RSAConference2019
Asia Pacific & Japan
Singapore | 16–18 July | Marina Bay Sands

SESSION ID: FLE-R01

Drones' Cryptanalysis: Smashing Cryptography with a Flicker

Raz Ben Netanel

Security Researcher
Cyber@BGU (CBG)

Co. Authors

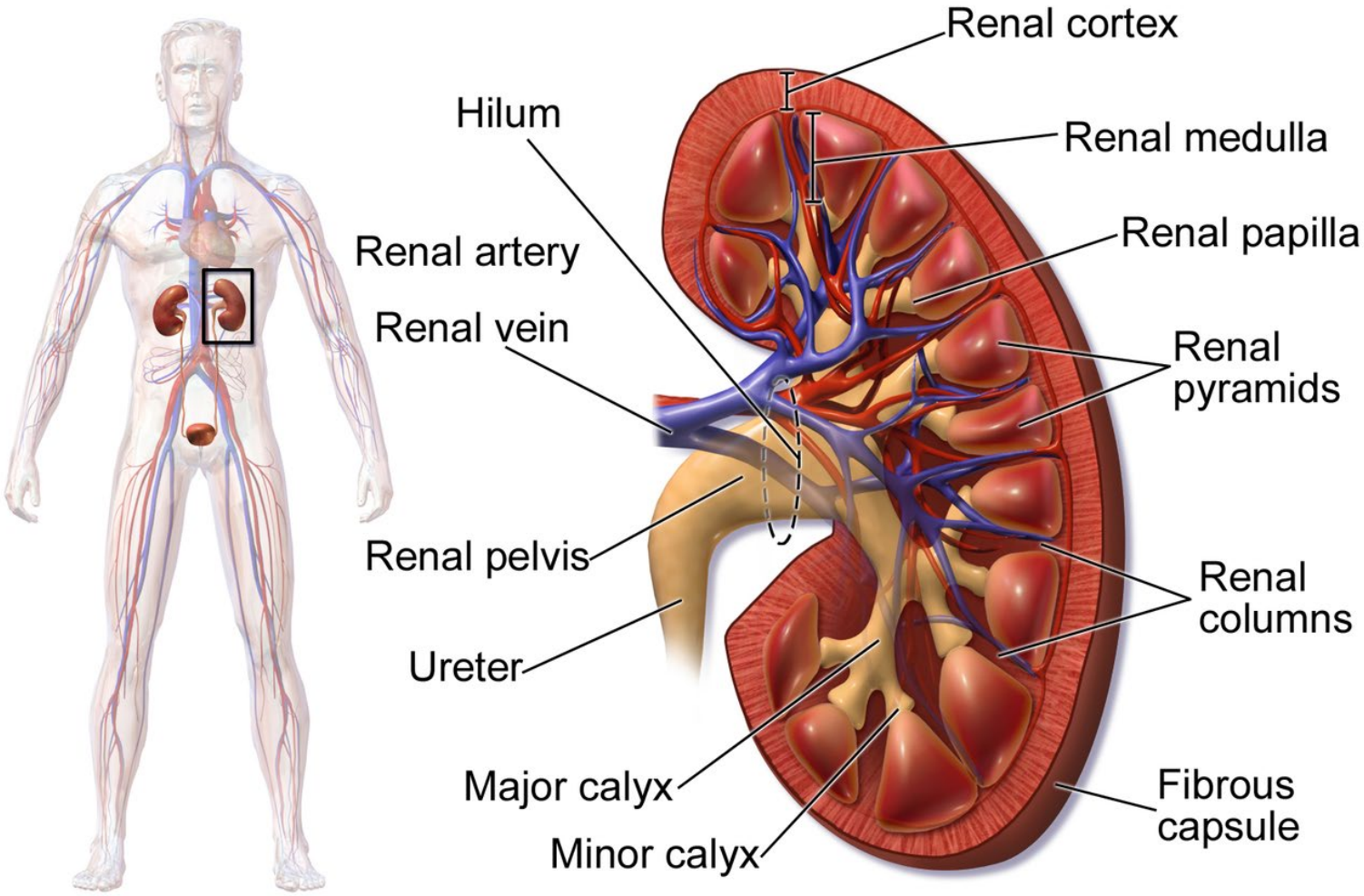
DRONES' CRYPTANALYSIS - SMASHING CRYPTOGRAPHY WITH A FLICKER

Preliminary Version of the Paper:
Game of Drones - Detecting Streamed POI from Encrypted FPV Channel

Ben Nassi

Prof. Adi Shamir

Prof. Yuval Elovici



Kidney Anatomy

Kidneys Donation and Transplantation

- Over **3,000** new patients are added to the kidney waiting list each month.
- **13** people die each day while waiting for a life-saving kidney transplant.
- In 2014, **4,761** patients died while waiting for a kidney transplant. Another, **3,668** people became too sick to receive a kidney transplant.

The New York Times

April 30, 2019

Like 'Uber for Organs': Drone Delivers Kidney to Maryland Woman

Advantages of Drones

- Fast
- Cheap
- Easy to use
- Life saving

Drones Create a New Threat to Privacy

Not in my backyard! Woman throws stones before using a GUN to get rid of nosy neighbour's drone

Mail Online

Kentucky Man Arrested After Shooting Down Neighbor's Drone

NBC NEWS

Spouses are using DRONES to catch their cheating partners

Mail Online

Eyes In The Sky: The Public Has Privacy Concerns About Drones

Forbes

Are Drones Spying on Miley Cyrus and Selena Gomez?

People

Drone complaints soar as concerns grow over snooping

theguardian

The drones among us: Reports of drone-related incidents are going up and up and up

NATIONAL POST

Legitimate vs Illegitimate Purpose

Taking a selfie

Spying

Methods for Drone Detection

Radar

Camera

LiDAR

Microphone Array

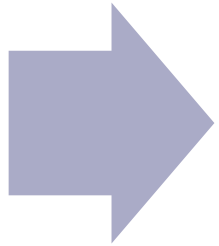
THESE METHODS ARE ABLE TO DETECT THE PRESENCE OF NEARBY DRONES.

Research Question

How can we determine whether a drone that is passing near a house is being used by its operator for a legitimate purpose or an illegitimate purpose?

Objectives

Classifying a suspicious radio transmission as an FPV channel



Detecting whether an FPV channel is being used to spy on a victim

Target Detection Scheme

Malicious Drone Operator

Wi-Fi FPV Channel

Spying Detection Mechanism

Watermarker

Victim

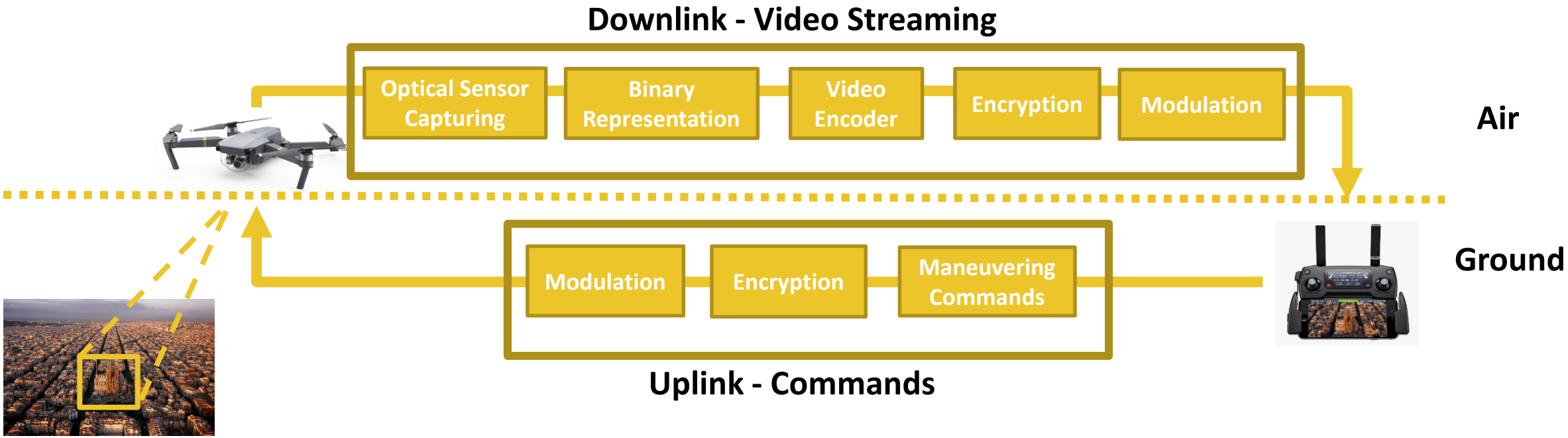
Assumptions:

- The attacker is using a Wi-Fi FPV drone (located in a range of up to 5 KM from the victim).
- The spy detection mechanism is connected to an RF scanner with a proper antenna for intercepting suspicious radio transmissions.

Wi-Fi First-Person View Channel

Wi-Fi First-Person View (FPV) Channel - a communication channel based on Wi-Fi communication designed to:

- Stream the video captured by the drone's video camera to the operator's controller.
- Maneuver the drone.



Wi-Fi FPV Channel

- Distance up to 5 KM
- Eliminates the need for using a dedicated controller
- Examples of Wi-Fi FPV drones include:

DJI – Mavic Air

DJI Spark

DJI Mavic Pro

Parrot – Bebop 2

GoPro – Karma

Intercepted Bitrate Signal

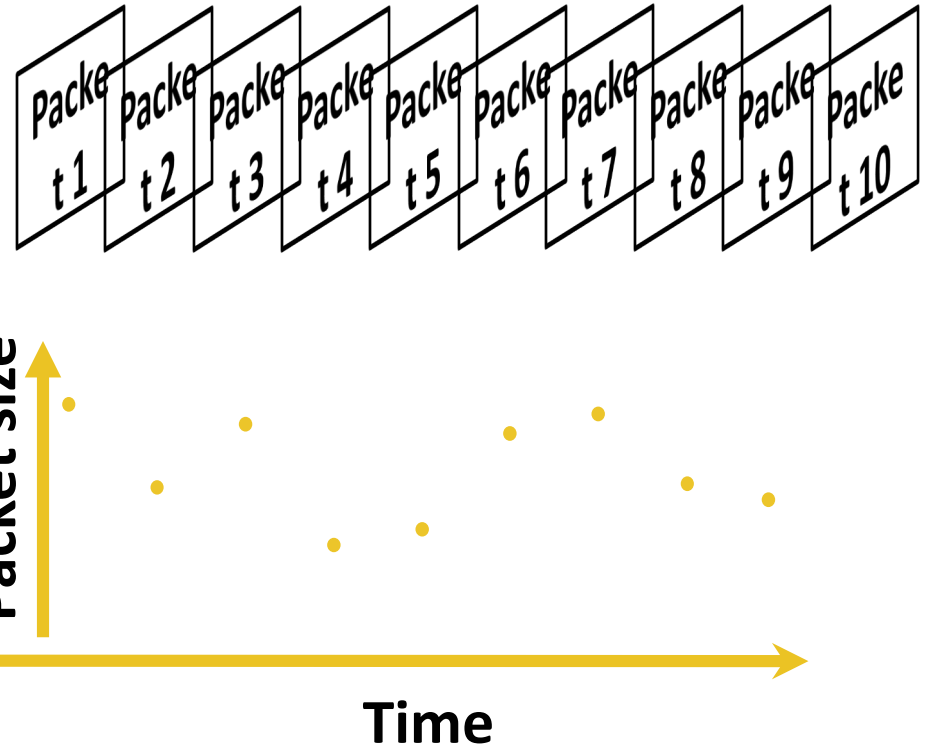
1) Sniffing Wi-Fi Packets

- Enabling NIC's monitoring mode (attack mode)
- Sniffing a network using **Airmon**

2) Extracting a time series signal from unencrypted metadata (2nd layer)

- Packet length (frame.len)
- Packet arrival time (frame.number)

