EM Eye: Characterizing Electromagnetic Side-channel Eavesdropping on Embedded Cameras

Yan Long[1], (yanlong@umich.edu),
Qinhong Jiang[2], Chen Yan[2], Tobias Alam[1],
Xiaoyu Ji[2], Wenyuan Xu[2], Kevin Fu[3]

[1] University of Michigan, EECS

[2] Zhejiang University, EE

[3] Northeastern University, ECE & CS

Northeastern University

Cameras Getting Pervasive

[Photo: Car and Driver, NY TImes, Simpled, Apple]

Camera Data Confidentiality

Software Vulnerabilities

Default Password & Unencrypted Comms [Abdalla et al., 2020]

Brute-force Attacks against 4-digit Passwords [Ling et al., 2017]

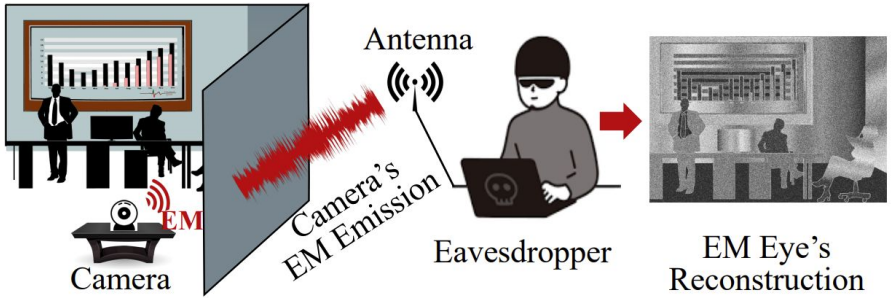
Known Serial Number Camera Hijacking [Herodotou et al., 2023]

Network Traffic Sniffing and Reconstruction [Tekeoglu et al., 2015]

Hardware Vulnerabilities

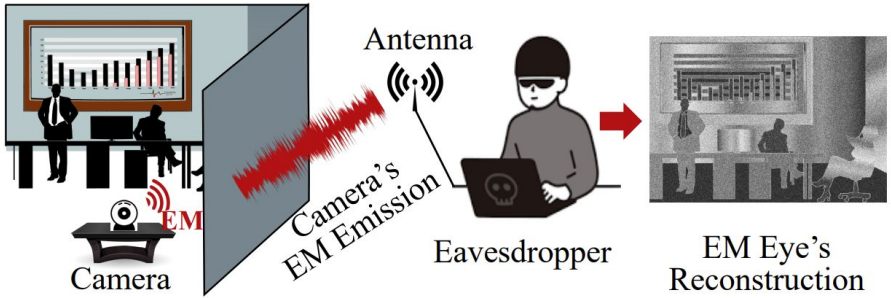
?

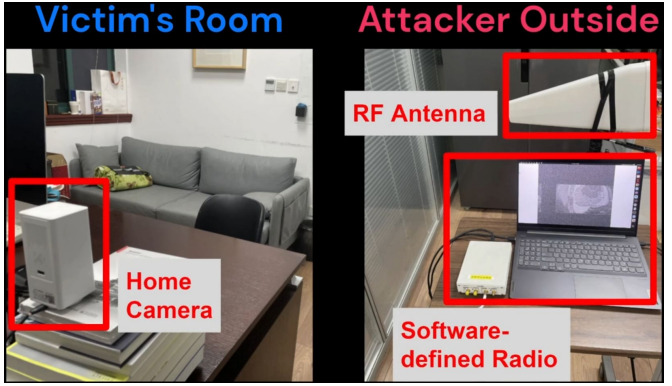
Threat Model: EM Eavesdropping on Cameras



- No software/network entry point
- External physical eavesdropper
- **Unintentional electromagnetic leakage (not wireless comm signals)**

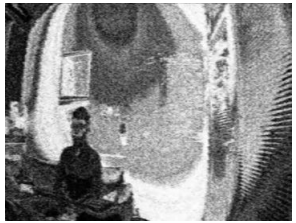
Threat Model: EM Eavesdropping on Cameras





Demo, tutorial, simulation:
https://emeyeattack.github.io/Website/

Image-specific Electromagnetic Leakage



$$I_{EM} = \mathcal{R}\{S_{EM}\}$$

$$S_{EM} = f_{CamLeak}(I_{GT})$$

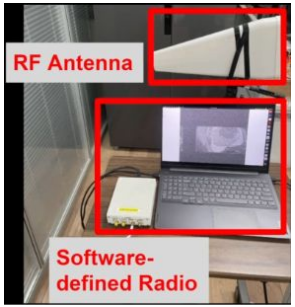
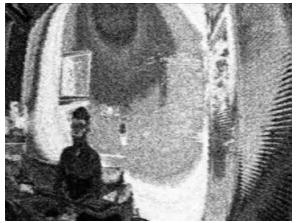


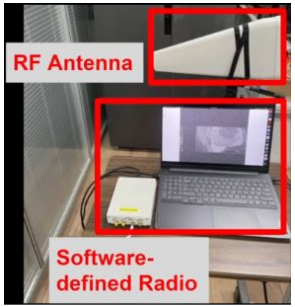
Image-specific Electromagnetic Leakage



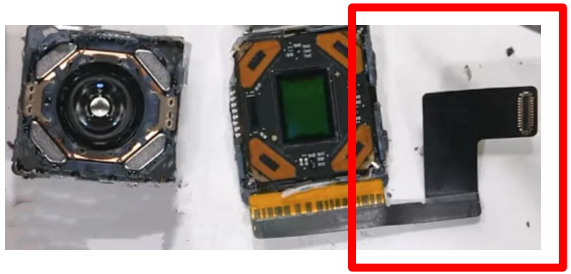
$$I_{EM} = \mathcal{R}\{S_{EM}\}$$

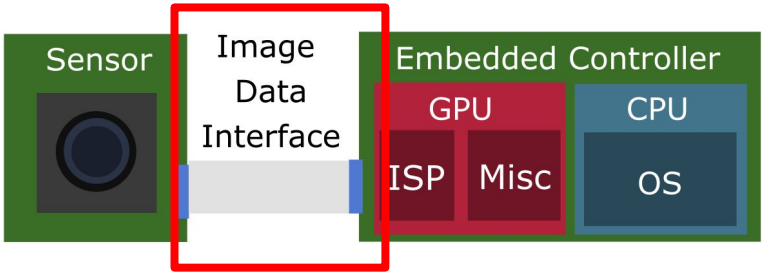
$$S_{EM} = f_{CamLeak}(I_{GT})$$

?



