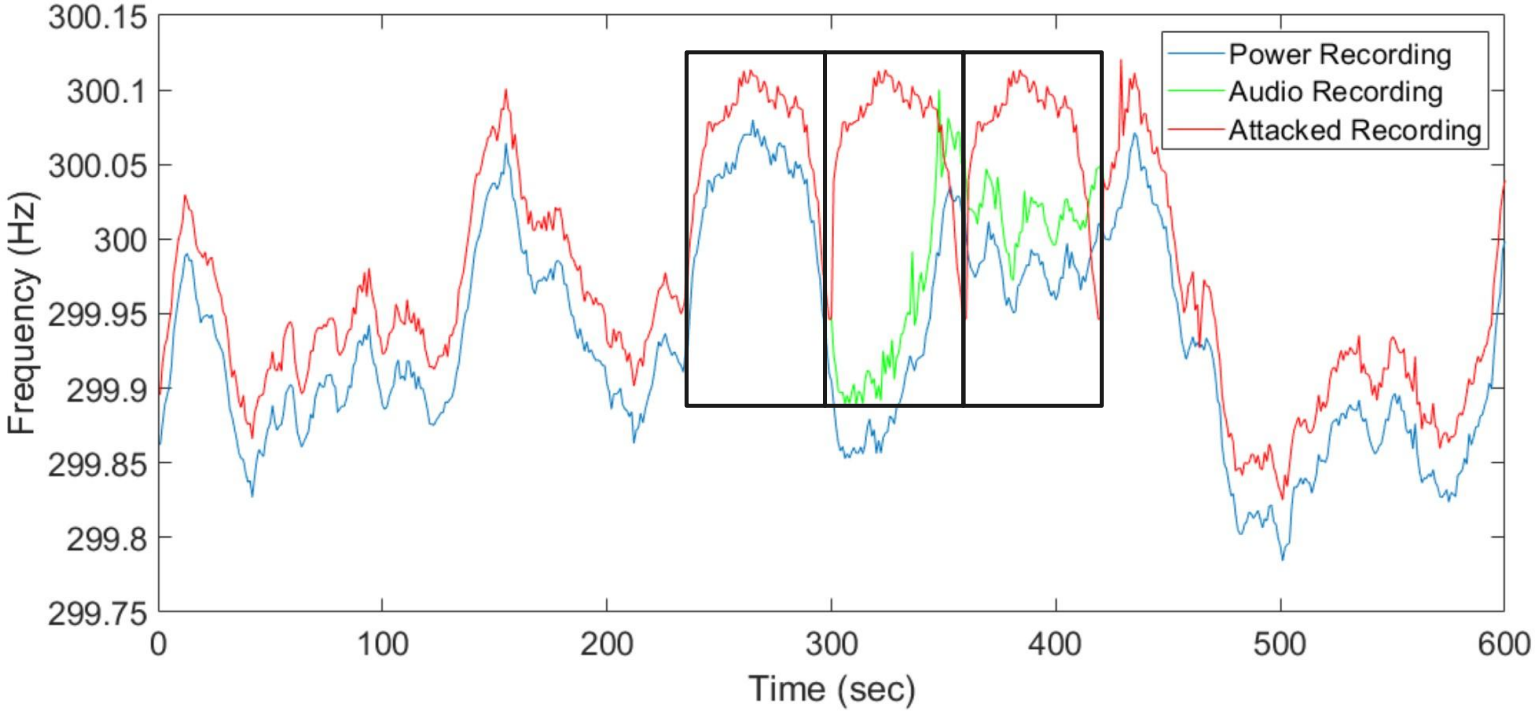


Image source: nagothu2019detecting

Shifting Window Correlation

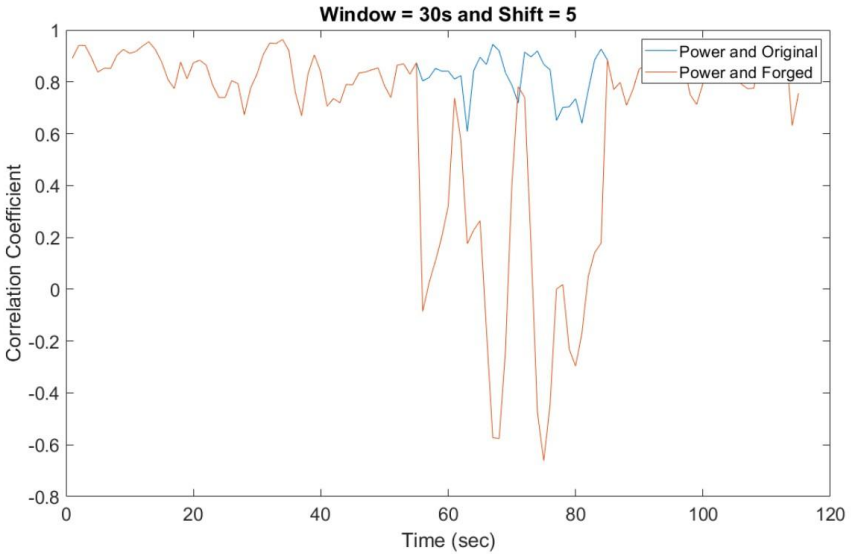


Figure 16. Detecting the forged audio recording using correlation coefficient.

Image source: nagothu2019detecting

Future Work

- Using real camera systems
- Noise interference for ENF recording
- Video based ENF recording

nagothu2019detecting:
Nagothu, D., Chen, Y., Blasch, E., Aved, A., and Zhu, S., “Detecting malicious false frame injection attacks on the internet of video things using electrical network frequency signals,”*Sensors, Special Issue on Intelligent Signal Processing, Data Science and the IoT World,*