3) Downsampling (by aggregating time series in a fixed window)



Objective #1

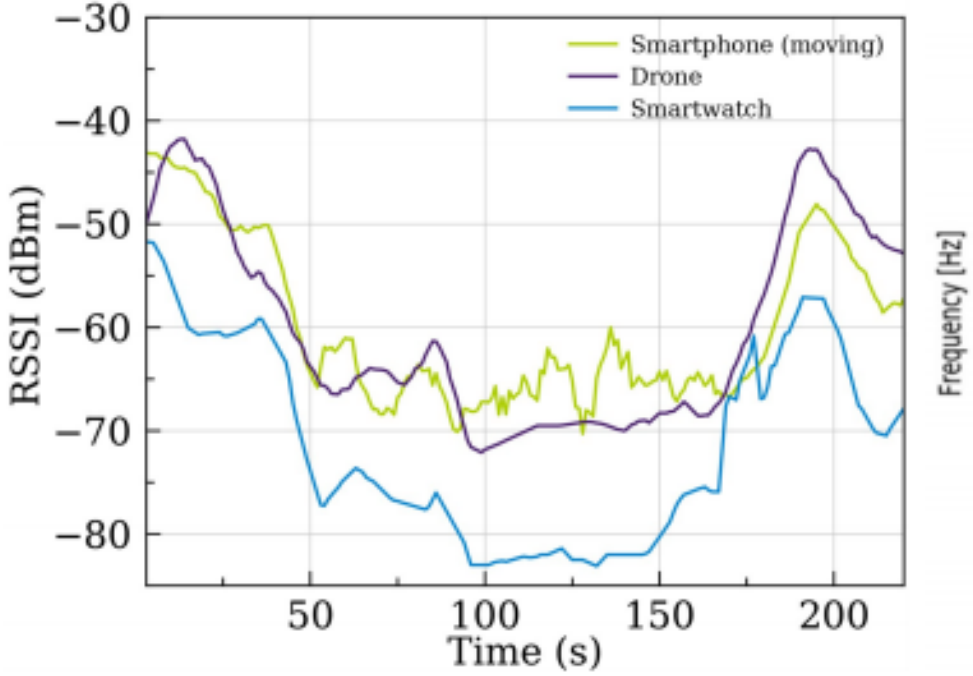
Classifying a Suspicious Transmission as an FPV Channel

Classifying a Suspicious Transmission as an FPV Channel

Key Observation: A drone is a flying camera.

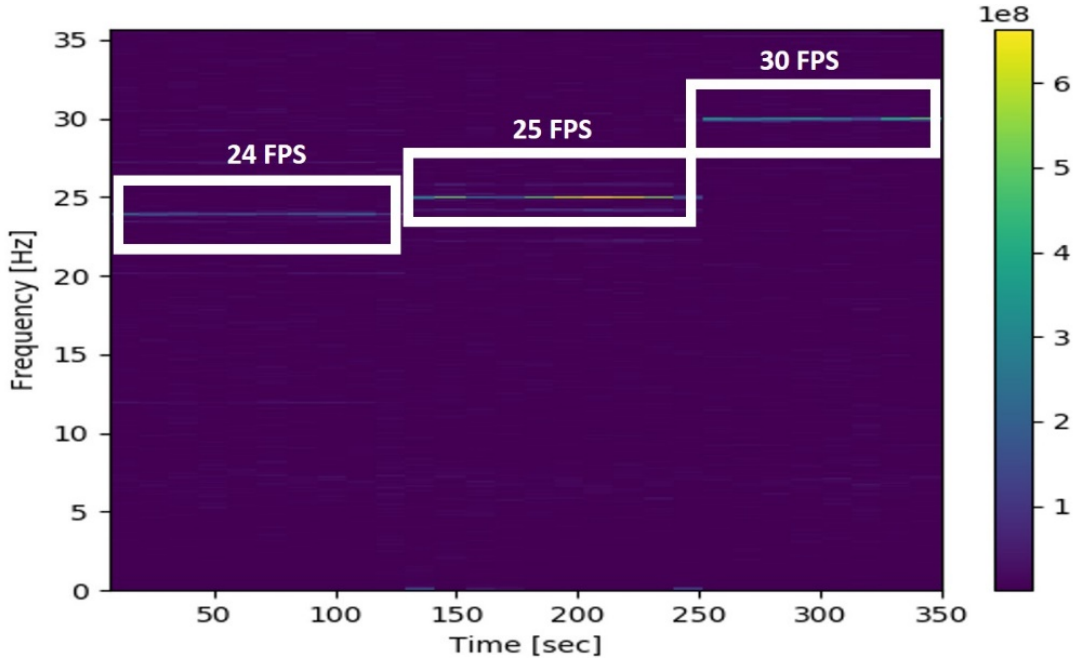
Moving Object Detection

- Analyzing received signal strength indication measurements for a given device (MAC) over time.
- Determining that a device is on the move according to measurement changes.



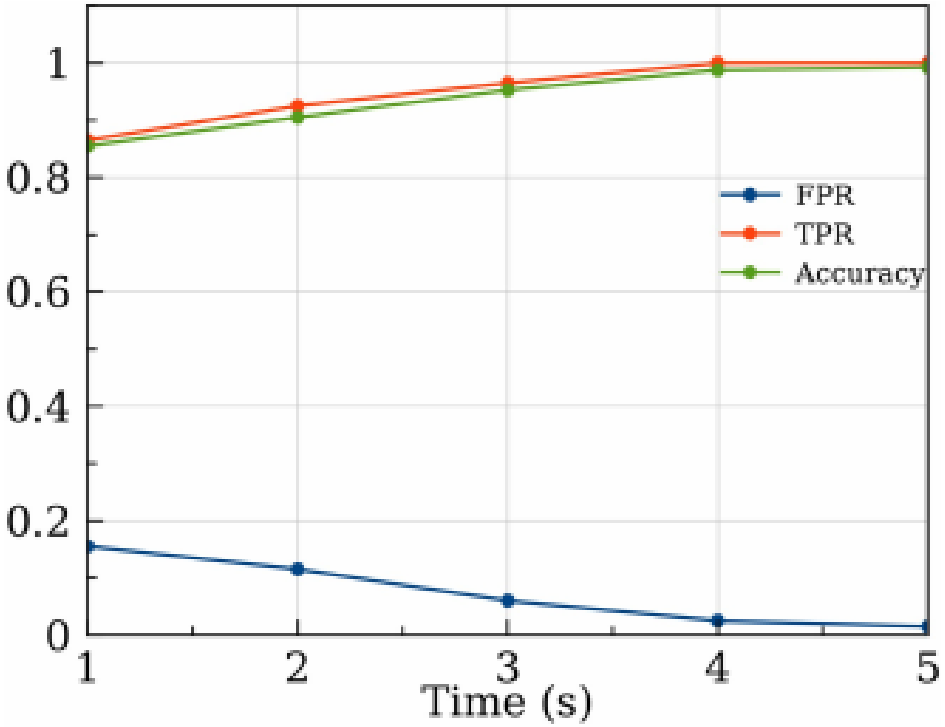
Camera Detection

- Analyzing the intercepted bitrate signal in the frequency domain.
- Finding the frequency with the maximum magnitude.
- Compare the frequency with the maximum magnitude to known frame per second rates of drones {24,25,30,60,96,120}.



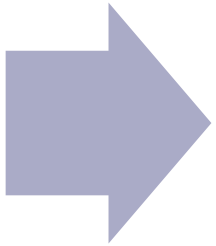
Results

We can determine whether a suspicious radio transmission is an FPV channel within 4 seconds with accuracy of 99.9%.



Objectives

Classifying a suspicious radio transmission as an FPV channel

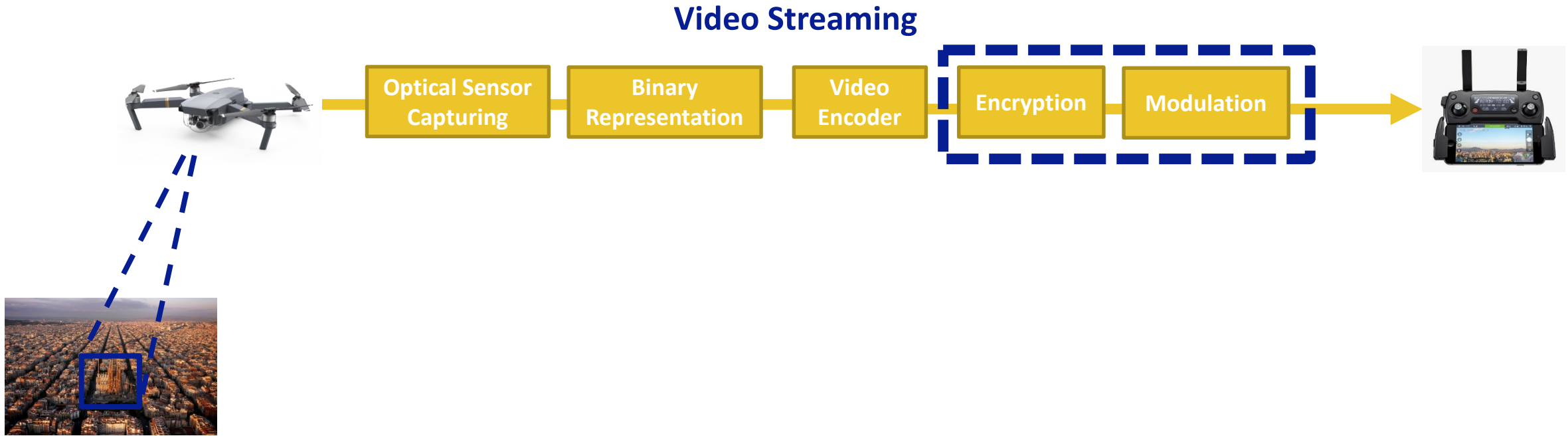


Detecting whether an FPV channel is being used to spy on a victim

Objective #2

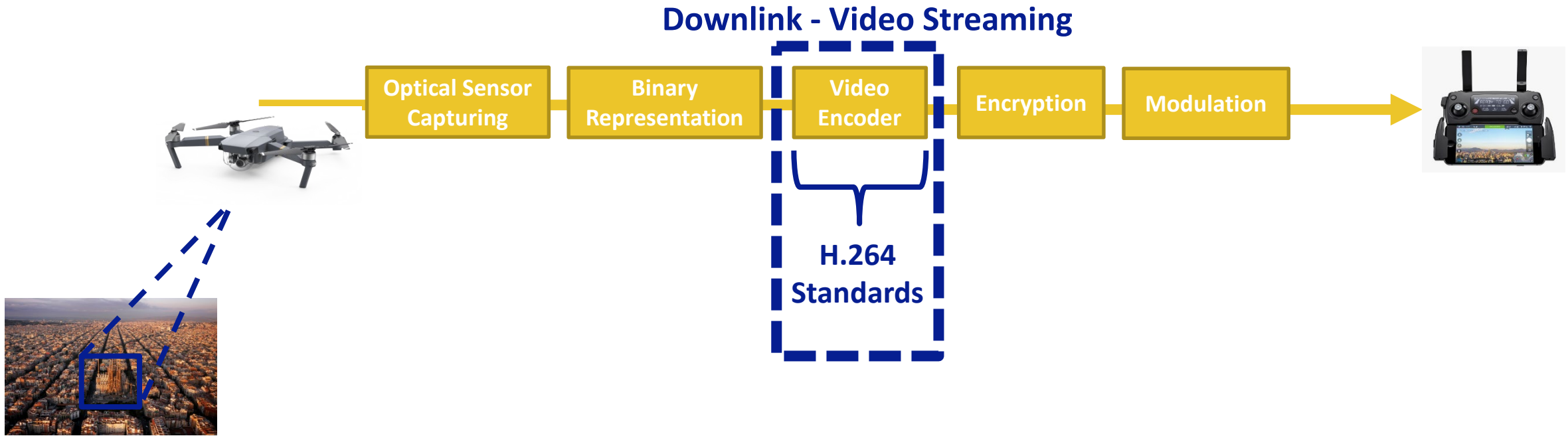
Detecting whether an FPV channel is being used to spy on a victim