Interface: Standardization





Rambus Products Soluti

Home > Blogs > Automotive > Accelerating MIPI CSI-2 Adoption in Automotive

Back to Blog

Accelerating MIPI CSI-2 Adoption in Automotive

August 15, 2023 by Rambus Press — Leave a Comment

By Joe Rodriguez | Product Marketing Manager, Interface IP

LOW POWER-HIGH PERFORMANCE

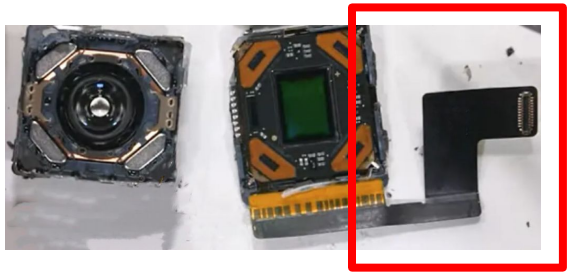
MIPI Standards Gaining Traction In New Markets

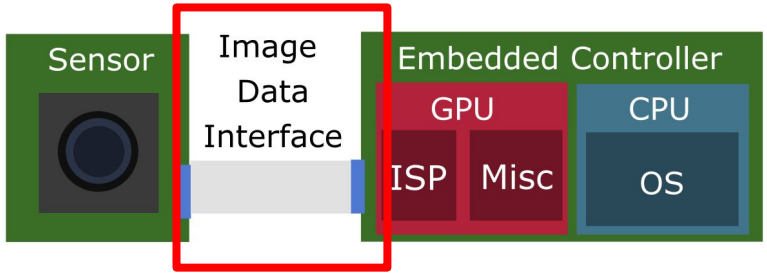
118 Shares | 47 | 14 | in 54

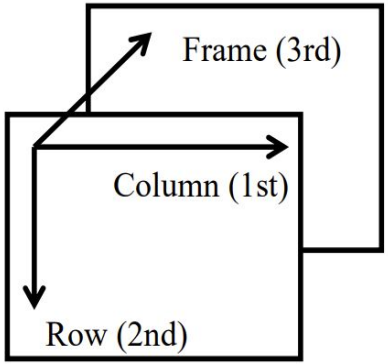
Convergence of vision and AI is driving adoption of MIPI standards beyond just mobile phones.

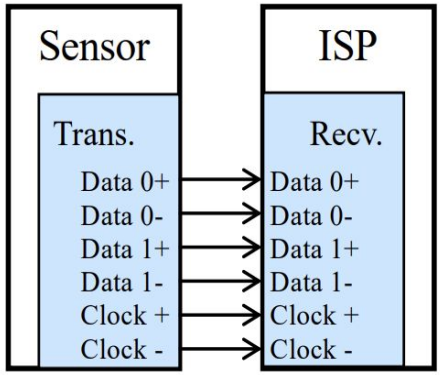
JANUARY 26TH, 2022 - BY: **ANN MUTSCHLER**

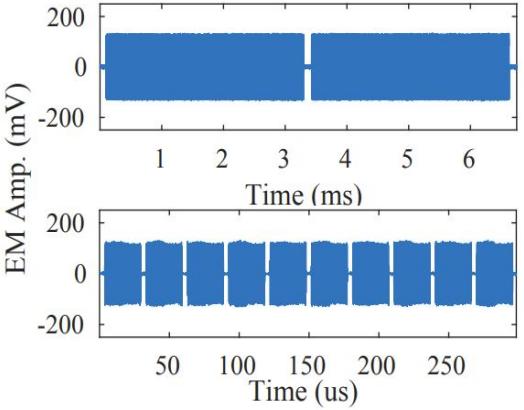
Interface: Serialized, Predictable Data Structure







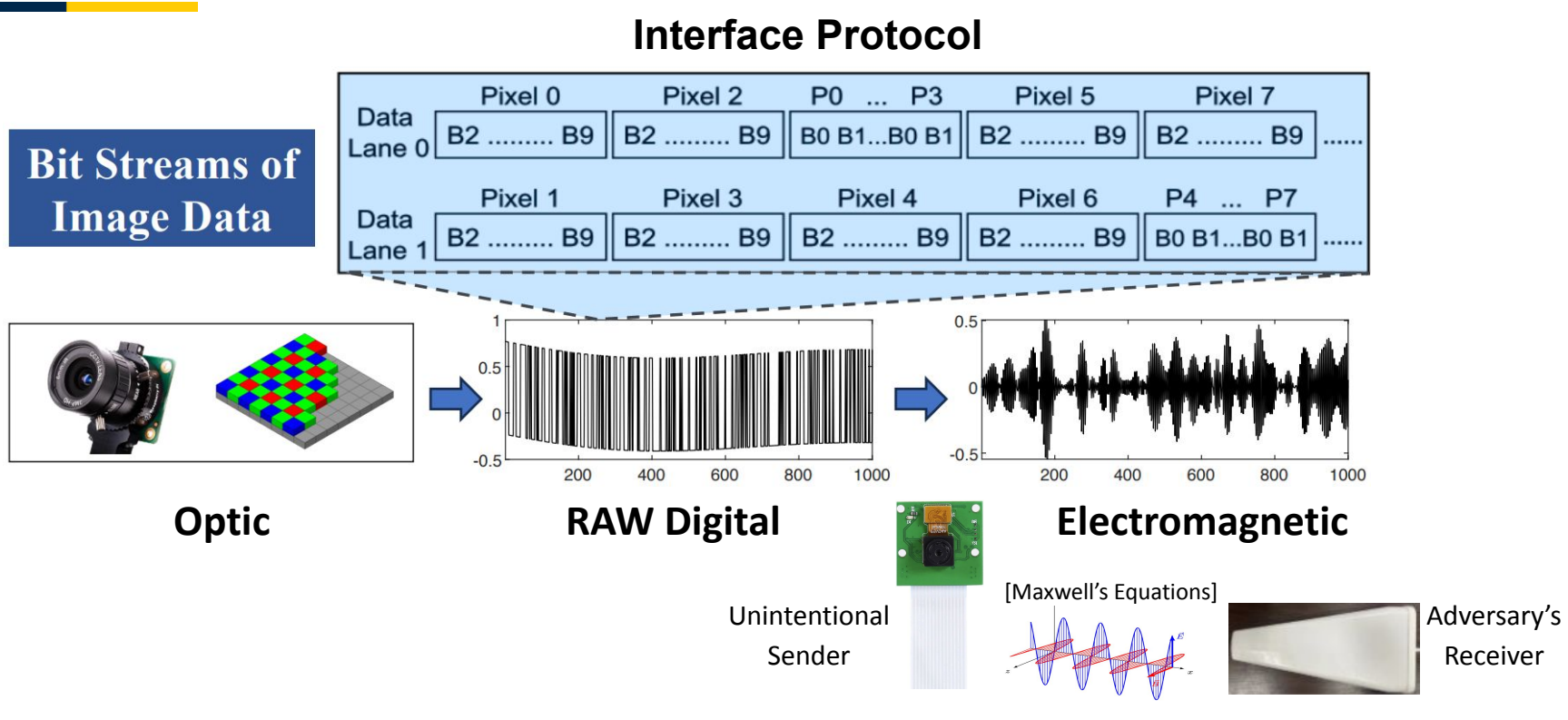




2 frames
(c)