Downlink - Video Streaming Channel

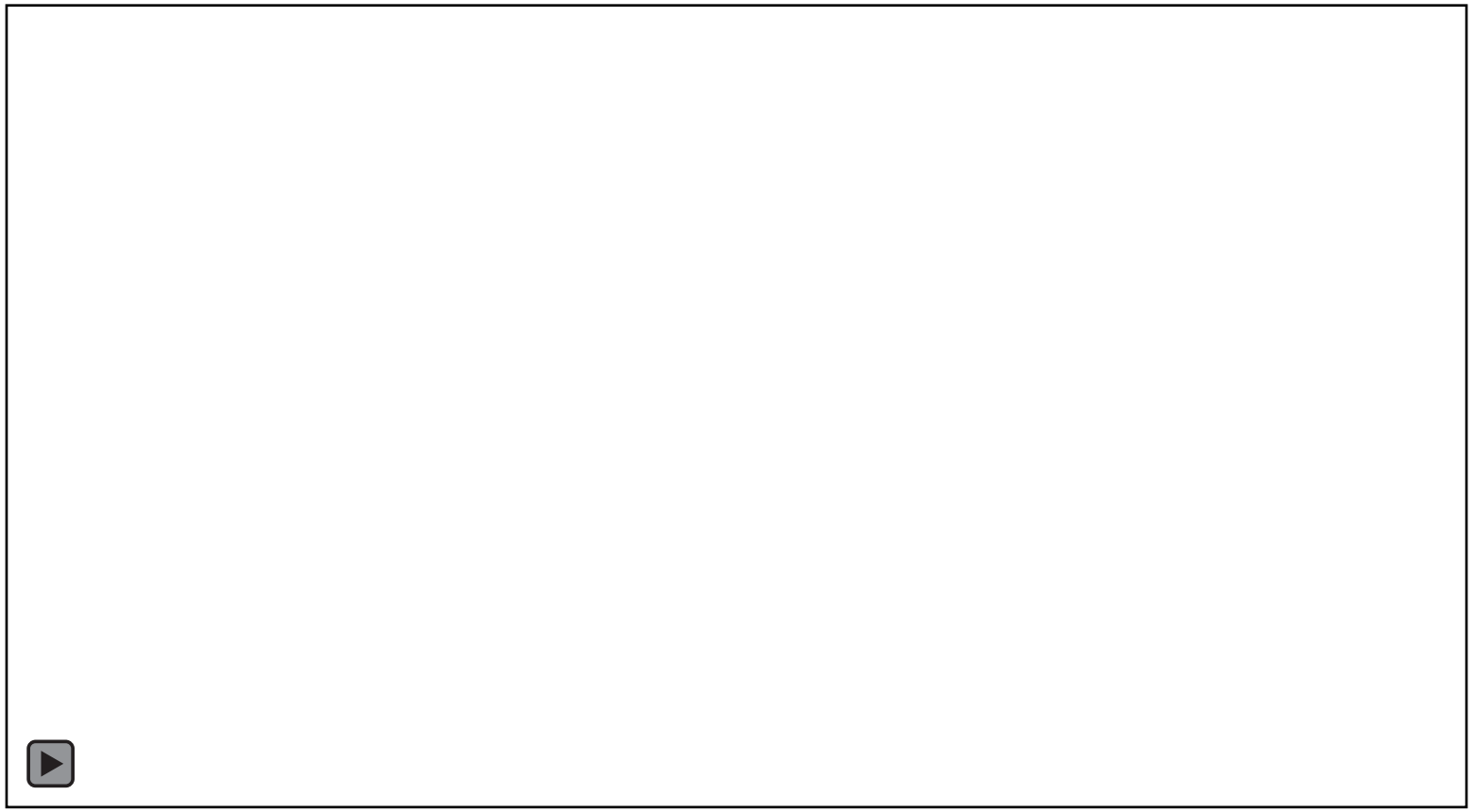


VIDEO STREAM IS ENCRYPTED.
DOES ENCRYPTION ENSURES CONFIDENTIALITY?

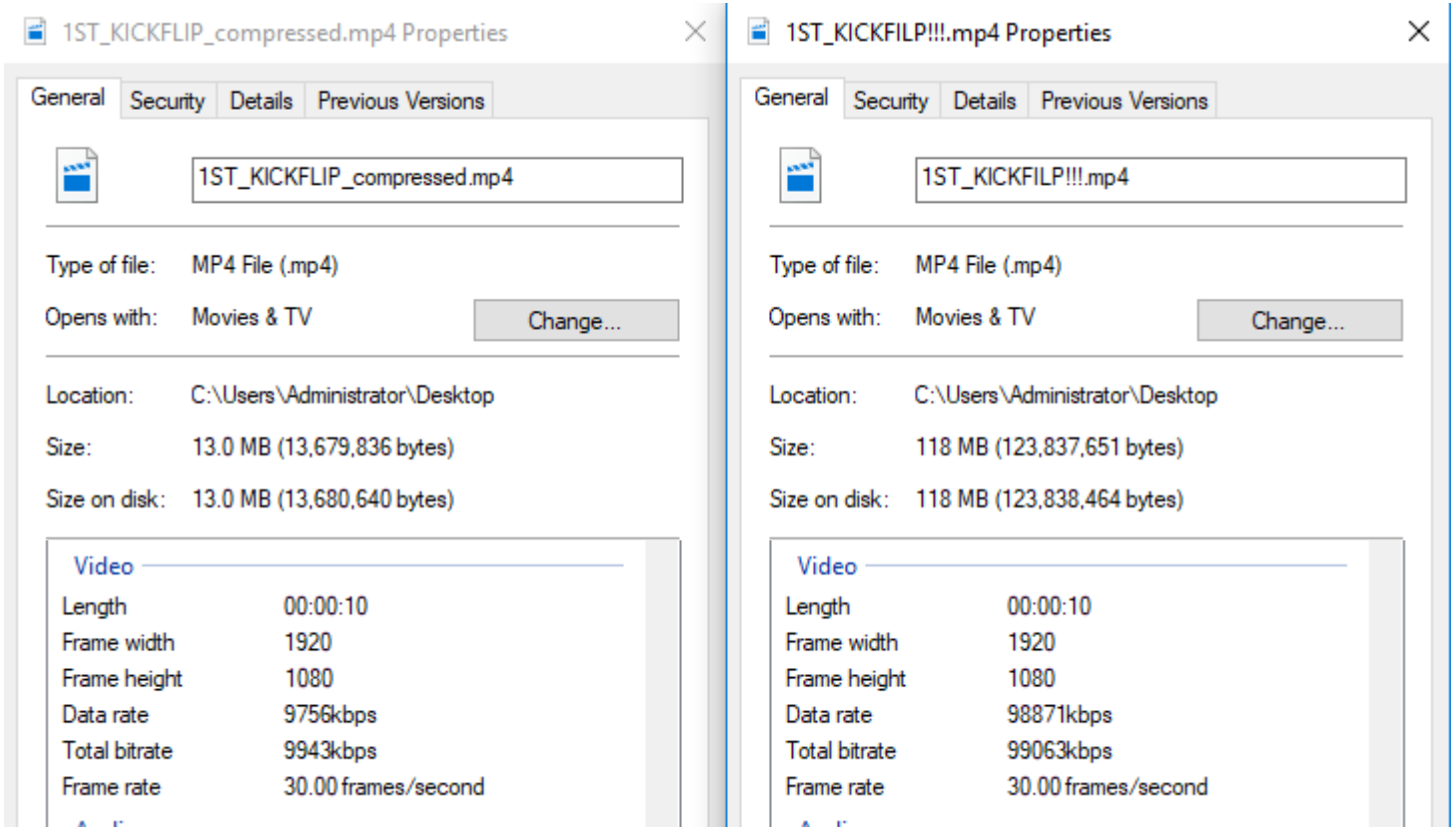
Video Compression Stage



Compression Efficiency

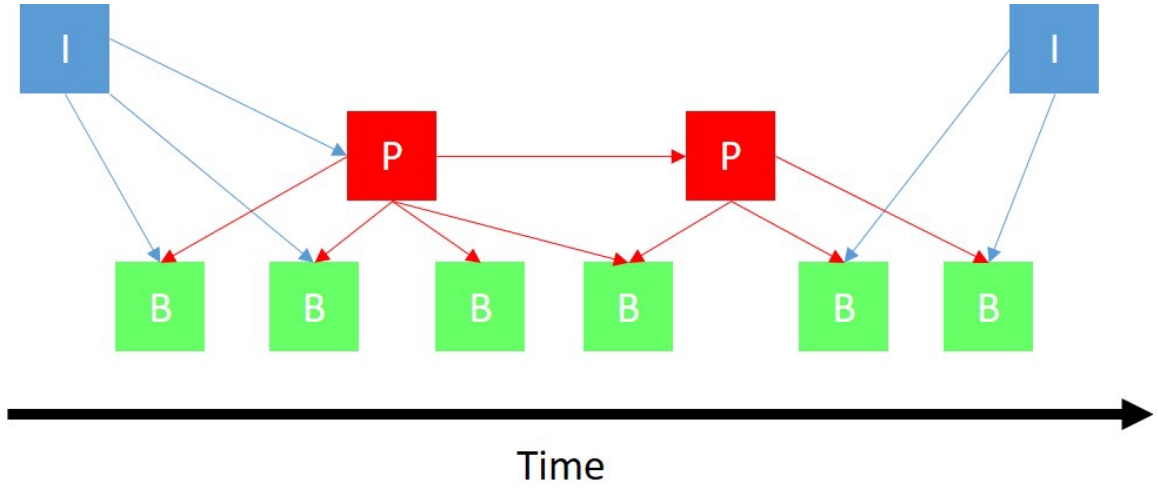


Compression Efficiency

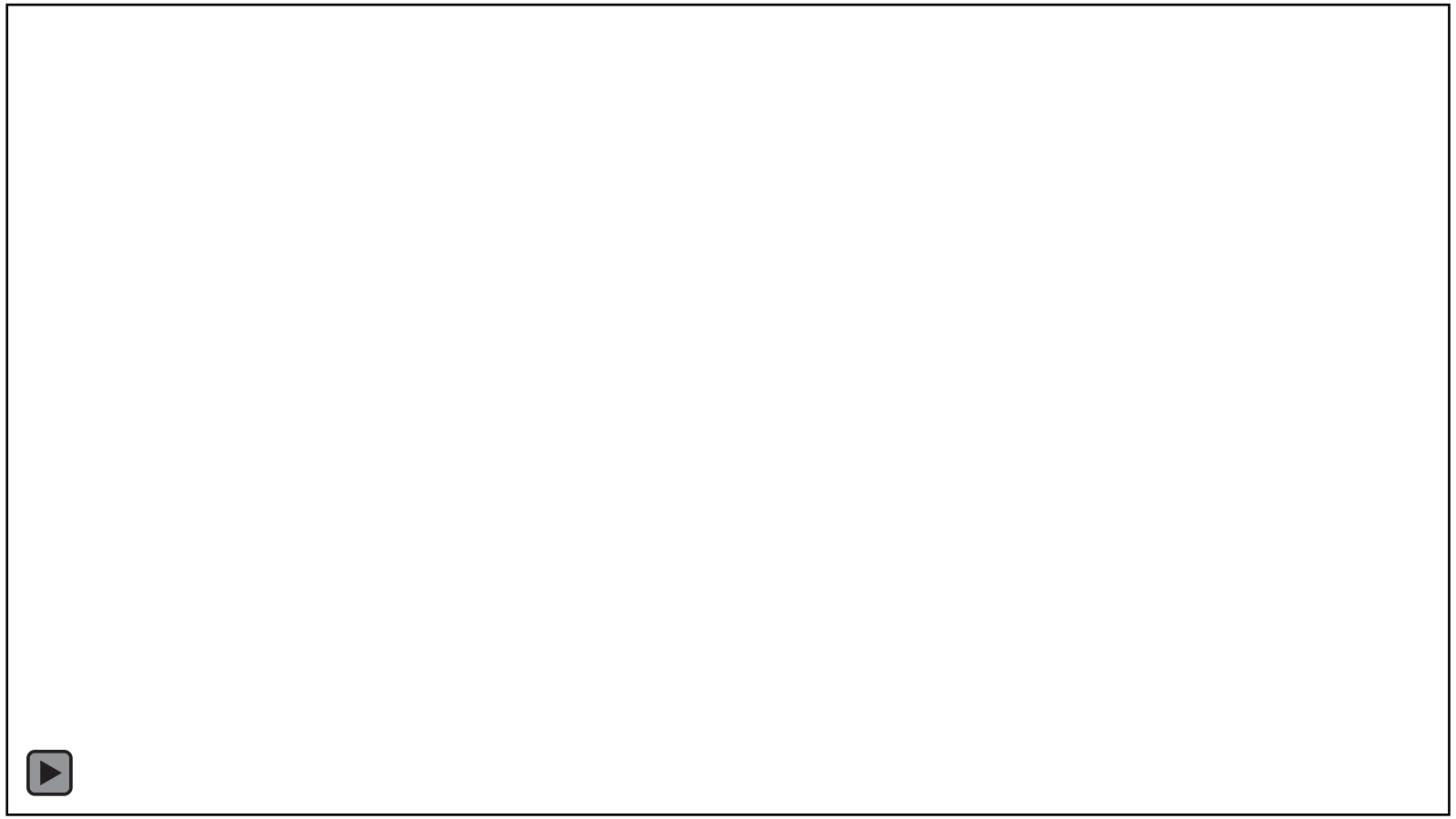


Motion Compensation Algorithm

Instead of sending an entire frame, a frame is described as a delta (changes) from another frame, and this information is sent.