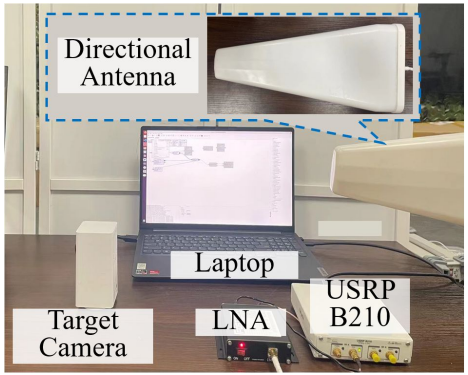
10 rows
(d)

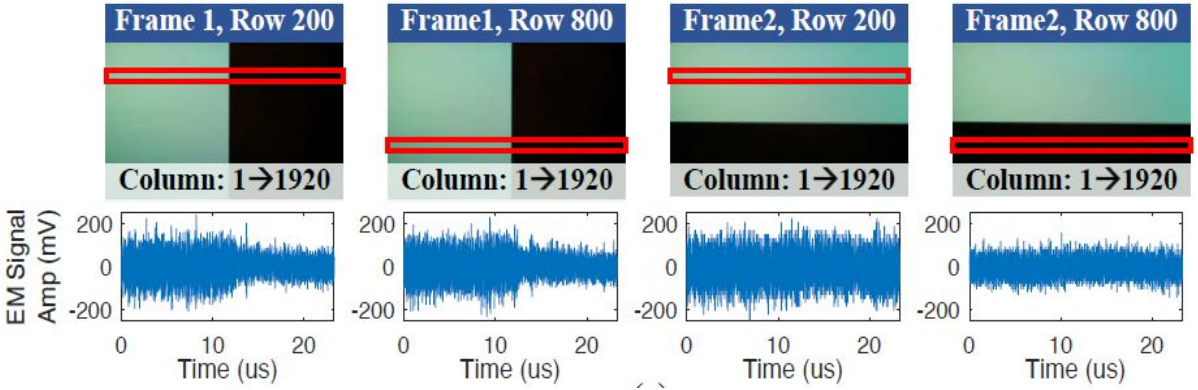
Unprotected Data & EM Emanation



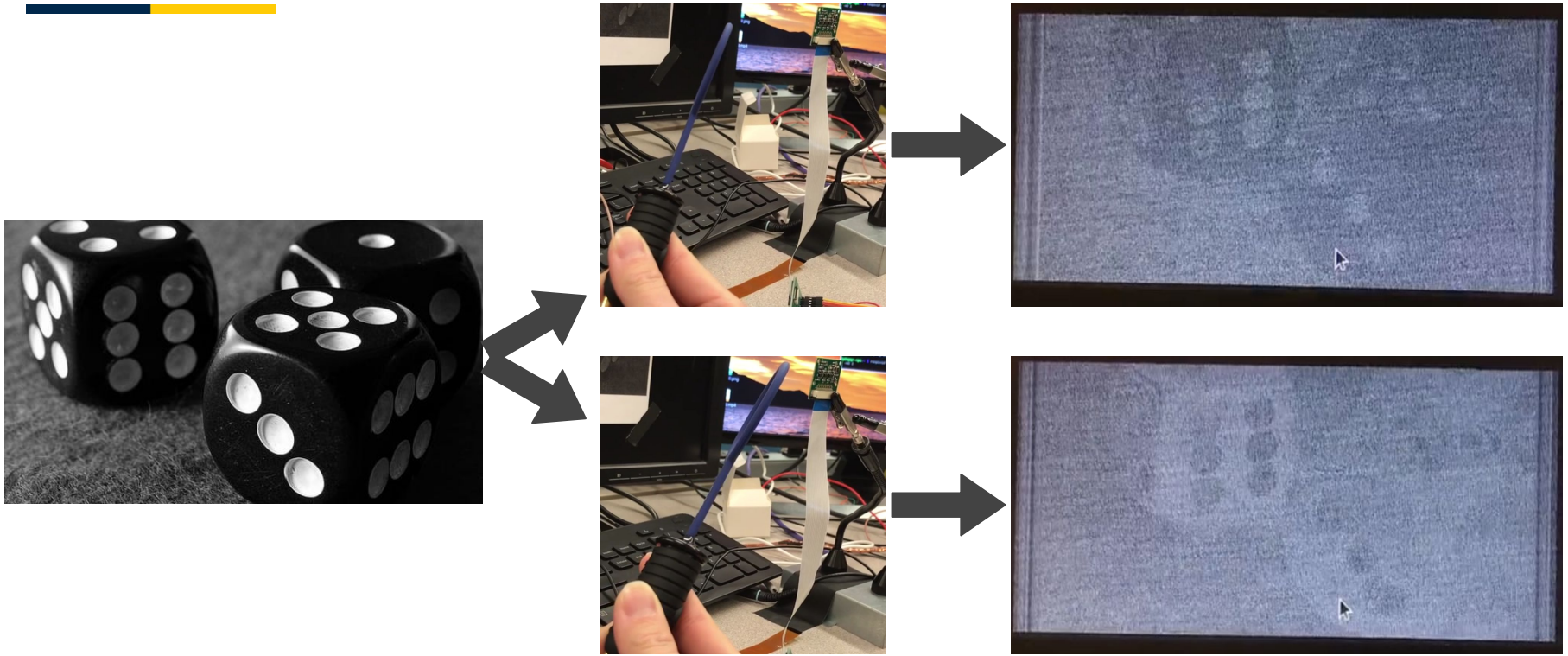
Yan Long | yanlong@umich.edu

EM-image Correlations

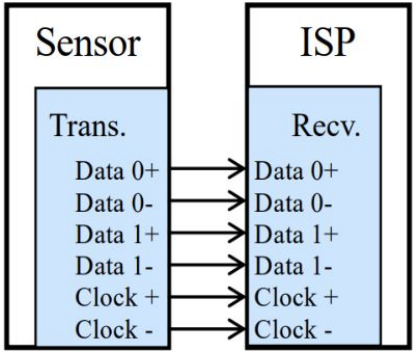


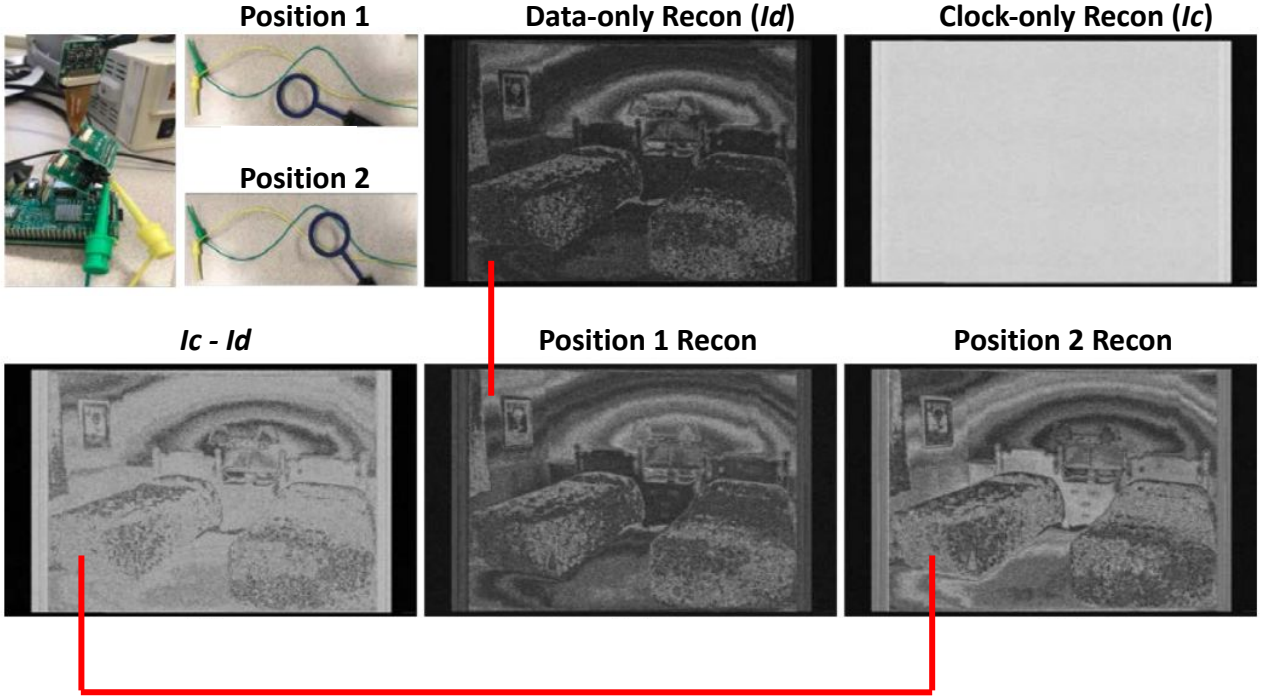


Leakage Modeling: Multi-wire Signal Polarity Inversion

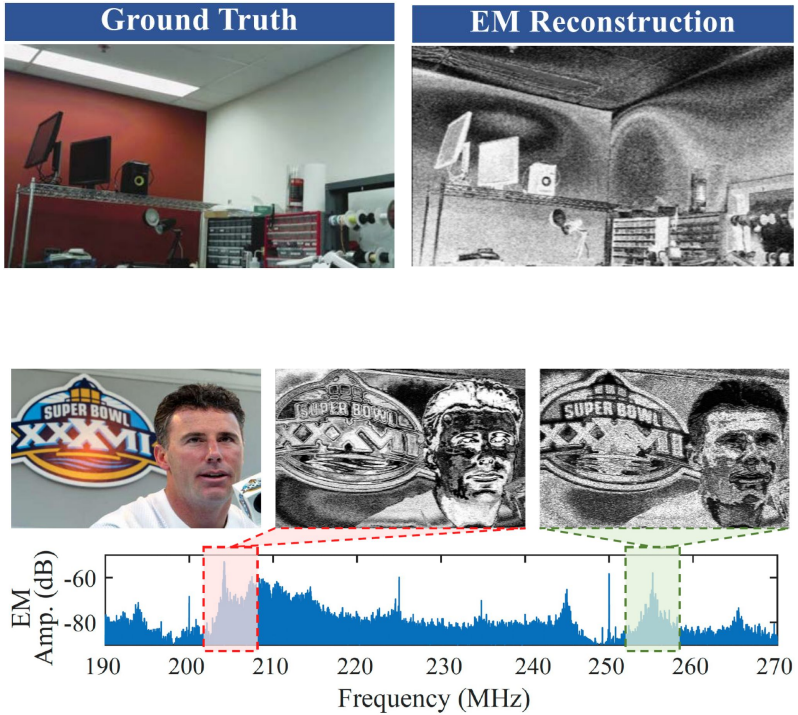


Leakage Modeling: Multi-wire Signal Polarity Inversion





Leakage Modeling: Practical Sampling Distortion



Practical Sampling: ~10 MHz bandwidth (no info of individual bits)

- Loss of color
- Shuffled gray-scale mapping
- Light gradient & high-frequency noise
- Frequency dependency

Reconstructions

$$I_{EM} = \mathcal{R}\left\{S_{EM}\right\}$$

$$S_{EM} = f_{CamLeak}(I_{GT})$$

EM Recon in *[l, h]*

Response in Freq Band *[l, h]*

Noise

Interface Protocol

$$I_{EM}^{[l,h]} = \mathcal{R}\left\{ z + b_{clk} + \mathcal{F}_{filt}\left[l, h, \mathcal{F}_{data}(I_{GT})\right] \right\}$$