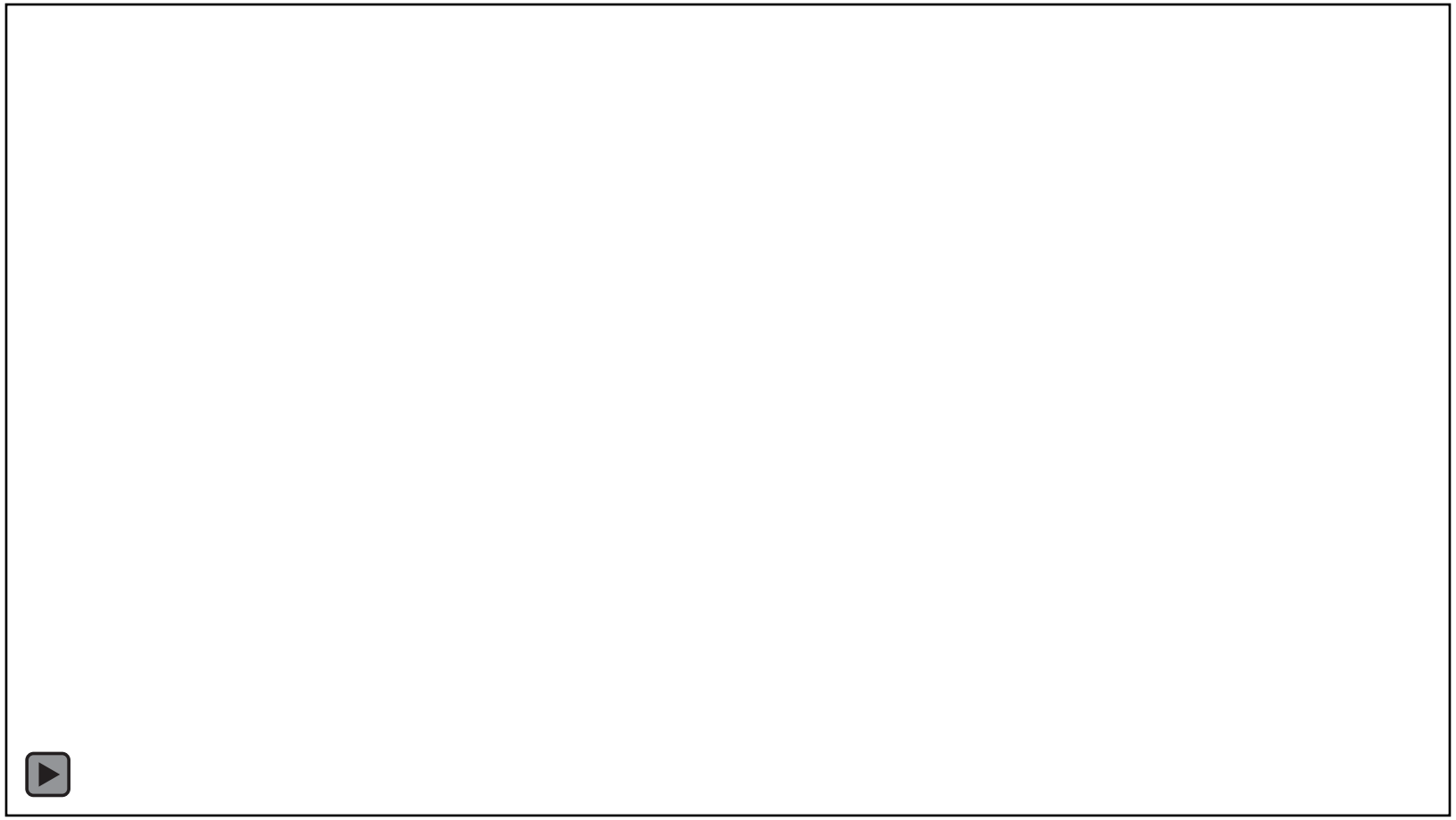


Data Leakage

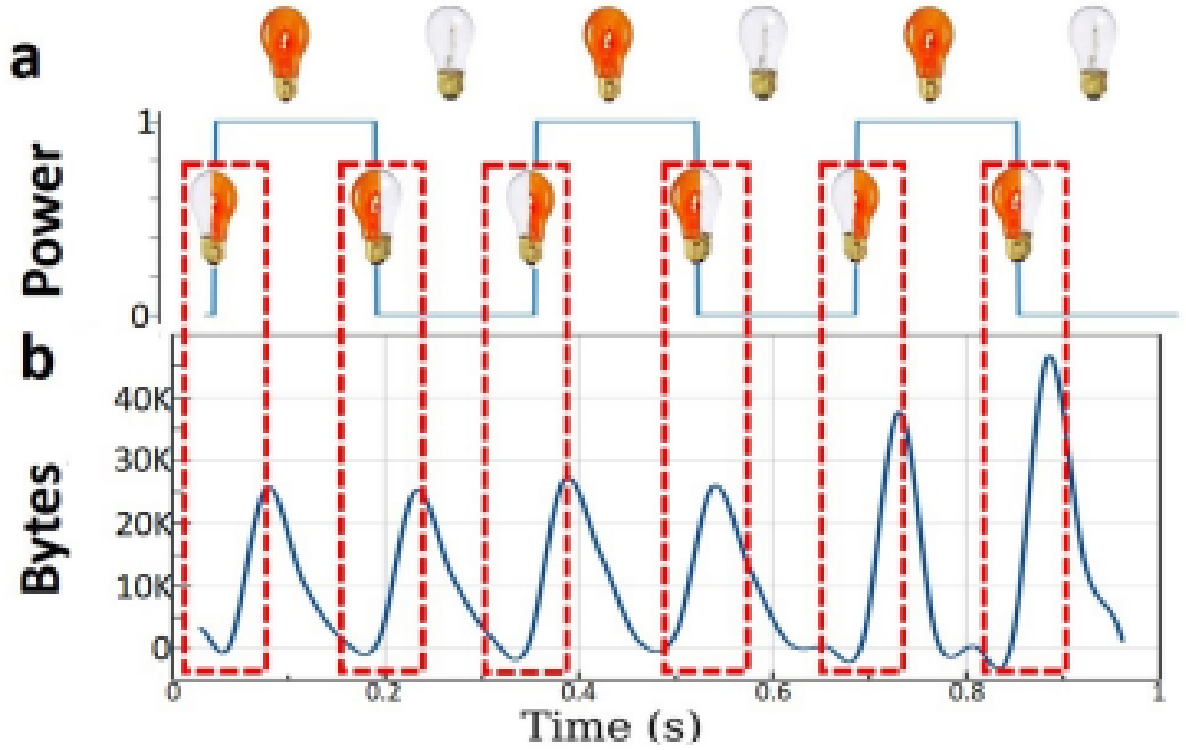


Time Domain Analysis Problems

Grain Moving

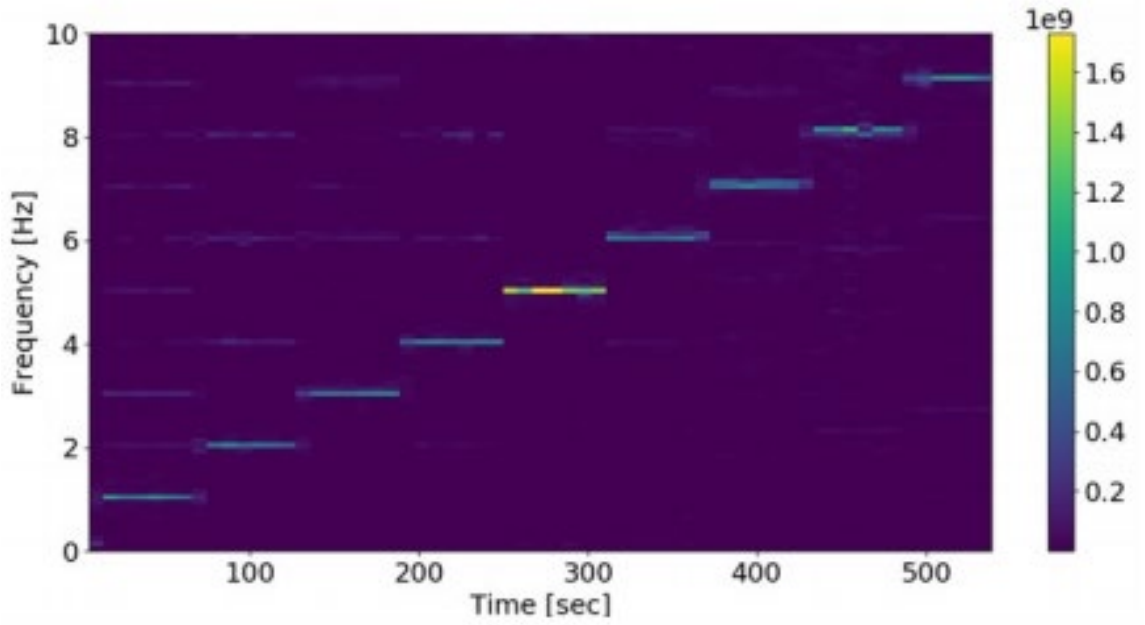


Influence of Periodic Physical Stimulus on the Frequency Domain



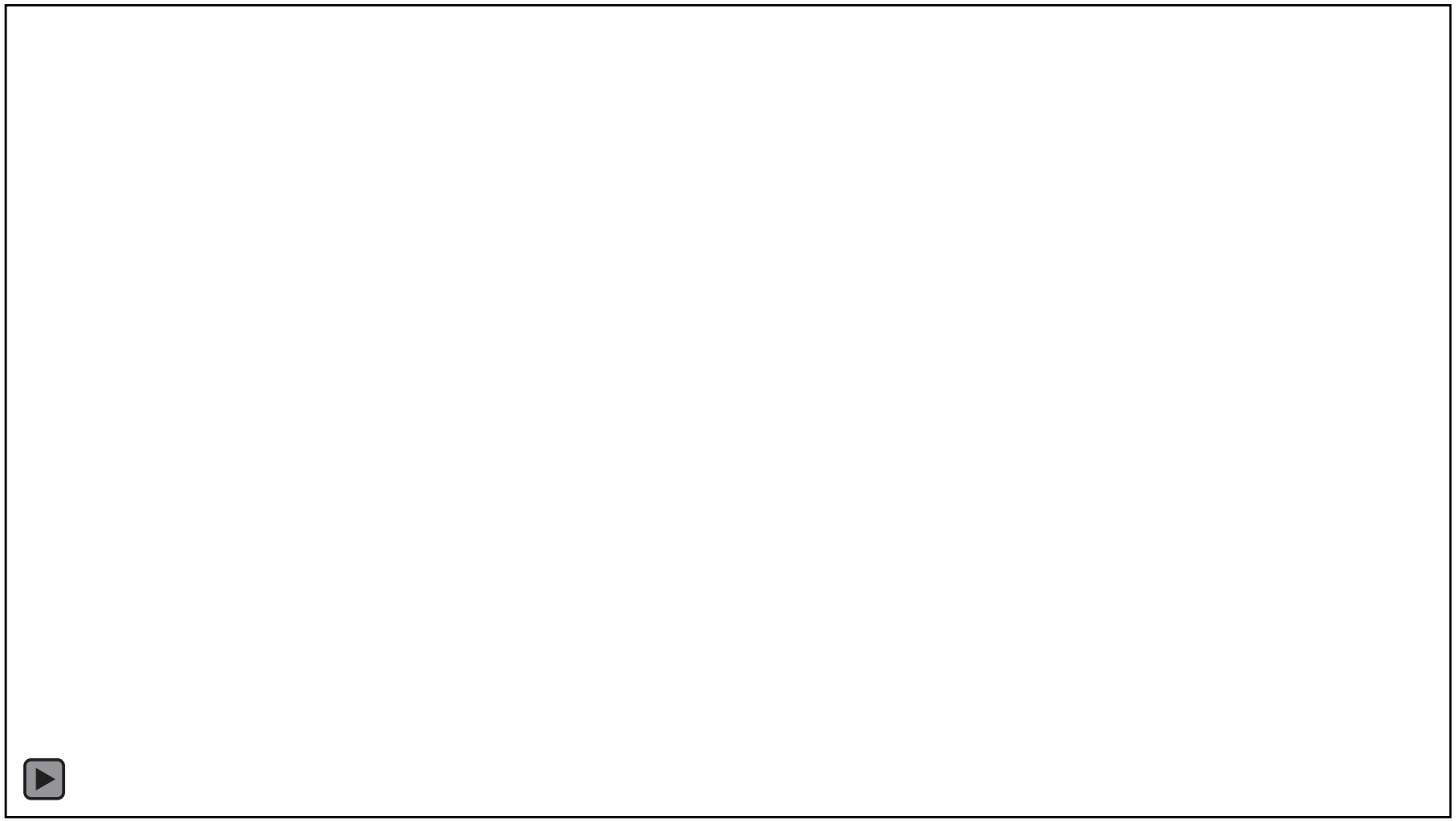
A 3 HZ FLICKERING LED CREATED 6 BURSTS IN THE INTERCEPTED BITRATE SIGNAL.

Watermarking a Target Frequency

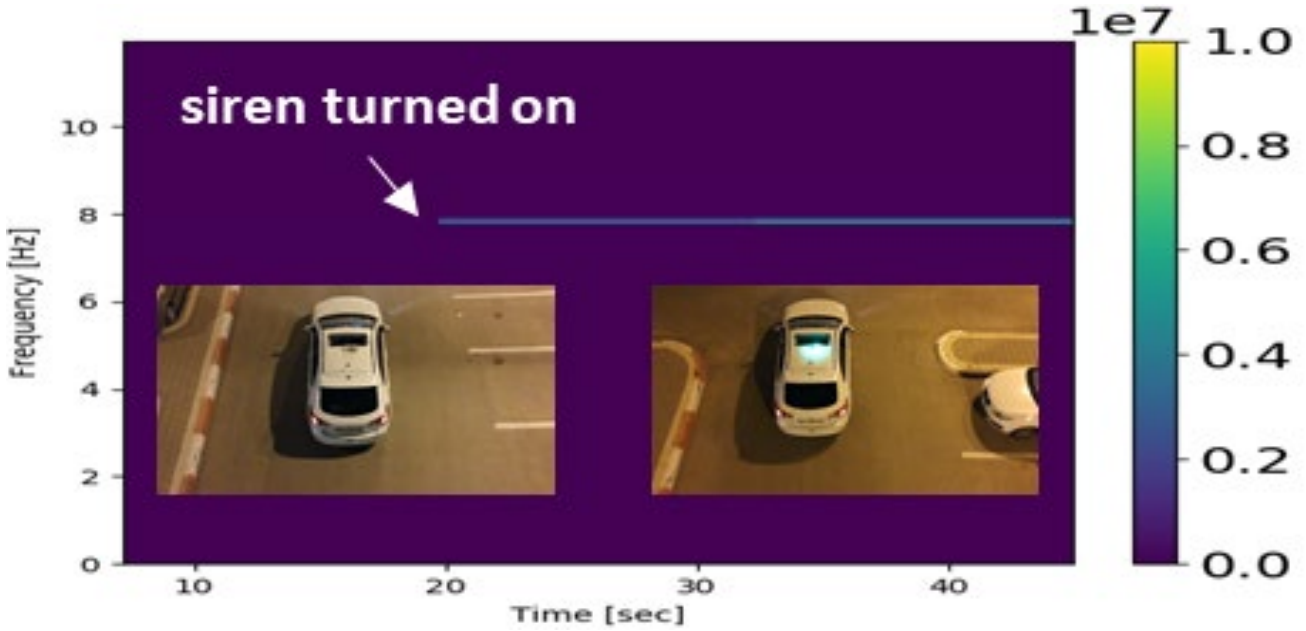


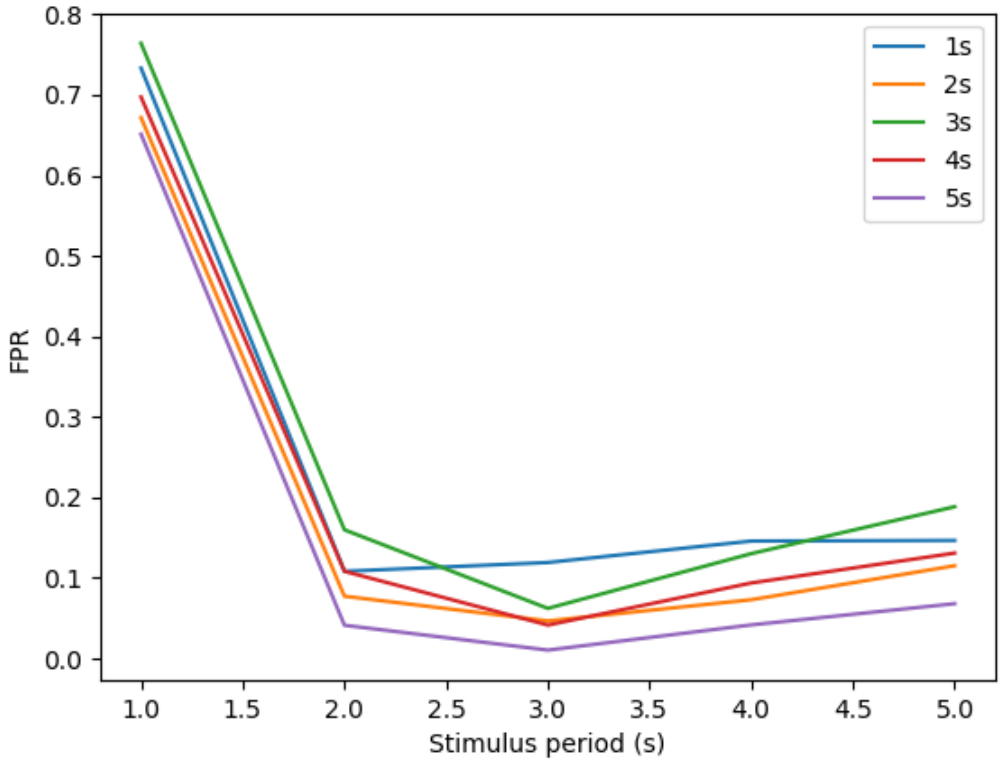
WE CAN WATERMARK EACH AND EVERY FREQUENCY OF THE INTERCEPTED BITRATE SIGNAL USING A FLICKERING LED