Clock Interference

Reconstructions

$$I_{EM} = \mathcal{R}\{S_{EM}\}$$
$$S_{EM} = f_{CamLeak}(I_{GT})$$

EM Recon in *[l, h]*

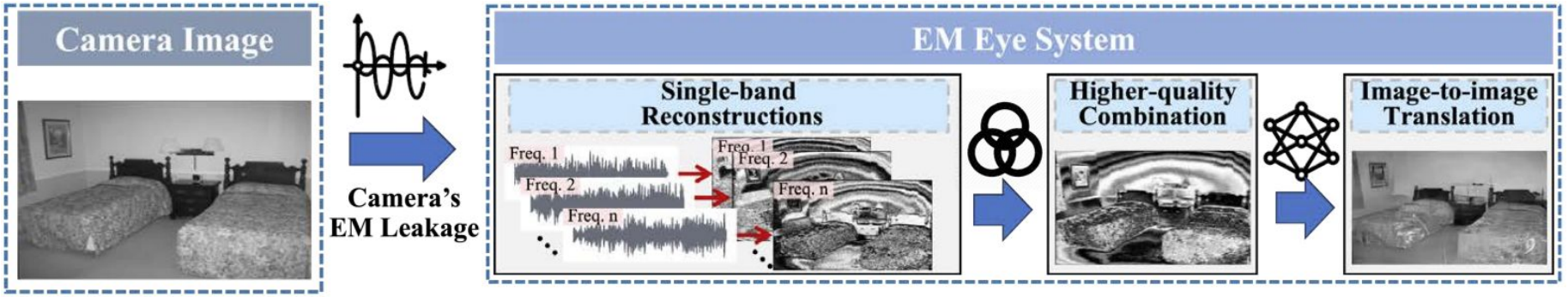
Response in Freq Band *[l, h]*

Noise

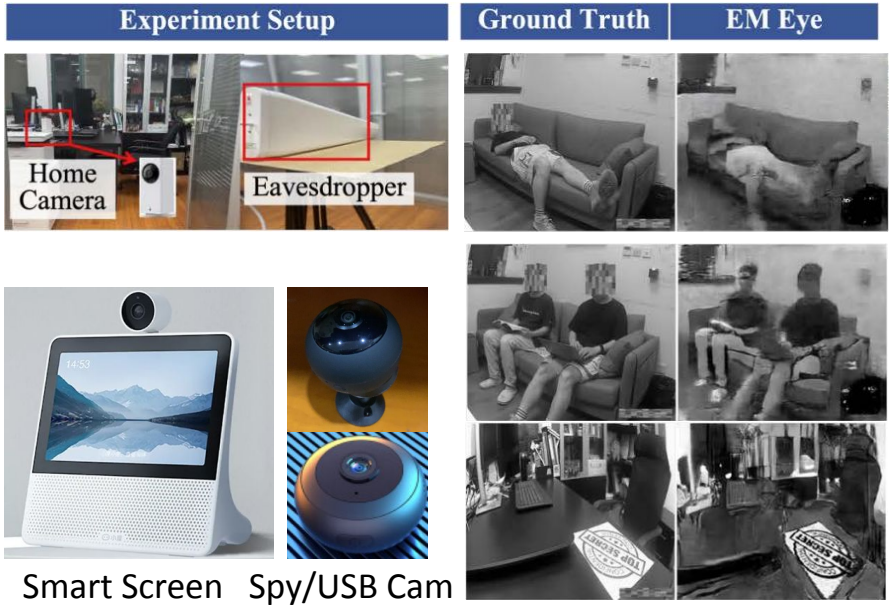
Interface Protocol

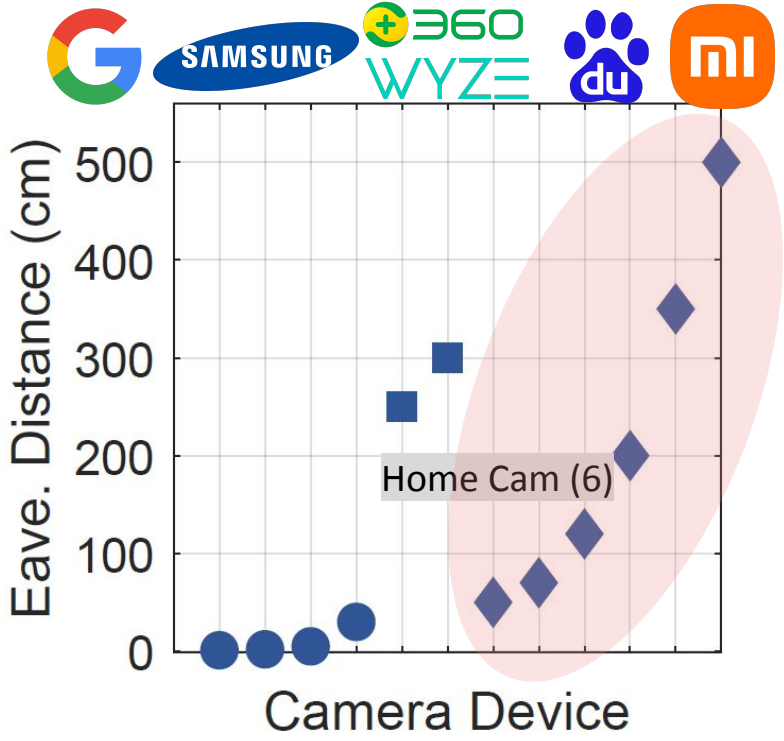
$$I_{EM}^{[l,h]} = \mathcal{R}\left\{ z + b_{clk} + \mathcal{F}_{filt}\left[l, h, \mathcal{F}_{data}(I_{GT}) \right] \right\}$$

Clock Interference

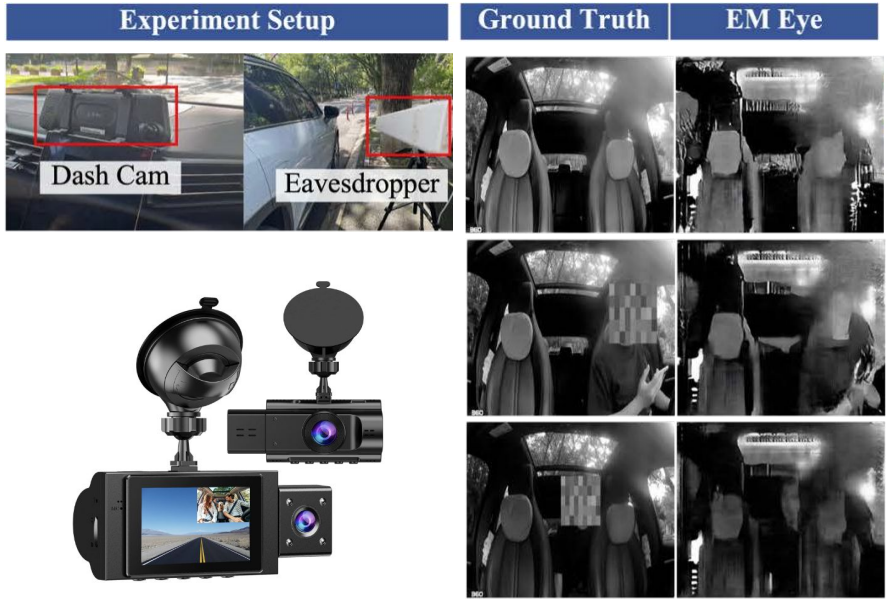


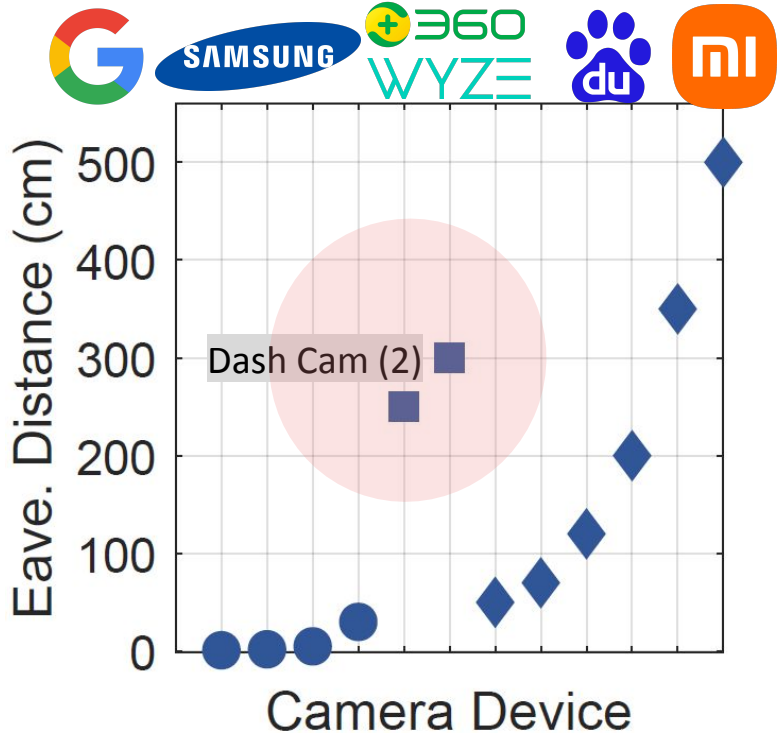
Susceptible Devices: Home Cams



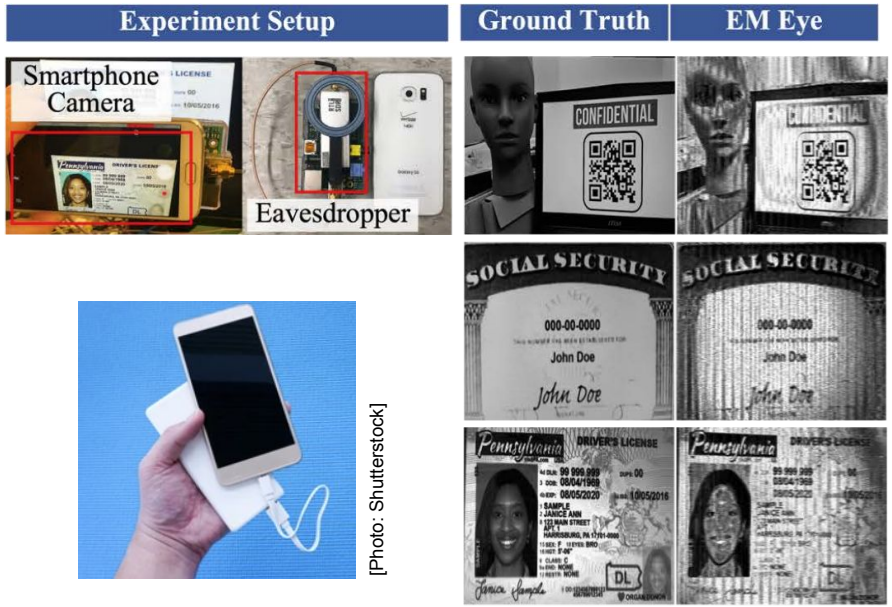


Susceptible Devices: Dash Cams

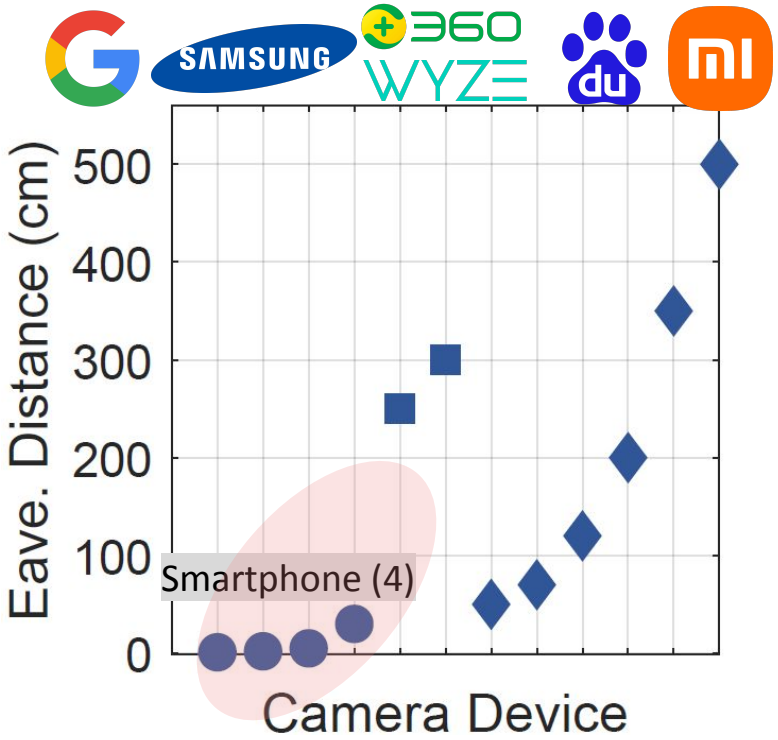




Susceptible Devices: Smartphone Cams



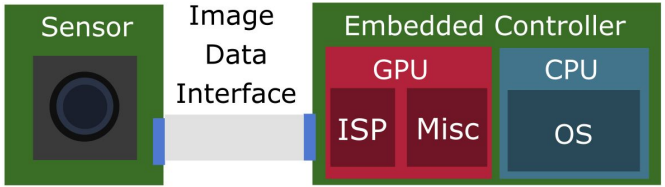
[Photo: Shutterstock]

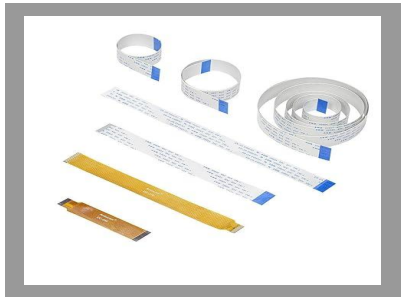


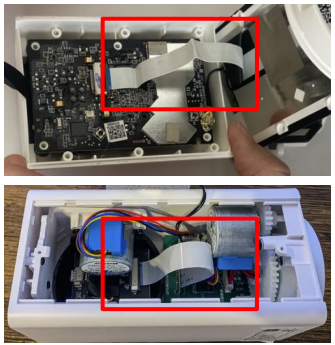
Factors & Mitigation: Shorter Cables

Reconstruction with Different

Cable Length @ Antenna-camera Distance



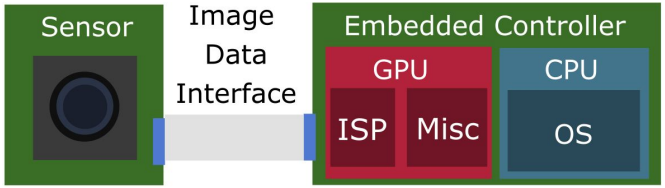


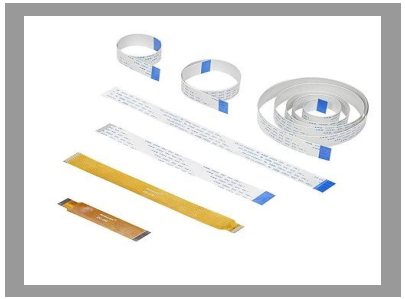


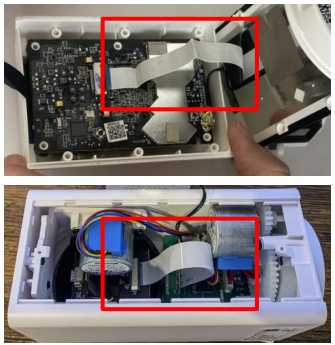
Factors & Mitigation: Better Shielding

Reconstruction with Different Cable Shielding Types

[Photo: Adobe Stock]