Demo

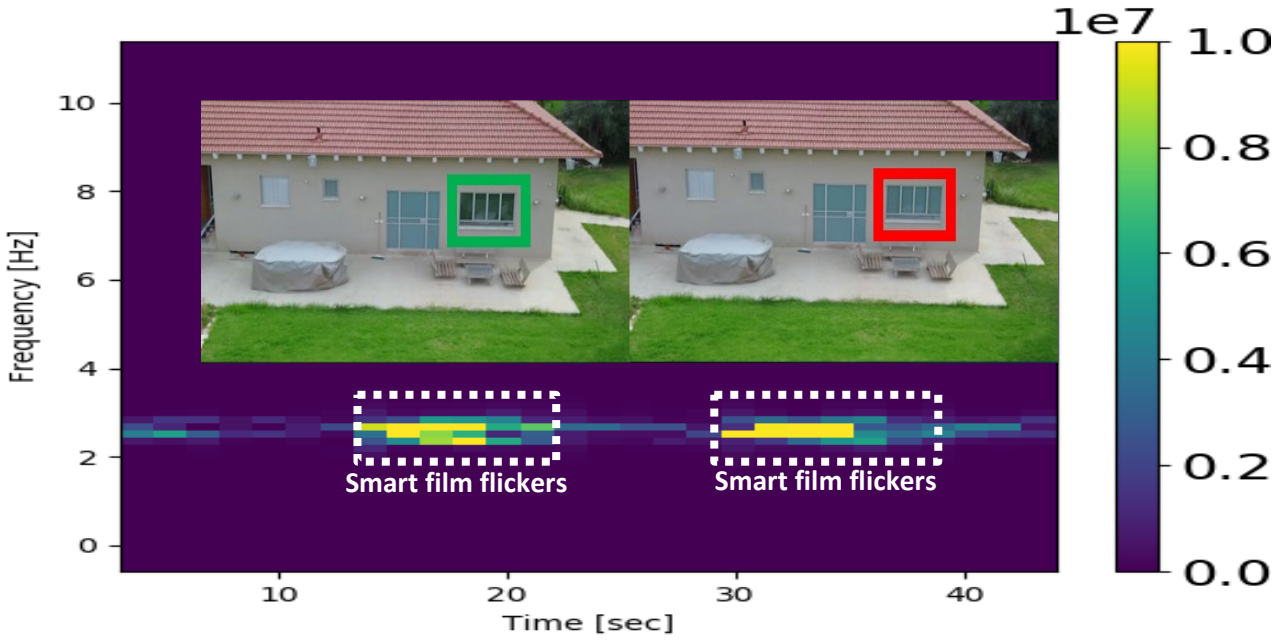


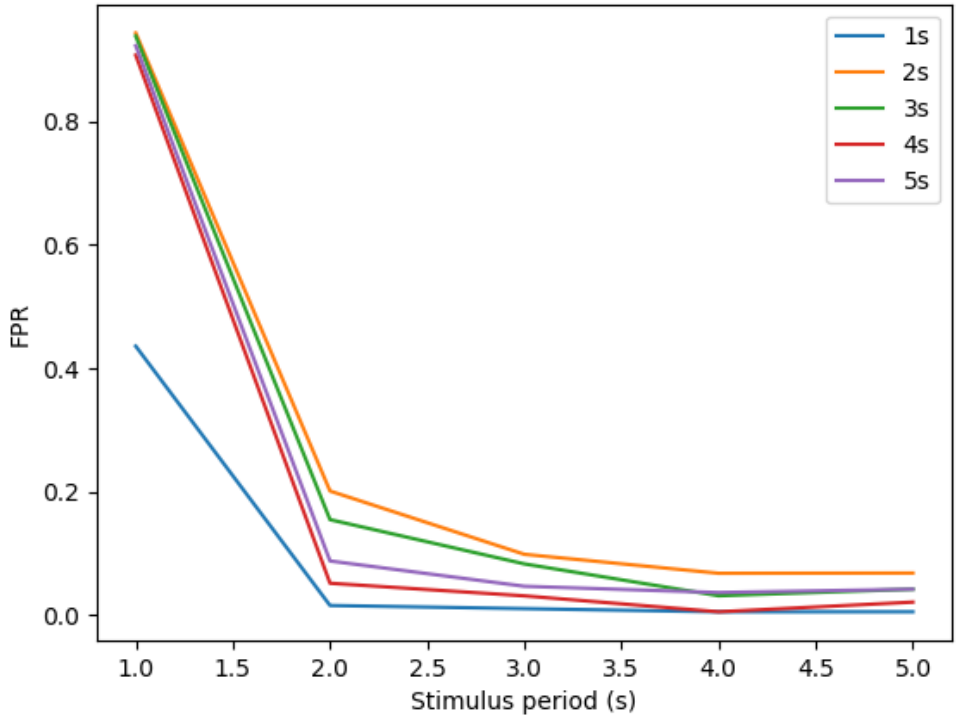
Results


siren turned on
1e7
1.0
0.8
0.6
0.4
0.2
0.0
Frequency [Hz]
Time [sec]


1s
2s
3s
4s
5s
FPR
Stimulus period (s)

Results

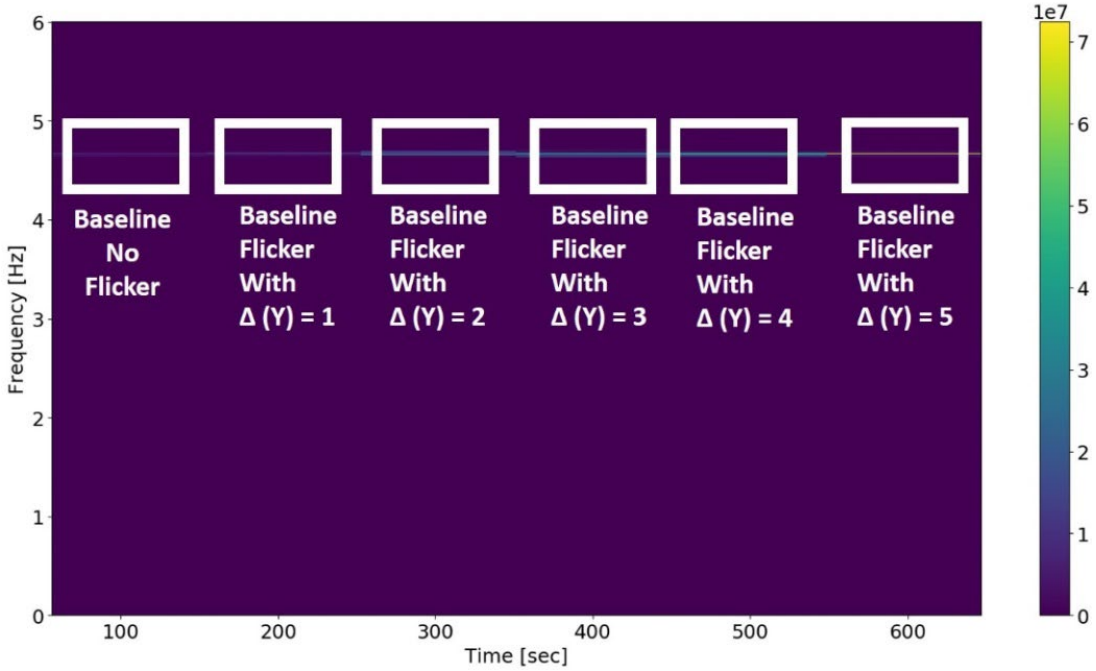

1e7
1.0
0.8
0.6
0.4
0.2
0.0
Frequency [Hz]
10
8
6
4
2
0
10
20
30
40
Time [sec]
Smart film flickers
Smart film flickers

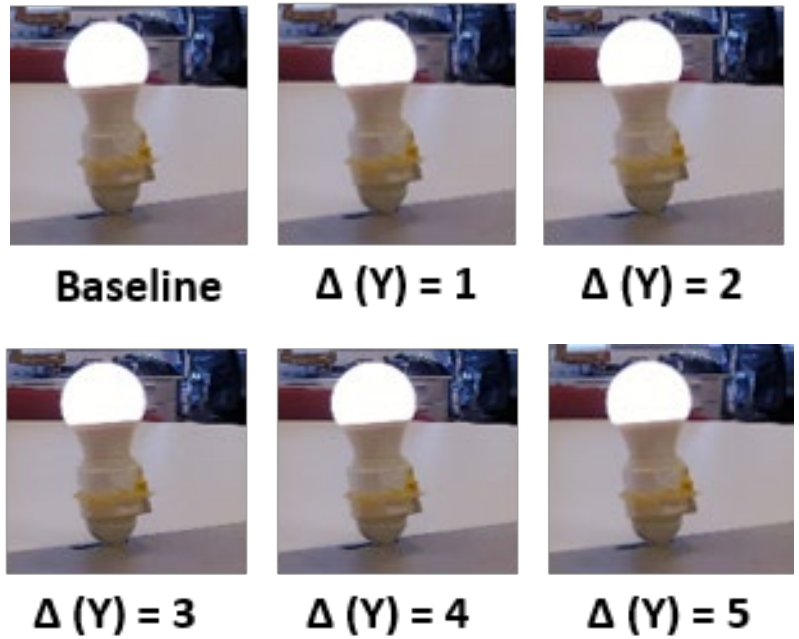

FPR
0.8
0.6
0.4
0.2
0.0
1.0
1.5
2.0
2.5
3.0
3.5
4.0
4.5
5.0
Stimulus period (s)
1s
2s
3s
4s
5s

Hiding the Physical Stimulus

- Undetectable by direct observation
- Undetectable via the controller
- Watermark

Similar Hues





Luma (Δ)	YUV	RGB
Baseline	**231**,26,143	253,255,51
1	**230**,26,143	252,254,50
2	**229**,26,143	251,253,49
3	**228**,26,143	250,252,48
4	**227**,26,143	249,251,47
5	**226**,26,143	248,250,46

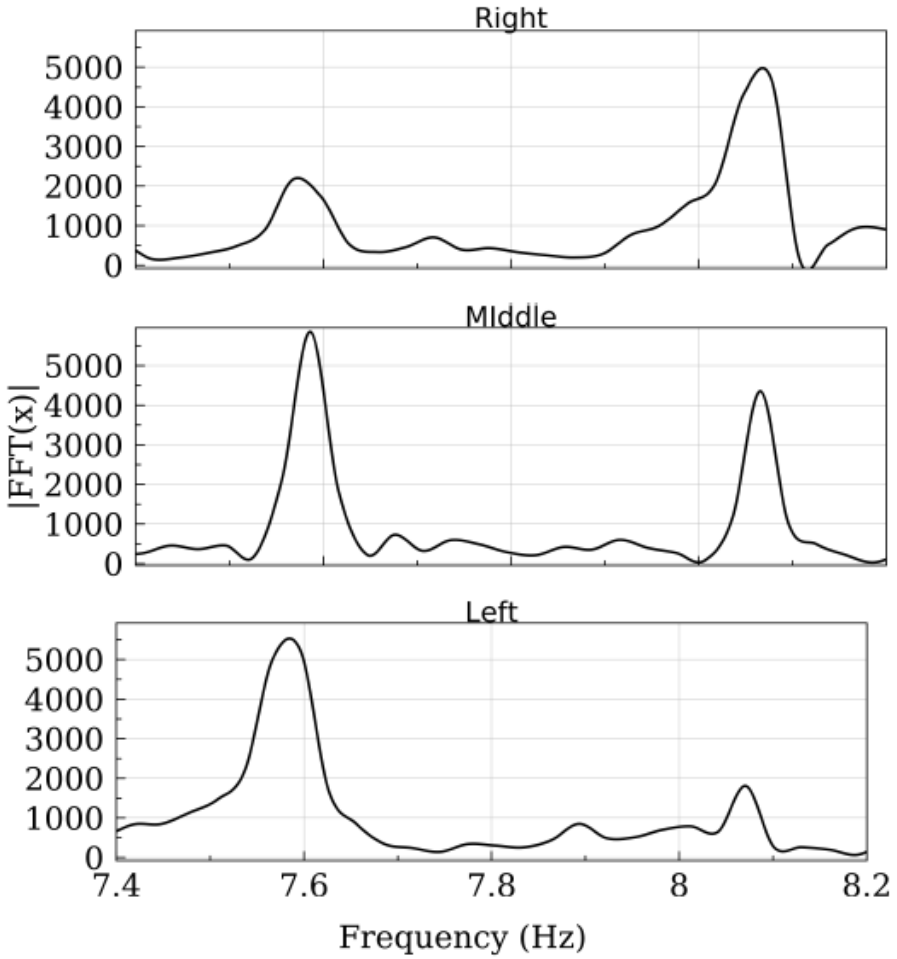
Objectives


BONUS OBJECTIVE!!!
Classifying a suspicious radio transmission as an FPV channel
Detecting whether an FPV channel is being used to spy on a victim
Locating a spying drone in space