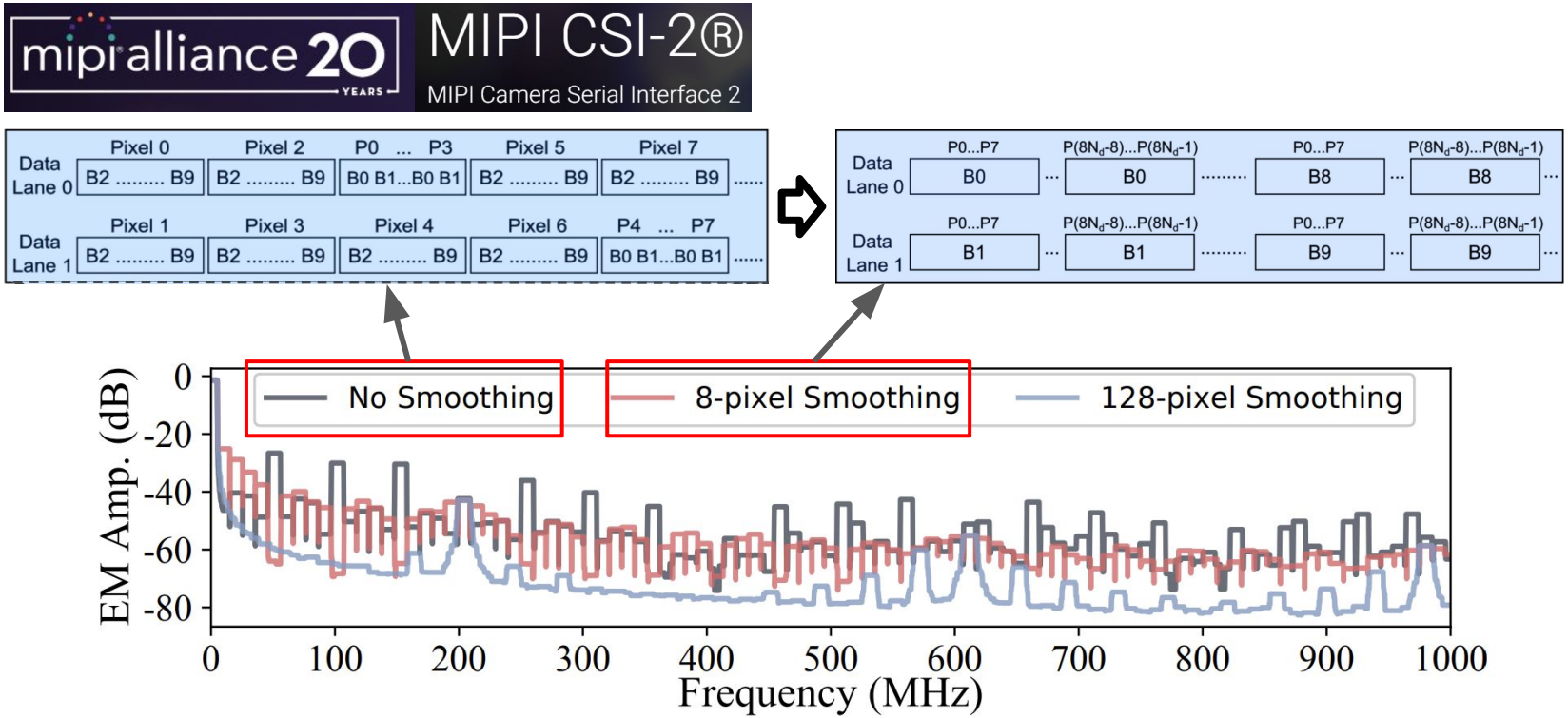






Factors & Mitigation: Better Shielding

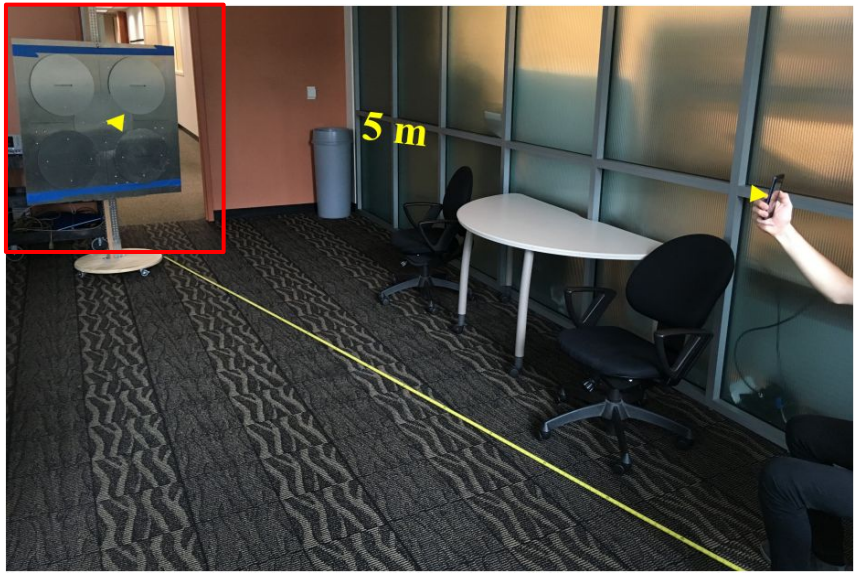
Factors & Mitigation: Minimize Bit Transitions



Yan Long | yanlong@umich.edu

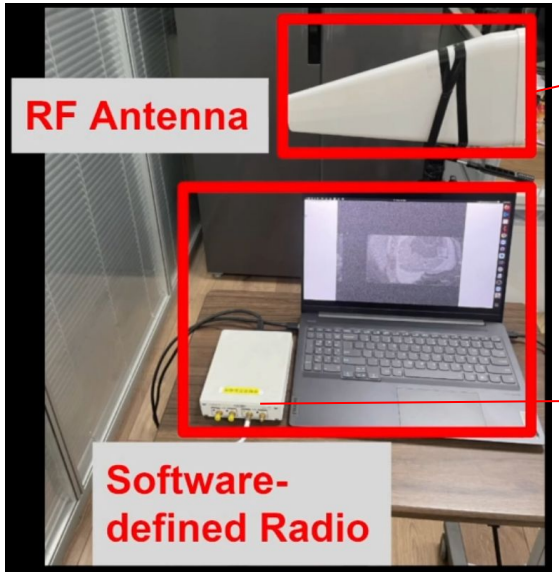
Discussion: Distance

Lab Customized Receiver



[Yilmaz et al., IEEE MILCOM 2019]

COTS Receiver



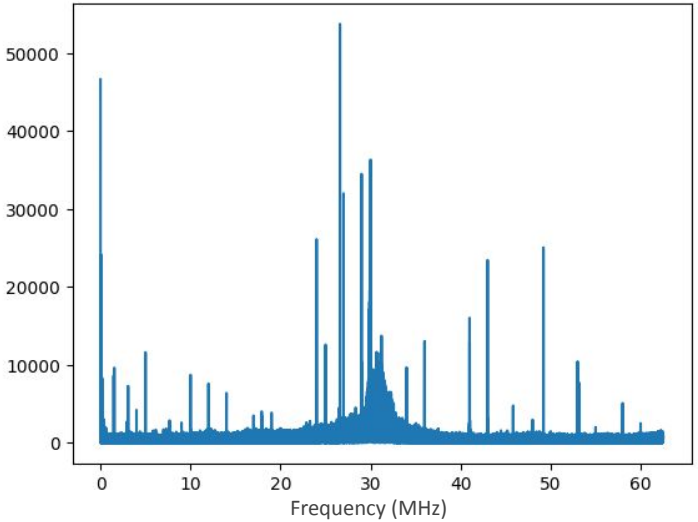
$15 on Amazon

$30 to $2000

[EM Eye]