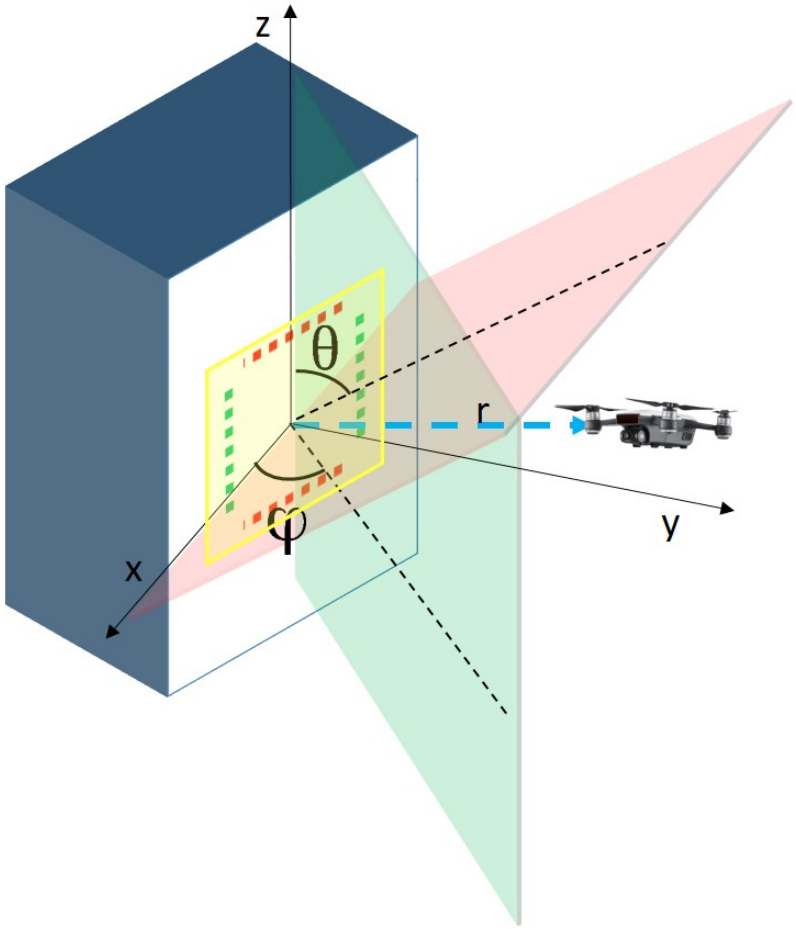
Objective #3

Locating a spying drone in space

The Great Finding



Locating Drones in Space



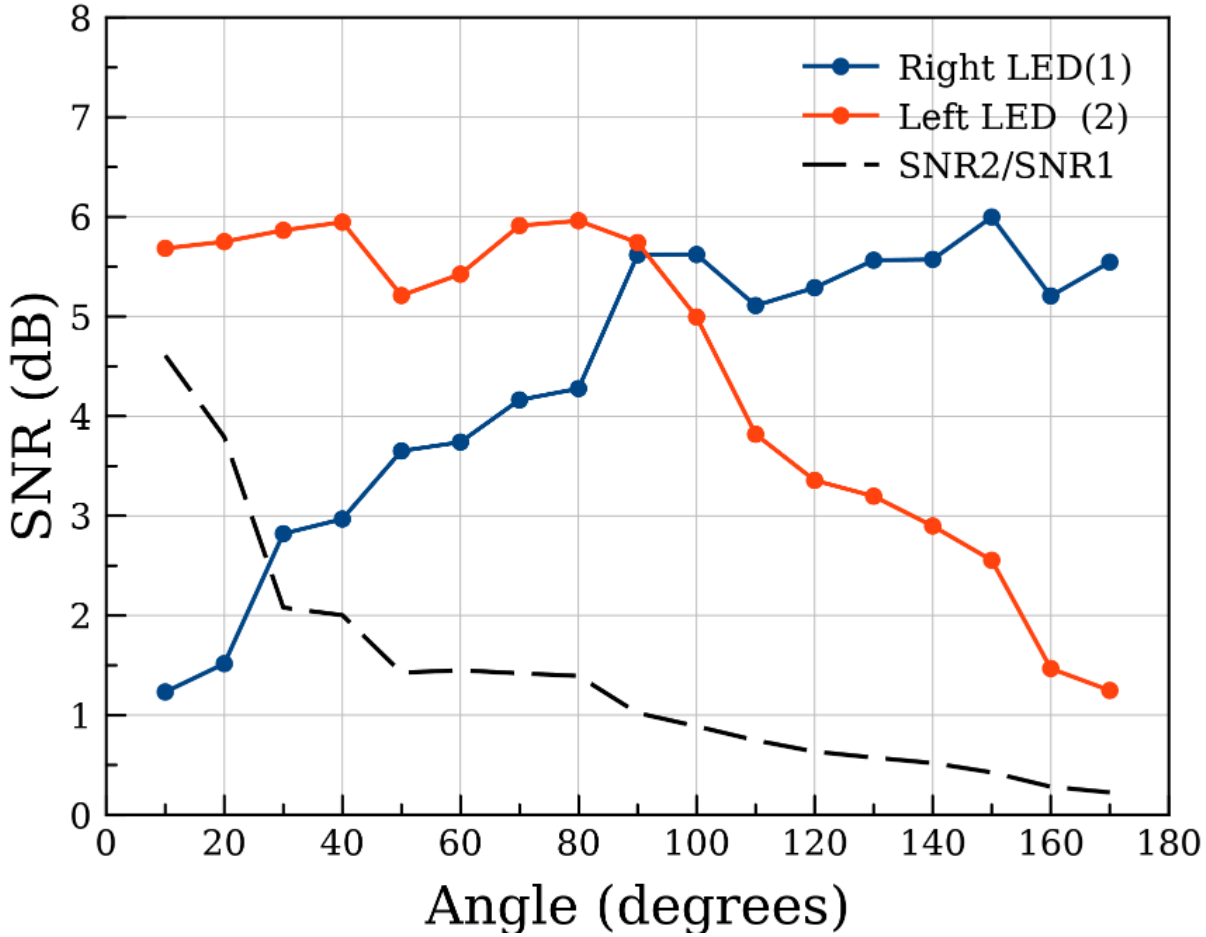
1. Calculating spherical coordinates (θ, φ,r):
   - **θ** and **φ** - using the formula to detect angle.
   - **r** - using the formula to detect distance.
2. Calculating spying drone's location (longitude, latitude, altitude) from the equations of spherical coordinates (θ, φ,r):

$$x = \boldsymbol{r} \sin(\boldsymbol{\theta}) \cos(\boldsymbol{\varphi})$$

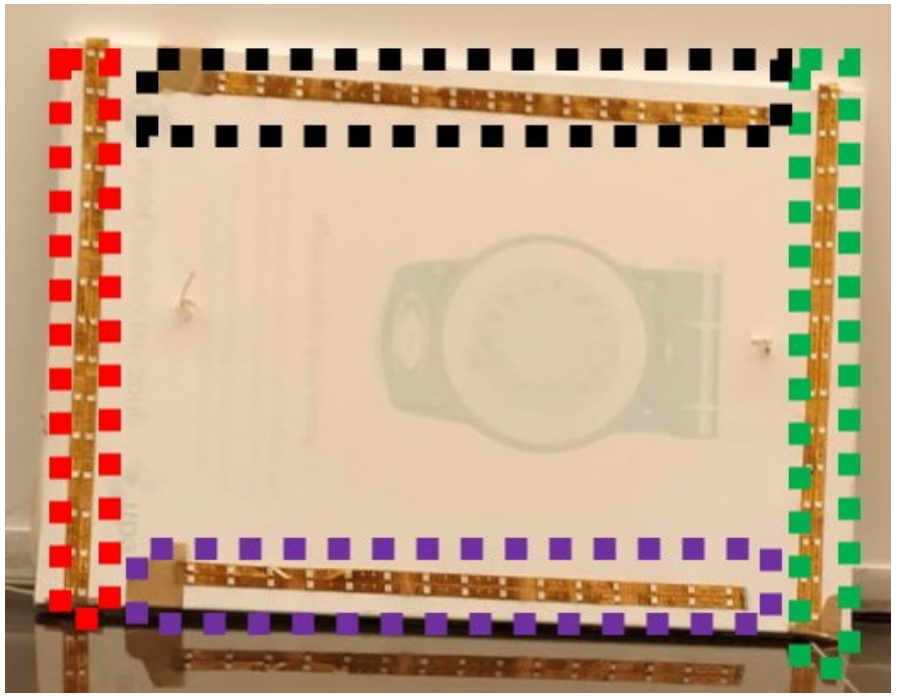
$$y = \boldsymbol{r} \sin(\boldsymbol{\theta}) \sin(\boldsymbol{\varphi})$$

$$z = \boldsymbol{r} \cos(\boldsymbol{\theta})$$

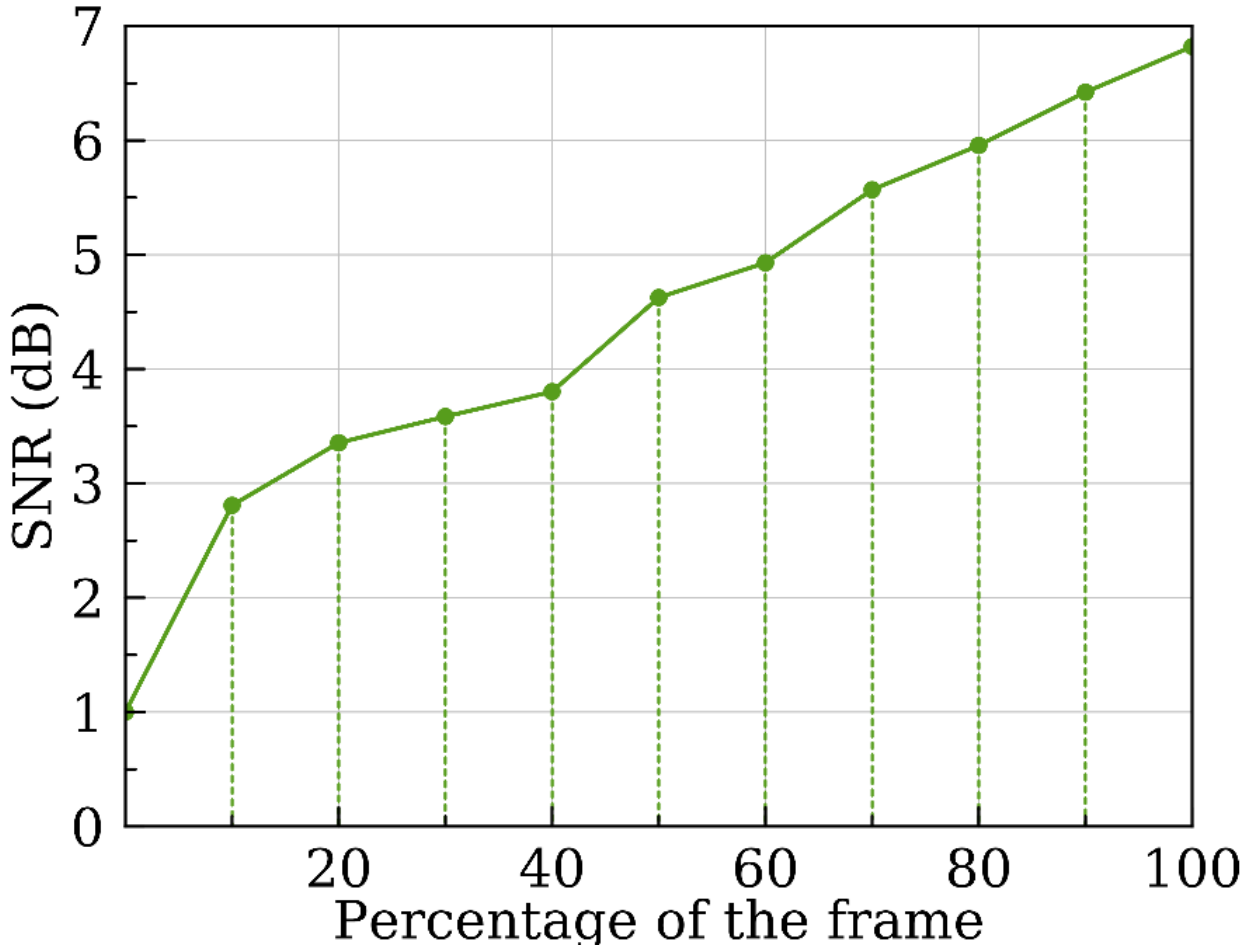
Detecting the Angle Between the Drone and the Target



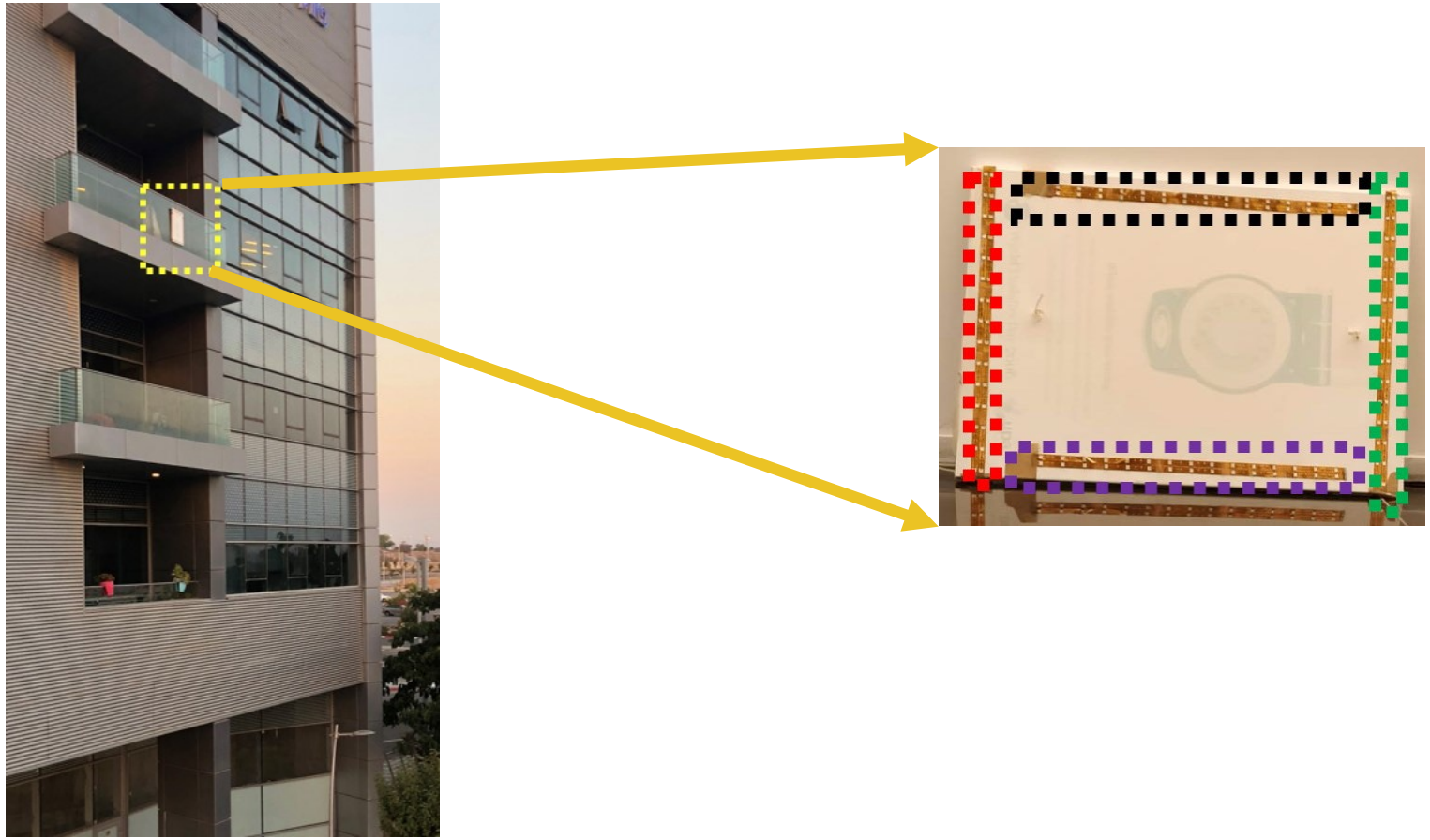
Detecting the Angle Between the Drone and the Target



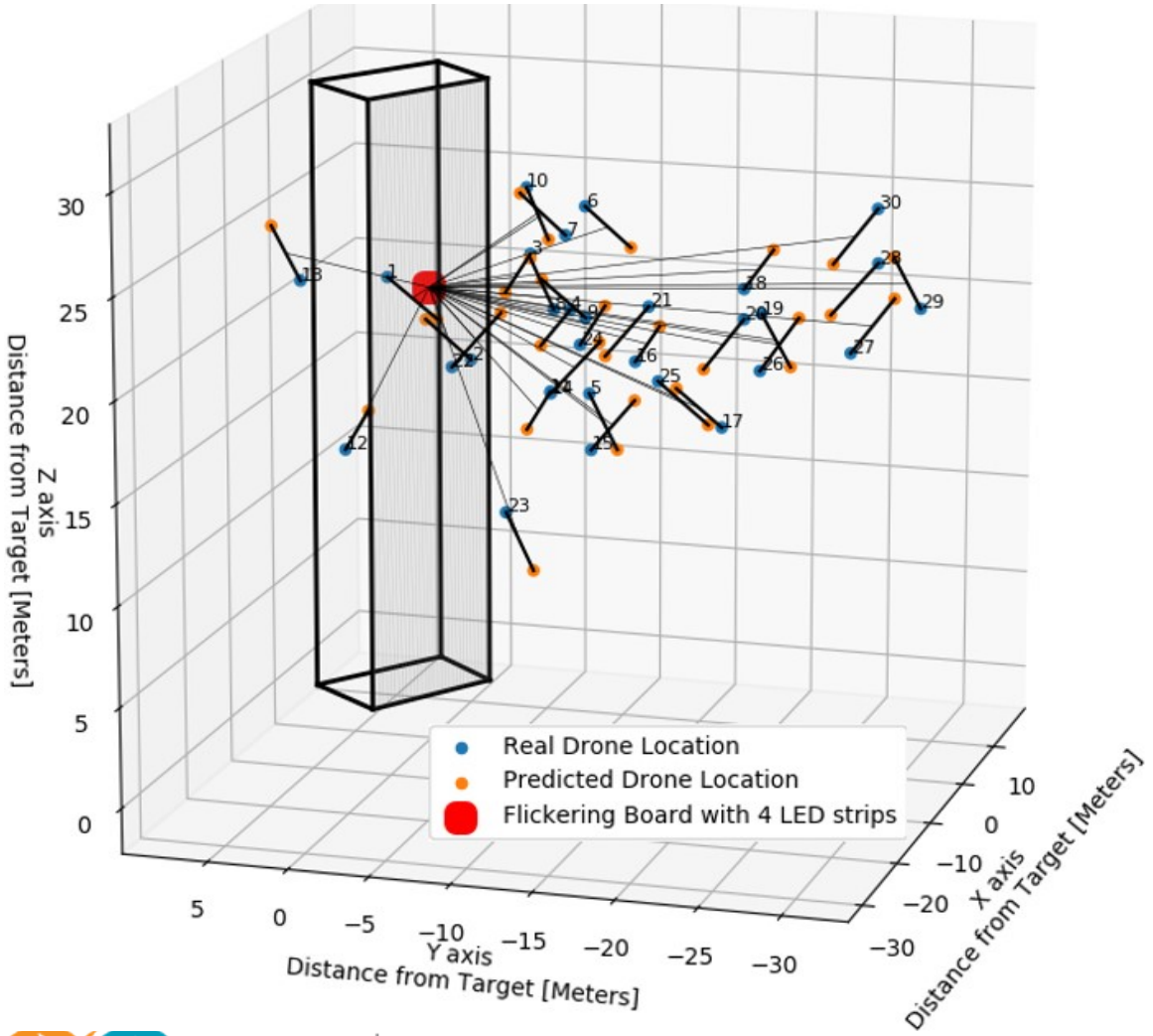
Detecting the Distance Between the Drone and the Target

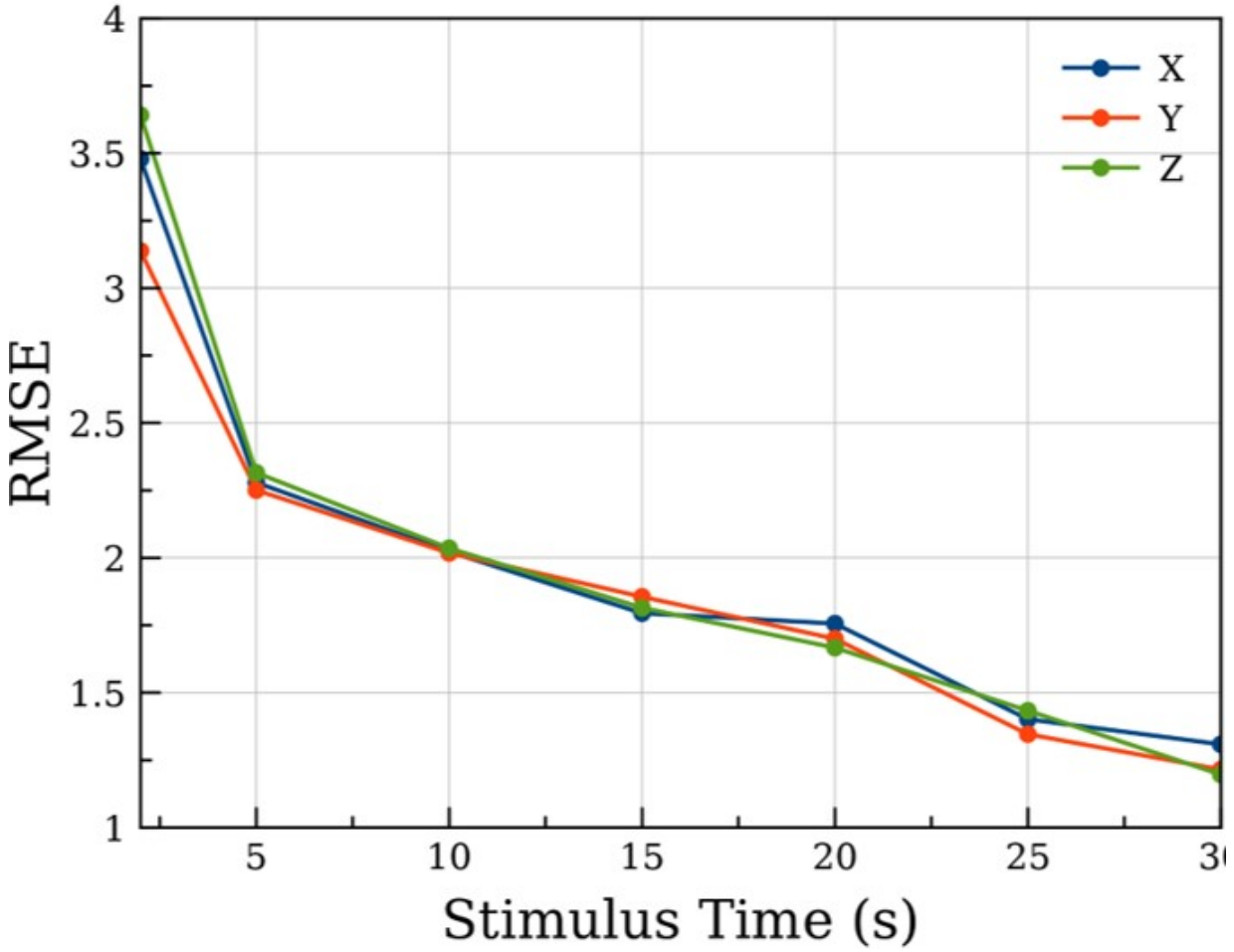


Locating Drones in Space



Results


Real Drone Location
Predicted Drone Location
Flickering Board with 4 LED strips
Z axis
Distance from Target [Meters]
Y axis
Distance from Target [Meters]
X axis
Distance from Target [Meters]


RMSE
Stimulus Time (s)
X
Y
Z

Objectives

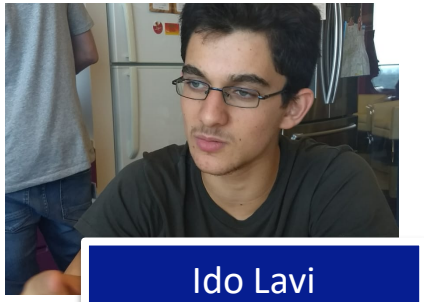
Classifying a suspicious radio transmission as an FPV channel

Detecting whether an FPV channel is being used to spy on a victim

Locating a spying drone in space

Special Thanks

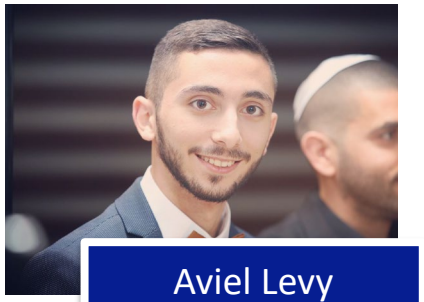
Yehuda Hido Cohen



Ido Lavi

Roei Cohen

Yaron Pirutin



Aviel Levy

Idan Sokolovsky

Moshe Sror

Dudi Nassi

RSAConference2019
Asia Pacific & Japan

Questions


Raz Ben Netanel


@r__.bn


Raz Ben Netanel


razx@gmail.com