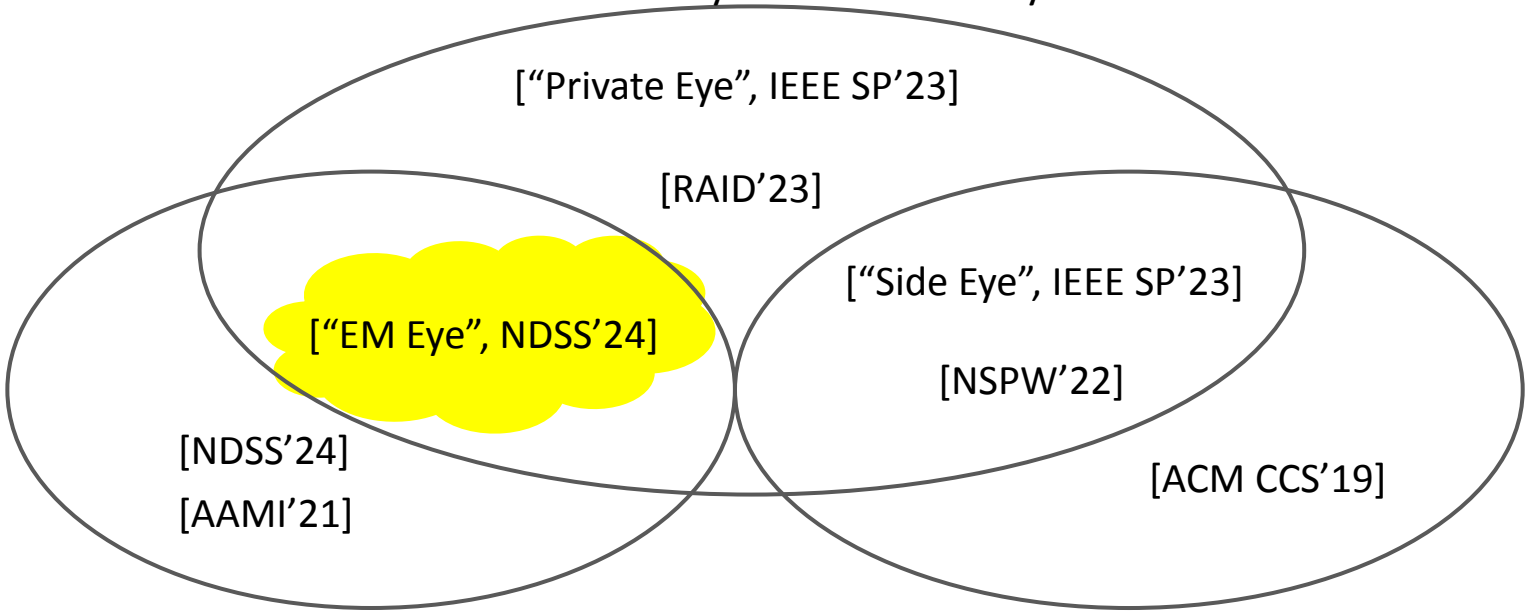
Discussion: Encoded Image Transmission

- Simple FFT-LDA (spectral) features
- >90% accuracy recognizing 100 scenes



Discussion: Bigger Picture

Leakage Channels:
Data Security and User Privacy



Injection Channels:
CPS Infrastructure Security and Safety

Novel Sensing Channels:
Multimodal Sensing for Authentication

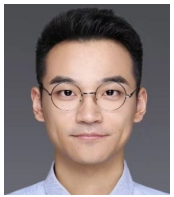
Summary

- EM leakage from cameras allows reconstructing image streams.
- Both hardware and software designs of existing systems can/should be improved.
- Better not DIY your own home security cameras……

Team


Yan Long


Qinhong Jiang


Chen Yan


Tobias Alam


Xiaoyu Ji

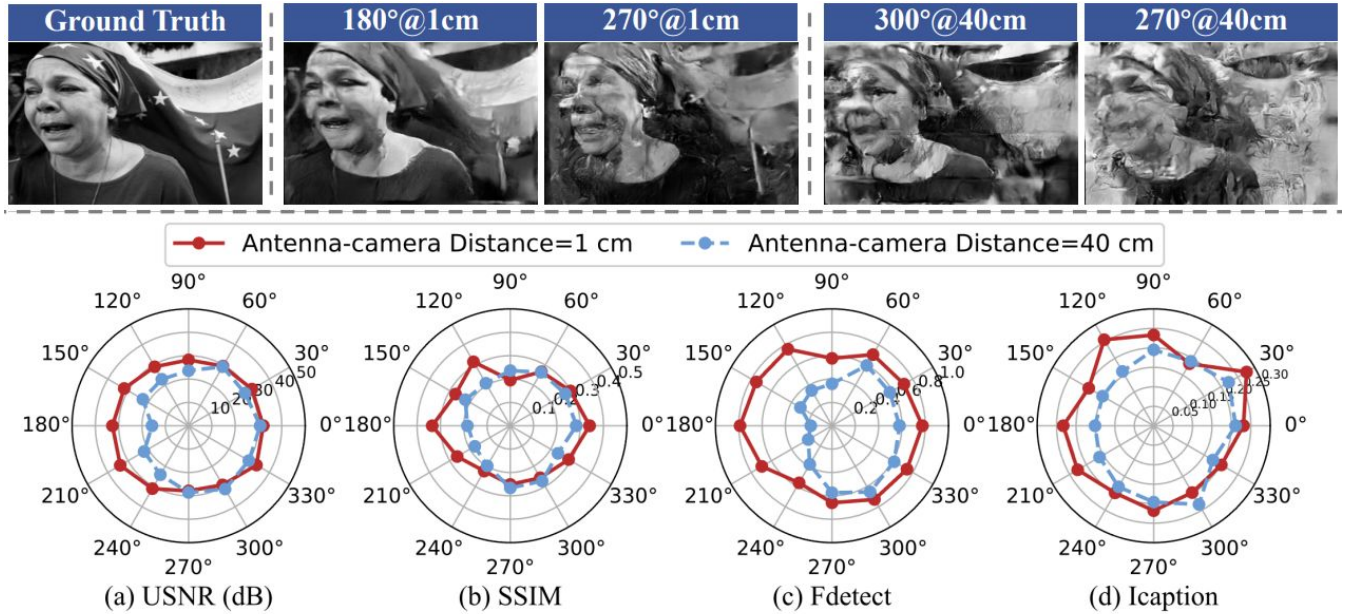

Wenyuan Xu


Kevin Fu

https://emeyeattack.github.io/Website/

Color

Angle



Yan Long | yanlong@umich.edu

Analog Filtering

Protocol	Frequency Band	Protocol	Frequency Band
GSM	880 - 960~MHz	Wi-Fi	2.4~GHz and 5~GHz
3G	800 - 2100~MHz	ZigBee	915~MHz and 2.4~GHz
LTE	700 - 2600~MHz	LoRa	868~MHz and 915~MHz
5G	850~MHz, 1900~MHz 1850 - 1990~MHz	NB-IoT	824 - 849~MHz, 869 - 894~MHz
Bluetooth	2.4~GHz	Z-Wave	868.42~MHz and 908.42~MHz